NSOC (Network Security Operation Center)

Sgt **PABLO PEREIRA** DA SILVA
Sgt **JAIME** DE MELO GAMA DA SILVA

***Resumo*—O objetivo principal do estudo sobre o NSOC (Network Security Operation Center) é desenvolver e implementar um centro de operações de segurança de rede usando ferramentas e tecnologias open-source como Zabbix, Pfsense, Snort, Vyos, Exos e GNS3. O objetivo do projeto é estabelecer um ambiente de monitoramento e resposta a incidentes cibernéticos que garantam a integridade, disponibilidade e confidencialidade dos ativos de rede da organização, detectando, analisando e mitigando ameaças em tempo real. As descobertas do estudo mostram que a implementação de um NSOC usando essas tecnologias de código aberto é viável e eficaz, oferecendo uma solução sólida para a segurança cibernética em redes corporativas. O novo sistema se destaca como uma ferramenta estratégica para proteger os ativos digitais, pois pode monitorar o tráfego de rede, descobrir problemas e responder rapidamente a incidentes. O uso de ferramentas open-source também permite uma personalização e escalabilidade maior do sistema, tornando-o uma opção viável para organizações que buscam melhorar sua postura de segurança cibernética sem comprometer o orçamento.**

***Palvras-chave*—NSOC. Zabbix. Pfsense. Snort. DMZ. Vyos. Exos. GNS3.**

***Abstract*— The main objective of the Network Security Operation Center (NSOC) study is to develop and implement a network security operations center using open-source tools and technologies such as Zabbix, Pfsense, Snort, Vyos, Exos, and GNS3. The goal of the project is to establish a cyber incident monitoring and response environment that ensures the integrity, availability, and confidentiality of the organization's network assets by detecting, analyzing, and mitigating threats in real time. The study's findings show that implementing an NSOC using these open-source technologies is feasible and effective, offering a solid solution for cyber security in corporate networks. The new system stands out as a strategic tool for protecting digital assets, as it can monitor network traffic, discover issues, and respond quickly to incidents. The use of open-source tools also allows for greater customization and scalability of the system, making it a viable option for organizations looking to improve their cyber security posture without compromising their budget.**

***Keywords*— NSOC. Zabbix. Pfsense. Snort. DMZ. Vyos. Exos. GNS3.**

I. INTRODUÇÃO

Uma instalação conhecida como centro de operações de segurança de rede (NSOC) abriga uma equipe de segurança da informação que monitora e avalia regularmente a posição de segurança de uma organização [1].

O objetivo da equipe do NSOC é detectar, analisar e responder os incidentes de segurança cibernética usando uma série de processos e soluções tecnológicas. Em geral, os centros de operações de segurança têm analistas e engenheiros de segurança, além de gerentes que supervisionam os procedimentos de segurança [2].

A equipe do NSOC trabalha em conjunto com as equipes de resposta a incidentes para garantir que os problemas de segurança sejam resolvidos rapidamente durante e/ou após a descoberta. Os centros de operações de segurança monitoram e analisam as atividades dos ativos de suas redes, como servidores, terminais de usuários, bancos de dados, aplicativos, sites e outros sistemas, para detectar incidentes ou ativos comprometidos [3].

Neste projeto, propomos a criação de um NSOC (Network Security Operations Center) utilizando o simulador de redes GNS3. Para a construção desse NSOC, serão empregados dis- positivos como roteadores Vyos e Exos, além de ferramentas como Zabbix e Pfsense.

II.Referencial Teórico

Registrar pacotes com facilidade. Ele também pode registrar pacotes do protocolo de controle de transmissão TCP. Ele é um sistema sofisticado de prevenção à intrusão, registrador de pacotes e sniffer de pacotes. A análise de protocolo pode detectar ataques de buffer overflow, stealth port scans, ataques CGI, SMB probes, identificação do sistema operacional, entre outros ataques [13].

A.Zabbix

O Zabbix [4] é uma ferramenta de monitoramento de código aberto projetada para monitorar a infraestrutura de rede. Ele pode monitorar redes, servidores, máquinas virtuais e serviços em nuvem. Essa ferramenta funciona para o monitoramento convencional e monitoramento de serviços simples sem a necessidade do uso de agentes, possui suporte nativo ao protocolo SNMP e disponibiliza uma interface web para a administração e monitoramento dos dados, onde pode ser configurado alertas de sistema para comunicação com o gerenciador da rede [5].

A coleta de dados, a ativação de triggers e o envio de notificações aos usuários são feitos pelo componente central da gerência do Zabbix. Os agentes e proxys que monitoramos dispositivos fornecem informações ao servidor Zabbix. A instalação deste servidor deve ocorrer em sistemas Unix ou Linux [6].

Zabbix Proxy é uma ferramenta que pode ser usada de forma opcional para monitorar e centralizar dados em infraestrutura de TI de forma remota. Ele transmite os dados coletados parao servidor Zabbix. O agente Zabbix é instalado nos hosts e pode usar scripts para capturar métricas como uso de CPU, memória e métricas personalizadas. É com base nesses dados que você pode criar gráficos personalizados para o usuário [7].

B. Pfsense

O pfsense [8], baseado no FreeBSD e projetado para funcionar tanto como firewall quanto como roteador, é um dos firewalls opensource mais conceituados e robustos disponíveis no mercado atualmente.

O pfsense é um firewall baseado em software que protege a rede monitorando o tráfego de entrada e saída e tomando decisões de permitir ou bloquear tráfego específico de acordo com as regras de segurança definidas [9].

Uma das principais vantagens de usar o pfsense é que ele é Open Source, estável, leve e possui uma licença de código aberto. Além disso, ele não exige hardware muito grande. Ele possui algumas características que facilitam a utilização, como uma interface WEB fácil de usar, uma grande variedade de pacotes de software, visualização de ambiente em tempo real e gerenciamento de ameaças unificadas [10].

C. Snort

A segurança da informação é um componente crucial do monitoramento de tráfego em uma rede de computadores. O Snort [11] é um IDS (Sistema de detecção de intrusão) bem conhecido e amplamente utilizado porque não requer muito poder de processamento e é fornecido como software livre, gratuito e mantido pela Cisco via rede [12].

O Snort se destaca por analisar tráfegos em tempo real e registrar pacotes com facilidade. Ele também pode registrar pacotes do protocolo de controle de transmissão TCP. Ele é um sistema sofisticado de prevenção à intrusão, registrador de pacotes e sniffer de pacotes. A análise de protocolo pode detectar ataques de buffer overflow, stealth port scans, ataques CGI, SMB probes, identificação do sistema operacional, entre outros ataques [13].

D. SNMP versão 3

O protocolo padrão chamado Simple Network Management Protocol (SNMP) é usado para gerenciar dispositivos em redes de computadores e na internet. Existem várias versões do SNMP, mas as 2c (SNMPv2c) e 3 (SNMPv3) são as mais usadas. O SNMPv3 é o mais recente e seguro. Foi introduzido para corrigir os problemas de segurança encontrados nas versões anteriores do protocolo [14]. O SNMPv3 tem as seguintes características principais:

- Autenticação: A SNMPv3 suporta forte autenticação, o que significa que as mensagens SNMP são autenticadas para garantir que são enviadas por uma fonte confiável. O HMAC-MD5-96 e o HMAC-SHA-96 são métodos de validação.
- Privacidade (Criptografia): É possível criptografar as mensagens SNMP para proteger os dados durante a transmissão. Isso é executado principalmente com o protocolo DES, mas pode também suportar o AES.

- Controle de Acesso: A SNMPv3 inclui controles de acesso mais complexos, o que permite que os administra- dores configurem permissões específicas para quem podeacessar informações em um dispositivo de rede.

Por fim, a SNMPv3 é recomendada para ambientes com altos requisitos de segurança devido às suas capacidades avançadas de autenticação e criptografia, enquanto a SNMPv2cpode ser usada em ambientes menos críticos onde a compati- bilidade e a simplicidade são mais importantes [15].

III. METODOLOGIA

Para a construção da topologia deste trabalho, utilizou- se o simulador GNS3 [16]. No GNS3, foram empregadas appliances de roteadores VyOS e Exos, ferramentas do PfSense e do Zabbix, sistemas operacionais Ubuntu 18.04 e Kali Linux, além das appliances nativas do GNS3, como modem, switch e VPCS.

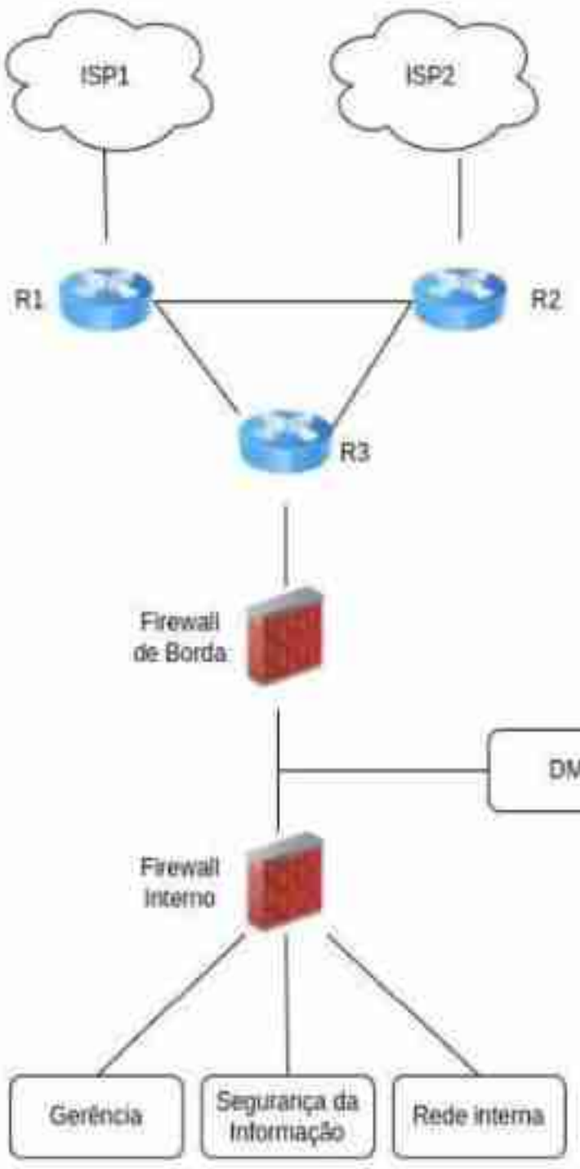
O trabalho foi desenvolvido utilizando uma metodologia científica que combina pesquisa aplicada, metodologia experimental, estudo de caso, e simulação. Usando ferramentas de código aberto em um ambiente simulado, o estudo se concentrou na implementação prática e avaliação de um Network Security Operation Center (NSOC). A técnica experimental permitiu o teste de algumas configurações e a análise da eficácia das tecnologias usadas para detectar e proteger ameaças cibernéticas. Além disso, uma pesquisa de desenvolvimento tecnológico ajudou a desenvolver soluções úteis para monitoramento e segurança de redes [17].

IV. TOPOLOGIA

A topologia proposta é ilustrada na Figura 1, sendo composta por um Backbone de ISPs, uma área DMZ, uma área de Gerência, uma área de Segurança da Informação e uma Rede Interna. A estrutura também inclui dois firewalls: um firewall de borda e um firewall interno.

Para simular essa topologia, foi utilizado o software GNS3. O GNS3 (Graphical Network Simulator-3) uma ferramenta de simulação de redes que permite a criação e teste de topologias de rede. Ele oferece uma interface gráfica que facilita a configuração e o gerenciamento de dispositivos de rede, como roteadores, switches e firewalls, possibilitando simulações em um ambiente controlado. A topologia proposta no GNS3 está exposta na Figura 2

Figura 1: Topologia Proposta



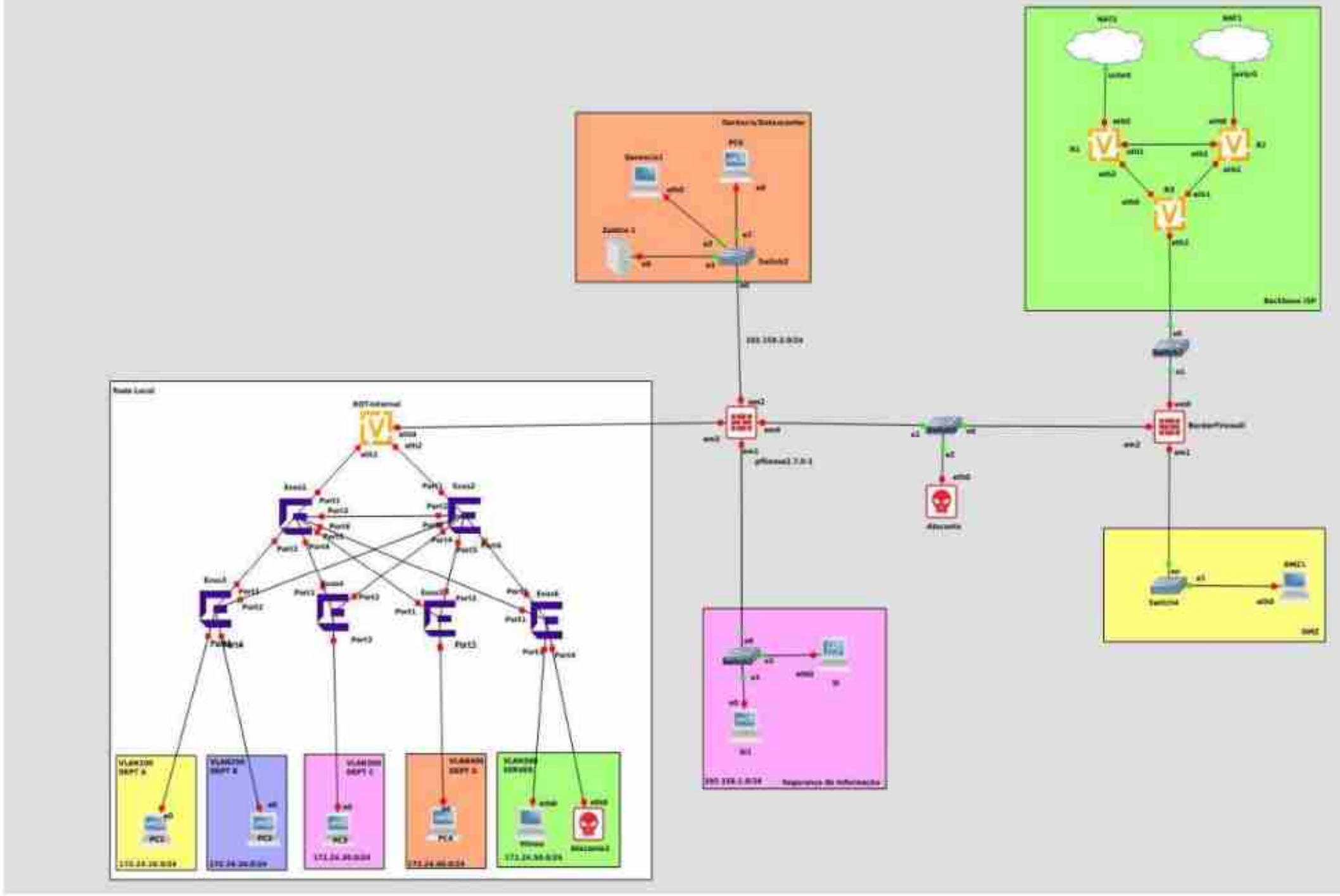


Figura 2: Topologia Proposta No GNS3

V. Backbone de Provedores de Internet

Foi criada uma área de simulação de provedores de internet, que inclui duas nuvens NAT e três roteadores VyOS. A utilização de duas nuvens NAT visa proporcionar redundância de rede, garantindo maior confiabilidade e disponibilidade dos serviços.

Essa será a área responsável por prover acesso à internet para todos os dispositivos da topologia. Em uma rede, os provedores de internet (ISPs - Internet Service Providers) são entidades que oferecem serviços de conectividade à internet para usuários finais, empresas e outras organizações.

A área utiliza o intervalo de IP 192.168.15.0/24 como base. Os IPs atribuídos a cada interface podem ser visualizados na Tabela I.

Dispositivo	Interface	IP/Máscara
R1	eth0	via DHCP Nuvem
	eth1	192.168.15.1/28
	eth2	192.168.15.17/28
R2	eth0	via DHCP nuvem
	eth1	192.168.15.14/28
	eth2	192.168.15.33/28
R3	eth0	192.168.15.30/28
	eth1	192.168.15.46/28
	eth2	192.168.15.49/28

Tabela I: Tabela de roteadores da área de provedores

Para a distribuição de rotas, foi configurado o protocolo OSPF em todos os roteadores da área de provedores. A utilização do OSPF (Open Shortest Path First) elimina a necessidade de cadastrar manualmente as rotas entre os roteadores, simplificando a administração da rede.

A configuração do OSPF no roteador R1 pode ser visualizada na Figura 3, enquanto a sua tabela de roteamento está apresentada na Figura 4.

A configuração do OSPF no roteador R2 pode ser visualizada na Figura 5, enquanto a sua tabela de roteamento está apresentada na Figura 6.

A configuração do OSPF no roteador R3 pode ser visualizada na Figura 7, enquanto a sua tabela de roteamento está apresentada na Figura 8.

No roteador R3, foi configurado um servidor DHCP na interface eth3 para que o firewall de borda pudesse receber automaticamente o IP e o gateway dessa sub-rede. Isso elimina a necessidade de configurar manualmente os endereços IP e os gateways nos dispositivos conectados. Além disso, garante uma configuração consistente e correta, reduzindo a probabilidade de erros de configuração.

Para testar a redundância dos ISPs, foi realizado um teste de ping no servidor gns3 com o endereço IP 192.168.122.1. Inicialmente, verificou-se que, no roteador R3, a rota utilizada passava pelo roteador R2. Para validar a funcionalidade da

```
vyos@vyos# show protocols ospf
 area 0 {
     network 192.168.122.0/24
     network 192.168.15.0/28
     network 192.168.15.16/28
 }
 default-information {
     originate {
         metric 10
         metric-type 2
     }
 }
 log-adjacency-changes {
 }
 parameters {
     router-id 10.1.1.1
 }
 redistribute {
     connected {
         metric-type 2
         route-map CONNECT
     }
 }
[edit]
vyos@vyos#
```

Figura 3: Configuração do OSPF do roteador R1

```
vyos@vyos:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O>* 0.0.0.0/0 [110/10] via 192.168.122.1, eth0, 00:05:06
S   0.0.0.0/0 [210/0] via 192.168.122.1, eth0, 00:06:07
C>* 10.1.1.1/32 is directly connected, lo, 00:06:12
O>* 10.2.2.2/32 [110/20] via 192.168.15.14, eth1, 00:05:06
  *                     via 192.168.122.160, eth0, 00:05:06
O>* 10.3.3.3/32 [110/20] via 192.168.15.30, eth2, 00:04:23
O   192.168.15.0/28 [110/100] is directly connected, eth1, 00:06:10
C>* 192.168.15.0/28 is directly connected, eth1, 00:06:12
O   192.168.15.16/28 [110/100] is directly connected, eth2, 00:06:10
C>* 192.168.15.16/28 is directly connected, eth2, 00:06:11
O>* 192.168.15.32/28 [110/200] via 192.168.15.14, eth1, 00:04:24
  *                            via 192.168.15.30, eth2, 00:04:24
  *                            via 192.168.122.160, eth0, 00:04:24
O>* 192.168.15.48/28 [110/200] via 192.168.15.30, eth2, 00:04:24
O   192.168.122.0/24 [110/100] is directly connected, eth0, 00:05:07
C>* 192.168.122.0/24 is directly connected, eth0, 00:06:08
```

Figura 4: Tabela de Roteamento do roteador R1

```
vyos@vyos# show protocols ospf
 area 0 {
     network 192.168.122.0/24
     network 192.168.15.0/28
     network 192.168.15.32/28
 }
 default-information {
     originate {
         metric 10
         metric-type 2
     }
 }
 log-adjacency-changes {
 }
 parameters {
     router-id 10.2.2.2
 }
 redistribute {
     connected {
         metric-type 2
         route-map CONNECT
     }
 }
[edit]
vyos@vyos#
```

Figura 5: Configuração do OSPF do roteador R2

```
vyos@vyos:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O>* 0.0.0.0/0 [110/10] via 192.168.122.1, eth0, 00:13:26
S   0.0.0.0/0 [210/0] via 192.168.122.1, eth0, 00:14:08
O>* 10.1.1.1/32 [110/20] via 192.168.15.1, eth1, 00:13:20
  *                      via 192.168.122.38, eth0, 00:13:20
C>* 10.2.2.2/32 is directly connected, lo, 00:14:12
O>* 10.3.3.3/32 [110/20] via 192.168.15.46, eth2, 00:12:44
O   192.168.15.0/28 [110/100] is directly connected, eth1, 00:14:11
C>* 192.168.15.0/28 is directly connected, eth1, 00:14:12
O>* 192.168.15.16/28 [110/200] via 192.168.15.1, eth1, 00:12:45
  *                            via 192.168.15.46, eth2, 00:12:45
  *                            via 192.168.122.38, eth0, 00:12:45
O   192.168.15.32/28 [110/100] is directly connected, eth2, 00:14:11
C>* 192.168.15.32/28 is directly connected, eth2, 00:14:12
O>* 192.168.15.48/28 [110/200] via 192.168.15.46, eth2, 00:12:45
O   192.168.122.0/24 [110/100] is directly connected, eth0, 00:14:08
C>* 192.168.122.0/24 is directly connected, eth0, 00:14:08
```

Figura 6: Tabela de Roteamento do roteador R2

```
vyos@vyos# show protocols ospf
 area 0 {
     network 192.168.15.16/28
     network 192.168.15.32/28
     network 192.168.15.48/28
 }
 default-information {
     originate {
         metric 10
         metric-type 2
     }
 }
 log-adjacency-changes {
 }
 parameters {
     abr-type cisco
     router-id 10.3.3.3
 }
 redistribute {
     connected {
         metric-type 2
         route-map CONNECT
     }
 }
[edit]
vyos@vyos#
```

Figura 7: Configuração do OSPF do roteador R3

```
vyos@vyos:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O>* 0.0.0.0/0 [110/10] via 192.168.15.17, eth0, 00:13:56
  *                    via 192.168.15.33, eth1, 00:13:56
O>* 10.1.1.1/32 [110/20] via 192.168.15.17, eth0, 00:13:56
O>* 10.2.2.2/32 [110/20] via 192.168.15.33, eth1, 00:14:08
C>* 10.3.3.3/32 is directly connected, lo, 00:14:20
O>* 192.168.15.0/28 [110/200] via 192.168.15.17, eth0, 00:13:57
  *                           via 192.168.15.33, eth1, 00:13:57
O   192.168.15.16/28 [110/100] is directly connected, eth0, 00:14:06
C>* 192.168.15.16/28 is directly connected, eth0, 00:14:18
O   192.168.15.32/28 [110/100] is directly connected, eth1, 00:14:01
C>* 192.168.15.32/28 is directly connected, eth1, 00:14:17
O   192.168.15.48/28 [110/100] is directly connected, eth2, 00:14:17
C>* 192.168.15.48/28 is directly connected, eth2, 00:14:17
O>* 192.168.122.0/24 [110/200] via 192.168.15.17, eth0, 00:13:57
  *                            via 192.168.15.33, eth1, 00:13:57
vyos@vyos:~$
```

Figura 8: Tabela de Roteamento do roteador R3

redundância, o roteador R2 foi pausado, forçando o roteador R3 a encontrar uma rota alternativa através do roteador R1, conforme mostrado na Figura 9.

A. SNMP versão 3 no Vyos

Para que a equipe de gerência pudesse administrar corretamente todos os dispositivos necessários da topologia, foi necessário configurar o protocolo SNMPv3 nos roteadores. Como todos os roteadores são VyOS, a configuração foi a mesma em todos os dispositivos, alterando apenas os IPs. Uma demonstraçao da configuração pode ser visto no Código 1.

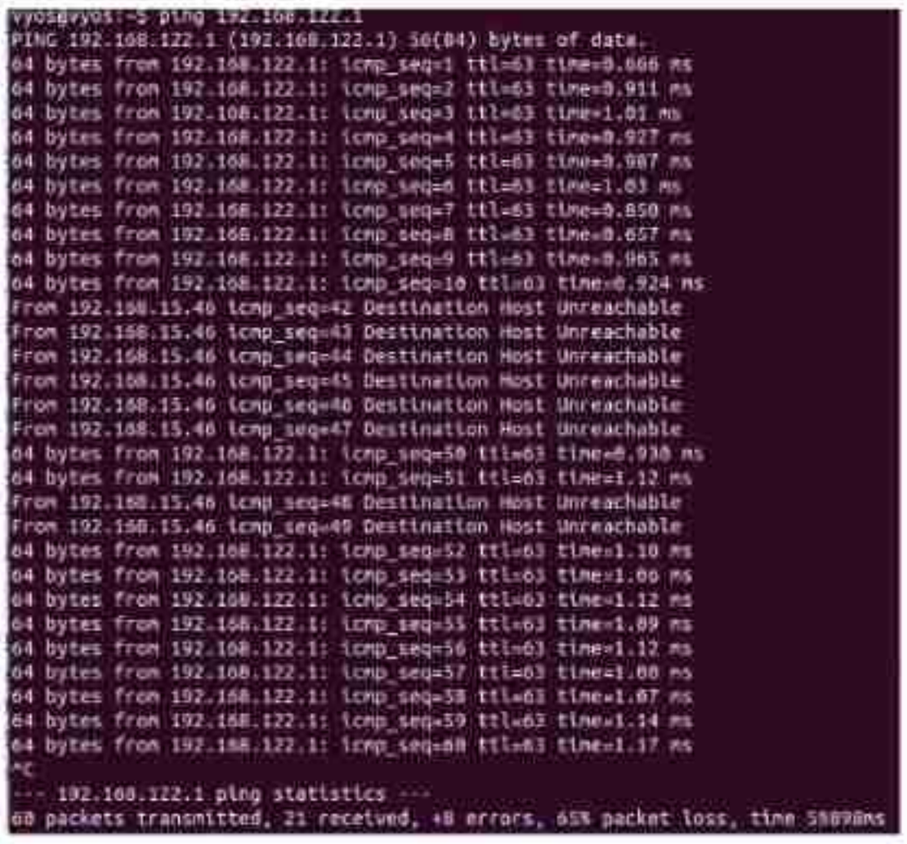


Figura 9: Ping para teste da redundância de ISPs

```
set service snmp listen-address 192.168.15.1
set service snmp listen-address 192.168.15.17
set service snmp location 'VyosISP'
set service snmp v3 engineid '000000000000000000000002'
set service snmp v3 view snmpview1 oid 1
set service snmp v3 group vyosgroup mode ro
set service snmp v3 group vyosgroup seclevel priv
set service snmp v3 group vyosgroup view snmpview1
set service snmp v3 user vyos auth plaintext-key xeglannajaime
set service snmp v3 user vyos auth type 'sha'
set service snmp v3 user vyos group vyosgroup
set service snmp v3 user vyos privacy plaintext-key xeglannajaime
set service snmp v3 user vyos privacy type 'aes'
```

Código 1: Configuração do SNMP versão 3 no Vyos

Para a configuração do SNMPv3, foi criado um grupo chamado "vyosgroup", associado ao OID 1. O OID (Object Identifier) é um identificador usado para especificar uma determinada variável ou objeto gerenciado na MIB (Management Information Base).

O grupo "vyosgroup"foi configurado no modo "ro"(read-only), o que significa que os usuários deste grupo têm permissão apenas para ler informações dos dispositivos gerenciados.

Além disso, o grupo foi configurado com autenticação SHA (Secure Hash Algorithm) e privacidade AES (Advanced Encryption Standard). A autenticação SHA garante que apenas usuários autorizados possam acessar o dispositivo, enquanto a privacidade AES criptografa os dados transmitidos, protegendo contra interceptações e garantindo a confidencialidade das informações.

Esse padrão de configuração do SNMPv3 foi seguido em toda a topologia.

VI. Firewall de Borda

O firewall de borda é importante para a segurança de uma rede. Ele atua como a primeira linha de defesa contra ameaças externas, bloqueando tráfego malicioso e impedindo tentativas de invasão. Além disso, o firewall regula o tráfego de entrada e saída, permitindo apenas o acesso autorizado aos recursos da rede e impedindo acessos não autorizados.

O pfSense foi escolhido como firewall de borda nesta topologia, pois ele oferece recursos como prevenção e detecção de intrusões (IDS/IPS), VPNs para conexões seguras, e filtragem de conteúdo, além de possuir uma interface web que facilita a administração.

Foram utilizadas três interfaces no firewall de borda: a interface em0 conecta-se à área de ISPs, a interface em1 liga-se à área DMZ, e a interface em2 estabelece conexãocom o firewall interno. Os IPs do firewall de borda pode ser visualizada na Figura 10.

```
WAN (wan)       -> em0      -> v4/DHCP4: 192.168.15.50/28
LAN (lan)       -> em1      -> v4: 192.168.1.1/24
OPT1 (opt1)     -> em2      -> v4: 192.168.2.1/24
```

Figura 10: Configuração dos IPs do Firewall de Borda

A interface em0 recebe seu IP através do servidor DHCP do roteador R3 da área de provedores. As demais interfaces possuem endereços IP na faixa 192.168.0.0/16. Especificamente, a interface em1 está configurada na subrede 192.168.1.0/24, enquanto a interface em2 está na subrede 192.168.2.0/24.

As interfaces em1 e em2 também possuem servidores DHCP configurados. Isso permite que essas interfaces atribuam automaticamente endereços IP a dispositivos conectados a elas.

Para configurar o DHCP no pfSense, é preciso acessar a guia *Services -> DHCP Server* e selecionar a interface desejada. Em seguida, é necessário informar o intervalo de IPs disponíveis para serem atribuídos aos dispositivos da rede. Isso permite que o pfSense gerencie dinamicamente a atribuição de endereços IP dentro desse intervalo.

Embora não tenham sido configuradas regras de firewall para as interfaces do firewall de borda, é importante notar que a área da DMZ funciona de forma isolada, sem qualquer conhecimento da rede interna, que inclui as áreas de gerência, segurança da informação e rede local. Essa estratégia de isolamento garante a segurança da rede interna, protegendo-a de possíveis ameaças que possam surgir na DMZ. Ao restringir o acesso direto da DMZ à rede interna, diminui a superficie de ataque e os riscos a infraestrutura interna.

A. SNMP versão 3 no Pfsense

No pfSense, foi possível habilitar e configurar o protocolo SNMPv3 através da instalação de um pacote externo chamado "net-snmp", configurado para utilizar o protocolo UDP na porta 161.

Assim como no VyOS, foi configurado um usuário com permissões de leitura apenas (read-only), utilizando autenticação SHA e privacidade AES, como mostra a Figura 11.

É importante ressaltar que, para que este pacote funcione corretamente, o serviço SNMP nativo do pfSense deve ser desabilitado.

B. Sistemas de prevenção e detecção de intrusão

Para a detecção e prevenção de intrusões, foi implementado o Snort no firewall de borda. O Snort é um sistema capaz de monitorar o tráfego de rede em tempo real, identificar padrões suspeitos ou maliciosos e tomar medidas para mitigar possíveis ameaças.

Figura 11: Configuração do SNMPv3 no pfsense

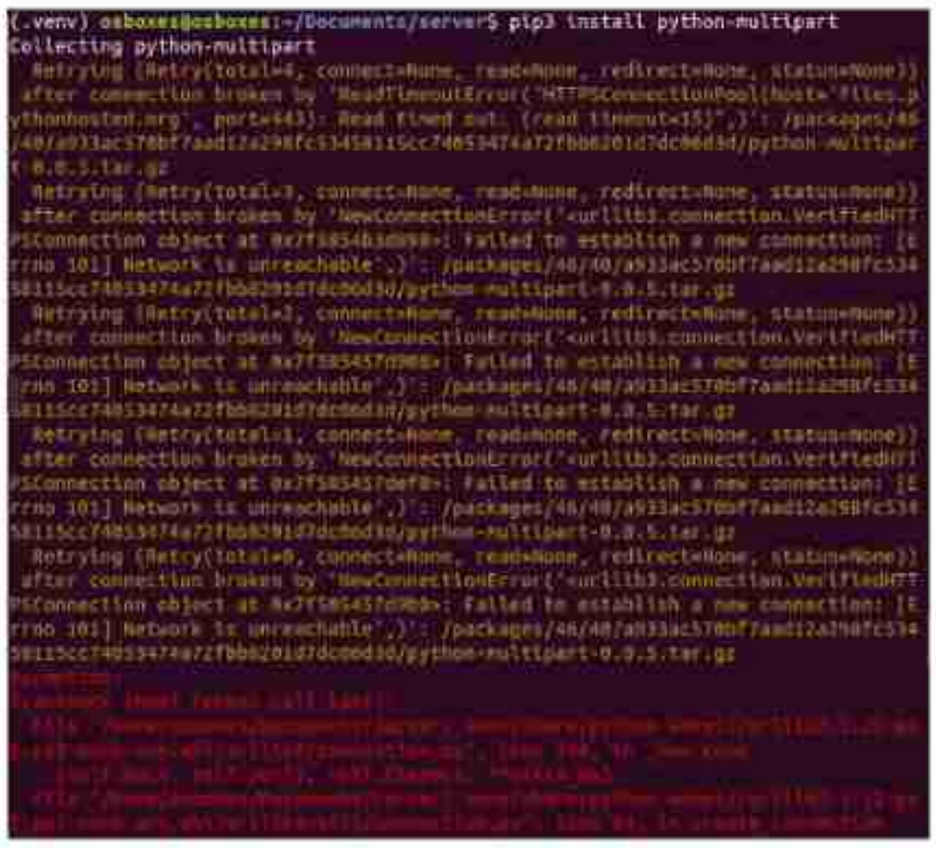


Figura 13: pyhosted.org sendo bloquado pelo IPS do Snort

O Snort não é uma ferramenta nativa no pfSense, sendo necessário instalá-lo através do Gerenciador de Pacotes disponível, com o nome "snort". Além disso, para utilizar o pacote, é necessário obter um código do Snort Oinkmaster, que pode ser adquirido na página oficial do Snort.

O Snort foi habilitado nas três interfaces ativas do firewall de borda, com mostra a Figura 12. As configurações padrão do pfSense já constituem um IDS. Para habilitar o IPS, é necessário, nas configurações de interface, ativar as opções "Block Offender"e "Kill States". Isso fará com que, ao detectar um alerta, o Snort bloqueie o host e rejeite a comunicação.

Figura 12: Configuração do Snort nas Interfaces

Por padrão, muitos IPs são bloqueados pelo IPS, incluindo os IPs associados aos pacotes do Ubuntu e do Python, como mostra Figura.13. Supondo que existam desenvolvedores python nas áreas da topologia, foi necessário criar uma lista de permissões (whitelist) contendo o IP do pyhosted.org, permitindo que os desenvolvedores acessem e baixem bibliotecas Python via pip. Isso garante que o acesso aos recursos necessários seja concedido de forma segura, enquanto mantém a integridade e a segurança da rede.

Deve-se incluir os IPs necessários para o funcionamento e desenvolvimento nas áreas específicas da topologia na lista de permissões (pass list) do Snort, garantindo que esses IPs não sejam bloqueados pelo sistema de prevenção de intrusões. Isso assegura que o tráfego legítimo relacionado às atividades de operação e desenvolvimento da rede não seja interrompido, enquanto se mantém a segurança e a integridade do ambiente de rede.

VII. Firewall Interno

Enquanto o firewall de borda protege a rede como um todo contra ameaças externas, o firewall interno é usado para garantir a segurança dentro da própria rede, controlando o tráfego entre diferentes partes da infraestrutura interna.

O firewall interno é posicionado dentro da rede interna, aplicando políticas de segurança específicas para diferentes grupos de usuários e dispositivos, ele é utilizado para segmentar a rede interna e controlar o tráfego entre diferentes partes da infraestrutura interna.

O pfSense também foi escolhido como firewall interno nesta configuração. A interface em0 está conectada ao firewall externo, a interface em1 está ligada à área de segurança da informação, a interface em2 está conectada à área de gerência e a interface em3 está conectada à área de rede local. A tabela de IPs correspondente pode ser visualizada na Figura 14.

Figura 14: Configuração dos IPs do Firewall Interno

A interface em0 recebe seu IP através do servidor DHCP do firewall de borda. As demais interfaces possuem endereços IP na faixa 192.158.0.0/16. Especificamente, a interface em1 está configurada na subrede 192.158.1.0/24, a interface em2 está na subrede 192.158.2.0/24, enquanto a interface em3 está na subrede 192.158.3.0/24.

As interfaces em1, em2 e em3 possuem servidores DHCP configurados. Isso permite que essas interfaces atribuam automaticamente endereços IP a dispositivos conectados a elas.

O protocolo SNMPv3 também foi configurado no firewall interno, utilizando as mesmas configurações aplicadas no firewall de borda, conforme descrito na subseção VI-A.

A. Regras do firewall interno

Para o controle de tráfego da rede, foram estabelecidas algumas regras de segurança no firewall interno:

- A área de gerência terá acesso a toda a topologia.
- Nenhuma outra área terá permissão para acessar a área de gerência.
- A área de rede local não terá acesso à área de segurança da informação.

Essas regras foram implementadas para garantir a integridade e a segurança da rede, limitando o acesso apenas as áreas autorizados e impedindo comunicações não autorizadas entre áreas específicas da infraestrutura. Essas configurações podem ser vizualizadas na Figura 15.

Para permitir que a área de gerência possa acessar os departamentos da rede local, foi necessário configurar uma rota estática no firewall interno. Essa rota encaminha todo o tráfego destinado à rede 172.24.0.0/16 para o gateway 192.168.3.10, que é o endereço associado à interface eth0 do ROT-Internal.

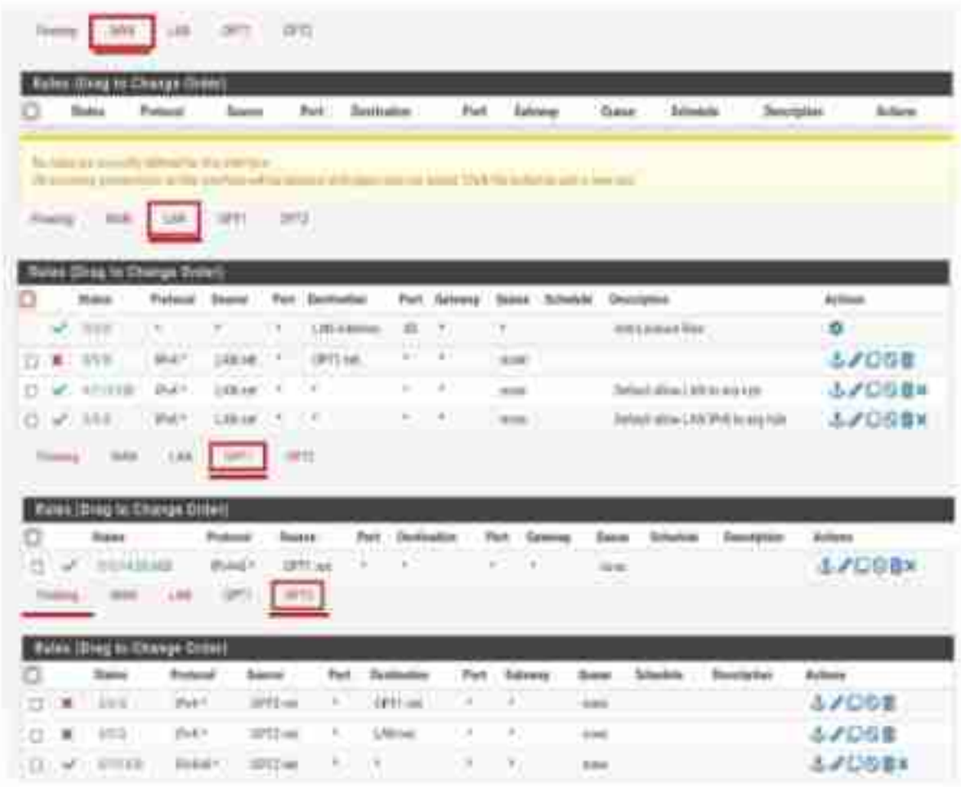


Figura 15: Configuração das regras no firewall interno

VIII. Rede Local

A área nomeada como rede local, é onde estão os diferentes departamentos ou setores de uma organização, simulando um ambiente de trabalho interno. Nessa topologia, cada departamento pode ser considerado uma subdivisão da rede local, com suas próprias necessidades de comunicação e segurança.

Foi implementado um backbone da rede local com redundância, utilizando 1 roteador VyOS e 2 dispositivos Exos, que operam na camada de rede 3, desempenhando o papel de roteadores. Essa configuração visa garantir alta disponibilidade e tolerância a falhas na infraestrutura de rede local.

Foram implementados também 4 dispositivos Exos que operam na camada de rede 2, desempenhando a função de switches.

Os três dispositivos que atuam como roteadores na rede local têm o protocolo OSPF configurado. Além disso, os dois roteadores Exos também têm o protocolo DHCP configurado, permitindo que os usuários dos departamentos da topologia recebam endereços IP automaticamente.

A rede base utilizada nas VLANs do backbone e nos departamentos da rede interna possui o endereço IP base 172.24.0.0/16. Para configurar e conectar o VyOS com os Exos, foi necessário criar VLANs.

A configuração das VLANs no ROT-Internal pode ser vista na Figura 16, enquanto a configuração das VLANs no Exos1 e Exos2 pode ser visualizada nas Figuras 17 e 18, respectivamente.

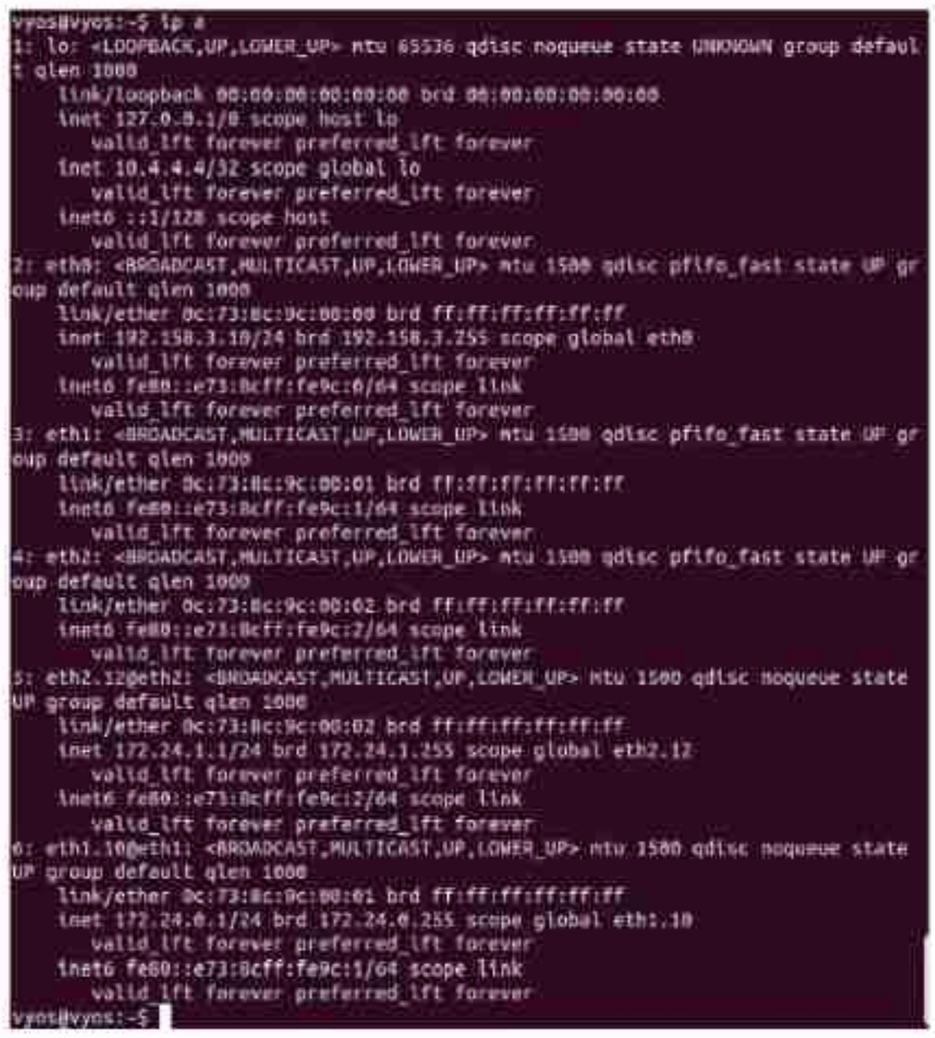


Figura 16: Configuração dos IPs do ROT-Internal

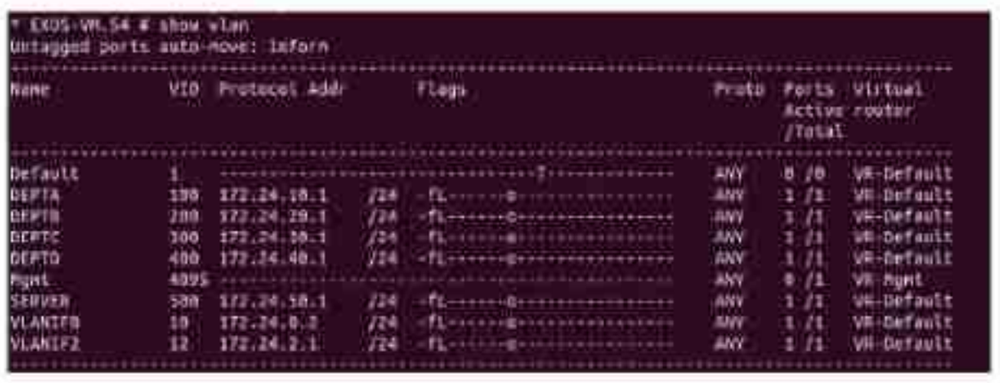


Figura 17: Configuração dos IPs do Exos1

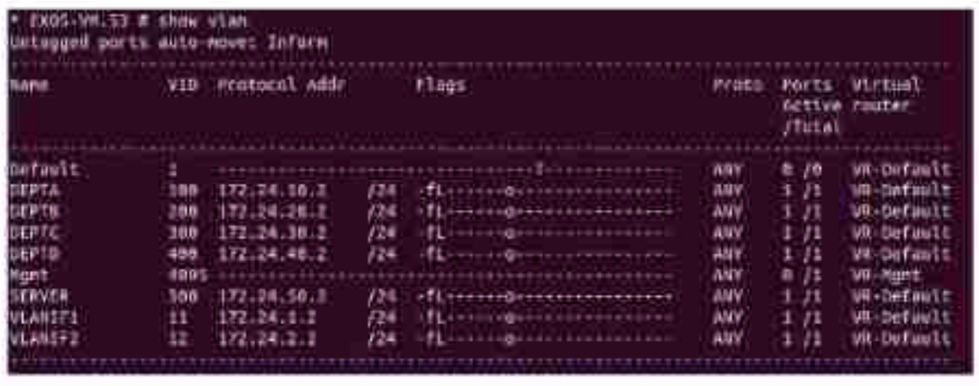


Figura 18: Configuração dos IPs do Exos2

A. SNMPv3 no Exos

A configuração do SNMPv3 no Exos seguiu o mesmo padrão já utilizado nos roteadores VyOS e no pfSense. Um usuário foi criado, com autenticação SHA e privacidade AES habilitadas, conforme ilustrado no Código 2.

```
configure snmpv3 add user exosuser authentication sha seglannajaime priv
aes seglannajaime

configure snmpv3 add group exosgroup user exosuser sec-model usm

configure snmpv3 add access exosgroup sec-model usm sec-level priv
read-view default Admin View write-view default Admin View notify-view default Admin View

enable snmp access snmpv3
```

Código 2: Configuração do SNMP versão 3 no Exos

A configuração foi realizada nos dois dispositivos Exos que operam na camada 3, não sendo necessária nos Exos que funcionam apenas como switches.

IX. DATASCENTER/GERÊNCIA

A área de gerência de redes é onde será feito o monitoramento e controle dos dispositivos e serviços da topologia. Para isso, será utilizado o Zabbix, que supervisiona o desempenho da rede, detecta e soluciona problemas, além de garantir a segurança.

Para descobrir todos os dispositivos da topologia, é necessário configurar o protocolo SNMPv3 em todos os dispositivos relevantes.

Para a busca dinâmica dos dispositivos no Zabbix, é necessário configurar regras de descoberta na aba Configuration -> Discovery. Foram cadastradas três regras: a primeira para encontrar os dispositivos conectados ao firewall de borda, a segunda para encontrar os dispositivos conectados ao firewall interno, e a terceira para encontrar os dispositivos da rede local, conforme mostrado na Figura 19. Para cada regra, foi informado os ranges de IPs que deveriam ser procurados.

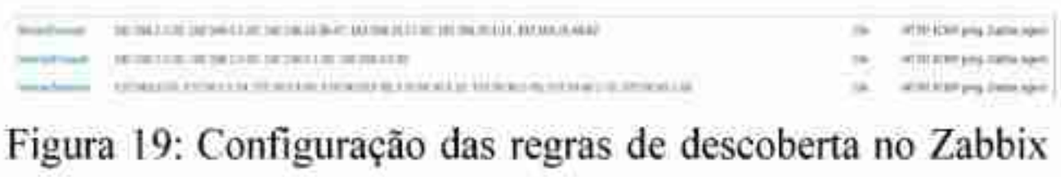


Figura 19: Configuração das regras de descoberta no Zabbix

Para maior automação, também foram criadas ações de descoberta (Actions) no Zabbix, permitindo a adição automática desses hosts encontrados aos grupos de hosts escolhidos, especificando novamente os intervalos de IP necessários, como mostra a Figura 20

Figura 20: Configuração das Actions no Zabbix

Isso permitiu, através dos grupos de hosts criados, a criação do mapa da topologia, que foi simplificado para melhor visualização, conforme mostrado na Figura 21.

É importante notar que nem todos os dispositivos da topologia possuem o protocolo SNMPv2 ou v3 configurado, como, por exemplo, os computadores com Ubuntu.

Para monitorar as interfaces dos dispositivos, é necessário configurar o protocolo SNMPv3 em todos os hosts relevantes. Um exemplo dessa configuração no Zabbix pode ser visualizado na Figura 22.

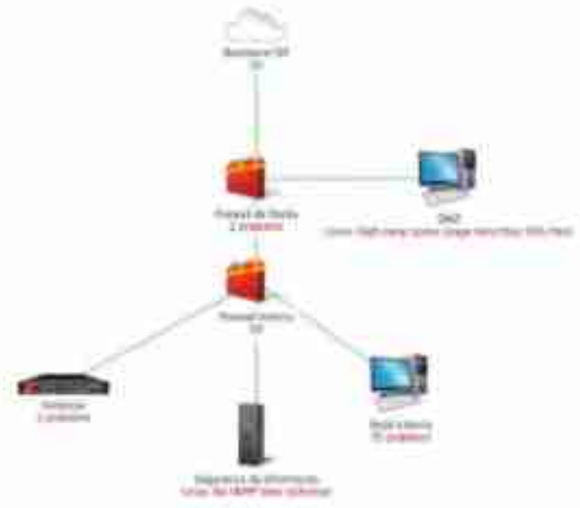


Figura 21: Mapa da topologia no Zabbix

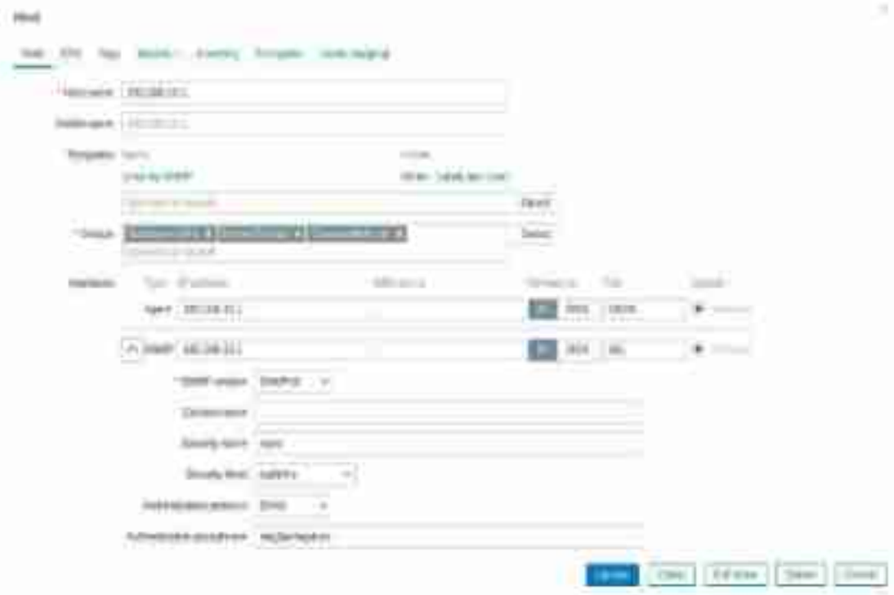


Figura 22: Exemplo de configuração do SNMPv3 nos hosts do Zabbix

O template do Zabbix, que é um conjunto pré-configurado de itens, gráficos e ações de monitoramento aplicáveis a múltiplos hosts, o escolhido para todos os hosts foi o "Linux by SNMP". Este template foi selecionado por oferecer bons gráficos e dashboards, que exibem informações como espaço de disco utilizado e tráfego de rede em todas as interfaces. Exemplos dos gráficos gerados para os hosts gerenciados podem ser visualizados nas Figuras 23 e 24.

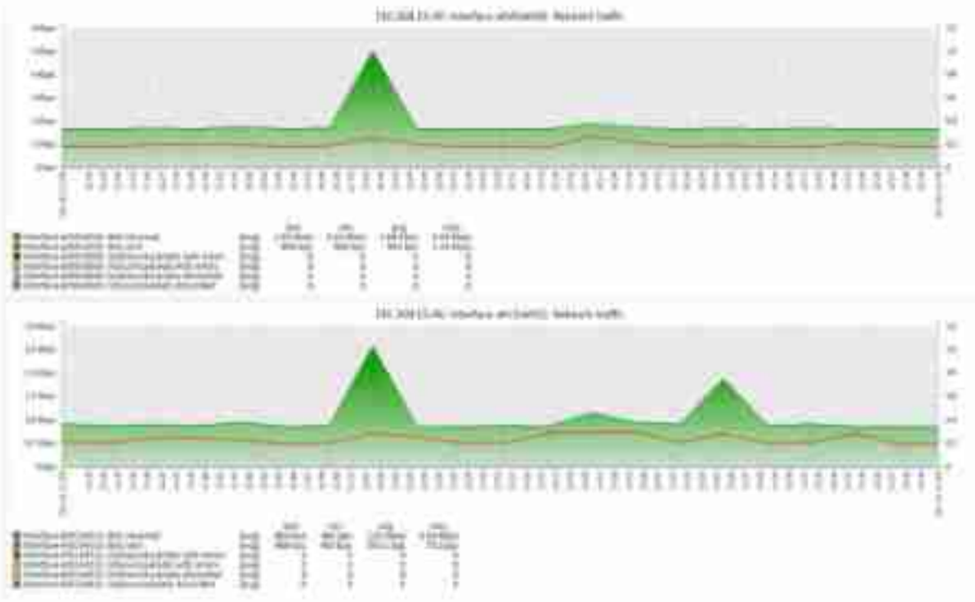


Figura 23: Exemplo das informações de tráfego de rede no Zabbix

X. DMZ

A DMZ (Demilitarized Zone) é uma área de rede que fica entre a rede interna de uma organização e a internet externa. Essa zona é criada para fornecer uma camada adicional de

Figura 24: Exemplo das informações de espaço em disco no Zabbix

segurança, segregando os sistemas críticos da rede interna daqueles acessíveis ao público externo.

Na DMZ, foi hospedada uma API REST utilizando o framework FastAPI, que simula uma API com autenticação para fins de teste. O código dessa API pode ser encontrado em [18]. Foi hospedado também um site HTTP com um formulário de login simples e seu código pode ser encontrado em [19].

Além disso, foi instalado um servidor SSH com o OpenSSH Server para simular um servidor acessível remotamente.

XI. Ataques e Vulnerabilidades Exploradas

Para simulação dos ataques foram usados máquinas com sistema kali linux. A localização dos atacantes na topologia pode ser visualizado na figura 2.

A. DHCP

O servidor DHCP foi configurado em todas as portas dos dois firewalls da topologia. No entanto, o range de IPs disponível foi escolhido sem levar em consideração a quantidade de dispositivos que seriam conectados. Como resultado, sobraram IPs disponíveis, facilitando para que um atacante se conectasse aos switches da topologia e solicitasse um IP via DHCP, obtendo assim livre acesso ao firewall e à rede DMZ. Na Figura 25 mostra como o atacante conseguiu dinamicamente um IP da sub-rede 192.168.2.0/24, através do servidor DHCP.

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group defaul
t qlen 1000
    link/ether 0c:96:73:3d:00:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.11/24 brd 192.168.2.255 scope global dynamic noprefixroute eth0
       valid_lft 4750sec preferred_lft 4750sec
    inet6 fe80::2902:53a3:950:f250/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Figura 25: IP do atacante recebido dinamicamente via DHCP

Para evitar que um atacante obtenha um IP via DHCP e tenha acesso não autorizado à rede, deve-se configurar o range de IPs disponíveis no servidor DHCP para corresponder exatamente à quantidade de dispositivos autorizados na rede. Isso reduz a chance de que IPs ociosos sejam usados por atacantes. Além disso, é importante implementar monitoramento e alertas para detectar dispositivos não autorizados na rede.

Essa vulnerabilidade pode resultar em dois tipos de ataques conhecidos: DHCP Starvation Attack e DHCP Flood Attack [20]. No DHCP Starvation Attack, o atacante envia uma grande quantidade de solicitações de novos endereços IPs ao servidor DHCP, esgotando o pool de endereços disponíveis e impedindo que dispositivos legítimos obtenham endereços IP. Já no DHCP Flood Attack, o objetivo é sobrecarregar o servidor DHCP com um grande volume de requisições, causando lentidão ou falhas no serviço.

B. Varredura

Como o atacante conseguiu IP e gateway via DHCP, ele pode usar o Nmap, uma ferramenta de código aberto para exploração de rede e auditoria de segurança, para fazer uma varredura na rede em busca de informações importantes. Sabendo que estava na sub-rede 192.168.0.0/16, ele realizou a varredura em toda a sub-rede, como mostra a Figura 26.

```
root@kali:~/Documents/bruteforce# nmap 192.168.0.0/16
Starting Nmap 7.80 ( https://nmap.org ) at 2024-06-08 18:31 UTC
Nmap scan report for 192.168.1.1
Host is up (0.00056s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap scan report for 192.168.1.101
Host is up (0.0013s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
```

Figura 26: Resultado da varredura na sub-rese 192.168.0.0/16

Algumas informações importantes foram obtidas durante a varredura. Foi descoberto que havia uma máquina com o IP 192.168.1.101 (localizada na DMZ) com a porta 22 aberta, usada para comunicação via SSH. Utilizando a opção -A do Nmap, que permite a detecção do sistema operacional, a verificação de versões, a varredura de scripts e o traceroute, foi possível obter informações detalhadas sobre o host. Descobriu-se que a porta SSH estava executando o serviço OpenSSH e que o sistema operacional era Linux, como mostrado na Figura 27.

```
root@kali:~/Documents/bruteforce# nmap -A 192.168.1.101
Starting Nmap 7.80 ( https://nmap.org ) at 2024-06-08 18:38 UTC
Nmap scan report for 192.168.1.101
Host is up (0.00094s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.
0)
| ssh-hostkey:
|   2048 5f:25:43:43:f5:43:01:b9:07:5d:78:69:03:49:5f:e3 (RSA)
|   256 78:c3:21:7b:f6:98:a0:05:a5:ba:52:67:60:db:24:2a (ECDSA)
|_  256 00:02:73:0a:f3:3c:de:9b:0e:e4:2f:89:c8:86:80:70 (ED25519)
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=6/8%OT=22%CT=1%CU=31725%PV=Y%DS=2%DC=T%G=Y%TM=6664A530
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10C%TI=Z%II=I%TS=A)OPS(O1=M5
OS:B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O
OS:6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%D
OS:F=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0
OS:%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T
OS:6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%R
OS:UD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 587/tcp)
HOP RTT     ADDRESS
1   0.67 ms 192.168.2.1
2   1.41 ms 192.168.1.101
```

Figura 27: Resultado da varredura no IP 192.168.1.101

C. Força bruta

Sabendo que a porta 22 estava aberta e provavelmente executando um servidor SSH, o atacante pode procurar listas de senhas e usuários padrão para tentar um ataque de força bruta, visando obter acesso ao host. A lista de teste utilizada pode ser encontrada em [21].

Um ataque de força bruta é uma técnica de hacking onde o atacante tenta adivinhar senhas ou chaves de criptografia ao tentar todas as combinações possíveis até encontrar a correta. Esse ataque é eficaz contra senhas fracas, mas pode ser demorado e exigir muitos recursos computacionais, principalmente se a senha for complexa ou se houver medidas de segurança, como bloqueio após várias tentativas falhas [22].

Para o ataque de força bruta, foi utilizada a ferramenta Metasploit, um framework de código aberto utilizado para testes de penetração e desenvolvimento de exploits. No ataque, foi configurada uma tentativa de login utilizando a lista de teste com possíveis usuários e senhas no host 192.168.1.101. A configuração do Metasploit pode ser visualizada na Figura 28.

Figura 28: Configuração do Metasploit

Após diversas tentativas sem sucesso, foi descoberto que o usuário do host era "osboxes"e a senha "osboxes.org", como mostra a Figura 29, que são as credenciais padrão das máquinas fornecidas pelo OSBoxes, um serviço que oferece máquinas virtuais pré-configuradas para diversas distribuições de sistemas operacionais.

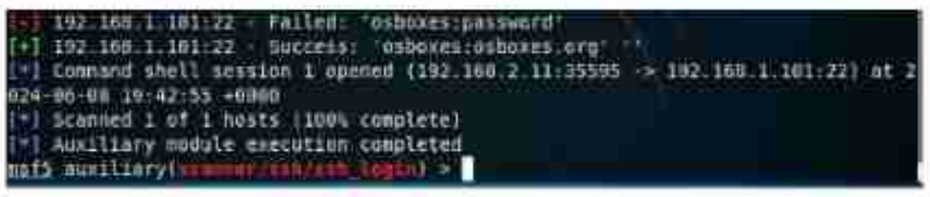


Figura 29: Resultado da tentativa de força bruta para acesso via ssh

Com o usuário e a senha em mãos, o atacante conseguiu acessar o host utilizando o comando SSH. Isso representa uma grave falha de segurança, pois as credenciais padrão do dispositivo deveriam ter sido alteradas para evitar acessos não autorizados. Manter as credenciais padrão torna o sistema vulnerável a ataques simples e previsíveis. É crucial que, ao configurar novos dispositivos, as senhas e os nomes de usuários padrões sejam substituídos por credenciais fortes e únicas.

Além de ser importante trocar as credenciais padrão, é fundamental implementar autenticação no OpenSSH Server para reforçar a segurança do sistema. A autenticação no OpenSSH Server é um processo que verifica a identidade do usuário antes de conceder acesso ao sistema. Isso é geralmente feito por meio de autenticação baseada em senha, autenticação baseada em chave pública ou uma combinação de ambas.

D. Man-in-the-Middle (MitM)

Foi implementado um site HTTP simples na DMZ, contendo um esquema básico de login, conforme ensinado em [18]. No entanto, como o site não utiliza criptografia nem HTTPS, ele é suscetível a ataques cibernéticos.

Com a ferramenta Ettercap do Kali Linux, é possível monitorar uma interface de rede. O Ettercap é uma ferramenta de segurança de rede, utilizada para realizar ataques Man-in-the-Middle (MitM) [23]. Ele permite a interceptação, inspeção e manipulação de tráfego de rede em tempo real, possibilitando a captura de senhas, a injeção de conteúdo malicioso e a realização de ataques de spoofing.

Foi simulado um atacante e uma vítima, localizados na rede interna, na área de 'Server'. Vale ressaltar que o atacante pode se conectar à rede através do servidor DHCP configurado nos Exos.

Para iniciar o ataque, é necessário abrir o Ettercap, selecionar a interface eth0 e escolher a opção Unified Sniffing. A partir desse momento, já é possível visualizar os logs da interface selecionada.

Com o Ettercap, é possível identificar hosts na mesma sub-rede em que o atacante está localizado. Conforme ilustrado na Figura 30, foi possível encontrar os hosts dos Exos e do computador da vítima.

Figura 30: Hosts encontrados no Ettercap

Foi criado um alvo no host 172.24.50.10, que é a vítima, e foi iniciado um ataque MitM do tipo ARP poisoning, conforme mostrado na Figura 31. Esse tipo de ataque funciona manipulando as tabelas ARP da rede, associando o endereço MAC do atacante ao endereço IP da vítima. Dessa forma, o tráfego destinado à vítima é redirecionado para o atacante, permitindo que ele monitore e possivelmente altere os dados transmitidos.

Quando a vítima se conecta ao site exposto na DMZ, que não possui segurança, o atacante consegue visualizar o cabeçalho da requisição, com as credenciais da vítima. Isso é

Figura 31: Ataque de ARP Poisoning no host da vítima

ilustrado nas Figuras 32 e 33. Esta situação é extremamente perigosa, pois permite ao atacante acessar as credenciais da vítima, possibilitando o uso mal-intencionado dessas informações. Tendo em vista isso, o uso de criptografia SSL/TLS é essencial além de manter os certificados digitais válidos e emitidos por uma autoridade certificadora.

Figura 32: Vítima acessando o site da DMZ

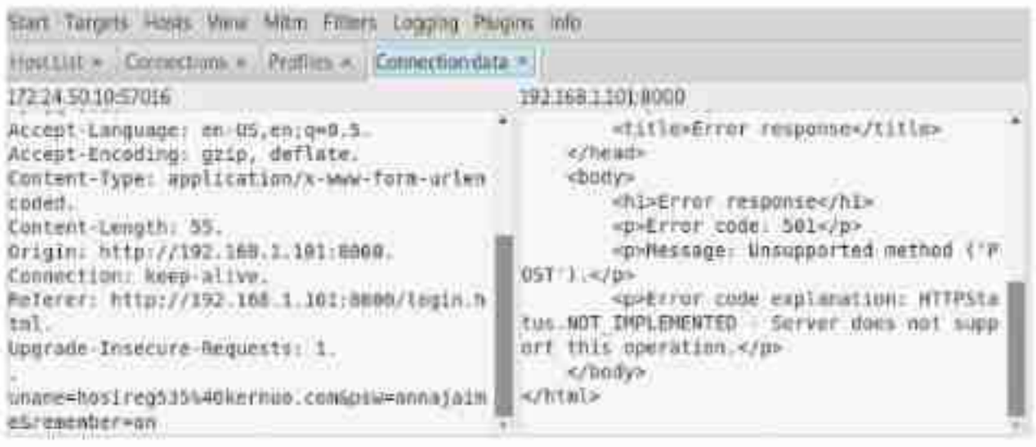


Figura 33: Atacante tendo acesso as credenciais da vítima

E. Clone de Sites

Um ataque bastante conhecido é o de clonagem de sites, onde o atacante cria uma réplica idêntica de um site legítimo para enganar os usuários e roubar suas informações sensíveis [24]. Este ataque pode ser facilmente realizado com a ferramenta Social Engineering Toolkit do Kali Linux. Sabendo que há um serviço HTTP exposto na DMZ, o atacante pode usar essa ferramenta para clonar o site e aplicar técnicas de engenharia social para induzir as vítimas a fornecer suas credenciais e outros dados pessoais.

Isso é realizado utilizando as opções de ataque a websites disponíveis na ferramenta. Conforme ilustrado na Figura 34, com apenas algumas etapas é possível clonar o site da DMZ e hospedá-lo no endereço IP da máquina do atacante. A partir do computador da vítima, o site clonado se apresenta idêntico ao site original da DMZ, como mostrado na Figura 35, induzindo a vítima a acreditar que está acessando o site legítimo e, assim, fornecendo suas credenciais ao atacante.

Para isso, nada melhor do que aumentar a conscientização e o treinamento em segurança. Embora os recursos técnicos possam permitir a autenticação do acesso, os usuários precisam ter um pouco mais de conhecimento digital e procurar sinais de segurança, como o https, representado por um cadeado, entre outras informações cruciais ao navegar na web.

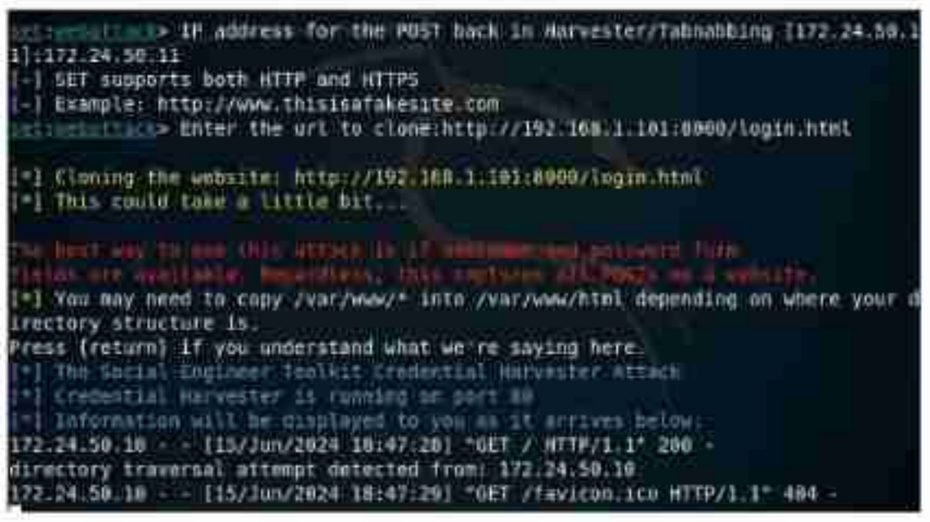


Figura 34: Ferramenta de Engenharia Social

Figura 35: Site clonado pelo atacante

XII. CONCLUSÕES

O objetivo deste projeto é desenvolver e implementar um Network Security Operation Center (NSOC) usando tecnologias e ferramentas sofisticadas como Zabbix, Pfsense, Snort, Vyos, Exos e GNS3. Os resultados mostram a eficácia do NSOC na monitoração e mitigação continuas de ameaças à segurança cibernética e destacam sua importância estratégica para proteger ativos de rede. As simulações ajudaram a identificar e explorar algumas vulnerabilidades. Isso reforçou a importância de práticas de segurança e políticas de resposta a incidentes.

Para proteger contra novas vulnerabilidades e ataques, recomendamos a continuidade do desenvolvimento de abordagens de segurança adaptativas ao contexto, melhorias nas configurações de segurança dos dispositivos e atualizações regulares dos sistemas.

Por fim este trabalho resume os objetivos, os resultados alcançados e a importância estratégica do NSOC na instituição, visando menos gastos e utilizando em alguns locais, sempre adaptados aos contextos, a implementação desse tipo de segurança.

REFERÊNCIAS

[1] K. Demertzis, N. Tziritas, P. Kikiras, S. L. Sanchez, and L. Iliadis, "The next generation cognitive security operations center: Adaptive analytic lambda architecture for efficient defense against adversarial attacks," *Big Data and Cognitive Computing*, vol. 3, no. 1, 2019. [Online]. Available: https://www.mdpi.com/2504-2289/3/1/6

[2] J. Wang, T. Yan, D. An, Z. Liang, C. Guo, H. Hu, Q. Luo, H. Li, H. Wang, S. Zeng, C. Zhou, L. Ma, and F. Qi, "A comprehensive security operation center based on big data analytics and threat intelligence," *PoS*, vol. ISGC2021, p. 028, 2021.

[3] S. Bhatt, P. Manadhata, and L. Zomlot, "The operational role of security information and event management systems," *Security Privacy, IEEE*, vol. 12, pp. 35–41, 09 2014.

[4] "Zabbix :: The enterprise-class open source network monitoring solution," Jun 2024. [Online]. Available: https://www.zabbix.com/index

[5] A. Pradana, I. R. Widiasari, and R. Efendi, "Implementasi sistem monitoring jaringan menggunakan zabbix berbasis snmp," *AITI*, vol. 19, no. 2, p. 248–262, Nov. 2022. [Online]. Available: https://ejournal.uksw.edu/aiti/article/view/6873

[6] A. Hartono and U. Y. Oktiawati, "Pemantauan router cpe pada jaringan metro ethernet menggunakan zabbix berbasis raspberry pi," *Journal of Internet and Software Engineering*, vol. 2, no. 1, pp. 29–38, Jun. 2021. [Online]. Available: https://jurnal.ugm.ac.id/v3/JISE/article/view/868

[7] "Proxy." [Online]. Available: https://www.zabbix.com/documentation/current/en/manual/api/reference/proxy

[8] "pfsense® - world's most trusted open source firewall." [Online]. Available: https://www.pfsense.org/

[9] K. Patel* and P. Sharma, "A review paper on pfsense – an open source firewall introducing with different capabilities & customization," *International Journal of Advance Research and Innovative Ideas in Education*, vol. 3, pp. 635–641, 2017. [Online]. Available: https://api.semanticscholar.org/CorpusID:169639872

[10] V. Asghari, S. Amiri, and S. Amiri, "Implementing utm based on pfsense platform," in *2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI)*, 2015, pp. 1150–1152.

[11] "Snort," Jun 2024. [Online]. Available: https://www.snort.org

[12] N. Khamphakdee, N. Benjamas, and S. Saiyod, "Improving intrusion detection system based on snort rules for network probe attack detection," in *2014 2nd International Conference on Information and Communication Technology (ICoICT)*, 2014, pp. 69–74.

[13] G. Jain and Anubha, "Application of snort and wireshark in network traffic analysis," *IOP Conference Series: Materials Science and Engineering*, vol. 1119, no. 1, p. 012007, mar 2021. [Online]. Available: https://dx.doi.org/10.1088/1757-899X/1119/1/012007

[14] A. Boyko, V. Varkentin, and T. Polyakova, "Advantages and disadvantages of the data collection's method using snmp," in *2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*, 2019, pp. 1–5.

[15] A. H. Alhilali, A. Al Farawn, and A. Y. Mjhool, "Design and implement a real-time network traffic management system using snmp protocol," *Eastern-European Journal of Enterprise Technologies*, vol. 5, no. 9 (125), p. 35–44, Oct. 2023. [Online]. Available: https://journals.uran.ua/eejet/article/view/286528

[16] [Online]. Available: https://www.gns3.com/

[17] MARCONI, Marina de Andrade; LAKATOS, Eva Maria. Fundamentos de metodologia científica. 8ª ed. São Paulo: Atlas, 2017.

[18] "pasan1/simple-fastapi-user-authentication," Jun 2024. [Online]. Available: https://github.com/pasan1/Simple-FastAPI-User-Authentication

[19] "How to create a login form." [Online]. Available: https://www.w3schools.com/howto/howto_css_login_form.asp

[20] A. AbdulGhaffar, S. K. Paul, and A. Matrawy, "An analysis of dhcp vul- nerabilities, attacks, and countermeasures," in *2023 Biennial Symposiumon Communications (BSC)*, 2023, pp. 119–124.

[21] "Seclists - passwords - default-credentials - ssh-betterdefaultpasslist.txt at master · danielmiessler/seclists," Jun 2024. [Online]. Available: https://github.com/danielmiessler/SecLists/blob/master/Passwords/Default-Credentials/ssh-betterdefaultpasslist.txt

[22] "What is a brute force attack? | definition, types how it works," Jun 2024. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/brute-force-attack

[23] "What is a man-in-the middle (mitm) attack? types examples," Jun 2024. [Online]. Available: https://www.fortinet.com/br/resources/cyberglossary/man-in-the-middle-attack.html

[24] Jun 2024. [Online]. Available: https://ironscales.com/guides/ phishing-prevention-best-practices/clone-phishing