



Ri IP

Mapeando a Superfície de Ataque

Com Nmap, Nikto e OpenVAS

Educação, Pesquisa
e Inovação em Rede



Agenda

- Importancia de mapear a superfície de ataques
 - Shadow IT: O inimigo oculto
- Identificação de Live Hosts
 - Métodos
 - Nmap
 - Desafios
- Identificação de vulnerabilidades
 - Métodos
 - Desafios
 - Openvas
 - Nikto
- Cases
 - Problemas
 - Soluções



Shadow IT

- Shadow IT
 - O que é?
 - Ativos, sistemas, serviços que não sabemos que estão na rede
 - Não podemos tornar seguro e monitorar o que não conhecemos
 - Excelente ponto de entrada para criminosos
 - Vamos falar do tema durante toda apresentação



Compleitude

- Compleitude
 - O que é?
 - Garantir que você encontrou tudo que procura
 - Live hosts
 - Portas abertas
 - Serviços rodando
 - Vulnerabilidades conhecidas
 - **Muito difícil garantir a completude**
 - Principalmente em dispositivos na internet
 - Um dos maiores inimigos é o tempo



Metodologia

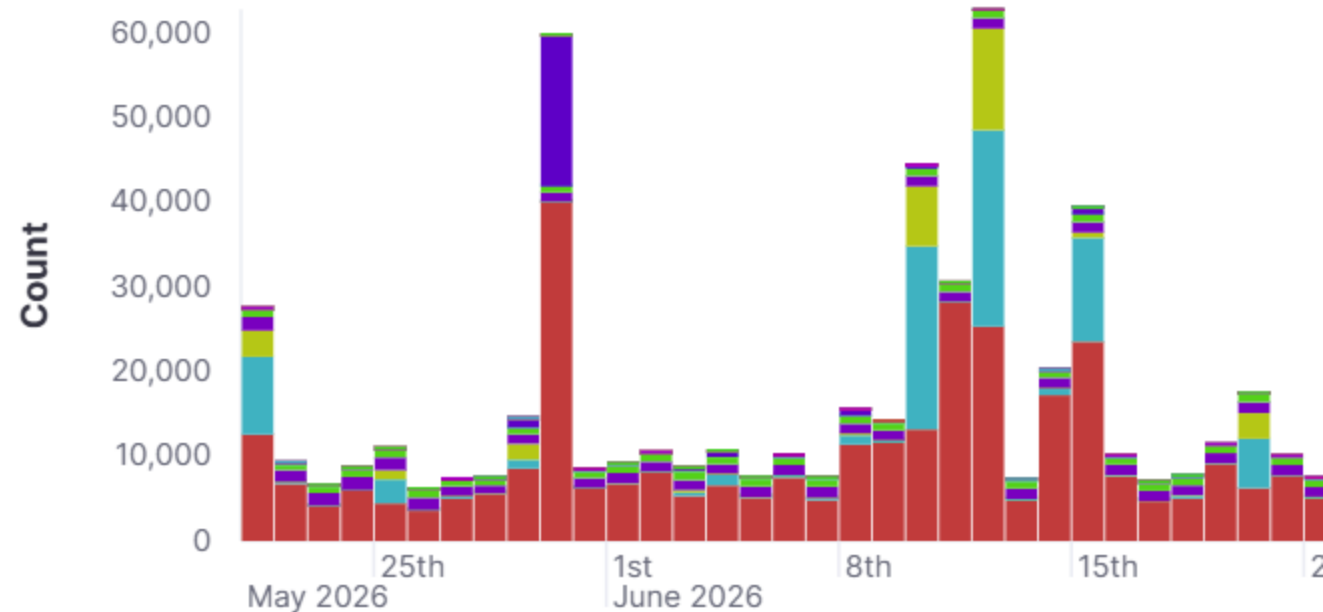
- Teorico vs Prática
- Teoria é importante, pois apenas rodar a ferramenta com o planejamento errado, pode invalidar os testes
- As ferramentas tem sua peculiaridade e não é simples transpor a teoria para a prática



Live Hosts

- Importância
 - Todos os sistemas online são atacados diariamente
 - De um honeypot em 24 horas tivemos 60 mil eventos em um dia
 - OBS: Nosso sistema não está listado em buscadores

Activity Types over Time [Filebeat Suricata]





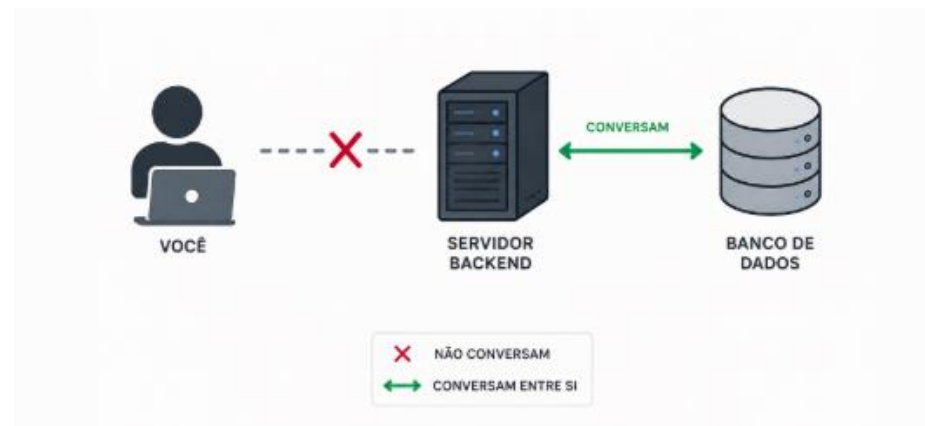
Live Hosts

- Descobrir os dispositivos na sua rede
 - Rede interna vs externa
 - Mais simples e rápido na rede interna
 - Bom ir por partes
 - Dispositivo online -> Descobrir o que é o dispositivo -> Serviços Rodando (portas abertas)
 - Quais os desafios?



Live Hosts

- Descobrir os dispositivos na sua rede
 - Rede interna vs externa
 - Mais simples e rápido na rede interna
 - Bom ir por partes
 - Dispositivo online -> Descobrir o que é o dispositivo -> Serviços Rodando (portas abertas)
 - Quais os desafios?
 - Técnica, tempo, dispositivos que não vão responder pra você (Alcançabilidade)

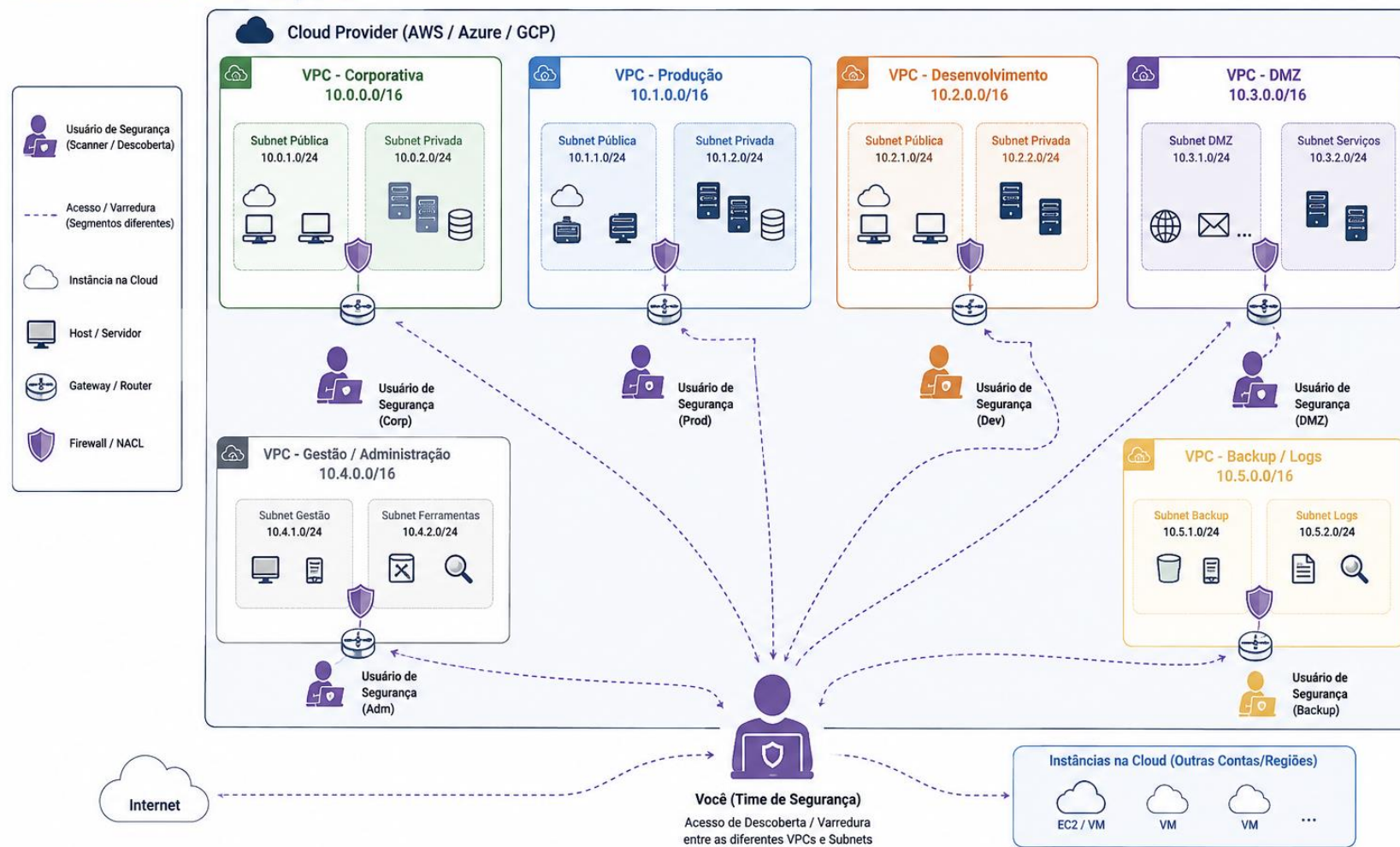




Live Hosts

Descoberta de Hosts (Live Hosts)

Ambiente Multi-VPC e Multi-Segmento





Live Hosts

- Técnicas

O objetivo é **obter evidências de que existe um host ativo em determinado endereço IP**, sem necessariamente realizar um port scan completo.

Técnica	Probe enviado	Resposta que indica host ativo
ARP	ARP Request	ARP Reply
ICMP Echo	ICMP Echo Request (Type 8)	Echo Reply (Type 0)
ICMP Timestamp	Timestamp Request (Type 13)	Timestamp Reply (Type 14)
TCP SYN	SYN para porta específica	SYN/ACK ou RST
TCP ACK	ACK para porta específica	RST
UDP	pacote UDP	Resposta UDP ou certos ICMP errors



Nmap

- Nmap
 - Site pro projeto nmap.org
 - Muito mais do que um portscan
 - Serve para identificar live hosts
 - Identificar serviços
 - Scripts interessantes (smb, vulnerabilidades, etc)
 - Você criar seus scripts em LUA
 - Ferramenta muito poderosa
 - Faz muitas coisas por padrão (tomar cuidado)



Nmap

- Comando: `nmap -sV 192.168.0.10`



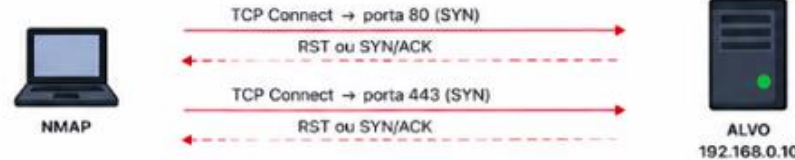
Nmap

- Comando: `nmap -sV 192.168.0.10`

 **SEM ROOT (usuário comum)**

`$ nmap -sV 192.168.0.10`

1 Host Discovery
Usa técnicas permitidas ao usuário comum (ex: TCP Connect nos ports 80 e 443).



2 Port Scan
Scan das TOP 1000 portas TCP mais comuns.
Método usado: **TCP CONNECT (-sT)** ← padrão sem root

3 Service/Version Detection (-sV)
Tenta identificar serviços e versões nas portas abertas.

```
$ nmap -sV 192.168.0.10
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-25 10:15 -03
Nmap scan report for 192.168.0.10
Host is up (0.0098s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd/2.4.57 ((Ubuntu))
443/tcp   open  ssl/http nginx 1.18.0 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.85 seconds
```

 Sem root, o Nmap não consegue enviar pacotes "raw" (SYN, ACK, etc).
Por isso usa **TCP CONNECT (-sT)**, que completa a conexão TCP.

 **COM ROOT (privilegios elevados)**

`# nmap -sV 192.168.0.10`

1 Host Discovery
Usa ARP (na rede local) e/ou probes mais completos para descobrir hosts.



2 Port Scan
Scan das TOP 1000 portas TCP mais comuns.
Método usado: **SYN SCAN (-sS)** ← padrão com root



3 Service/Version Detection (-sV)
Tenta identificar serviços e versões nas portas abertas.

```
# nmap -sV 192.168.0.10
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-25 10:15 -03
Nmap scan report for 192.168.0.10
Host is up (0.00083s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd/2.4.57 ((Ubuntu))
443/tcp   open  ssl/http nginx 1.18.0 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds
```

 Com root, o Nmap pode enviar pacotes "raw" (SYN, ACK, etc).
Por isso usa **SYN SCAN (-sS)**, que é mais rápido e menos detectável.



Nmap

- IP Externo

SEM ROOT (usuário comum)

```
$ nmap IP_EXTERNO
```

1 Host Discovery (sem root)
Sem privilégios, o Nmap não usa ARP ni raw packets.
Ele tenta descobrir o host usando TCP Connect nas portas 80 e 443.

TCP Connect → porta 80 (SYN)
Sem resposta (timeout)
TCP Connect → porta 443 (SYN)
Sem resposta (timeout)
...

! Usa TCP CONNECT (-sT).
Tenta se conectar nas portas 80 e 443 e interpreta a ausência de resposta.

2 Wireshark (externo_sem.pcap)
Comportamento observado sem root: tentativas TCP nas portas 80 e 443 (sem resposta).

Protocol	Length	Info
TCP	76	50592 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460
TCP	76	51750 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460
TCP	76	53870 → 443 [SYN] Seq=0 Win=32120 Len=0 MSS=1460
TCP	76	44108 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460
...		

3 Resultado do Nmap (IP DOWN)

```
Nmap scan report for IP_EXTERNO
Host is down (0.065s latency).
Nmap done: 1 IP address (0 hosts up) scanned in 5.21 seconds
```

COM ROOT (sudo)

```
# nmap IP_EXTERNO
```

1 Host Discovery (com root)
Com privilégios, o Nmap pode enviar e receber raw packets.
Na internet não há ARP, então ele usa métodos mais completos (ICMP + TCP).

ICMP Echo Request (ping)
Sem resposta
ICMP Timestamp Request
Sem resposta
TCP SYN → porta 80
Sem resposta
TCP SYN → porta 443
Sem resposta
...

✓ Usa métodos avançados (-PE -PP -PS -PA etc).
Mais técnicas = maior chance de descobrir o host.

2 Wireshark (externo_com.pcap)
Comportamento observado com root: ICMP (echo e timestamp) + TCP nas portas 80 e 443 (sem resposta).

Protocol	Length	Info
ICMP	44	Echo (ping) request id=0x685a, seq=0/0, ttl=45 (no response found!)
ICMP	56	Timestamp request id=0x4db1, seq=0/0, ttl=42
ICMP	56	Timestamp request id=0xfd1f, seq=0/0, ttl=50
TCP	56	42857 → 80 [SYN] Seq=1 Ack=1 Win=1024 Len=0
TCP	60	42859 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
ICMP	44	Echo (ping) request id=0x19b4, seq=0/0, ttl=54 (no response found!)
...		

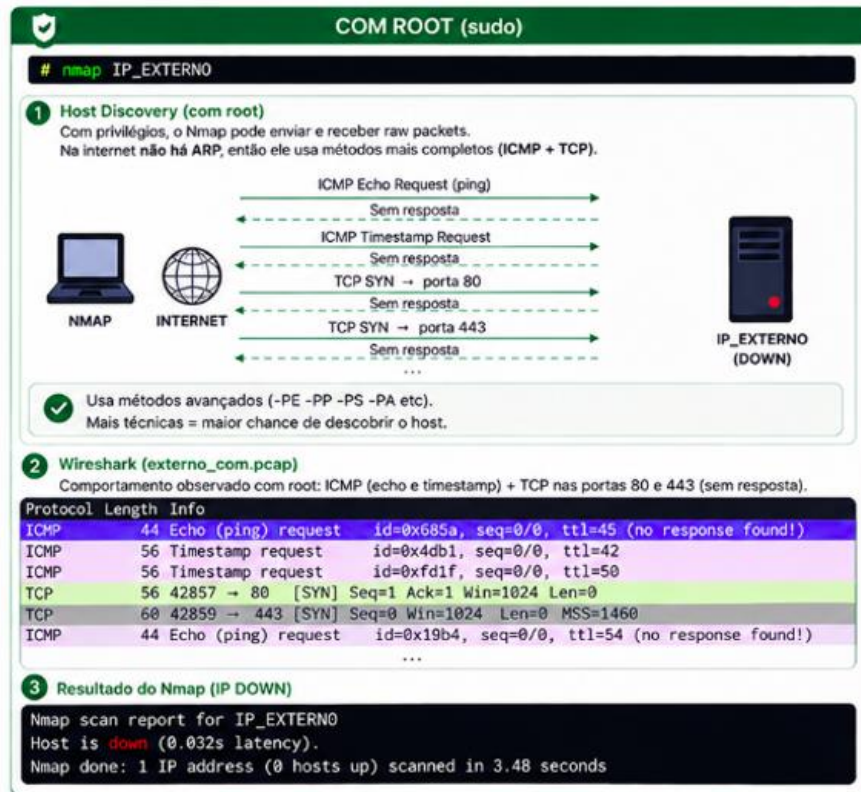
3 Resultado do Nmap (IP DOWN)

```
Nmap scan report for IP_EXTERNO
Host is down (0.032s latency).
Nmap done: 1 IP address (0 hosts up) scanned in 3.48 seconds
```



Nmap

- IP Externo



4 Comandos

- PE ICMP ECHO
- PP ICMP Timestamp
- PS80 TCP SYN 80
- PS443 TCP SYN 443

Considera UP se responder há qualquer um dos 4



Nmap

- Comando: nmap -PU (UDP) interna vs externa

Comando utilizado:

`nmap -PU 192.168.0.1/24`

Sou	Protocol	Length	Info
P...	ARP	44	Who has 192.168.0.13? Tell 192.168.0.182
P...	ARP	44	Who has 192.168.0.14? Tell 192.168.0.182
P...	ARP	44	Who has 192.168.0.15? Tell 192.168.0.182
P...	ARP	44	Who has 192.168.0.16? Tell 192.168.0.182
P...	ARP	44	Who has 192.168.0.19? Tell 192.168.0.182
P...	ARP	44	Who has 192.168.0.20? Tell 192.168.0.182
P...	ARP	44	Who has 192.168.0.21? Tell 192.168.0.182
P...	ARP	44	Who has 192.168.0.22? Tell 192.168.0.182
P...	ARP	44	Who has 192.168.0.23? Tell 192.168.0.182
P...	ARP	44	Who has 192.168.0.23? Tell 192.168.0.182
P...	ARP	44	Who has 192.168.0.24? Tell 192.168.0.182
P...	ARP	44	Who has 192.168.0.25? Tell 192.168.0.182
P...	ARP	44	Who has 192.168.0.26? Tell 192.168.0.182
P...	ARP	44	Who has 192.168.0.29? Tell 192.168.0.182
P...	ARP	44	Who has 192.168.0.30? Tell 192.168.0.182
P...	ARP	44	Who has 192.168.0.31? Tell 192.168.0.182
P...	ARP	44	Who has 192.168.0.35? Tell 192.168.0.182

Comando utilizado:

`nmap -PU 192.168.0.1/24`

200.171.1.43	1...	UDP	84	43176 → 40125	Len=40
200.171.1.44	1...	UDP	84	43176 → 40125	Len=40
200.171.1.45	1...	UDP	84	43176 → 40125	Len=40
200.171.1.46	1...	UDP	84	43176 → 40125	Len=40
200.171.1.47	1...	UDP	84	43176 → 40125	Len=40
200.171.1.48	1...	UDP	84	43176 → 40125	Len=40
200.171.1.49	1...	UDP	84	43176 → 40125	Len=40
200.171.1.50	1...	UDP	84	43176 → 40125	Len=40
200.171.1.51	1...	UDP	84	43176 → 40125	Len=40
200.171.1.52	1...	UDP	84	43176 → 40125	Len=40
200.171.1.43	1...	UDP	84	43178 → 40125	Len=40
200.171.1.44	1...	UDP	84	43178 → 40125	Len=40
200.171.1.44	1...	UDP	84	43178 → 40125	Len=40
200.171.1.45	1...	UDP	84	43178 → 40125	Len=40
200.171.1.46	1...	UDP	84	43178 → 40125	Len=40
200.171.1.47	1...	UDP	84	43178 → 40125	Len=40
200.171.1.48	1...	UDP	84	43178 → 40125	Len=40



Nmap

- Conclusões
 - Nmap faz muita coisas além dos comandos
 - Concluí coisas e muda a forma de atuar (rede interna vs externa)
 - Bom fazer scan de teste
 - Leia o manual



Host Discovery

- Conclusões
 - Seu sistema pode lutar contra você
 - Firewalls, regras internas, etc
 - Talvez seja interessante fazer scan da rede interna vs externa
 - O que responde está ativo, você não pode concluir o mesmo do que não responde
 - Criar um sistema para realizar o Discovery periodicamente



Scan de Vulnerabilidades

- Se o seu sistema está na internet, pessoas estão atacando ele
 - Números de um dia de um dos nossos honeypots
 - Mais de 30 mil tentativas de conexão no ssh
 - Mais de 2 mil HTTP requests
 - IP não está listado em buscadores
- Objetivo
 - Encontrar vulnerabilidades antes que um atacante encontre
 - Fazer levantamento de serviços
- Problemas
 - Completude
 - Tempo
 - Falsos positivos



Scan de Vulnerabilidades

- Se o seu sistema está na internet, pessoas estão atacando ele
 - Números de um dia de um dos nossos honeypots
 - Mais de 30 mil tentativas de conexão no ssh
 - Mais de 2 mil HTTP requests
 - IP não está listado em buscadores
- Objetivo
 - Encontrar (classificar e priorizar) vulnerabilidades antes que um atacante encontre
 - Fazer levantamento de serviços
- Problemas
 - Completude
 - Tempo
 - Falsos positivos



Scan de Vulnerabilidades

- Ponto de consideração
- Scan não autenticado: Scanner olha o ativo como um ataque o vê
- Scan autenticado: Scanner consegue acesso ao ativo
- Qual é melhor?
 - Não autenticado traz uma visão mais realista, bom pra justificar mudanças críticas
 - Autenticado, acha mais falhas, que podem ser exploradas

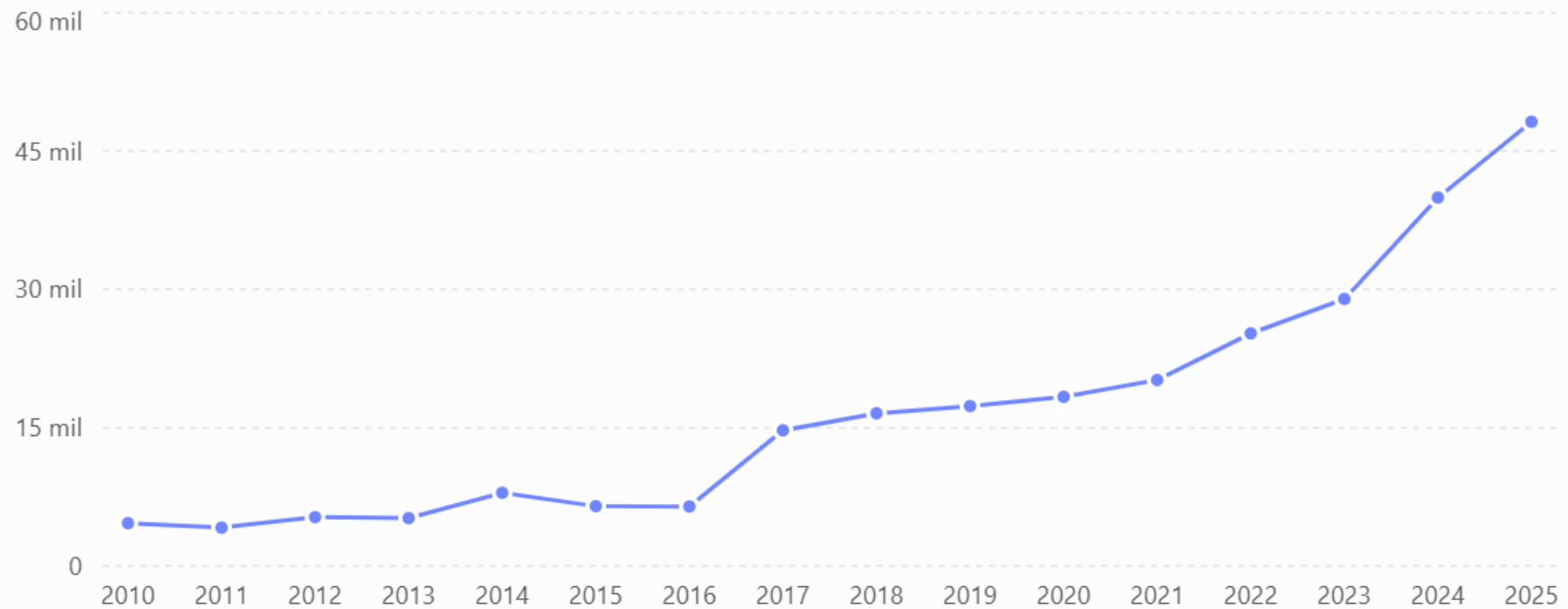


Situação atual

- Explosão de CVE

CVEs publicados por ano

Número de novos registros CVE publicados anualmente, 2010–2025.



Fonte: CVE Program / CVE Metrics. 2025: 48.185 registros publicados.

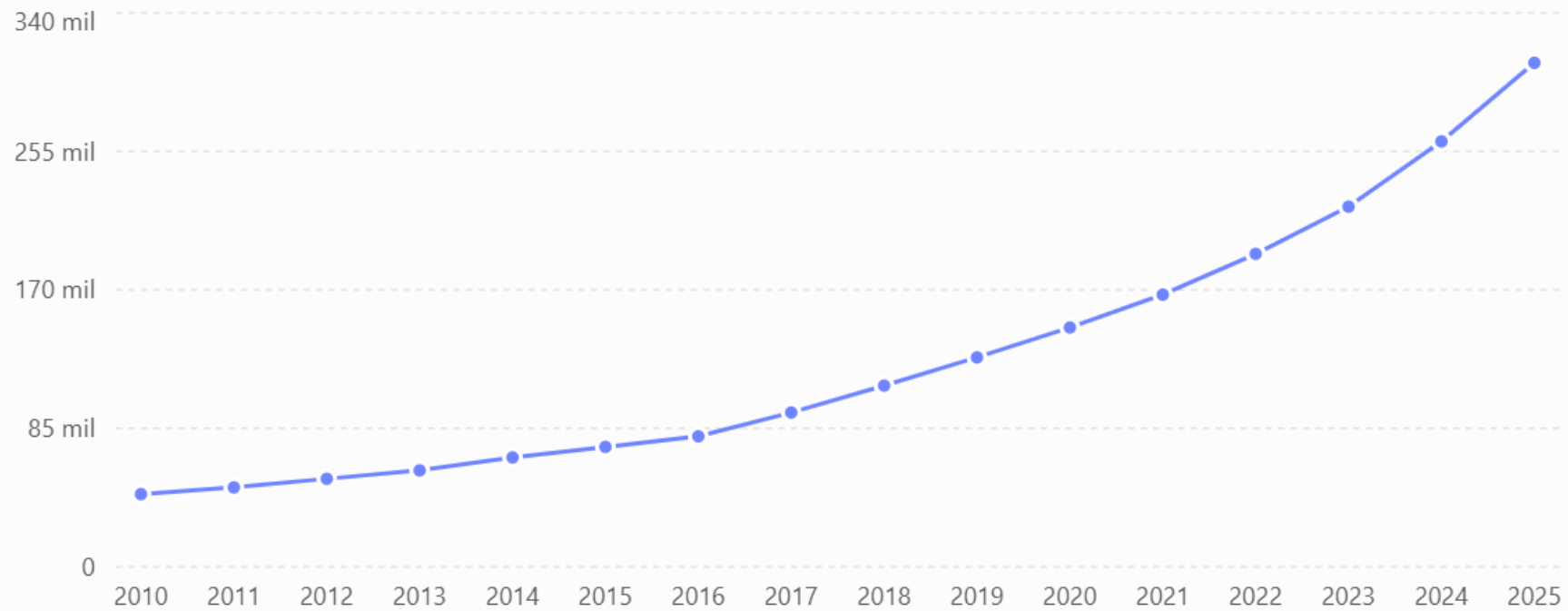


Situação atual

- Explosão de CVE

Total acumulado de CVEs

Crescimento do total de registros CVE publicados, acumulado desde 1999.



Fonte: CVE Program / CVE Metrics





Nikto

- Extremamente ao ponto
- Em torno de 7 mil testes (padrão)
- Relativamente flexível
- Possível fazer fuzz com ele (tem opções melhores, como o wfuzz)
- Uma ótima opção simples e prática
- Pontos fracos
 - Simples de mais
 - Fácil de detectar e bloquear
 - Payloads pouco flexíveis podem dar falsos “falso negativo”



Nikto

- Uso básico nikto -h SITE
 - -o RELATORIO -Format (htm, csv, xml, txt, json)
 - -Tuning 1: Arquivos, 4 Injeção, etc
 - -Tuning xNUMERO: Pula o teste **(-Tuning x6 pula DoS)**
 - -evasion: 1 Hex, 2 double //, 5 mistura maiúscula e minúscula
 - -Display (3 mostra 200, V verboso, S limpa ip e hostname)
 - Pode ser integrado com o formato grepable (-oG) do nmap
 - -timeout X (inteiro em segundos)
 - -useheaders "Cabeçalho browser"
 - Utilizar header padrão
 - Utilizar header de PC
 - Utilizar header de mobile
 - Apertar V ele começa a mostrar o teste atual



Nikto

- Report do nikto...

scanme.nmap.org /
45.33.32.156 port 80

Target IP	45.33.32.156
Target hostname	scanme.nmap.org
Target Port	80
HTTP Server	Apache/2.4.7 (Ubuntu)
Site Link (Name)	http://scanme.nmap.org:80/
Site Link (IP)	http://45.33.32.156:80/
URI	/
HTTP Method	GET
Description	/: The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://scanme.nmap.org:80/ http://45.33.32.156:80/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
URI	/
HTTP Method	GET
Description	/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
Test Links	http://scanme.nmap.org:80/ http://45.33.32.156:80/
References	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
URI	/index
HTTP Method	GET
Description	/index: Uncommon header 'tcn' found, with contents: list.
Test Links	http://scanme.nmap.org:80/index http://45.33.32.156:80/index
References	
URI	/index
HTTP Method	GET
Description	/index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html.
Test Links	http://scanme.nmap.org:80/index http://45.33.32.156:80/index
References	http://www.wisec.it/sectou.php?id=4698ebdc59d15 , https://exchange.xforce.ibmcloud.com/vulnerabilities/8275



Nikto

- Procurar consoles
- Nikto -h SITE -Tuning e -Display V

```
GET: /index.asp
GET: /junk999.asp
GET: /index.aspx
GET: /junk988.aspx
GET: /login.asp
GET: /login.aspx
GET: /
GET: /images
GET: /Autodiscover/Autodiscover.xml
GET: /Autodiscover/
GET: /Microsoft-Server-ActiveSync
GET: /Microsoft-Server-ActiveSync/default.css
GET: /ECP
GET: /EWS
GET: /EWS/Exchange.asmx
GET: /Exchange
GET: /OWA
GET: /Microsoft-Server-ActiveSync/default.eas
GET: /Rpc
GET: Web/HT/EWS/Services.wsdl -Options
GET: /ecp
GET: /OAB
GET: /aspnet_client
GET: /PowerShell
GET: .
GET: /
GET: /
scan for "Drupal Specific Tests" plugin
scan for "SSL and cert checks" plugin
scan for "IBM/Lotus Domino Specific Tests" plugin
GET: /domcfg.nsf
GET: /admin.nsf
GET: /admin4.nsf
GET: /admin5.nsf
GET: /webadmin.nsf
GET: /nonexistent.nsf
scan for "Apache Users" plugin
```



Nikto

- Pc vs mobile (tirando DOS, timeout bom, gerando relatório)
- `nikto -h http://SITE -Tuning x6 -timeout 1 -nossl -o relatorio_pc.html -Format htm -useheaders "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"`
- `nikto -h http://SITE -Tuning x6 -timeout 1 -nossl -o relatorio_mobile.html -Format htm -useheaders "User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 17_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.2 Mobile/15E148 Safari/604.1"`

— OpenVAS

- Scanner de vulnerabilidade consideravelmente completo
- Escaneia devices, e procura por vulnerabilidades conhecidas (problema do CVE)
- Possui dois componentes
 - GVM (Greenbone Vulnerability Manager): O motor que gerencia os testes.
 - GSAD ((Greenbone Security Assistant): A interface web.

A login form for Greenbone Security Assistant. It includes a small logo on the left, a "Username" field with "admin" entered, a "Password" field with "Password" entered, and a "Login" button.

	Username admin
	Password Password
	Login



OpenVAS

- Os feeds NVTs

- NVTs (Network Vulnerability Tests): São os scripts (manuais de instruções) que o OpenVAS usa para testar cada falha específica.
- Temos em torno de 160.00 NVTs
- Atualizado diariamente (atualizar o seu OpenVas antes de utiliza-lo)
- São feitos na sua própria linguagem NASL
- Quase sempre ligado a um CVE (foco caso queira testar um CVE em particular)
- Possui o QoD que diz a probabilidade da falha ser um positivo positivo
- Existe o público e o privado, e obviamente o privado é muito melhor.



OpenVAS

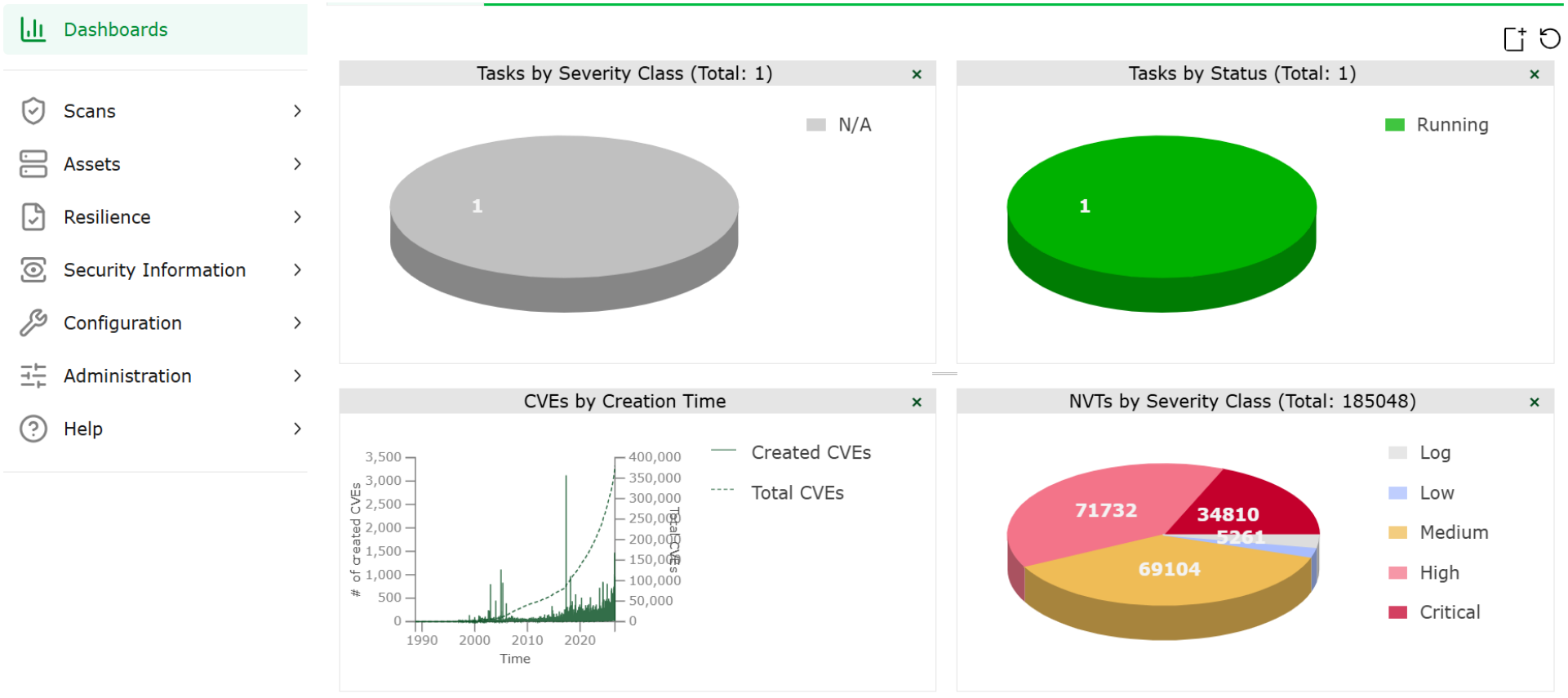
- Os feeds NVTs

- NVTs (Network Vulnerability Tests): São os scripts (manuais de instruções) que o OpenVAS usa para testar cada falha específica.
- Temos em torno de 160.00 NVTs
- Atualizado diariamente (atualizar o seu OpenVas antes de utiliza-lo)
- São feitos na sua própria linguagem NASL
- Quase sempre ligado a um CVE (foco caso queira testar um CVE em particular)
- Possui o QoD que diz a probabilidade da falha ser um positivo positivo
- Existe o público e o privado, e obviamente o privado é muito melhor.



OpenVAS

- Bashboard





OpenVAS

- Opções simples

Advanced Task Wizard



Quick start: Create a new task

This wizard can help you by creating a new scan task and automatically starting it.

All you need to do is enter a name for the new task and the IP address or host name of the target, and select a scan configuration.

You can choose, whether you want to run the scan immediately, schedule the task for a later date and time, or just create the task so you can run it manually later.

In order to run an authenticated scan, you have to select SSH and/or SMB credentials, but you can also run an unauthenticated

Task Name

Scan Config

Base

Discovery

empty

Full and fast

Host Discovery

Log4Shell

System Discovery

Start Time

Cancel

Create



OpenVAS

- 0 "problema" dos 98, 99%

Name ↑	Type	Status ↑↓	Reports ↑↓
Scan Autenticado		Done	1
Scan full		98 %	1
Scan não autenticado		Done	1

Edit Scan Config Full and fast Clone 1

non_simult_ports	139,445,3389,	139, 445, 3389, Service
open_sock_max_attempts	5	5
optimize_test	☒ Yes ☐ No	Yes
plugins_timeout	320	320
report_host_details	☒ Yes ☐ No	Yes
results_per_host	10	10
safe_checks	☒ Yes ☐ No	Yes
scanner_plugins_timeout	36000	36000



OpenVAS

- A questão do DoS

Edit Scan Config Full and fast Clone 1					
CentOS Local Security Checks	3255 of 0	   			
Citrix Xenserver Local Security Checks	30 of 0	   			
Compliance	16 of 0	   			
Databases	1200 of 0	   			
Debian Local Security Checks	18583 of 0	   			
Default Accounts	315 of 0	   			
Denial of Service	2407 of 0	   			
F5 Local Security Checks	125 of 0	   			
FTP	176 of 0	   			



Dúvidas?



Adobe Stock | #218820745