



Port Scan



Todo serviço que roda uma máquina está relacionando a uma porta, que é um numero inteiro compreendido entre 0 a 65000.

As portas menores que 1024 só podem ser utilizadas pelo root.

Como o *Port Scan* podemos fazer uma varredura dos serviços que estão rodando numa máquina e conseqüentemente saber quais portas estão abertas.

Tipos de *Port Scanning*



Os *scans* diferenciam-se pela método que usam para varrer as portas.

O TCP usa as flags para saber quais portas estão abertas ou fechadas.

O UDP usa o ICMP Port Unreachable, já que o mesmo não utiliza o conceito de flags.

SYN scan



Baseia-se no envio de um pacote com a flag SYN ativa ao servidor, se a porta estiver aberta o servidor responderá com um pacote com as flags SYN e ACK ativas e o atacante responderá com um pacote com as flags RST e ACK ativas fazendo com que a conexão seja cancelada.

Caso o servidor envie um pacote com a flag RST ativa indica que a porta está fechada ou que não há serviço escutando nela.

ACK scan



O atacante envia um pacote com a flag ACK ao servidor alvo. Se o pacote de respostas do servidor tiver com ttl menor ou igual 64 ou se o campo window for maior que zero a porta estará aberta.

UDP scan



Neste método são enviados pacotes UDP de 0 bytes para cada porta alvo. Caso seja recebida a mensagem *ICMP Port Unreachable* que indica que a porta está fechada. Caso contrário, imprime a mensagem alegando a porta como em estado de aberta.



Nmap



É um software livre que realiza port scan desenvolvido pelo hacker Fyodor. É muito utilizado para avaliar a segurança dos computadores, e para descobrir serviços ou servidores em uma rede de computadores.

Conhecido por sua rapidez e pelas opções que dispõe.

Principais Opções do Nmap



- iL : faz uma verificação do host/rede (s) a partir de um arquivo.
- p : especifica quais portas deveram ser rastreadas.
- F : rastreia por portas que encontram-se descritas no /etc/services.
- D : utiliza vários IPs falsificados durante a varredura.

Principais Opções do Nmap



- sS : rastreia usando a técnica SYN scan
- sA : rastreia usando a técnica ACK scan
- sU : rastreia usando a técnica UDP scan
- s0 : rastreia quais protocolos IPs são suportados pela máquina-alvo.
- sP : envia pacote ICMP *echo request* para verificar se o host está ativo.
- sV : depois de verificar as portas TCP e/ou UDP, determinará qual o serviço está rodando.



Exemplos

Com SYN scan



```
Terminal
File Edit View Terminal Tabs Help
Wed May 28 21:33:58
root@jiraya ~
# nmap -sS localhost

Starting Nmap 4.53 ( http://insecure.org ) at 2008-05-28 21:34 BRT
Interesting ports on localhost (127.0.0.1):
Not shown: 1711 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
631/tcp   open  ipp
5900/tcp   open  vnc

Nmap done: 1 IP address (1 host up) scanned in 0.154 seconds
Wed May 28 21:34:00
root@jiraya ~
#
```

Com UDP scan



```
Terminal
File Edit View Terminal Tabs Help
Wed May 28 21:53:04
root@jiraya ~
# nmap -sU -vv 192.168.1.6

Starting Nmap 4.53 ( http://insecure.org ) at 2008-05-28 21:53 BRT
Initiating Parallel DNS resolution of 1 host. at 21:53
Completed Parallel DNS resolution of 1 host. at 21:53, 9.14s elapsed
Initiating UDP Scan at 21:53
Scanning 192.168.1.6 [1488 ports]
Completed UDP Scan at 21:53, 1.24s elapsed (1488 total ports)
Host 192.168.1.6 appears to be up ... good.
Interesting ports on 192.168.1.6:
Not shown: 1485 closed ports
PORT      STATE      SERVICE
137/udp   open|filtered netbios-ns
138/udp   open|filtered netbios-dgm
5353/udp  open|filtered zeroconf

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 10.472 seconds
           Raw packets sent: 1491 (41.748KB) | Rcvd: 2976 (124.908KB)
Wed May 28 21:53:34
root@jiraya ~
#
```

Com Protocolo IP scan



```
File Edit View Terminal Tabs Help
TAMBAIR TAMBAIR LEIA PADME SALU ROSSI
Thu May 29 09:55:49
root@tambair ~
# nmap -s0 localhost

Starting Nmap 4.53 ( http://insecure.org ) at 2008-05-29 09:55 BRT
sendto in send_ip_packet: sendto(4, packet, 40, 0, 127.0.0.1, 16) => Operation not permitted
Offending packet: TCP 127.0.0.1:56155 > 127.0.0.1:56155 A ttl=44 id=32516 iplen=40 seq=274008
3587 win=1024 ack=1227599889
sendto in send_ip_packet: sendto(4, packet, 40, 0, 127.0.0.1, 16) => Operation not permitted
Offending packet: TCP 127.0.0.1:56156 > 127.0.0.1:56155 A ttl=56 id=40470 iplen=40 seq=263413
7701 win=1024 ack=625243730
Interesting protocols on localhost (127.0.0.1):
Not shown: 250 closed protocols
PROTOCOL STATE SERVICE
1 open icmp
2 open|filtered igmp
6 open|filtered tcp
17 open udp
136 open|filtered udplite
255 open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 2.376 seconds
Thu May 29 09:56:00
root@tambair ~
#
```

Com Version Detection



```
File Edit View Terminal Tabs Help
TAMBAIR TAMBAIR LEIA PADME SALU ROSSI cbo@tambair: ~
Thu May 29 12:08:12
root@tambair ~
# nmap -sV localhost

Starting Nmap 4.53 ( http://insecure.org ) at 2008-05-29 12:08 BRT
Interesting ports on localhost (127.0.0.1):
Not shown: 1706 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
25/tcp    open  smtp         Exim smtpd 4.69
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) mod_fastcgi/2.4.6 mod_perl/2.0.3 Perl/v5.8.8)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: CESAR)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: CESAR)
631/tcp   open  ipp          CUPS 1.2
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
8080/tcp  open  http         Apache httpd 2.2.8 ((Unix) mod_perl/2.0.3 Perl/v5.8.8)
Service Info: Host: tambair.cesar.org.br; OS: Linux

Host script results:
|_ Discover OS Version over NetBIOS and SMB: Unix

Service detection performed. Please report any incorrect results at http://insecure.org/nmap/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.537 seconds
Thu May 29 12:08:27
root@tambair ~
#
```



Dúvidas???



www.google.com