



FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Superior de Tecnologia em Segurança da Informação

Kenya Marri Pereira Braga
Matheus Henrique Dutra Okazaki

HONEYPOT: Detecção e análise de ataques

Americana, SP

2020

FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Superior de Tecnologia em Segurança da Informação

KENYA MARRI PEREIRA BRAGA
MATHEUS HENRIQUE DUTRA OKAZAKI

HONEYPOT: Detecção e análise de ataques

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do(a) Prof(a). Especialista Marcus Vinícius Lahr Giraldi.

Área de concentração: Segurança em Sistemas Operacionais e redes de computadores.

Americana, SP.

2020

KENYA MARRI PEREIRA BRAGA
MATHEUS HENRIQUE DUTRA OKAZAKI

HONEYPOT: Detecção e análise de ataques

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/Americana.

Área de concentração: Segurança em Sistemas Operacionais e redes de computadores.

Americana, Dezembro de 2020.

Banca Examinadora:

MARCUS VINICIUS LAHR GIRALDI (Presidente)
Especialista
Fatec Americana Ministro Ralph Biasi

MARIA CRISTINA ARANDA (Membro)
Doutor(a)
Fatec Americana Ministro Ralph Biasi

RENAN MERCURI PINTO (Membro)
Doutor
Fatec Americana Ministro Ralph Biasi

AGRADECIMENTOS

Gostaríamos de agradecer todas as pessoas que estiveram ao nosso lado durante esta trajetória, principalmente nossos professores e famílias.

DEDICATÓRIA

Aos nossos familiares e amigos que sempre nos apoiaram em nossas escolhas.

RESUMO

A Tecnologia traz benefícios incomparáveis à sociedade, com o passar do tempo novas soluções tecnológicas são criadas, nos tornando mais conectados e conseqüentemente mais expostos aos riscos digitais, assim é essencial aplicar políticas de Segurança da Informação e utilizar ferramentas para minimizar possíveis falhas em uma rede e assegurar a confidencialidade, integridade e disponibilidade da informação. O *honeypot* é um método/ferramenta utilizada para o apoio ao monitoramento da rede, seu objetivo é "enganar e atrair" o invasor a tentar um ataque cibernético, pois o ambiente parece um sistema real com dados e aplicativos. Ao atrair o *hacker*, podemos captar informações do atacante, a ferramenta é capaz de identificar qualquer acesso à rede, e armazenar as informações, auxiliando na análise por exemplo do tipo de invasor e suas motivações. A partir dos dados coletados dos ataques é possível realizar estudos e melhorias contínuas na rede para prever ataques e reduzir as possíveis falhas de segurança. Objetivo é através de pesquisas e a implantação de um ambiente, realizar testes utilizando as Ferramentas Valhala e Cowrie, e apresentar as configurações, testes, resultados, e os benefícios em utilizar um *honeypot* como ferramenta de apoio a segurança da rede. Com os *honeypots* Valhala e Cowrie foi possível identificar diversas tentativas de ataques reais e simulados utilizando os seguintes protocolos de rede: TELNET, SMTP, FTP, TFTP, POP3 e SSH, com base nas informações captadas foi possível entender quais IPs e o que os invasores tentaram exatamente fazer ao invadir.

Palavras Chave: *honeypot*, invasão, ataque.

ABSTRACT

Technology brings incomparable benefits to society, with the passage of time new technological solutions are created, making us more connected and consequently more exposed to digital risks, so it is essential to apply Information Security policies and use tools to minimize possible failures in a network and ensure the confidentiality, integrity and availability of information. Honeypot is a method/tool used to support network monitoring, its purpose is to "trick and attract" the attacker to attempt a cybernetic attack, as the environment looks like a real system with data and applications. When attracting the hacker, we can capture information from the attacker, the tool is able to identify any access to the network, and store the information, assisting in the analysis, for example, of the type of attacker and their motivations. Based on the data collected from the attacks, it is possible to carry out studies and continuous improvements on the network to predict attacks and reduce possible security flaws. Objective is through research and the implantation of an environment, carry out tests using the Valhala and Cowrie, and configurations, tests, results, and the benefits of using a honeypot as a tool to support network security, with the valhala and cowrie honeypots it was possible to identify the various real attackers and simulated, using the network protocols: TELNET, SMTP, FTP, TFTP, POP3 and SSH, based on the information captured it was possible to understand which IPs and what the attackers tried to do exactly when to break into.

Keywords: honeypot, invasion, attack.

SUMÁRIO

1	INTRODUÇÃO	141.1	OBJETIVO		
152			HONEYPOT		
162.1	TIPOS	DE	HONEYPOT		
172.2	NÍVEIS	DE	INTERAÇÃO		
182.3	POSICIONAMENTO	NA	REDE		
192.4			HONEYNET		
193	PRINCIPAIS		FERRAMENTAS		
214	PRINCIPAIS	PROTOCOLOS	UTILIZADOS	NOS	HONEYPOTS
244.1					TELNET
244.2					FTP
254.3					POP3
264.4					TFTP
264.5					SSH
274.6					SMTP
285	TESTES	REALIZADOS	EM	AMBIENTE	REAL
295.1	INFORMAÇÕES	GERAIS	-	TESTES	VALHALA
295.1.1					AMBIENTE
295.1.2					FERRAMENTAS
305.1.2.1					VALHALA
305.1.2.2					PUTTY
305.1.2.3			EM		CLIENT
315.1.4		CONFIGURANDO			SERVIÇOS
315.1.4.1		INSTALAÇÃO			VALHALA
315.1.4.2					TELNET
325.1.4.3					FTP
325.1.4.4					POP3
335.1.4.5					TFTP
335.1.4.6					SMTP
335.1.5		TESTES			REALIZADOS
345.1.5.1					TELNET
345.1.5.2					FTP
385.1.5.3					POP3

435.1.5.4				TFTP
485.1.5.5				SMTP
495.2	INFORMAÇÕES	GERAIS	-	TESTES
545.2.1				COWRIE
545.2.2		FERRAMENTA		AMBIENTE
545.2.3		INSTALAÇÃO		COWRIE
555.2.4	CONFIGURAÇÃO		SERVIÇO	SSH
585.2.5	TESTE		SERVIÇO	SSH
596		RESULTADO		TESTES
626.1		INVASÕES		SIMULADAS
626.2	INVASÕES		REAIS	CAPTADAS
637				CONCLUSÃO
		65	REFERÊNCIAS BIBLIOGRÁFICAS	67

LISTA DE FIGURAS

Figura 1: Comparativo níveis de interação	18
Figura 2: Posicionamento <i>honeypot</i>	19
Figura 3: Topologia <i>Honeynet</i>	20
Figura 4: Ferramenta Deception Toolkit (DTK)	21
Figura 5: Ferramenta Backofficer Friendly (BOF)	21
Figura 6: Ferramenta Honeyd	22
Figura 7: Ferramenta Kfsensor	22
Figura 8: Ferramenta Specter	23
Figura 9: Tentativas de Invasão Projeto Honeynet(Cert-br) - Principais Protocolos	24
Figura 10: Protocolo SSH	28
Figura 11: Tela inicial Valhala	31
Figura 12: Configuração Telnet	32
Figura 13: Configuração FTP	32
Figura 14: Configuração POP3	33
Figura 15: Configuração TFTP	33
Figura 16: Configuração SMTP	33
Figura 17: Ferramenta Putty	34
Figura 18: Acessando serviço Telnet	34
Figura 19: Verificando diretórios	35
Figura 20: Valhala - Log Telnet	35
Figura 21: Log de uma tentativa real via telnet	36
Figura 22: Log - 8 IPs diferentes	36
Figura 23: Site IP GreyNoise 109.147.189.209	36
Figura 24: Log - Invasão Telnet	37
Figura 25: Log - Invasão Telnet	38
Figura 26: Invasão serviço FTP	38
Figura 27: Valhala - Log FTP	39
Figura 28: Invasões externas	39
Figura 29: Log - Invasões FTP	40
Figura 30: Site GreyNoise IP104.206.128.30	40
Figura 31: Log - Invasão FTP	41
Figura 32: Log - Invasão FTP	41

Figura 33: Log - Invasão FTP	42
Figura 34 - Quantidade de tentativas de ataques por IP	42
Figura 35: EM Client - Configurando E-mail falso	43
Figura 36: EM Client - Configurando E-mail falso	43
Figura 37: EM Client - Configurando Servidor de Entrada	44
Figura 38: EM Client - Configurando Servidor de Saída	44
Figura 39: EM Client – Testando POP3	45
Figura 40: Valhala - Log POP3	45
Figura 41: Valhala - Outro invasor	46
Figura 42: Invasão Externa POP3	46
Figura 43: Log - Invasão POP3	47
Figura 44: Log - Invasão POP3	47
Figura 45: Log - Invasão POP3	47
Figura 46: Log - Invasão POP3	48
Figura 47: Serviço TFTP	48
Figura 48: Valhala - Log TFTP	48
Figura 49: Invasão Externa - TFTP	49
Figura 50: Log - Invasão TFTP	49
Figura 51: Invasão Externa - SMTP	50
Figura 52: Log - Invasão SMTP	50
Figura 53: Log - Invasão SMTP	51
Figura 54: Log - Invasão SMTP	51
Figura 55: E-mail Phishing	52
Figura 56: Log - Invasão SMTP	53
Figura 57: Honeypot Cowrie	55
Figura 58: Arquivo de log	55
Figura 59: Análise em tempo real de invasões	55
Figura 60: Atualização biblioteca Ubuntu	56
Figura 61: Instalação biblioteca python	56
Figura 62: Adicionando usuário e senha ao Cowrie	56
Figura 63: Realizando download do Cowrie	57
Figura 64: Instalação Sistema Operacional falso	57
Figura 65: Configuração serviço SSH	58
Figura 66: Atualização do arquivo de Configuração do Cowrie	58

Figura 67: Configuração porta 22 - usuário comum	59
Figura 68: Configuração porta do SSH	59
Figura 69: Verificando LOG	60
Figura 70: Log - Invasão SSH	60
Figura 71: Log - Invasão SSH	60
Figura 72: Log - Invasão SSH	60
Figura 73: Quantidade de invasões por serviço	63
Figura 74: Invasão a outros serviços pelo mesmo IP	64

LISTA DE TABELAS

Tabela 1: Combinações de usuário e senha utilizados pelo IP 2.87.225.195.....37

1 INTRODUÇÃO

A Era Digital e os avanços tecnológicos tornaram a Segurança da Informação indispensável em todas as áreas e serviços. Para garantir a integridade, confidencialidade e disponibilidade dos dados, é necessário aplicar metodologias, políticas, ferramentas de gerenciamento, apoio e proteção aos dados.

Com a difusão da rede os ataques evoluíram e se tornaram cada vez mais frequentes e prejudiciais, tornando essenciais o uso de ferramentas para a proteção da rede, dentre elas o *honeypot*, que deve ser usado como apoio ao monitoramento da rede, pois o objetivo é atrair hackers a “tentar invadir” a rede.

Para Spitzer (2002), o *honeypot* tem como objetivo ser invadido, e captar informações dos ataques, onde pode ser utilizado para: deter ataques, detectar ataques, captar ataques automatizados, captar informações digitadas e diversas outras finalidades.

As informações coletadas do ataque e atacante, permitem analisar por exemplo o tipo de invasor e suas motivações e ao conhecer o perfil dos *hackers* é possível prever os tipos de ataques que a rede poderia sofrer e de forma preventiva minimizar as possíveis falhas de segurança.

O *honeypot* é capaz de identificar qualquer acesso à rede, até mesmo o IP do invasor, assim realizamos testes reais e simulados, onde utilizamos as ferramentas Valhala e Cowrie, e através da análise dos resultados, foram obtidos grandes ganhos em segurança ao aplicar um *honeypot* a rede, pois com as informações dos “ataques”, foram identificados pontos que exigiam mais atenção a rede.

1.1 OBJETIVO

Existem diversas formas e ferramentas de segurança que podem ser aplicadas a uma rede, porém não é possível garantir que ela seja 100% segura, pois está exposta a diversos fatores, como *hackers*, má configuração de equipamento, falta de atualização etc.

O objetivo deste trabalho é implementar um sistema em forma de pesquisa, cujo objetivo é ser invadido e atacado, e, com base nos resultados, serão criados perfis de invasores, detectando seus objetivos e entendendo as técnicas utilizadas no ataque.

Com o *honeypot* é possível identificar possíveis falhas na segurança do seu ambiente, já que as máquinas configuradas estão vulneráveis e preparadas para tal. Além de receber ataques e tentativas de invasões, a máquina configurada com o *honeypot* armazenará informações que poderão ser usadas posteriormente para estudos e melhorias do ambiente.

2 HONEYPOT

Com base no NIC.BR (2003) a primeira menção de monitorar um invasor a rede, ocorreu em 1988, pelo especialista Clifford Stoll, que investigou e monitorou uma invasão nos sistemas do laboratório *Lawrence Berkeley Laboratory (LBL)*, o relato é descrito no livro “*The Cuckoo’s Egg: Tracking a Spy Through the Maze of Computer Espionage*”. De acordo TechBizForense (2011) Clifford descobriu a invasão, ao analisar uma divergência de 0,75 centavos de dólar, em um relatório de uso dados de usuários no sistema Unix e VAX, Clifford encontrou um acesso não permitido de 09 segundos ao sistema e resolveu monitorá-lo por 10 meses ao invés de o barrar, a partir dessa descoberta de invasão foi possível analisar diversos outros sistemas que haviam sido invadidos.

A ideia de preparar uma rede para ser invadida a fim de monitorar o invasor, ocorreu somente em 1991, por Bill Cheswick, ao instalar um dos *gateways AT&T*, decidiu criar ferramentas para monitorar os invasores, assim nasceu o conceito de *honeypot* que é basicamente simular um ambiente, deixando brechas para que *Hackers* sejam atraídos a invadi-lo e assim monitorá-los, para colher informações que poderão ser usadas na análise do tipo de invasor e ataque, e desenvolver melhorias para rede real, sem que ela seja colocada em risco, já que a invasão é apenas na rede simulada.

Em 1998 de acordo com NIC.BR (2003) surgiu a ferramenta *The Deception ToolKit (TDK)* desenvolvida por Fred Cohen, onde ao ser instalada em um sistema operacional, simulava *softwares* com diversas vulnerabilidades, e ao ser invadida realmente parecia ser uma rede, ludibriando os *hackers*, armazenando e colhendo informações técnicas dos ataques.

Para Assunção (2009), o *honeypot* pode ser definido como uma “armadilha”, e pode ser usado também como um sistema de detecção de intrusos:

“Podemos dizer que o *honeypot* possui como finalidade ajudar as ferramentas de detecção de intrusos adicionais, ajudando-as a melhorar suas assinaturas através do descobrimento de novos tipos de ataque. Também pode-se utilizar um pote de mel como um sistema de IDS totalmente independente. Tudo depende do objetivo.” (Assunção 2009, pg. 12)

Para Spitzer (2002) no livro *honeypots: Tracking Hackers*, pode se usar a definição de *honeypot* como uma ferramenta de segurança, que tem como objetivo ser invadido, para fins da análise das informações. O *honeypot* se diferencia dos

outros serviços de segurança, pois esses serviços normalmente têm um objetivo claro, já o *honeypot* pode ser usado de diferentes maneiras, como para: deter ataques, detectar ataques, captar ataques automatizados, como *worms*, captar informações digitadas e diversas outras finalidades.

O *honeypot* deve ser utilizado com as demais ferramentas de segurança, e é considerado ferramenta de apoio ao monitoramento da rede já que não a protege” diretamente”, mas sim colhe informações de invasões, pode ser empregada apenas em um computador, ou também em diversos equipamentos como roteadores e modems. Uma das grandes vantagens de utilizar a ferramenta é que qualquer tentativa de acesso é considerada uma invasão, eliminando os falsos positivos que ocorrem nas redes comuns, já que devido a elevada quantidade de dados, nem sempre os tráfegos maliciosos são detectados.

2.1 TIPOS DE HONEYPOT

O *honeypot* pode ser aplicado a pesquisa ou produção com base no Cert.br (2003):

“*Honeynets* de Pesquisa são ferramentas de pesquisa que podem ser utilizadas para observar o comportamento de invasores, permitindo análises detalhadas de suas motivações, das ferramentas utilizadas e vulnerabilidades exploradas.

Honeypots de Produção podem ser utilizados em redes de produção como complemento ou no lugar de sistemas de detecção de intrusão.” (Cert.br, 2003).

Para Assunção (2009), quando empregado para pesquisa, seu principal objetivo é colher informações: como mapear os ataques, atacantes, táticas empregadas e a motivação do ataque, tudo por fins de pesquisa e análise dados, com a finalidade de buscar novos métodos e como exemplo o desenvolvimento de ferramentas que auxiliam de proteção dos dados, quando utilizado para fins de pesquisa.

De acordo com Assunção (2009), ao ser utilizado em organizações para prevenir ataques a rede é considerado de produção, pois seu principal objetivo é detectar ataques, assim devem ser muito bem configurados, pois caso o invasor consiga acessar a rede haverá um resultado “desastroso”.

2.2 NÍVEIS DE INTERAÇÃO

Para Spitzer (2002), os *honeypots* podem ser classificados, pelo nível de interação que o invasor possui com a ferramenta, podem ser de interação: baixa, média ou alta.

É considerado de interação baixa, quando os serviços da ferramenta são simulados, como serviços e respostas falsas, na interação baixa as informações do atacante são bem limitadas, e sem acesso a rede real, um exemplo é a ferramenta *Netcat* que pode ser utilizada para redirecionar os acessos feitos a porta 80, para um arquivo, gerando um registro de log.

O nível de interação médio, permite o invasor acessar o sistema operacional, tornando possível registrar mais informações do ataque, porém necessita de mais atenção ao analista da ferramenta *honeypot*, já que o invasor pode acessar ferramentas disponíveis do sistema, embora seja um ambiente de testes, é possível como por exemplo iniciar ataques a outras máquinas através do sistema acessado.

A alta interatividade, permite o invasor acessar serviços, sistemas e aplicações reais, as configurações representam por exemplo, uma rede física composta por computadores e dispositivos configurados para receberem ataques, embora tragam vantagens de monitoramento, ao tornar possível a rastreabilidade dos passos do invasor, quando mal implementada pode oferecer grandes riscos, deve ser utilizada apenas por profissionais especialistas e em redes que possuem um grande controle e proteção dos dados.

Figura 1: Comparativo níveis de interação

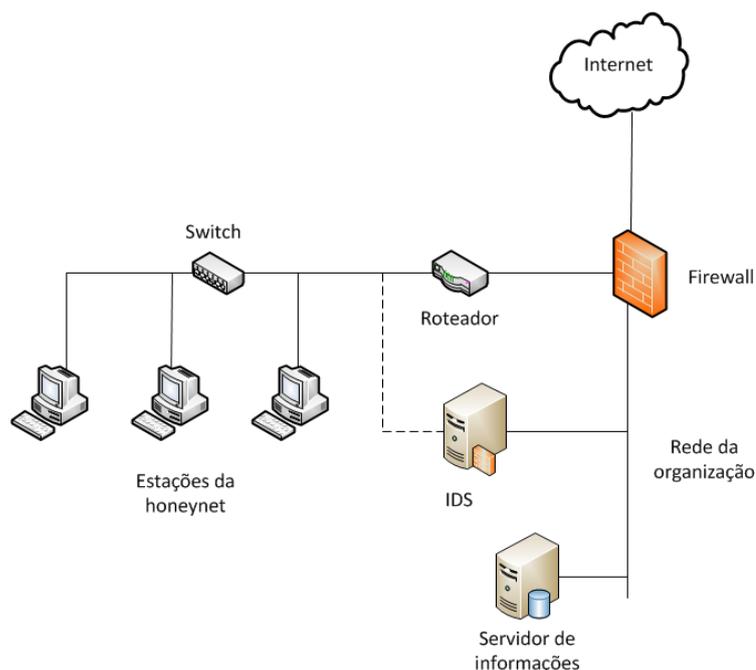
Características	Honeypot de baixa interatividade	Honeypot de média interatividade	Honeypot de alta interatividade
Instalação	fácil	média/difícil	difícil
Manutenção	fácil	média	trabalhosa
Risco de comprometimento	baixo	baixo	alto
Obtenção de informações	muito limitada	limitada	extensiva
Necessidade de mecanismos de contenção	não	sim	sim
Atacante tem acesso ao S.O. real	não	não	sim
Aplicações e serviços oferecidos	emulados	emulados	reais
Atacante pode comprometer o honeypot	não (em teoria)	não (em teoria)	sim

Fonte: Portal DevMedia.

2.3 POSICIONAMENTO NA REDE

Os *honeypots* geralmente são configurados na parte interna da rede, de acordo com a ilustração na Figura 1, ele é configurado atrás do roteador principal da rede e entre os *switchs*, fazendo com que todo o tráfego de saída e entrada passe pelos *honeypots*.

Figura 2: Posicionamento *honeypot*



Fonte: DevMedia.

Neste cenário, o roteador tem como função esconder o *firewall* em um possível comprometimento do *honeypot*, assim criando um ambiente mais realista para os invasores. Outra função muito importante é o roteador ser um ponto de controle de acesso, onde irá auxiliar o *firewall* a evitar possíveis ataques cujas fontes sejam os *honeypots*.

2.4 HONEYNET

Em 1999, surgiu o conceito de *honeynet* de acordo com NIC.BR(2003) através de um projeto criando por um grupo de especialistas, o objetivo era criar uma rede somente para ser atacada, era composta por diversos *honeypots*, assim surgiu o *honeynet*, caracterizado pelo conjunto de *honeypots* frequentemente de alta

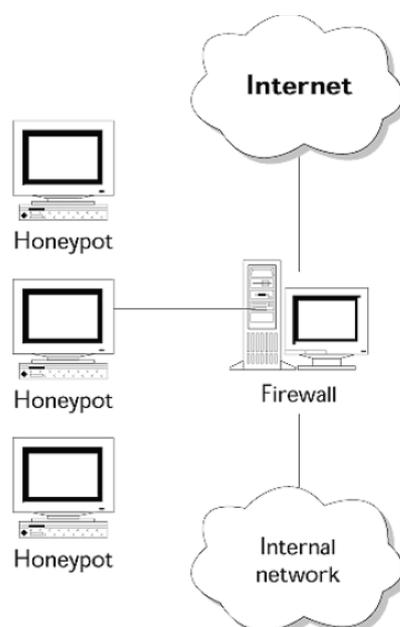
interatividade, são capazes de captar grande volume de dados, auxiliando na análise e estudos das práticas e motivações do ataque.

Para Assunção (2009) *honeynet* é:

“Para entender uma *honeynet* é necessário levar o conceito de *honeypot* a um sentido mais amplo. Se ao invés de você utilizar um único computador como armadilha, que tal uma sala cheia deles formando uma rede com o único objetivo de servir de armadilha? Isso é uma *Honeynet*. A *Honeynet* então basicamente é uma rede na qual todo o tráfego que entra e sai do gateway/roteador é malicioso. Lembre-se do conceito de Segurança por Obscuridade: ninguém conhece os computadores dessa rede, portanto qualquer pacote que se destine a qualquer um deles é um ataque em potencial.” Assunção (2009 pg. 17).

O *Honeynet* pode ser classificado em real e virtual de acordo com o CERT.BR (2007), é considerado real quando o equipamento é físico, onde capta informações, possui alertas e realiza a contenção de dados, pode ser formado por diversos equipamentos físicos, o que gera a desvantagem de manutenção mais complexa, já o *honeypot* virtual possui o mínimo de equipamentos físicos, trazendo vantagens na manutenção. A Figura 2 ilustra uma topologia de *Honeynet*:

Figura 3: Topologia *Honeynet*



Fonte: The Honeynet Project.

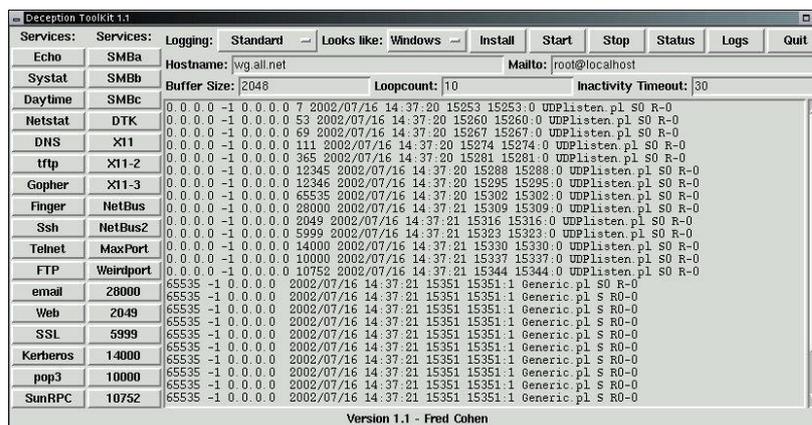
3 PRINCIPAIS FERRAMENTAS

Atualmente existem diversas ferramentas específicas para serviços de *honeypot*, as principais são:

- **DECEPTION TOOLKIT (DTK)**

De acordo com NIC.BR(2003) o DTK foi criado por Fred Cohen a primeira ferramenta que simula vários serviços básicos com vulnerabilidades, a ferramenta permite rastrear as tentativas de invasão do atacante. Veja a seguir na Figura 3, uma imagem do DTK.

Figura 4: Ferramenta Deception Toolkit (DTK)

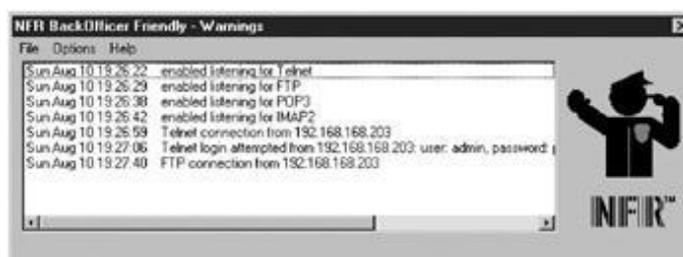


Fonte: Site ALL.

- **BACKOFFICER FRIENDLY (BOF)**

De acordo com CenPRA (2004) o BOF, que pode ser visto na Figura 4, é considerado um software de fácil manuseio, emula serviços básicos e simula respostas quando recebe protocolos como Telnet, FTP, SMTP e POP3.

Figura 5: Ferramenta Backofficer Friendly (BOF)



Fonte: Site FLYLIB.

- **HONEYD**

De acordo com CenPRA (2004) o *Honeyd*, que pode ser observado na Figura 5, é uma ferramenta que permite simular sistemas e aplicações, armazena log e permite criar filtros, é uma das principais ferramentas para a construção de *honeypots*, pode ser utilizada para monitorar as portas baseadas em UDP e TCP.

Figura 6: Ferramenta Honeyd

```

C:\Command Prompt - honeyd -f honeyd.conf 147.100.100.8-147.100.100.9
R:\honeypot\honeyd-0.5a>honeyd -p nnap.prints -f honeyd.conf 147.100.100.8
honeyd.conf:11: parse error
parsing configuration file failed

R:\honeypot\honeyd-0.5a>honeyd -p nnap.prints -f honeyd.conf 147.100.100.8
honeyd.conf:11: parse error
parsing configuration file failed

R:\honeypot\honeyd-0.5a>honeyd -p nnap.prints -f honeyd.conf 147.100.100.8
honeyd.conf:9: parse error
parsing configuration file failed

R:\honeypot\honeyd-0.5a>honeyd -p nnap.prints -f honeyd.conf 147.100.100.8
^C
R:\honeypot\honeyd-0.5a>honeyd -d -i 2 -l LOGFILE -p nnap.prints -x xprobe2.conf
-a nnap.assoc -f honeyd.conf 147.100.100.8
listening on \Device\NPF_{939D763B-B042-494C-B1D5-0EFADFF4981E}: ip and (dst 147
.100.100.8) and not ether src 00:50:ba:b9:72:ba
^C
R:\honeypot\honeyd-0.5a>honeyd -f honeyd.conf 147.100.100.8-147.100.100.9
^C
R:\honeypot\honeyd-0.5a>honeyd -f honeyd.conf 147.100.100.8-147.100.100.9
^C
R:\honeypot\honeyd-0.5a>honeyd -f honeyd.conf 147.100.100.8-147.100.100.9

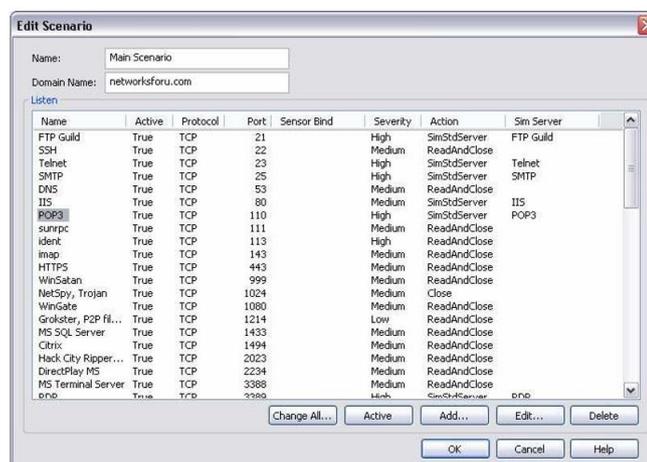
```

Fonte: Brien Posey.

- **KFSENSOR**

De acordo com CenPRA(2004) o Kfsensor, que pode-se ver na Figura 6, é considerado de baixa interação, onde emula os serviços de NetBIOS, SMB, FTP, POP3, HTTP, Telnet, SMTP e SOCKS.

Figura 7: Ferramenta Kfsensor

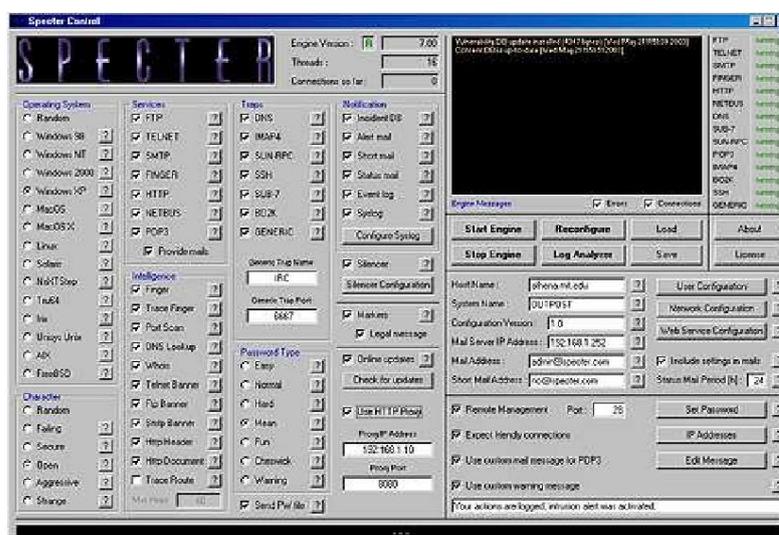


Fonte: GTS.

- **SPECTER**

De acordo com CenPRA (2004), Specter, onde ilustra-se sua tela de configuração na Figura 7, é considerado de baixa interação, onde pode simular até 14 sistemas operacionais diferentes, emula serviços como Http e Telnet, armazena diversas informações como IP, hora, e tipo de serviço atacado.

Figura 8: Ferramenta Specter



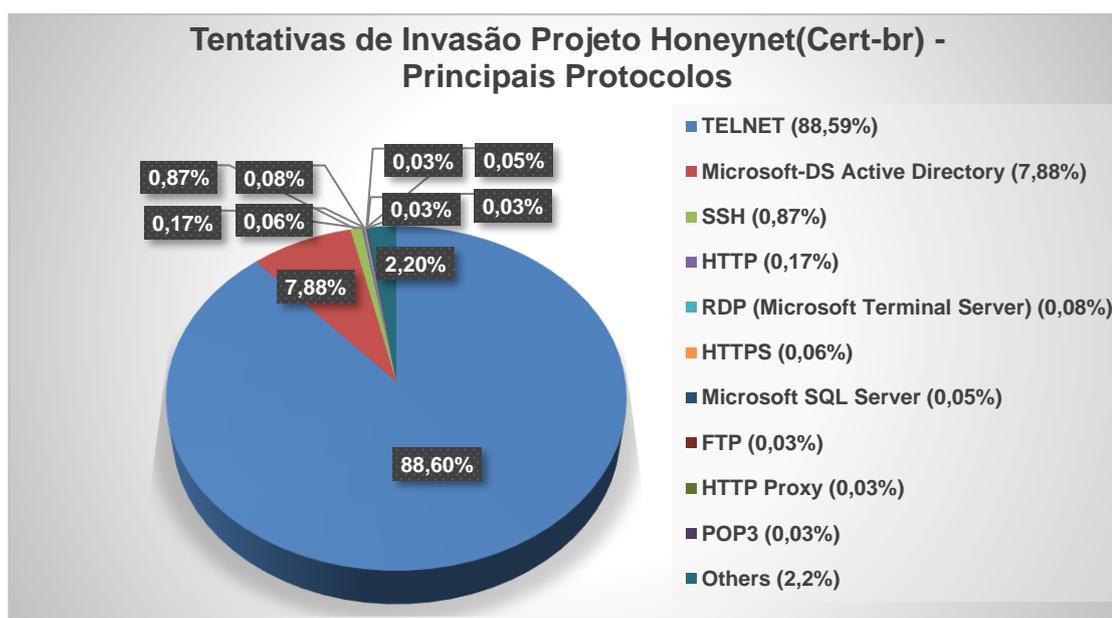
Fonte: GTS.

4 PRINCIPAIS PROTOCOLOS UTILIZADOS NOS HONEYPOTS

Os protocolos são um conjunto de definições que padronizam um tipo de conexão na rede, para que os equipamentos possam se comunicar na internet, por exemplo o envio de arquivos, e-mails, acesso remoto e diversos outros serviços são realizados através de protocolos.

Foram realizados testes com os protocolos: Telnet, FTP, POP3, TFTP, SSH e SMTP, pois frequentemente sofrem invasões. Com base nos dados do projeto *honeypot* do Cert-br do dia 07/10/2020, foi gerado o gráfico ilustrado na Figura 8 onde é possível ver os principais protocolos que sofreram invasão, onde o Telnet recebeu a maior parte das tentativas de invasões com 88% dos ataques, seguido do Microsoft Active Directory com 7,88% e o SSH com 0,87%.

Figura 9: Tentativas de Invasão Projeto Honeynet(Cert-br) - Principais Protocolos



Fonte: Elaborado com base nos dados do Projeto Honeypot(Cert-br).

4.1 TELNET

De acordo com o Portal PTComputador (Acesso em 2020) o protocolo Telnet surgiu em meados de 1969, com a chegada da RFC 15 que depois foi estendida para a RFC 855, e a necessidade da conexão a máquinas remotas, em 1973 tornou-se um protocolo oficial, a princípio era utilizado por universidades, governos, mas em 1990

com o crescimento da internet, foi largamente utilizado para acesso remoto a outros computadores.

O Telnet é considerado um dos protocolos mais estáveis, na época trouxe mudanças significativas para a tecnologia, pois antes para acessar um servidor, era necessário ir fisicamente onde estava localizado, mas o Telnet possibilitou o acesso remoto em tempo real e execução de comandos, padronizou a comunicação cliente servidor, trouxe grandes ganhos, porém com o desenvolvimento da tecnologia e Internet, o Telnet apresentou grandes vulnerabilidades de segurança, pois não possui criptografia, sendo um alvo fácil para invasores, assim surgiu o SSH um protocolo para acesso remoto, porém com criptografia, que substituiu na maioria dos casos o Telnet.

Embora o Telnet não seja tão utilizado quanto antigamente, ainda é aplicado para depuração e análise da interação entre computadores, jogos de multiusuários, alguns programas ainda utilizam o Telnet, e empresas usam o Telnet para hospedar aplicativos, redes, sistemas de BBS e redes STN.

4.2 FTP

Segundo o Portal Hostinger (2019) o protocolo *File Transfer Protocol* (FTP) foi criado em 1970 por Abhay Bhushan, com o objetivo de realizar transferências de arquivos entre computadores e servidores de forma segura, com o passar do tempo se tornou um dos principais protocolos de transferência de arquivos na internet.

O FTP está presente na camada de aplicação, onde realiza duas conexões paralelas, a de controle que é responsável por informações do usuário, diretório e do arquivo, e a conexão de dados que envia os arquivos.

O protocolo se inicia com a conexão de controle enviando informações através da porta 21 ao servidor, após a validação, a conexão de controle permanece aberta e ao cliente solicitar um arquivo o servidor abre a conexão de dados por meio da porta 20, caso seja solicitado outro arquivo é iniciada outra sessão TCP, todas as informações relacionadas à conexão são monitoradas.

Comandos FTP:

USER name - Indica usuário

PASS password - Indica Senha

LIST - Solicita a lista de arquivos do diretório

RETR filename - extrair arquivos do servidor

STOR filename - inserir arquivo no diretório do servidor

4.3 POP3

De acordo com o Portal CCM (2017) o *Post Office Protocol* (POP) ou protocolo de correios é utilizado para o acesso remoto ao servidor de correio eletrônico onde permite que o usuário baixe os e-mails por meio de um dispositivo, acesse a caixa por meio de outros aplicativos e outros equipamentos, acesso à leitura, deleção e envio de e-mails, e também o uso *offline* da caixa de correio.

O POP3 utiliza as portas TCP 110, onde se realiza a conexão TCP entre a aplicação e o servidor, onde é realizada a autenticação e todos os e-mails presentes são transferidos do servidor para a aplicação.

Comandos POP3:

USER login - Indicar usuário

PASS senha - Indicar Senha

STAT - Informações das mensagens no servidor

RETR - Quantidade de mensagens a serem extraídas

DELE - Quantidade de mensagens a serem deletadas

LIST [msg] - Quantidade de mensagens a serem exibidas

NOOP - Deixa a conexão aberta mesmo sem utilização

4.4 TFTP

Segundo Gavidia (1995) o *Trivial File Transfer Protocol* (TFTP) ou protocolo de transferência de arquivos é utilizado para realizar a transferência de pequenos arquivos na internet, não utiliza autenticação ou criptografia. O TFTP utiliza a porta 69 UDP, onde realiza a transferência de blocos com o tamanho fixo de 512 *bytes*, valida o recebimento do bloco anterior antes de enviar outro, e embora envie muitos pacotes, é utilizado o UDP, e torna-se mais rápido, simples e leve para a transferência de dados.

4.5 SSH

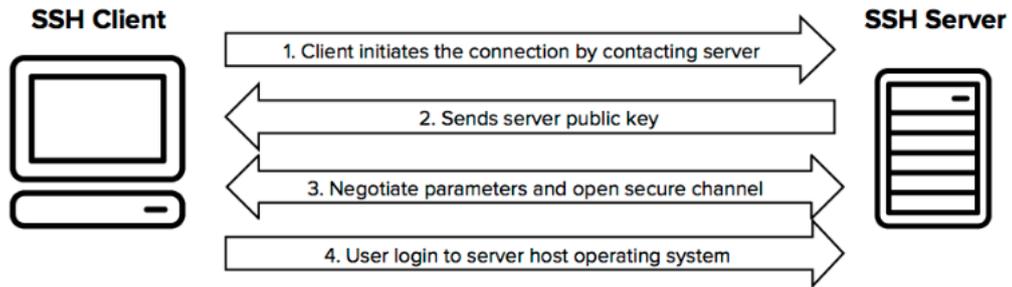
De acordo com o Portal HostMidia (Acessado em 2020) o protocolo *Secure Shell* (SSH), foi desenvolvido em 1995, por Tatu Ylonen, para substituir o protocolo Telnet, pois após um ataque a rede da universidade, onde um *sniffer* de senha, havia sido instalado em um servidor, o banco de dados da ferramenta continha diversos usuários e senhas, o que o fez Ylonen estudar e desenvolver uma solução de código aberto o OpenSSH, que permitia o acesso remoto criptografado.

O protocolo é utilizado para realizar o acesso remoto ao servidor, tornando possível que administradores de rede controlam e gerenciam a rede de forma remota, conta com criptografia entre o cliente e servidor, baseada na autenticação, criptografia e integridade, garante a segurança dos acessos, comandos, transferências de arquivos, e integridade das informações transferidas, a chave de acesso permite que os dados sejam acessados apenas por usuários autorizados tornando o serviço seguro. É possível também realizar o tunelamento, redirecionamento de portas TCP, conexões X11 e transferência de arquivos.

A criptografia do SSH é baseada na criptografia simétrica, assimétrica e *hashing*. A criptografia simétrica utiliza um código secreto para codificar a mensagem criptográfica trocada entre o usuário e servidor, nesse ponto tudo é criptografado (mensagens, arquivos etc.), para cada sessão SSH é necessário um *token*. A Criptografia Assimétrica possui uma chave pública e outra privada, o par forma a chave pública-privada, onde é aplicada para codificar e decodificar a mensagem e o *hashing* é empregado para autenticar a mensagem e verificar sua validade.

O SSH é acessado através do *Shell* onde a porta padrão para se conectar é a 22, e o comando para iniciar o acesso é o SSH que indica a abertura de comunicação, depois é indicado o usuário e o IP do servidor que se pretende acessar, o modelo do comando é *SSH (Usuário)@(IP do servidor)*, após dar enter, será necessário realizar a autenticação. A Figura 9 ilustra seu funcionamento.

Figura 10: Protocolo SSH



Fonte: SSH (Secure Shell).

4.6 SMTP

Segundo o Portal SpeedCheck (Acessado em 2020), o SMTP (*Simple Mail Transfer Protocol*) é um protocolo TCP/IP, formado por um conjunto de regras e diretrizes que deve ser seguido pelo sistema operacional, é usado para envio e recebimentos de e-mails. mas ele é um pouco limitado e carente de recursos, como por exemplo a capacidade de realizar o enfileiramento de mensagens na extremidade receptora, recursos já existentes nos protocolos IMAP (*Internet Message Access Protocol*) e POP3 (*Post Office Protocol 3*).

5 TESTES REALIZADOS EM AMBIENTE REAL

Os testes da Ferramenta Valhala e Cowrie, foram executados em ambiente real, onde as ferramentas permaneceram ativas na rede em serviços hospedados em Cloud, configuradas para receberem ataques, e realizados alguns testes de invasões onde iniciamos os ataques. A seguir, serão apresentados os testes e resultados.

5.1 INFORMAÇÕES GERAIS – TESTES VALHALA

Para realizar os testes de monitoramento de intrusos à rede com um *honeypot* de pesquisa, foi utilizada a ferramenta Valhala e Cowrie, que simula serviços e capta informações para posterior análise. A ferramenta foi escolhida para os testes de invasão, pois não traz riscos a rede, possui simples instalação, configuração, não exige máquinas robustas, é gratuita, e é considerada de baixo nível de interação.

5.1.1 AMBIENTE

Para realizar os testes de invasão utilizando a ferramenta de *honeypot*, foi contratado um servidor VPS no BHSERVERS, onde foi instalado o Windows Server 2012, a ferramenta Valhala e configurados os serviços, manteve-se a ferramenta ativa do dia 10/10/2020 ao dia 24/10/2020 para monitorar invasões externas, após os testes.

Especificações técnicas dos equipamentos utilizados:

Máquina utilizada para ser atacada (*honeypot*):

Hospedada no BHSERVERS

Sistema Operacional: Windows Server 2012

RAM: 5 GB

5vCPU

HD: 40 GB

Localização: Canadá

Máquina utilizada realizar alguns testes de invasão ao *honeypot*:

Sistema Operacional: Windows 10

RAM: 16 gb

HD: 512 gb

5.1.2 FERRAMENTAS

Para realizar os testes com a ferramenta Valhala, foi necessário utilizar a ferramenta Putty para acesso do protocolo Telnet, e o aplicativo Em Client para realizar os testes com o protocolo POP3.

5.1.2.1 VALHALA

O Valhala foi desenvolvido pelo Brasileiro Marcos Flávio Assunção, onde o principal intuito é oferecer uma ferramenta gratuita, com simples configuração e de fácil instalação, para a detecção de intrusos, assim foi criada para sistema Windows, porém através de *softwares* de emulação é possível utilizar em sistemas Linux, o código é aberto para possíveis alterações de melhoria.

A ferramenta oferece serviços como: HTTP, FTP, SMTP, POP3, TELNET, TFTP, FINGER e PROXY.

5.1.2.2 PUTTY

Segundo o Tectudo (2013) a ferramenta PUTTY, possui código aberto que emula terminais, e pode ser utilizado em outras plataformas, a aplicação permite o SSH para suporte remoto, via Shell, e também os serviços Telnet, conexão direta, rlogin e porta serial, não é necessário instalar, apenas abrir o arquivo executável. É normalmente usado por administradores de rede, pois tem uma interface simples de ser configurada e várias opções de configuração.

Nos testes com o Valhala, foi utilizada a ferramenta *putty* para realizar a conexão remota através do protocolo Telnet.

5.1.2.3 EM CLIENT

O Em Client segundo o Techtudo (2013) é uma ferramenta bem intuitiva e simples de configurar, possui serviço de gerenciamento de e-mail para o Windows, e suporta os principais serviços de correio eletrônico, utilizados nos testes para o protocolo POP3.

5.1.4 CONFIGURANDO SERVIÇOS

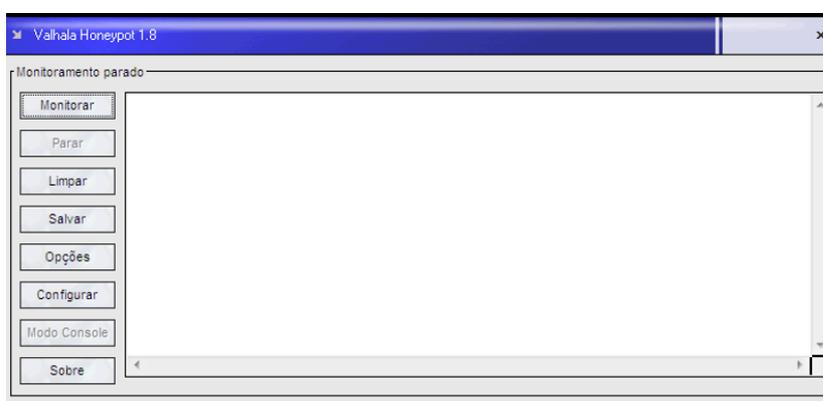
Foi necessário instalar a ferramenta Valhala no sistema operacional de testes, assim como seus serviços, que estão descritos nos tópicos a seguir.

5.1.4.1 INSTALAÇÃO VALHALA

O Valhala foi instalado em um servidor VPS hospedado no BHSERVERS com o sistema operacional Windows Server 2012, onde o download do *honeypot* foi realizado no link <http://valhalahoneypot.sourceforge.net>, e não foi necessário instalar, apenas abrir o arquivo executável.

Ao abrir o Valhala essa é a tela inicial, que pode ser vista na Figura 10, onde o menu possui as opções: monitorar, parar o serviço, limpar a tela de logs, salvar os logs, em opções é possível configurar alertas para receber por e-mail e configurar os serviços

Figura 11: Tela inicial Valhala



Fonte: Próprio autor.

5.1.4.2 TELNET

O protocolo Telnet foi configurado com as informações que aparecem na Figura 11. Porta 23, *login* e senha, nome dos diretórios que aparecerão quando o sistema for invadido, e data e hora da criação dos diretórios, são informações básicas para a configuração.

Figura 12: Configuração Telnet

Fonte: Próprio autor.

5.1.4.3 FTP

O protocolo FTP, ilustrado na Figura 12, foi configurado na porta 21, com o *login* e senha e o diretório que poderá ser acessado na invasão.

Figura 13: Configuração FTP

Fonte: Próprio autor.

5.1.4.4 POP3

O protocolo POP3, podemos ver a sua tela de configuração na Figura 13 foi configurado, na porta 110 com *login* e senha.

Figura 14: Configuração POP3



The screenshot shows a window titled "Servidor POP3". It contains a checked checkbox labeled "Habilitar servidor POP3". Below this, there are four input fields: "Porta:" with the value "110", "Banner:" with the value "Microsoft POP3 Server", "Login:" with the value "root", and "Senha:" with the value "xxxx".

Fonte: Próprio autor.

5.1.4.5 TFTP

O protocolo TFTP foi habilitado na porta 69 como pode-se ver na Figura 14.

Figura 15: Configuração TFTP



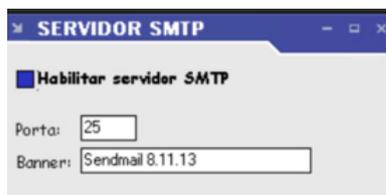
The screenshot shows a window titled "SERVIDOR TFTP". It contains a checked checkbox labeled "Habilitar Servidor TFTP". Below this, there are two input fields: "Porta:" with the value "69" and a checkbox labeled "Modo funcional (cuidado)" which is currently unchecked.

Fonte: Próprio autor.

5.1.4.6 SMTP

O protocolo SMTP foi habilitado na porta 25, como ilustra a Figura 15.

Figura 16: Configuração SMTP



The screenshot shows a window titled "SERVIDOR SMTP". It contains a checked checkbox labeled "Habilitar servidor SMTP". Below this, there are two input fields: "Porta:" with the value "25" and "Banner:" with the value "Sendmail 8.11.13".

Fonte: Próprio autor.

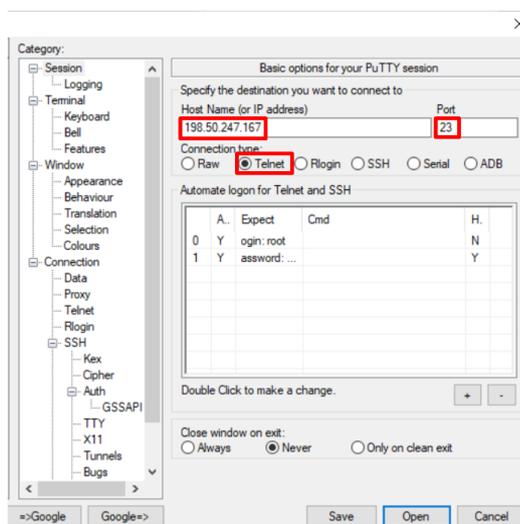
5.1.5 TESTES REALIZADOS

Todos os testes foram executados em um ambiente real através dos serviços de Telnet, FTP, POP3, FTFP e SMTP que serão apresentados a seguir.

5.1.5.1 TELNET

Foram também realizados testes com outra máquina tentando acessar o *honeypot* através do serviço Telnet. Na Figura 16 podemos ver que as configurações usadas foram: porta 23, utilizando o programa putty, para realizar a conexão acessando o IP 198.50.247.167.

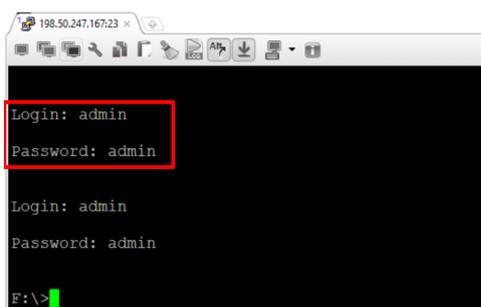
Figura 17: Ferramenta Putty



Fonte: Próprio autor.

O serviço Telnet foi acessado usando as credenciais admin/admin, na Figura 17 pode-se ver o sucesso ao acessar.

Figura 18: Acessando serviço Telnet



Fonte: Próprio autor.

E após acessar, ilustra-se na Figura 18 que foi possível ver as supostas pastas importantes, definidas no *honeypot*.

Figura 19: Verificando diretórios

```
F:\>dir
O volume da unidade F e SISTEMA
O numero de serie do volume e F078-2A14

Diretório Honeypot
Pasta de F:\
22/03/2001  14:53  <DIR>      .
22/03/2001  14:53  <DIR>      ..
22/03/2001  14:53  <DIR>      arquivos
22/03/2001  14:53  <DIR>      backup
22/03/2001  14:53  <DIR>      clientes
22/03/2001  14:53  <DIR>      documentos
22/03/2001  14:53  <DIR>      funcionarios
22/03/2001  14:53  <DIR>      windows
                0 arquivo(s)          0 bytes
                6 pasta(s) 49.962.553.344 bytes disponiveis
```

Fonte: Próprio autor.

No *honeypot* pode-se ver o LOG das invasões, como a hora, IP, protocolo utilizado, usuário e senha usados para a invasão, comando DIR. Enquanto realizou-se os testes, houve outras tentativas de invasões por atacantes desconhecidos, pode-se ver na Figura 19 os 2 IPs tentando acessar o serviço.

Figura 20: Valhala - Log Telnet

VALHALA HONEYPOT 1.9

Monitorando o sistema desde às 10:27:43 no ip 198.50.247.167

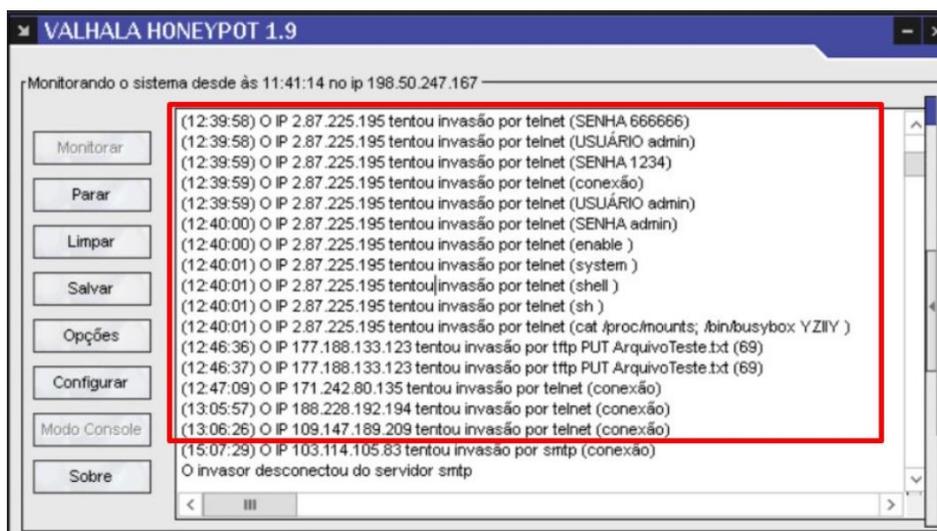
Outros IPs tentando invadir o serviço

```
(10:31:43) O IP 177.188.133.123 tentou invasão por telnet (USUÁRIO admin)
(10:31:45) O IP 177.188.133.123 tentou invasão por telnet (SENHA admin)
(10:31:47) O IP 177.188.133.123 tentou invasão por telnet ( )
(10:31:47) O IP 177.188.133.123 tentou invasão por telnet ( )
(10:32:05) O IP 34.53.80.170 tentou invasão por telnet (conexão)
(10:32:54) O IP 71.246.46.135 tentou invasão por telnet (conexão)
(10:33:15) O IP 177.188.133.123 tentou invasão por telnet (conexão)
(10:33:19) O IP 177.188.133.123 tentou invasão por telnet (USUÁRIO yúyú yú lÿyÿy yú lÿyÿ ladmin)
(10:33:20) O IP 177.188.133.123 tentou invasão por telnet (SENHA admin)
(10:33:26) O IP 177.188.133.123 tentou invasão por telnet (USUÁRIO admin)
(10:33:30) O IP 177.188.133.123 tentou invasão por telnet (SENHA admin)
(10:35:16) O IP 177.188.133.123 tentou invasão por telnet (conexão)
(10:35:21) O IP 177.188.133.123 tentou invasão por telnet (USUÁRIO yúyú yú lÿyÿy yú lÿyÿ ladmin)
(10:35:25) O IP 177.188.133.123 tentou invasão por telnet (SENHA admin)
(10:35:27) O IP 177.188.133.123 tentou invasão por telnet (USUÁRIO admin)
(10:35:29) O IP 177.188.133.123 tentou invasão por telnet (SENHA admin)
(10:36:05) O IP 177.188.133.123 tentou invasão por telnet (dir )
```

Fonte: Próprio autor.

Após as simulações, o *honeypot* ficou ativo na rede para receber ataques reais, na Figura 20, foram identificados 4 IPs diferentes tentando invadir via protocolo telnet, e serão apresentadas outras invasões que ficaram armazenadas no arquivo de log da ferramenta.

Figura 21: Log de uma tentativa real via telnet



Fonte: Próprio autor.

Serão apresentados apenas alguns trechos do log, pois foram geradas 131 linhas, para 27 tentativas de conexões por 8 IPs diferentes, na Figura 21 pôde-se identificar os 8 IPs diferentes tentando acessar o serviço de Telnet.

Figura 22: Log - 8 IPs diferentes

```

(11:50:59) O IP 193.111.198.162 tentou invasão por telnet (conexão)
(11:51:42) O IP 103.71.20.10 tentou invasão por telnet (conexão)
(12:23:48) O IP 45.5.146.149 tentou invasão por telnet (conexão)
(12:25:55) O IP 1.52.200.141 tentou invasão por telnet (conexão)
(12:39:13) O IP 2.87.225.195 tentou invasão por telnet (conexão)
(12:47:09) O IP 171.242.80.135 tentou invasão por telnet (conexão)
(13:05:57) O IP 188.228.192.194 tentou invasão por telnet (conexão)
(13:06:26) O IP 109.147.189.209 tentou invasão por telnet (conexão)
  
```

Fonte: Próprio autor.

Através do site *GreyNoise* ilustrado na Figura 22, foi identificado que o IP 109.147.189.209 localizado no Estados Unidos já é conhecido na internet pelas suas tentativas de invasão via Telnet.

Figura 23: Site IP GreyNoise 109.147.189.209



Fonte: Próprio autor.

Na Figura 23, o IP 2.87.225.195 chamou a atenção, pois realizou 18 conexões, onde digitava 3 combinações de usuário e senha e ao errar, realizava uma nova conexão e tentava mais 3 usuários e senhas, no total realizou 52 combinações diferentes.

Figura 24: Log - Invasão Telnet

```
(12:39:13) O IP 2.87.225.195 tentou invasão por telnet (conexão)
(12:39:14) O IP 2.87.225.195 tentou invasão por telnet (USUÁRIO root)
(12:39:14) O IP 2.87.225.195 tentou invasão por telnet (SENHA default)
(12:39:14) O IP 2.87.225.195 tentou invasão por telnet (USUÁRIO admin)
(12:39:15) O IP 2.87.225.195 tentou invasão por telnet (SENHA smcadmin)
(12:39:15) O IP 2.87.225.195 tentou invasão por telnet (USUÁRIO Administrator)
(12:39:16) O IP 2.87.225.195 tentou invasão por telnet (SENHA admin)
(12:39:16) O IP 2.87.225.195 tentou invasão por telnet (conexão)
(12:39:16) O IP 2.87.225.195 tentou invasão por telnet (USUÁRIO root)
(12:39:17) O IP 2.87.225.195 tentou invasão por telnet (SENHA GM8182)
(12:39:17) O IP 2.87.225.195 tentou invasão por telnet (USUÁRIO admin)
(12:39:18) O IP 2.87.225.195 tentou invasão por telnet (SENHA )
(12:39:18) O IP 2.87.225.195 tentou invasão por telnet (USUÁRIO admin)
(12:39:18) O IP 2.87.225.195 tentou invasão por telnet (SENHA 12345)
(12:39:19) O IP 2.87.225.195 tentou invasão por telnet (conexão)
```

Fonte: Próprio autor.

O atacante utilizou os principais usuários: admin e root, que pode ser vista na Tabela 1, e quase conseguiu chegar na nossa combinação que era usuário: admin e senha: admin. Foi possível verificar pelo curto espaço de tempo de 1 segundo entre as tentativas de acessos, que provavelmente o atacante, estava usando alguma ferramenta de auxílio para as tentativas de invasões.

Tabela 01: Combinações de usuário e senha utilizados pelo IP 2.87.225.195

IP 2.87.225.195			
Usuário	Senha	Usuário	Senha
666666	666666	root	oelinux123
888888	888888	root	oelinux1234
admin	123456	root	xc3511
admin	smcadmin	root	hi3518
admin		root	anko
admin	1234567890	root	realtek
admin	5up	root	cat1029
admin	admin1234	root	aquario
admin	ipcam_rt5350	root	0
admin	meinsm	root	root
admin	win1dow\$	root	founder88
admin	54321	root	aquario
admin	7ujmko0admin	root	user
admin	password	root	5up
admin	vertex25ektk12	root	jvzbd
admin	1111	root	ikwb
admin	1234	root	7ujmko0admin
admin	admin	root	hunt5759
admin	admin	root	dreambox
admin1	password	root	system
administrator	1234	root	666666
Administrator	admin	root	klv1234
default	antslq	root	default
guest	friend	support	support
root	pass	tech	tech
root	GM8182	ubnt	ubnt

Fonte: Próprio autor.

Além de o IP 2.87.225.195 tentar diversas combinações de usuário e senha, também utilizou os comandos: enable, system, shell sh e cat /proc/mounts; /bin/busybox YZIIY que podem ser vistos na **Figura 25**:

Figura 25: Log - Invasão Telnet

```
(12:40:00) O IP 2.87.225.195 tentou invasão por telnet (enable )
(12:40:01) O IP 2.87.225.195 tentou invasão por telnet (system )
(12:40:01) O IP 2.87.225.195 tentou invasão por telnet (shell )
(12:40:01) O IP 2.87.225.195 tentou invasão por telnet (sh )
(12:40:01) O IP 2.87.225.195 tentou invasão por telnet (cat /proc/mounts; /bin/busybox YZIIY )
```

Fonte: Próprio autor.

5.1.5.2 FTP

O teste foi realizado com outra máquina tentando acessar o *honeypot* através do serviço FTP, na porta 21, utilizando o Comando *ftp 198.50.247.167*, onde foi solicitando usuário e senha, e como padrão foi utilizado a senha e usuário Root.

Na Figura 25, o invasor obteve sucesso ao usar as credenciais root/root para acessar a máquina, e conseguiu verificar os arquivos através do comando DIR, como é um servidor falso, o diretório mostrado é o c:/temp da máquina 'cobaia'.

Figura 26: Invasão serviço FTP

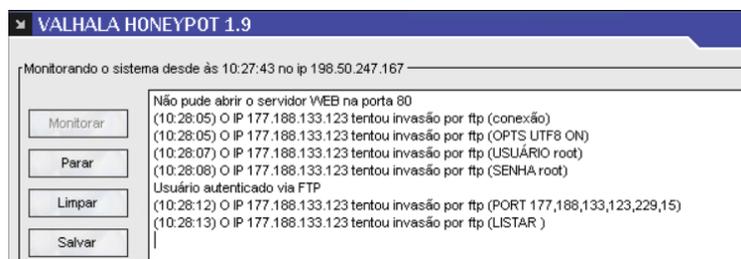
```
C:\Users\Matheus Okazaki>ftp 198.50.247.167 ← Comando 1
Conectado a 198.50.247.167.
220 War-ftpd 2.3.4
500 'OPTS': command not understood.
Usuário (198.50.247.167:(none)): root ← Usuário
331 Password required for root.
Senha: ← Senha
230 User root logged in. ← Foi possível acessar
ftp> dir ← Comando 2
200 Port command successful.
150 Opening data connection for directory list.
drw-rw-rw- 1 ftp ftp 0 Oct 10 10:01 .
drw-rw-rw- 1 ftp ftp 0 Oct 10 10:01 ..
-rw-rw-rw- 1 ftp ftp 83712 Oct 08 17:18 chrome_installer.log
drw-rw-rw- 1 ftp ftp 0 Sep 25 01:08 comtypes_cache
drw-rw-rw- 1 ftp ftp 0 Aug 10 19:09 Crashpad
-rw-rw-rw- 1 ftp ftp 608 Aug 11 19:00 fwtsqmfile00.sqm
-rw-rw-rw- 1 ftp ftp 0 Mar 21 2014 FXSAPIDebugLogFile.txt
-rw-rw-rw- 1 ftp ftp 0 Mar 21 2014 FXSTIFFDebugLogFile.txt
226 File sent ok
ftp: 557 bytes recebidos em 0.01Segundos 37.13Kbytes/s.
ftp>
```

Diretórios Simulados pelo Honeypot

Fonte: Próprio autor.

No Figura 26, pode-se ver o LOG das invasões como a hora, IP, protocolo utilizado, portas, usuário e senha usados para a invasão.

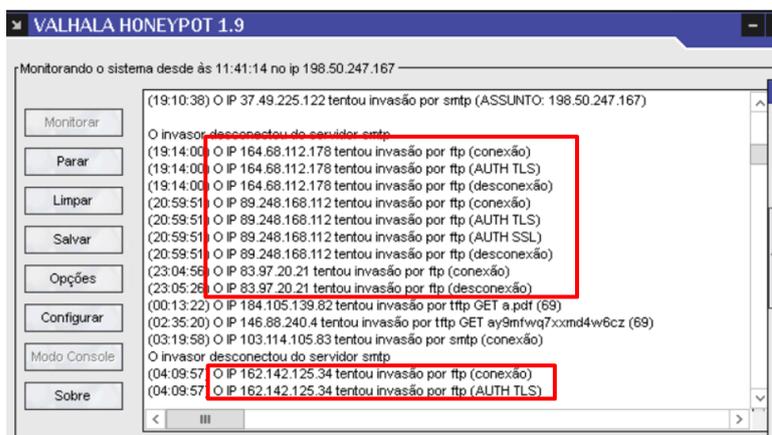
Figura 27: Valhala - Log FTP



Fonte: Próprio autor.

Após as simulações, o *honeypot* ficou ativo e configurado para receber ataques reais, na Figura 27 é possível ver que 4 IPs diferentes tentaram invadir, via protocolo FTP, porém diversas outras tentativas foram captadas e serão apresentadas a seguir, pelo log da ferramenta.

Figura 28: Invasões externas



Fonte: Próprio autor.

Conforme logs exibidos na **Figura 29**, é possível identificar as principais invasões ao serviço FTP, pois foram geradas 476 linhas de logs para 183 tentativas de invasões por 85 IPs diferentes.

Foram identificadas as tentativas de conexão padrões das invasões, pelos seguintes IPs: 104.206.128.30, 83.97.20.21, 167.248.133.52, 162.243.128.12, 192.241.234.251 e 176.230.98.55.

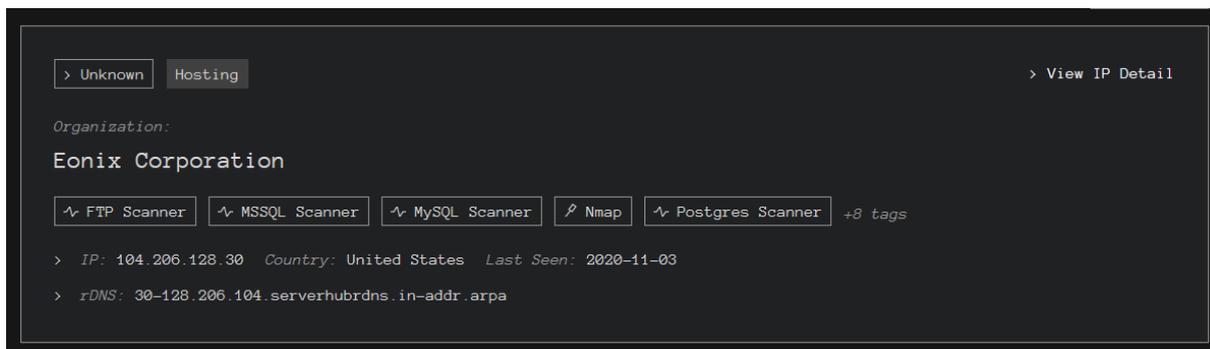
Figura 29: Log - Invasões FTP

```
(15:29:34) O IP 104.206.128.30 tentou invasão por ftp (conexão)
(15:29:34) O IP 104.206.128.30 tentou invasão por ftp (AUTH TLS)
(15:29:34) O IP 104.206.128.30 tentou invasão por ftp (desconexão)
(17:25:57) O IP 83.97.20.21 tentou invasão por ftp (conexão)
(17:26:27) O IP 83.97.20.21 tentou invasão por ftp (desconexão)
(17:31:42) O IP 167.248.133.52 tentou invasão por ftp (conexão)
(17:31:42) O IP 167.248.133.52 tentou invasão por ftp (AUTH TLS)
(17:31:42) O IP 167.248.133.52 tentou invasão por ftp (AUTH SSL)
(17:31:42) O IP 167.248.133.52 tentou invasão por ftp (desconexão)
(17:41:28) O IP 162.243.128.12 tentou invasão por ftp (conexão)
(17:41:28) O IP 162.243.128.12 tentou invasão por ftp (desconexão)
(18:05:00) O IP 192.241.234.251 tentou invasão por ftp (conexão)
(18:05:01) O IP 192.241.234.251 tentou invasão por ftp (AUTH TLS)
(18:05:01) O IP 192.241.234.251 tentou invasão por ftp (AUTH SSL)
(18:05:02) O IP 192.241.234.251 tentou invasão por ftp (desconexão)
(18:57:23) O IP 176.230.98.55 tentou invasão por ftp (conexão)
(18:57:23) O IP 176.230.98.55 tentou invasão por ftp (AUTH TLS)
(18:57:24) O IP 176.230.98.55 tentou invasão por ftp (desconexão)
```

Fonte: Próprio autor.

Através do site *GreyNoise* que pode ser ilustrado na Figura 29, é possível ver que o IP 104.206.128.30 localizado no Estados Unidos, já é bem conhecido pelas suas tentativas de invasão via protocolo FTP.

Figura 30: Site GreyNoise IP104.206.128.30



Fonte: Próprio autor.

Nos logs da Figura 30, pôde-se identificar 7 tentativas de invasões com usuário e senha, porém todas falharam, realizadas pelos IPs: 112.12.30.31, 80.82.77.139, 185.9.19.90, 43.250.243.125, 35.187.170.152, 89.248.172.16.

Figura 31: Log - Invasão FTP

```
(22:16:36) O IP 112.12.30.31 tentou invasão por ftp (conexão)
(22:16:36) O IP 112.12.30.31 tentou invasão por ftp (USUÁRIO anonymous)
(22:16:36) O IP 112.12.30.31 tentou invasão por ftp (SENHA admin123)
Falha de autenticação via FTP
(16:47:04) O IP 80.82.77.139 tentou invasão por ftp (conexão)
(16:47:04) O IP 80.82.77.139 tentou invasão por ftp (USUÁRIO anonymous)
(16:47:04) O IP 80.82.77.139 tentou invasão por ftp (SENHA anonymous@)
Falha de autenticação via FTP
(02:05:22) O IP 185.9.19.90 tentou invasão por ftp (USUÁRIO anonymous)
(02:05:22) O IP 185.9.19.90 tentou invasão por ftp (SENHA Jgpuser@home.com)
Falha de autenticação via FTP
(02:44:48) O IP 185.9.19.90 tentou invasão por ftp (conexão)
(02:44:48) O IP 185.9.19.90 tentou invasão por ftp (USUÁRIO anonymous)
(02:44:49) O IP 185.9.19.90 tentou invasão por ftp (SENHA Jgpuser@home.com)
Falha de autenticação via FTP
(00:46:55) O IP 43.250.243.125 tentou invasão por ftp (USUÁRIO admin)
(00:46:56) O IP 43.250.243.125 tentou invasão por ftp (SENHA backdoor)
Falha de autenticação via FTP
(07:16:59) O IP 35.187.170.152 tentou invasão por ftp (conexão)
(07:16:59) O IP 35.187.170.152 tentou invasão por ftp (USUÁRIO anonymous)
(07:16:59) O IP 35.187.170.152 tentou invasão por ftp (SENHA anonymous@)
Falha de autenticação via FTP
(07:38:39) O IP 89.248.172.16 tentou invasão por ftp (USUÁRIO anonymous)
(07:38:39) O IP 89.248.172.16 tentou invasão por ftp (SENHA anonymous@)
```

Fonte: Próprio autor.

Nos logs da Figura 31, foram identificadas 2 tentativas de acesso via autorização TLS ou SSL, e comandos digitados, pelos IPs 74.120.14.36 e 80.82.77.139.

Figura 32: Log - Invasão FTP

```
(09:10:15) O IP 74.120.14.36 tentou invasão por ftp (conexão)
(09:10:15) O IP 74.120.14.36 tentou invasão por ftp (AUTH TLS)
(09:10:15) O IP 74.120.14.36 tentou invasão por ftp (AUTH SSL)
(09:10:15) O IP 74.120.14.36 tentou invasão por ftp (desconexão)
(16:47:04) O IP 80.82.77.139 tentou invasão por ftp (HELP )
(16:47:04) O IP 80.82.77.139 tentou invasão por ftp (FEAT )
(16:47:04) O IP 80.82.77.139 tentou invasão por ftp (AUTH TLS)
(16:47:07) O IP 80.82.77.139 tentou invasão por ftp (desconexão)
```

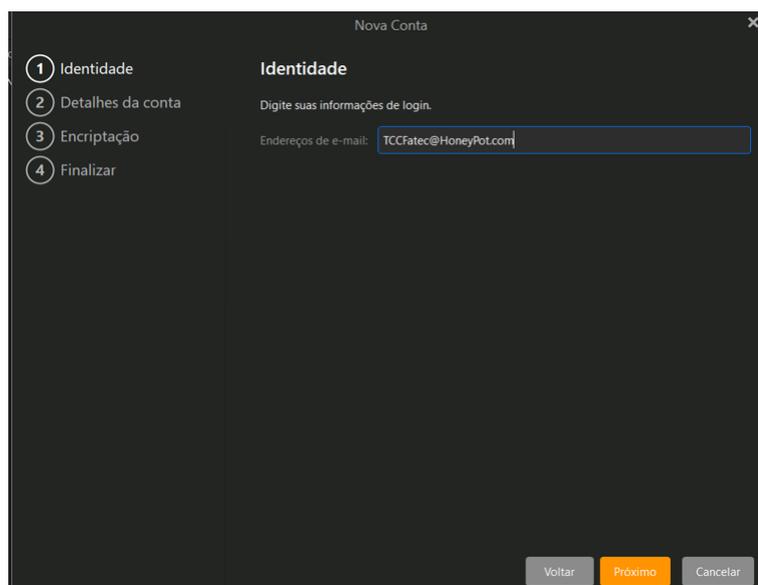
Fonte: Próprio autor.

Outro ponto que chamou a atenção foram as diversas tentativas de invasões pelo IP 139.162.202.108, conforme logs exibidas na Figura 32, em poucos segundos.

5.1.5.3 POP3

Neste teste foi feita a configuração de um e-mail falso que pode ser visto na Figura 34, utilizado um e-mail falso: TCCFatec@HoneyPot.com, para realizar os testes com o serviço POP3, foi utilizado a aplicação EM Client como *client* de e-mail. As configurações de e-mail falsas podem ser vistas na Figura 34 e Figura 35.

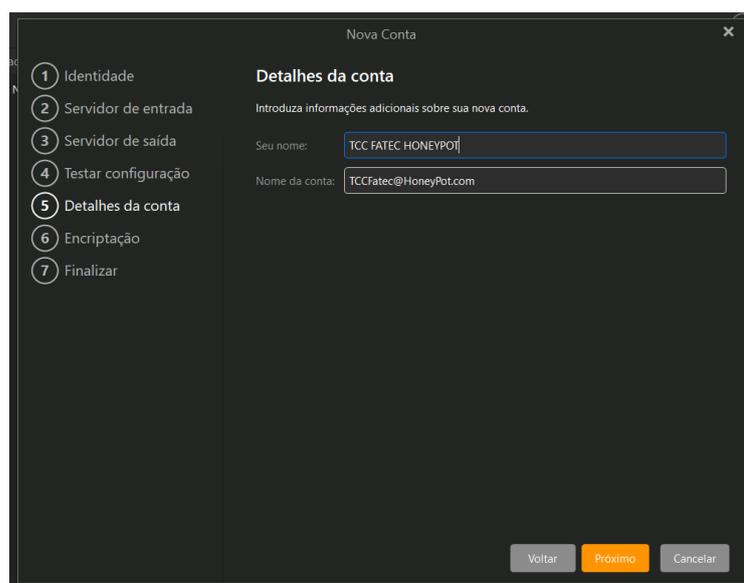
Figura 35: EM Client - Configurando E-mail falso



The screenshot shows the 'Nova Conta' (New Account) window in the EM Client application. The window is titled 'Nova Conta' and has a close button (X) in the top right corner. On the left side, there is a vertical list of steps: 1 Identidade (selected), 2 Detalhes da conta, 3 Encriptação, and 4 Finalizar. The main area is titled 'Identidade' and contains the instruction 'Digite suas informações de login.' Below this, there is a label 'Endereços de e-mail:' followed by a text input field containing 'TCCFatec@HoneyPot.com'. At the bottom right, there are three buttons: 'Voltar' (disabled), 'Próximo' (active), and 'Cancelar' (disabled).

Fonte: Próprio autor.

Figura 36: EM Client - Configurando E-mail falso

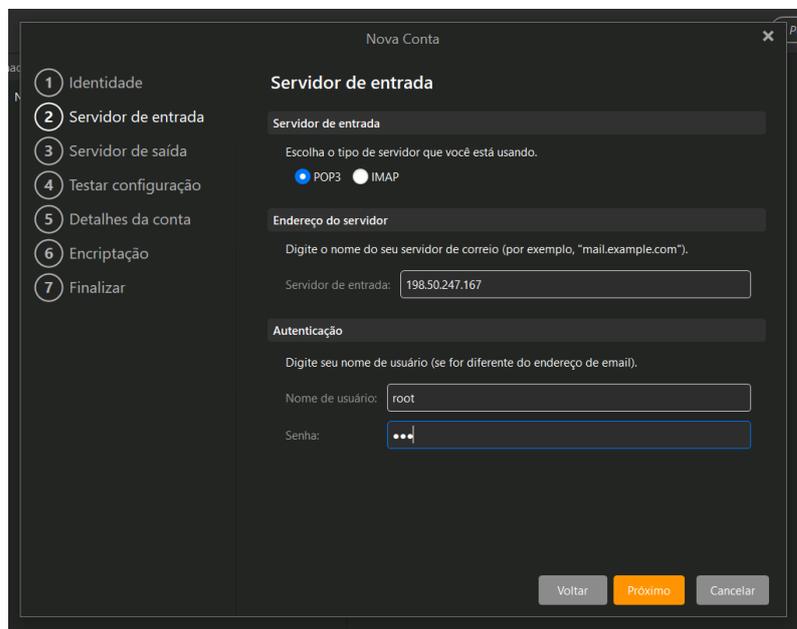


The screenshot shows the 'Nova Conta' (New Account) window in the EM Client application. The window is titled 'Nova Conta' and has a close button (X) in the top right corner. On the left side, there is a vertical list of steps: 1 Identidade, 2 Servidor de entrada, 3 Servidor de saída, 4 Testar configuração, 5 Detalhes da conta (selected), 6 Encriptação, and 7 Finalizar. The main area is titled 'Detalhes da conta' and contains the instruction 'Introduza informações adicionais sobre sua nova conta.' Below this, there are two text input fields: 'Seu nome:' containing 'TCC FATEC HONEYPOT' and 'Nome da conta:' containing 'TCCFatec@HoneyPot.com'. At the bottom right, there are three buttons: 'Voltar' (disabled), 'Próximo' (active), and 'Cancelar' (disabled).

Fonte: Próprio autor.

Foi necessário configurar o servidor de entrada, para acessar o IP do servidor *honeypot* e as credenciais falsas que criamos. Usuário: Root e senha: 123. Que podem ser vistas na Figura 36.

Figura 37: EM Client - Configurando Servidor de Entrada



The screenshot shows the 'Nova Conta' (New Account) window in the EM Client. The window is divided into a sidebar with seven numbered steps and a main configuration area. The second step, 'Servidor de entrada' (Incoming Server), is active. The main area contains the following fields and options:

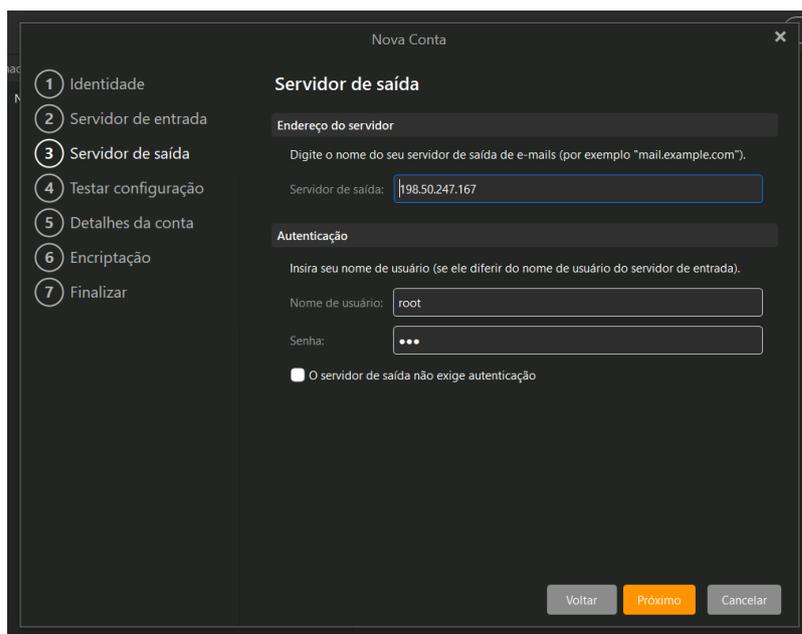
- Servidor de entrada:** A text field with the value '198.50.247.167'.
- Escolha o tipo de servidor que você está usando:** Two radio buttons, 'POP3' (selected) and 'IMAP'.
- Endereço do servidor:** A text field with the value '198.50.247.167'.
- Autenticação:** A section with a label 'Digite seu nome de usuário (se for diferente do endereço de email)'. It contains a 'Nome de usuário:' field with 'root' and a 'Senha:' field with three dots.

At the bottom right, there are three buttons: 'Voltar' (grey), 'Próximo' (orange), and 'Cancelar' (grey).

Fonte: Próprio autor.

Como pode-se ver na Figura 37, foi configurado o servidor de saída.

Figura 38: EM Client - Configurando Servidor de Saída



The screenshot shows the 'Nova Conta' (New Account) window in the EM Client. The window is divided into a sidebar with seven numbered steps and a main configuration area. The third step, 'Servidor de saída' (Outgoing Server), is active. The main area contains the following fields and options:

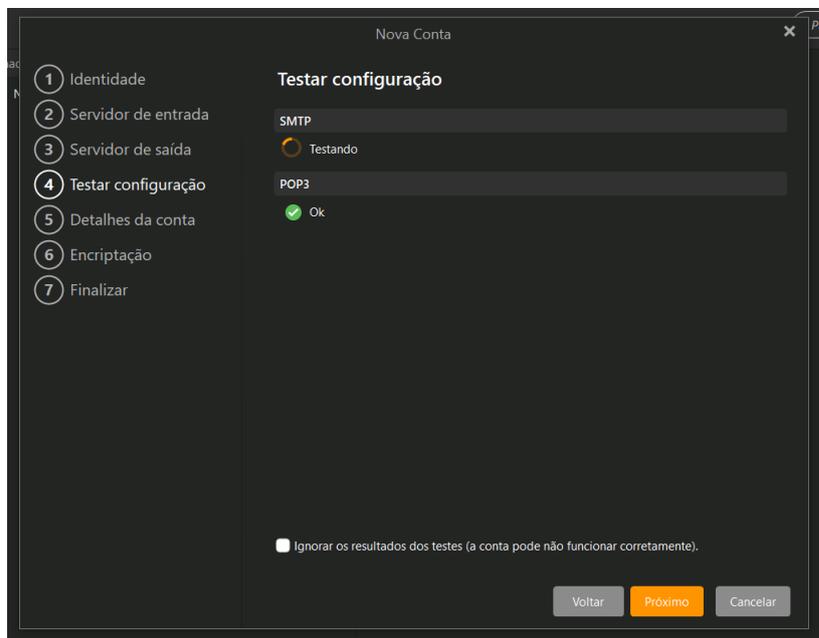
- Endereço do servidor:** A text field with the value '198.50.247.167'.
- Autenticação:** A section with a label 'Insira seu nome de usuário (se ele diferir do nome de usuário do servidor de entrada)'. It contains a 'Nome de usuário:' field with 'root' and a 'Senha:' field with three dots.
- O servidor de saída não exige autenticação:** A checkbox that is currently unchecked.

At the bottom right, there are three buttons: 'Voltar' (grey), 'Próximo' (orange), and 'Cancelar' (grey).

Fonte: Próprio autor.

Após configurar o serviço de POP3 foram realizados testes que podem ser vistos na Figura 38, para validar se serviço estava funcionando.

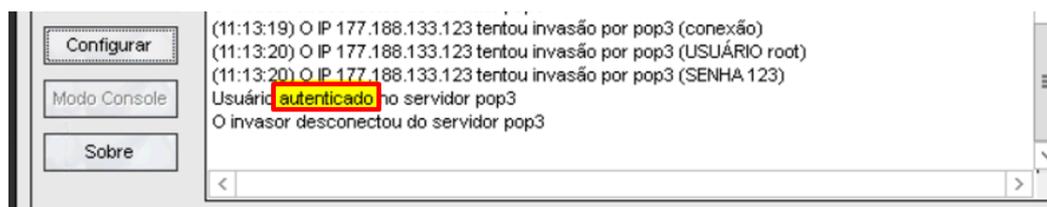
Figura 39: EM Client – Testando POP3



Fonte: Próprio autor.

Na Figura 39, pode-se ver o log das invasões, como a hora, IP, protocolo utilizado, portas, usuário e senha usados para a invasão.

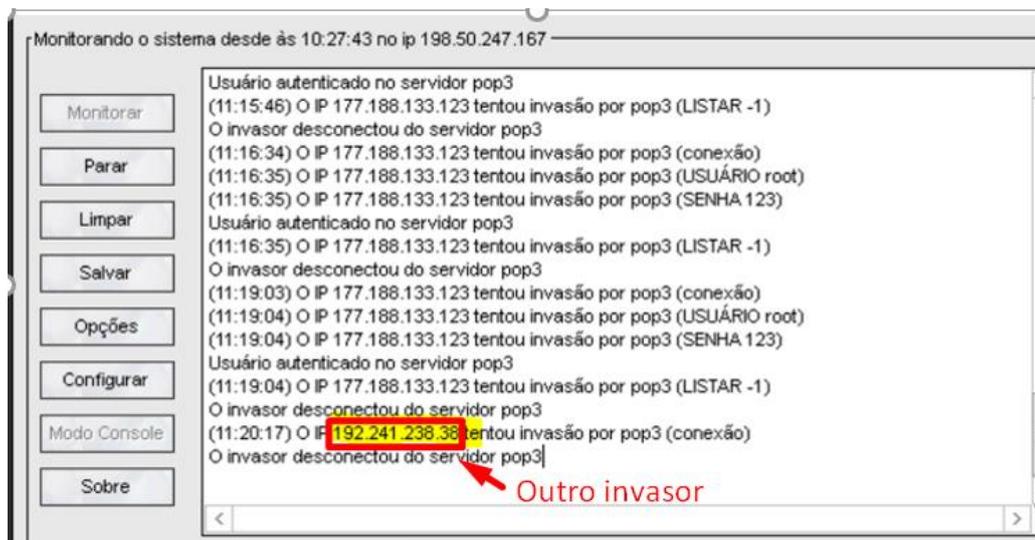
Figura 40: Valhala - Log POP3



Fonte: Próprio autor.

Durante os testes, foi possível captar tentativas reais de invasão, que podem ser vistas na Figura 40.

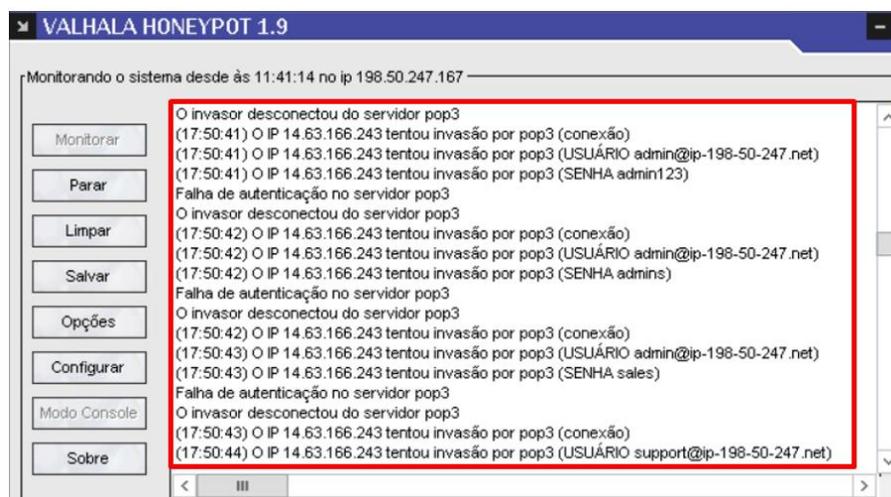
Figura 41: Valhala - Outro invasor



Fonte: Próprio autor.

Após as simulações, o *honeypot* ficou ativo na rede para receber ataques reais, na Figura 41 podemos ver tentativas de invasão via ao protocolo POP3:

Figura 42: Invasão Externa POP3



Fonte: Próprio autor.

Conforme os logs a seguir, foram identificadas as principais invasões ao serviço POP3, pois a ferramenta gerou 482 linhas de logs para 130 tentativas de invasões, dentre essas tentativas 75 foram utilizando combinações de usuário e senha, por 23 IPs diferentes.

Na Figura 42 é ilustrado o padrão de 3 tentativas de invasões, pelos seguintes IPs: 74.120.14.35, 167.248.133.51, 162.142.125.36.

Figura 43: Log - Invasão POP3

```
(20:06:34) O IP 74.120.14.35 tentou invasão por pop3 (conexão)
O invasor desconectou do servidor pop3
(20:06:34) O IP 74.120.14.35 tentou invasão por pop3 (conexão)
O invasor desconectou do servidor pop3
(20:06:34) O IP 74.120.14.35 tentou invasão por pop3 (conexão)
O invasor desconectou do servidor pop3
(04:42:01) O IP 167.248.133.51 tentou invasão por pop3 (conexão)
O invasor desconectou do servidor pop3
(04:42:01) O IP 167.248.133.51 tentou invasão por pop3 (conexão)
O invasor desconectou do servidor pop3
(04:42:01) O IP 167.248.133.51 tentou invasão por pop3 (conexão)
O invasor desconectou do servidor pop3
(11:26:07) O IP 162.142.125.36 tentou invasão por pop3 (conexão)
O invasor desconectou do servidor pop3
(11:26:07) O IP 162.142.125.36 tentou invasão por pop3 (conexão)
O invasor desconectou do servidor pop3
(11:26:07) O IP 162.142.125.36 tentou invasão por pop3 (conexão)
O invasor desconectou do servidor pop3
```

Fonte: Próprio autor.

Nos testes com o POP3 o que chamou atenção foi o IP 14.63.166.243, que realizou 75 tentativas de invasões com diversas combinações de usuário e senha, em menos de 1 minuto, seguem algumas tentativas de invasões por esse IP.

A primeira tentativa pode ser visualizada na Figura 43 que ocorreu às 17:50:34:

Figura 44: Log - Invasão POP3

```
(17:50:34) O IP 14.63.166.243 tentou invasão por pop3 (conexão)
(17:50:34) O IP 14.63.166.243 tentou invasão por pop3 (USUÁRIO admin@ip-198-50-247.net)
(17:50:34) O IP 14.63.166.243 tentou invasão por pop3 (SENHA 1)
Falha de autenticação no servidor pop3
O invasor desconectou do servidor pop3
```

Fonte: Próprio autor.

A última tentativa ocorreu às 17:51:33 e pode ser visualizada na Figura 44:

Figura 45: Log - Invasão POP3

```
(17:51:33) O IP 14.63.166.243 tentou invasão por pop3 (conexão)
(17:51:33) O IP 14.63.166.243 tentou invasão por pop3 (USUÁRIO newsletter@ip-198-50-247.net)
(17:51:34) O IP 14.63.166.243 tentou invasão por pop3 (SENHA newsletter123)
```

Fonte: Próprio autor.

Os usuários mais utilizados foram: admin@ip-198-50-247.net, support@ip-198-50-247.net, info@ip-198-50-247.net, test@ip-198-50-247.net, mike@ip-198-50-247.net, sales@ip-198-50-247.net, root@ip-198-50-247.net, postmaster@ip-198-50-247.net e guest@ip-198-50-247.net.

Pode-se ver na Figura 45 que as senhas mais utilizadas foram incrementadas um número a sequência de números.

Figura 46: Log - Invasão POP3

```

(17:50:34) O IP 14.63.166.243 tentou invasão por pop3 (USUARIO admin@ip-198-50-247.net)
(17:50:34) O IP 14.63.166.243 tentou invasão por pop3 (SENHA 1)
(17:50:35) O IP 14.63.166.243 tentou invasão por pop3 (USUARIO admin@ip-198-50-247.net)
(17:50:35) O IP 14.63.166.243 tentou invasão por pop3 (SENHA 12)
(17:50:36) O IP 14.63.166.243 tentou invasão por pop3 (USUARIO admin@ip-198-50-247.net)
(17:50:36) O IP 14.63.166.243 tentou invasão por pop3 (SENHA 123)
(17:50:36) O IP 14.63.166.243 tentou invasão por pop3 (USUARIO admin@ip-198-50-247.net)
(17:50:36) O IP 14.63.166.243 tentou invasão por pop3 (SENHA 1234)
(17:50:37) O IP 14.63.166.243 tentou invasão por pop3 (USUARIO admin@ip-198-50-247.net)
(17:50:37) O IP 14.63.166.243 tentou invasão por pop3 (SENHA 12345)
(17:50:38) O IP 14.63.166.243 tentou invasão por pop3 (USUARIO admin@ip-198-50-247.net)
(17:50:38) O IP 14.63.166.243 tentou invasão por pop3 (SENHA 123456)

```

Fonte: Próprio autor.

5.1.5.4 TFTP

Na Figura 46, identifica-se que foi realizado um teste com outra máquina tentando acessar e enviar arquivos para o *honeypot* através do serviço TFTP porta 69, utilizando um arquivo teste e o comando `tftp -t 198.50.247.167 put Arquivoteste.txt`

Figura 47: Serviço TFTP

```

Prompt de Comando
C:\Users\Matheus Okazaki\Documents\Fatec\TCC> tftp -t 198.50.247.167 put ArquivoTeste.txt
Falha ao tentar conectar-se

C:\Users\Matheus Okazaki\Documents\Fatec\TCC>tftp -t 198.50.247.167 GET teste.txt
Falha ao tentar conectar-se

C:\Users\Matheus Okazaki\Documents\Fatec\TCC>

```

Fonte: Próprio autor.

Na Figura 47 houve a tentativa de enviar e receber um arquivo ao servidor TFTP, como o servidor não existe de fato e sim é uma simulação, houve a falha na comunicação, mas é possível ver que, na próxima imagem aparece a tentativa de acesso e qual IP tentou enviar e obter os arquivos.

Figura 48: Valhala - Log TFTP

```

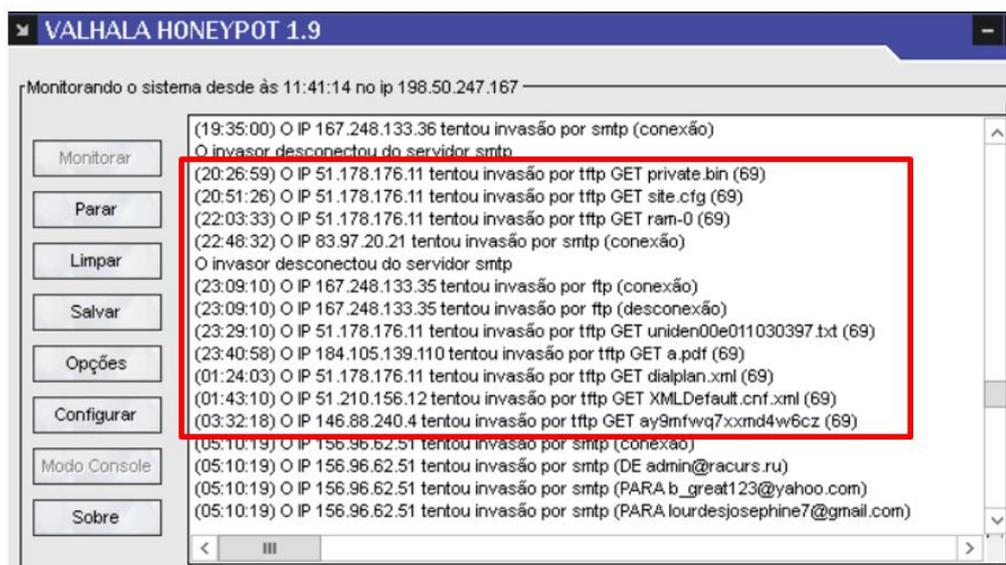
(11:24:39) O IP 216.218.206.67 tentou invasão por ftp (AUTH TLS)
(11:24:39) O IP 216.218.206.67 tentou invasão por ftp (AUTH SSL)
(11:24:40) O IP 216.218.206.67 tentou invasão por ftp (desconexão)
(11:32:33) O IP 177.188.133.123 tentou invasão por tftp PUT ArquivoTeste.txt (69)
(11:32:46) O IP 177.188.133.123 tentou invasão por tftp PUT ArquivoTeste.txt (69)
(11:32:47) O IP 177.188.133.123 tentou invasão por tftp PUT ArquivoTeste.txt (69)
(11:33:01) O IP 177.188.133.123 tentou invasão por tftp GET teste.txt (69)
(11:33:14) O IP 177.188.133.123 tentou invasão por tftp PUT ArquivoTeste.txt (69)
(11:33:17) O IP 177.188.133.123 tentou invasão por tftp GET teste.txt (69)
(11:34:00) O IP 61.53.253.243 tentou invasão por telnet (conexão)
(11:34:12) O IP 61.53.253.243 tentou invasão por telnet (conexão)

```

Fonte: Próprio autor.

Após as simulações, o *honeypot* ficou ativo e configurado para receber ataques reais como pode-se ver na Figura 48, é possível identificar várias tentativas de invasões via protocolo TFTP:

Figura 49: Invasão Externa - TFTP



Fonte: Próprio autor.

Conforme log abaixo pode-se identificar as principais invasões ao serviço TFTP, onde houve 43 tentativas de invasões com 21 IPs diferentes.

Nos logs exibidos na Figura 49, foi identificado que as principais extensões de arquivos utilizadas foram: txt, pdf, xml, bin e cfg, através dos comandos PUT e GET para adicionar e ler arquivos no diretório.

Figura 50: Log - Invasão TFTP

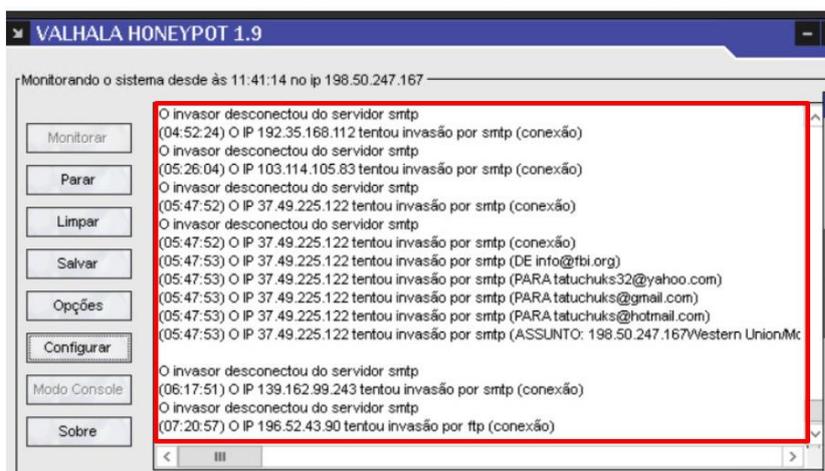
```
(12:46:36) O IP 177.188.133.123 tentou invasão por tftp PUT ArquivoTeste.txt (69)
(23:08:08) O IP 184.105.139.82 tentou invasão por tftp GET a.pdf (69)
(14:29:17) O IP 51.178.176.11 tentou invasão por tftp GET cfg0305.xml (69)
(20:26:59) O IP 51.178.176.11 tentou invasão por tftp GET private.bin (69)
(20:51:26) O IP 51.178.176.11 tentou invasão por tftp GET site.cfg (69)
```

Fonte: Próprio autor.

5.1.5.5 SMTP

Nos testes com o SMTP que podem ser vistos na Figura 50, o *honeypot* ficou ativo na rede receber ataques reais, conforme imagem abaixo, pode-se ver tentativas de invasões via protocolo SMTP:

Figura 51: Invasão Externa - SMTP



Fonte: Próprio autor.

Conforme os logs a seguir, foram identificadas as principais invasões ao serviço SMTP, pois houve mais de 1200 linhas de log e 496 tentativas de invasões, por 74 IPs diferentes.

Na Figura 51, pode-se ver 3 IPs diferentes tentando realizar conexões com o serviço de SMTP, o IP 165.231.148.179 estava tentando encaminhar um e-mail para spameri@tiscali.it, do e-mail spameri@tiscali.it, com o assunto 198.50.247.167.

Figura 52: Log - Invasão SMTP

```

12:32:53) O IP 165.231.148.179 tentou invasão por smtp (DE spameri@tiscali.it)
(12:32:53) O IP 165.231.148.179 tentou invasão por smtp (PARA spameri@tiscali.it)
(12:32:54) O IP 165.231.148.179 tentou invasão por smtp (ASSUNTO: 198.50.247.167)
t_Smtp.LocalIP
t_Smtp.LocalIP
(15:07:29) O IP 103.114.105.83 tentou invasão por smtp (conexão)
O invasor desconectou do servidor smtp
(19:01:48) O IP 74.120.14.36 tentou invasão por smtp (conexão)
O invasor desconectou do servidor smtp
(19:01:48) O IP 74.120.14.36 tentou invasão por smtp (conexão)
O invasor desconectou do servidor smtp
(20:22:15) O IP 165.231.148.179 tentou invasão por smtp (conexão)
O invasor desconectou do servidor smtp

```

Fonte: Próprio autor.

No log da Figura 52 foi identificada uma tentativa de *phishing* ao IP 156.96.62.51 tentar encaminhar um e-mail falso, onde ele informava ao destinatário do e-mail que alguém foi ao banco e tentou retirar \$2,500,000.00 do seus fundos, e era necessário o destinatário responder o e-mail em 72 horas. Esse IP tentou encaminhar outros e-mails parecidos como esse para outros destinatários. Os endereços de e-mails foram removidos do log.

Figura 53: Log - Invasão SMTP

```
(15:13:13) O IP 156.96.62.51 tentou invasão por smtp (conexão)
(15:13:14) O IP 156.96.62.51 tentou invasão por smtp (DE ( ))
(15:13:14) O IP 156.96.62.51 tentou invasão por smtp (PARA ( ))
(15:13:14) O IP 156.96.62.51 tentou invasão por smtp (PARA ( ))
(15:13:14) O IP 156.96.62.51 tentou invasão por smtp (ASSUNTO: ARE YOU DEAD OR
ALIVE??198.50.247.167)
```

Fonte: Próprio autor.

Segue abaixo corpo do e-mail que seria enviado:

Urgent Attention:

I am Ms. Lourdes Josephine, The Executive Managing Director of East West Private Bank. This morning an email was received by Mr Casey Jackson of the USA, saying that you sent him to claim your fund with our bank in the amount of \$2,500,000.00 United State Dollars.

Here comes the big question, ARE YOU DEAD OR ALIVE? Kindly respond to this email as soon as possible to enable us know the real status of things before we proceed further in remitting the fund to the above named person.

If we do not hear from you within 72 working days, that means we will remit the fund to the above claimed person.

Best Regards,

Ms. Lourdes Josephine

Executive Managing Director: East West Private Bank

Urgent Attention:

O invasor desconectou do servidor smtp

Nessas outras linhas do LOG na Figura 53 pode-se identificar e acompanhar o IP 80.82.67.42, tentando encaminhar um *phishing*, informando que devido ao surto do Covid-19, as Nações Unidas estavam recompensando aleatoriamente pessoas pelo mundo todo, e que esse usuário foi selecionado, onde era necessário responder esse e-mail com as informações, para receber \$ 605.000. Diferente da outra tentativa de e-mail essa está mais elaborada pois está em HTML.

Figura 54: Log - Invasão SMTP

```
(09:31:49) O IP 80.82.67.42 tentou invasão por smtp (conexão)
(09:31:49) O IP 80.82.67.42 tentou invasão por smtp (DE ( ))
(09:31:49) O IP 80.82.67.42 tentou invasão por smtp (PARA ( ))
(09:31:49) O IP 80.82.67.42 tentou invasão por smtp (PARA ( ))
(09:31:49) O IP 80.82.67.42 tentou invasão por smtp (PARA ( ))
(09:31:50) O IP 80.82.67.42 tentou invasão por smtp (ASSUNTO: Attention Beneficiary
.198.50.247.167)
```

Fonte: Próprio autor.

Copiamos a tentativa de envio de e-mail e salvamos na extensão HTML, o modelo de e-mail encaminhado seria como na Figura 54.

Figura 55: E-mail Phishing

Attention Beneficiary,
I am António Guterres, from the Corona virus Reward Department United Nations. Due to the outbreak of this deadly disease Corona virus (COVID-19) which has caused a lot of death and hardship. The United Nations is rewarding randomly selected individuals with a Sum of \$605,000 to help and support lives all over the world. Your email was luckily selected and has been listed among individuals to receive this payment, please kindly confirm the details below to enable us to file and facilitate your payment.

1. Full Name:
2. Home Address:
3. Nationality:
4. Date of Birth:
5. Occupation:
6. Tel Phone/Mobile:

We await your response as soon as possible and please advise you to wash and sanitize your hands always (stay at home and stay safe).
Best Regards,
António Guterres
United Nations Reward Department
Contact Email: accesstrasferdepartment@outlook.com
Phone: 209 691 9231

Attention Beneficiary,
I am António Guterres, from the Corona virus Reward Department United Nations. Due to the outbreak of this deadly disease Corona virus (COVID-19) which has caused a lot of death and hardship. The United Nations is rewarding randomly selected individuals with a Sum of \$605,000 to help and support lives all over the world. Your email was luckily selected and has been listed among individuals to receive this payment, please kindly confirm the details below to enable us to file and facilitate your payment.

1. Full Name:
2. Home Address:
3. Nationality:
4. Date of Birth:
5. Occupation:
6. Tel Phone/Mobile:

We await your response as soon as possible and please advise you to wash and sanitize your hands always (stay at home and stay safe).
Best Regards,
António Guterres
United Nations Reward Department
Contact Email: accesstrasferdepartment@outlook.com
Phone: 209 691 9231

Fonte: Próprio autor.

Pôde-se acompanhar outra tentativa de envio de e-mail que se enquadra no *phishing* na Figura 55, onde o IP 129.205.124.135, tentou encaminhar um e-mail informado que o usuário estava na lista para ser recompensado por uma fraude, que já havia sido feito um depósito, mas para o usuário receber o total de \$ 950.000,00, seria necessário pagar \$ 85, para ativar arquivo de pagamento.

Figura 56: Log - Invasão SMTP

```

(20:31:45) O IP 129.205.124.135 tentou invasão por smtp (conexão)
(20:31:46) O IP 129.205.124.135 tentou invasão por smtp (DE ( [REDACTED] ))
(20:31:46) O IP 129.205.124.135 tentou invasão por smtp (PARA ( [REDACTED] ))
(20:31:46) O IP 129.205.124.135 tentou invasão por smtp (PARA ( [REDACTED] ))
(20:31:47) O IP 129.205.124.135 tentou invasão por smtp (PARA ( [REDACTED] ))
(20:31:47) O IP 129.205.124.135 tentou invasão por smtp (PARA ( [REDACTED] ))
(20:31:47) O IP 129.205.124.135 tentou invasão por smtp (PARA ( [REDACTED] ))
(20:31:47) O IP 129.205.124.135 tentou invasão por smtp (PARA ( [REDACTED] ))
(20:31:48) O IP 129.205.124.135 tentou invasão por smtp (PARA ( [REDACTED] ))
(20:31:48) O IP 129.205.124.135 tentou invasão por smtp (PARA ( [REDACTED] ))
(20:31:49) O IP 129.205.124.135 tentou invasão por smtp (ASSUNTO: 198.50.247.167
AMS)

```

Fonte: Próprio autor.

Segue abaixo corpo do e-mail que seria enviado:

Attention E-mail Address Owner:

Sequel to the first edition 2020 meeting held today with Federal Bureau of Investigation, The International Monetary Fund IMF is compensating all the scam victims and your name and email address was found in the scam victims list. This Western Union office has been mandated by the IMF to transfer your compensation to you via Western Union Money Transfer. However, we have concluded to effect your payment through MoneyGram Transfer \$5,000 twice per day until your total sum of \$950,000.00 is completely transferred to you. We have made your first payment this morning but your payment file need to activate before you will pick up the payment today and it will cost you \$85 only to activate your payment file.

THIS IS YOUR FIRST PAYMENT INFORMATION:

<https://secure.moneygram.com/embed/track>

MTCN: 702-898-95

Amount: \$6,000.00

Note that your payment files will be returned to the IMF within 72 hours if we did not hear from you, this was the instruction given to us by the IMF. Send the \$85 with this information below.

Receiver Name ===== KEN EZE

Country ===== Benin Republic

City ===== Cotonou

Test Question ===== When

Answer ===== Now

Amount ===== \$85

Thanks,

Mr James Morgan

Director MoneyGram Transfer Head Office Benin Republic

Attention E-mail Address Owner:

O invasor desconectou do servidor smtp

Nos logs acima foram identificadas algumas tentativas de envio de e-mails falsos, no total houve 8 tentativas de e-mail *phishing*, onde 3 foram feitas pelo IP 156.96.62.51, encaminhando o e-mail do banco, 1 realizada pelo IP 80.82.67.42 encaminhando o e-mail do covid, 3 realizados pelo IP 165.231.148.223 onde encaminhou um e-mail oferecendo serviços suspeitos e 1 do IP 129.205.124.135 que encaminhou o e-mail da solicitando o pagamento dos 85 dólares.

5.2 INFORMAÇÕES GERAIS – TESTES COWRIE

Para realizar os testes de monitoramento com um *honeypot* de média interação na internet, foi escolhido o *Cowrie*, pois disponibiliza serviços de SSH e Telnet, protocolos comuns utilizados na rede, onde foi mantido ativo na Internet, para receber tentativas externas de invasões, e assim foi possível captar e armazenar o log dos ataques.

O serviço escolhido para realizar os testes, foi o SSH, pois é um protocolo utilizado para acesso, administração e modificação de servidores de forma remota, tornando-se extremamente importante para administradores de redes, e “perigoso” caso seja invadido.

5.2.1 AMBIENTE

O ambiente para testes reais na rede foi preparado na Plataforma *Cloud Digital Ocean*, onde foi utilizado o sistema Linux Ubuntu 18.04 (LTS) x64, com 1 GB de memória, 25 GB SSD, e instalado o *honeypot Cowrie*, mantendo ativo o serviço de SSH para possíveis invasões externas no dia 22/09/2020. O servidor da Plataforma contratada está localizado fisicamente em Nova York.

5.2.2 FERRAMENTA COWRIE

A ferramenta *Cowrie*, ilustrada na Figura 56, foi desenvolvida na linguagem de programa *Python* por Michel Oosterhof, baseada no *honeypot Kippo*, tornando possível integrar a interfaces do *Kippo* ao *Cowrie*, a ferramenta emula o *Shell* do

Linux, e permite acompanhar as tentativas de invasão em tempo real ou por meio do log gerado, que pode ser visto na Figura 57. O Cowrie é um *honeypot* de média interação, com serviços de SSH e Telnet, onde armazena *logs* de ataques de força bruta, interação de shell realizada pelo invasor, e com o protocolo Telnet, é possível analisar invasões a outros sistemas.

Figura 57: Honeypot Cowrie

```
2020-09-22T22:19:59.513987Z [cowrie.ssh.factory.CowrieSSHFactory] New connection: 222.186.42.155:51049 (157.230.51.160:2222) [session: 30e6a9af4e7f]
2020-09-22T22:20:00.753132Z [HoneyPotSSHTransport,87,222.186.42.155] Remote SSH version: b'SSH-2.0-PUTTY'
2020-09-22T22:20:00.754077Z [HoneyPotSSHTransport,87,222.186.42.155] SSH client hash fingerprint: 1616c6d18e845e7a01168a44591f7a35
2020-09-22T22:20:00.755602Z [HoneyPotSSHTransport,87,222.186.42.155] kex alg, key alg: b'ecdh-sha2-nistp256' b'ssh-rsa'
2020-09-22T22:20:00.755713Z [HoneyPotSSHTransport,87,222.186.42.155] outgoing: b'aes128-ctr' b'hmac-sha2-512' b'none'
2020-09-22T22:20:00.755780Z [HoneyPotSSHTransport,87,222.186.42.155] incoming: b'aes128-ctr' b'hmac-sha2-512' b'none'
2020-09-22T22:20:59.817561Z [-] Timeout reached in HoneyPotSSHTransport
2020-09-22T22:20:59.818022Z [HoneyPotSSHTransport,86,222.186.30.35] connection lost
2020-09-22T22:20:59.818119Z [HoneyPotSSHTransport,86,222.186.30.35] Connection lost after 120 seconds
```

Fonte: Próprio autor.

Figura 58: Arquivo de log

```
2020-09-22T21:45:11.467760Z [HoneyPotSSHTransport,78,222.186.30.76] Remote SSH version: b'SSH-2.0-PUTTY'
2020-09-22T21:45:11.468999Z [HoneyPotSSHTransport,78,222.186.30.76] SSH client hash fingerprint: 1616c6d18e845e7a01168a44591f7a35
2020-09-22T21:45:11.470822Z [HoneyPotSSHTransport,78,222.186.30.76] kex alg, key alg: b'ecdh-sha2-nistp256' b'ssh-rsa'
2020-09-22T21:45:11.470974Z [HoneyPotSSHTransport,78,222.186.30.76] outgoing: b'aes128-ctr' b'hmac-sha2-512' b'none'
2020-09-22T21:45:11.471062Z [HoneyPotSSHTransport,78,222.186.30.76] incoming: b'aes128-ctr' b'hmac-sha2-512' b'none'
2020-09-22T21:47:10.338552Z [-] Timeout reached in HoneyPotSSHTransport
2020-09-22T21:47:10.339109Z [HoneyPotSSHTransport,78,222.186.30.76] connection lost
2020-09-22T21:47:10.339250Z [HoneyPotSSHTransport,78,222.186.30.76] Connection lost after 120 seconds
2020-09-22T21:48:54.655553Z [cowrie.ssh.factory.CowrieSSHFactory] New connection: 222.186.31.83:10527 (157.230.51.160:2222) [session: 26b0b2db6a7e]
2020-09-22T21:48:55.988250Z [HoneyPotSSHTransport,79,222.186.31.83] Remote SSH version: b'SSH-2.0-PUTTY'
2020-09-22T21:48:55.989569Z [HoneyPotSSHTransport,79,222.186.31.83] SSH client hash fingerprint: 1616c6d18e845e7a01168a44591f7a35
2020-09-22T21:48:55.991313Z [HoneyPotSSHTransport,79,222.186.31.83] kex alg, key alg: b'ecdh-sha2-nistp256' b'ssh-rsa'
2020-09-22T21:48:55.991475Z [HoneyPotSSHTransport,79,222.186.31.83] outgoing: b'aes128-ctr' b'hmac-sha2-512' b'none'
2020-09-22T21:48:55.991570Z [HoneyPotSSHTransport,79,222.186.31.83] incoming: b'aes128-ctr' b'hmac-sha2-512' b'none'
2020-09-22T21:48:56.439058Z [HoneyPotSSHTransport,79,222.186.31.83] NEW KEYS
2020-09-22T21:48:56.715707Z [HoneyPotSSHTransport,79,222.186.31.83] starting service b'ssh-userauth'
2020-09-22T21:48:56.945549Z [HoneyPotSSHTransport,79,222.186.31.83] Got remote error, code 11 reason: b''
2020-09-22T21:48:56.946179Z [HoneyPotSSHTransport,79,222.186.31.83] connection lost
2020-09-22T21:48:56.946370Z [HoneyPotSSHTransport,79,222.186.31.83] Connection lost after 2 seconds
```

Fonte: Próprio autor.

Figura 59: Análise em tempo real de invasões

```
2020-09-22T22:19:59.513987Z [cowrie.ssh.factory.CowrieSSHFactory] New connection: 222.186.42.155:51049 (157.230.51.160:2222) [session: 30e6a9af4e7f]
2020-09-22T22:20:00.753132Z [HoneyPotSSHTransport,87,222.186.42.155] Remote SSH version: b'SSH-2.0-PUTTY'
2020-09-22T22:20:00.754077Z [HoneyPotSSHTransport,87,222.186.42.155] SSH client hash fingerprint: 1616c6d18e845e7a01168a44591f7a35
2020-09-22T22:20:00.755602Z [HoneyPotSSHTransport,87,222.186.42.155] kex alg, key alg: b'ecdh-sha2-nistp256' b'ssh-rsa'
2020-09-22T22:20:00.755713Z [HoneyPotSSHTransport,87,222.186.42.155] outgoing: b'aes128-ctr' b'hmac-sha2-512' b'none'
2020-09-22T22:20:00.755780Z [HoneyPotSSHTransport,87,222.186.42.155] incoming: b'aes128-ctr' b'hmac-sha2-512' b'none'
2020-09-22T22:20:59.817561Z [-] Timeout reached in HoneyPotSSHTransport
2020-09-22T22:20:59.818022Z [HoneyPotSSHTransport,86,222.186.30.35] connection lost
2020-09-22T22:20:59.818119Z [HoneyPotSSHTransport,86,222.186.30.35] Connection lost after 120 seconds
```

Fonte: Próprio autor.

5.2.3 INSTALAÇÃO COWRIE

Para instalar o *cowrie* foi necessário atualizar a biblioteca do *apt-get* do Ubuntu, ilustrado na Figura 59, foi utilizado o comando: *sudo apt-get update*.

Figura 60: Atualização biblioteca Ubuntu

```

Last login: Mon Sep 21 20:53:42 2020 from 200.236.199.127
root@ubuntu-s-1vcpu-1gb-nyc1-01:~# sudo apt-get update
Get:1 http://security.ubuntu.com/ubuntu bionic-security InRelease [
88.7 kB]
Get:2 http://mirrors.digitalocean.com/ubuntu bionic InRelease [242
kB]
Hit:3 http://mirrors.digitalocean.com/ubuntu bionic-updates InRelea
se
Hit:4 http://mirrors.digitalocean.com/ubuntu bionic-backports InRel
ease
Fetched 331 kB in 1s (601 kB/s)
Reading package lists... Done

```

Fonte: Próprio autor.

Como pode-se ver na Figura 60, foi necessário também instalar a biblioteca python-virtualenv, através do comando: *sudo apt-get install git python-virtualenv libssl-dev libffi-dev build-essential libpython3-dev python3-minimal authbind*.

Figura 61: Instalação biblioteca python

```

root@ubuntu-s-1vcpu-1gb-nyc1-01:~# sudo apt-get install git python-virtualenv libssl-dev libffi-dev build-essential
3-minimal authbind
Reading package lists... Done
Building dependency tree
Reading state information... Done
git is already the newest version (1:2.17.1-1ubuntu0.7).
git set to manually installed.
python3-minimal is already the newest version (3.6.7-1~18.04).
python3-minimal set to manually installed.
The following package was automatically installed and is no longer required:
  grub-pc-bin
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:

```

Fonte: Próprio autor.

Foi adicionado um usuário ao COWRIE, ilustrado na Figura 61, e foi acessado, através dos comandos

1º Comando: *sudo adduser --disabled-password cowrie*.

2º Comando: *sudo su – cowrie*.

Figura 62: Adicionando usuário e senha ao Cowrie

```

root@ubuntu-s-1vcpu-1gb-nyc1-01:~# sudo adduser --disabled-password cowrie
Adding user `cowrie' ...
Adding new group `cowrie' (1000) ...
Adding new user `cowrie' (1000) with group `cowrie' ...
Creating home directory `/home/cowrie' ...
Copying files from `/etc/skel' ...
Changing the user information for cowrie
Enter the new value, or press ENTER for the default
  Full Name []: Cowrie Honeypot
  Room Number []: 01
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] Y
root@ubuntu-s-1vcpu-1gb-nyc1-01:~#

```

Fonte: Próprio autor.

Após criar usuário e senha e atualizar e instalar as bibliotecas importantes para a ferramenta rodar foi efetuado o download do Cowrie, por meio do comando: `git clone http://github.com/cowrie/cowrie` que pode ser visto na Figura 62.

Figura 63: Realizando download do Cowrie

```
root@ubuntu-s-1vcpu-1gb-nyc1-01:~# git clone http://github.com/cowrie/cowrie
Cloning into 'cowrie'...
warning: redirecting to https://github.com/cowrie/cowrie/
remote: Enumerating objects: 30, done.
remote: Counting objects: 100% (30/30), done.
remote: Compressing objects: 100% (27/27), done.
remote: Total 13748 (delta 10), reused 8 (delta 2), pack-reused 13718
Receiving objects: 100% (13748/13748), 8.80 MiB | 17.80 MiB/s, done.
Resolving deltas: 100% (9486/9486), done.
root@ubuntu-s-1vcpu-1gb-nyc1-01:~#
```

Fonte: Próprio autor.

Após realizar o download da ferramenta foi necessário configurar o ambiente virtual para o *honeypot* (um Sistema Operacional falso) ilustrado na Figura 63, por meio dos comandos abaixo:

1º Comando: `cd /home/cowrie/cowrie`

2º Comando: `virtualenv --python=python3 cowrie-env`

3º Comando: `source cowrie-env/bin/activate`

4º Comando: `(cowrie-env) $ pip install --upgrade pip`

5º Comando: `(cowrie-env) $ pip install --upgrade -r requirements.txt`

Figura 64: Instalação Sistema Operacional falso

```
root@ubuntu-s-1vcpu-1gb-nyc1-01:~# virtualenv --python=python3 cowrie-env
Already using interpreter /usr/bin/python3
Using base prefix '/usr'
New python executable in /root/cowrie-env/bin/python3
Also creating executable in /root/cowrie-env/bin/python
Installing setuptools, pkg_resources, pip, wheel...done.
root@ubuntu-s-1vcpu-1gb-nyc1-01:~# source cowrie-env/bin/activate
(cowrie-env) root@ubuntu-s-1vcpu-1gb-nyc1-01:~# (cowrie-env) $ pip
install --upgrade pip
-bash: syntax error near unexpected token `$('
(cowrie-env) root@ubuntu-s-1vcpu-1gb-nyc1-01:~# (cowrie-env) $ pip
install --upgrade -r requirements.txt
-bash: syntax error near unexpected token `$('
(cowrie-env) root@ubuntu-s-1vcpu-1gb-nyc1-01:~#
(cowrie-env) root@ubuntu-s-1vcpu-1gb-nyc1-01:~#
```

Fonte: Próprio autor.

5.2.4 CONFIGURAÇÃO SERVIÇO SSH

Na Figura 64 após realizar a instalação do Cowrie, atualizar e configurar o ambiente virtual foi configurado o serviço de SSH. Foi necessário realizar uma cópia do arquivo de configuração do Cowrie, utilizando o comando `cp /home/cowrie/etc/cowrie.cfg.dist /home/cowrie/etc/cowrie.cfg`.

Figura 65: Configuração serviço SSH

```
(cowrie-env) root@ubuntu-s-1vcpu-1gb-nyc1-01:/home/cowrie# cp /home/cowrie/etc/cowrie.cfg.dist /home/cowrie/etc/cowrie.cfg
(cowrie-env) root@ubuntu-s-1vcpu-1gb-nyc1-01:/home/cowrie#
```

Fonte: Próprio autor.

Na configuração do arquivo do *cowrie*, foi necessário alterar o *hostname* e a habilitar a porta 22 para ser ouvida também, conforme Figura 65, por padrão o *cowrie* vem com a 2222 configurada, utilizamos os comandos:

1º Comando: `cd /etc/`

2º Comando: `vi cowrie.cfg`

Adicionamos as linhas

`hostname = UbuntuServer4`

`listen_endpoints = tcp:22:interface=0.0.0.0`

Figura 66: Atualização do arquivo de Configuração do Cowrie

```
# Hostname for the honeypot. Displayed by the shell prompt of the virtual
# environment
#
# (default: svr04)
hostname = UbuntuServer4
```

Fonte: Próprio autor.

Foi configurado também para que um usuário comum possa ouvir a porta 22, já que não podemos utilizar o Cowrie como root (Figura 66). utilizamos os comandos abaixo:

1º Comando: `sudo apt-get install authbind`

2º Comando: `sudo touch /etc/authbind/byport/22`

3º Comando: `sudo chown cowrie:cowrie /etc/authbind/byport/22`

4º Comando: sudo chmod 770 /etc/authbind/byport/22

Figura 67: Configuração porta 22 - usuário comum

```
(cowrie-env) root@ubuntu-s-1vcpu-1gb-ny1-01:/home/cowrie/etc# sudo apt-get install authbind ← Comando 1
Reading package lists... Done
Building dependency tree
Reading state information... Done
authbind is already the newest version (2.1.2).
The following package was automatically installed and is no longer required:
  grub-pc-bin
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 38 not upgraded.
(cowrie-env) root@ubuntu-s-1vcpu-1gb-ny1-01:/home/cowrie/etc# sudo touch /etc/authbind/byport/22 ← Comando 2
(cowrie-env) root@ubuntu-s-1vcpu-1gb-ny1-01:/home/cowrie/etc# sudo chown cowrie:cowrie /etc/authbind/byport/22 ← Comando 3
(cowrie-env) root@ubuntu-s-1vcpu-1gb-ny1-01:/home/cowrie/etc# sudo chmod 770 /etc/authbind/byport/22 ← Comando 4
(cowrie-env) root@ubuntu-s-1vcpu-1gb-ny1-01:/home/cowrie/etc#
```

Fonte: Próprio autor.

Vemos na Figura 67 que foi editado o arquivo / etc / ssh / sshd_config (), foi modificada a linha da porta para fazer a porta SSH verdadeira do *honeypot* escutar em uma porta aleatória (não escolher a 2222), foi utilizado o comando: vim /etc/ssh/sshd_config

Figura 68: Configuração porta do SSH

```
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Port 2600
#AddressFamily any
#ListenAddress 0.0.0.0
```

Fonte: Próprio autor.

Para iniciar o serviço foi necessário acessar o diretório (/home/cowrie1/cowrie/bin) do COWRIE e utilizamos o comando /cowrie start.

5.2.5 TESTE SERVIÇO SSH

Após iniciar o serviço, é possível ver na Figura 68 que foi feita uma análise do log em tempo real, acessando o diretório `cd /home/cowrie1/cowrie/var/log/`, e utilizando o comando `tail -f cowrie/cowrie.log`.

Figura 69: Verificando LOG

```

root@ubuntu-s-1vcpu-1gb-nyc1-01:/home/cowrie1/cowrie/var/log# tail -f cowrie/cowrie.log
2020-09-22T22:19:01.2303252 [HoneyPotSSHTransport,86,222.186.30.35] incoming: b'aes128-ctr' b'hmac-sha2-512' b'none'
2020-09-22T22:19:59.5139872 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 222.186.42.155:51049 (157.230.51.160:2222) [session: 30e6a9af4e7f]
2020-09-22T22:20:00.7531322 [HoneyPotSSHTransport,87,222.186.42.155] Remote SSH version: b'SSH-2.0-PUTTY'
2020-09-22T22:20:00.7540772 [HoneyPotSSHTransport,87,222.186.42.155] SSH client hassh fingerprint: 1616c6d18e845e7a01168a44591f7a35
2020-09-22T22:20:00.7556022 [HoneyPotSSHTransport,87,222.186.42.155] kex alg, key alg: b'ecdh-sha2-nistp256' b'ssh-rsa'
2020-09-22T22:20:00.7557132 [HoneyPotSSHTransport,87,222.186.42.155] outgoing: b'aes128-ctr' b'hmac-sha2-512' b'none'
2020-09-22T22:20:00.7557802 [HoneyPotSSHTransport,87,222.186.42.155] incoming: b'aes128-ctr' b'hmac-sha2-512' b'none'
2020-09-22T22:20:59.8175612 [-] Timeout reached in HoneyPotSSHTransport
2020-09-22T22:20:59.8180222 [HoneyPotSSHTransport,86,222.186.30.35] connection lost
2020-09-22T22:20:59.8181192 [HoneyPotSSHTransport,86,222.186.30.35] Connection lost after 120 seconds

```

Fonte: Próprio autor.

O arquivo de log gerado pela ferramenta cowrie permanece disponível no diretório `/home/cowrie1/cowrie/var/log/cowrie/`, ao acesar o log identifica-se 3 tentativas de acesso.

Na Figura 69 onde ocorre a primeira invasão pode-se identificar o IP 222.186.31.83 tentando realizar conexão no dia 22/09/2020 às 21:48.

Figura 70: Log - Invasão SSH

```

2020-09-22T21:48:54.6555532 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 222.186.31.83:10527 (157.230.51.160:2222) [session: 26b0b2db6a7e]
2020-09-22T21:48:55.9882502 [HoneyPotSSHTransport,79,222.186.31.83] Remote SSH version: b'SSH-2.0-PUTTY'
2020-09-22T21:48:55.9895692 [HoneyPotSSHTransport,79,222.186.31.83] SSH client hassh fingerprint: 1616c6d18e845e7a01168a44591f7a35
2020-09-22T21:48:55.9913132 [HoneyPotSSHTransport,79,222.186.31.83] kex alg, key alg: b'ecdh-sha2-nistp256' b'ssh-rsa'
2020-09-22T21:48:55.9914752 [HoneyPotSSHTransport,79,222.186.31.83] outgoing: b'aes128-ctr' b'hmac-sha2-512' b'none'
2020-09-22T21:48:55.9915702 [HoneyPotSSHTransport,79,222.186.31.83] incoming: b'aes128-ctr' b'hmac-sha2-512' b'none'
2020-09-22T21:48:56.4390582 [HoneyPotSSHTransport,79,222.186.31.83] NEW KEYS
2020-09-22T21:48:56.7157072 [HoneyPotSSHTransport,79,222.186.31.83] starting service b'ssh-userauth'
2020-09-22T21:48:56.9455492 [HoneyPotSSHTransport,79,222.186.31.83] Got remote error, code 11 reason: b''
2020-09-22T21:48:56.9461792 [HoneyPotSSHTransport,79,222.186.31.83] connection lost

```

Fonte: Próprio autor.

Na Figura 70 onde acontece a segunda invasão pode-se identificar o IP 222.186.15.62 tentando realizar conexão no dia 22/09/2020 às 21:56.

Figura 71: Log - Invasão SSH

```

2020-09-22T21:56:23.6179952 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 222.186.15.62:34201 (157.230.51.160:2222) [session: 37b6d7c11a0b]
2020-09-22T21:56:24.9677992 [HoneyPotSSHTransport,80,222.186.15.62] Remote SSH version: b'SSH-2.0-PUTTY'
2020-09-22T21:56:24.9686352 [HoneyPotSSHTransport,80,222.186.15.62] SSH client hassh fingerprint: 1616c6d18e845e7a01168a44591f7a35
2020-09-22T21:56:24.9697882 [HoneyPotSSHTransport,80,222.186.15.62] kex alg, key alg: b'ecdh-sha2-nistp256' b'ssh-rsa'
2020-09-22T21:56:24.9698812 [HoneyPotSSHTransport,80,222.186.15.62] outgoing: b'aes128-ctr' b'hmac-sha2-512' b'none'
2020-09-22T21:56:24.9699332 [HoneyPotSSHTransport,80,222.186.15.62] incoming: b'aes128-ctr' b'hmac-sha2-512' b'none'
2020-09-22T21:58:23.6995312 [-] Timeout reached in HoneyPotSSHTransport
2020-09-22T21:58:23.7001422 [HoneyPotSSHTransport,80,222.186.15.62] connection lost
2020-09-22T21:58:23.7002832 [HoneyPotSSHTransport,80,222.186.15.62] Connection lost after 120 seconds

```

Fonte: Próprio autor.

Já na terceira e última invasão, pode-se identificar na Figura 71 que o IP 222.186.42.137 tentou realizar conexão no dia 22/09/2020 às 22:02.

Figura 72: Log - Invasão SSH

```
2020-09-22T22:02:43.295238Z [cowrie.ssh.factory.CowrieSSHFactory] New connection: 222.186.42.137:26023 (157.230.51.160:2222) [session: 90f52c8ae252]
2020-09-22T22:02:44.515270Z [HoneyPotSSHTransport,81,222.186.42.137] Remote SSH version: b'SSH-2.0-PUTTY'
2020-09-22T22:02:44.516243Z [HoneyPotSSHTransport,81,222.186.42.137] SSH client hassh fingerprint: 1616c6d18e845e7a01168a44591f7a35
2020-09-22T22:02:44.517595Z [HoneyPotSSHTransport,81,222.186.42.137] kex alg, key alg: b'ecdh-sha2-nistp256' b'ssh-rsa'
2020-09-22T22:02:44.517682Z [HoneyPotSSHTransport,81,222.186.42.137] outgoing: b'aes128-ctr' b'hmac-sha2-512' b'none'
2020-09-22T22:02:44.517761Z [HoneyPotSSHTransport,81,222.186.42.137] incoming: b'aes128-ctr' b'hmac-sha2-512' b'none'
2020-09-22T22:04:43.397247Z [-] Timeout reached in HoneyPotSSHTransport
```

Fonte: Próprio autor.

As 3 tentativas de invasões captadas pelo cowrie ao serviço de SSH ocorreram no espaço de tempo de 14 minutos, sendo realizadas, por IPs diferentes, onde não tentaram realizar novas conexões.

6 RESULTADO TESTES

A análise será apresentada em 2 tópicos, a primeira será os resultados dos testes quando foram realizadas as tentativas de invasão e a segunda parte será os testes onde o *honeypot* ficou ativo na rede para receber invasões externas.

6.1 INVASÕES SIMULADAS

Nos testes, foi realizada a invasão ao *honeypot* instalado com o propósito de fins educacionais, o Valhala mostrou ser consistente nos testes, e por ser de simples instalação, não necessitar de máquinas robustas para processar e serviços de fácil configuração, considera-se como ponto positivo, pois apresentou resultados importantes, como IP, hora das tentativas de ataques, protocolos, senha, usuário e comandos que o invasor estava utilizando, a ferramenta permite o monitoramento em tempo real e também através do arquivo de log gerado.

Os testes iniciaram-se às 10:38:05 do dia 10/10/2020, no mesmo minuto, ao realizar os testes do serviço de Telnet na porta 23, para acesso remoto, foram captadas duas tentativas de invasões por outros usuários além dos testes já programados. Após "invadir" o serviço, foi utilizado o comando DIR, onde foi possível verificar os diretórios com os nomes de documentos, funcionários, *backup*, *windows* e clientes que estavam definidas na configuração do *honeypot*. Na visão do atacante parecem ser arquivos importantes de uma empresa, tornando-se "um pote de mel", e a princípio parece ser uma rede real, o que pode distrair por algum tempo os invasores e assim o analista de rede pode ao captar o IP e outras informações, bloquear o acesso desse IP a rede real ou monitorá-lo.

No serviço de FTP, ao utilizar o comando LIST, foi possível verificar os diretórios simulados pelo *honeypot* e informações das conexões FTP, enquanto isso no Valhala foram captadas informações como a hora, IP, protocolo, porta, usuário e senha usadas para a invasão.

No protocolo POP3, logo após subir o serviço, já foi possível capturar uma tentativa de invasão que não foi realizada como teste, e sim uma tentativa real. Assim pode-se ver que possuem "hackers" sem um alvo definido de ataque, mas ficam procurando oportunidades de invasões. A ferramenta Valhala foi de grande ajuda, pois armazenou no *Log* informações como IP, hora, serviço, usuário e senha, comandos utilizados e quando o atacante conectou e desconectou, sendo possível ao administrador do serviço de e-mail definir por exemplo políticas de senha e usuário de e-mail, que dificultam a invasão, pois hoje infelizmente muitas pessoas utilizam senhas dedutivas, como data do aniversário, o que torna mais fácil para um *hacker* invadir os serviços.

Os testes realizados com o protocolo TFTP, que é utilizado para o envio de arquivos, no *honeypot* foi identificada uma falha na conexão e que o atacante tentou enviar e receber arquivos, através do comando PUT e GET, auxiliando na análise das intenções do atacante que gostaria talvez de encaminhar um arquivo "malicioso" ou captar arquivos importantes da rede.

6.2 INVASÕES REAIS CAPTADAS

Após realizar os testes de invasões com a ferramenta Valhala, foram mantidos os serviços ativos na rede do dia 10/10/2020 à 24/10/2020, onde foi possível captar mais de 879 tentativas de invasão aos serviços de Telnet, POP3, FTP, TFTP e SMTP, com 196 IPs diferentes. Na Figura 72 pode-se ver que o serviço SMTP recebeu mais tentativas de conexões, devido a tentativa de envio de e-mails com grande quantidade de linhas.

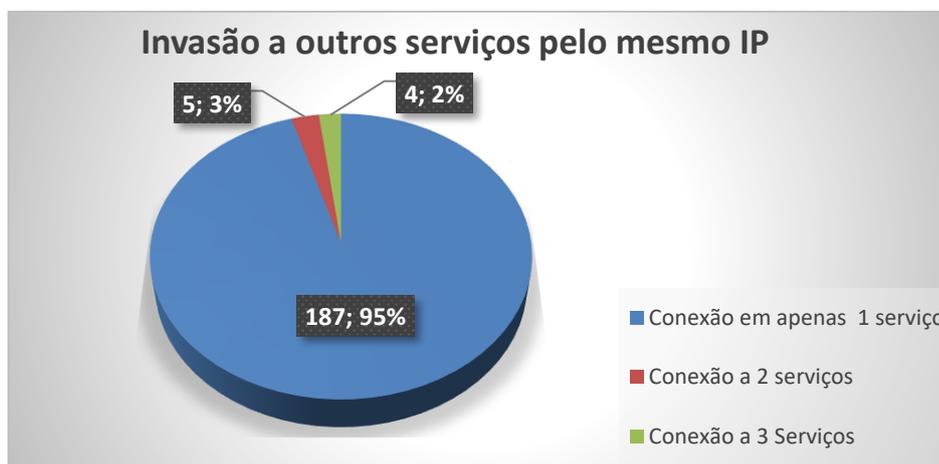
Figura 73: Quantidade de invasões por serviço



Fonte: Próprio autor.

Na Figura 73, pode-se identificar que apenas 5% dos IPs tentaram realizar a invasão a outros serviços ativos do *honeypot*, e 95% realizaram a conexão em apenas um serviço.

Figura 74: Invasão a outros serviços pelo mesmo IP



Fonte: Próprio autor.

Ao analisar os dados gerados pela ferramenta, foi identificado que o serviço SMTP recebeu mais tentativas de conexões, é possível ver que os principais usuários utilizados para tentativas de acesso foram o root e admin, também foram captadas tentativas de utilização de comandos, alta quantidade de tentativas de conexões aos serviços, além da alta quantidade de e-mails *phishing* tentando serem enviados pelo serviço do *honeypot*.

Ao analisar os dados da ferramenta Cowrie com serviço de SSH configurado, que ficou ativo no dia 22/09/2020, foram identificadas 3 tentativas de acesso por IPs diferentes, porém não tentaram realizar novos acessos ao serviço, por se tratar de um serviço com criptografia, não houve muitas tentativas de acesso.

7 CONCLUSÃO

A Segurança da Informação é essencial para qualquer serviço ou aplicação tecnológica, o *honeypot* aplicado a rede, nos trouxe grandes benefícios, pois embora não seja um método direto de segurança, contribui para a análise das possíveis invasões e possibilita a prevenção e redução das vulnerabilidades da rede.

O *honeypot* mostrou ser de grande apoio, pois ao simular os testes com a Ferramenta Valhala que é de baixa interação, foi possível captar diversas informações de ataques, e ao deixar a ferramenta configurada para receber ataques, foi alvo de um grande volume de tentativas de invasões nos trazendo dados importantes das invasões, e o Cowrie uma ferramenta de média interação com o serviço de SSH configurado, sofreu também tentativas de invasões, ao analisar os resultados das ferramentas mapeamos informações dos ataques.

Os Logs da ferramenta Valhala auxiliaram a analisar os IPs que estavam tentando invadir, os comandos utilizados, e as possíveis intenções dos atacantes, foram recebidas uma grande quantidade de tentativas de invasões, mostrando que existem hackers sem alvos definidos, que verificam possibilidades de ataques, tornando indispensável a aplicação de segurança nas redes, já que logo após subir os serviços na internet, já houveram rapidamente, várias tentativas de invasões. Nos testes executados com os *honeypots*, foi constatado que é de grande auxílio para a segurança de uma rede, pois tornou possível analisar as informações dos atacantes, como identificar os principais serviços alvo de ataques, comandos utilizados, identificação de e-mails padrões *phishing*, usuário e senhas padrões, além de captar os IPs que estavam realizando as tentativas de invasões. Embora a rede utilizada, não fosse de grande organização, só por estar na internet já foi considerada um alvo para os atacantes.

Portanto, ao empregar o *honeypot* como auxílio a segurança de uma organização, é possível analisar as tentativas de invasões sem comprometer ou pôr em risco à rede real, quando configurado corretamente, traz grandes benefícios, já que a análise dos

possíveis ataques, permite "prever" os principais ataques, auxiliando na prevenção e melhoria contínua dos métodos Segurança.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSUNÇÃO, Marcos. **Honeypots e honeynets: aprenda a detectar e enganar invasores (2009)**:<https://books.google.com.br/books?id=DaC-CQAAQBAJ&printsec=frontcover&hl=pt-BR&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false> Acesso em: 23 out. 2020. Brasil, Visual Books 2009.

SPITZER, Lance. **Honeypots: Tracking Hackers**. USA, Addison Wesley 2002.

CenPRA, **INSTALAÇÃO E USO DE HONEYPOT DE BAIXA INTERATIVIDADE**: <<ftp://ftp.registro.br/pub/gts/gts0104/gts012004-00tutorial-honeypots.pdf>> Acesso em: 25 out. 2020.

Cert.br, **Honeypots e Honeynets: Definições e Aplicações**: <<https://www.cert.br/docs/whitepapers/honeypots-honeynets/>> Acesso em: 25 out. 2020.

Cert.br, **Microcurso: Honeypots e Honeynets**, <<https://www.cert.br/docs/palestras/nbso-ssi2003-mchnets.pdf>> Acesso em: 23 out. 2020.

Cert.br, **Distributed Honeypots Project** <<https://honeytarg.cert.br/stats/flows/2020/10/07/flows-2020-10-07.html>> Acesso em: 03 nov. 2020.

DevMedia, **Honeypots: Evitando invasões**: <<https://www.devmedia.com.br/honeypots-evitando-invasoes/29983>> Acesso em: 26 ago. 2020.

DevMedia, **Procolo FTP** <<https://www.devmedia.com.br/protocolo-ftp/17493>> Acesso em: 11 out. 2020.

FLYLIB, **Chapter 8: Other Windows-Based Honeypots** <<https://flylib.com/books/en/1.48.1.55/1/>> Acesso em: 27 ago. 2020.

Gavidia, **TFTP (Trivial File Transfer Protocol)**<<http://penta2.ufrgs.br/rc952/trab1/tftp.html>> Acesso em: 11 out. 2020.

Greynoise, <<https://greynoise.io/>> Acesso em: 02 nov. 2020.

Hostinger, **FTP: o que é, como funciona e qual o melhor tipo para gerenciar arquivos na internet** <<https://www.hostinger.com.br/tutoriais/ftp-o-que-e-como-funciona>> Acesso em: 11 out. 2020.

HostMidia, **O que é SSH? História e vantagens do seu uso?** <<https://www.hostmidia.com.br/blog/ssh/>> Acesso em: 26 set. 2020.

Informit, **Honeynet Project: What a Honeynet Is** <<https://www.informit.com/articles/article.aspx?p=23948&seqNum=3>> Acesso em: 26 ago. 2020.

Luis Rocha, **Honeynet: eficácia no mapeamento das ameaças virtuais - Parte 1**: <<https://www.nic.br/noticia/na-midia/honeynet-eficacia-no-mapeamento-das-ameacas-virtuais-parte-1/>> Acesso em: 26 ago. 2020.

Marcos Assunção, **Honeypots e Honeynets: Aprenda a detectar e enganar os invasores**: <<https://docplayer.com.br/7969405-Honeypots-e-honeynets-aprenda-a-detectar-e-enganar-os-invasores.html>> Acesso em: 29 ago. 2020.

Marcos Assunção, **HoneyPots e HoneyNets: Aprenda a detectar e enganar os invasores**, A segurança através do disfarce: <https://pt.slideshare.net/mflavio2k/honeypots-e-honeynets?from_action=save> Acesso em: 26 ago. 2020.

Portal ALL, **Deception Toolkit** <<http://www.all.net/dtk/>> Acesso em: 26 ago. 2020.

Portal CCM, **os protocolos de serviço de mensagens: SMTP, POP3 e IMAP4** <<https://br.ccm.net/contents/282-os-protocolos-de-servico-de-mensagens-smtp-pop3-e-imap4>> Acesso em: 11 out. 2020.

Portal SpeedCheck, **SMTP** <<https://www.speedcheck.org/pt/wiki/smtp/>> Acesso em: 24 out. 2020.

Portal SSH.com, **SSH (Secure Shell)**<<https://www.ssh.com/ssh/>> Acesso em: 26 set. 2020.

Portal TechTudo, **Tudo sobre Putty** <<https://www.techtudo.com.br/tudo-sobre/putty.html>> Acesso em: 10 out. 2020.

Portal TechTudo, **eM Client gerencia e-mails e possui mensageiro instantâneo integrado** <<https://www.techtudo.com.br/tudo-sobre/em-client-app.html>> Acesso em: 10 out. 2020.

Posey, Brien. **Catch malicious network activity with a Honeyd virtual honeypot**: <<https://www.techrepublic.com/article/catch-malicious-network-activity-with-a-honeyd-virtual-honeypot/>> Acesso em: 26 ago. 2020.

PTComputador, **Sobre o Telnet** <<http://ptcomputador.com/Networking/ftp-telnet/66750.html>> Acesso em: 26 set. 2020.

SPITZER, Lance. **Honeypots: Tracking Hackers**. USA, Addison Wesley 2002.

Techbizforense, **O Ovo do Cuco** <<http://techbizforense.blogspot.com/2011/01/o-ovo-do-cuco.html>> Acesso em: 19 out. 2020.