A Aplicabilidade do Honeypot Valhala Utilizando Serviços de Alta e Baixa Interatividade

Carlos Augusto Machado Fernandes [1], Daves Márcio Silva Martins

[1] Centro de Ensino Superior de Juiz de Fora

cafernandeseng@gmail.com, davesmartins@gmail.com

Abstract. *The purpose of this article is to demonstrate the applicability of low and high interaction honeypots exploiting security vulnerabilities. For this, it is necessary to approach concepts, techniques and tools that served as the basis for the implementation of a honeynet and the subsequent tests.*

Resumo. *O objetivo deste artigo é demonstrar a aplicabilidade de honeypots de baixa e alta interação explorando vulnerabilidades de segurança. Para isso, é necessário abordar conceitos, técnicas e ferramentas que serviram de base para a implementação de uma honeynet e os testes subsequentes.*

1.INTRODUÇÃO

A informação é um ativo essencial para os negócios de uma organização. A interconectividade e o intenso tráfego de dados entre os ambientes computacionais contribuem para o aumento da exposição das informações e o surgimento de ataques inteligentes e ambiciosos. É crescente a preocupação das organizações com relação aos valores e vulnerabilidades de seus ativos (ABNT, 2005).

A Segurança da Informação passa a ser um fator determinante para garantir a continuidade do negócio, minimizando os riscos e maximizando o retorno sobre os investimentos. A identificação e implementação de um conjunto de controles, compreendendo políticas, processos, procedimentos, estruturas organizacionais e funções de *hardware* e *software* é indispensável para que a informação esteja devidamente segura. Os controles devem ser monitorados, analisados e atualizados para atender as exigências do negócio e da segurança das organizações (Coelho *et al.*, 2014).

Os *honeypots* são importantes ferramentas que atuam na prevenção de atividades maliciosas em uma rede de computadores. Baseiam-se na criação de um ambiente com falhas

de segurança, atraindo o invasor e proporcionando o estudo detalhado de suas táticas, comportamentos e ferramentas utilizadas.

Algumas questões contribuíram para o desenvolvimento do estudo proposto: Qual a importância dos *honeypots* no âmbito da segurança de redes? O que é necessário para implementá-los? Em qual contexto atuam? O artigo foi estruturado em seis seções, abordando conceitos, técnicas e ferramentas, buscando responder as questões colocadas anteriormente. A Segunda seção retrata os princípios básicos de segurança e os define como medidas preventivas contra ameaças. A Terceira seção conceitua componentes e ferramentas de segurança. A Quarta seção defende a utilização de máquinas virtuais em sistemas de segurança, além de mostrar a arquitetura da *honeynet* e as regras de controle de tráfego. A Quinta seção descreve os testes para exploração das vulnerabilidades do ambiente. A Sexta e conclusiva seção faz uma breve análise da aplicabilidade dos *honeypots* em diferentes contextos.

2. A IMPORTÂNCIA DOS SERVIÇOS DE SEGURANÇA DA INFORMAÇÃO NA CONTENÇÃO DE AMEAÇAS

O compartilhamento de recursos de informação entre redes públicas e privadas e a tendência da computação distribuída aumentam a dificuldade de se controlar o acesso à informação. É iminente o aparecimento de ameaças como fraudes eletrônicas, espionagem, sabotagem, vandalismo, códigos maliciosos, *hackers* e ataques de *denial of service* (ABNT,2005).

Conforme Coelho et al. (2014), o padrão ISO 7498-2 define os serviços de segurança como medidas preventivas contra ameaças identificadas e podem ser classificados como:

1) **Confidencialidade**: Proteção contra acesso não autorizado envolvendo medidas como controle de acesso e criptografia. A perda da confidencialidade pode ser caracterizada quando ocorre a quebra de sigilo de determinada informação;
2) **Autenticidade**: Origem e destino podem verificar se a outra parte envolvida é realmente quem alega ser;
3) **Integridade:** Trata-se da proteção contra alterações ou remoções não autorizadas. A perda da integridade pode estar associada a confidencialidade quando um sistema de controle de acesso tem sua integridade violada, violando também a confidencialidade de seus arquivos;
4) **Não repúdio:** Origem e destino são impedidos de negar a transmissão das mensagens;
5) **Conformidade:** Dever de cumprir regulamentos internos e externos impostos às atividades da organização;
6) **Disponibilidade**: Garante que recursos estejam disponíveis para acessos autorizados quando solicitados. A perda da disponibilidade pode ser caracterizada em caso de falha de comunicação com um sistema importante para a organização.

3. COMPONENTES E FERRAMENTAS DE SEGURANÇA

3.1. Firewall

O *firewall* é um conjunto de recursos de *hardware* e *software* responsável pela interconexão de uma rede interna e a *internet* através do controle de tráfego de pacotes (de Moraes, 2005). Os *firewalls* são classificados como:

Filtragem de pacotes *(*packet filtering). É baseado na verificação de informações contidas no cabeçalho dos pacotes, controlando-os de acordo com uma lista de acesso (*Access List*).

Inspeção de estados *(*stateful inspection). É um mecanismo de filtragem orientado à conexão, ou seja, uma lista de estados de conexão é analisada antes de verificar as regras para determinado pacote.

Proxy. É um servidor que faz a intermediação entre a rede interna e a *internet*, rescrevendo e remontando os pacotes em nível de protocolo de aplicação.

3.2. NAT (Network Address Translation)

O *NAT (Network Address Translation*) é uma solução que foi implementada para resolver o problema de esgotamento de endereços IP versão 4. Consiste em traduzir endereços IP válidos em endereços internos que não são válidos na internet (de Moraes, 2005). Os *NATS* são classificados como:

NAT estático. Um conjunto de endereços IP válidos (públicos) é traduzido para um conjunto de endereços IP internos privados. Utilizado para mapear servidores que necessitem de um endereço fixo para acesso à *internet*.

NAT dinâmico. Ocorre quando os endereços privados são mapeados dinamicamente para um número limitado de endereços públicos. O acesso à internet é limitado pela quantidade de endereços IP disponíveis.

PAT (*Port Address Translation*). Permite que vários computadores utilizem o mesmo endereço IP. O *PAT* mantém uma tabela da conexão, trocando a porta e o endereço de origem para o endereço público.

3.3. Redes

DMZ. *Demilitarized Zone* é uma rede ou sub-rede que contém servidores e serviços disponíveis para acessos provenientes de uma rede externa. Seu propósito é isolar o tráfego potencialmente malicioso, evitando que ele passe por dentro da rede corporativa (de Moraes, 2005).

LAN. *Local Area Network* é uma rede de computadores restrita a um local físico definido como casa, escritório, empresa ou prédio. Possui sua própria faixa de endereços IP (HelpDigital, 2017).

WAN. *Wide Area Network* é uma rede que cobre uma área física maior como cidade, estado, país ou o *campus* de uma universidade. Também pode ser genericamente referida à internet. As redes *WAN* se tornaram essenciais para atender grande quantidade de informações trafegadas entre computadores e empresas (HelpDigital, 2017).

3.4. Honeypots

Honeypots são ferramentas para monitoração de ataques que colecionam informações importantes, contribuindo para a melhoria das metodologias de segurança de uma empresa. Ao contrário dos *firewalls* e sistemas *IDS*, não dependem de regras, assinaturas ou algoritmos (Marcelo e Pitanga, 2003).

Essas ferramentas consideram qualquer tipo de atividade como maliciosa e anômala, capturando os ataques e armazenando em *logs* para posterior análise. Podem representar alto risco para a organização, sendo importante fazer a correta configuração do ambiente para evitar acesso a outras máquinas da rede. São usadas para identificação de ataques, varreduras e tendências, isolar sistemas importantes, capturar assinaturas de ataques e códigos maliciosos e detectar máquinas comprometidas ou com problemas de configuração (Hoepers *et al.*, 2007). Os *honeypots* são classificados como:

Honeypots de baixa interatividade. Nos *honeypots* de baixa interatividade os invasores interagem com serviços ou sistemas emulados. Possuem baixo risco de comprometimento, sendo indicados para redes de produção.

Honeypots de alta interatividade. Nos *honeypots* de alta interatividade os invasores interagem com sistemas operacionais, serviços e aplicações reais. Proporcionam maior risco de comprometimento, podendo ceder acesso a outros locais da rede. São indicados para redes de pesquisa, monitoradas por profissionais qualificados que visam estudar o comportamento dos invasores.

3.5. Honeynet

Honeynet consiste em uma rede projetada para ser comprometida, com mecanismo de controle capaz de evitar ataques a outras redes. Estes ambientes podem abranger uma série de *honeypots* instalados em vários sistemas operacionais, além de sistemas de contenção, coleta de dados e geração de alerta (Hoepers *et al.*, 2007). As *honeynets* são classificadas como:

Honeynets Virtuais. *Honeynets virtuais* baseiam-se no conceito de utilizar um número reduzido de máquinas físicas, normalmente um computador. Nas *honeynets virtuais de autocontenção* todos os mecanismos, incluindo contenção, captura, coleta de dados, geração de alertas e *honeypots* se encontram em um único computador. Nas *honeynets virtuais híbridas* os *honeypots* são executados em dispositivos distintos. Apesar de pouco tolerante a falhas, as *honeynets virtuais* possuem manutenção simples, necessidade de menor espaço físico e menor custo final dos equipamentos.

Honeynets Reais. Em *honeynets reais*, os sistemas de contenção, captura, coleta, alerta de informações e *honeypots* são físicos. Possuem manutenção difícil e trabalhosa, necessidade de maior espaço físico e custo elevado. Contudo, são mais tolerantes a falhas por se tratarem de sistemas distribuídos.

3.6. PFSENSE

O *pfSense* é um *firewall* roteador executado sobre o sistema operacional *FreeBSD*. É responsável pela restrição, liberação e roteamento de pacotes e disponibiliza uma *interface web* para criação das regras (Damasceno, 2005). As regras de roteamento podem ser definidas como:

Port Forward. Responsável pelo redirecionamento de pacotes da rede *WAN* para rede *LAN* através da especificação de endereço IP e porta de destino.

1 x 1. Responsável pelo redirecionamento de pacotes da rede *WAN* para rede *LAN,* sendo necessário especificar apenas o endereço IP de destino.

Outbound. Faz o roteamento de pacotes da rede *LAN* para a rede *WAN* . O *pfsense* cria de forma automática uma regra de saída de pacotes da rede.

3.7. Honeypot Valhala

O *valhala* é um *software* livre que oferece serviços de baixa e alta interatividade, destacando-se *HTTP*, *FTP*, *SMTP*, *POP3*, *TELNET*, *TFTP*, *FINGER* e *PROXY*. Ao contrário de algumas ferramentas, como é o caso da h*oneyd*, não suporta a criação de hosts virtuais. O endereço IP utilizado deve ser o da máquina que hospeda o programa (Assunção, 2009). Através da Figura 1 é possível identificar opções gerais como alertas de invasão, armazenamento de *logs*, atualização da ferramenta, ativação de portas extras e monitoramento automático e oculto.

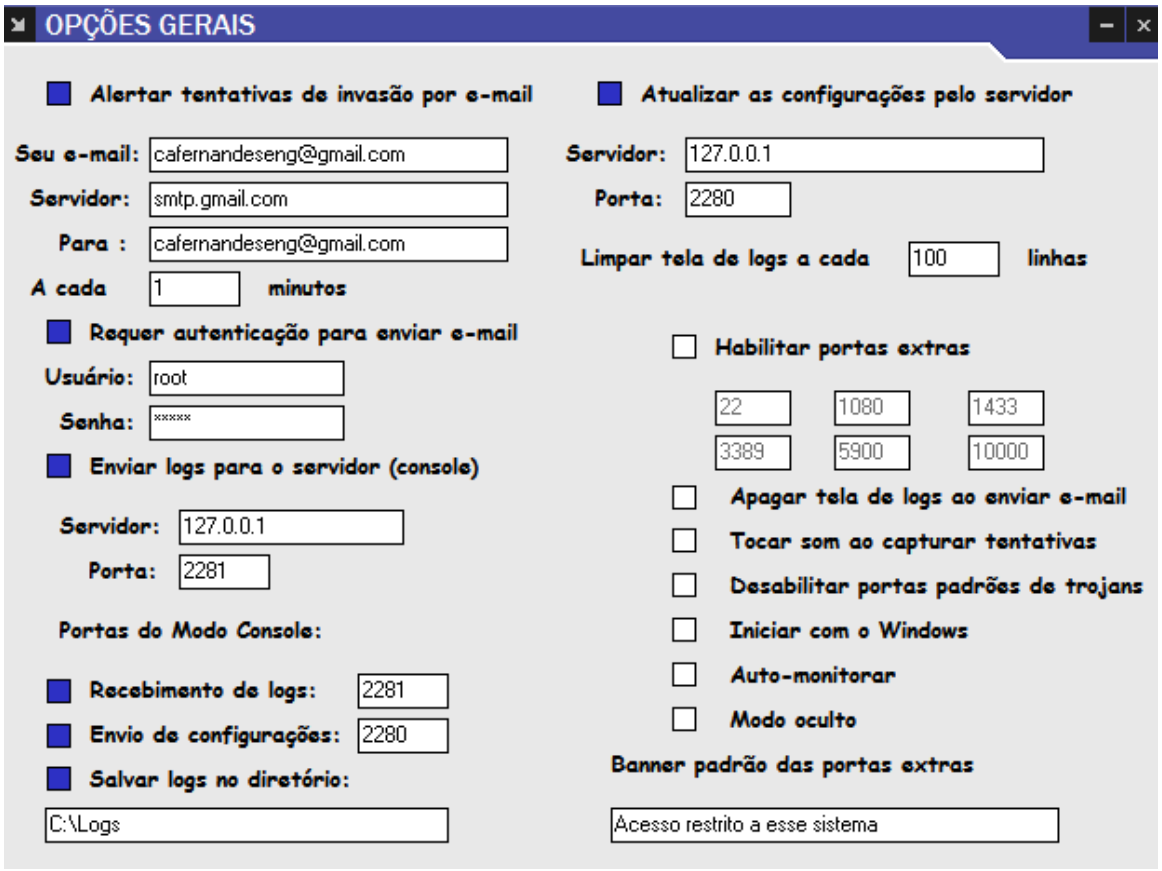

Figura 1. Tela de opções

Fonte: Do autor (2018)

Servidor FTP. O servidor *FTP* é um serviço de alta interatividade que permite a transferência de arquivos reais. A Figura 2 mostra configurações como acesso total aos diretórios e arquivos, porta comprometida, mensagem ao invasor e credenciais de acesso.

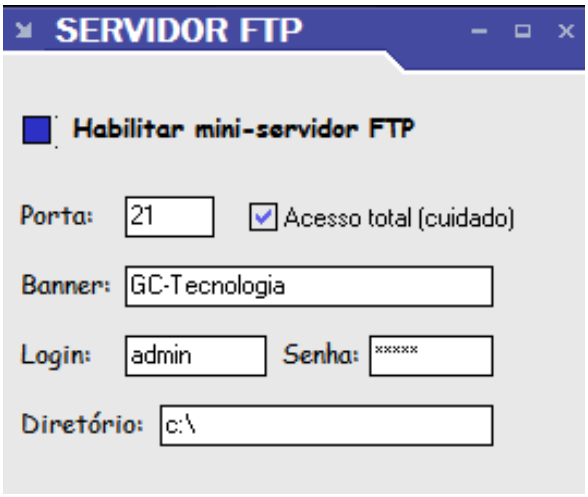

Figura 2. Tela de configurações do servidor FTP

Fonte: Do autor (2018)

Servidor TELNET. O servidor *TELNET* é um serviço de baixa interatividade capaz de simular um *shell* de comandos do *MS-DOS*. A melhor experiência de interatividade do usuário (invasor) com o sistema depende da correta configuração das informações visualizadas no ambiente emulado, tais como nome dos diretórios, arquivos, informações de rede e disco rígido. A Figura 3 ilustra as opções para criação do ambiente:

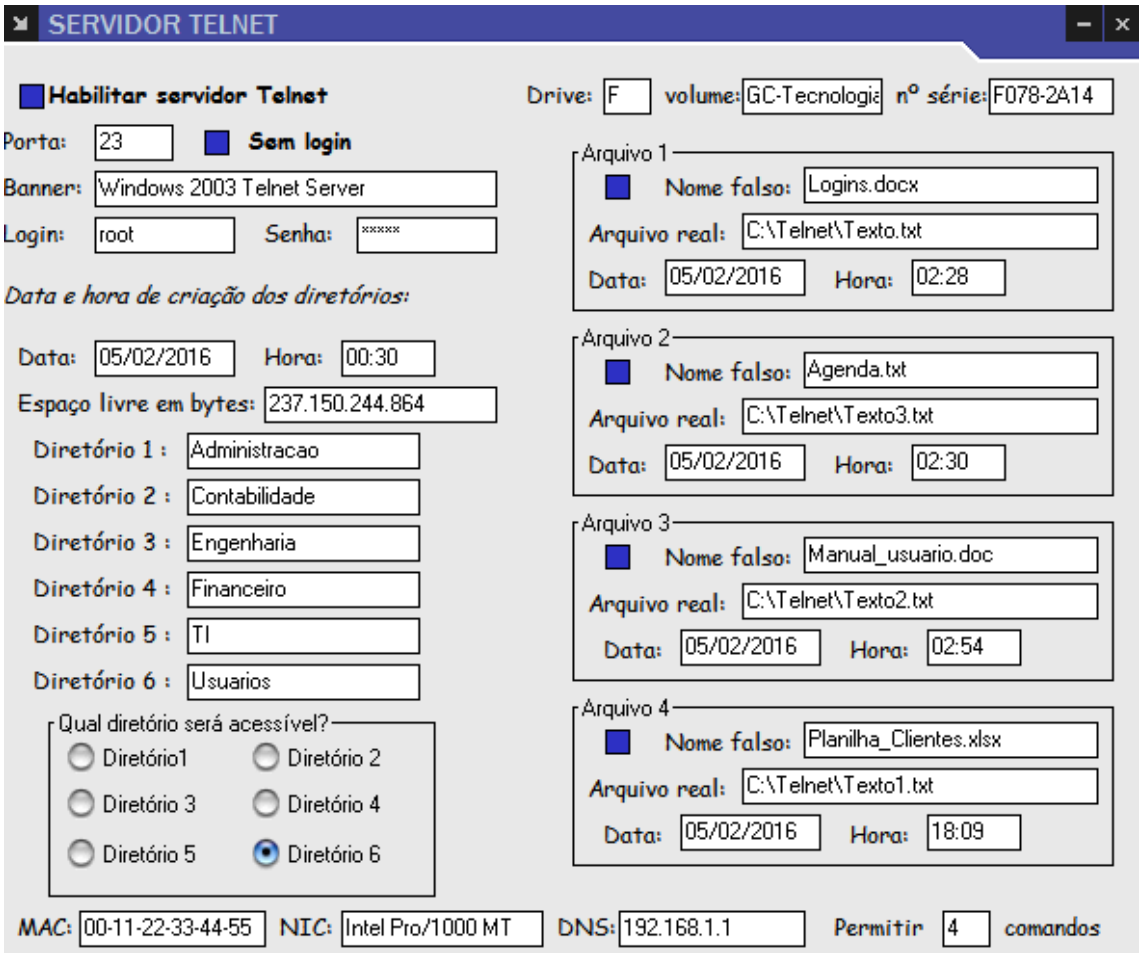

Figura 3. Tela de configurações do servidor TELNET

Fonte: Do autor (2018)

4. IMPLEMENTAÇÃO DA HONEYNET VIRTUAL

4.1. Máquinas Virtuais

De acordo com Rosenblum and Garfinkel (2005), a resolução de alguns problemas relacionados ao desempenho de *hipervisores* tem permitido ampla adoção da tecnologia de máquinas virtuais em sistemas de produção. Em busca de redução de custos de hardware, software e gerência de parque tecnológico, as empresas estão buscando a consolidação de seus servidores através da tecnologia de virtualização (Newman *et al.*, 2005).

Para compreender a utilização de máquinas virtuais na implementação da *honeynet* é necessário discutir propriedades dos *hipervisores* e como elas podem ser aplicadas na segurança de sistemas:

Isolamento. Através do isolamento dos ambientes virtuais, o *hipervisor* provê a confidencialidade dos dados entre os sistemas convidados, ou seja, os dados de uma máquina virtual só podem ser acessados por aplicações convidadas, preservando sua integridade. O isolamento também permite a contenção de erros de *software* acidentais ou intencionais, melhorando a disponibilidade dos sistemas (LeVasseur *et al.*, 2004).

Controle de recursos. O *hipervisor* faz o controle dos acessos do sistema ao *hardware*, sendo possível implementar mecanismos para verificar a consistência desses acessos e seus resultados, aumentando a integridade do sistema convidado. Para fins de auditoria, é possível registrar e acompanhar as atividades das máquinas convidadas (Dunlap *et al.*, 2002).

Inspeção. O *hipervisor* pode extrair informações do convidado para o sistema hospedeiro, permitindo externamente implementar mecanismos de verificação de integridade do ambiente do convidado, tais como antivírus e detectores de intrusão (Laureano *et al.*, 2007).

Encapsulamento. A possibilidade de salvar estados do sistema convidado torna viável a implementação de mecanismos de *rollback* em caso de quebra de integridade. Também é possível fazer a migração das máquinas virtuais para resolver problemas de disponibilidade (Fu and Xu, 2005).

4.2. Topologia de rede

Com base nos estudos apresentados nesse trabalho, foi implementada uma *honeynet virtual* de autocontenção para receber os testes de vulnerabilidade de segurança. Todos os itens do ambiente podem ser identificados na Figura 4 e são posteriormente descritos:

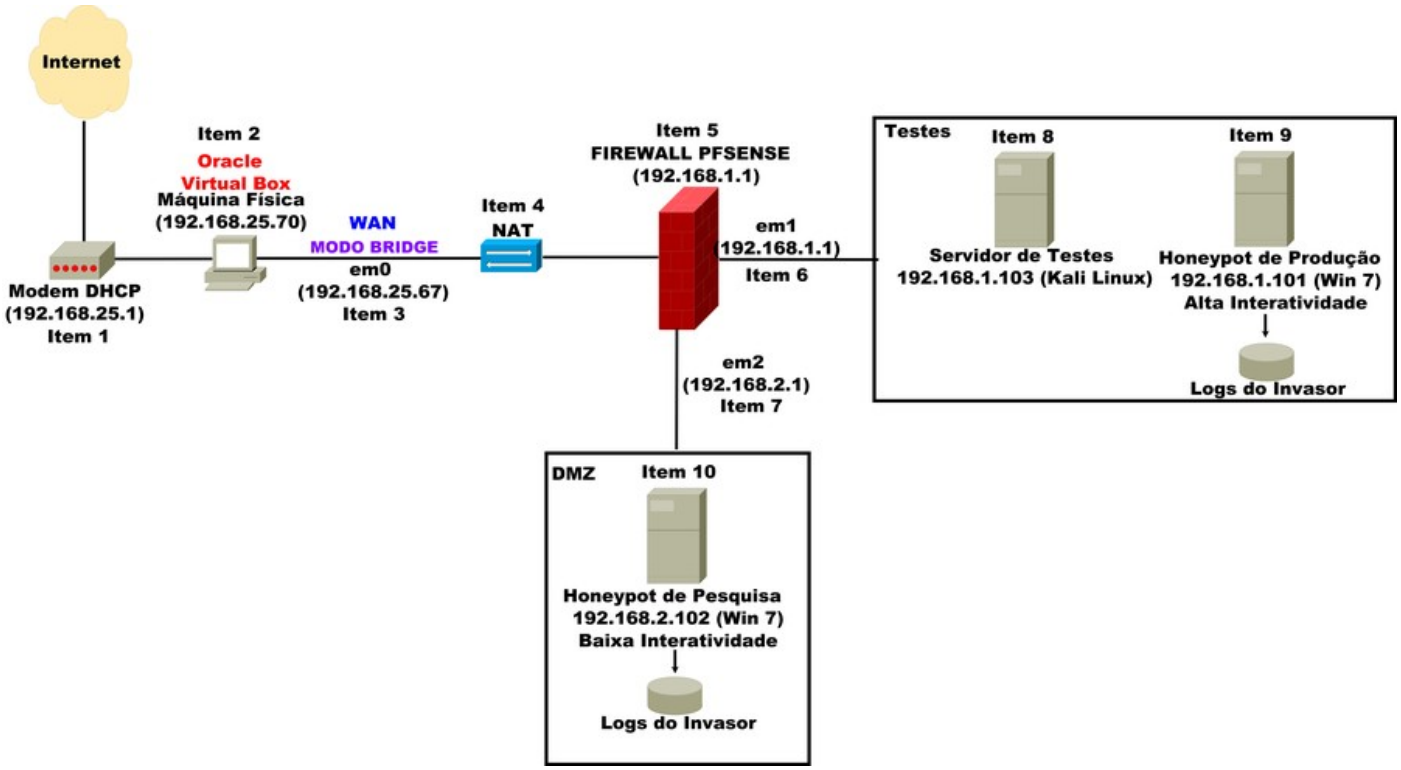

Figura 4. Honeynet Virtual

Fonte: Do autor (2018)

O *virtual box* foi configurado na máquina física (item 2) para criar a estrutura da *honeynet virtual*. A interface *Wan* (item 3) recebeu seu endereço IP automaticamente, de acordo com a faixa de endereços IP do Modem *DHCP* (item 1). As *interfaces* de comunicação com as redes Testes e *DMZ*, respectivamente em1 (item 6) e em2 (item 7), receberam endereços IP estáticos. O controle do tráfego de dados foi realizado pelo *firewall (item 5)*. O NAT (item 4) fez a tradução automática de endereços, permitindo que as máquinas das redes Testes e DMZ obtivessem acesso à *internet* através de endereço IP único. O servidor de testes (item 8) foi responsável pelo mapeamento de serviços comprometidos dos honeypots e invasão ao honeypot de pesquisa (item 10). A máquina física foi responsável pela invasão ao *honeypot* de produção (item 9).

4.3. Configuração das Máquinas

A tabela 1 apresenta as configurações das máquinas pertencentes à honeynet:

Tabela 1. Máquinas e suas configurações

Fonte: Do autor (2018)

Máquinas	**Configurações**
Máquina Física	Processador com 8 núcleos, 8 GB de memória RAM, 220 GB de HD e 3 i*nterfaces* virtuais de rede (em0, em1 e em2). Sistema Operacional Windows 10
Servidor de Testes	Processador com 2 núcleos, 2 GB de memória RAM, 16 GB de HD. Sistema Operacional Kali Linux com o *scanner* de rede *Nmap* 7.60 e o Filezilla Client 3.33.0
Honeypot de Produção	Processador com 2 núcleos, 1 GB de memória RAM, 32 GB de HD. Sistema Operacional Windows 7 com o *Honeypot Valhala* 1.9
Honeypot de Pesquisa	Processador com 2 núcleos, 1 GB de memória RAM, 32 GB de HD. Sistema Operacional Windows 7 com o *Honeypot Valhala* 1.9
Firewall Pfsense	Processador com 2 núcleos, 1 GB de memória RAM, 16 GB de HD. *Firewall Pfsense* 2.4.3 baseado no Sistema Operacional *FreeBSD*

4.4. Controle de dados

As regras de controle de tráfego de dados foram definidas no *pfsense* e no firewall dos sistemas operacionais dos *honeypots:*

NAT Port Forward. Fez o roteamento de pacotes da máquina física para a porta 23 do honeypot de produção.

Acesso Irrestrito à Internet para o Servidor de Testes. Permitiu o mapeamento de serviços dos *honeypots* e acesso à porta 21 do *honeypot* de pesquisa.

Isolamento do *Honeypot* de Pesquisa. O *honeypot* de pesquisa não teve acesso à rede *LAN*, impedindo que as vulnerabilidades fossem exploradas para acesso a outros locais da rede.

Liberação de Portas *ICMP* dos *Honeypots*. Permitiu que o *Nmap* exibisse o diagnóstico completo dos serviços disponíveis nos *honeypots;*

Liberação de Portas *TCP* dos *Honeypots*. Acréscimo de portas abertas, aumentando a vulnerabilidade dos *honeypots.*

5. TESTES DE VULNERABILIDADE COM O HONEYPOT VALHALA

Os testes de vulnerabilidade foram reproduzidos a partir de um cenário hipotético de invasão. O *valhala* foi ativado e configurado nos *honeypots* de pesquisa e produção para receber, respectivamente, conexões via *FTP* e *TELNET*. O suposto invasor utilizou o *scanner* de redes *nmap* para fazer a varredura de máquinas ativas, serviços comprometidos e executar um ataque por *brute force*, atuando na descoberta das credenciais do *honeypot* de pesquisa. O *honeypot* de produção foi configurado para conceder acesso sem a necessidade de credenciais. As ações registradas pelo valhala foram armazenadas em logs e serviram para o estudo do perfil do atacante.

5.1. Serviço de alta interatividade

A Figura 5 representa o mapeamento do *honeypot* de pesquisa e os serviços comprometidos.

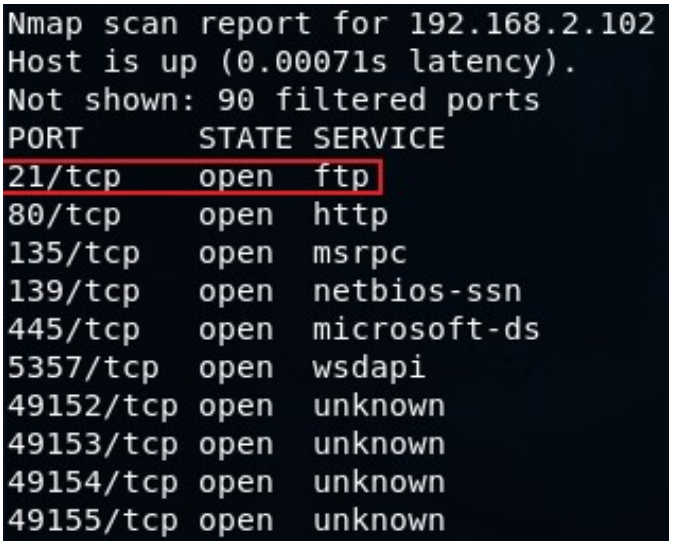

Figura 5. Honeypot de pesquisa e os serviços comprometidos

Fonte: Do autor (2018)

A identificação do endereço IP e a porta permitiram o ataque por *brute force*, caracterizado pela tentativa automatizada de detecção de *logins* e senhas. Como pode ser observado na Figura 6, foram feitas 58.042 tentativas visando a descoberta de credenciais válidas (admin:admin) para acesso ao servidor *FTP* na porta 21.

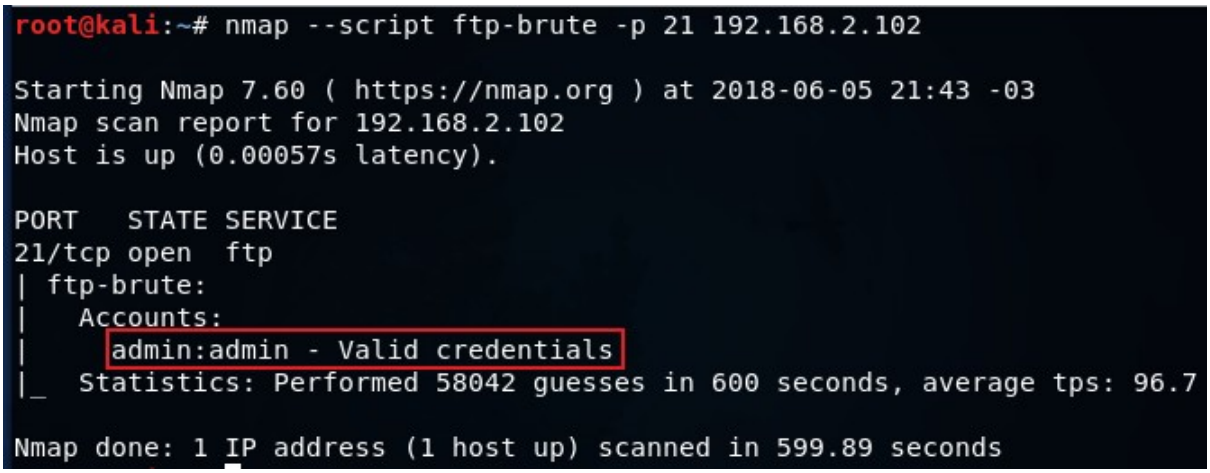

Figura 6. Resultado do *brute force*

Fonte: Do autor (2018)

A Figura 7 representa o *log* gerado pelo valhala após a execução do ataque por brute force. É possível identificar informações como horário do ataque, endereço IP do invasor, serviço comprometido e as tentativas de acerto.

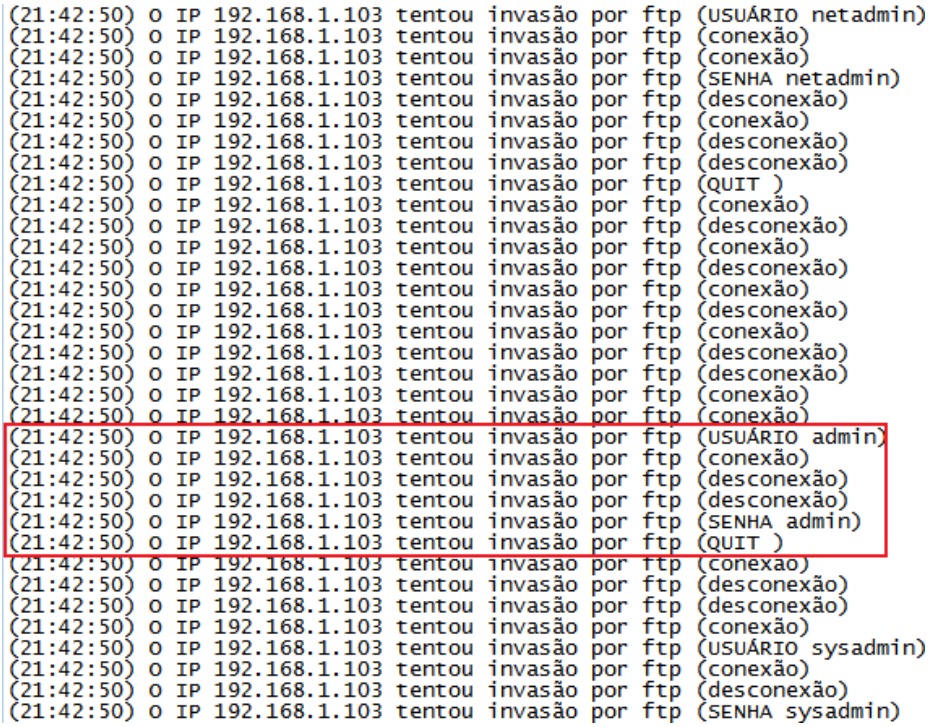

Figura 7. Log de registros - *brute force*

Fonte: Do autor (2018)

A descoberta das credenciais possibilitou o acesso ao servidor *FTP* através da ferramenta *filezilla client*. A análise do log representado pela Figura 8 permite concluir que, após a autenticação, o suposto invasor obteve o controle das pastas e arquivos. O valhala registrou comandos como criação de diretório (*MKD*), alteração de nome de diretório (*RNFR/RNTO*), envio de arquivo (ENVIAR) e exclusão de diretório (*RMD*), determinando o controle de um sistema real.

```
(07:29:28) O IP 192.168.1.103 tentou invasão por ftp (AUTH TLS)
(07:29:28) O IP 192.168.1.103 tentou invasão por ftp (AUTH SSL)
(07:29:28) O IP 192.168.1.103 tentou invasão por ftp (USUARIO admin)
(07:29:28) O IP 192.168.1.103 tentou invasão por ftp (SENHA admin)
(07:29:28) O IP 192.168.1.103 tentou invasão por ftp (SYST )
(07:29:28) O IP 192.168.1.103 tentou invasão por ftp (FEAT )
(07:29:28) O IP 192.168.1.103 tentou invasão por ftp (PWD )
(07:29:28) O IP 192.168.1.103 tentou invasão por ftp (BINARIO)
(07:29:28) O IP 192.168.1.103 tentou invasão por ftp (PASV )
(07:29:28) O IP 192.168.1.103 tentou invasão por ftp (MLSD )
(07:29:46) O IP 192.168.1.103 tentou invasão por ftp (MKD Importante)
(07:29:46) O IP 192.168.1.103 tentou invasão por ftp (PASV )
(07:29:46) O IP 192.168.1.103 tentou invasão por ftp (MLSD )
(07:29:48) O IP 192.168.1.103 tentou invasão por ftp (DIRETORIO /c:/Importante)
(07:29:48) O IP 192.168.1.103 tentou invasão por ftp (PWD )
(07:29:48) O IP 192.168.1.103 tentou invasão por ftp (PASV )
(07:29:48) O IP 192.168.1.103 tentou invasão por ftp (MLSD )
(07:29:54) O IP 192.168.1.103 tentou invasão por ftp (DIRETORIO /c:)
(07:29:54) O IP 192.168.1.103 tentou invasão por ftp (PWD )
(07:30:25) O IP 192.168.1.103 tentou invasão por ftp (RNFR Importante)
(07:30:25) O IP 192.168.1.103 tentou invasão por ftp (RNTO Essencial)
(07:30:25) O IP 192.168.1.103 tentou invasão por ftp (PASV )
(07:30:25) O IP 192.168.1.103 tentou invasão por ftp (MLSD )
(07:30:25) O IP 192.168.1.103 tentou invasão por ftp (DIRETORIO /c:/Essencial)
(07:30:25) O IP 192.168.1.103 tentou invasão por ftp (PWD )
(07:30:25) O IP 192.168.1.103 tentou invasão por ftp (PASV )
(07:30:25) O IP 192.168.1.103 tentou invasão por ftp (MLSD )
(07:31:24) O IP 192.168.1.103 tentou invasão por ftp (PASV )
(07:31:24) O IP 192.168.1.103 tentou invasão por ftp (ENVIAR install.exe)
(07:32:28) O IP 192.168.1.103 tentou invasão por ftp (DIRETORIO /c:)
(07:32:28) O IP 192.168.1.103 tentou invasão por ftp (PWD )
(07:32:28) O IP 192.168.1.103 tentou invasão por ftp (RMD Essencial)
(07:32:28) O IP 192.168.1.103 tentou invasão por ftp (PASV )
```

Figura 8. Log de registros - Invasão ao FTP

Fonte: Do autor (2018)

5.2. Serviço de baixa interatividade

A Figura 9 representa o mapeamento do *honeypot* de produção e os serviços comprometidos.

```
Nmap scan report for 192.168.1.101
Host is up (0.00027s latency).
Not shown: 90 filtered ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
```

Figura 9. Honeypot de produção e os serviços comprometidos

Fonte: Do autor (2018)

A comunicação entre a máquina física (192.168.25.70) e o *honeypot* de produção (192.168.1.101) foi possível através da tradução automática de endereços, fazendo-se necessária a criação de uma regra de roteamento do tipo *port forward*. O *NAT* alterou as informações contidas no cabeçalho do pacote (IP e porta de origem) para que ele pudesse trafegar até o destino, com IP e porta válidos na rede interna. Antagonicamente ao ataque por *brute force*, não foi necessário utilizar qualquer mecanismo para descoberta de credenciais. A Figura 10 mostra o *shell* simulado do MS-DOS, determinando o controle de um sistema fictício. As informações visualizadas pelo atacante foram previamente inseridas na *interface* de configurações do serviço *FTP*. É importante salientar que os serviços de baixa interatividade são facilmente detectados por usuários mais experientes.

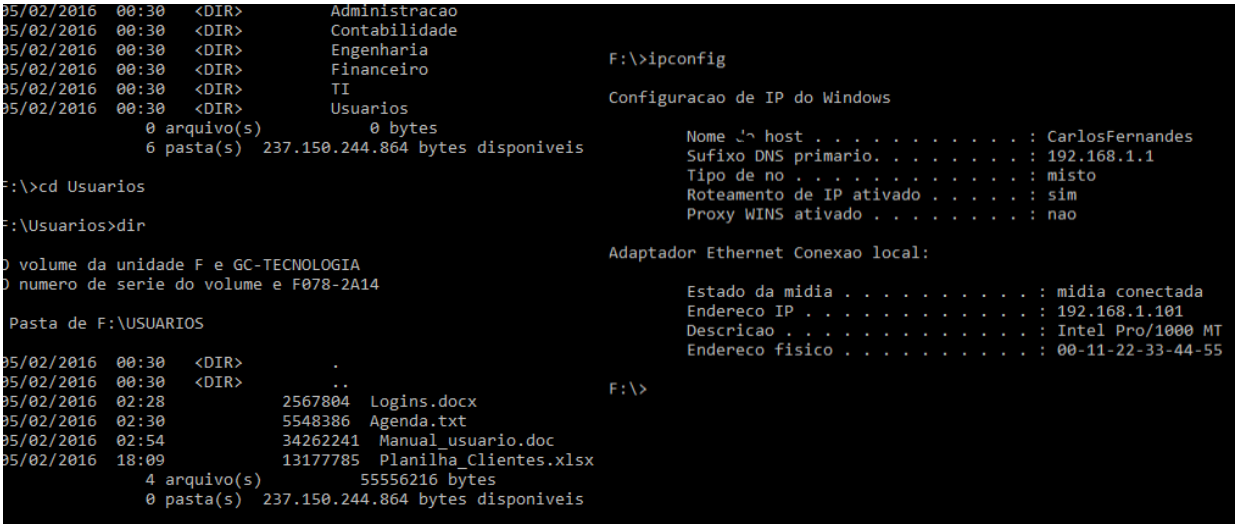

Figura 10. *Shell* Simulado

Fonte: Do autor (2018)

O valhala foi configurado para limitar os comandos do invasor, desconectando-o após o quarto comando. As ações do invasor foram registradas no arquivo log e podem ser verificadas na Figura 11.

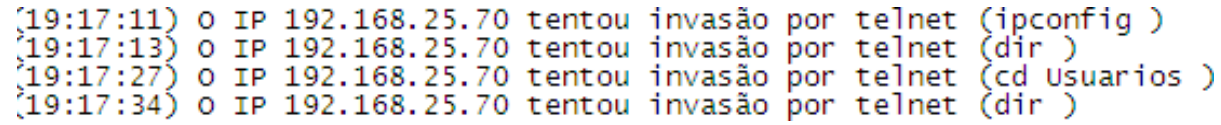

Figura 11. Log de registros – Invasão ao TELNET

Fonte: Do autor (2018)

6. CONSIDERAÇÕES FINAIS

A eficácia dos *honeypots* depende da implementação por profissionais da área, com amplos conhecimentos em infraestrutura de rede, sistemas de segurança e sistemas operacionais. Os ambientes reproduzidos mostraram diferentes características, tornando fundamental a análise do contexto de aplicação, considerando riscos, custos e a necessidade da organização. Embora o serviço de alta interatividade tenha produzido um resultado mais satisfatório e informações de maior relevância, apresenta risco elevado por se tratar de um ambiente real.

A captura de eventos e dados possibilitou uma análise mais detalhada do suposto invasor, identificando fatores comportamentais e o tipo de ferramenta utilizada, contribuindo na prevenção de futuros ataques.

Referências

ABNT (2005). *ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação*. Rio de janeiro, 1 edition.

Assunção, M. F. A. (2009). *Honeypots e Honeynets: Aprenda a detectar e enganar os invasores*. Visual Books.

Coelho, F. E. S., de Araújo, L. G. S., e Bezerra, E. K. (2014). *Gestão da segurança da informação : NBR 270001 e NBR 27002*. RNP/ESR.

Damasceno, L. (2005). *PFsense*.

de Moraes, A. F. (2005). *Firewalls - Segurança no Controle de Acesso*. Érica, 1 edition.

Dunlap, G. W., King, S. T., Cinar, S., Basrai, M. A., e Chen (2002). Revirt: Enabling intrusion analysis through virtual-machine logging and replay. In Proceedings of the 5th Symposium on Operating Systems Design and Implementation (OSDI).

Fu, S. e Xu, C. (2005). Service migration in distributed virtual machines for adaptive grid computing. In 34th IEEE Intl Conference on Parallel Processing.

HelpDigital (2017). O que é uma rede LAN e uma rede WAN?

Hoepers, C., Steding-Jessen, K., e Chaves, M. H. P. C. (2007). Honeypots e Honeynets: Definições e Aplicações.

Laureano, M., Maziero, C., e Jamhour, E. (2007). *Protecting host-based intrusion detectors through virtual machines*, volume 51. Computer Networks.

LeVasseur, J., Uhlig, V., Stoess, J., e Götz, S. (2004). Unmodified device driver reuse and improved system dependability via virtual machines. In Proceedings of the 6th Symposium on Operating Systems Design and Implementation.

Marcelo, A. e Pitanga, M. (2003). *Honeypots: a arte de iludir hackers*. Brasport, Rio de Janeiro.

Newman, M., Wiberg, C., e Braswell, B. (2005). Server Consolidation with VMware ESX Server. *IBM RedBooks*.

Rosenblum, M. e Garfinkel, T. (2005). Virtual machine monitors: current tecnology and future trends. *IEEE Computer Magazine*.