Referência Rápida de nmap

Varredura de portas, descoberta de hosts, detecção de serviços e scripts NSE

Varreduras Básicas

Alvos de Varredura

```
nmap 192.168.1.1              # single host
nmap 192.168.1.0/24           # entire subnet
nmap 192.168.1.1-50           # IP range
nmap -iL targets.txt          # hosts from file
```

Especificação de Alvos

192.168.1.1	Endereço IP único
192.168.1.0/24	Notação CIDR (256 hosts)
192.168.1.1-254	Intervalo de IPs
example.com	Hostname (resolvido para IP)
-iL file.txt	Ler alvos de arquivo
--exclude 192.168.1.1	Excluir hosts específicos
--excludefile skip.txt	Excluir hosts de arquivo

Varredura de Portas

Tipos de Varredura

-sS	Varredura TCP SYN (padrão, discreta, requer root)
-sT	Varredura TCP connect (handshake completo, sem root)
-sU	Varredura UDP (lenta, frequentemente filtrada)
-sA	Varredura TCP ACK (detectar firewalls)
-sN	Varredura TCP NULL (sem flags)
-sF	Varredura TCP FIN (apenas flag FIN)
-sX	Varredura Xmas (flags FIN+PSH+URG)

Seleção de Portas

```
nmap -p 80,443 target         # specific ports
nmap -p 1-1000 target         # port range
nmap -p- target               # all 65535 ports
nmap --top-ports 100 target   # most common 100 ports
```

Estados de Porta

open	Aplicação aceitando conexões
closed	Porta acessível mas sem serviço ativo
filtered	Firewall bloqueando, estado indeterminado
unfiltered	Porta acessível, estado desconhecido
open|filtered	Não é possível determinar se aberta ou filtrada

Descoberta de Hosts

Métodos de Descoberta

-sn	Apenas ping (sem varredura de portas)
-Pn	Pular descoberta de host (tratar todos como ativos)
-PS 80,443	Descoberta TCP SYN em portas
-PA 80	Descoberta TCP ACK
-PU 53	Descoberta UDP
-PE	Requisição echo ICMP
-PR	Descoberta ARP (rede local)

Varredura de Rede

```
nmap -sn 192.168.1.0/24       # ping sweep subnet
nmap -sn -n 10.0.0.0/24       # sweep, skip DNS
nmap -sn -PR 192.168.1.0/24   # ARP scan (fastest)
```

Detecção de Serviços

Detecção de Versão

```
nmap -sV target               # detect service versions
nmap -sV --version-intensity 5 target  # deeper probing
nmap -sV --version-all target  # try every probe (slow)
nmap -A target                 # OS + version + scripts + traceroute
```

Flags de Serviço

-sV	Verificar portas abertas para serviço/versão
--version-intensity 0-9	Intensidade de sondagem (padrão 7)
--version-light	Sondagem leve (intensidade 2)
--version-all	Tentar todas as sondas (intensidade 9)
-A	Agressivo: -sV -O --script=default -traceroute
-sC	Executar scripts NSE padrão

Detecção de Sistema Operacional

Fingerprinting de SO

```
nmap -O target                # OS detection (needs root)
nmap -O --osscan-limit target # only scan promising hosts
nmap -O --osscan-guess target # aggressive OS guessing
nmap -A target                # includes OS detection
```

Flags de Detecção de SO

-O	Habilitar detecção de SO
--osscan-limit	Ignorar hosts sem portas TCP abertas+fechadas
--osscan-guess	Estimar SO com mais agressividade
--max-os-tries N	Máximo de tentativas de detecção de SO por host

Scripts (NSE)

Uso de Scripts

```
nmap --script=default target   # default category
nmap --script=vuln target      # vulnerability scripts
nmap --script=http-headers target
nmap --script="http-*" target  # wildcard match
```

Categorias de Scripts

default	Scripts seguros e úteis (atalho -sC)
vuln	Verificar vulnerabilidades conhecidas
safe	Scripts não intrusivos
intrusive	Podem travar alvos ou acionar IDS
discovery	Descoberta de rede e serviços
auth	Verificações relacionadas a autenticação
brute	Teste de credenciais por força bruta
exploit	Tentativas de exploração ativa

Scripts Úteis

http-title	Capturar títulos de páginas web
ssl-cert	Exibir detalhes do certificado SSL
ssh-hostkey	Exibir fingerprints de chaves do host SSH
dns-brute	Enumerar subdomínios DNS
smb-os-discovery	Detectar SO Windows via SMB
vuln	Executar todas as verificações de vulnerabilidade

Formatos de Saída

Opções de Saída

```
nmap -oN scan.txt target      # normal text output
nmap -oX scan.xml target      # XML output
nmap -oG scan.gnmap target    # grepable output
nmap -oA scan_all target      # all formats at once
```

Flags de Saída

-oN file	Saída normal para arquivo
-oX file	Saída XML (para ferramentas/parsing)
-oG file	Saída grepável (um host por linha)
-oA basename	Todos os três formatos (basename.nmap/xml/gnmap)
-v	Aumentar verbosidade (-vv para mais)
-d	Saída de debug (-dd para mais)
--open	Mostrar apenas portas abertas
--reason	Mostrar motivo do estado da porta

Tempo e Desempenho

Templates de Temporização

-T0 (paranoid)	Muito lento, evasão de IDS (5 min entre sondas)
-T1 (sneaky)	Lento, evasão de IDS (15 seg entre sondas)
-T2 (polite)	Velocidade reduzida, menos largura de banda
-T3 (normal)	Temporização padrão
-T4 (aggressive)	Rápido, assume rede confiável
-T5 (insane)	Mais rápido, pode perder resultados

Ajuste Fino

--min-rate 1000	Enviar no mínimo 1000 pacotes/seg
--max-rate 500	Limitar a 500 pacotes/seg
--max-retries 2	Máximo de retransmissões de sondas
--host-timeout 30m	Pular host se varredura exceder 30 min
--scan-delay 1s	Atraso entre sondas
--min-parallelism 10	Mínimo de grupos de sondas paralelas

Evasão de Firewall

Técnicas de Evasão

-f	Fragmentar pacotes (blocos de 8 bytes)
-D RND:5	Varredura com decoys (5 IPs aleatórios)
-S spoof_ip	Falsificar IP de origem (requer pacotes brutos)
-e eth0	Usar interface de rede específica
--source-port 53	Usar porta de origem específica (ex.: DNS)
--data-length 25	Anexar dados aleatórios aos pacotes
--spoof-mac 0	Randomizar endereço MAC

Exemplos de Evasão

```
nmap -f -D RND:3 target       # fragments + decoys
nmap --source-port 53 target  # DNS port (often allowed)
nmap -T1 --scan-delay 5s target  # slow to evade IDS
```

Padrões Comuns

Reconhecimento Rápido

```
nmap -T4 -F target            # fast common ports
nmap -T4 -A -v target         # OS + service detection
nmap -sV --top-ports 1000 target  # top 1000 + versions
```

Varredura Abrangente

```
# Full TCP + service + OS + scripts
nmap -sS -sV -O -sC -p- -T4 -oA full target
# UDP scan on common ports
nmap -sU --top-ports 50 target
```

Auditoria de Servidor Web

```
nmap -p 80,443 --script=http-title,http-headers,\
ssl-cert,http-methods target
# Check for open proxies and vulns
nmap -p 80,443,8080 --script=http-open-proxy,vuln target
```

Inventário de Rede

```
# Discover all live hosts with OS info
nmap -sn 192.168.1.0/24 -oG - | grep "Up"
# Service inventory for subnet
nmap -sV -T4 192.168.1.0/24 -oX inventory.xml
```