Mississippi State UNIVERSITY

J. A. "Drew" Hamilton, Jr., Ph.D.

Director, Center for Cyber Innovation

Professor, Computer Science & Engineering

CCI
Post Office Box 9627
Mississippi State, MS 39762

Voice: (662) 325-2294
Fax: (662) 325-7692
hamilton@cci.msstate.edu

Scanning

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

What is Scanning?

- Scanning is the process of engaging and probing a target network with the intent of revealing useful information and then using that information for later phases of the pen test or attack.
- The scanning process is possible from the previous step of footprinting.
- Need a good understanding of networks, protocols, and operating systems.

Types of Scans

- **Port Scan – sending carefully crafted packets to a target computer to learn more about the network. Usually targeted toward common ports like FTP, Telnet, and SSH.**
- **Network Scan – locates all the live hosts, i.e. ping sweeps, nmap, AngryIP**
- **Vulnerability Scan – identifies weaknesses in applications, i.e. Nessus, Nexpose, Burp Suite, Nikto, and WebInspect.**

Information gathered

- Live hosts on a network
- Information on open/closed ports
- Operating system info
- Services and processes running
- Info about patches
- Presence of a firewall
- Router and device addresses

Checking for Live Systems

- **Wardialing**
- **Wardriving**
- **Pinging**
- **Port scanning**

- **Understand the difference between these processes**

Wardialing

- Modems and dial-ups are still used on a lot of systems
- Dial a block of numbers and you can locate computers connected
- Old systems can be pivot points
- Programs: ToneLoc, THC-SCAN, NIKSUN's PhoneSweep
- Older systems may not be getting a lot of attention, stealthly

Ping

- Tool used to determine network connectivity
- Works using ICMP, so Ping is also called ICMP Scanning
- ICMP echo checks if connection is live
- Should be very familiar with Ping as a network user
- Ping command: ping <target ip address>
- Nmap ping command:
  - Nmap –sn –v <target ip address>

Hping3

- The Heavy Artillery
- TCP/IP packet crafter
- Hping -1 <domain name>
- Hping –c 1 –V –p 80 –s 5050 –A <domain name>
  - Checks to see if there is a firewall blocking ping requests

Checking the Status of Ports

- Review TCP/IP fundamentals
- Three way handshake
- Packet Flags: SYN, ACK,URG,PSH,FIN,RST
- Create an ACK packet
  - Hping3 –A <target ipaddress> -p 80
  - Learn how to use Hping3 in detail and how to use options to craft packets

Full-Open Scan

- Systems involved have completed the three-way handshake
- Gain lots of information, but this is a very ‘noisy’ scan
- Shows up in logs
- Nmap –sT <ip address or range>

Stealth or Half-Open Scan

- Also known as a SYN scan
- Quieter because it does not complete the three-way handshake
- Does not complete handshake with final ACK message
- Less likely to trigger detection
- Nmap –sS <ip address or range>

Xmas Tree Scan

- Sends out lots of flags such as URG, PSH, FIN set to ON
- Illogical combination forces system to determine what to do
- Lack of response from a system will tell you a port is open
- Nmap –sX –v <target ip address>

FIN Scan

- FIN flag is set to ON
- Very quiet
- Passes through firewalls
- Victim's response determines if port is open or closed
- If FIN is sent to open port, there is no response. If the port is closed, the victim will return a RST packet.
- Nmap –sF <target IP address>

NULL Scan

- No flags are set in the packet
- Similar results to Xmas Scan and FIN scan
- Nmap –sN <target ip address>

Idle Scanning

- Probe the zombie's IP ID and record it
- Forge a SYN packet from the zombie and send it to the desired port on the target. Depending on the port state, the target's reaction may or may not cause the zombie's ID to be incremented.
- Probe the zombie's IP ID again. The target port state is then determined by comparing this new IP ID with the one recorded in step 1

When a Scan is Blocked

- **Fragmenting a packet**
- **Prevents detection**
- **Nmap –sS –T4 –A –f –v <target ip address>**

UDP Scanning

- Connectionless
- Doesn’t have flags
- Once a packet leaves the system, that’s it
- If port is open, there will be no response
- If port is closed, it will say “ICMP Port Unreachable”

OS Fingerprinting

- Active vs. Passive fingerprinting
- Common techniques
  - IP TTL values
  - IP ID values
  - TCP window size
  - TCP options
  - DHCP requests
  - ICMP requests
  - HTTP packets
  - Running services
  - Open port patterns

Active Fingerprinting with Nmap

- **OS detection with Nmap**
  - **Nmap –O <ip address>**

Passive Fingerprinting an OS

- p0f
- Passively analyzes network traffic
- Displays operating system info
- Available on Linux (Kali)
- Listen on eth0
  - Sudo p0f –I eth0

Banner Grabbing

- Banners have useful information about services running
- Usually done with Telnet
- telnet <ip address>:<port> HEAD / HTTP/1.1
- telnet <target ip> 80 head/http/1.0
- Netcraft, Xprobe, p0f, and Maltego are other really good programs

Countermeasures

- Disable or change banners
- Internet Information Server
- Hide file extensions on webservers
- ASP.NET and JavaServer Pages can be identified by the file extensions

Mapping the Network

- Can give you a big picture of how everything is connected
- Helps you see what might be vulnerable

Using Proxies

- System that stands in between the scanner and target
- Proxy Servers can filter traffic, anonymize traffic, provide a layer of protection between outside world and network
- Learn how to use a free proxy with your web browser
- Learn more about the TOR project

Summary

- Remember the basic concept of scanning
- Understand targets
- Know the vulnerabilities
- Know different scanning types
- Know when to use each scan
- Know preventive measures
- Know your tools and terms