RELATÓRIO DE AUDITORIA & ANÁLISE FORENSE

Projeto: Simulação — Lab de Segurança (segurancaRedes)
Data do experimento: Mon Nov 10 2025
Autor: Rafael Teixeira
Relatório gerado em: (data atual)

---

1. Resumo executivo

Durante uma execução controlada dos scripts de auditoria no laboratório isolado, foi realizada enumeração de rede e ataques de força bruta contra a VM vítima `192.168.56.101`. A enumeração identificou o serviço SSH aberto com OpenSSH 8.9p1 e chaves públicas com fingerprints registrados; a ofensiva com Hydra obteve **uma credencial válida** (usuário `linuxmint`, senha `linuxmint`) conforme saída do Hydra. Todos os artefatos gerados (Nmap, PCAPs, resultados do Hydra) foram coletados e têm seus hashes registrados no manifesto de execução.

Conclusão técnica: o host alvo aceita autenticação por senha em SSH com uma senha fraca reutilizada — vulnerabilidade de **autenticação fraca** que permite acesso não autorizado.

---

2. Escopo e objetivos

- Reproduzir e documentar a sequência de testes conduzidos no laboratório: enumeração (Nmap), captura de tráfego (pcap), ataque SSH (Hydra), simulação USB, demo web e coleta de evidências.
- Reunir e preservar evidências técnicas para inclusão no relatório final e para análise forense posterior.
- Fornecer recomendações práticas de mitigação.

---

3. Artefatos obtidos (evidências)

O manifesto central da execução registra todos os artefatos e seus hashes. Ver o manifesto: `evidencias/MANIFEST_20251110_125416.txt`.

Resumo das entradas relevantes: - `nmap_full_192.168.56.101_2025-11-10_125416.gnmap`
- `nmap_full_192.168.56.101_2025-11-10_125416.nmap`
- `nmap_full_192.168.56.101_2025-11-10_125416.xml`
- `02_PRE_CAPTURE_20251110_125416.pcap`
- `05_POST_CAPTURE_20251110_125416.pcap`
- `03_SSH_BRUTEFORCE_20251110_125416/hydra_output.txt`

O manifesto também lista avisos relativos a scripts não encontrados/executáveis na execução original.

---

4. Linha do tempo (timeline)

- Manifest criado: `Mon Nov 10 18:54:16 UTC 2025`
- Nmap scan iniciado: `Mon Nov 10 12:54:16 2025`
- Hydra run: `2025-11-10 13:02:27` → `2025-11-10 13:02:41`

Interpretação: os tempos podem refletir fusos locais diferentes. Sempre incluir UTC e local ao citar evidências.

---

5. Resultados técnicos detalhados

5.1 Enumeração — Nmap

Nmap identificou um único serviço TCP aberto: - Host: `192.168.56.101`
- Porta: **22/tcp** (ssh)
- Versão: **OpenSSH 8.9p1 (Ubuntu)**
- Fingerprints: - ECDSA: `1ce4e089eeda51aad3f86a05f0f914ff`
- ED25519: `67d183a5314866848d0e85eefd389810`

Impacto: exposição do SSH com senha habilitada permite brute-force e comprometimento.

5.2 Ataque SSH — Hydra

- Target: `192.168.56.101:22`
- Login: `linuxmint`
- Senha: `linuxmint`
- Mensagem: `[22][ssh] host: 192.168.56.101 login: linuxmint password: linuxmint`

Impacto: autenticação fraca e sucesso de login confirmam vulnerabilidade crítica.

5.3 Capturas de rede (PCAPs)

- `02_PRE_CAPTURE_20251110_125416.pcap`: captura pré-ataque (30s)
- `05_POST_CAPTURE_20251110_125416.pcap`: captura pós-ataque (30s)

Recomenda-se inspecionar com Wireshark ou Tshark para validar sessões SSH.

---

6. Procedimento de reprodução

1. Preparar ambiente:

```
git clone https://github.com/<usuario>/segurancaRedes.git
cd segurancaRedes
chmod +x scripts/*.sh
```

2. Executar orquestrador:

```
bash ./run_all_attacks.sh 2>&1 | tee run_all_attacks_$(date +
%Y%m%d_%H%M%S).log
```

3. Execução manual:

```
./scripts/nmap_enum.sh 192.168.56.101 evidencias/01_NMAP_<ts>
sudo timeout 30 tcpdump -i eth0 -w evidencias/02_PRE_CAPTURE_<ts>.pcap
./scripts/ssh_bruteforce.sh 192.168.56.101 linuxmint wordlists/
minhaLista.txt evidencias/03_SSH_BRUTEFORCE_<ts> 4
sudo timeout 30 tcpdump -i eth0 -w evidencias/05_POST_CAPTURE_<ts>.pcap
```

---

7. Cadeia de custódia e integridade

Verificação de integridade:

```
sha256sum -c evidencias/MANIFEST_20251110_125416.txt
```

Sempre comparar hashes com os do manifesto original.

---

8. Observações sobre lacunas

Alguns scripts não estavam presentes na execução original (simulação USB, demo web). As execuções foram parciais. Recomenda-se completar para uma nova coleta consolidada.

---

9. Conclusões e recomendações

Conclusões: - Senha fraca detectada (linuxmint/linuxmint) - Autenticação por senha permitida - SSH exposto na rede

Mitigações: 1. Desativar login por senha no SSH (`PasswordAuthentication no`). 2. Aplicar políticas de senha forte / MFA. 3. Restringir acesso SSH via firewall / sub-redes seguras. 4. Revisar sudoers e contas padrão. 5. Ativar auditoria (`auditd`) e logs centralizados. 6. Reexecutar testes após correções.

---

10. Anexos e próximos passos

- `MANIFEST_20251110_125416.txt`
- Resultados Nmap e Hydra
- PCAPs

Próximos passos: - Executar `hardening_lab.sh` na vítima. - Reexecutar orquestrador após correções. - Adicionar tabela de evidências e resumo final de hashes em `docs/EVIDENCIAS_SUMARIO.md`.