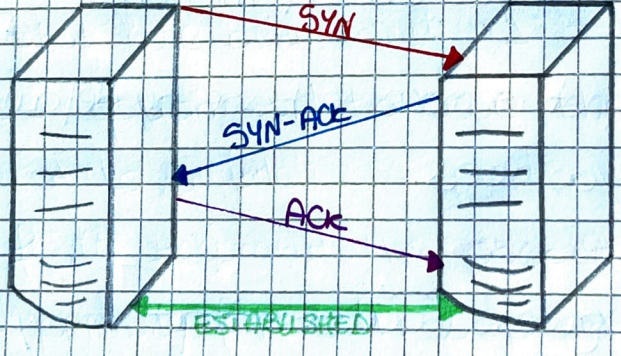
Internet. Although almost any firewall can filter ICMP packets, organizational needs may dictate that the firewall pass some ICMP traffic. If a true need exists, you should carefully consider which types of ICMP traffic you allow pass. If ICMP traffic can be limited with ACLs to your ISP's specific IP address, you are better off.

3ª lezione 26-02-2021

Determining Which Services are running or listening.

Port scanner is the process of sending packets to TCP/UDP ports on the target system to determine what services are running or are in a LISTENING state. Scan types:

- TCP Connect Scan
  - This type of scan connects to the target port and completes a full three-way handshake (SYN, SYN/ACK, ACK).
  - Longer than some of the other scan types
  - Logged from the target system.



- TCP SYN SCAN
  - Only a SYN packet is sent to the target port. If a SYN/ACK is received from the target port, we can deduce that it's in the LISTENING state.
  - If an RST/ACK is received, it usually indicates that the port is not listening.

- No logged from the target system
- This form of scanning can produce a DOS condition on the target by opening a large number of half-open connections.
- Relatively safe.

• TCP FIN SCAN

- Send a FIN packet to the target port
- Based on the RFC 793, the target system should send back an RST for all closed ports.
- Only works on UNIX-based TCP/IP stacks.

• TCP Xmas Tree scan

- Send a FIN, URG and PUSH packet to the target port.
- Based on the RFC 793, the target system should send back an RST for all closed ports.

• TCP NULL Scan

- Turns off all flags.
- Based on the RFC 793, the target system should send back an RST for all closed ports.

• TCP ACK Scan

- Used to map out firewall rulesets.
- It can help determine if the firewall is a simple packet filter allowing only established connections or a stateful firewall performing advance packet filtering.

• TCP Windows Scan

- May detect open as well as filtered/non filtered ports on some systems.
- Due to an anomaly in the way the TCP window size is reported.

TCP RPC Scan

- Specific in Unix System
- Used to detect an identify RPC (Remote Procedure Call) ports, their associated program and version number.

UDP Scan

- Send an UDP packet to the target port
- If the target port responds with an "ICMP port unreachable" msg, the port is closed.
  If you don't receive this msg, the port is open.
- Very slow process, unreliable results.

SYN and connect scan should work against one host.
Identifying TCP/UDP Services Running: nowadays many tools incorporate both host discovery and port scanning functionality. Nmap is one of the most feature rich port-scanning tools out there.
First perform host discovery and by then port scanning only if the host that have been identified as being alive. TCP SYN SCAN option -sS option -oN to save the report in human-readable format to a file.
Option -f to fragment the packet, against a simple packet filter as primary firewall. Depending on the sophistication of the target network and hosts, the scans performed thus far may have easily been detected. Nmap provides the decoy-scan capabilities with the -D option, making it more difficult to discern legitimate port scans from bogus ones. FASULLO
You simply spoof the src address of legitimate servers and intermix these bogus-scan with the real port scan.

RAGGIUNGERE

Option -b to perform a FTP bounce scanning FTP bounce attack is an exploit of the FTP protocol whereby an attacker is able to use the PORT command to request access to port indirectly through the use of the victim machine as a middle man for the request. SuperScan allows for ping scanning, TCP/UDP (PORT) scanning, and includes numerous techniques for doing them all.

SuperScan allows you to choose from four different ICMP host-discovery techiques, including traditional ECHO REQUESTS and the less familiar TIME STAMP REQUESTS, ADDRESS MASK REQUESTS and INFORMATION REQUESTS.

The tool allows you to choose the ports to be scanned, the techineques for UDP/TCP.

Scanline like netcat, it's just a single executable, which maces it easy to load onto a compromised host and pivot to target internal system that may be inaccessible from your initial attack system.

Netcat is an excellent utility that deserves an honorable mention. Netcat's basic TCP/UDP port-scanning capabilities are useful in some scenarios when you need to minimize your footprint on a compromise system. By default, netcat uses TCP ports. Therefore, we must specify the -u option for UDP scanning. Option -v and -vv provide verbose (DETTAGLIATO) and very verbose output. Option -z provides zero mode I/O, option -w2 provides a timeout value for each connection.

PORT SCANNING COUNTERMEASURES:

DETECTION: The primary method is to use a network-based IDS program like Snort.

From UNIX host-based prospective, the SCANLOG utility from

Solar Designer is a TCP port scan detection tool that detects and logs such attacks.
We also recommend configuring your alerts to fire in real time via e-mail. Most firewalls can and should be configured to detect port scan attempts. PREVENTION:
- Disabling all unnecessary services
In the UNIX environment, you can accomplish this by commenting out unnecessary services in /etc/inetd.conf and disabling services.

DETECTING THE OPERATING SYSTEM

-ACTIVE OPERATING SYSTEM DETECTION

We can perform simple banner-grabbing techniques which grab information from such services as FTP, telnet, SMTP, HTTP, POP, and others. Banner grabbing is the simplest way to detect an operating system and the associated version number of the service running.
Accurate technique: the stack fingerprinting.

Making Guesses from available port

We're trying to identify open ports that provide telltale signs of the operating system.
Windows based systems listen ports: 135, 139, 445.
Windows 95/98 only listen on port 139.
Remote Desktop Protocol (RDP): TCP port 3389.
UNIX: SSH port 22/TCP
Older UNIX servers: portmapper TCP/111
Berkeley R service TCP/512-514
NFS TCP/2049
high-number ports 32777 (and above) listening

By performing a simple TCP and UDP port scan, we can make quick

assumptions about the exposure of the systems we are targeting.

- FIN PROBE

- A FIN packet is sent to an open port. Many stack implementations respond with a FIN/ACK. RFC 793 states that the correct behavio is not respond.

- Bogus Flag Probe

- An undefined TCP flag in set in the TCP header of a SYN packet. Some operating system, like linux, respond with the flag set in the response.

- ISN Sampling

- Find a pattern in the initial sequence chosen by the TCP implementation.

- "Don't fragment bit" monitoring

- Some OS set bit to enhance perform.

- TCP initial window size

- For some stack implementations, this size is unique.

- ACK Value

- Some implementations return the sequence number you sent, and others return a sequence number + 1

- ICMP error message quenching

- OS may follow RFC 1812 and limit the rate at which error msg are sent.

- Count the number of unreachable msg received within a given time.

- ICMP message quoting

- OS differ in the amount of information that is quoted when ICMP errors are encountered.

- Examine quote msgs.

- ICMP error message - echoing integrity

- Some stack implementations may alter the IP headers when sending back ICMP error msgs.

- TOS (Type of Service)

- Most stack implementations use value set at 0 (ICMP PORT UNREACHABLE), but this can vary.

- Fragmentation handling

- Different stacks handle overlapping fragments differently.

- Nothing how probe packets are reassembled

- TCP options

By sending a packet with multiple options set you can make assumptions about the target OS.

Nmap employs the techniques mentioned earlier by using the -O option.

Countermeasures:

Detection: You can use many of the aforementioned port-scanning detection tools to watch for OS detection.

PREVENTION: If attackers know the OS, they should have a difficult time obtaining access to the target system.

PASSIVE OPERATING SYSTEM IDENTIFICATION

Active scanning it was relatively easy for a network-based IDS system to determine that OS identification. Active stack fingerprinting is note one of the most stealthy techiques an attacker will employ.

PASSIVE STACK FINGERPRINTING: Instead of sending packets to the target system, however, an attacker possively monitors network traffic to determine the OS in use. Exclusively dependent on being in a central location on the network and on the port that allows packet capture (mirrored port). We limit our discussion to several attribute associated with a TCP/IP session to fingerprint the OS with passive stack fingerprinting:

TTL
- What does the OS set as the TTL on the outbound packet?
Window size
- What does the OS set as the window size?
DF (don't fragment)
- Does the OS set the "Don't Fragment bit"?

By passively analyzing each attribute and comparing the results to a know database of attribute, you can determine the remote OS. Fairly reliable results. This technique is exactly what siphon tool uses. Siphon contain a database file of operating system matches with TTL, window size and DF bit.

COUNTERMEASURES:

DETECTION:
You can use many of the aforementioned port-scanning detection tools to watch for operating system detection.

PREVENTION: (vedi la prevention scritta nella pagina precedente)
like the yellow PREVENTION.

PROCESSING AND STORING SCAN DATA

Metasploit
General exploit framework used to modularize exploits and payloads. Metasploit's installation sets up a PostgreSQL server for managing data to allow you to make specific queries to the database for scan data. Use the Metasploit console (msfconsole) to execute framework commands:
"db_connect" → command to connect to the database
"db_nmap" → " within Metasploit allows you to run basic Nmap scan and import the data directly into the database.

"db_import" → to import external results into the database

"hosts" → command to list the hosts in the database

"services" → command to show the available open port and services on the identified hosts.

4a lezione 02-03-2021

ENUMERATION 3° CAPITOLO