[NOME DA MÁQUINA/DESAFIO]

[Logo do Desafio]

Penetration Testing Writeup

Plataforma	[HackTheBox / TryHackMe / CTF / Bug Bounty]
Dificuldade	[Easy / Medium / Hard / Insane]
Sistema Operacional	[Linux / Windows / Other]
Data de Conclusão	[DD/MM/AAAA]
IP do Alvo	[IP Address]
Técnicas Utilizadas	[Enumeration, SQLi, XXE, RCE, Privilege Escalation, etc.]

Índice

1. Resumo Executivo

[Breve descrição do alvo e principais descobertas. Destacar vulnerabilidades críticas encontradas e impacto potencial.]

2. Metodologia

A abordagem seguiu as seguintes fases:

1. Reconhecimento e Enumeração
2. Análise de Vulnerabilidades
3. Exploração
4. Pós-Exploração e Escalação de Privilégios
5. Documentação e Relatório

3. Reconhecimento e Enumeração

3.1. Scan de Portas (Nmap)

Comando executado:

```
nmap -sC -sV -oN nmap.txt [TARGET_IP]
```

Portas abertas encontradas:

- [Porta/Serviço - ex: 22/SSH]
- [Porta/Serviço - ex: 80/HTTP]
- [Adicionar mais conforme necessário]

3.2. Enumeração Web (se aplicável)

Ferramentas utilizadas:

- Gobuster/Dirbuster para enumeração de diretórios
- Burp Suite para análise de requisições
- Nikto para identificação de vulnerabilidades web

[Descrever descobertas importantes]

3.3. Outras Enumerações

[SMB, FTP, DNS, LDAP, etc. - descrever conforme relevante]

4. Análise de Vulnerabilidades

[Listar e descrever vulnerabilidades identificadas com CVEs quando aplicável]

Vulnerabilidade	Descrição	Severidade
[Ex: SQLi]	[Descrição da vulnerabilidade]	[Alta/Média/Baixa]

5. Exploração

5.1. Acesso Inicial

[Descrever como o acesso inicial foi obtido]

Exploit utilizado:

```
[Código do exploit ou comando]
```

Resultado:

```
[Output do comando]
```

5.2. User Flag

Localização: [caminho do arquivo]

```
Flag: [user_flag_aqui]
```

6. Pós-Exploração e Escalação de Privilégios

6.1. Enumeração Interna

Ferramentas utilizadas:

- [LinPEAS / WinPEAS]
- [LinEnum / Windows-Exploit-Suggester]
- [Outras ferramentas]

6.2. Vetor de Escalação

[Descrever a vulnerabilidade/misconfiguration que permitiu escalação]

Exploit/Técnica utilizada:

```
[Comando ou exploit]
```

6.3. Root/Administrator Flag

Localização: [caminho do arquivo]

```
Flag: [root_flag_aqui]
```

7. Recomendações de Remediação

[Listar recomendações específicas para corrigir cada vulnerabilidade encontrada]

- [Recomendação 1]
- [Recomendação 2]
- [Recomendação 3]

8. Lições Aprendidas

[Reflexões sobre o processo, técnicas novas aprendidas, dificuldades encontradas, etc.]

9. Referências

[Listar CVEs, links de exploits, artigos de referência, etc.]

- [Referência 1]
- [Referência 2]
- [Referência 3]

10. Anexos

[Screenshots, outputs completos de comandos, código de exploits customizados, etc.]