Information Gathering Techniques

K.K.S. GAUTAM
ASSISTANT PROFESSOR
SHIVAJI COLLEGE

Evolution of Scanners

Scanners first appeared even before the creation of ARPANET, the precursor to the Internet in 1969.

Prior to ARPANET, the computing world was made up of mainframes and dumb terminals. But even in this limited model.

A terminal operator might have occasionally been unable to connect to the mainframe.

There were ways to scan for dead terminals from the mainframe even then.

It was a great convenience to be able to ping over the Internet and access networks segmented by routers and switches not under and administrator's direct control.

The internet was launched in the 1970s and the first PC was not released unitl the mid 1970s.

The early UNIX like languages has no security al all.

The first virus was released in 1988-99 years after ARPANET launched, and 12 years after the first PC were shipped.

When hackers wanted to crack a system in the 1970s, they would examine the target system for all known vulnerablitites.

Scanning(Scanners)

A Scanner is a software tool that examines and reports about vulnerabilities on local and remote hosts.

It available as a specialized tool designed only to scan ports(port scanners).

As network tools, or as parts of networking utility suites.

These tools, either in whole or in parts, are designed to detect which of the 65535 network ports that exist are “open”.

A number of these ports have been assigned the task of handling specific network protocols and services.

For example:- most people are aware that port 80 sends and receives the http traffic that runs much of the internet.

If there is a vulnerability identified in the latest version of Telnet, then Port 23 may be a point of focus for someone hopping to exploit that vulnerability.

Port Scanner

It examines and reports on the condition(open or closed) of a port as well as the application that is listening on that port, if possible.

Network utilities such as dig, ping and trace are limited use port scanners.

Scanners were originally developed to aid security professionals and system administrators in examining networks for security vulnerabilities.

It is open source software(scanners), allow students, hobbyists, and hackers to test the security of their own networks.

The legitimate use of scanners has made many networks safer and less vulnerable to attack.

The public availability of scanners and the quality of their vulnerability reporting have made them very popular hacking tools.

How Scanners Work

Scanners automate the process of examining network weakness.

Scanners are not heuristic: they don't discover new vulnerabilti4es.

They check for known vulnerabilities and open ports.

A scanner performs these functions:-

- Connects to target hosts.
- Examines the target host for the services running on it.
- Examines each service for any known vulnerability.

  (Scanners can be set to target a single IP address or a range of IP address.)

Types of Scanning

Transmission Control Protocol (TCP) connect scanning

Half-open scanning

User Datagram Protocol(UDP) scanning

IP Protocol scanning

Ping scanning

Stealth scanning

TCP Connect Scanning:-

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

Half-Open Scanning:-

- It doesn't complete the connections. In typical TCP connections a host initially sends a synchronization message, SYN to the target host. The target host replies back with a SYN and an acknowledgment requesting ACK to the host that requested a connection.

UDP Scanning:-

- UDP scanning examines the status of UDP ports on a target system. First the scanner sends a 0-byte UDP packet to all the ports on a target host.
- If port is closed, the target host replies with an ICMP unreachable message to the computer on which the scanner is installed.
- If the port is active, then no such message is sent back.

IP Protocol Scanning:-

- In this method, 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 target host does not use that protocol.
- If there is no reply, then the hacker assumes that the target host supports that protocol.

Ping Scanning:-

- A ping scan demonstrates whether a remote host is active by sending ICMP echo request packets to that host.
- If the target host sends back packets, it can be assumed that the host is active
- However, sometimes hosts block or drop ICMP echo request packets. This results in a false negative reading on that specific host.

Stealth Scanning:-

- Stealth scanning lets you examines hosts behind firewalls and packet filters, in some ways, it is similar to half-open scanning in that most stealth scanners do not allow target hosts to log the scanning activities.

Password Crackers

Programs that guess and crack passwords are widely available on the internet, even to a novice cracker.

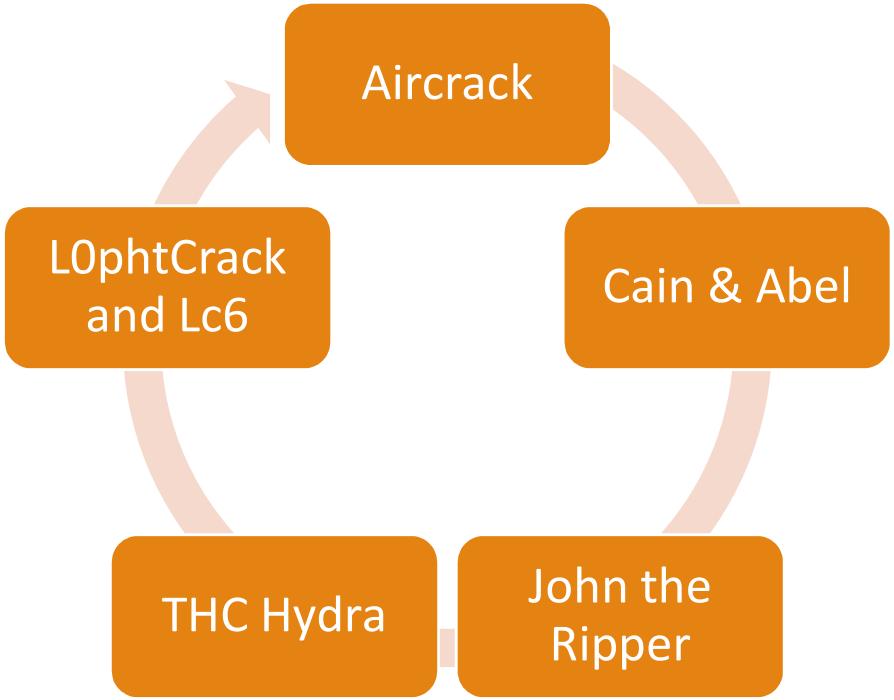
It is available for both Windows and Linux Platforms.

Password crackers are wonderful when passwords are lost or key personnel have been fired or are otherwise not available.

An administrator does is change the root passwords on the servers.

Security administrators also use password crackers to check for weak passwords on their networks

Some widely used Crackers programs



Aircrack

- Aircrack is a suite of tools designed to compromise Wireless Equipment Privacy(WEP) and Wi-Fi Protocol Access(WPA).
- They are commonly implemented encryption solutions for wireless networks.
- It was created in 2010 and works with a number of other tools, each of which contributes to the collecting of packets, cracking of passwords, and decryption of information.
- Aircrack is the component that cracks WEP and WPA passwords.

Cain & Abel

- In 2011, insecure.org named Cain & Abel among the top password-recovery tools for the Windows platforms.
- It is capable of handling an enormous variety of tasks: recovering passwords by sniffing the networks, cracking encrypted passwords using dictionary, brute force, and cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, revealing password boxes, uncovering cached passwords, and analyzing routing protocols.
- It can also do ARP poisoning.

John the Ripper

- Currently available for many versions of UNIX, DOS, Win32,BeOS, and Open VMS.
- It is a fast password cracker.
- It s primary purpose is to detect weak UNIX passwords.
- It supports several crypt password hash types, which are most commonly found on various UNIX versions as well as Kerberos AFS, and Windows NT/200/XP LM hashes.
- It has own optimized modules for different cipher text formats and architectures.
- It can detect cipher text encrypted by programs utilizing algorithms, such as the standards DES, the double-length DES, the extended DES, MD-5 and Blowfish.
- The latest stable version of John the Ripper is v1.7.9.
- John the Ripper supports several modes for cracking passwords:-
  - **Wordlist mode-** The simplest mode, this compares passwords against a list of words in a test file.
  - **Single-crack mode-** Faster than wordlist mode, this uses logon or GECOS information for cracking passwords. It limits the cracking process to the accounts related to the logon information. If more than one user has the same password, it repeats the comparison of guessed passwords.
  - **Incremental mode-** The most powerful mode used by John the Ripper, this attempts all possible combinations of letters, numbers and special characters. It is used for conducting brute –force attacks.
  - **External mode- It is defined by using the [List. External: Mode] section of the john.ini file. Here, "mode" is the name of the external mode. External mode can be used to specify customized functions for trying passwords, these cutomized functions are added to the [List. External: Mode] section.**

THC Hydra

- THC Hydra is a very useful network authentication cracker that supports many different services.
- It is available from THC at www.thc.org.
- It is a brute force cracker for testing remote authentication services.
- It can perform raped dictionary attacks against more than 40 of the most commonly used protocols.

L0phtCrack and Lc6

L0pht Heavy Industries developed L0phtCrack as a security tool to help system administrators and security professionals check password weakness of the the Windows NT operating system.

In 2006, the company that owned L0phtCrack, the @Stake company, was purchased by Symantec.

L0phtCrack was revived as L6 by the original creators in 2009 in three different versions: professional, administrator, and consultant.

References

1. Charles P. Pfleeger, Shari Lawrence Pfleeger, Security in Computing 4th Edition, Pearson.

2. A. Basta, N.Basta and M. Brown, Computer Security and Penetration Testing 2nd Edition, Cengage Learning India.