Port Scanning

Objectives

1. Introduce the techniques of port scanning.
2. Use port scanning audit tools such as Nmap.

Introduction:

- All machines connected to a LAN or connected to Internet via a modem run many services that listen at certain ports.
- A service is a program that waits inside a loop for a request message from a client, and acts on the request.
- By port scanning, one discovers which ports are available (i.e., being listened to by a service). Essentially, a port scan consists of sending a message to each port, one at a time and examining the response received. If the port is in use, it can then be probed further for weakness.
- Port Scanning is one of the most popular among the reconnaissance techniques attackers use.

Port Scanning

Port scanning allows a hacker to determine what services are running on the systems that have been identified. If vulnerable or insecure services are discovered, the hacker may be able to exploit these to gain unauthorized access. There are a total of 65,535 * 2 ports (TCP & UDP). While a complete scan of all these ports may not be practical, analysis of popular ports should be performed.

Many port scanners ping first, so make sure to turn this feature off to avoid missing systems that have blocked ICMP.
Popular port scanning programs include: Nmap, Netscan Tools, Superscan and Angry IP Scanner.

**The port numbers are divided into three ranges:**

1. Well Known Ports (from 0 through 1023)
2. Registered Ports (from 1024 through 49151)
3. Dynamic and/or Private Ports (from 49152 through 65535).

**TCP and UDP Port Scanning**

Remember that TCP offers robust communication and is considered a connection protocol. TCP establishes a connection by using what is called a *three-way handshake*.

The TCP header contains a 1-byte field for the flags. Look at the figure below to see TCP flag structure.

![TCP Flag Structure](image)

- **ACK**: The receiver will send an ACK to acknowledge data.
- **SYN**: Used during the three-step session setup to inform the other party to begin communication and used to agree on initial sequence numbers.
- **FIN**: Used during a normal shutdown to inform the other host that the sender has no more data to send.
- **RST**: Used to abort an abnormal session.
- **PSH**: Used to force data delivery without waiting for buffers to fill.
- **URG**: Used to indicate priority data.

At the conclusion of communication, TCP terminates the session by using what is called a four-step shutdown. See the figure below.
From a scanning standpoint, this means that TCP has the capability to return many different types of responses to a scanning program. By manipulating these features, an attacker can craft packets in an attempt to coax a server to respond or to try and avoid detection of an intrusion detection system (IDS). Many of these methods are built in to popular port-scanning tools. Before we look specifically at the tools and its popular port-scanning techniques, let’s see the port number of the common services.

**Common Ports**

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>20/21</td>
<td>FTP</td>
<td>TCP</td>
</tr>
<tr>
<td>22</td>
<td>SSH</td>
<td>TCP</td>
</tr>
<tr>
<td>23</td>
<td>Telnet</td>
<td>TCP</td>
</tr>
<tr>
<td>25</td>
<td>SMTP</td>
<td>TCP</td>
</tr>
<tr>
<td>53</td>
<td>DNS</td>
<td>TCP/UDP</td>
</tr>
<tr>
<td>67/68</td>
<td>DHCP</td>
<td>UDP</td>
</tr>
<tr>
<td>69</td>
<td>TFTP</td>
<td>UDP</td>
</tr>
<tr>
<td>80</td>
<td>HTTP</td>
<td>TCP</td>
</tr>
<tr>
<td>110</td>
<td>POP3</td>
<td>TCP</td>
</tr>
<tr>
<td>161/162</td>
<td>SNMP</td>
<td>UDP</td>
</tr>
<tr>
<td>443</td>
<td>HTTPS</td>
<td>TCP</td>
</tr>
</tbody>
</table>
Nmap

Nmap was developed by Fyodor Yarochkin and is one of the most well-known port-scanning tools. Nmap is available for Windows and Linux as a GUI and command-line program. It can do many types of scans and OS identification. It also has the ability to blind scan and zombie scan, and it enables you to control the speed of the scan from slow to very fast.

The name Nmap implies that the program was ostensibly developed as a network mapping tool. As you can imagine, such a capability is attractive to the people who secure networks as well as those who attack networks. Nmap is considered one of the best port-scanning tools in part because it offers an easy command-line interface (CLI) and has ready availability of documentation, and because of the way in which the tool has been developed and maintained.

Common Scan types

TCP Full Connect scan: This type of scan is the most reliable but also the most detectable. It is easily logged and detected because a full connection is established. Open ports reply with a SYN/ACK; closed ports respond with a RST/ACK.

TCP SYN scan: This type of scan is known as half-open, because a full TCP connection is not established. This type of scan was originally developed to be stealthy and evade IDS systems, although most now detect it. Open ports reply with a SYN/ACK; closed ports respond with a RST/ACK.

TCP FIN scan: Forget trying to set up a connection; this technique jumps straight to the shutdown. This type of scan sends a FIN packet to the target port. Closed ports should send back an RST. This technique is usually effective only on Unix devices.
**TCP NULL scan:** Sure, there should be some type of flag in the packet, but a NULL scan sends a packet with no flags set. If the OS has implemented TCP per RFC 793, closed ports will return an RST.

**TCP XMAS scan:** just a port scan that has toggled on the FIN, URG, and PSH flags. Closed ports should return an RST.

**Nmap output:**

The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that information is the “interesting ports table”.

- That table lists the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered. **Open means** that an application on the target machine is listening for connections/packets on that port. **Filtered means** that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed. **Closed ports** have no application listening on them, though they could open up at any time. Ports are classified as **unfiltered** when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed. Nmap reports the state combinations **open|filtered** and **closed|filtered** when it cannot determine which of the two states describe a port.

- The port table may also include software version details when version detection has been requested.
In addition to the interesting ports table, Nmap can provide further information on targets, including reverse DNS names, operating system guesses, device types, and MAC addresses.

Nmap Scan Options

When we use the command line in the Nmap tool instead of GUI, we need some option which listed with the command to define the type of scan methods. The table below lists some of these options.

<table>
<thead>
<tr>
<th>Scan Option</th>
<th>Name</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>-sS</td>
<td>TCP SYN</td>
<td>Stealth scan</td>
</tr>
<tr>
<td>-sT</td>
<td>TCP FULL</td>
<td>Full connect</td>
</tr>
<tr>
<td>-sF</td>
<td>FIN</td>
<td>No reply from open port</td>
</tr>
<tr>
<td>-sN</td>
<td>Null</td>
<td>No flags are set</td>
</tr>
<tr>
<td>-sX</td>
<td>Xmas</td>
<td>URG, PUSH, and FIN are set</td>
</tr>
<tr>
<td>-sP</td>
<td>Ping</td>
<td>Performs ping</td>
</tr>
<tr>
<td>-sU</td>
<td>UDP Scan</td>
<td>Like Null scan</td>
</tr>
<tr>
<td>-sA</td>
<td>ACK</td>
<td>Performs an ACK scan</td>
</tr>
<tr>
<td>-sI</td>
<td>Idle Scan</td>
<td>Performs zombie scan</td>
</tr>
</tbody>
</table>
Lab Experiment

Requirements

Setup a network contains at least two machines (in the lab) or you can use software like VMware or Virtual PC to build you virtual lab (in your home). In this experiment you can use BackTrack 3 live cd to run Nmap or you can install windows version for your machine.

Procedures

1. From windows

   Graphical interface
   
   1. From PC1 (windows xp or backtrack 3) setup nmap , in the target field type the ip address or name of the target.
   2. Determine the scan type according your need ; you can change scan type from profile field (each scan has different parameters and will return different results).
   3. Click Scan to start scanning , be patient until the result appears , the time it takes depend on the scan type.
   4. Nmap output give you a summary for scanning process and other tabs give you the output in different shape. The output will be as previously discussion.
   5. An example for these is shown in figure 1

Command line

Note that the previous process can be done using command line interface ; Click start, run and type the following command :

Nmap [nmap switches](ip address of the target)
Example :Nmap -a -t4 iugaza.edu.ps

The summary will appear in command line with no GUI as in figure 2
2. From backtrack

Graphical interface

1. Click start – All Applications – Backtrack – Network Mapping – choose Zenmap; then a GUI similar to that will appear in windows appears and we use it like windows.

Command line

1. Click start – All Applications – Backtrack – Network Mapping – choose Nmap; then the shell will opened with help contains switches of nmap, usage of each one and examples.
Exercise

1. Use Nmap port scanner to scan three different environments; Do your work on machine on your network and secure website and normal website. Use different switches (or different scan modes: eg. Stealth scan) and compare the result for each and the time that take for each scan mode. The work should be done on windows version using GUI and command line.

   **BONUS:** try to do the work in step 1 using BackTrak Linux version.

2. As you know from this lab, **Zombie** scanning is an advanced technique used for port scanning.

   Search on the internet about this technique and give me no more than half paper about it including how it works, why this name for this method, and advantages and disadvantages of it.

   Also, try to use this scan on the Nmap tool. What is the result?