Network Asset Discovery & Exposure Report

---

1. Resumo Executivo

Este relatório apresenta os resultados de uma análise de descoberta de ativos e exposição de rede realizada em um ambiente controlado da plataforma TryHackMe.

O objetivo deste projeto foi identificar ativos na rede, serviços expostos e possíveis riscos de segurança que poderiam ser explorados por um atacante durante a fase de reconhecimento.

Durante a avaliação, foi identificado um host ativo com diversos serviços expostos, incluindo SSH e HTTP. Além disso, foram encontradas informações sensíveis acessíveis publicamente no serviço web, o que representa um risco potencial de segurança.

Este projeto demonstra habilidades práticas em:

- Reconhecimento de rede
- Enumeração de serviços
- Análise de exposição
- Avaliação de riscos
- Produção de relatórios de segurança

Exemplo prático:

Esse tipo de análise é utilizado diariamente por equipes de SOC para descobrir ativos desconhecidos, reduzir a superfície de ataque e prevenir incidentes de segurança.

---

2. Escopo

Ambiente alvo:
Laboratório controlado da plataforma TryHackMe

Endereço IP analisado:
10.65.180.97

Tipo de avaliação:
Reconhecimento externo e análise de exposição

Limitações:
- Ambiente com apenas um host
- Sem exploração ativa
- Sem testes de autenticação
- Foco em visibilidade e defesa

---

3. Metodologia

A metodologia seguiu uma abordagem estruturada semelhante à utilizada por profissionais de Blue Team e alinhada com boas práticas do NIST.

Fase 1 – Descoberta de Host
Identificação de ativos na rede.

Fase 2 – Enumeração de Portas e Serviços
Identificação de portas abertas e serviços expostos.

Fase 3 – Identificação de Versões
Análise das versões dos serviços para avaliar possíveis vulnerabilidades.

Fase 4 – Enumeração Web
Análise do serviço HTTP para detectar:

- **Diretórios ocultos**
- **Informações sensíveis**
- **Falhas de configuração**
- **Vazamento de dados**

Fase 5 – Avaliação de Riscos

Classificação dos achados com base no impacto e probabilidade.

---

4. Descobertas

4.1 Host Ativo

Foi identificado um host ativo no ambiente.

Latência observada:
0.00028s

Isso confirma que o ativo está acessível externamente.

4.2 Portas e Serviços Abertos

Porta	Serviço
7/tcp	Echo
9/tcp	Discard
13/tcp	Daytime
17/tcp	QOTD
22/tcp	SSH
8008/tcp	HTTP

Observações:

- **SSH acessível externamente**
- **Serviços antigos e potencialmente desnecessários expostos**
- **Servidor web público**

4.3 Identificação de Versões

Serviço	Versão
SSH	OpenSSH 9.6p1 Ubuntu
HTTP	lighttpd 1.4.74

Essa informação é crítica, pois atacantes utilizam essas versões para buscar vulnerabilidades conhecidas em bases públicas como CVE.

4.4 Exposição Web

Durante a análise do serviço HTTP, foi identificado:

- **Servidor web acessível**
- **Enumeração de diretórios realizada**
- **Possível vazamento de informações**

Exemplo prático:

Em ambientes reais, esse tipo de exposição pode permitir o reconhecimento de tecnologias internas e facilitar ataques direcionados.

4.5 Vazamento de Informação

Foi identificado vazamento de informação sensível no código-fonte da aplicação web:

THM{SECRET_PAGE_38B9P6}

Esse tipo de falha indica problemas de controle de acesso e configuração segura, podendo auxiliar atacantes na coleta de dados internos e planejamento de ataques.

4.6 Classificação de Severidade

Achado	Severidade
Vazamento de informação	Médio
Serviços desnecessários expostos	Médio
SSH acessível externamente	Alto

---

5. Análise de Risco

Os dados coletados poderiam permitir que um atacante:

- **Mapeie a infraestrutura**
- **Identifique tecnologias utilizadas**
- **Busque vulnerabilidades conhecidas**
- **Planeje ataques direcionados**

Caso explorado, esse cenário poderia resultar em acesso não autorizado, comprometimento de sistemas e impacto na continuidade do negócio.

---

6. Impacto de Segurança

Principais riscos:

- **Aumento da superfície de ataque**
- **Serviços críticos expostos**
- **Falhas de configuração**
- **Vazamento de dados**

Esse tipo de exposição pode gerar impacto financeiro, reputacional e operacional em ambientes corporativos.

---

7. Recomendações

Segurança de Rede

- **Restringir acesso externo aos serviços**
- **Aplicar regras de firewall**
- **Implementar segmentação de rede**
- **Limitar acesso ao SSH por IP ou VPN**

Segurança Web

- **Remover informações sensíveis**
- **Implementar autenticação**
- **Aplicar configuração segura do servidor**
- **Monitorar acessos suspeitos**

Monitoramento

- **Implementar logs centralizados**
- **Monitoramento contínuo com SIEM**
- **Detecção de varreduras de rede**

Hardening

- **Atualizações regulares**
- **Remoção de serviços desnecessários**
- **Princípio do menor privilégio**

---

8. Mapeamento com Frameworks de Segurança

Este projeto está alinhado com fases de ataque descritas no MITRE ATT&CK:

- **Reconnaissance**
- **Discovery**
- **Initial Access**

---

9. Conclusão

Este projeto reforça a importância da visibilidade contínua dos ativos e da análise da superfície de ataque. Mesmo ambientes simples podem conter falhas relevantes de segurança.

A atividade demonstra habilidades fundamentais de um analista de SOC, com foco em prevenção, visibilidade e defesa proativa, evidenciando capacidade de análise técnica e comunicação de riscos.