VIT UNIVERSITY SCHOOL OF COMPUTER SCIENCE ENGINEERING

Chapter 1: ETHICAL HACKING

By
Dr. Ravi Verma

Contents To Be Discuss

- Types of Attacks in Network
- Web Based Attacks
  - DNS Spoofing
  - Session Hijacking
  - Phishing
  - Brute Force
  - DoS
  - Dictionary Attack
  - Other Attacks

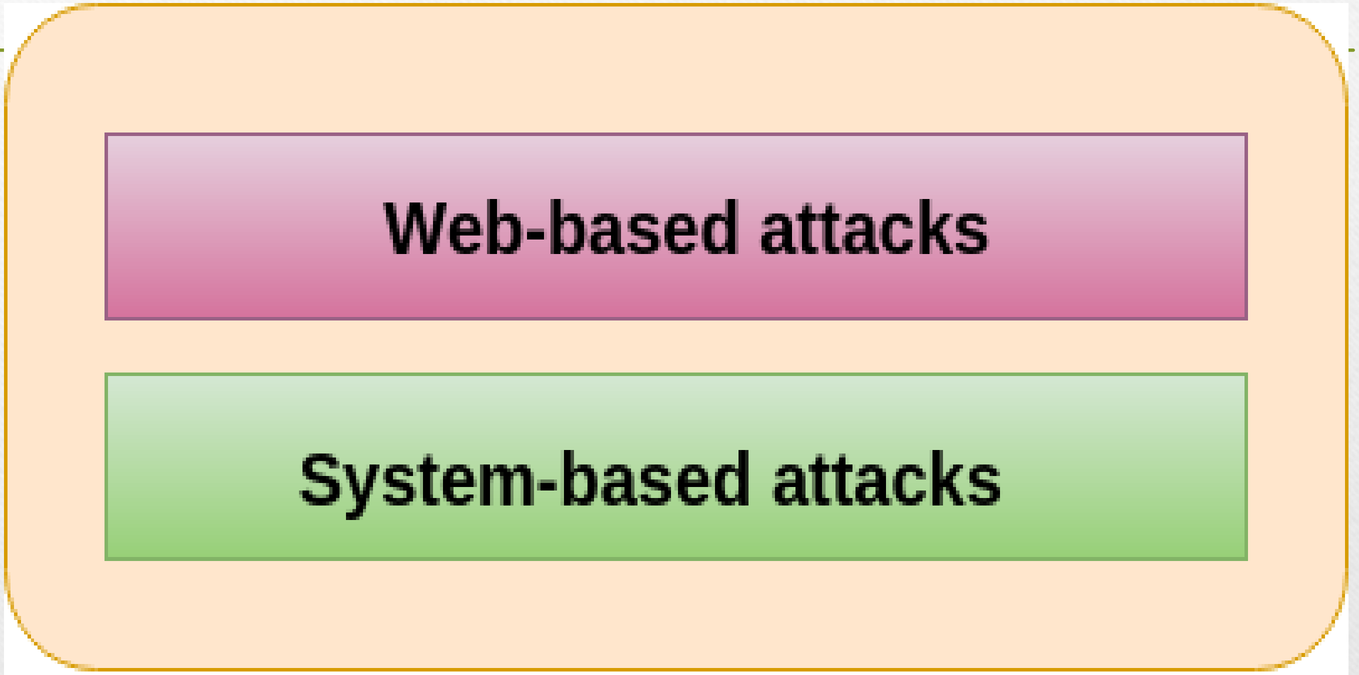
Contents To Be Discuss Cont....

- System Based Attacks
  - Virus
  - Worms
  - Trojan Horse
  - Back Door
  - Bots
  - Vulnerabilities in Information Security System
  - Hardware Vulnerabilities
  - Software Vulnerabilities
  - Network Vulnerabilities
  - Procedural Vulnerabilities
  - Ethical Hacking Terminologies

Types of Attacks in Network?

- A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.
- We are living in a digital era. Now a day, most of the people use computer and internet. Due to the dependency on digital things, the illegal computer activity is growing and changing like any type of crime.

Cyber-attacks can be classified into the following categories:



Classification of Cyber attacks

Web based Attacks

- These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-
- **Injection attacks**
- It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.
- **Example-** SQL Injection, code Injection, log Injection, XML Injection etc.

DNS Spoofing

- DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attackers? computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

Session Hijacking

- It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

Phishing

- Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

Brute force

It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

Denial of Service

- It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-

Denial of Service Cont..

- **Volume-based attacks-** Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.
- **Protocol attacks-** It consumes actual server resources, and is measured in a packet.
- **Application layer attacks-** Its goal is to crash the web server and is measured in request per second.

Dictionary attacks

- This type of attack stored the list of a commonly used password and validated them to get original password.

URL Interpretation

- It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

Other Attacks

File Inclusion attacks

- It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

Man in the middle attacks

- It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

System-based attacks

- These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

System-based attacks Cont..

- **Virus**
- It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

System-based attacks Cont..

- **Worm**
- It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

System-based attacks Cont..

- **Trojan horse**
- It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

System-based attacks Cont..

- **Backdoors**
- It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.
- **Bots**
- A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

Vulnerabilities in Information Security

- **Vulnerabilities** are weaknesses in a system that gives threats the opportunity to compromise assets. All systems have vulnerabilities. Even though the technologies are improving but the number of vulnerabilities are increasing such as tens of millions of lines of code, many developers, human weaknesses, etc. Vulnerabilities mostly happened because of Hardware, Software, Network and Procedural vulnerabilities.

Hardware Vulnerability

- A hardware vulnerability is a weakness which can used to attack the system hardware through physically or remotely. For examples:

1. Old version of systems or devices
2. Unprotected storage
3. Unencrypted devices, etc.

Software Vulnerability

- A software error happen in development or configuration such as the execution of it can violate the security policy. For examples:

1. Lack of input validation
2. Unverified uploads
3. Cross-site scripting
4. Unencrypted data, etc.

Network Vulnerability

A weakness happen in network which can be hardware or software.
For examples:

1. Unprotected communication
2. Malware or malicious software (e.g.: Viruses, Keyloggers, Worms, etc)
3. Social engineering attacks
4. Misconfigured firewalls

Procedural Vulnerability

- A weakness happen in an organization operational methods. For examples:

1. Password procedure – Password should follow the standard password policy.
2. Training procedure – Employees must know which actions should be taken and what to do to handle the security. Employees must never be asked for user credentials online. Make the employees know social engineering and phishing threats.

Ethical Hacking - Terminologies

- Following is a list of important terms used in the field of hacking
- **Adware** − Adware is software designed to force pre-chosen ads to display on your system.
- **Attack** − An attack is an action that is done on a system to get its access and extract sensitive data.
- **Back door** − A back door, or trap door, is a hidden entry to a computing device or software that bypasses security measures, such as logins and password protections.

Ethical Hacking – Terminologies Cont..

- **Bot** − A bot is a program that automates an action so that it can be done repeatedly at a much higher rate for a more sustained period than a human operator could do it. For example, sending HTTP, FTP or Telnet at a higher rate or calling script to create objects at a higher rate.
- **Botnet** − A botnet, also known as zombie army, is a group of computers controlled without their owners' knowledge. Botnets are used to send spam or make denial of service attacks.

Ethical Hacking – Terminologies Cont..

- **Brute force attack** − A brute force attack is an automated and the simplest kind of method to gain access to a system or website. It tries different combination of usernames and passwords, over and over again, until it gets in.
- **Buffer Overflow** − Buffer Overflow is a flaw that occurs when more data is written to a block of memory, or buffer, than the buffer is allocated to hold.
- **Clone phishing** − Clone phishing is the modification of an existing, legitimate email with a false link to trick the recipient into providing personal information.

Ethical Hacking – Terminologies Cont..

- **Cracker** − A cracker is one who modifies the software to access the features which are considered undesirable by the person cracking the software, especially copy protection features.
- **Denial of service attack (DoS)** − A denial of service (DoS) attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet.
- **DDoS** − Distributed denial of service attack.

Ethical Hacking – Terminologies Cont..

- **Exploit Kit** − An exploit kit is software system designed to run on web servers, with the purpose of identifying software vulnerabilities in client machines communicating with it and exploiting discovered vulnerabilities to upload and execute malicious code on the client.
- **Exploit** − Exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to compromise the security of a computer or network system.
- **Firewall** − A firewall is a filter designed to keep unwanted intruders outside a computer system or network while allowing safe communication between systems and users on the inside of the firewall.

Ethical Hacking – Terminologies Cont..

- **Keystroke logging** − Keystroke logging is the process of tracking the keys which are pressed on a computer (and which touchscreen points are used). It is simply the map of a computer/human interface. It is used by gray and black hat hackers to record login IDs and passwords. Keyloggers are usually secreted onto a device using a Trojan delivered by a phishing email.
- **Logic bomb** − A virus secreted into a system that triggers a malicious action when certain conditions are met. The most common version is the time bomb.
- **Malware** − Malware is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.

Ethical Hacking – Terminologies Cont..

- **Master Program** − A master program is the program a black hat hacker uses to remotely transmit commands to infected zombie drones, normally to carry out Denial of Service attacks or spam attacks.
- **Phishing** − Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking emails, in an attempt to gather personal and financial information from recipients.
- **Phreaker** − Phreakers are considered the original computer hackers and they are those who break into the telephone network illegally, typically to make free long distance phone calls or to tap phone lines.

Ethical Hacking – Terminologies Cont..

- **Spoofing** − Spoofing is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.
- **Spyware** − Spyware is software that aims to gather information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.
- **SQL Injection** − SQL injection is an SQL code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).
- **Threat** − A threat is a possible danger that can exploit an existing bug or vulnerability to compromise the security of a computer or network system.

Ethical Hacking – Terminologies Cont..

- **Trojan** − A Trojan, or Trojan Horse, is a malicious program disguised to look like a valid program, making it difficult to distinguish from programs that are supposed to be there designed with an intention to destroy files, alter information, steal passwords or other information.
- **Virus** − A virus is a malicious program or a piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.
- **Vulnerability** − A vulnerability is a weakness which allows a hacker to compromise the security of a computer or network system.
- **Worms** − A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself.

Ethical Hacking – Terminologies Cont..

- **Cross-site Scripting** − Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side script into web pages viewed by other users.
- **Zombie Drone** − A Zombie Drone is defined as a hi-jacked computer that is being used anonymously as a soldier or 'drone' for malicious activity, for example, distributing unwanted spam e-mails.

Question Please?

THANK YOU