Anaisy Garcia PID:5734454

Overview-

Scanners can be used for both legal and illegal practices. Scanners being used ethically are used by network administrators to find and fix vulnerabilities on their network on their own machines. The unethical use of scanners consists of crackers, who are people that engage in illegally hacking into a computer without permission, looking and exploiting vulnerabilities rather than fixing them. Scanners where originally designed to aid security professionals and system administrators with examining networks and computers to find security vulnerabilities.

A scanner is a software that will find, examine, and report about vulnerabilities on local and remote hosts. Most popular scanners are made freely on the internet making it easier to access not only for ethical hacking purposes but for unethical hacking purposes. These scanners are specialized tools that are designed to detect which of the network ports that exist are open. Knowing which ports are available can be a way to being looking for vulnerabilities or exploits. Most of these ports have the duty of handing specific network protocols and services.

The easiest one to remember is port 80 which deals with sending and receiving the http traffic that runs much of the internet.

A port scanner determines whether a port is open or closed and which application is listening on that port.

Understanding the concept of scanning and how to use the scanning tools can be used to make many networks safer and less vulnerable to attacks.

Background-

To understand fully where the concept of scanning originated from we need to go back to 1969. Scanners became a reality before the internet even existed in 1969. This is back when computers where just mainframes and terminals. In this era, they would scan for dead terminals from the mainframe.

ARPANET was the father of the internet had its first virus in 1988. This was 19 years after its launch and 12 years after the first PCs were shipped. Back then security was a second thought. With the early UNIX languages having no security at all. By the time the internet became “normal”, hackers started publishing vulnerabilities on the internet. As new vulnerabilities arose the old ones would be patched.

When the internet became popular legitimate network users would connect to servers using their telephone numbers. This telephone number would be connected with a shell account providing them with different usernames and passwords. Hackers would take these telephone numbers and experimented with different usernames and passwords. Trying to dial all telephone numbers was very time consuming so the war dialer was invented.

War dialers is a script that tells the modem to dial a range of phone numbers defined by the user and then identifies those numbers that connect to remote computers. These were just automated scanners that scanned for open phone numbers.

Now a days, scanners are available freely. Searching up “hacking scanning tools download” alone brings up over 2 million finds. The first website having 15 of them already with downloads.

How do they work and what types are there-

Scanners examine network weaknesses in an automated process. They do no discover vulnerabilities. They simply check for ones that already exist and open ports as well. Scanners can be set to target either a single IP or range of IPs.

A scanner does the following:

1. Connects to a target host or hosts
2. Examines the target host or hosts for the services running on it
3. Examines each service for any known vulnerability

Types of scanners-

The six most important types of scanning are TCP, half-open, UDP, IP protocol, Ping, and Stealth.

TCP stands for transmission control protocol. A TCP connect scan attempts to make TCP connections with all the ports on a remote system. In this scan the target host transmits connection succeeded messages for active ports and host-unreachable messages for inactive ports.

In TCP a host sends a SYN which is a synchronization messages to the target host. The target host will then send back a SYN and an ACK which is an acknowledgement message to the host that requested the connection. After this the host will send back another ACK establishing the connection.

A user does not need root privileges to perform a TCP attack but the IDS, which is the Intrusion Detection System can recognize this attack.

Half-open scanning is like TCP connection scanning except it will not complete the connections. In half-open only a SYN is sent from the scanner. The reply can be a SYN/ACK which indicates the port is open or an RST/ACK which means that no listening is done from the port.

A user does need root privileges to perform a half-open scan. Most operating systems IDS don’t log half-open attack signature making it safe and effective.

UDP stands for user datagram protocol. UDP scanning examines the UDP ports on a target system. In UDP scanning the scanner sends a 0-byte UDP packet to all the ports on a target host. If the port is closed, the scanner receives an ICMP or internet control message protocol unreachable message. If the port is active however, no message is sent back.

Since most operating systems generate UDPs very slowly, UDP scanning is impractical and time consuming.

IP protocol scanning examines a target host for supported IP protocols. Here the scanner transmits IP packets to each protocol on the target host. If a protocol on the target host replies with an ICMP unreachable message to the scanner, then the attacker does not use that protocol. However just like UDP if nothing is sent back the attacker assumes that the target supports that protocol.

Ping scanning can tell whether a remote host is active by sending ICMP echo requests packets to the host. If the packet is sent back the host is active. However, there is a drawback with this being if a host blocks or drops the packets a false reading may occur.

Stealth scanning allows for examining hosts behind firewalls and packet filters. This also will not be logged in most operating systems like half-open scanning.

Scanning has four phases, discovery, reconnaissance, vulnerability identification, and exploitation.

Discovery is where actual testing occurs. This is the phase that gathers early stages of information. The tool used for this is Nmap. Nmap performs TCP, half-open, ping, UDP, and IP protocol scans.

Reconnaissance is the stage of penetration testing. Here the tools used maltego and wireshark to do a deeper search.

Vulnerability identification is the stage is where vulnerability discovery lies. Here the tool used is Nessus to identify these vulnerabilities.

Exploitation is the last stage where an attacker can go beyond the limits of ethical hacking by exploiting already found vulnerabilities. Here the tool used is Metasploit.

Here show the different tools.

End.

Source: Computer Security and Penetration Testing. Second Edition.