Reconnaissance and DOS Attacks with Nmap

Introduction

Nmap is the world's leading port scanner. Nmap can scan your perimeter network devices and servers from outside your firewall. Nmap gathers information necessary for a hack.

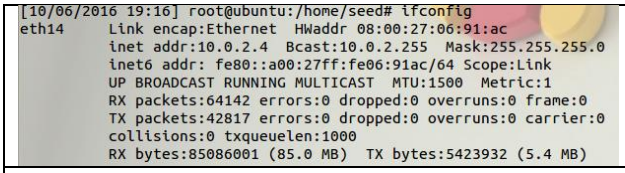
Warning: The risk with active scanning is that you will be detected and the security hardware or security admin will block any further attempts by you to communicate the site, or worse—report you to law enforcement. Nmap has multiple modes of scanning a potential target and many ways of evading detection. You only can use it in the lab setting.

Lab Environment

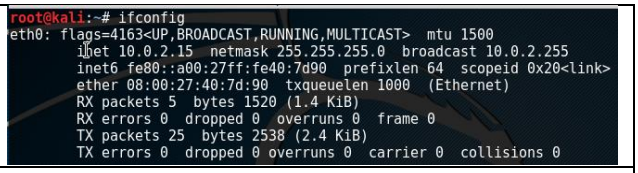
1. Install Kali Linux.
   1.1. Watch the installation tutorial at https://www.youtube.com/watch?v=GpTIM9OroIY
   1.2. Set the root account as:
      - Username: root
      - Password: dees
2. We have created two accounts in the Seed Ubuntu. The instructions for installing Seed Ubuntu virtual image is here http://www.cis.syr.edu/~wedu/seed/labs.html. The usernames and passwords are listed in the following:
   - User ID: root, Password: seedubuntu.
     - Note: Ubuntu does not allow root to login directly from the login window. You have to login as a normal user, and then use the command su to login to the root account.
   - User ID: seed, Password: dees

Task 1: Scan Victim's Machine Using a Default Setting

1. Open a terminal in both Seed Ubuntu and Kali Linux
   1.1. Assume the victim uses Seed Ubuntu
   1.2. Assume the attacker uses Kali Linux
2. Find IPs of both virtual images



Victim (Seed Ubuntu)



Attacker (Kali Linux)

3. In Attacker's Machine
   3.1. Same as nmap –sT, where scan (-s) using TCP (T)

```
root@kali:~# nmap 10.0.2.4

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-07 21:20 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00016s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
3128/tcp open  squid-http
8080/tcp open  http-proxy
MAC Address: 08:00:27:06:91:AC (Oracle VirtualBox virtual NIC)
```

4. If you need help information

```
root@kali:~# nmap -h
Nmap 7.25BETA1 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
```

Task 2: Open a Port in Victim's Machine and Show it in Attacker's Machine

1. In victim's machine, listen to port 1234

```
[10/07/2016 19:02] root@ubuntu:/home/seed# nc -l 1234
```

2. In Attacker's Machine

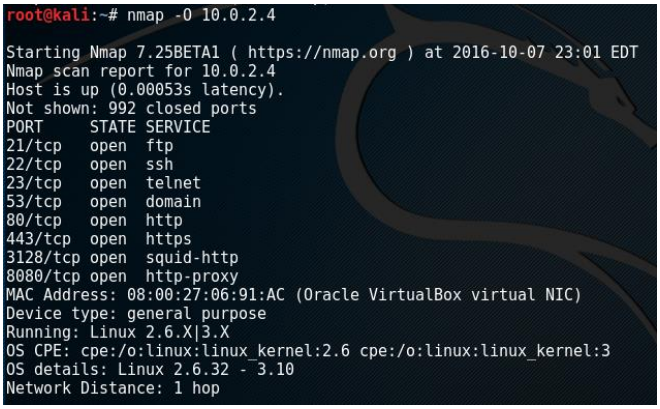
```
root@kali:~# nmap 10.0.2.4

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-10-07 22:02 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00021s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
1234/tcp open  hotline
3128/tcp open  squid-http
8080/tcp open  http-proxy
MAC Address: 08:00:27:06:91:AC (Oracle VirtualBox virtual NIC)
```

3. Go to the following website Listing of Port and Protocol, with known attacks
   http://web2.clarkson.edu/projects/itl/projects/honey/ports-attacks.txt

```
1234      tcp         search-agent            Infoseek Search Agent
1234      udp         search-agent            Infoseek Search Agent
1234      tcp         hotline                 HotLine
1234      tcp         SubSevenJavaclient      [trojan] SubSeven Java client
1234      tcp         UltorsTrojan            [trojan] Ultors Trojan
```

4. Question: Open a port number from the list and scan it to see if nmap can find the port

Task 3: Detect Operating System



Task 4: Stealth Scan Using -sS

The above scan by nmap is highly reliable, but its drawback is that it's also easily detectable. Nearly every system admin will know that you are scanning their network as it creates a full TCP connection, and this is logged with your IP address in the log files.

A more stealthy scan can be conducted using the -sS switch in nmap. This scan uses SYN flagged packets that do NOT create a connection on the target machine and therefore are not logged. This type of scan is slightly less reliable but is much more stealthy.

Task 5: Evading Intrusion Detection Systems Using -T2

The -T2 setting tells nmap to use the sneaky speed. This scan will likely take longer, but it is much more likely to go undetected by the IDS

Using -T2 setting for Nmap and write your observation.

Task 6: Denial of Service Using –T5

Nmap can also be an excellent denial of service (DOS) tool. If several individuals all send packets from nmap at a target simultaneously at high speed (nmap "insane" speed or -T5), they are likely to overwhelm the target, and it will be unable to process new website requests effectively, rendering it useless.

Launch the DOS attack to the victim’s machine, and write your observation.

How Does It Work?

Understanding Open, Closed and Filtered

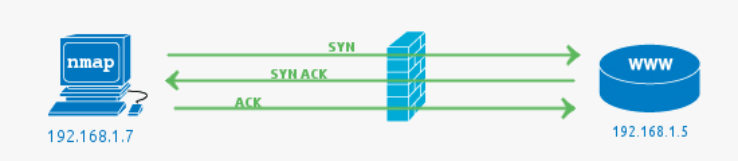
Nmap has a variety of scan types, understanding how the default and most common SYN scan works is a good place to start to examine how the scan works and interpreting the results.

The 3 way TCP handshake

First a bit of background, during communication with a TCP service, a single connection is established with the TCP 3 way handshake.

1. This involves a SYN sent to a TCP open port that has a service bound to it, typical examples are HTTP (port 80), SMTP (port 25), POP3 (port 110) or SSH (port 22)
2. The server side will see the SYN and respond with SYN ACK
3. The client answers an ACK.

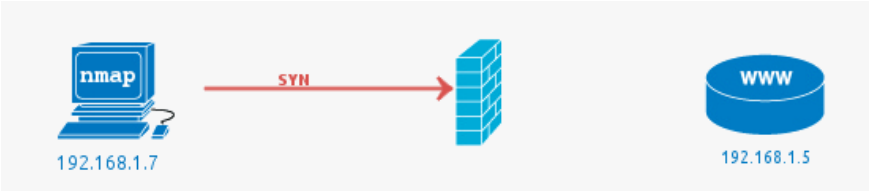
This completes the set up and the data of the service protocol can now be communicated.



In this example the firewall passes the traffic to the web server (HTTP -> 80) and the web server responds with the acknowledgement. In all these examples a firewall could be a separate hardware device, or it could be a local software firewall on the host computer.

Filtered ports or when the Firewall drops a packet

The job of a firewall is to protect a system from unwanted packets that could harm the system. In this simple example the port scan is conducted against port 81, there is no service running on this port using a firewall to block access to it is best practice.



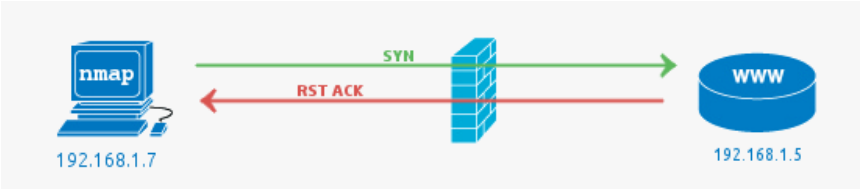
In the case of a filtered port result from Nmap it indicates that the port has not responded at all the SYN packet has simply been dropped by the firewall. See the following Wireshark packet capture, which shows the initial packet with no response.

Closed ports or when the Firewall fails

In this case the closed ports most commonly indicate that there is no service running on the port but the firewall has allowed the connection to go through to the server. It can also mean there is no firewall at all present.

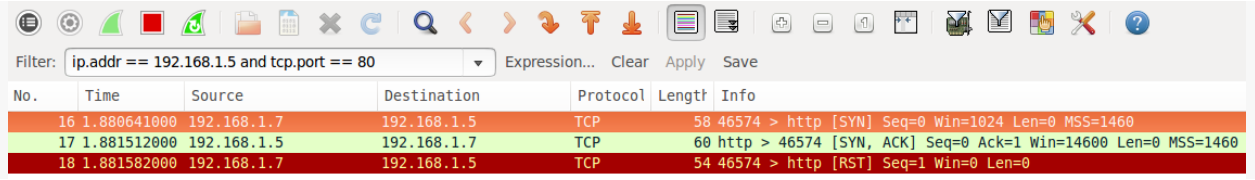
Note that while we are discussing the most common scenarios here it is possible to configure a firewall to reject packets rather than drop. This would mean packets hitting the firewall would be seen as closed (the firewall is responding with RST ACK).

Pictured below is a case where a firewall rule allows the packet on port 81 through even though there is no service listening on the port. This is most likely due to the fact that the firewall is poorly configured.



An Open Port (service) is found

Open Ports are usually what you are looking for when kicking off Nmap scans. The open service could be a publicly accessible service that is by its nature supposed to be accessible. It could also be a back-end service that does not need to be publicly accessible and therefore should be blocked by a firewall.



An interesting thing to notice in the wireshark capture is the RST packet sent after accepting the SYN ACK from the web server. The RST is sent by Nmap as the state of the port (open) has been determined by the SYN ACK if we were looking for further information such as the HTTP service version or to get the page, the RST would not be sent. A full connection would be established.

Reference:

- http://null-byte.wonderhowto.com/how-to/hack-like-pro-conduct-active-reconnaissance-and-dos-attacks-with-nmap-0146950/
- http://www.cis.syr.edu/~wedu/seed/labs.html
- https://hackertarget.com/nmap-tutorial/