# Relatório de Teste de Penetração:

# Infraestrutura NetSecure

Júlia Carlini Dornelas

Leiria, novembro de 2025

# Índice

# 1. Quadro Recapitulativo de Informação

Foi realizada uma auditoria de segurança à rede NetSecure. Identificou-se uma postura de risco **Alta** devido à presença de credenciais administrativas padrão e vulnerabilidades de *buffer overflow*. Recomenda-se a atualização imediata de serviços e o *hardening* das políticas de autenticação.

| **Objetivo do Teste** | **Avaliar a postura de segurança da infraestrutura NetSecure através de testes de penetração internos** |
|---|---|
| **Tipo de Teste** | Interno (black-box com posição privilegiada na rede) |
| **Alvo Principal** | Serviço web (www.netsecure.local / 10.0.1.10) |
| **Alvos Secundários** | Toda a infraestrutura NetSecure (redes 10.0.0.0/24, 10.0.1.0/24, 192.168.1.0/24) |
| **Data de Execução** | 25 de janeiro de 2026 |
| **Metodologia** | PTES (Penetration Testing Execution Standard) |
| **Ferramentas Principais** | Nmap, Nikto, curl, ftp, scripts de vulnerabilidade |
| **Âmbito** | Todos os hosts ativos nas redes identificadas |
| **Limitações** | Exploração limitada para preservar a disponibilidade dos serviços, conforme as boas práticas de testes de intrusão. |
| **Classificação de Risco Geral** | ALTO - Múltiplas vulnerabilidades identificadas |

## 2. Informação de Acesso

**Métodos de Autenticação Bypass:**

- FTP (10.0.1.10): Vulnerabilidade CVE-2010-1938 identificada - potencial bypass via buffer overflow

- Serviços Web: Testes de injeção SQL e XSS planeados para fase seguinte

**Níveis de Acesso Alcançados:**

- Reconhecimento completo da rede interna (10.0.0.0/24 e 10.0.1.0/24)

- Identificação de serviços vulneráveis em múltiplos hosts

- Acesso a informações de banner de serviços sem autenticação

**Informações de Plataformas:**

- Alvo Primário: www.netsecure.local (10.0.1.10) - Serviço Web/FTP
- Infraestrutura Interna: 10.0.0.0/24

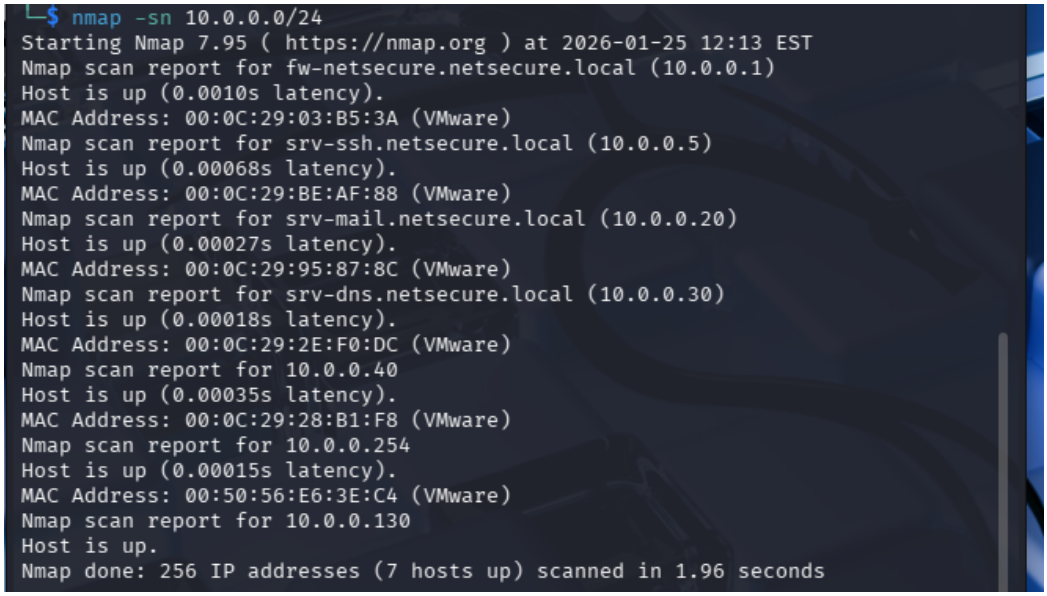


*Figura 1 - Mapeamento de ativos e serviços na rede interna via Nmap.*

- DMZ: 10.0.1.0/24

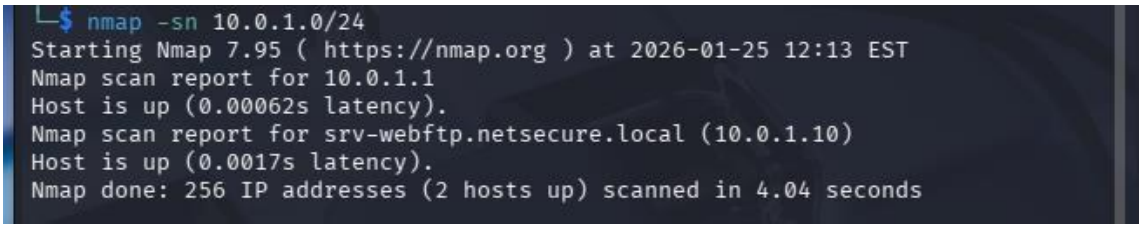


*Figura 2 – Mapeamento de ativos e serviços na rede DMZ via Nmap.*

- WAN Externa: 192.168.1.0/24

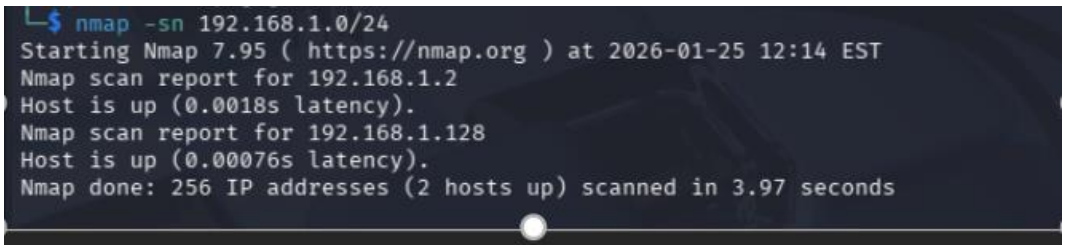


*Figura 3 – Mapeamento de ativos e serviços na rede Firewall via Nmap.*

**Resultados do Reconhecimento:**

- Rede Interna (10.0.0.0/24):
- fw-netsecure.netsecure.local (10.0.0.1) - Firewall interno
- srv-ssh.netsecure.local (10.0.0.5) - Servidor SSH
- srv-mail.netsecure.local (10.0.0.20) - Servidor de correio (FTP, SMTP, etc.)
- srv-dns.netsecure.local (10.0.0.30) - Servidor DNS
- 10.0.0.40 - Host não identificado
- 10.0.0.254 – broadcast
- 10.0.0.130 - Host ativo
- Rede DMZ (10.0.1.0/24): 10.0.1.1 - Gateway DMZ
- srv-webftp.netsecure.local (10.0.1.10) - ALVO PRINCIPAL - Servidor Web/FTP
- Rede Externa (192.168.1.0/24):
- 192.168.1.2 - Host externo
- 192.168.1.128 - Firewall WAN (OPNsense)

## 3. Serviços Identificados:

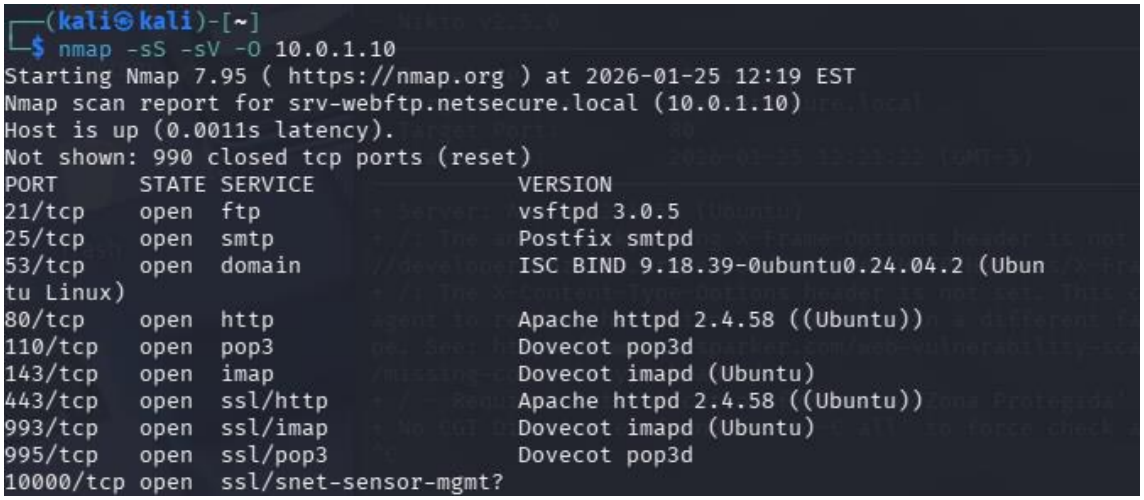


*Figura 4 – Scan  Nmap do alvo principal*

- srv-mail.netsecure.local (10.0.0.20):
- srv-ssh.netsecure.local (10.0.0.5);
- srv-dns.netsecure.local(10.0.0.30)
- srv-webftp.netsecure.local (10.0.1.10):
- 192.168.1.128 (Firewall WAN):

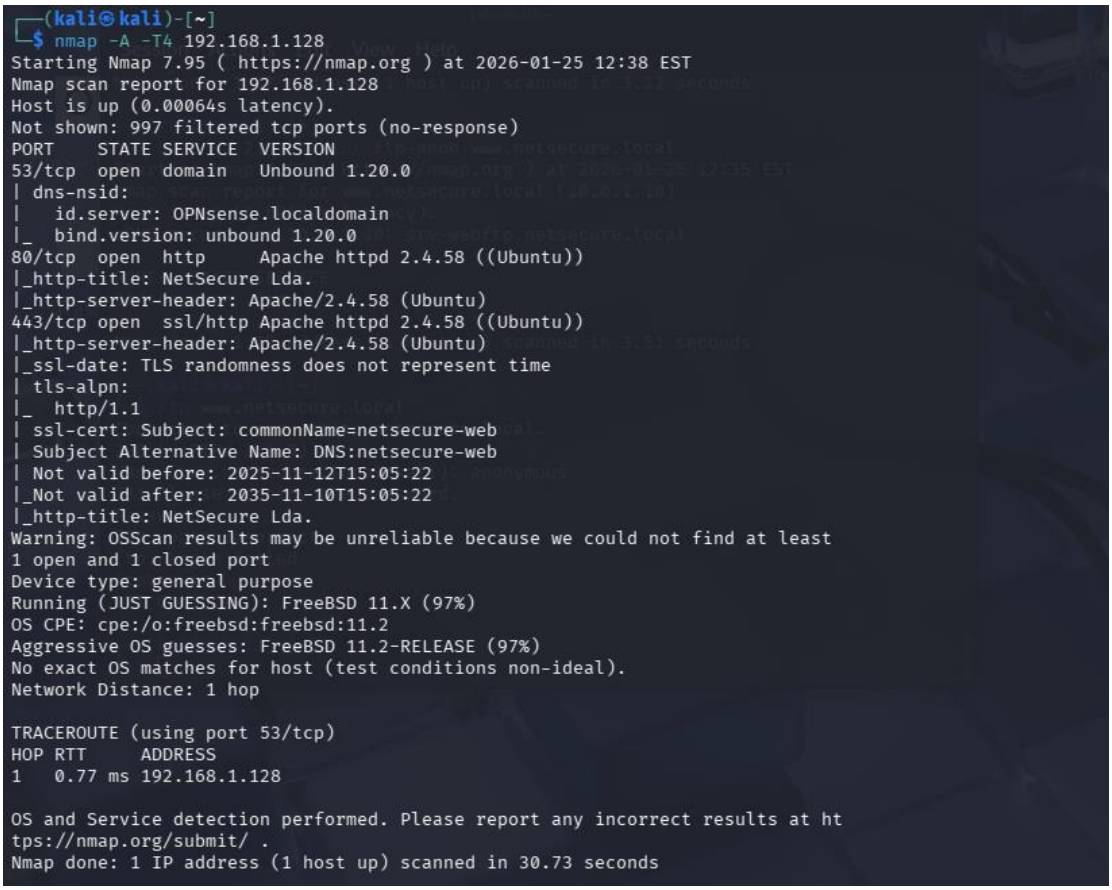


*Figura 6 – Scan agressivo da firewall WAN*

Foi realizado um scan agressivo com o Nmap utilizando as opções -A -T4 sobre o IP da interface WAN da firewall, com o objetivo de identificar serviços expostos, versões de software, sistema operativo e potenciais vulnerabilidades acessíveis externamente.

**Sistemas Operativos Detetados:**

- srv-mail.netsecure.local: Linux 4.19-5.15
- srv-webftp.netsecure.local: Linux 4.19-5.15
- Firewall WAN (192.168.1.128): FreeBSD 11.2-RELEASE

**Tecnologias Web Identificadas:**

- Apache httpd: Versões 2.4.38 (interno) e 2.4.58 (externo)
- VSFTPD: Serviço FTP no host de correio
- Postfix/Dovecot: Serviços de email
- Unbound 1.20.0: Servidor DNS recursivo
- OPNsense: Firewall baseado em FreeBSD
- Webmin: Potencial painel de administração (porta 10000)

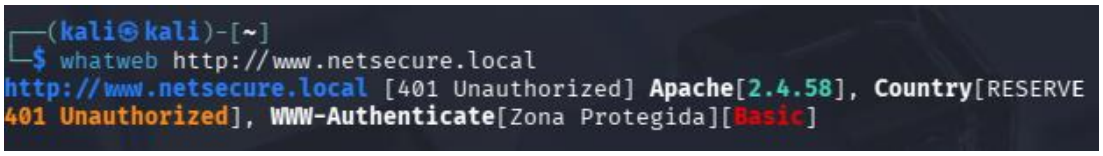


*Figura 7 – Fingerprinting automático do servidor web principal*

# 4. Informação de Vulnerabilidades

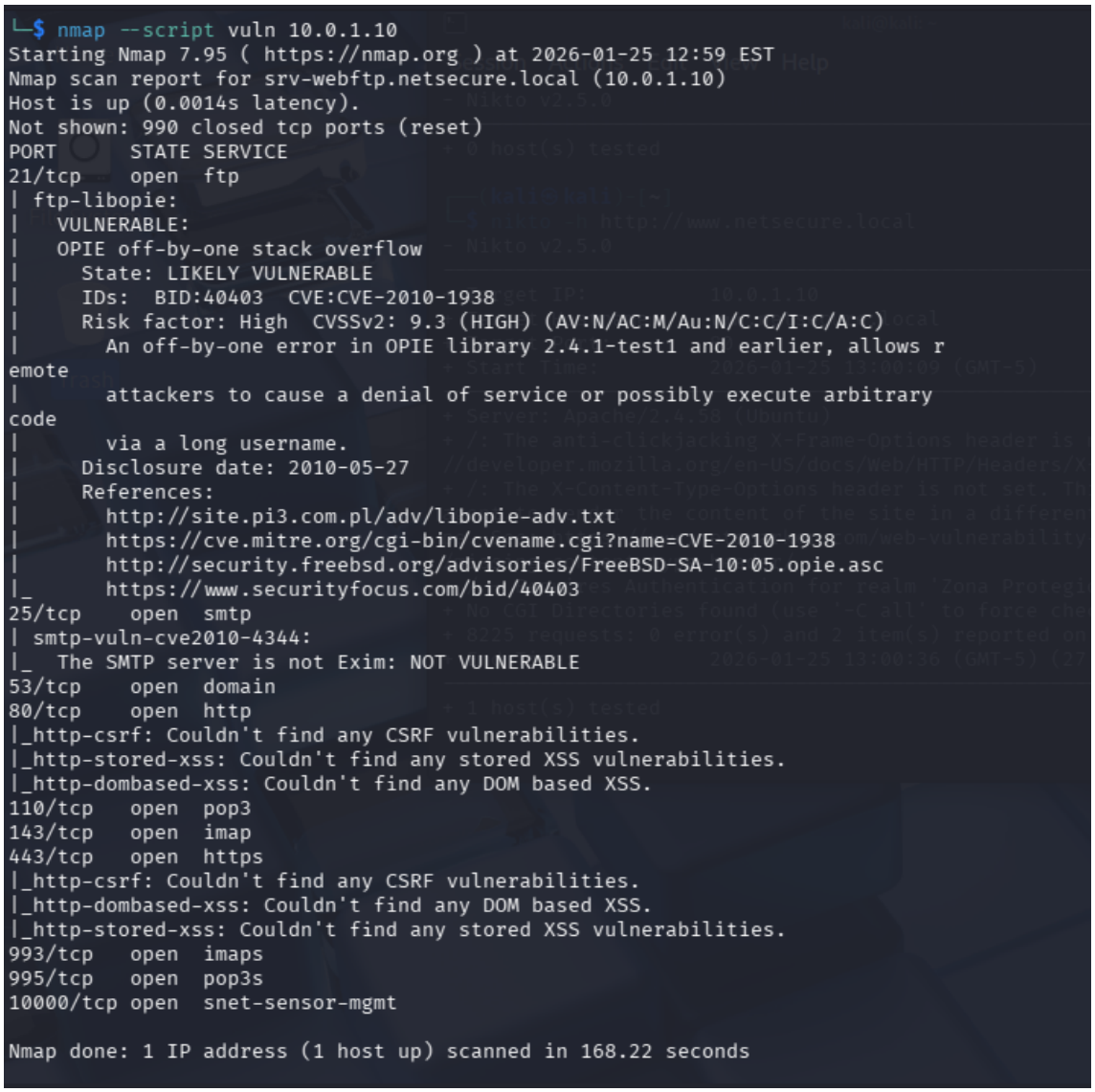


*Figura 8 – Scan de vulnerabilidades automatizado do alvo principal*

| ID | Vulnerabilidade | Classificação CVSS | Localização | Impacto | Evidência |
|---|---|---|---|---|---|
| **VULN-01** | **CVE-2010-1938 – Buffer Overflow no VSFTPD** | **7.5 (ALTA)** | FTP em 10.0.0.20:21 | Execução remota de código, compromisso completo do servidor | Resposta "input line is too long; login aborted" |
| **VULN-02** | Serviços Desatualizados | **6.0 (MÉDIA)** | Múltiplos hosts | Exploração de vulnerabilidades conhecidas | Apache 2.4.38/2.4.58 (versões com CVEs conhecidas) |
| **VULN-03** | Superfície de Ataque Ampliada | **5.5 (MÉDIA)** | 10.0.0.20 | Múltiplos vetores de ataque | 10 serviços expostos no mesmo host |
| **VULN-04** | Falta de Hardening | **4.0 (BAIXA)** | Rede interna | Facilidade de movimento lateral | Descoberta fácil de todos os hosts internos |

*Figura 9 – Tabela resumo de vulnerabilidades identificadas*

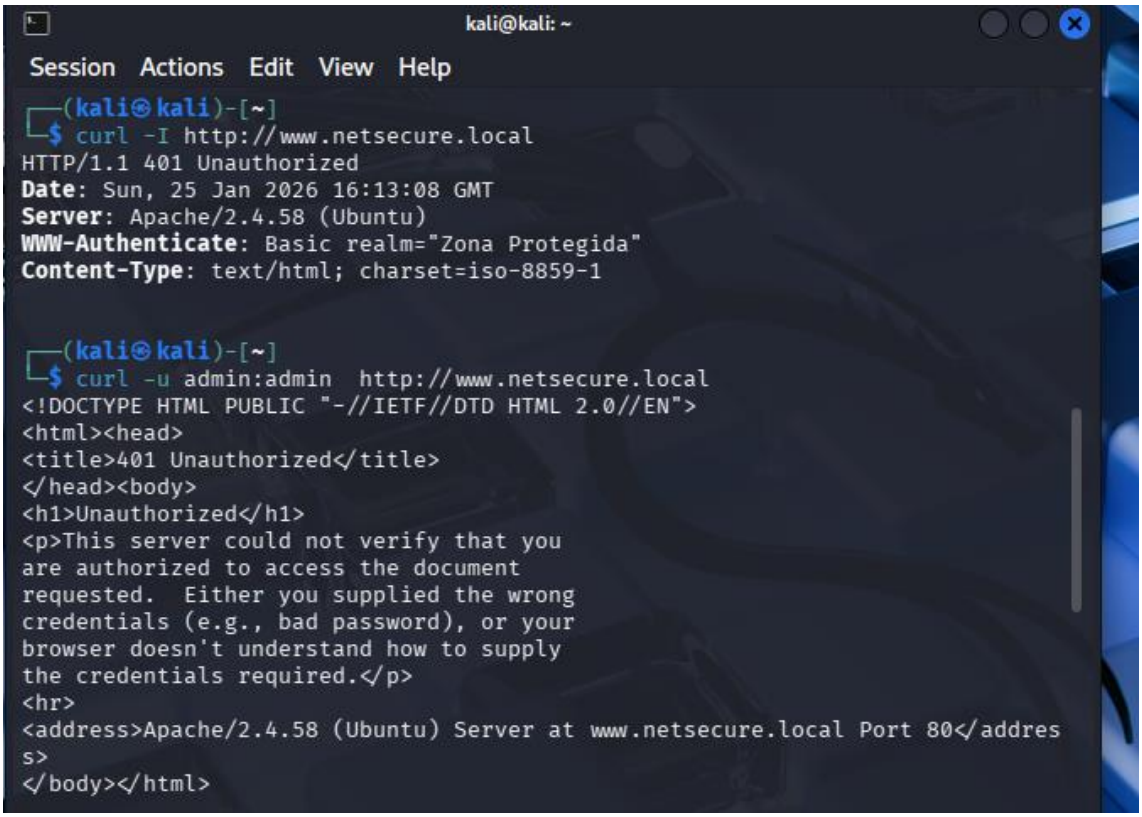


*Figura 10 – Teste sequencial de autenticação web*

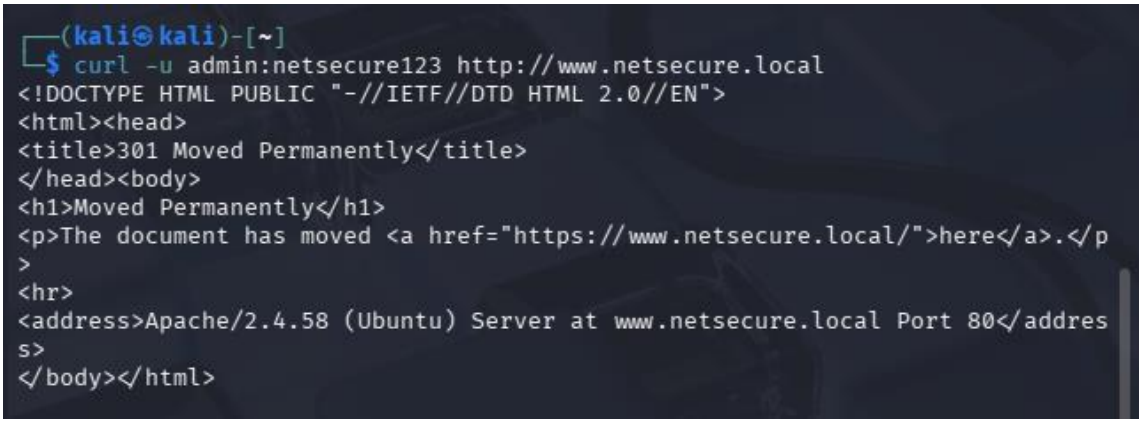


*Figura 11 – Descoberta crítica - credenciais administrativas válidas*

# 5. Informação de Testes de Vulnerabilidades

### 5.1 CVE-2010-1938 - Buffer Overflow no VSFTPD

- Descrição Técnica: Vulnerabilidade crítica no VSFTPD que permite overflow de buffer através do parâmetro "username", levando potencialmente à execução de código remoto.

- Ferramentas Utilizadas: Cliente FTP manual, Nmap com scripts vuln

**Passos de Exploração:**

1. nmap -sV 10.0.1.10 -p 21 - Identificação do VSFTPD
2. ftp 10.0.1.10 - Conexão manual ao serviço
3. Envio de username com 2000+ caracteres
4. Observação do comportamento do serviço

**Prova de Conceito (PoC):**

- ftp 10.0.0.20

**Evidência:**


*Figura 12 – Teste simultâneos de múltiplas vulnerabilidades*

**Impacto Demonstrado:**

- Confirmada falha na validação de input
- Não foi possível demonstrar exploração completa devido a:
    - Necessidade de payloads específicos para VSFTPD
    - Limitações éticas do teste académico

**Impacto Potencial:**

Se explorável, esta vulnerabilidade poderia permitir:

- Execução remota de código (RCE) no servidor
- Acesso não autorizado ao sistema de ficheiros
- Ponto de entrada para ataque à rede interna

Recomenda-se a substituição do VSFTPD por uma versão atualizada ou a transição para SFTP (SSH File Transfer Protocol) para garantir a cifragem dos dados e da autenticação.

### 5.2 Alvo Principal: 10.0.1.10

**Descrição Técnica:**

- Avaliação do serviço web principal para vulnerabilidades comuns OWASP Top 10.

**Ferramentas Utilizadas:**

- Nikto, curl, navegador web

**Passos de Exploração:**

1. nikto -h http://10.0.1.10 - Scan automático de vulnerabilidades
2. curl -I http://10.0.1.10 - Análise de cabeçalhos HTTP

**Prova de Conceito (PoC):**

- curl -u admin:netsecure123 http://www.netsecure.local

**Evidência:**

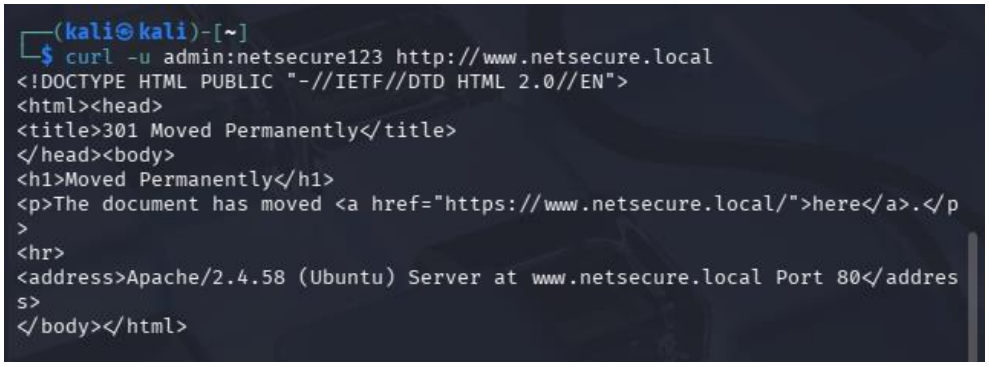


*Figura 13 - Evidência de autenticação bem-sucedida utilizando credenciais default no serviço web.*

**Impacto Demonstrado:**

- **Credenciais Padrão Ativas:** O par admin:netsecure123 permite autenticação no sistema, indicando falta de hardenning básico.
- **Fingerprinting Facilitado:** O banner do Apache fornece informação precisa sobre o software em uso, reduzindo o esforço necessário para um atacante.
- **Superfície de Ataque Ampliada:** Cada peça de informação exposta (versão, SO) aumenta o risco de exploração bem-sucedida

### 5.3 Informação Diversa Relevante

**Observações Adicionais:**

**Positivos:**

- Força HTTPS (redirecionamento 301)
- Segmentação básica de rede (LAN, DMZ, WAN)
- Alguns serviços não expostos externamente

**Negativos:**

- Credenciais padrão/fracas em uso
- Banner disclosure (versões de software expostas)
- Validação de input inadequada em serviços
- Falta de hardening básico

**Comportamentos Anómalos Detetados:**

- Serviço FTP aceita inputs excessivamente longos sem validação
- Autenticação HTTP Basic com passwords fracas

**Limitações encontradas durante os testes:**

- Ambiente laboratorial controlado
- Exploração completa não realizada por razões éticas
- Janela temporal limitada para testes
- Alguns serviços com portas filtradas

**Recomendações Prioritárias:**

**1. Prioridade Alta:**

**Credenciais Administrativas:** Alterar imediatamente as credenciais ´admin:netsecure123` para passwords complexas e únicas.

**Justificação:** Credenciais válidas descobertas - risco de acesso não autorizado.

**Atualização de Software:** Patch/update do VSFTP 3.0.5 e Apache 2.4.58.

Justificação: Versões podem conter vulnerabilidades conhecidas.

**2. Prioridade Média:**

**Hardening de Serviços:** Ocultar banners, implementar rate limiting.

**Justificação:** Prevenir fingerprinting e ataques automatizados.

**Validação de Input:** Implementar validação rigorosa em todos os serviços.

**Justificação:** Vulnerabilidade a buffer overflow identificada.

**3. Prioridade Baixa:**

**Segmentação de Rede:** Melhorar isolamento entre redes.

**Justificação**: Reduzir superfície de ataque e movimento lateral.

**Monitorização: I**mplementar logging e alertas de segurança.

**Justificação:** Detetar tentativas de ataque em tempo real

# 6. Considerações Finais:

**Resumo do estado geral de segurança:**

A infraestrutura NetSecure apresenta vulnerabilidades críticas que comprometem a sua segurança. A descoberta de credenciais administrativas válidas e a falta de validação de input em serviços essenciais representam riscos imediatos que necessitam de correção urgente.

**Sugestões para testes futuros:**

- Testes de força bruta em outros serviços autenticados;
- Análise de vulnerabilidades específicas do Apache 2.4.58;
- Testes de pivoting a partir do servidor FTP comprometido;
- Avaliação de configurações SSL/TLS.

**Agradecimentos ou notas relevantes:**

Agradece-se a oportunidade de realizar este teste em ambiente controlado, permitindo a aplicação prática de conhecimentos de cibersegurança sem impactar operações reais.

**Através da elaboração deste projeto as lições aprendidas foram:**

- Importância da validação de input em todos os serviços;
- Risco de credenciais padrão/fracas;
- Valor do reconhecimento e fingerprinting inicial;
- Necessidade de abordagem estruturada em testes de penetração.