🔍

NMAP

Created	@September 6, 2025 3:11 PM
Tags	

O que é?

O NMAP é uma ferramenta usada para realizar o mapeamento da rede. Pode ser usada para listar hosts e portas abertas na rede.

Opções úteis

- `nmap -sS <host>` → Syn Scan;
- `nmap -sU <host>` → UDP Scan;
- `nmap -O <host>` → Descobrir o sistema operacional;
- `nmap -sV <host>` → Descobrir a versão dos serviços;
- `nmap -v` → Aumentar a verbosidade do output (quantos mais “v”, maior a verbosidade. Exemplo: `nmap -vv`);
- `nmap -oA` → Salvar o output nos 3 principais formatos;
- `nmap -oN` → Salvar o output no formato normal;
- `nmap -oG` → Salvar o output no formato em que seja possível usar o grep;
- `nmap -A` → Ativar o modo “agressivo”. Esse modo ativa serviços de detecção, detecção de sistemas operacionais...
- `nmap -T<1-5>` → Usado para acelerar as operações de escaneamento;
- `nmap -p <num>` → Especifica que o scan deve ser feito na porta *num;*

- `nmap -p <num1>-<num2>` → Especifica que o scan deve ser feito da porta *num1* a *num2;*
- `nmap -p-` → Especifica que o scan deve ser feito em todas as portas;
- `nmap --script=<script_name>` → Ativar um script da biblioteca do NMAP;

Mapeamento de portas

▼ TCP Connect Scans (`-sT`)

Tenta fazer um three-way handshake (conexão TCP) com cada porta. O NMAP envia um pacote TCP com a flag SYN setada para o host na porta especificada. Se o host responder com um pacote TCP com as flags SYN e ACK setadas, a porta está aberta e o NMAP envia um pacote TCP com a flag ACK setada. Se o host responder com um pacote TCP com a flag RST setada, a porta está fechada. Se o host não responder, a porta está protegida por um firewall (filtered).

▼ SYN Scans (`-sS`)

Também tenta fazer um three-way handshake com cada porta do host. Porém, quando o host responde com um pacote TCP com as flags SYN e ACK setadas, o NMAP responde com um pacote TCP com a flag RST setada, evitando que o host tente realizar conexões. É usado por padrão quando o NMAP é executado por privilégios de administrador.

- Vantagens:
  - Pode ser usado para dar bypass em sistemas de detecção antigos, os quais esperam um three-way handshake completo;
  - Normalmente, não são gravados nos logs de aplicações ouvindo nas portas, já que o padrão é apenas gravar tentativas de conexões completas;
  - São um pouco mais rápidos que os scans de conexões TCP.
- Desvantagens:
  - Precisa de permissões de administrador para funcionar corretamente;

- Pode derrubar serviços instáveis.

▼ UDP Scans (`-sU`)

Envia um pacote UDP para o host de destino. Se recebermos um pacote UDP em resposta ao pacote enviado, a porta é marcada como `open`. Se não recebermos uma resposta, a porta é marcado como `open|filtered` , já que não tem como saber se ela está protegida por um firewall. Se recebermos um pacote ICMP indicando que a não é possível alcançar a porta, a porta é marcada como `closed`. Como as conexões UDP não possuem estado, é bem mais complicado determinar se uma porta está aberta ou não. Quando não recebemos uma resposta, o NMAP envia um segundo pacote para tentar verificar novamente se a porta está aberta. Por causa disso, os scans UDP demoram bem mais que os scans baseados em conexões TCP. Dessa forma, é uma boa prática realizar UDP scans com a opção `--top-ports <number>` , a qual só realiza o mapeamentos das `<number>` portas UDP mais comuns.

▼ NULL Scans (`-sN`)

Envia um pacote TCP ao host com nenhuma flag setada. Se a porta estiver fechada, o host responderá com um pacote TCP com a flag RST setada. Se não obtivermos reposta, a porta é classificada como `open|filtered`. Se recebermos um pacote ICMP indicando que não é possível alcançar a porta, a porta é classificada como `filtered`. É mais furtivo que o SYN scans.

▼ FIN Scans (`-sF`)

Envia um pacote TCP ao host com apenas a flag FIN setada, a qual é usada para encerrar uma conexão TCP. Se a porta estiver fechada, o host responderá com um pacote TCP com a flag RST setada. Se não obtivermos reposta, a porta é classificada como `open|filtered`. Se recebermos um pacote ICMP indicando que não é possível alcançar a porta, a porta é classificada como `filtered`. É mais furtivo que o SYN scans.

▼ XMAS Scans (`-sX`)

Envia uma pacote TCP mal formatado ao host. Se a porta estiver fechada, o host responderá com um pacote TCP com a flag RST setada. Se não obtivermos reposta, a porta é classificada como `open|filtered`. Se recebermos um

pacote ICMP indicando que não é possível alcançar a porta, a porta é classificada como `filtered`. É mais furtivo que o SYN scans.

Mapeamento de Rede

Em um primeiro momento, precisamos descobrir quais hosts estão ativos na rede. Para isso, podemos usar o NMAP para realizar um “ping sweep”, o qual consiste em enviar um pacote ICMP para cada endereço IP possível em uma rede. Se obtivermos resposta, marcamos o IP como ativo. Para realizar um ping sweep usamos o comando:

```
nmap -sn <ip_range>
```

onde o `<ip_range>` pode ser especificado de duas formas: por uma sub rede (192.168.0.0/16) ou com a notação CIDR (192.168.0.1-254). Além da requisição ICMP, o comando `-sn` também envia um pacote TCP com a flag SYN setada para a porta 443 e um pacote TCP com a flag ACK setada para a porta 80.

NSE

O NSE (NMAP Scripting Engine) é uma extensão muito poderosa do NMAP. Ela nos permite executar scripts desenvolvidos na linguagem de programação Lua que podem realizar desde scans de vulnerabilidades até a automação da exploração de vulnerabilidades. As principais categorias de scripts são:

- `safe`: não afeta o alvo;
- `intrusive`: não seguro: provavelmente afetará o alvo;
- `vuln`: escaneamento de vulnerabilidades;
- `exploit`: tenta explorar uma vulnerabilidade;
- `auth`: tenta ignorar autenticações para serviços em execução;
- `brute`: executa um bruteforce nas credenciais de serviços em execução;

- `discovery`: tenta consultar serviços em execução para adquirir mais informações sobre a rede.

Para executar um script específico, executa-se o comando:

```
nmap --script=<script-name>
```

Alguns scripts precisam de argumentos, os quais são fornecidos da seguinte maneira:

```
nmap --script=<script-name> --script-args <script-name>.<argument1>, <sc
ript-name>.<argument2>
```

O comando abaixo pode ser usado para fornecer mais informações sobre um determinado script.

```
nmap --script-help <script-name>
```

Para encontrar scripts, podemos usar o site oficial do NMAP listado nas referências ou procurar os scripts localmente. No Linux, o NMAP armazena os scripts instaladas no diretório `/usr/share/nmap/scripts`. Podemos procurar por scripts instaladas usando o `grep` e o arquivo “scripts.db”, o qual é usado pelo NMAP para gerenciar os scripts instalados. Segue abaixo um exemplo de consulta para scripts da categoria `safe` .

```
grep "safe" /usr/share/nmap/scripts/script.db
```

Caso não encontrarmos localmente um script listado na documentação inicial, podemos tentar atualizar o NMAP, forçando-o a instalar o script que está faltando.

```
sudo apt update && sudo apt install nmap
```

Evasão de Firewall

Muitas vezes, os firewall bloqueiam requisição ICMP por padrão. Por padrão, o NMAP realiza um `ping` ao host antes de escaneá-lo e, caso o host não responda, ele marca o host para inativo, porém o firewall pode ter bloqueado o pacote. Para contornar esses casos, podemos usar a opção `-Pn`, indicando ao NMAP que precisa realizar o `ping` antes de escanear o host. Dessa maneira, o NMAP sempre considerará os hosts como ativos, entretanto isso aumenta consideravelmente o tempo do mapeamento. Além da opção `-Pn`, pode-se utilizar outras opções para evitar firewalls:

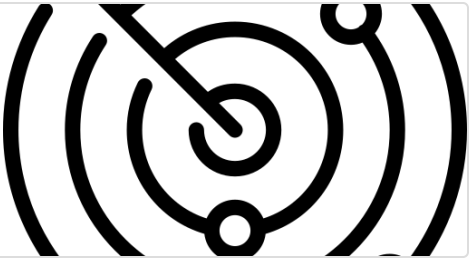
- `-f`: fragmenta os pacotes, fazendo com que a chance de detecção por um firewall ou IDS seja menor;
- `--scan-delay <time>ms`: usado para adicionar um delay no envio dos pacotes. Muito útil em redes instáveis e para burlar qualquer trigger baseado em tempo de firewalls e IDS;
- `--bad-sum`: usado para gerar checksum inválidos nos pacotes. Usado para detectar um firewall/IDS.

Referências

Nmap

An in depth look at scanning with Nmap, a powerful network scanning tool.

https://tryhackme.com/room/furthernmap



NSEDoc Reference Portal — Nmap Scripting Engine documentation

Documentation, options, and usage for NSE scripts using the Nmap Scripting Engine. Script-args, scan ideas, and source code for Nmap scripts, libraries, and NSE categories.

https://nmap.org/nsedoc/