FACULDADE DE TECNOLOGIA E CIÊNCIAS SOCIAIS APLICADAS – FATECS
ENGENHARIA DE COMPUTAÇÃO

YURI DE MELO SILVA
22153209

DEFESA EM PROFUNDIDADE NA SEGURANÇA CIBERNÉTICA

BRASÍLIA
2022

YURI DE MELO SILVA

DEFESA EM PROFUNDIDADE NA SEGURANÇA CIBERNÉTICA

Trabalho de Conclusão de Curso (TCC) apresentado como um dos requisitos para a conclusão do curso de Engenharia de Computação do CEUB– Centro Universitário de Brasília

Orientador (a)**: Prof. MsC Francisco Javier de Obaldia Diaz**

BRASÍLIA
2022

YURI DE MELO SILVA

DEFESA EM PROFUNDIDADE NA SEGURANÇA CIBERNÉTICA

Trabalho de Conclusão de Curso (TCC) apresentado como um dos requisitos para a conclusão do curso de Engenharia de Computação do CEUB – Centro Universitário de Brasília

Orientador (a)**: Prof. MsC Francisco Javier de Obaldia Diaz**

Brasília, 2022.

BANCA EXAMINADORA

_____
Prof. MsC Francisco Javier de Obaldia Diaz
Orientador (a)

_____
Prof. Fabio Oliveira Guimaraes
Examinador (a)

_____
Prof. Dr. Tiago Leite Pereira
Examinador (a)

Defesa em profundidade na segurança cibernética
Defense in depth in cybersecurity

Yuri de Melo Silva[1], Francisco Javier de Obaldia Diaz[2], Fabio Oliveira Guimaraes[3], Tiago Leite Pereira[4]

RESUMO

Com o crescimento de tecnologias e uso da internet, aumenta-se também o número de vetores de ataque usados por agentes maliciosos espalhados pelo mundo, devido a este fato, organizações podem tirar grandes proveitos da utilização da *defesa em profundidade*, estratégia a qual faz uso de diversos produtos e práticas com o objetivo de proteger seus ativos de informação das mais diversas categorias de ameaças cibernéticas. Neste trabalho estudaremos o conceito de defesa em profundidade, e como a mesma é aplicada na segurança cibernética. Para a metodologia foram configurados dois ambientes, sendo um com apenas uma camada de segurança e o outro com mais camadas, demonstrando assim, por meio de ataques simulados, que o ambiente com menos camadas de proteção fica vulnerável e o outro não.

Palavras-chave: Segurança. Cibernética. Defesa. Redes.

Abstract:

With the growth of technologies and use of the internet, the number of attack vectors used by malicious agents around the world also increases, due to this fact, organizations take great advantage of the use of defense in depth, a strategy that makes use of various products and practices in order to protect their information assets from the most diverse categories of cyber threats. In this work you study the concept of defense in depth, and how it is applied in cybersecurity. For the methodology, two environments were configured, one with only one security layer and the other with more layers, thus demonstrating, through simulated attacks, that the environment with fewer layers of protection is vulnerable and the other is not.

keywords: Security. Cybersecurity. Defense. Networks. DiD.

[1] UniCEUB, aluno.
[2] UniCEUB, orientador.
[3] UniCEUB, primeiro examinador.
[4] UniCEUB, segundo examinador.
[2]

1 INTRODUÇÃO

O mundo avança cada vez mais em tecnologia, surgem computadores cada vez mais poderosos disponíveis ao público, o acesso a informação também pode ser feito com mais facilidade a cada dia, com isso aumenta-se também o número de ameaças cibernéticas, as quais trazem grandes perigos às organizações e exigem grandes esforços destas para protegerem seus ativos de informação.

Diante do exposto as equipes de segurança utilizam diversas estratégias e técnicas para se proteger contra os mais diversos tipos de ameaças, sendo uma dessas estratégias a defesa em profundidade, ou como também é conhecida com o termo defesa em camadas, estratégia a qual será abordada neste trabalho.

O objetivo da defesa em profundidade é implementar diferentes camadas de segurança para proteger a rede de uma organização contra agentes maliciosos. A estratégia é usada baseando-se na ideia de que apenas uma camada de segurança não é capaz de proteger totalmente as informações internas, então para que um nível de segurança maior seja alcançado, diferentes produtos e práticas de segurança são implementados para trabalharem em conjunto contra ameaças externas.

Este trabalho tem como foco a demonstração de algumas ferramentas de controles técnicos de segurança utilizadas na estratégia de defesa em profundidade, como também irá expor a efetividade desta, contra uma estratégia com uma única camada de segurança.

A demonstração será feita em um ambiente controlado que foi implementado somente para esta pesquisa, ambiente que irá simular a rede interna de uma organização que oferece serviços à internet. Serão executados alguns ataques básicos, demonstrando assim o sucesso de bloqueio no ambiente que possui mais camadas de segurança, ou seja, o ambiente com defesa em profundidade, e também serão executados os mesmo ataques no ambiente com segurança simples, que possui apenas uma camada de segurança.

2 REVISÃO BIBLIOGRÁFICA

Diversas tarefas do cotidiano das pessoas podem ser realizadas por sistemas na internet, proporcionando uma enorme facilidade ao realizá-las. Tarefas como operações bancárias e compras, que antes necessitavam de um certo deslocamento por parte do comprador, hoje podem ser realizadas pela internet, de acordo com TAHA (2017).

Junto com essa facilidade proporcionada pelo uso da tecnologia, cresce também as maneiras pelas quais criminosos podem agir. Para ROCHA (2013, p. 1): “Hoje, o agente delituoso não necessita ir às ruas para cometer determinados ilícitos como furto, racismo, crimes contra à honra, dentre outros.”

Para MARTINEZ (2019), segurança cibernética é a proteção da informação, ativos, serviços e sistemas de valor, com o objetivo de reduzir a probabilidade de perda, danos, comprometimento ou uso indevido. Sendo uma coleção de processos interativos destinados a fazer o ciberespaço protegido e seguro.

Um incidente de segurança da informação é um evento ou uma série deles, que ocorre de maneira inesperada ou indesejada, podendo comprometer e ameaçar a segurança da informação, de acordo com ABNT (2005).

Em 2020, o CERT.BR publicou estatísticas, que mostram que 665079 incidentes foram reportados a eles, destes, 59% (398057) foram relacionados a *scan*, 10% (68200) relacionados a *DoS* e 3% (26567) relacionados a *web*.

Um *scan* é uma técnica utilizada para coletar informações da rede, os

administradores podem usar esta técnica para verificar portas abertas e restringir o acesso a elas, já os atacantes podem fazer o uso da mesma técnica com o objetivo de descobrir quais pontos podem explorar, de acordo com SINGH et. al, (p.34. 2015).

Um ataque de negação de serviço ou *Denial of Service (DOS)*, faz a exaustão dos recursos que provêem um serviço, com o objetivo de interrompê-lo ou diminuir sua performance, de acordo com GU e LIU (p.5, 2007).

Um ataque direcionado a aplicações *web* possui objetivo de obter acesso não autorizado ou obter informações de usuário. De acordo com OWASP (2021), em seu TOP 10 de ataques, o primeiro lugar é o ataque de quebra de controle de acesso, onde o atacante manipula algum argumento para contornar o controle de acesso de uma aplicação, e em terceiro lugar vem o ataque de injeção, onde o atacante consegue executar comandos a partir da aplicação explorando alguma vulnerabilidade que a mesma possui.

Diante dos ataques citados, existem inúmeras ferramentas utilizadas para fazer a proteção contra eles, porém vamos destacar apenas 3: *firewall*, *IDS/IPS*, *WAF*.

O *firewall* é uma ferramenta usada para proteger uma rede de computadores, todo o tráfego de dados, que entra ou sai da rede, passa pelo firewall, assim é possível definir políticas de segurança, as quais liberam o acesso com base no endereço de origem e destino, como também nas portas de origem e destino, então somente os acessos permitidos acontecem e todo o resto é bloqueado, de acordo com ABIE (p.1, 2000).

De acordo com CHAKRABORTY (2013), um *Intrusion detection system (IDS)* é uma ferramenta que analisa todo o tráfego que passa por ela, esta faz uma análise profunda nos pacotes buscando por características que possam ser maliciosas ou que violem alguma política de segurança definida anteriormente, por outro lado um *Intrusion prevention system (IPS)* toma ações de resposta de acordo com as políticas pré-estabelecidas que detectaram algo malicioso ou que não é permitido, fazendo o bloqueio do tráfego indesejado.

Por fim um *Web Application firewall (WAF)* funciona como um firewall, porém analisa somente o tráfego que é direcionado às aplicações web, procurando por algum tipo de requisição maliciosa que possa contornar algum controle de acesso, fazer injeção de comandos ou explorar alguma vulnerabilidade, de acordo com GUPTA et. al (2007).

Diante das explicações acima, percebe-se que apenas uma dessas ferramentas sozinha não conseguem proteger uma rede de computadores dos ataques também citados. O *firewall* vai impedir o acesso que não foi definido antes, o *IDS/IPS* irá analisar os pacotes mais profundamente procurando e bloqueando um tráfego que foi permitido pelo firewall porém é malicioso e por fim o *WAF* irá aprofundar ainda mais a análise dos pacotes direcionados a aplicação *web* em busca de requisições maliciosas que conseguiram passar pelas duas últimas ferramentas, assim é introduzido a estratégia da defesa em profundidade, ou defesa em camadas.

A defesa em profundidade foi criada pela *National Security Agency (NSA)*, baseada em estratégias militares, onde eram implementadas barreiras de segurança de perímetro, com o objetivo de vencer o inimigo à medida que o mesmo passasse por cada uma das barreiras, de acordo com GROAT et. al (2012).

Segundo KUIPERS e FABRO (2006), infraestruturas modernas compartilham características semelhantes, sendo assim estas são divididas internamente em zonas, onde cada zona possui níveis diferentes de segurança, como comunicação entre sedes da organização, ou entre a internet e rede interna e também entre aplicações internamente, assim a comunicação de entrada e saída passa por diferentes camadas de segurança, como por exemplo, pelas ferramentas que foram anteriormente citadas.

Basicamente, quanto mais camadas de

segurança forem adicionadas, mais seguro ficará a infraestrutura alvo, de acordo com KEWLEY e LOWRY (2001). Deste modo a estratégia da defesa em profundidade se dá pela adição de camadas de segurança com o objetivo de aumentar a possibilidade de detectar e bloquear atividades maliciosas, pois diferentes ferramentas estarão ativas e caso uma delas não conseguir detectar e bloquear um ataque, poderá contar com a ação de outra ferramenta dentre as camadas.

3 METODOLOGIA DO TRABALHO

O trabalho toma como base a pesquisa em diversas fontes de material especializado sobre segurança cibernética como exposto na seção anterior. Quanto à natureza da pesquisa, trata-se de uma pesquisa aplicada que objetiva gerar conhecimentos aplicados à solução de problemas relacionados aos incidentes mais frequentes que atingem a segurança cibernética. Quanto à forma de abordagem do problema, busca-se quantificar, com base em simulação, resultados de ataques a ambiente com mais e com menos camadas de segurança, buscando qualificar a defesa em profundidade como uma técnica que precisa ser aprofundada e aplicada. Na busca dos objetivos buscou-se explorar critérios e técnicas já utilizadas na segurança cibernética, permitindo realizar descritivos de estudos e análises que fundamentam a aplicação da defesa em profundidade, como uma técnica que deve ser melhor observada e implementada na proteção dos ambientes de redes de comunicação de dados e sua segurança nas organizações.

Foram configurados dois ambientes para a execução dos testes. O primeiro ambiente faz uso de uma estratégia simples de segurança, por outro lado, o segundo ambiente utiliza a estratégia de defesa em profundidade. O objetivo é demonstrar a eficiência de ambas as estratégias na defesa contra alguns tipos de ataques mais comuns. As estruturas de cada ambiente e os ataques feitos, foram relacionadas em 2 tópicos a seguir.

3.1 Estruturas dos ambientes

Ambos os ambientes são compostos pelas ferramentas de segurança e as máquinas virtuais pertencentes a rede de testes. Os ambientes possuem alguns elementos que são exatamente iguais em ambos, como a máquina virtual de onde irão partir os ataques e a que será o servidor web da aplicação vulnerável.

Em ambos os ambientes utilizamos uma ou mais *De-militarized Zone (DMZ)*, que é uma rede a qual serve como uma ligação segura entre uma rede não confiável e uma confiável, são redes com políticas de acesso mais restritas usadas para abrigar servidores que disponibilizam serviços a terceiros.

Além disso, outra configuração semelhante em ambos ambientes, são as políticas de segurança existentes no firewall, este está configurado da melhor forma possível, o que significa que todo o tráfego e acessos que não são necessários ou podem aumentar a chance de ataque ao ambiente foram bloqueados, somente os acessos necessários para o funcionamento do ambiente estão permitidos, qualquer outro além desses não são permitidos

3.1.1 Ambiente de segurança simples

O ambiente de segurança simples, possui apenas uma camada de segurança em sua estrutura, essa camada é feita por um *firewall*, além desta ferramenta, possui também uma máquina virtual, onde está instalado o servidor *web* com a aplicação vulnerável. O ambiente foi projetado para ser uma estrutura que forneça um site que é acessado por meio da internet, assim foram implementadas 3 redes lógicas. A primeira dessas redes simula a internet do ambiente, a segunda rede foi pensada para ser uma intranet, que por definição (HORTON, 2001) é uma rede que pertence a uma organização e é acessada somente por ela. Por fim, a última

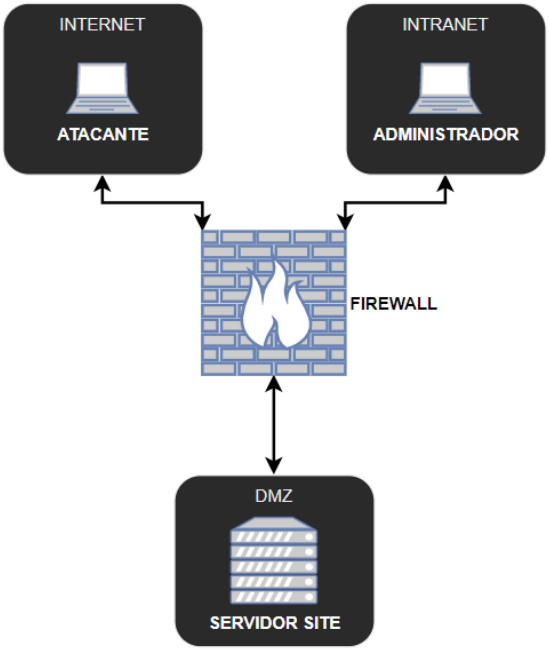
rede, é uma rede desmilitarizada, sendo esta uma rede interna que funciona como uma ligação entre uma rede segura e uma menos segura (DADHEECH et. al, 2018), na qual, se encontra o servidor com a aplicação de testes.

Neste ambiente o site, que receberá os ataques, é acessado diretamente pelo cliente, não passando por nenhum tipo de análise ou inspeção de tráfego.

A figura 1 a seguir mostra a topologia de rede deste ambiente, contendo a rede *Internet* que simulará a rede global por onde chegará os ataques, a *Intranet* que servirá apenas para administração do firewall e por fim a *DMZ* que é a rede que abrigará o servidor do site onde será feito os testes, sendo que neste ambiente as requisições são feitas diretamente ao servidor do site.

Na figura todos os elementos estão ligados ao elemento central, o firewall, pois fisicamente é como as ligações são feitas, porém logicamente o firewall faz a segregação de todas as redes, por meio de políticas de segurança, impedindo conexões diretas entre as redes a menos que sejam necessárias.

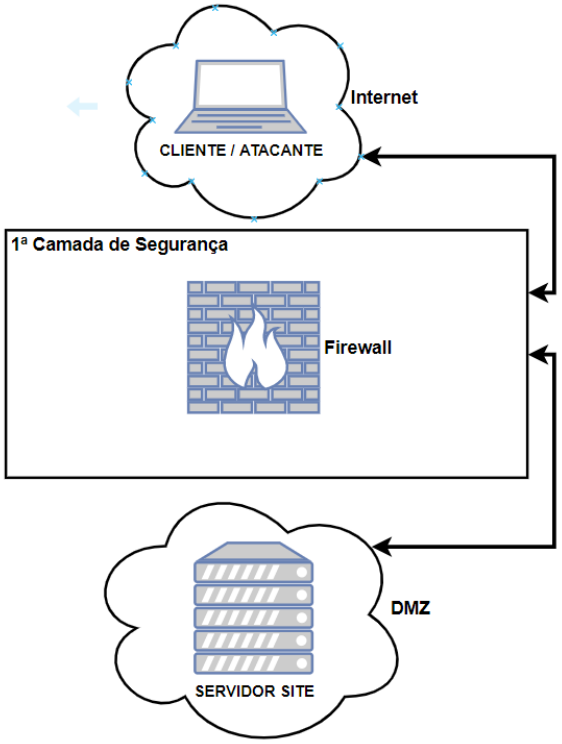
Figura 1: Topologia de rede - Ambiente 1



Fonte: Autor

A figura 2 mostra o caminho que as requisições fazem no ambiente, sendo geradas pelo cliente, passando pela única camada de segurança e por fim o destino.

Figura 2: Fluxo das requisições - Ambiente 1



Fonte: Autor

A tabela a seguir, relaciona os intervalos de endereços IP utilizados.

Tabela 1. Intervalos de endereços usados

Rede	Intervalo
Internet	192.168.0.0/24
Intranet	192.168.56.0/24
DMZ	172.16.100.0/24

Fonte: Autor

A estrutura possui 3 máquinas virtuais, sendo um firewall, um servidor web com a aplicação vulnerável que será o site, e uma última que será a máquina da qual os ataques serão disparados. A seguir é apresentada uma

tabela (2) com a rede e endereço IP de cada máquina.

Tabela 2. Rede e endereço IP de cada máquina

Máquina virtual	IP	Rede
Firewall	192.168.0.100	Internet
	192.168.56.254	Intranet
	172.16.100.1	dmz
Servidor site	172.16.100.50	dmz
Atacante	Dinâmico	Internet

Fonte: Autor

Além dos endereços IP's relacionados na tabela 2, existe mais um na rede de internet simulada, 192.168.0.111, que é o endereço de *NAT (Network Address Translation)* do Servidor, este serve para traduzir e permitir o roteamento entre um endereço privado e público (WING p.4, 2010).

Neste primeiro ambiente, a única camada de segurança, o firewall, foi configurada com todas as políticas de segurança necessárias para restringir acessos desnecessários e permitir os necessários, inclusive o acesso a administração do firewall pela rede intranet e o acesso a aplicação por meio da internet simulada, todo e qualquer tipo de acesso que não é necessário está sendo bloqueado.

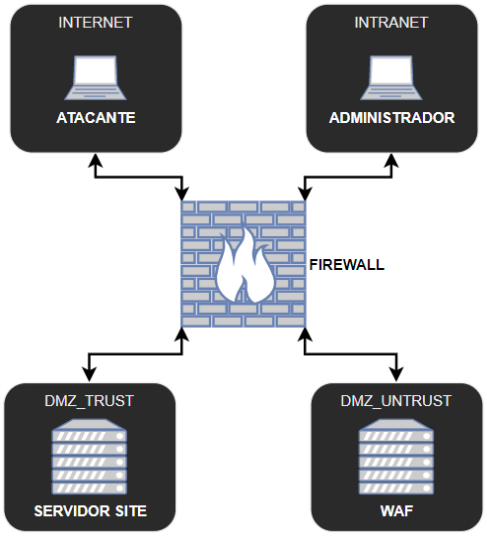
3.1.2 Ambiente com defesa em profundidade

O ambiente com defesa em profundidade possui 4 máquinas virtuais, semelhantes ao primeiro ambiente, porém neste, além das 3 que se encontram no primeiro, existe mais uma que é o *web application firewall*. Além disso, o ambiente com defesa em profundidade possui 4 redes, uma a mais que o anterior. A primeira rede é a que simula a internet, a segunda a intranet da infraestrutura, a terceira uma zona desmilitarizada chamada dmz_trust e por fim outra dmz chamada dmz_untrust, a frente será explicado a função destas duas últimas.

A figura a seguir mostra a topologia de rede do ambiente 2, com defesa em profundidade.

Conforme já explicado anteriormente, todos elementos são ligados ao firewall que é o elemento central responsável por rotear o tráfego, porém logicamente as redes são segregadas por meio de políticas de segurança, não tendo conexão direta entre elas a menos que seja necessário.

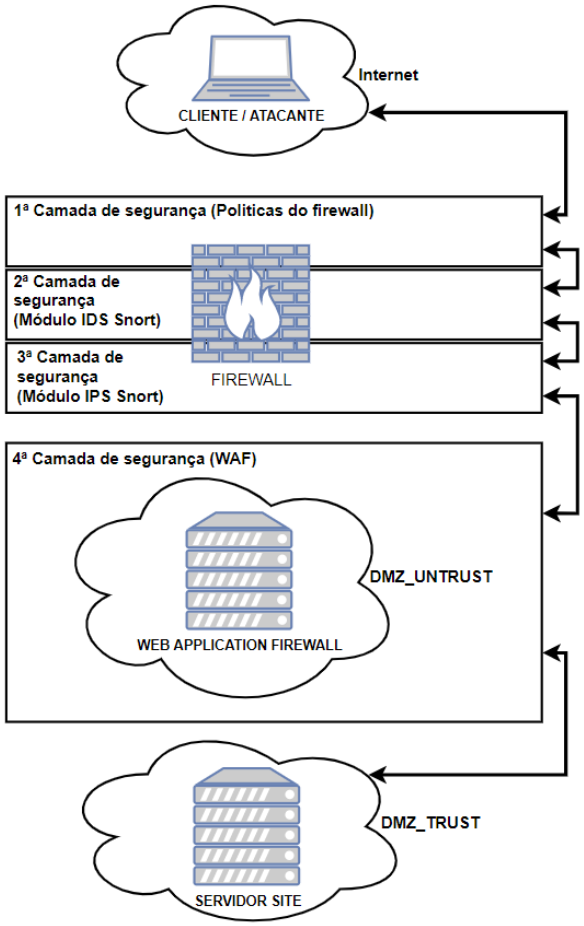
Figura 3: Topologia de rede - Ambiente 2



Fonte: Autor

A figura 4 mostra o caminho das requisições no ambiente com defesa em profundidade. A primeira camada de segurança que a requisição passa são as políticas de segurança do firewall, após isso caso seja uma política de liberação, a próxima camada é o *Intrusion Detection System (IDS)* implementado pelo módulo *snort* instalado no firewall, caso seja detectado algo próxima camada é o *Intrusion Prevention System (IPS)* também implementado pelo snort, e por fim caso nenhuma das camadas anteriores detecte algo nas requisições, a quarta e última camada é o *Web Application Firewall (WAF)* que irá realizar uma analise mais profunda nas requisições web direcionadas ao servidor do site dentro do ambiente.

Figura 4: Fluxo das requisições - Ambiente 2



Fonte: Autor

A seguir tem-se uma tabela com o intervalo dos endereços usados em cada rede.

Tabela 3. Intervalos de endereços usados

Rede	Intervalo
Internet	192.168.0.0/24
Intranet	192.168.56.0/24
dmz_trust	172.16.100.0/24
dmz_untrust	172.16.66.0/24

Fonte: Autor

Esta segunda estrutura possui 4 máquinas virtuais, sendo um *firewall*, dois servidores, um com o *web application firewall* e outro com o site que receberá os ataques e por fim a máquina de onde os ataques serão realizados. A tabela 4 apresenta a rede e endereço IP de cada máquina.

Tabela 4. Rede e endereço IP de cada máquina

Máquina virtual	IP	Rede
Firewall	192.168.0.100	Internet
	192.168.56.254	Intranet
	172.16.100.1	dmz_trust
	172.16.66.1	dmz_untrust
Servidor site	172.16.100.50	dmz_trust
Servidor WAF	172.16.66.1	dmz_untrust
Atacante	Dinâmico	Internet

Fonte: Autor

Este ambiente possui 4 camadas de segurança, 3 a mais do que o primeiro. Estas camadas são, em primeiro lugar, o firewall, que permite apenas os acessos necessários, este possui todas as políticas de segurança criadas para bloquear requisições não definidas por elas, em segundo existe o *Intrusion Detection System (IDS)* e o *Intrusion Prevention System (IPS)* para detectar e bloquear requisições que foram permitidas pelo firewall porém tem características maliciosas. A seguir, a terceira camada é o *Web Application Firewall (WAF)* que irá inspecionar as requisições direcionadas ao site e procurar por algo malicioso. Por fim, a última camada foi a criação das duas redes desmilitarizadas, a dmz_trust e a dmz_untrust, onde a primeira é a qual vai hospedar o servidor com o site e possui políticas de segurança mais restritas, e a segunda é a qual vai hospedar o *Web Application Firewall (WAF)*, que possui políticas de segurança que permitem acesso externo, o que permitirá o acesso ao site após o tráfego ser analisado pela ferramenta de segurança.

3.2 Ataques feitos nos ambientes

Em ambos os ambientes foram executados os mesmos ataques, o objetivo nisto é demonstrar o comportamento de cada ambiente diante dos testes, mostrando qual deles obtém sucesso no bloqueio e segurança da infraestrutura. Foram executados um total de 3 ataques distintos, relacionados nos tópicos a seguir.

3.2.1 Escaneamento de portas (*scan)*

Neste ataque é executado um escaneamento do alvo com o objetivo de coletar informações sobre quais portas estão abertas para que possa ser feito um melhor direcionamento dos próximos ataques com objetivos mais específicos. Este ataque pode ser direcionado a apenas um endereço IP ou URL, como também para todo um intervalo de endereços.

3.2.2 Negação de serviço (*DoS*)

Este ataque tem o objetivo de exceder algum recurso da infraestrutura alvo, conseguindo assim interromper ou causar mal funcionamento em algum serviço do alvo. O ataque de negação de serviço pode ser feito tanto por apenas um atacante, como também pode ser feito de maneira distribuída, quando o atacante infecta várias máquinas e desta dispara o ataque de negação em um outro alvo.

3.2.3 Injeção de comando

O ataque de injeção de comando é quando o atacante faz uso de alguma vulnerabilidade para executar comandos no sistema operacional alvo ou em algum serviço como um banco de dados. Este ataque tem o objetivo de executar ações, como uma conexão com a máquina do atacante partindo do alvo, como também exfiltração de dados em um banco de dados.

4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

4.1 Ferramentas usadas para implementação dos ambientes

4.1.1 *PFSense*

O PFSense é um projeto open source e gratuito, usado como gateway e roteador de um rede, possui capacidade de bloquear e permitir tráfego, e também possui uma administração web fácil e simples. A ferramenta permite a instalação de diversos módulos para agirem em conjunto com a função de firewall, incrementando a segurança da rede.

4.1.2 *Snort*

Snort é uma ferramenta com a capacidade de bloquear tráfego fazendo uma análise da assinatura dos pacotes buscando por características maliciosas.

4.1.3 *Nginx* + *modsecurity*

Nginx é um serviço usado como servidor web em seu uso básico, porém muitas vezes utilizado também como proxy, conseguindo ser usado juntamente com um de seus módulos de segurança, *ModSecurity*, permitindo fazer a análise do tráfego direcionado a aplicações web buscando por alguma característica maliciosa.

4.1.4 *VirtualBox*

O *VirtualBox* é uma ferramenta usada para virtualização de sistemas operacionais usando como base um sistema operacional hospedeiro onde a ferramenta será instalada. Possibilita a execução de diversos sistemas operacionais simultaneamente e de maneira segregada dentro de um mesmo sistema operacional hospedeiro, o que facilita a execução de testes sem necessidade de grandes recursos de hardware na maioria dos casos e também a exportação das máquinas virtuais para a importação em sistemas de

virtualização de grande porte para serem usados em *data centers* e afins.

4.2 Ferramentas usadas para execução dos ataques

4.2.1 *Nmap*

Nmap é uma ferramenta open source usada para escaneamento de rede e auditoria de segurança.

4.2.2 *Hping3*

O *hping3* é um comando existente para sistemas operacionais linux, que possui a capacidade de realizar alguns testes de rede, incluindo testes de negação de serviço.

4.2.3 *Kali Linux*

O Kali Linux é uma sistema operacional baseado em linux utilizado para realizar testes de penetração em sistemas, pois possui uma série de ferramentas instaladas para esse fim.

4.2.4 *Damn Vulnerable Web Application (DVWA)*

Damn Vulnerable Web Application (DVWA) é uma aplicação web utilizada para testes de conhecimento e de infraestrutura pois possui inúmeras vulnerabilidades em seu código fonte que permite que os profissionais de segurança avaliem a capacidade de suas ferramentas detectarem tais vulnerabilidades.

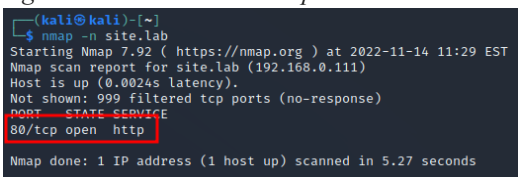
4.3 Execução e resultados dos testes em cada ambiente

4.3.1 Ambiente de segurança simples

4.3.1.1 Escaneamento de portas

O *nmap* foi usado em seu estado mais simples para efetuar um escaneamento no endereço site.lab, nome dado ao IP 192.168.0.111, endereço de nosso site vulnerável, e a ferramenta obteve sucesso conforme figura 5.

Figura 5: Escaneamento de portas do ambiente 1

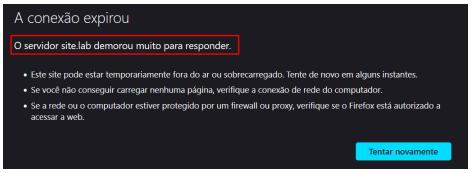


Fonte: Autor

4.3.1.2 Negação de serviço

O hping3 foi usado para realizar o ataque de negação de serviço, foram utilizadas as opções do comando que direcionando requisições para a aplicação web do alvo. O apontamento do comando foi feito para o endereço site.lab e este obteve sucesso no ataque, como pode ser visto na figura 6, o erro de "A conexão expirou" indicando a sobrecarga no site.

Figura 6: Negação de serviço no ambiente 1

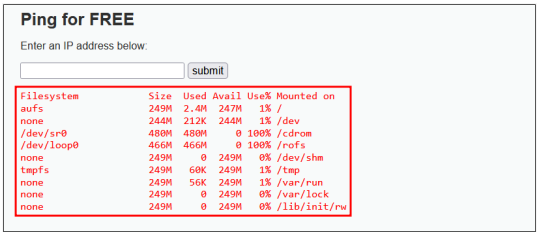


Fonte: Autor

4.3.1.3 Injeção de código

Para o ataque de injeção de código foi usado o navegador para passar parâmetros maliciosos em um campo vulnerável da aplicação. Como podemos ver na figura 7, o ataque obteve sucesso na listagem de todos pontos de montagem do sistema quando era somente para executar um ping.

Figura 7: Injeção de comando no ambiente 1



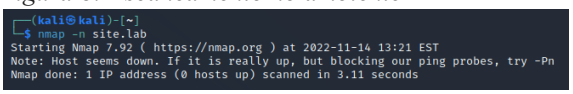
Fonte: Autor

4.3.2 Ambiente com defesa em profundidade

4.3.2.1 Escaneamento de portas

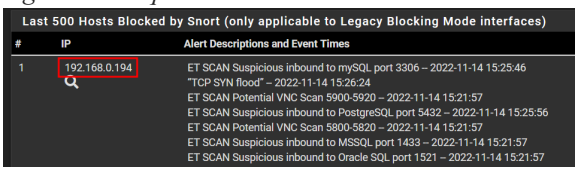
No ambiente com defesa em profundidade foi possível observar que ao executar o nmap para fazer o escaneamento de portas do alvo, foi observado que o mesmo obtém sucesso na primeira vez, porém a ferramenta snort, identifica o tráfego malicioso e faz o bloqueio do *IP* de origem dos ataques, assim as próximas requisições vindas deste mesmo endereço serão bloqueadas conforme figuras 8 e 9.

Figura 8: Escaneamento no ambiente 2



Fonte: Autor

Figura 9: Bloqueio scan ambiente 2

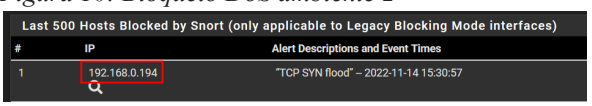


Fonte: Autor

4.3.2.2 Negação de serviço

Após usar o hping3 para direcionar um ataque de negação de serviço no ambiente 2, foi possível observar que novamente o snort bloqueou o tráfego malicioso, conforme figura 10.

Figura 10: Bloqueio DoS ambiente 2



Fonte: Autor

4.3.2.3 Injeção de código

O mesmo ataque de injeção de comando que foi direcionado com sucesso para o ambiente 1, foi direcionado neste momento para o ambiente 2. Foi observado que o *Web Application Firewall (WAF)* obteve sucesso no bloqueio do ataque como consta na figura 11, mostrando o código de erro 403 conforme configurado nas regras de segurança da ferramenta.

Figura 11: Bloqueio injeção de código ambiente 2

Fonte: Autor

5 CONSIDERAÇÕES FINAIS

O objetivo proposto na seção 3 deste artigo é demonstrar a eficiência de ambas estratégias na defesa contra alguns tipos de ataques comuns. Como foi observado na seção 4, o ambiente que foi implementado utilizando uma estratégia com apenas uma camada de segurança, o *firewall*, não obteve sucesso no bloqueio de nenhum dos ataques feitos contra ele. Embora as políticas de segurança existentes no *firewall* sejam configuradas de maneira correta e bem restritiva, sua função de bloquear acessos não permitidos não foi capaz de impedir nenhum dos ataques, isto se dá pelo fato de que o firewall utiliza informações como endereços de origem e destino para fazer liberações e bloqueios, assim sua forma de análise do tráfego e bastante superficial, o que impede que ele analise de forma mais profunda o tráfego que passa por ele, assim os ataques feitos contra o ambiente não foram vistos pela camada de segurança existente.

O ambiente implementado com a estratégia de defesa em profundidade, com 4 camadas de segurança, obteve sucesso no bloqueio de todos os ataques feitos contra o ambiente. Com a adição de várias camadas de segurança, os ataques podem passar por uma delas, porém mesmo que uma das camadas não faça o bloqueio do ataque, a

próxima provavelmente fará, se não a próxima, este é o objetivo de várias camadas, caso uma não consiga obter sucesso, as chances do bloqueio em outras camadas acontecer é grande. O *scan* executado não é visto pelo firewall, porém é identificado pelo *Intrusion Detection System (IDS)*, assim uma única vez o ataque acontece, após isso, como o tráfego foi identificado, o endereço de origem é bloqueado pelo *Intrusion Prevention System (IPS)* e assim o ataque não obtém sucesso nas próximas vezes. O ataque de negação de serviço também não é bloqueado pelo firewall, porém é identificado pelo *Intrusion Detection System (IDS)* e bloqueado imediatamente pelo *Intrusion Prevention System (IPS)*. Por fim, a injeção de código no site não é identificado pelo *firewall* e *pelo Intrusion Detection System (IDS)*, porém o *Web Application Firewall (WAF)* tem sucesso no bloqueio do mesmo pois possui uma análise mais profunda das requisições direcionadas ao site. Para cada ataque, foram feitas 3 tentativas de cada um contra ambos os ambientes, a tabela 5 mostra a efetividade de cada ambiente com a porcentagem de sucesso.

Tabela 5. Efetividade de cada ambiente

Ataque	Ambiente 1	Ambiente 2
Scan	0%	66.67%
Negação de serviço	0%	100%
Injeção de código	0%	100%

Fonte: Autor

REFERÊNCIAS

[1] ABNT. Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação: ABNT NBR ISO/IEC 27002:2005. 2a. ed. Rio de Janeiro, 2005.

[2] CERT.BR. **CERT.br Stats (janeiro a dezembro de 2020)**. 2020. Disponível em: https://www.cert.br/stats/incidentes/2020-jan-dec/total.html. Acesso em: 20 out. 2022.

[3] CHAKRABORTY, Nilotpal. Intrusion detection system and intrusion prevention system: A comparative study. **International Journal of Computing and Business Research (IJCBR)**, v. 4, n. 2, p. 1-8, 2013.

[4] DADHEECH, Krati; CHOUDHARY, Arjun; BHATIA, Gaurav. De-militarized zone: a next level to network security. In: **2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)**. IEEE, 2018. p. 595-600.

[5] GitHub - **Damn Vulnerable Web Application (DVWA).** 2022. Disponível em: https://github.com/digininja/DVWA

[6] Gordon “Fyodor” Lyon. **Chapter 15. Nmap Reference Guide**. 1997. Disponível em: https://nmap.org/book/man.html

[7] GROAT, Stephen; TRONT, Joseph; MARCHANY, Randy. Advancing the defense in depth model. In: **2012 7th International Conference on System of Systems Engineering (SoSE)**. IEEE, 2012. p. 285-290.

[8] GU, Qijun; LIU, Peng. Denial of service attacks. **Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications**, v. 3, p. 454-468, 2007.

[9] GUPTA, Namit; SAIKIA, Abakash; SANGHI, D. Web application firewall. **Indian Institute of Technology, Kanpur**, v. 61, p. 62, 2007.

[10] HORTON, Robin P. et al. Explaining intranet use with the technology acceptance model. **Journal of information technology**, v. 16, n. 4, p. 237-249, 2001.

[11] Oracle. **VirtualBox.** Disponível em: https://www.virtualbox.org/

[12] KEWLEY, Dorene L.; LOWRY, John. Observations on the effects of defense in depth on adversary behavior in cyber warfare. In: **Proceedings of the IEEE SMC Information Assurance Workshop**. 2001. p. 1-8.

[13] KUIPERS, David; FABRO, Mark. Control systems cyber security: Defense in depth strategies. 2006.

[14] MARTÍNEZ TORRES, Javier; IGLESIAS

COMESAÑA, Carla; GARCÍA-NIETO, Paulino J. Machine learning techniques applied to cybersecurity. **International Journal of Machine Learning and Cybernetics**, v. 10, n. 10, p. 2823-2836, 2019.

[15] Nginx. **Nginx documentation.** Disponível em: https://nginx.org/en/docs/

[16] OWASP. **OWASP Top 10:2021**. 2021. Disponível em: https://owasp.org/Top10/

[17] PFSense. **Netgates docs.** Disponível em: https://docs.netgate.com/pfsense/en/latest/general/index.html

[18] ROCHA, Carolina Borges. A evolução criminológica do Direito Penal: Aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012. **Jus Navigandi, Teresina, ano**, v. 18, 2013.

[19] SINGH, Rajni Ranjan; TOMAR, Deepak Singh. Network forensics: detection and analysis of stealth port scanning attack. **scanning**, v. 4, p. 8, 2015.

[20] SNORT. **Snort users manual 2.9.16.** Disponível em: http://manual-snort-org.s3-website-us-east-1.amazonaws.com/

[21] TAHA, Antonio Marco da Costa et al. Guia de testes de segurança para aplicações web. 2017.

[22] Kali Linux. **Kali Linux Features.** Disponível em: https://www.kali.org/features/

[23] WING, Dan. Network address translation: Extending the internet address space. **IEEE internet computing**, v. 14, n. 4, p. 66-70, 2010.