

Documentação do Projeto

Tatiane de Matos Silva

Henrique Christopher de Castro Leão

1. Introdução	1
2. Problema a ser resolvido	1
3. Objetivos.....	2
4. Desafios.....	2
5. Ambiente de Testes e Configuração Técnica	2
6. Personas.....	7
7. Histórias de Usuário.....	8
8. Prototipação das Interfaces	9
9. Arquitetura do Sistema	9
10. Testes de Segurança	9
11. Telas – pfSense e VirtualBox	10
12. Diagrama	14
13. Segurança e recomendações	15
14. Requisitos.....	15
15. Requisitos Técnicos.....	15
16. Métricas e Indicadores.....	16
17. Plano de ação.....	16
18. Observações finais	16
19. Conclusão	17
20. Referências.....	17

Projeto: Testes de Vulnerabilidades Web

O projeto se baseia na realização de testes de vulnerabilidades web no objetivo de identificar falhas de segurança que possam ser exploradas por atacantes do sistema e como a empresa possa corrigir tais falhas e garantir uma melhor proteção de seus dados, ativos e tudo aquilo que esteja relacionado a segurança da informação.

1. Introdução

Este projeto tem como objetivo desenvolver códigos que possam ser utilizados por atacantes para a exploração de vulnerabilidades no sistema da empresa. A partir daí poderemos detectar os tipos de falhas, onde se encontram, como foram originadas e como corrigi-las através de um relatório especificando todos os eventos. Para garantir a segurança dos testes, foi criado um ambiente controlado e isolado utilizando o pfSense e máquinas virtuais no VirtualBox. Nesse ambiente, simularam-se ataques e defesas, evitando qualquer risco à rede real da instituição.

2. Problema a ser resolvido

A instituição PUC Minas tem sido alvo constante de ameaças e ataques cibernéticos que tentam fazer explorações de seus dados, como invasões, roubo de arquivos sensíveis, informações confidenciais e acesso não autorizado.

Essa lacuna compromete a segurança, a rastreabilidade e a eficiência operacional do ativo.

3. Objetivos

- Desenvolver um código capaz de simular os mesmos ataques que a empresa tem sofrido e demonstrar onde está o erro e o porquê ele tem ocorrido
- Implementar uma aplicação console em C# ou Python para execução de comandos e interação com o usuário na tentativa de demonstrar como essas vulnerabilidades são exploradas.
- Utilizar as diretivas da framework OWASP Top 10 para se basear em quais são os principais tipos de vulnerabilidades mais exploradas atualmente.
- Criar um laboratório de testes virtual seguro e isolado.

- Gerar relatórios detalhados de vulnerabilidades e soluções.
- Permitir que somente o computador físico (host) acesse o pfSense, mantendo as máquinas virtuais isoladas.

4. Desafios

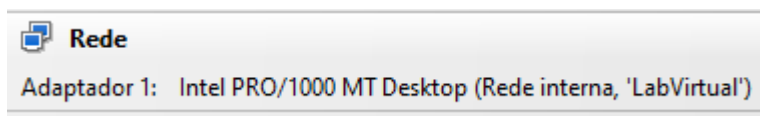
- **Segurança cibernética:** Como o sistema envolve testes de segurança, é essencial proteger tanto o ambiente de testes quanto os dados sensíveis da instituição.
- **Ambiente isolado e controlado:** Criar um ambiente que simule condições reais, mas que seja seguro e isolado, exige planejamento detalhado e infraestrutura adequada, para isso configurar o pfSense e as redes virtuais corretamente é essencial.
- **Definição clara de requisitos:** A falta de alinhamento entre os objetivos da instituição parceira e os desenvolvedores pode gerar retrabalho.
- **Documentação e manutenção:** Garantir que o sistema seja bem documentado e fácil de manter ao longo do tempo é essencial para sua longevidade.

5. Ambiente de Testes e Configuração Técnica

O ambiente foi criado no VirtualBox com o uso do pfSense como firewall e roteador, garantindo isolamento entre as redes.

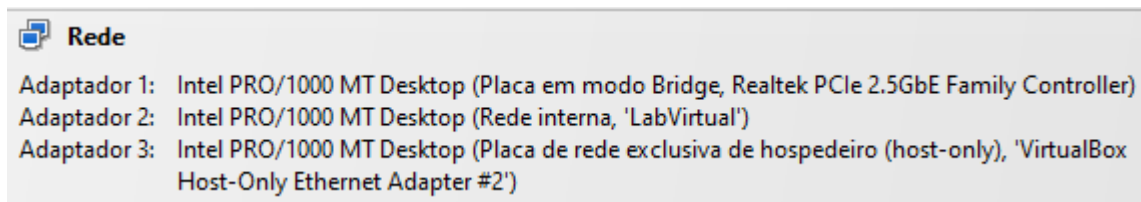
No VirtualBox

Criar/definir rede Host-Only com IP base 192.168.200.1/24 (ou usar padrão do VirtualBox).
Criar rede interna LabVirtual para VMs (Internal Network).



Configurar pfSense VM com 3 adaptadores:

- Adapter 1: Bridged/ WAN (conexão externa)
- Adapter 2: Rede Interna/LAN (LabVirtual)
- Adapter 3: Host-Only → (em2)



Configurar VMs para usar LabVirtual (Internal Network) para comunicação entre si.

Configuração do pfSense

Interface WAN (Bridge Adapter): Conectada à rede física, permitindo acesso apenas pelo computador host

- Interface LAN (Rede Interna “**LabVirtual**”): Conectada às máquinas virtuais de teste; Windows, Ubuntu, Parrot.
- Rede LAN configurada: **192.168.200.0/24**
- DHCP ativado: Intervalo de IPs de **192.168.200.100** a **192.168.200.200**

```
VirtualBox Virtual Machine - Netgate Device ID: d033d4ad76c9fd11337d
*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***

WAN (wan)    -> em0 -> v4/DHCP4: 192.168.100.49/24
              v6/DHCP6: 2804:d45:ac05:6d00::1/128
LAN (lan)    -> em1 ->
OPT1 (opt1)  -> em2 -> v4: 192.168.200.1/24
```

Regras de firewall criadas:

Atua como camada de segurança e roteamento entre a rede externa (Internet) e a rede interna do laboratório. Controla o tráfego de entrada e saída e mantém o isolamento entre o ambiente de teste e o host físico. Apenas o host físico tem permissão de acessar sua interface WebGUI (<https://192.168.200.1>).

- Bloqueio de acesso à interface WebGUI para todas as máquinas virtuais.
- Liberação de acesso apenas para o IP do computador físico.
- Permissão de comunicação entre as máquinas virtuais (para simulação de ataques e defesas).

Configuração das Máquinas Virtuais

Cada VM representa um papel dentro do ambiente de teste:

- **VM1 – Windows 10.0.0.101** → Servidor Web vulnerável (ex: OWASP Juice Shop).
- **VM2 – Ubuntu (10.0.0.102)** → Cliente atacante/testador.
- **VM3 - Parrot (10.0.0.103)** → Máquina de análise, coleta de logs e relatórios (ex: Kali Linux).
- Todas pertencem à rede **interna “labvirtual”**, isolada do host e da Internet.
- **Podem se comunicar entre si**, mas **não possuem rota para o pfSense ou o host físico** — garantindo total segurança.

Configuração da Máquina Física

- Responsável por administrar o ambiente virtual (VirtualBox).
- Conecta-se ao pfSense via OPT1 (192.168.200.100).
- Executa testes, coleta logs e configurações de segurança.
- Tem acesso à interface administrativa do pfSense e pode monitorar as VMs.

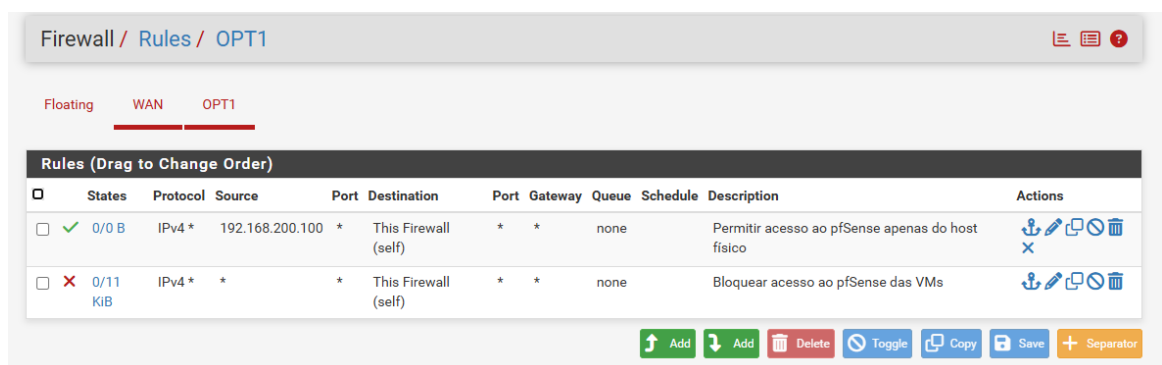
Todas configuradas na rede interna **“LabVirtual”**.

Dessa forma, as máquinas virtuais comunicam entre si, mas sem acessar o pfSense nem a internet, tornando o ambiente seguro e isolado.

Regras de firewall aplicadas

OPT1:

1. Permitir tráfego do IP do host para This Firewall (garante acesso WebGUI e ping).
2. Bloquear todo o restante para This Firewall (impede VMs).
3. (Opcional) Bloquear tráfego entre hosts de OPT1 (isolar VMs).



LAN:

1. Bloquear destino This Firewall (caso LAN esteja ativa), para garantir que VMs conectadas à LAN não acessem o pfSense.

Testes realizados e resultados

DHCP: PC físico obteve 192.168.200.100 do pfSense (DHCP OPT1).

```
Adaptador Ethernet Ethernet:
  Sufixo DNS específico de conexão. . . . . :
  Descrição . . . . . : Realtek PCIe 2.5GbE Family Controller
  Endereço Físico . . . . . : 3C-7C-3F-7B-EB-29
  DHCP Habilitado . . . . . : Sim
  Configuração Automática Habilitada. . . . . : Sim
  Endereço IPv6 . . . . . : 2804:d45:ac05:6d00:17de:5703:7205:8ed7(Preferencial)
  Endereço IPv6 Temporário. . . . . : 2804:d45:ac05:6d00:f579:db15:a299:353d(Preferencial)
  Endereço IPv6 de link local . . . . . : fe80::b896:70e7:aa57:6342%8(Preferencial)
  Endereço IPv4. . . . . : 192.168.100.2(Preferencial)
  Máscara de Sub-rede . . . . . : 255.255.255.0
  Concessão Obtida. . . . . : sexta-feira, 31 de outubro de 2025 12:15:42
  Concessão Expira. . . . . : sábado, 1 de novembro de 2025 12:15:42
  Gateway Padrão. . . . . : fe80::1%8
  192.168.100.1
  Servidor DHCP . . . . . : 192.168.100.1
  IAID de DHCPv6. . . . . : 104627263
  DUID de Cliente DHCPv6. . . . . : 00-01-00-01-30-50-14-8B-3C-7C-3F-7B-EB-29
  Servidores DNS. . . . . : fe80::1%8
  192.168.100.1
  fe80::1%8
  NetBIOS em Tcpi. . . . . : Desabilitado

Adaptador Ethernet Ethernet 3:
  Sufixo DNS específico de conexão. . . . . : home.arpa
  Descrição . . . . . : VirtualBox Host-Only Ethernet Adapter #2
  Endereço Físico . . . . . : 0A-00-27-00-00-03
  DHCP Habilitado . . . . . : Sim
  Configuração Automática Habilitada. . . . . : Sim
  Endereço IPv6 de link local . . . . . : fe80::d0bf:509a:5148:5cfa%3(Preferencial)
  Endereço IPv4. . . . . : 192.168.200.101(Preferencial)
  Máscara de Sub-rede . . . . . : 255.255.255.0
  Concessão Obtida. . . . . : sexta-feira, 31 de outubro de 2025 12:23:28
  Concessão Expira. . . . . : sexta-feira, 31 de outubro de 2025 14:23:28
  Gateway Padrão. . . . . : 192.168.200.1
  Servidor DHCP . . . . . : 192.168.200.1
  IAID de DHCPv6. . . . . : 403308583
  DUID de Cliente DHCPv6. . . . . : 00-01-00-01-30-50-14-8B-3C-7C-3F-7B-EB-29
  Servidores DNS. . . . . : 192.168.200.1
  NetBIOS em Tcpi. . . . . : Desabilitado

Adaptador Ethernet Ethernet 4:
  Sufixo DNS específico de conexão. . . . . :
  Descrição . . . . . : VirtualBox Host-Only Ethernet Adapter
  Endereço Físico . . . . . : 0A-00-27-00-00-09
  DHCP Habilitado . . . . . : Não
  Configuração Automática Habilitada. . . . . : Sim
  Endereço IPv6 de link local . . . . . : fe80::43e:58e0:d7a5:2512%9(Preferencial)
  Endereço IPv4. . . . . : 192.168.56.1(Preferencial)
  Máscara de Sub-rede . . . . . : 255.255.255.0
  Gateway Padrão. . . . . :
  IAID de DHCPv6. . . . . : 420085799
  DUID de Cliente DHCPv6. . . . . : 00-01-00-01-30-50-14-8B-3C-7C-3F-7B-EB-29
  Servidores DNS. . . . . : fec0:0:0:ffff::1%1
  fec0:0:0:ffff::2%1
  fec0:0:0:ffff::3%1
  NetBIOS em Tcpi. . . . . : Desabilitado
```

```
C:\Users\Tatiane>arp -a
```

Interface: 192.168.200.1 --- 0x3		
Endereço IP	Endereço físico	Tipo
192.168.200.1	08-00-27-ab-89-f5	dinâmico
224.0.0.22	01-00-5e-00-00-16	estático
224.0.0.251	01-00-5e-00-00-fb	estático
224.0.0.252	01-00-5e-00-00-fc	estático
239.255.255.250	01-00-5e-7f-ff-fa	estático
255.255.255.255	ff-ff-ff-ff-ff-ff	estático

Interface: 192.168.100.2 --- 0x8		
Endereço IP	Endereço físico	Tipo
192.168.100.1	14-89-cb-a7-e4-14	dinâmico
224.0.0.22	01-00-5e-00-00-16	estático
224.0.0.251	01-00-5e-00-00-fb	estático
224.0.0.252	01-00-5e-00-00-fc	estático
239.255.255.250	01-00-5e-7f-ff-fa	estático
255.255.255.255	ff-ff-ff-ff-ff-ff	estático

Interface: 192.168.56.1 --- 0x9		
Endereço IP	Endereço físico	Tipo
224.0.0.22	01-00-5e-00-00-16	estático
224.0.0.251	01-00-5e-00-00-fb	estático
224.0.0.252	01-00-5e-00-00-fc	estático
239.255.255.250	01-00-5e-7f-ff-fa	estático

Conectividade: ping 192.168.200.1 respondeu quando firewall temporariamente desativado para teste; após regras permanentes, ping do host responde e VMs não conseguem pingar.

```
C:\Users\Tatiane>ping 192.168.200.1
```

Disparando 192.168.200.1 com 32 bytes de dados:

Resposta de 192.168.200.1: bytes=32 tempo<1ms TTL=64

Resposta de 192.168.200.1: bytes=32 tempo<1ms TTL=64

Resposta de 192.168.200.1: bytes=32 tempo<1ms TTL=64

Resposta de 192.168.200.1: bytes=32 tempo<1ms TTL=64

Estatísticas do Ping para 192.168.200.1:

Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),

Aproximar um número redondo de vezes em milissegundos:

Mínimo = 0ms, Máximo = 0ms, Média = 0ms

WebGUI: acesso via <https://192.168.200.1> a partir do PC físico. VMs não conseguem acessar 192.168.200.1 nem 192.168.1.1 após regras/bloqueios.

Isolamento VMs: VMs continuam a se comunicar entre si na LabVirtual, sem acessar o pfSense nem o host.

6. Personas

Persona1: Analista de Segurança da Informação

- **Nome:** João, 32 anos
- **Profissão:** Analista de Segurança da Informação
- **Sistemas que usa:** Linux, pfSense
- **Expectativas:** Executar teste automatizados de vulnerabilidade
- **Desilusões:** Ambientes pouco realistas e com pouca documentação

Persona 2: Administrador de Redes

- **Idade:** 35 anos
- **Profissão:** Setor de TI da PUC Minas
- **Sistemas que usa:** Active Directory, pfSense, Linux
- **Expectativas:** Manter o controle total do ambiente e receber relatórios claros
- **Desilusões:** Ferramentas complexas e pouco intuitivas

Persona 3: Gestor de TI

- **Nome:** Marcelo
- **Profissão:** Gestor
- **Idade:** 45
- **Sistemas que usa:** Windows, Teams, Portais institucionais
- **Expectativas:** Acompanhar a segurança da rede de forma visual e didática
- **Desilusões:** Falta de indicadores e painéis de monitoramento

7. Histórias de Usuário

Como Analista de Segurança da Informação, **eu preciso** de criar formas para desmistificar e alterar o formato atual da empresa PUC, pois **eu quero** executar testes de penetração em um ambiente controlado para identificar vulnerabilidades e documentar falhas.

Como administrador de redes **eu quero** executar testes de vulnerabilidade em servidores Linux e gerenciar as regras do firewall **para garantir isolamento e controle total das máquinas virtuais** para garantir que não haja brechas de segurança.

Como gestor de TI **eu quero** visualizar o status dos ativos testados **para** acompanhar a evolução da segurança da rede institucional.

8. Prototipação das Interfaces

As interfaces serão projetadas na PUC Minas, com foco em:

- Segurança e autenticação de acesso
- Proteção dos Dados
- Melhoria da qualidade dos serviços
- Simplicidade e clareza visual

9. Arquitetura do Sistema

A arquitetura será diagramada em blocos, com os seguintes componentes:

- **Backend (Web API .NET Core):** Lógica de negócio e comunicação com os demais módulos
- **Console App (C# ou Python):** Responsável por executar comandos no ativo
- **Banco de Dados:** Armazenamento de logs, usuários e resultados de testes

10. Testes de Segurança

Será implementado um módulo para simular e explorar vulnerabilidades da lista OWASP Top 10, como:

- Injeção de SQL
- Criptografia de dados sensíveis
- Exposição de dados sensíveis
- Falhas de configuração de segurança
- Conecta ao ZAP (proxy local).
- Faz **Spider** para descobrir URLs do alvo.

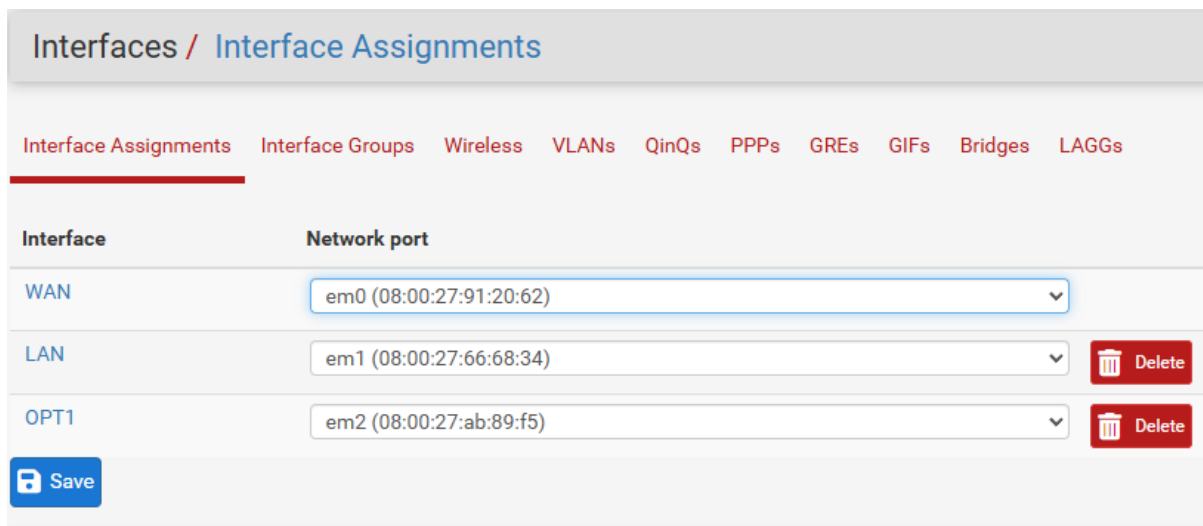
- Executa **Passive Scan** (ZAP analisa tráfego passivo enquanto a spider navega).
- Coleta **alertas** do ZAP.
- Gera **estatísticas por nível de risco**.
- Exporta relatórios em **JSON** e **CSV**.

Os testes serão realizados em ambiente controlado (pfSense + VirtualBox), com o código podendo ser desenvolvido em **C#** ou **Python**, dependendo da opção da equipe responsável, mas o nosso projeto foi desenvolvido em Python.

11. Telas – pfSense e VirtualBox

pfSense WebGUI locais

Interfaces → Assignments (atribuição de interfaces)



Interfaces / Interface Assignments

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs

Interface	Network port	
WAN	em0 (08:00:27:91:20:62)	
LAN	em1 (08:00:27:66:68:34)	Delete
OPT1	em2 (08:00:27:ab:89:f5)	Delete

Save

Interfaces → [OPT1] (configurar IP estático)

Enable	<input checked="" type="checkbox"/> Enable interface	
Description	<input type="text" value="OPT1"/> Enter a description (name) for the interface here.	
IPv4 Configuration Type	<input type="text" value="Static IPv4"/>	
IPv6 Configuration Type	<input type="text" value="None"/>	
MAC Address	<input type="text" value="xx:xx:xx:xx:xx:xx"/> This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.	
MTU	<input type="text"/> If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.	
MSS	<input type="text"/> If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.	
Speed and Duplex	<input type="text" value="Default (no preference, typically autoselect)"/> Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.	
Static IPv4 Configuration		
IPv4 Address	<input type="text" value="192.168.200.1"/>	<input type="text" value="/ 24"/>
IPv4 Upstream gateway	<input type="text" value="None"/>	<input type="button" value="+ Add a new gateway"/>

Services → DHCP Server → OPT1 (habilitar DHCP)

Interfaces / WAN (em0) ⚙️ 📄 ?

General Configuration

Enable

☒ Enable interface

Description

WAN

Enter a description (name) for the interface here.

IPv4 Configuration Type

DHCP

IPv6 Configuration Type

DHCP6

MAC Address

xx:xx:xx:xx:xx:xx

This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU

If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex

Default (no preference, typically autoselect)

Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Firewall → Rules → OPT1 (criar regras de Permitir/Bloquear)

Firewall / Rules / OPT1 📄 📄 ?

Floating WAN OPT1

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	192.168.200.100	*	This Firewall (self)	*	*	none		Permitir acesso ao pfSense apenas do host físico	📌 ✎ 📄 🚫
<input type="checkbox"/>	✗ 0/11 KiB	IPv4 *	*	*	This Firewall (self)	*	*	none		Bloquear acesso ao pfSense das VMs	📌 ✎ 📄 🚫

Diagnostics → Backup & Restore (backup configuração)

Diagnostics / Backup & Restore / Backup & Restore

Backup & Restore Configuration History

Backup Configuration

Backup area

All

Skip packages

☐ Do not backup package information.

Skip RRD data

☒ Do not backup RRD data (NOTE: RRD Data can consume 4+ megabytes of config.xml space!)

Include extra data

☐ Backup extra data.
Backup extra data files for some services. i

Backup SSH keys

☒ Backup SSH keys (otherwise clients would fail to recognize the host keys after restore)

Encryption

☐ Encrypt this configuration file.

Download configuration as XML

Restore Backup

Open a pfSense configuration XML file and click the button below to restore the configuration.

Restore area

All

Configuration file

Escolher arquivo

Nenhum arquivo escolhido

Encryption

☐ Configuration file is encrypted.

Restore Configuration

The firewall will reboot after restoring the configuration.

Procedimentos operacionais:

- **Iniciar ambiente**

Ligar VirtualBox → iniciar pfSense VM → iniciar VMs.

Verificar pfSense: Status → Interfaces — confirmar IPs.

- **Se o host não obtiver IP**

No host: ipconfig /release → ipconfig /renew.

Verifique DHCP em Services → DHCP Server → OPT1.

Conferir regras de firewall em Firewall → Rules → OPT1.

Recuperação rápida (se travar acesso WebGUI)

Acessar console da VM pfSense no VirtualBox.

Entrar em shell (8) e, se necessário, pfctl -d para desativar temporariamente o firewall (caso não há conexão com a máquina hosty only).

Ajustar regras via console ou reiniciar/desligar pfSense.

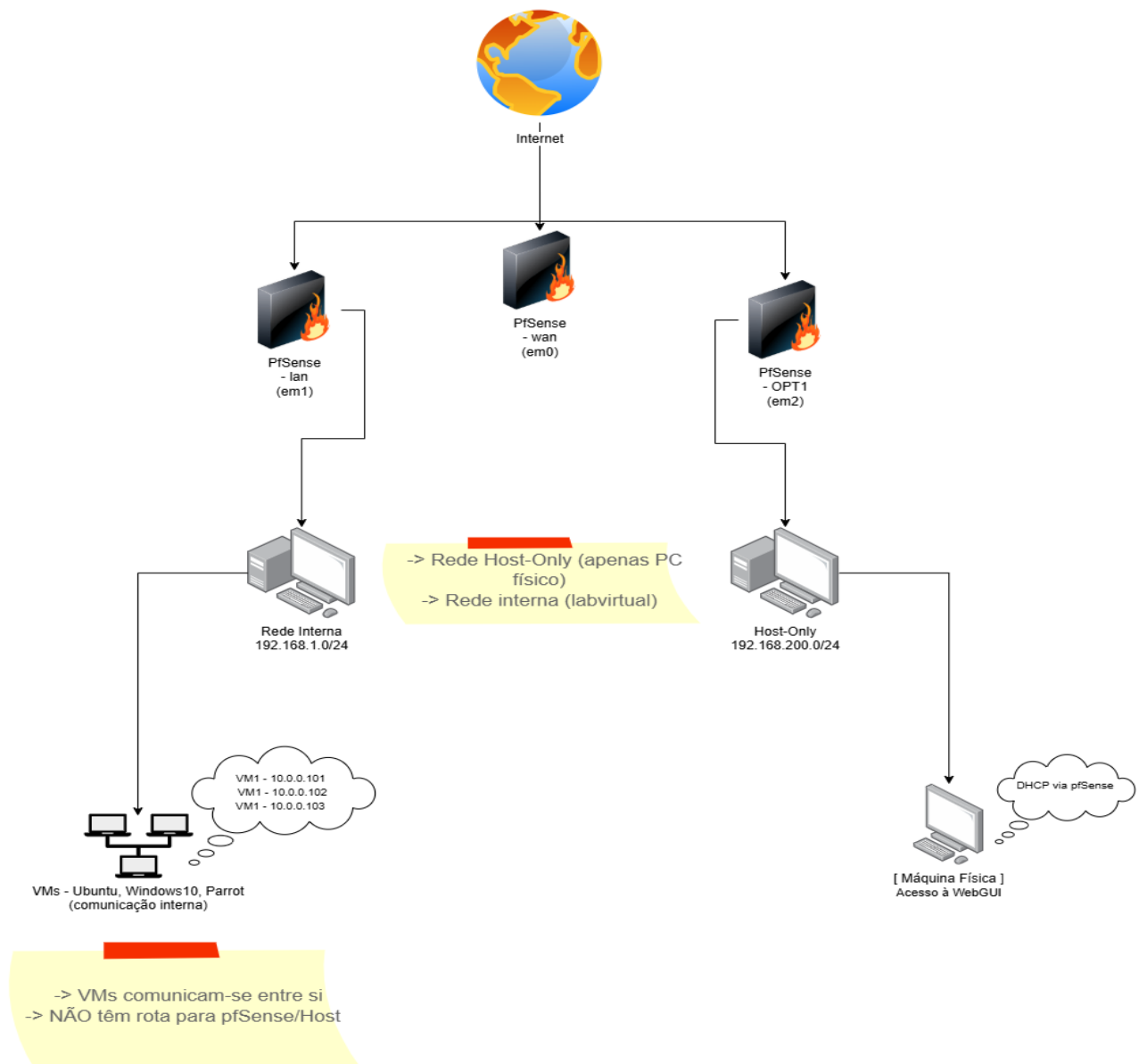
- **Backup e restauração**

Fazer export de configuração: Diagnostics → Backup & Restore (baixar XML).

salvar backup antes de aplicar.

12. Diagrama

- pfSense atua como firewall e roteador principal, recebendo conexão da Internet (WAN/em0).
- A interface OPT1 (**192.168.200.1/24**) está configurada como Host-Only, e faz a comunicação somente com o PC físico.
- O PC físico (host) recebe IP **192.168.200.100** via DHCP do pfSense, mas está isolado das VMs internas.
- A rede labvirtual (LAN/em1) hospeda as VMs:
 - VM1 → 10.0.0.101
 - VM2 → 10.0.0.102
 - VM3 → 10.0.0.103
- As VMs comunicam-se entre si, porém não possuem rota de saída para o pfSense ou para o host físico.



13. Segurança e recomendações

- Salvar backups do pfSense sempre antes de mudanças significativas.
- Coloque descrições nas regras do firewall.

14. Requisitos

- Conhecimento em ciberseguranças
- Conhecimento em segurança da informação
- Conhecimento das principais vulnerabilidades web

15. Requisitos Técnicos

Requisitos de Software:

- Python ou C#
- VirtualBox
- PfSense
- Suricata

Requisitos de Hardware:

- Processador compatível com virtualização
- Espaço livre em disco para Máquinas Virtuais (+/- 30 GB)

16. Métricas e Indicadores

- Número de vulnerabilidades identificadas
- Tempo médio de correção das falhas
- Disponibilidade e estabilidade do ambiente de testes
- Clareza e completude dos relatórios gerados

17. Plano de ação

- Entregáveis imediatos:
 1. Arquivo de configuração do pfSense (backup XML).
 2. Documentação técnica
 3. Relatório de achados (vulnerabilidades, evidências, recomendações).
- Etapas seguintes:
 1. Rodar módulo de testes OWASP (scripts em Python/C#).
 2. Coletar logs e evidências.
 3. Preparar relatório e passos de correção.
 4. Realizar testes após correções.

18. Observações finais

- O ambiente foi projetado para ser seguro, reversível e ideal para testes de vulnerabilidade.
- Qualquer alteração no ambiente deve ser precedida de backup.
- A configuração garante que apenas o PC físico administre o pfSense, enquanto as VMs permanecem isoladas para testes.

19. Conclusão

A criação da nossa área de testes de vulnerabilidades representou um avanço significativo, proporcionando um ambiente seguro, controlado para a compreensão e mitigação de riscos cibernéticos. A estrutura que montamos, junto com as ferramentas, possibilitou não apenas a simulação de cenários reais de ataque, mas também a geração de conhecimento prático e valioso. Tudo isso ajuda a melhorar a segurança digital das empresas parceiras.

O que conseguimos mostrar que o projeto alcançou o que queríamos: aumentar a atenção sobre segurança da informação, dar formas fáceis e boas de achar pontos fracos e ajudar nossos parceiros a decidir o que fazer para proteger seus sistemas. A área de testes também pode crescer e receber melhorias no futuro, permitindo futuras expansões, melhorias e integrações de acordo com o que a empresa precisar.

O projeto não só oferece uma ferramenta que funciona, mas também incentiva a prevenção, o que é muito importante para enfrentar os desafios. Assim, nossos parceiros estão mais prontos, informados e fortalecidos para lidar com ameaças, protegendo seus processos, informações e clientes.

20. Referências

- Suricata + PfSense : Instalação e Configuração:
https://www.youtube.com/watch?v=mg8DWETsN_k&t=114s
- How to install VirtualBox Guest Additions on Kali Linux:
<https://www.youtube.com/watch?v=9up2oPu-hkA&t=182s>
- pfsense 2.4.4 – Como configurar IDS/IPS no pfSense usando o Suricata (1/2):
<https://www.youtube.com/watch?v=SobzXrDOnm8&t=1s>
- Curso de Figma 2025 do básico ao avançado:
<https://www.youtube.com/watch?v=SJ6sTj-LCjA>
- CRIANDO USUÁRIOS, GRUPOS e PRIVILÉGIOS no UTM/NGFW pfSENSE FIREWALL v2.5.x no Oracle VirtualBOX:

<https://www.youtube.com/watch?v=14DpdhR5Veo&list=PLozhsZB1lLUN7vHnCDA2NF6rMfTBs-vAs>

- COMO CONFIGURAR as Regras de FIREWALL na Interface LAN no pfSENSE PLUS+ 22.05: <https://www.youtube.com/watch?v=C5bg-Ec2jb4&t=2066s>
- How To Install Kali Linux In Virtual Box + Guest Additions Fix: <https://www.youtube.com/watch?v=nvImI7rJwdI&t=1s>
- Aula 1 - Como instalar PFSENSE do Zero, Passo a Passo no VirtualBox: <https://www.youtube.com/watch?v=YFPEVB6OmWc&t=605s>