Lab 12.1 Port Scanning
IN618 Security

May 17, 2016

Introduction

Nmap[1] is a tool for network discovery and auditing. It is basically a *port scanner* that gathers information by sending packets to various hosts and ports to determine what services are available on the network. For example, we can see if a web server is running on a particular host by sending packets to port 80 on that host and checking for a reply.

Tools like Nmap are useful for

- Network discovery and inventory;
- Security auditing;
- System monitoring;
- System management.

Of course, they are also useful for reconnaissance in preparation for an attack.

In this lab you will try out Nmap to get a sense of how the tool can be used for both good and bad purposes. Note that port scanning another party's hosts may be viewed as malicious activity, so use Nmap and similar tools responsibly.

For this lab, you will ssh into a system set up at 10.25.2.22. From this machine you will conduct scans on the network 192.168.2.0/24

1 Basic host discovery

In general we invoke Nmap in the following manner:

```
nmap [<scan type>] [<options>] <target specification>
```

So, suppose we want to catalog all of the hosts on a network with a simple ping sweep. The command for this is:

```
nmap -sn -e eth1 192.168.2.0/24
```

In this example our *scan type* is `-sn`, which is a simple ping sweep. We use the *option* `-e eth1` to indicate that we want to use the `eth1` network interface, and we have specified the network `192.168.2.2/24` as our target.

Run this scan on network and see what hosts you find.

[1] http://nmap.org

Not all hosts on your target network may respond to ping. An alternative is to perform a TCP SYN scan. This will send an empty TCP packet to the specified ports to see which answer back. This scan is performed as follows:

```
nmap -PS- -e eth1 192.168.2.0/24
```

The - after the PS specifies scanning all the low (<1024) ports.

2 Target specifications

Nmap provides a number of ways to specify targets. A single target can be specified by ip address or hostname:

```
nmap -sL www.foo.org.nz
```

```
nmap -sL 172.16.11.4
```

You can also specify a network using standard CIDR notation.

```
nmap -sL 10.20.0.0/16
```

You can also use this to specify the network or network segment containing a particular host.

```
nmap -sL www.foo.org.nz/24
```

You can also specify lists or ranges in particular octets of an address.

```
nmap -sL 192.168.2,3,17.100
```

```
nmap -sL 172.16.10-25.1-254
```

Note that the -sL option above will cause Nmap to print a list of hosts to be scanned but will not perform and scans. This is a good way to check you scan targets before you start firehosing your network with scans.

Specify two different ways to scan the 192.168.2.0 network using methods shown above.

3 A more intense scan

Once you have identified a host with a broad scan like the ping sweep above, you can try a more intense scan on a specific host. For example,

`nmap -A 192.168.2.102` to perform the most comprehensive scan on the target host.

If you just want to attempt OS fingerprinting, try

```
nmap -O 192.168.2.101
```

Or you can attempt to fingerprint services by running

```
nmap -sV 192.168.2.101
```

These scans will attempt to determine what operating system and precisely what server software is running on target hosts.

Try some of these scans on hosts running on your network. Note that some of these scans can be very time consuming.

Consult the online documentation to see some other scans you can run. Try a few of these scans on your hosts.

4 Port states

Nmap will identify ports as being in one of these six states[2]:

open An application is actively accepting TCP connections, UDP datagrams or SCTP associations on this port. Finding these is often the primary goal of port scanning. Security-minded people know that each open port is an avenue for attack. Attackers and pen-testers want to exploit the open ports, while administrators try to close or protect them with firewalls without thwarting legitimate users. Open ports are also interesting for non-security scans because they show services available for use on the network.

closed A closed port is accessible (it receives and responds to Nmap probe packets), but there is no application listening on it. They can be helpful in showing that a host is up on an IP address (host discovery, or ping scanning), and as part of OS detection. Because closed ports are reachable, it may be worth scanning later in case some open up. Administrators may want to consider blocking such ports with a firewall. Then they would appear in the filtered state, discussed next.

filtered Nmap cannot determine whether the port is open because packet filtering prevents its probes from reaching the port. The filtering could be from a dedicated firewall device, router rules, or host-based firewall software. These ports frustrate attackers because they provide so little information. Sometimes they respond with ICMP error messages such as type 3 code 13 (destination unreachable: communication administratively prohibited), but filters that simply drop probes without responding are far more common. This forces Nmap to retry several times just in case the probe was dropped due to network congestion rather than filtering. This slows down the scan dramatically.

unfiltered The unfiltered state means that a port is accessible, but Nmap is unable to determine whether it is open or closed. Only the ACK scan, which is used to map firewall rulesets, classifies ports into this state. Scanning unfiltered ports with other scan types such as Window scan, SYN scan, or FIN scan, may help resolve whether the port is open.

open-filtered Nmap places ports in this state when it is unable to determine whether a port is open or filtered. This occurs for scan types in which open ports give no response. The lack of response could also mean that a packet filter dropped the probe or any response it elicited. So Nmap does not know for sure whether the port is open or being filtered. The UDP, IP protocol, FIN, NULL, and Xmas scans classify ports this way.

closed-filtered This state is used when Nmap is unable to determine whether a port is closed or filtered. It is only used for the IP ID idle scan.

5 Using and recognising port scans

Running port scans on your own networks can give you an attackers-eye view of your systems and identify ports that you may wish to protect with a firewall. On the other hand, you can also use tools like Nmap to be sure that services that should be accessible are online and available.

Since port scans may also be a precursor to an attack, you should also learn how to recognise port scans so that you can respond to unwanted scans and block subsequent attacks.

See http://www.linuxjournal.com/article/4234 for more information on this.

[2] http://nmap.org/book/man-port-scanning-basics.html

6 Exercise

Besides the machine on which you are running nmap, there are four other hosts on the 192.168.2.0/24 network. Find each one and determine as much as you can about them.