

UNIVERSIDADE FEDERAL DO MARANHÃO
Programa de Pós-Graduação em Ciência da Computação

Hans Newton Fonseca Cantanhede

MeviDoS: Uma metodologia para Análise Forense em Redes de Computadores com foco em Ataques de Negação de Serviço

São Luís
2020

HANS NEWTON FONSECA CANTANHEDE

MeviDoS: Uma metodologia para Análise Forense em Redes de Computadores com foco em Ataques de Negação de Serviço

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação da UFMA, como requisito parcial para a obtenção do grau de Mestre em Ciência da Computação.

Orientador: Samyr Béliche Vale (Orientador)

Doutor em Informática - UFMA

São Luís

2020

Ficha gerada por meio do SIGAA/Biblioteca com dados fornecidos pelo(a) autor(a).
Núcleo Integrado de Bibliotecas/UFMA

CANTANHEDE, HANS NEWTON FONSECA.

MeviDoS: Uma metodologia para Análise Forense em Redes de Computadores com foco em Ataques de Negação de Serviço / HANS NEWTON FONSECA CANTANHEDE. - 2020.

106 p.

Orientador(a): SAMYR BÉLICHE VALE.

Dissertação (Mestrado) - Programa de Pós-graduação em Ciência da Computação/ccet, Universidade Federal do Maranhão, SAO LUIS, 2020.

1. Análise Forense em Redes de Computadores. 2. Arquitetura Computacional. 3. Ataque de Negação de Serviço. 4. Lei de Crimes Informáticos. 5. Metodologia de Auxílio. I. VALE, SAMYR BÉLICHE. II. Título.

HANS NEWTON FONSECA CANTANHEDE

MeviDoS: Uma metodologia para Análise Forense em Redes de Computadores com foco em Ataques de Negação de Serviço

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação da UFMA, como requisito parcial para a obtenção do grau de Mestre em Ciência da Computação.

Aprovado em 23 de Abril de 2020

BANCA EXAMINADORA

Samyr Béliche Vale (Orientador)

Doutor em Informática - UFMA

Francisco José da Silva e Silva

Doutor em Ciência da Computação - UFMA

Paulo Antonio Leal Rêgo

Doutor em Ciências da Computação - UFC

*"Dedico a todos que me apoiaram e
acreditaram
na minha capacidade para realizar este
trabalho"*

Agradecimentos

Primeiramente quero agradecer a **Deus** pelo dom da vida e por me dar toda a vontade e a sabedoria para escrever.

Ao meu orientador Prof. Dr. Samyr Béliche Vale, pela paciência, constante apoio, incentivo, dedicação e amizade essenciais para o desenvolvimento deste trabalho e para o meu desenvolvimento como pesquisador.

Agradeço a toda a minha família e meus amigos que sempre se fizeram presentes na minha vida e ajudaram direta ou indiretamente no apoio durante todo o curso de Mestrado.

A todos, os meus sinceros agradecimentos.

*“Muitos me perguntam
qual o segredo para o meu sucesso...
Existem apenas duas regras:
1: Trabalhe pra valer;
2: Nunca ouça aos que só dizem não.”
(Arnold Schwarzenegger)*

Resumo

O problema abordado neste trabalho é a dificuldade encontrada em responsabilizar agentes infratores de ataques de negação de serviço nas infraestruturas e demais sistemas de redes de computadores do Brasil. Com o advento da Lei 12.737 de 2012 no Brasil, conhecida como Lei de Crimes Informáticos, esses ataques são considerados crimes. É necessário, portanto, a identificação dos elementos que tipificam a atividade maliciosa como criminosa e a elaboração de procedimentos que auxiliem nessa tipificação para responsabilização de agentes infratores de crimes em meio informático. No entanto, nenhum procedimento foi encontrado, para servir de apoio aos operadores do direito, na aplicação da lei ao caso concreto. Nesse contexto, este trabalho propõe então a metodologia MeviDoS, à luz da Lei de Crimes Informáticos de 2012, para a análise forense de redes de computadores, com foco em evidenciar os elementos para responsabilização de agentes infratores que cometem ataques de negação de serviço, além de apresentar uma arquitetura computacional para automatizar suas etapas. Para tanto, foi promovida uma revisão dos trabalhos relacionados e também seções dedicadas ao esclarecimento dos termos e tecnologias necessárias para contextualizar a pesquisa. Este trabalho também apresenta a metodologia constituída de suas etapas, além da arquitetura para realizá-las e os resultados dos experimentos utilizados para validar a metodologia. Concluiu-se que o acesso aos elementos necessários para formalização da responsabilização do agente infrator como: a origem, o destino, a técnica utilizada, o tempo e lugar do crime podem ser descobertos mediante utilização da metodologia MeviDoS proposta. Demonstrando assim que a autoridade da investigação pode prosseguir com a responsabilização, devidamente fundamentada, dos agentes infratores que cometem ataques de negação de serviço.

Palavras-chave: análise forense em redes de computadores; metodologia; ataque de negação de serviço; lei de crimes informáticos 12.737 de 2012 no Brasil; arquitetura computacional; investigação forense digital

Abstract

The problem addressed in this work is the difficulty in holding agents responsible for making denial of service attacks in Brazil's network infrastructures and systems. With the advent of Law 12,737 of 2012 in Brazil, known as the Computer Crimes Law, these attacks are considered crimes. It is therefore necessary to identify the elements that characterize the malicious activity as criminal and that there are procedures that assist in this clarification for the accountability of criminal offenders in computerized media. However, no procedure was found to support the operators of the law in applying the Computer Crimes Law to the specific case. This paper proposes, therefore, the MeviDoS methodology enlightened by Computer Crimes Law of 2012 for forensic analysis of computer networks, with a focus on highlighting the elements of accountability for offending agents who commit denial of service attacks, in addition to presenting a computational architecture to automate its steps. To this end, a review of related works and sections dedicated to clarifying the terms and technologies necessary to contextualize the research were promoted. This work also presents the methodology constituted of its stages, the architecture to accomplish those stages and the results of the experiments carried out to validate the methodology. It is concluded that the access to the necessary information to formalize the accountability of the offending agent, such as: the origin, the destination, the technique used, the time and place of the crime can be discovered using the proposed MeviDoS methodology. Thus demonstrating that the investigating authority can proceed with the duly substantiated accountability of the offending agents who commit denial of service attacks.

Key-words: computer network forensic analysis; methodology; denial of service; Brazil's computer crime law 12,737 of 2012; computer architecture; digital forensic investigation

Lista de Siglas

AI *Artificial Intelligence* - Inteligência Artificial

Cert.br Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CNJ Conselho Nacional de Justiça

CPU *Central Process Unit* - Unidade Central de Processamento

DDoS *Distributed Denial of Service* - Negação de Serviço Distribuído

DFRWS *Digital Forensics Research Workshop* - Workshop de pesquisa forense digital

DMZ *Demilitarized Zone* - Área Desmilitarizada

DNS *Domain Name Server* - Servidor de Domínio

DoS *Denial of Service* - Negação de Serviço

EEDI *End-to-End Digital Investigation* - Investigação Digital Fim-a-Fim

FTK *Forensic Toolkit* - Kit Ferramental Forense

HTTP *Hypertext Transfer Protocol* - Protocolo de Transferência de Hipertexto

IDS *Intrusion Detection System* - Sistema de Detecção de Intrusos

IP *Internet Protocol* - Protocolo de Internet

IPED Indexador e Processador de Evidências Digitais

ISP *Internet Service Provider* - Provedor de Serviços de Internet

IoT *Internet of Things* - Internet das Coisas

LAN *Local Area Network* - Redes Locais

POP Procedimento Operacional Padrão

RAM *Random Access Memory* - Memória de Acesso Aleatório

SQL *Structured Query Language* - Linguagem de Consulta Estruturada

SMTP *Simple Mail Transfer Protocol* - Protocolo de Transferência de Correio Simples

SSL *Secure Socket Layer* - Camada de *socket* segura

UDP *User Datagram Protocol* - Protocolo de Datagrama do Usuário

TCP *Transmission Control Protocol* - Protocolo de Controle de Transmissão

TSK *The Sleuth kit*

VoIP *Voice over Internet Protocol* - Voz sob o Protocolo de Internet

Lista de Figuras

2.1	Cenário habitual de uma rede de computadores corporativa	29
2.2	Comparação entre abstração, de serviços e portas, e exemplo real	31
2.3	Exemplo de ataque de SQL <i>injection</i>	33
2.4	Exemplo de ataque de negação de serviço distribuído	33
2.5	Macroprocesso do evento que deixa vestígios até a sentença do crime	34
2.6	Hierarquia de algumas áreas da criminalística	37
2.7	Regra do IDS para alertar ataques de negação de serviço	43
2.8	Alerta sinalizado pelo Snort através da correlação da regra do IDS com o comportamento do ataque de negação de serviço	44
3.1	Visão geral do autopsy	47
4.1	Fluxo abstrato para implementação da arquitetura computacional	59
4.2	Arquitetura da Solução Proposta	60
4.3	Arquitetura de testes usada nos experimentos	64
4.4	Cenário <i>online</i> dos experimentos	66
4.5	Cenário <i>offline</i> dos experimentos	66
4.6	Diagrama de classes da arquitetura implantada	68
4.7	Modelagem ER da arquitetura implantada	69
4.8	Exemplos de regras de associação.	70
4.9	<i>Workflow</i> para experimentos	71
4.10	Regra para captura de atividades maliciosas pelo IDS	72
4.11	Regras para correlação de crimes e danos utilizadas pelo captor forense	72
4.12	Simulação de usuário através do JMeter para experimento 1	75

4.13	Arquivos de saída slowhttp.csv e slowhttp.html gerados pela ferramenta slowhttpstest após execução	75
4.14	Execução comando da ferramenta goldeneye	76
4.15	Simulação de usuário através do JMeter para experimento 1	77
4.16	Mapeamento evidências encontradas com marcações conhecidas no CIC DoS <i>dataset</i>	79
4.17	Relatório experimento 3 obtido pelo Captor Forense	80
4.18	Mapeamento evidências encontradas com marcações conhecidas no CIC IDS <i>dataset</i>	81
4.19	Relatório experimento 4 obtido pelo Captor Forense	82
4.20	Simulação de usuário através do JMeter para experimento 5	82

Lista de Tabelas

2.1	Exemplos de número de portas comuns e seus serviços correspondentes . . .	31
2.2	Informação extraída do alerta do IDS	44
3.1	Exemplo de evidências digitais voláteis e não voláteis	49
3.2	Tabela comparativa de trabalhos relacionados	52
4.1	Elementos principais, resultados e motivação identificados sobre o artigo 266 da lei 12.737	56
4.2	Modelo de caracterização do crime	58
4.3	Modelo de comportamento da atividade maliciosa	58
4.4	Mapeando elementos principais e exemplos de atividades maliciosas	62
4.5	Modelo de comportamento da atividade maliciosa com exemplo de extração de alerta de IDS	63
4.6	Detalhamento das máquinas virtuais e seus objetivos	65
4.7	Fontes de evidência	65
4.8	Vantagens e fraquezas dos cenários pensados	67
4.9	Métricas e sua fonte de evidência mapeadas	70
4.10	Resumo da características dos a serem observadas nos experimentos após realização	71
4.11	comando slowris, com parâmetros utilizados	74
4.12	comando goldeneye, com parâmetros utilizados	76
4.13	Comando executado para experimento 3	78
4.14	Comando executado para experimento 4	80
4.15	Comando hulk.py, com parâmetros utilizados	81

5.1	Sumarização das respostas dos resultados	86
5.2	Sumarização de métricas coletadas durante a execução dos experimentos segundo o modelo de crime	87
5.3	Sumarização de resultados de experimentos	87

Sumário

Lista de Siglas	10
Lista de Figuras	12
Lista de Tabelas	14
1 Introdução	19
1.1 Objetivos	26
1.2 Organização do Trabalho	27
2 Fundamentação Teórica	28
2.1 Serviços e portas	30
2.2 Vulnerabilidades e ataques	32
2.3 Do crime à responsabilização	34
2.4 Crimes digitais no Brasil e no exterior até 2012	35
2.5 Lei de crimes informáticos e os elementos utilizados pela ciência forense	36
2.6 Computação Forense	39
2.7 Ferramentas para identificação de atividades maliciosas em redes	41
2.8 Ataques cibernéticos criminosos à margem da lei	42
2.8.1 Constatação de ataques DoS	43
3 Trabalhos Relacionados	45
3.1 Classificação de ataques cibernéticos	45
3.2 Ferramentas de análise de evidências digitais	46
3.3 Datasets para testes de IDS	48

3.4	Evidências em redes de computadores	49
3.5	Metodologias genéricas para análise forense	50
3.6	Procedimento operacional padrão para análise de DoS	50
3.7	Considerações finais	51
4	MeviDoS: (Metodologia para Evidência de Ataques DoS)	53
4.1	Metodologia Aplicada	54
4.2	Modelo de dados	55
4.3	Arquitetura computacional	59
4.4	Identificação das atividades maliciosas e captura de alertas sinalizados pelo IDS	61
4.5	Associação das atividades maliciosas ao modelo	61
4.6	Tipificação	62
4.7	Experimentos	63
4.8	Fluxo de execução dos experimentos	71
4.9	Cenário experimento 1	73
4.10	Cenário experimento 2	76
4.11	Cenário experimento 3	78
4.12	Cenário experimento 4	79
4.13	Cenário experimento 5	81
4.14	Considerações Finais	83
5	Resultados	85
5.1	Discussão	88
6	Conclusão, Publicações e Trabalhos Futuros	90
6.1	Publicações	90
6.2	Trabalhos Futuros	91

Referências Bibliográficas	92
A Apêndice	100
A.1 Relatório experimento 1	100
A.2 Relatório experimento 2	101
A.3 Relatório experimento 3	102
A.4 Relatório experimento 4	104
A.5 Relatório experimento 5	105

1 Introdução

Vive-se um momento em que um dos bens mais valiosos é a informação. Chamada de 4ª Revolução Industrial, a predominância de produções digitais, vínculos por redes sociais e softwares como um serviço são objeto de interesse para as empresas, pois o entendimento das suas relações e de seus consumidores pode aumentar sua produtividade, eficiência e alcance (SCHWAB, 2018). *Internet of Things* - Internet das Coisas (IoT), Sistemas Ciberfísicos, *Artificial Intelligence* - Inteligência Artificial (AI), *Big Data* e Computação em Nuvem são áreas da computação que têm surgido com o objetivo de resolver problemas, de maneira eficiente, com agilidade, em busca de sustentabilidade (CHEN, 2017). Os produtos e serviços digitais dessa nova revolução podem envolver vários ativos que são vitais para o funcionamento das áreas citadas. Um ativo, na perspectiva contábil, é um patrimônio, ou seja, um bem ou direito da empresa que possui valor para esta (BASTOS, 2018). Para redes de computadores, os ativos são os equipamentos de rede e os serviços por eles fornecidos, tais como: firewall, servidores, switches, roteadores, dentre outros que, além do valor patrimonial, armazenam informações valiosas para as mais diversas empresas e instituições (LEITE, 2018), (MOLINA et al., 2019). Sob a perspectiva do direito, o ativo é um bem jurídico tutelado, protegido por lei, sujeito a sanções penais em caso de crime (AZEVEDO; NETO, 2018).

Os ativos, na perspectiva de redes de computadores, podem conter vulnerabilidades, que são falhas devido à má configuração ou programação dos equipamentos. Exemplos de vulnerabilidades são: a autenticação quebrada, ou seja, a possibilidade de acessar dados de usuários presentes em sessões do navegador web devido a falhas na programação desses serviços; ausência de um antivírus, no momento de baixar um arquivo ou programa contaminado, contendo uma *backdoor*; página da internet manipulada para roubar informações, sendo redirecionada para o atacante, através de uma modificação do serviço de tradução de endereços web; indisponibilidade de serviço, pelo grande volume mal intencionado de requisições, causando sobrecarga e impossibilitando novas requisições de serem respondidas; e a recuperação de informações pessoais, de forma não autorizada, utilizando comandos específicos, não bloqueados pelo administrador do sistema (OWASP, 2017).

Essas vulnerabilidades são exploradas através de ataques cibernéticos, como: injeção

de *Structured Query Language* - Linguagem de Consulta Estruturada (SQL), *Denial of Service* - Negação de Serviço (DoS), exposição de dados sensíveis, manipulação de páginas da internet, roubo de informações e segredos industriais. Esses ataques somados à falta de monitoramento, ao registro de atividades ocorridas e ao anonimato na internet proporcionam, juntamente, um sentimento de impunidade aos agentes infratores (OWASP, 2017).

Nos últimos anos tem crescido o número de ocorrências de ameaças cibernéticas no Brasil. Martines e Coelho (2019) apresentaram uma notícia em que o Conselho Nacional de Justiça (CNJ) sofreu um vazamento de dados, na manhã de primeiro de abril de 2019, no qual foram divulgados nomes completos, números de contas bancárias, telefones, CPFs e senhas de pessoas que já utilizaram os serviços do CNJ. Outra notícia da revista Veja informa que *hackers* se passaram pela Netflix, enviando uma mensagem de atualização de dados, com ameaça de perda de assinatura, objetivando identificar e coletar e-mails ativos e válidos, para serem utilizados em futuras campanhas maliciosas (ROMANI, 2019). Segundo a Symantec, entre 2017 e 2018, o Brasil subiu para terceiro lugar no ranking de países que mais sofrem ataques cibernéticos em dispositivos conectados a internet (SCHNEIDER, 2019).

Além das ameaças já citadas, o Brasil é confrontado com outras variações de ameaças cibernéticas, tais como: fraudes online, crime cibernético e vigilância digital. Em um relatório sobre atividades *botnet*, da Kaspersky Lab, no primeiro semestre de 2018, que analisa mais de 150 famílias de *malwares* (*Malicious Software* - Programas Maliciosos) e suas modificações, é destacado que o Brasil é líder de participação em redes de computadores zumbi, do *malware* Njrat, que configura uma *backdoor* no computador infectado, permitindo a criação de uma *botnet* com o mínimo de conhecimento técnico da ferramenta, facilitando assim a disseminação de *malwares*, ataques *Distributed Denial of Service* - Negação de Serviço Distribuído (DDoS) e *spam* (KASPERSKY, 2018).

A fabricante de antivírus Symantec publicou, em um Relatório sobre Ameaças à Segurança na Internet, que o ano de 2017 foi marcado pela descoberta de fragilidades e ataques *hacker*, não somente de grupos independentes, mas de grupos organizados e mesmo governos que exploram vulnerabilidades de sistemas. Segundo estudo feito, via questionários *online*, projeção e coleta de dados de outras fontes pela empresa, 44% dos seus consumidores haviam sofrido algum contato com crimes cibernéticos nos últimos 12 meses. No ano de 2017, mais de 62 milhões de pessoas no Brasil foram afetadas por

crimes digitais e mais de 22 bilhões foram roubados por meio de crimes digitais no Brasil. Os crimes mais frequentes envolviam aparelhos infectados por vírus, senhas de contas online descobertas, emails fraudulentos ou compras online em sites falsos (FÁBIO, 2018). Apesar dessa situação, os cidadãos são pouco informados de como responder numa situação semelhante. Um grande desafio para as empresas e governos é antecipar e rastrear ameaças cibernéticas (DINIZ et al., 2014).

O crescimento da popularização dos dispositivos de IoT está na mira dos atacantes. Com uma população de mais de 210 milhões de habitantes, 70% dos brasileiros acessa internet, existem mais de 257 milhões de dispositivos móveis que são utilizados diariamente para acesso à internet (STATS, 2018). É comum que países com grande número de pessoas conectadas à internet liderem *ranks* de ciberataques (SCHNEIDER, 2019).

O DoS e DDoS são outros exemplos de ataques com ocorrências crescentes (GUPTA; BADVE, 2016), e vários usuários ou fornecedores de serviços não sabem que estão sofrendo esse ataque, por não investirem em algum tipo de monitoramento. A motivação do ataque, apesar de muitas vezes subjetiva, deve ser explicada para fundamentar sua ocorrência (MAUÉS, 2016). Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.br) (CERT.BR, 2019), seu relatório anual tem apresentado que o DoS é um dos principais incidentes de segurança contabilizados, sendo 23,42% em 2018 e 34,42% dos incidentes em 2019.

Casos do vírus do tipo *ransomware*, conhecido como WannaCry em 2017, se disseminaram no Brasil mediante uma vulnerabilidade no sistema operacional *Windows*. Um *worm* executava um conjunto de comandos para se copiar, sem a interação do usuário. Apesar da correção de segurança para esta falha já existir, muitos administradores de sistemas demoraram a perceber a falha. Como resultado, diversas empresas e órgãos governamentais, como o Instituto Nacional do Seguro Social, tiveram seu serviço interrompido e pessoas comuns tiveram seus dados criptografados, sendo solicitado um resgate na moeda *bitcoin* para descriptografar seus dados (RODRIGUES, 2018). Em 2019, um caso relatado foi a invasão de informações do aplicativo Telegram, nos celulares de procuradores da operação Lava Jato, mediante uma falha no serviço de telefonia, que permitia que uma chamada *Voice over Internet Protocol* - Voz sob o Protocolo de Internet (VoIP) acessasse a caixa postal. Através uma sobrecarga de ligações para o telefone, por meio do serviço VoIP, o código de ativação do Telegram foi enviado para a caixa postal do número, dessa forma, o invasor conseguiu, mediante a falha no serviço, descobrir o código de acesso, e assim

acessar as mensagens da vítima(UOL, 2019).

A segurança da informação está presente nos requisitos e planejamentos de serviços (LANDAUER et al., 2018). A utilização de tecnologias como *Intrusion Detection System* - Sistema de Detecção de Intrusos (IDS), que são responsáveis por realizar um monitoramento da rede (LATHA; PRAKASH, 2017), (ELDOW et al., 2016), demonstra uma tentativa de garantir os princípios da segurança da informação: privacidade, integridade, confiabilidade, disponibilidade e o não repúdio. O IDS propõe resolver o problema de identificar uma atividade maliciosa através de módulos com focos específicos: o módulo de monitoramento na aquisição dos dados da rede; o módulo máquina de detecção, que realiza a correlação entre as regras configuradas com os dados obtidos pelo módulo anterior; e um módulo sistema de saída de alertas, que sinaliza o casamento positivo entre a atividade maliciosa conhecida e previamente configurada (ROESCH, 1999). Através da escrita de regras para o IDS e sua utilização, é possível a correlação entre os dados que trafegam no fluxo da rede monitorada e o que se diz ser malicioso. Percebe-se a necessidade de conhecimento especializado por parte daquele que criará regras para identificação de atividades maliciosas.

A infraestrutura de segurança das empresas, moldada nos princípios da segurança da informação, é muitas vezes analisada com intenções prejudiciais. Agentes infratores, conhecidos como *crackers*, aproveitam-se das vulnerabilidades nos serviços, aplicações ou comunicações que operam na internet com más intenções no sentido de causar danos como furto de dados, indisponibilidade de serviços ou destruição de dados.

As estatísticas desses crimes, que utilizam computador como meio, têm crescido, provavelmente, pelo sentimento de impunidade dos agentes infratores. A própria mídia tem relatado vários casos de empresas como o do Facebook e a empresa Cambridge Analytica (CADWALLADR; GRAHAM-HARRISON, 2018), ou no caso da Google e a divulgação de dados pessoais da sua ferramenta Google+ (WAKABAYASHI, 2018), no entanto, dificilmente observa-se responsabilização de agentes infratores (OLIVEIRA; DANI, 2011), quanto a esses crimes, provavelmente por carência de dispositivos penais que tipifiquem essas atividades como criminosas. O OWASP (2017) é um documento de boas práticas para desenvolvedores e profissionais de segurança de aplicativos da web, no qual as primeiras dez vulnerabilidades mais contabilizadas, em aplicações e de segurança na web, são apresentadas. São elas: injeção de comandos com objetivo de recuperar informações de forma não autorizada, autenticação quebrada, exposição de dados sensíveis, má configuração e falta de monitoramento e registro dos eventos pelas empresas que

mantém serviços informáticos dentre outros riscos são analisados.

Quando as empresas realizam algum tipo de monitoramento, com o objetivo de proteger a rede, a utilização de ferramentas para tal fim, gera um grande volume de dados representados pelos registros dos eventos das aplicações em arquivos (*logs*). Esse grande volume de dados, pode conter informações relevantes, que comprovem a fonte do ataque e os danos causados por atividades maliciosas (MAUÉS, 2016). Assim, essas informações podem auxiliar na responsabilização desses agentes infratores.

No entanto, isso dificilmente acontece (ARASTEH et al., 2007), muitas vezes por lacunas da lei, metodologias ou tecnologias voltadas para esse fim. Os autores SANTANA (2019) e Neto e Rocha (2019) explicam que a impunidade, causada , ou mesmo brechas na lei, que não tipifica tais atividades como criminosas, somada a carência de dos mecanismos de segurança por parte das empresas, motiva e facilita o trabalho dos agentes infratores. Em contrapartida, as consequências para a empresa vítima do ataque existem, os resultados disso são: custos com reparos, instalação de novas infraestruturas, comprometimento da imagem da empresa, havendo contrato de prestação de serviços, podem ocasionar indenizações, necessitando de advogados, ou seja, custos com honorários, como explica a autora Meisner (2018). A mesma autora cita um exemplo hipotético de gastos decorrentes da violação de dados cibernéticos, em um hospital polonês, no valor de R\$ 10.420.185,64 (Valores de referência: 1 USD = 3,25 R\$, 1 USD = 3,4546 PLN, 2018).

Verificou-se um aumento de atividades maliciosas expondo material pessoal como fotos e imagens, por meio de falhas de segurança no computador da vítima (KHAN; HASAN, 2017). No Brasil, criou-se a lei 12.737 de 2012, para criminalizar essas atividades maliciosas e possibilitar a responsabilização de agentes infratores, e assim, assegurar a segurança da informação. Tornou-se possível, a partir da lei conhecida como Lei de Crimes Informáticos, a adequação típica de algumas atividades, em meio informático, como criminosas. Nem todas as atividades maliciosas em meio informático foram tipificadas, no entanto, verifica-se um avanço para responsabilização dos agentes infratores. Dois artigos do Código Penal Brasileiro (Decreto-Lei n. 2.848/1940) são citados neste trabalho: o artigo 154-A, que trata da invasão de dispositivo informático, e o artigo 266, que trata da interrupção de serviços de informação de utilidade pública.

A Ciência Forense, também conhecida como Criminalística, tem como base um formalismo jurídico e um conhecimento cientificamente comprovado com o objetivo de

desvendamento de crimes (STEPHENSON, 2003). A Computação Forense, também conhecida como Ciência Forense Computacional, é uma área que estuda técnicas para análise de evidências digitais no intuito de responder questionamentos feitos por uma autoridade policial ou judicial (JAYAKRISHNAN; VASANTHI, 2018). Uma subárea dela é a Análise Forense em Redes de Computadores que tem seu foco nas evidências coletadas de tráfegos de rede, bem como de *logs* de eventos de aplicações (KHAN et al., 2016).

O quanto antes um ataque for identificado melhor será para diminuição dos danos em uma rede (S.MANGRULKAR et al., 2014). A classificação de ataques cibernéticos que tem como objetivo enquadrar um ataque através de suas características em uma classe, diferenciando assim o tráfego normal da rede do tráfego malicioso, é considerada parcialmente relacionada com a pesquisa. No entanto, não foram encontradas tentativas de classificar atividade maliciosa como criminosa.

Adicionalmente, os autores Jazi et al. (2017) e Sharafaldin et al. (2018) produziram *datasets*, ou seja, bases de dados para área de segurança. Essas bases de dados são reflexo de um monitoramento das comunicações trocadas de um ambiente de testes, durante determinado tempo, com um servidor web representado como vítima, e ferramentas que produzem ataques sob a camada de aplicação, direcionadas ao servidor web, com objetivo de indisponibilizar o serviço. Estas bases simulam tráfego de rede para treinamento de IDS ou ferramentas de classificação de ataques cibernéticos. Verificou-se uma lacuna para base de dados com interesse a auxiliar uma análise forense contendo cenários focados em simular a ocorrência de crimes em redes de computadores, com fins científicos.

Em seguida, foram observadas metodologias genéricas de análise forense digital com o objetivo de produzir um roteiro genérico a ser seguido para qualquer investigação com foco em evidências digitais (STEPHENSON, 2003), (PILLI et al., 2010), (MEROUANE, 2017). Contudo, não foram observadas metodologias que auxiliem uma análise forense em redes de computadores focadas em ataques cibernéticos específicos como o DoS.

Além disso, ferramentas computacionais para auxílio dos especialistas em rede de computadores são propostas, na tentativa de suprir as deficiências das etapas de análise forense como a extração de *logs* de ferramentas de segurança, o armazenamento inteligente do espaço e armazenamento de informações relevantes, assim como a análise de dados, utilizando técnicas para correlação dos dados e facilitar sua visualização (PILLI et al., 2010), (KUMARAVEL; NIRAIISHA, 2013), (LATHA; PRAKASH, 2017). Essas

ferramentas possuem algumas lacunas, a exemplo da identificação positiva da atividade maliciosa, porém, sem conformidade com a lei e com poucas informações para reconhecer tais atividades como criminosas, tendo em vista que não foram construídas para reconhecer legislação criminal.

Dessa forma, notaram-se lacunas, tais como a carência de metodologias para análise forense em redes, ou seja, de um conjunto de etapas logicamente ordenadas com objetivo de comprovar a ocorrência de crime em redes de computadores, e também a ausência de arquiteturas computacionais que auxiliem na responsabilização de agentes infratores de atividades maliciosas, ocorridas em meio informático.

Apesar do IDS rastrear atividades maliciosas, esse registro fica perdido dentro do grande volume de dados que estas ferramentas geram. A identificação dessa atividade maliciosa fica a cargo do especialista em rede que precisa identificar, através de evidências: a autoria, a técnica utilizada para o ataque cibernético, a rede na qual ocorreu o fato e em qual estação de destino, a intenção do autor, o dano causado, e se houve ataque de fato ou tentativa de reação ao ataque, construindo diretivas de segurança para proteger a rede.

Apesar do especialista em redes de computadores ou mesmo o responsável pelo caso ser capaz de identificar as atividades maliciosas, tais profissionais não possuem o conhecimento jurídico necessário para determinar, dentre as atividades maliciosas que ocorreram, quais são crime ou não, nem quais são seus elementos tipificadores, procedimentos para preservação de prova ou subsunção do fato à norma. No processo de investigação realizado pela análise forense, é necessário que haja comunicação por parte do especialista em redes de computadores que deve fornecer as evidências, representadas pelos históricos das ferramentas de detecção de intrusão, para então haver uma análise da ocorrência delitiva. Outro problema é a possibilidade desses dados serem apagados ou perdidos, eliminando assim as provas que poderiam ser obtidas, com a atividade maliciosa ocorrida, em virtude do dinamismo e do volume em que acontece no tráfego de rede.

Após determinada a legislação que embasa a pesquisa, optou-se por selecionar o artigo 266, do Código Penal, que trata de interrupção de serviços, por sua demonstração da tipicidade do DoS como crime e, dado que o DoS é um ataque já demonstrado como bastante reportado e suas consequências negativas, optou-se por sua escolha como foco na pesquisa.

Este trabalho vem preencher essa lacuna entre as duas áreas a saber, direito e

redes de computadores, elaborando uma abordagem metodológica jurídico-computacional que, à luz das determinações legais existentes atualmente no Brasil, a ser utilizada pelos profissionais que realizam perícia na área de informática como peritos criminais, assistentes técnicos e especialistas em redes de computadores questionados em uma instrução penal, permita a identificação dos elementos dos ilícitos cometidos, fazendo a subsunção das referidas atividades com as normas penais, servindo como meio de prova, para a autoridade policial ou judiciária, a fim de culminar em uma efetiva responsabilização dos agentes do fato.

Como contribuições do presente trabalho citam-se a apresentação de uma metodologia pautada nos princípios da computação forense e legislação brasileira que possibilite a evidencia dos elementos que auxiliam na responsabilização de agente infratores de crimes informáticos, com foco na responsabilização do ataque de negação de serviço; a metodologia é implementada através de uma arquitetura computacional que automatiza suas etapas; apresentados experimentos com cenários de ataques de negação de serviço com objetivo de validar a metodologia, sendo estes experimentos submetidos a todas as etapas da metodologia desde a ocorrência do fato até a conclusão obtida.

1.1 Objetivos

Considerando o contexto atual, o objetivo deste trabalho é, a criação de uma metodologia para Análise Forense em Redes de Computadores, com foco em associar os ataques com que as leis brasileiras consideram crime, embasadas primordialmente pela lei de crimes informáticos e assim possibilitar a responsabilização de atividades maliciosas tipificadas por essa lei.

Esta metodologia é composta por fases, dentre elas a elaboração do modelo de comportamentos das atividades maliciosas e do modelo dos crimes informáticos. Seguindo as fases definidas nessa metodologia, é proposta uma arquitetura computacional para automatização dessas fases na qual, mediante a utilização de um IDS para captura, interpretação, geração de alertas e locais de armazenamento de evidências, são feitas correlações para definir o que é crime ou não.

Há portanto a necessidade de descrever o comportamento da atividade maliciosa e contabilizá-lo, bem como caracterizar o que é crime ou não. O modelo de dados deve

auxiliar nessa identificação das atividades maliciosas, que ocorrem na rede de computadores, através do registro e a interpretação das fontes de evidência como *logs* das ferramentas de segurança, IDS e servidores *web*, bem como sua associação com os elementos constitutivos das atividades maliciosas, previstas na lei de crimes informáticos.

A arquitetura forense computacional, proposta para a análise forense em redes de computadores, proporciona a extração de evidência das atividades maliciosas, a correlação dos vestígios encontrados, que formam o modelo dos comportamentos das atividades maliciosas, com o modelo descritivo do crime e, assim, e identifica os elementos do crime necessários à persecução penal: a origem, o autor e o tempo do fato, disponibilizando essas informações de forma que possam ser interpretadas pelas autoridades policiais e judiciárias. Além disso, foram realizados experimentos para validação da arquitetura computacional, com cenários de simulação de ataques de negação de serviço.

1.2 Organização do Trabalho

No capítulo 2, é apresentada a fundamentação teórica necessária para contextualização da pesquisa, definindo conceitos basilares bem como a apresentação da lei utilizada. No capítulo 3, apresentam-se os trabalhos relacionados a pesquisa. No capítulo 4, apresenta-se a solução proposta para o problema, representada pelas etapas da metodologia para análise forense em redes de computadores, focada em ataques de negação de serviço. No capítulo 5, são apresentados os materiais e métodos utilizados para realização dos experimentos, bem como seus cenários detalhados. O capítulo 6, apresenta os resultados da pesquisa e uma breve discussão sobre estes. No capítulo 7, é apresentada conclusão do trabalho, as publicações realizadas e trabalhos futuros.

2 Fundamentação Teórica

Desde sua invenção nos anos 60 a ARPAnet, como era conhecida na época e hoje chamada **internet**, tem evoluído e, nos dias atuais, ela se assemelha a recursos básicos como água e eletricidade. A internet pode ser verificada em áreas (MIRAZ et al., 2018) como o comércio eletrônico, serviços públicos, jogos, educação ou redes sociais, gerando assim, benefícios que vão desde a disponibilização de informação de forma mais rápida, compartilhamento de recursos, até a troca de informações. No entanto, este cenário traz facilidades também para a criminalidade. Quanto mais os serviços e recursos de rede se expandem, tornando os dados mais acessíveis para qualquer usuário que se integre a uma rede, mais vulneráveis esses ativos tendem a se tornar. Uma frágil política de segurança implantada nas infraestruturas de rede pode facilitar a ocorrência de furto ou destruição de dados, interrupção de serviços, estelionatos, transformando o meio digital interconectado em um ambiente ou um alvo de ataques criminosos.

Um cenário habitual, que demonstra uma rede de computadores corporativa, é apresentado na Figura 2.1. Esse cenário contém ativos de rede, que são os elementos físicos ou lógicos presentes em uma rede de computadores, a saber: roteadores, *switches*, servidores *firewalls*, *Domain Name Server* - Servidor de Domínio (DNS), servidor de serviços web, servidor de envio de email, entre outros. A utilização de ativos de rede geralmente implica em algum armazenamento realizado pelos mesmos em *logs*, que podem ser entendidos como ativos de dados. Uma página web, um arquivo de configuração, um email, um arquivo pessoal ou um *log* de evento de sistema ou aplicação são exemplos de ativos de dados que podem ser o objeto de interesse dos agentes infratores. Um *log* de evento é um registro ou um conjunto deles, armazenado em arquivo(s) ou em banco de dados, que contém atividades de aplicações ou do sistema operacional (STUDIAWAN et al., 2019). Juntos são utilizados para documentar as operações ou eventos de entrada ou saída ocorridos para possíveis manutenções, depurações ou análises necessárias.

Percebe-se, também na mesma Figura 2.1, uma divisão em duas áreas: a pública e a privada. A pública representada pelo *link* para acesso à internet, que representa o exterior, com ativos de rede que não são controlados por quem se encontra na rede privada, mas através do *Internet Service Provider* - Provedor de Serviços de Internet (ISP). O roteador

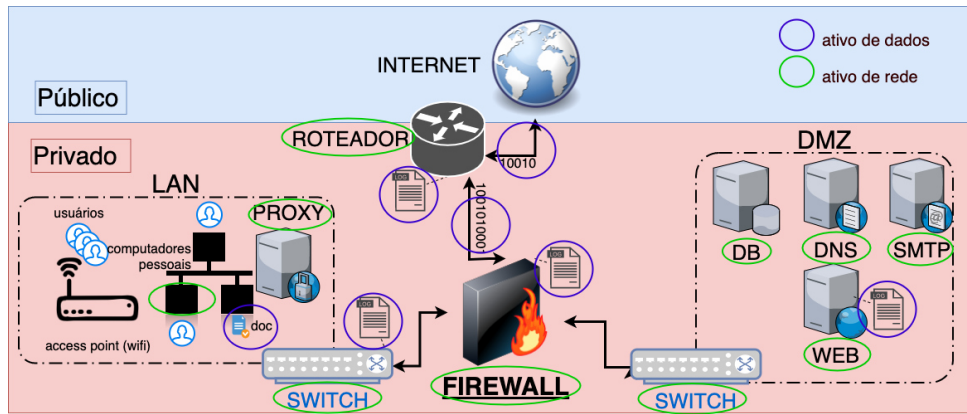


Figura 2.1: Cenário habitual de uma rede de computadores corporativa

que, na fronteira entre a área pública e privada, faz a intermediação da informação entre elas. Na área privada, existe a capacidade de haver um controle e gerenciamento pois, os ativos de rede estão sob um administrador da mesma, assim como na rede pública, também há gerenciamento pelo ISP, no entanto, com a menor flexibilidade que a rede privada pode ter.

A presença de *Local Area Network* - Redes Locais (LAN) cabeadas e sem fio, servidores *firewall*, *web*, DNS e *proxy*, *Demilitarized Zone* - Área Desmilitarizada (DMZ) representam exemplos de ativos de rede na área privada e estes contêm aplicações e sistemas em execução, serviços de acesso a banco de dados, serviço de tradução de domínios, arquivos pessoais, arquivos de configuração, bancos de dados e arquivos de *logs*, os quais representam exemplos de ativos de dados que são geralmente objeto de interesse dos agente infratores. A utilização de ativos de rede com segurança envolve o desafio de garantir os princípios da segurança da informação.

A segurança, em redes de computadores, é caracterizada pela privacidade, integridade, confiabilidade, disponibilidade, não-repúdio e controlabilidade. **Privacidade** indica que a informação na rede não será liberada para usuários não autorizados, entidades ou procedimentos, mas apenas para usuários autorizados. Quando transferindo informação a privacidade precisa ser garantida. **Integridade** significa que a informação pode ser guardada sem ser modificada, sabotada ou perdida durante o processo de armazenamento e transmissão. Integridade garante facticidade, que significa que a informação, mesmo sendo checada por terceiros ou não autorizados, mantém o conteúdo íntegro. **Confiabilidade** indica que o sistema pode realizar funções reguladas com condições estabelecidas e com tempo limitado. Outra característica que remete à confiabilidade é a capacidade de assegurar a comunicação bem como a visualização da informação apenas para pessoas que estejam

autorizadas. **Disponibilidade** mostra que a rede de informação pode ser visitada por entidades autorizadas e utilizada de acordo com sua demanda. O **não repúdio** significa que os participantes não podem negar as operações concluídas. Uma forma de trabalhar com não repúdio é utilizar assinaturas digitais.(CHEN et al., 2010)

A segurança em redes de computadores se preocupa com a prevenção de ataques aos ativos de rede que, por sua vez, contêm ativos de dados, para que não sejam acessados indevidamente, alterados ou mesmo destruídos. Os princípios da segurança da informação anteriormente listados, funcionam como orientações aos profissionais de informática.

Muito da segurança aplicada é baseada na experiência pessoal do profissional, que pode não estar ciente de alguma falha específica ou de novas ameaças que surgem. Geralmente, medidas corretivas incluem, por exemplo, modificar regras de *firewall*, atualizar *software* em ativos na rede, desabilitar serviços do sistema ou modificar uma rotina de autenticação (PURBOYO; KUSPRIYANTO, 2013).

O objetivo da segurança em redes de computadores é, portanto, proporcionar e garantir que o acesso à informação móvel ou estática seja possível apenas às pessoas autorizadas, assegurando os princípios de confidencialidade, integridade e disponibilidade da informação de ativos (ZHENG, 2011).

2.1 Serviços e portas

A diferenciação da comunicação entre os serviços nas redes de computadores se dá através da abstração de protocolos e portas. Não pretende-se aqui explicar detalhadamente o funcionamento das redes de computadores, mas o necessário para entendimento de sua comunicação. Os serviços de rede utilizam protocolos que, por sua vez, como explicam Kurose e Ross (2013), são acordos de procedimentos que devem ser realizados para efetivar a comunicação entre os ativos de rede e entedimento da informação transmitida. Caso um serviço executado em um ativo de rede não utilize o protocolo corretamente, a informação não será garantida.

Ao observar-se o último nível da comunicação ao ponto de transmissão em redes, percebe-se que só existe um canal para compartilhar a informação: os *bits* e *bytes* transmitidos. Resta agora entender como que os diferentes ativos de rede executam diferentes serviços de rede e utilizam o mesmo canal, sem perder ou alterar as informações

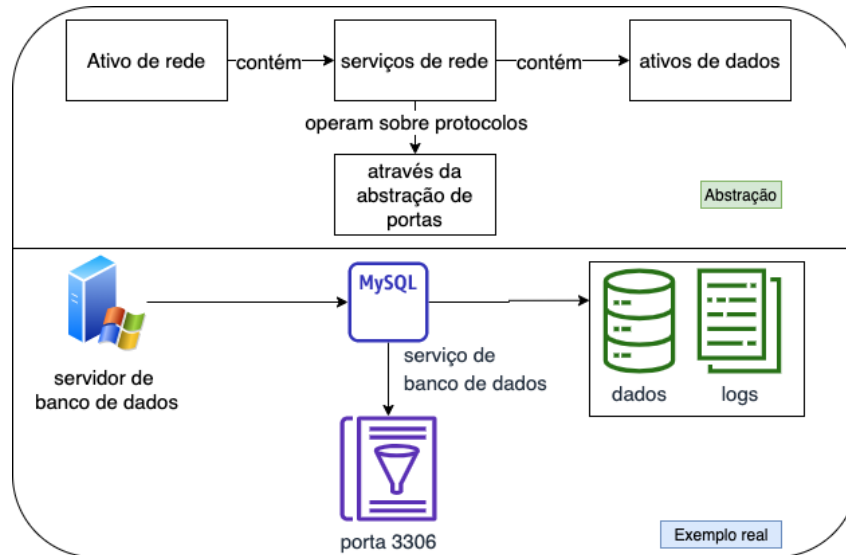


Figura 2.2: Comparação entre abstração, de serviços e portas, e exemplo real

transmitidas. Trata-se da utilização do recurso de portas, um mecanismo que diferencia a informação para cada tipo de serviço. A Figura 2.2 exemplifica esse mecanismo utilizado nas redes de computadores. Fazendo uma analogia com os correios, várias cartas chegam para serem enviadas e o carteiro utiliza o endereço contido nelas para saber em quais casas entregá-las. É possível entender a porta como este endereço lógico que informa ao ativo de rede para qual serviço a informação deve ser transmitida. A Tabela 2.1 apresenta exemplos de números de portas comuns, seus serviços de rede associados em redes de computadores usuais.

<i>Porta</i>	<i>Serviço</i>	<i>Descrição</i>
20,21	FTP	utilizado para transferência de arquivos
22	SSH	possibilita o gerenciamento de serviços da rede de forma segura
23	Telnet	proporciona a comunicação orientada a texto interativo bidirecional utilizando uma conexão de terminal virtual
25	SMTP	utilizado para transferência de emails
53	DNS	possibilita a tradução de IPs para nomes
80	HTTP	proporciona a comunicação de hiper mídias através da internet
443	HTTPS	http seguro
3306	MYSQL	serviço de banco de dados
1433	MYSSQL	serviço de banco de dados seguro

Tabela 2.1: Exemplos de número de portas comuns e seus serviços correspondentes

2.2 Vulnerabilidades e ataques

Existe muita utilidade para a internet de forma positiva, no entanto, existe um lado obscuro, no qual agentes infratores tentam causar problemas no cotidiano, danificando os computadores conectados à internet, violando a privacidade dos usuários ou tornando inoperantes os serviços da rede dos quais dependem (KUROSE; ROSS, 2013).

Os ativos de rede são configurados pelos seres humanos, na tentativa de garantir proteção de dados e organização do funcionamento do ambiente de rede porém, estão sujeitos a falhas e vulnerabilidades causadas em decorrência da má administração ou ainda pelo mal gerenciamento dos ativos pelos seus responsáveis. Muitas vezes, é necessária a abertura de portas para que os serviços sejam disponibilizados, ou seja, é uma vulnerabilidade necessária para que o serviço exista. Contudo, as técnicas contra os ataques devem sempre ser buscadas pelos profissionais responsáveis por administrar a rede.

Os ataques de DoS/DDoS visam esgotar os recursos computacionais de um ativo de rede de forma que ele não seja capaz de responder a uma requisição legítima. Um exemplo deste ataque é o ataque volumétrico, na camada de aplicação, através do protocolo *Hypertext Transfer Protocol* - Protocolo de Transferência de Hipertexto (HTTP). Neste cenário, várias requisições são realizadas a um servidor *web* até que se esgotem seus recursos computacionais como memória, processamento e armazenamento, de forma que as requisições oriundas de usuários legítimos sejam negadas, causando transtornos ou até mesmo danos à infraestrutura focada. A Figura 2.4 mostra um cenário típico de um ataque de negação de serviço.

O ataque injeção de SQL consiste em inserir uma instrução SQL através de uma entrada de dados do cliente, como um navegador da *web*, modificando seu comportamento. Entende-se que o objetivo desta técnica é a recuperação de informações ou até mesmo destruição de informações de forma não autorizada, conforme pode ser exemplificado na Figura 2.3.

Exemplos das consequências da má configuração ou gerenciamento dos ativos são apresentados nas Figuras 2.3 e 2.4. Essas consequências muitas vezes ocorrem pela abertura de portas não seguras ou utilização de senhas fracas ou triviais como nomes comuns, cadeias de números sequenciais, datas de nascimento, ou também quando o agente infrator realiza um grande volume de requisições no sentido de exaurir os recursos do ativo de rede.

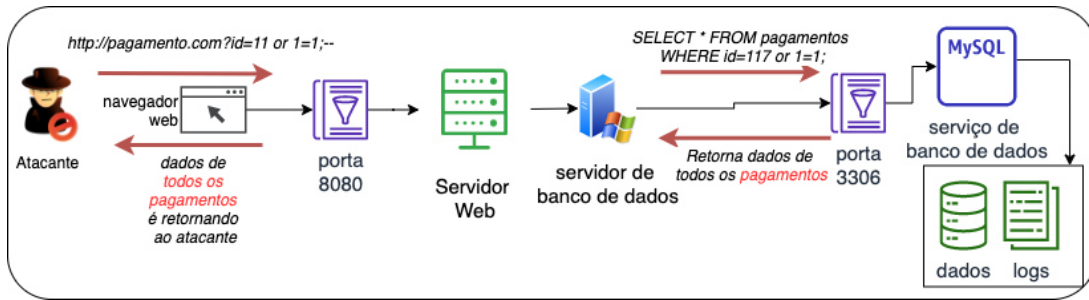


Figura 2.3: Exemplo de ataque de SQL *injection*

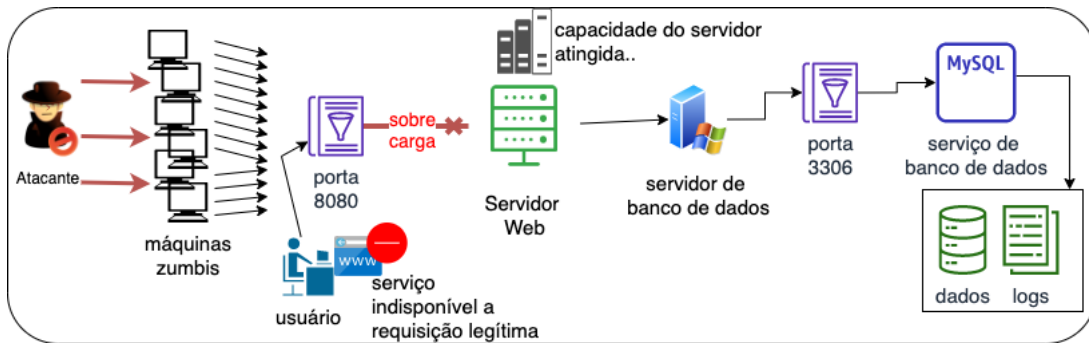


Figura 2.4: Exemplo de ataque de negação de serviço distribuído

Tanto na topologia física (em *hardware*), quanto na topologia lógica (como *software*) podem haver vulnerabilidades e assim serem alvo de ataques. Uma vulnerabilidade é definida como uma falha encontrada, geralmente causadas por erro humano, como a abertura de portas ou fraquezas em um sistema que permitem que intruso execute comandos de forma não autorizada (ABOMHARA; KØIEN, 2015).

Cada serviço opera sobre um protocolo e utiliza uma porta para disponibilizar seu serviço. É através destas portas de comunicações que os usuários externos acessam o serviço. Possibilitando assim que, a partir dessas vulnerabilidades necessárias, ocorram ataques aos ativos de rede.

Os ataques são manifestações dos intrusos com objetivo bem definido, como causar danos a um sistema ou aplicação, roubo ou destruição de informações ou indisponibilizar um serviço explorando suas vulnerabilidades (ABOMHARA; KØIEN, 2015). É necessário frisar que, na computação é difícil encontrar sistemas totalmente a prova de falhas, entretando, o que se busca é a possibilidade de minimizar seus efeitos negativos tanto quanto possível.

Dado que o ataque é uma atividade danosa ou no mínimo prejudicial ela pode ser considerada como atividade criminosa. No Brasil, para que uma atividade seja efetivamente criminosa, ela deve violar princípios constitucionais e penais previstos como o princípio da legalidade, que diz em seu artigo 1º que "*Não há crime sem lei anterior que o defina.* (art

1º, *Código Penal*)" (TRUZZI; DAOUN, 2009), ou seja, que só será considerado crime a atividade expressa em lei e ocorrida após a criação da mesma lei.

2.3 Do crime à responsabilização

Desde a ocorrência da atividade maliciosa, passando por sua constatação, até a responsabilização do agente, quando provada a existência do crime, existem etapas bem definidas que podem ser representadas como ciclos: o policial e o judicial. O ciclo investigador (policial) é aquele que envolve a ocorrência do fato, identificação do vestígio, convocação da autoridade policial ao local do fato, requisição de exames especializados pela perícia e a produção do Inquérito Policial, que formaliza a denúncia. Em sequência, inicia-se o ciclo judicial, no qual o suspeito vira réu ou não. Caso a denúncia seja aceita, a instrução processual é formalmente iniciada e, a partir desse ponto, deve haver alguém que apresenta as evidências do crime ao juiz de direito, garantida a defesa do acusado, eventuais recursos, até o trânsito em julgado e consequente execução da pena. A Figura 2.5 apresenta o fluxo de atividades entre os ciclos policial e judicial, tendo início no fato e culminando na execução penal (RODRIGUES et al., 2010).

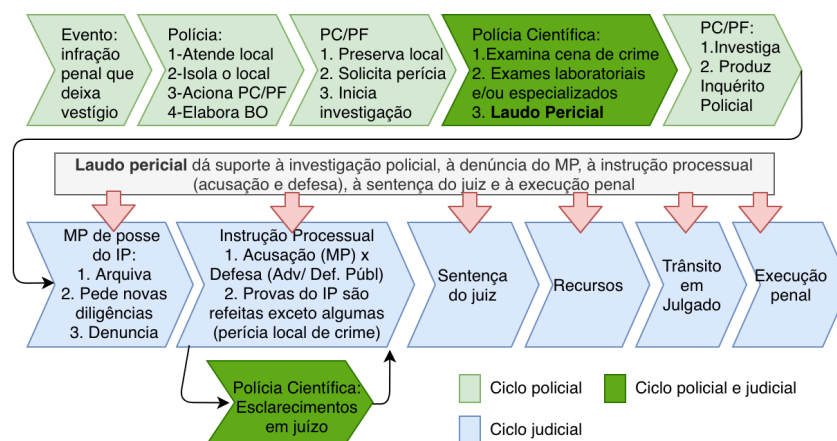


Figura 2.5: Macroprocesso do evento que deixa vestígios até a sentença do crime

Percebe-se também na Figura 2.5 que o Laudo Pericial produzido ao final do primeiro ciclo é subsidiariamente utilizado em todas as etapas do segundo ciclo, quando necessário, mostrando, portanto, a importância do Laudo ser construído com responsabilidade e de tal forma que represente apenas os fatos obtidos dos vestígios, ou seja, a importância da busca pela verdade nos fatos, devidamente fundamentada, para o livre convencimento pelo juiz. E, para produção do Laudo Pericial, surge a figura do perito, detentor da *expertise*

no assunto em questão, que torna-se alguém que auxilia o juiz, trazendo à tona e contando a verdade que está nos vestígios encontrados, mediante exames especializados, dos quais o juiz sozinho não detém conhecimento para realizá-los. (RODRIGUES et al., 2010).

2.4 Crimes digitais no Brasil e no exterior até 2012

A ocorrência de crimes contra a pessoa é uma realidade. No Brasil, narrando (ROCHA, 2013), o Código Penal de 1940 mostra que a lei contra crimes não era focada em crimes virtuais, justamente pelo fato da invenção e disseminação da internet ter acontecido por volta dos anos 70. A maioria dos crimes tipificados refere-se a crimes contra a pessoa como: furto e roubo, racismo, crimes contra a honra. No entanto, percebe-se que esses delitos transcendem o mundo físico, nos dias atuais, e se estendem a um novo ambiente: o virtual.

Segundo Oliveira e Dani (2011), a internet era um espaço em que cresceu a ocorrência de crimes. A sua constante evolução com novas tecnologias bem como a falta de dispositivos legais voltados as suas características, faz com que o ambiente virtual cresça como foco dos agentes infratores tanto como meio, como fim. Considerado um atraso para o Brasil, quando comparado a outros países como: Alemanha e Estados Unidos da América (EUA) que, desde 1986, já possuíam lei específica para delitos digitais, como espionagem e falsificação de dados e a fraude eletrônica, para a Alemanha, e tipificação de atos de transmissão de vírus, para o EUA; a Espanha que, desde 1995, já tipificava várias condutas ilícitas sobre meio informático como: apropriação e interceptação de email; a Argentina que possui em seu Código Penal ou em legislações especiais medidas protetivas dos meios informáticos; Portugal com sua legislação específica conhecida como lei de criminalidade em informática, de 1991. Assim como vários outros países que assinaram a Convenção de Budapeste, definindo crimes praticados pela internet e suas formas de persecução (GATTO, 2011).

Devido ao crescente número de delitos ocorrendo em meio informático, o Brasil deparou-se com a necessidade de tipificação de tais delitos, de forma a conter seus danos.

2.5 Lei de crimes informáticos e os elementos utilizados pela ciência forense

Didaticamente, o crime pode ser definido de três formas: material, formal e analítico. No material, informa-se que é necessário haver um bem jurídico que seja tutelado, ou seja, protegido por lei com sanções penais. No formal, define-se como crime o que a lei disser que é crime, ou seja, a previsão legal. No analítico, tem-se elementos que buscam facilitar o entendimento do que é necessário ocorrer para considerar-se crime, são eles: tipicidade, ilicitude, culpabilidade e punibilidade (NUCCI, 2019). Típico é o fato que se assemelha ao descrito no dispositivo legal. Ilícito é o fato contrário à conduta humana voluntária e o ordenamento jurídico. Culpável é o fato imputável, ou seja, trata-se da consciência do agente infrator sobre o fato. Punibilidade é a possibilidade do agente ser punido pelos seus atos, na forma prevista pela lei.

Segundo Nucci (2019), majoritariamente no Brasil adota-se que, do ponto de vista analítico do crime, um fato típico, ilícito e culpável, ou seja, o agente infrator imputável que realizar um ato ilícito, que possua previsão legal, poderá ser responsabilizado por seus atos. Esse entendimento é suficiente para abordar o contexto da criminalização de atividades informáticas, pois tais elementos devem ser buscados e, se encontrados, há então a materialidade fundamentada.

A Criminalística, segundo Crespo (2012), também conhecida como Ciência Forense, é a disciplina técnico-científica e jurídico-penal e que tem por objetivo a elucidação e prova da infração penal, ou seja, sua materialidade e sua autoria. Existem várias áreas abordadas pela criminalística, portanto, sempre que houver um interesse forense, ou seja, relativo ao desvendamento de crime, provavelmente existirá uma área com especialistas. A Figura 2.6 exemplifica algumas áreas da criminalística e suas subdivisões. Quanto mais particular o nível de expertise, mais técnico será o profissional necessário para a análise.

A Perícia Forense Criminal é a atuação concreta da Criminalística, parte-se dos seus procedimentos, técnicas, métodos e teorias, para a realização dos exames periciais dos vestígios (COVER et al., 2017). A perícia é, portanto, o exercício da criminalística.

O perito é o especialista que analisa tecnicamente uma situação, ou seja, de forma imparcial, através de um conjunto de passos bem definidos, amparado por uma base metodológica científica, de tal forma que outras pessoas que realizarem os mesmos passos,

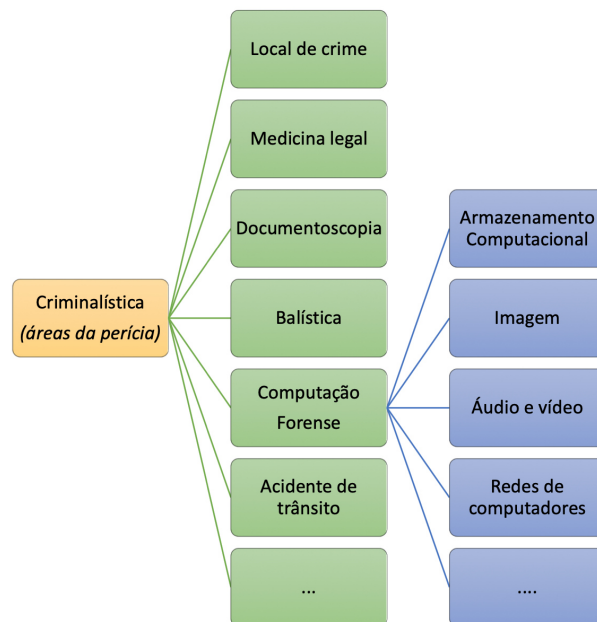


Figura 2.6: Hierarquia de algumas áreas da criminalística

chegarão aos mesmos resultados (RODRIGUES et al., 2010). A perícia criminal é a análise de uma situação em que um possível crime ocorreu, da qual o especialista coleta evidências e chega a uma conclusão sobre ter ocorrido ou não um crime, em um documento formal denominado laudo pericial (VARGAS; KRIEGER, 2014).

Segundo Yasinsac e Manzano (2001), para solucionar um crime, é preciso responder algumas perguntas:

1. O que ocorreu ?
2. Onde ocorreu ?
3. Como ocorreu ?
4. Quando ocorreu?
5. Quem praticou ?
6. Por quê ?

Os itens 1, 2, 3 e 4 referem-se à materialidade, o item 5 refere-se à autoria e o item 6 refere-se à motivação. Conhecida a atividade criminosa, descoberto o agente infrator responsável pela atividade e sabendo que ocorreu fato típico descrito em lei, deve-se constatar a culpabilidade do agente. Somente o agente que seja imputável, ou seja, aquele que pode ser alvo de acusação e que possui consciência da ilicitude, pode ser penalmente

responsabilizado por seus atos. Portanto, deve-se ter claramente definida a motivação do agente infrator para dar prosseguimento às fases de responsabilização penal. Na redação original do DECRETO-LEI Nº 2.848, DE 7 DE DEZEMBRO DE 1940, também conhecido como Código Penal Brasileiro, há dois artigos relevantes a esta pesquisa: o art. 154 e o art. 266.

Art. 154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: Pena - detenção, de três meses a um ano, ou multa de um conto a dez contos de réis. Parágrafo único - Somente se procede mediante representação.(BRASIL, 1940)

Interrupção ou perturbação de serviço telegráfico ou telefônico
Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Vigência Pena - detenção, de um a três anos, e multa.(BRASIL, 1940)

Em sua redação original, o artigo 154 trata da exposição de dados sigilosos ou sensíveis. Todavia, não há referência sobre essa exposição em meio informático. Já o artigo 266 trata da interrupção de serviço telefônico ou telegráfico porém, também não há um detalhamento desses serviços em informática.

A legislação brasileira que fundamenta a identificação de crimes em redes computadores é a Lei 12.737 de 2012, a Lei de Crimes Informáticos, que incluiu novo artigo ou alterou os artigos supracitados. Aquele que trata da interrupção serviço, foi alterado e incluído o aspecto do serviço informático, que é o embasamento legal utilizado nesta pesquisa, por dar suporte à persecução penal, quando identificada a atividade maliciosa de negação de serviço:

Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública
Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
Pena - detenção, de um a três anos, e multa. § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. (BRASIL, 2012)

O artigo 154-A do Código Penal, inserido pela lei 12.737/2012, incluiu o aspecto da exposição de dados, através de uma invasão de dispositivo informático, tornando-se assim uma evolução para o tratamento de atividades maliciosas, que podem ocorrer em meio informático. Apresenta-se a seguir o dispositivo:

Invasão de dispositivo informático

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não a rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena – detenção, de 3 meses a 1 ano, e multa. (BRASIL, 2012)

No âmbito jurídico, os verbos são os elementos presentes nas leis, que descrevem a conduta, a ser verificada para assim constatar a existência do fato. Portanto se, a título de exemplo, o verbo presente na lei for "subtrair", e se, no caso em questão, a ação representada por esse verbo não tenha ocorrido, não há crime, visto que a lei é clara no elemento que a precede.

2.6 Computação Forense

A Computação forense também conhecida como ciência forense computacional, ou forense digital, é entendida como o processo de identificar, preservar, analisar e preservar uma evidência digital de forma que seja legalmente aceita (MARTINI; CHOO, 2012).

É necessário que o fato ocorrido, ou seja, a atividade maliciosa, seja bem explicada sem que a análise comprometa a cadeia de custódia ou a evidência em si. A Computação forense é a disciplina que analisa as evidências digitais, envolvendo os elementos que os norteiam (VELHO, 2016).

A utilização de sistemas computacionais como meio ou fim para o cometimento de crimes, produz evidências de natureza lógica ou física (ALLEN, 2005), (BSI, 2012). No âmbito da Computação Forense, existem várias áreas, conforme já apresentado na Figura 2.6, e uma sub-área interessada em evidências geradas por comunicações em redes de computadores, que é chamada Forense em Redes de Computadores.

A análise forense em Redes de Computadores, subárea da Computação Forense, estuda os procedimentos formais para caracterizar uma atividade maliciosa em Redes de Computadores, e busca encontrar os elementos que formalizam o crime, caso ele tenha ocorrido. Os procedimentos envolvem: a identificação do vestígio, o isolamento e sua preservação, a extração para análise e correlação, e a apresentação em formato de Laudo Pericial (JAYAKRISHNAN; VASANTHI, 2018). A seguir estes procedimentos são detalhados:

- **Identificação:** No processo de identificação, os vestígios de interesse como os lógicos e os físicos são identificados, exemplificados pelo tráfego de rede, ou mesmo *logs* das ferramentas de detecção de intrusos. A listagem de evidências não é absoluta, resume-se que qualquer vestígio relacionado que faça parte da cadeia de custódia é um indício e deve ser coletado.
- **Preservação:** No processo de preservação gera-se uma *hash*. O *hash* é um mecanismo de garantia de integridade que utiliza criptografia para sinalizar alterações em um artefato digital (PILLI et al., 2010). Todas as evidências encontradas, como *logs* de sistemas, devem passar por esta etapa e ter suas respectivas *hashes* armazenadas. Este é um requisito importante quando apresentada uma evidência a uma autoridade policial ou judiciária. Outra forma de se garantir a integridade e autenticidade é a utilização da *blockchain*. Conhecida como "protocolo de confiança", ela é uma base de dados distribuída que utiliza a descentralização como segurança. Funciona como um local aberto, em que todos podem publicar dados. Formando uma cadeia de blocos estruturados, na qual a informação de um bloco é garantida pelo bloco anterior (ZIKRATOV et al., 2017). A publicação das evidências nessa cadeia de blocos aumentaria a garantia de integridade e autenticidade de vestígios encontrados.
- **Extração:** Após serem identificadas e preservadas, é feita uma cópia de trabalho das evidências, para que não haja risco de alteração da evidência de origem. Muitas dessas evidências, quando digitais, estão em formato ininteligível pelo homem, como *bits*. No processo de extração, são feitas transformações, normalizações e limpezas, ou seja, manipulações que não afetam a informação, mas que permitam sua correlação e sua visualização.
- **Análise:** No processo de Análise o conhecimento é descoberto. Muitas informações podem estar ininteligíveis e essas informações, que podem ser a chave para a persecução penal, são descobertas neste processo, através de investigações em exames próprios de cada vestígio. Todos os conhecimentos devem partir dos vestígios. Na análise, cria-se toda a cadeia de custódia, que é a comprovação da correlação dos eventos, mostrando desde quando foram coletados, até quando se encontra o conhecimento chave nos exames dos eventos ocorridos, documentando as operações e chegando assim, nas respostas aos questionamentos das autoridades policiais ou judiciárias (STEPHENSON, 2003).

- **Apresentação:** Por fim o Laudo Pericial é formalizado, documentando todas as etapas que foram procedidas, as informações extraídas, as fontes de informações, bem como os procedimentos realizados, que permitam a replicabilidade e sirvam para livre convencimento do juiz, ou seja, o juiz tomará o Laudo Pericial como base para sua decisão, mas o Laudo não o obriga a seguir o que nele consta. Este ponto mostra o quanto as informações devem ser bem fundamentadas e os procedimentos bem descritos para que o juiz entenda todas as questões envolvidas do fato analisado.

2.7 Ferramentas para identificação de atividades maliciosas em redes

Como dito anteriormente, o objetivo da segurança em redes de computadores é garantir a confidencialidade, autenticidade, integridade, disponibilidade, não-repúdio, ou seja, ser auditável. Tecnologias aplicadas à segurança em redes de computadores são autenticação, criptografia de dados, *firewall*, IDS, redes privadas virtuais, entre outras. Pode-se citar que autenticação e criptografia, *firewall* e IDS são umas das mais importantes linhas de defesas em segurança de redes. Técnicas de autenticação têm por objetivo garantir que a origem expressa enviou a mensagem ao destino. É possível citar como técnicas de autenticação: usuário e senha, criptografia simétrica, criptografia assimétrica, resumos de hash, listas de controles de acesso, assinaturas digitais (YAN et al., 2015).

O *firewall* é a segurança entre a rede interna e a rede externa e serve para fortalecer o controle de acesso entre as redes. Serviços básicos do *firewall* são: filtragem dos pacotes de dados que passam pela rede, gerenciamento dos comportamentos dos acessos à rede, por meio de gravação dos conteúdos e atividades de informações que passam através dele, e também detecção e produção de alarmes de ataques à rede. As principais técnicas de um *firewall* são: filtragem de pacotes, *gateway* de aplicações e *proxy* (ELDOW et al., 2016).

IDS são um tipo de tecnologia de segurança em rede que suplementam o *firewall*. Coletam informação ativamente e analisam o tráfego na rede por possíveis ataques ou invasões. Portanto os IDSs estendem a habilidade de gerenciamento da segurança, incluindo auditoria de segurança, monitoramento, reconhecimento de ataques e resposta a incidentes, melhorando a integridade da arquitetura de segurança da informação. As principais funcionalidades de um sistema de detecção de intrusos são: detectar e analisar as atividades

de usuário e sistema; auditar as configurações e vulnerabilidades do sistema; identificar os padrões conhecidos de ataques e reportar para as pessoas relacionadas, estatísticas e análises de padrões anormais de comportamentos; avaliar a integridade de sistemas e dados importantes; gerenciar o sistema operacional e identificar os comportamentos de usuários que violaram estratégias de segurança (ROESCH, 1999).

Tecnologias de detecção de intrusos são de dois tipos: baseadas em anomalias ou mal uso (GARG; MAHESHWARI, 2016). Detecção baseada em anomalias assume que todos os comportamentos dos intrusos são diferentes dos comportamentos dos usuários normais. Todo tráfego diferente dos esperados é considerado suspeito. Algoritmos populares incluem métodos probabilísticos, padrões preditivos e redes neurais. A detecção através de uso indevido assume que os comportamentos de intrusos e meios podem ser expressos com o mesmo padrão, ou seja, através do mesmo casamento de padrões. Algoritmos populares incluem sistemas especialistas, casamento de padrões, raciocínio de modelo e análise de transição de estados (YAN et al., 2015).

2.8 Ataques cibernéticos criminosos à margem da lei

Um ataque cibernético muito conhecido na literatura é o ataque DoS. Ele afeta a qualidade dos serviços da rede de computadores através de, por exemplo, uma sobrecarga de pacotes que a largura de banda da rede consiga suportar, fazendo com que requisições não possam ser atendidas (ELDOW et al., 2016). Dependendo da estratégia utilizada o DoS pode ser categorizado como ataque, baseado no volume, ataque DoS em protocolos ou ataques baseados na camada de aplicação (GUPTA; BADVE, 2016).

Ataques baseados na camada de aplicação são aqueles que focam protocolos da camada de aplicação, ou seja HTTP, DNS, *Simple Mail Transfer Protocol* - Protocolo de Transferência de Correio Simples (SMTP), *Secure Socket Layer* - Camada de *socket* segura (SSL), por exemplo, ou aplicações que suportam ou são suportadas por estes protocolos como sistemas operacionais, servidores Apache, dentre outros. O seu objetivo é quebrar o servidor *web*, enviando mensagens legítimas até que este não consiga responder, por sobrecarga de requisições (WU; ZHAO, 2015). Percebe-se um foco desta categoria de ataques em servidores *web* e, portanto, aplicações que se utilizam da *web* para entrega de seus serviços. Exemplos de ataques nessa categoria são: *slow post*, *get flood* e *slowris*.

Entende-se que na maior parte desses casos a motivação dos agentes que realizam este tipo de ataque é a negação dos serviços a requisições legítimas, ou seja, causar a indisponibilidade do serviço. A identificação e correta verificação da ocorrência desses ataques deve ser alcançada, para que assim auxilie na responsabilização dos agentes infratores.

2.8.1 Constatação de ataques DoS

Para constatação do ataque cibernético é necessário um monitoramento do tráfego de rede ou do sistema em questão. Os IDSs possuem essa finalidade e, para além disso, são capazes de filtrar comunicações e sinalizar alertas para atividades maliciosas, que tentam quebrar os princípios da segurança da informação: confidencialidade, integridade, autenticidade e disponibilidade, ou ainda violar mecanismos de segurança de um computador ou rede de computadores (BROWN et al., 2002). O IDS possui três módulos: o módulo de monitoramento, realizando decodificação das fontes de dados, como pacotes de tráfego de rede; o módulo máquina de detecção, que utiliza regras para correlação e casamento de padrões; e o módulo sistema de saída de alertas, que possibilita ao especialista analisar informações sobre as atividades maliciosas identificadas (ROESCH, 1999).

Escrever regras de detecção de intrusos pode ser uma tarefa complexa. É necessário conhecimento sobre as comunicações que ocorrem, a nível de protocolos de rede de computadores. Um especialista em redes de computadores geralmente é o responsável por escrever tais regras. Nas Figuras 2.7 e 2.8, é apresentado um exemplo de regra para detecção de ataque de negação de serviço e seu respectivo alerta sinalizado pelo IDS snort.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
(msg:"SLR - LOIC DoS Tool (HTTP Mode)"; flow:
established,to_server; content:"|47 45 54 20 20 48 54 54 50 2f 31 2e
30 0d 0a 0d 0a 0d 0a|"; threshold: type threshold, track by_src, count
10 , seconds 10; reference: url, www.uni-blida.dz ; classtype:misc-
activity; sid:1234569; rev:1; )
```

Figura 2.7: Regra do IDS para alertar ataques de negação de serviço
Fonte: (MEROUANE, 2017)

Dos alertas sinalizados, podem ser extraídas as informações que caracterizam a atividade maliciosa como crime. Na Tabela 2.2 essas características (a origem, a técnica, o momento) são extraídas e ficam à disposição para análise.

```

1/24-14:59:11.405063 [**] [1:123456:1] SLR - LOIC DoS Tool (TCP
Mode) - Behavior Rule (tracking/threshold) [**] [Classification: Misc
activity] [Priority: 3] {TCP} 193.194.8.1:55331 -> 193.194.8.1:8001/24-
14:59:11.996198 [**] [1:123456:1] SLR - LOIC DoS Tool (TCP Mode)
- Behavior Rule (tracking/threshold) [**] [Classification: Misc activity]
[Priority: 3] {TCP} 193.194.8.1:55331 -> 193.194.8.1:8001/24-
14:59:12.318804 [**] [1:123456:1] SLR - LOIC DoS Tool (TCP Mode)
- Behavior Rule (tracking/threshold) [**] [Classification: Misc activity]
[Priority: 3] {TCP} 193.194.8.1:55332 -> 193.194.8.1:80

```

Figura 2.8: Alerta sinalizado pelo Snort através da correlação da regra do IDS com o comportamento do ataque de negação de serviço

Fonte: (MEROUANE, 2017)

Utilizar o IDS é, portanto, uma forma de conseguir evidências de que uma atividade maliciosa em redes de computadores ocorreu. Essas evidências têm validade perante ao juiz, bastando que um especialista as extraia e, utilizando dos procedimentos da análise forense, garanta que os meios de prova apresentados foram lícitos e que não houve alteração do conteúdo probatório.

Informação nas redes de computadores	Informação extraída no alerta do IDS
Endereço Lógico de Origem (IP), Endereço Físico de Origem (MAC)	193.194.8.1:55332
Técnica utilizada	SLR - LOIC DoS Tool (TCP Mode)
Explica como ocorreu	+10 PACOTES em 10 SEG
Data de acontecimento	1/24-14:59:11.405063
Endereço Lógico de Destino (IP), Endereço Físico de Destino (MAC)	193.194.8.1:80
Elemento principal identificado: perturbar, interromper, prevenir, impedir ou dificultar o estabelecimento	PERTUBAR

Tabela 2.2: Informação extraída do alerta do IDS

Existem outras ferramentas que tentam mitigar atividades maliciosas em redes de computadores, como *firewalls*. Essas também podem ser fontes de evidências, quando devidamente configuradas para armazenarem os vestígios que possam ser analisados com interesse forense.

3 Trabalhos Relacionados

O aumento da utilização da internet tem proporcionado um cenário de interesse aos ataques cibernéticos (JAYAKRISHNAN; VASANTHI, 2018). Nesta seção, apresentam-se trabalhos que estejam relacionados à área de segurança da informação, identificação de ataques de negação de serviço e tipificação de crimes digitais.

3.1 Classificação de ataques cibernéticos

Os sistemas de detecção de intrusos realizam classificação de ataques cibernéticos, gerando alertas da ocorrência de atividades maliciosas na rede ou no próprio computador (KUMARAVEL; NIRAIISHA, 2013). Argumenta-se que o aumento de ameaças tem impulsionado a busca por novas formas de identificação de ataques cibernéticos em uma rede de computadores. Utilizando várias técnicas baseadas na análise estatística, como algoritmos de aprendizagem de máquina, análise de correlação multivariável, classificador de *naive bayes*, perfis de comportamentos e mineração de dados, trazem um aumento na detecção de ataques cibernéticos (S.MANGRULKAR et al., 2014). O objetivo é identificar os ataques cibernéticos o quanto antes, possibilitando uma contramedida mais rápida e, diminuindo assim, os efeitos dos ataques, no entanto, não há foco na classificação de crimes cibernéticos.

Os autores Wang et al. (2002), Perlin et al. (2011) e Mallikarjunan et al. (2016) apresentam modelos de detecção baseados no algoritmo CUSUM, que já foi utilizado na detecção de ataques DDoS, e abordam ataques de negação de serviço que usam pouca quantidade de pacotes, com intuito de perturbar um serviço de rede. Cenários de ataques de negação de serviço a nível de aplicação são realizados e têm seu tráfego armazenado em formato PCAP, com disponibilização dos tempos de duração, bem como informações de ativos de rede atingidos.

Vítimas do ataque de negação de serviço crescem a cada ano. Uma forma de identificar este ataque é monitorando: o fluxo de rede, a memória do servidor, a utilização da *Central Process Unit* - Unidade Central de Processamento (CPU) e o espaço do banco

de dados ou o espaço do disco de armazenamento (PAINE, 2018). O autor Merouane (2017) utilizou uma arquitetura do IDS Snort e criou um algoritmo mais eficiente na detecção de ataques DoS e DDoS propondo um modelo ou mudança arquitetural para filtragem desses ataques de forma automática, em um monitoramento, em tempo real da rede de computadores. O autor escolheu ataques DoS do tipo *User Datagram Protocol* - Protocolo de Datagrama do Usuário (UDP), *Transmission Control Protocol* - Protocolo de Controle de Transmissão (TCP) e HTTP implementados em ferramenta própria para avaliar sua proposta, obtendo uma melhora de 43,5% na detecção de ataques DoS e DDoS. Apesar de identificar o DoS, a lacuna deste trabalho é o interesse forense em criminalizar o ataque DoS, identificado responsabilizando assim o agente infrator.

3.2 Ferramentas de análise de evidências digitais

O *The Sleuth kit* (TSK)¹ é uma biblioteca de código aberto com utilitários contendo um conjunto de comandos para realizar análise forense de evidências. Não contém interface gráfica e seu objetivo é analisar sistemas de arquivos de mídias digitais como Discos de armazenamento e pendrives. O *Autopsy*² é uma ferramenta gráfica de código aberto que se acopla a interface do TSK para possibilitar análises forense de forma mais amigável, como pode ser verificado na Figura 3.1 (CARRIER, 2011).

O *Forensic Toolkit* - Kit Ferramental Forense (FTK)³, da empresa *Accessdata*, é uma ferramenta comercial e aceita para a forense digital. É capaz de processar evidências, realizar análises rápidas de memória *Random Access Memory* - Memória de Acesso Aleatório (RAM), além de ser uma ferramenta estável, baseada em um banco de dados para armazenamento de casos, e que suporta vários tipos de imagens, arquivos e extensões, proporcionando ainda investigação compartilhada de forma remota (KHOBRADE; MALIK, 2014).

O Indexador e Processador de Evidências Digitais (IPED)⁴, desenvolvido pelo Perito Criminal Federal Luis Nassif, no Brasil, é outro exemplo de ferramenta forense. Utilizando a linguagem Java⁵, é uma ferramenta amplamente utilizada para processar

¹<https://www.sleuthkit.org/>

²<https://www.sleuthkit.org/autopsy/>

³<https://accessdata.com/products-services/forensic-toolkit-ftk>

⁴<https://github.com/lfcnassif/IPED>

⁵<https://docs.oracle.com/javase/tutorial/java/index.html>

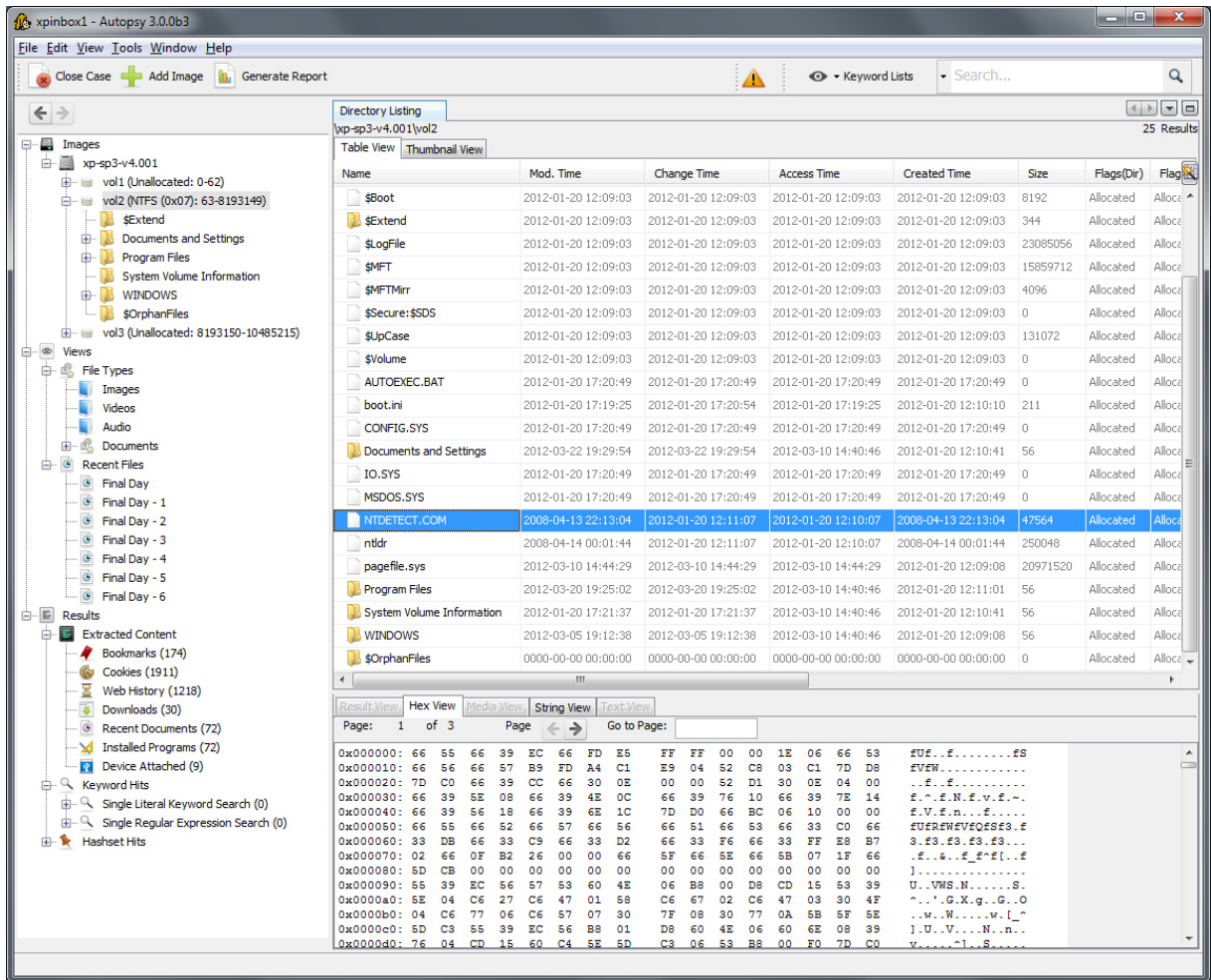


Figura 3.1: Visão geral do autopsy
Fonte: (CARRIER, 2011)

evidências de mídias ópticas e utiliza várias ferramentas de código aberto como TSK e outras bibliotecas, para processamento e interpretação de imagens, indexação rápida, georeferenciamento, recuperação de arquivos apagados, reconhecimento óptico de caracteres, dentre outras funcionalidades. Contribuiu para diminuição de pagamento de licenças em ferramentas proprietárias como FTK (SANTOS et al., 2019).

As ferramentas anteriormente citadas, são amplamente utilizadas no campo da perícia forense em informática, no entanto, vale atentar que as mesmas não são voltadas para análise de fluxos de rede de computadores, constatando assim uma lacuna para tais ferramentas.

*Wireshark*⁶ é uma ferramenta para monitoramento e análise do tráfego de rede, possibilitando analisar a pilha completa de protocolos de rede, dentro de cada pacote que trafega na rede. Possui uma boa interface gráfica para operação e permite a inclusão de

⁶<https://www.wireshark.org/>

filtros de informação e rastreamento de streaming de uma comunicação, possibilitando a análise entre a informação trocada entre a origem e o destino (SANDERS, 2017). Esta ferramenta é utilizada para análise forense no sentido de analisar o fluxo de rede e análise manual de informações que trafegam na rede, mas não é capaz de realizar a correlação entre a informação e o que se conhece como crime ocorrido em meio informático.

3.3 Datasets para testes de IDS

Para testar arquiteturas de monitoramento, avaliar a eficiência de configurações de sistemas de detecção de intrusos, necessita-se de uma forma de simular o tráfego de rede. Foram observados trabalhos para simulação de tráfego malicioso e geração de bases de dados - *datasets*, para treinamentos e testes de eficiência em detecção de atividades maliciosas (TAVALLAEE et al., 2009). Os autores Sharafaldin et al. (2018), criaram o *dataset*, conhecido como *CIC IDS data set*⁷ e os autores Jazi et al. (2017) criaram o *CIC DoS data set*⁸ ambos representados por arquivos em formato PCAP, que é uma extensão de pacotes de tráfego de rede bem conhecida (ALSMADI; ALAZAB, 2017), com vários cenários de avaliações de ataques cibernéticos em redes de computadores, incluindo ataques DoS e DDoS.

A arquitetura, os ativos de rede do ambiente de testes, foi apresentada e os horários de cada ataque ocorrido foram marcados, assim, ao analisar os arquivos em formato PCAP do *dataset*, será possível visualizar os cenários de avaliações, bem como características extraídas que podem ser utilizadas, para auxiliar na detecção de ataques cibernéticos. A falta de *datasets* voltados para ataques de negação de serviço na camada de aplicação foi a motivação dos autores Jazi et al. (2017) e tráfegos realistas de infraestruturas de rede de computadores pelos autores Sharafaldin et al. (2018).

Os autores Souza e Santos (2018) também realizam um estudo voltado para criação de um *dataset* para ataques de negação de serviço com baixas taxas de transmissão. Com a motivação de preencher lacunas de ataques *slowris* e *socketstress*, por carências de *datasets* de simulação desses ataques. Esse *dataset* produzido contém: além de *dumps* em formato PCAP do tráfego de rede, *logs* do servidor, informações da memória e CPU, bem como metadados dos ataques, através de ferramentas próprias.

⁷<https://www.unb.ca/cic/datasets/ids-2017.html>

⁸<https://www.unb.ca/cic/datasets/dos-dataset.html>

3.4 Evidências em redes de computadores

O autor Hampton e Baig (2016) relata que a qualidade das evidências capturadas é um dos grandes fatores para possibilitar sua aceitação. Ele relata que as evidências podem estar em vários locais e é necessário a coleta dessas evidências de forma mais acurada possível. O autor ainda propõe um método de análise de estampas de tempo em evidências de rede, no entanto seus experimentos são feitos apenas sobre requisições legítimas e nenhum experimento envolvia atividades maliciosas.

Existem informações voláteis e não voláteis, as primeiras são aquelas que existem para fins necessários, mas que em algum momento são perdidas como a memória RAM de um computador que é sempre apagada no início da inicialização do sistema, já as do segundo tipo são aquelas que, mesmo após o tempo e não sendo apagadas intencionalmente, persistem no local armazenado. O autor Maués (2016) traz um conjunto de evidências voláteis e não voláteis em meio digital, a Tabela 3.1 apresenta exemplos de evidências digitais em meio informático.

Evidências digitais voláteis	Evidências digitais não voláteis
Configurações de rede	Informações de contas
Conexões de rede	Arquivos de configuração e logs
Processos em execução	Arquivos de dados
Arquivos abertos	Arquivos de páginas e swap
Sessões de login	Arquivos temporários ou cache
Informações de data e hora	Registro do sistema operacional

Tabela 3.1: Exemplo de evidências digitais voláteis e não voláteis

O autor Maués (2016) faz uma modelagem de ameaças antiforenses contemplando a gerencia de riscos, auxiliando na celeridade da tomada de decisão, priorizando a análise pelos riscos. No entanto, o autor não trouxe exemplos relacionados à ameaças de redes de computadores.

Os *logs*, registros de operações, servem para vários propósitos, conforme explica Studiawan et al. (2019) entre eles: evidência para aplicação da lei, podem auxiliar na reconstrução do ataque, podem ainda auxiliar na identificação de relações entre eventos aparentemente separados ou ainda serem utilizados para detectar comportamentos maliciosos de usuários ou de atividades de sistema. O mesmo autor apresenta alguns modelos para serem seguidos em uma extração de *logs* usando uma abordagem com centralização e criptografia. No entanto, percebe-se em seu trabalho uma lacuna para modelos voltados a

representação de crimes utilizando as informações obtidas pelos *logs*, objeto de interesse para responsabilização de agentes infratores de crimes digitais.

3.5 Metodologias genéricas para análise forense

Existem também processos genéricos de investigação de crimes digitais, baseado no *Digital Forensics Research Workshop - Workshop de pesquisa forense digital (DFRWS)*, um roteiro genérico de atividades base, que são: identificação, preservação, coleta, exames, análise e apresentação. O autor Stephenson (2003), define o processo *End-to-End Digital Investigation - Investigação Digital Fim-a-Fim (EEDI)*, para auxiliar investigações digitais. Esse processo contém etapas que o investigador deve realizar para cumprir a base do *framework*. As etapas coleta de evidências, análise individual de eventos, correlação preliminar, normalização de eventos, deconflitar eventos, segundo nível de correlação, análise de linha do tempo, construção de cadeia de custódia e corroboração devem ser aplicadas em cada atividade do *framework* base, servindo como um *checklist*, garantindo a aplicação do processo ao *framework* base. Sem dar foco a uma atividade maliciosa específica, o autor fala também sobre técnicas para determinar: se o ataque realmente aconteceu, se houve premeditação, ou seja, a motivação do ataque ou caso ele tenha sido mascarado, para assim não ser reconhecido.

O autor (MAUÉS, 2016) também realiza uma revisão de 20 metodologias forenses digitais desenvolvidas ao longo dos anos de 1995 a 2012. Citando ainda que não há como determinar qual o melhor processo, pois cada metodologia possui suas vantagens e desvantagens. Dessas metodologias, não percebe-se a busca por procedimentos para atividades maliciosas ocorridas em redes de computadores.

3.6 Procedimento operacional padrão para análise de DoS

No Brasil, o Ministério da Justiça (MJ) possui um manual no formato de tarefas conhecido como Procedimento Operacional Padrão (POP) (BRASIL, 2013), (NERES; SANCHES, 2018). Funciona como orientações para execução de passos em busca de um objetivo e padroniza as tarefas relacionadas à perícia. Para sua confecção, é necessário o uso

de extensa busca bibliográfica, bem como são enumerados passos a serem realizados. Este é o procedimento utilizado pelos profissionais especializados para realização de perícias (SILVA, 2009).

Orientando o profissional de perícia da área de informática e outras áreas a realizar exames (BRASIL, 2013), ressalta-se a seção de procedimentos feitos na área de informática:

- Exame pericial de mídia de armazenamento computacional;
- Exame pericial de equipamento computacional portátil;
- Exame pericial de local de informática;
- Exame pericial de local de internet.

Dos exames citados o último é o que mais se aproxima do trabalho por tratar diretamente de informações do contexto de redes de computadores, mas se limita a analisar endereços de *Internet Protocol* - Protocolo de Internet (IP), análise de sites, buscando verificar práticas de infração penal ocorridas na internet. Percebe-se uma carência de procedimentos relativos à realização de análises para o ataque de negação de serviço, atividade maliciosa já passível de criminalização.

3.7 Considerações finais

Por ser uma lei relativamente nova, existem também trabalhos voltados ao seu entedimento e aos alcances que a lei 12.737, de 2012, pode ter (SILVA et al., 2016). No entanto, foi encontrada uma lacuna de trabalhos voltados para tipificação criminal, ou seja, trabalhos que mostrem quais atividades maliciosas podem ser caracterizadas como crime, segundo a lei brasileira.

Outra lacuna foi a ausência de metodologias que façam o processo de subsunção entre o disposto na lei 12.737, de 2012, para sua caracterização, e possibilitem sua correlação com a atividade maliciosa ocorrida, para apresentação de documento formal como, Laudo Pericial, Parecer ou Relatório Técnico.

Também não foi encontrada uma arquitetura computacional que automatize este processo, e possibilite que pessoas designadas a demonstrar a autoria e materialidade dos fatos consigam elaborar um documento formal. Apresentando provas para responsabilização

Trabalho	Relação com este trabalho/ Lacuna encontrada
Classificação de ataques cibernéticos	
Wang et al. (2002), Perlin et al. (2011), Mallikarjunan et al. (2016), Merouane (2017), Paine (2018).	Lacuna em evidenciar elementos que auxiliem na responsabilização de agentes infratores do ataque de negação de serviço.
Ferramentas de análise de evidências digitais	
Carrier (2011), Khobragade e Malik (2014), Santos et al. (2019) e Sanders (2017).	Lacuna de ferramentas voltadas a análise de evidências de rede de computadores bem como capacidade de realizar a correlação entre a informação encontrada e o que se conhece como crime ocorrido segundo a lei.
Datasets para testes de IDS	
Sharafaldin et al. (2018), Jazi et al. (2017) e Souza e Santos (2018).	Relação com este trabalho, disponibilizando bases de dados para simulação de tráfego malicioso.
Evidências em redes de computadores	
Hampton e Baig (2016), Maués (2016) e Studiawan et al. (2019).	Relação com este trabalho, fundamentando a utilização de evidências digitais e sua validade perante a autoridade judicial.
Metodologias genéricas para análise forense	
Stephenson (2003) e Maués (2016).	Lacuna de metodologias focadas no responsabilização de atividades maliciosas ocorridas em redes de computadores.
Procedimento operacional padrão para análise de DoS	
Silva (2009), BRASIL (2013) e Neres e Sanches (2018).	Lacuna de POPs relativos para análises do ataque de negação de serviço.

Tabela 3.2: Tabela comparativa de trabalhos relacionados

de agentes infratores de ataques de negação de serviço ou quaisquer outras atividades maliciosas que possam ser enquadradas neste dispositivo penal. Na Tabela 3.2 apresenta-se de forma resumida uma comparação entre a relação com este trabalho bem como as lacunas encontradas dos trabalhos relacionados.

4 MeviDoS: Metodologia para Evidência de Ataques DoS

À luz dos princípios da computação forense e da criminalística e, embasado pela lei de crimes informáticos, apresenta-se uma **Metodologia**, denominada **MeviDoS**, para análise forense em redes de computadores, com vistas a evidenciar os elementos que criminalizam o ataque **DoS**. Entende-se por metodologia a definição dos autores Arnes et al. (2006), que apresentam um conjunto de etapas para reconstrução do fato, e dos autores P. et al. (2014), na qual definem metodologia como um conjunto de etapas que devem seguir atividades básicas em uma investigação digital forense que são: coleta, exame, análise e apresentação.

A abordagem desenvolvida, na solução do problema, envolveu uma análise para identificação das técnicas de ataques cibernéticos utilizadas e o que está disposto na lei de crimes informáticos, a fim de subsumir técnica ao injusto, ou seja, a identificação da atividade maliciosa, realizada pela aplicação de uma determinada tentativa hacking e sua associação ao tipo penal, ou seja, do dispositivo penal violado. A metodologia proposta visa a identificação dos injustos penais definidos pela Lei nº. 12.737/2012, denominada de Lei dos Crimes Informáticos, que acrescentou alguns artigos no Código Penal brasileiro. Foram identificados os elementos necessários para caracterizadores dos ataques de negação de serviço (DoS) em redes de computadores, assim gerando um modelo associativo entre o que define-se como crime e o comportamento observado nas evidências identificadas pela análise do tráfego na rede.

A metodologia para análise forense em redes de computadores para ataques de negação de serviço segue o roteiro de Procedimento Operacional Padrão (POP) (BRASIL, 2013), com intuito de servir como recurso complementar tanto para iniciantes, quanto para experientes em análise forense em redes de computadores, podendo também ser utilizado como um *checklist* de operações necessárias para a realização de uma tarefa.

Essas tarefas são desenvolvidas, normalmente, por um *framework* de computação forense, dentre elas estão: a identificação de evidências, sua preservação, procedimentos de coleta, exames, análise e apresentação formal. Não obstante, como mencionado em

outro momento, as ferramentas existentes - estrangeiras, em sua maioria, não aplicam a legislação pátria.

Será apresentada também, a criação de uma arquitetura computacional que faça a automatização do processo feito por um especialista em redes de computadores para geração de documentos formais, que sirvam para apreciação e fundamentação das autoridades policial e judiciária em seu convencimento. As fases da metodologia são detalhadas a seguir.

4.1 Metodologia Aplicada

A metodologia para análise forense em redes de computadores deve estar de acordo com os princípios fundamentais da Computação Forense, com o foco em evidenciar os elementos necessários para criminalização de ataques de negação de serviço.

Essa metodologia assume na prática o formato de tarefas de um POP e mineração de dados nas evidências em busca da descoberta de conhecimento, ou seja, da ocorrência do crime. A seguir, são listadas as etapas do processo a ser seguido para análise de ataques de negação de serviço:

1. **Identificar as atividades maliciosas que se enquadram na lei de crimes informáticos:** nesta etapa são realizados os estudos preliminares para definir que conduta é um crime, nos termos da legislação utilizada. Se necessário um especialista em redes de computadores, ele pode ser consultado. Ao final desta etapa, as atividades maliciosas de interesse seriam identificadas;
2. **Identificação e registro dos elementos do crime:** conhecido o dispositivo legal, podem ser definidos parâmetros para rastreamento do crime em atividades maliciosas, ou seja, um conjunto de indicadores podem ser elencados de forma a possibilitar a observação ou monitoramento da ocorrência de fatos que contribuem para demonstração do fato delituoso. Um especialista na área do direito pode ser consultado. Ao final desta etapa, os elementos principais da lei que tipificam o crime são elencados.
3. **Criar o modelo de dados dos comportamentos e dos crimes:** conhecida a atividade hacking e seu respectivo dispositivo legal, podem ser mensurados em forma de modelo de dados para possibilitar o armazenamento dos vestígios, até que atinjam

o mínimo necessário para serem considerados relevantes, ou seja, considerados como crimes. Para isso, o comportamento será observado a partir das evidências geradas e suas informações vem a partir do contexto informático das redes de computadores. O crime será um conjunto de indicadores em conjunto com regras de associação que ao serem executadas mensuram, através desses indicadores, a presença do crime;

4. **Capturar Evidências geradas:** Os eventos sinalizados pelo IDS, bem como os *logs* no servidor ou até mesmo o monitoramento dos recursos computacionais se tornam indícios de ataques, portanto devem ser capturados para análise posterior. O IDS é escolhido como uma das fontes sinalizadoras de evidências, por ter como foco a identificação dos ataques cibernéticos mediante regras cadastradas;
5. **Preservação de dados e sua análise:** Os eventos, bem como qualquer vestígio relacionado, devem ser preservados para garantir integridade e assim, utilizando os exames especializados para correlação dos fatos, haver a extração de informações necessárias para elucidação do crime. Após a captura, as evidências podem ser analisadas e assim, utilizando de regras de associação, o conhecimento pode ser descoberto. Ao final desta etapa, tem-se a base de comportamentos ocorridos, ou seja, as evidências coletadas para análise;
6. **Subsunção fato (atividades maliciosas) à norma (tipo penal descrito em lei):** A correlação entre a atividade maliciosa e o verbo descrito no tipo penal. São definidas as regras utilizadas para a correlação. Ao final desta etapa, consegue-se definir o que é e o que não é crime, a partir do modelo de dados pré-definido;
7. **Disponibilização das evidências em formato de Laudo pericial para a autoridade competente:** A necessidade de formalizar as informações em um documento que possa ser apreciado pelas autoridades da investigação e acusação.

4.2 Modelo de dados

A seguir são definidos dois modelos: o de crimes e o de comportamentos de atividades maliciosas. O modelo de crimes serve como parâmetro para realçar os elementos na atividade maliciosa, que caracterizam o crime e deve partir dos requisitos que a lei de crimes informáticos define como tal. A partir desses requisitos, é possível identificar as

Base Legal	Elemento Principal Identificado	Resultado	Motivação
ARTIGO 266	interromper	Interrupção do serviço	Negar serviço a solicitações legítimas, ou seja, causar indisponibilidade
ARTIGO 266	perturbar	Perturba o serviço, impossibilitando responder algumas requisições por falta de recursos	
ARTIGO 266	impedir ou dificultar o restabelecimento	Impedir resposta de algumas algumas requisições	

Tabela 4.1: Elementos principais, resultados e motivação identificados sobre o artigo 266 da lei 12.737

características que devem ser observadas nos comportamentos de atividades maliciosas.

Através da análise da Lei n.º. 12.737/2012, na Tabela 4.1, os elementos para definição do ataque de negação de serviço são: a interrupção, a perturbação, impedir ou dificultar o estabelecimento de serviço, causando indisponibilidade do mesmo a requisições legítimas. Portanto, as atividades maliciosas que realizem indisponibilidade de serviço, ou seja, realizam o ataque de negação de serviço têm características próprias que as definem. Estas características devem ser monitoradas e assim definidos os parâmetros para sinalizar variações relevantes nesse monitoramento.

Vale ressaltar que essa análise é resultado da interpretação da lei, no entanto, como esta, por mais que tente ser objetiva em definir os elementos para sua tipicidade, é passível de interpretação pelos operadores da lei. A motivação do ataque DoS é característica e marcada pelo aspecto de causar a indisponibilidade.

O ataque de negação de serviço do tipo HTTP, realiza um grande volume de tentativas de conexões através do protocolo HTTP, sobrecarregando o servidor, portanto, o elemento monitorado neste tipo de ataque deve ser a quantidade de requisições não atendidas (ALIM et al., 2018), sinalizadas pelo código 408 *REQUEST TIMEOUT*: Tempo de Requisição Excedido. Um grande volume desse tipo de resposta em um servidor pode ser indício de que esteja sob ataque de negação de serviço bem como evidência para indisponibilidade do serviço.

A presença de alertas sinalizados pelo IDS, após um monitoramento da rede de computadores, sobre um determinado tipo de ataque, também gera evidências da ocorrência

do ataque cibernético. Um grande volume de alertas desse ataque, somado a presença de provas quanto a indisponibilidade citada anteriormente, enriquece ainda mais um laudo de ataque em rede de computadores. A flutuação da utilização de recursos de hardware como memória, processamento de CPU, temperatura e armazenamento podem também estar relacionados a ocorrência de ataques.

Infelizmente não há na literatura a exata definição de quantas requisições sobre o protocolo HTTP, ou quantos alertas do IDS são sinalizados, ou mesmo valores no monitoramento de recursos de hardware são necessários para um servidor se tornar indisponível. É possível que este valor possa variar dado que a infraestrutura disponível pode conter recursos de processamento de tal porte que atenda a mais que outra de menor porte, com menos recursos.

Para esta solução será analisado apenas as evidências geradas pelo IDS bem como os *logs* de servidor. Será considerado, portanto, que a quantidade necessária para indisponibilidade será a quantidade mínima necessária observada que tornar o servidor indisponível, ou seja, recebeu tantas requisições quantas foram possíveis antes de começar a negar respostas a requisições por não ter recursos disponíveis para respondê-las, causando indisponibilidade às requisições legítimas.

Os alertas sinalizados por um IDS enriquecem a análise e disponibilizam mais informações importantes sobre o ataque. Caso seja um ataque DoS direto, o endereço IP de origem irá se repetir nos alertas, comprovando a intenção de causar indisponibilidade. No entanto, é conhecida uma técnica de mascaramento de IP que proporciona o envio de requisições com endereços de IP diferentes do real utilizado. Nestes casos haverá vários IP candidatos a autoria e a diferença de tempos entre as requisições pode ser um elemento que conseguirá reduzir o espaço de busca de possíveis endereços de origem. Na Tabela 4.2 é apresentado o modelo para caracterização de crime do ataque de negação de serviço. Os elementos ou métricas são indicadores que auxiliam a observação de anomalias na rede de computadores, nas evidências sob análise.

Do total de requisições em um intervalo de tempo, pode ser calculada a média de requisições por segundo, calcular assim se houve aumento e estimar quando o ataque foi iniciado, gerando dessa forma a cadeia de custódia dos eventos, buscando explicar a verdade nos vestígios encontrados.

Para caracterização do comportamento malicioso, serão necessárias informações

Elementos (Métricas)	Tipo	Descrição
alertas IDS	número	Quantidade de alertas sinalizados pelo IDS
requisições	número	requisições no servidor web
requisicoes por segundo	número	média de requisições por segundo
requisições atendidas	número	requisições com status 200
requisições negadas	número	requisições com status 408
acumulo ips nas requisicoes	número	quantidade acumulada dos IPs encontrados das requisições
acumulo ips nos alertas	número	quantidade acumulada dos IPs nos alertas do IDS
qtd ip mais notado req	número	qtd de vezes do IP que mais se repetiu nas requisições
qtd ip mais notado alerta	número	qtd de vezes do IP que mais se repetiu nos alertas
tempo indisponivel	número	Diferença entre o primeiro e o último alerta gerados pelo IDS

Tabela 4.2: Modelo de caracterização do crime

que sinalizem a presença de atividades maliciosas ocorridas na rede de computadores. Os alertas sinalizados pelo IDS indicam exatamente estas informações. É possível, portanto, mapear as informações para tipificação criminal no contexto de redes de computadores, conforme apresentado na Tabela 4.3. Constata-se também que as informações na rede de computadores são os elementos que caracterizam o comportamento das atividades maliciosas, formando o modelo representativo do comportamento das atividades maliciosas.

<i>Informação para tipificação penal</i>	<i>Informação nas redes de computadores</i>
AUTOR (quem)	Endereço Lógico de Origem (IP), Endereço Físico de Origem (MAC)
MATERIALIDADE (o que)	Técnica utilizada
FATOS (como)	Explica como ocorreu
TEMPO (quando)	Data de acontecimento
VÍTIMA (onde)	Endereço Lógico de Destino (IP), Endereço Físico de Destino (MAC)
TIPO PENAL (por que)	Elemento principal identificado: perturbar, interromper, prevenir, impedir ou dificultar o estabelecimento

Tabela 4.3: Modelo de comportamento da atividade maliciosa

Para a implantação da metodologia proposta, a Figura 4.1 mostra de forma abstrata, ou seja, sem definir tecnologias, as atividades a serem seguidas pelo profissional interessado em replicá-la tanto para o dispositivo penal focado pelo trabalho, quanto em outros dispositivos.

Estas atividades dão o embasamento para criação de uma arquitetura computacional que automatize as etapas definidas na metodologia. Após identificada a lei que embasa a

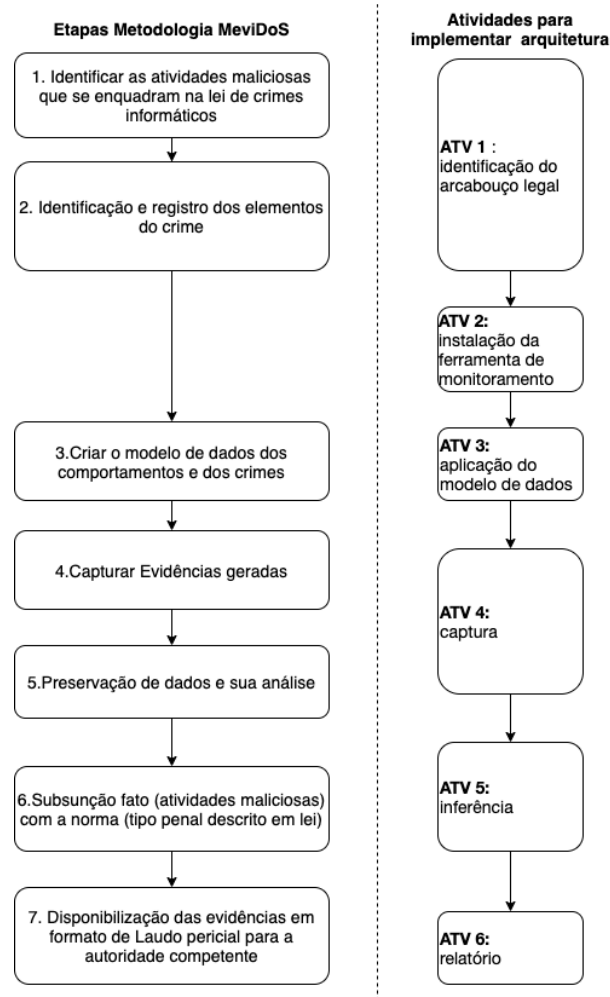


Figura 4.1: Fluxo abstrato para implementação da arquitetura computacional

responsabilização de crimes digitais (ATV. 1), para implantar a metodologia em uma arquitetura computacional deve-se escolher e instalar uma ferramenta de monitoramento (ATV. 2), aplicar o modelo de dados às ferramentas (ATV. 3), executar captura das evidências (ATV. 4), realizar as inferências necessárias para descoberta do conhecimento (ATV. 5) e assim apresentar o relatório que documenta os resultados para a autoridade da investigação.

4.3 Arquitetura computacional

Para alcançar os objetivos e atividades definidos na metodologia, foi desenvolvida uma arquitetura computacional para subsidiar o especialista no âmbito forense que, preservando os indícios das atividades fornecidos pelos sistemas de detecção de intrusão, através de um mapeamento dos incidentes de segurança caracterizados como crime sua interpretação até a visualização e sua tipificação penal conforme a lei brasileira, para subsidiar a

geração de laudos periciais no contexto de análise forense em redes de computadores. A arquitetura proposta é apresentada na Figura 4.2.

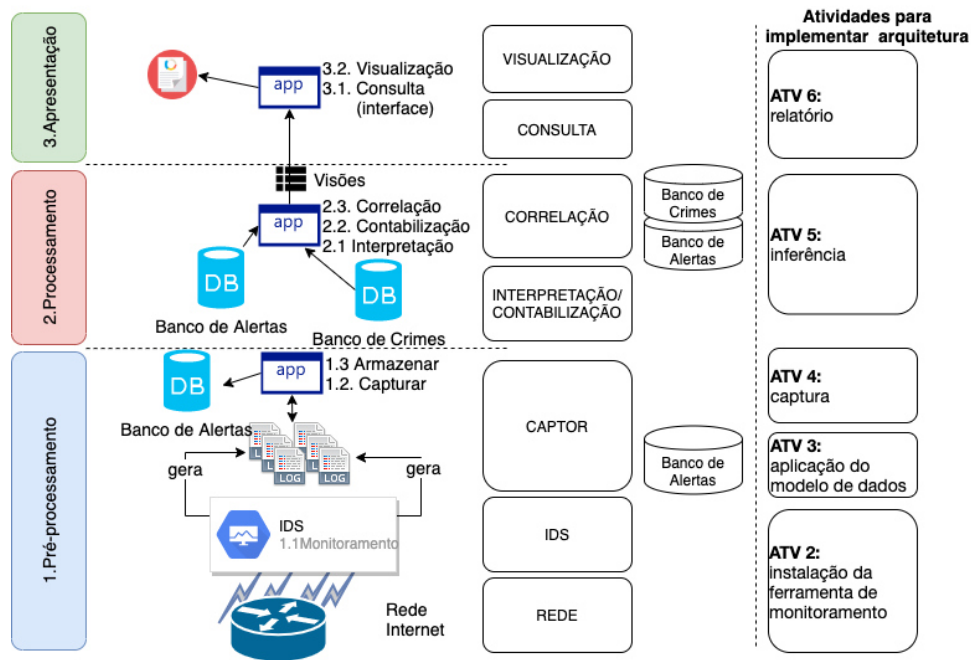


Figura 4.2: Arquitetura da Solução Proposta

A Fase 1 - Pré-Processamento contempla atividades de captura de dados, armazenamento e normalizações primárias nos dados. A Fase 2 - Processamento possui como principais etapas a interpretação, contabilização e correlação. A Fase 3 - Apresentação confere a formalização e disponibilização dos dados organizados em formato a serem apresentados para a autoridade da investigação.

Iniciada pelo monitoramento de um IDS na etapa 1.1, serão gerados arquivos de *logs* com alertas de atividades maliciosas. Auxiliado pelo captor forense de redes de computadores, na etapa 1.2, para registro dessas informações em uma base de dados de alertas. Na etapa 2.1 a 2.3, haverá a interpretação, contabilização e correlação com a base de crimes, tipificados pela lei brasileira de crimes informáticos com as atividades maliciosas, utilizando a técnica de visões no banco de dados. A base de crimes será configurada previamente com as regras utilizadas para identificação das atividades criminosas em redes de computadores.

Por fim, na etapa 3, a exposição dos dados em um relatório produzido através da consulta das visões disponibilizadas pela Fase 2, sendo possível assim a geração de relatórios das atividades, para auxiliar na responsabilização de atividades maliciosas, em um contexto de redes de computadores devidamente subsidiadas pela lei brasileira de crimes

4.4 Identificação das atividades maliciosas e captura de alertas sinalizados pelo IDS

Esta etapa consiste da utilização de um IDS para sinalização de alertas das atividades maliciosas que ocorrem em uma rede de computadores. Dentre os IDS disponíveis, o Suricata foi escolhido por ser uma ferramenta gratuita, que disponibiliza não somente os alertas sinalizados, como várias informações sobre a origem do alertas como, pacotes de tráfego de rede, informações do estado da rede durante o monitoramento dentre outras informações que podem ser utilizadas em uma análise forense.

A escrita de regras para funcionamento do IDS é geralmente tarefa do especialista encarregado pela redes de computadores, como o administrador de redes, que possui o conhecimento necessário para tal fim. O Suricata já disponibiliza um conjunto de regras gratuitas, escritas pela sua comunidade e podem ser utilizadas para detecção de alguns ataques dentre eles, ataques de negação de serviço.

Após configurado o IDS, são sinalizados alertas que estarão disponibilizados em arquivos de logs da ferramenta que devem ser armazenados e mecanismos de garantia de integridade como *hashs* devem ser aplicados, seguindo o princípio de integridade da segurança da informação. Sugere-se também que estes logs possam ser publicados em uma rede *blockchain* pois, como citam os autores Ray (2019) e Koumidis et al. (2018), esta rede de blocos também é utilizada para garantia de integridade de dados. Essas informações compõem a base de comportamentos das atividades maliciosas.

4.5 Associação das atividades maliciosas ao modelo

Após configurado o IDS, tendo a base de dados de atividades maliciosas suspeitas e a base de dados dos crimes previstos, é possível realizar a correlação entre as duas bases e assim sinalizar os crimes ocorridos de forma automatizada e inteligente.

- Caso existam alertas de ataques de negação de serviço **E** existam *logs* do servidor do tipo 408 *REQUEST TIMEOUT*, pode-se concluir que ocorreu um crime.

- Caso existam alertas de ataques de negação de serviço E **NÃO** existam *logs* do servidor do tipo 408 *REQUEST TIMEOUT*, pode-se concluir que ocorreu um dano.
- Caso **NÃO** existam alertas de ataques de negação de serviço E existam *logs* do servidor do tipo 408 *REQUEST TIMEOUT*, pode-se concluir que ocorreu um dano.

Dessa forma, pode-se inferir que a ocorrência de crimes suscita a necessidade de responsabilizar os agentes infratores. Os danos causados servem de alerta para os donos e proprietários de infraestruturas para que consigam tomar atitudes que tentem mitigar essas atividades maliciosas antes que sejam constatadas outras de maior grau, terminando por causar transtornos e custos para reparação.

4.6 Tipificação

Inserido pelo advento da Lei 12.737/2012, o artigo 266 do Código Penal constitui a base legal para fundamentação da pesquisa. Na Tabela 4.4, tem-se o mapeamento dos verbos relacionados, a lei brasileira de crimes informáticos com as atividades maliciosas exemplificadas que podem ocorrer em uma rede de computadores e seu resultado, que vem fundamentado pelo objetivo geralmente proposto pela atividade maliciosa de negação de serviço. Esta Tabela servirá de base como referência para futuras consultas por operadores do direito a fim de tipificar uma atividade maliciosa no contexto da computação.

<i>BASE LEGAL</i>	<i>ELEMENTO PRINCIPAL IDENTIFICADO</i>	<i>ATIVIDADE MALICIOSA</i>	<i>RESULTADO</i>	<i>MOTIVAÇÃO</i>
ARTIGO 266	interromper	HTTP Slowris, Goldeneye, HTTP Hulk	Interrupção do serviço	NEGAR SERVIÇO A SOLICITAÇÕES LEGÍTIMAS, OU SEJA, CAUSAR INDISPONIBILIDADE
ARTIGO 266	perturbar		Perturba o serviço, impossibilitando responder algumas requisições por falta de recursos	
ARTIGO 266	impedir ou dificultar o restabelecimento		Impedir resposta de algumas algumas requisições	

Tabela 4.4: Mapeando elementos principais e exemplos de atividades maliciosas

Os ataques de negação de serviço devem obedecer a norma descrita para que sejam passíveis de responsabilização. Caso alguma atividade maliciosa, que cause prejuízos ao serviço, seja mapeada, e não se enquadre na lei, ela não poderá ser tipificada como crime, mas apenas como uma atividade maliciosa danosa. Tendo o artigo definido, necessita-se caracterizar a atividade maliciosa e analisar os elementos necessários para sua tipificação penal, bem como o objetivo do agente infrator para continuar em uma persecução penal e propor o indiciamento dos autores da atividade maliciosa.

Assim, verifica-se importância de definir os seguintes pontos para caracterização da atividade maliciosa: a origem ou autoria (quem realizou o ataque cibernético), o destino ou vítima (quem sofreu o ataque cibernético), a técnica utilizada (materialidade), o tempo do crime (quando ocorreu), motivo do crime e uma lei que defina a atividade maliciosa como crime (MATE; KAPSE, 2015). Verifica-se na Tabela 4.5 as informações necessárias para caracterização do crime com as disponíveis pela atividade ocorrida na redes de computadores.

Informação para tipificação penal	Informação nas redes de computadores	Extração em um alerta de IDS
AUTOR (quem)	Endereço Lógico de Origem (IP), Endereço Físico de Origem (MAC)	193.194.8.1:55332
MATERIALIDADE (o que)	Técnica utilizada	SLR - LOIC DoS Tool (TCP Mode)
FATOS (como)	Explica como ocorreu	+10 PACOTES em 10 SEG
TEMPO (quando)	Data de acontecimento	1/24-14:59:11.405063
VÍTIMA (onde)	Endereço Lógico de Destino (IP), Endereço Físico de Destino (MAC)	193.194.8.1:80
TIPO PENAL (por que)	Elemento principal identificado: perturbar, interromper, prevenir, impedir ou dificultar o estabelecimento	PERTUBAR

Tabela 4.5: Modelo de comportamento da atividade maliciosa com exemplo de extração de alerta de IDS

A Tabela 4.5 mostra os elementos para subsunção das informações necessárias para tipificação penal, em um contexto de redes de computadores, extraídos de um alerta de IDS. Estas informações são de suma importância pois, após identificada a atividade maliciosa criminosa, deve-se proceder com a elaboração do laudo que demonstrará a sua tipificação para responsabilização dos agentes infratores.

4.7 Experimentos

No sentido de validar a metodologia, foram realizados experimentos em uma arquitetura de testes, através de uma simulação das entidades participantes de um cenário de ataques cibernéticos em uma rede de computadores. Assim, entende-se que o processo para descoberta dos fatos ocorridos consistirá de utilizar a metodologia proposta meviDoS, analisar as informações obtidas através da aplicação da mesma e assim apresentação das

conclusões obtidas através das etapas propostas.

Portanto, o objetivo dos experimentos é provar que é possível evidenciar os elementos que auxiliam a responsabilização de agentes infratores de ataques de negação de serviço, categorizando-os em conclusão de ocorrência de crime ou dano.

Esse objetivo será atingido através da observação da geração de evidências nos experimentos e extração de informações através da contabilização dos dados para preenchimento dos indicadores representados através das métricas definidas.

A arquitetura de testes desenvolvida utiliza, como mostra a Figura 4.3, quatro máquinas virtuais, criadas através ferramenta virtualbox, denominados VM_VITIMA, VM_ATACANTE, VM_IDS e VM_USUARIO.

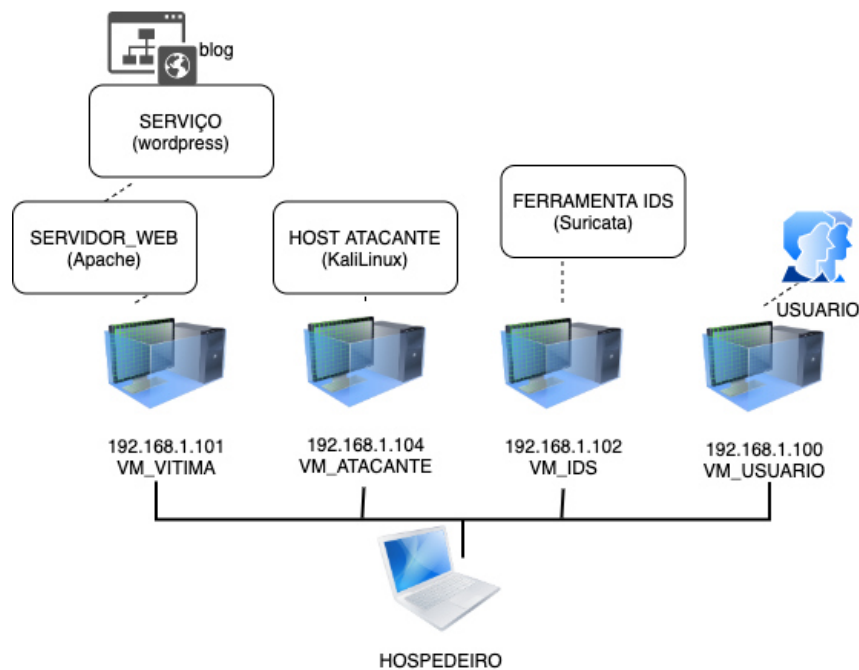


Figura 4.3: Arquitetura de testes usada nos experimentos

Essas máquinas virtuais representaram as entidades participantes de um cenário de ataques cibernéticos em redes de computadores. A Tabela 4.6 trás detalhes do objetivos de cada máquina virtual criada.

A Tabela 4.7 apresenta os tipos de evidência a serem observados.

A evidência **access.log** relaciona-se com a requisição feita ao servidor web, mostrando os IPs que realizaram alguma solicitação do serviço. As requisições tanto de um atacante quanto as legítimas estarão neste arquivo. Para constatar a ocorrência da atividade maliciosa em si utiliza-se a fonte de evidência **fast.log** que apresenta detalhes do

Entidade	Objetivo
VM_VITIMA	Disponibiliza o serviço que é alvo de ataques cibernéticos. Representa a rede corporativa.
VM_ATACANTE	Representa o agente infrator que realizou o ataque.
VM_IDS	Representa o sistema de detecção de intrusos, que monitora a rede.
VM_USUARIO	Representa o usuário final, que tenta realizar requisições legítimas ao serviço

Tabela 4.6: Detalhamento das máquinas virtuais e seus objetivos

Entidade Associada	Fonte Evidência	Evidência	Descrição
VM_VITIMA VM_USUARIO VM_ATACANTE	apache	access.log	arquivo contendo requisições realizadas ao servidor WEB
VM_ATACANTE VM_IDS	suricata	fast.log	arquivo contendo os alertas de atividades maliciosas capturadas pelo IDS
VM_IDS VM_ATACANTE	suricata	log.pcap.<NUMBER>	arquivo contendo o fluxo monitorado em formato PCAP permitindo replicabilidade. <NUMBER> é um número aleatório.
VM_USUARIO	JMeter	summary_report, reponse_time_graph,	evidências dos momentos de indisponibilidade do serviço.

Tabela 4.7: Fontes de evidência

ataque, já apresentados no modelo do comportamento da atividade maliciosa na Tabela 4.3 na seção 4.2.

A evidência **log.pcap.<NUMBER>** permite a replicação do experimento e possibilita que outros possam replicar experimentos na mesma fonte de dados. Já a evidência proporcionada pela ferramenta JMeter possibilita simular o comportamento do usuário que está tentando realizar requisições para usufruir do serviço de utilidade pública, representado pelo blog hospedado na VM_VITIMA, e mostra os momentos de indisponibilidade do serviço causados durante o ataque.

Nas Figuras 4.4 e 4.5, são apresentados os cenários de simulação realizados nos experimentos: *online* e *offline*. O cenário *online* tem a característica de ser executado através de uma ferramenta real de ataques cibernéticos, ou seja, a fonte das evidências é o tráfego de redes monitorado em tempo real.

O cenário *offline* conta com um arquivo do tipo PCAP previamente coletado, sob uma arquitetura específica, contendo diversos tipos de ataques cibernéticos, ou seja, a

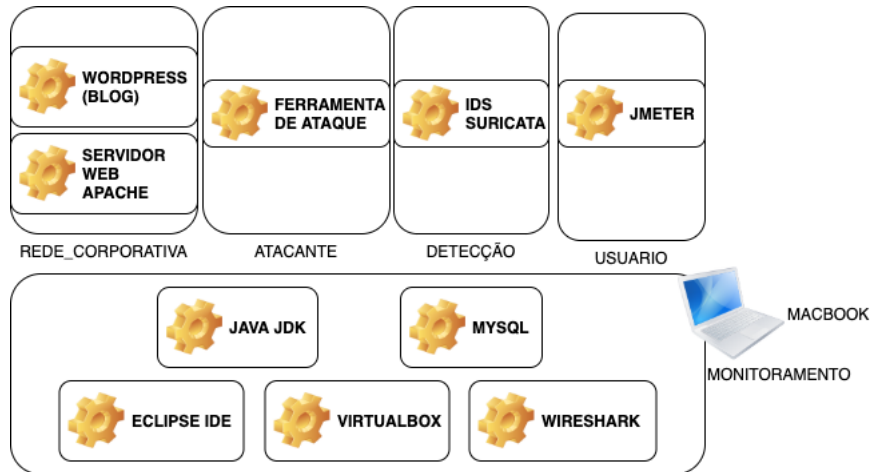


Figura 4.4: Cenário *online* dos experimentos

fonte das evidências é o tráfego previamente armazenado.

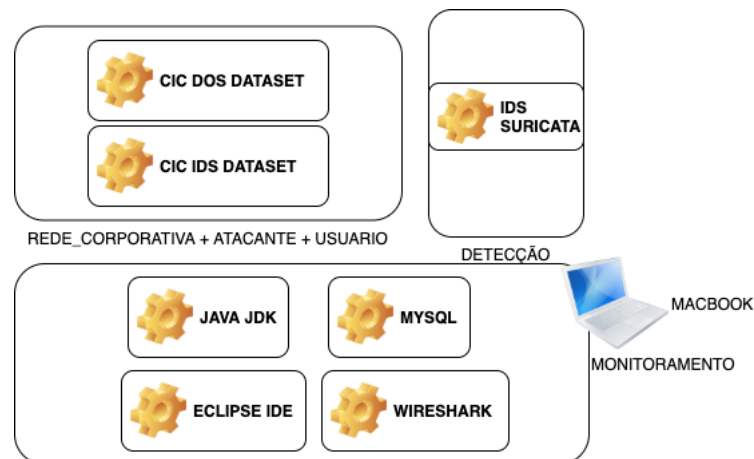


Figura 4.5: Cenário *offline* dos experimentos

Um resumo das vantagens e fraquezas dos cenários é apresentado na Tabela 4.8.

A vantagem de utilizar o cenário *online* é a flexibilidade para análise de diversos tipos de evidências capturadas, suas fraquezas compreendem a necessidade de correta configuração da ferramenta, necessitando assim de conhecimento aprofundado de sua utilização, para melhor aproveitamento.

A vantagem do cenário *offline* é utilizar uma base de dados validada pela literatura e riqueza de ataques coletados. Como fraquezas, tem-se que este cenário geralmente possui arquivos de armazenamento elevado, de difícil análise manual e não disponibilizam todas as evidências possíveis como estado de utilização da máquina ou *logs* do servidor no momento do ataque cibernético.

Os outros materiais utilizados são listados a seguir:

Cenário	Vantagens	Fraquezas
ONLINE	- Acesso a maior quantidade de evidências; - Flexibilidade para controle na execução.	- Necessário conhecimento aprofundado da ferramenta; - Configuração manual da ferramenta.
OFFLINE	- Riqueza em ataques cibernéticos já realizados; - Base validada pela literatura.	- Dificuldade na análise pelo tamanho do arquivo; - Não gera todas as evidências possíveis.

Tabela 4.8: Vantagens e fraquezas dos cenários pensados

1. Macbook Pro (equipamento)
2. Virtualbox (programa)
3. KaliLinux (Sistema operacional)
4. Linux com LAMP instalado e executando Wordpress (Sistema Operacional)
5. Sistema de Detecção de intrusos (IDS) Suricata (programa)
6. Java Development Kit (JDK) 1.8 (utilitário)
7. Eclipse Integrated Development Environment (programa)
8. *CIC DoS data set*¹ no formato pcap (Arquivo) [Simulação de ataque offline]
9. *CIC IDS data set*² no formato pcap (Arquivo) [simulação de ataque offline]
10. Wireshark (programa)
11. Slowhttptest³ (programa) [simulação de ataque online]
12. HULK.py⁴ (programa) [simulação de ataque online]
13. Goldeneye⁵ (programa) [simulação de ataque online]
14. Mysql (programa)
15. JMeter (programa)⁶

¹<https://www.unb.ca/cic/datasets/dos-dataset.html>

²<https://www.unb.ca/cic/datasets/ids-2017.html>

³<https://github.com/shekyaan/slowhttptest>

⁴<https://packetstormsecurity.com/files/112856/HULK-Http-Unbearable-Load-King.html>

⁵<https://github.com/jseidl/GoldenEye>

⁶<https://jmeter.apache.org/>

Escolhido o ataque cibernético a ser alvo do estudo, que neste caso é o DoS, procedeu-se por montar um ambiente de simulação de ataques cibernéticos do tipo negação de serviço, bem como um ambiente de monitoramento, através do IDS Suricata ou Wireshark. Após a execução dos experimentos, as evidências geradas são coletadas e analisadas através da implantação de uma arquitetura computacional desenvolvida.

A implantação da arquitetura computacional utilizada para inferência e contabilização das evidências, realça os elementos que tipificam o possível crime ocorrido. O diagrama de classes que contém um conjunto das classes que representam a estrutura da implementação da arquitetura. O sistema computacional compreende três ÁREAS com classes, cada uma voltada para uma responsabilidade, como pode ser verificado na Figura 4.6.

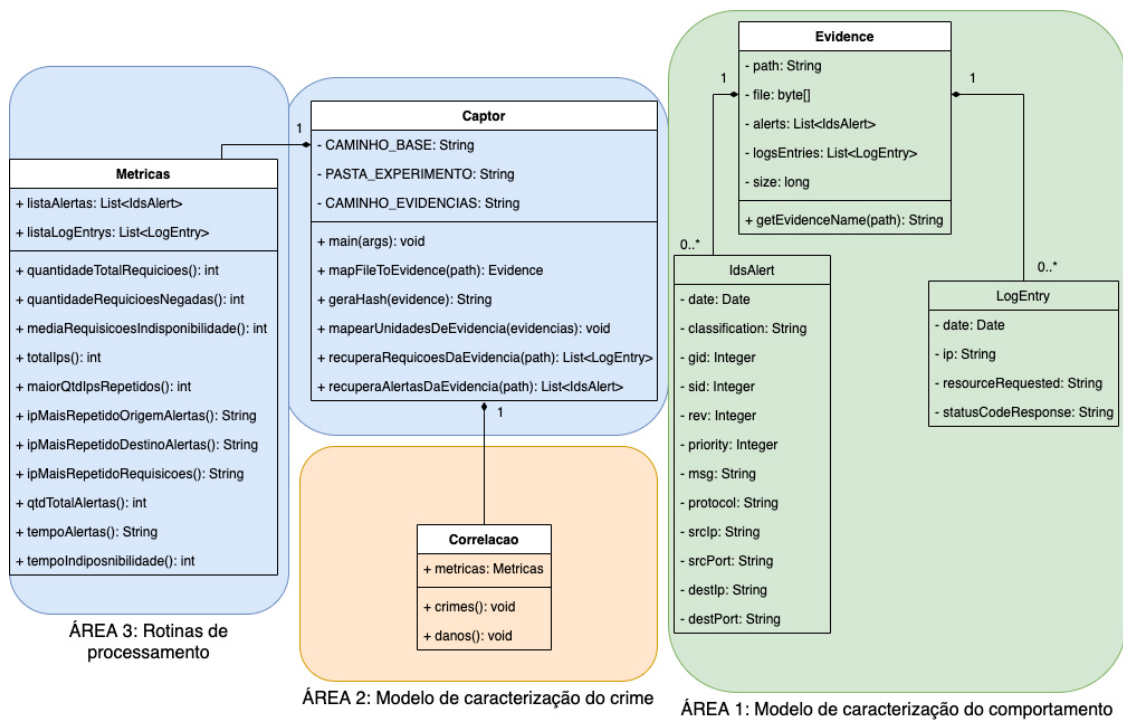


Figura 4.6: Diagrama de classes da arquitetura implantada

Na ÁREA 1 estão as classes voltadas para implementar o modelo de caracterização do comportamento das atividades maliciosas como: os registros encontrados na evidência gerada pelo servidor *web* e os registros dos alertas encontrados no IDS, oriundos das evidências: *LogEntry*, *Evidence* e *IdsAlert*.

Na ÁREA 2 está a classe responsável pela implementação do modelo de caracterização do crime, em conformidade com a legislação aplicável. Ela utiliza regras de correlação para conferir se houve crimes ou danos ocorridos.

Na Área 3 estão as classes relacionadas ao processamento das evidências. A primeira classe (Captor.java) relaciona-se à chamada das rotinas de carregamento das evidências e contagem de métricas e correlação. A segunda (Metricas.java) realiza a contagem das métricas de acordo com o modelo de comportamento previamente definido.

Na Figura 4.7, é apresentada a modelagem lógica do banco de dados do Captor Forense, que representa o local de armazenamento dos registros a serem utilizados para contabilização. Nesse modelo são armazenadas informações relativas as evidências em um banco de dados, que possibilita mediante linguagem própria (SQL) a recuperação das informações.

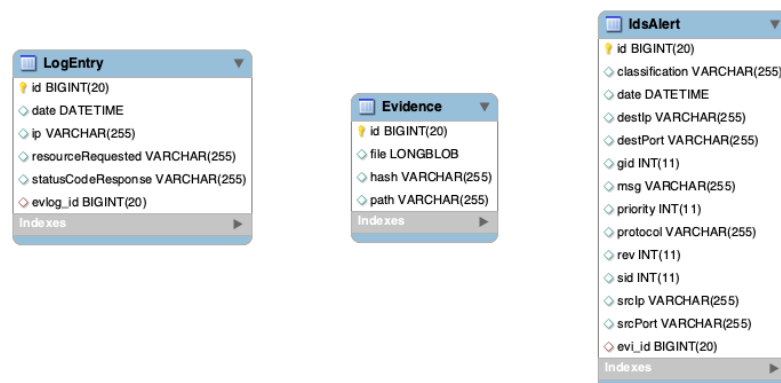


Figura 4.7: Modelagem ER da arquitetura implantada

Como protocolo para a solução desenvolvida, tem-se que as evidências geradas durante os experimentos deveriam ser coletadas e preservadas, para posterior análise. A coleta seria através transferência das evidências de sua origem até um repositório, que permitisse manipulação para correlação, para isso foi utilizada a linguagem JAVA e o banco de dados MYSQL, juntamente, através de programação no ambiente de desenvolvimento integrado Eclipse no qual, por decisão de projeto, estes foram escolhidos dentre as ferramentas disponíveis.

Para acalçar o objetivo de evidenciar os elementos que tipificam o crime, foram definidas métricas que servem como indicadores da ocorrência ou não de crimes. As medições são feitas utilizando a linguagem JAVA, através de programação orientada a objetos. Na Tabela 4.9 as métricas já previamente definidas são mapeadas as suas fontes de evidências associadas.

As métricas relacionadas ao modelo de comportamento são contadas e cronfontadas, através de correlação por regras de associação com o modelo de crimes. A correlação

Elementos (Métricas)	Tipo	Descrição	Fonte Evidência
alertas IDS	número	Quantidade de alertas sinalizados pelo IDS	Fast.log
requisições	número	requisições no servidor web	Acces.log
requisições por segundo	número	média de requisições por segundo	Access.log
requisições atendidas	número	requisições com status 200	JMeter
requisições negadas	número	requisições com status 408	JMeter
acumulo ips nas requisicoes	número	quantidade acumulada dos IPs encontrados das requisições	Access.log
acumulo ips nos alertas	número	quantidade acumulada dos IPs nos alertas do IDS	Fast.log
qtd ip mais notado nas requisições	número	quantidade de vezes do IP que mais se repetiu nas requisições	Access.log
qtd ip mais notado nos alertas	número	quantidade de vezes do IP que mais se repetiu nos alertas	Fast.log
tempo indisponivel	número	Diferença entre o primeiro e o último alerta gerados pelo IDS	Fast.log

Tabela 4.9: Métricas e sua fonte de evidência mapeadas

também utiliza a linguagem JAVA para realizar seu objetivo, na Figura 4.8, é apresentado exemplos de regras de associação utilizados.

Regra 1: SE existem ALERTAS AND existem LOGS DO SERVIDOR DO TIPO 408 ENTÃO ocorreu um crime
Regra 2: SE existem ALERTAS AND NÃO existem LOGS DO SERVIDOR DO TIPO 408 ENTÃO ocorreu um dano
Regra 3: SE NÃO existem ALERTAS AND existem LOGS DO SERVIDOR DO TIPO 408 ENTÃO ocorreu um dano

Figura 4.8: Exemplos de regras de associação.

Através da execução de experimentos realizados sob cenários configurados foi possível verificar a eficiência pela quantidade de evidências geradas e assim contabilização das métricas, bem como dos elementos encontrados que evidenciam a atividade maliciosa para a elucidação de um crime informático.

Além das métricas contabilizadas e dos elementos que evidenciam a atividade maliciosa como criminosa ou danosa, um conjunto de características resumo da execução dos experimentos, também foi computado após execução dos experimentos e é apresentado na Tabela 4.10.

As fontes de evidência são oriundas do servidor web (VM_VITIMA), IDS (VM_IDS) e do usuário (VM_USUARIO). Entende-se que o alerta do IDS já seria um forte indício para constatação do crime, mas optou-se por demonstrar também a indisponibilidade pelo

Característica	Resultados Prováveis
Evidências geradas	todas / parcial / nenhuma
Tipo execução	online / offline
Aplicação ao modelo de crimes	total / parcial / nenhuma
Aplicação ao modelo de comportamentos	total / parcial / nenhuma
Ocorrência de crimes	sim / não
Ocorrência de danos	sim / não

Tabela 4.10: Resumo da características dos a serem observadas nos experimentos após realização

registro no servidor web quando houvesse.

4.8 Fluxo de execução dos experimentos

Um fluxograma de passos realizados nos experimentos é apresentado na Figura 4.9. O artefato resultante deste fluxo é apresentação dos relatórios dos experimentos, contendo a avaliação dos mesmos.

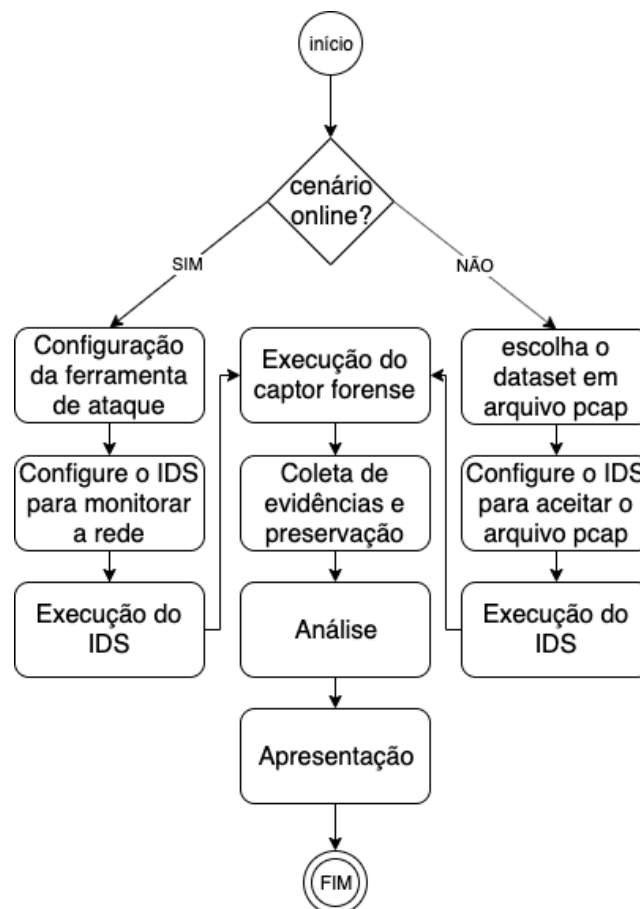


Figura 4.9: *Workflow* para experimentos

Os experimentos foram conduzidos em um computador do tipo macbook pro com

256GB de armazenamento, 8GB de memória RAM e sistema operacional MacOSx a ser denominado hospedeiro.

Na VM_IDS foi configurado um IDS Suricata (v4.1.2) para monitoramento da rede. Apesar de ser possível a utilização das regras da comunidade do suricata, optou-se pela criação de uma regra específica para monitoramento de ataques de negação de serviço. A regra utilizada é apresentada na Figura 4.10.

```

alert tcp any any -> any any (flags:S; msg:"Possible TCP DoS
attack occurring, be careful !!"; flow: stateless; threshold: type both,
track by_dst, count 70, seconds 10; classtype:attempted-dos;
sid:10001; rev:2;)

```

Figura 4.10: Regra para captura de atividades maliciosas pelo IDS

A configuração do Suricata permite que todo o fluxo de rede seja armazenado. Este passo é importante pois, além de já iniciar no processo de preservação de uma evidência, garante a replicabilidade, visto que, outros poderão ter acesso a este arquivo e realizar outras análises e métodos que acharem necessários. A seguir, explicam-se os cenários executados e seus resultados obtidos.

```

private Metricas metricas;

public Correlacao(Metricas metricas) {
    this.metricas = metricas;
}

public void crimes() {
    if (this.metricas.qtdTotalAlertas() > 0
        && this.metricas.quantidadeRequicoesNegadas() > 0) {
        System.out.println("\nCRIME OCORRIDO: Tipo Penal violado: Interromper,");
    }

    System.out.println("verificação de crimes concluída...");
}

public void danos() {
    //se possui alerta, é indicio de crime, é no minimo dano
    //ou se possui req negadas e nao possui alerta é danoso
    if ( (this.metricas.qtdTotalAlertas() > 0
        && this.metricas.quantidadeRequicoesNegadas() == 0)
        ||
        (this.metricas.qtdTotalAlertas() == 0
        && this.metricas.quantidadeRequicoesNegadas() > 0) ) {
        System.out.println("\nDANO OCORRIDO !!\n");
    }

    System.out.println("verificação de danos concluída...");
}
}

```

Figura 4.11: Regras para correlação de crimes e danos utilizadas pelo captor forense

Para todos os cenários considerou-se que para sua execução, a configuração e monitoramento através do IDS Suricata já havia sido realizada e o IDS estava em execução, sendo as regras de correlação consideradas as informadas na Figura 4.11. Importante

lembrar que outras regras de correlação podem ser criadas para melhorar a rastreabilidade de crimes ou danos ocorridos.

Para as configurações das ferramentas de ataque no cenário online, consistiu de 300 segundos de execução. Nos primeiros 20 segundos realizou-se um monitoramento para estabelecimento de uma linha base com tempos de resposta considerados normais. Nos 120 segundos seguintes foi realizado o ataque. Em seguida a ferramenta foi encerrada, parando o ataque e foi monitorado por mais 160 segundos para verificar o comportamento da arquitetura após o ataque. Foi considerado um Tempo limite de 3 segundos para o tempo de resposta.

4.9 Cenário experimento 1

Utilizando a ferramenta *slowhttptest*, realizou-se um ataque de negação de serviço do tipo *Slowris* na VM_VITIMA através do comando apresentado na Tabela 4.11. Este ataque recai sob o fato de que o protocolo HTTP necessita realizar uma confirmação para realização da comunicação, necessitando que a requisição seja completamente recebida pelo servidor antes de ser processada. Estando a requisição HTTP incompleta, o servidor mantém os recursos ocupados, até que o resto dos dados cheguem, no entanto, eles nunca chegam. Se o servidor mantém muitos recursos ocupados, isso cria uma negação do serviço.

Durante a execução da ferramenta *slowhttptest*, foi possível acompanhar através da ferramenta JMeter que rodava na VM_USUARIO simulando um usuário realizando requisições ao serviço conforme verificado na Figura 4.12. Durante a execução das 300 requisições feitas (300 requisições em 300 segundos sendo 1 req/seg) o tempo médio de resposta das requisições era de 20 milisegundos no início do experimento.

Após a execução da ferramenta de ataque esse tempo de resposta cresceu, caracterizando as requisições que foram negadas. Ao final do experimento foi constatada que das 300 amostras coletadas, 240 (80%) foram atendidas e 60 (20%) foram negadas. A Figura 4.12 mostra os momentos em que ocorreu essa indisponibilidade. Dado que requisições tinham um tempo limite de 3 segundos, nota-se que a ferramenta foi capaz de registrar esse aumento do tempo de resposta pelo servidor demonstrando os momentos de indisponibilidade do serviço.

Esta ferramenta também gera o arquivo *slowhttp.csv* e *slowhttp.html*, que armaze-

<code>slowhttptest -c 1000 -H -g -o slowhttp -i 10 -r 200 -t GET -u http://192.168.1.101 -x 24 -p 3 -l 120</code>	
-c 1000	Número de conexões estabelecidas durante o teste
-H	Modo SlowLoris, enviando solicitações HTTP inacabadas
-g -o slowhttp	Gera arquivo CSV e HTML quando o teste terminar com tempos e estados capturados no arquivo definido pelo argumento -o"
-i 10	Intervalo entre os dados de acompanhamento dos testes slowrois, ou seja, quando serão armazenados as amostras.
-r 200	Taxa de conexões realizadas por segundo pela ferramenta
-t GET	Verbo utilizado na requisição HTTP
-u http://192.168.1.101	URL da vítima
-x 24	Tamanho máximo dos dados de acompanhamento dos testes slowrois, ou seja, quando serão armazenados as amostras.
-p 3	Tempo de espera para considerar time out

Tabela 4.11: comando slowris, com parâmetros utilizados

nam reespectivamente amostras da execução do programa, como valores absolutos, bem como uma representação visual em forma de gráfico, que podem ser visualizados na Figura 4.13.

O Apêndice A.1 apresenta o relatório em sua totalidade. Nele pode ser verificado o relatório do experimento 1 realizado pelo Captor Forense. observam-se as métricas avaliadas, as verificações de integridade das evidências, ou seja, é gerada a *hash* das evidências. Outro aspecto que pode ser observado é o tipo penal violado pelo experimento realizado, esse tipo penal identificado reflete a regra de associação informada.

Para efeito de formalização em um Laudo Pericial e, como explica a Computação forense, busca-se responder algumas questões em exames forenses que envolvem detecção de intrusos em redes de computadores. Inicialmente pelas evidências geradas, verificou-se a presença de todas as evidências : *fast.log*, *access.log* e *log.pcap.1589919678*.

A primeira evidência *log.pcap.1589919678* representa o armazenamento do fluxo da rede no momento do experimento, este arquivo poderia, a partir desse momento, ser utilizado como fonte de origem para outras análises posteriores. Gerada a *hash* da evidência, outras pessoas poderiam validar o que foi encontrado, verificando que não há alterações da evidência original.



Figura 4.12: Simulação de usuário através do JMeter para experimento 1

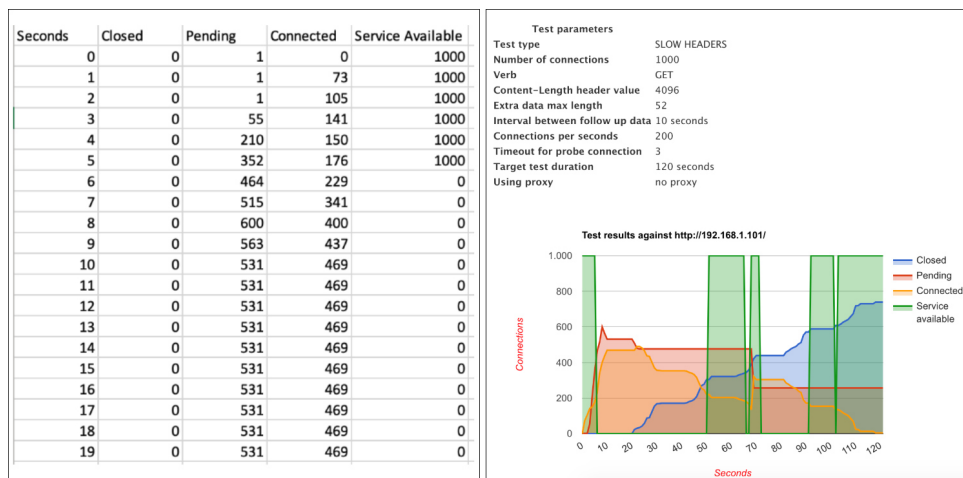


Figura 4.13: Arquivos de saída `slowhttp.csv` e `slowhttp.html` gerados pela ferramenta `slowhttpstest` após execução

A segunda evidência *fast.log* mostra os alertas sinalizados, comprovando que houve um ataque de negação de serviço ocorrido. A presença dos 6 alertas caracteriza a ocorrência do ataque de negação de serviço, bem como é possível fazer a extração dos elementos para evidenciar o ataque. Nesta evidência encontrou-se informações do *IP* de origem do atacante, bem como o *IP* da vítima. Corroborando o comportamento esperado, dado que o *IP* informado na ferramenta refletiu no alerta sinalizado. A presença dos alertas também auxiliam a estimar o tempo do crime, pois os alertas apresentam marcação do tempo, os quais são também extraídos pelo captor forense.

A terceira evidência *access.log* apresenta os *logs* do servidor web, ou seja, as requisições que foram respondidas corretamente serão percebidas neste arquivo. A média de requisições por segundo através do arquivo *access.log*, dá o indício da ocorrência de ataque, pois das 1298 requisições encontradas no servidor web, calculou-se uma média de

4,35 requisições por segundo. Em um Laudo Pericial, poderia ser feita uma analogia que considerando para o intervalo definido, seria anormal que um usuário estivesse realizando durante o mesmo segundo quase 4 requisições por segundo.

Ao final do relatório, constatou-se que, devido a presença de evidências no IDS e de indisponibilidade do serviço, houve casamento entre o descrito na norma penal, portanto, pode-se afirmar categoricamente que ocorreu um crime. Fundamentado no artigo 266 do Código Penal, há violação do tipo penal descrito.

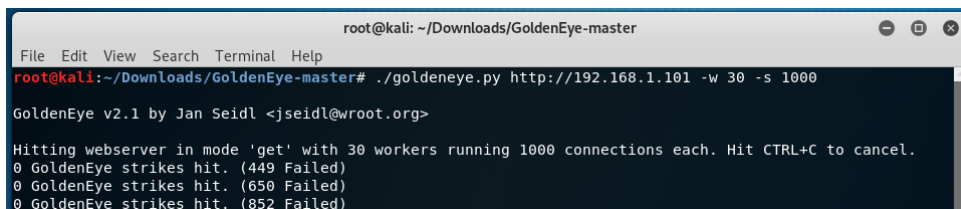
4.10 Cenário experimento 2

Utilizando a ferramenta *goldeneye*, realizou-se um ataque de negação de serviço do tipo inundação na camada de aplicação, utilizando a técnica *HTTP KeepAlive+NoCache*, no computador convidado vítima. A Tabela 4.12 mostra o comando executado, já a Figura 4.14 mostra a execução da ferramenta e mostra que, após alguns segundos, algumas requisições começam a falhar.

<code>./goldeneye.py http://192.168.1.101 -w 30 -s 1000</code>	
<code>http://192.168.1.101</code>	URL da vítima
<code>-w 30</code>	Número de threads simultâneas
<code>-s 1000</code>	Número de conexões simultâneas

Tabela 4.12: comando goldeneye, com parâmetros utilizados

O Apêndice A.2 apresenta o relatório em sua totalidade. Nele, podem ser verificados os detalhes das informações extraídas do experimento 2, realizado pelo Captor Forense. Observam-se as métricas avaliadas, as verificações de integridade das evidências bem como as contabilizações realizadas.



```
root@kali: ~/Downloads/GoldenEye-master
File Edit View Search Terminal Help
root@kali:~/Downloads/GoldenEye-master# ./goldeneye.py http://192.168.1.101 -w 30 -s 1000
GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>
Hitting webserver in mode 'get' with 30 workers running 1000 connections each. Hit CTRL+C to cancel.
0 GoldenEye strikes hit. (449 Failed)
0 GoldenEye strikes hit. (650 Failed)
0 GoldenEye strikes hit. (852 Failed)
```

Figura 4.14: Execução comando da ferramenta goldeneye

Como pode ser visualizado na Figura 4.14, após alguns instantes, de acordo com a ferramenta *goldeneye* o número de requisições começa a falhar.

Durante a execução da ferramenta *goldeneye*, foi possível acompanhar através da ferramenta JMeter que rodava na VM_USUARIO simulando um usuário realizando requisições ao serviço conforme verificado na Figura 4.15. Durante a execução das 300 requisições feitas (300 requisições em 300 segundos sendo 1 req/seg) o tempo médio de resposta das requisições era de 20 milissegundos no início do experimento. As requisições acima de 3.000 milissegundos (3 segundos) indicam os momentos da indisponibilidade do serviço.

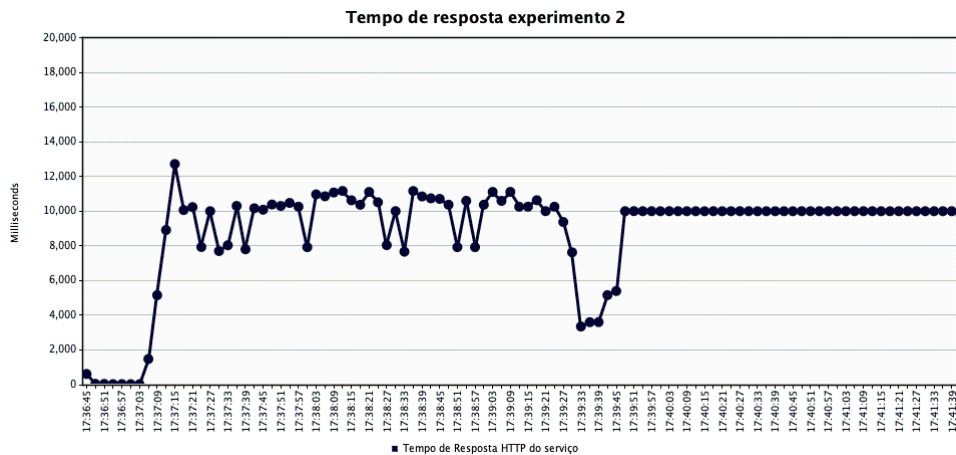


Figura 4.15: Simulação de usuário através do JMeter para experimento 1

Foi possível observar que o serviço se encontrava indisponível através da ferramenta JMeter. Das 300 amostras de requisições coletadas, 47(15,67%) foram atendidas e 253(84,33%) foram negadas, constatando assim a indisponibilidade do serviço.

Após executado o experimento e as evidências coletadas, as verificações de integridade foram realizadas, representadas pelas *hashes* geradas.

Na evidência *access.log* foram encontradas 983 requisições ao serviço. Entre a primeira requisição e a última requisição presente nesta evidência calculou-se a medida de requisições por segundo, totalizando 5,27 requisições por segundo. Um número também elevado para um usuário comum. O que prova a ocorrência da negação de serviço.

A presença dos 14 alertas sinalizados pelo IDS, evidencia que a atividade maliciosa de negação de serviço ocorreu e assim foi possível extrair informações para os elementos que evidenciam a atividade maliciosa.

Ao final do relatório, constatou-se que, devido a presença de evidências no IDS e de indisponibilidade do serviço, houve casamento entre o descrito na norma penal, portanto, pode-se afirmar categoricamente que ocorreu um crime. Fundamentado no artigo 266 do

Código Penal, há violação do tipo penal descrito.

4.11 Cenário experimento 3

Utilizando a base de dados CIC DoS *dataset* (JAZI et al., 2017), realizou-se uma verificação do comportamento da arquitetura proposta. O *dataset* utilizado foi o arquivo "AppDDos.pcap", de 4.62GB. Após sua execução pelo comando listado na Tabela 4.13, pode-se verificar parte do resultado na Figura 4.16, contendo o arquivo "attacks.txt" contendo marcações da ocorrência dos ataques disponibilizado pelo *dataset* e o arquivo "stats.log", evidência gerada pelo IDS Suricata, contendo os alertas de atividades maliciosas.

Na Figura 4.17, pode ser verificado o relatório do experimento CIC DoS *dataset* 2017 realizado pelo Captor Forense. Nele observam-se as métricas avaliadas, as verificações de integridade das evidências, ou seja, é gerada a *hash* das evidências. O Apêndice A.3 apresenta o relatório em sua totalidade.

Neste relatório observa-se também que algumas métricas aparecem com valor zerado. Isso indica que para este experimento algumas métricas não se aplicam por não constarem evidências necessárias a sua análise.

<code>suricata -c /usr/local/etc/suricata/suricata.yaml -r ...BASES_PESQUISA/AppDDos.pcap</code>	
<code>-c /usr/local/etc/suricata/suricata.yaml</code>	Informando arquivo de configuração do IDS
<code>-r ...BASES_PESQUISA/AppDDos.pcap</code>	Informando arquivo externo de simulação de tráfego de rede em formato PCAP

Tabela 4.13: Comando executado para experimento 3

A parte interessante nesse *data set* é observar como a arquitetura proposta se comporta numa situação com vários cenários em uma mesma execução. Como parte do *data set* havia um arquivo *attacks.txt* que continha marcações dos ataques ocorridos, o IP de destino associado e o tempo que ocorreu o referido ataque.

Após a execução da arquitetura, percebeu-se que esta foi capaz de capturar alertas para todos os ataques descritos no arquivo *attacks.txt*. No entanto, dos 185 alertas gerados, 168 (90%) tratam dos ataques, os outros 17 (10%) se tratariam de falsos positivos. Para individualizar cada atividade seria necessário uma análise mais minuciosa, que separasse as características intrínsecas de cada atividade e que não fosse confundida com tráfego legítimo, ou seja, de requisições de usuários verdadeiros.

A presença do alerta é grande indício da ocorrência de crimes, no entanto, seria interessante o acesso aos *logs* do servidor para enriquecer o Laudo, demonstrando o fato

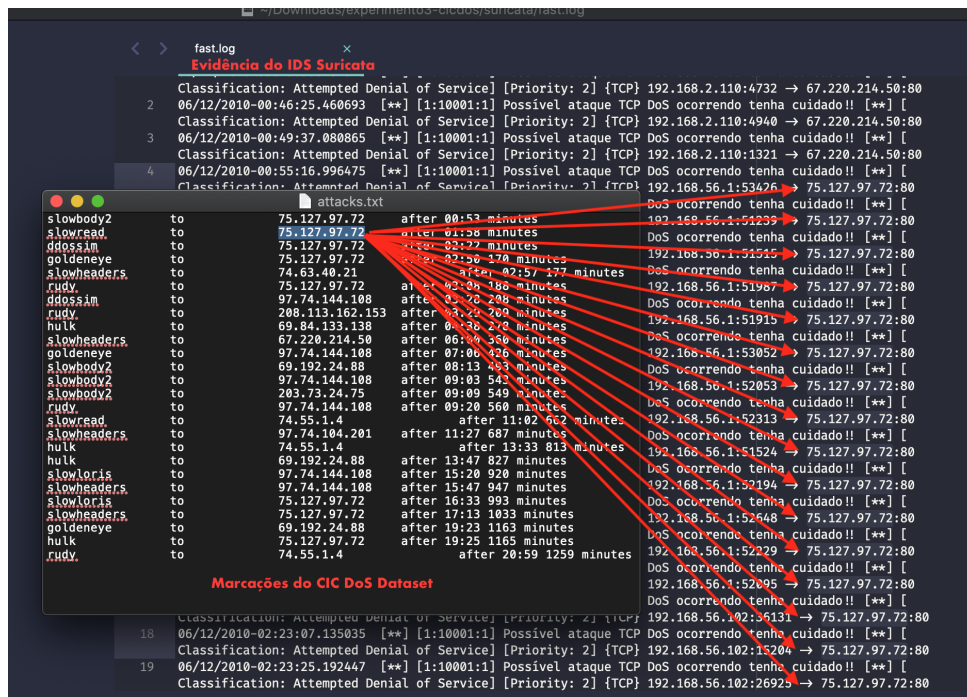


Figura 4.16: Mapeamento evidências encontradas com marcações conhecidas no CIC DoS dataset

e mostrando a verdade contada pelas evidências. Tendo este experimento a constatação apenas de Dano ocorrido. O tempo de indisponibilidade neste experimento foi bem alto, pois considerou-se a diferença entre o primeiro alerta sinalizado e o último e como neste experimento, a base de dados CIC DOS foi feita de um monitoramento de 24 horas, gerou-se essa quantidade elevada de indisponibilidade do serviço.

4.12 Cenário experimento 4

Utilizando a base de dados CIC IDS 2017 (SHARAFALDIN et al., 2018), realizou-se uma verificação do comportamento da arquitetura proposta. Neste experimento, utilizou-se o dataset "Wednesday-WorkingHours.pcap" coletado na quarta-feira, julho de 2017, de tamanho 13.42GB. Após sua execução pelo comando listado na Tabela 4.14, pode-se verificar parte do resultado na Figura 4.18, contendo o arquivo "quarta.txt" contendo marcações da ocorrência dos ataques disponibilizado pelo dataset e o arquivo "stats.log", evidência gerada pelo IDS Suricata, contendo os alertas de atividades maliciosas.

Na Figura 4.19 pode ser verificado o relatório do experimento realizado pelo Captor Forense. Nele notam-se as métricas avaliadas, as verificações de integridade das evidências, ou seja, é gerada a hash das evidências. O Apêndice A.4 apresenta o relatório em sua

```

Iniciando captor forense..

Lendo evidencias.. e Carregando metricas..

Verificacao de integridade de evidencias.. Gerando hashes..
fast.log          68aa9e09dcd4597a8dc97e762b5201cb3b5a994dcf8cc5dca26f86a1159
AppDDos.pcap     79ec7fb78649a8e577ccd6724905b73e4b32cfe383edeeb652a6fc50a73c1

Metricas do experimento: /experimento3-cicdos
Quantidade total de requisicoes: 0
Quantidade de requisicoes negadas: 0
Quantidade total de IPs encontrados: 14
Maior quantidade de IPs repetidos: 49
IP que mais se repete no servidor web: nao_se_aplica
listaIpsObservadosNosAlertas:{75.127.97.72=49, 97.74.144.108=34, 74.55.1.4=20,
IP que mais se repete nos alertas do IDS: 75.127.97.72=49
Tempo indisponivel em segundos: 83733
Quantidade total de alertas no IDS: 185
Media de requisicoes no intervalo de indisponibilidade: 0

Realizando correlacoes..
Processo finalizado, gerando relatorio de crimes..
verificação de crimes concluída...

DANO OCORRIDO !!

verificação de danos concluída...
Finalizando captor..

```

Figura 4.17: Relatório experimento 3 obtido pelo Captor Forense

totalidade.

Neste relatório observa-se também que algumas métricas aparecem com valor zerado. Isso indica que, para este experimento, algumas métricas não se aplicam por não constarem evidências necessárias a sua análise.

<code>suricata -c /usr/local/etc/suricata/suricata.yaml -r ...BASES_PESQUISA/Wednesday-WorkingHours.pcap</code>	
<code>-c /usr/local/etc/suricata/suricata.yaml</code>	Informando arquivo de configuração do IDS
<code>-r ...BASES_PESQUISA/Wednesday-WorkingHours.pcap</code>	Informando arquivo externo de simulação de tráfego de rede em formato PCAP

Tabela 4.14: Comando executado para experimento 4

Neste experimento, contendo também vários cenários em um único arquivo, foi analisado o comportamento da arquitetura. Novamente, a arquitetura foi capaz de sinalizar alertas para a ocorrência de ataques DoS identificados. A marcação informada pelo *data set* foi constatada, mostrando fortes indícios da ocorrência de crimes informáticos. Porém, este *data set* também não disponibiliza os *logs* do servidor, que seriam enriquecedores para o Laudo Pericial.

A listagem de IPs observados nos alertas também confere as marcações informadas pelo *data set*. O tempo de indisponibilidade neste experimento, pela diferença entre o primeiro alerta sinalizado e o último e como a base de dados CIC IDS foi feita a partir do monitoramento de 1 dia de monitoramento, ocasionou em um tempo de indisponibilidade elevado. Pelo fato de existirem fortes indícios de ataques, mas sem a presença dos registros

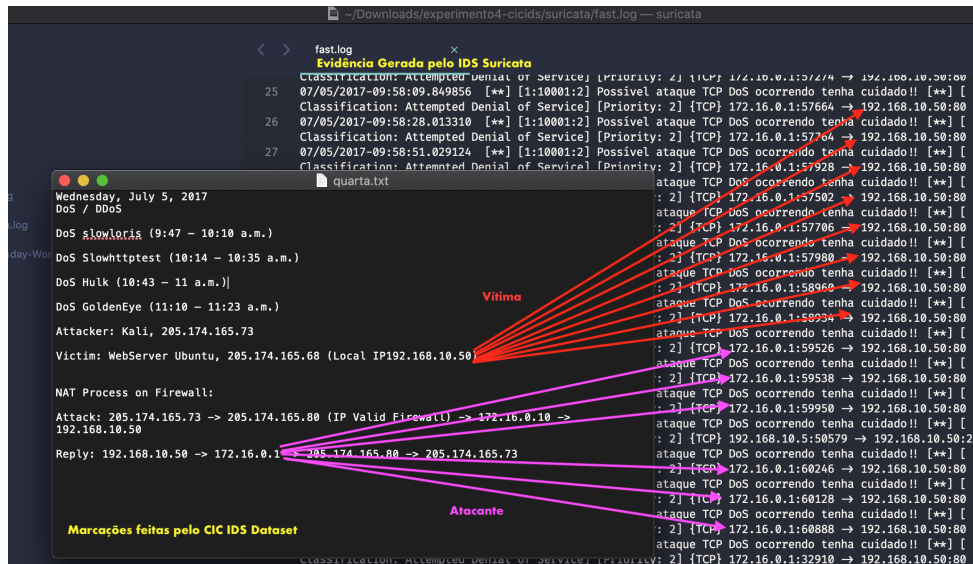


Figura 4.18: Mapeamento evidências encontradas com marcações conhecidas no CIC IDS dataset

do servidor, as atividades presentes neste experimento foram classificadas como danosas.

4.13 Cenário experimento 5

Utilizando a ferramenta *hulk.py*, realizou-se um ataque de negação de serviço do tipo *HTTP* da VM_ATACANTE para a VM_VITIMA. Na Tabela 4.15, verifica-se o comando executado.

O Apêndice A.5 apresenta o relatório em sua totalidade. Nele, encontram-se as análises, realizadas pelo Captor Forense. Percebem-se as métricas avaliadas, as verificações de integridade das evidências, ou seja, a *hash* das evidências.

<code>python hulk.py http://192.168.1.101</code>	
python	Biblioteca para execução da ferramenta.
hulk.py	Arquivo responsável pelo ataque
http://192.168.1.101	endereço da vítima

Tabela 4.15: Comando *hulk.py*, com parâmetros utilizados

Durante a execução da ferramenta *hulk.py*, foi possível acompanhar através da ferramenta JMeter que rodava na VM_USUARIO simulando um usuário realizando requisições ao serviço conforme verificado na Figura 4.20. Durante a execução das 300 requisições feitas (300 requisições em 300 segundos sendo 1 req/seg) o tempo médio de resposta das requisições era de 20 milissegundos no início do experimento.

```

Iniciando captor forense..
Lendo evidencias.. e Carregando metricas..

Verificacao de integridade de evidencias.. Gerando hashes..
fast.log          f7165e946721ecdde468ebf8d87a7c8f68b079edc8e78b53214889c58f69
Wednesday-WorkingHours.pcap  cd2674db7559a53f24bc3be3239b31570174ccaef72d10f5edc4c1a08f6186

Metricas do experimento: /experimento4-cicids
Quantidade total de requisicoes: 0
Quantidade de requisicoes negadas: 0
Quantidade total de IPs encontrados: 6
Maior quantidade de IPs repetidos: 178
IP que mais se repete no servidor web: nao_se_aplica
ListaIpsObservadosNosAlertas:{192.168.10.50=178, 162.208.20.178=21, 162.208.22.34=18, 178.172.160.3=1,
IP que mais se repete nos alertas do IDS: 192.168.10.50=178
Tempo indisponivel em segundos: 21848
Quantidade total de alertas no IDS: 220
Media de requisicoes no intervalo de indisponibilidade: 0

Realizando correlacoes..
Processo finalizado, gerando relatorio de crimes..
verificacao de crimes concluida...

DANO OCORRIDO !!

verificacao de danos concluida...
Finalizando captor..

```

Figura 4.19: Relatório experimento 4 obtido pelo Captor Forense

Após a execução da ferramenta de ataque esse tempo de resposta cresceu, caracterizando as requisições que foram negadas. Ao final do experimento foi constatada que das 300 amostras coletadas, 49 (16.33%) foram atendidas e 251 (83,67%) foram negadas. A Figura 4.20 mostra os momentos em que ocorreu essa indisponibilidade. Dado que requisições tinham um tempo limite de 3 segundos, nota-se que a ferramenta foi capaz de registrar esse aumento do tempo de resposta pelo servidor demonstrando os momentos de indisponibilidade do serviço.

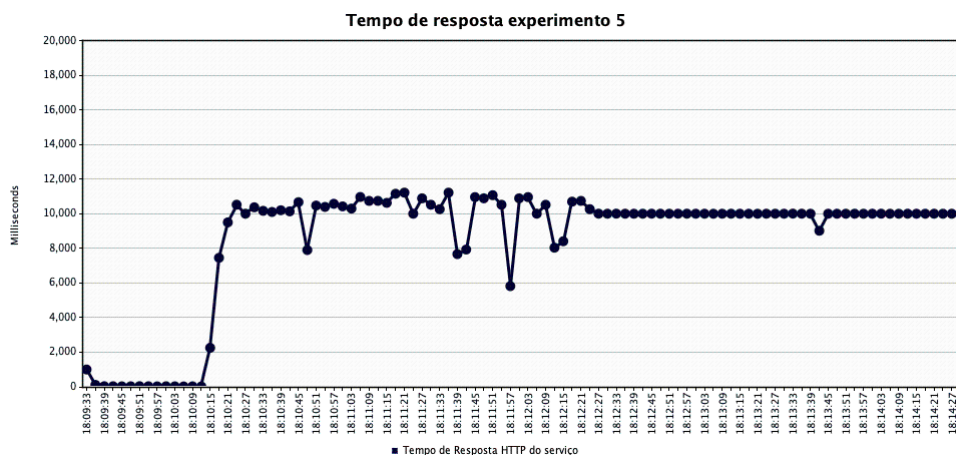


Figura 4.20: Simulação de usuário através do JMeter para experimento 5

Para efeito de formalização em um Laudo Pericial e, como explica a Computação forense, busca-se responder algumas questões em exames forenses que envolvem detecção de intrusos em redes de computadores. Inicialmente pelas evidências geradas, verificou-se a presença de todas as evidências : *fast.log*, *access.log* e *log.pcap.1589922568*.

A primeira evidência *log.pcap.1589922568* representa o armazenamento do fluxo da rede no momento do experimento, este arquivo poderia, a partir desse momento, ser utilizado como fonte de origem para outras análises posteriores. Gerada a *hash* da evidência, outras pessoas poderiam validar o que foi encontrado, verificando que não há alterações da evidência original.

A segunda evidência *fast.log* mostra os 13 alertas sinalizados, comprovando que houve um ataque de negação de serviço ocorrido. A presença de alertas caracteriza a ocorrência do ataque de negação de serviço, bem como é possível fazer a extração dos elementos para evidenciar o ataque. Nesta evidência encontrou-se informações do *IP* de origem do atacante, bem como o *IP* da vítima. Corroborando o comportamento esperado, dado que o *IP* informado na ferramenta refletiu no alerta sinalizado. A presença dos alertas também auxiliam a estimar o tempo do crime, pois os alertas apresentam marcação do tempo, os quais são também extraídos pelo captor forense.

A terceira evidência *access.log* apresenta os *logs* do servidor web, ou seja, as requisições que foram respondidas corretamente serão percebidas neste arquivo. A média de requisições por segundo através do arquivo *access.log*, dá o indício da ocorrência de ataque, pois das 1888 requisições encontradas no servidor web, calculou-se uma média de 5,68 requisições por segundo. Em um Laudo Pericial, poderia ser feita uma analogia que considerando para o intervalo definido, seria anormal que um usuário estivesse realizando durante o mesmo segundo quase 6 requisições ao serviço.

Ao final do relatório, constatou-se que, devido a presença de evidências no IDS e de indisponibilidade do serviço, houve casamento entre o descrito na norma penal, portanto, pode-se afirmar categoricamente que ocorreu um crime. Fundamentado no artigo 266 do Código Penal, há violação do tipo penal descrito.

4.14 Considerações Finais

Para o contexto da pesquisa as provas e evidências consideradas foram os *logs*, de servidor e alertas sinalizados pelo IDS, bem como arquivos que indicam a disponibilidade ou não do serviço. Os alertas por serem prova de que a atividade maliciosa descrita e configurada ocorreu e os registros de eventos do servidor por enriquecerem ainda mais a evidência de que o serviço foi indisponibilizado. Não foram monitorados os recursos

computacionais armazenamento, RAM e CPU durante os experimentos.

As evidências são objeto intrínseco da situação analisada, não é possível extrapolar, ou seja, generalizar métricas através do que foi observado, pois as provas estão diretamente ligadas à situação em questão, ou seja, foram considerados os comportamentos apenas da vítima, os recursos computacionais do ambiente controlado, configurado em situação mínima necessária para validar a pesquisa.

A proposta gira em torno de três áreas principais: Direito, Redes de Computadores e Perícia Criminal, para evidenciar os elementos das atividades maliciosas em redes de computadores que as tipificam como crime, assim foi selecionado o ataque DoS como foco da pesquisa. Proposta a metodologia de forma que ela possa ser aplicada ao contexto do ataque DoS, foi possível definir um modelo de dados tanto para o comportamento da atividade maliciosa, quanto para o crime e assim foram definidas as atividades necessárias para implantar uma arquitetura computacional que automatize este processo.

Selecionada a ferramenta computacional para monitoramento, proporcionando assim a captura das evidências das atividades maliciosas de forma que outros possam replicar os procedimentos, tem-se que a associação das atividades é consequência da cadeia de custódia mantida e preservada. Podem assim ser verificadas as atividades maliciosas que são consideradas como criminosas ou não pela tipificação, utilizando regras de correlação para descoberta do conhecimento.

5 Resultados

Como resultados tem-se que o objetivo dos experimentos foi alcançado. A resposta de perguntas básicas relacionadas a detecção de intrusos em redes de computadores como quem realizou o ataque, quais os equipamentos envolvidos, qual a origem, o destino, quando ocorreu, a técnica utilizada, foram essenciais para concluir a ocorrência do fato nos experimentos como criminosa ou danosa. A arquitetura computacional auxiliou ainda na automatização de tarefas repetitivas de forma que obtivesse melhores informações em pouco tempo.

Vale lembrar que em um caso real, na visão do perito criminal, ele terá apenas as evidências para análise bem como os relatos das pessoas envolvidas, portanto todas as informações devem partir das evidências. Na Tabela 5.1, podem ser visualizadas todas as informações coletadas e inferidas através das evidências e fatos sobre o ocorrido.

A Tabela 5.2 mostra a sumarização das referidas métricas obtidas pelos relatórios dos experimentos descritos na seção anterior, que são utilizadas para comparação e para evidenciar a adequação dos experimentos ao esperado. O rótulo **não_se_aplica** refere-se as métricas que não foram aferidas pela ausência da evidência associada.

Outro resultado foi a implantação da arquitetura computacional utilizada para inferência e contabilização das evidências, realçando assim os elementos que tipificam o possível crime ocorrido. O diagrama de classes que contém um conjunto de entidades que representam a estrutura da implementação da arquitetura, como pode ser verificado na Figura 4.6 já previamente apresentado na seção anterior.

A Tabela 5.3 mostra um resumo da execução dos experimentos. Percebe-se que os experimento 1, 2 e 5 tiveram resultado mais próximo do esperado, contando com todas as evidências geradas, total aplicação ao modelo de crimes, por conter todas as características do modelo.

Os experimentos 3 e 4 foram importantes para verificar a ocorrência de tipos penais descritos na lei, pela presença de alertas do IDS. Estes alertas já confirmam a ocorrência de atividades maliciosas e que por si só já seriam elementos para iniciar a responsabilização dos agentes infratores. No entanto, a falta de outras evidências, neste caso a falta dos

Perguntas	O que ocorreu? (fatos relatados)	Onde ocorreu ? (local do crime)	Como ocorreu? (técnica)	Quando ocorreu? (tempo)	Quem praticou? (origem)	Quem sofreu? (vítima)	Por que ? (Motivo)
<i>Exp. 1</i>	[1]	[2]	Ataque DoS	Primeiro alerta: 19/05/2020 16:21:54 Último alerta: 19/05/2020 16:23:03	192.168.1.104	192.168.1.101	Ataque DoS
<i>Exp. 2</i>	[1]	[2]	Ataque DoS	Primeiro alerta: 19/05/2020 16:37:08 Último alerta: 19/05/2020 16:39:26	192.168.1.104	192.168.1.101	Ataque DoS
<i>Exp. 3</i>	[1]	[2]	<i>Indício de ataque DoS</i>	Primeiro alerta: 12/06/2010 00:45:30 Último alerta: 13/06/2010 00:01:03	192.168.56.1 192.168.56.102 192.168.4.121 192.168.3.114 192.168.4.118 192.168.2.110 192.168.3.116 192.168.1.104 192.168.4.119 192.168.2.106 192.168.3.115 192.168.3.117 192.168.1.102 192.168.2.113 192.168.2.108 192.168.2.109	75.127.97.72 97.74.144.108 74.55.1.4 74.63.40.21 97.74.104.201 192.168.5.122 69.192.24.88 67.220.214.50 203.73.24.75 69.84.133.138 125.6.164.51 208.113.162.153 208.116.9.82 72.46.153.146	<i>dano a prestação do serviço</i>
<i>Exp. 4</i>	[1]	[2]	<i>Indício de ataque DoS</i>	Primeiro alerta: 05/07/2017 09:17:00 Último alerta: 05/07/2017 15:21:08	172.16.0.1 192.168.10.5 192.168.10.15 192.168.10.17 192.168.10.12 192.168.10.25 192.168.10.14	192.168.10.50 162.208.20.178 162.208.22.34 178.172.160.3 178.172.160.4 151.101.209.127	<i>dano a prestação do serviço</i>
<i>Exp. 5</i>	[1]	[2]	Ataque DoS	Primeiro alerta: 19/05/2020 17:10:16 Último alerta: 19/05/2020 17:12:18	192.168.1.104	192.168.1.101	Ataque DoS
[1] = em todos os experimentos os fatos relatados seriam direcionados a indicar uma indisponibilidade dos serviços [2] = em todos os experimentos o local do crime seria a rede de computadores							

Tabela 5.1: Sumarização das respostas dos resultados

Elementos (Métricas)	Exp. 1	Exp. 2	Exp. 3	Exp. 4	Exp. 5
requisições	1.298	2.020	nao_se_aplica	nao_se_aplica	1.888
requisições por segundo	4,35	5,27	nao_se_aplica	nao_se_aplica	5,68
requisições atendidas	240	47	nao_se_aplica	nao_se_aplica	49
requisições negadas	60	253	nao_se_aplica	nao_se_aplica	251
acumulo ips nas requisicoes	4	3	14	6	3
qtd ip mais notado nas requisições	896	1.589	49	178	1.521
alertas IDS	6	14	185	220	13
acumulo ips nos alertas	2	2	16	7	2
qtd ip mais notado nos alertas	5	10	148	174	12
tempo indisponivel	69	138	83.733	21.848	122

Tabela 5.2: Sumarização de métricas coletadas durante a execução dos experimentos seguindo o modelo de crime

Experimento (Cenário)	Exp. 1	Exp. 2	Exp. 3	Exp. 4	Exp. 5
Evidências geradas	TODAS	TODAS	<i>PARCIAL</i>	<i>PARCIAL</i>	TODAS
Tipo execução	online	online	<i>offline</i>	<i>offline</i>	online
Aplicação ao modelo de crimes	TOTAL	TOTAL	<i>PARCIAL</i>	<i>PARCIAL</i>	TOTAL
Aplicação ao modelo de comportamentos	TOTAL	TOTAL	TOTAL	TOTAL	TOTAL
Ocorrência de crimes	SIM	SIM	<i>NÃO</i>	<i>NÃO</i>	SIM
Ocorrência de danos	SIM	SIM	SIM	SIM	SIM
Tipo Penal identificado	Interromper	Interromper	-	-	Interromper

Tabela 5.3: Sumarização de resultados de experimentos

registros do servidor *web*, impediria uma melhor fundamentação para responsabilização dos agentes, mas ainda assim gera um grande indício da ocorrência de crimes.

O ponto principal desses experimentos foi validar que a arquitetura computacional é capaz de analisar tanto cenários *online* quanto *offlines*, para assim conseguir diminuir o esforço humano em uma análise forense em redes de computadores. Outro ponto importante foi que estes experimentos continham vários cenários de ataques DoS em um mesmo arquivo e a arquitetura computacional foi capaz de identificá-los e apresentar as informações relevantes para o especialista responsável. Pelos fatos acima relatados, entende-se também que estes experimentos adequaram-se de forma satisfatória ao esperado.

5.1 Discussão

Percebe-se que, seguindo as atividades definidas na metodologia MeviDoS, é possível extrair as informações básicas necessárias para tipificação penal de crimes informáticos como: a origem, o destino, o tempo do crime, o local, a motivação e a técnica utilizada. Os cenários idealizados também foram importantes para validação da metodologia proposta, mostrando adequação em situações de simulação *online* e *offline* próximas da realidade.

Nos experimentos do tipo *online* o monitoramento foi armazenado pelo IDS em arquivo do tipo PCAP (*log.pcap.<NUMBER>*) que possibilitaria uma replicação do experimento de forma integral, já nos do tipo *offline* esse armazenamento não foi necessário, visto que estes já originam de arquivos do tipo PCAP. A informação de verificação de integridade das evidências foi gerada em todos os experimentos, tendo o princípio da replicabilidade garantido, de modo que outras pessoas possam chegar ao mesmo resultado observado por este trabalho. A expectativa era de que os experimentos do tipo *online* fossem executados até que o servidor não conseguisse responder.

Os experimentos 1, 2 e 5 comportaram-se como esperado, gerando evidências fortes da ocorrência de atividades maliciosas interrompendo o serviço e possibilitando um avanço numa investigação forense para responsabilização de agentes infratores.

Nos experimentos 3 e 4, o que se propõe é a execução da arquitetura em uma base de dados já conhecida na literatura. Demonstrando assim a geração de alertas que seriam indicativo de ocorrência de crimes, ou seja, as atividades maliciosas nestes experimentos podem ser consideradas como criminosas, ou seja, o modelo de comportamentos seria

bem adequado, visto que pode-se verificar o comportamento das atividades maliciosas que ocorrem e, conforme descrito pelos autores, os ataques foram executados até que a indisponibilidade do serviço fosse alcançada.

Para estes experimentos, no entanto, não há como obter total adequação ao modelo de crimes, por falta de algumas evidências. O que tornam os fatos concluídos apenas como indícios de crimes e a falta de evidências do monitoramento do servidor *web* empobreceria um documento formal de responsabilização de agentes infratores. Estes experimentos foram feitos, no entanto, para verificar o máximo de informações possíveis para formalização e que a arquitetura computacional é capaz de encontrar atividades maliciosas tanto quanto possível.

Munido dessas informações poderia o perito criminal proceder com a solicitação da quebra de sigilo junto à ISP para determinar a pessoa que realizou os ataques e, portanto, cometeu a infração penal. Esta etapa é algo que está além do escopo pretendido por este trabalho, mas é um passo importante para responsabilização do agente infrator em redes de computadores.

6 Conclusão, Publicações e Trabalhos Futuros

Este trabalho apresentou a MeviDos, uma proposta de metodologia para análise forense em redes de computadores, com foco em evidenciar os elementos necessários para criminalização dos ataques de negação de serviço e com o objetivo auxiliar o perito forense, interessado em resolver crimes dessa natureza, embasado pela lei de crimes informáticos (Lei nº. 12.737/2012).

Essa metodologia baseou-se no formalismo jurídico da busca por elementos constitutivos dos ataques cibernéticos, bem como na base legal existente. Além disso, forneceu um conjunto de atividades que, seguindo os princípios da computação forense, permitiram a tipificação dos crimes cometidos, a identificação de sua origem, autor, tempo do crime, alvo, "iter criminis" (caminho do crime), assim como o bem jurídico atingido.

Os resultados dos experimentos mostram impressões positivas do estudo, visto que dos 5 experimentos realizados 3 (60%) tiveram total adequação ao esperado, podendo ser classificados como atividades criminosas, e os outros 2 (40%) apenas adequação parcial por falta de evidências disponibilizadas, podendo apenas serem classificadas como atividades danosas. Com os elementos necessários para individualização encontrados, é possível assim prosseguir com a responsabilização de agentes infratores.

Os resultados dos experimentos são classificados como satisfatórios visto que foi possível através da metodologia MeviDoS, subsidiada pela implementação da arquitetura computacional e sua utilização, para a categorização da ocorrência de ataques de negação de serviço como criminos ou danosos. A sua correta utilização mostra que seguindo um conjunto de procedimentos, pautada em um método científico é possível embasar uma responsabilização para agentes infratores de ataques cibernéticos.

6.1 Publicações

Para divulgar os resultados obtidos ao longo desta pesquisa foi realizada a publicação de um artigo científico em periódico conforme mostrado a seguir:

- Cantanhede, Hans Newton Fonseca; Vale, Samyr Béliche. Computer Network Fo-

rensic Assistance Methodology Focused on Denial of Service Attacks. International Journal of Computer Applications 177(33):1-11. ISSN: 0975-8887. Publicado dia 16 de Janeiro de 2020. DOI: 10.5120/ijca2020919788. ISBN : 973-93-80900-77-4. **Qualis Capes:** A4 pelo Qualis Capes.

Situação: Publicado

6.2 Trabalhos Futuros

Como indicação de trabalhos futuros, sugerem-se :

1. Análise de outras métricas para enriquecer e fortalecer as conclusões do Laudo como por exemplo a observação e do estado físico das máquinas do experimento para analisar as alterações de utilização dos recursos como memória, processamento e armazenamento. Outras evidências a nível mais baixos da pilha de protocolos do TCP/IP, como fluxos de rede e conexões efetivamente realizadas a pela troca de pacotes na rede;
2. Coleta de evidências e sua publicação em uma *blockchain* e assim o aumento de sua validade perante o juiz;
3. A possibilidade de demonstrar a tipicidade do crime, apenas com um fluxo de rede representado pelo arquivo PCAP como evidência. Através de uma engenharia reversa nos pacotes, demonstrar o crime evidenciando os elementos que tipificam o crime.
4. Outros tipos de crimes que possam ser considerados pela lei de crimes informáticos, devem ser apontados para aumentar a responsabilização de agentes infratores.
5. A aplicação desta metodologia apresentada em outros artigos penais como o artigo 154-A da incluído pela lei 12.737/12.
6. Outras implantações de arquitetura computacional podem ser consideradas, objetivando alcançar outros crimes. Selecionando outras tecnologias e medindo assim sua eficiência na identificação dos elementos para tipificação penal de crimes informáticos.

Referências Bibliográficas

- ABOMHARA, M.; KØIEN, G. M. **Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks**. [S.l.], 2015. v. 4, n. 1, 65-88 p. Disponível em: <<https://doi.org/10.13052%2Fjcs2245-1439.414>>. Citado na página 33.
- ALIM, M.; RIADI, I.; PRAYUDI, Y. **Live Forensics Method for Analysis Denial of Service (DOS) Attack on Routerboard**. [S.l.], 2018. v. 180, n. 35, 23–30 p. Disponível em: <<https://doi.org/10.5120%2Fijca2018916879>>. Citado na página 56.
- ALLEN, W. **Computer Forensics**. [S.l.], 2005. v. 3, n. 4, 59–62 p. Disponível em: <<https://doi.org/10.1109%2Fmsp.2005.95>>. Citado na página 39.
- ALSMADI, I.; ALAZAB, M. **A Model Based Approach for the Extraction of Network Forensic Artifacts**. [S.l.], 2017. Disponível em: <<https://doi.org/10.1109%2Ffcc.2017.13>>. Citado na página 48.
- ARASTEH, A. R.; DEBBABI, M.; SAKHA, A.; SALEH, M. **Analyzing multiple logs for forensic evidence**. [S.l.], 2007. v. 4, 82–91 p. Disponível em: <<https://doi.org/10.1016%2Fj.diin.2007.06.013>>. Citado na página 23.
- ÅRNES, A.; HAAS, P.; VIGNA, G.; KEMMERER, R. A. **Digital Forensic Reconstruction and the Virtual Security Testbed ViSe**. [S.l.], 2006. 144–163 p. Disponível em: <https://doi.org/10.1007%2F11790754_9>. Citado na página 53.
- AZEVEDO, A. M. L.; NETO, O. F. **O bem jurídico penal: duas visões sobre a legitimação do direito penal a partir da teoria do bem jurídico**. [S.l.], 2018. Citado na página 19.
- BASTOS, R. B. **A situação do registro contábil e patrimonial dos ativos de infraestrutura pelos cinco municípios mais populosos do Rio Grande do Sul**. [S.l.], 2018. Citado na página 19.
- BRASIL. **Código Penal. DECRETO-LEI No 2.848, DE 7 DE DEZEMBRO DE 1940**. [S.l.], 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Citado na página 38.
- BRASIL. **LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012**. [S.l.], 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm>. Citado 2 vezes nas páginas 38 e 39.
- BRASIL. **Procedimento operacional padrão : perícia criminal**. [S.l.], 2013. Disponível em: <https://www.justica.gov.br/sua-seguranca/seguranca-publica/analise-e-pesquisa/download/pop/procedimento_operacional_padrao-pericia_criminal.pdf>. Citado 4 vezes nas páginas 50, 51, 52 e 53.

- BROWN, D. J.; SUCKOW, B.; WANG, T. **A survey of intrusion detection systems**. [S.l.], 2002. Disponível em: <<https://pdfs.semanticscholar.org/0744/c1c4c8ae5048131931dbea4acf4560b6f521.pdf>>. Citado na página 43.
- BSI, B. S. **Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence**. [S.l.], 2012. Disponível em: <<https://doi.org/10.3403%2F30207800u>>. Citado na página 39.
- CADWALLADR, C.; GRAHAM-HARRISON, E. **Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach**. [S.l.], 2018. v. 17, 22 p. Citado na página 22.
- CARRIER, B. **The sleuth kit**. [S.l.], 2011. Disponível em: <<https://www.sleuthkit.org/>>. Citado 3 vezes nas páginas 46, 47 e 52.
- CERT.BR. **Incidentes Reportados ao CERT.br – Janeiro a Dezembro de 2019**. [S.l.], 2019. Disponível em: <<https://www.cert.br/stats/incidentes/2019-jan-dec/tipos-ataque.html>>. Citado na página 21.
- CHEN, Y. **Integrated and Intelligent Manufacturing: Perspectives and Enablers**. [S.l.], 2017. v. 3, n. 5, 588–595 p. Disponível em: <<https://doi.org/10.1016%2Fj.eng.2017.04.009>>. Citado na página 19.
- CHEN, Y. ping; LIU, D. liang; GUO, R. **Security and precaution on computer network**. [S.l.], 2010. Disponível em: <<https://doi.org/10.1109%2Ffitme.2010.5656536>>. Citado na página 30.
- COVER, A.; POSSER, R. D.; CAMPOS, J. P. A.; RIEDER, R. **Methodology of Communication between a Criminal Database and a Virtual Reality Environment for Forensic Study**. [S.l.], 2017. Disponível em: <<https://doi.org/10.1109%2Fsvr.2017.35>>. Citado na página 36.
- CRESPO, M. X. de F. **Do conhecimento da ilicitude em face da expansão do direito penal**. [S.l.], 2012. Disponível em: <<https://doi.org/10.11606%2Ft.2.2012.tde-22042013-085043>>. Citado na página 36.
- DINIZ, G.; MUGGAH, R.; GLENNY, M. **Deconstructing cyber security in brazil**. [S.l.], 2014. Citado na página 21.
- ELDOW, O.; CHAUHAN, P.; LALWANI, P.; M.B.POTDAR. **Computer network security ids tools and techniques (snort/suricata)**. [S.l.], 2016. v. 6, n. 1, 593 p. Disponível em: <<http://www.ijsrp.org/research-paper-0116.php?rp=P495049>>. Citado 3 vezes nas páginas 22, 41 e 42.
- FÁBIO, A. C. **Qual foi o alcance de crimes cibernéticos em 2017. E como eles são encarados**. [S.l.], 2018. Acessado em 29/04/2018. Disponível em: <<https://www.nexojornal.com.br/expresso/2018/02/05/Qual-foi-o-alcance-de-crimes-cibern%C3%A9ticos-em-2017.-E-como-eles-s%C3%A3o-encarados>>. Citado na página 21.
- GARG, A.; MAHESHWARI, P. **Performance analysis of snort-based intrusion detection system**. [S.l.], 2016. v. 1, 1–5 p. Citado na página 42.

- GATTO, V. H. G. **Tipicidade penal dos crimes cometidos na internet**. [S.l.], 2011. Disponível em: <<https://ambitojuridico.com.br/edicoes/revista-91/tipicidade-penal-dos-crimes-cometidos-na-internet/>>. Citado na página 35.
- GUPTA, B. B.; BADVE, O. P. **Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a Cloud computing environment**. [S.l.], 2016. v. 28, n. 12, 3655–3682 p. Disponível em: <<https://doi.org/10.1007%2Fs00521-016-2317-5>>. Citado 2 vezes nas páginas 21 e 42.
- HAMPTON, N.; BAIG, Z. A. Timestamp analysis for quality validation of network forensic data. In: **Network and System Security**. Springer International Publishing, 2016. p. 235–248. Disponível em: <https://doi.org/10.1007%2F978-3-319-46298-1_16>. Citado 2 vezes nas páginas 49 e 52.
- JAYAKRISHNAN, A. R.; VASANTHI, V. **Empirical Survey on Advances of Network Forensics in the Emerging Networks**. [S.l.], 2018. v. 7, n. 1, 38–46 p. Disponível em: <<https://doi.org/10.17781%2Fp002320>>. Citado 3 vezes nas páginas 24, 39 e 45.
- JAZI, H. H.; GONZALEZ, H.; STAKHANOVA, N.; GHORBANI, A. A. **Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling**. [S.l.], 2017. v. 121, 25–36 p. Disponível em: <<https://doi.org/10.1016%2Fj.comnet.2017.03.018>>. Citado 4 vezes nas páginas 24, 48, 52 e 78.
- KASPERSKY. **Brasil é líder em rede de bot multifuncional**. [S.l.], 2018. Acessado no dia 29/04/2019. Disponível em: <<https://www.kaspersky.com.br/blog/redes-bots-multifuncionais/10756/>>. Citado na página 20.
- KHAN, R.; HASAN, M. **NETWORK THREATS, ATTACKS AND SECURITY MEASURES: A REVIEW**. [S.l.], 2017. v. 8, n. 8, 116–120 p. Disponível em: <<https://doi.org/10.26483%2Fijarcs.v8i8.4641>>. Citado na página 23.
- KHAN, S.; GANI, A.; WAHAB, A. W. A.; SHIRAZ, M.; AHMAD, I. **Network forensics: Review, taxonomy, and open challenges**. [S.l.], 2016. v. 66, 214–235 p. Disponível em: <<https://doi.org/10.1016%2Fj.jnca.2016.03.005>>. Citado na página 24.
- KHOBRAGADE, P. K.; MALIK, L. G. **Data generation and analysis for digital forensic application using data mining**. [S.l.], 2014. 458–462 p. Citado 2 vezes nas páginas 46 e 52.
- KOUMIDIS, K.; KOLIOS, P.; PANAYIOTOU, C. **Optimizing Blockchain for data integrity in Cyber Physical Systems**. [S.l.], 2018. Disponível em: <<https://doi.org/10.14236%2Fwic%2Fics2018.9>>. Citado na página 61.
- KUMARAVEL, A.; NIRAIISHA, M. **Multi-classification approach for detecting network attacks**. [S.l.], 2013. Disponível em: <<https://doi.org/10.1109%2Fcict.2013.6558266>>. Citado 2 vezes nas páginas 24 e 45.
- KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet**. [S.l.], 2013. Citado 2 vezes nas páginas 30 e 32.

- LANDAUER, M.; WURZENBERGER, M.; SKOPIK, F.; SETTANNI, G.; FILZMOSER, P. **Dynamic log file analysis: An unsupervised cluster evolution approach for anomaly detection**. [S.l.], 2018. v. 79, 94–116 p. Disponível em: <<https://doi.org/10.1016%2Fj.cose.2018.08.009>>. Citado na página 22.
- LATHA, S.; PRAKASH, S. J. **A survey on network attacks and Intrusion detection systems**. [S.l.], 2017. Disponível em: <<https://doi.org/10.1109%2Ficaccs.2017.8014614>>. Citado 2 vezes nas páginas 22 e 24.
- LEITE, L. M. **Políticas de segurança física e lógica de tecnologia da informação em redes de computadores e seus ativos**. [S.l.], 2018. Citado na página 19.
- MALLIKARJUNAN, K. N.; MUTHUPRIYA, K.; SHALINIE, S. M. **A survey of distributed denial of service attack**. [S.l.], 2016. Disponível em: <<https://doi.org/10.1109%2Fisco.2016.7727096>>. Citado 2 vezes nas páginas 45 e 52.
- MARTINES, F.; COELHO, G. **VULNERABILIDADE CIBERNÉTICA - CNJ sofre ataque de hacker e dados de milhares de pessoas são vazados**. [S.l.], 2019. Acessado em 29/04/2019. Disponível em: <<https://www.conjur.com.br/2019-abr-01/cnj-sofre-ataque-hacker-dados-milhares-pessoas-vazam>>. Citado na página 20.
- MARTINI, B.; CHOO, K.-K. R. **An integrated conceptual digital forensic framework for cloud computing**. [S.l.], 2012. v. 9, n. 2, 71–80 p. Disponível em: <<https://doi.org/10.1016%2Fj.diin.2012.07.001>>. Citado na página 39.
- MATE, M. H.; KAPSE, S. R. **Network Forensic Tool – Concept and Architecture**. [S.l.], 2015. Disponível em: <<https://doi.org/10.1109/csnt.2015.204>>. Citado na página 63.
- MAUÉS, M. B. **Modelagem de ameaças antiforenses aplicada ao processo forense digital**. [S.l.], 2016. Citado 5 vezes nas páginas 21, 23, 49, 50 e 52.
- MEISNER, M. **FINANCIAL CONSEQUENCES OF CYBER ATTACKS LEADING TO DATA BREACHES IN HEALTHCARE SECTOR**. [S.l.], 2018. v. 6, n. 3, 63 p. Disponível em: <<https://doi.org/10.12775%2Fcfjfa.2017.017>>. Citado na página 23.
- MEROUANE, M. **An approach for detecting and preventing DDoS attacks in campus**. [S.l.], 2017. v. 51, n. 1, 13–23 p. Disponível em: <<https://doi.org/10.3103%2Fs0146411616060043>>. Citado 5 vezes nas páginas 24, 43, 44, 46 e 52.
- MIRAZ, M.; ALI, M.; EXCELL, P.; PICKING, R. **Internet of Nano-Things, Things and Everything: Future Growth Trends**. [S.l.], 2018. v. 10, n. 8, 68 p. Disponível em: <<https://doi.org/10.3390%2Ffi10080068>>. Citado na página 28.
- MOLINA, D.; SILVEIRA, S. R.; SANTOS, F. B. dos. **Um Estudo de Caso sobre a Implantação de um Ambiente de Segurança de Redes de Computadores**. [S.l.], 2019. v. 9, n. 1. Citado na página 19.
- NERES, A. D. J.; SANCHES, C. P. **Procedimento Operacional Padrão na PMGO**. [S.l.], 2018. v. 11, n. 1. Disponível em: <<https://doi.org/10.29377/rebsp.v11i1.340>>. Citado 2 vezes nas páginas 50 e 52.

- NETO, U. A. de C.; ROCHA, P. B. N. de M. **ASPECTOS CONSTITUCIONAIS E PENAS DA INTERCEPTAÇÃO TELEMÁTICA: sua força probante.** [S.l.], 2019. v. 1, n. 3. Citado na página 23.
- NUCCI, G. de S. **Manual de direito penal.** [S.l.], 2019. Citado na página 36.
- OLIVEIRA, L. G. C. de; DANI, M. G. S. **Os crimes virtuais e a impunidade real.** [S.l.], 2011. Disponível em: <<https://ambitojuridico.com.br/edicoes/revista-91/os-crimes-virtuais-e-a-impunidade-real/>>. Citado 2 vezes nas páginas 22 e 35.
- OWASP, T. **Top 10-2017.** [S.l.], 2017. Citado 3 vezes nas páginas 19, 20 e 22.
- P., C.; S., M. C.; S., B. Cybercrime and digital forensics – technologies and approaches. In: **DAAAM International Scientific Book 2014.** DAAAM International Vienna, 2014. p. 525–542. Disponível em: <<https://doi.org/10.2507%2Fdaaam.scibook.2014.42>>. Citado na página 53.
- PAINE, J. **System and Method for Cyber Security Threat Detection.** [S.l.], 2018. US Patent App. 15/699,777. Citado 2 vezes nas páginas 46 e 52.
- PERLIN, T.; NUNES, R. C.; KOZAKEVICIUS, A. de J. **Detecção de Anomalias em Redes de Computadores e o uso de Wavelets.** [S.l.], 2011. v. 3, n. 1, 2–15 p. Disponível em: <<https://doi.org/10.5335%2Frbca.2011.002>>. Citado 2 vezes nas páginas 45 e 52.
- PILLI, E. S.; JOSHI, R.; NIYOGI, R. **Network forensic frameworks: Survey and research challenges.** [S.l.], 2010. v. 7, n. 1-2, 14–27 p. Disponível em: <<https://doi.org/10.1016%2Fj.diin.2010.02.003>>. Citado 2 vezes nas páginas 24 e 40.
- PURBOYO, T. W.; KUSPRIYANTO. **Methods for strengthening a Computer network security.** [S.l.], 2013. Disponível em: <<https://doi.org/10.1109%2Ffrict-icevt.2013.6741559>>. Citado na página 30.
- RAY, B. **Extending the Blockchain: Ensuring Transactional Integrity in Relational Data via Blockchain Technology.** [S.l.], 2019. Disponível em: <<https://doi.org/10.2172/1557484>>. Citado na página 61.
- ROCHA, C. B. **A evolução criminológica do Direito Penal: Aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012.** [S.l.], 2013. Disponível em: <<https://jus.com.br/artigos/25120/a-evolucao-criminologica-do-direito-penal-aspectos-gerais-sobre-os-crimes-ciberneticos-e-a-lei-12-737-2012>>. Citado na página 35.
- RODRIGUES, C. V.; SILVA, M. T. da; TRUZZI, O. M. S. **Perícia criminal: uma abordagem de serviços.** [S.l.], 2010. v. 17, n. 4, 843–857 p. Disponível em: <<https://doi.org/10.1590%2Fs0104-530x2010000400016>>. Citado 3 vezes nas páginas 34, 35 e 37.
- RODRIGUES, R. **Há um ano, WannaCry infectava mais de 200 mil sistemas. Maior infecção de ransomware da história causou prejuízos em 150 países.** [S.l.], 2018. Disponível em: <<https://www.kaspersky.com.br/blog/um-ano-wannacry-ransomware/10282/>>. Citado na página 21.

- ROESCH, M. **Snort: Lightweight intrusion detection for networks**. [S.l.], 1999. v. 99, 229–238 p. Disponível em: <https://www.usenix.org/legacy/event/lisa99/full_papers/roesch/roesch.pdf>. Citado 3 vezes nas páginas 22, 42 e 43.
- ROMANI, A. **Hackers se passam por Netflix em novo golpe cibernético**. [S.l.], 2019. Acessado em 02/05/2019. Disponível em: <<https://veja.abril.com.br/economia/hackers-se-passam-por-netflix-em-novo-golpe-cibernetico/>>. Citado na página 20.
- SANDERS, C. **Practical packet analysis: Using Wireshark to solve real-world network problems**. [S.l.], 2017. Citado 2 vezes nas páginas 48 e 52.
- SANTANA, D. R. D. [graduação| monografia] sistema de provas nos crimes virtuais os desafios da instrução probatória em ações penais relativas aos crimes virtuais no brasil. **Portal de Trabalhos Acadêmicos**, v. 3, n. 1, 2019. Citado na página 23.
- SANTOS, R. H. d. et al. **Contabilidade forense na investigação criminal: aplicação da prova pericial contábil nos processos criminais de lavagem de capitais**. [S.l.], 2019. Citado 2 vezes nas páginas 47 e 52.
- SCHNEIDER, J. V. **Brasil é o 3º em ranking de ataques cibernéticos - Jornal do Comércio**. [S.l.], 2019. Acessado em 02/05/2019. Disponível em: <https://www.jornaldocomercio.com/_conteudo/economia/2019/02/672396-brasil-e-o-3-em-ranking-de-ataques-ciberneticos.html>. Citado 2 vezes nas páginas 20 e 21.
- SCHWAB, K. **THE FOURTH INDUSTRIAL REVOLUTION (INDUSTRY 4.0) A SOCIAL INNOVATION PERSPECTIVE**. [S.l.], 2018. Disponível em: <<https://doi.org/10.25073%2F0866-773x%2F97>>. Citado na página 19.
- SHARAFALDIN, I.; LASHKARI, A. H.; GHORBANI, A. A. **Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization**. [S.l.], 2018. Disponível em: <<https://doi.org/10.5220%2F0006639801080116>>. Citado 4 vezes nas páginas 24, 48, 52 e 79.
- SILVA, A. A. G. da. **A perícia forense no Brasil**. [S.l.], 2009. Disponível em: <<https://doi.org/10.11606/d.3.2009.tde-11082010-152328>>. Citado 2 vezes nas páginas 51 e 52.
- SILVA, A. C. Q.; BEZERRA, M. D.; SANTOS, W. T. **Relações Jurídicas Virtuais: Análise de Crimes Cometidos por meio do uso da Internet**. [S.l.], 2016. v. 21, n. 1, 7–28 p. Disponível em: <<https://periodicos.unicesumar.edu.br/index.php/revcesumar/article/view/3952>>. Citado na página 51.
- S.MANGRULKAR, N.; PATIL, A. R. B.; PANDE, A. S. **Network Attacks and Their Detection Mechanisms: A Review**. [S.l.], 2014. v. 90, n. 9, 37–39 p. Disponível em: <<https://doi.org/10.5120%2F15606-3154>>. Citado 2 vezes nas páginas 24 e 45.
- SOUZA, E. B. de; SANTOS, A. F. P. dos. **Um dataset de ataques Low Rate DDoS**. [S.l.], 2018. v. 35, n. 2, 49–56 p. Disponível em: <http://rmct.ime.eb.br/arquivos/RMCT_2_tri_2018/RMCT_41518.pdf>. Citado 2 vezes nas páginas 48 e 52.
- STATS, I. W. **Internet World Stats**. [S.l.], 2018. Acessado no dia 29/04/2018. Disponível em: <<https://www.internetworldstats.com/south.htm>>. Citado na página 21.

- STEPHENSON, P. **Structured Investigation of Digital Incidents in Complex Computing Environments**. [S.l.], 2003. v. 12, n. 3, 29–38 p. Disponível em: <<https://doi.org/10.1201%2F1086%2F43327.12.3.20030701%2F43624.5>>. Citado 4 vezes nas páginas 24, 40, 50 e 52.
- STUDIAWAN, H.; SOHEL, F.; PAYNE, C. **A survey on forensic investigation of operating system logs**. [S.l.], 2019. v. 29, 1–20 p. Disponível em: <<https://doi.org/10.1016%2Fj.diin.2019.02.005>>. Citado 3 vezes nas páginas 28, 49 e 52.
- TAVALLAEE, M.; BAGHERI, E.; LU, W.; GHORBANI, A. A. **A detailed analysis of the KDD CUP 99 data set**. [S.l.], 2009. Disponível em: <<https://doi.org/10.1109%2Fcisda.2009.5356528>>. Citado na página 48.
- TRUZZI, G.; DAOUN, A. **Crimes Informáticos: O Direito Penal na Era da Informação**. [S.l.], 2009. Disponível em: <<https://doi.org/10.5769%2Fc2007017>>. Citado na página 34.
- UOL. **Falha em caixa postal ajudou hackers a atacar celular de Moro, diz MPF**. [S.l.], 2019. Disponível em: <<https://noticias.uol.com.br/politica/ultimas-noticias/2019/07/24/falha-em-caixa-postal-ajudou-hackers-a-atacar-celular-de-moro-diz-mpf.htm>>. Citado na página 22.
- VARGAS, J. P. S.; KRIEGER, J. R. **A Perícia Criminal em Face da Legislação**. [S.l.], 2014. v. 5, n. 1, 382–396 p. Disponível em: <<https://www.univali.br/graduacao/direito-itajai/publicacoes/revista-de-iniciacao-cientifica-ricc/edicoes/Lists/Artigos/Attachments/998/Arquivo%2020.pdf>>. Citado na página 37.
- VELHO, J. A. **Tratado de Computação Forense**. [S.l.], 2016. Citado na página 39.
- WAKABAYASHI, D. **Google Plus Will Be Shut Down After User Information Was Exposed**. [S.l.], 2018. Acessado no dia 29/02/2020. Disponível em: <<https://www.nytimes.com/2018/10/08/technology/google-plus-security-disclosure.html>>. Citado na página 22.
- WANG, H.; ZHANG, D.; SHIN, K. G. **Detecting SYN flooding attacks**. [S.l.], 2002. v. 3, 1530–1539 p. Disponível em: <<https://doi.org/10.1109%2Fincom.2002.1019404>>. Citado 2 vezes nas páginas 45 e 52.
- WU, H.; ZHAO, L. **Application-Layer Denial-of-Service Attacks**. [S.l.], 2015. 343–368 p. Disponível em: <<https://doi.org/10.1201%2Fb18327-17>>. Citado na página 42.
- YAN, F.; JIAN-WEN, Y.; LIN, C. **Computer Network Security and Technology Research**. [S.l.], 2015. Disponível em: <<https://doi.org/10.1109%2Ficmtma.2015.77>>. Citado 2 vezes nas páginas 41 e 42.
- YASINSAC, A.; MANZANO, Y. **Policies to Enhance Computer and Network Forensics**. [S.l.], 2001. 289–295 p. Citado na página 37.
- ZHENG, X. **Computer network security and measures**. [S.l.], 2011. Disponível em: <<https://doi.org/10.1109%2Femeit.2011.6023622>>. Citado na página 30.

ZIKRATOV, I.; KUZMIN, A.; AKIMENKO, V.; NICULICHEV, V.; YALANSKY, L. **Ensuring data integrity using blockchain technology**. [S.l.], 2017. Disponível em: <<https://doi.org/10.23919%2Ffruct.2017.8071359>>. Citado na página 40.

A Apêndice

A.1 Relatório experimento 1

```

Iniciando captor forense..
2
Lendo evidencias.. e Carregando metricas..
4
Verificacao de integridade de evidencias.. Gerando hashes..
6 fast.log
  ↪ 3512f083465c795923743cdc3642afd847edbf35787f687f0d63c8e7416cc4b
8 aggregate_report.csv
  ↪ c2a88c21dc71185ba93a97db9867aa5bbd3fcf8fe9bbf1c058f73078242b0
10 access.log
  ↪ 67f7b14412969b2487b83c7d1e4f918eb43b2a53ae610e78e7b7b194bc5612b
12 log.pcap.1589919678
  ↪ 15159c34821d8252bc5be9f74ae3d57467ed40b336593cc7185b6c5449985
14
16 Metricas do experimento: /experimento1-slowhttpstest
18 Evidencias observadas no servidor web
  Quantidade total de requisicoes: 1298
20 Media de requisicoes por segundo: 4.355705
  Quantidade requisicoes atendidas: 240
22 Quantidade requisicoes negadas: 60
  Quantidade total de IPs encontrados: 4
24 Maior quantidade de IPs repetidos: 896
  listaIpsObservadosNasRequisicoes:{192.168.1.104=896, 192.168.1.100=261,
    ::1=140, 192.168.1.101=1}
26 IP que mais se repete no servidor web: 192.168.1.104=896
28 Evidencias observadas no IDS Suricata
  Quantidade total de alertas no IDS: 6
30 listaIpsObservadosOrigemAlertas:{192.168.1.104=5, 192.168.1.100=1}
  IP origem que mais se repete nos alertas do IDS: 192.168.1.104=5
32 listaIpsObservadosDestinoAlertas:{192.168.1.101=6}

```

```
IP destino que mais se repete nos alertas do IDS: 192.168.1.101=6
34 Tempo do primeiro e ultimo alerta sinalizados:
  ↪ Primeiro alerta: [Tue May 19 16:21:54 BRT 2020]
36 ↪ Utimo alerta: [Tue May 19 16:23:03 BRT 2020]
Tempo indisponivel em segundos: 69
38
40 Realizando correlacoes..
Processo finalizado , gerando relatorio de danos e crimes..
42
  ↪ CRIME OCORRIDO: Tipo Penal violado: Interromper , Perturbar , Impedir ou
    Dificultar o restabelecimento !!
44
verificacao de crimes concluida...
46 verificacao de danos concluida...
Finalizando captor..
```

Apêndice A.1: Relatório experimento 1

A.2 Relatório experimento 2

```
Iniciando captor forense..
2
Lendo evidencias.. e Carregando metricas..
4
Verificacao de integridade de evidencias.. Gerando hashes..
6 fast.log
  ↪ 5fdeb7f6930dde8b916f24f65d9c253dc147e95f18ff7ac571cdee2626dcdd
8 aggregate_report.csv
  ↪ f916db1a511160e486c0fa233e12d96bae9c31de74f6575a52e0aa1980e1c7fb
10 log.pcap.1589920599
  ↪ 4893672f8ebce244b3e7a6f098a24084864622185be62d2f3507b82f25c1819
12 access.log
  ↪ 2d562acfb9cb8993114336744a78bd15281b26436d29fb7b70dd7f8cb6c823
14
16 Metricas do experimento: /experimento2-goldeneye
18 Evidencias observadas no servidor web
```

```
Quantidade total de requisicoes: 2020
20 Media de requisicoes por segundo: 5.2741513
Quantidade requisicoes atendidas: 47
22 Quantidade requisicoes negadas: 253
Quantidade total de IPs encontrados: 3
24 Maior quantidade de IPs repetidos: 1589
listaIpsObservadosNasRequisicoes:{192.168.1.104=1589, 192.168.1.100=291,
::1=140}
26 IP que mais se repete no servidor web: 192.168.1.104=1589

28 Evidencias observadas no IDS Suricata
Quantidade total de alertas no IDS: 14
30 listaIpsObservadosOrigemAlertas:{192.168.1.104=10, 192.168.1.100=4}
IP origem que mais se repete nos alertas do IDS: 192.168.1.104=10
32 listaIpsObservadosDestinoAlertas:{192.168.1.101=14}
IP destino que mais se repete nos alertas do IDS: 192.168.1.101=14
34 Tempo do primeiro e ultimo alerta sinalizados:
  ⇨ Primeiro alerta: [Tue May 19 16:37:08 BRT 2020]
36 ⇨ Utimo alerta: [Tue May 19 16:39:26 BRT 2020]
Tempo indisponivel em segundos: 138
38

40 Realizando correlacoes..
Processo finalizado , gerando relatorio de danos e crimes..
42
  ⇨ CRIME OCORRIDO: Tipo Penal violado: Interromper , Perturbar , Impedir ou
    Dificultar o restabelecimento !!
44
verificacao de crimes concluida...
46 verificacao de danos concluida...
Finalizando captor..
```

Apêndice A.2: Relatório experimento 2

A.3 Relatório experimento 3

```
Iniciando captor forense..
2
Lendo evidencias.. e Carregando metricas..
```

```
4 Verificacao de integridade de evidencias.. Gerando hashes..
6
fast.log
8 ⇨ 68aa9e09dcd4597a8dc97e762b5201cb3b5a994dcf8cc5dca26f86a1159
AppDDos.pcap
10 ⇨ 79ec7fb78649a8e577ccd6724905b73e4b32cfe383edeeb652a6fc50a73c1
12
Metricas do experimento: /experimento3-ciclos
14
Evidencias observadas no servidor web
16 Quantidade total de requisicoes: 0
Quantidade de requisicoes negadas: 0
18 Quantidade total de IPs encontrados: 14
Maior quantidade de IPs repetidos: 49
20 IP que mais se repete no servidor web: nao_se_aplica
22
Evidencias observadas no IDS Suricata
Quantidade total de alertas no IDS: 185
24 listaIpsObservadosOrigemAlertas:{192.168.56.1=148, 192.168.56.102=10,
    192.168.4.121=4, 192.168.3.114=3, 192.168.4.118=3, 192.168.2.110=3,
    192.168.3.116=2, 192.168.1.104=2, 192.168.4.119=2, 192.168.2.106=2,
    192.168.3.115=1, 192.168.3.117=1, 192.168.1.102=1, 192.168.2.113=1,
    192.168.2.108=1, 192.168.2.109=1}
IP origem que mais se repete nos alertas do IDS: 192.168.56.1=148
26 listaIpsObservadosDestinoAlertas:{75.127.97.72=49, 97.74.144.108=34,
    74.55.1.4=20, 74.63.40.21=13, 97.74.104.201=12, 192.168.5.122=12,
    69.192.24.88=12, 67.220.214.50=11, 203.73.24.75=9, 69.84.133.138=5,
    125.6.164.51=3, 208.113.162.153=3, 208.116.9.82=1, 72.46.153.146=1}
IP destino que mais se repete nos alertas do IDS: 75.127.97.72=49
28 Tempo do primeiro e ultimo alerta sinalizados:
⇨ Primeiro alerta: [Sat Jun 12 00:45:30 BRT 2010]
30 ⇨ Utimo alerta: [Sun Jun 13 00:01:03 BRT 2010]
Tempo indisponivel em segundos: 83733
32 Media de requisicoes no intervalo de indisponibilidade: 0
34
Realizando correlacoes..
36 Processo finalizado , gerando relatorio de danos e crimes..
```

```
verificacao de crimes concluida...
38
↔ DANO OCORRIDO !!
40
verificacao de danos concluida...
42 Finalizando captor..
```

Apêndice A.3: Relatório experimento 3

A.4 Relatório experimento 4

```
Iniciando captor forense..
2
Lendo evidencias.. e Carregando metricas..
4
Verificacao de integridade de evidencias.. Gerando hashes..
6
fast.log
8 ↔ f7165e946721ecdde468ebf8d87a7c8f68b079edc8e78b53214889c58f69
Wednesday-WorkingHours.pcap
10 ↔ cd2674db7559a53f24bc03be3239b315700174ccaef72d10f5edc4c1a08f6186
12 Metricas do experimento: /experimento4-cicids
14 Evidencias observadas no servidor web
Quantidade total de requisicoes: 0
16 Quantidade de requisicoes negadas: 0
Quantidade total de IPs encontrados: 6
18 Maior quantidade de IPs repetidos: 178
IP que mais se repete no servidor web: nao_se_aplica
20
Evidencias observadas no IDS Suricata
22 Quantidade total de alertas no IDS: 220
listaIpsObservadosOrigemAlertas:{172.16.0.1=174, 192.168.10.5=41,
192.168.10.15=1, 192.168.10.17=1, 192.168.10.12=1, 192.168.10.25=1,
192.168.10.14=1}
24 IP origem que mais se repete nos alertas do IDS: 172.16.0.1=174
listaIpsObservadosDestinoAlertas:{192.168.10.50=178, 162.208.20.178=21,
162.208.22.34=18, 178.172.160.3=1, 178.172.160.4=1, 151.101.209.127=1}
```



```
26 IP destino que mais se repete nos alertas do IDS: 192.168.10.50=178
Tempo do primeiro e ultimo alerta sinalizados:
28 ⇔ Primeiro alerta: [Wed Jul 05 09:17:00 BRT 2017]
⇔ Utimo alerta: [Wed Jul 05 15:21:08 BRT 2017]
30 Tempo indisponivel em segundos: 21848
Media de requisicoes no intervalo de indisponibilidade: 0
32
34 Realizando correlacoes..
Processo finalizado , gerando relatorio de danos e crimes..
36 verificacao de crimes concluida...
38 ⇨ DANO OCORRIDO !!
40 verificacao de danos concluida...
Finalizando captor..
```

Apêndice A.4: Relatório experimento 4

A.5 Relatório experimento 5

```
Iniciando captor forense..
2
Lendo evidencias.. e Carregando metricas..
4
Verificacao de integridade de evidencias.. Gerando hashes..
6 fast.log
⇨ e467a25173efe8ab38f3f779849e1a57c097f240b6427bfe3d76e6d84e93b61
8 aggregate_report.csv
⇨ 3e61bddfe87a71a65f6e3d4a842e9befef9b5854ef8dc65163c478c584e513
10 log.pcap.1589922568
⇨ 6bef52a69ac034cd374a7755e260c6c4ca1d206f62a68f9fb0543e19ee57636a
12 access.log
⇨ 86ad2b1f65d7c7f3a7b1ec6db5f38ef1da7a10c7add52257b5093b4887338
14
16 Metricas do experimento: /experimento5-hulk
18 Evidencias observadas no servidor web
```

```
Quantidade total de requisicoes: 1888
20 Media de requisicoes por segundo: 5.686747
Quantidade requisicoes atendidas: 49
22 Quantidade requisicoes negadas: 251
Quantidade total de IPs encontrados: 3
24 Maior quantidade de IPs repetidos: 1521
listaIpsObservadosNasRequisicoes:{192.168.1.104=1521, 192.168.1.100=293,
::1=74}
26 IP que mais se repete no servidor web: 192.168.1.104=1521

28 Evidencias observadas no IDS Suricata
Quantidade total de alertas no IDS: 13
30 listaIpsObservadosOrigemAlertas:{192.168.1.104=12, 192.168.1.100=1}
IP origem que mais se repete nos alertas do IDS: 192.168.1.104=12
32 listaIpsObservadosDestinoAlertas:{192.168.1.101=13}
IP destino que mais se repete nos alertas do IDS: 192.168.1.101=13
34 Tempo do primeiro e ultimo alerta sinalizados:
↔ Primeiro alerta: [Tue May 19 17:10:16 BRT 2020]
36 ↔ Utimo alerta: [Tue May 19 17:12:18 BRT 2020]
Tempo indisponivel em segundos: 122
38

40 Realizando correlacoes..
Processo finalizado , gerando relatorio de danos e crimes..
42
↔ CRIME OCORRIDO: Tipo Penal violado: Interromper , Perturbar , Impedir ou
Dificultar o restabelecimento !!
44
verificacao de crimes concluida...
46 verificacao de danos concluida...
Finalizando captor..
```