Module 1: Port Scanning

Difficulty: Beginner
Completion Time: 20 minutes
Points: 10 points

Scenario

Prior to sniffing a network for vulnerable traffic, an attacker can find vulnerable services by scanning devices on the network, then exploiting them. Port scanning can either be targeted or random. An attacker interested in a particular network will attempt to track down information about that network and scan for vulnerabilities. Alternatively, attackers will scan large blocks from a scanner and let it run for days, trying to find any machine that is available and able to be exploited.

In this scenario, you are penetration tester for a small company. You have been given the task to find the topology of a network and the find all the IP addresses and services on a network. You are going to act as an attacker and scan all the devices connected to an closed Local Area Network (LAN) network.

Introduction

A tool commonly used for port scanning is nmap (www.insecure.org/nmap/). Nmap allows users to enter a range of IP addresses, choose the type of scan desired, and let the program run in the background. When it has completed its sweep, it will produce a report, showing the ports that responded on each network device:

Directions

First, install nmap onto your machine.

Open a terminal and type:

```
~# sudo nmap --help
```

This should give you a summary of the nmap command line options.

Next find the devices connected to ‘gatechftp’ server, which has ip address 57.35.6.245. Type the following:

```
~# sudo nmap –p80 172.168.1.10
```

Make sure your set an IP address to be within this range. For example, type

```
~# sudo –i
~# ifconfig eth0 down
~# ifconfig eth0 172.168.1.40
~# ifconfig eth0 up
```

As a vulnerability tester your job is to scan the network and find all the open servers in the 172.168.5.0/24 using nmap and compile a small report of the following:

- All IP addresses, of devices connected, that are on the range of 172.168.5.0/24
- All operating systems or kernels

- All open ports (TCP and UDP)
- All services and version on each ip address that is up on the network
- Point out which services are vulnerable

Be sure to use a search engine, man nmap command, or nmap –help command to figure out how t get all the information above. Send a text file or screen shots to NetSecLab Site as a zipped file.