NMAP (Newtwork MAPer)

nmap

Um dos primeiros passos de um ataque é verificar quais serviços o alvo oferece a rede.

Essa ação é conhecida como port scaning.

nmap

Cada serviço está relacionado a uma porta, que é um número inteiro compreendido entre 0 a 65535 no IPv4.

As portas baixas, até o 1024, só podem ser abertas pelo root ou administrador, as demais podem ser abertas pelo usuário comum.

nmap

Para que saber a porta de determinado serviço pode-se acessar o arquivo /etc/services no Linux.

Um dos port-scan mais conhecidos é o nmap, desenvolvido por Fyodor, que pode ser encontrado em:

http://www.nmap.org

nmap

A sintaxe mais básica do nmap é:

$ nmap localhost

nmap

As saídas do nmap são classificados da seguinte forma:

Open: Há uma aplicação aceitando conexões TCP, UPD etc.

Closed: A porta é acessível mas não há serviço rodando.

Filtred: Não consegue determinar se está aberta, pois há um filtro de pacotes (firewall).

Unfiltred: É acessível, mas não pode identificar se está aberta ou fechada.

Open | Filtred: Não consegue determinar se está aberta ou filtrada. Não há resposta da porta.

Closed | Filtred: Não consegue determinar se está aberta ou filtrada.

nmap

As opções de cada tipo de varredura do nmap são:

-sP : envia um pacote ICMP Ping Scan, que é usado para encontrar um host na rede.

-sU : determina quais portas UDP estão ativas.

-sS : além de mandar o pacote e esperar uma confirmação, no meio da conexão interrompe, assim consegue burlar algumas sistemas de proteção; procura por portas do tipo TCP.

nmap

-sL (list scan): É a forma mais básica, onde o Nmap só lista os Hosts de uma rede, sem mandar nenhum pacote até eles. Também faz resolução de DNS reverso para descobrir seus nomes.

-sP (ping scan): Realiza um Ping no Host alvo, para descobrir se ele está ou não ativo. Caso o pacote seja rejeitado, envia um TCP ACK na porta 80, e se ainda houver rejeição, envia um pacote TCP SYN. Esta técnica é utilizada quando há um Firewall antes de alvo, que pode estar bloqueando os pacotes ECHO REQUEST.

nmap

-P0 (zero ping): Desabilita o Ping antes de fazer qualquer varredura. Utilizado contra Firewalls que rejeitem o ECHO REQUEST.

-PS [portas] (syn scan): Envia pacotes SYN na porta 80 para verificar se o Host está ativo, pode-se especificar portas diferentes.

-PA [portas] (ack scan): Mesmo que o de cima, porém envia pacotes ACK.

nmap

-PR [portas (arp scan): Realiza o scan pela tabela ARP, há ganho de performance.

-n : Não faz resolução de nomes DNS.

-sV (version scan): O principal scan para enumeração de serviços. O scan de versão retorna a porta, seu estado, serviço e versão.

nmap

-O (operational scan): Realiza o scan para descobrir qual sistema operacional o sistema está rodando. O retorno se baseia em porcentagens de acerto.

-A (advanced scan): Retorna resultados avançados, como o banner do sistema operacional e alguns dados fornecidos por scripts, como detalhes do serviço Samba.

-sT : scan via TCP connect() - é o tipo mais básico de scaneamento; semelhante a opção -sS, com mais garantia de sucesso, utiliza a chamada connect().

nmap

Exemplo:

```
# nmap -sT 192.168.1.1

Starting Nmap 6.00 ( http://nmap.org ) at 2014-12-07 08:22 AMST

Nmap scan report for B (192.168.43.244)

Host is up (0.0080s latency).

Not shown: 995 closed ports

PORT    STATE SERVICE

22/tcp  open  ssh

53/tcp  open  domain

111/tcp open  rpcbind

139/tcp open  netbios-ssn

445/tcp open  microsoft-ds

MAC Address: 08:00:27:F2:DD:46 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
```

nmap

Exemplo:

```
# nmap -sT 192.168.1.1

Starting Nmap 7.60 ( https://nmap.org ) at 2019-04-29 03:35 -04

Nmap scan report for hk (192.168.15.39)

Host is up (0.00013s latency).

All 1000 scanned ports on hk (192.168.15.39) are closed

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

nmap

$ nmap -O 192.168.1.1

Starting Nmap 7.60 (https://nmap.org) at 2019-04-29 03:39 -04

Nmap scan report for hk (192.168.15.39)

Host is up (0.000046s latency).

All 1000 scanned ports on hk (192.168.15.39) are closed

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running: Linux 2.6.X|3.X

OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3.13

OS details: Linux 2.6.14 - 2.6.34, Linux 2.6.17, Linux 2.6.17 (Mandriva), Linux 3.13

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 4.64 seconds

nmap

Exercícios

Experimente as outras opções do nmap citadas na aula e verifique a saída de casa comando.

Importante notar que saída será dada e qual a informação que se pode tirar de cada saída.

Assista a vídeo-aula no site e faça suas perguntas caso ache necessário.