TOOLS AND METHODS USED IN CYBERCRIME:

INTRODUCTION
PROXY SERVERS AND ANONYMIZERS
PHISHING
PASSWORD CRACKING
KEYLOGGERS AND SPYWARES
VIRUS AND WORMS
TROJAN HORSE AND BACKDOORS
STEGANOGRAPHY
DOS AND DDOS ATTACKS
SQL INJECTION
BUFFER OVERFLOW

UNIT-4

INTRODUCTION

- Different forms of attacks through which attackers target the computer systems are as follows:
- 1. Initial uncovering:
  - Two steps are involved here.

    i. In the first step called as reconnaissance, the attacker gathers information about the target on the Internet websites.

    ii. In the second step, the attacker finds the company's internal network, such as, Internet domain, machine names and the company's Internet Protocol (IP) address ranges to steal the data.
- 2. Network probe (investigation):
  - At the network probe stage, the attacker scans the organization information through a "ping sweep" of the network IP addresses.
  - Then a "port scanning" tool is used to discover exactly which services are running on the target system.
  - At this point, the attacker has still not done anything that would be considered as an abnormal activity on the network or anything that can be classified as an intrusion.

INTRODUCTION

- 3. Crossing the line toward electronic crime (E-crime):
  - Once the attackers are able to access a user account, then they will attempt further exploits to get an administrator or “root” access.
  - Root access is a UNIX term and is associated with the system privileges required to run all services and access all files on the system (readers are expected to have a basic familiarity with Unix-based systems).
  - “Root” is an administrator or super-user access and grants them the privileges to do anything on the system.

INTRODUCTION

Websites and tools used to find the common vulnerabilities

Website	*Brief Description*
http://www.us-cert.gov/	US-CERT is the operational arm of the National Cyber Security Division (NCSD) at the Department of Homeland Security (DHS). US-CERT also provides a way for citizens, businesses and other institutions to communicate and coordinate directly with the US government about cybersecurity. US-CERT publishes information about a variety of vulnerabilities under "US-CERT Vulnerabilities Notes."
http://cve.mitre.org/	Common Vulnerabilities and Exposures (CVE) is a dictionary of publicly known information security vulnerabilities and exposures and free for public use. CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.
http://secunia.com/	It has thousands of vulnerability lists that are updated periodically. It has vulnerability database and provides in-depth analysis about virus, worm alerts and software vulnerability.
http://www.hackerstorm.com/	This website was created for open-source vulnerability database (OSVBD) tool. Since then it has grown in popularity and provides additional information about penetration testing. The site is updated with whole bunch of news and alerts about vulnerability research.

INTRODUCTION

http://www.hackerwatch.org/	It is an online community where Internet users can report and share information to block and identify security threats and unwanted traffic.
http://www.zone-h.org/	It reports on recent web attacks and cybercrimes and lists them on the website. One can view numerous defaced webpages and details about them.
http://www.milworm.com/	It contains day-wise information about exploits.
http://www.osvdb.org/	**OSVDB:** This is an open-source vulnerability database providing a large quantity of technical information and resources about thousands of vulnerabilities.
http://www.metasploit.com/	Metasploit is an open-source computer security project that provides information about security vulnerabilities and aids in penetration testing. Its most well-known subproject is the Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. The Metasploit Project is also well-known for antiforensic and evasion tools, some of which are built into the Metasploit Framework.
http://www.w00w00.org/files/LibExploit	LibExploit is a generic exploit creation library. It helps cybersecurity community when writing exploits to test vulnerability.
http://www.immunitysec.com/products-canvas.shtml	Canvas is a commercial vulnerability exploitation tool from Dave Aitel's ImmunitySec. It includes more than 150 exploits and also available are VisualSploit Plugin for drag and drop GUI exploit creation (optional).

INTRODUCTION

http://www.coresecurity.com/content/core-impact-overview	Core Impact is widely considered to be the most powerful exploitation tool available. It sports a large, regularly updated database of professional exploits, and can do neat tricks such as exploiting one system and then establishing an encrypted tunnel through that system to reach and exploit other systems.

- 4. Capturing the network:
  - At this stage, the attacker attempts to “own” the network. The attacker gains the internal network quickly and easily by target systems.
  - The next step is to remove any evidence of the attack. The attacker will usually install a set of tools that replace existing files and services with Trojan files and services that have a backdoor password.

INTRODUCTION

- 5. Grab the data:
  - Now that the attacker has “captured the network,” he/she takes advantage of his/her position to steal confidential data.
- 6. Covering tracks:
  - This is the last step in any cyber attack, which refers to the activities undertaken by the attacker to extend misuse of the system without being detected.
  - The attacker can remain undetected for long periods.
  - During this entire process, the attacker takes optimum care to hide his/her identity(ID) from the first step itself.

INTRODUCTION

CYBERSECURITY

Tools used to cover tracks

Website	*Brief Description*
http://www.ibt.ku.dk/jesper/ELSave/	**ELSave:** It is a tool to save and/or clear an NT event log. ELSave is written by Jesper Lauritsen. The executable is available on the weblink, but source code is not available.
http://ntsecurity.nu/toolbox/winzapper/	**WinZapper:** This tool enables to erase event records selectively from the security log in Windows NT 4.0 and Windows 2000. This program corrupts the event logs, therefore, they must be cleared completely.
http://www.evidence-eliminator.com/	**Evidence eliminator:** It is simple and one of the top-quality professional PC cleaning program that is capable of defeating all known investigative Forensic Software. Evidence eliminator permanently wipes out evidence so that forensic analysis becomes impossible.
http://www.traceless.com/computer-forensics/	**Traceless:** It is a privacy cleaner for Internet explorer (IE) that can delete common Internet tracks, including history, cache, typed URLs, cookies, etc.

INTRODUCTION

CYBERSECURITY

Website	*Brief Description*
http://www.acesoft.net/	**Tracks Eraser Pro:** It deletes following history data: • Delete address bar history of IE, Netscape, AOL, Opera. • Delete cookies of IE, Netscape, AOL, Opera. • Delete Internet cache (temporary Internet files). • Delete Internet history files. • Delete Internet search history. • Delete history of autocomplete. • Delete IE plugins (selectable). • Delete index.dat file. • Delete history of start menu run box. • Delete history of start menu search box. • Delete windows temp files. • Delete history of open/save dialog box. • Empty recycle bin.

INTRODUCTION

Scareware:

- It comprises several classes of scam software with malicious payloads, or of limited or no benefit which ore sold to consumers via certain unethical marketing practices. The selling approach uses social engineering to cause shock, anxiety or the perception of a threat generally directed at an unsuspecting user.

Malvertising:

- It is a malicious advertising - malware + advertising - on online criminal methodology that appears focused on the installation of unwanted or outright malicious software through the use of Internet advertising media networks, exchanges and other user-supplied content publishing services common to the social networking space.

INTRODUCTION

ClickJacking:

- It is a malicious technique of tricking netizens into revealing confidential information and/or taking control of their system while clicking on seemingly innocuous webpages.

Ransomware:

- It is computer malware that holds a computer system or the data it contains hostage against its user by demanding a ransom for its restoration.

PROXY SERVERS AND ANONYMIZERS

- Proxy server is a computer on a network which acts as an intermediary for connection with other computers on that network.
- The attacker first connects to a proxy server and establishes a connection with the target system through existing connection with proxy.
- This enables an attacker to surf on the Web anonymously and/or hide the attack.
- A client connects to the proxy server and requests some services (such as a file, webpage) available from a different server.
- The proxy server evaluates the request and provides the resource by establishing the connection to the respective server and/or requests the required service on behalf of the client.
- Using a proxy server can allow an attacker to hide ID (i.e., become anonymous on the network).

PROXY SERVERS AND ANONYMIZERS

- A proxy server has following purposes:
  1. Keep the systems behind the curtain (mainly for security reasons).
  2. Speed up access to a resource (through “caching”). It is usually used to cache the web pages from a web server.
  3. Specialized proxy servers are used to filter unwanted content such as advertisements.
  4. Proxy server can be used as IP address multiplexer to enable to connect number of computers on the Internet, whenever one has only one IP address
- One of the advantages of a proxy server is that its cache memory can serve all users. If one or more websites are requested frequently, may be by different users, it is likely to be in the proxy’s cache memory, which will improve user response time.
- In fact there are special servers available known as *cache servers.* A proxy can also do logging.

PROXY SERVERS AND ANONYMIZERS

- Listed are few websites where free proxy servers can be found:
  1. http:// www.proxy4free.com
  2. http://www.publicproxyservers.com
  3. http://www.proxz.com
  4. http:// www.anonymicychecker.com
  5. http://www.surf24h.com
  6. http:// www.hidemyass.com

PROXY SERVERS AND ANONYMIZERS

- An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable. It accesses the Internet on the user's behalf, protecting personal information by hiding the source computer's identifying information.
- Anonymizers are services used to make Web surfing anonymous by utilizing a website that acts as a proxy server for the web client.
- The anonymizer hides/removes all the identifying information from a user's computer while the user surfs on the internet, which ensures the privacy of the user.
- Listed are few websites where more information about anonyrnizers can be found:
- 1. http://www.aoonymizer.com
- 2. http://www.browzar.com
- 3. http://www.anonymize.net
- 4. http://www.anonymouse.ws
- 5. http://www.anonymousindex.com

PROXY SERVERS AND ANONYMIZERS

Google Cookie:

- Google was the first search engine to use a cookie. Google set the standard and nowadays cookies are commonplace among search engines. This cookie places a unique ID number on your hard disk. Anytime you visit Google. user gets a Google cookie if a user doesn't already have one. If a user has one then it will read and record the unique ID number. Google con build a detailed list of your search terms over many years.

Cookie:

- Cookie (also know as HTIP cookie/browser cookie) is a small text file that contains a string of alphanumeric characters and is used for storing netizen's website preferences/authentication while visiting the some webpage again and again or also acts as identifier for server-based session - such browser mechanism of setting and reading cookies invites attackers to use these cookies as "Spywore.“

PROXY SERVERS AND ANONYMIZERS

- There are two types of cookies:
  - Persistent cookie is stored by the web browser into the cookie folder on the PC's hard disk. It remains under the cookie folder. which is maintained by the web browser.
  - Session cookie is a temporary cookie and does not reside on the PC once the browser is closed.

G-Zapper

- G-Zapper helps to protect users' ID and search history. G-Zapper reads the Google cookie installed on users' PC, displays the date it was installed, determines how long user searches have been tracked and displays Google searches. G-Zapper allows user to automatically delete or entirely block the Google search cookie from future installation.

DoubleClick

- It is a subsidiary of Google and provides Internet ad-serving services and paid search products listing *(DART* Search) and utilize the cookies, which are called DART cookie.
- The DART cookie is a persistent cookie, which consists of the name of the domain that has set the cookie, the lifetime of the cookie and a "value."
- DoubleClick's DART mechanism generates a unique series of characters for the "value" portion of the cookie. These DoubleClick DART cookies help marketers learn how well their Internet advertising campaigns or paid search listings perform. Many marketers and Internet websites use DoubleClick's DART technology to deliver and serve their advertisements or manage their paid search listings.

PHISHING

- “Phishing” refers to an attack using mail programs to deceive Internet users into disclosing confidential information that can be then exploited for illegal purposes.
- While checking electronic mail (E-Mail) one day a user finds a message from the bank threatening to close the bank account if he/she does not reply immediately.
- Although the message seems to be suspicious from the contents of the message, it is difficult to conclude that it is a fake/false E-Mail.
- This message and other such messages are examples of Phishing – in addition to stealing personal and financial data – and can infect systems with viruses and also a method of online ID theft in various cases.
- These messages look authentic and attempt to get users to reveal their personal information.
- It is believed that Phishing is an alternative spelling of “fishing,” as in “to fish for information.”
- The first documented use of the word “Phishing” was in 1996

PHISHING

- **How Phishing Works?**
- Phishers work in the following ways:
  - 1. Planning: Criminals, usually called as phishers, decide the target.
  - 2. Setup: Once phishers know which business/business house to spoof and who their victims.
  - 3. Attack: the phisher sends a phony message that appears to be from a reputable source.
  - 4. Collection: Phishers record the information of victims entering into webpages or pop-up windows.
  - 5. Identity theft and fraud: Phishers use the information that they have gathered to make illegal purchases or commit fraud.
- Nowadays, more and more organizations/institutes provide greater online access for their customers and hence criminals are successfully using Phishing techniques to steal personal information and conduct ID theft at a global level.

PASSWORD CRACKING

- Password is like a key to get an entry into computerized systems like a lock.
- Password cracking is a process of recovering passwords from data that have been stored in or transmitted by a computer system.
- Usually, an attacker follows a common approach – repeatedly making guesses for the password.
- The purpose of password cracking is as follows:
  1. To recover a forgotten password.
  2. As a preventive measure by system administrators to check for easily crackable passwords.
  3. To gain unauthorized access to a system.
- Manual password cracking is to attempt to logon with different passwords. The attacker follows the following steps:
  1. Find a valid user account such as an Administrator or Guest;
  2. create a list of possible passwords;
  3. rank the passwords from high to low probability;
  4. key-in each password;
  5. try again until a successful password is found.

PASSWORD CRACKING