



IT-ICT Department
L.J. Institute of Engineering Technology,
Ahmedabad



Cyber Security (2150002)

Semester : 5th
Academic Year : 2019-20

Unit 1

Vulnerability Scanning

Introduction

A vulnerability scanner is a computer program designed to assess computers, computer systems, networks or applications for known weaknesses. In plain words, these scanners are used to discover the weak points or poorly constructed parts. It's utilized for the identification and detection of vulnerabilities relating to mis-configured assets or flawed software that resides on a network-based asset such as a firewall, router, web server, application server, etc. Modern vulnerability scanners will allow for both authenticated and unauthenticated scans to occur.



Types of Vulnerability Scanner

Vulnerability scanners can be divided broadly into two groups: network-based scanners that run over the network, and host-based scanners that run on the target host itself.

NETWORK-BASED SCANNERS

A network-based scanner is usually installed on a single machine that scans a number of other hosts on the network. It helps detect critical vulnerabilities such as mis-configured firewalls, vulnerable web servers, risks associated with vendor-supplied software, and risks associated with network and systems administration.

Different types of network-based scanners include:

1. **Port Scanners** that determine the list of open network ports in remote systems;
2. **Web Server Scanners** that assess the possible vulnerabilities (e.g. potentially dangerous files or CGIs) in remote web servers;
3. **Web Application Scanners** that assess the security aspects of web applications (such as cross site scripting and SQL injection) running on web servers. It should be noted that web application scanners cannot provide comprehensive security checks on every aspect of a target web application. Additional manual checking (such as whether a login account is locked after a number of invalid login attempts) might be needed in order to supplement the testing of web applications.

HOST-BASED SCANNERS

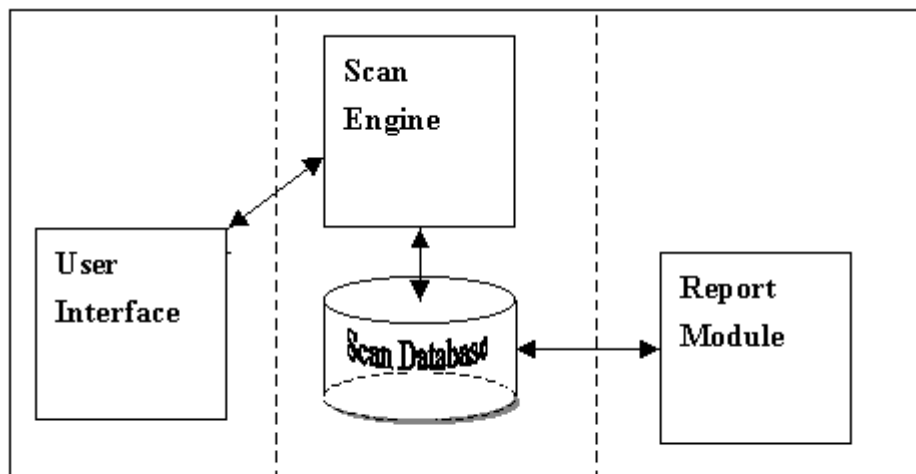
A host-based scanner is installed in the host to be scanned, and has direct access to low-level data, such as specific services and configuration details of the host's operating system. It can therefore provide insight into risky user activities such as using easily guessed passwords or even no password. It can also detect signs that an attacker has already compromised a system, including looking for suspicious file names, unexpected new system files or device files, and unexpected privileged programs. Host-based scanners can also perform baseline (or

file system) checks. Network-based scanners cannot perform this level of security check because they do not have direct access to the file system on the target host.

A database scanner is an example of a host-based vulnerability scanner. It performs detailed security analysis of the authorization, authentication, and integrity of database systems, and can identify any potential security exposures in database systems, ranging from weak passwords and security mis-configurations to Trojan horses.

The Architecture Of Vulnerability Scanners

In general, a vulnerability scanner is made up of four main modules, namely, a Scan Engine, a Scan Database, a Report Module and a User Interface.



Components of Scanner

1. The Scan Engine executes security checks according to its installed plug-ins, identifying system information and vulnerabilities. It can scan more than one host at a time and compares the results against known vulnerabilities.
2. The Scan Database stores vulnerability information, scan results, and other data used by scanner. The number of available plug-ins, and the updating frequency of plug-ins will vary depending on the corresponding vendor. Each plug-in might contain not only the test case itself, but also a vulnerability description, a Common Vulnerabilities and Exposures (CVE)² identifier; and even fixing instructions for a detected vulnerability. Scanners with an "auto-update" feature can download and install the latest set of plug-ins to the database automatically.
3. The Report Module provides different levels of reports on the scan results, such as detailed technical reports with suggested remedies for system administrators, summary reports for security managers, and high-level graph and trend reports for executives.
4. The User Interface allows the administrator to operate the scanner. It may be either a Graphical User Interface (GUI), or just a command line interface.

Types of vulnerability scanner :

- Port scanner (e.g. Nmap)
- Network vulnerability scanner (e.g. Nessus, SAINT, OpenVAS, INFRA Security Scanner)
- Web application security scanner (e.g. Nikto, Acunetix, Burp Suite, OWASP ZAP, w3af)
- Database security scanner
- Host based vulnerability scanner (Lynis)
- ERP security scanner
- Single vulnerability tests


A **port scanner** is an application designed to probe a server or host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify network services running on a host and exploit vulnerabilities. A port scan or portscan is a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port; this is not a nefarious process in and of itself.[1] The majority of uses of a port scan are not attacks, but rather simple probes to determine services available on a remote machine.

The Open Vulnerability Assessment System (OpenVAS) collects and manages security information for networks, devices, and systems. Its home page, including source code and installers, is at www.openvas.org. At its core, OpenVAS sweeps through a network to identify known network mis-configurations and known vulnerabilities associated with common services and software. Vulnerability detections are defined in scripts called Network Vulnerability Tests (NVTs).

SQL injection is a code injection technique, used to attack data-driven applications, in which nefarious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).[1] SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy.

Network Sniffer and Injection Tools

A network sniffer is a program that monitors and analyzes network traffic, detecting bottlenecks and problems. Using this information, a network manager can keep traffic flowing efficiently. 

A sniffer can also be used legitimately or illegitimately to capture data being transmitted on a

network. A network router reads every packet of data passed to it, determining whether it is intended for a destination within the router's own network or whether it should be passed further along the Internet. A router with a sniffer, however, may be able to read the data in the packet as well as the source and destination addresses. Sniffers are often used on academic networks to prevent traffic bottlenecks caused by file-sharing applications.

Network Sniffer Tools



Wireshark (formerly known as Ethereal) is widely recognized as the world's most popular network sniffer. It's a free, open source application that displays traffic data with color coding to indicate which protocol was used to transmit it.

On Ethernet networks, its user interface displays individual frames in a numbered list and highlights by separate colors whether they are sent through TCP, UDP, or other protocols. It also helps group together message streams being sent back and forth between a source and destination (which are normally intermixed over time with traffic from other conversations).

Wireshark supports traffic captures through a start/stop push button interface. The tool also contains various filtering options that limit what data is displayed and included in captures - a critical feature since traffic on most networks contain many different kinds of routine control messages that are usually not of interest.

Many different probing software applications have been developed over the years. Here are just a few examples:

tcpdump (a command line tool for Linux and other Unix-based operating systems)

CloudShark

Cain and Abel

Microsoft Message Analyzer

CommView

Omnipeek

Capsa

Ettcap

PRTG

Free Network Analyzer

NetworkMiner

IP Tools

Unit 2

Network Defence Tools

Firewall

Firewalls are not strictly hardware devices. The capability of a firewall, to deny or accept traffic, is often built in to devices like wireless access points and cable and DSL modems. It's also a part of almost all operating systems. At its core, firewall software examines traffic on a network interface to determine whether packets should be allowed to enter or leave the interface. Thus, firewall software blocks inbound connections to a system's services that shouldn't be exposed to other systems on a public Wi-Fi network.

How Firewall Protect the Network :

Most firewalls have three ways to enforce a rule for network traffic:

- **Accept** the packet and pass it on to its intended destination.
- **Deny** the packet and indicate the denial with an Internet Control Message Protocol (ICMP) message or similar acknowledgment to the sender. This provides explicit feedback that such traffic is not permitted through the firewall.
- **Drop** the packet without any acknowledgment. This ends the packet's life on the network.

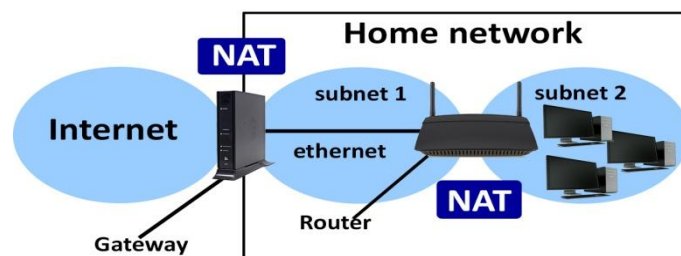
Stateful vs Stateless Firewall:

A **stateless firewall** examines individual packets in isolation from each other; it doesn't track whether related packets have arrived before or are coming after.


A **stateful firewall** places that packet in the context of related traffic and within a particular protocol, such as TCP/IP or FTP. This enables stateful firewalls to group individual packets together into concepts like connections, sessions, or conversations.

Network address translation

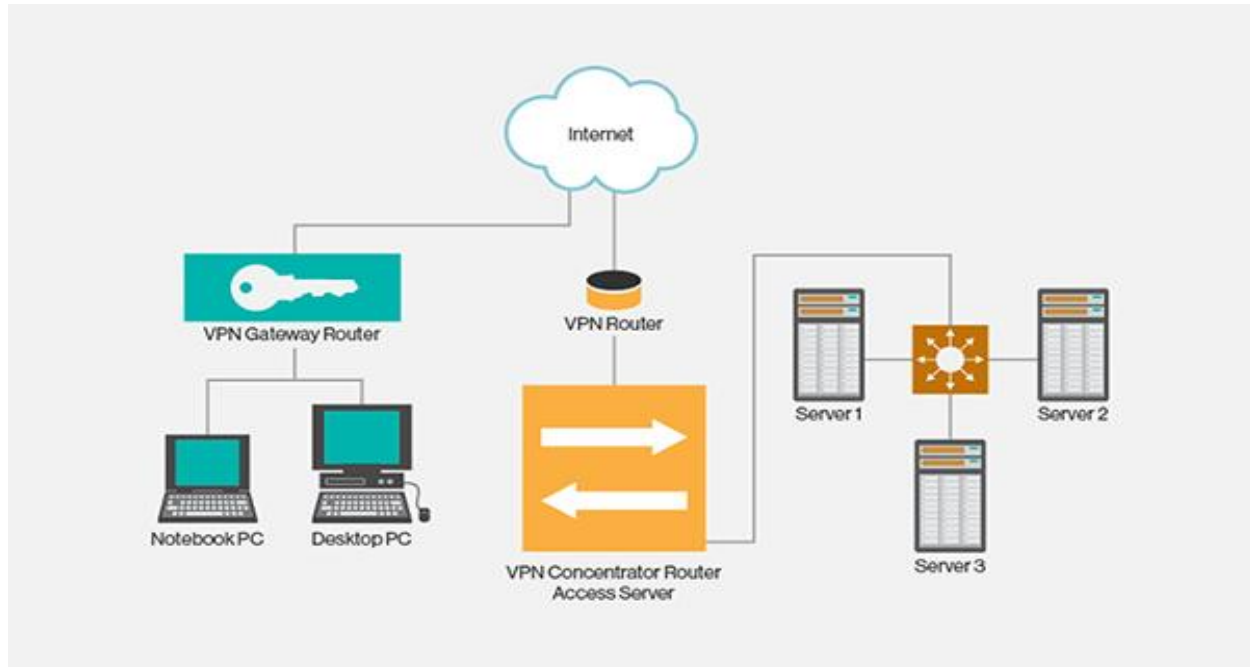
Network address translation (NAT) is a method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device. The technique was originally used for ease of rerouting traffic in IP networks without readdressing every host. In more advanced NAT implementations featuring IP masquerading, it has become a popular and essential tool in conserving global address space allocations in face of IPv4 address exhaustion by sharing one Internet-routable IP address of a NAT gateway for an entire private network.



Virtual Private Network

A **VPN**, or **Virtual Private Network**, is a secure tunnel between two or more devices. VPNs are used to protect private web traffic from snooping, interference, and censorship. 

A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN). From a user perspective, the resources available within the private network can be accessed remotely.



Snort: An Intrusion-Detection System

Snort is a network monitoring tool that watches traffic for signs of malicious activity (e.g., buffer overflows being executed against a service, command and control traffic from malware), suspicious activity (e.g., port scans and service enumeration), and anything else that you wish to look out for.

At its core, an intrusion-detection system (IDS) is a sniffer like tcpdump or Wireshark, but with specialized filters that attempt to identify malicious activity. A good IDS can find anything from a buffer overflow attack against an SSH server to the transmission of /etc/password files over FTP. Network administrators place these systems where they can best monitor traffic, such as a point where they can see all traffic through a firewall or see all traffic between network segments with different security contexts (e.g., production servers and developer systems). The IDS examines packets, looking for particular signatures or patterns that are associated with suspicious or prohibited activity. The IDS then reports on all traffic that matches those signatures. Snort is a robust IDS that runs on Unix-based and Windows systems. It is also completely free.

Unit 3

Scanning for web vulnerabilities Tools

Web Application Security Scanner is a software program which performs automatic black box testing on a web application and identifies security vulnerabilities. Scanners do not access the source code, they only perform functional testing and try to find security vulnerabilities.

These are the best open source web application penetration testing tools:

Scanning for web vulnerabilities

Nikto

Nikto, by Chris Sullo and David Lodge, is a Perl-based scanner that searches for known vulnerabilities in common web applications, looks for the presence of common files that have the potential to leak information about an application or its platform, and probes a site for indicators of common misconfigurations. It is an outgrowth of the

Use Nikto for assessing the security of a web application's deployment. The tool focuses on identifying vulns in commercial and open source web application frameworks. It won't be as helpful for assessing the security of a custom web application. For example, it may tell you that a site uses an outdated (and insecure) version of WordPress, but it won't be able to tell you if the blogging application you wrote from scratch is secure or not.

HTTP Utilities



The following tools serve as workhorses for making connections over HTTP or HTTPS. Alone, they do not find vulnerabilities or secure a system, but their functionality can be put to use to extend the abilities of a web vulnerability scanner, peek into SSL traffic, or encrypt client/server communication to protect it from network sniffers.

Curl



Where Netcat deserves bragging rights for being a flexible, all-purpose network tool, curl deserves considerable respect as a flexible tool for HTTP connections. It consists of a command-line tool (which is the focus of this section) and a high-performance, crossplatform, open source library. Its home page, <http://curl.haxx.se>, contains links to source code, documentation, and mailing lists. You'll find that the curl mailing lists are helpful, active lists regardless of whether you're trying to understand the command line or using one of the library's APIs.

OpenSSL



The S in HTTPS represents the security (Secure Sockets Layer) provided for the connection used to transport data; SSL establishes confidentiality by preventing eavesdroppers from sniffing the plaintext traffic and provides integrity by establishing a trusted identity of the web server to prevent intermediation attacks that try to manipulate traffic without being detected. It doesn't improve any other aspect of a site's security. A site that uses HTTPS everywhere remains as vulnerable to SQL injection and HTML injection as it would be using unencrypted HTTP instead.

The OpenSSL library is the most commonly used open source library for establishing encrypted connections. The openssl command is present by default on most Unix-based systems. Under Windows, you can use the command as provided by the Cygwin environment or you can build OpenSSL from source.

Stunnel

OpenSSL is excellent for one-way SSL conversions. Unfortunately, you can run into situations in which the client sends out HTTPS connections and cannot be downgraded to HTTP. In these cases, you need a tool that can either decrypt SSL or sit between the client and server and watch traffic in clear text. Stunnel provides this functionality. Install this tool with your system's package manager or download it from <https://www.stunnel.org>.

You can also use stunnel to wrap SSL around any network service. For example, you could set up stunnel to manage connections to an Internet Message Access Protocol (IMAP) service to provide encrypted access to e-mail (you would also need stunnel to manage the client side as well). Fortunately, modern operating systems and services recognize the importance of encrypting connections with SSL/TLS. Stunnel is now needed less as a "patch" for plaintext services and more as a tool for redirecting traffic in order to manipulate it for security testing.

Application Inspection

Zed Attack Proxy

Zed Attack Proxy is also known as ZAP. This tool is open source and is developed by AWASP. It is available for Windows, Unix/Linux and Macintosh platforms. I personally like this tool. It can be used to find a wide range of vulnerabilities in web applications. The tool is very simple and easy to use. Even if you are new to penetration testing, you can easily use this tool to start learning penetration testing of web applications.

These are the key functionalities of ZAP:

- Intercepting Proxy
- Automatic Scanner
- Traditional but powerful spiders
- Fuzzer
- Web Socket Support
- Plug-n-hack support
- Authentication support
- REST based API
- Dynamic SSL certificates
- Smartcard and Client Digital Certificates support

SQLMap

SQLMap is another popular open source penetration testing tool. It automates the process of finding and exploiting SQL injection vulnerability in a website's database. It has a powerful detection engine and many useful features. So, a penetration tester can easily perform SQL injection check on a website.

It supports range of database servers including MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase and SAP MaxDB. It offers full support to 6 kinds of SQL injection techniques: time-based blind, boolean-based blind, error-based, UNION query, stacked queries and out-of-band.

Password Cracking and Brute Force Tools

Password OpSec

We can't control what happens to our passwords once they leave our phone, laptop, or other device. In fact, we can rarely control what happens to them once they leave our fingertips and are typed on a keyboard or touchscreen. But we can follow some basic Operations Security (OpSec) in choosing, managing, and using passwords. The following list of recommendations is biased toward users of web applications, but the principles should be applicable to using passwords in general:

- Keep your system up to date. This reduces your exposure to compromise by malware and viruses.
- Do not use the unique password of your primary e-mail account for any other account you create. Most web apps rely on e-mail for password reset and recovery mechanisms. E-mail accounts are a prime target for theft. Losing access to your e-mail account (or unwittingly divulging the account's password to someone else) means not only losing contact with friends and family via that account, but an attacker may be able to leverage the e-mail to access other accounts.
- Enable multifactor authentication whenever a web app offers support for it. This helps protect your account from compromise even if your password is weak (and easily guessed) or disclosed (by a server-side hack). Avoid entering your credentials on public or shared computers. The security of such systems cannot be guaranteed and they are excellent targets for hackers to

install keyloggers.

- Avoid authenticating to web apps when using public Wi-Fi networks. Or at least restrict your activity to apps that use HTTPS for all communication. See Chapter 10 for reasons why this matters.
- Avoid any web site whose password recovery mechanism e-mails your original password rather than a new, temporary one. Sending an e-mail with your original password means the site does not hash passwords (against all recommended security practices) and its developers are ignorant of secure programming.
- Choose a password that isn't based on easily discoverable personal information such as school names, demographic details, a favorite topic you always blog about, or pets. If you're a pet, don't use any of this information about your human. On the Internet, no one knows you're a dog. Make sure they don't know your password either.
- If you use your social media account (e.g., Facebook or Twitter) as the ID for other apps, follow the same advice given for your e-mail password. Plus, always make sure the login prompt you receive points to the correct domain for the social media site.

Pwdump

The original pwdump program was written by Jeremy Allison in 1997 to demonstrate how to extract password hashes from the Windows Registry. Pwdump2, by Todd Sabin, followed a year later; it expanded on the original program's capabilities. Since then, other developers have created many versions of pwdump to keep up with various updates to Windows. But they all rely on extracting hashes from the Registry, SAM file, or the lsass.exe process's memory space. The lsass.exe process handles the Local Security Subsystem Service; it's essentially responsible for authentication, which is why its memory contains the system's password hashes.

THC-Hydra

THC-Hydra (aka simply Hydra) easily surpasses the majority of brute-force tools available on the Internet for two reasons: it is fast, and it targets authentication mechanisms for several dozen protocols. Its source code and documentation are available from <https://www.thc.org/thc-hydra/>. The Hacker's Choice web site (<https://www.thc.org>) contains many security tools, although some of them have not been maintained for several years. Even so, its tools, papers, and information are informative. Compile Hydra from source or look for it in your system's package manager. It will compile under any Unix-based system and Cygwin.

Unit 4

Introduction to Cyber Crime and law

Cyber space:



Cyberspace can be defined as an intricate environment that involves interactions between people, software, and services. It is maintained by the worldwide distribution of information and communication technology devices and networks.

With the benefits carried by the technological advancements, the cyberspace today has become a common pool used by citizens, businesses, critical information infrastructure, military and governments in a fashion that makes it hard to induce clear boundaries among these different groups. The cyberspace is anticipated to become even more complex in the upcoming years, with the increase in networks and devices connected to it.

Cyber crime

Cyber crime is the use of computers and networks to perform illegal activities such as spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc. Most cybercrimes are committed through the internet. Some cybercrimes can also be carried out using Mobile phones via SMS and online chatting applications.

Type of Cybercrime

The following list presents the common types of cybercrimes:

Computer Fraud: Intentional deception for personal gain via the use of computer systems.

Privacy violation: Exposing personal information such as email addresses, phone number, account details, etc. on social media, websites, etc.

Identity Theft: Stealing personal information from somebody and impersonating that person.

Sharing copyrighted files/information: This involves distributing copyright protected files such as eBooks and computer programs etc.

Electronic funds transfer: This involves gaining an un-authorized access to bank computer networks and making illegal fund transfers.

Electronic money laundering: This involves the use of the computer to launder money.

ATM Fraud: This involves intercepting ATM card details such as account number and PIN numbers. These details are then used to withdraw funds from the intercepted accounts.

Denial of Service Attacks: This involves the use of computers in multiple locations to attack servers with a view of shutting them down.

Spam: Sending unauthorized emails. These emails usually contain advertisements.

What is Ethical Hacking?

Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses. Ethical hackers must abide by the following rules.

Get written permission from the owner of the computer system and/or computer network before hacking.

Protect the privacy of the organization been hacked.

Transparently report all the identified weaknesses in the computer system to the organization.

Inform hardware and software vendors of the identified weaknesses.

Why Ethical Hacking?

Information is one of the most valuable assets of an organization. Keeping information secure can protect an organization's image and save an organization a lot of money.

Hacking can lead to loss of business for organizations that deal in finance such as PayPal. Ethical hacking puts them a step ahead of the cyber criminals who would otherwise lead to loss of business.

Legality of Ethical Hacking

Ethical Hacking is legal if the hacker abides by the rules stipulated in the above section on the definition of ethical hacking. The International Council of E-Commerce Consultants (EC-Council) provides a certification program that tests individual's skills. Those who pass the examination are awarded with certificates. The certificates are supposed to be renewed after some time.

The I.T. Act, 2000 defines the terms –

- access in computer network in **section 2(a)**
- computer in **section 2(i)**
- computer network in **section (2j)**
- data in **section 2(0)**
- information in **section 2(v).**

To understand the concept of Cyber Crime, you should know these laws. The object of offence or target in a cyber-crime are either the computer or the data stored in the computer.

Types of Cyber crime:





1. Hacking:

Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access. Example of Hacking: Using password cracking algorithm to gain access to a system. Computers have become mandatory to run a successful businesses. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. Hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cyber crimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

Who is a Hacker? Types of Hackers

A Hacker is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.

Hackers are classified according to the intent of their actions. The following list classifies hackers according to their intent.

Symbol	Description
	Ethical Hacker (White hat): A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration Testing and vulnerability assessments.
	Cracker (Black hat): A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.
	Grey hat: A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.
	Script kiddies: A non-skilled person who gains access to computer systems using already made tools.



Hacktivist: A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.



Phreaker: A hacker who identifies and exploits weaknesses in telephones instead of computers.

2. Virus dissemination

- Viruses are computer programs that attach themselves to or infect a system or files, and have a tendency to circulate to other computers on a network. They disrupt the computer operation and affect the data stored – either by modifying it or by deleting it altogether.
- “Worms” unlike viruses don’t need a host to cling on to. They merely replicate until they eat up all available memory in the system. The term “worm” is sometimes used to mean selfreplicating “malware” (MALicious softWARE).
- These terms are often used interchangeably in the context of the hybrid viruses/worms that dominate the current virus scenario. “Trojan horses” are different from viruses in their manner of propagation.

3. Logic bombs

- A logic bomb, also known as “slag code”, is a malicious piece of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event. It’s not a virus, although it usually behaves in a similar manner. It is stealthily inserted into the program where it lies dormant until specified conditions are met.
- Malicious software such as viruses and worms often contain logic bombs which are triggered at a specific payload or at a predefined time.
- The payload of a logic bomb is unknown to the user of the software, and the task that it executes unwanted. Program codes that are scheduled to execute at a particular time are known as “time-bombs”. For example, the infamous “Friday the 13th” virus which attacked the host systems only on specific dates; it “exploded” (duplicated itself) every Friday that happened to be the thirteenth of a month, thus causing system slowdowns.
- There’s another use for the type of action carried out in a logic bomb “explosion” – to make restricted software trials. The embedded piece of code destroys the software after a defined period of time or renders it unusable until the user pays for its further use. Although this piece of code uses the same technique as a logic bomb, it has a non-destructive, non-malicious and user-transparent use, and is not typically referred to as one.

4. Denial-of-Service attack

- A Denial-of-Service (DoS) attack is an explicit attempt by attackers to deny service to intended users of that service. It involves flooding a computer resource with more requests than it can handle consuming its available bandwidth which results in server overload. This causes the resource (e.g. a web server) to crash or slow down significantly so that no one can access it.
- Using this technique, the attacker can render a web site inoperable by sending massive amounts of traffic to the targeted site. A site may temporarily malfunction or crash completely, in any case resulting in inability of the system to communicate adequately. DoS attacks violate the acceptable use policies of virtually all internet service providers.
- Another variation to a denial-of-service attack is known as a “Distributed Denial of Service” (DDoS) attack wherein a number of geographically widespread perpetrators flood the network traffic. Denial-of-Service attacks typically target high profile web site servers belonging to banks and credit card payment gateways. Websites of companies such as Amazon, CNN, Yahoo, Twitter and eBay! are not spared either.

5. Phishing

- This a technique of extracting confidential information such as credit card numbers and username password combos by masquerading as a legitimate enterprise. Phishing is typically carried out by email spoofing. You’ve probably received email containing links to legitimate appearing websites. You probably found it suspicious and didn’t click the link. Smart move.
- The malware would have installed itself on your computer and stolen private information. Cyber-criminals use social engineering to trick you into downloading malware off the internet or make you fill in your personal information under false pretenses. A phishing scam in an email message can be evaded by keeping certain things in mind.
 - Look for spelling mistakes in the text. Cyber-criminals are not known for their grammar and spelling.
 - Hover your cursor over the hyperlinked URL but don’t click. Check if the address matches with the one written in the message.
 - Watch out for fake threats. Did you receive a message saying “Your email account will be closed if you don’t reply to this email”? They might trick you by threatening that your security has been compromised.
 - Attackers use the names and logos of well-known web sites to deceive you. The graphics and the web addresses used in the email are strikingly similar to the legitimate ones, but they lead you to phony sites.

6. Email bombing and spamming

- Email bombing is characterized by an abuser sending huge volumes of email to a target address resulting in victim's email account or mail servers crashing. The message is meaningless and excessively long in order to consume network resources. If multiple accounts of a mail server are targeted, it may have a denial-of-service impact. Such mail arriving frequently in your inbox can be easily detected by spam filters. Email bombing is commonly carried out using botnets (private internet connected computers whose security has been compromised by malware and under the attacker's control) as a DDoS attack.

7. Web jacking

- Web jacking derives its name from "hijacking". Here, the hacker takes control of a web site fraudulently. He may change the content of the original site or even redirect the user to another fake similar looking page controlled by him. The owner of the web site has no more control and the attacker may use the web site for his own selfish interests. Cases have been reported where the attacker has asked for ransom, and even posted obscene material on the site.
- The web jacking method attack may be used to create a clone of the web site, and present the victim with the new link saying that the site has moved. Unlike usual phishing methods, when you hover your cursor over the link provided, the URL presented will be the original one, and not the attacker's site. But when you click on the new link, it opens and is quickly replaced with the malicious web server. The name on the address bar will be slightly different from the original website that can trick the user into thinking it's a legitimate site. For example, "gmail" may direct you to "gmali". Notice the one in place of 'L'. It can be easily overlooked.

8. Cyber stalking

- Cyber stalking is a new form of internet crime in our society when a person is pursued or followed online. A cyber stalker doesn't physically follow his victim; he does it virtually by following his online activity to harvest information about the stalkee and harass him or her and make threats using verbal intimidation. It's an invasion of one's online privacy.
- Cyber stalking uses the internet or any other electronic means and is different from offline stalking, but is usually accompanied by it. Most victims of this crime are women who are stalked by men and children who are stalked by adult predators and pedophiles. Cyber stalkers thrive on inexperienced web users who are not well aware of netiquette and the rules of internet safety. A cyber stalker may be a stranger, but could just as easily be someone you know.
- Cyber stalking is done in two primary ways:

- **Internet Stalking:** Here the stalker harasses the victim via the internet. Unsolicited email is the most common way of threatening someone, and the stalker may even send obscene content and viruses by email. However, viruses and unsolicited telemarketing email alone do not constitute cyber stalking. But if email is sent repeatedly in an attempt to intimidate the recipient, they may be considered as stalking. Internet stalking is not limited to email; stalkers can more comprehensively use the internet to harass the victims. Any other cyber-crime that we've already read about, if done with an intention to threaten, harass, or slander the victim may amount to cyber stalking.
- **Computer Stalking:** The more technologically advanced stalkers apply their computer skills to assist them with the crime. They gain unauthorised control of the victim's computer by exploiting the working of the internet and the Windows operating system. Though this is usually done by proficient and computer savvy stalkers, instructions on how to accomplish this are easily available on the internet.

9. Data diddling

- Data Diddling is unauthorized altering of data before or during entry into a computer system, and then changing it back after processing is done. Using this technique, the attacker may modify the expected output and is difficult to track. In other words, the original information to be entered is changed, either by a person typing in the data, a virus that's programmed to change the data, the programmer of the database or application, or anyone else involved in the process of creating, recording, encoding, examining, checking, converting or transmitting data.

10. Identity Theft and Credit Card Fraud

- Identity theft occurs when someone steals your identity and pretends to be you to access resources such as credit cards, bank accounts and other benefits in your name. The imposter may also use your identity to commit other crimes. "Credit card fraud" is a wide ranging term for crimes involving identity theft where the criminal uses your credit card to fund his transactions. Credit card fraud is identity theft in its simplest form. The most common case of credit card fraud is your pre-approved card falling into someone else's hands.
- He can use it to buy anything until you report to the authorities and get your card blocked. The only security measure on credit card purchases is the signature on the receipt but that can very easily be forged. However, in some countries the merchant may even ask you for an ID or a PIN. Some credit card companies have software to estimate the probability of fraud. If an unusually large transaction is made, the issuer may even call you to verify.

Unit 5

Introduction to Cyber Crime Investigation

Firewalls and Packet Filters:

- During network communication, a node transmits a packet that is filtered and matched with predefined rules and policies. Once matched, a packet is either accepted or denied.
- Packet filtering checks source and destination IP addresses. If both IP addresses match, the packet is considered secure and verified. Because the sender may use different applications and programs, packet filtering also checks source and destination protocols, such as User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). Packet filters also verify source and destination port addresses.
- Some packet filters are not intelligent and unable to memorize used packets. However, other packet filters can memorize previously used packet items, such as source and destination IP addresses.
- Packet filtering is usually an effective defense against attacks from computers outside a local area network (LAN). As most routing devices have integrated filtering capabilities, packet filtering is considered a standard and cost-effective means of security.

Password cracking :

In cryptanalysis and computer security, password cracking is the process of recovering passwords from data that have been stored in or transmitted by a computer system. A common approach (brute-force attack) is to try guesses repeatedly for the password and check them against an available cryptographic hash of the password.

The purpose of password cracking might be to help a user recover a forgotten password (installing an entirely new password is less of a security risk, but it involves System Administration privileges), to gain unauthorized access to a system, or as a preventive measure by system administrators to check for easily crackable passwords. On a file-by-file basis, password cracking is utilized to gain access to digital evidence for which a judge has allowed access but the particular file's access is restricted.

Spyware

Spyware is software that aims to gather information about a person or organization without their knowledge, that may send such information to another entity without the consumer's consent, or that asserts control over a device without the consumer's knowledge.

Spyware is mostly used for the purposes of tracking and storing Internet users' movements on the Web and serving up pop-up ads to Internet users. Whenever spyware is used for malicious purposes, its presence is typically hidden from the user and can be difficult to detect. Some spyware, such as keyloggers, may be installed by the owner of a shared, corporate, or public computer intentionally in order to monitor users.

Keylogger

A keylogger (short for keystroke logger) is software that tracks or logs the keys struck on your keyboard, typically in a covert manner so that you don't know that your actions are being monitored. This is usually done with malicious intent to collect your account information, credit card numbers, user names, passwords, and other private data.

Legitimate uses do exist for keyloggers. Parents can monitor their children's online activity or law enforcement may use it to analyze and track incidents linked to the use of personal computers, and employers can make sure their employees are working instead of surfing the web all day.

Viruses

A computer virus is a type of malware that propagates by inserting a copy of itself into and becoming part of another program. It spreads from one computer to another, leaving infections as it travels. Viruses can range in severity from causing mildly annoying effects to damaging data or software and causing denial-of-service (DoS) conditions. Almost all viruses are attached to an executable file, which means the virus may exist on a system but will not be active or able to spread until a user runs or opens the malicious host file or program. When the host code is executed, the viral code is executed as well. Normally, the host program keeps functioning after it is infected by the virus. However, some viruses overwrite other programs with copies of themselves, which destroys the host program altogether. Viruses spread when the software or document they are attached to is transferred from one computer to another using the network, a disk, file sharing, or infected e-mail attachments.

Worms

Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate. To spread, worms either exploit a vulnerability on the target system or use some kind of social engineering to trick users into executing them. A worm enters a computer through a vulnerability in the system and takes advantage of file-transport or information-transport features on the system, allowing it to travel unaided.

Trojans

A Trojan is another type of malware named after the wooden horse the Greeks used to infiltrate Troy. It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems. After it is activated, it can achieve any number of attacks on the host, from irritating the user (popping up windows or changing desktops) to damaging the host (deleting files, stealing data, or activating and spreading other malware, such as viruses). Trojans are also known to create back doors to give malicious users access to the system.

Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate. Trojans must spread through user interaction such as opening an e-mail attachment or downloading and running a file from the Internet.

Back Door

A back door is an undocumented way of accessing a system, bypassing the normal authentication mechanisms. Some back doors are placed in the software by the original programmer and others are placed on systems through a system compromise, such as a virus or worm. Usually, attackers use back doors for easier and continued access to a system after it has been compromised.

Buffer-overflow

In a buffer-overflow attack, the extra data sometimes holds specific instructions for actions intended by a hacker or malicious user; for example, the data could trigger a response that damages files, changes data or unveils private information.

Attacker would use a buffer-overflow exploit to take advantage of a program that is waiting on a user's input. There are two types of buffer overflows: stack-based and heap-based. Heap-based, which are difficult to execute and the least common of the two, attack an application by flooding the memory space reserved for a program. Stack-based buffer overflows, which are more common among attackers, exploit applications and programs by using what is known as a stack: memory space used to store user input.

Attack on Wireless Network

In a wired network, packets of information are transferred along a physical medium, such as a copper cable or fiber optics. In a wireless setup, your data is quite literally broadcast through the air around you. Furthermore, physical access is not required to gain access to a network. What this means is that cyber criminals now have new ways to wreak havoc on your network infrastructure. Let's take a look at these wireless attacks.

TYPES OF WIRELESS ATTACKS

Wireless Attacks can come at you through different methods. For the most part you need to worry about WiFi. Some methods rely on tricking users, others use brute force, and some look for people who don't bother to secure their network. Many of these attacks are intertwined with each other in real world use. Here are some of the kinds of attacks you could encounter:

Packet Sniffing: When information is sent back and forth over a network, it is sent in what we call packets. Since wireless traffic is sent over the air, it's very easy to capture. Quite a lot of traffic (FTP, HTTP, SNMP, etc.) is sent in the clear, meaning that there is no encryption and files

are in plain text for anyone to read. So using a tool like Wireshark allows you to read data transfers in plain text! This can lead to stolen passwords or leaks of sensitive information quite easily. Encrypted data can be captured as well, but it's obviously much harder for an attacker to decipher the encrypted data packets.

Rogue Access Point: When an unauthorized access point (AP) appears on a network, it is referred to as a rogue access point. These can pop up from an employee who doesn't know better, or a person with ill intent. These APs represent a vulnerability to the network because they leave it open to a variety of attacks. These include vulnerability scans for attack preparation, ARP poisoning, packet captures, and Denial of Service attacks.

Password Theft: When communicating over wireless networks, think of how often you log into a website. You send passwords out over the network, and if the site doesn't use SSL or TLS, that password is sitting in plain text for an attacker to read. There are even ways to get around those encryption methods to steal the password. I'll talk about this with man in the middle attacks.

Man in the Middle Attack: It's possible for hackers to trick communicating devices into sending their transmissions to the attacker's system. Here they can record the traffic to view later (like in packet sniffing) and even change the contents of files. Various types of malware can be inserted into these packets, e-mail content could be changed, or the traffic could be dropped so that communication is blocked.

Jamming: There are a number of ways to jam a wireless network. One method is flooding an AP with deauthentication frames. This effectively overwhelms the network and prevents legitimate transmissions from getting through. This attack is a little unusual because there probably isn't anything in it for the hacker. One of the few examples of how this could benefit someone is through a business jamming their competitors WiFi signal. This is highly illegal (as are all these attacks), so businesses would tend to shy away from it. If they got caught they would be facing serious charges.

War Driving: War driving comes from an old term called war dialing, where people would dial random phone numbers in search of modems. War driving is basically people driving around looking for vulnerable APs to attack. People will even use drones to try and hack APs on higher floors of a building. A company that owns multiple floors around ten stories up might assume nobody is even in range to hack their wireless, but there is no end to the creativity of hackers!

Bluetooth Attacks: There are a variety of Bluetooth exploits out there. These range from annoying pop up messages, to full control over the a victims Bluetooth enabled device. Check out this blog post on hacking bluetooth for an in depth look.