Ethical Hacking(Unit 1 & 2), Integrated Ethical Hacking Course, VelTech University, Chennai(Notes for students)

Presentation · February 2024

CITATIONS
0

READS
128

1 author:

Arun Anoop Mandankandy
Vivekananda College of Engineering & Technology
71 PUBLICATIONS **89** CITATIONS

SEE PROFILE

Ethical Hacking(Unit 1 & 2)

Dr.Arun Anoop M CEH CHFI
Associate Professor
Dept. of CSE
SoC, Veltech University, Chennai.

https://ciet.nic.in/upload/cyber%20safety%20and%20security.pdf

Module-1

- **Introduction to Ethical Hacking**
- **Penetration testing**
- **TCP/IP concepts**
- **EH Essential terminologies**
- **Malicious software**
- **Protection against malware attacks**
- **Physical security**
- **Security policies and procedures.**

https://www.greycampus.com/opencampus/ethical-hacking/penetration-testing

Ethical Hacking

- What is Hacking?
- What is Ethical Hacking?
- Who is an Ethical Hacker?

Introduction to Ethical Hacking

- CIA Triangle
- Important characteristics of Information
- Security, Functionality and Usability Triangle
- Phases of Hacking
- Different types of attacks
- Vulnerability Assessment
- Penetration Testing
- Information Security Laws, Standards and frameworks

Malware Threats

- Introduction to Malware Threats and its Types
- Virus
- Trojans
- Worms
- Rootkits, Spyware and Ransomware
- How to Detect Malicious Software

Ethical Hacking ×

What is Hacking?

What is Ethical Hacking?

Who is an Ethical Hacker?

Who is an Ethical Hacker?

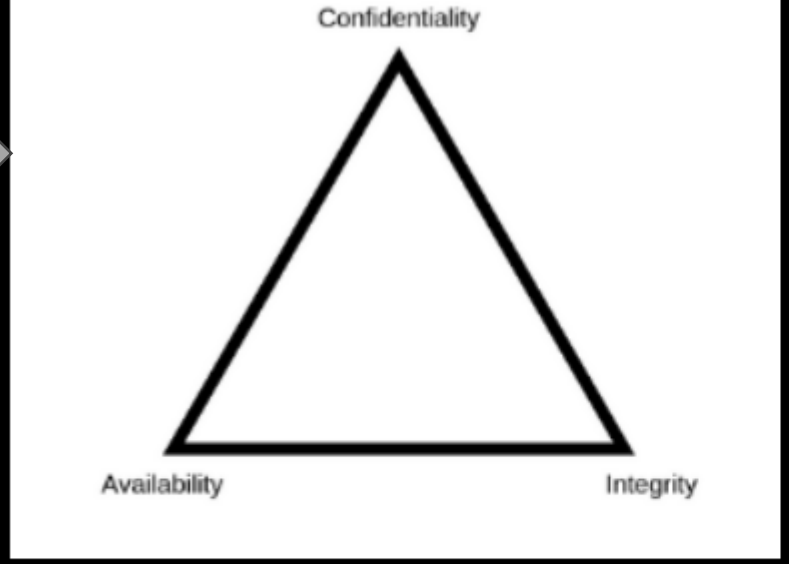
An Ethical Hacker is a skilled professional who has excellent technical knowledge and skills and knows how to identify and exploit vulnerabilities in target systems. He works with the permission of the owners of systems. An ethical Hacker must comply with the rules of the target organization or owner and the law of the land and their aim is to assess the security posture of a target organization/system.

Ethical Hacking sometimes called as Penetration Testing is an act of intruding/penetrating into system or networks to find out threats, vulnerabilities in those systems which a malicious attacker may find and exploit causing loss of data, financial loss or other major damages. The purpose of ethical hacking is to improve the security of the network or systems by fixing the vulnerabilities found during testing. Ethical hackers may use the same methods and tools used by the malicious hackers but with the permission of the authorized person for the purpose of improving the security and defending the systems from attacks by malicious users.
Ethical hackers are expected to report all the vulnerabilities and weakness found during the process to the management.

Hacking is the process of identifying and exploiting weakness in a system or a network to gain unauthorized access to data and system resources. It can also be defined as an unauthorized intrusion into the information systems/networks by an attacker by compromising the security. Example of Hacking: Exploiting the weakness of default password to gain access to the data stored inside the system.

Introduction to Ethical Hacking

- CIA Triangle
- Important characteristics of Information
- Security, Functionality and Usability Triangle
- Phases of Hacking
- Different types of attacks
- Vulnerability Assessment
- Penetration Testing
- Information Security Laws, Standards and frameworks



Untitled design.png 13.87 KB

CIA Triangle guides different information security policies for an organization. This is used to achieve the correct balance of these three attributes for the better security of an organization.

Introduction to Ethical Hacking ×

- CIA Triangle
- Important characteristics of Information
- Security, Functionality and Usability Triangle
- Phases of Hacking
- Different types of attacks
- Vulnerability Assessment
- Penetration Testing
- Information Security Laws, Standards and frameworks

1. Confidentiality

Confidentiality ensures that an Information is accessible to only an authorized user. The main pupose of confidentiality is to protect the sensitive information from reaching the wrong hands.It is used to maintain the privacy of the people. Encryption is a good example of confidentiality.

2. Availability

Information should be available to an authorised person when it is requested for. It is the guarantee of access to the authorised individual to information. Keeping all the hardware and software up to date and keeping back up, taking proper recovery measures will ensure availability of data.

3. Integrity

Integrity maintains the correctness or accuracy of the information while the data is in transit, storage or processing. It is the guarantee that information is trust worthy and not tampered. This attribute ensures that an unauthorised person will not be able to modify the data.
RSA digital signature, SHA1 hash codes are good examples.

4. Authentication

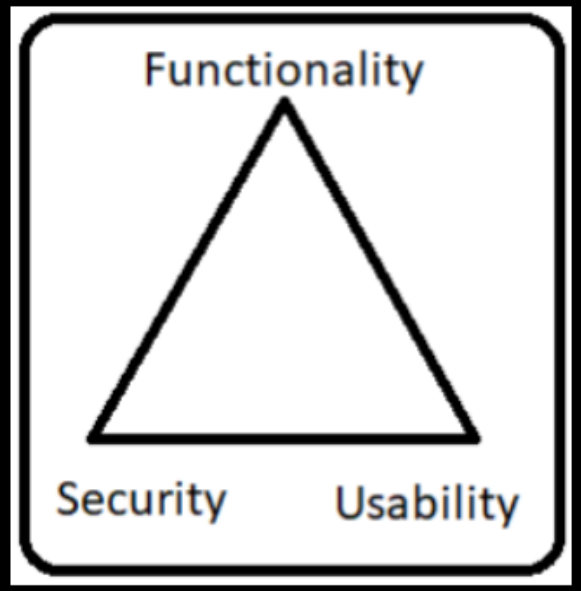
It is verifying whether the user, data, transactions involved is genuine. This attribute ensures that only genuine or right people are given access to the information. Login mechanisms can be used to verify the authenticity of users

5. Non-Repuditiation

This is a property of information which is used to holds a person responsible for the information he sent or received. In future, he cannot deny his role in sending or receiving the information.

Introduction to Ethical Hacking

- CIA Triangle
- Important characteristics of Information
- Security, Functionality and Usability Triangle
- Phases of Hacking
- Different types of attacks
- Vulnerability Assessment
- Penetration Testing
- Information Security Laws, Standards and frameworks



Some important terms to consider in hacking are

Threat: Anything that has potential to cause harm. There are various threats available to system threats, Network threats, application threats, cloud threats, malicious files threats etc.

Vulnerability: A weakness or a flaw in the system which an attacker may find and exploit. An updated OS, Default Passwords, Unencrypted protocols are all good examples of vulnerabilities.

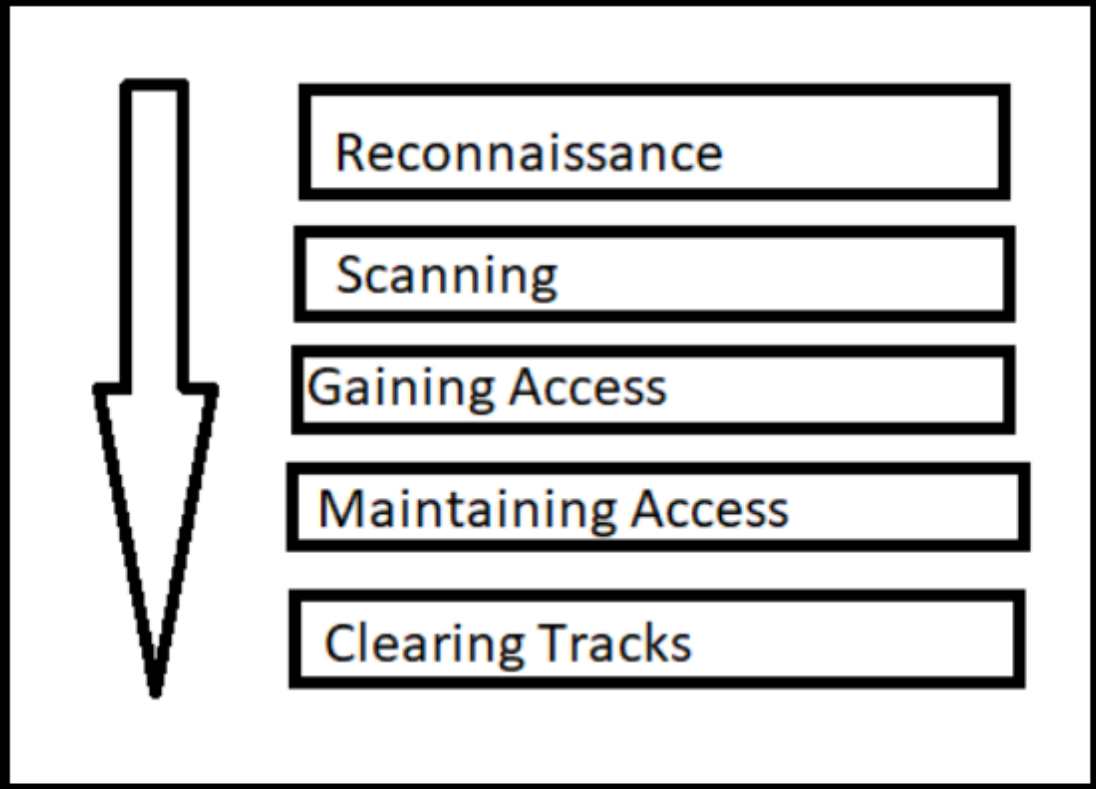
Attack: Method followed by a hacker/Individual to break into the system. Denial of service attack, Misconfiguration attacks, Operating system attacks, Virus, and Worms are all example of Attacks.

Attack vectors: Path or means by an attacker gains access to an information system to perform malicious activities.

Introduction to Ethical Hacking ×

- CIA Triangle
- Important characteristics of Information
- Security, Functionality and Usability Triangle
- Phases of Hacking
- Different types of attacks
- Vulnerability Assessment
- Penetration Testing
- Information Security Laws, Standards and frameworks

There are mainly 5 phases in hacking. Not necessarily a hacker has to follow these 5 steps in a sequential manner. It's a stepwise process and when followed yields a better result.



1. Reconnaissance:

This is the first step of Hacking. It is also called as Footprinting and information gathering Phase. This is the preparatory phase where we collect as much information as possible about the target. We usually collect information about three groups,

Introduction to Ethical Hacking ×

CIA Triangle

Important characteristics of Information

Security, Functionality and Usability Triangle

Phases of Hacking

Different types of attacks

Vulnerability Assessment

Penetration Testing

Information Security Laws, Standards and frameworks

1. Network
2. Host
3. People involved

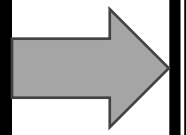
There are two types of Footprinting:

- **Active:** Directly interacting with the target to gather information about the target. Eg Using Nmap tool to scan the target
- **Passive:** Trying to collect the information about the target without directly accessing the target. This involves collecting information from social media, public websites etc.

2. Scanning:

Three types of scanning are involved:

- **Port scanning:** This phase involves scanning the target for the information like open ports, Live systems, various services running on the host.



- **Vulnerability Scanning:** Checking the target for weaknesses or vulnerabilities which can be exploited. Usually done with help of automated tools

- **Network Mapping:** Finding the topology of network, routers, firewalls servers if any, and host information and drawing a network diagram with the available information. This map may serve as a valuable piece of information throughout the haking process.

3. Gaining Access:

This phase is where an attacker breaks into the system/network using various tools or methods. After entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data.

4. Maintaining Access:

Hacker may just hack the system to show it was vulnerable or he can be so mischievous that he wants to maintain or persist the connection in the background without the knowledge of the user. This can be done using Trojans, Rootkits or other malicious files. The aim is to maintain the access to the target until he finishes the tasks he planned to accomplish in that target.

Introduction to Ethical Hacking

- CIA Triangle
- Important characteristics of Information
- Security, Functionality and Usability Triangle
- Phases of Hacking
- Different types of attacks
- Vulnerability Assessment
- Penetration Testing
- Information Security Laws, Standards and frameworks

5. Clearing Track:

No thief wants to get caught. An intelligent hacker always clears all evidence so that in the later point of time, no one will find any traces leading to him. To achieve this, the hacker focuses on modifying/corrupting/deleting the values of Logs, altering registry values, uninstalling all applications used, and deleting all folders created. In the event of a compromised site, it becomes crucial to promptly address and fix the hacked site to minimize potential damage and prevent further unauthorized access.

Introduction to Ethical Hacking

- CIA Triangle
- Important characteristics of Information
- Security, Functionality and Usability Triangle
- Phases of Hacking
- Different types of attacks
- Vulnerability Assessment
- Penetration Testing
- Information Security Laws, Standards and frameworks

Types of attacks:

Operating System Attacks:

Finding OS Vulnerabilities and Exploit them For.eg. buffer overflow, un-patched system.

Misconfiguration Attacks:

Targeted towards databases, networks, web servers, application platforms etc, It Happens due to the misconfiguration of the deployed devices or system.

Application Level Attacks:

Attacks are targeted towards the installed applications, e.g: Buffer overflow, cross-site scripting, SQL injection etc.

Shrink Wrap Code Attacks:

Using default or off the shelf components, it happens if the code/script is not fine-tuned.

Introduction to Ethical Hacking

- CIA Triangle
- Important characteristics of Information
- Security, Functionality and Usability Triangle
- Phases of Hacking
- Different types of attacks
- Vulnerability Assessment
- Penetration Testing
- Information Security Laws, Standards and frameworks

It is the process of identifying vulnerabilities in the computer systems, networks, and the communication channels. It is performed as a part of auditing and also to defend the systems from further attacks. The vulnerabilities are identified, classified and reported to the authorities so that necessary measures can be taken to fix them and protect the organization.

It is the process of evaluating the security of an organization by exploiting the vulnerabilities in a way the attackers could exploit them and thereby defending as well as documenting the procedure of attack.

Types of penetration testing**:**

- **Black box:** The penetration tester will not be given any details pertaining to the network, or infrastructure of the network/ organization
- **White Box:** the penetration tester will be aware of the complete details of the infrastructure to be tested
- **grey box:** The penetration tester will be provided with a limited knowledge about the systems to be tested.

Introduction to Ethical Hacking

- CIA Triangle
- Important characteristics of Information
- Security, Functionality and Usability Triangle
- Phases of Hacking
- Different types of attacks
- Vulnerability Assessment
- Penetration Testing
- Information Security Laws, Standards and frameworks

- PCI-DSS: Payment card industry Data security standard
- HIPPA – Health Insurance Privacy Protection Act
- ISO:IEC 27001:2013
- Sarbanes Oxley attack (SOX)
- The digital Millenium copyright Act (DMCA)
- The federal Information secuirty Management act (FISMA)

Essential Terminologies

- *Threat – An action or event that might compromise security. A threat is a potential violation of security*

- *Vulnerability – Existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the system*

- *Exploit – A defined way to breach the security of an IT system through vulnerability*

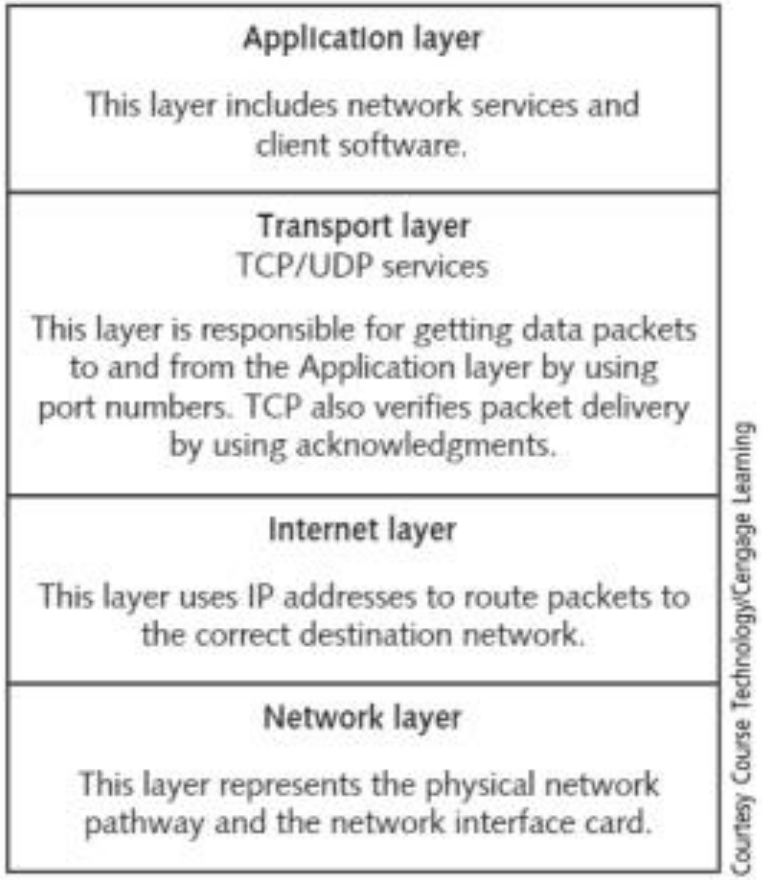
- *Target of Evaluation – An IT system, product, or component that is identified/subjected as requiring security evaluation*

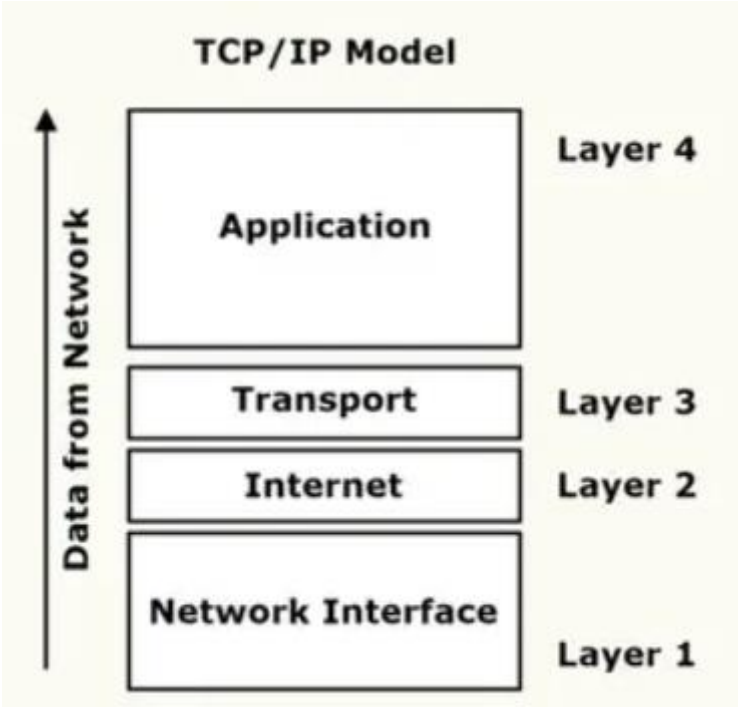
- *Attack – An assault on system security that derives from an intelligent threat. An attack is any action that violates security*

EC-Council

TCP/IP concepts

TCP/IP Reference Model is a four-layered suite of communication protocols. It was developed by the DoD (Department of Defence) in the 1960s. It is named after the two main protocols that are used in the model, namely, TCP and IP. **TCP** stands for "**Transmission Control Protocol**" and **IP** stands for "**Internet Protocol**".





TCP/IP Reference Model

Application Layer

- Responsible for the user interfaces and application services.
- Responsible for formatting messages for transport layer.

Transport Layer or Host-to-Host Layer

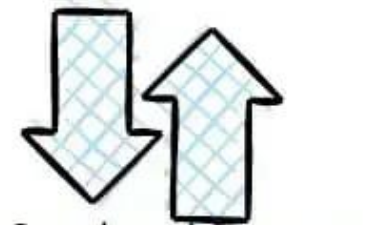
- Ensures data is delivered reliably and in order.

Internet Layer

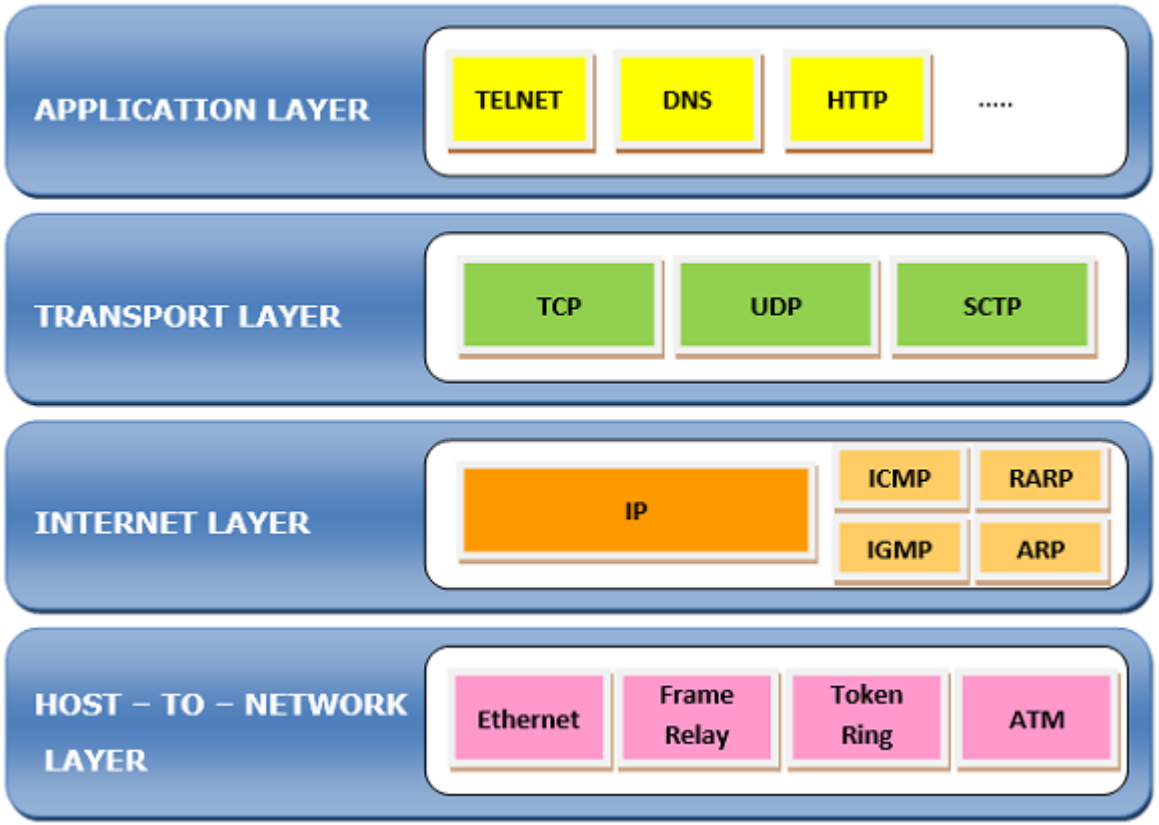
- Provides IP address and Routing data between devices.

Network Access Layer or Link Layer

- Transmits raw data bits over a physical medium.
- Provide MAC addressing and LLC.



AfrozAhmad



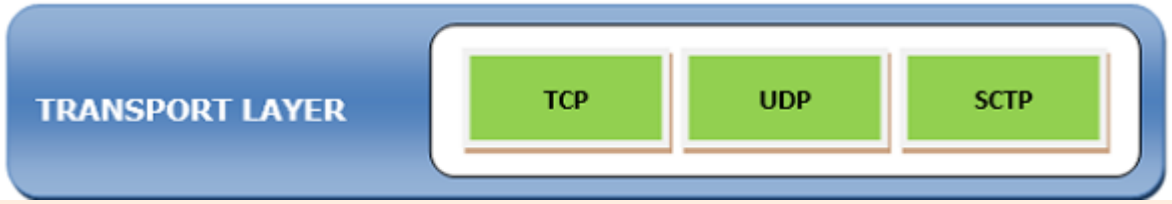
Application Layer – This is the topmost layer and defines the interface of host programs with the transport layer services. This layer includes all high-level protocols like Telnet, DNS, HTTP, FTP, SMTP, etc.

Transport Layer – It is responsible for error-free end-to-end delivery of data. The protocols defined here are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

Internet Layer –It defines the protocols for logical transmission of data over the network. The main protocol in this layer is Internet Protocol (IP) and it is supported by the protocols ICMP, IGMP, RARP, and ARP.

The host-to-network layer is the lowest layer of the TCP/IP model and is concerned with the physical transmission of data. It is also called a network interface layer or link layer. It can be considered as the combination of physical layer and data link layer of the OSI model.

- Hyper Text Transfer Protocol, HTTP – It is the underlying protocol for world wide web. It defines how hypermedia messages are formatted and transmitted.
- File Transfer Protocol, FTP – It is a client-server based protocol for transfer of files between client and server over the network.
- Simple Mail Transfer Protocol, SMTP – It lays down the rules and semantics for sending and receiving electronic mails (e-mails).
- Domain Name System, DNS – It is a naming system for devices in networks. It provides services for translating domain names to IP addresses.
- TELNET – It provides bi-directional text-oriented services for remote login to the hosts over the network.
- Simple Network Management Protocol, SNMP – It is for managing, monitoring the network and for organizing information about the networked devices.

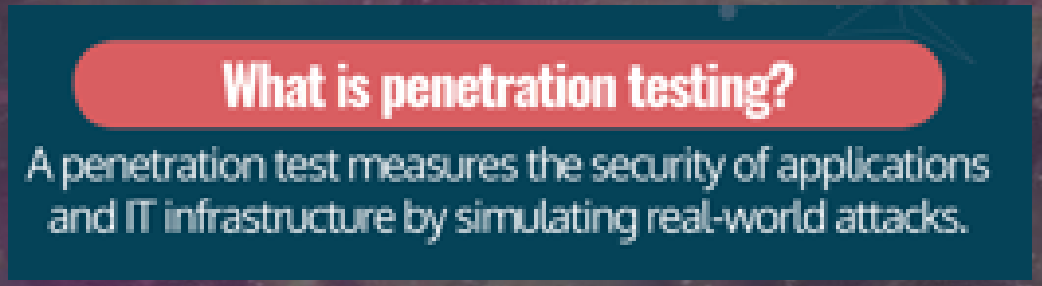


- Transmission Control Protocol, TCP – It is a reliable connection-oriented protocol that transmits data from the source to the destination machine without any error. A connection is established between the peer entities prior to transmission. At the sending host, TCP divides an incoming byte stream into segments and assigns a separate sequence number to each segment. At the receiving host, TCP reorders the segments and sends an acknowledgment to the sender for correct receipt of segments. TCP also manages flow control so that a fast sender does not overwhelm a slow receiver.
- User Datagram Protocol, UDP – It is a message-oriented protocol that provides a simple unreliable, connectionless, unacknowledged service. It is suitable for applications that do not require TCP's sequencing, error control or flow control. It is used for transmitting a small amount of data where the speed of delivery is more important than the accuracy of delivery.
- Stream Control Transmission Protocol, SCTP – It combines the features of both TCP and UDP. It is message oriented like the UDP, which providing the reliable, connection-oriented service like TCP. It is used for telephony over the Internet.

- Internet Protocol, IP – It is a connectionless and unreliable protocol that provides a best effort delivery service. It transports data packets called datagrams that travel over different routes across multiple nodes.
- Address Resolution Protocol, ARP –This protocol maps the logical address or the Internet address of a host to its physical address, as printed in the network interface card.
- Reverse Address Resolution Protocol, RARP – This is to find the Internet address of a host when its physical address is known.
- Internet Control Message Protocol, ICMP – It monitors sending the queries as well as the error messages.
- Internet Group Message Protocol, IGMP –It allows the transmission of a message to a group of recipients simultaneously.

Penetration Testing

Penetration testing is a systematic process of probing for vulnerabilities in your applications and networks.



WHAT IS A **PENETRATION TEST?**

An authorized attack on a computer system, network, or application to identify security vulnerabilities bad actors might exploit.

The Process

1. INFORMATION GATHERING
2. THREAT MODELING
3. VULNERABILITY ANALYSIS
4. EXPLOITATION
5. POST-EXPLOITATION
6. REPORTING

Types of Penetration Tests

- Application
- Network
- Physical
- IoT/Mobile

Why Conduct a Penetration Test?

- Identify security vulnerabilities
- Validate compliance with policies
- Evaluate effectiveness of defenses

Phases of Penetration Testing

STAGES OF PEN TESTING

Stage 1

Profiling

In this stage, the target will be profiling by identifying user entry points, interfaces to external or internal applications, assets, roles with varying trust levels, and determining the data flow path with privilege boundaries.

Stage 2

Automated Scanning

Automated vulnerability scanners (i.e., commercial and open-source) will be used to scan for vulnerabilities covering all OWASP, WASC, and SANS references.

Stage 3

Vulnerability Detection

This phase involves a hybrid approach of identifying the security vulnerabilities with automated tools and scripts and manual assessment to eliminate false positives and negatives. The manual assessment was done using various vulnerability databases to identify missed vulnerabilities during automated scans and security verification of business logic flaws, broken access controls, and more.

Stage 4

Vulnerability Exploitation

The primary focus in this phase is on using manual security testing techniques to exploit the systems, including several exploits to assess the application/system hardening measures, cryptography issues, authentication & authorization controls, session management module, business logic flaws, and various validation measures.

Stage 5

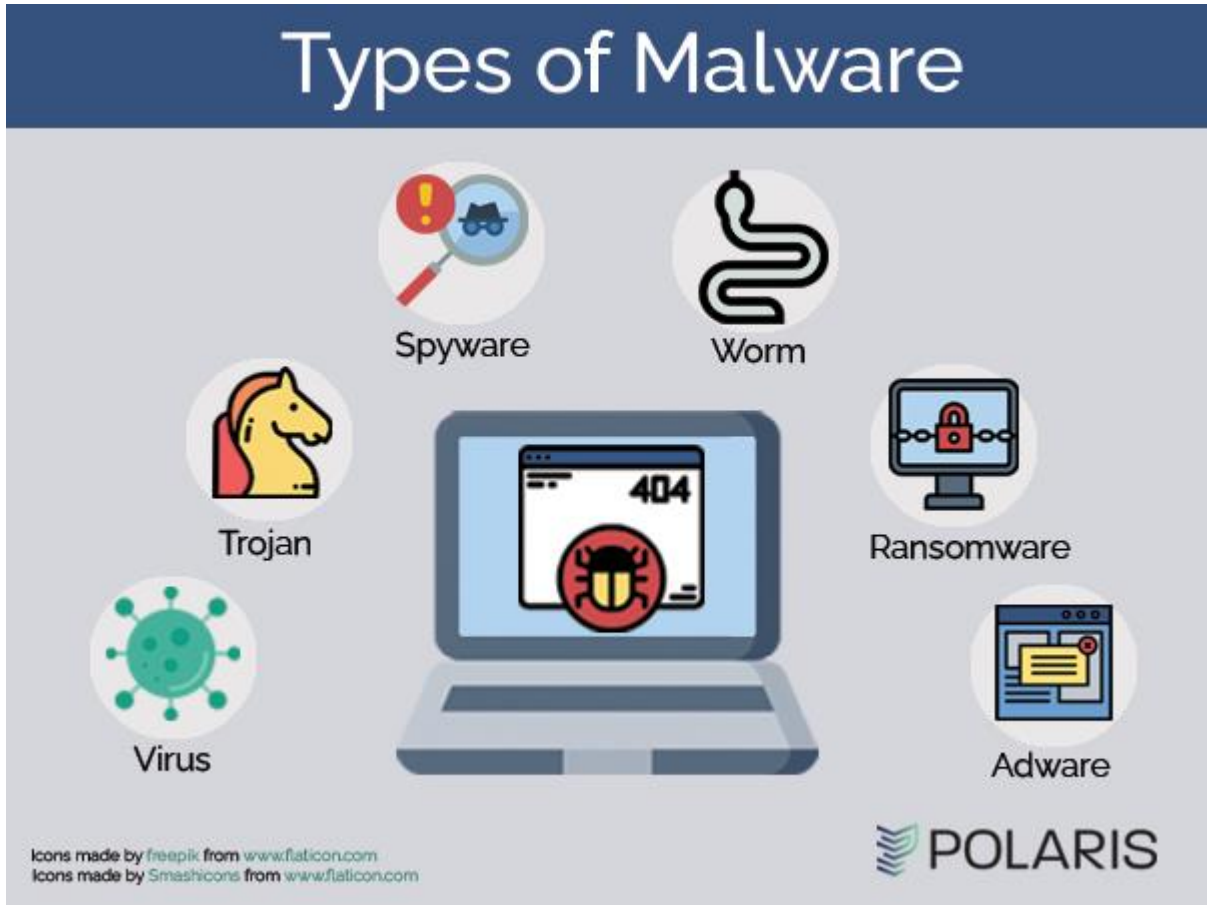
Reporting

All exploitable security vulnerabilities in the target application/system are recorded with associated CVSS v3 based scores reported to the client. The security vulnerability will be assessed and reported with appropriate recommendations or mitigation measures.

spiceworks

PENETRATION TESTER : ROLES AND RESPONSIBILITIES

Malicious Software(malware)



Types of malware

Virus
Malicious software attached to a document or file that can execute its code.

Worms
Malicious software that rapidly replicates and spreads to any device within the network.

Trojan Virus
Virus disguised as helpful software programs.

Spyware
Malicious software that runs secretly on a computer and reports back to a remote user.

Adware
Used to collect data on you computer usage and provide advertisements.

Ransomware
Gains sensitive information and encrypts the information before demanding a financial payout.

Fileless Malware
Malware that operates from a victims computer memory, not the files on the hard drive.

www.cyber.gov.rw 9009

Types of Malware

VIRUS

- Viruses attach themselves to the legitimate programs and replicate when the infected programs runs.
- E.g. Stuxnet (2010)

WORM

- Programs that replicate & spread across a network independently.
- Don't need to attach to files, unlike viruses.
- E.g. Conficker (2008)

TROJAN HORSE

- Disguises themselves as legitimate software.
- Once inside a system, they create a backdoor for attackers
- E.g. Zeus

SPYWARE

- Secretly monitors user activities, capturing keystrokes, browsing habits, and personal information.
- E.g. Pegasus

RANSOMWARE

- Encrypts files on a victim's system and demands a ransom for decryption keys.
- E.g. AKIRA

ADWARE

- Adware displays unwanted advertisements on a user's computer, often in the form of pop-up ads.
- E.g. Superfish

ROOTKITS

- Are designed to conceal malicious software and processes.
- Operates stealthily within a compromised system.
- E.g. Sony BMG Rootkit (2005)

BOTNETS

- Networks of infected computers controlled remotely by a single entity.
- E.g. Mariposa

KEYLOGGERS

- Records keystrokes on a computer to capture sensitive information like passwords, credit card numbers, and personal data.
- E.g. DarkTequila

Malicious Software(malware) terminologies

Name	Description
Advanced Persistent Threat (APT)	Cybercrime directed at business and political targets, using a wide variety of intrusion technologies and malware, applied persistently and effectively to specific targets over an extended period, often attributed to state-sponsored organizations.
Adware	Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.
Attack kit	Set of tools for generating new malware automatically using a variety of supplied propagation and payload mechanisms.
Auto-rooter	Malicious hacker tools used to break into new machines remotely.
Backdoor (trapdoor)	Any mechanism that bypasses a normal security check; it may allow unauthorized access to functionality in a program, or onto a compromised system.
Downloaders	Code that installs other items on a machine that is under attack. It is normally included in the malware code first inserted on to a compromised system to then import a larger malware package.

Drive-by-download	An attack using code in a compromised Web site that exploits a browser vulnerability to attack a client system when the site is viewed.
Exploits	Code specific to a single vulnerability or set of vulnerabilities.
Flooders (DoS client)	Used to generate a large volume of data to attack networked computer systems, by carrying out some form of denial-of-service (DoS) attack.
Keyloggers	Captures keystrokes on a compromised system.
Logic bomb	Code inserted into malware by an intruder. A logic bomb lies dormant until a predefined condition is met; the code then triggers an unauthorized act.
Macro virus	A type of virus that uses macro or scripting code, typically embedded in a document, and triggered when the document is viewed or edited, to run and replicate itself into other such documents.
Mobile code	Software (e.g., script, macro, etc) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access.

Spammer programs	Used to send large volumes of unwanted e-mail.
Spyware	Software that collects information from a computer and transmits it to another system by monitoring keystrokes, screen data, and/or network traffic; or by scanning files on the system for sensitive information.
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes it.
Virus	Malware that, when executed, tries to replicate itself into other executable machine or script code; when it succeeds, the code is said to be infected. When the infected code is executed, the virus also executes.
Worm	A computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network, usually by exploiting software vulnerabilities in the target system.
Zombie, bot	Program activated on an infected machine that is activated to launch attacks on other machines.

5.1.2 Classification of Malware

- classified into two broad categories based on:
  - how it spreads or propagates to reach the desired targets
  - the actions or payloads it performs once a target is reached
- also classified by:
  - those that need a host program
    - parasitic code such as viruses
  - those that are independent, self-contained programs
    - worms, trojans, and bots
  - malware that does not replicate
    - trojans and spam e-mail
  - malware that does replicate
    - viruses and worms

Protect from Malicious Software

1. ***INSTALL AN ANTIVIRUS SOLUTION*** to detect and remove the malware in real time.
2. ***INSTALL A FIREWALL APPLICATION*** to inspect the traffic from websites, e-mails and applications.
3. ***UPDATE THE OPERATING SYSTEMS AND THE APPLICATIONS*** to patch the existent vulnerabilities.
4. ***DISABLE AUTOMATIC EXECUTION OF CODE ON WEBSITES*** to prevent the installation of file-less malware.
5. ***USE E-MAIL FILTERING*** to recognize and detect the malicious emails and attachments.
6. ***AVOID USING ADMIN ACCOUNTS*** to prevent malware to have administrator privileges.
7. ***BACKUP YOUR DATA*** to restore it in case of a successful infection with malware.
8. ***USE ADVANCED TOOLS***, for malware detection and mitigation, like *Intrusion Detection and Prevention Systems (IDPS).*
9. ***MONITOR THE LOGS*** using *Security Incident and Event Management (SIEM)* solution.
10. ***USE SECURITY POLICIES*** that specify the steps to be followed in case of infection.
11. ***REDUCE ACCESS TO POWERSHELL*** functions, to limit the malware to execute malicious code into the console.
12. ***REPORT THE SECURITY INCIDENTS*** to the National Computer Security Incident Response Team.

Stay Safe From MALWARE

Stay Safe

- Use anti-virus software, and keep it updated.
- Keep operating systems updated and patched.
- Install software and apps only from trusted sites.
- Only click on links or open attachments in emails you were expecting.
- Report incidents, such as if you have been hacked. We are here to help.

Stop Malware

- Do not open unexpected email attachments.
- Never pay a ransom to unlock encrypted files.
- Do not click on suspicious or untrusted email links.
- Do not plug untrusted USB drives into work computers or devices.
- If your computer has been infected, don't try to fix the problem, report it instead.

Malware is malicious software, but you can stop it in its tracks.

Malware is a type of program designed to infect computers and devices. Once installed, malware allows cyber attackers to spy on your online activities, steal passwords, delete or encrypt files, or use your system to attack others.

UNIVERSITY OF TORONTO

SANS SECURITY AWARENESS

This factsheet is published by example.
For more information, please contact us at:

https://securitymatters.utoronto.ca

Protection against malware attacks

- Educate your users
- Avoiding fear tactics

Educating Your Users

No matter how hard you try to protect a network from malware being introduced, the most effective approach is conducting structured training of all employees and management. In fact, many U.S. government agencies make security awareness programs mandatory, and many private-sector companies are following their example. A simple but effective method of educating users is e-mailing monthly security updates to all employees to inform them of the most recent viruses, spyware, and adware detected on the Internet.

To help prevent viruses from being introduced into corporate networks, the most important recommendation you should make to a client is to update virus signature files as soon as they're available from the vendor. Most antivirus software does this updating automatically or prompts the user to do so. An organization can't depend on employee vigilance to protect its systems, however, so centralizing all antivirus updates from a corporate server is prudent.

To counter the introduction of spyware and adware into a corporate network, you might need to download additional software from the Internet. Many antivirus packages don't fully address the problem of spyware and adware. As of this writing, the two most popular spyware and adware removal programs are SpyBot and Ad-Aware. Both are free and easy to install and can be downloaded from *www.pcworld.com/downloads*. Many other Web sites offer these programs, but remember to use caution when downloading any programs from unknown Web sites.

You can also help protect a network by installing a firewall (covered in more detail in Chapter 13). Many of the top antivirus vendors also offer software firewalls for home and small-business users who don't have a hardware firewall or an intrusion detection system (IDS) installed. Companies using firewalls can follow the vendor's configuration instructions. For example, the W32/Sobig.F worm uses UDP port 8998 to contact the attacker's server. By blocking all outbound traffic on this port, you can prevent this attack from occurring. Also, many services are started by default on a computer, and they don't need to be. For example, the average home user or small-business owner doesn't typically use Telnet. This service shouldn't be active on most computers because it's vulnerable to many outside attacks.

Avoiding Fear Tactics

You'd be surprised how many users don't know that clicking an icon in an e-mail message can activate a virus or Trojan program or allow another person to access their computers from a remote location. Consequently, some security professionals use fear tactics to scare users into complying with security measures. Their approach is to tell users that if they don't take a particular action, their computer systems will be attacked by every malcontent who has access to the Internet. This method is sometimes used to generate business for security testers and is not only unethical, but also against the OSSTMM's Rules of Engagement (included with the manual on this book's online resources). The rule states: "The use of fear, uncertainty, and doubt may not be used in the sales or marketing presentations, websites, supporting materials, reports, or discussion of security testing for the purpose of selling or providing security tests. This includes but is not limited to crime facts, criminal or hacker profiling, and statistics."

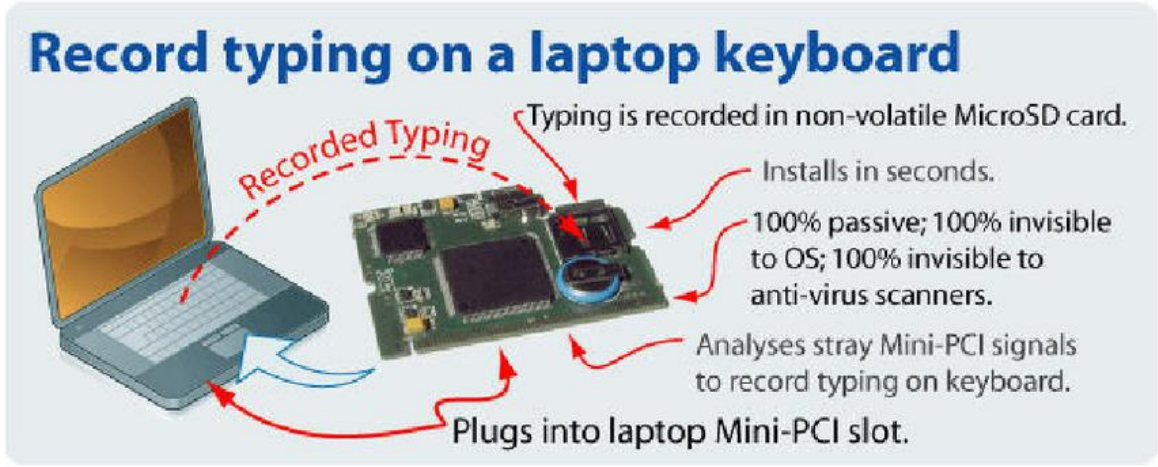
Your approach to users or potential customers should promote awareness rather than instill fear. You should point out to users how important it is not to install programs—especially those not approved by the company—on their desktops because of the possibility of introducing malware. Users should be aware of potential threats, not terrified by them.

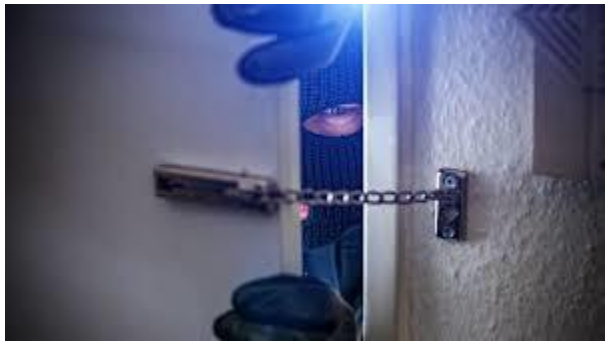
In addition, when training users, be sure to build on the knowledge they already have. For example, some users are familiar with Windows XP Remote Assistance or other remote control programs, such as Symantec pcAnywhere. Users' experience with these programs makes the job of explaining how an intruder can take control of their computers easier because they already know the technology is available.

Hands-On Ethical Hacking and Network Defense (PDFDrive).pdf

Physical Security

- Keylogger
- Behind Locked doors

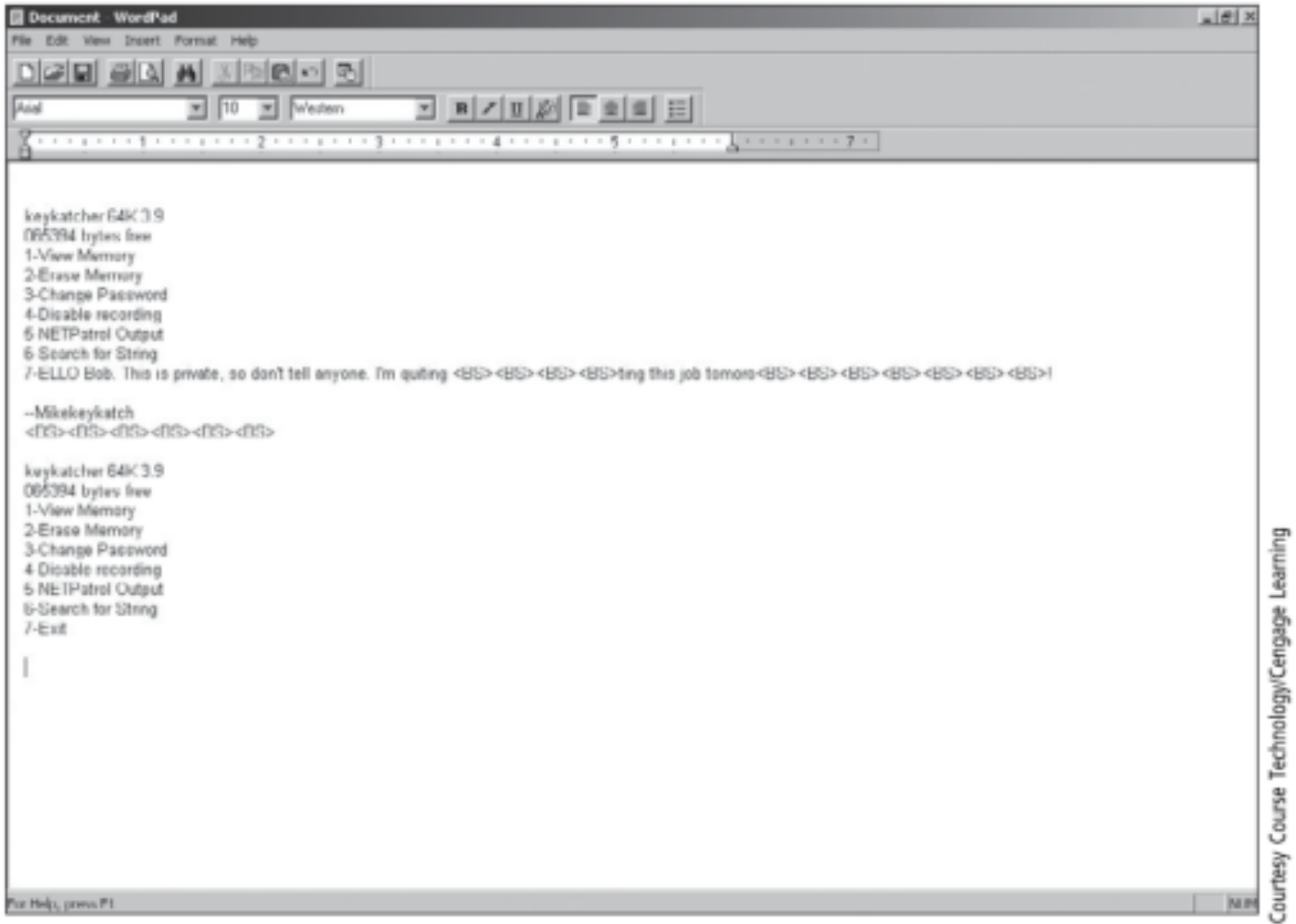




Keylogger

Keyloggers are hardware devices or software that can be used to capture keystrokes on a computer. Software keyloggers behave like Trojan programs and are loaded on a computer. A hardware keylogger is a small device, often smaller than an inch long. It can usually be installed in less than 30 seconds. It's a simple matter of unplugging the keyboard, plugging the small device into the keyboard input jack, and then plugging the keylogger jack into the computer's keyboard port. After installing the hardware, most vendors require you to run a word processing program, such as WordPad, and then enter the vendor-supplied password in a blank document. After entering the password, a menu is displayed. Some common hardware keyloggers are KeyKatcher and KeyGhost. In Figure 3.4, the KeyKatcher keylogger program captured a private message sent in an e-mail; the sender is informing Bob that he's going to quit his job. If you're conducting a security test on a system and need to obtain passwords, key-loggers can be a helpful tool. Of course, you should have written permission from the client before using software or hardware keyloggers.

Hands-On Ethical Hacking and Network Defense (PDFDrive).pdf



Courtesy Course Technology/Cengage Learning

Figure 3.4
An e-mail message captured by KeyKatcher

Hands-On Ethical Hacking and Network Defense (PDFDrive).pdf

Behind the doors

As a security professional, you should be aware of the types of locks used to secure a company's assets. If an intruder gets physical access to a server, whether it's running Linux, Windows, or another OS, it doesn't matter how good your firewall or IDS is. Encryption or public key infrastructure (PKI) enforcements don't help in this situation, either. If intruders can sit in front of your server, they can hack it. Simply put, *lock up your server*.

In the same way that terrorists can learn how to create a bomb by doing Internet research, attackers can find countless articles about lock picking. One paper, "MIT Guide to Lock Picking" by an author calling himself Ted the Tool (*www.lysator.liu.se/mit-guide/ MITLockGuide.pdf*), discusses the vulnerabilities of tumbler locks. After a week or two of practice, the average person can learn how to pick a deadbolt lock in less than 5 minutes. Those who have more time on their hands, such as hackers, can learn to pick a deadbolt lock in under 30 seconds. If you're responsible for protecting a network infrastructure that has night-shift workers, don't assume that locked doors or cabinets can keep out unscrupulous employees with time on their hands. Typically, fewer employees are around during non-standard business hours, which makes it easier for them to get into areas to which they might not normally have access. Your server room should have the best lock your company can afford. Take the time to look into locks that organizations such as the Department of Defense use, where protecting resources might be a life-or-death situation. Spending $5000 to $10,000 on a lock isn't unheard of in these organizations.

Rotary locks that require pushing in a sequence of numbered bars are more difficult to crack than deadbolt locks. However, neither lock type keeps a record of who has entered the locked room, so some businesses require using card access for better security. With this method, a card is scanned, and access is given to the cardholder while documenting the time of entry. This method also makes it possible for one card to allow access to several doors without having to issue multiple keys or having users memorize different combinations.

Hands-On Ethical Hacking and Network Defense (PDFDrive).pdf

WHAT IS KEYLOGGER

Keylogger is one kind of surveillance technology that is used to monitor and capture keystrokes of a specific device. It can work from both hardware and software

HOW CAN YOU PROTECT YOURSELF FROM KEYLOGGERS?

1

USE A FIREWALL

2

USE A PASSWORD MANAGER

3

USE ANTIVIRUS SOFTWARE

4

REGULARLY UPDATE YOUR COMPUTER

HOW KEYLOGGING WORKS

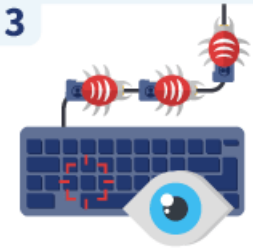
1

YOU ACCIDENTALLY DOWNLOAD MALWARE

2

THE MALWARE CONTAINED A KEYLOGGER INSTALLS ITSELF

3



THE KEYLOGGER BEGINS TO CAPTURE YOUR KEYSTROKES

4

FILES ARE PERIODICALLY EMAILED TO A HACKER

5

CHANGE YOUR PASSWORDS REGULARLY

6

AVOID SUSPICIOUS LINKS AND UNKNOWN FILES

7

USE ANTI-KEYLOGGER TOOLS

WHAT IS A KEYLOGGER?

A keylogger is able to record & learn any of the following:

- Keystroke pattern
- Words
- Symbols
- Characters

After collecting data, it reverts all information back to the attacker.v

There are two types of keyloggers:

Hardware Keyloggers

Physical devices used to access computers.

Software Keyloggers

Malicious programs used to access computers

What is Keylogger?

What is Keylogger?

Keylogger is a malicious computer program that records everything you type on the keyboard and learns the keystroke pattern including words, characters, symbols and send all the recorded details to the malicious hackers.

Type of Keyloggers

Hardware Keyloggers: Devices that can be attached in our computer which will act as a keylogger and collects information about the specified target.
Software keyloggers: Probably a malicious program that does not infect your system but still can steal your passwords, account details, etc.

How does Keylogger work?

Just like any other malicious program that sends its reports to the attackers, keyloggers also send information about keystrokes that a victim enters in his/her keyboard to its creator or a remote server or a specified email address.

How to Protect From Keyloggers?

- Do not download any attachments from unknown websites.
- Keep your AntiVirus software updated.
- Use Virtual Keyboards which will prevent from typing keystrokes.
- Use Two-Factor Authentication Methods on important sites.
- User firewall and password manager

www.cybersecuritynews.com

Security Policies and procedures

A policy is a document that outlines specific requirements or rules that must be met

- Communicate a consensus of judgment
- Define what appropriate behavior for users is
- Identify what tools and procedures are needed
- Provides a foundation for HR action in response to inappropriate behavior

Security Policies and procedures

- Although passwords often form the weakest link in information security, they are still the most widely used
- A password management policy should clearly address how passwords are managed
- In addition to controls that can be implemented through technology, password policies should also outline characteristics of weak and strong passwords and provide examples

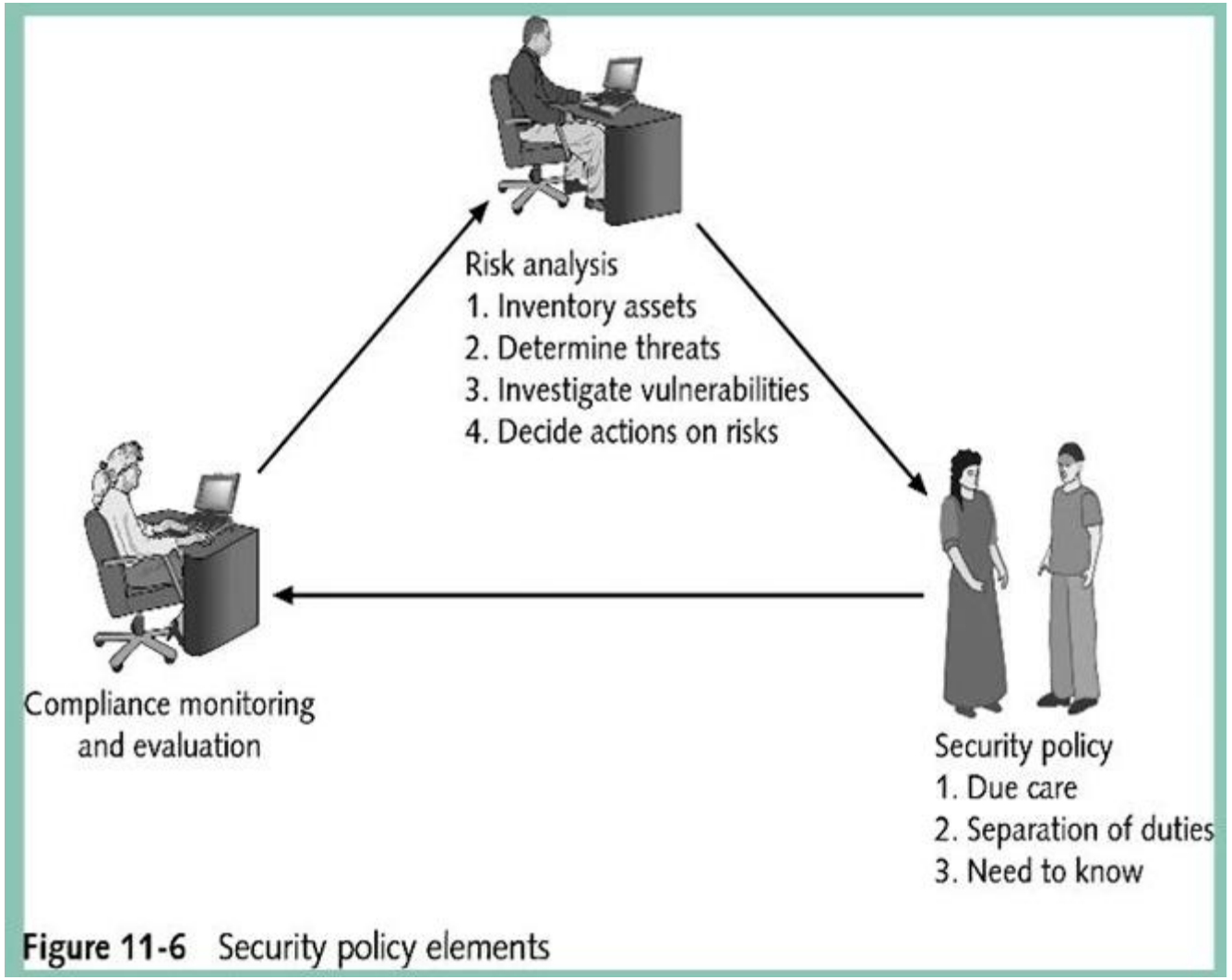


Figure 11-6 Security policy elements

Security Policies and procedures

Table 11-7 Examples of security policies

Name of Security Policy	Description
Acceptable encryption policy	Defines requirements for using cryptography
Analog line policy	Defines standards for use of analog dial-up lines for sending and receiving faxes and for connection to computers
Antivirus policy	Establishes guidelines for effectively reducing the threat of computer viruses on the organization's network and computers
Audit vulnerability scanning policy	Outlines the requirements and provides the authority for an information security team to conduct audits and risk assessments and investigate incidents to ensure conformance to security policies or to monitor user activity
Automatically forwarded e-mail policy	Prescribes that no e-mail will be automatically forwarded to an external destination without prior approval from the appropriate manager or director
Database credentials coding policy	Defines requirements for storing and retrieving database usernames and passwords
Dial-in access policy	Outlines appropriate dial-in access and its use by authorized personnel

Table 11-7 Examples of security policies (continued)

Name of Security Policy	Description
Demilitarized zone (DMZ) security policy	Defines standards for all networks and equipment located in the DMZ
E-mail policy	Creates standards for using corporate e-mail
E-mail retention policy	Helps employees determine what information sent or received by e-mail should be retained and for how long
Extranet policy	Defines the requirements for third-party organizations to access the organization's networks
Information sensitivity policy	Establishes criteria for classifying and securing the organization's information in a manner appropriate to its level of security
Router security policy	Outlines standards for minimal security configuration for routers and switches
Server security policy	Creates standards for minimal security configuration for servers
Virtual private network (VPN) security policy	Establishes requirements for Remote Access IP security (IPSec) or Layer 2 Tunneling Protocol (L2TP) VPN connections to the organization's network
Wireless communication policy	Defines standards for wireless systems used to connect to the organization's networks

What is Footprinting

Refers to the process of collecting as much as information as possible about the target system to find ways to penetrate into the system. An Ethical hacker has to spend the majority of his time in profiling an organization, gathering information about the host, network and people related to the organization.

Information such as ip address, Whois records, DNS information, an operating system used, employee email id, Phone numbers etc is collected.

What is Footprinting?

- Footprinting is the process of collecting as much information as possible about a target network, for identifying various ways to intrude into an organization's network system.
- Footprinting is the first step of any attack on information systems; attacker gathers publicly available sensitive information, using which he/she performs social engineering, system and network attacks, etc. that leads to huge financial loss and loss of business reputation.
- **Know Security Posture**: Footprinting allows attackers to know the external security posture of the target organization.
- **Reduce Focus Area**: It reduces attacker's focus area to specific range of IP address, networks, domain names, remote access, etc.
- **Identify Vulnerabilities**: It allows attacker to identify vulnerabilities in the target systems in order to select appropriate exploits.
- **Draw Network Map**: It allows attackers to draw a map or outline the target organization's network infrastructure to know about the actual environment that they are going to break.

Objectives of Footprinting

Network Footprinting

This is the process of collecting information related to a target network. Information like Domain name, subdomains, network blocks, IP addresses of reachable systems, IDSes running, Rouge websites/private websites, TCP & UDP services running, VPN points, networking protocols, ACL's, etc are collected.

Collect System Information

The information related to the target system like user and group names, system banners, routing tables, SNMP information, system names etc are collected using various methods.

Collect Organization's information –

The information related to employee details, organization website, Location details, security policies implemented, the background of the organization may serve as an important piece of information for compromising the security of the target using direct or social engineering attacks.

Objectives of Footprinting

- **Collect Network Information**:
  - Domain name
  - Internal domain names
  - Network blocks
  - IP addresses of the reachable systems
  - Rogue websites/private websites
  - TCP and UDP services running
  - Access control Mechanisms and ACL's
  - Networking protocols
  - VPN Points
  - IDSes running
  - Analog/digital telephone numbers
  - Authentication mechanisms
  - System Enumeration
- **Collect System Information**:
  - User and group names
  - System banners
  - Routing tables
  - SNMP information
  - System architecture
  - Remote system type
  - System names
  - Passwords
- **Collect Organization's Information**:
  - Employee details
  - Organization's website

Footprinting Methodology

Various methods used to collect information about the target organization. They are

Footprinting through Search Engines

This is a passive information gathering process where we gather information about the target from social media, search engines, various websites etc. Information gathered includes name, personal details, geographical location detrails, login pages, intranet portals etc. Even some target specific information like Operating system details, IP details, Netblock information, technologies behind web application etc can be gathered by searching through search engines

Eg: collecting information from Google, Bingo etc

Google Hacking:

Google hacking refers to collecting information using google dorks (keywords) by constructing search queries which result in finding sensitive information.details collected include compromised passwords, default credentials, competitor information, information related to a particular topic etc.

Eg:inurl:, site:, allintitle etc

Examining HTML Source and Examining Cookies:

Html source codes of a web application may give us an understanding of the application functionality, hidden fields, comments, variable names etc. Cookies are used to identify a user in his session. these cookies may be stored in the browser or passed in the URL, or in the HTTP header.

The entire website can be mirrored using tools like HTTtracker to gather information at our own phase.

Extract website Archives: older versions of website can be obtained which may reveal some information related to the target.

eg: www.archive.org

Email Footprinting

email header reveals information about the mail server, original sender's email id, internal IP addressing scheme, as well as the possible architecture of the target network

Competitive Intelligence

Competitive intelligence gathering is the process of gathering information about the competitors from resources such as the Internet.

Eg: company website, search engine, internet, online databases, press releases, annual reports, trade journals

Google Hacking/Google Dorks

This is a process of creating search queries to extract hidden information by using Google operators to search specific strings of text inside the search results.

Some google operators, site, allinurl, inurl, allintitle

Google Advance Search Operators (重要)

- Google supports several advanced operators that help in modifying the search:
  - [**cache:**] Displays the web pages stored in the Google cache
  - [**link:**] Lists web pages that have links to the specified web page
  - [**related:**] Lists web pages that are similar to a specified web page
  - [**info:**] Presents some information that Google has about a particular web page
  - [**site:**] Restricts the results to those websites in the given domain
  - [**allintitle:**] Restricts the results to those websites with all of the search keywords in the title
  - [**intitle:**] Restricts the results to documents containing the search keyword in the title
  - [**allinurl:**] Restricts the results to those with all of the search keywords in the URL
  - [**inurl:**] Restricts the results to documents containing the search keyword in the URL

- Google Hacking Database (GHDB): http://www.hackersforcharity.org
- Google Dorks: http://www.exploit-db.com

What is Social Engineering?

- Social engineering is the art of convincing people to reveal confidential information. Common targets of social engineering include help desk personnel, technical support executives, system administrators, etc.
- Social engineers depend on the fact that people are unaware of their valuable information and are careless about protecting it.

Impersonation Scenario: Repairman

- Attacker may pretend to be telephone repairman or computer technician and enters into target organization.
- He/she may then plant a snooping device or gain hidden passwords during activities associated with their duties.

Types of Social Engineering

- **Human-based Social Engineering**: Gathers sensitive information by interaction.
- **Computer-based Social Engineering**: Social engineering is carried out with the help of computers.
- **Mobile-based Social Engineering**: It is carried out with the help of mobile applications.

Human-based Social Engineering: Impersonation

- It is most common human-based social engineering technique where attacker pretends to be someone legitimate or authorized person.
- Attackers may impersonate a legitimate or authorized person either personally or using a communication medium such as phone, email, etc.
- Impersonation helps attackers in tricking a target to reveal sensitive information.
- **Posing as a legitimate end user**: Give identity and ask for the sensitive information.
- **Posing as an important user**: Posing as a VIP of a target company, valuable customer, etc.
- **Posing as technical support**: Call as technical support staff and request IDs and passwords to retrieve data.

- **Eavesdropping**:
  - Eavesdropping or unauthorized listening of conversations or reading of messages.
  - Interception of audio, video, or written communication.
  - It can be done using communication channels such as telephone lines, email, instant messaging, etc.
- **Shoulder Surfing**:
  - Shoulder surfing uses direct observation techniques such as looking over someone's shoulder to get information such as passwords, PINs, account numbers, etc.
  - Shoulder surfing can also be done from a longer distance with the aid of vision enhancing devices such as binoculars to obtain sensitive information.

- **Dumpster Diving**: Dumpster diving is looking for treasure in someone else's trash.

and tech support.

- **Piggybacking**:
  - "I forgot my ID badge at home. Please help me."
  - An authorized person allows (intentionally or unintentionally) an unauthorized person to pass through a secure door.
- **Tailgating**:
  - An unauthorized person, wearing a fake ID badge, enters a secured area by closely following an authorized person through a door requiring key access.

Computer-based Social Engineering: Phishing

- An illegitimate email falsely claiming to be from a legitimate site attempts to acquire the user's personal or account information.
- Phishing emails or pop-ups redirect users to fake webpages of mimicking trustworthy sites that ask them to submit their personal information.

Computer-based Social Engineering: Spear Phishing

- Spear phishing is a direct, targeted phishing attack aimed at specific individuals within an organization.

- **Pop-up Windows**: Windows that suddenly pop up while surfing the Internet and ask for users' information to login or sign-in.
- **Hoax Letters**: Hoax letters are emails that issue warnings to the user on new viruses, Trojans, or worms that may harm the user's system.
- **Chain Letters**: Chain letters are emails that offer free gifts such as money and software on the condition that the user has to forward the mail to the said number of persons.
- **Instant Chat Messenger**: Gathering personal information by chatting with a selected online user to get information such as birth dates and maiden names.
- **Spam Email**: Irrelevant, unwanted, and unsolicited email to collect the financial information, social security numbers, and network information.

Mobile-based Social Engineering: Publishing Malicious Apps

- Attackers create malicious apps with attractive features and similar names to that of popular apps, and publish them on major app stores.
- Unaware users download these apps and get infected by malware that sends credentials to attackers.

Mobile-based Social Engineering: Fake Security Applications

1. Attacker infects the victim's PC.
2. The victim logs onto his/her bank account.
3. Malware in PC pop-ups a message telling the victim to download an application onto his/her phone in order to receive security messages.
4. Victim downloads the malicious application on his/her phone.
5. Attacker can now access second authentication factor sent to the victim from the bank via SMS.

What is Scanning?

Scanning is a set of procedures for identifying live hosts, ports, and services, discovering Operating system and architecture of target system, Identifying vulnerabilities and threats in the network. Network scanning is used to create a profile of the target organization.

Scanning refers to collecting more information using complex and aggressive reconnaissance techniques.

Network Scanning

Network Scanning:

The purpose of each scanning process is given below:

- **Port Scanning** – detecting open ports and services running on the target.
- **Network Scanning** – IP addresses, Operating system details, Topology details, trusted routers information etc
- **Vulnerability scanning** – scanning for known vulnerabilities or weakness in a system

Banner Grabbing

Banner grabbing is a process of collecting information like operating system details, the name of the service running with its version number etc.

Vulnerability scanning:

Mainly automated tools are used for this purpose. These automated scanners scan the target to find out vulnerabilities or weakness in the target organization which can be exploited by the attackers. Vulnerabilities include application vulnerabilities, configuration vulnerabilities, network vulnerabilities, operating system vulnerabilities etc.

Some examples include operating system is not updated, default passwords used, plain text protocols used, vulnerable protocols running etc.

Tools: Nessus, Acunetix

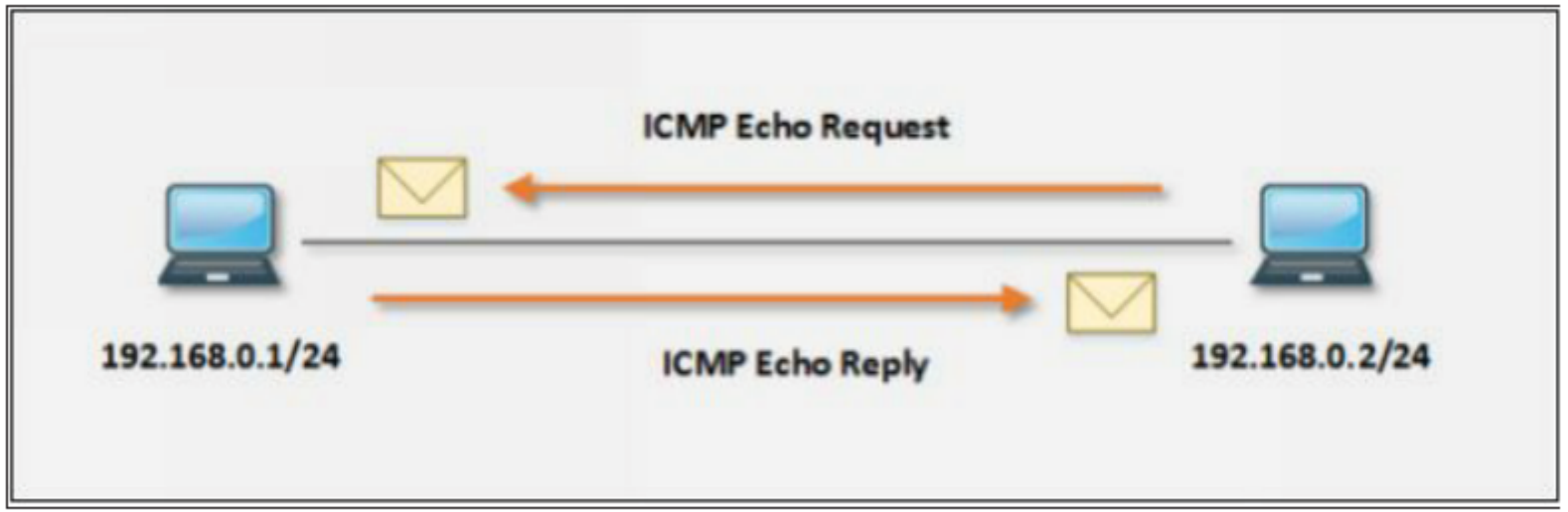


Figure 3-07 ICMP Echo Request & Reply Packets

Scanning Techniques

Scanning techniques include UDP & TCP Scanning technique. Observe the following figure showing the classification of Scanning techniques: -

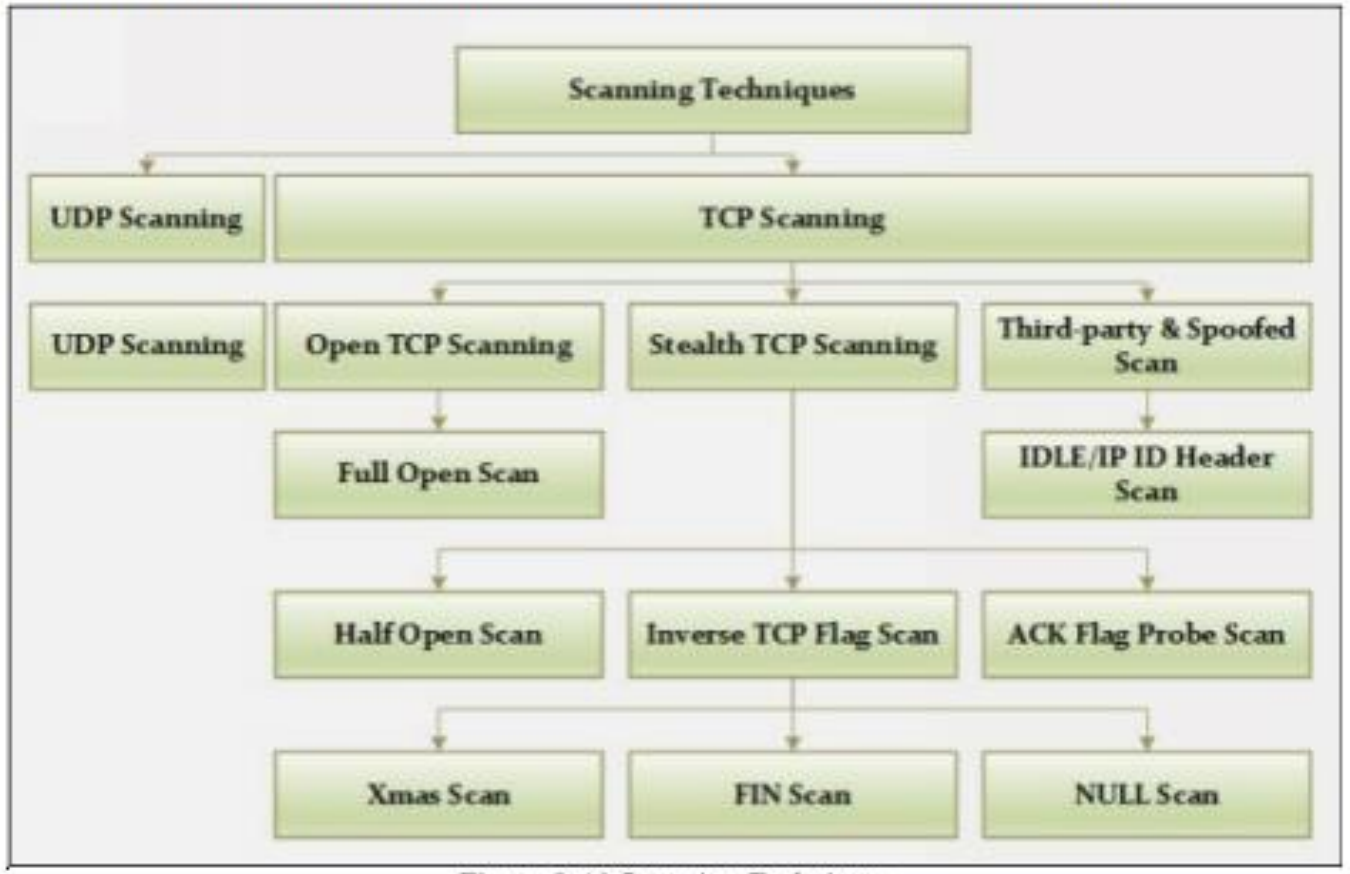


Figure 3-19 Scanning Techniques

Figure 3-19 Scanning Techniques

TCP Connect / Full Open Scan

Full Open Scan is the type of Scanning technique in which Three-way handshaking session initiates and completed. Full Open Scanning ensures the response that the targeted host is live and the connection is complete. It is a

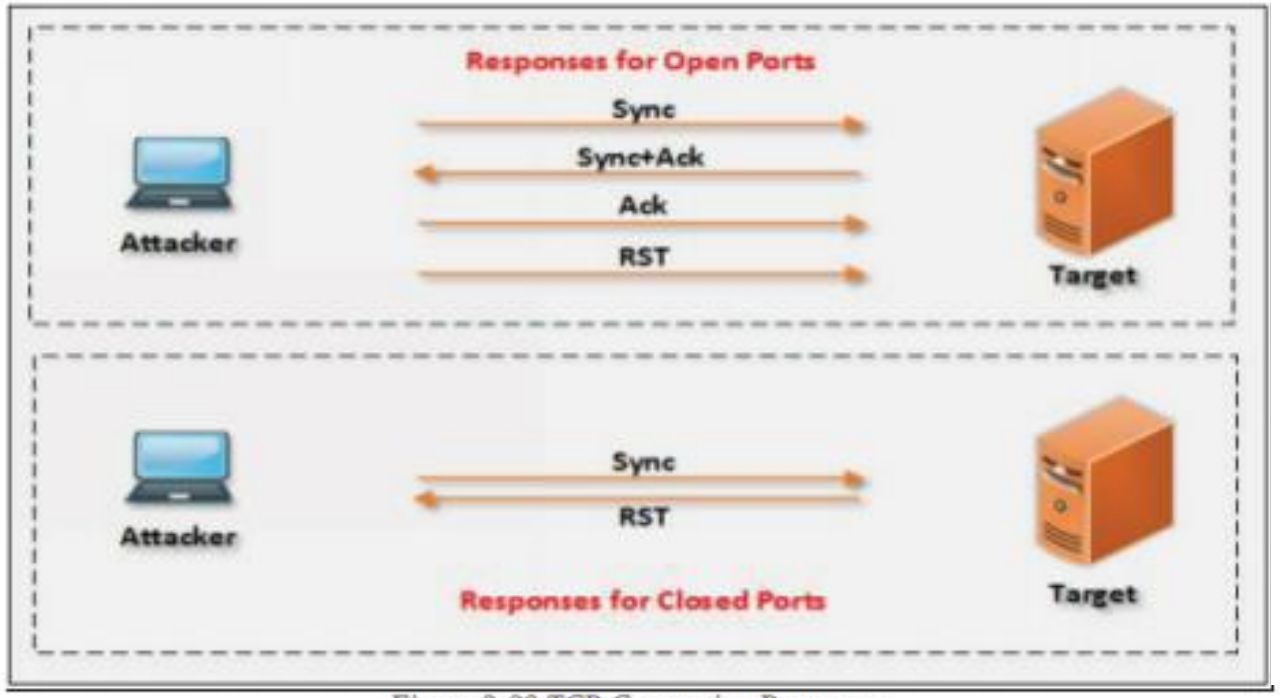


Figure 3-20 TCP Connection Responses

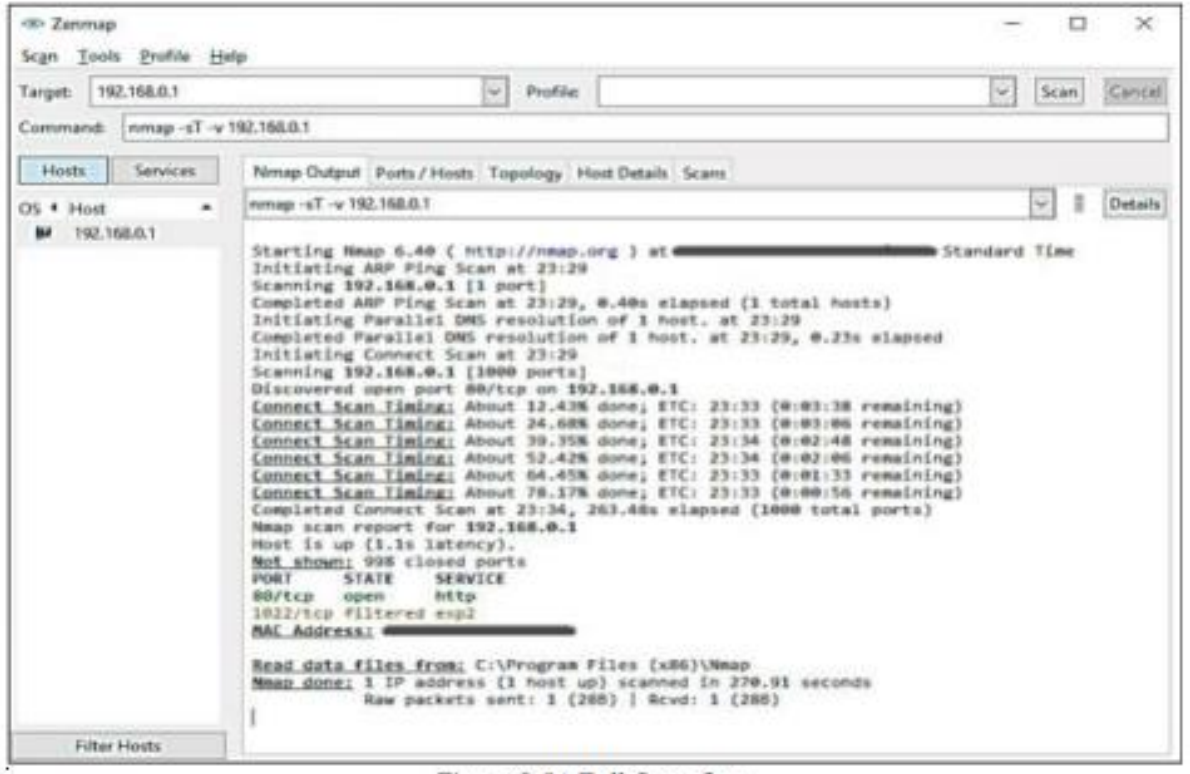


Figure 3-21 Full Open Scan

Stealth Scan (Half-open Scan)

Half-Open Scan is also known as Stealth Scan. To understand the Half-Open Scan processes, Consider the scenario of two hosts, Host A & Host B. Host A is the initiator of the TCP connection handshaking. Host A sends the Sync packet to initiate the handshaking. Receiving host (Host B) replies with Sync+Ack packet. Host A, Instead of Acknowledging the Host B with Ack packet, it responds with RST.

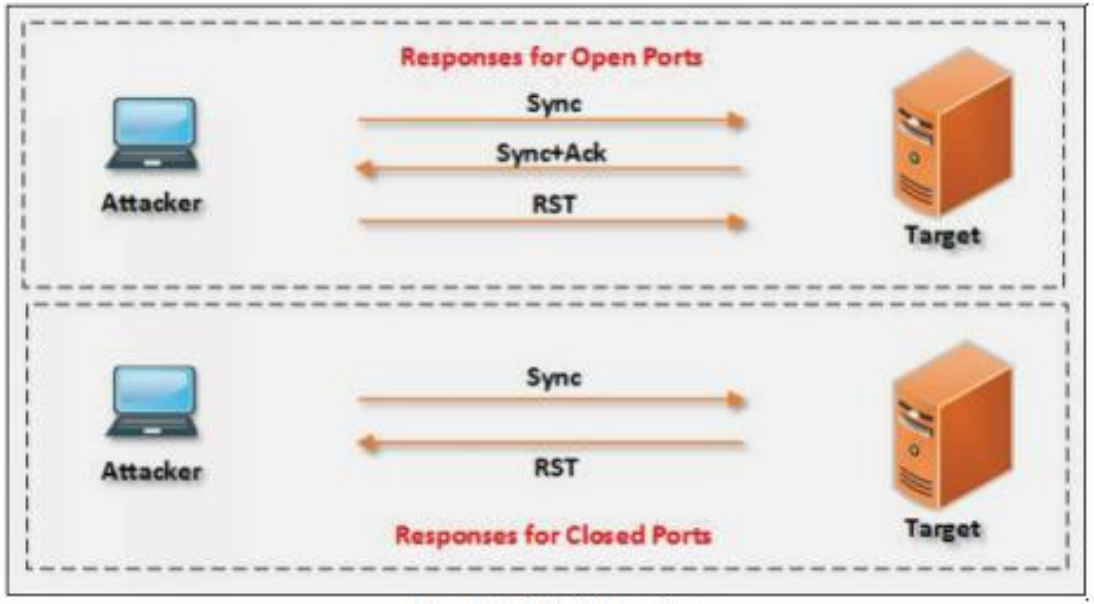


Figure 3-21 Half-Open Scan

To perform this type of scan in nmap use the syntax:

nmap –sS <*ip address or range*>

Observe the result in the following figure: -

Xmas Scan

Xmas Scan is the type of scan in which contains multiple flags. Packet sent to the target along with URG, PSH & FIN; or a packet having all flags creates an abnormal situation for the receiver. Receiving system has to take a decision when this condition occurs. Closed port responds with single RST packet. If the port is open, some systems respond as an open port, but the modern system ignores or dropped these requests because the combination of these flags is bogus. FIN Scan works only with Operating Systems with RFC-793 based TCP/IP Implementation. FIN Scan does not work with any current version of Windows typically Windows XP or later.

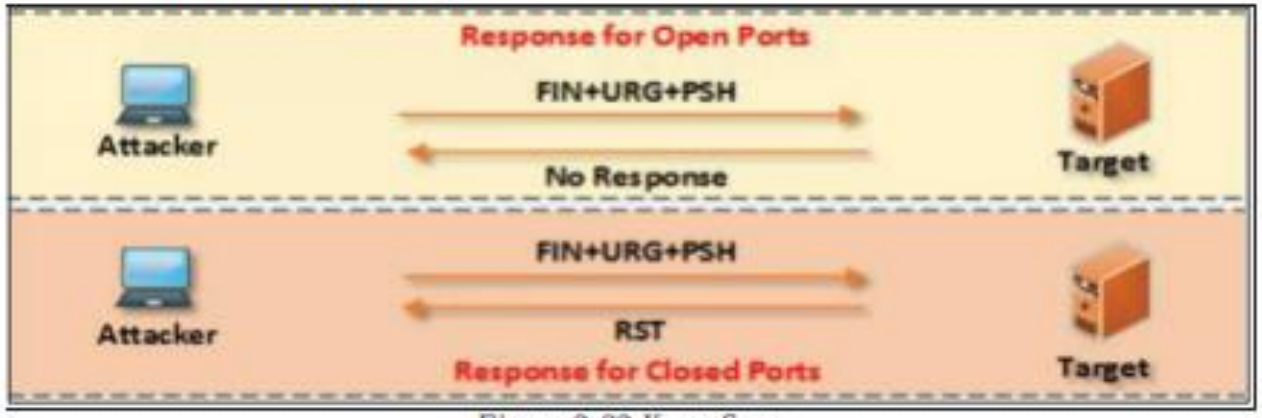


Figure 3-23 Xmas Scan

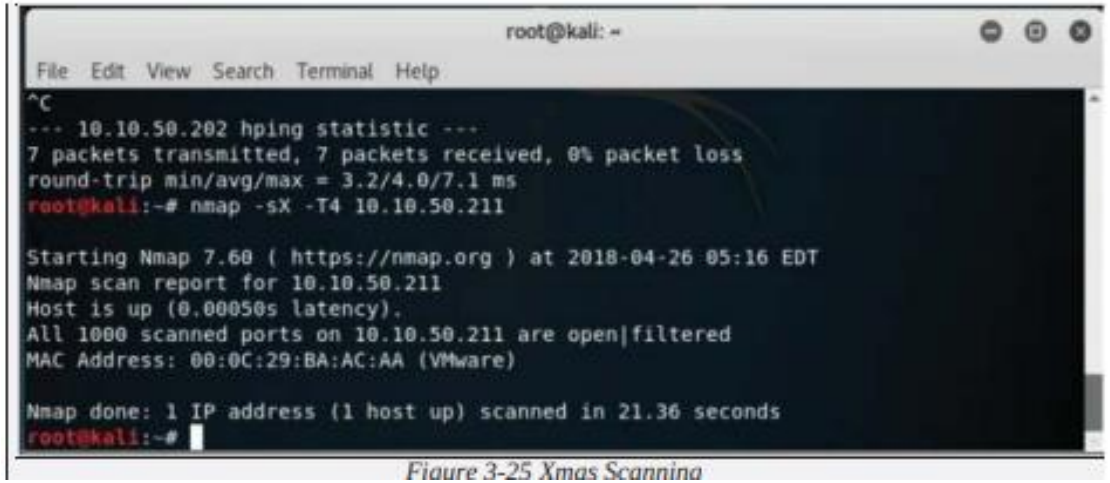


Figure 3-25 Xmas Scanning

FIN Scan

FIN Scan is the process of sending the packet having only FIN flag set. These packets can reliably pass the firewall. FIN Scan packets, when sent to the target, the port is considered to be open if there is no response. If the port is closed, RST is returned.

To perform this type of scan, use the syntax:

nmap –SF <*ip address or range*>

NULL Scan

NULL Scan is the process of sending the packet without any flag set. Responses are similar to FIN and XMAS Scan. If Null Scan packet sends to an open port, it brings no response. If Null Scan packet sends to the closed port, it brings RST packet. Performing this scan is comparatively easier to be detected as there is logically no reason to send a TCP packet without any flag.

To perform this type of scan, use the syntax:

nmap –sN <*ip address or range*>

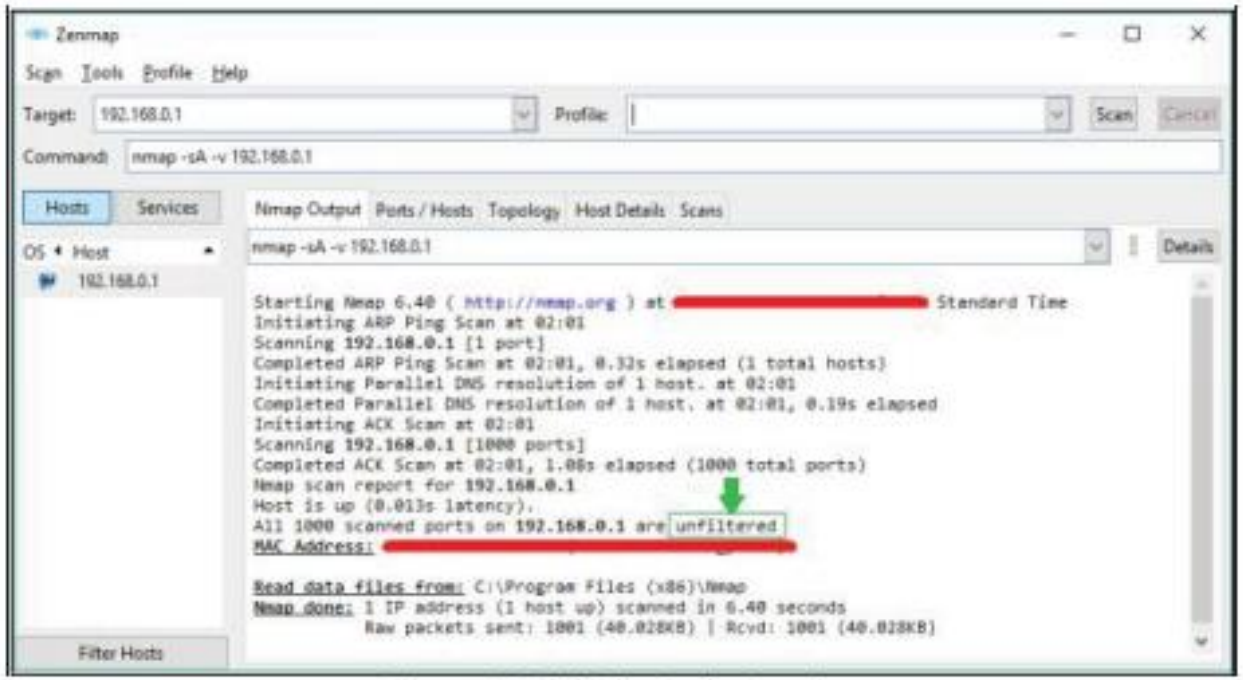


Figure 3-28 Ack Flag Probe Scanning

ACK Probe scanning also helps in identifying the filtering system. If RST packet receives from the target, it means that packets toward this port are not filtering. If there is no response, it means Stateful firewall is filtering the port.

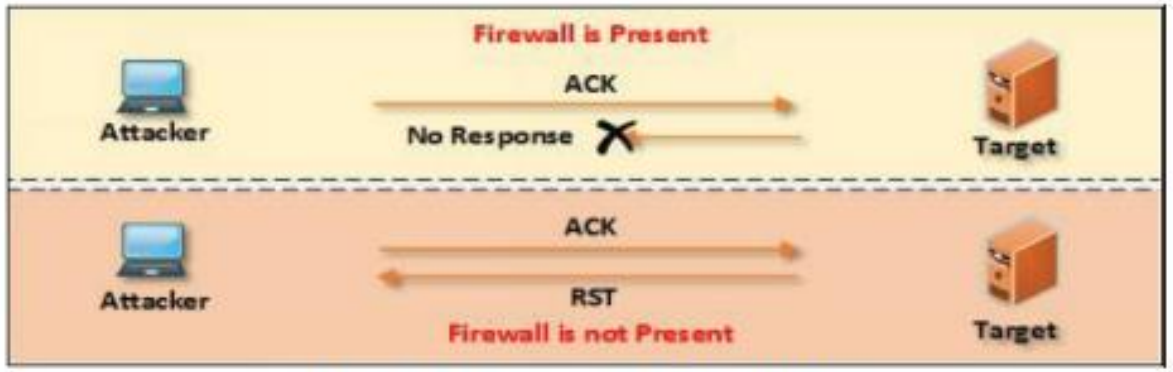


Figure 3-29 Ack Flag Probe Scanning Response

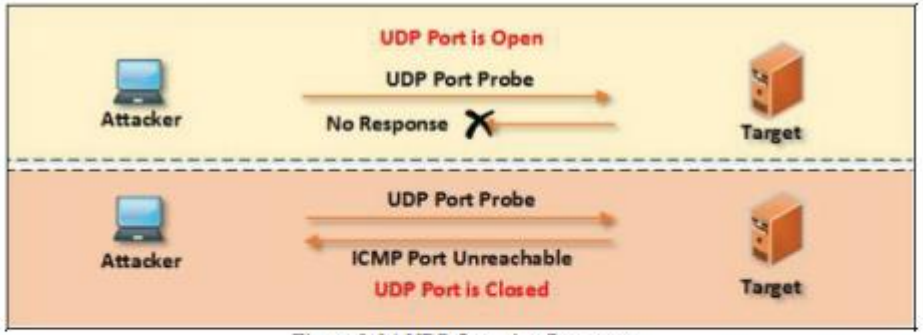


Figure 3-34 UDP Scanning Response

To perform this type of scan in nmap use the syntax:

nmap –sU –v <*ip address or range*>

Observe the result in the following figure: -

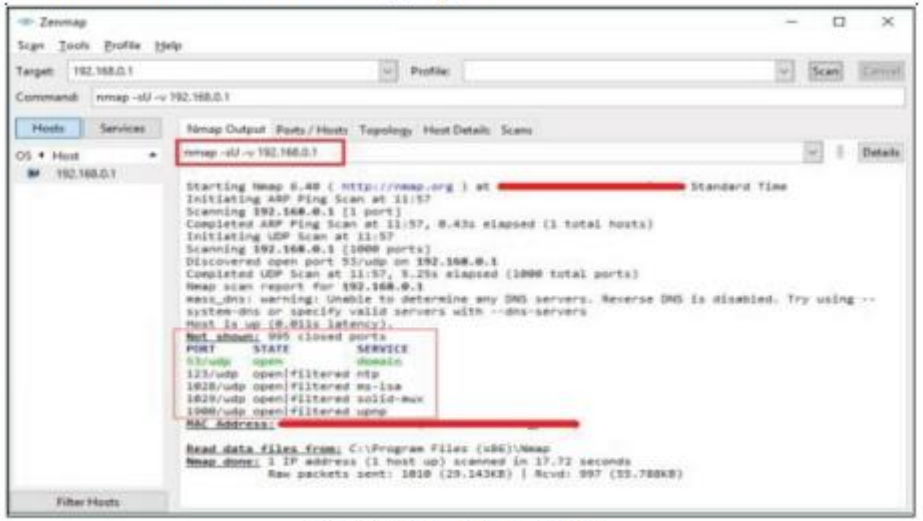


Figure 3-35 UDP Port Scanning

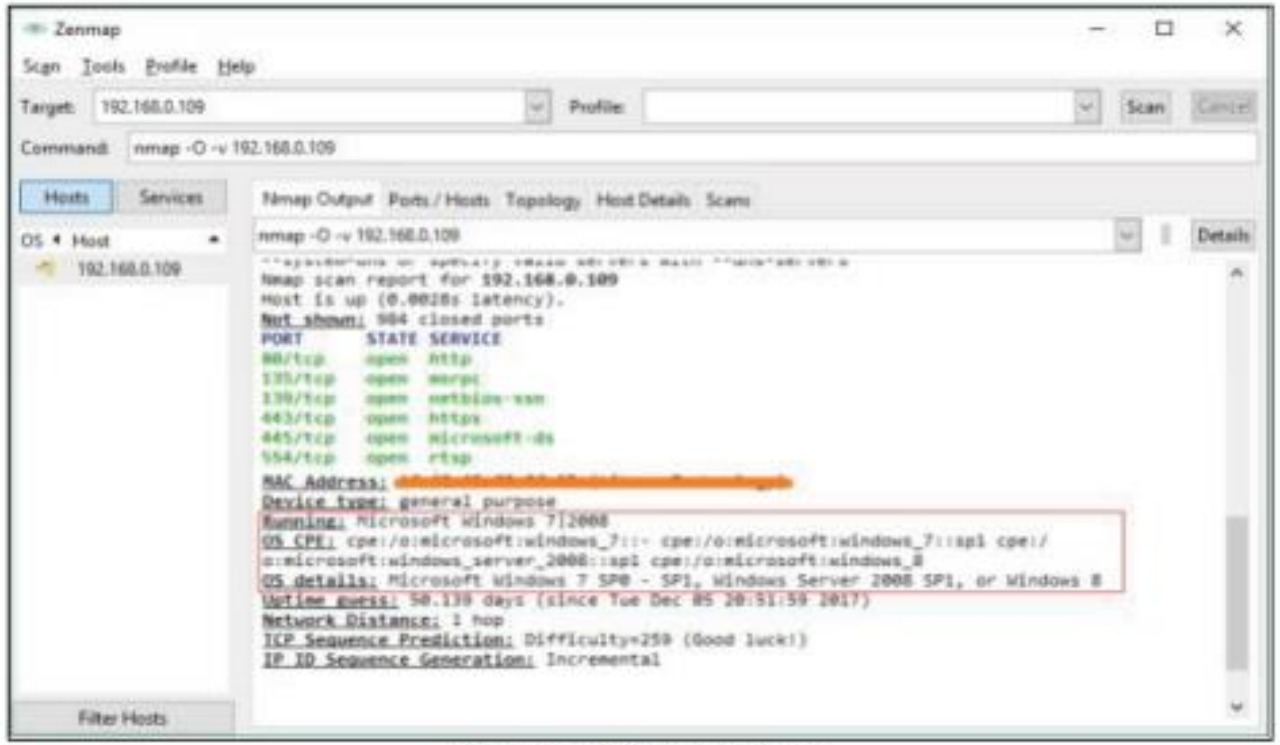


Figure 3-41 OS Fingerprinting

Nmap

Originally written for *Phrack* magazine in 1997 by Fyodor, Nmap has become one of the most popular port scanners and adds new features constantly, such as OS detection and fast multiple-probe ping scanning. Nmap also has a GUI front end called Zenmap that makes working with complex options easier. Nmap has been enhanced over the years because, like many other security tools, it's open source; if bugs are found, users can offer suggestions for correcting them.

Unicornscan

Unicornscan was developed to assist security testers in conducting tests on large networks and to consolidate many of the tools needed for large-scale endeavors. The developers thought that many current products were too slow at scanning thousands of IP addresses. Also, maintaining several security tools can be daunting, so the Unicornscan developers created a product to meet all the needs of security testers.

Unicornscan running on a typical Pentium computer can scan one port on each IP address of a Class B network. This equates to scanning 65,535 computers in 3 to 7 seconds, which brings UDP scanning to a new level. Most scanners using UDP scans can just make best guesses when trying to determine whether a port is closed, open, or filtered. Many security testers consider UDP scanning an unreliable method

Nessus and OpenVAS

Security testers should also investigate Nessus, a tool first released in 1998. Although Nessus is no longer under the GPL license, as most open-source software is, you can still download it free from Tenable Network Security Corporation (*www.nessus.org*) for noncommercial personal use. An open-source fork of Nessus called OpenVAS was developed in 2005, and it's one of the tools included in the online resources. OpenVAS functions much like a database server, performing complex queries while the client interfaces with the server to simplify reporting and configuration.

Conducting Ping Sweeps

Port scanners can also be used to conduct a ping sweep of a large network to identify which IP addresses belong to active hosts. In other words, to find out which hosts are

is returned. The problem with relying on ping sweeps to identify live hosts is that a computer might be shut down at the time of the sweep and indicate that the IP address doesn't belong to a live host. Another problem with ping sweeps is that many network administrators configure nodes to not respond to an ICMP Echo Request (type 8) with an ICMP Echo Reply (type 0). This response doesn't mean the computer isn't running; it just means it isn't replying to the attack computer.

Fping

With the Fping tool (*www.fping.com*), you can ping multiple IP addresses simultaneously. Fping, included on the companion website, can accept a range of IP addresses entered at a command prompt, or you can create a file containing multiple IP addresses and use it as input for the Fping command. For example, the `fping -f ip_address.txt` command uses ip_address.txt, which contains a list of IP addresses, as its input file. The input file is usually created with a shell-scripting language so that you don't need to type the thousands of IP addresses needed for a ping sweep on a Class B network, for example. Figure 5.4 shows some parameters you can use with the Fping command.

To ping sweep a range of IP addresses without using an input file, you use the command `fping -g BeginningIPaddress EndingIPaddress`. The `-g` parameter is used when no input file is available. For example, the `fping -g 193.145.85.201 193.145.85.220` command returns the results shown in Figure 5.5.

Hping

You can also use the Hping tool (*www.hping.org/download*) to perform ping sweeps.

or otherwise modified IP packets. This tool offers a wealth of features, and security testers should spend as much time as possible learning this advanced port-scanning tool. For a quick overview, use the `hping -help |less` command, and browse

Understanding Scripting

Some tools might need to be modified to better suit your needs as a security tester. Creating a customized script—a program that automates a task that takes too much time to perform manually—can be a time-saving solution. As mentioned, Fping can

```
File  Edit  View  Terminal  Go  Help
#!/bin/sh
# Myshell
# This program creates a text file named ip_address.txt that contains 254
# IP addresses using 193.145.85.0 as the network ID. The file created can
# be used as an input file for the fping utility. For example:
#   fping -f ip_address.txt

# Initialize variables

network_id="193.145.85."
count=0

# Stop the loop when count is equal to 254. The 'le' signifies less than
# or equal to 253, so the count variable will be incremented one more
# time after count is equal to 253. We do not want to create an IP
# address of 193.145.85.255  because this would be the broadcast address
# of the 193.145.85.0/24 network. Ping sweeping a broadcast address can
# be problematic.

while [ "$count" -le 253 ]
do

        count=$(($count+1))
        printf "%s%s\n" $network_id $count >> ip_address.txt
done

exit 0
~
"Myshell" 27L, 818C written                                2,2           All
```

Courtesy Course Technology/Cengage Learning

Figure 5.9
A shell script

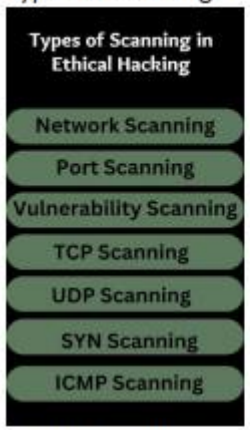
Bash script header file #!/bin/sh
//You are going to create 253 ip address in some seconds using scripts. If you are manually entering it, will take time.
// Example: 192.168.1.0 to 192.168.1.253
Constant part: "192.168.1."
Here you can set that as network_id="192.168.1."
0 to 253 only you are changing, so keep it as counter, count. Initially set it as 0. Place a condition and do some thing. So you while…do statement.
In bash script, for getting values you have to place dollar symbol before variable name.
In side do, you have to increment counter and also print result and append all results in a text file. For appending in linux you can to use >> syntax.
Save it as MyShell.sh
chmod +x MyShell.sh
./MyShell.sh

Colourful Thank You Slide Design

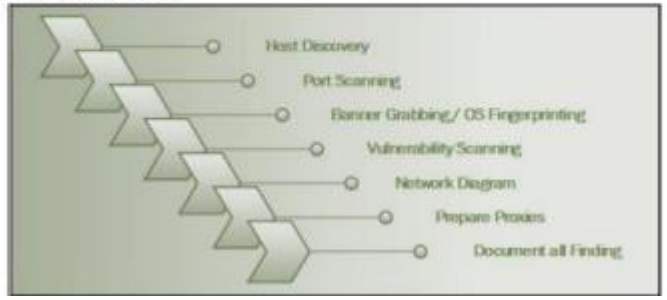
T H A N K Y O U

Question Bank

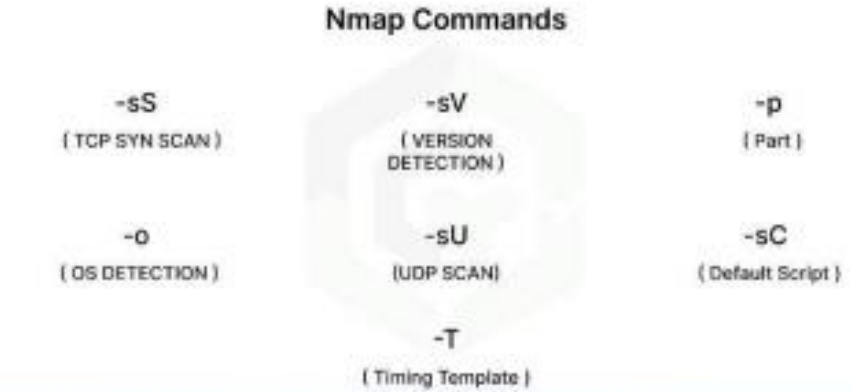
1. Types of scanning

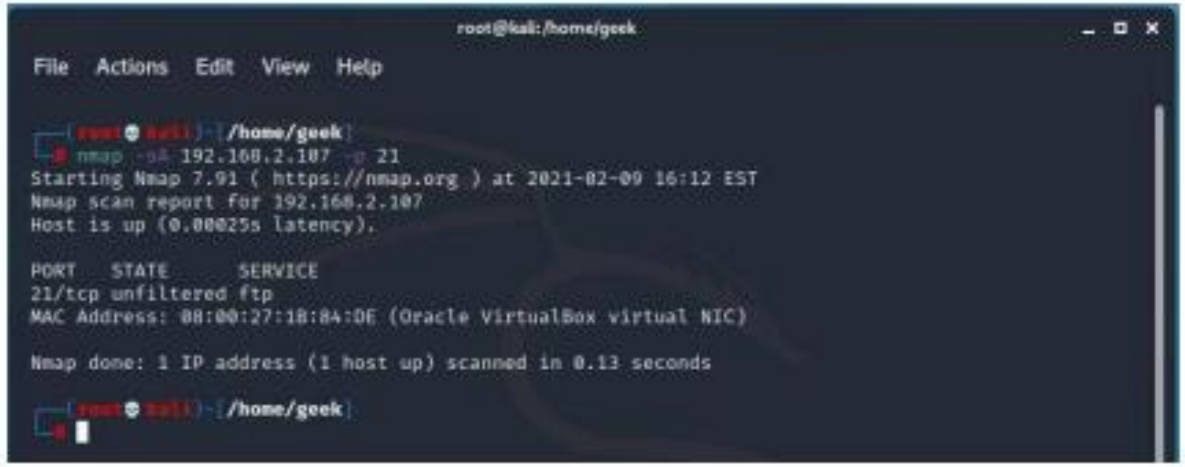


Scanning steps:

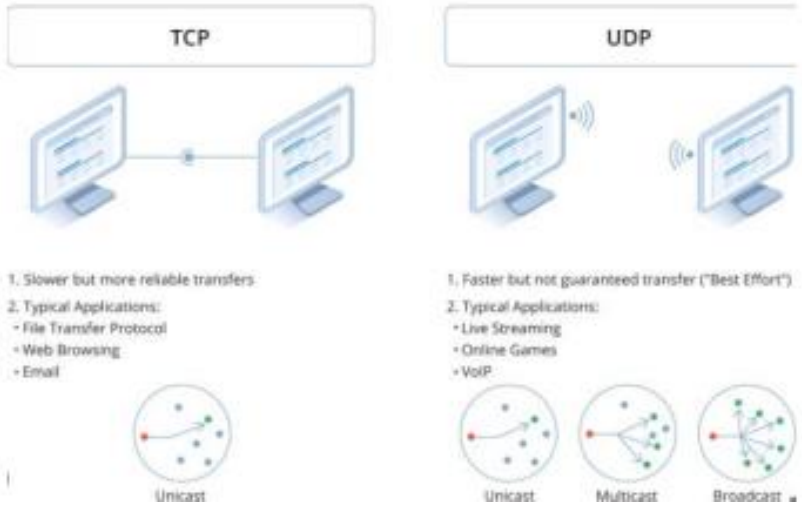


3. How to do network scanning.





4. Logical ports and its types



The 6 Different Types of Hackers

Black Hat Hackers: Bad hackers who use cyber attacks to gain money or to achieve another agenda.

These hackers penetrate systems without permission to exploit known or zero-dav vulnerabilities.

White Hat Hackers: Ethical hackers who protect your systems from black hat hackers.

Penetrate the system with the owner's permission to find and fix security vulnerabilities and mitigate cyberattacks.

Grey Hat Hackers: Hackers who cruise the line between being good and bad. Penetrate systems without permission but typically don't cause harm.

Draw attention to vulnerabilities and often offer a solution to patch them by charging fees.

Red Hat Hackers: Hackers who use cyber attacks to attack black hat hackers.

Their intentions are noble, but these hackers often take unethical or illegal routes to take down bad hackers.

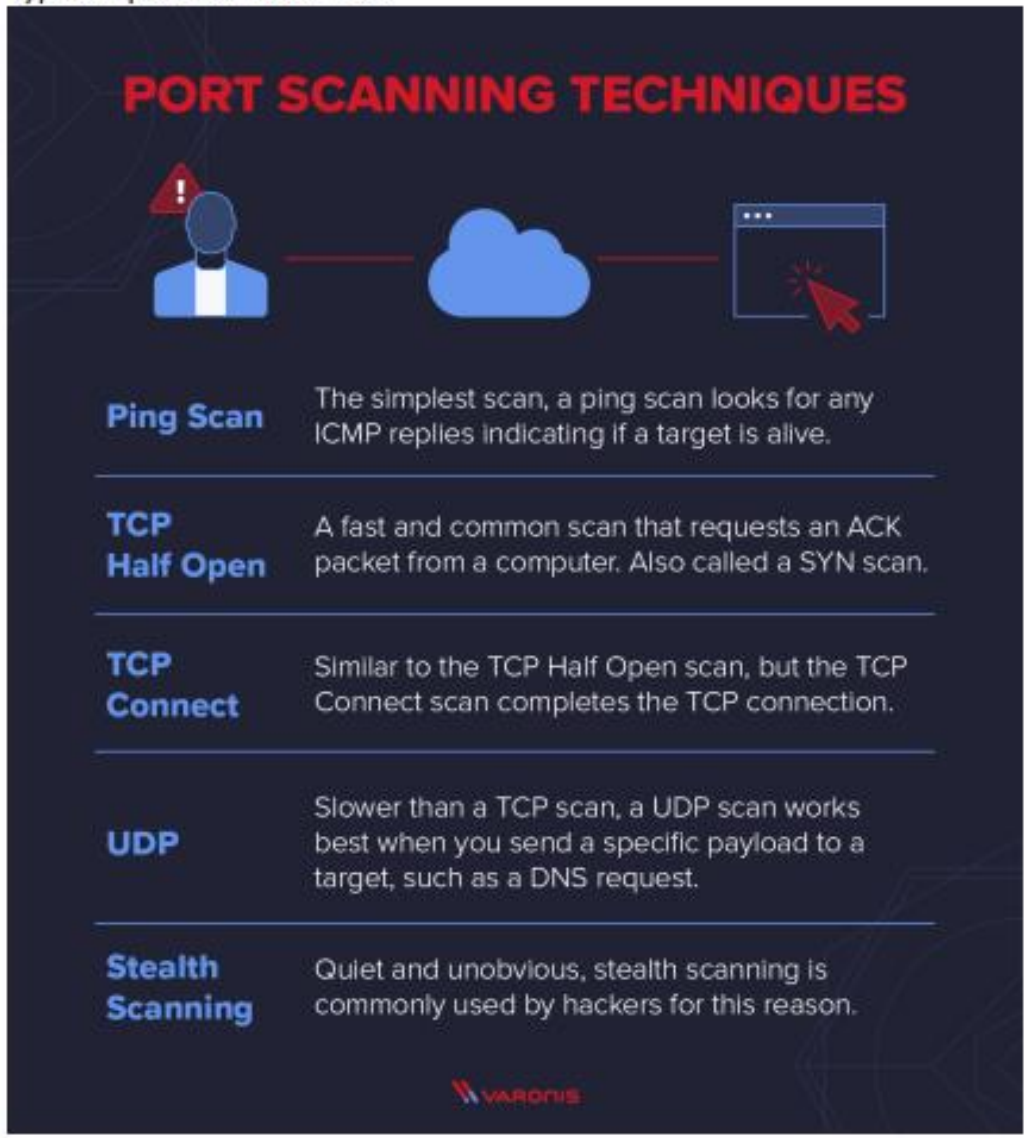
Blue Hat Hackers: Hackers who seek to take personal revenge, or outside security professionals that companies hire to test new software & other products to find vulnerabilities prior to release.

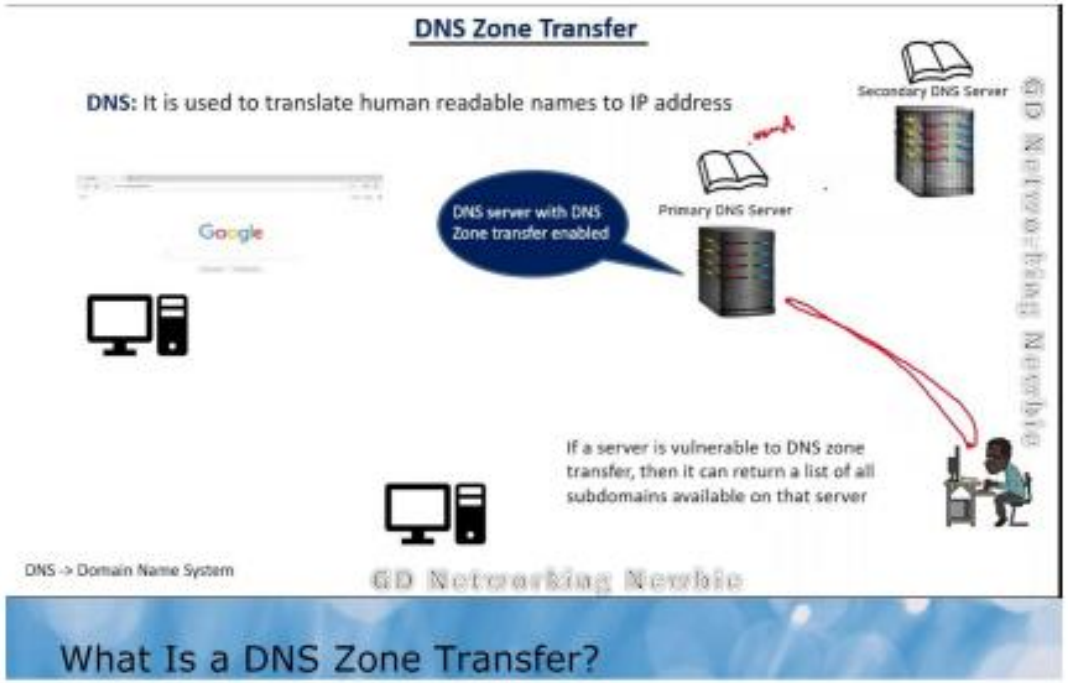
Green Hat Hackers: Newbie hackers who are learning to hack.

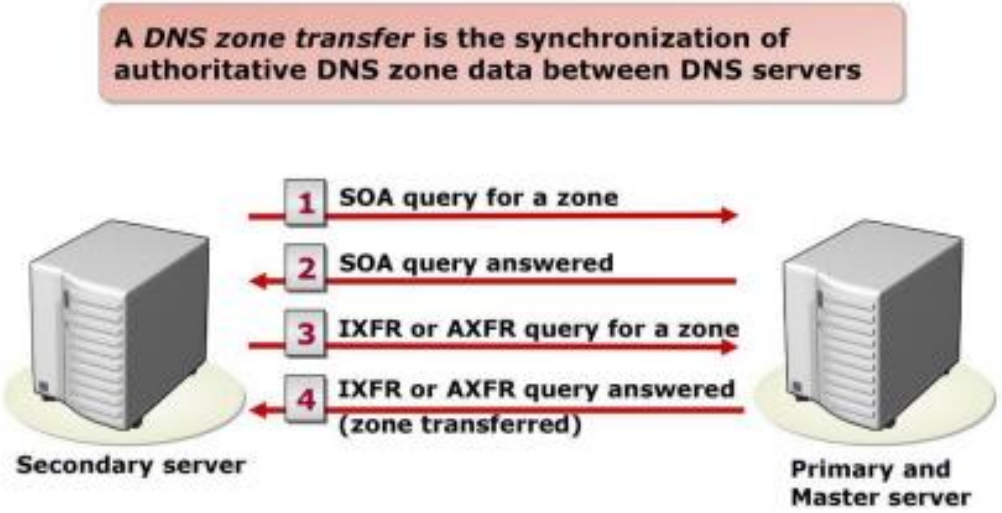
They're often not aware of the consequences of their actions & cause unintentional damage without knowing how to fix it.

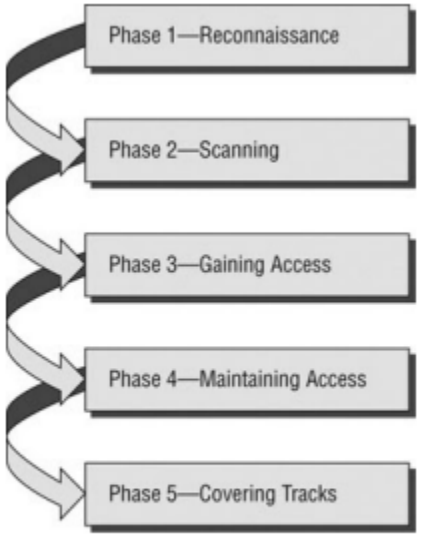
6. Why ethical hacking is required in firms: Ethical hacking is important for cybersecurity because it is used to secure crucial data from adversaries. Ethical hacking helps prevent malicious actors from exploiting the organisation or an individual. It also helps bolster cybersecurity measures and reduces the risk of getting blackmailed.
7. Types of reconnaissance?
   There are two main types of reconnaissance: active and passive reconnaissance.
   a) With active reconnaissance, hackers interact directly with the computer system and attempt to obtain information through techniques like automated scanning or manual testing and tools like ping and netcat. Active recon is generally faster and more accurate, but riskier because it creates more noise within a system and has a higher chance of being detected.
   b) Passive reconnaissance gathers information without directly interacting with systems, using tools such as Wireshark and Shodan and methods such as OS fingerprinting to gain information.

8. Types of port scan methods?









Phase 1: Passive and Active Reconnaissance

Passive reconnaissance involves gathering information about a potential target without the targeted individual's or company's knowledge. Passive reconnaissance can be as simple as watching a building to identify what time employees enter the building and when they leave. However, most reconnaissance is done sitting in front of a computer.

When hackers are looking for information on a potential target, they commonly run an Internet search on an individual or company to gain information. I'm sure many of you have performed the same search on your own name or a potential employer, or just to gather information on a topic. This process when used to gather information regarding a TOE is generally called *information gathering*. Social engineering and dumpster diving are also considered passive information-gathering methods.

Sniffing the network is another means of passive reconnaissance and can yield useful information such as IP address ranges, naming conventions, hidden servers or networks, and other available services on the system or network. Sniffing network traffic is similar to building monitoring: a hacker watches the flow of data to see what time certain transactions take place and where the traffic is going. Sniffing network traffic is a common hook for many ethical hackers. Once they use some of the hacking tools and are able to see all the data that is transmitted in the clear over the communication networks, they are eager to learn and see more.

Sniffing tools are simple and easy to use and yield a great deal of valuable information which literally let you see all the data that is transmitted on the network. Many times this includes usernames and passwords and other sensitive data. This is usually quite an eye-opening experience for many network administrators and security professionals and leads to serious security concerns.

Active reconnaissance involves probing the network to discover individual hosts, IP addresses, and services on the network. This process involves more risk of detection than passive reconnaissance and is sometimes called *rattling the doorknobs*. Active reconnaissance can give a hacker an indication of security measures in place (is the front door locked?), but the process also increases the chance of being caught or at least raising suspicion. Many software tools that perform active reconnaissance can be traced back to the computer that is running the tools, thus increasing the chance of detection for the hacker.

Both passive and active reconnaissance can lead to the discovery of useful information to use in an attack. For example, it's usually easy to find the type of web server and the operating system (OS) version number that a company is using. This information may enable a hacker to find a vulnerability in that OS version and exploit the vulnerability to gain more access.

Phase 2: Scanning

Scanning involves taking the information discovered during reconnaissance and using it to examine the network. Tools that a hacker may employ during the scanning phase include

- Dialers
- Port scanners
- Internet Control Message Protocol (ICMP) scanners
- Ping sweeps
- Network mappers
- Simple Network Management Protocol (SNMP) sweepers
- Vulnerability scanners

Hackers are seeking any information that can help them perpetrate an attack on a target, such as the following:

- Computer names
- Operating system (OS)
- Installed software
- IP addresses
- User accounts

Phase 3: Gaining Access

Phase 3 is when the real hacking takes place. Vulnerabilities exposed during the reconnaissance and scanning phase are now exploited to gain access to the target system. The hacking attack can be delivered to the target system via a local area network (LAN), either wired or wireless; local access to a PC; the Internet; or offline. Examples include stack-based buffer overflows, denial of service, and session hijacking. Gaining access is known in the hacker world as *owning* the system because once a system has been hacked, the hacker has control and can use that system as they wish.

Phase 4: Maintaining Access

Once a hacker has gained access to a target system, they want to keep that access for future exploitation and attacks. Sometimes, hackers *harden* the system from other hackers or security personnel by securing their exclusive access with backdoors, rootkits, and Trojans. Once the hacker owns the system, they can use it as a base to launch additional attacks. In this case, the owned system is sometimes referred to as a *zombie* system.

Phase 5: Covering Tracks

Once hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action. Hackers try to remove all traces of the attack, such as log files or intrusion detection system (IDS) alarms. Examples of activities during this phase of the attack include

- Steganography
- Using a tunneling protocol
- Altering log files

11. Trojan horse and its working

A **Trojan horse**, or **Trojan**, is a type of malicious code or software that looks legitimate but can take control of your computer. A **Trojan** is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network. ... Once installed, a **Trojan** can perform the action it was designed for.

12. Reconnaissance phase apply in information gathering and foot printing: Footprinting involves gathering information about a target system, while reconnaissance is the broader process of information gathering in ethical hacking. By conducting thorough **reconnaissance footprinting**, security professionals can assess risks, strengthen defences, and prevent potential cyber threats.
13. Port scanning doing is a crime or not?

Unauthorized port scanning, for any reason, is strictly prohibited. Even if an ISP does not explicitly ban unauthorized port scanning, they might claim that some "anti-hacking" provision applies.

Keylogger is one kind of surveillance technology that is used to monitor and capture keystrokes of a specific device. It can work from both hardware and software

Logic Bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

15. Mitigating the risk of malware infection

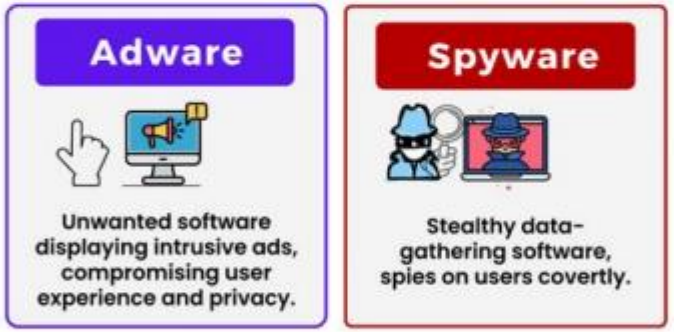
PROTECTION AGAINST MALWARE

cyber-security-1915628_640.png

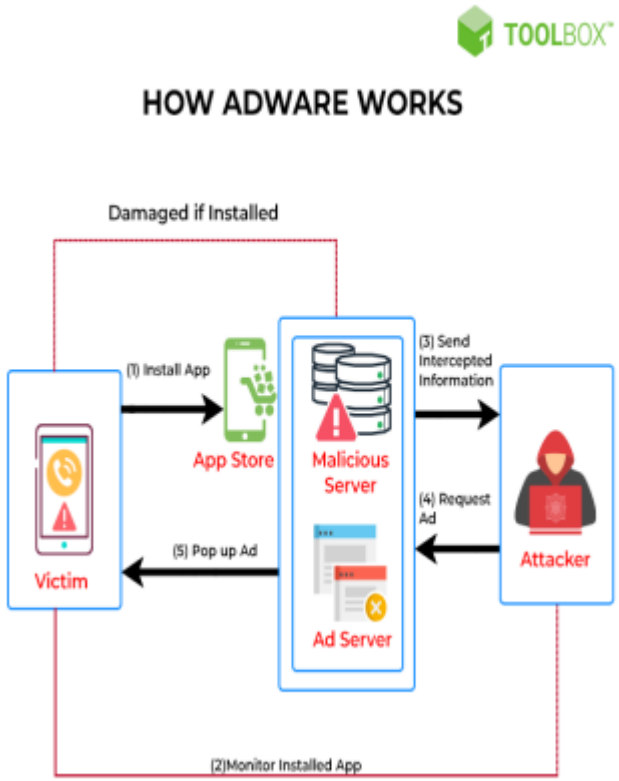
As technically feasible, deploy anti-malware software on all endpoints capable of running anti-malware software including, but not limited to: laptops, desktops, servers, tablets, and smartphones.

- Configure anti-malware software to perform periodic scans of the endpoint and real-time scans of all files from external sources as the files are downloaded, opened, or executed;
- Configure anti-malware software to quarantine any malicious code detected and to send an alert to the organization's IT service desk and/or information security team;
- Configure anti-malware software to automatically apply and keep current with anti-malware vendor updates;
- Ensure anti-malware mechanisms are actively running and cannot be disabled or altered by users; and
- Configure anti-malware software to maintain an audit log of all anti-malware software activity.

16. Spyware and adware working with example



- **Adware** is software that displays unwanted advertisements to a user, often via pop-up windows or banners in web browsers.
- **Spyware** is software that covertly gathers user information without the user's knowledge. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else.



17. Network and system-based information gathering tools

Information Gathering is the process of collecting, organizing and analyzing data and intelligence about a target, such as computer network, website or individual, to identify vulnerabilities that can be

a) Nmap (Network Mapper): Nmap is an open-source network scanning tool that is used in identifying open ports, services and hosts on a network.
b) Wireshark: Wireshark is a powerful network packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development. It displays captured packet data in a much more detailed format.
c) Buster: Buster is used to generate and verify emails and return information associated with them.
d) R3conlz3r: This is a passive reconnaissance tool for web information gathering. It provides a powerful environment in which open source intelligence web-based footprinting can be conducted thoroughly.
e) Shodan: Shodan is a search engine for discovering internet-connected devices. It allows search for various types of servers (webcams, routers, etc) connected to the internet using a variety of filters.
f) theHarvester: theHarvester is a tool that was developed in python. It is used to gather information like emails, subdomains, hosts, employee names, open ports and banners from different public domains like search engines and Shodan database.
g) Maltego: Maltego is a powerful OSINT tool for visualizing and analyzing the links between people, organizations, and online resources. It helps in mapping the digital footprint of a target.
h) Metagoofil: Metagoofil is an information gathering tool designed for extracting metadata of public documents (pdf,doc,xls,ppt,docx,pptx,xlsx) belonging to a target.
i) Recon-ng: Recon-ng is an open-source reconnaissance framework designed with the goal of providing a powerful environment to conduct open source web-based reconnaissance quickly and thoroughly.
j) FinalRecon: FinalRecon is an all in one automatic web reconnaissance tool written in python. It's goal is to provide an overview of the target in a short amount of time while maintaining the accuracy of results.
k) UserRecon: UserRecon is a simple username recognition tool. It can search a username from over 180 different social media platforms.
l) Photon: Photon is a fast website crawler that can extract URLs with parameters, intel (social media account, email), files, secret keys, subdomains and DNS related data while crawling.
m) Th3 Insp3ctor: This is an OSINT tool which is used to gather information about a target, such as details about the server, whois info, target IP, hosting phone, email, sub-domains, visitors per day, etc.
n) EmailHarvester: EmailHarvester is a powerful tool used to retrieve domain email addresses from search engines (Google, Bing, Yahoo, ASK, Baidu, Dogpile, Exalead).
o) Pymeta: Pymeta is an automated tool developed in python which can search for queries, identify and get the following file types (pdf, xls, xlsx, csv, doc, docx, ppt, pptx) from a given target domain using google and bing scraping engines.
p) WHOIS Lookup: WHOIS lookup tools provide information about domain registrations, including the owner's contact details and registration history.
q) SpiderFoot: SpiderFoot is an OSINT automation tool that collects information about domains, IP addresses, email addresses, and other online assets. It provides a comprehensive report on potential security risks.
r) Gobuster: Gobuster is a directory and file brute-forcing tool. It helps identify hidden directories and files on web servers, which can be useful for finding vulnerabilities.
s) TinEye: TinEye is a reverse image search engine and a valuable tool for discovering information about images found online.
t) Google Dorks: Google Dorks are specific search queries used to extract sensitive information from search engines like Google. They are often used to find vulnerable web applications and exposed data.

18. Malware detection based on signatures and white or black listing.

Signature-based malware detection uses signatures and the best way to describe them is like the 'fingerprint' of a virus which is unique to that specific virus. This makes signature-based malware detection accurate in identifying known threats, as it matches the threat with its known code.

Signature-based malware detection is a very effective technique used against known and frequent attacks, such as phishing, malware, or denial-of-service. It is also very easy to install and maintain, as it relies on regular updates of the signature database from security experts or vendors.

Whitelisting and blacklisting are two methodologies to control access to websites, email, software and IP addresses on networks. Whitelisting denies access to all resources and only the "owner" can allow access. Blacklisting allows access to all with the provision that only certain items are denied.

FACT 1: WHITELISTING

Whitelisting has advantages in that you control access to the website or virtual resource you want your business to use, however, is less dynamic and more restrictive in terms of ease of use and versatility. This is a control mechanism where you deny access to all resources by default then allow access to resources by name. Think of your home, where only you and your family can get access the front door. Everyone in your family would have a front door key, but some individuals don't have keys to every door. You may have a shed out back that only you have they key because dangerous chemicals are stored there. The disadvantage is that not everyone in your family has open access to the shed and would have to ask permission to get something out. Now, that may work for a small family, but would be unworkable unless the number of employees requiring access is small. This type of access control is useful for financial or personnel records, where a business might have only 2-5 employees who access these files, software or websites.

FACT 2: BLACKLISTING

Blacklisting is advantageous in that it allows free and open access to any email, website, IP address or software as long as it's not a security risk. This is the concept that all web traffic is allowed, and certain items are disallowed by name or circumstance (aka security risk).

FACT 4: EXAMPLES

Some specific examples of white listing and blacklisting that might apply to your small business:

- Software
  - Whitelisting
    - Employers restrict access to applications used by a select number of employees to perform their role for the business – such as accounting, human resources, and/or payroll. Access would be restricted on the machine or server used for these functions.
  - Blacklisting
    - Employers restrict access to games or prevent applications, which could contain malware.
- Email
  - Whitelisting
    - Employers would only receive emails from clients, or other employees.
  - Blacklisting
    - Employers would block domains who are known to send spam, junk, or phishing emails.
- Websites
  - Whitelisting
    - Employers restrict access to websites used by a select number of employees to perform their role for the business – such as accounting.
  - Blacklisting
    - Employers restrict access to sites which may interfere with workplace performance such as: pornography, gaming sites, social networking

19. Information systems and its threats.

Threats

To protect an organization's information, you must

1. Know yourself

(i.e) be familiar with the information to be protected, and the systems that store, transport and process it.

2. Know the threats you face

To make sound decisions about information security, management must be informed about the various threats facing the organization, its application, data and information systems.

- A threat is an object, person, or other entity, that represents a constant danger to an asset.
- By examining each threat category in turn, management effectively protects its information through **policy, education and training, and technology controls**

Threats to Information Security

Categories of threat		Examples
Acts of human error or failure	--	Accidents, employee mistakes
Compromises to intellectual property	--	Piracy, copyright infringement
Deliberate acts of espionage or trespass	--	Unauthorized access and/or/data collection
Deliberate acts of information extortion	--	Blackmail or information disclosure
Deliberate acts of sabotage or vandalism	--	Destruction of systems or information
Deliberate acts of theft	--	Illegal confiscation of equipment or information

Deliberate software attacks	--	Viruses, worms, macros, denial-of-service
Forces of nature	--	Fire, flood, earthquake, lightning
Deviations in quality of service	--	ISP, power, or WAN service providers
Technical hardware failures or errors	--	Equipment failure
Technical software failures or errors	--	Bugs, code problems, unknown loopholes
Technological obsolescence	--	Antiquated or outdated technologies

Colourful Thank You Slide Design

THANK YOU