An Introduction to Ethical Hacking

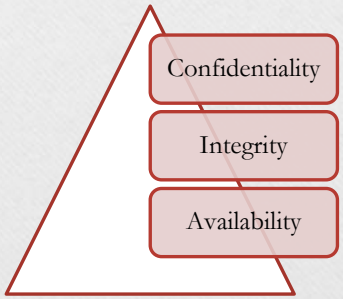
Content

- Introduction
- Ethical Hacking
- Hackers
- Types of Hackers
- Hacking Process
- Why do We need Ethical Hacking
- Required Skills of an Ethical Hacker

Introduction

SECURITY

- Security is the condition of being protect against danger or loss. In the general sense, security is a concept similar to safety.
- Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.



CIA TRIAD

Ethical Hacking

Ethical hacking can also ensure that vendors claims about the security of their products legitimate.

- Ethical hacking also known as penetration testing or white-hat hacking, involves the same tools, tricks, and techniques that hackers use, but with one major difference that Ethical hacking is legal.

Ethical Hacking

- Independent computer security Professionals breaking into the computer systems.
- Neither damage the target systems nor steal information.
- Evaluate target systems security and report back to owners about the vulnerabilities found.

“Ethical Hacking is when a person is allowed to hacks the system with the permission of the product owner to find weakness in a system and later fix them.”

What is Ethical Hacking?

- **Ethical hacking** refers to the act of locating weaknesses and vulnerabilities of computer and information systems by duplicating the intent and actions of malicious **hackers.**
- Identify vulnerabilities visible from Internet at particular point of time.
- It is Legal.
- Permission is obtained from the target.
- Part of an overall Security Program.
- Ethical Hacker possesses same skills, mindset and tools of a hacker but the attacks are done in a non-destructive manner.

Clip slide

Hacker v/s Ethical Hacker?

- **Hacker**
  - Access computer system or Network without authorization
  - Breaks the law
- **Ethical Hacker**
  - Performs most of same activities but with owner's permission
  - Employed by organizations to perform Penetration Tests

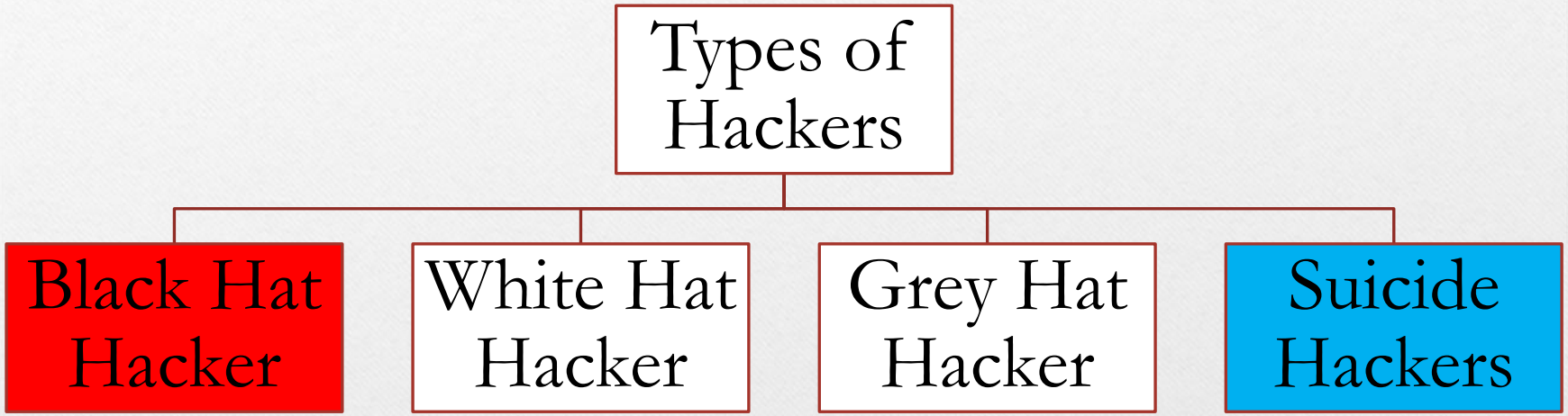
Why do People Hack?

- To make Security Stronger (Ethical Hacking)
- Hack other systems secretly & steal important information that causes financial loss, reputation loss to targeted organization
- Revenge
- Show off
- Just for Fun

Hackers

- A person who enjoys learning details of a programming language or system
- A person who enjoys actually doing the programming rather than just theorizing about it
- A person capable of appreciating someone else's hacking
- A person who picks up programming quickly
- A person who is an expert at a particular programming language or system

Types of Hackers



Types of Hacker

- White Hat Hacker
  - Good guys who don't use their skills for illegal purposes.
  - Computer Security Experts & help to protect from Black Hat.

- Black Hat Hacker
  - Bad guys who use their skills maliciously for personal gain.
  - Hack banks, steal credit cards & deface websites.

- Grey Hat Hacker
  - It is combination of both Black & White Hat Hackers.
  - Goal of Grey Hat Hackers is to provide National Security.

Black-Hat Hacker

- A black hat hackers or crackers are individuals with extraordinary computing skills, resorting to malicious or destructive activities.

- That is black hat hackers use their knowledge and skill for their own personal gains probably by hurting others.

White-Hat Hacker

- White hat hackers are those individuals professing hacker skills and using them for defensive purposes.
- This means that the white hat hackers use their knowledge and skill for the good of others and for the common good.

Grey-Hat Hackers

- These are individuals who work both offensively and defensively at various times.
- We cannot predict their behavior.
- Sometimes they use their skills for the common good while in some other times he uses them for their personal gains.

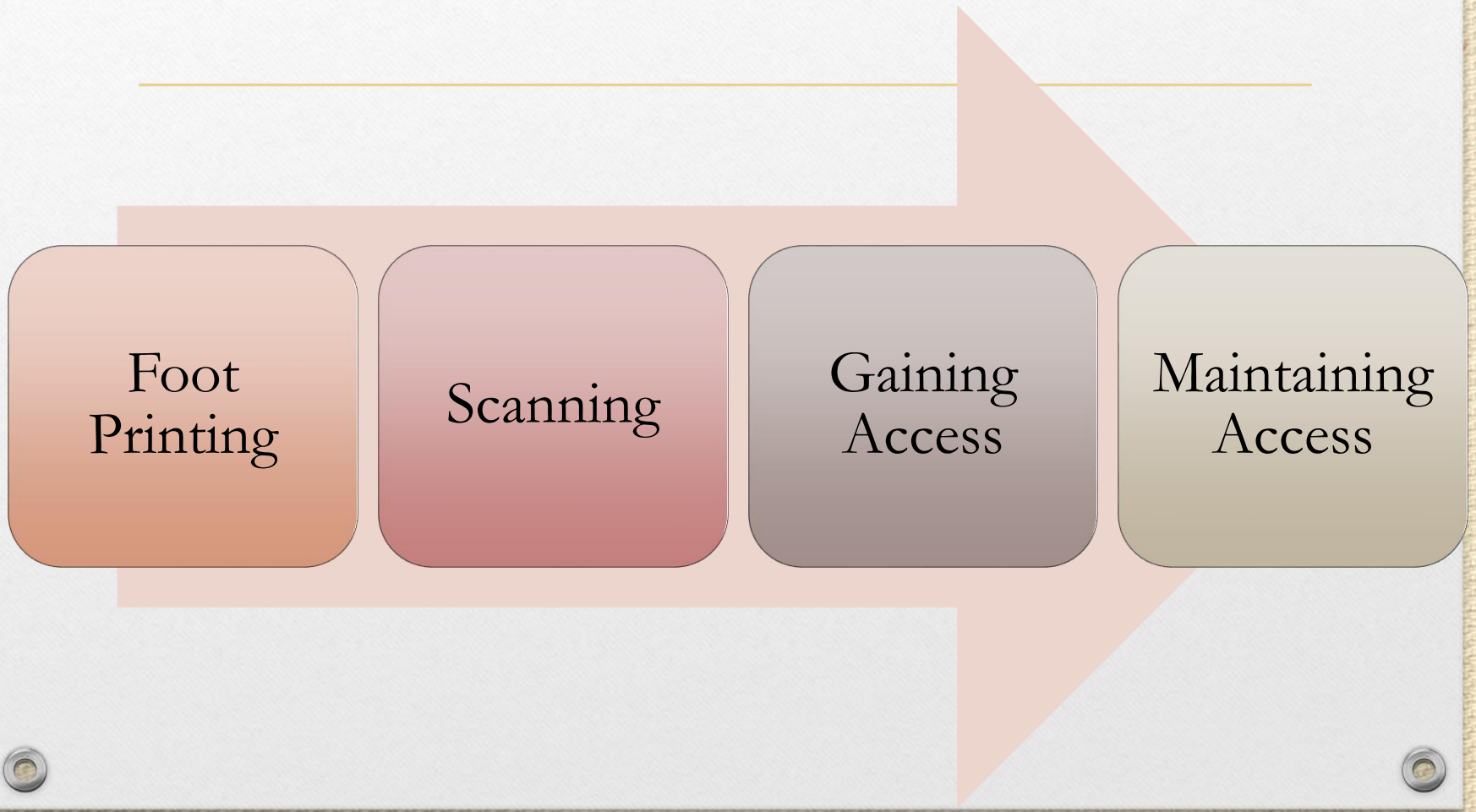
Threats to the organization

1. Natural disasters
2. Hacker Attacks
3. Cyber attack (country infrasture)
4. Virus and malware
5. DoS and Ddos
6. Disclosure of confidential information

Vulnerability: weakness

1. Application
2. Operating system
3. Misconfiguration
4. Shrinkwrap software

Hacking Process



Foot Printing

"Foot printing refers accumulating and uncovering as much as information about the target network before gaining access into any network."

Reconnaissance

This literal meaning of the Word reconnaissance means a preliminary survey to gain the information . This is also known as foot-printing.

As given in the analogy, this is the stage in which the hacker collects information about the company which the personal is going to hack. This is one of the pre-attacking phases.

- Whois lookup
- NS lookup
- IP lookup

Clip slide

1. Footprinting

- Footprinting refers to gathering all useful information about the target
- Tools for Footprinting:-
  - WhoIs Lookup
  - NS Lookup
  - IP Lookup

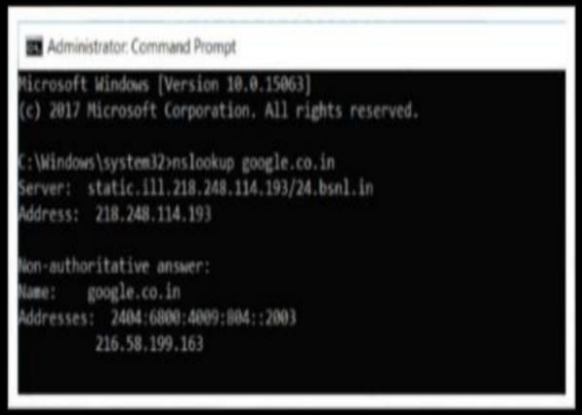


Fig. :- NS Lookup Tool

Foot Printing Techniques

- **Open Source Footprinting** : It will look for the contact information of administrators that will be used in guessing the password in Social engineering
- **Network Enumeration** : The hacker tries to identify the domain names and the network blocks of the target network
- **Scanning :** Once the network is known, the second step is to spy the active IP addresses on the network. For identifying active IP addresses (ICMP) Internet Control Message Protocol is an active IP addresses
- **Stack Fingerprinting** : Once the hosts and port have been mapped by scanning the network,the final footprinting step can be performed. This is called Stack fingerprinting.

WhoIs Lookup

Clip slide

Ethical Hacking P....html

Show all

X

Enumeration

The process of extracting machine name, user names, network resources, shares and services from a system. Under Intranet environment enumeration techniques are conducted.

2. Scanning & Enumeration

Scanning

The hacker tries to make a blue print of the target network.

The blue print includes the IP addresses of the target network which are live, the services which are running on those systems and so on Modern port scanning uses TCP protocol to do scanning and they could even detect the operating systems running on the particular hosts.

- Port Scanning
- Network Scanning

Clip slide

3. Gaining Access

- Password Attacks
- Social Engineering
- Viruses

Gaining Access

Password Cracking

There are many methods for cracking the password and then get in to the system. The simplest method is to guess the password. But this is a tedious work. But in order to make this work easier there are many automated tools for password guessing like legion.

Privilege escalation

Privilege escalation is the process of raising the privileges once the hacker gets in to the system The privilege escalation process usually uses the vulnerabilities present in the host operating system or the software. There are many tools like hk.exe, metasploit etc. One such community of hackers is the metasploit

- **Password Attacks (Technical & Non technical)**

Terminology

- Virus is a software or computer program that connect itself to another software or computer program to harm computer system.
- **Worms** replicate itself to cause slow down the computer system.
- Trojan Horse rather than replicate capture some important information about a computer system or a computer network.
- A **crypter** is a type of software that can encrypt, obfuscate, and manipulate malware, to make it harder to detect by security programs.
- Spyware is software that is installed on your computer either directly or inadvertently. It runs in the background of your computer and secretly monitors different programs.

It can be used to monitor your keystrokes, for example, and steal your login information to different sites. It can also monitor your Internet activity--which pages you visit, what things you buy, etc. Some parents use spyware to monitor their child's computer usage

Clip slide

4. Maintaining Access & Clearing Tracks

- OS Backdoors
- Trojans
- Clearing Tracks

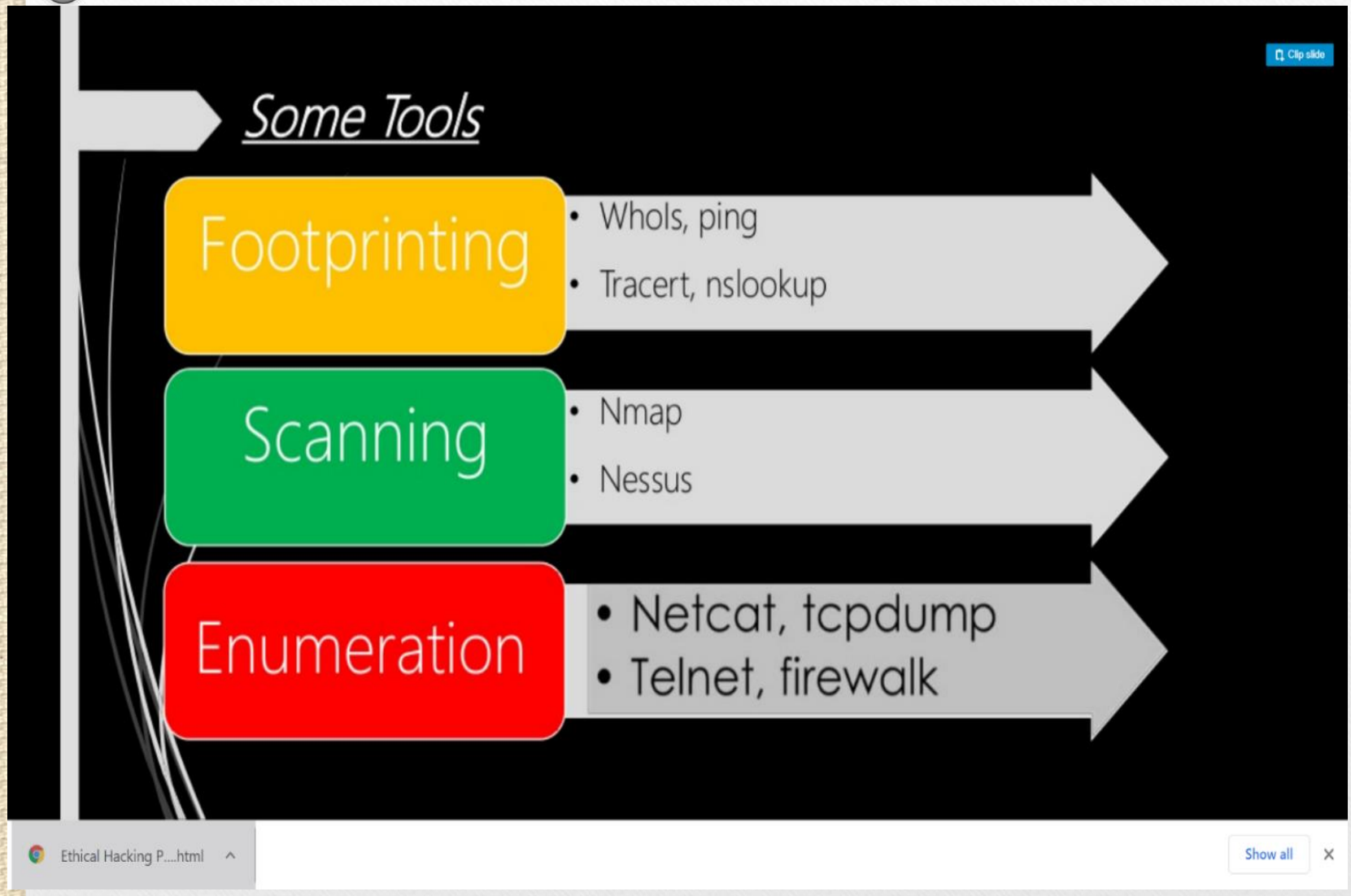
Maintaining Access

- Os BackDoors

  Cybercriminals install the malware through unsecured points of entry, such as outdated plug-ins or input fields. ... As the name suggests, a **backdoor attack is** stealthy, and cybercriminals often slip in undetected

- Trojans

  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.



Security Testing

- Black BoX : no knowledge testing (outsider attack)
- White Box: tester has full knowledge of system and infrastructure
- Gray Box

Backing up data to Reduce risk

often, much, stored, in day how much

1. Full backups
2. Differential backups
3. Incremental backups

An Introduction to Ethical Hacking

Risk Assessment

- A risk assessment is a process to identify potential security hazards and evaluate what would happen if a hazard or unwanted event were to occur.
  1. Qualitative (Prioritized list of critical concerns)
  2. Quantities (Monetary)

Quantities (Monetary)

- Step 1. **Determine the single loss expectancy (SLE):** **SLE = asset value × exposure factor**. The exposure factor (EF) is the subjective, potential portion of the loss to a specific asset if a specific threat were to occur.
- Step 2. **Evaluate the annual rate of occurrence (ARO):** The purpose of evaluating the ARO is to determine how often an unwanted event is likely to occur on an annualized basis.
- Step 3. **Calculate the annual loss expectancy (ALE):** This final step of the quantitative assessment seeks to combine the potential loss and rate pe year to determine the magnitude of the risk. This is expressed as annualloss expectancy (ALE), which is calculated as follows: **ALE = SLE × ARO.**

- If you have data worth $500 that has an exposure factor of 50 percent due to lack of countermeasures such as antivirus, what would the SLE be?" You would use the following formula to calculate the answer:
  - SLE × EF = SLE, or $500 × .50 = $250

- As part of a follow-up test question, could you calculate the annualized loss expectance (ALE) if you knew that this type of event typically happened four times a year?

Yes, as this would mean the ARO is 4. Therefore:

- ALE = SLE × ARO or $250 × 4 = $1,000

This means that, on average, the loss is $1,000 per year.

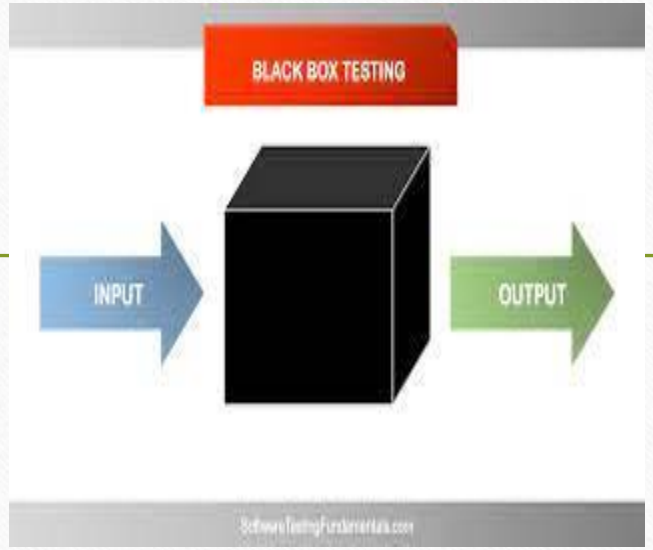
Exploit

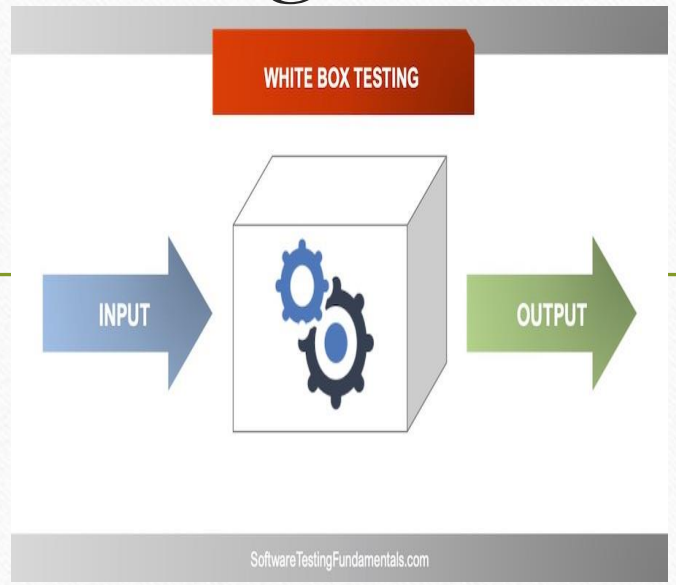
An *exploit* refers to a piece of software, a tool, a technique, or a process that takes advantage of a vulnerability that leads to access, privilege escalation, loss of integrity, or denial of service on a computer system.

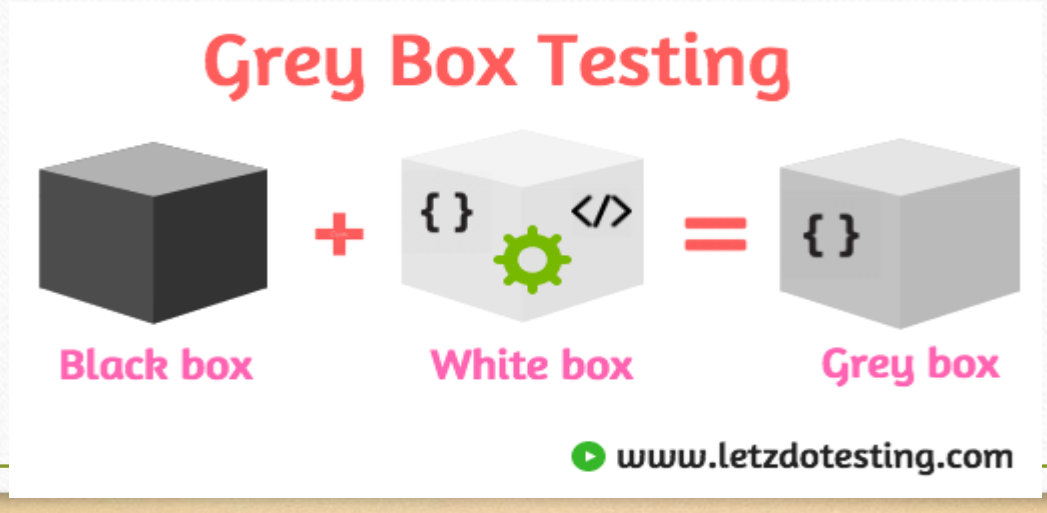
Why it is dangerous?

Sometimes you may not even know the vulnerability exists, and that is known as **zero day exploit**.

Security Testing







Types of Security Tests

- Vulnerability Testing
- Network evaluation
- Red-team exercise
- Penetration testing
- Host Vulnerability assessment
- Vulnerability assessment
- Ethical Hacking

Who attackers are

The more commonly used terms:

- **Phreakers:** The original hackers. These individuals hacked telecommunication and PBX systems to explore the capabilities and make free phone calls.
- Their activities include **physical theft,** stolen calling cards, access to telecommunication services, reprogramming of telecommunications equipment, and compromising user IDs and passwords to gain unauthorized use of facilities, such as phone systems and voicemail.

Continue…..

- **Script kiddies:** A term used to describe often younger attackers who use widely available freeware vulnerability-assessment tools and hacking tools that are designed for attacking purposes only.
- **Disgruntled employees:** Employees who have lost respect and integrity for the employer.
- **System crackers/hackers:** Elite hackers who have specific expertise in attacking vulnerabilities of systems and networks by targeting operating systems.

- **Software crackers/hackers:** Individuals who have skills in reverse engineering software programs and, in particular, licensing registration keys used by software vendors when installing software onto workstations or servers.
- Although many individuals are eager to participate of their services, anyone who downloads programs with cracked registration keys is breaking the law and can be a greater potential risk and subject to malicious code and malicious software threats that might have been injected into the code.

- **Cyberterrorists/cybercriminals:** An increasing category of threat that can be used to describe individuals or groups of individuals who are usually funded to conduct secret or intelligence/spying activities on governments, corporations, and individuals in an unlawful manner.
- These individuals are typically engaged in sponsored acts of defacement(damage/destruction): DoS/DDoS attacks, identity theft, financial theft, or worse, compromising critical infrastructures in countries, such as nuclear power plants, electric plants, water plants, and so on.

Ethical Hacking PPT (CEH)

Clip slide

What are Various Qualities a Hacker should posses?

- Good Coder
- Well knowledgeable person of both Hardware as well as Software
- Should have knowledge on Security System
- Trusted Person

Modes of Ethical Hacking

1. Information gathering
2. External penetration testing
3. Internal penetration testing
4. Network gear testing
5. DoS testing
6. Wireless network testing
7. Application testing
8. Social engineering
9. Physical security testing
10. Authentication system testing
11. Database testing
12. Communication system testing
13. Stolen equipment attack

Every ethical hacker must abide by the following rules when performing the tests
described previously.

1. **Never exceed the limits of your authorization**
2. **Protect yourself by setting up damage limitations**
3. **Be ethical**
4. **Do not harm**
5. **Maintain confidentiality**

some basic
questions to help establish the goals and objectives of the tests, including the
following:

- What is the organization's mission?
- What specific outcomes does the organization expect?
- What is the budget?
- When will tests be performed: during work hours, after hours, on weekends?
- How much time will the organization commit to completing the security evaluation?
- Will insiders be notified?
- Will customers be notified?
- How far will the test proceed? Root the box, gain a prompt, or attempt to retrieve another prize, such as the CEO's password?
- Whom do you contact should something go wrong?
- What are the deliverables?
- What outcome is management seeking from these tests?

- Getting Approval
- Ethical Hacking
  - Introduction
  - ■ Statement of work performed
  - ■ Results and conclusions
  - ■ Recommendations Report
- Vulnerability Research—Keeping Up with Changes


Ethical Hacking PPT (CEH)
Some tips to protect your System from Hackers
Keep your system fully patched
All OS Security Updates should be installed periodically
Don't use Pirated Software's
Remove unused Programs
Have a Good Anti-Virus and keep its virus definitions up-to-date
Firewall should be turned ON
Setup IDS (Hardware Firewall)
19 of 22
Ethical Hacking P....html
Show all

Ethical Hacking PPT (CEH)

Clip slide

Advantages of Ethical Hacking

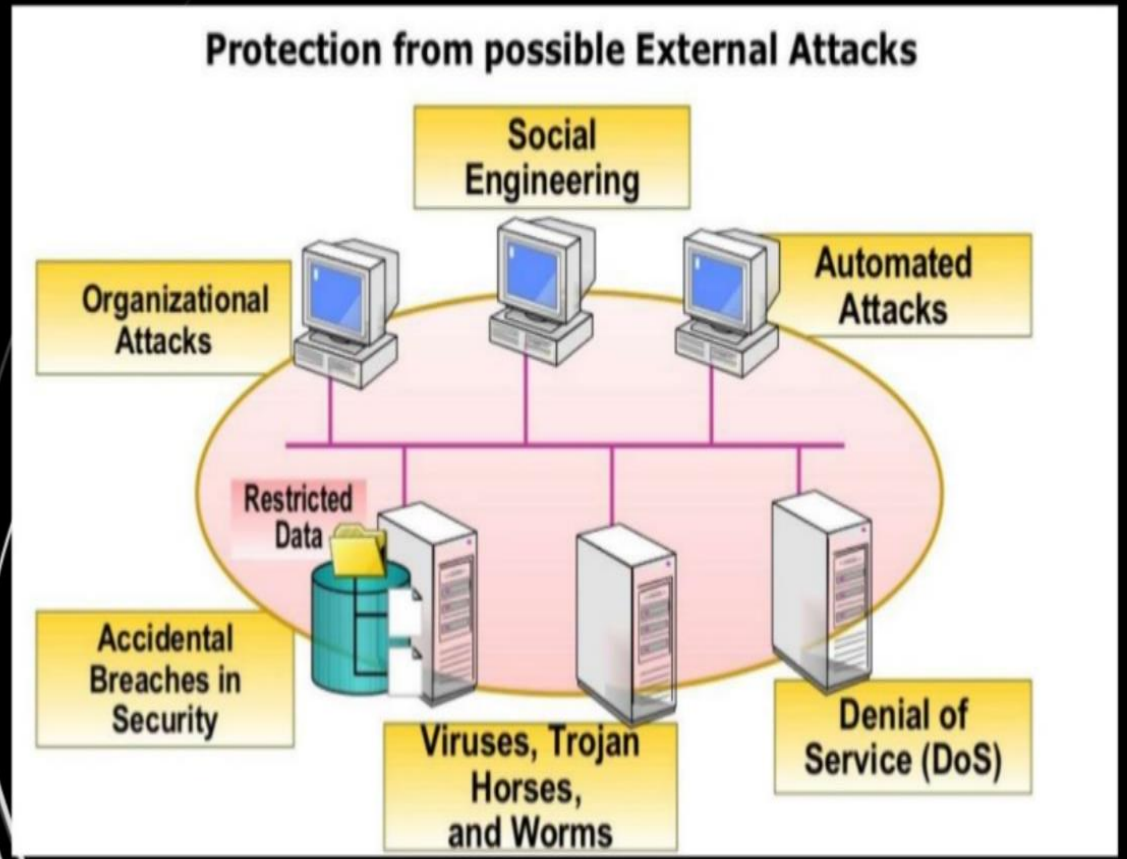
- Can be used to recover lost information
- Teaches that no technology is 100% secure
- To test how good security is on your own system, known as White Hat Hacking
- To prevent website, system or network hacking from Black Hat Hackers.

Ethical Hacking P....html

Show all


Ethical Hacking PPT (CEH)
Clip slide
Disadvantages
All depends upon the trustworthiness of the Ethical Hacker
Allowing the company's financial and banking details to be seen
Hiring Professionals is Expensive
21 of 22
Ethical Hacking P....html
Show all

Why Ethical Hacking



Clip slide

Ethical Hacking P....html

Show all

- “To catch the thief you have think like a thief”

Thank You

Ethical Hacking PPT (CEH)

What is CEH?

- CEH refers to Certified Ethical Hacker.
- CEH is 100% Network Offensive Course, not Defensive.
- This course includes System Hacking, Web Servers Hacking, Mobile Platforms Hacking, Wireless Networks Hacking etc.

Ethical Hacking P....html

Show all

Foot Printing And Scanning

Phase 1: Reconnaissance

- This phase is also called as Footprinting and information gathering Phase, and in this phase hacker gathers information about a target before launching an attack. It is during this phase that the hacker finds valuable information such as old passwords, names of important employees.
- What's footprinting? It's a method that used for collecting data from target system. These data include important areas such as:
- Finding out specific IP addresses
- TCP and UDP services
- Identifies vulnerabilities
- Having such information is enough to start a successful attack.

- There are two types of Footprinting:
- **Active**: Directly interacting with the target to gather information about the target.
- **Passive**: Trying to collect the information about the target without directly accessing the target. To this purpose, hacker can use social media, public websites etc.
- Hacker may do so by : using a search engine like maltego, researching the target say a website (checking links, jobs, job titles, email, news, etc.), or a tool like HTTPTrack to download the entire website for later enumeration, the hacker is able to determine the following: Staff names, positions, and email addresses. (Source: geeksforgeeks.org)
-

Phase 2: Scanning

- In this phase, hackers are probably seeking any information that can help them perpetrate attack such as computer names, IP addresses, and user accounts. In fact, hacker identifies a quick way to gain access to the network and look for information. This phase includes usage of tools like **dialers, port scanners, network mappers, sweepers, and vulnerability scanners to scan data**.
- Basically, at this stage, four types of scans are used:
- **Pre-attack**: Hacker scans the network for specific information based on the information gathered during reconnaissance.
- **Port scanning/sniffing**: This method includes the use of dialers, port scanners, and other data-gathering equipment.
- **Vulnerability Scanning**: Scanning the target for weaknesses/vulnerabilities.
- **Information extraction**: In this step, hacker collects information about ports, live machines and OS details, topology of network, routers, firewalls, and servers.

Footprinting

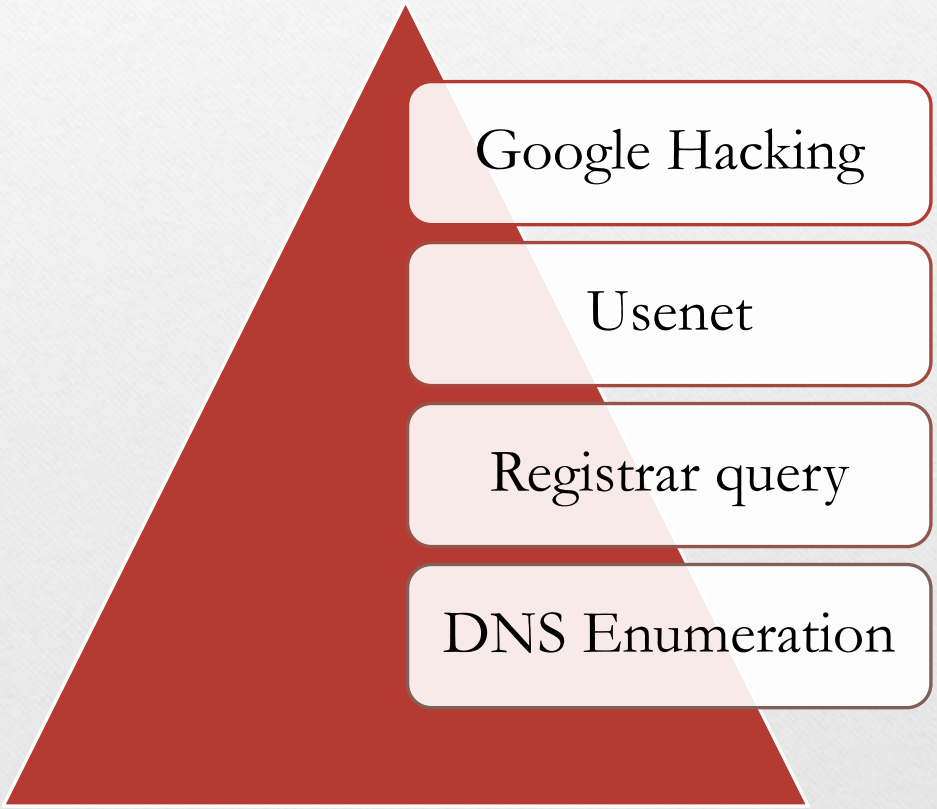
- Footprinting is the blueprint (a plan how it works) of the security profile of an organization, undertaken in a methodological manner
- Footprinting is one of the three pre-attack Phases
- An attacker spends **90% of the time in profiling** an organization and another 10% in launching the attack
- Footprinting results in a unique organization profile with respect to networks (Internet/intranet/extranet/wireless) and systems involved

Seven Step Information Gathering Process

- The EC-Council divides footprinting and scanning into seven basic steps, as follows.
  1. Information gathering
  2. Determining the network range
  3. Identifying active machines
  4. Finding open ports and access points
  5. OS fingerprinting
  6. **Fingerprinting services**
  7. **Mapping the network attack surface**

Information Gathering

Information Gathering



Documentation

	A	B	C	D	E
1	**Obtained Thru Search Engine**	**Results**	**Social Network Sites**	**Results**	**Website Footprinting**
2	Employees		Profile		OS's
3	Login pages		News		Scripting
4	Portal URL's		Education		Job requests
5	Technologies		Family		Other
6	**Email Footprinting**	**Results**	**People Search Sites**	**Results**	**Google Hacking**
7	IP address		Date of birth		Files containing passwords
8	Email Address		Email		Error messages
9	Geo location		Photos		Other findings
10	**Whois Footprinting**	**Results**	**Network footprinting**	**Results**	**DNS footprinting**
11	Domain name		Network range		DNS servers
12	Contact details		Subnet mask		Zone transfer (Y/N)
13	Domain creation date		Traceroute findings		Types of Servers
14	Hosting company		Other data		DNSSEC (Y/N)

Documentation Finding

The Organiztion's Website

- **Company URL:** Domain name.
- **Internal URLs:** As an example, not only Dell.com but also support.Dell.com.
- **Restricted URLs:** Any domains not accessible to the public.
- **Internal pages:** Company news, employment opportunities, addresses, and phone numbers. Overall, you want to look for all open source information, which is information freely provided to clients, customers, or the general public.
- **Tool: Netcraft**

Job Boards

- Popular sites include the following:
- ■ Careerbuilder.com
- ■ Monster.com
- ■ Dice.com
- ■ Indeed.com

Type of information usually found on Job Boards

■ Primary responsibilities for this position include management of a Windows 2008 Active Directory environment, including MS Exchange 2008, SQL 2008, and Citrix

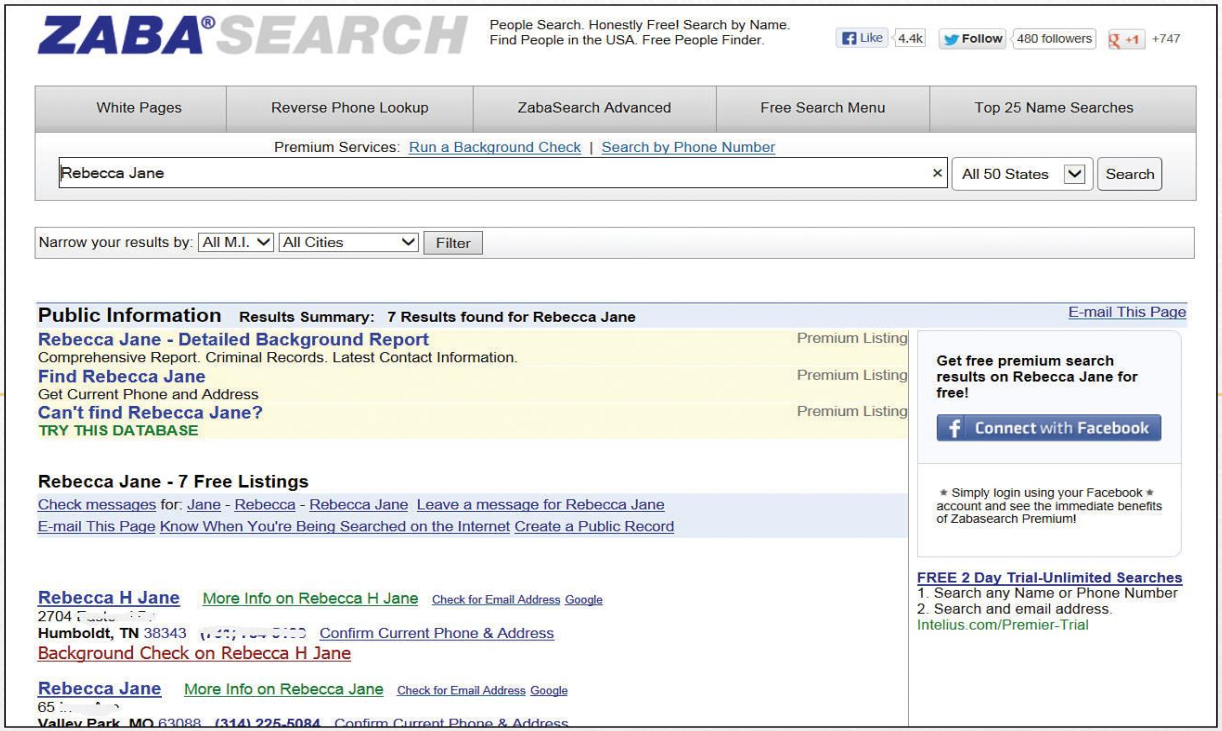
■ Interact with the technical support supervisor to resolve issues and evaluate/maintain patch level and security updates

Experience necessary in Active Directory, Microsoft Clustering and Network, Load Balancing, MS Exchange 2007, MS SQL 2003, Citrix MetaFrame, XP, EMC CX-400 SAN-related or other enterprise level SAN, Veritas Net Backup, BigBrother, and NetIQ Monitoring SW

■ Maintain, support, and troubleshoot a Windows 7 LAN

Employee and People Search

- **Pipl:** https://pipl.com/
- **Spokeo:** http://www.spokeo.com/
- **BirthdayDatabase.com:** http://www.birthdatabase.com/
- **Whitepages:** http://www.whitepages.com/
- **People Search Now:** http://www.peoplesearchnow.com/
- **Zabasearch:** http://www.zabasearch.com/
- **Peoplefinders:** http://www.peoplefinders.com/
- **Justia email finder:** http://virtualchase.justia.com/content/finding-email-addresses



Facebook

- Twitter
- LinkedIn
- Google+
- Pinterest

EDGAR Database

- The Electronic Data Gathering, Analysis, and Retrieval system, performs automated collection, validation, indexing, acceptance, and forwarding of submissions by companies and others who are required by law to file forms with the U.S. Securities and Exchange Commission

Google Hacking

- Despite what you may infer from the name, this method does not involve hacking Google! This is a means by which you can collect information from the Google search engine in a smart way.
- Search engines have many features using which you can get uncommon, but very specific search results from the internet
- Let's take an example.
- Go to google.com and paste this- allinurl:tsweb/default.htm

- Go to http://groups.google.com to search the Google newsgroups. The following commands can be used to have the Google search engine gather target information:
- **site** Searches a specific website or domain. Supply the website you want to search after the colon.
- **filetype** Searches only within the text of a particular type of file. Supply the file type you want to search after the colon. Don't include a period before the file extension.
- **link** Searches within hyperlinks for a search term and identifies linked pages.
- **cache** Identifies the version of a web page. Supply the URL of the site after the colon.
- **intitle** Searches for a term within the title of a document.
- **inurl** Searches only within the URL (web address) of a document. The search term must follow the colon.
- For example, a hacker could use the following command to locate certain types of vulnerable web applications: INURL:["parameter="] with FILETYPE:[ext] and INURL:[scriptname] Or a hacker could use the search string intitle: "BorderManager information alert" to look for Novell BorderManager proxy/firewall servers.

Usenet

- Usenet is a user's network, which is nothing more than a collection of the thousands of discussion groups that reside on the Internet. Each discussion group contains information and messages centered on a specific topic
- Messages are posted and responded to by readers either as public or private emails. Even without direct access to Usenet, a convenient way to browse the content is by using Google Groups.
- Google Groups allows any Internet user a way to post and read Usenet messages. During a penetration test, you will want to review Google Groups for postings from the target company.

Registrar Query

- Currently many tools are available that can be used for obtaining types of basic information, like:
- • whois
- • nslookup
- • Internet Assigned Numbers Authority (IANA) and Regional Institute Registries (RIRS) to find the range of Internet Protocol (IP) address
- • traceroute to determine the location of the network

- Numerous Web sites are dedicated to providing network range information automatically. Some of the more common search machines are: • http://www.betterwhois.com • http://geektools.com • http://www.all-nettools.com • http://www.smartwhois.com • http://www.dnsstuff.com • http://whois.domaintools.com

Automatic Registrar Query

- The aim of using of these tools is to obtain registrar information. Underlying all these tools is is Whois tool, which is software designed to query the databases that hold registration information. whois:
- primarily used to verify whether a domain name is available or whether it has been registered.
- The whois information contains the name, address and phone number of the administrative, billing and technical contacts of the domain name.

What is Enumeration (list one by one-count)?

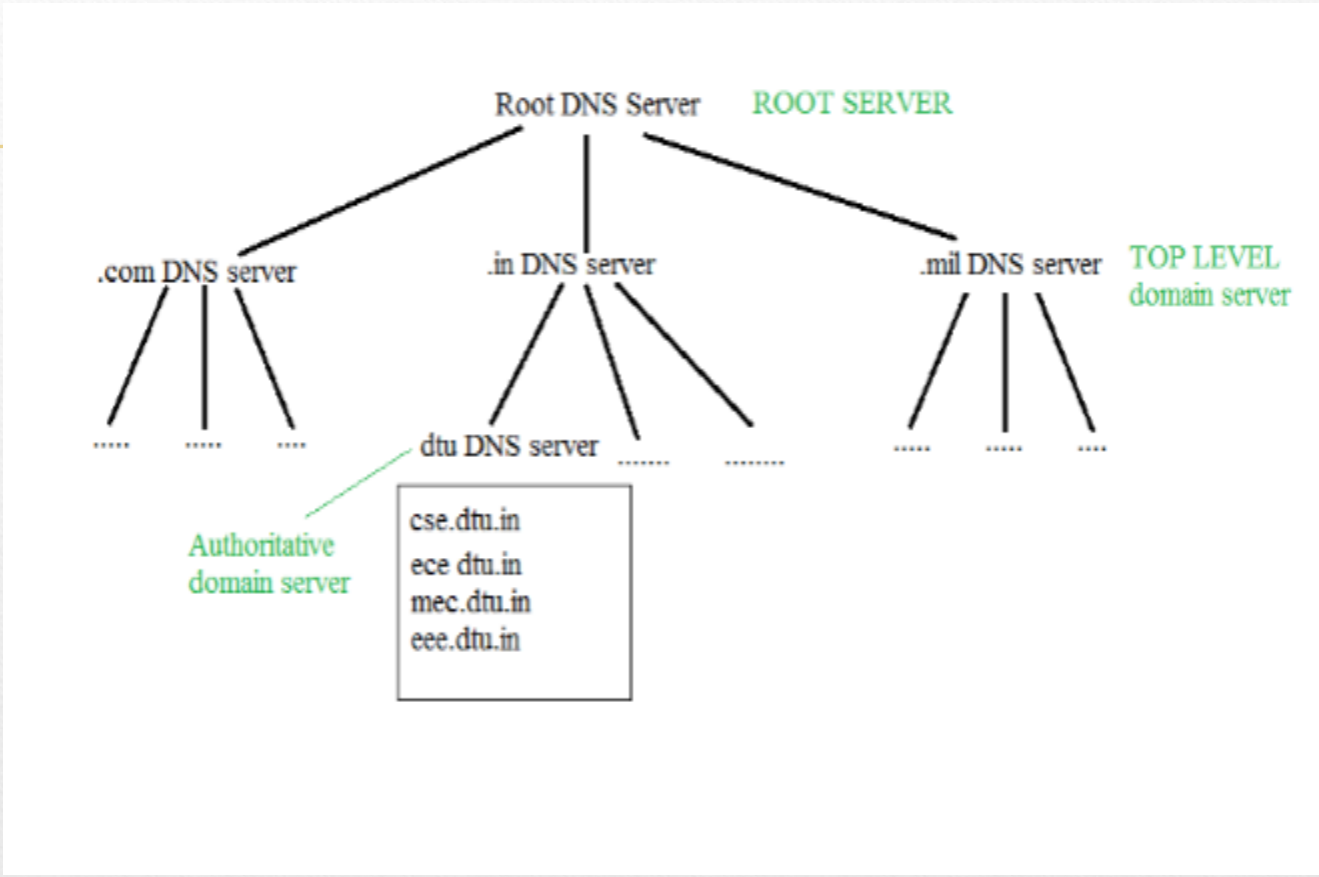
Once an attacker creates an active connection with the target, they are able to perform directed queries to gain more information. For example,

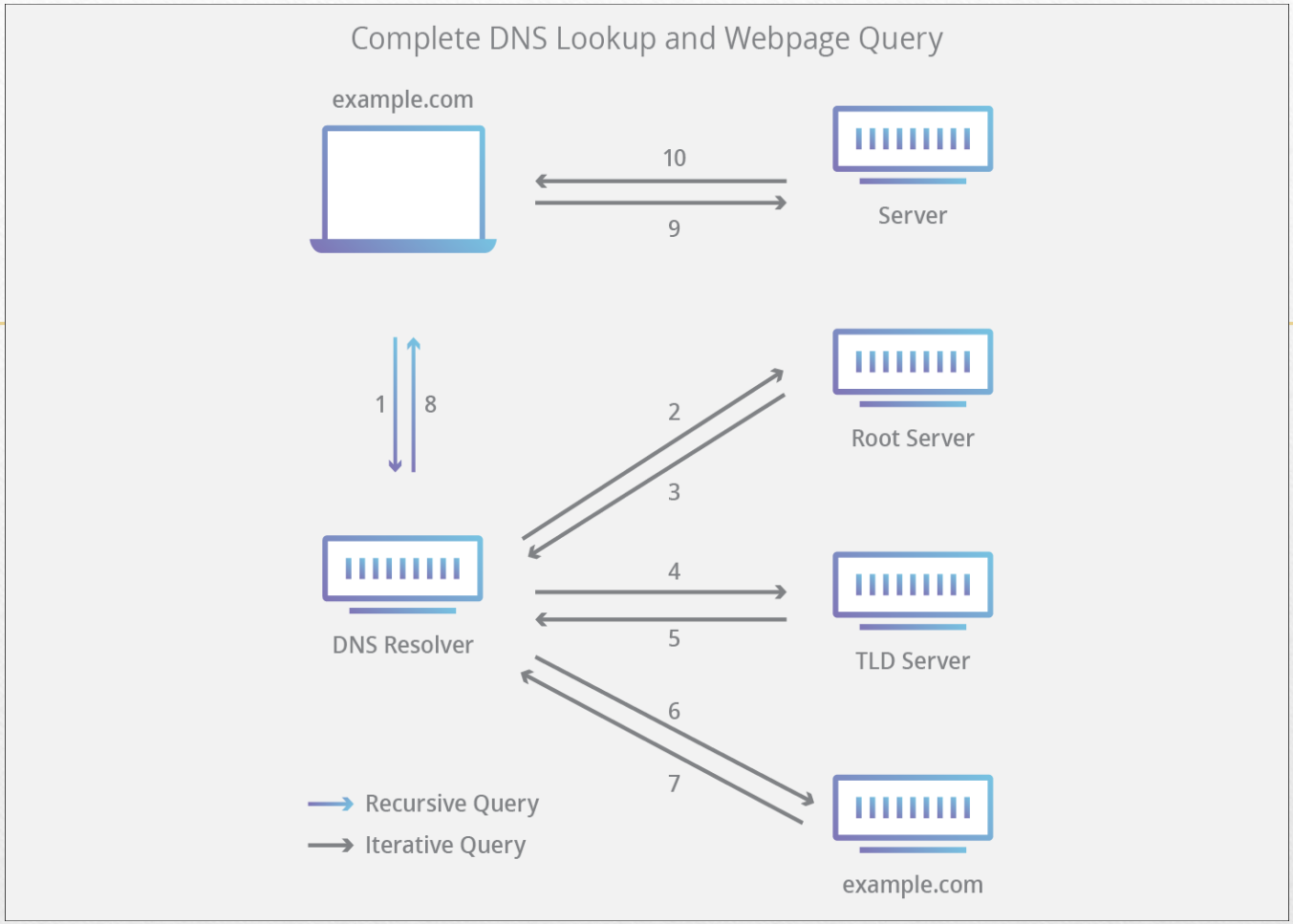
- Usernames
- hostnames
- IP address
- Passwords (or strength)
- configuration

The information gathered about the target can be used to identify vulnerabilities in the target system. Once an attacker gains this information, they can steal private data and sometimes, even worse, change the configuration.

DNS Servers

- The Domain Name System (DNS) is the phonebook of the Internet. When users type domain names such as 'google.com' or 'nytimes.com' into web browsers, DNS is responsible for finding the correct IP address for those sites.
- Browsers then use those addresses to communicate with origin servers to access website information.
- This all happens thanks to DNS servers: machines dedicated to answering DNS queries.


Root DNS Server
ROOT SERVER
.com DNS server
.in DNS server
.mil DNS server
TOP LEVEL
domain server
dtu DNS server
Authoritative
domain server
cse.dtu.in
ece dtu.in
mec.dtu.in
eee.dtu.in


Complete DNS Lookup and Webpage Query
example.com
10
9
Server
1
8
2
3
Root Server
DNS Resolver
4
5
TLD Server
6
7
Recursive Query
Iterative Query
example.com

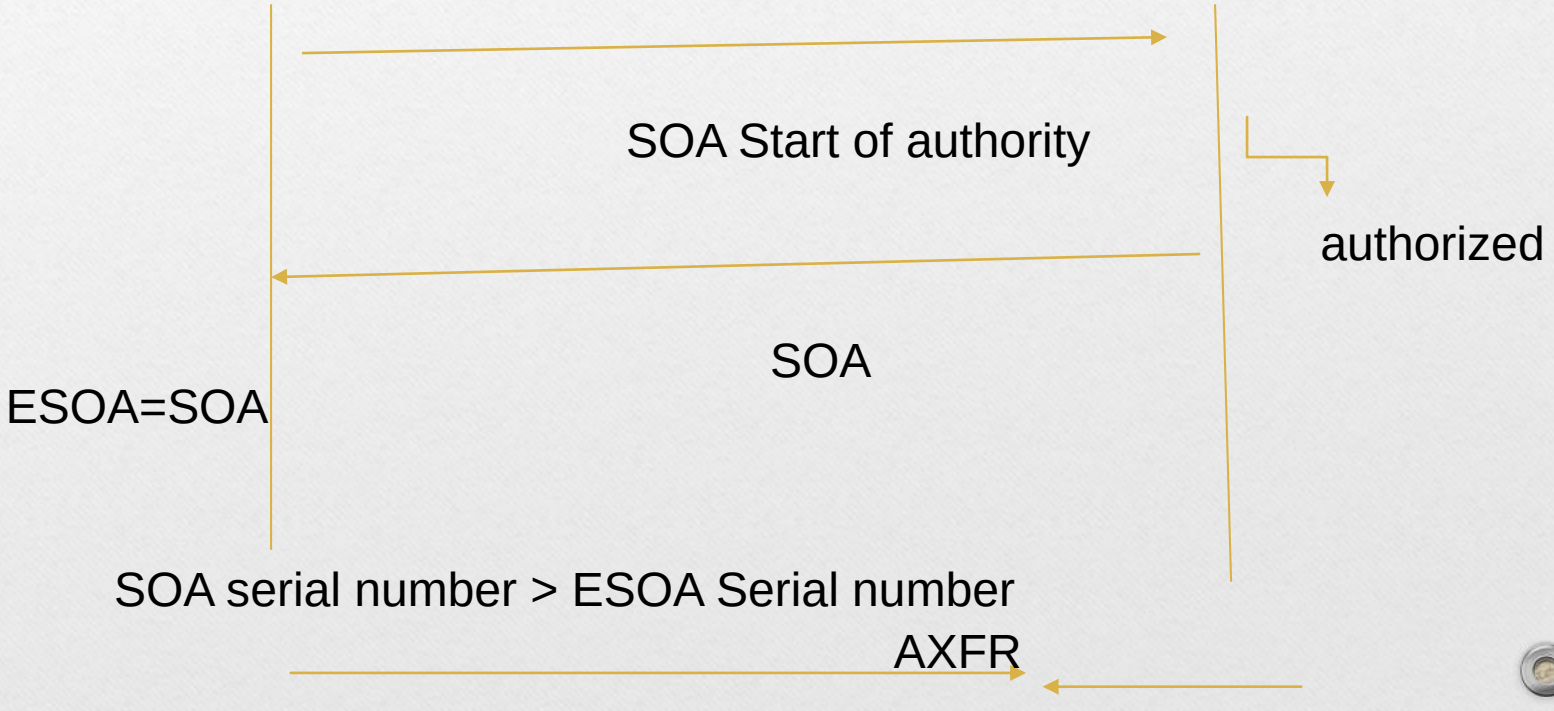
- First the resolver queries the root nameserver. The root server is the first step in translating (resolving) human-readable domain names into IP addresses. The root server then responds to the resolver with the address of a Top Level Domain (TLD) DNS server (such as .com or .net) that stores the information for its domains.
- Next the resolver queries the TLD server. The TLD server responds with the IP address of the domain's authoritative nameserver. The recursor then queries the authoritative nameserver, which will respond with the IP address of the origin server.
- The resolver will finally pass the origin server IP address back to the client. Using this IP address, the client can then initiate a query directly to the origin server, and the origin server will respond by sending website data that can be interpreted and displayed by the web browser.

DNS Enumeration

- DNS enumeration is the technique employed to find all the DNS servers and their corresponding records for an organization
- A list of DNS records provides an overview of database records.
- A company may have both internal and external DNS servers that can yield information such as usernames, computer names, and IP addresses of potential target systems
- DNS normally moves information from one DNS server to another through the DNS zone transfer process. If a domain contains more than one name server, only one of these servers will be the primary. Any other servers in the domain will besecondary servers.
- DNS zone transfer will allow replication of DNS data or DNS files. The user will perform a DNS zone transfer query from the name server. If the name server allows transfer by any other unauthorized user than all DNS names and IP addresses hosted by the name server will return in ASCII Test.
- Some of the tools that can be for this include nslookup, maltego, dnenum, dnsrecon, etc.

Zone transfer

- Secondary server
- Primary server



2. Determining the Network Range

- Suppose pen test team has been able to locate names, phone numbers, addresses, some server names, and IP addresses, it's important to find out what IP addresses are available for scanning and further enumeration.
- If you take the IP address of a web server discovered earlier and enter it into the Whois lookup at https://www.arin.net, you can determine the network's range.
- Traceroute and ping are useful tools for identifying active systems, mappingtheir location, and learning more about their location.

3. Identifying Active Machine

- Attackers will want to know whether machines are alive before they attempt to attack.
- Ping uses ICMP and works by sending an echo request to a system and waiting for the target to send an echo reply back

4. Finding Open ports and access points

Common Ports and Protocols

- Port Protocol Service/Transport
- 20/21 FTP TCP
- 22 SSH TCP
- 23 Telnet TCP
- 25 SMTP TCP
- 53 DNS TCP/UDP
- 69 TFTP UDP
- 80 HTTP TCP
- 110 POP3 TCP
- 135 RPC TCP
- 161/162 SNMP UDP
- 1433/1434 MSSQL TCP

Introduction to Port Scanning

- Port Scanning
- Finds out which services a host computer offers
- Identifies vulnerabilities
- Scan all ports when testing, not just well-known ports
- Open services can be used on attacks
- Identify a vulnerable port via scanning
- Then launch an exploit

TCP -a three-way handshake

- TCP offers robust communication and is considered a connection protocol.
- TCP establishes a connection by using what is called a three-way handshake

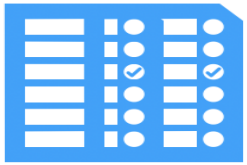
Flag	Description
SYN	Synchronize and initial sequence number (ISN)
ACK	Acknowledgment of packets received
FIN	Final data flag used during the four-step shutdown of a session

Client

send SYN
(seq = x)

receive SYN
(seq = y, ACK= x+1)

send ACK
(ack = y+1)



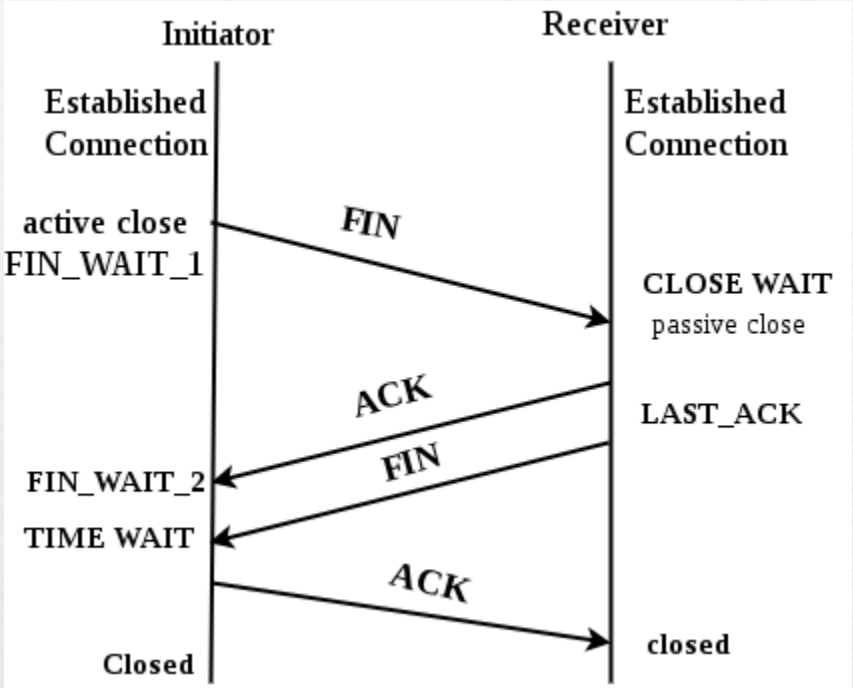
Server

received SYN
(seq = x)

send SYN
(seq = y, ACK= x+1)

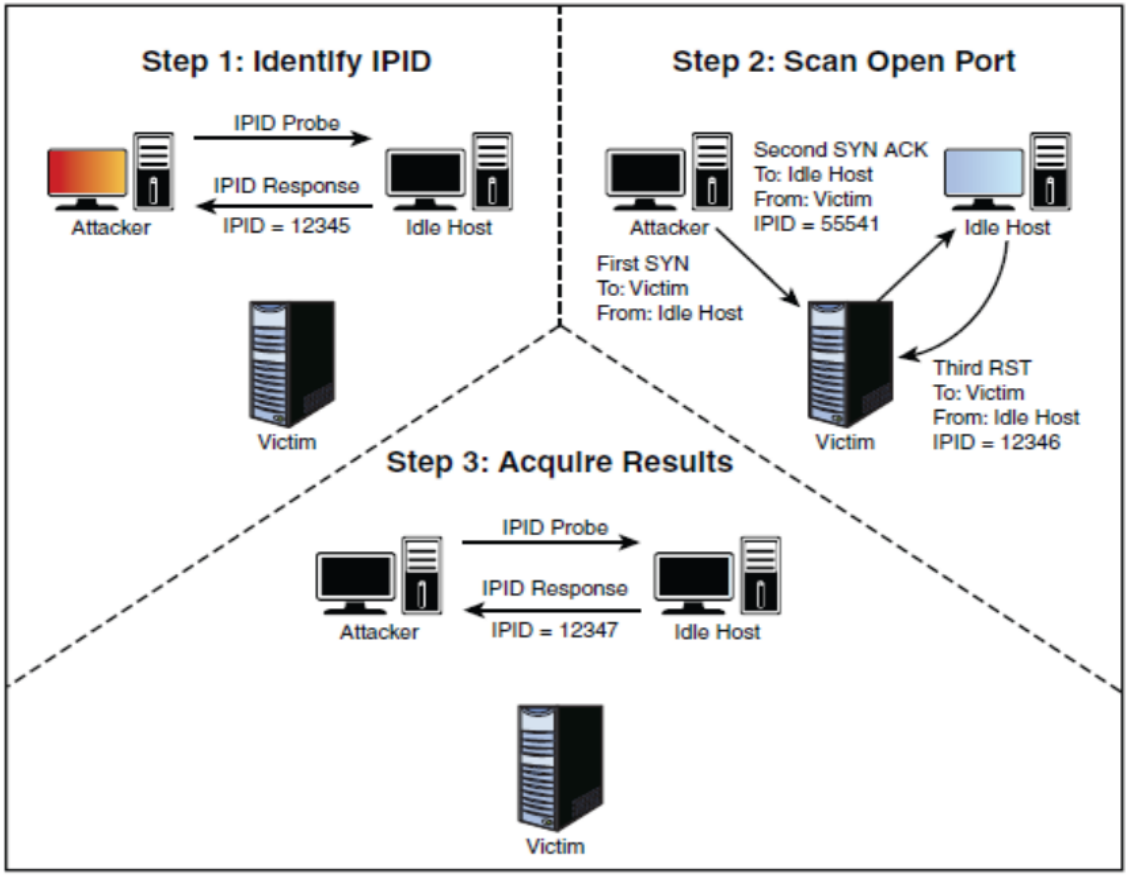
receive ACK
(ack = y+1)

TCP terminates the session by using a four step shutdown:

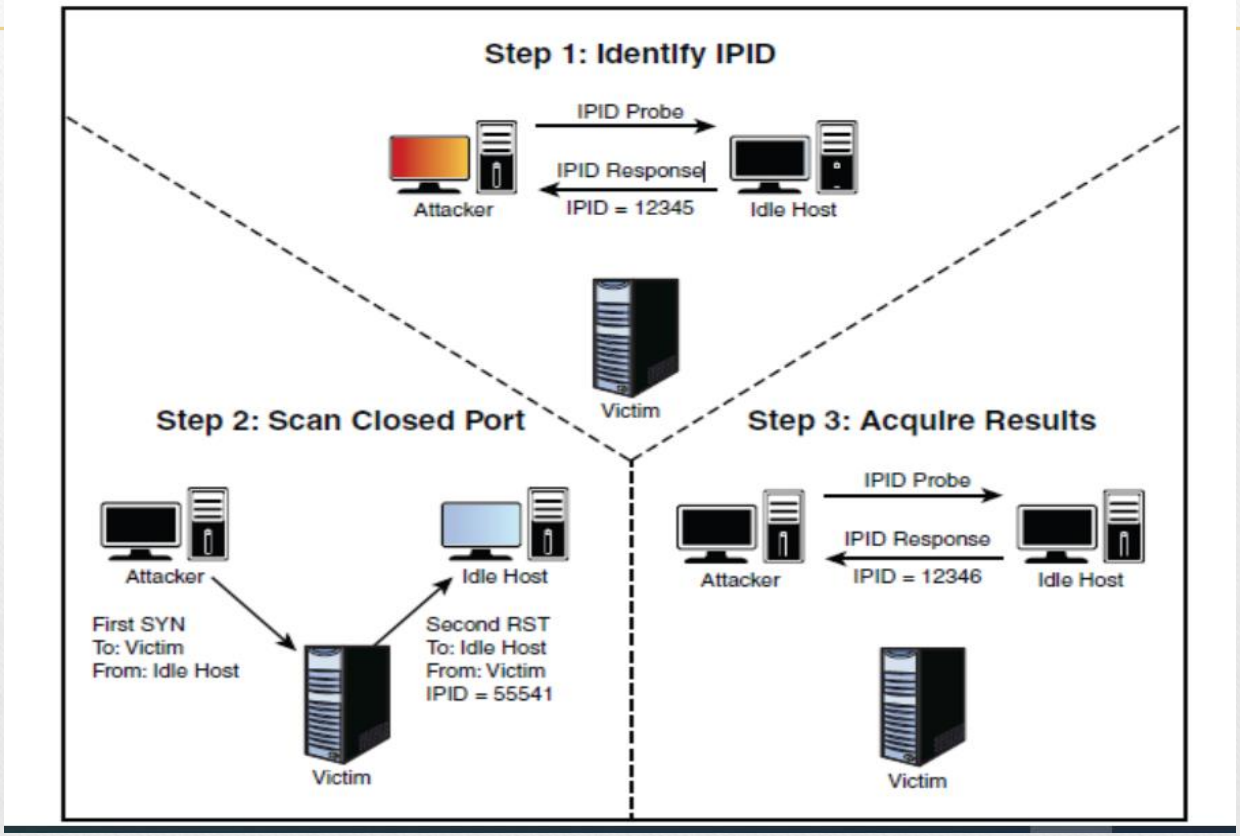


IP makes use of an identification number known as an IPID.

IPID port Open



IPID port closed



5. OS Fingerprinting

- Passive fingerprinting is really sniffing, as the hacker is sniffing packets as they come by. These packets are examined for certain characteristics that can be pointed out to determine the OS.
- **IP TTL value:** Different operating systems set the TTL to unique values on outbound packets.
- ■ **TCP window size:** OS vendors use different values for the initial window size.
- ■ **IP DF option:** Not all OS vendors handle fragmentation in the same way. 1500 bytes is a common size with Ethernet.
- ■ **IP Type of Service (TOS) option:** TOS is a 3-bit field that controls the priority of specific packets. Again, not all vendors implement this option in the same way.

- Active fingerprinting is more powerful than passive fingerprint scanning because the hacker doesn't have to wait for random packets, but as with every advantage, there is usually a disadvantage.
- This disadvantage is that active fingerprinting is not as stealthy as passive fingerprinting. The hacker actually injects the packets into the network. Active fingerprinting has a much higher potential for being discovered or noticed.

Basic methods used in active fingerprinting:

- ■ **The FIN probe:** A FIN packet is sent to an open port, and the response is recorded. Although RFC 793 states that the required behavior is not to respond, many operating systems such as Windows will respond with an RST.
- ■ **Bogus flag probe:** As you might remember from Table 3-6, the flag field is only 1 byte in the TCP header. A bogus flag probe sets one of the used flags along with the SYN flag in an initial packet. Linux will respond by setting the same flag in the subsequent packet.
- ■ **Initial sequence number (ISN) sampling:** This fingerprinting technique works by looking for patterns in the ISN. Although some systems use truly random numbers, others, such as Windows, increment the number by a small fixed amount.
- ■ **IPID sampling:** Many systems increment a systemwide IPID value for each packet they send. Others, such as older versions of Windows, do not put the IPID in network byte order, so they increment the number by 256 for each packet.

- **TCP initial window:** This fingerprint technique works by tracking the window size in packets returned from the target device. Many operating systems use exact sizes that can be matched against a database to uniquely identify the OS.
- **ACK value:** Again, vendors differ in the ways they have implemented the TCP/IP stack. Some operating systems send back the previous value +1, whereas others send back more random values.
- ■ **Type of service:** This fingerprinting type tweaks ICMP port unreachable messages and examines the value in the TOS field. Whereas some use 0, others return different values.

- **TCP options:** Here again , different vendors support TCP options in different ways. By sending packets with different options set, the responses will start to reveal the server's fingerprint.
- ■ **Fragmentation handling:** This fingerprinting technique takes advantage of the fact that different OS vendors handle fragmented packets differently. RFC 1191 specifies that the maximum transmission unit (MTU) is normallyset between 68 and 65535 bytes. This technique was originally discovered by Thomas Ptacek and Tim Newsham.

- “Most hackers are young because young people tend to be adaptable. As long as you remain adaptable, you can always be a good hacker.”

— Emmanuel Goldstein, Dear Hacker: Letters to the Editor of 2600

Thank You

Enumeration and System Hacking

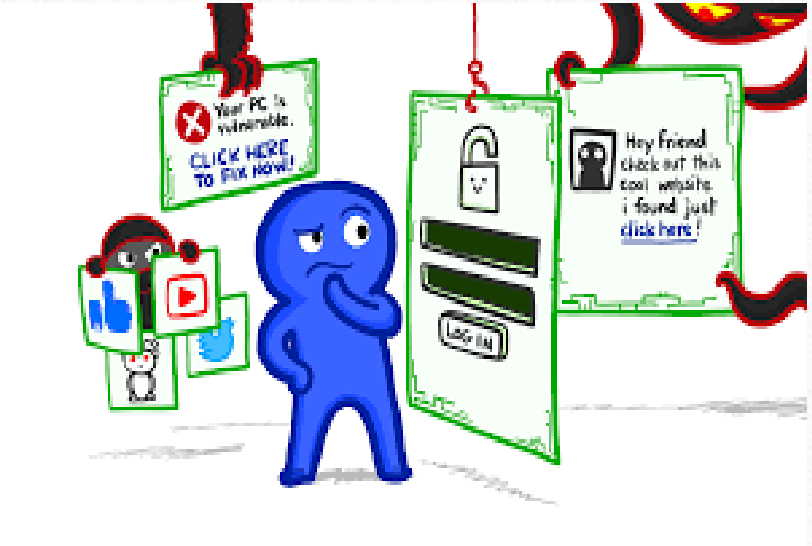
-Dr. Zakiya Malek

System Hacking

- Previous steps, such as footprinting, scanning, and enumeration, are all considered pre-attack stages.
- The primary goal of the system hacking stage is to authenticate to the remote host with the highest level of access.


A D G
Passwords
Hacker
Victim

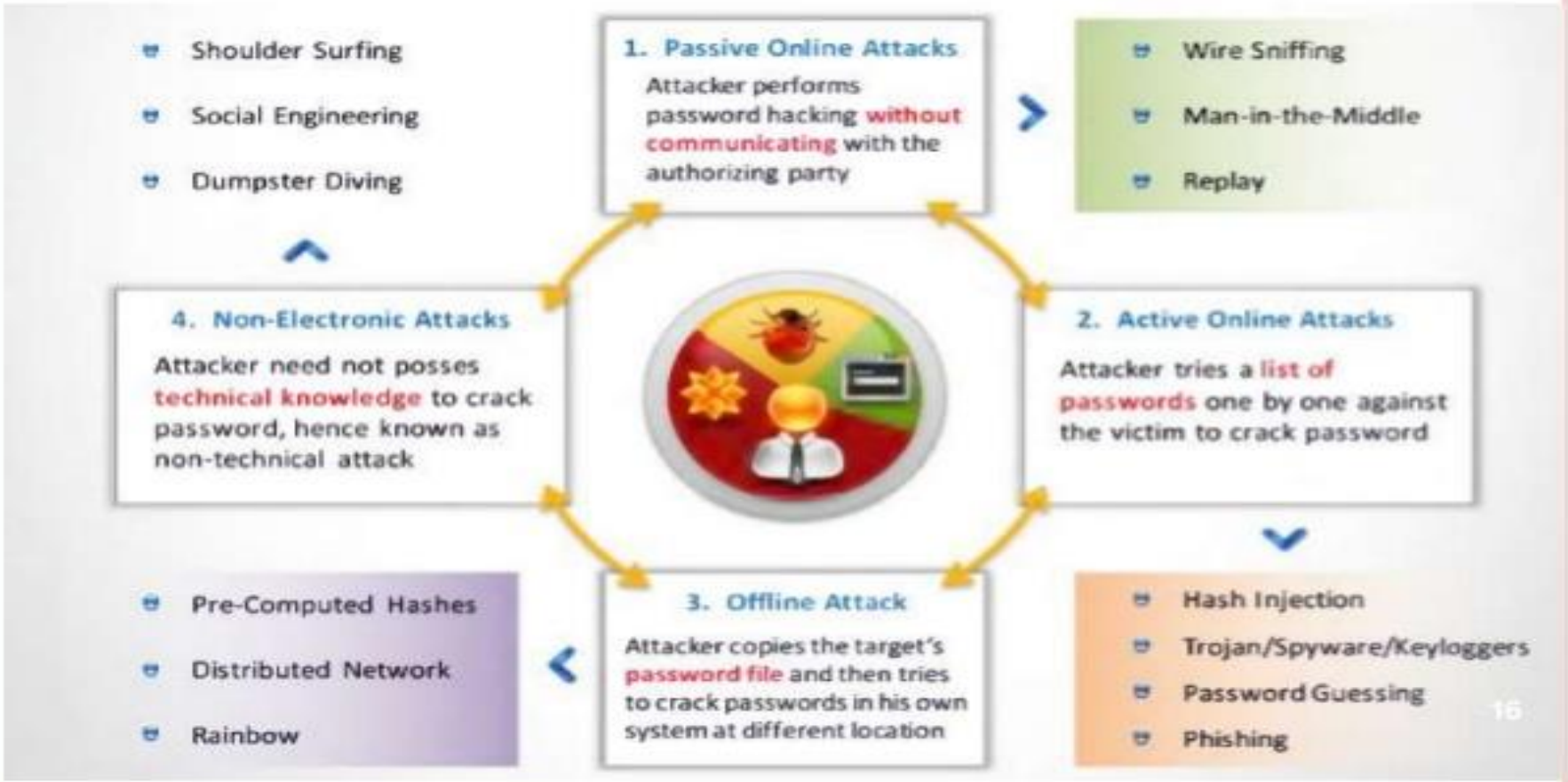

DUMPSTER DIVERS
A TECHNICALLY LEGAL THREAT TO YOUR INFO


Your PC is vulnerable.
CLICK HERE TO FIX NOW!
Hey Friend check out this cool website i found just click here!
LOG IN

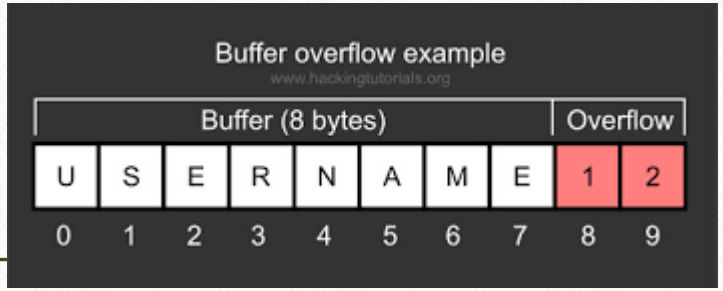
Technical Password Attacks

- Password guessing
- Automated password guessing
- Keylogging

TYPES OF PASSWORD ATTACKS



Exploiting a Buffer Overflow



- A buffer is a temporary data storage area whose length is defined in the program that creates it or by the operating system. Ideally, programs should be written to check that you cannot stuff 32 characters into a 24-character buffer.
- However, this type of error checking does not always occur. Error checking is really nothing more than making sure that buffers accept only the correct type and amount of information required.
- Programs are vulnerable to buffer overflows for a variety of reasons, although primarily because of poor error checking.
- The easiest way to prevent buffer overflows is to stop accepting data when the buffer is filled.

Linux Authentication and Passwords

- Linux requires that user accounts have a password, but by default it will not preventyou from leaving one set as blank. During installation, Linux gives the user the choice of setting the password encryption standard.
- Most versions of Linux, such as Fedora and others, use message digest algorithm 5 (MD5) by default.
- If you choose not to use MD5, you can choose Data Encryption Standard (DES); be aware, however, that it limits passwords to eight alphanumeric characters.
- Linux also includes the /etc/shadow file for additional password security. Take a look at an entry from an /etc/shadow file here:

Approaches To Message Authentication

- Problem :
  - Encryption protects against passive attack but it does not protect against active attack so for that we require message authentication.

Message Authentication using Two types:

- Authentication Using Conventional Encryption
- Message Authentication without message Encryption

Message Authentication without message Encryption

- In this method authentication tag is generated and appended to each message for transmission.
- 3 situations are there where we don't require encryption :

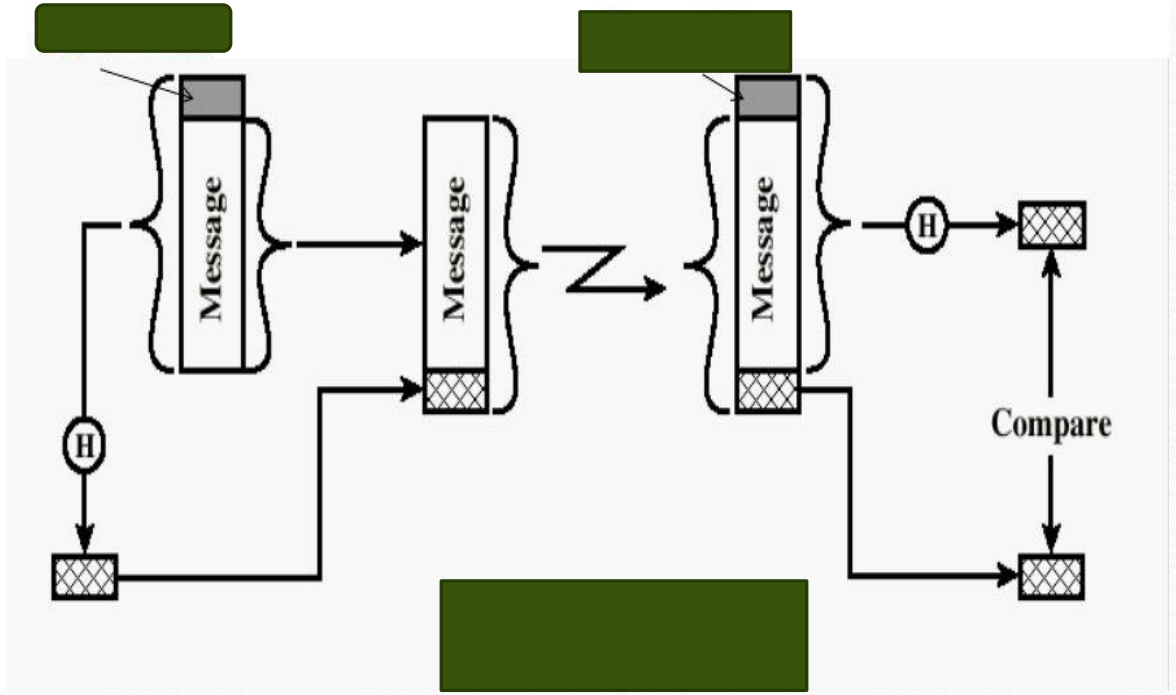
1. Number of applications in which same message is broadcast to many application.

2. One side has heavy load and can not afford the time to decrypt the all incoming messages.

3. Computer program can be executed without having to decrypt but it decrypts everytime so it is wasteful of resources.

One-Way HASH Function

- Secret value is added before the hash and removed before transmission.



The 9 fields of /etc/shadow

No.	Description
1	Login name
2	Encrypted password
3	Date of last password change (in days since epoch)
4	Number of days until change allowed
5	Number of days until change required
6	Number of days prior to expiration to begin warning
7	Number of days after expiration before account disabled
8	Date that password expired (in days since epoch)
9	Reserved for future use.

The /etc/shadow file

Field	Example	Description
name	sysadmin	This is the name of the account, which matches the account name in the `/etc/passwd` file.
password	6.....rl1	The password field contains the encrypted password for the account.
last change	15020	This field contains a number that represents the last time the password was changed.
min	5	The password can't be changed again for the specified number of days.
max	30	This field is used to force users to change their passwords on a regular basis
warn	7	If the **max** field is set, the **warn** field indicates that the user would be "warned" when the **max** timeframe is approaching.
inactive	60	The **inactive** field provides the user with a "grace" period in which their password can be changed.
expire	15050	This field represents the number of days from January 1, 1970 and the day the account will "expire".

- Moving the passwords to the shadow file makes it less likely that the encrypted password can be decrypted, because only the root user has access to the shadow file. The format of the password file is as follows:
- Account_name:Password:Last:Min:Max:Warn:Expire:Disable:Reserved

Examine:

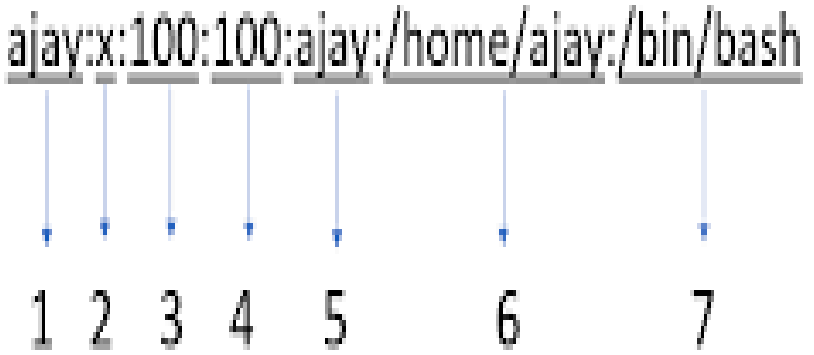
cat /etc/passwd

- Notice that the second field has an "X" (*mike*:**x**:*503*). That is because the passwords have been shadowed. Because so many hacking tools are Linux only, you should know some basic Linux commands so you can navigate distributions such as Kali.

The seven fields of /etc/passwd file

Field	Description
1	Username. This is mapped to numeric UID
2	Historically encrypted password was here. Today passwords are in /etc/shadow.
3	User ID (UID) is a numeric. Used to identify user into the system
4	Group ID (GID) is a numeric
5	GECOS is used to include any arbitrary text. Usually it is used include user's real name.
6	User's home directory. It is the location for user's personal data and configuration files.
7	User's shell. It is the program that run when user logs in. For a regular user, this is the program that provides user's command prompt.

Structure of **/etc/passwd** file:



1. Username
2. Password: An x character indicates that password is encrypted and stored in /etc/shadow file.
3. UID (User ID)
4. GID (Group ID)
5. User information
6. Home Directory: detailed path of home directory of the user.
7. Shell

Errors

- Measurement will not exactly match reference template. (Different from passwords)
- Two kinds of errors
  - False positives (Accepting wrong user, security related)
  - False negatives (Rejecting legitimate user, comfort related)
- Matching algorithm used to compare with templates
- The matching is converted to a *score*. Better match gives higher score
- A threshold will determine what the minimum score must be to accept user as valid

FAR & FRR

FAR – False Acceptance Rate

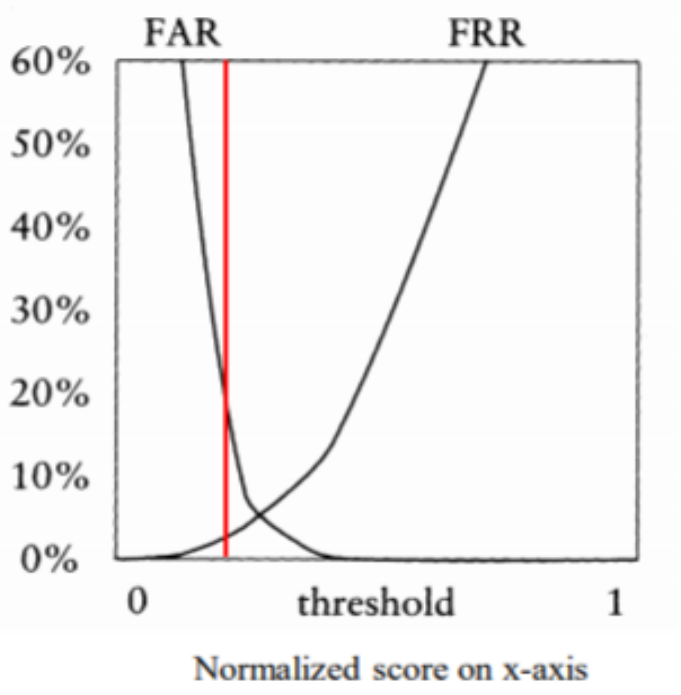
FRR – False Rejection Rate

Equal Error Rate (EER) when FAR=FRR

Course book also includes FTA – Failure To Aquire

We assume it is zero!

Graph for typical system



Password Salting

- Add some extra info, **salt**, to the password before hashing.
  - Username
  - Randomly generated characters
- Salt stored with hashed password.

Username	Salt	Password
Alice	Gfgh5	g6F4fdsg8h...h5NHa
Bob	kd6sd	dsjk7H5dg0...d2a5V
Charlie	dsfjh	KJ7YtrcZa2...l9j7G
David	J7Fj2	p09J7h6bD3...73Dnt

- **Three advantages:**
  1. Slows down dictionary attacks when trying to break several passwords at once.
  2. One Rainbow table for each salt needed
  3. Two users with same password will have different hash

Cracking Linux Passwords

- Linux has a host of password-cracking tools available such as Hashcat, Ophcrack, and John the Ripper. John the Ripper is available at http://www.openwall.com/John/. It is probably the most well-known, most versatile, password-cracking program around

Password TIPS

- "***They should be changed often, not shared with others, and not displayed in public.***"

Hiding Files and Covering Tracks

- Before moving on to other systems, the attacker must attend to a few unfinished items. According to Locard's exchange principle , "**Whenever someone comes in contact with another person, place, or thing, something of that person is left behind.**"
- This means that the attacker must disable logging, clear log files, eliminate evidence, plant additional tools, and cover his tracks. If this is on a Linux system, the attacker may attempt to stop the syslog server, **/etc/init.d/syslogd stop/**

Techniques that an attacker can use to cover his tracks

- **Disabling logging:** Auditpol, a Windows tools for auditing policies, works well for hackers, too, as long as they have administrative access. Just point it at the victim's system as follows:

C:\ >auditpol \\ 192.168.13.10 /disable

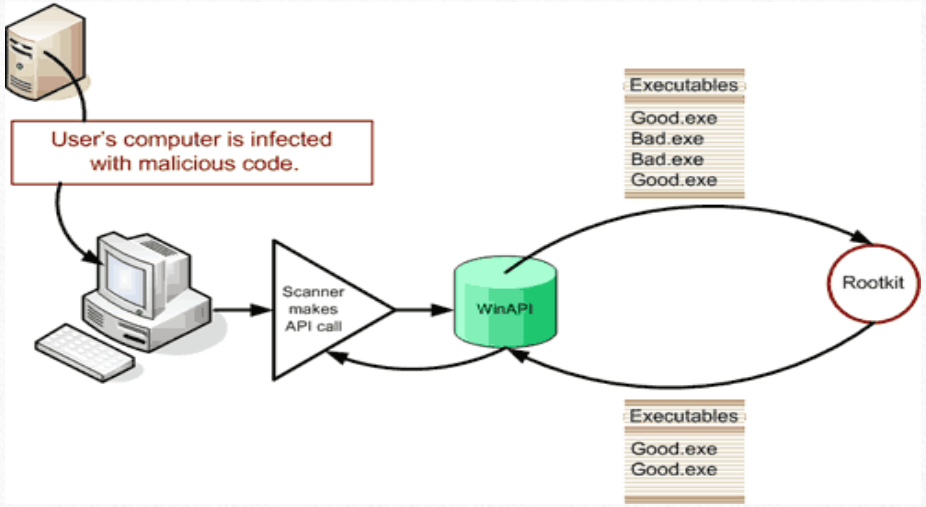
Auditing Disabled

- **Clear the log file:** The attacker will also attempt to clear the log. Tools such as Winzapper, Evidence Eliminator, and ELSave can be used. ELSave will remove all entries from the logs, except one entry that shows the logs were cleared. It is used as follows:

elsave -s \\192.168.13.10 -l "Security" -C

Rootkits

Rootkit is a term applied to a type of malware that is designed to infect a target PC and allow an attacker to install a set of tools that grant him persistent remote access to the computer. ... In recent years, a new class of mobile **rootkits** have emerged to **attack** smartphones, specifically Android devices.



One way for attackers to cover their tracks is with **Rootkits.**

- A rootkit contains a set of tools and replacement executables for many of the operating system's critical components
- Once installed, a rootkit can be used to hide evidence of the attacker's presence and to give the attacker backdoor access to the system.
- Rootkits require root access, but in return they give the attacker complete control of the system.
- The attacker can come and go at will and hide his activities from the administrator.
- Rootkits can contain log cleaners that attempt to remove all traces of an attacker's presence from the log files.

- rootkits replaced binaries, such as **ls**, **ifconfig**, **inetd**, **killall**, **login**, **netstat**, **passwd**, **pidof**, and **ps**, with Trojaned versions that were written to hide certain processes or information from the administrators.
- Rootkits of this type are detectable because of the change in size of the Trojaned binaries.
- Tools such as MD5Sum and Tripwire can be a big help in uncovering these types of hacks.

Rootkits can be divided into several categories:

- **Hypervisor:** Modifies the boot sequence of a virtual machine
- **Hardware/firmware:** Hides in hardware or firmware
- **Bootloader:** Replaces the original bootloader
- **Library level:** Replaces original system calls
- **Application level:** Replaces application binaries with fake ones
- **Loadable kernel level:** Adds malware to the security kernel

- Some rootkits target the loadable kernel module (LKM). A kernel rootkit is loaded as a driver or kernel extension. Because kernel rootkits corrupt the kernel, they can do basically anything, including avoiding detection by many software methods.
- The best way to avoid these rootkits is just to recompile the kernel without support for LKMs.
- Some rootkits can also hide their existence by using application programming interface (API) hooks. These hooks usually only work against other processes on the infected computer while the system is running.
- If the system is analyzed as a static drive or by a third-party system, the existence of the hooks may become apparent.

How should an ethical hacker respond if he believes that a system has been compromised and has had a rootkit installed?

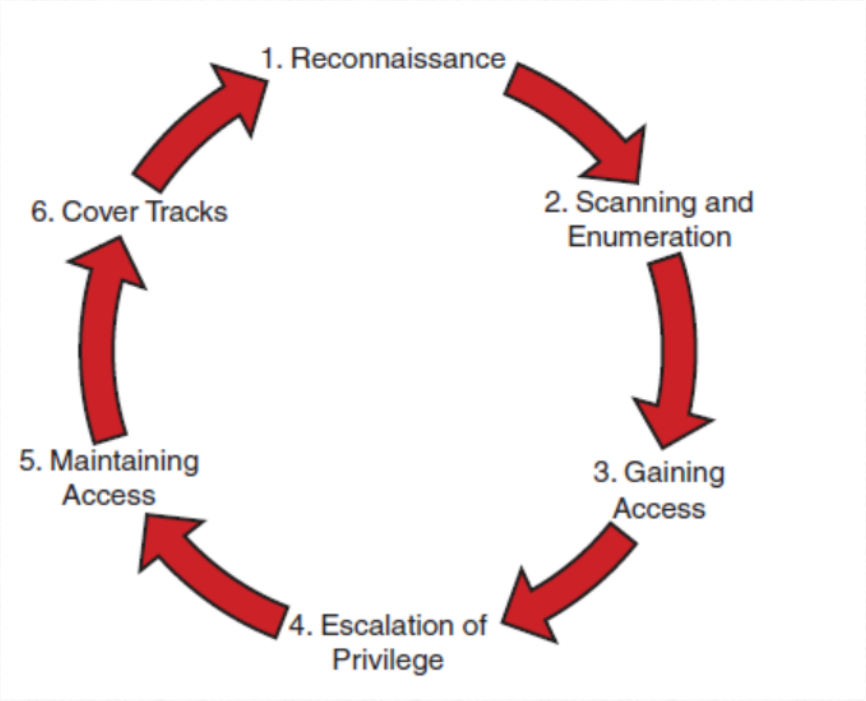
- First action to remove the infected host from the network.
- An attacker who knows that he has been discovered might decide to trash the system in an attempt to cover his tracks.
- After isolating the host from the network, you can then begin the process of auditing the system and performing some forensic research.
- A number of tools enable you to detect rootkits.
- Most work by one or more of the following techniques: integrity-based detection, signature-based detection, cross-view detection, and heuristic detection.

Tools that you can use to audit suspected rootkit attacks include the following:

- **Chkrootkit:** An excellent tool that enables you to search for signs of a rootkit.
- **RootKitRevealer:** A standalone utility used to detect and remove complex rootkits.
- **McAfee Rootkit Detective:** Designed to look for and find known rootkits. It can examine system binaries for modification.
- **Trend Micro RootkitBuster:** Another tool that scans file and system binariesfor known and unknown rootkits.

File Hiding

- Various techniques are used by attackers to hide their tools on the compromised computer.


1. Reconnaissance
2. Scanning and Enumeration
3. Gaining Access
4. Escalation of Privilege
5. Maintaining Access
6. Cover Tracks

Thank you

- ***"It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it."***
  — Stephane Nappo