Enumeration and Scanning

Sam Roethemeyer

University of Advancing Technology

NTW330 – Applied Exploits

Enumeration and Scanning

For this assignment, we had a vulnerable machine on the same network as out kali boxes, and we needed to find out information about the vulnerable machines. We needed the IP addresses, server versions, what we used to find it, and evidence of all this.

First, I started an NMAP scan using the -sC and -sV options and on the entire network of 10.120.1.0/24 and found these two suspicious machines. There are a lot of open ports so these must be the vulnerable machines we need to find. Although it doesn't say which machine has which OS, I believe that the machine with the address 10.120.1.147 is a Windows box, because of the service open on port 139. I also believe the machine with the address 10.120.1.146 is a Linux machine. I can do another scan to help figure this out. "namp -sC -sV -script vuln 10.120.1.0/24" finds out which services are running and tries to find a vulnerability for these. In doing this I can see that the 10.120.1.146 machine is running a mysql server that is configured for Linux, so my assumptions are correct.

```
Nmap scan report for 10.120.1.146
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap scan report for 10.120.1.147
Host is up (0.0010s latency).
Not shown: 985 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1028/tcp open  unknown
1029/tcp open  ms-lsa
1084/tcp open  ansoft-lm-2
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
5800/tcp open  vnc-http
5900/tcp open  vnc
```

```
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 8861
|   Capabilities flags: 43564
|   Some Capabilities: SupportsTransactions, Support41Auth, SwitchToSSLAfter
andshake, SupportsCompression, LongColumnFlag, Speaks41ProtocolNew, ConnectW
thDatabase
|   Status: Autocommit
|_  Salt: +t(hURz0}G*9"=KAEu?w
```