Network Scanners

Timo Ralli

A brief history

- Scanning as a method has been around for ages
- Basic idea is to probe as many listeners as possible
- Earlier this was done by calling through modem numbers
- The modern way is to scan all IP-addresses within some range

What is a network scanner?

- Application that runs on one system and probes other systems
- Mainly used to attack TCP/IP ports and services
- The response might include valuable information about the target host

What is a network scanner? (2)

- Example:

If one manages to find out the operating system of the target host, he is able to take advantage of the known weaknesses of that system

- Previous scanners mostly Unix based, nowadays there is a program almost for every OS

Why to use scanners?

- Scanners used to detect the security weaknesses
- Usage dualistic: both Sys. Admins & hackers use the same programs
- Do not guarantee security!
- Only helps to find the weak spots
- Important to use regularly and systematicly

Operating principle

- Based on the operations of the TCP/IP protocol suite and service ports
- In more detail, takes advantage of the messages sent by UDP, TCP, IP and ICMP protocols

The 9 basic scanning techniques

- TCP connect() scanning
- TCP SYN (half open) scanning
- TCP FIN (stealth) scanning
- TCP ftp proxy (bounce attack) scanning
- SYN/FIN scanning using IP fragments (bypasses packet filters)

The 9 basic scanning techniques (2)

- UDP recvfrom() scanning
- UDP raw ICMP port unreachable scanning
- ICMP scanning (ping-sweep)
- reverse-ident scanning

ICMP Scans

- ICMP (Internet Control Message Protocol) used e.g. in error reporting & gathering of network information
- Ping & traceroute use ICMP
- Reply messages may help to identify the remote OS
- Not a port scan technique!

UDP Scans

- Uses the information derived from the receipt of an ICMP port unreachable message
- Scanner sends an UDP data gram to an UDP port on a target system
- If no message received -> port might be listening (open)

TCP Scans

- Also a port scan technique
- TCP connect the most basic scanning
- Based on the three way handshake
- Pick a port & attempt to connect it
- If the port is open the connect should succeed

TCP Scans (2)

- Problem: easy to detect
- Solution: First send a SYN message then RST (reset) if SYN/ACK received -> harder to detect

TCP Scans (3)

- TCP FIN also a common technique
- Situation: no connection in the beginning, then a TCP FIN is sent
- Because no previous connection existed, an open port probably ignores the packet
- A non listening port probably sends a RST

TCP Scans (4)

- So if no answer, the port is probably open!
- If RST, the port is not listening or the host is a Windows system

TCP Scans (5)

- The attempt detection probability can be minimised
- Set all the flags (XMAS Tree) all no flags (NULL) -> isn’t likely to be logged (stealth scan)

Identify the remote OS

- Important -> many security holes are OS dependant
- Some systems provide useful information in a banner, most of them doesn’t
- Other techniques must be used

Identify the remote OS (2)

- Vendors implement the TCP/IP in different ways
- These differences can help us to identify the OS
- For example the TTL (Time To Live) varies between different systems