

UNIVERSIDADE NOVE DE JULHO – UNINOVE
DIRETORIA DE INFORMÁTICA



PROJETO DE SEGURANÇA
COLETÂNEA DE FERRAMENTAS E TESTES DE SEGURANÇA
COMPUTACIONAL

SÃO PAULO
2021

COLETÂNEA DE FERRAMENTAS E TESTES DE SEGURANÇA COMPUTACIONAL

| | |
|-------------------------------------|----------------|
| GABRIEL BRITO DE MOURA | RA: 2219108437 |
| KELVER DANIEL DO AMARAL MATA | RA: 2219104613 |
| LEANDRO BARBOSA DA SILVA | RA: 2218106814 |
| LUDMILLE DAMASCENO DE BARROS | RA: 920129341 |
| LUIZ ENRIQUE DA COSTA SANTOS | RA: 2220112596 |
| MATHEUS DOS SANTOS BRASIL | RA: 921113230 |
| MATHEUS HENRIQUE ANSELMO DOS SANTOS | RA: 2221104180 |
| ROBERTO TIYOZO WATANABE JUNIOR* | RA: 2219109625 |
| VINICIUS CALMONA CREPALDI DE LIMA | RA: 3021101411 |
| WILLIAM FERREIRA DO CARMO | RA: 2221013364 |

Trabalho apresentado ao curso de Tecnologia em Segurança da Informação da Universidade Nove de Julho, como parte dos requisitos para a obtenção do Grau de Tecnólogo em Segurança da Informação.

Orientador: Prof. Me. Norberto Santos
Unidade: Campus: MM, SA, VP, VG, VM
Curso: Tecnologia em Segurança da Informação
Período: Primeiro Semestre 2021

São Paulo
2021

FOLHA DE APROVAÇÃO

| | |
|-------------------------------------|----------------|
| GABRIEL BRITO DE MOURA | RA: 2219108437 |
| LEANDRO BARBOSA DA SILVA | RA: 2218106814 |
| LUDMILLE DAMASCENO DE BARROS | RA: 920129341 |
| LUIZ ENRIQUE DA COSTA SANTOS | RA: 2220112596 |
| KELVER DANIEL DO AMARAL MATA | RA: 2219104613 |
| MATHEUS DOS SANTOS BRASIL | RA: 921113230 |
| MATHEUS HENRIQUE ANSELMO DOS SANTOS | RA: 2221104180 |
| ROBERTO TIYOZO WATANABE JUNIOR* | RA: 2219109625 |
| VINICIUS CALMONA CREPALDI DE LIMA | RA: 3021101411 |
| WILLIAM FERREIRA DO CARMO | RA: 2221013364 |

COLETÂNEA DE FERRAMENTAS E TESTES DE SEGURANÇA COMPUTACIONAL

Trabalho de conclusão aprovado como requisito parcial para a obtenção do grau de Tecnólogo, do curso de Tecnologia em Segurança da Informação, da Universidade Nove de Julho, pelo professor orientador abaixo mencionado.

São Paulo, 08 de junho de 2021

Prof. Me. Norberto Santos

RESUMO

A pesquisa aborda elementos de redes de computadores, ameaças que podem atingir a integridade e funcionamento de sua infraestrutura, mecanismos de proteção, com enfoque na proteção do ativo mais crucial em uma empresa, que é a informação, será dissertado sobre ferramentas para análise de perícia e teste computacionais, relacionadas à rede e sistemas instalados. O estudo também permitiu uma análise do mercado de trabalho de perícia digital, abordando a rotina de trabalho, principais requisitos técnicos procurados por empresas, atividades chaves, empresas que contratam e faixa salarial esperada. Além disso, será mostrada uma parte da internet que não é indexada, não existe censura, onde todos os usuários são anônimos, chamada de Deepweb.

Palavras-chaves: Mercado de Perícia, Deep-Web, Snort, Metasploit, Tails, TOR, Redes de Computadores, Ferramentas de Segurança da Informação, Ameaças de Redes, Forense Digital.

ABSTRACT

The research addresses elements of computer networks, threats that can affect the integrity and functioning of its infrastructure, protection mechanisms, with a focus on protecting the most crucial asset in a company, which is information, will be discussed tools for forensic analysis and computational testing, related to the network and installed systems. The study also allowed an analysis of the digital forensic job market, addressing the work routine, main technical requirements sought by companies, key activities, companies that hire and the expected salary range. In addition, it will show a part of the internet that is not indexed, there is no censorship, where all users are anonymous, called Deep-web.

Keywords: Digital Forensics Market, Deep-Web, Snort, Metasploit, Tails, TOR, Computer Networks, Information Security Tools, Network Threats, Digital Forensic.

LISTA DE FIGURAS

| | |
|--|----|
| FIGURA 1 - Diferenças IDS e IPS..... | 6 |
| FIGURA 2 - Logo Snort..... | 7 |
| FIGURA 3 - Processos do Snort | 8 |
| FIGURA 4 - Inicialização do SNORT | 8 |
| FIGURA 5 - Output do comando de inicialização | 9 |
| FIGURA 6 - Network Scan do NMAP..... | 9 |
| FIGURA 7 - Network Scan sendo detectado | 10 |
| FIGURA 8 - Ataque DOS sendo detectado..... | 10 |
| FIGURA 9 - Interface do Metasploit..... | 12 |
| FIGURA 10 - Comando Msfupdate | 12 |
| FIGURA 11 - Comando Search | 13 |
| FIGURA 12 - Comando Info..... | 13 |
| FIGURA 13 - Engenharia Social..... | 15 |
| FIGURA 14 – Campanha de Phising | 15 |
| FIGURA 15 - Definindo nome da campanha Phising..... | 16 |
| FIGURA 16 - Configurando E-mail..... | 16 |
| FIGURA 17 – Conteúdo do e-mail Phising | 17 |
| FIGURA 18 - Definindo redirecionamento por URL | 17 |
| FIGURA 19 - Definindo nome da página a ser direcionada | 18 |
| FIGURA 20 - Criando conteúdo da Página WEB..... | 18 |
| FIGURA 21- Componentes da Campanha | 18 |
| FIGURA 22 - Criando conteúdo da Página Redirecionada..... | 19 |
| FIGURA 23 - Configurando parâmetros da página de redirecionamento..... | 19 |
| FIGURA 24 - Abrindo configurações do servidor de e-mail | 20 |
| FIGURA 25 - Alterando configurando do servidor de e-mail..... | 20 |
| FIGURA 26 - Outras notificações da campanha | 20 |
| FIGURA 27 - Iniciar o envio de e-mail phishing..... | 21 |
| FIGURA 28 - Gerar relatório da campanha Phising | 21 |
| FIGURA 29 - Sistema Tails | 22 |
| FIGURA 30 - Utilidades da ferramenta DNSenum | 24 |

| | |
|--|----|
| FIGURA 31 - Surface Web e Deep Web | 28 |
| FIGURA 32 - Nós do tráfego de rede do circuito TOR | 30 |
| FIGURA 33 - Link Onion do Facebook..... | 31 |
| FIGURA 34 - Estrutura da Rede TOR | 32 |
| FIGURA 35 - Navegador TOR | 33 |

LISTA DE ABREVIATURAS E SIGLAS

IP – Internet Protocol

IPS – Intrusion Prevention System

IDS – Intrusion Detection System

IT – Tecnologia da informação

BSD - Berkeley Software Distribution

PIN - Personal Identification Number

ID - Identidade

URL - Uniform Resource Locator

DNS – Domain Name System

HSC – High Security Center

CPF – Cadastro de Pessoa Física

CNPJ - Cadastro Nacional da Pessoa Jurídica

IPOG – Instituto de pós-graduação

CCFT – Certified Computer Forensic Technical

CEH – Certified Ethical Hacker

CHFI – Certified Hacker Forensic Investigator

IBAPE – Instituto Brasileiro de Avaliações e Perícias de Engenharia

HTML - Hyper Text Markup Language

TOR – The Onion Router

WWW – World Wide Web

MX – Mail Exchanger

HD – Hard Drive

SUMÁRIO

| | |
|--|-----------|
| CAPÍTULO 1 – INTRODUÇÃO | 1 |
| CAPÍTULO 2 – REDES DE COMPUTADORES..... | 2 |
| 2.1 – Ameaças e Proteções a Redes | 3 |
| 2.2.1 – Sistema de Detecção de Intrusão | 6 |
| 2.2.2 – Sistema de Prevenção de Intrusão | 6 |
| CAPÍTULO 3 – FERRAMENTAS | 7 |
| 3.1 – Snort..... | 7 |
| 3.1.1 – Exemplo de Utilização da Ferramenta SNORT | 8 |
| 3.1.2 – Treinamento SNORT..... | 11 |
| 3.2 – Metasploit | 11 |
| 3.2.1 – História | 12 |
| 3.2.2 – Comandos | 12 |
| 3.2.3 – Engenharia Social no Metasploit..... | 14 |
| 3.2.5 – Ataque de Engenharia Social no Metasploit | 15 |
| 3.3 – Tails..... | 22 |
| 3.4 – DNSenum..... | 24 |
| CAPÍTULO 4 – MERCADO DE PERÍCIA..... | 25 |
| 4.1 – Rotina De Trabalho de um Perito Criminal Digital..... | 26 |
| 4.2 – Principais Competências | 26 |
| 4.3 – Atividades-Chave..... | 26 |
| 4.4 – O Que Fazer Para Atuar Na Área | 26 |
| 4.5 – Quem Contrata | 27 |
| 4.5.1 – Salário | 27 |
| CAPÍTULO 5 – INTERNET E AS QUESTÕES DE SEGURANÇA..... | 28 |
| 5.1 – O que é Deep Web | 28 |
| 5.2 – Ameaças na Deep Web..... | 29 |
| 5.2.1 – Conteúdos da Deep Web | 29 |

| | |
|---|-----------|
| 5.5 – Navegador Tor e Rede..... | 30 |
| 5.5.1 – Como funciona | 30 |
| 5.5.2 – Endereços de sites “.onion” | 31 |
| 5.5.3 – Estrutura de Rede TOR..... | 31 |
| 5.5.4 – Executando o navegador Tor | 32 |
| CONCLUSÃO..... | 34 |
| REFERÊNCIA BIBLIOGRÁFICA | 35 |

CAPÍTULO 1 – INTRODUÇÃO

Gabriel Brito de Moura RA:2219108437

Roberto Tiyoza Watanabe Junior RA: 2219109625

“A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, conseqüentemente, necessita ser adequadamente protegida” (NAKAMURA E GEUS,2002, p.9)

Atualmente em um mundo quase que completamente conectado em rede, onde a informação transcorre constantemente, empresas privadas ou governamentais, carecem de processos e controles de segurança a fim de garantir e conservar suas informações de uma variedade de ameaças que surgem gradualmente (ARAÚJO, 2009).

“Porque a informação é um ativo muito importante para qualquer instituição, podendo ser considerada, atualmente, o recurso patrimonial mais crítico” (TRIBUNAL DE CONTAS DA UNIÃO, 2012, p.10)

Esse projeto tem como objetivo descrever sobre a segurança de redes de computadores e suas vulnerabilidades, mostrando os vários tipos de criminosos existentes, os estragos que eles podem causar a uma rede se ela estiver desprotegida, e algumas ferramentas utilizadas para realizar esses ataques.

Será mostrado algumas das principais ferramentas de defesa contra-ataques cibernéticos, mercado de trabalho que existe em torno da segurança em redes de computadores, as principais competências necessárias para se tornar um profissional na área, principais atividades que este profissional exerce, os tipos de empresas que contratam, o salário e sua rotina de trabalho.

O projeto também visa falar sobre a internet e as suas principais ameaças, descrevendo riscos que são corridos ao acessar sites desconhecidos, mostrando uma de suas camadas mais profundas que é chamada de *Deep-Web* (CORREIO BRAZILIENSE, 2020).

CAPÍTULO 2 – REDES DE COMPUTADORES

Gabriel Brito de Moura RA:2219108437

Roberto Tiyoza Watanabe Junior RA: 2219109625

Segundo Tanenbaum (2003), a maioria das dificuldades está diretamente envolvida com à segurança, sendo instigada propositalmente por indivíduos, com a finalidade de obter favor, benéfico ou até mesmo prejudicar outrem. Provocando que, independentemente do tamanho da infraestrutura de redes, seja doméstica ou corporativa, para estar seguro não basta apenas estar livre de problemas de programação, há o fator humano intrínseco nessa questão. *“Toda força será fraca, se não estiver unida”* (LA FONTAINE ,1866, p. 132)

Conforme estatísticas apresentadas pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERTBR, 2021) o número concernente as notificações de incidentes e intrusões a redes de computadores, reportados até junho de 2020, são 318.697 incidentes. Segundo a empresa líder de mercado Kaspersky (2021), uma das maiores empresas privadas de segurança cibernética do mundo, em abril de 2021, o Brasil está entre os cinco países que mais sofreram com ataques cibernéticos.

Segundo Sêmola (2011) para uma rede ser definida como segura é necessário atender algumas noções básicas de segurança que serão mostradas abaixo:

- Autenticação – ter certeza de que os lados envolvidos dentro de uma comunicação são de fato quem dizem ser, tornando a comunicação entre eles autêntica;
- Controle de acesso – a entrada no sistema deve ser restrita, permitindo apenas pessoas devidamente identificadas e autorizadas o acesso ao serviço;
- Confidencialidade – está associada com a garantia de que as informações pessoais não serão reveladas para indivíduos não autorizadas.
- Disponibilidade – é a garantia de que a informação esteja sempre disponível para pessoas autorizadas, durante todo o tempo em que precisarem.
- Integridade – garantir que as informações não sejam modificadas ou excluídas, se mantendo íntegra durante todos os processos.

2.1 – Ameaças e Proteções a Redes

Carvalho (2005) comenta que o atacante é caracterizado como o indivíduo que exerce ataque a um sistema computacional, de forma que comprometa à integridade estrutural e/ou operacional, possibilitando a obtenção de dados. O termo popularmente conhecido é chamado de *hacker*, para Levy (2010) o acesso aos computadores deve ser ilimitado e total, todas as informações deveriam ser livres. Os *hackers* promovem a descentralização das informações, eles devem ser julgados pelos seus feitos e não por posição social, idade, escolaridade. Levy (2010) ainda comenta que os computadores podem mudar sua vida para melhor, tudo depende do que você irá fazer com o conhecimento obtido.

Conforme Carvalho (2005), o termo hacker possui algumas ramificações:

- *Script Kiddies* – possuem pouco ou nenhum conhecimento sobre *hacking*, e por ter visto vídeos na internet pensam que sabem tudo sobre o assunto, mas na verdade não possuem ideia alguma do ato que estão cometendo.
- *Crackers* – são indivíduos com grande conhecimento em computação, e sua principal intenção é de prejudicar o alvo que estão invadindo ou atacando;
- *Carders* – fazem uso de cartões roubados, clonados, ou gerados automaticamente através de um software, para efetuar compras sem nenhuma autorização de seu legítimo dono;
- *Cyberpunks* – com um imenso conhecimento na área, se importam principalmente com a privacidade da informação, e se preocupam em divulgar falhas e erros como forma de ajudar;
- *Insiders* – funcionários ou ex-funcionários que utilizam engenharia social para prejudicar a própria empresa, ou cometer um ato de espionagem em busca de vantagem comercial;
- *Coders* – não fazem mais o uso do conhecimento para agir ilegalmente e compartilham esse conhecimento na área de segurança como forma de contribuir com a comunidade;
- *White hats* – aproveitam de seus conhecimentos para identificar vulnerabilidades em redes, aplicativos de celulares e de computadores, até mesmo de páginas web e depois compartilham suas descobertas para que os contratam, também conhecido como *Hacker Ético*, atuam em conformidade com a legislação federal, não infringindo-a;
- *Black hats* – desfrutam das habilidades e experiências técnicas com o intuito de prejudicar e/ou acarretar dano massivo a uma pessoa física ou jurídica, roubando informações sigilosas em troca de ganho financeiro;
- *Phreakers* – conhecidos por *hackers* que possuem seu enfoque na área de telefonia móvel ou fixa, utilizam de mecanismo com a finalidade de alterar e/ou burlar sistemas de empresas de telefonias para obtenção de serviços de maneira gratuita.

Segundo Nakamura e Geus (2002, p. 80), “*A proteção da informação depende da segurança em todos os níveis, que incluem: sistema operacional, serviços e protocolos, rede e telecomunicações, aplicação, usuários e organização, e físico*”.

Com base na recomendação X.800 da *International Telecommunication Union* (1991), os ataques cibernéticos à segurança são classificados em passivos, com o propósito de coletar informações que são comunicadas na rede, a partir da inspeção das transmissões sem prejudicar seus recursos, e em ataques ativos, que modificam o fluxo de dados ou forjam falso-positivo, com o intuito de decompor ou incapacitar a operação.

De acordo com Nakamura e Geus (2007) a primeira etapa para realização de um ataque cibernético é a coleta de dados a respeito do sistema operacional que será atacado, através de inúmeras técnicas que existem atualmente, após obtenção das informações, o hacker atua das seguintes formas:

- Intrusão do sistema;
- Fiscalização da rede;
- Adição de códigos maliciosos ou dados fictícios ao sistema;
- Excesso de carga ao sistema com pacotes insignificantes, implicando em sua indisponibilidade.

Nakamura e Geus (2007) ainda conclui que, as complicações após um ataque quase ininterruptamente serão negativas, alternando entre:

- Auditoria sem permissão;
- Furto de informações privadas;
- Alteração no banco de dados e sistemas da empresa;
- Vagoriedade ou indisponibilização do serviço;
- Perdas financeiras;
- Perda de credibilidade no mercado;
- Custos com recuperação pós incidente;
- Quebra de contratos.

2.2 – Ferramentas E Técnicas De Segurança

Atualmente existe uma gama de procedimentos de segurança disponíveis, com o propósito de garantir a segurança na infraestrutura de rede (CHESWICK ET AL. 2005).

Destacam-se os seguintes procedimentos:

- Criptografia – Segundo Carvalho (2005, p.34) é o procedimento no qual as informações são transcritas em forma de códigos, permitindo que apenas indivíduos autorizados consigam acessá-las. “A criptografia é a ciência de transformar dados que aparentemente podem ser entendidos e interpretados pelas pessoas, em dados que não possuem significado algum, e que quando necessário podem ser recuperados à sua forma original”.
- Firewall – De acordo com Cheswick et al. (2005), seria todo equipamento, *software*, ou aparelhagem que restringe a circulação na rede. Hoje em dia, os firewalls vêm “gratuitamente” inclusos em muitos dispositivos, como: estações de base *wireless*, modems, roteadores, e *switches* de IP. Os *softwares* de *firewall* são disponibilizados em todos os sistemas operacionais atuais. Se tornando uma camada de *software* dentro de uma máquina, ou uma lista de regras que discriminam as informações implementadas em um *Kernel Unix*.
- Autenticação – Carvalho (2005) relata que existem muitas formas de autenticar o usuário, que são fundamentadas a partir do que o usuário possui conhecimento: número de identificação pessoal, chave ou *password*; a partir do que ele tem em mãos: *smart card* ou *token*; e em seus próprios aspectos corporais: a tecnologia de biometria.
- Sistemas de detecção de intrusão – identifica ações indevidas ou nocivas à rede, criando alertas, notificando ao responsável pela proteção da rede (NAKAMURA, 2007).
- Sistemas de prevenção de intrusão – segundo Doherty et al. (2008) não apenas identifica e alerta uma intrusão à rede, como também bloqueia imediatamente qualquer ameaça, impedindo assim um dano maior à rede.

2.2.1 – Sistema de Detecção de Intrusão

Para Silva (2008) sistema de detecção de intrusão (IDS – Intrusion Detection System) são *softwares* utilizados em parceria com outros sistemas de segurança como por exemplo, antivírus e firewalls para aumentar a segurança de um ambiente de rede, reportando atividades maliciosas ou impossibilitando que ações ardilosas obtenham sucesso e se espalhem pela infraestrutura de rede.

Neto et al. (2011) diz que, entre os anos de 1950 e 1960 foi estabelecida as técnicas de auditorias para a análise fraudes, dados e erros. Em 1970, foram criadas diversas formas de segurança cibernética que legitimam a auditoria como um importantíssimo mecanismo de investigação.

2.2.2 – Sistema de Prevenção de Intrusão

O Sistema de Prevenção de Intrusão age em conjunto com o IDS, ele agrega na identificação de ataques e torna possível sua mitigação. Tanto o IDS, quanto o IPS precisam de um banco de dados contendo assinaturas comumente utilizadas para análise comparativa com ataques cibernéticos possíveis. A Figura 1 ilustra de maneira lúdica essa diferença. Não obstante, o IDS é restrito a detectar tentativas de intrusão, registrar e enviar ao responsável pela rede. O IPS atua de forma “*inline*”, toma medidas preventivas bloqueando tentativas de invasão em *real-time*. Como são conceitos parecidos, ou seja, aparentam ter mesmas funções, podendo inclusive substituir alguns tipos de *firewalls*, essas tecnologias adicionam mais uma barreira de segurança à rede (DOHERTY et al. 2008).



FIGURA 1 - Diferenças IDS e IPS
Fonte: (Canal TI, 2017)

CAPÍTULO 3 – FERRAMENTAS

3.1 – Snort

Roberto Tiyoza Watanabe Junior RA: 2219109625

Gabriel Brito de Moura RA:2219108437



FIGURA 2 - Logo Snort

Fonte: (SNORT, 2021)

Segundo Snort (2021) o SNORT é um sistema de detecção de intrusão voltado a rede, amplamente utilizado e a Figura 2 ilustra seu logo. Foi desenvolvido por Martin Roesch em 1998. E tem como principal objetivo destacar se alguém está tentando entrar no sistema ou se algum usuário está tentando fazer mau uso dele. *“Detecção de intrusão é um processo de coleta de informações que procura identificar sinais de que um ataque está iniciando ou ocorrendo”* (NORTHCUTT, 2001, p. 48)

O sistema IDS é composto primariamente por dois dispositivos O console de comando e o sensor. *“O sensor é o dispositivo responsável pela coleta de informação para análise de descoberta de uma invasão. O console de comando tem como função permitir o controle do IDS, monitorar o estado do sensor e processar os alertas enviados pelo sensor.”* (PROCTOR, 2000, p. 20)

O SNORT possui vários recursos entre os quais pode - se citar um farejador de pacotes para a captura dos dados, um mecanismo de registro de pacotes e de detecção de invasão. Ele também pode ser configurado para enviar alertas em tempo real evitando assim a necessidade de monitorar o sistema continuamente. O Snort é considerado um IDS leve, por possuir uma estrutura pequena e ser um software multiplataforma (CASWELL, 2004).

O SNORT pode ser implantado para trabalhar juntamente com o *firewall* da rede, conseguindo interromper/bloquear pacotes, possuindo três usos principais: como um farejador de pacotes, como *tcpdump*, como um registrador de pacotes, como mostrado na Figura 3. Que é útil para depuração de tráfego de rede, ou pode ser utilizado como um sistema de prevenção de intrusão de rede (IPS) completo (SNORT, 2021).

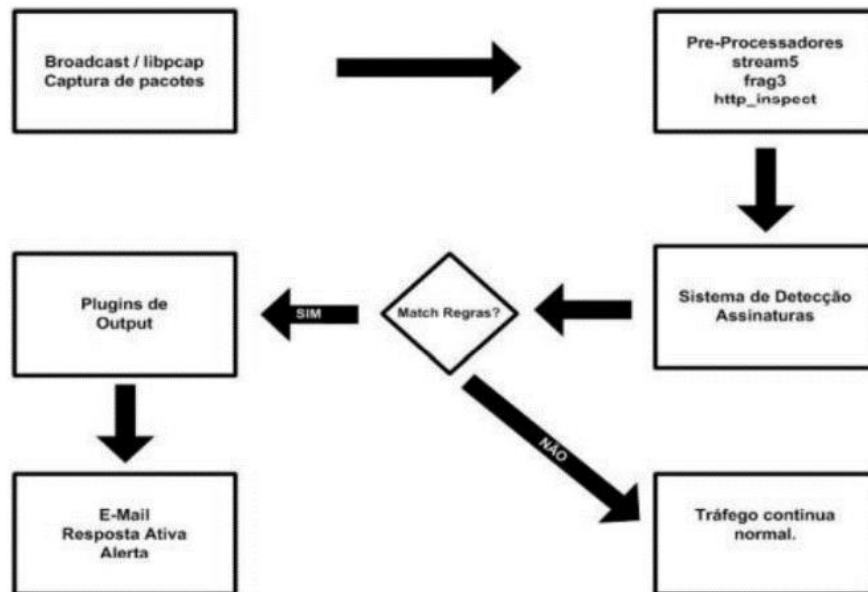


FIGURA 3 - Processos do Snort

Fonte: (Montoro, 2012)

3.1.1 – Exemplo de Utilização da Ferramenta SNORT

O tutorial abaixo é baseado em Vanney (2018).

Para inicializar o SNORT, é utilizado o seguinte comando:

```
# snort -d -l /var/log/snort/ -h 10.0.0.0/24 -A console -c /etc/snort/snort.conf
```

Onde:

d – Diz ao SNORT para mostrar os dados

l – Determina o diretório onde será salvo os logs

h – Especifica a rede a ser monitorada

A – Instrui ao SNORT para mostrar os alertas no console

c – Especifica o caminho do arquivo de configuração

Este comando pode ser visto na Figura 4.

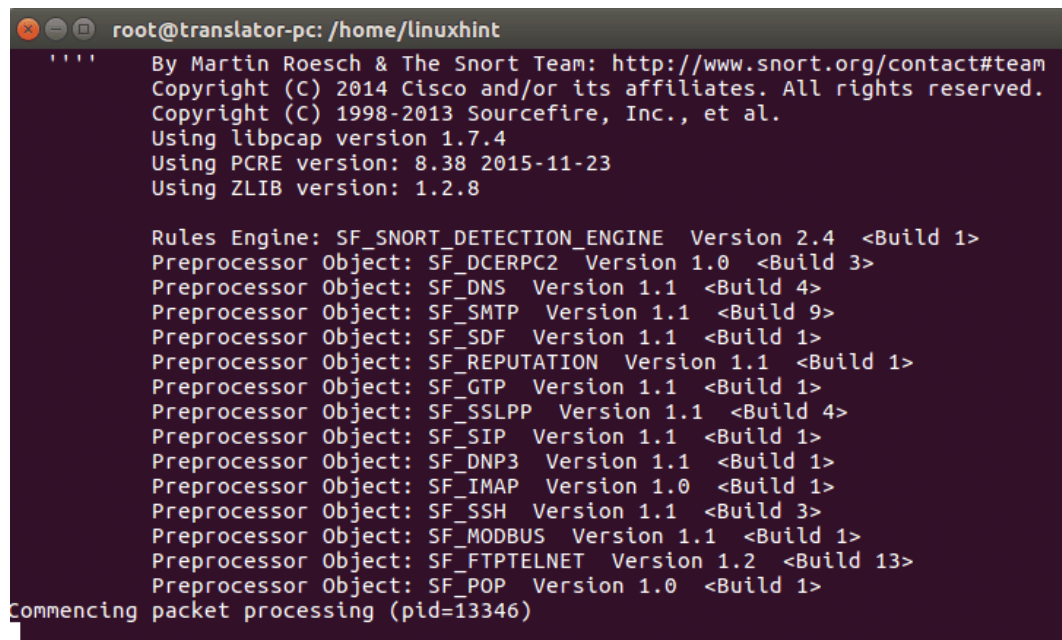
```

root@translator-pc: /home/linuxhint
root@translator-pc:/home/linuxhint# snort -d -l /var/log/snort/ -h 10.0.0.0/24 -
A console -c /etc/snort/snort.conf
  
```

FIGURA 4 - Inicialização do SNORT

Fonte: (Linuxhint, 2018)

Após a execução do comando acima, o SNORT estará em execução e retornará na tela os processos de inicialização como pode ser visto na Figura 5.

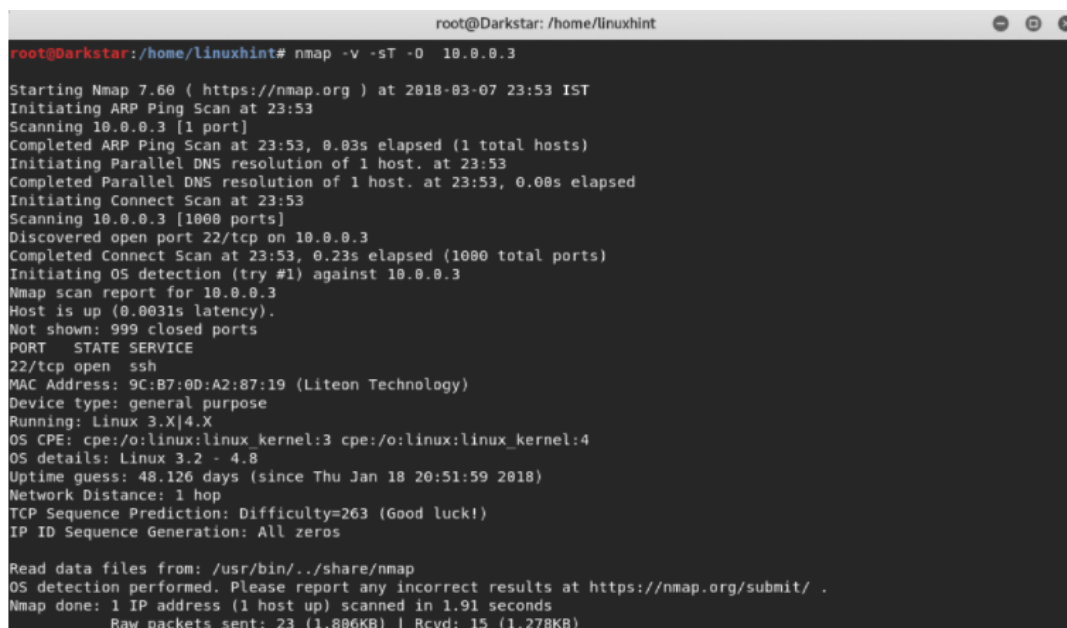
A terminal window titled 'root@translator-pc: /home/linuxhint' displays the output of the Snort initialization command. The output includes copyright information for Martin Roesch, Cisco, and Sourcefire, followed by the versions of libpcap (1.7.4), PCRE (8.38), and ZLIB (1.2.8). It then lists the Rules Engine (SF_SNORT_DETECTION_ENGINE, Version 2.4) and various Preprocessor Objects (SF_DCERPC2, SF_DNS, SF_SMTP, SF_SDF, SF_REPUTATION, SF_GTP, SF_SSLPP, SF_SIP, SF_DNP3, SF_IMAP, SF_SSH, SF_MODBUS, SF_FTPTELNET, SF_POP) with their respective versions and build numbers. The final line indicates 'Commencing packet processing (pid=13346)'.

```
root@translator-pc: /home/linuxhint
''' By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.7.4
Using PCRE version: 8.38 2015-11-23
Using ZLIB version: 1.2.8

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Commencing packet processing (pid=13346)
```

FIGURA 5 - Output do comando de inicialização
Fonte: (Linuxhint, 2018)

Com o programa em execução, foi realizada uma network scan utilizando a ferramenta NMAP, como pode ser visto na figura 6.

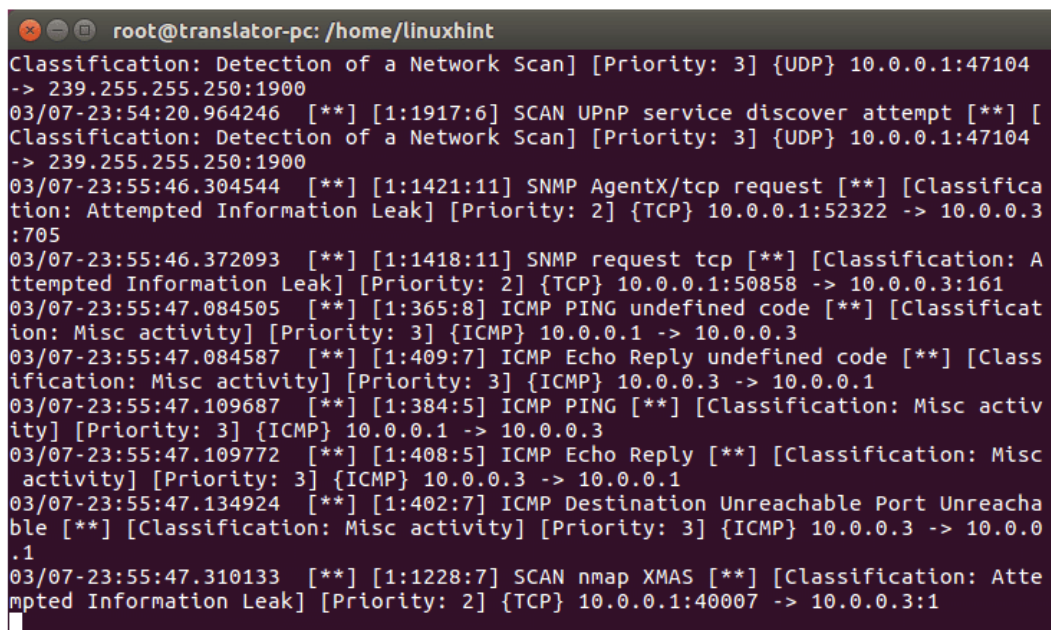
A terminal window titled 'root@Darkstar: /home/linuxhint' shows the output of an Nmap scan command: 'nmap -v -sT -O 10.0.0.3'. The output details the scan process, including ARP ping scan, DNS resolution, connect scan, and OS detection. It identifies the host as up, reports 999 closed ports, and finds an open port 22/tcp (ssh). It also provides MAC address, device type, running OS (Linux 3.X|4.X), OS CPE, OS details, uptime guess, network distance, TCP sequence prediction, and IP ID sequence generation. The scan is completed in 1.91 seconds.

```
root@Darkstar: /home/linuxhint# nmap -v -sT -O 10.0.0.3
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-07 23:53 IST
Initiating ARP Ping Scan at 23:53
Scanning 10.0.0.3 [1 port]
Completed ARP Ping Scan at 23:53, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:53
Completed Parallel DNS resolution of 1 host. at 23:53, 0.00s elapsed
Initiating Connect Scan at 23:53
Scanning 10.0.0.3 [1000 ports]
Discovered open port 22/tcp on 10.0.0.3
Completed Connect Scan at 23:53, 0.23s elapsed (1000 total ports)
Initiating OS detection (try #1) against 10.0.0.3
Nmap scan report for 10.0.0.3
Host is up (0.0031s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 9C:B7:0D:A2:87:19 (Liteon Technology)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.8
Uptime guess: 48.126 days (since Thu Jan 18 20:51:59 2018)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/bin/./share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.91 seconds
Raw packets sent: 23 (1.886KB) | Rcvd: 15 (1.278KB)
```

FIGURA 6 - Network Scan do NMAP
Fonte: (Linuxhint, 2018)

Após a execução do Network Scan do nmap, conforme Figura 7, se o SNORT o detectou.



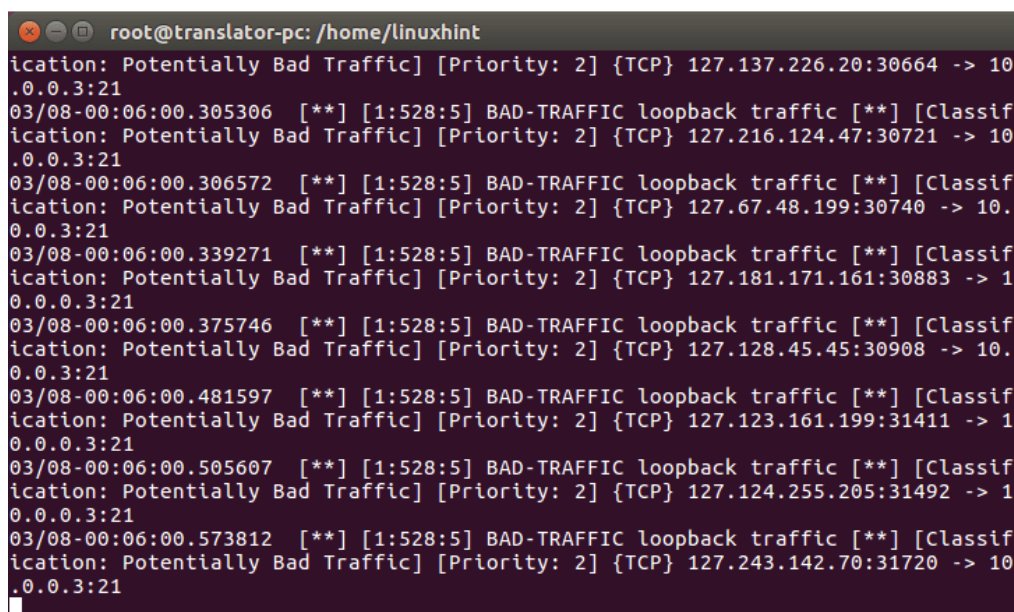
```
root@translator-pc: /home/linuxhint
Classification: Detection of a Network Scan] [Priority: 3] {UDP} 10.0.0.1:47104
-> 239.255.255.250:1900
03/07-23:54:20.964246  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [
Classification: Detection of a Network Scan] [Priority: 3] {UDP} 10.0.0.1:47104
-> 239.255.255.250:1900
03/07-23:55:46.304544  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classifica
tion: Attempted Information Leak] [Priority: 2] {TCP} 10.0.0.1:52322 -> 10.0.0.3
:705
03/07-23:55:46.372093  [**] [1:1418:11] SNMP request tcp [**] [Classification: A
ttempted Information Leak] [Priority: 2] {TCP} 10.0.0.1:50858 -> 10.0.0.3:161
03/07-23:55:47.084505  [**] [1:365:8] ICMP PING undefined code [**] [Classificat
ion: Misc activity] [Priority: 3] {ICMP} 10.0.0.1 -> 10.0.0.3
03/07-23:55:47.084587  [**] [1:409:7] ICMP Echo Reply undefined code [**] [Class
ification: Misc activity] [Priority: 3] {ICMP} 10.0.0.3 -> 10.0.0.1
03/07-23:55:47.109687  [**] [1:384:5] ICMP PING [**] [Classification: Misc activ
ity] [Priority: 3] {ICMP} 10.0.0.1 -> 10.0.0.3
03/07-23:55:47.109772  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc
activity] [Priority: 3] {ICMP} 10.0.0.3 -> 10.0.0.1
03/07-23:55:47.134924  [**] [1:402:7] ICMP Destination Unreachable Port Unreacha
ble [**] [Classification: Misc activity] [Priority: 3] {ICMP} 10.0.0.3 -> 10.0.0
.1
03/07-23:55:47.310133  [**] [1:1228:7] SCAN nmap XMAS [**] [Classification: Atte
mpted Information Leak] [Priority: 2] {TCP} 10.0.0.1:40007 -> 10.0.0.3:1
```

FIGURA 7 - Network Scan sendo detectado

Fonte: (Linuxhint, 2018)

Foi especificado no comando de inicialização do SNORT que seria mostrado os aletas no console, e como visto na imagem acima, o SNORT detectou o Network Scan.

Tambem sera mostrado a execução de um programa chamado Hping3, que efetua ataques DOS, contra a mesma rede utilizada neste exemplo, e o resultado da detecção do SNORT pode ser visto na imagem Figura 8.



```
root@translator-pc: /home/linuxhint
ication: Potentially Bad Traffic] [Priority: 2] {TCP} 127.137.226.20:30664 -> 10
.0.0.3:21
03/08-00:06:00.305306  [**] [1:528:5] BAD-TRAFFIC loopback traffic [**] [Classif
ication: Potentially Bad Traffic] [Priority: 2] {TCP} 127.216.124.47:30721 -> 10
.0.0.3:21
03/08-00:06:00.306572  [**] [1:528:5] BAD-TRAFFIC loopback traffic [**] [Classif
ication: Potentially Bad Traffic] [Priority: 2] {TCP} 127.67.48.199:30740 -> 10
.0.0.3:21
03/08-00:06:00.339271  [**] [1:528:5] BAD-TRAFFIC loopback traffic [**] [Classif
ication: Potentially Bad Traffic] [Priority: 2] {TCP} 127.181.171.161:30883 -> 1
0.0.0.3:21
03/08-00:06:00.375746  [**] [1:528:5] BAD-TRAFFIC loopback traffic [**] [Classif
ication: Potentially Bad Traffic] [Priority: 2] {TCP} 127.128.45.45:30908 -> 10
.0.0.3:21
03/08-00:06:00.481597  [**] [1:528:5] BAD-TRAFFIC loopback traffic [**] [Classif
ication: Potentially Bad Traffic] [Priority: 2] {TCP} 127.123.161.199:31411 -> 1
0.0.0.3:21
03/08-00:06:00.505607  [**] [1:528:5] BAD-TRAFFIC loopback traffic [**] [Classif
ication: Potentially Bad Traffic] [Priority: 2] {TCP} 127.124.255.205:31492 -> 1
0.0.0.3:21
03/08-00:06:00.573812  [**] [1:528:5] BAD-TRAFFIC loopback traffic [**] [Classif
ication: Potentially Bad Traffic] [Priority: 2] {TCP} 127.243.142.70:31720 -> 10
.0.0.3:21
```

FIGURA 8 - Ataque DOS sendo detectado

Fonte: (Linuxhint, 2018)

3.1.2 – Treinamento SNORT

A Sourcefire (agora parte da Cisco), os criadores do Snort, oferece treinamento em sala de aula e com instrutor virtual, bem como treinamento sob demanda e no local para o Snort e práticas recomendadas de escrita de regras (SNORT, 2021).

O treinamento pode ser feito também através de cursos disponibilizados por empresas especializadas, como por exemplo a 4Bios IT Academy. Segundo eles o treinamento completo visa ensinar ao profissional o real funcionamento do Snort, demonstrando e explicando o funcionamento de protocolos além das funcionalidades, combinando fortemente a teoria e a prática (4BIOS IT ACADEMY, 2021).

3.2 – Metasploit

Matheus Henrique Anselmo dos Santos RA: 2221104180

De acordo com Viera (2011) o *Metasploit* é um conjunto que contém plataformas de aprendizagem e investigação para o profissional da área de segurança. Ele possui diversos *exploits* e ferramentas avançadas que nos permite testar vulnerabilidades em muitas plataformas, sistemas operacionais e servidores.

Segundo Viera (2011) o principal objetivo do *Metasploit* é criar um ambiente de pesquisa, desenvolvimento e exploração de vulnerabilidades, fornecendo algumas ferramentas necessárias para pesquisa que pode ser dividido em:

- **Descoberta da Vulnerabilidade:** Onde o pesquisador descobre um erro de programação que pode levar ou não a uma brecha de segurança.
- **Análise:** Onde o pesquisador analisa a vulnerabilidade para determinar quais as maneiras pelas quais a mesma pode ser explorada.
- **Desenvolvimento do *exploit*:** Nesta fase começa o desenvolvimento da exploração em si, como prova da existência real da vulnerabilidade. Técnicas de engenharia reversa, e programação. São usadas nessa fase.
- **Teste do *exploit*:** Nessa fase o *exploit* é testado em diferentes variáveis e ambientes, *packs*, *patches* e *services*. O *exploit* é a prova definitiva de que a vulnerabilidade pode ser explorada.

Como dito Viera (2011), o *Metasploit* possui uma aceitação maciça, pois qualquer que seja a sua escolha de plataforma de uso (*BSD*, *Like-Uinx*, *Windows*, *Mac X*), pode instalá-lo e usar todas suas ferramentas sem dificuldades. Sua interface pode ser vista na Figura 9.

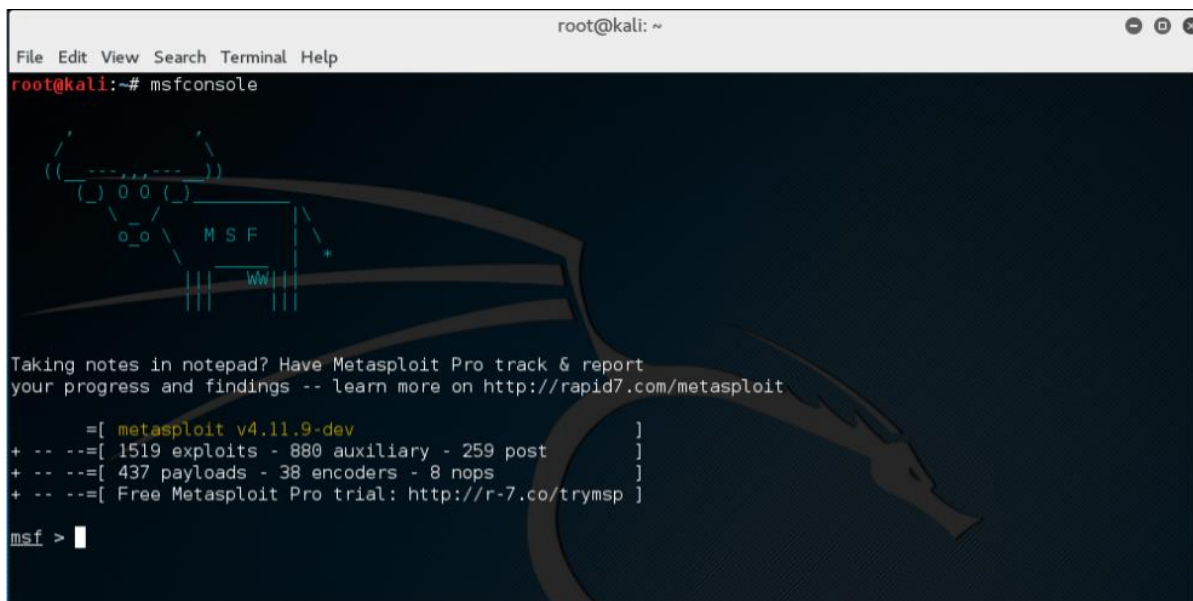


FIGURA 9 - Interface do Metasploit
Fonte: (Veiga, 2019)

3.2.1 – História

Segundo Porup (2019) H. D. Moore lançou o *Metasploit* 1.0 em 2003 escrito em *perl*, desde então o projeto cresceu drasticamente. Com o crescimento do projeto a empresa de segurança Rapid7 adquiriu o *Metasploit*, tornando H. D. Moore diretor de segurança do Rapid7 e arquiteto-chefe do *Metasploit*. A partir disto o *Metasploit* se tornou de fato a estrutura para desenvolvimento de *exploits*. Moore deixou o projeto em 2016.

3.2.2 – Comandos

Abaixo será apresentado alguns comandos *do metasploit* segundo Kumar (2021):

- *Msfupdate* é um comando de administração usado para atualizar o *Metasploit* com *exploits* de vulnerabilidade mais recentes. A execução do comando pode ser vista na Figura 10.

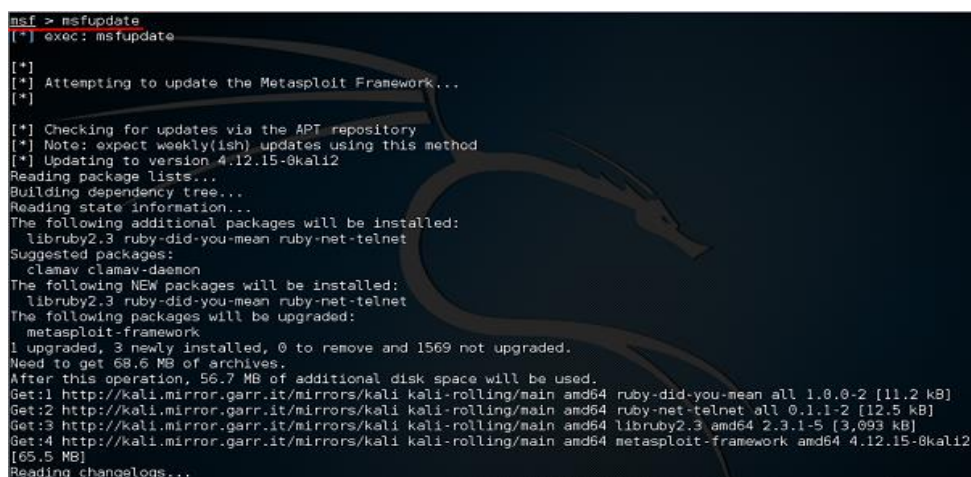


FIGURA 10 - Comando Msfupadate
Fonte: (Tutorialspoint, 2021)

- *Search* é um comando que você pode usar para localizar informações sobre o que deseja. Exemplo, se você quer encontrar *exploits* relacionados à Microsoft, o comando será: *msf >search name:Microsoft type:exploit*. Conforme Figura 11.

```
msf > search name:microsoft type:exploit

Matching Modules
=====


| Name                                                 | Disclosure Date | Rank   | Description                                                              |
|------------------------------------------------------|-----------------|--------|--------------------------------------------------------------------------|
| auxiliary/admin/http/iis_auth_bypass                 | 2010-07-02      | normal | MS10-065 Microsoft IIS 5 NTFS Stream Authentication Bypass               |
| auxiliary/admin/kerberos/ms14_068_kerberos_checksum  | 2014-11-18      | normal | Microsoft Kerberos Checksum Validation Vulnerability                     |
| auxiliary/admin/ms/ms08_059_his2006                  | 2008-10-14      | normal | Microsoft Host Integration Server 2006 Command Execution Vulnerability   |
| auxiliary/admin/mssql/mssql_enum                     |                 | normal | Microsoft SQL Server Configuration Enumerator                            |
| auxiliary/admin/mssql/mssql_enum_domain_accounts     |                 | normal | Microsoft SQL Server SUSER SNAME Windows Domain Account Enumeration      |
| auxiliary/admin/mssql/mssql_enum_domain_accounts_sql |                 | normal | Microsoft SQL Server SQLi SUSER SNAME Windows Domain Account Enumeration |
| auxiliary/admin/mssql/mssql_enum_sql_logins          |                 | normal | Microsoft SQL Server SUSER SNAME SQL Logins Enumeration                  |
| auxiliary/admin/mssql/mssql_escalate_dbowner         |                 | normal | Microsoft SQL Server Escalate Db Owner                                   |
| auxiliary/admin/mssql/mssql_escalate_dbowner_sql     |                 | normal | Microsoft SQL Server SQLi Escalate Db Owner                              |
| auxiliary/admin/mssql/mssql_escalate_execute_as      |                 | normal | Microsoft SQL Server Escalate EXECUTE AS                                 |
| auxiliary/admin/mssql/mssql_escalate_execute_as_sql  |                 | normal | Microsoft SQL Server Escalate EXECUTE AS SQL                             |


```

FIGURA 11 - Comando Search
Fonte: (Tutorialspoint, 2021)

- *Info* é um comando que fornece informações sobre uma plataforma ou módulo, como quem é o autor, como e onde é usado, referências de vulnerabilidades. A execução do comando pode ser vista na Figura 12.

```
msf auxiliary(iis_auth_bypass) > info auxiliary/admin/http/iis_auth_bypass

Name: MS10-065 Microsoft IIS 5 NTFS Stream Authentication Bypass
Module: auxiliary/admin/http/iis_auth_bypass
License: Metasploit Framework License (BSD)
Rank: Normal
Disclosed: 2010-07-02

Provided by:
Soroush Dalili
sinn3r <sinn3r@metasploit.com>

Basic options:


| Name      | Current Setting | Required | Description                                                  |
|-----------|-----------------|----------|--------------------------------------------------------------|
| Proxies   |                 | no       | A proxy chain of format type:host:port[,type:host:port][...] |
| RHOST     |                 | yes      | The target address                                           |
| RPORT     | 80              | yes      | The target port                                              |
| SSL       | false           | no       | Negotiate SSL/TLS for outgoing connections                   |
| TARGETURI | /               | yes      | The URI directory where basic auth is enabled                |
| VHOST     |                 | no       | HTTP server virtual host                                     |



Description:
This module bypasses basic authentication for Internet Information Services (IIS). By appending the NTFS stream name to the directory name in a request, it is possible to bypass authentication.

References:
http://cvedetails.com/cve/2010-2731/
http://www.osvdb.org/66168
http://technet.microsoft.com/en-us/security/bulletin/MS10-065
http://soroush.secproject.com/blog/2010/07/iis5-1-directory-authentication-bypass-by-using-i30index_allocation
```

FIGURA 12 - Comando Info
Fonte: (Tutorialspoint, 2021)

3.2.3 – Engenharia Social no Metasploit

Para Kumar (2021) a engenharia social pode ser definida como um processo de extração de informações confidenciais como (usuários, nomes e senhas). Os *hackers* por diversas vezes utilizam sites falsos e ataques de *phishing* para essa finalidade. Kumar (2021) menciona também como funciona os ataques de Engenharia Social por meio de alguns exemplos:

- Pode ser notado que documentos antigos da empresa são jogados no lixo. Alguns desses documentos podem conter informações confidenciais, como números de contas, números de telefones, nomes, números de segurança social, endereços. Embora pareça improvável, os hackers podem recuperar informações das lixeiras da empresa vasculhando o lixo.
- O invasor pode fazer amizade com funcionários da empresa e obter um bom relacionamento com ele por um período. Essa relação pode ser obtida por salas de bate papo online, por meio das redes sociais, ou offline, em festas, bares. O invasor adquire a confiança dos funcionários do escritório e, finalmente, obtém as informações confidenciais necessárias sem ser descoberto.
- O engenheiro social pode fingir se passar por um funcionário da empresa, um usuário válido falsificando um cartão de identificação ou convencendo os funcionários de sua posição na empresa. Assim o invasor obtém acesso a áreas restritas, dando a ele mais oportunidades para ataques.
- Em diversos casos o invasor pode estar perto de você e “navegar pelos ombros” enquanto você digita informações confidenciais, como senhas, PIN da conta, ID de usuário.

3.2.5 – Ataque de Engenharia Social no Metasploit

Abaixo será mostrado um tutorial de criação de uma campanha de *Phishing* segundo Kumar (2021):

Acessando a página inicial do *Metasploit Pro* e selecionando *Phishing Campaign*, conforme Figura 13.

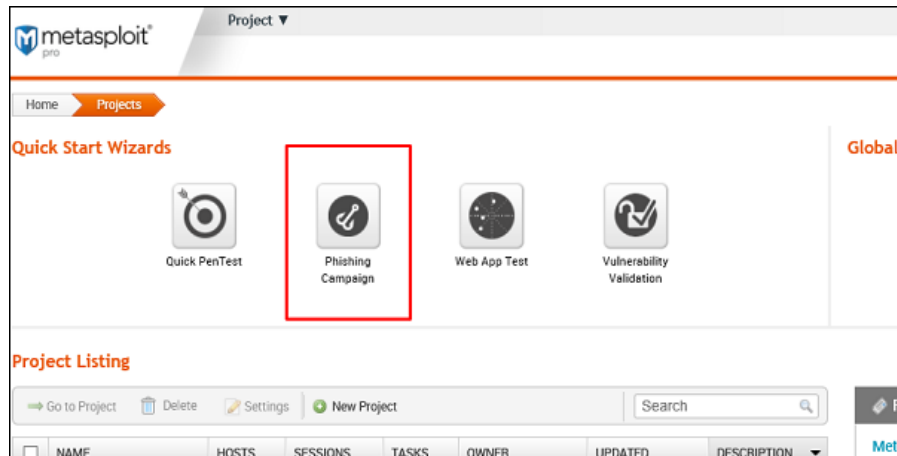


FIGURA 13 - Engenharia Social
Fonte: (Tutorialspoint, 2021)

Escolhendo o nome do projeto e clicando em *Next*, conforme Figura 14.

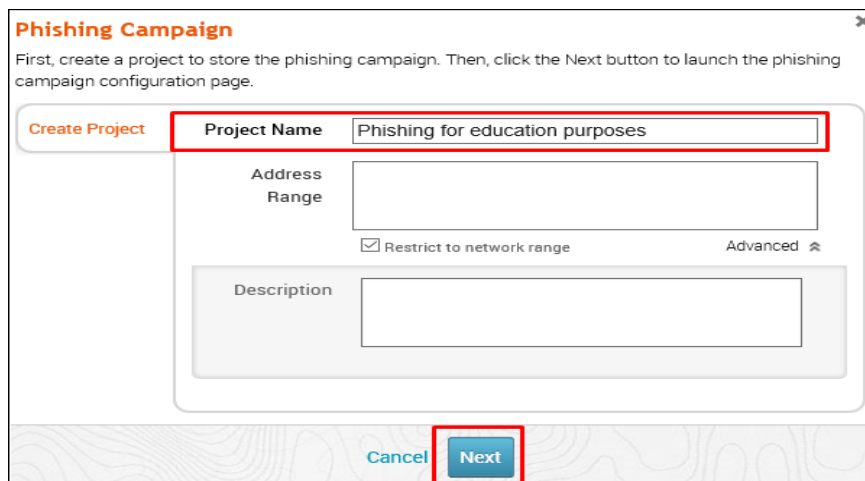
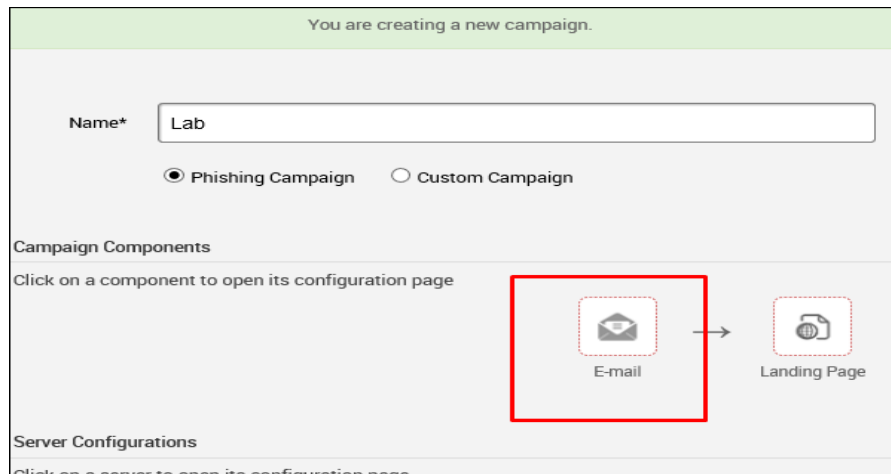
The image shows a 'Phishing Campaign' configuration dialog box. It has a title bar with a close button. The main text says: 'First, create a project to store the phishing campaign. Then, click the Next button to launch the phishing campaign configuration page.' Below this, there's a 'Create Project' section. It contains a 'Project Name' text box with the value 'Phishing for education purposes' (highlighted with a red box), an 'Address Range' text box, a 'Description' text box, and a checked checkbox labeled 'Restrict to network range'. There's also an 'Advanced' link with a chevron icon. At the bottom, there are 'Cancel' and 'Next' buttons, with the 'Next' button highlighted by a red box.

FIGURA 14 – Campanha de Phishing
Fonte: (Tutorialspoint, 2021)

Digitando o nome da campanha. No nosso caso, é *Lab*. Clicando no ícone *E-mail* em *Campaign Components*, conforme Figura 15.



You are creating a new campaign.

Name*

☒ Phishing Campaign ☐ Custom Campaign

Campaign Components

Click on a component to open its configuration page

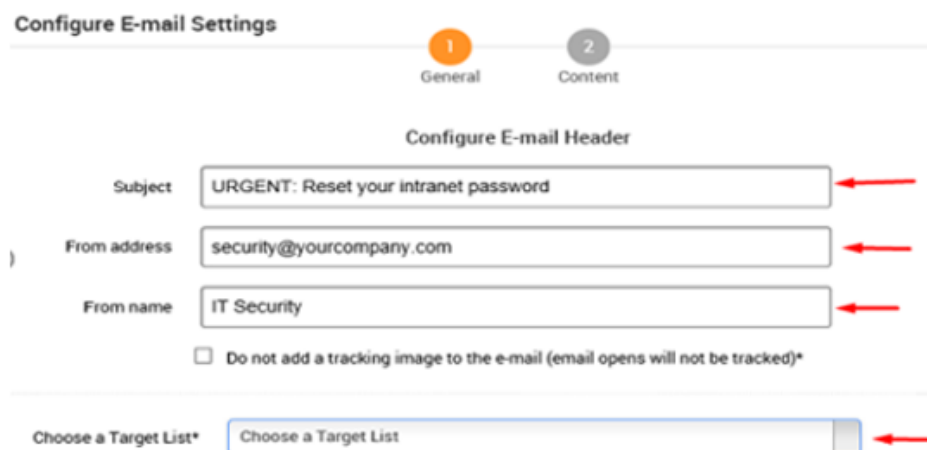
☒ E-mail ☐ Landing Page

Server Configurations

Click on a server to open its configuration page

FIGURA 15 - Definindo nome da campanha Phishing
Fonte: (Tutorialspoint, 2021)

Nessa tela será fornecido os dados solicitados de acordo com a sua campanha, conforme Figura 16.



Configure E-mail Settings

1 General 2 Content

Configure E-mail Header

Subject

From address

From name

☐ Do not add a tracking image to the e-mail (email opens will not be tracked)*

Choose a Target List*

FIGURA 16 - Configurando E-mail
Fonte: (Metasploit, 2021)

Logo em seguida clicando no ícone *Content*, caso deseje alterar algo no conteúdo do e-mail. Após alteração o conteúdo, selecionando a opção *Save*, conforme Figura 17.

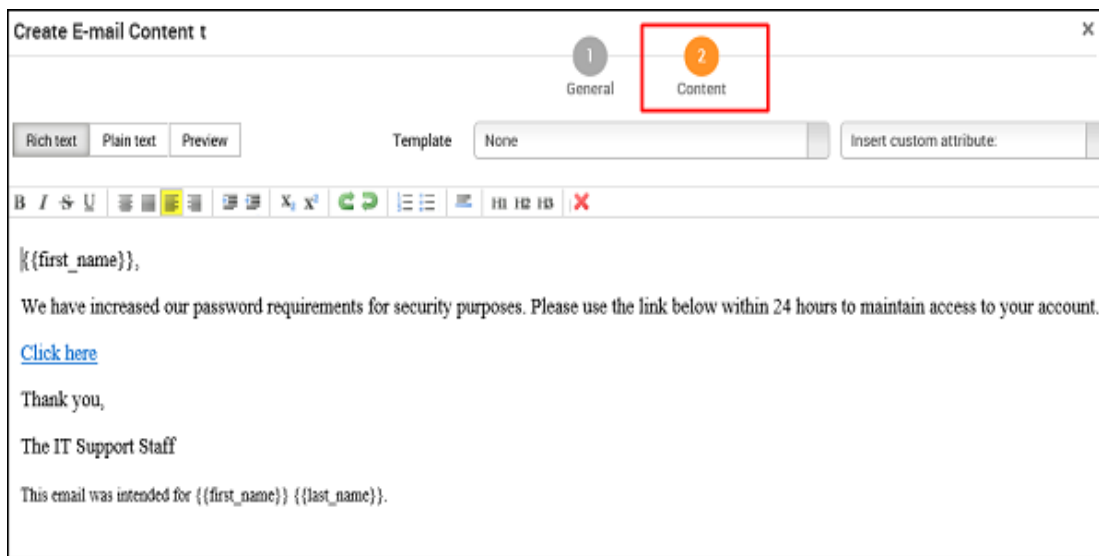


FIGURA 17 – Conteúdo do e-mail Phishing
Fonte: (Tutorialspoint,2021)

Selecionando a opção *Landing Page* para definir os *URLs* para onde deseja direcionar seus usuários enganados, conforme Figura 18.

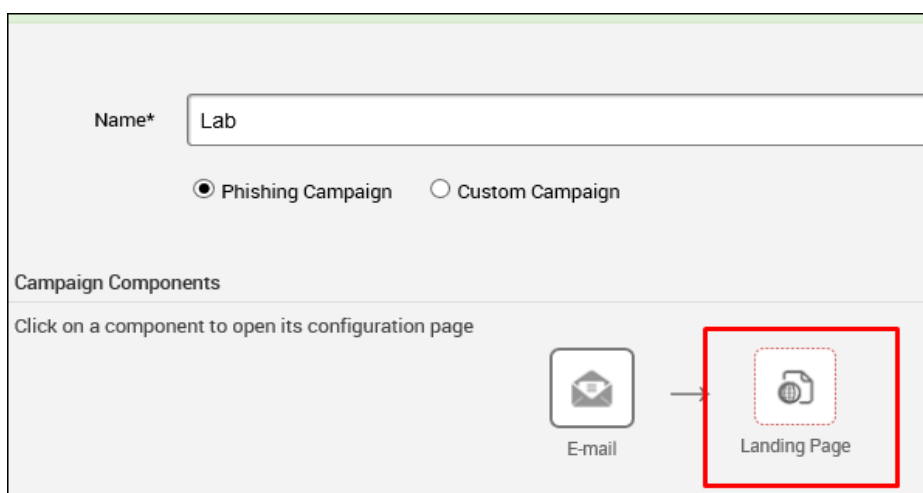


FIGURA 18 - Definindo redirecionamento por URL
Fonte: (Tutorialspoint, 2021)

Como mostrado na Figura 19, deverá ser inserida a *URL* em *Path* e clicando em *Next*.

FIGURA 19 - Definindo nome da página a ser direcionada
Fonte: (Tutorialspoint. 2021)

Na tela seguinte, clicando no botão *Clone Website* que abrirá outra janela. Nessa janela deverá ser inserido o site que a ser clonado. Como exemplo foi inserido o site *tutorialpoint.com* neste campo. Clicando no botão *Clone* e salvando as alterações, conforme Figura 20.

FIGURA 20 - Criando conteúdo da Página WEB
Fonte: (Tutorialspoint, 2021)

Clicando em *Redirect Page*, conforme Figura 21.

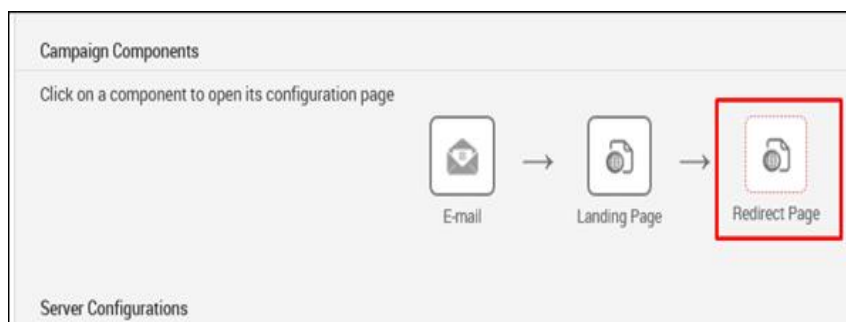


FIGURA 21- Componentes da Campanha
Fonte: (Tutorialspoint, 2021)

Selecione a opção *Next* aparecerá a tela, conforme Figura 22.

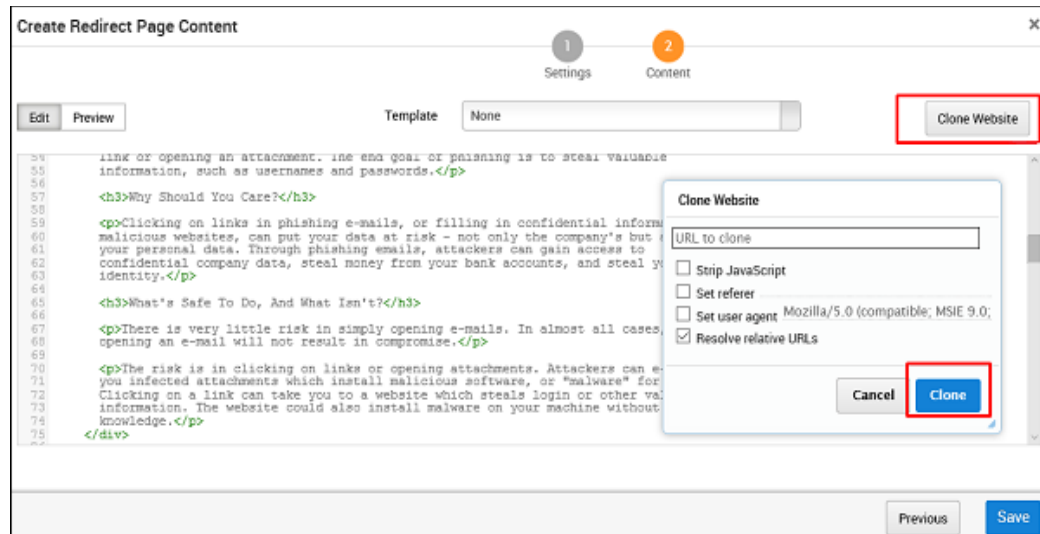


FIGURA 22 - Criando conteúdo da Página Redirecionada
Fonte: (Tutorialspoint, 2021)

Clicando no botão *Clone Website* para clonar o site redirecionado novamente, conforme Figura 23.

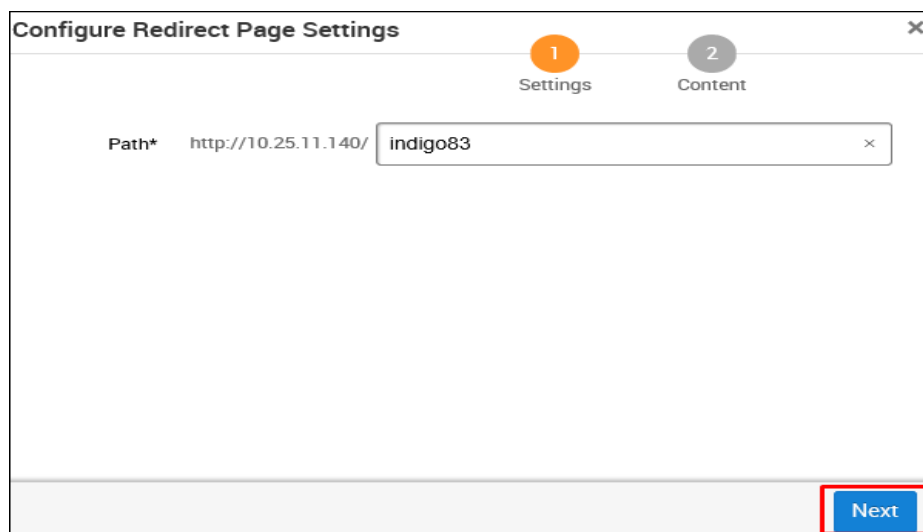


FIGURA 23 - Configurando parâmetros da página de redirecionamento
Fonte: (Tutorialspoint, 2021)

Selecione a opção *Server Configuration*, e clique no botão *E-mail Server*, conforme Figura 24.



FIGURA 24 - Abrindo configurações do servidor de e-mail
Fonte: (Tutorialspoint, 2021)

Na tela a seguir, digite a informação *mailserver settings* que será usado como retransmissão para enviar o e-mail de *phishing*. Em seguida, clique em *Save*, conforme Figura 25.

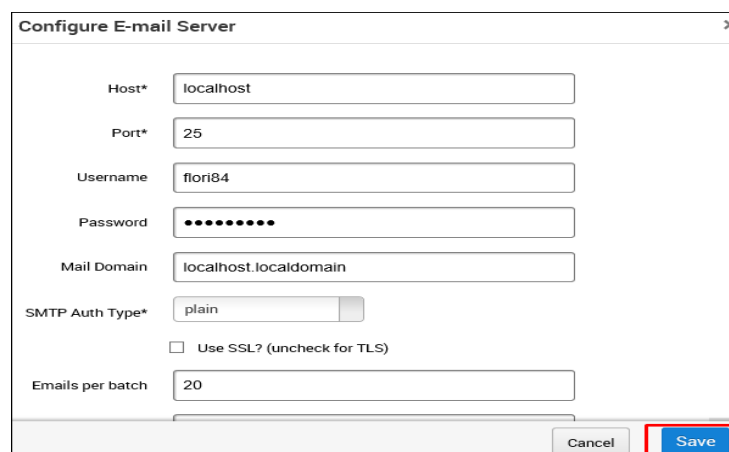


FIGURA 25 - Alterando configurando do servidor de e-mail
Fonte: (Tutorialspoint, 2021)

Na área de *Notifications*, haverá a opção *Notify others before launching the campaign*. Podendo escolher opcionalmente esta opção para outras pessoas serem notificadas. Em seguida, selecione a opção *save*, conforme Figura 26.



FIGURA 26 - Outras notificações da campanha
Fonte: (Tutorialspoint, 2021)

Na próxima imagem aparecerá uma nova janela. Em que será preciso clicar em *Start* para iniciar o envio de *emails* de *phishing*, conforme Figura 27.

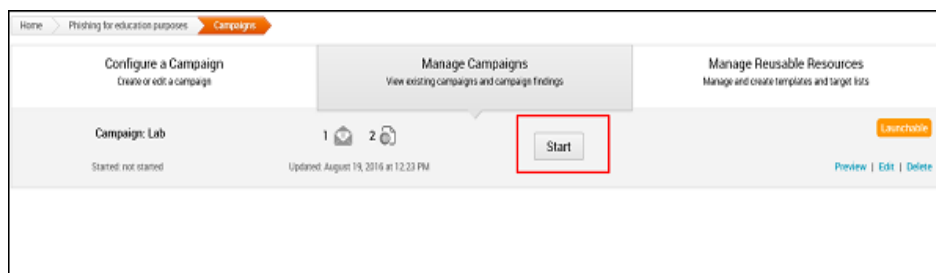


FIGURA 27 - Iniciar o envio de e-mail phishing

Fonte: (Tutorialspoint, 2021)

O *Metasploit Pro* tem a opção de gerar relatório estatístico de sua campanha de *phishing*, conforme Figura 28.

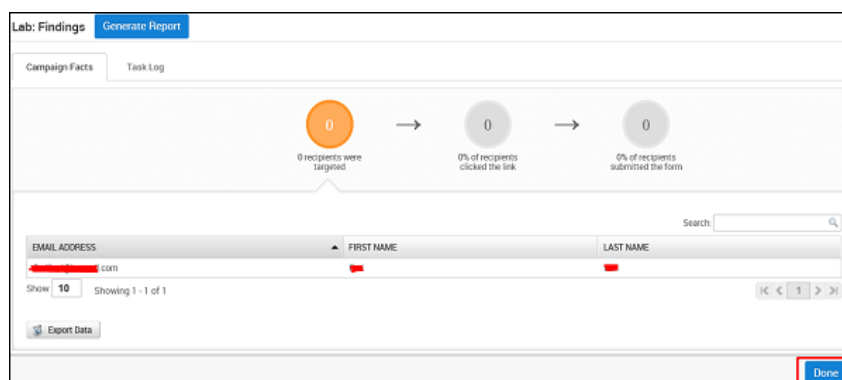


FIGURA 28 - Gerar relatório da campanha Phishing

Fonte: (Tutorialspoint, 2021)

3.3 – Tails

Leandro Barbosa RA:2218106814

De acordo com Brito (2013) Tails, trata-se de um sistema operacional que foi desenvolvido com base na distribuição Debian do Linux. A ferramenta tem como foco, manter sua navegação e qualquer informação no extremo anonimato, rodando em modo live, a ferramenta utiliza criptografia para proteger tudo que está sendo executado naquele momento. Existem algumas opções onde o sistema pode ser instalado, tais como o DVD e o pen drive, e ao final do processo, tudo que foi feito naquele momento em que o sistema estava sendo executado, é eliminado em seguida, após o usuário desconectar o dispositivo USB ou desligar/reiniciar o computador.

Segundo Prass (2016), após o computador ser reiniciado, o pen drive devidamente conectado e com o sistema instalado, será necessário que o modo de inicialização na BIOS esteja habilitado, dependendo do modelo do computador, a configuração para o modo de inicialização tem uma grande chance de variar. Em praticamente todos os modelos encontrados no mercado, seria necessário pressionar alguma dessas teclas: DEL, F2, F10, ESC e em seguida, aguardar até tela de configuração seja exibida, conforme a figura 29.

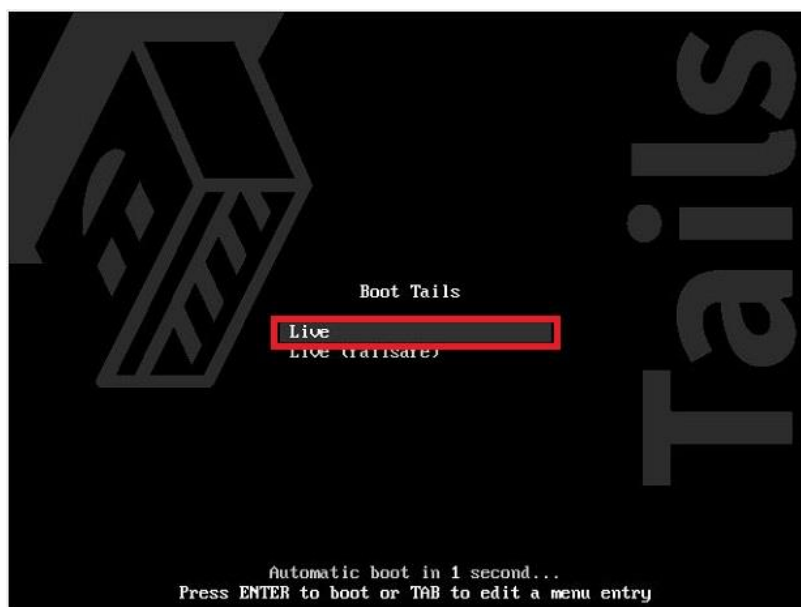


FIGURA 29 - Sistema Tails

Fonte: (G1.Globo, 2016)

Conforme Tails (2020), o sistema utiliza uma grande variedade de ferramentas, focando sempre na segurança digital, tais como:

- Navegador Tor focado em segurança e acoplado com um bloqueador de anúncios;
- Thunderbird, utilizado para criptografar os e-mails;
- KeePassXC, criação de senhas fortes e armazenamento;
- LibreOffice, se trata de um pacote de ferramentas para escritório;
- OnionShare, utilizado para compartilhamento de arquivos usando a rede Tor
- Caso ocorra alguma tentativa de conexão com a internet sem utilizar a rede Tor, todas as aplicações serão bloqueadas automaticamente;
- Todos os dados/informações que estão no armazenamento persistente, são criptografados automaticamente;
- O Tails não efetua a gravação das informações no disco rígido, sendo assim, a memória é totalmente apagada ao desligar o computador.

Tails (2020) também relata, cita uma grande vantagem em usar o Tor Browser como navegador, evitando que os sites aos quais serão acessados durante a navegação pela internet, descubram a sua identidade e localização, apenas sendo possível, se o próprio usuário fornece as informações, sendo assim, será possível efetuar o gerenciamento a alguma rede social sem que seja descoberta a verdadeira identidade do usuário.

Luiz Enrique da Costa Santos RA:2220112596

The screenshot displays the dnstenum tool interface, which is a command-line utility for performing DNS enumeration. The interface is divided into several sections:

- Host's addresses:** Shows the IP address 600 IN A 82.98.86.174 for the host example.com.
- Reverse Servers:** Lists reverse DNS records for the IP address 82.98.86.174, showing results for ns2.revenueirect.com, ns1.revenueirect.com, and ns1.revenueirect.com.
- Mail (MX) Servers:** Shows the MX records for the domain example.com, listing mail servers like aspmx.l.google.com and aspmx2.l.google.com.
- Trying Zone Transfers and getting Bind Versions:** Shows the results of zone transfer attempts and bind version detection for the domain example.com.
- Trying Zone Transfer for example.com on ns2.revenueirect.com ...:** Shows the results of zone transfer attempts for the domain example.com on the server ns2.revenueirect.com.

The interface also includes a menu bar at the top with options: File, Edit, View, Bookmarks, Settings, Help. The bottom status bar shows the command dnstenum : dnstenum.pl.

Fonte: (Junovan, 2013)

CAPÍTULO 4 – MERCADO DE PERÍCIA

Roberto Tiyoza Watanabe Junior RA: 2219109625

Gabriel Brito de Moura RA:2219108437

Ludmille Damasceno De Barros RA: 920129341

Em janeiro de 2021, ocorreu um dos maiores vazamentos de dados da história, cerca de 223 milhões de informações foram vazadas, incluindo e-mail, CPF, CNPJ sexo, nome, data de nascimento, telefone e informações fiscais de brasileiros. Criminosos estão tentando vender os dados, não sendo possível comprar o pacote de maneira integral, mas somente trechos, segundo (ROHR, 2021)

A transformação digital fez da informação uma poderosa ferramenta de geração de valor para as organizações. Consequentemente, a cibersegurança ganhou ainda mais importância (HSC, 2020). Segundo analistas do Fórum Econômico Mundial (2018) uma única invasão a um servidor que armazena informações na nuvem pode gerar um prejuízo de até 120 bilhões de dólares

Para proteger as organizações desse problema, foi criada uma carreira profissional, chamada de perito forense digital. *“Existe uma demanda alta nos órgãos públicos e um mercado para ser explorado nas empresas privadas”*, Marcos Supioni (2020, VOCÊ S/A, ed. 263), professor na HSM University. A partir da função clássica de perito forense, o foco na área digital surgiu após os avanços da informática.

Existem diversas oportunidades de emprego na área, é possível atuar por conta própria como perito técnico das partes (ou seja, diretamente com o cliente que esteja com processo aberto na Justiça), como perito judicial (designado pelo juiz do caso), como funcionário público concursado e como empregado de empresas e consultorias. Segundo Morales (2020, VOCÊ S/A, ed. 263) perito em computação forense e sócio-diretor da STW Brasil, empresa de segurança em TI, *“Há oportunidades, mas é difícil encontrar profissionais qualificados”*

Morales (2020, VOCÊ S/A, ed. 263) ainda complementa que, o caminho mais comum é graduar-se em tecnologia da informação e complementar com o aprendizado jurídico. Não é necessário ter formação superior em direito. É preciso saber sobre o meio jurídico, mas existem certificações próprias que valem mais do que uma graduação. Ou seja, a carreira tem foco em técnicas de informática, como rastreamento de sistemas, e não em conhecimentos jurídicos.

4.1 – Rotina De Trabalho de um Perito Criminal Digital

As horas trabalhadas chegam a até 10 horas por dia, porém a rotina varia de acordo com o projeto. O tempo é separado, 40% em análise (buscando caminhos e falhas no sistema e investigando crimes), 40% em elaboração de relatórios, e 20% em coleta de material e provas. (VOCÊ S/A, ed. 263, 2020).

4.2 – Principais Competências

É indispensável que o profissional tenha raciocínio lógico, domínio sobre os meios tecnológicos e possua conhecimento jurídico. O conhecimento em inglês deve ser avançado ou fluente, para melhor utilização dos programas e sistemas de investigação. Atenção, calma e disciplina são *soft skills* recomendadas. (VOCÊ S/A, ed. 263, 2020)

4.3 – Atividades-Chave

Segundo o coordenador e professor do curso de pós-graduação em Perícia Criminal e Ciências Forenses do Instituto de Pós-Graduação e Graduação (IPOG), Walber Pinheiro (2017) as principais atividades seriam, analisar informações de computadores, celulares, pontos eletrônicos e outros dispositivos para a elaboração de laudos que comprovem crimes ou fraudes virtuais, a coleta e a preservação de evidências, assim como testes de segurança de sistemas.

4.4 – O Que Fazer Para Atuar Na Área

Segundo Milagre (2017) Diretor de Relacionamentos com *Law Enforcement na LegalTech* Brasil, Diretor do GU de Direito Digital e CyberCrimes da SUCEUSU-SP, e Professor da Pós em Computação Forense na Universidade Presbiteriana Mackenzie, novos e desafiadores casos são constantes. O perito digital não pode ser apenas um técnico, muito menos o jurista. É necessário ter conhecimentos de projetos, especialidade em conduzir o processo de perícia, avaliando os interesses e dados das partes, mediar e ser um profundo conhecedor da Ciência da Informação, Análise de Sistemas, Ciência da Computação e tecnologia da informação dão uma base, porém a especialização na área é fundamental, podendo ser feita através de cursos internacionais, como CCFT (*Certified Computer Forensic Technical*), CEH (*Certified Ethical Hacker*) e CHFI (*Certified Hacker Forensic Investigator*).

4.5 – Quem Contrata

Empresas de tecnologia que trabalham com grande volume de dados, como bancos, consultorias e institutos de pesquisa. As esferas federal e estadual do governo também recrutam por meio de concursos públicos dos setores criminal, trabalhista e civil. (CHALIZED, 2021)

4.5.1 – Salário

Pinheiro (2017) explica que é difícil estimar a média salarial, pois existem vários campos de atuação do profissional de carreira forense com salários bem distintos que dependem do cargo (perito federal, perito estadual, perito judicial, perito particular, entre outros). Por exemplo, um perito federal, no início de carreira, tem vencimento mensal de aproximadamente R\$ 20.000,00, já um perito particular pode ganhar em um único caso pericial os mesmos R\$ 20.000,00. Segundo o IBAPE (2020) os salários giram em torno de R\$19.000,00 para concursados e quem trabalha em empresas, ou R\$ 430,00 por hora para autônomos.

CAPÍTULO 5 – INTERNET E AS QUESTÕES DE SEGURANÇA

5.1 – O que é Deep Web

Matheus Brasil RA: 921113230

William do Carmo RA: 2220103364

Segundo Pompéo e Seefeldt (2013), a expressão Deep Web foi criada por Michael K. Bergman, fundador do programa Bright Planet, software especializado em captura, classificar e vasculhar conteúdo nessa esfera da Web. A expressão Deep Web, traduzida ao português, remete ao significado de profundidade, tanto que fixada em oposição a Surface Web, vocábulo que visa dar a ideia de superficialidade.

Para Wright (2009) a Deep Web consistente em sites que, diferente da internet convencional, são desenvolvidos propositamente para que não sejam encontrados. Assim, mesmo existindo, esses sites não são acessados pelo grande público, ficando invisíveis nas “profundidades” da rede.

Ainda conforme Wright (2009) em relação ao alcance de seu conteúdo, assim como a internet tradicional, a *Deep Web* é usualmente classificada em camadas, conforme Figura 31. Quando o usuário adentra à *Deep Web*, ele possui acesso gradual. A primeira camada concentra a maioria das informações necessárias aos iniciantes, mas, desde que se tenha um conhecimento mais avançado de informática e outros requisitos exigidos, é possível ir mais além. Bergman acredita que existem, no mínimo, dez camadas de conteúdo da *Deep Web*. Dentro das acepções de arquitetura da rede, a configuração dessas páginas pode se dar por inúmeros conteúdos, conteúdo dinâmico, conteúdo isolado, conteúdo de acesso limitado, conteúdo de script, conteúdo não-HTML/texto, conteúdo antigo, web contextual e web privada.



FIGURA 31 - Surface Web e Deep Web
Fonte: Ronaldo Gogoni (2019)

5.2 – Ameaças na Deep Web

Matheus Brasil RA: 921113230

Para Timochenco (2016) a facilitação e benefício que a web obtém, contém riscos aos quais estamos expostos neste ambiente, páginas falsificadas, vírus, vazamento de informações, pessoas mal-intencionadas, e-mails maliciosos, roubo de dados e de identidade, são apenas alguns do risco que a web carrega. Se, com está visão compreendemos que podemos nos conectar a ela sem muita dificuldade, também observamos que nos tornamos vulneráveis a ela, tendo riscos à segurança e à privacidade. Não são todos os usuários que compreendem os riscos, se até a primeira camada da surface web nós expomos a altos riscos, os demais níveis podem ser muito mais perigosos.

Segundo Castells (1999), a prática criminosa internacional passa a existir de dois jeitos. A primeira acontece após o enraizamento em uma determinada localidade de uma organização criminosa dita tradicional, por motivos diversos, e espalha-se para países terceiros e conseguir assimilar diferentes associados e aumentar sua zona de atuação. Por isso, essas organizações não diminuem seus integrantes com a globalização, mas aumenta seu grupo criminoso. A segunda está na criação de operações criminosas locais, geralmente fundadas em populações de renda baixa, que barganha seu crime para mercados de todas as partes do planeta.

Para Aragão (2013), diante à intensa supervisão das autoridades policiais, a comunicação entre essas organizações criminosas não consegue ser por meio da Surface Web. Por isso, muitas delas usam a Deep Web para criptografar e enviar informações, barganhar dados com suas associadas e espalhar suas atividades em diversos cantos do mundo. Por isso, a Deep Web já tem inúmeros casos conhecidos.

5.2.1 – Conteúdos da Deep Web

Kelver Daniel RA: 2219104613

Vinicius Calmona Crepaldi De Lima RA: 2219104613

“A Dark Web ilustra a tensão entre a privacidade e a publicidade: a liberdade de expressão e até valores maniqueístas do bem e do mal, arquétipos humanos ressignificados ou virtualizados no ciberespaço” (MONTEIRO E FIDÊNCIO, 2013, p. 44)

Para Franco (2016), a maioria dos dados contidos na *Dark Web* são de péssima qualidade, ilícitos e normalmente dispensáveis, pode-se dizer que a Dark Web é dividida em duas camadas, sendo uma destas, onde fica a *Hidden Wiki*, e uma camada que contém conteúdos criados por indivíduos ou grupos que realmente entendem sobre privacidade e segurança, e somente quem tem permissão e o link de acesso conseguem entrar. Para Chen (2012) nesta segunda camada,

algumas pessoas más intencionadas se utilizam da navegação anônima para cometer crimes, como por exemplo, cenas de atentados terroristas verídicos, guias para confecção de explosivos, grupos nazistas, terrorismo biológico e armamentos nucleares.

Porém o conteúdo encontrado na *Dark Web* não são apenas coisas ruins, podem-se encontrar diversos materiais, como por exemplo, materiais acadêmicos, hackers éticos, filmes, livros, e por ser um local que garante anonimidade, este possibilita a participação de diversas manifestações contra sistemas totalitários ao redor do mundo (ORTEGA E ORTIS, 2013).

5.5 – Navegador Tor e Rede

Leandro Barbosa RA:2218106814

De acordo com Harada (2016), o Tor se trata de um software gratuito, e de código aberto, onde seus usuários podem navegar por toda rede de internet sem ter o risco de ter a sua identidade revelada. O nome Tor vem das iniciais “*The Onion Router*”, um projeto criado na linguagem C, tratando-se de uma ideia iniciada pelo Laboratório de Pesquisa Naval dos Estados Unidos, que vem ajudando inúmeros usuários a continuarem anônimos enquanto estiverem online na internet.

5.5.1 – Como funciona

Segundo Lozhkin (2014), todos os recursos que deixam o usuário completamente no anonimato, só é possível devido a grande quantidade de serviços ou roteadores chamados de “nós”, operando através dos anéis de cebola, onde se originou o nome “O Roteador de Cebola”. Todas as informações que estão passando pela rede, todo o tráfego, precisa passar por vários nós, sendo criptografada constantemente, além do mais, não é possível saber o conteúdo do tráfego que está sendo passado pelos nós da rede, a fonte e nem o destino, assegurando um nível elevado de anonimato. A Figura 32 Mostra um exemplo de nós do tráfego de rede TOR.

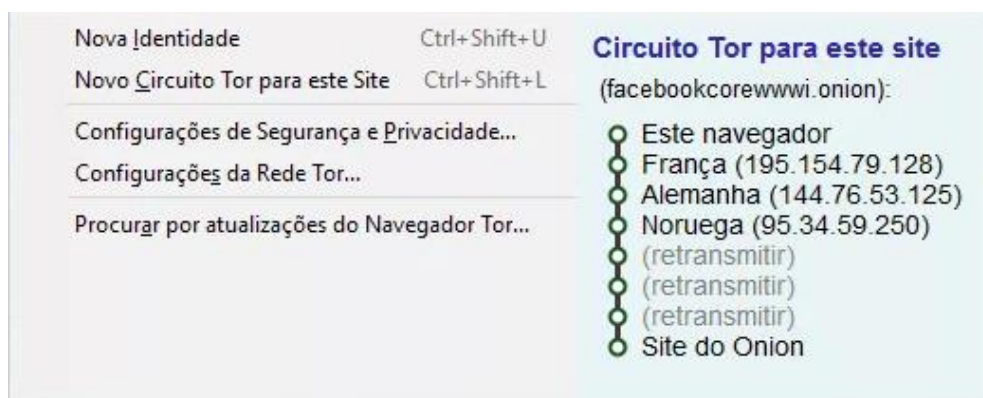


FIGURA 32 - Nós do tráfego de rede do circuito TOR

Fonte: (Tecnundo, 2016)

5.5.2 – Endereços de sites “.onion”

Para Brito (2016), um site “.onion” trata-se de endereços para um serviço oculto, ou seja, só podem ser acessados utilizando a rede Tor, sem correr o risco das informações e atividades que estão sendo efetuadas, estarem sendo monitoradas por algum terceiro. Esses domínios estão ligados diretamente com a *deep web*, não sendo possível acesso por um navegador da internet normal, desta forma, qualquer usuário que hospede um site nesta rede, teoricamente ninguém irá conseguir encontra-lo, tendo como exemplo o Facebook, o mesmo possui um endereço Tor oficial, sendo acessado através do <https://facebookcorewwwi.onion/>, conforme Figura 33, portanto, é possível o acesso de qualquer um, sem que em momento algum, a conexão saia da rede Tor, conseqüentemente, não podendo ser monitorada, uma forma muito utilizada em países que efetuam o bloqueio ao acesso para redes sociais.

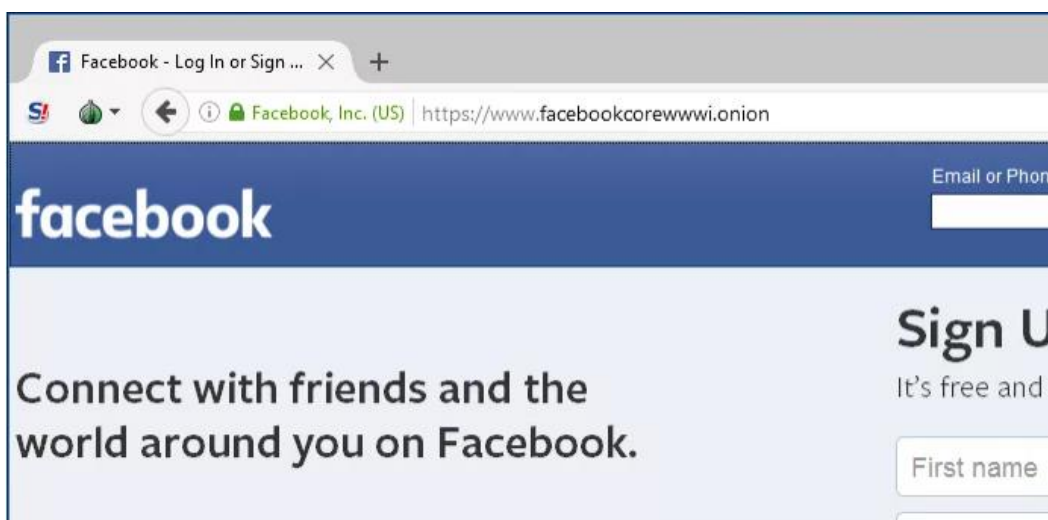


FIGURA 33 - Link Onion do Facebook
Fonte: (Tecnundo, 2016)

5.5.3 – Estrutura de Rede TOR

Segundo Barbosa (2020), Toda a parte técnica, que envolve os roteamentos no Tor, seria uma questão bem complexa, para tentar simplificar, o mesmo apresenta na Figura 34.

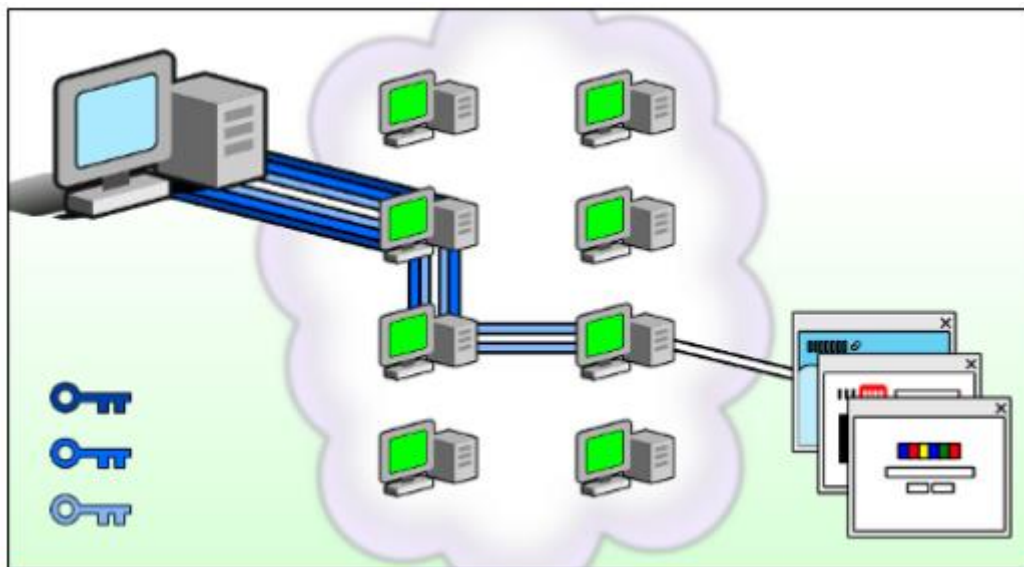


FIGURA 34 - Estrutura da Rede TOR
Fonte: (Torproject, 2017)

Referente a imagem acima, representa a divisão em 3 partes: origem, *relays* e destino, respectivamente.

Barbosa (2020) complementa, a origem: trata-se de todos usuários da rede Tor, que precisam ter seu tráfego pela rede protegido. *Relays* refere-se aos voluntários que concederam as suas conexões, para possibilitar a navegação de outros usuários, sendo três relays no mínimo para todas as conexões utilizando a rede TOR, tais como:

- Relays de entrada (*Entry/Guard*): Possibilitando que a origem tenha liberado o primeiro acesso à rede TOR;
- Relays intermediários (*Middle*): Encaminham todo tráfego do que se encontram no relay de entrada, direto para o relay de saída;
- Relays de saída (*Exit*): Enviam uma requisição solicitada pelo usuário de origem, para o destino original.

Ainda para Barbosa (2020) destino refere-se as páginas de internet que desejam ser acessadas pela origem.

Com a existência dos 3 níveis de criptografia, surge uma dificuldade para que ataques à esta rede sejam executados, fazendo com que os provedores de internet, tenham conhecimento sobre quais destinos os usuários tentam navegar, portanto, fica inviável uma aplicação de restrições para sites específicos (BARBOSA, 2020).

5.5.4 – Executando o navegador Tor

A instalação do navegador é extremamente simples, sendo necessário apenas selecionar o idioma e escolher a pasta onde o arquivo será instalado.

Após efetuar o download do arquivo, irá apresentar uma janela de configuração da rede Tor, sendo assim, será possível efetuar a primeira conexão apenas clicando no botão “conectar”, conforme figura 35 (TOR PROJECT, 2021).



FIGURA 35 - Navegador TOR
Fonte: (Tor Project, 2021)

Normalmente, clicando no botão citado, já será possível efetuar a conexão na rede Tor sem nenhuma configuração complementar, após clicar, irá aparecer a barra de status, com o progresso da conexão (TOR PROJECT, 2021).

CONCLUSÃO

Em síntese, a problemática abordada com relação a proteção das informações pessoais e corporativas em um ambiente virtual está relacionado à segurança de redes de computadores, e assim como a tecnologia evolui, as formas e ferramentas de ataques cibernéticos também. Atualmente existem diversas classificações de atacantes, desde o básico até o avançado, estes são categorizados de acordo com seu conhecimento técnico e ideologias. Para manter-se seguro é necessário existir uma boa infraestrutura de rede, utilizando-se de mecanismos, ferramentas e fundamentos que foram exemplificados no decorrer do artigo.

O estudo possibilitou o conhecimento sobre o mercado de trabalho na área de segurança, mostrando o que é necessário para se tornar um profissional, empresas que contratam, quanto pagam e principais competências requisitadas.

Com base nas pesquisas realizadas no projeto conclui-se que, a internet não é tão segura quanto se imagina, existem locais em que a anonimidade permite a realização de vários atos ilegais e as consequências que podem advir dessas ações. E apesar dessa anonimidade sempre estar relacionada a algo negativo, ela também pode ser utilizada para algo positivo, como por exemplo em um governo que censura o acesso à informação da sua população, proporcionando liberdade de expressão e acesso a conteúdo antes não permitido.

REFERÊNCIA BIBLIOGRÁFICA

4BIOS IT ACADEMY (2021) “IDS Snort. 4Bios IT Academy” acesso em 04/2021:
<https://www.4biosacademy.com.br/4bios-snort>

ARAGÃO, Alexandre (2013) “Nas Profundezas da WEB”. Jornal Folha de São Paulo, p. F1.

ARAUJO, Wagner J. D (2009) “A segurança do conhecimento nas práticas da gestão de segurança da informação e da gestão do conhecimento”. Tese de Doutorado em Ciência da Informação, Brasília.

BARBOSA, Daniel C (2020) “O que é o TOR e para que serve?” acesso em 04/2021:
<https://www.welivesecurity.com/br/2020/12/30/o-que-e-o-tor-e-para-que-serve>

BRITO, Edivaldo (2013) “Tails. Tech Tudo” acesso em 04/2021:
<https://www.techtudo.com.br/tudo-sobre/tails.html>

CANAL TI (2017) “IDS e IPS: Conceitos e diferença” acesso em 04/2021:
<https://www.canalti.com.br/seguranca-da-informacao/ids-ips-conceitos-e-diferencas>

CARVALHO, Luciano G. (2005) Segurança de Redes. Rio de Janeiro: Ciência Moderna.

CASTELLS, Manuel (1999) “A era da informação: economia, sociedade e cultura” 3°. ed. São Paulo: Paz e Terra

CASWELL, B. Beale, J. (2004) “Snort 2.1 Intrusion Detection” 2. Ed. Rockland: Syngress.

CERTBR (2021) “Estatísticas dos Incidentes Reportados ao CERT.br” acesso em 03/2021:
<https://www.cert.br/stats/incidentes>.

CHEN, H (2012) “Dark Web: Exploring and data mining the dark site of the web” 2. Ed. Stillwater: Springer

CHESWICK, William R.; BELLOVIN, Steven M.; RUBIN, Aviel D (2005). “Firewalls e Segurança na Internet Repelindo o hacker ardiloso”. 2. ed. São Paulo: Saraiva

CORREIO BRAZILIENSE (2020) “Entenda o que é a deep web e a dark web” acesso em 18/05: <https://www.correiobraziliense.com.br/tecnologia/2020/09/4878415-entenda-o-que-e-a-deep-web-e-a-dark-web-as-camadas-profundas-da-internet.html>

DOHERTY, Jim; ANDERSON, Neil; MAGGIORA, Paul D. (2008) Cisco Networking. 2. ed. Indianapolis: Cisco Press

FANTIN, Junovan (2016) “Obtendo informações de um servidor DNS usando dnsenum” acesso em 04/2021: <https://home.junovan.com.br/obtendo-informacoes-de-um-servidor-dns-usando-dnsenum>.

FRANCO, Deivison P. (2016) “Deep Web: Mergulhando no sub-mundo da Internet”. Revista Crypto ID, acesso em 05/2019:
<https://cryptoid.com.br/banco-de-noticias/mergulhando-e-navegando-no-submundo-da-deep-web/>

- GIAVAROTO, Sílvia C. R.; SANTOS, Gerson R. D (2013) “Estudo das Técnicas e Aplicabilidade da Ferramenta Backtrack 5 R3 Linux” Rio de Janeiro: Editora Ciência Moderna Ltda
- HARADA, Eduardo (2016) “Tor: entenda como esta rede garante o seu anonimato na internet. Tecmundo” acesso em 04/2021:
<https://www.tecmundo.com.br/seguranca/104364-tor-entenda-rede-garante-anonimato-internet.htm>
- HSC - HIGHT SECURITY CENTER (2021) “Conheça as principais ameaças virtuais” acesso em: <https://www.hscbrasil.com.br/principais-ameacas-virtuais>.
- KASPERSKY (2021) “Cyberthreat real-time map, Cybermap” acesso em 04/2021:
<https://cybermap.kaspersky.com/stats>
- KUMAR, Ramagiri R. (2021) “Learn Metasploit. Tutorials Point” acesso em 04/2021:
https://www.tutorialspoint.com/metasploit/metasploit_basic_commands.htm
- LA FONTAINE, Jean D. (1866) “La Fontaine's Fables” A. Mame et fils, p. 132
- LEVY, Steven. Hackers: Heroes of the Computer Revolution. 25. ed.
- LOZHKIN, Sergey (2014) “Entenda a Rede Tor. Kaspersky” acesso em 05/2021:
<https://www.kaspersky.com.br/blog/entenda-a-rede-tor/2411/>
- METASPLOIT (2021) “Quick Start Guide” metasploit.com, acesso em 03/2021:
<https://docs.rapid7.com/metasploit>
- MILAGRE, José A. (2017) “A profissão do futuro: Como ser um perito digital ou perito em informática e iniciar na carreira” acesso em 03/2021:
<https://josemilagre.com.br/blog/2017/07/31/a-profissao-do-futuro-como-ser-um-perito-digital-ou-perito-em-informatica-e-iniciar-na-carreira-2017>
- MONTEIRO, S. D.; V, FIDÊNCIO M. (2013) “As dobras semióticas do ciberespaço: da web visível à invisível”. Campinas, V. 1, p. 35-46, acesso em 03/2021: <https://www.puc-campinas.edu.br/periodicocientifico>
- MONTORO, Rodrigo (2012) “Introdução ao Snort - Série Snortando” Spookerlabs, acesso em 04/2021: <http://spookerlabs.blogspot.com.br/2012/01/introducao-ao-snort-serie-snortando.html>
- NAKAMURA, Emilio G. P. (2002) Segurança de redes em ambientes corporativos. Novatec, 1. Ed, p. 07 e 80
- NETO, Daniel J. D. S.; MAURICIO, Lucas H.; COSTA, Vitor P. D. (2011) “Sistema de Detecção de Intrusão” UFRJ, acesso em 03/2021:
http://www.gta.ufrj.br/grad/11_1/sdi/index.html
- NORTHCUTT, Stephen (2001) “Segurança e Prevenção em Redes” Berkley: p. 48
- ORTEGA E ORTIS, J. (2013) “Você sabe o que é a Deep Web?” Olhar Digital, acesso em 02/2021: <http://olhardigital.uol.br/video/voce-sabe-o-que-e-a-deep-web/32156>.

PINHEIRO, Walber. (2017) “Profissão do Futuro: Como ser um Perito Digital? Profissionais, 21321” acesso em 03/2021: <https://www.profissionais.com.br/profissao-do-futuro-como-ser-um-perito-digital>

POMPEO, Wagner A. H.; SEEFELDT, João P. (2013) “Nem tudo está no Google: Deep Web e o Perigo da Invisibilidade” 2º Congresso Internacional de Direito e Contemporaneidade.

PORUP, J.M. (2019) “What is Metasploit? And how to use this popular hacking tool. CSO Online” acesso em 04/2021: <https://www.csoonline.com/article/3379117/what-is-metasploit-and-how-to-use-this-popular-hacking-tool.html>

PRASS, Ronaldo (2016) “Tails: saiba usar o sistema operacional que promete total anonimato na internet” G1 Globo, acesso em 04/2021: <http://g1.globo.com/tecnologia/blog/tira-duvidas-de-tecnologia/post/tails-saiba-usar-o-sistema-operacional-que-promete-total-anonimato-na-internet.html>

PROCTOR, Paul E. (2001) “The Practical Intrusion Detection Handbook” 1 Ed. Prentice Hall p.20

ROHR, Altieres (2021) “Megavazamentos de dados expõem informações de 223 milhões de números de CPF” G1.GLOBO, acesso em 03/2021: <https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/01/25/vazamentos-de-dados-expoem-informacoes-de-223-milhoes-de-numeros-de-cpf.ghtml>

ROUFA, Timothy (2021) “Como se tornar um examinador forense digital” Chalized. acesso em 03/2021: <https://pt.chalized.com/como-se-tornar-um-examinador-forense-digital/>

SÊMOLA, Marcos (2011) “Gestão da Segurança da Informação” Uma visão executiva, 2. Ed. Modulo.

SILVA, Liliam D. S. (2008) “Uma Metodologia para Detecção de Ataques no Tráfego de Redes Baseada em Redes Neurais” Doutorado em Computação Aplicada – Instituto Nacional de Pesquisas Espaciais, São José dos Campos, 256f.

SNORT, CISCO (2021) “Snort” acesso em 04/2021: <https://snort.org/>

TAILS BOUM ORG (2020) “How Tails works” Tails Boum Org, acesso em 05/2021: <https://tails.boum.org/about/index.pt.html>

TANEMBAUM, Andrew S. (2003) “Redes de Computadores” 4. Ed. Campus

THE INTERNATIONAL TELECOMMUNICATION UNION (1991) “X-800: Security Architecture for Open Systems Interconnection for CCITT Applications”

TIMOCHENCO, Longinus (2016) “Deep web e dark web: Os perigos da web profunda e obscura” Infra New Telecom, acesso em 04/2021: <https://infranewstelecom.com.br/deep-web-e-dark-web-os-perigos-da-web/>

TOR PROJECT (2021) “Executando o navegador Tor pela primeira vez” Tor Project Org, acesso em 05/2021: <https://tb-manual.torproject.org/pt-BR/running-tor-browser/>

TRIBUNAL DE CONTAS DA UNIÃO (2012) “Cartilha de boas práticas em segurança da Informação” 4. Ed. Brasília: p.10

VANNEY, Ivan (2018) Configure Snort IDS and Create Rules. Linux Hint, acesso em 04/2021: <https://linuxhint.com/configure-snort-ids-create-rules/>

VEIGA, Miguel S. D. (2019) “Metasploit desmistificado - Usar a MSFConsole” acesso em 04/2021: <https://medium.com/canivete-sui%C3%A7o-hacker/metasploit-desmistificado-ii-1-68ee353114d1>

VIEIRA, Luiz (2011) “Metasploit Framework – Parte 01” Imasters, acesso em 04/2021: <https://imasters.com.br/devsecops/metasploit-framework-parte-01>

WIRED (2014) “Tails: the operating system that blew open the NSA” acesso em 04/2021: <https://www.wired.co.uk/article/tails-operating-software>

WRIGHT, Alex (2009) “Exploring a ‘Deep Web’ That Google Can’t Grasp”. The New York Times, acesso em 04/2021: https://www.nytimes.com/2009/02/23/technology/internet/23search.html?th&emc=th&_r=1&