🧾RELATÓRIO DE AUDITORIA & ANÁLISE FORENSE

Projeto: Simulação — Lab de Segurança (segurancaRedes) **Data do experimento:** Nov 10 2025
Autores: Rafael Teixeira e Jhannyfer Sweyvezes Rodrigues Biangulo

---

1. Resumo executivo 📝

Durante a execução controlada no laboratório isolado, foram realizados testes de enumeração de rede, força bruta SSH e simulação de ataque via dispositivo USB. A enumeração identificou o serviço SSH aberto (OpenSSH 8.9p1) e a ofensiva Hydra obteve **uma credencial válida** (`linuxmint:linuxmint`). Na sequência, foi conduzida uma **simulação de inserção USB**, com execução automática de payload (`poc.sh`) obtendo privilégio root e gerando a evidência `/tmp/poc_run.txt`.

Todos os artefatos (Nmap, Hydra, PCAPs e logs USB) foram coletados, armazenados em diretórios por timestamp e possuem **hashes SHA256** registrados no manifesto.

Conclusão técnica: o experimento confirma vulnerabilidades críticas de **autenticação fraca** e **execução arbitrária via mídia removível**, indicando ausência de controles de mídia e hardening insuficiente.

---

2. Escopo e objetivos 🕐

- Reproduzir ataques controlados dentro do laboratório `segurancaRedes`.
- Coletar evidências digitais para análise forense.
- Demonstrar vetores reais de comprometimento (SSH e USB).
- Documentar resultados e recomendar mitigação.

---

3. Artefatos obtidos 📁

O manifesto central registra todos os artefatos: `evidencias/MANIFEST_20251110_125416.txt`

Tipo	Caminho	Descrição
Nmap	`evidencias/nmap_full_192.168.56.101_2025-11-10_125416.*`	Varredura e fingerprint SSH
PCAP	`evidencias/02_PRE_CAPTURE_20251110_125416.pcap`	Tráfego pré-ataque (30s)
PCAP	`evidencias/05_POST_CAPTURE_20251110_125416.pcap`	Tráfego pós-ataque (30s)

Tipo	Caminho	Descrição
SSH	`evidencias/hydra_output.txt`	Resultado do Hydra (credencial válida)
USB	`evidencias/06_USB_SIMULATION_20251110_125416/usb_simulation.log`	Log da simulação USB
USB	`evidencias/06_USB_SIMULATION_20251110_125416/poc_run.txt`	Prova de execução root (copiado de /tmp)

Todos os arquivos referenciados possuem SHA256 registrados no manifesto.

---

4. Linha do tempo ⏱️

Evento	Timestamp (local/UTC)
Manifest criado	Mon Nov 10 18:54:16 UTC 2025
Nmap scan iniciado	Mon Nov 10 12:54:16 2025
Hydra (início → fim)	2025-11-10 13:02:27 → 2025-11-10 13:02:41
Simulação USB (POC)	Mon Nov 10 19:58:25 Local

Observação: sempre apresentar timestamps em UTC e horário local da máquina para clareza forense.

---

5. Resultados técnicos detalhados 🔬

5.1 Enumeração — Nmap

Host: `192.168.56.101`
Porta: `22/tcp` — *ssh*
Versão: `OpenSSH 8.9p1 (Ubuntu)`
Fingerprints: - ECDSA: `1ce4e089eeda51aad3f86a05f0f914ff`
- ED25519: `67d183a5314866848d0e85eefd389810`

Impacto: SSH exposto com autenticação por senha, risco de brute-force.

5.2 Ataque SSH — Hydra

Resultado: credencial válida encontrada

```
Host: 192.168.56.101
login: linuxmint
password: linuxmint
```

Impacto: acesso não autorizado confirmado (vulnerabilidade crítica).

5.3 Capturas de rede (PCAP)

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

Ação recomendada: analisar PCAPs no Wireshark/tshark para identificar tentativas e sessões SSH, confirmar timings e tráfego associado ao exploit.

5.4 Simulação USB — execução de payload

Script: `simula_usb_and_execute.sh`
Saída relevante (trecho do log):

```
[*] Escrevendo payload em /mnt/usbimg/poc.sh...
[*] Executando payload simulado...
[+] POC executada com sucesso:
POC executed by root at Mon Nov 10 07:58:25 PM EST 2025
```

Arquivos coletados: `usb_simulation.log`, `poc_run.txt`, `sha256sums.txt` (localizados em `evidencias/06_USB_SIMULATION_20251110_125416`).

Impacto: prova de execução remota de código com privilégio root via mídia removível — falha grave de controle de dispositivos e políticas de montagem/autorun.

---

6. Procedimento de reprodução 🛠️

> Executar somente em ambiente isolado e controlado.

1. Clonar repositório e permitir execução dos scripts:

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

2. Rodar orquestrador (gera pastas de evidência e manifesto):

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

3. Fluxo manual (exemplo):

```
./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
# Simulação USB (rodar na vítima):
sudo /home/linuxmint/Desktop/segurancaRedes/scripts/
simula_usb_and_execute.sh /home/linuxmint/Desktop/segurancaRedes/
evidencias/06_USB_SIMULATION_<ts>
```

Nota: o script USB deve ser executado na VM vítima para que os artefatos reflitam o contexto de execução local.

---

7. Cadeia de custódia e integridade 🔐

Para validar a integridade dos artefatos:

```
# validar manifesto (contendo sha256 de cada arquivo)
sha256sum -c evidencias/MANIFEST_20251110_125416.txt

# validar hashes específicos da simulação USB
sha256sum -c evidencias/06_USB_SIMULATION_20251110_125416/sha256sums.txt
```

Recomenda-se manter uma cópia do tar original gerado na vítima e trabalhar apenas em cópias durante a análise.

---

8. Observações sobre lacunas 🔍

- Execução original reportou avisos de scripts ausentes em alguns passos; esses foram corrigidos ou reexecutados posteriormente.
- Timestamps e fuso-horário devem ser normalizados (UTC + local) ao anexar às conclusões formais.

---

9. Conclusões e recomendações 🔗

Conclusões: - Autenticação por senha (fraca) permitiu acesso não autorizado.
- Mídia removível permitiu execução de payload root.

Recomendações (priorizadas): 1. Desabilitar `PasswordAuthentication` e forçar uso de chaves SSH + MFA.
2. Implementar controle de mídia removível (`udev`, `usbguard`) e políticas de montagem (`noexec,nodev,nosuid`).
3. Centralizar logs e ativar `auditd` para rastreabilidade.

4. Atualizar e aplicar gestão de patches; revisar sudoers e contas padrão.
5. Reexecutar testes após mitigação e compor relatório comparativo.

---

10. Anexos & próximos passos 📎

- `evidencias/MANIFEST_20251110_125416.txt`
- `evidencias/01_NMAP_*/nmap_full_*.xml`
- `evidencias/02_PRE_CAPTURE_20251110_125416.pcap`
- `evidencias/05_POST_CAPTURE_20251110_125416.pcap`
- `evidencias/06_USB_SIMULATION_20251110_125416/*` (logs + poc_run.txt + sha256sums.txt)

Próximo passo: gerar `docs/EVIDENCIAS_SUMARIO.md` com uma tabela final de hashes e metadados para anexar ao relatório principal.

Documento gerado automaticamente a partir da execução dos scripts do repositório `segurancaRedes`*. Alterações posteriores deverão atualizar o manifesto e os hashes correspondentes.*