Lab 12.2 Port Scanning Detection
IN618 Security

May 19, 2016

Introduction

In the last lab we performed some port scans and saw how an attacker might use them to reconnoitre for vulnerable hosts as a prelude to an attack. We also learned that such scans don't leave a lot of evidence behind, even though an intensive port scan should present a clear pattern of network traffic *if we look for it*. In this lab we will see one way to detect port scans, but also how an attacker may try to evade such detection.

1 Perform an initial scan

Get the address of an Ubuntu server from the lecturer that you can log into with our standard user name and password. Pair up with another student. Install nmap on this system with the command `sudo apt-get install nmap`. One of you should perform this scan

```
nmap -PS <target-ip-address>
```

while the other one watches for any sign of the scan by monitoring the logfile at `/var/log/syslog`. An easy way to do this is with the command `tail -f /var/log/syslog`. (Hit Ctrl-C to stop when you're done.). It's unlikely that you will see any evidence of the scan.

2 Detecting scans

An easy way to detect some port scans is by installing `scanlogd` with the command `sudo apt-get install scanlogd`. (Install the package `screen` at this time in the same way.) Take turns scanning your partner's system and then using `tail -f /var/log/syslog` to watch for messages from `scanlogd`. You should see a log message showing that the scan was detected.

Since a basic scan is fairly easy to detect, there are options that we can use with nmap scans to try to conceal the activity. Try these scans on your partner's machine while he or she watches `syslog` for messages.

```
sudo nmap -PS -D 10.25.2.10,10.25.2.25 <target-ip>
```

This scan uses decoy addresses (10.25.2.10 and 10.25.2.25) to hide the real scan with some decoy scans.

```
nmap -PS -randomize-hosts <target-ip-address>/24
```

This scan scans multiple hosts in random order to make it less obvious that it is an automated port scan.

```
nmap -PS -T polite <target-ip>
```

This scan uses the *polite* timing scheme to scan a host more slowly and thus less detectably. It should take about five minutes to complete.

Even the polite scan is typically detectable. A better option is to use the *sneaky* timing scheme instead. The thing is, that scan takes about **five hours** to complete. So here's how you do it

1. Start `screen`
2. Start your scan `nmap -PS -T sneaky <target-ip>`
3. Close PuTTY
4. At least five hours later, log back in to your machine and use `screen -r` to reattach to your screen session. Check for scan results.
5. Find out if your partner detected your scan.