CEFET/RJ
campus Nova Friburgo

IMPLEMENTAÇÃO E ANÁLISE DE TÉCNICAS DE HARDENING EM SERVIDORES DE HOSPEDAGEM

Alexandre Pontes Donato

Monografia apresentada ao Curso de Graduação em Sistemas de Informação, do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, CEFET/RJ Campus Nova Friburgo, como parte dos requisitos necessários à obtenção do certificado de Bacharel em Sistemas de Informação.

Orientador(a): Nilson Mori Lazarin

Rio de Janeiro
Março de 2022

IMPLEMENTAÇÃO E ANÁLISE DE TÉCNICAS DE HARDENING EM SERVIDORES DE HOSPEDAGEM

Monografia apresentada ao Curso de Graduação em Sistemas de Informação, do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, CEFET/RJ Campus Nova Friburgo, como parte dos requisitos necessários à obtenção do certificado de Bacharel em Sistemas de Informação.

Alexandre Pontes Donato

Banca Examinadora:

NILSON MORI LAZARIN:72809353115

Assinado de forma digital por NILSON MORI LAZARIN:72809353115
DN: cn=NILSON MORI LAZARIN:72809353115, ou=CEFET-RJ - Centro Fed. Educ. Tecnol. Celso S. Fonseca, o=ICPEdu, c=BR
Dados: 2022.05.12 18:49:22 -03'00'

Presidente, Professor Me. Nilson Mori Lazarin (CEFET/RJ) (orientador)

gov.br
Documento assinado digitalmente
BRUNO POLICARPO TOLEDO FREITAS
Data: 12/05/2022 16:20:08-0300
Verifique em https://verificador.iti.br

Professor Me. Bruno Policarpo Toledo Freitas (CEFET/RJ)

HELGA DOLORICO BALBI:09599358783

Assinado de forma digital por HELGA DOLORICO BALBI:09599358783
Dados: 2022.05.11 16:35:11 -03'00'

Professora Dra. Helga Dolorico Balbi (CEFET/RJ)

Rio de Janeiro

Março de 2022

CEFET/RJ – Sistema de Bibliotecas / Biblioteca Uned Nova Friburgo

D677i Donato, Alexandre Pontes.
Implementação e análise de técnicas de Hardening em servidores de hospedagem / Alexandre Pontes Donato. — 2022.
37f.; fig. (color.) : em PDF.

Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) - Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, 2022.
Bibliografia: f. 36 - 37.
Orientador: Nilson Mori Lazarin.

1. Sistemas de Informação. 2. Proteção de dados. 3. Segurança de dados – computação. 4.Servidores web. I. Lazarin, Nilson Mori (orientador) III. Título.

CDD 658.4038

Elaborada pela bibliotecária Cristina Rodrigues Alves CRB7/5932

RESUMO

IMPLEMENTAÇÃO E ANÁLISE DE TÉCNICAS DE HARDENING EM SERVIDORES DE HOSPEDAGEM

Com o avanço das tecnologias e da globalização, as pessoas estão cada vez mais conectadas à Internet, utilizando serviços, consumindo e produzindo conteúdo. A segurança de todos os dados produzidos e consumidos por todos é mais importante do que nunca. A partir disso, a proteção dos servidores de hospedagem que armazenam os dados utilizados por todos em suas relações diárias passa a ser prioridade, uma vez que um ataque impede os servidores de operarem corretamente ou rouba os dados, toda uma cadeia de produção e consumo é afetada com repercussões trágicas. Buscando melhorias na segurança este trabalho objetiva desenvolver uma configuração capaz de proteger os servidores de hospedagem de vários tipos de ataque através da implementação e análise de técnicas de hardening. Foram realizados quatro testes utilizando as ferramentas Kali Linux, Intrusion Prevention System(*IPS*), Web Application Firewall(*WAF*) e Metasploitable e os resultados mostraram que a configuração utilizando o WAF foi a mais eficiente na proteção do servidor de hospedagem.

Palavras-chave: Servidor de hospedagem, Segurança, Proteção

ABSTRACT

IMPLEMENTAÇÃO E ANÁLISE DE TÉCNICAS DE HARDENING EM SERVIDORES DE HOSPEDAGEM

With the advancement of technologies and globalization, people are increasingly connected to the Internet, using services, consuming and producing content. The security of all data produced and consumed by everyone is more important than ever. Consequently, the protection of the hosting servers that store the data used by everyone in their daily relationships becomes a priority, since an attack prevents the servers from operating correctly or steals data on them, the entire chain of production and consumption can be affected with tragic repercussions. Seeking security improvements, this work aims to develop a configuration capable of protecting hosting servers from various types of attack through the implementation and analysis of hardening techniques. Four tests were carried out using the Kali Linux, IPS(*Intrusion Prevention System*), WAF (*Web Application Firewall*) and Metasploitable tools and the results showed that the configuration using WAF was the most efficient in protecting the hosting server.

Keywords: Hosting server; Security; Protection

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

Introdução

De acordo com o *Global Cybersecurity Index* (CGI), 3.5 bilhões de pessoas estão conectadas com o mundo virtual atualmente e riscos à segurança cibernética são uma questão importante que não recebe atenção necessária no Brasil. Uma das medidas propostas pelo CGI é a implementação de uma legislação capaz de identificar as atividades ilegais praticadas online, acompanhada do procedimento necessário para investigar, processar e reforçar essa legislação (ITU, 2020).

No Brasil está vigente a Lei Geral de Proteção de Dados (LGPD), que regula o armazenamento, utilização e proteção dos dados a todos que tratem dados pessoais de forma online ou off-line, abrangendo dessa forma várias atividades empresariais.

Entre os princípios gerais da proteção de dados pessoais estão o princípio da segurança que prevê a utilização de medidas técnicas e administrativas para proteger os dados de acessos não autorizados ou situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, e o princípio de responsabilização e prestação de contas que determina que o possuidor dos dados pessoais seja capaz de demonstrar a adoção de medidas de segurança que protejam os dados, comprovando o cumprimento das determinações da lei e da eficácia das medidas.

Na categoria de crimes cibernéticos, alguns casos que merecem destaque são o Stuxnet (2009-2010): Primeiro vírus capaz de causar danos off-line. Foi capaz de danificar armas nucleares iranianas, desconfigurando toda a operação a atrasando em aproximadamente dois anos (Bertholdi, 2020).

Netsky & Sasser Vírus (2004): Um adolescente alemão foi responsável por espalhar 70% de todo o malware no ano de 2004. Entre os danos causados estão a suspensão do serviço ferroviário da Austrália, fechamento de 130 agências do Sampo Bank da Finlândia e o cancelamento de vários voos transatlânticos da Delta AirLines. A Microsoft pagou US$ 250.000 por informações que levassem à captura de Janschen (Bertholdi, 2020).

No Brasil, a demora na implementação de políticas públicas voltadas ao cibercrime produziu um custo relatado pela Polícia Federal. Em 2004, oito em cada dez hackers do mundo viviam no Brasil. Também de acordo com a Polícia Federal, os crimes cibernéticos movimentam mais dinheiro que o narcotráfico (Bertholdi, 2020).

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no

Brasil (CERT.br) é mantido pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), organização privada sem fins lucrativos que implementa decisões do Comitê Gestor da Internet no Brasil (CGI.br). O CERT.br tem como objetivo prover mais segurança e possibilitar procedimentos eficientes para os incidentes de redes conectadas à Internet no Brasil (NIC.br, 2022).

Figura 1 ilustra a quantidade de incidentes de segurança reportados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) de 1999 a 2020. Por ela, percebe-se uma tendência de aumento constante do número de incidentes no decorrer dos anos (CERT.br, 2021).

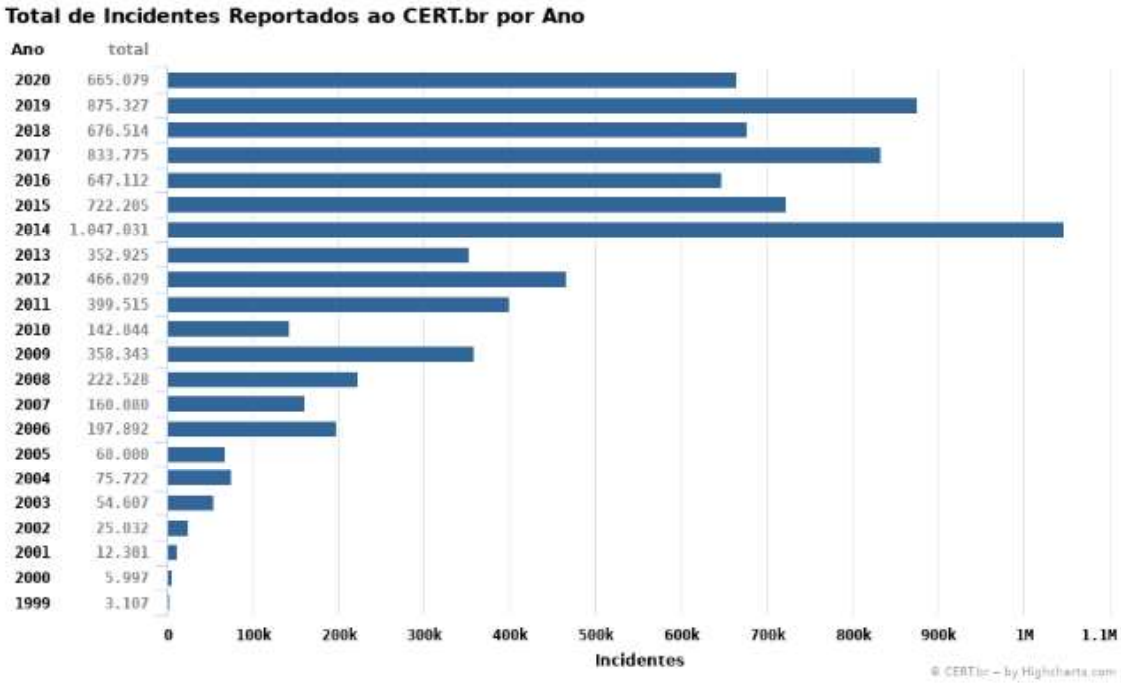

Figura 1 - Incidentes reportados aos CERT.br por ano (CERT.br, 2021)

1.1 Definição do Problema

De acordo com (HYPPÖNEN, 2021), um ataque é uma tentativa de romper ou fugir da segurança dos computadores ou redes de computadores. Os ataques podem ser divididos em passivos ou ativos. Um ataque passivo tenta escutar, espionar e aprender sobre um determinado sistema. Alguns ataques ocorrem sem que os sistemas atacados saibam que o ataque está ocorrendo, podendo ser executado como homem do meio, interceptando as comunicações entre cliente e servidor. Exemplos de ataques ativos são o *Denial-of-service* (*DoS*) e de força bruta. O primeiro tenta

sobrecarregar o servidor de requisições para que este não consiga responder os solicitantes e interrompa a comunicação e prestação do serviço, e o segundo tenta invadir a máquina servidora ou a rede de servidores com o intuito de extrair dados ou corromper a estrutura da rede.

Os principais incidentes de segurança reportados ao CERT.BR são:

- Scan: varredura em rede de computador que identifica as máquinas e os serviços disponíveis para descobrir vulnerabilidades com essas informações;
- Worm: disseminação de código malicioso na rede;
- DoS (*Denial of Service*): negação de serviço. Um atacante utiliza de várias máquinas para interromper o fornecimento de um determinado serviço da rede;
- Fraude: tentativa de obter algum tipo de vantagem;
- Web: ataque que objetiva danificar os serviços de um servidor web;
- Invasão: acesso não autorizado a um computador por um agente externo.

De acordo com o CERT.br, o *Scan* foi o tipo de ataque com maior incidência. A partir disso, o CERT.br determinou quais portas foram mais atacadas utilizando o protocolo tcp (CERT.br, 2021). A seguir, pode ser vista uma lista com as portas que receberam o maior número de ataques em ordem decrescente:

- 22 - SSH
- 25 - SMTP
- 3389 – Microsoft Terminal Server (RDP)
- 23 – Telnet Protocol
- 465 – SMTP over SSL
- 6379 - redis
- 143 - IMAP4
- 8291 - Winbox - Default port on a MikroTik RouterOS for a Windows application used to administer MikroTik RouterOS
- 8728 - mikrotik
- 443 - HTTPS - HTTP Protocol over TLS/SSL

1.2 Motivação

Com o avanço do desenvolvimento tecnológico, se torna cada vez mais importante garantir a segurança das máquinas servidoras uma vez que essas armazenam os dados e permitem a utilização dos diversos serviços necessários atualmente.

Segundo Tanenbaum (2003), grande parte dos problemas relacionados à segurança é provocada intencionalmente por pessoas que tentam obter algum benefício, chamar atenção ou prejudicar alguém. Isso mostra que uma rede de computadores, seja ela doméstica ou corporativa, para estar segura, não basta que esteja livre de erros de programação.

Segundo (PINHEIRO, 2017), os sistemas de segurança de informação devem seguir três princípios básicos: prevenção, detecção e recuperação. Ainda segundo José Maurício, quando uma invasão ocorre, a confiabilidade do sistema é colocada sob questionamento, assim como a capacidade de seu proprietário proteger os dados e manter seus serviços operacionais, o que pode ser desastroso para empresas que dependem da credibilidade de seus clientes e investidores para realizar seu trabalho de forma adequada.

Considerando os dados mostrados na Figura 1 e na Figura 2 logo abaixo, o número de incidentes relativos a invasões em redes só aumenta. Portanto, é cada vez mais importante implementar segurança em ambientes de servidores e, por isso, foi escolhido o tema de segurança para realizar o trabalho.

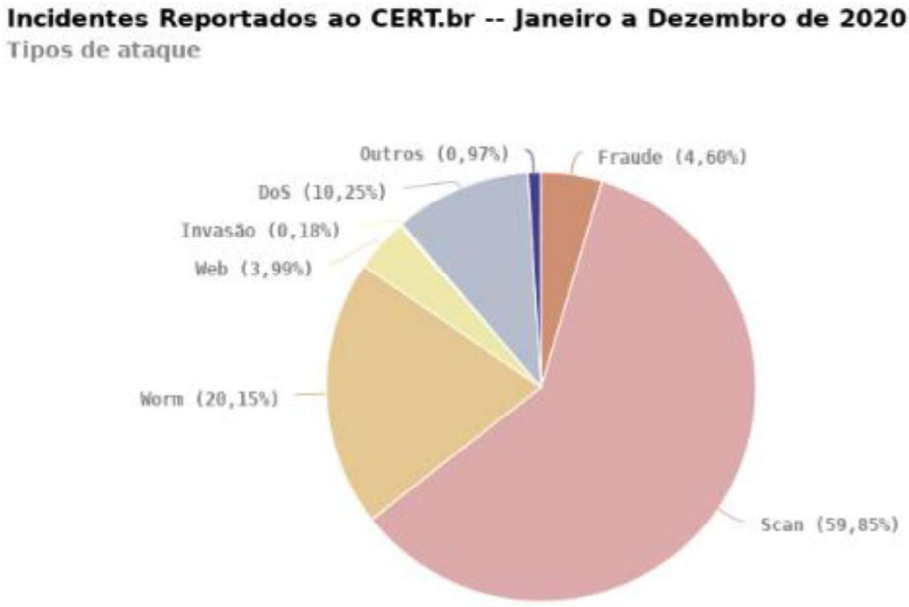

Figura 2 - Incidentes reportados ao CERT.br por tipo de ataque (CERT.br, 2021)

1.3 Contribuição

Este trabalho busca contribuir com o aumento da segurança de servidores de hospedagem através da análise de uma melhor configuração obtida por meio de testes utilizando a combinação de técnicas de *hardening,* que consiste no mapeamento de ameaças, na mitigação de riscos e na execução de atividades corretivas, utilizando as ferramentas IPS de camada 2 e o WAF de camada 7.

1.4 Estrutura do trabalho

No Capítulo 2, é apresentado o Referencial Teórico sobre as ferramentas utilizadas do desenvolvimento do trabalho.

No Capítulo 3, são abordados trabalhos relacionados.

No Capítulo 4, é apresentada a metodologia que foi utilizada para o desenvolvimento do trabalho.

No Capítulo 5 são apresentados os resultados dos experimentos realizados.

No Capítulo 6 é apresentada a conclusão.

2 Referencial Teórico

Nesta seção são apresentados os conceitos utilizados no trabalho.

2.1 Firewall

Segundo (TANENBAUM, Andrew S.; WETHERALL, David J., 2017) os firewalls são uma implementação cibernética dos fossos dos castelos medievais, uma vez que todos os que desejassem entrar no castelo deveriam passar por uma única entrada e serem revistados pelos guardas. Com as redes de computadores, é possível direcionar todo o tráfego para o firewall, que funcionará com um guarda, inspecionando e filtrando os pacotes. Se algum pacote não estiver de acordo com as especificações definidas para a rede, serão descartados.

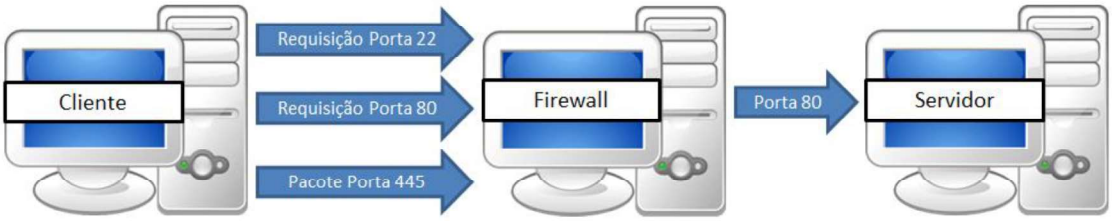

Figura 3 – Representação do funcionamento do Firewall

2.2 IPS

O Intrusion Prevention System (*IPS*) monitora o tráfego que chega da internet para determinar se existe algum comportamento fora do normal, de acordo com as configurações da rede. O IPS é capaz de bloquear o acesso caso identifique alguma anomalia e deve ser utilizado monitorando todo o tráfego da rede para que possa bloquear tentativas de invasão (ROHLING, 2020).

2.3 WAF

Web Application Firewall (*WAF*) é um sistema utilizado para proteger um servidor de ataques Hackers, Spammers, DDoS, Injeções de SQL etc. Funciona como proxy reverso posicionado à frente dos servidores web em uma infraestrutura de rede,

recebendo as requisições da rede externa e filtrando, de acordo com um conjunto de regras, quais requisições são seguras e podem ser encaminhadas ao servidor de destino e quais requisições contém ameaças à segurança da rede (MELCHIOR, 2019).

O WAF é um firewall que monitora a camada de aplicação, sendo capaz de decifrar as requisições para determinar se seu conteúdo não é malicioso. Além de monitorar o tráfego proveniente da internet, o WAF também é capaz de impedir requisições internas caso estejam fora das especificações definidas pelos administradores da rede (ROHLING, 2020).

2.4 Kali Linux

O Kali Linux é um sistema operacional baseado em Debian que tem o objetivo de realizar auditoria de segurança. Kali Linux possui várias ferramentas direcionadas para tarefas de pesquisa de segurança, engenharia reversa e forense digital e testes de penetração.

Kali Linux possui mais de 600 ferramentas para testes de penetração (OFFSEC SERVICES LIMITED, 2021). Neste trabalho, foram utilizadas as seguintes ferramentas:

- O Nmap[1] ("*Network Mapper*") é um utilitário usado para auditoria de segurança e descoberta de rede. O Nmap é capaz de descobrir máquinas disponíveis em determinada rede, quais serviços essas máquinas oferecem e quais sistemas operacionais elas possuem (NMAP.ORG).
- O Nikto[2] é um scanner para servidores web capaz de realizar testes para identificar arquivos ou programas perigosos à segurança do servidor, configuração incorreta do servidor e de aplicações, além de verificar se o servidor e os programas estão desatualizados (NIKTO).
- O ZAP[3] é uma ferramenta de teste de penetração mantida pelo *Open Web Application Security Project* (OWASP). O ZAP foi projetado para testar aplicações web. O ZAP é conhecido como homem do meio, se posicionando

[1] https://www.kali.org/tools/nmap/

[2] https://www.kali.org/tools/nikto/

[3] https://www.zaproxy.org/

entre o navegador de teste e a aplicação web, sendo capaz de interceptar e inspecionar as mensagens enviadas pelo navegador à aplicação, modificar o conteúdo das mensagens, se necessário, e em seguida enviar os pacotes para o destino (ZAPPROXY).

- O Armitage[4] é uma ferramenta do Kali Linux que possibilita a visualização de alvos, recomenda a exploração e exibe as informações sobre as máquinas exploradas em sua interface (Armitage).

2.5 Metasploitable

O Metasploitable é uma versão vulnerável do Ubuntu utilizada para testes de segurança, penetração e demonstração de fragilidades. Permite acesso a backdoors, senhas fracas e serviços web frágeis (RAPID7, 2021). Utilizando o Kali Linux e o utilitário Nmap, é possível listar todas as portas TCP de uma instância do metasploitable. A maior parte desses serviços permite um ponto de entrada para o sistema.

[4] https://www.kali.org/tools/armitage

3 Trabalhos Relacionados

Neste capítulo, serão apresentados trabalhos que serviram como base para elaboração do modelo proposto.

Estudo de caso sobre a implementação de técnicas de blindagem em servidores Linux baseada na detecção de vulnerabilidades e tentativas de intrusão

O trabalho de (SOUSA, Álisson et. al., 2020) tem como objetivo aumentar a segurança e diminuir as fraquezas de redes de servidores Linux. Para isso, foi realizado um estudo utilizando as ferramentas OpenVAS e Intrusion Detection System (IDS) Suricata, para detectar vulnerabilidades e tentativas de invasão na rede.

A rede utilizada para o experimento possui servidores de IP através de DHCP, servidores de nome de domínio (DNS) e servidores web acessíveis via internet. O escaneamento foi realizado pelo software OpenVAS que possui grande quantidade de testes de vulnerabilidade. Foram encontradas 27 vulnerabilidades sendo que alguns servidores apresentaram vulnerabilidades iguais. Dessa forma, foram encontradas 10 diferentes vulnerabilidades. Após a identificação das fraquezas, foram implementadas técnicas para corrigir esses problemas.

A ferramenta IDS Suricata foi utilizada de forma a monitorar os pacotes enviados e recebidos na rede visando encontrar tentativas de invasão nos servidores. Com a análise do relatório fornecido pela IDS Suricata, foi possível identificar que as tentativas de invasão eram do tipo *scans*, acesso remoto via SSH e *exploits*. Técnicas de proteção a esses tipos de invasão foram aplicadas de forma a melhorar a segurança dos servidores.

Com a utilização das ferramentas e técnicas descritas no artigo, foi possível aumentar a segurança dos servidores da rede em questão, ainda que a implementação dessas medidas seja complexa e demande tempo, será importante desenvolver uma ferramenta que execute toda essa proteção de forma automática.

As semelhanças do trabalho citado com o que foi realizado são o aprimoramento da segurança em servidores. As diferenças são que o no TCC foi utilizado o IPS, que além de reportar também bloqueia tentativas de acesso indevido e a inclusão do WAF para ampliar a proteção contra ataques aos servidores de hospedagem.

Ethical Hacking and Penetrate Testing using Kali and Metasploit Framework

O trabalho de (TABASSUM, Mujahid et. al., 2020), aborda o *hacking* ético, testes de invasão e experimentos práticos para informar jovens pesquisadores e estudantes sobre a implementação e uso da estrutura do Metasploit. Foram realizados experimentos tanto do lado do cliente como do lado do servidor para entender o processo. Foi utilizado o sistema operacional Kali Linux para complementar o hacking ético e os testes de invasão. O artigo explica detalhadamente os conceitos de hacker ético, teste de invasão e *reconnaissance*, outra forma de invasão conhecida e suas características.

O ambiente escolhido para realizar os ataques foi o de uma empresa e o objetivo era o de invadir o sistema da empresa para roubar informação confidencial. Para isso, foi utilizado o método de exploração pelo lado do cliente e pelo lado do servidor. O Metasploit foi usado para criar os dados que foram enviados para os laptops e telefones móveis da empresa. Para conseguir acesso do lado servidor, caso o acesso do lado cliente falhasse, foi necessário buscar informações sobre dispositivos móveis dos funcionários da empresa.

As formas de prevenção propostas são utilizar programas antivírus tais como Bitdefender, Kaspersky, e Norton, atualizar regularmente o sistema operacional para que falhas de segurança possam ser corrigidas e protejam o computador de ataques, bloquear portas não utilizadas, através de firewalls, de modo a dificultar o acesso aos computadores por invasores e implementar o *Intrusion Prevention System* (IPS) na rede para detectar ataques e prevenir invasões.

Como este artigo tem como objetivo educar e informar sobre a utilização do Metasploit e do Kali Linux já se diferencia do trabalho realizado neste TCC que objetiva criar uma configuração de segurança para servidores de hospedagem através de ferramentas como IPS e WAF. As semelhanças são o Metasploit e o Kali Linux, sistemas utilizados para implementação de ataques.

Security analysis of the Raspbian Linux operating system and its settings to increase resilience against attacks via network interface

O trabalho de (GALLUS, Petr.; FRANTIS, Petr., 2021) aborda configuração de

segurança do sistema operacional Raspbian Linux operando em endereços de IP públicos em ambiente de internet desprotegidos.

Foi realizado um experimento no qual cinco contas Raspbian Linux/Respberry PI foram criadas com uma variedade de níveis de segurança e conectadas à internet. Ferramentas foram utilizadas para monitorar o tráfego em busca de atividade suspeita, analisar esses dados para identificar ameaças e propor add-ons para segurança.

Os resultados do experimento conduziram a formulação de uma lista contendo mudanças ou melhorias recomendadas para qualquer usuário do Raspbian.

Este artigo tem um objetivo semelhante ao TCC quando se propõe a desenvolver medidas de segurança para um determinado ambiente, neste caso do sistema Rasbian Linux. As diferenças são as ferramentas utilizadas. No artigo foram os add-ons e no TCC foram o IPS e o WAF.

4 METODOLOGIA

O projeto consiste em implementar uma infraestrutura de rede contendo um Metasploitable, máquina contendo vulnerabilidades utilizada para diversos testes de penetração, uma máquina contendo WAF, uma máquina com IPS e uma máquina com Kai Linux, Sistema Operacional comumente utilizado para realizar ataques a outras máquinas contendo vários programas com diferentes características para invadir e prejudicar o funcionamento de servidores.

A partir dessa estrutura, serão realizados diversos testes para avaliar a segurança do servidor. Os testes serão realizados utilizando a máquina Kali Linux e tentando atacar a máquina Metasploitable, inicialmente sem a presença das máquinas com IPS e WAF e posteriormente adicionando esses sistemas e registrando os resultados das tentativas de invasão de forma a avaliar se a segurança aumenta.

No primeiro cenário, representado pela Figura 4 serão utilizados o Kali e o Metasploitable. Dessa forma ficarão evidentes as vulnerabilidades presentes na máquina Metasploitable que representa o servidor de hospedagem no ambiente proposto.

No segundo cenário, serão realizados dois testes, o primeiro incluindo o IPS para monitorar e impedir a chegada de requisições maliciosas do Kali Linux e no segundo será utilizado o WAF para filtrar as requisições na camada de aplicação.

O terceiro cenário terá o IPS e o WAF funcionando juntos para proteger o Metasploitable aumentando, dessa forma, a segurança do servidor de hospedagem de tentativas de invasão da máquina Kali Linux.

As figuras 5, 6 e 7 ilustram as configurações implementadas pelos experimentos.

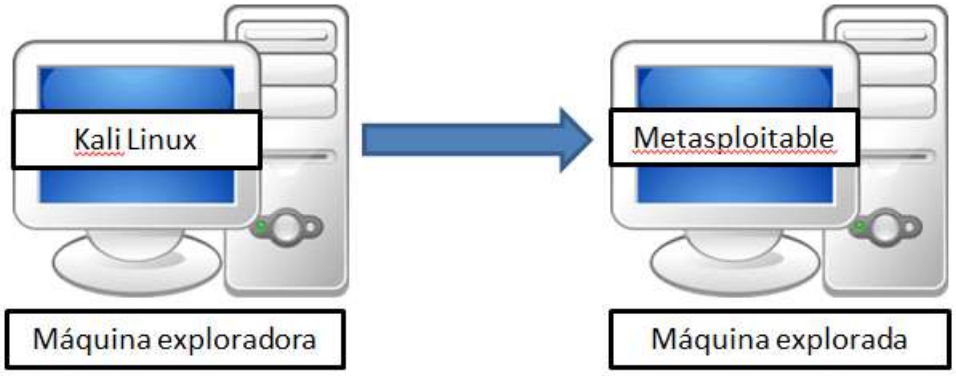

Figura 4 - Configuração do ambiente do experimento 1

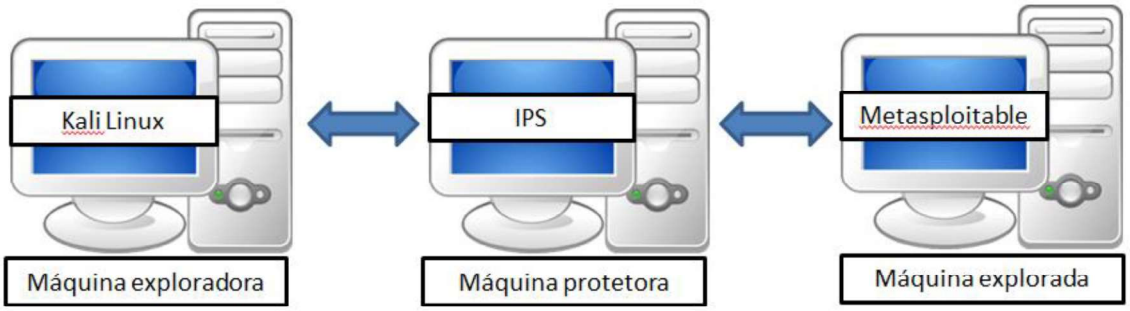

Figura 5 - Configuração do ambiente do experimento 2

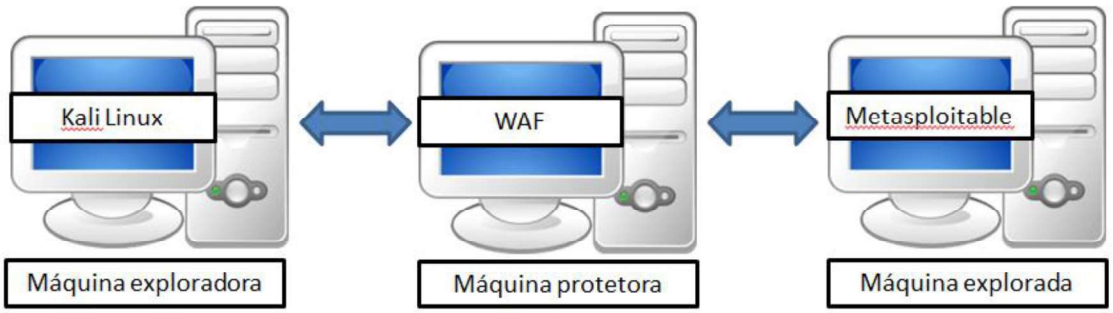

Figura 6 - Configuração do ambiente do experimento 3

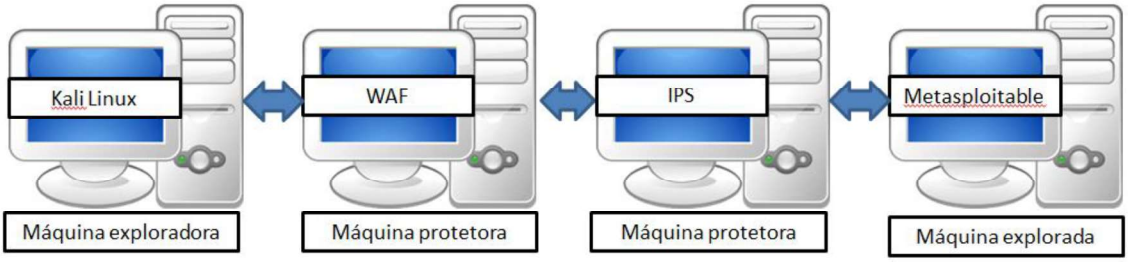

Figura 7 - Configuração do ambiente do experimento 4

5 Experimentos

Neste capítulo, são descritos os experimentos realizados nos cenários descritos no Capítulo 4.

5.1 Ataque direto ao Metasploitable

No primeiro teste, a máquina com o Metasploitable, sistema operacional Linux semelhante a uma distribuição para servidores, executando os serviços sem firewall ativo e com vulnerabilidades, simulando um servidor ligado diretamente à internet recebendo requisições dos usuários. A primeira verificação foi realizada com o Nikto que mostra as vulnerabilidades nas portas de diversos serviços de acordo com a Figura 8 descrita na Tabela 1. Os alertas encontrados pelo Nikto possuem os identificadores iniciando com as letras OSVDB que servem para demonstrar a gravidade das vulnerabilidades.

```
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific
QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific
QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific
QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific
QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 15:24:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3092: /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ 8726 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2022-01-17 16:46:17 (GMT-3) (21 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Figura 8 - Resultado do escaneamento do Nikto

Tabela 1 - Alertas encontrados pelo Nikto no experimento 1

ID	DESCRIÇÃO
OSVDB-877	HTTP TRACE method is active, the host is vulnerable to XST.
OSVDB-3268	/doc/: Directory indexing found.
OSVDB-48	The /doc/ directory is browsable. This may be /usr/doc.
OSVDB-12184	PHP reveals sensitive information via certain HTTP requests that contain specific QUERY strings.
OSVDB-3092	phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

OSVDB-3268	/icons/: Directory indexing found.
OSVDB-3233	PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
OSVDB-3233	/icons/README: Apache default file found. /phpMyAdmin/: phpMyAdmin directory found.
OSVDB-3092	/phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

Em seguida, foi realizada uma varredura com o ZAP, capaz de analisar requisições web e alterar seu conteúdo para identificar vulnerabilidades no Metasploitable. A Figura 9 mostra os alertas da varredura com o ZAP identificando os problemas mais graves com as bandeiras vermelhas, os problemas de nível médio com as bandeiras laranja, os problemas de nível baixo com as bandeiras amarelas e os informativos com as bandeiras azuis. A Tabela 2 traz a identificação de cada ocorrência encontrada pelo ZAP assim como o nível de risco e quantidade.

Figura 9 - Alertas obtidos após varredura do ZAP no experimento 1

Tabela 2 - Alertas do ZAP no experimento 1

ID	ALERTA	RISCO	QTD
6	Path Transversal	Alto	12
90022	Application Error Disclosure	Médio	256
10003	Biblioteca JS vulnerável	Médio	
10020-2	X-Frame-Options Header Not Set	Médio	4925
10202	Absence of Anti-CSRF Tokens	Baixo	6526
10010	Cookie No HttpOnly Flag	Baixo	20
10054	Cookie without SameSite Attribute	Baixo	30
10023	Information Disclosure – Debug Error Messages	Baixo	289

2	Private IP Disclousure	Baixo	138
10037	Server Leaks Information via “X-Powered-By” HTTP Response Header Field(s)	Baixo	117
10021	X-Content-Type-Options Header Missing	Baixo	5014
10024	Information Disclosure – Sensitive Information in URL	Informativo	9
10027	Information Disclousure – Suspicious Comment	Informativo	78
10096	Timestamp Disclosure – Unix	Informativo	1965

Por último, foi utilizado o Armitage que identificou uma fraqueza que foi explorada com vsftpd tendo sido possível acessar a máquina explorada através de um prompt de comando, visualizar arquivos em diretórios como o teste_invasao e identificar o usuário logado, nesse caso o root (administrador) como mostra a Figura 14. A Figura 10 mostra a interface do Armitage. A máquina explorada é exibida com o respectivo endereço IP na parte central e o exploit utilizado é listado do lado esquerdo destacado em vermelho.

A Figura 11 mostra a execução do ataque à máquina Metasploitable, a Figura 12 mostra a representação da máquina sob ataque, com raios ao seu redor, e abaixo o console exibindo o sucesso na execução do exploit.

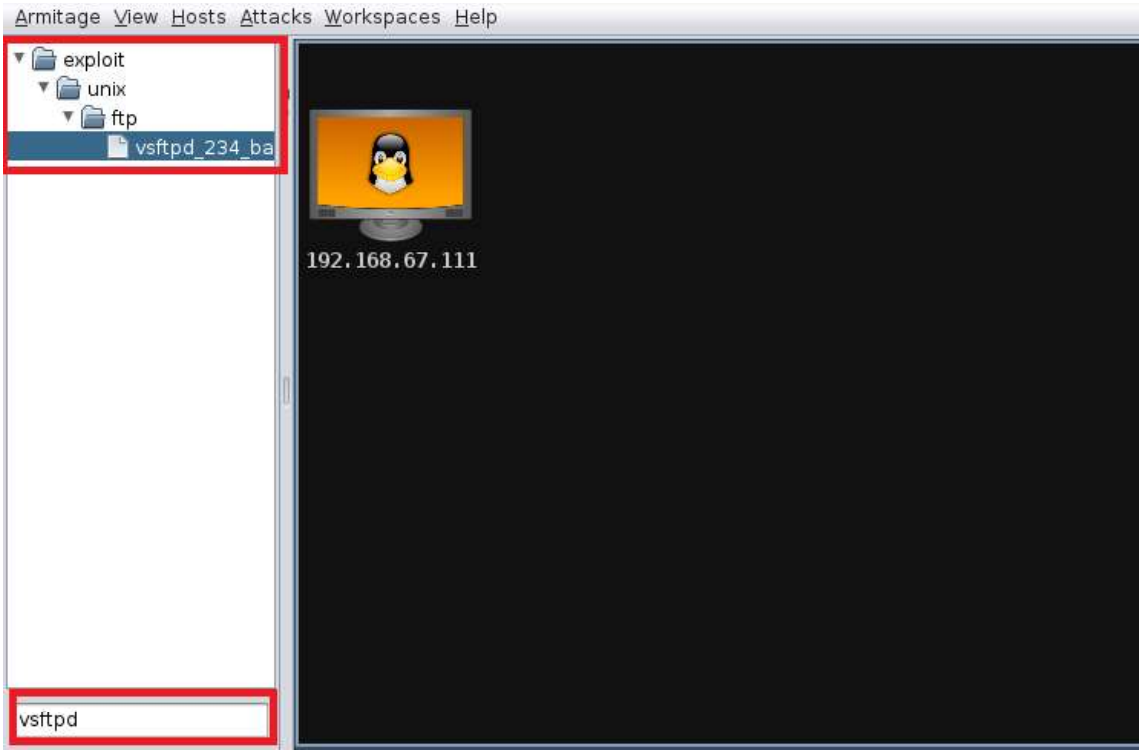

Figura 10 - Seleção do exploit usado no Armitage

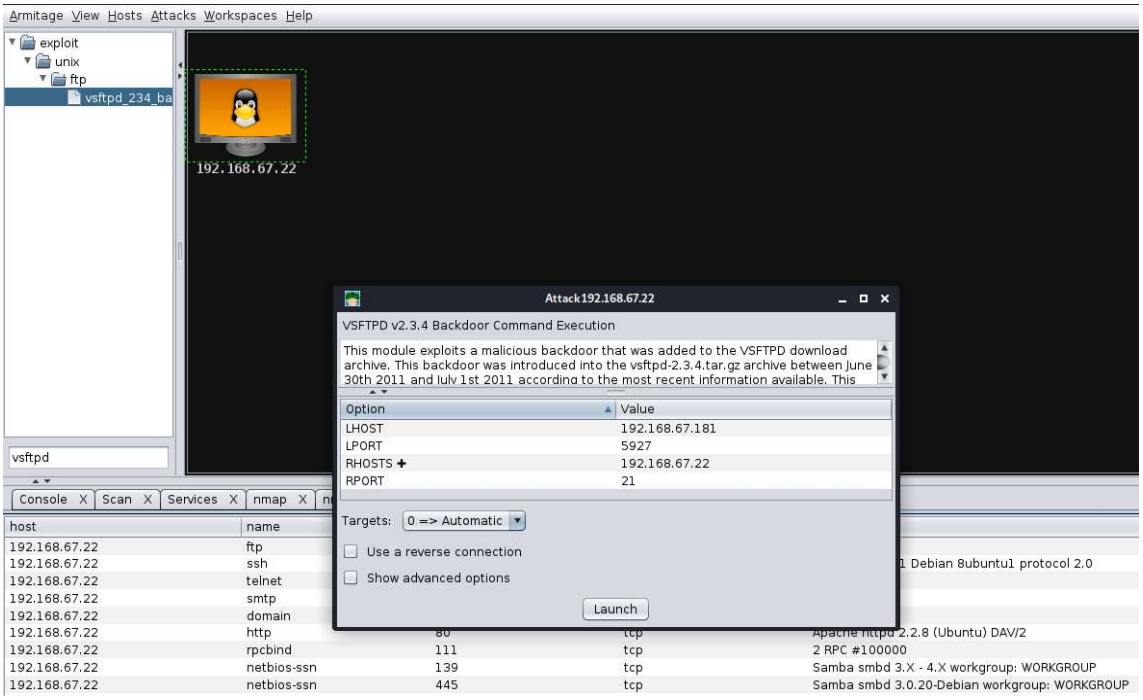

Figura 11 - Execução do ataque no Armitage

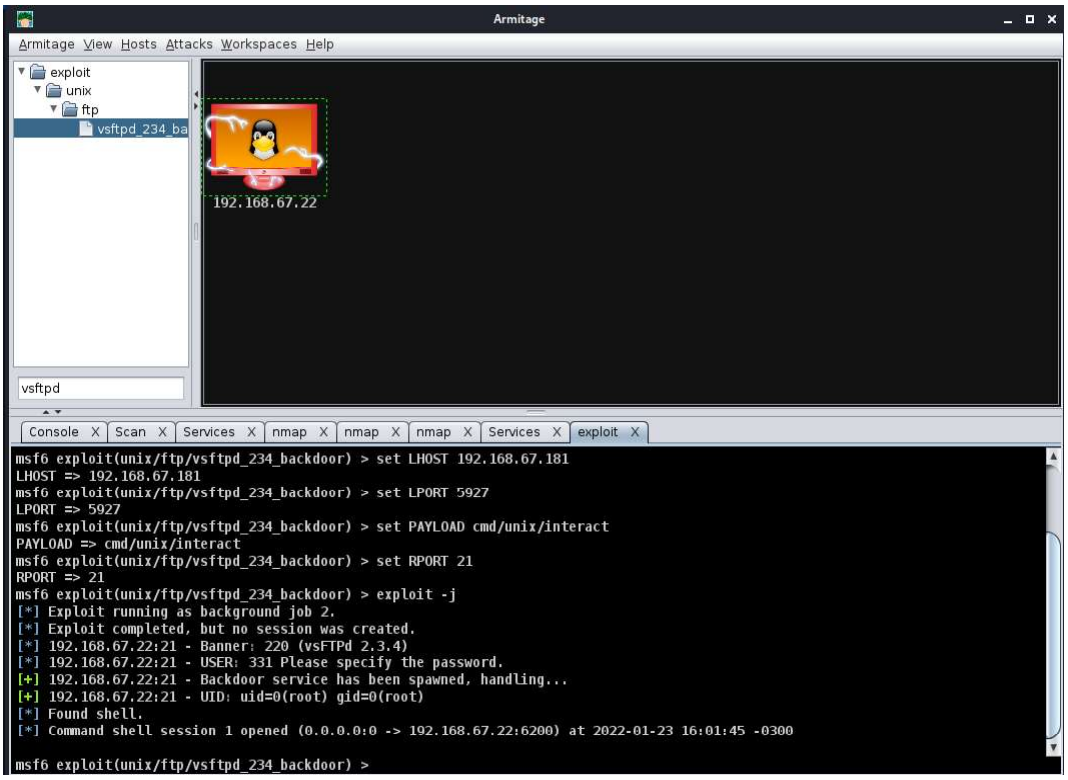

Figura 12 - Metasploitable invadido

Figura 13 - Arquivo na máquina Metasploitable

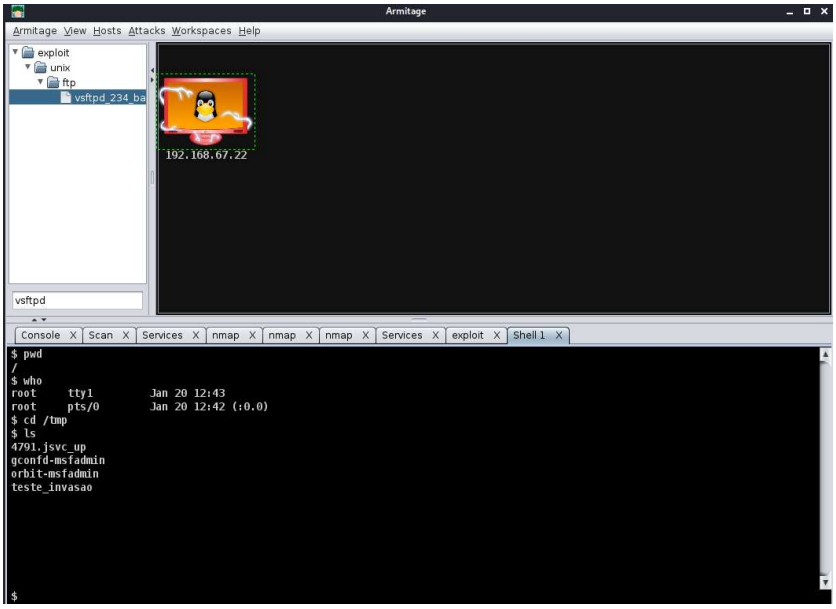

Figura 14 - Arquivo do Metasploitable acessado pelo Armitage

5.2 Ataque ao Metasploitable protegido por IPS

No segundo teste, foi incluído o IPS, aplicação que fará a análise das requisições para o Metasploitable detectando ameaças e impedindo que cheguem ao destino. Primeiro, foi realizado o teste com o Nikto, que já não foi capaz de listar as portas vulneráveis como no primeiro teste em função do IPS. A Figura 15 é o resultado da varredura com o Nikto no experimento 2, na Tabela 3 são exibidos alertas encontrados pelo Nikto porém, diferentemente do experimento 1 que encontrou vulnerabilidades que apresentam um risco maior à segurança da máquina Metasploitable, o segundo teste, com a inclusão do IPS, limitou o Nikto a apenas alguns alertas de menor risco à segurança da máquina explorada.

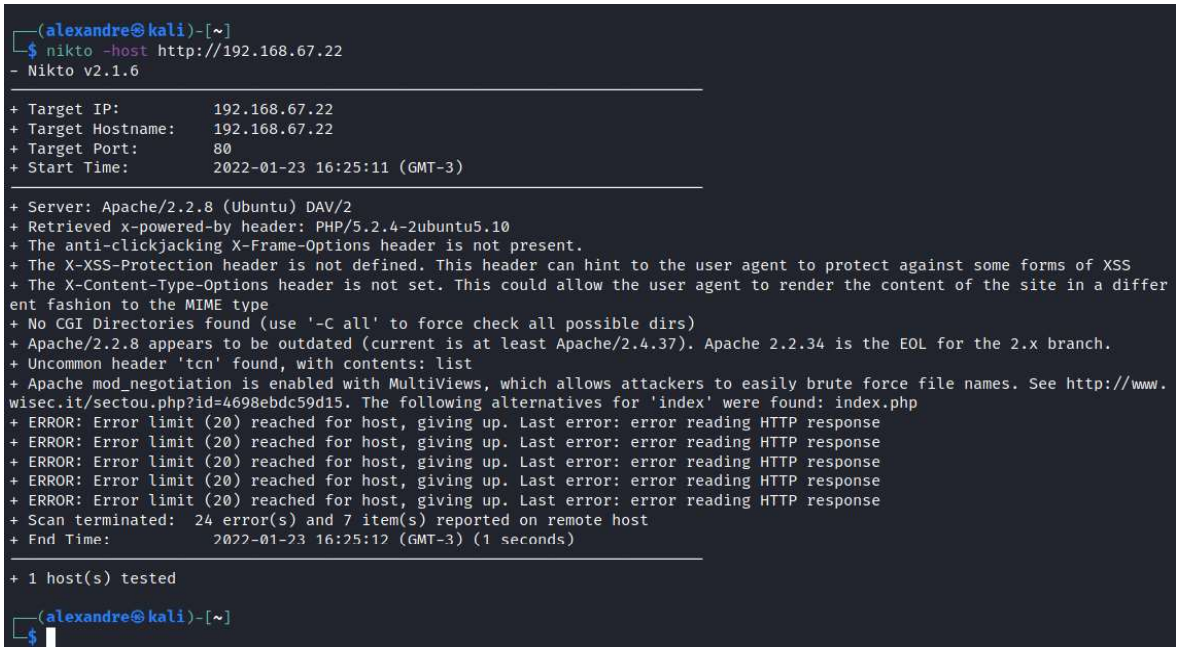

Figura 15 - Resultado da varredura do Nikto

Tabela 3 - Listagem de alertas do Nikto no experimento 2

DESCRIÇÃO
Server: Apache/2.2.8 (Ubuntu) DAV/2
Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
The anti-clickjacking X-Frame-Options header is not present.
The X-XSS-Protection header is not defined. Protection against some forms of XSS.
Apache/2.2.8 appears to be outdated.
Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names.
The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a diferent fashion to the MIME type.

Em seguida, a varredura com o OWASP ZAP, ainda foram encontradas vulnerabilidades, mas em menor quantidade que no primeiro teste, por exemplo, não houve nenhum caso de alerta de nível alto e nos casos listados de nível médio ocorreu uma redução em relação ao primeiro teste. O Application Error Disclosure teve 140 ocorrências no segundo experimento contra 256 no primeiro e o alerta sobre X-Frame-Options Header Not Set teve 2645 ocorrências no segundo experimento contra 4925 no primeiro experimento. A Figura 16 exibe os alertas do ZAP no segundo

experimento e a Tabela 4 traz a listagem dos alertas com o nível de risco e quantidade de vulnerabilidades encontradas.

Figura 16 - Alertas listados pelo ZAP

Tabela 4 - Listagem de alertas do ZAP no experimento 2

ID	ALERTA	RISCO	QTD
90022	Application Error Disclosure	Médio	140
10003	Biblioteca JS vulnerável	Médio	
10020-2	X-Frame-Options Header Not Set	Médio	2645
10202	Absence of Anti-CSRF Tokens	Baixo	3475
10010	Cookie No HttpOnly Flag	Baixo	18
10054	Cookie without SameSite Attribute	Baixo	28
10023	Information Disclosure – Debug Error Messages	Baixo	149
2	Private IP Disclousure	Baixo	25
10037	Server Leaks Information via “X-Powered-By” HTTP Response Header Field(s)	Baixo	115
10021	X-Content-Type-Options Header Missing	Baixo	2714
10024	Information Disclosure – Sensitive Information in URL	Informativo	9
10027	Information Disclousure – Suspicious Comment	Informativo	78
10096	Timestamp Disclosure – Unix	Informativo	1359

Após o ZAP, foi utilizado o Armitage para buscar vulnerabilidades e tentar utilizar algum ataque de penetração contra a máquina Metasploitable. O Armitage foi capaz de identificar a máquina e os serviços disponíveis, mas não conseguiu invadir como no primeiro teste. A Figura 17 exibe a seleção do exploit vsftpd, o mesmo utilizado no experimento 1, a Figura 18 tem a execução do exploit e a Figura 19 mostra que a tentativa de invasão não funcionou, o Kali Linux não foi capaz de invadir a máquina Metasploitable com o exploit vsftpd após a inclusão do IPS como medida de segurança.

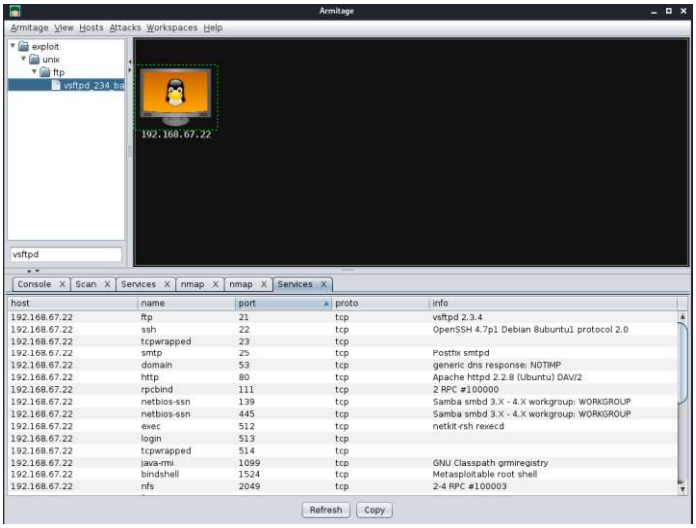

Figura 17 - Seleção do ataque no Armitage

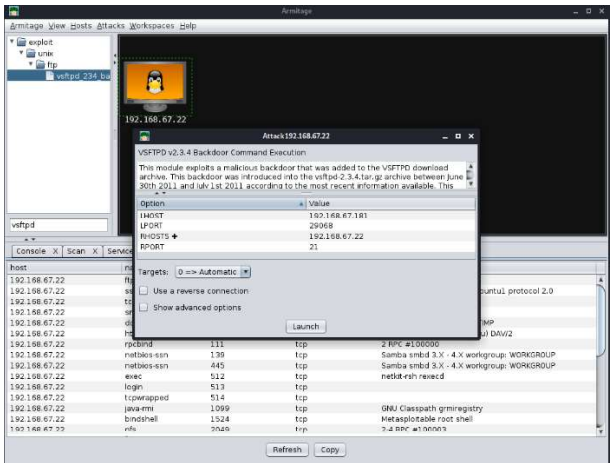

Figura 18 - Execução do ataque no Armitage

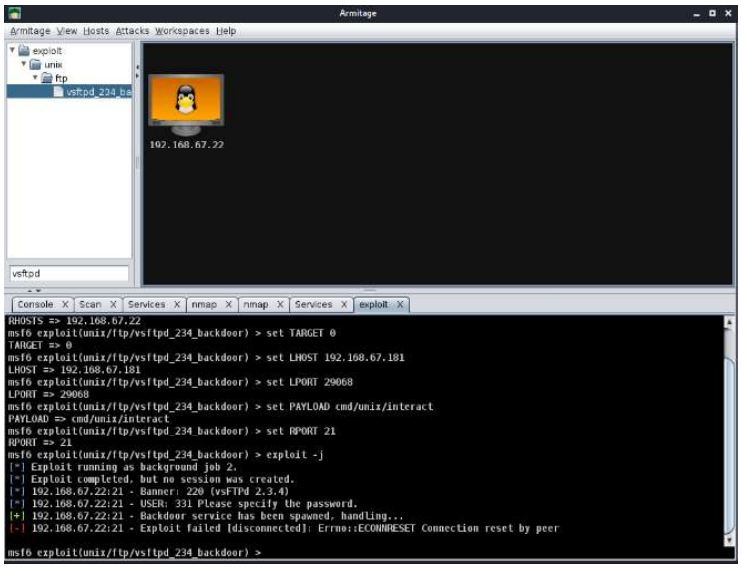

Figura 19 - Resultado do ataque do Armitage

5.3 Ataque ao Metasploitable protegido por WAF

O teste 3 foi realizado com o WAF (Web Application Firewall) protegendo a máquina Metasploitable. Nesse experimento, o Nikto não conseguiu listar as portas vulneráveis devido ao WAF. A Figura 20 e a Tabela 5 mostram o resultado da varredura do Nikto, os alertas encontrados não são de nível preocupante para a segurança da máquina Metasploitable.

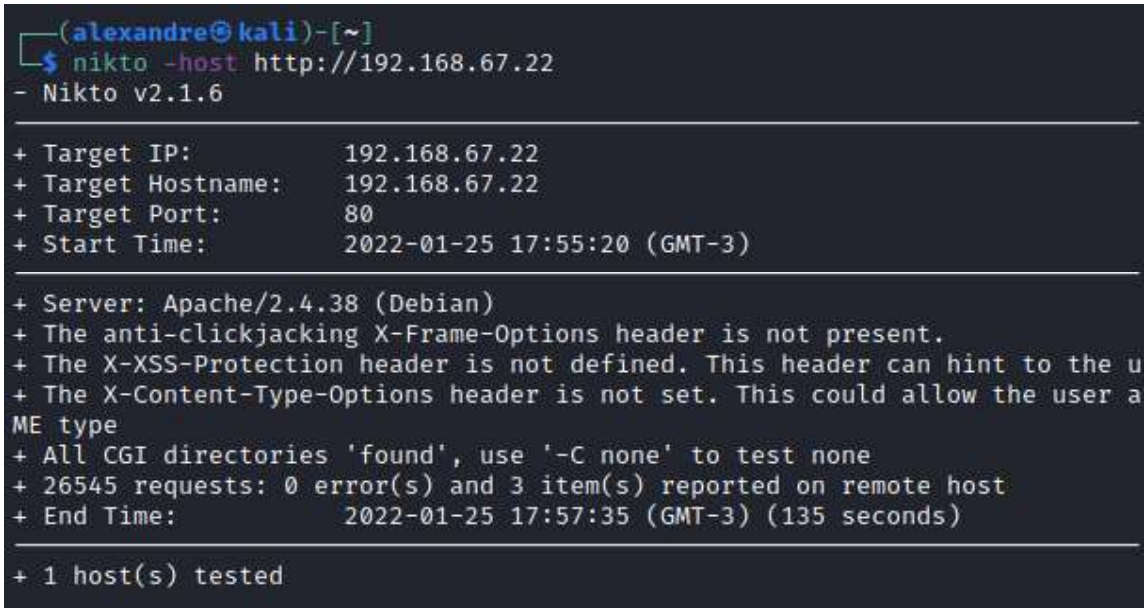

Figura 20 - Resultado da execução do Nikto

Tabela 5 - Listagem de alertas do Nikto no experimento 3

DESCRIÇÃO
Server: Apache/2.4.38 (Debian)
The anti-clickjacking X-Frame-Options header is not present.
The X-XSS-Protection header is not defined. Protection against some forms of XSS.
The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a diferent fashion to the MIME type.

O ZAP, que havia encontrado diversas vulnerabilidades e apresentado diversos alertas nos primeiros dois testes, dessa vez retornou um erro 403 Forbidden, de acesso proibido. A Figura 21 mostra a tentativa de escaneamento com o ZAP com o resultado recebido como erro 403.

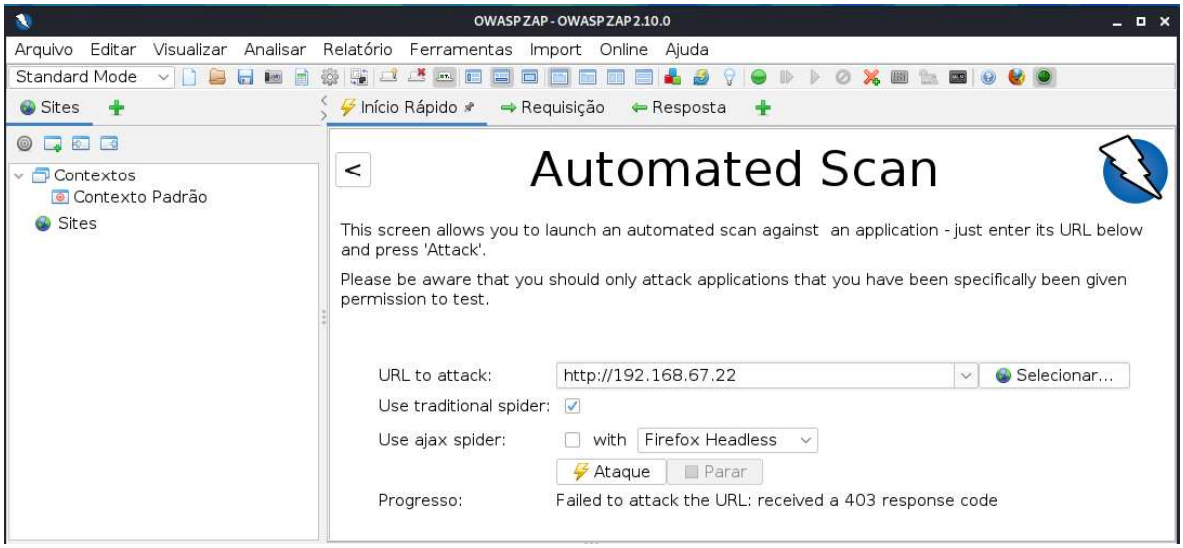

Figura 21 - Resultado da varredura do ZAP

O Armitage apenas foi capaz de listar um serviço disponível, o http na porta 80 como demonstrado pela Figura 22.

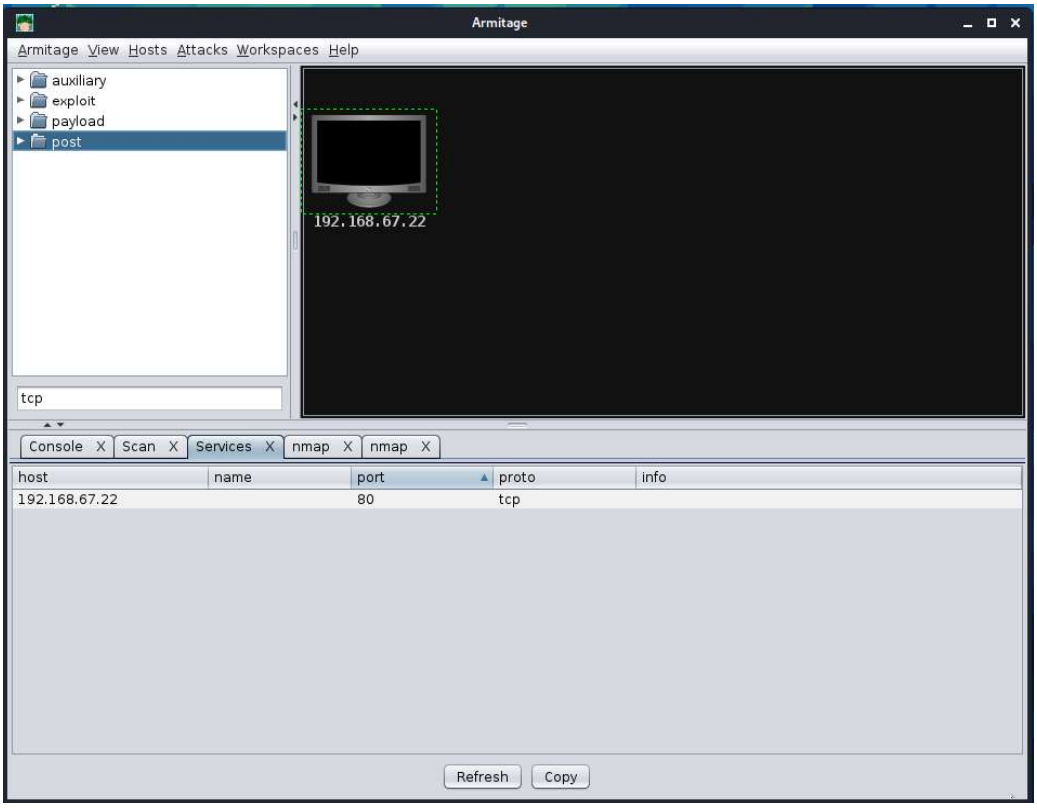

Figura 22 - Resultado do escaneamento do Armitage

5.4 Ataque ao Metasploitable protegido por IPS/IDS e WAF

O teste 4 foi implementado com o IPS e o WAF protegendo a máquina Metasplotable dos ataques do Kali Linux. Nesse experimento, o Nikto não conseguiu encontrar formas de explorar os serviços da máquina Metasploitable. De acordo com a Figura 23 e com a Tabela 6, os alertas encontrados pelo Nikto não apresentam risco para a segurança do Metasploitable.

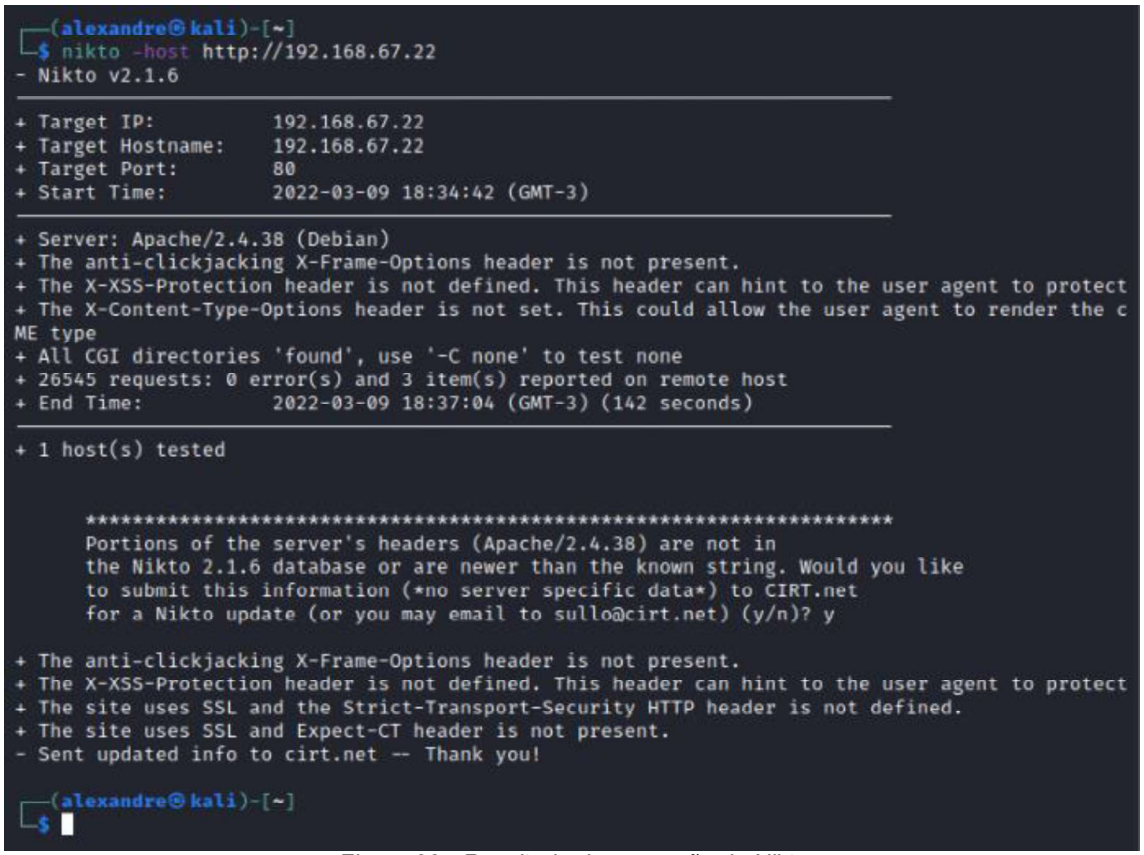

Figura 23 - Resultado da execução do Nikto

Tabela 6 - Resultado da análise do Nikto no experimento 4

DESCRIÇÃO
Server: Apache/2.4.38 (Debian)
The anti-clickjacking X-Frame-Options header is not present.
The X-XSS-Protection header is not defined. Protection against some forms of XSS.
The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a diferent fashion to the MIME type.
The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
The site uses SSL and Expect-CT header is not present.

O ZAP também não foi capaz de atacar o Metasploitable com essa configuração de segurança como mostra a Figura 24 em que o retorno da tentativa de invasão do ZAP foi o código 403, que significa acesso proibido.

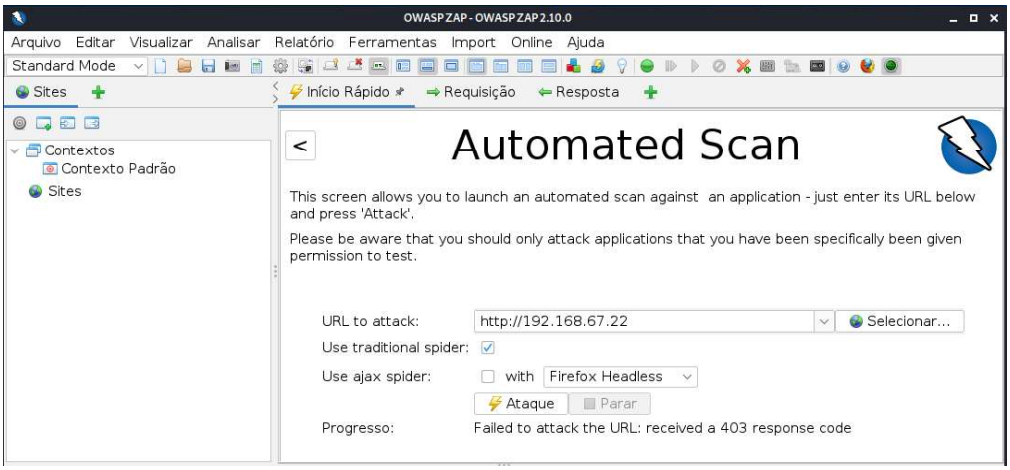

Figura 24 - Resultado da varredura do ZAP

O Armitage só conseguiu listar a porta 80 e não teve êxito em nenhum método de invasão sugerido para essa porta como mostra a Figura 25, o console do Armitage exibe a mensagem Connection failed, conexão falhou na tentativa de ataque.

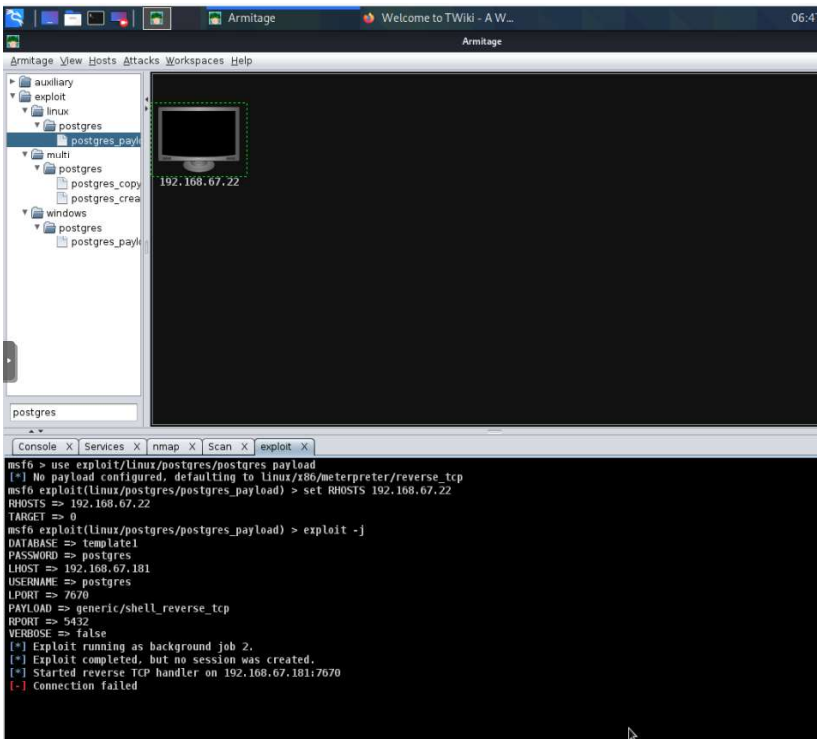

Figura 25 - Resultado do escaneamento do Armitage

5.5 Comparativo

A Tabela 7 mostra um comparativo entre os experimentos, exibindo as ferramentas utilizadas para atacar a máquina Metasploitable e os resultados obtidos em cada teste. Os componentes utilizados terão um ‘X’ em sua respectiva coluna para indicar sua presença no experimento.

Tabela 7 - Comparativo dos experimentos

Experimentos				Ferramentas		
Kali Linux	IPS	WAF	Metasploitable	Nikto	ZAP	Armitage
X			X	27 itens	14 alertas	Êxito na invasão
X	X		X	7 itens	13 alertas	Sem êxito na invasão
X		X	X	3 itens	Falhou na tentativa de ataque	Sem êxito na invasão
X	X	X	X	3 itens	Falhou na tentativa de ataque	Sem êxito na invasão

A partir dos dados dispostos na tabela, é possível observar que, no primeiro teste, a máquina com Kali Linux consegue acessar várias vulnerabilidades disponíveis no Metasploitable. A partir do segundo teste, com a inclusão do IPS pode-se perceber uma redução na efetividade dos ataques. O mesmo ocorreu no terceiro teste com a inclusão do WAF. O quarto teste teve um resultado similar ao terceiro o que traz o questionamento sobre a utilidade do IPS. Uma vez que o WAF recebe todas as solicitações na porta 80 e tem a sua disposição todo um aparato de filtragem e segurança contra invasões e está separado da máquina servidora, o mesmo poderia ser capaz de proteger o ambiente sem a ajuda do IPS.

6 Conclusão

Este trabalho apresentou uma configuração de segurança que melhorou a proteção de um servidor de hospedagem contra diversas ameaças. A partir disso pode-se desenvolver uma metodologia para configuração de segurança nesses ambientes, além de trazer um alerta sobre o quão importante é a segurança nos serviços disponíveis na Internet. Com as configurações de segurança implementadas, inclusão do IPS e do WAF, ferramentas que auxiliam na implementação do hardening, ficou evidente o aumento da segurança e da proteção no servidor de hospedagem.

Para trabalhos futuros, outras técnicas de invasão e outras ferramentas de proteção como Firewall e atualizações de segurança podem ser utilizadas para analisar o nível de proteção que podem oferecer e também identificar outras vulnerabilidades não encontradas neste trabalho.

Referências

TANENBAUM, Andrew S. Redes de Computadores. 4. ed. Rio de Janeiro: Elsevier Brasil, 2003.

OLIVEIRA, Gustavo. et. al. **Segurança de Redes Firewall.** Valinhos. Disponível em: <https://www.aedb.br/seget/arquivos/artigos05/318_Artigo-003.pdf>. Acesso em: 24 out. 2021

CLARO, João Ricardo. **Sistemas ids e ips – estudo e aplicação de ferramenta *open source* em ambiente linux.** Passo Fundo. Disponível em: <https://painel.passofundo.ifsul.edu.br/uploads/arq/20160331191141344853464.pdf>. Acesso em: 24 out. 2021.

KREUTZ, D. L. et al. Minicursos da XVII Escola Regional de Redes de Computadores. [s.l: s.n.].

PIMENTA, Alexandre Manuel Santareno. QUARESMA, Rui Filipe Cerqueira. **A SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO E O COMPORTAMENTO DOS USUÁRIOS.** São Paulo. Revista de Gestão da Tecnologia e Sistemas de Informação. 2016. pp. 533-552. Disponível em: <https://www.scielo.br/j/jistm/a/n6HBtP6htxYkTKKrjt9VsRz/?format=pdf&lang=pt>. Acesso em: 24 out. 2021.

Estatísticas do CERT.br -- Incidentes. Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em: 25 out. 2021.

CERT.br Stats (janeiro a dezembro de 2020). Disponível em: <https://www.cert.br/stats/incidentes/2020-jan-dec/tipos-ataque.html>. Acesso em: 25 out. 2021.

Introduction | Kali Linux Documentation. Disponível em: <https://www.kali.org/docs/introduction/>. Acesso em: 25 out. 2021.

Metasploitable 2 Exploitability Guide | Metasploit Documentation. Disponível em: <https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/>. Acesso em: 25 out. 2021.

SOUSA, Á. W. et al. **Estudo de caso sobre a implementação de técnicas de blindagem em servidores Linux baseada na detecção de vulnerabilidades e tentativas de intrusão**. Anais da Escola Regional de Redes de Computadores (ERRC). **Anais**... In: ANAIS DA XVIII ESCOLA REGIONAL DE REDES DE COMPUTADORES. SBC, 25 nov. 2020. Disponível em: <https://sol.sbc.org.br/index.php/errc/article/view/15204>. Acesso em: 25 out. 2021.

TABASSUM, Mujahid; MUSCAT, Oman; SHARMA, Tripti; MOHANAN, Saju. Ethical Hacking and Penetrate Testing using Kali and Metasploit Framework. **International Journal of Innovation in Computational Science and Engineering (IJICSE)**, v. 2, n. 1, p. 9–22, 2021. Disponível em: <https://webportal.hct.edu.om/ijicse/pages/upload/library/2020/2/P2.pdf>. Acesso em: 25 out. 2021.

GALLUS, P.; FRANTIS, P. Security analysis of the Raspbian Linux operating system and its settings to increase resilience against attacks via network interface. 2021 International Conference on Military Technologies (ICMT). Anais... In: 2021 INTERNATIONAL CONFERENCE ON MILITARY TECHNOLOGIES (ICMT). Brno, Czech Republic: IEEE, 8 jun. 2021. Disponível em: <https://ieeexplore.ieee.org/document/9502746/>. Acesso em: 25 out. 2021.

ITU Publications. Disponível em: <https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en>. Acesso em: 25 out. 2021.

Nmap: the Network Mapper - Free Security Scanner. Disponível em: <https://nmap.org/>. Acesso em: 27 out. 2021.

Overview & Description · sullo/nikto Wiki. Disponível em: <https://github.com/sullo/nikto>. Acesso em: 27 out. 2021.

OWASP ZAP – Getting Started. Disponível em: <https://www.zaproxy.org/getting-started/>. Acesso em: 11 jan. 2022.

armitage | Kali Linux Tools. Disponível em: <https://www.kali.org/tools/armitage/>. Acesso em: 13 jan. 2022.

CERT.br Stats (janeiro a dezembro de 2020). Disponível em: <https://www.cert.br/stats/incidentes/2020-jan-dec/scan-portas.html>. Acesso em: 13 fev. 2022.

PINHEIRO, J. M. DOS S. Ameaças e Ataques aos Sistemas de Informação: Prevenir e Antecipar. **Cadernos UniFOA**, v. 3, n. 5, p. 11–21, 2007.

BERTHOLDI, Juliana. **Crimes cibernéticos.** Curitiba: Contentus, 2020.

TANENBAUM, Andrew S.; WETHERALL, David J. **Redes de Computadores.** 5ª edição. Pearson, 1 janeiro 2017.

ROHLING, Luis José. **Segurança de redes de computadores.** Curitiba: Contentus, 2020.

HYPPÖNEN, Mikko. **Securing a Linux Server Against Cyber Attacks.** Disponível em : <https://trepo.tuni.fi/bitstream/handle/10024/131119/Hypp%C3%B6nenMikko.pdf>. Acesso em 16 fev. 2022.