

Relatório de Teste de Penetração: Infraestrutura NetSecure



Júlia Carlini Dornelas

Leiria, novembro de 2025

Índice

1. Quadro Recapitulativo de Informação.....	3
2. Informação de Acesso	4
3. Serviços Identificados:	6
4. Informação de Vulnerabilidades	9
5. Informação de Testes de Vulnerabilidades	12
6. Considerações Finais:.....	17

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

```
└─$ nmap -sn 10.0.0.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-25 12:13 EST
Nmap scan report for fw-netsecure.netsecure.local (10.0.0.1)
Host is up (0.0010s latency).
MAC Address: 00:0C:29:03:B5:3A (VMware)
Nmap scan report for srv-ssh.netsecure.local (10.0.0.5)
Host is up (0.00068s latency).
MAC Address: 00:0C:29:BE:AF:88 (VMware)
Nmap scan report for srv-mail.netsecure.local (10.0.0.20)
Host is up (0.00027s latency).
MAC Address: 00:0C:29:95:87:8C (VMware)
Nmap scan report for srv-dns.netsecure.local (10.0.0.30)
Host is up (0.00018s latency).
MAC Address: 00:0C:29:2E:F0:DC (VMware)
Nmap scan report for 10.0.0.40
Host is up (0.00035s latency).
MAC Address: 00:0C:29:28:B1:F8 (VMware)
Nmap scan report for 10.0.0.254
Host is up (0.00015s latency).
MAC Address: 00:50:56:E6:3E:C4 (VMware)
Nmap scan report for 10.0.0.130
Host is up.
Nmap done: 256 IP addresses (7 hosts up) scanned in 1.96 seconds
```

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

- DMZ: 10.0.1.0/24

```

$ nmap -sn 10.0.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-25 12:13 EST
Nmap scan report for 10.0.1.1
Host is up (0.00062s latency).
Nmap scan report for srv-webftp.netsecure.local (10.0.1.10)
Host is up (0.0017s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 4.04 seconds

```

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

- WAN Externa: 192.168.1.0/24

```

$ nmap -sn 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-25 12:14 EST
Nmap scan report for 192.168.1.2
Host is up (0.0018s latency).
Nmap scan report for 192.168.1.128
Host is up (0.00076s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 3.97 seconds

```

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:

```
(kali@kali)-[~]
$ nmap -sS -sV -O 10.0.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-25 12:19 EST
Nmap scan report for srv-webftp.netsecure.local (10.0.1.10)
Host is up (0.0011s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 3.0.5 (Ubuntu)
25/tcp    open  smtp           Postfix smtpd
53/tcp    open  domain         ISC BIND 9.18.39-0ubuntu0.24.04.2 (Ubuntu Linux)
80/tcp    open  http           Apache httpd 2.4.58 ((Ubuntu))
110/tcp   open  pop3           Dovecot pop3d
143/tcp   open  imap           Dovecot imapd (Ubuntu)
443/tcp   open  ssl/http       Apache httpd 2.4.58 ((Ubuntu))
993/tcp   open  ssl/imap       Dovecot imapd (Ubuntu)
995/tcp   open  ssl/pop3       Dovecot pop3d
10000/tcp open  ssl/snet-sensor-mgmt?
```

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):

```

(kali@kali)-[~]
$ nmap -A -T4 192.168.1.128
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-25 12:38 EST
Nmap scan report for 192.168.1.128
Host is up (0.00064s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
53/tcp    open  domain  Unbound 1.20.0
| dns-nsid:
|_ id.server: OPNsense.localdomain
|_ bind.version: unbound 1.20.0
80/tcp    open  http    Apache httpd 2.4.58 ((Ubuntu))
|_ http-title: NetSecure Lda.
|_ http-server-header: Apache/2.4.58 (Ubuntu)
443/tcp   open  ssl/http Apache httpd 2.4.58 ((Ubuntu))
|_ http-server-header: Apache/2.4.58 (Ubuntu)
|_ ssl-date: TLS randomness does not represent time
|_ tls-alpn:
|_ http/1.1
|_ ssl-cert: Subject: commonName=netsecure-web
| Subject Alternative Name: DNS:netsecure-web
|_ Not valid before: 2025-11-12T15:05:22
|_ Not valid after: 2035-11-10T15:05:22
|_ http-title: NetSecure Lda.
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (97%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (97%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE (using port 53/tcp)
HOP RTT ADDRESS
1 0.77 ms 192.168.1.128

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.73 seconds

```

Figura 6 – Scan agressivo da firewall WAN

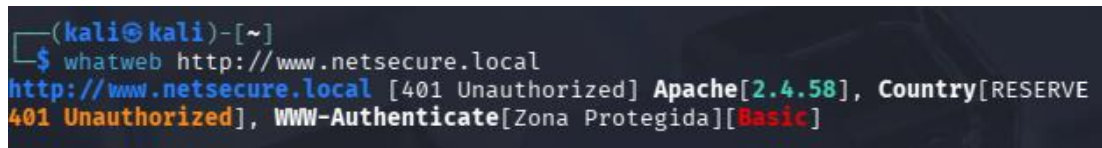
Foi realizado um scan agressivo com o Nmap utilizando as opções -A -T4 sobre o IP da interface WAN da firewall, com o objetivo de identificar serviços expostos, versões de software, sistema operativo e potenciais vulnerabilidades acessíveis externamente.

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)



```
(kali㉿kali)-[~]  
$ whatweb http://www.netsecure.local  
http://www.netsecure.local [401 Unauthorized] Apache[2.4.58], Country[RESERVE  
401 Unauthorized], WWW-Authenticate[Zona Protegida][Basic]
```

Figura 7 – Fingerprinting automático do servidor web principal

4. Informação de Vulnerabilidades

```
└─$ nmap --script vuln 10.0.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-25 12:59 EST
Nmap scan report for srv-webftp.netsecure.local (10.0.1.10)
Host is up (0.0014s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-libopie:
|   VULNERABLE:
|   OPIE off-by-one stack overflow
|   State: LIKELY VULNERABLE
|   IDs: BID:40403 CVE:CVE-2010-1938
|   Risk factor: High CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|   An off-by-one error in OPIE library 2.4.1-test1 and earlier, allows r
emote
|   attackers to cause a denial of service or possibly execute arbitrary
code
|   via a long username.
|   Disclosure date: 2010-05-27
|   References:
|   http://site.pi3.com.pl/adv/libopie-adv.txt
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1938
|   http://security.freebsd.org/advisories/FreeBSD-SA-10:05.opie.asc
|   https://www.securityfocus.com/bid/40403
25/tcp    open  smtp
| smtp-vuln-cve2010-4344:
|   The SMTP server is not Exim: NOT VULNERABLE
53/tcp    open  domain
80/tcp    open  http
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
993/tcp   open  imaps
995/tcp   open  pop3s
10000/tcp open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 168.22 seconds
```

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, comprometimento 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

```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ curl -I http://www.netsecure.local  
HTTP/1.1 401 Unauthorized  
Date: Sun, 25 Jan 2026 16:13:08 GMT  
Server: Apache/2.4.58 (Ubuntu)  
WWW-Authenticate: Basic realm="Zona Protegida"  
Content-Type: text/html; charset=iso-8859-1  
  
(kali@kali)-[~]  
$ curl -u admin:admin http://www.netsecure.local  
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">  
<html><head>  
<title>401 Unauthorized</title>  
</head><body>  
<h1>Unauthorized</h1>  
<p>This server could not verify that you  
are authorized to access the document  
requested. Either you supplied the wrong  
credentials (e.g., bad password), or your  
browser doesn't understand how to supply  
the credentials required.</p>  
<hr>  
<address>Apache/2.4.58 (Ubuntu) Server at www.netsecure.local Port 80</address>  
</body></html>
```

Figura 10 – Teste sequencial de autenticação web

```
(kali@kali)-[~]  
$ curl -u admin:netsecure123 http://www.netsecure.local  
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">  
<html><head>  
<title>301 Moved Permanently</title>  
</head><body>  
<h1>Moved Permanently</h1>  
<p>The document has moved <a href="https://www.netsecure.local/">here</a>.</p>  
<hr>  
<address>Apache/2.4.58 (Ubuntu) Server at www.netsecure.local Port 80</address>  
</body></html>
```

Figura 11 – Descoberta crítica - credenciais administrativas válidas

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

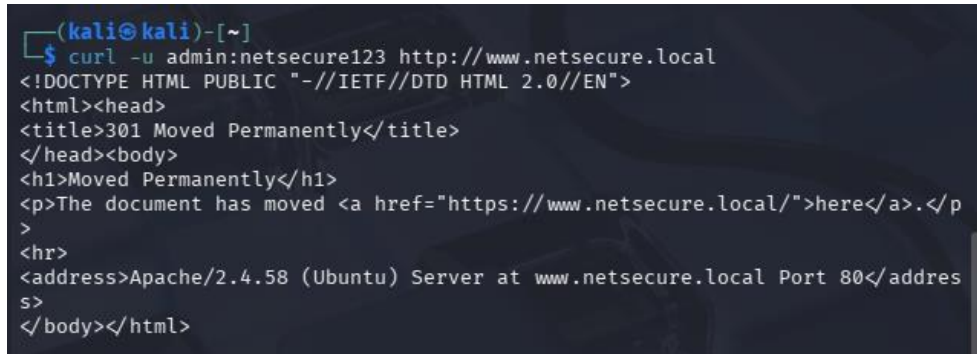
Passos de Exploração:

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:



```
(kali@kali)-[~]
$ curl -u admin:netsecure123 http://www.netsecure.local
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://www.netsecure.local/">here</a>.</p>
<hr>
<address>Apache/2.4.58 (Ubuntu) Server at www.netsecure.local Port 80</address>
</body></html>
```

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: Implementar 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.