RNP

Educação, Pesquisa
e Inovação em Rede

Mapeando a Superfície de Ataque

Com Nmap, Nikto e OpenVAS

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

Completude

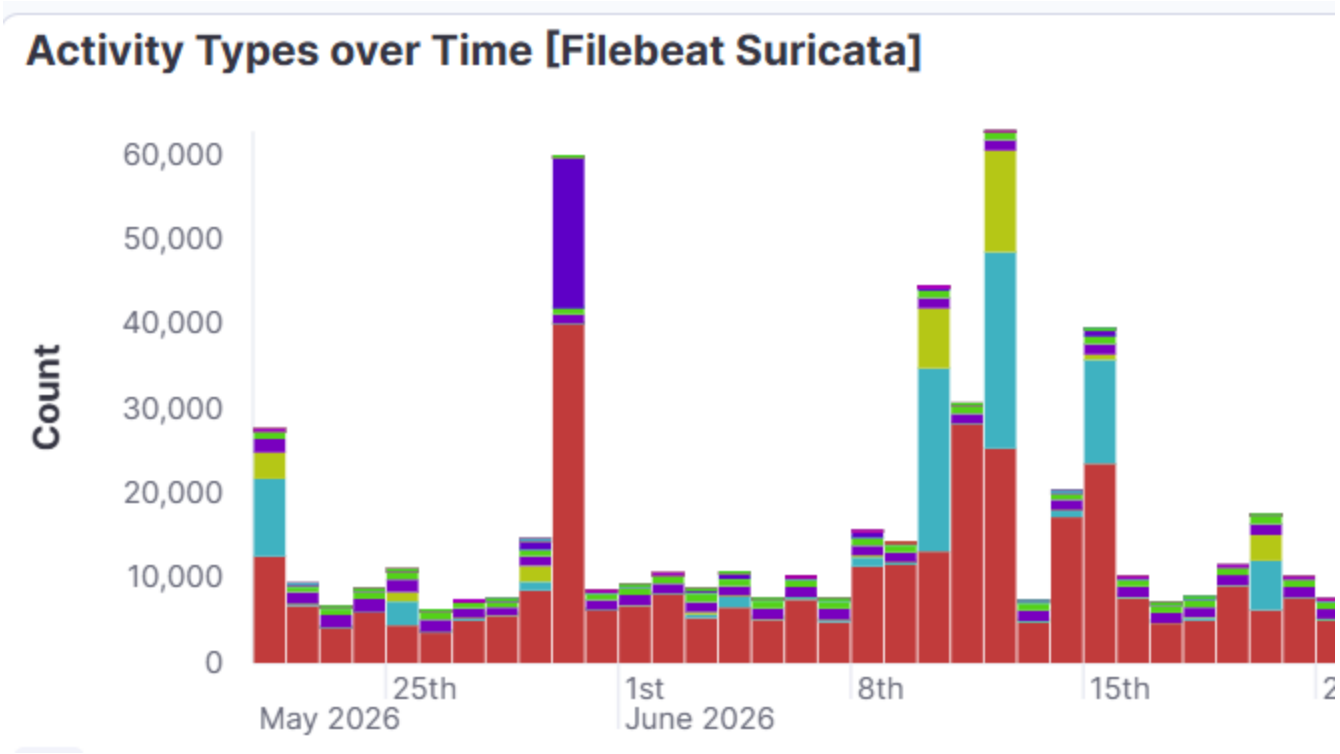
- Completude
  - O que é?
    - Garantir que você encontrou tudo que procura
  - Live hosts
  - Portas abertas
  - Serviços rodando
  - Vulnerabilidades conhecidas
  - **Muito difícil garantir a completude**
    - Principalmente em dispositivos na internet
  - Um dos maiores inimigos é o tempo

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

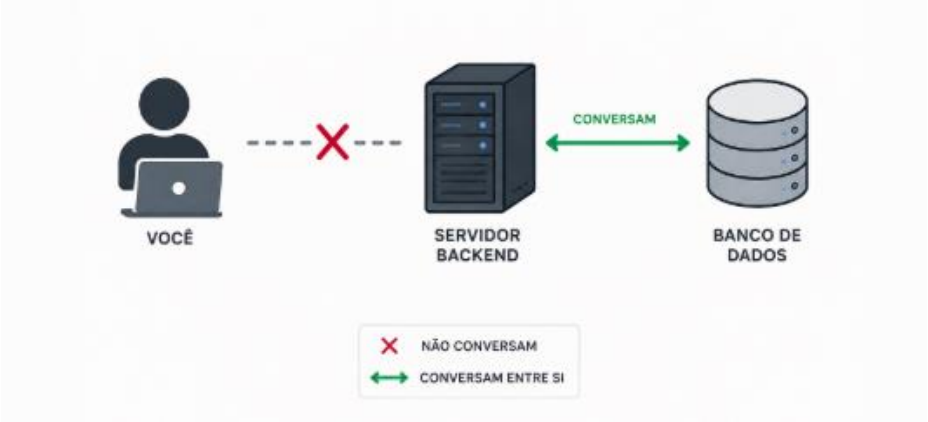


Live Hosts

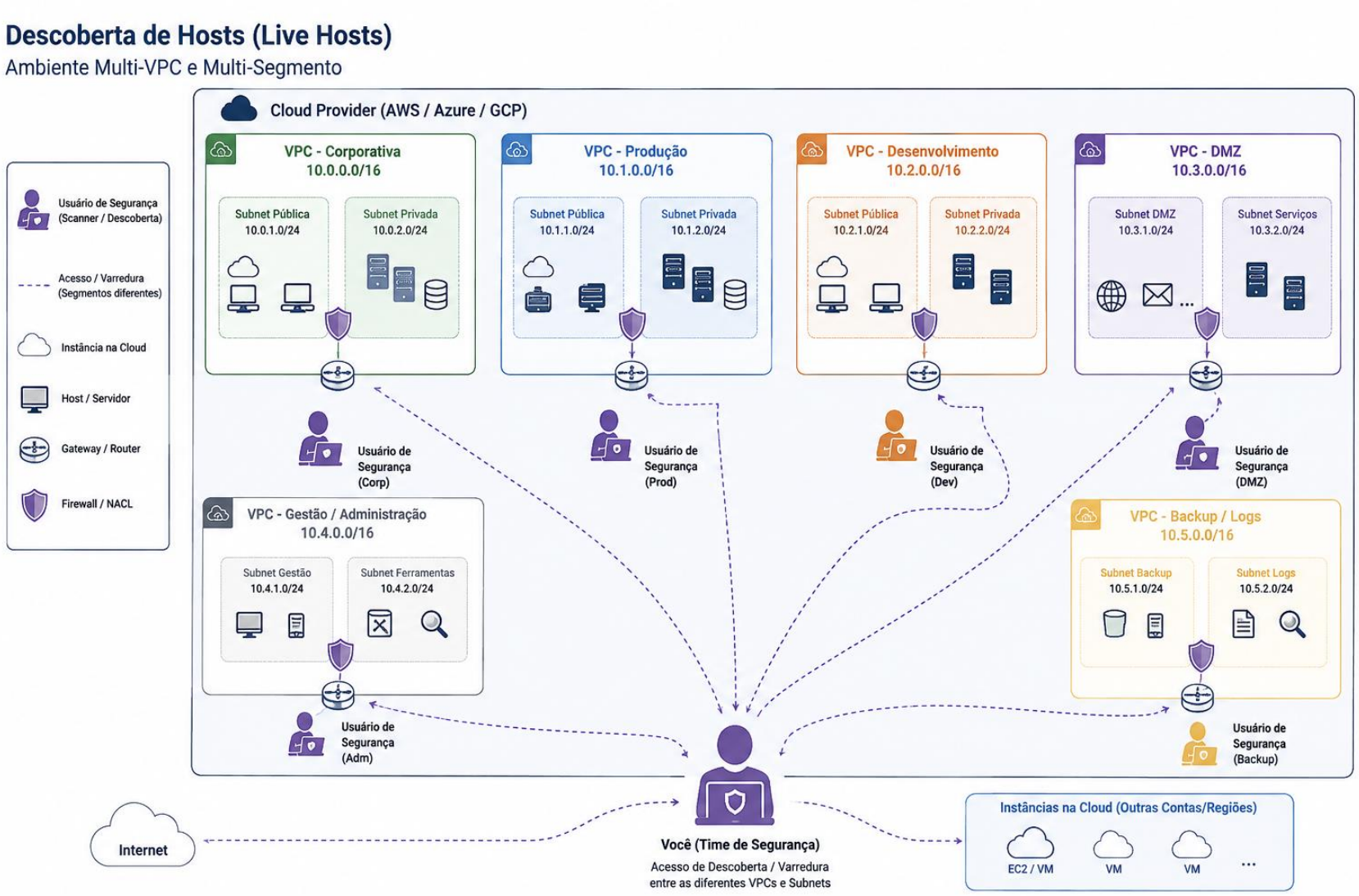
- Descobrir os dispositivos na sua rede
  - Rede interna vs externa
    - Mais simples e rápido na rede interna
  - Bom ir por partes
    - Dispositivo online -> Descobrir o que é o dispositivo -> Serviços Rodando (portas abertas)
  - Quais os desafios?

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
Cloud Provider (AWS / Azure / GCP)
Usuário de Segurança (Scanner / Descoberta)
Acesso / Varredura (Segmentos diferentes)
Instância na Cloud
Host / Servidor
Gateway / Router
Firewall / NACL
VPC - Corporativa
10.0.0.0/16
Subnet Pública
10.0.1.0/24
Subnet Privada
10.0.2.0/24
VPC - Produção
10.1.0.0/16
Subnet Pública
10.1.1.0/24
Subnet Privada
10.1.2.0/24
VPC - Desenvolvimento
10.2.0.0/16
Subnet Pública
10.2.1.0/24
Subnet Privada
10.2.2.0/24
VPC - DMZ
10.3.0.0/16
Subnet DMZ
10.3.1.0/24
Subnet Serviços
10.3.2.0/24
Usuário de Segurança (Corp)
Usuário de Segurança (Prod)
Usuário de Segurança (Dev)
Usuário de Segurança (DMZ)
VPC - Gestão / Administração
10.4.0.0/16
Subnet Gestão
10.4.1.0/24
Subnet Ferramentas
10.4.2.0/24
VPC - Backup / Logs
10.5.0.0/16
Subnet Backup
10.5.1.0/24
Subnet Logs
10.5.2.0/24
Usuário de Segurança (Adm)
Usuário de Segurança (Backup)
Internet
Você (Time de Segurança)
Acesso de Descoberta / Varredura entre as diferentes VPCs e Subnets
Instâncias na Cloud (Outras Contas/Regiões)
EC2 / VM
VM
VM

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

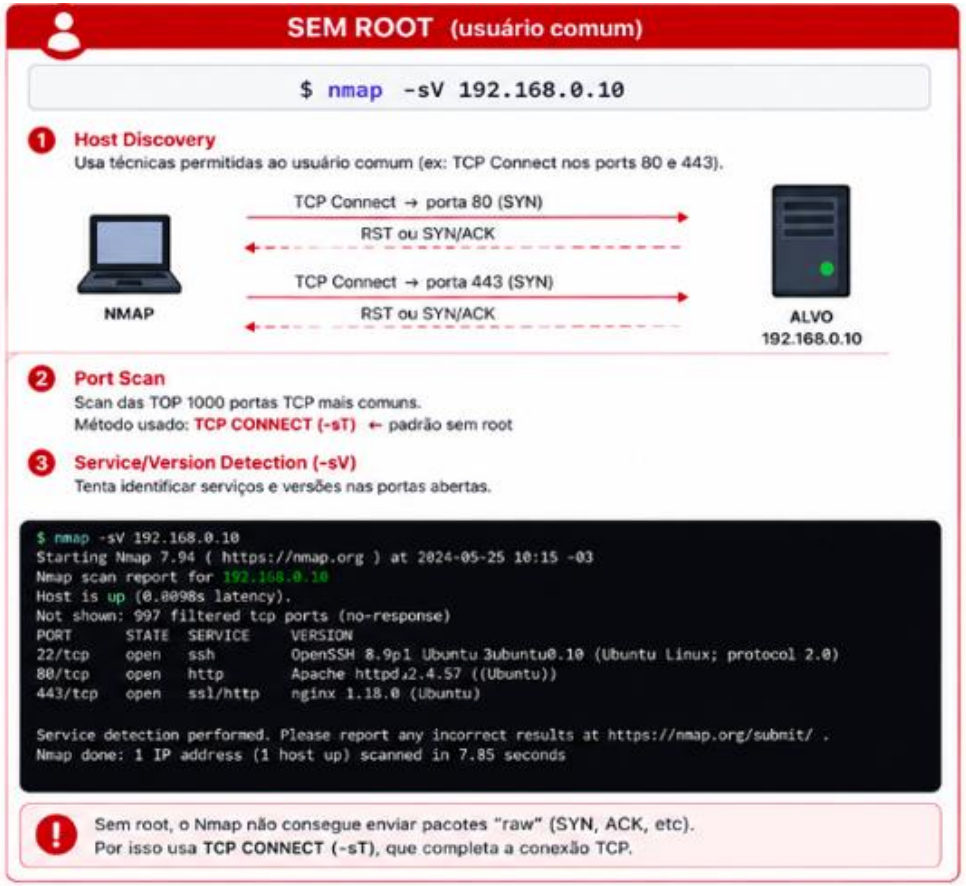
- Nmap
  - Site pro projeto nmap.org
  - Muito mais do que um portscan
  - Serve para identificar live hosts
  - Identificar serviços
  - Scripts interessantes (smb, vulnerabilidades, etc)
  - Você criar seus scripts em LUA
  - Ferramenta muito poderosa
  - Faz muitas coisas por padrão (tomar cuidado)

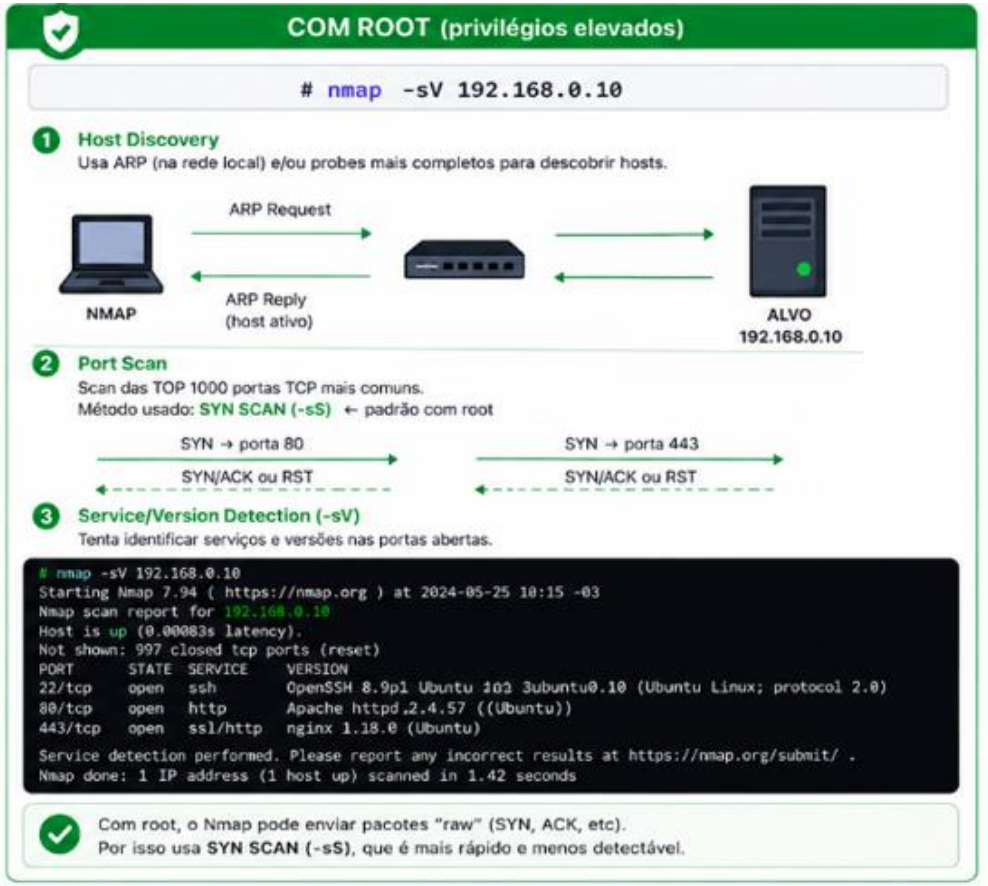
Nmap

- Comando: nmap –sV 192.168.0.10

Nmap

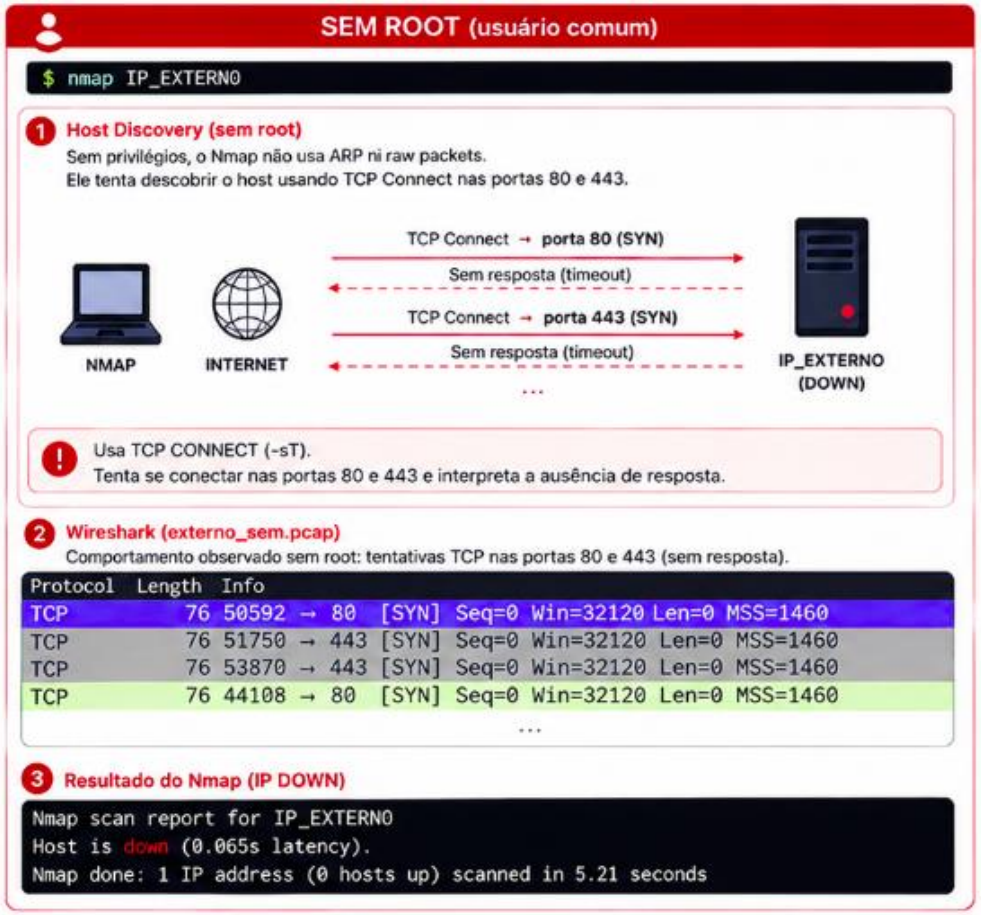
- Comando: nmap –sV 192.168.0.10

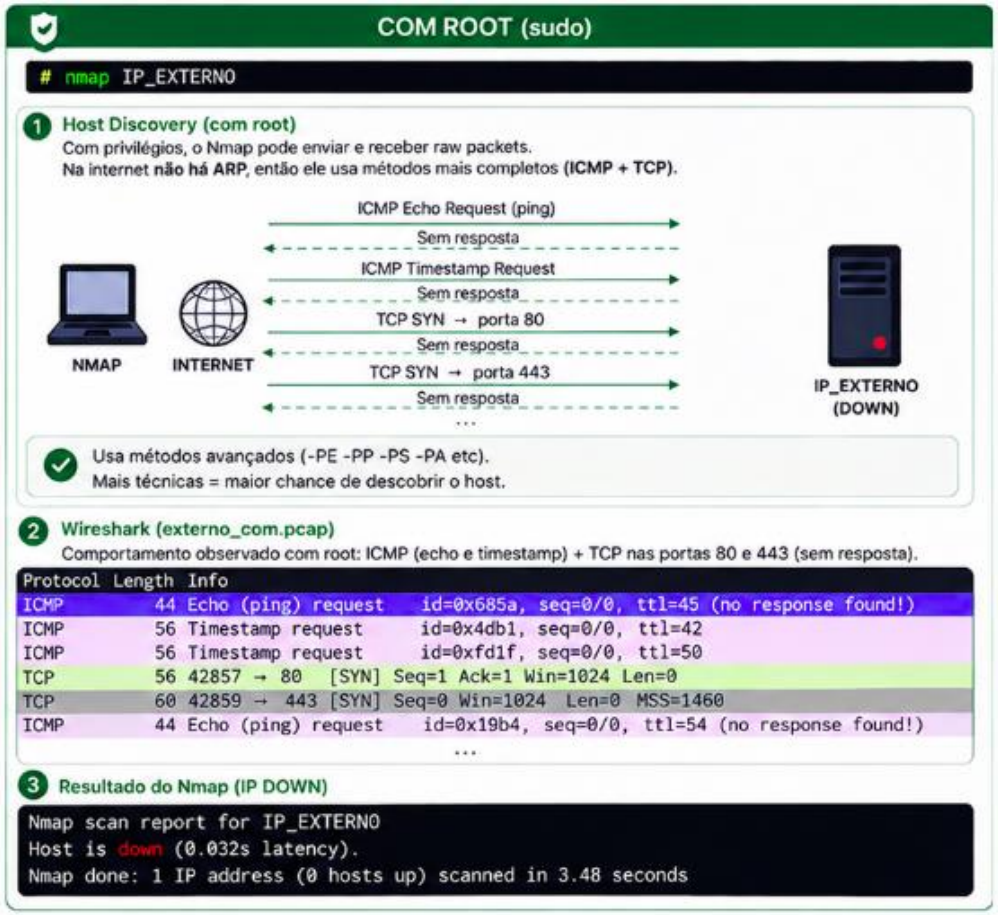




Nmap

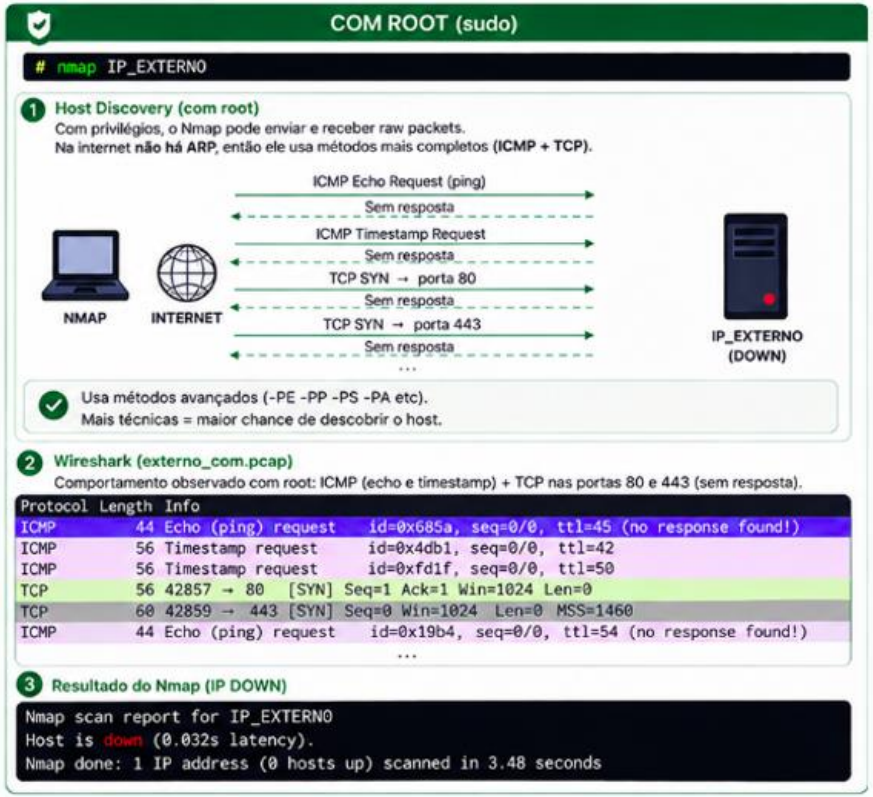
- IP Externo





Nmap

- IP Externo



4 Comandos

-PE ICMP ECHO
-PP ICMP Timestramp
-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

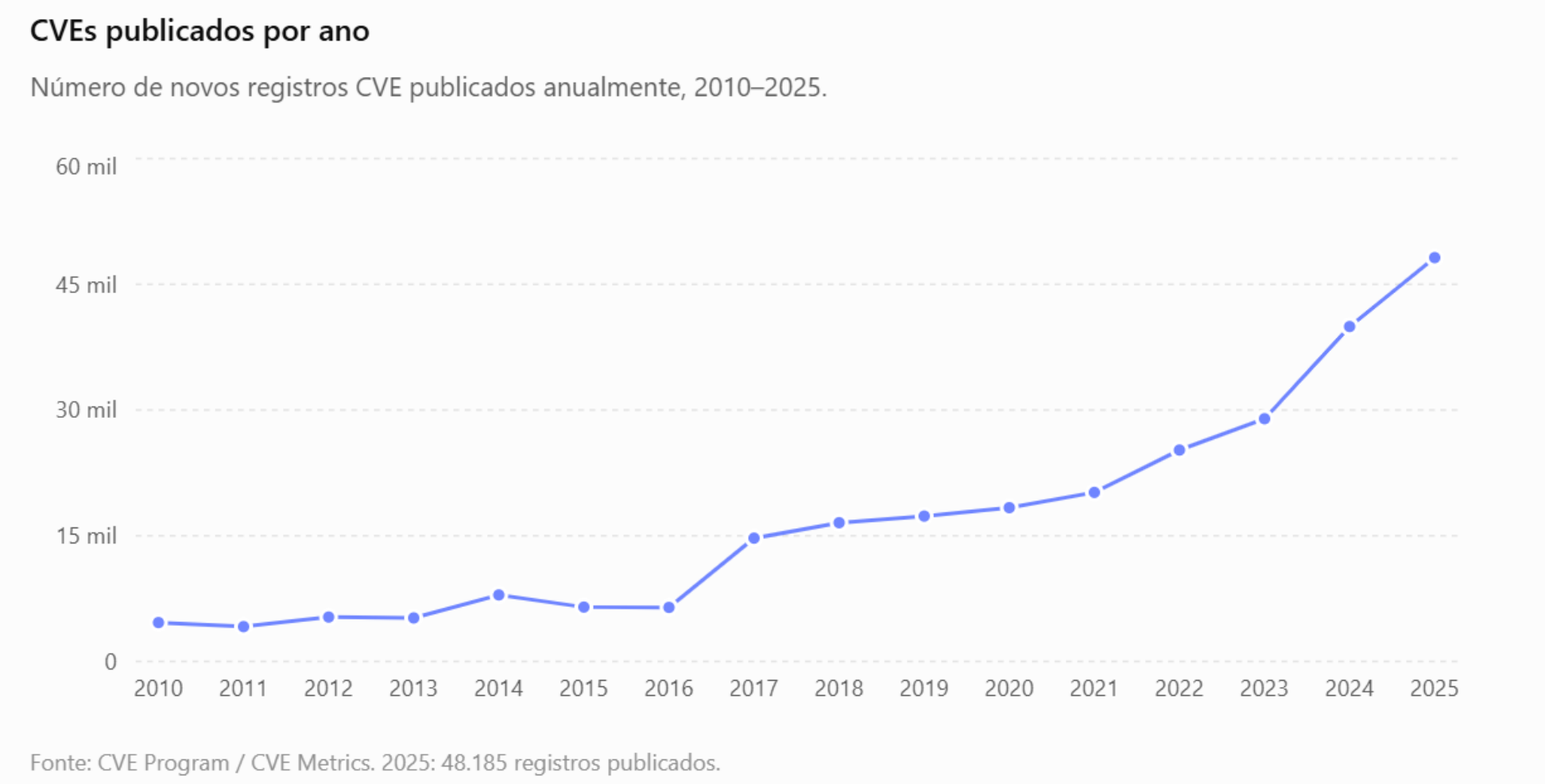
- Problemas
  - Completude
  - Tempo
  - Falsos positivos

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

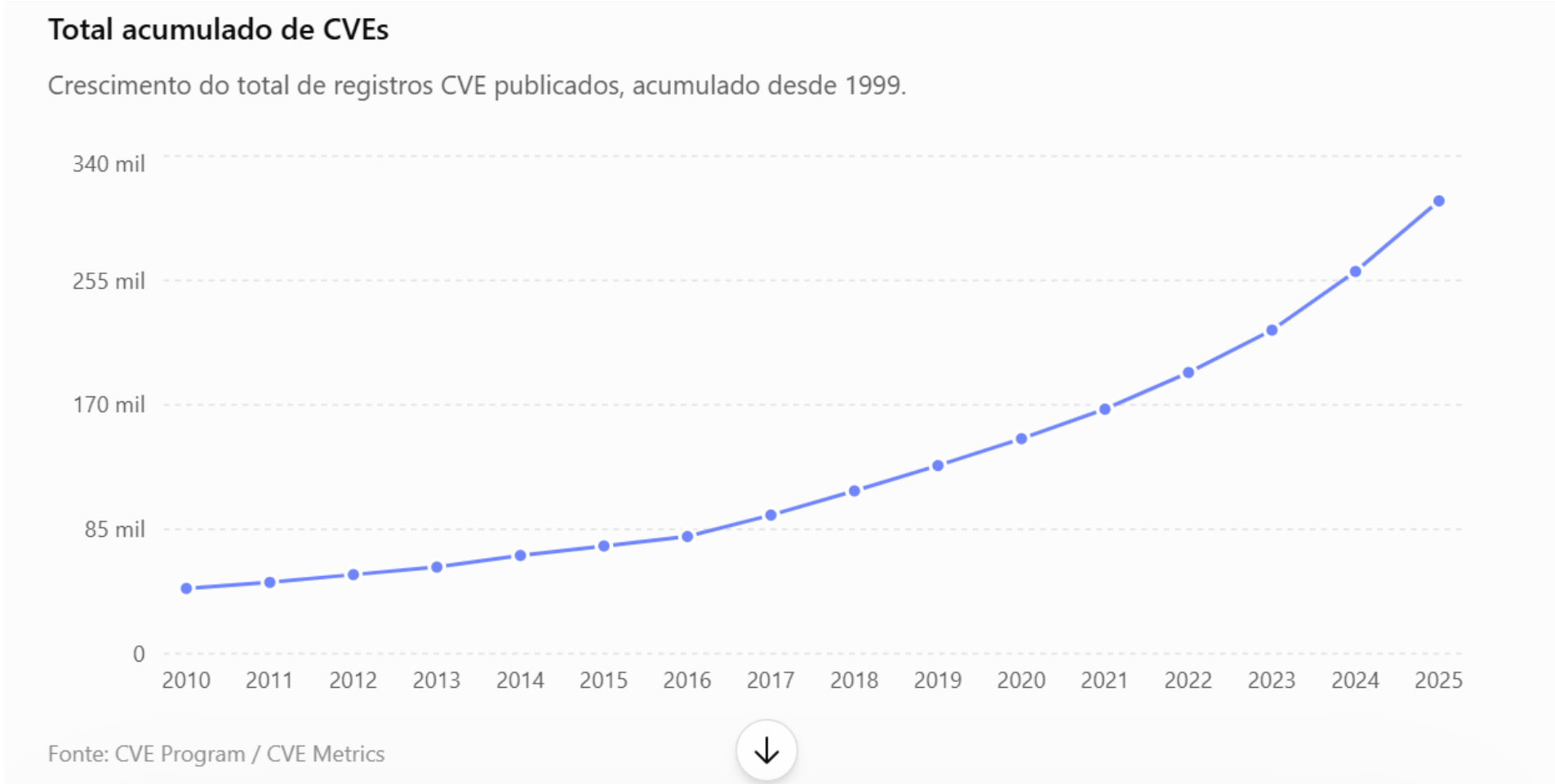
Situação atual

- Explosão de CVE



Situação atual

- Explosão de CVE



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 maiscula 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

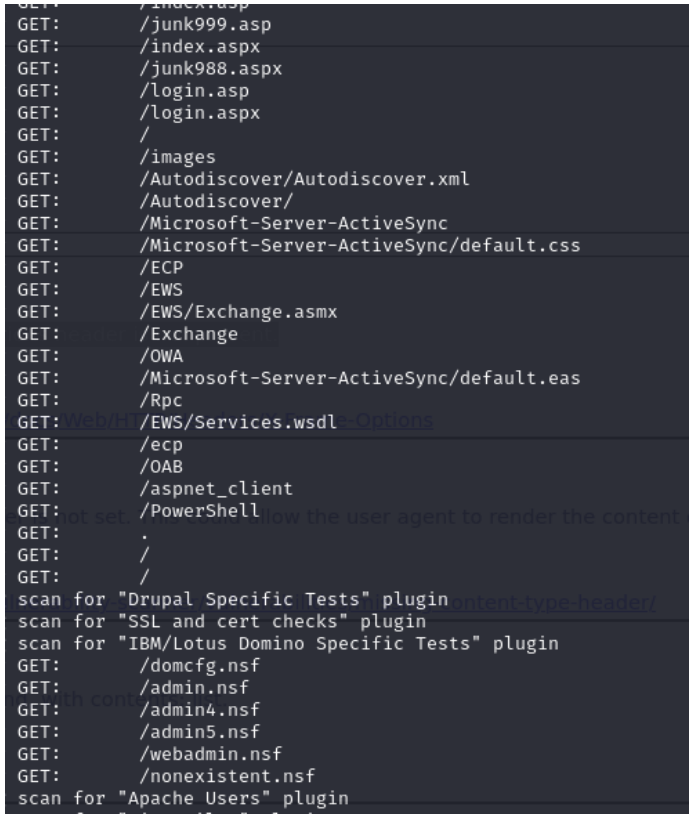
- Report do nikto...

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



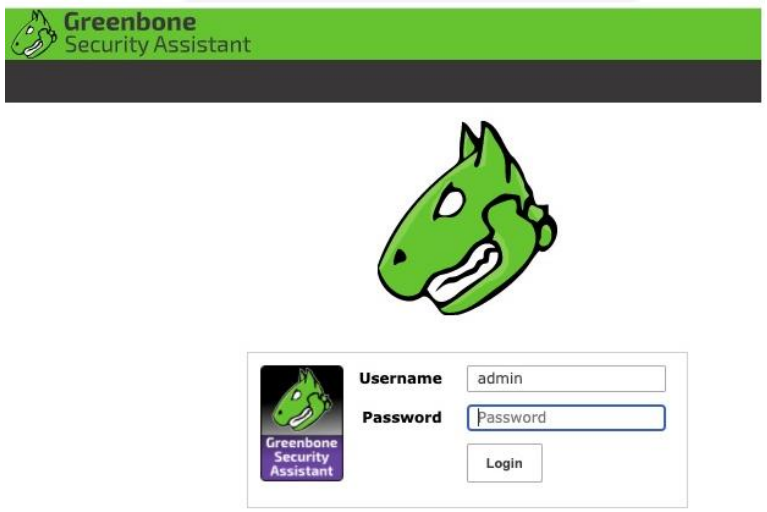
Nikto

- 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.



OpenVAS

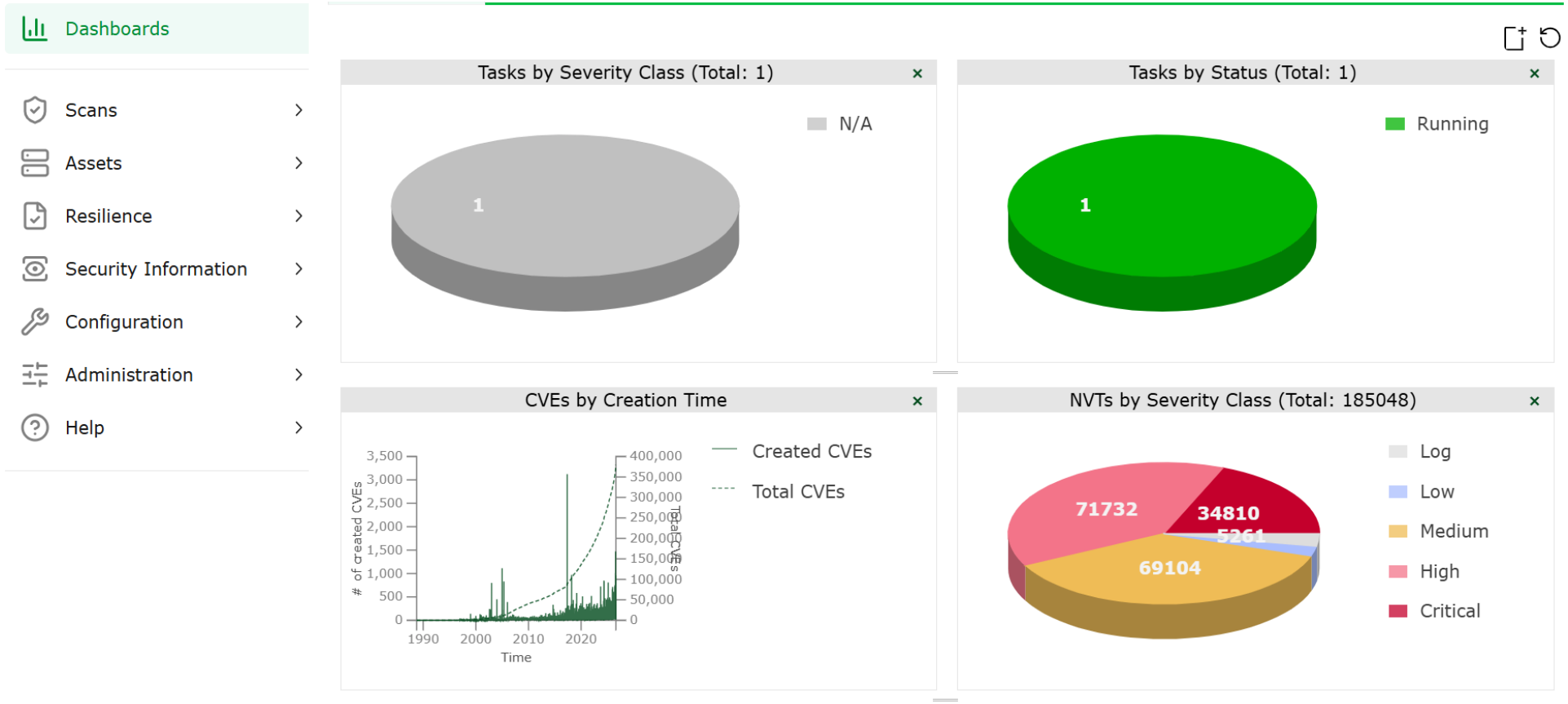
- Os feeds NVTs
  - NVTs (Network Vulnerability Tests): São os scripts (manuais de instruções) que o OpenVAS usa para testar cada falha específica.
  - Temos em torno de 160.00 NVTs
  - Atualizado diariamente (atualizar o seu OpenVas antes de utiliza-lo)
  - São feitos na sua própria linguagem NASL
  - 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.

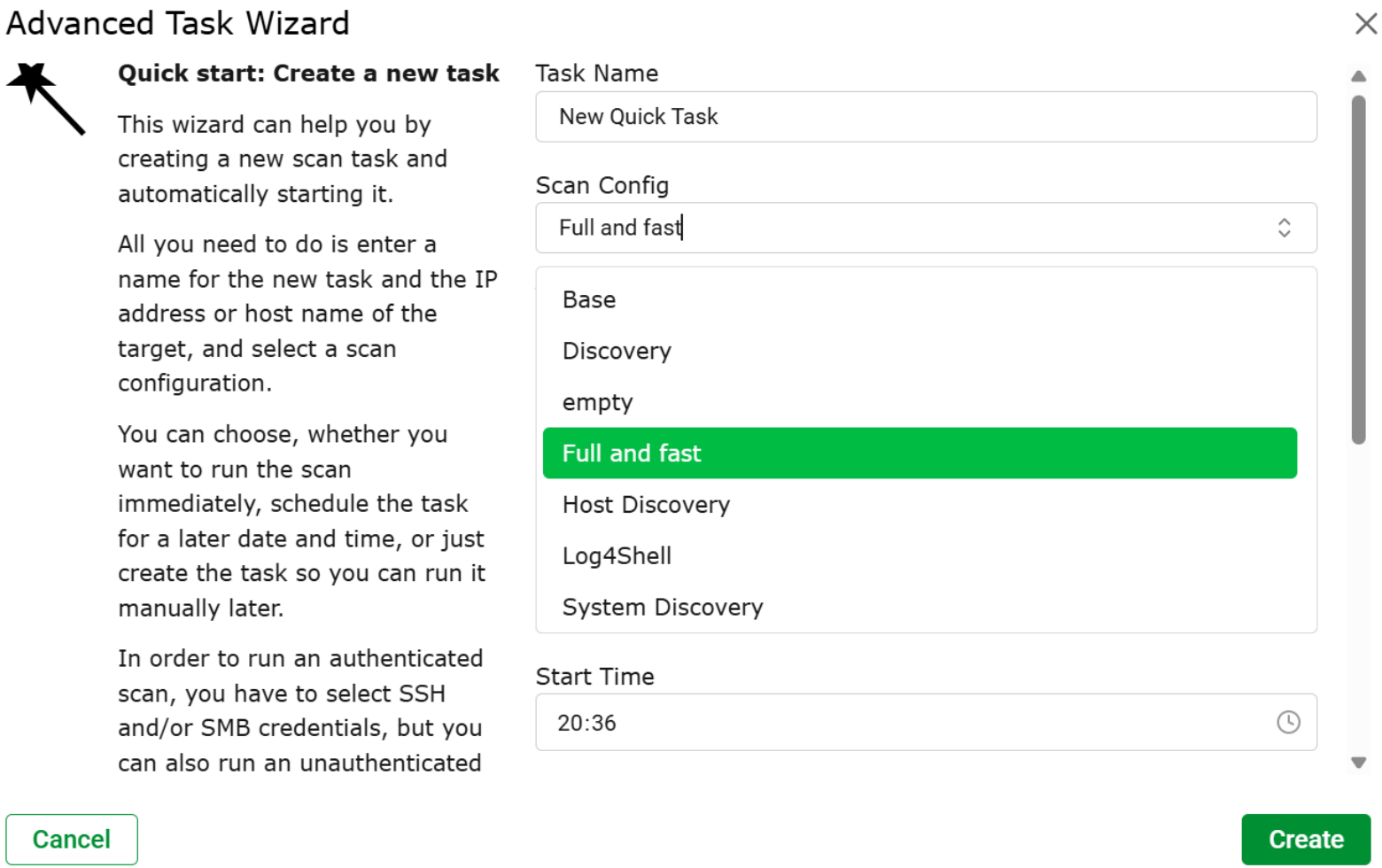
OpenVAS

- Bashboard



OpenVAS

- Opções simples



OpenVAS

- O "problema" dos 98, 99%

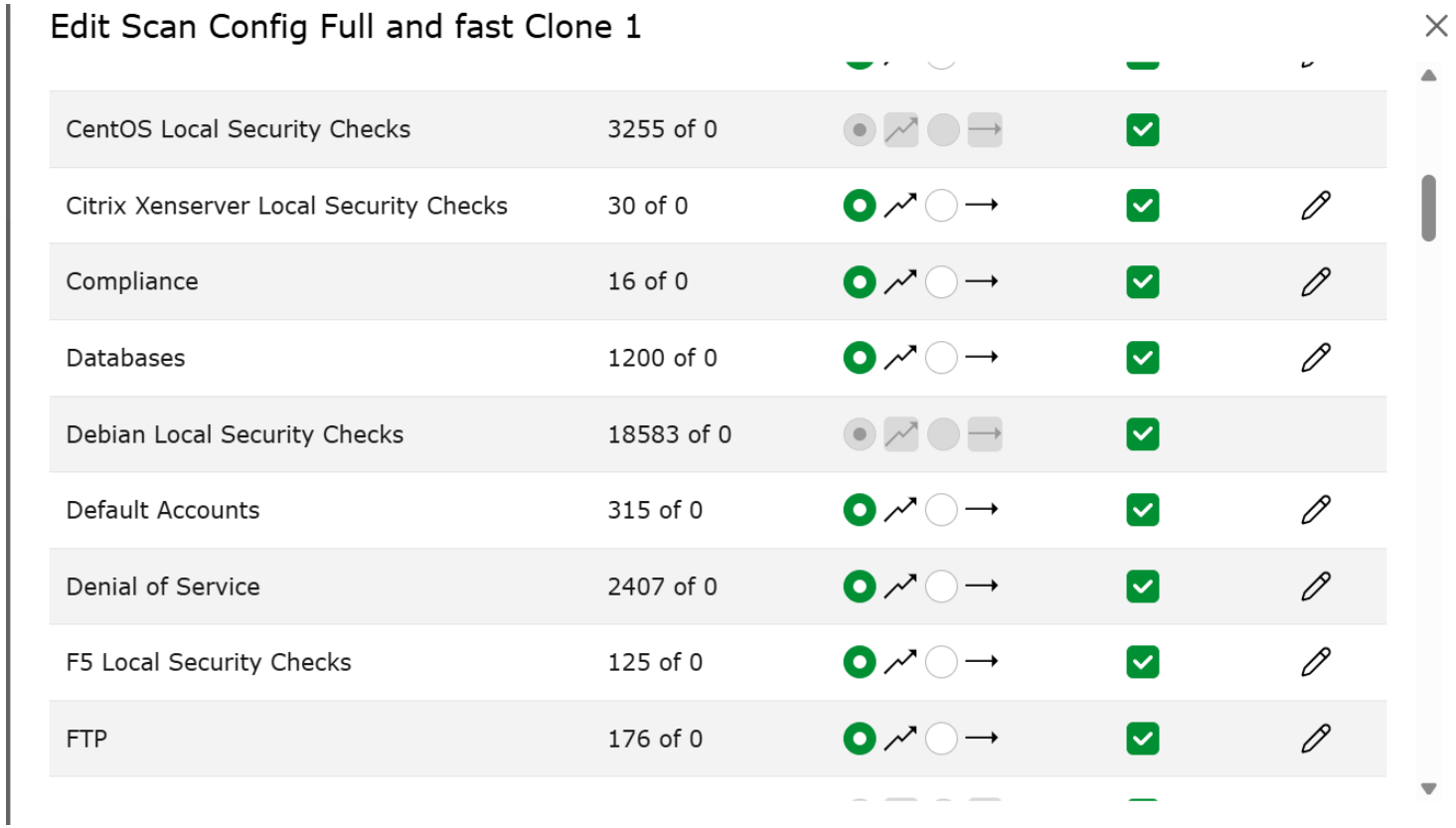
Name	Type	Status	Reports
Scan Autenticado		Done	1
Scan full		98 %	1
Scan não autenticado		Done	1

Edit Scan Config Full and fast Clone 1

non_simult_ports	139, 445, 3389,	139, 445, 3389, Servic
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



Dúvidas?