Pen Testing

By: Sydney Nguyen

1. PASSIVE INFORMATION GATHERING

What domain did you investigate?

www.youtube.com

What is its IP address?

142.250.191.206

When does the domain's registration expire?

2023-02-15T00:00:00+0000

What information, if any, did you learn about the people or corporation responsible for the domain in question?

The registrar is MarkMonitor inc. it gives this information to contact Registrar abuse contacts, both the phone number and email. MarkMonitor Inc. develops software intended to protect corporate brands from Internet counterfeiting, fraud, piracy, and cybersquatting. It is used for many other sites or at least listed as their registrar. I am surprised that youtube is not in complete control of its registrar and instead leases a separate company to do their security.

Note: this note is mainly for my own notes, but make sure you are putting in .com .org after the name and not just typing it into nslookup or whois as it will pull up google.com information.

2. HOST DETECTION

List the IP addresses for all the active hosts you found on the local network.

192.168.35.1
192.168.35.2
192.168.35.128
192.168.35.129

What entities do those IP addresses represent?

The first, second, and third address entities are internet assigned numbers authoirty (IANA). Whereas the .129 represents a metasploitable entity.

For each possible candidate IP address it was searched in the local network, what steps did nmap take?

1. Start a TCP handshake with ip address
2. nmap ping scans
3. Then we send out a APR broadcast
    a. a request packet to all the machines on the LAN and asks if any of the machines are using that particular IP address

For address 137.22.4.0/24
List the IP addresses for all the active hosts you found on the local network.

note: it is displaying only 3 hosts

137.22.4.5
137.22.4.17
137.22.4.131

What entities do those IP addresses represent?

Elegit.mathcs.carleton.edu
Perlman.mathcs.carleton.edu.
Maize.mathcs.carleton.edu.

For each possible candidate IP address it was searched in the local network, what steps did nmap take?

note: the process is very similar to local network

1. Start a TCP handshake with ip address
2. nmap ping scans
3. Then we send out a APR broadcast
    b. a request packet to all the machines on the LAN and asks if any of the machines are using that particular IP address

3. PORT SCANNING

Which ports does Metasploitable have open, and what services do they correspond to?

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

What database server(s) is/are available on Metasploitable?

3306/tcp open mysql
5432/tcp open postgresql

What is the value of the RSA SSH host key? What is the host key for?

56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3
Use: host key is a cryptographic key used for authenticating computers, the host key is used for SSH connection.

Pick one of the open ports that has a service you have never heard of, and explain what the service does.

I chose to explore the port 139/tcp that is called netbios-ssn. The purpose is for a netbios session service which is the connection of two computers with the intent to transmit large messages or heavy data traffic, netbios is used for error recovery, OSI reference model services, and NBSS naming.

Cite

https://en.wikipedia.org/wiki/MarkMonitor#:~:text=MarkMonitor%20Inc.%20is%20an%20American,brand%20abuse%20on%20the%20Internet.

https://www.iana.org/

https://www.ssh.com/academy/ssh/host-key

https://www.grc.com/port_139.htm

https://www.techopedia.com/definition/25190/netbios-session-service-nbss