

University of Technology
الجامعة التكنولوجية
Computer Science Department
قسم علوم الحاسوب



Subject: - Ethical Hacking

القرصنة الاخلاقية

by

Prof.Dr. Ekhlas Khalaf



cs.uotechnology.edu.iq

Ethical Hacking

Introduction:

Hacking is the act of finding the possible entry points that exist in a computer system or a computer network and finally entering into them. Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer.

1. Defining Ethical Hacking

- Traditionally, a hacker is someone who likes to tinker with software or electronic systems. Hackers enjoy exploring and learning how computer systems operate. They love discovering new ways to work electronically.
- Recently, hacker has taken on a new meaning — someone who maliciously breaks into systems for personal gain. Technically, these criminals are crackers (criminal hackers). Crackers break into (crack) systems with malicious intent. They are out for personal gain: fame, profit, and even revenge. They modify, delete, and steal critical information, often making other people miserable.

Hackers can be divided into three groups:-

- **White Hats** Good guys, ethical hackers
- **Black Hats** Bad guys, malicious hackers
- **Gray Hats** Good or bad hacker; depends on the situation.

Ethical hackers usually fall into the white-hat category, but sometimes they're former gray hats who have become security professionals and who now use their skills in an ethical manner.

White Hats

White hats are the good guys, the ethical hackers who use their hacking skills for defensive purposes. White-hat hackers are usually security professionals with knowledge of hacking and the hacker toolset and who use this knowledge to locate weaknesses and implement

countermeasures. White-hat hackers are prime candidates for the exam. White hats are those who hack with permission from the data owner. It is critical to get permission prior to beginning any hacking activity. This is what makes a security professional a white hat versus a malicious hacker who cannot be trusted.

Black Hats

Black hats are the bad guys: the malicious hackers or *crackers* who use their skills for illegal or malicious purposes. They break into or otherwise violate the system integrity of remote systems, with malicious intent. Having gained unauthorized access, black-hat hackers destroy vital data, deny legitimate users service, and just cause problems for their targets. Black-hat hackers and crackers can easily be differentiated from white-hat hackers because their actions are malicious.

Gray Hats

Gray hats are hackers who may work offensively or defensively, depending on the situation. This is the dividing line between hacker and cracker. Gray-hat hackers may just be interested in hacking tools and technologies and are not malicious black hats. Gray hats are self-proclaimed ethical hackers, who are interested in hacker tools mostly from a curiosity standpoint. They may want to highlight security problems in a system or educate victims so they secure their systems properly. These hackers are doing their “victims” a favor. For instance, if a weakness is discovered in a service offered by an investment bank, the hacker is doing the bank a favor by giving the bank a chance to rectify the vulnerability.

1.1 Types of Hacking

We can divide hacking into different categories, based on what is being hacked. Here is a set of examples –

- **Website Hacking** – Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.
- **Network Hacking** – Hacking a network means gathering information about a network by using tools like Telnet, Ping, Tracert, Netstat, etc. with the intent to harm the network system and hamper its operation.
- **Email Hacking** – It includes getting unauthorized access on an Email account and using it without taking the consent of its owner.
- **Ethical Hacking** – Ethical hacking involves finding weaknesses in a computer or network system for testing purpose and finally getting them fixed.
- **Password Hacking** – This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.
- **Computer Hacking** – This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.

1.2 Advantages of Hacking

Hacking is quite useful in the following scenarios –

- To recover lost information, especially in case you lost your password.
- To perform penetration testing to strengthen computer and network security.
- To put adequate preventative measures in place to prevent security breaches.
- To have a computer system that prevents malicious hackers from gaining access.

1.3 Disadvantages of Hacking

Hacking is quite dangerous if it is done with harmful intent. It can cause:

- Massive security breach.
- Unauthorized system access on private information.
- Privacy violation.
- Hampering system operation.
- Denial of service attacks.
- Malicious attack on the system.

1.4 Purposes of Hacking

There could be various positive and negative intentions behind performing hacking activities. Here is a list of some probable reasons why people indulge in hacking activities

- Just for fun
- Steal important information
- Damaging the system
- Hampering privacy
- Money extortion
- System security testing
- To break policy compliance

1.4 System Hacking

System hacking is a big step in the fact that **you** (as a hacker) are no longer simply scanning and enumerating a system. At this point, you are attempting to gain access. Things start to change because this stage is about breaking and entering into the targeted system. many steps, such as foot printing, scanning, and enumeration, are all considered pre-attack stages. As stated, before you begin, make sure that you have permission to perform these activities on other people's systems. The primary goal of the system hacking stage is to authenticate to the remote host with the highest level of access. This section covers some common nontechnical and technical password attacks against authentication systems.

1.4.1 Nontechnical Password Attacks

Attackers are always looking for **easy ways to gain access to systems**. Hacking authentication systems is getting harder because most organizations have upped their game, using strong authentication and improving auditing controls. That is one reason why nontechnical attacks remain so popular. Basic techniques include the following:

■ **Dumpster diving:** dumpster diving is the act of looking through a company's trash to find information that may help in an attack. Access codes, notes, passwords, and even account information can be found.

■ **Social engineering:** social engineering is the manipulation of people into performing actions or divulging confidential information.

■ **Shoulder surfing:** The act of watching over someone's shoulder to get information such as passwords, logins, and account details.

1.5.2 Technical Password Attacks

Technical password attacks require some **use of technology**. These attacks also build on the information you have obtained in the previous steps. Tools used during enumeration, such as Getacct, IP Network Browser, and net view, may have returned some valuable clues about specific accounts. By now, you may even have account names, know who is the administration, know whether there is a lockout policy, and even know the names of open shares. Technical password attack techniques discussed here include the following:

- Password guessing
- Automated password guessing
- Password sniffing
- Keyloggers

Many of today's most successful attacks involve both technical and nontechnical elements.

Password Guessing

Guessing usernames and passwords requires that you review your findings. Remember that good documentation is always needed during a penetration test, so make sure that you have recorded all your previous activities. When password guessing is successful, it is usually because people like to use easy to remember words and phrases. A diligent penetration tester or attacker will look for subtle clues throughout the enumeration process to key in on—probably words or phrases the account holder might have used for a password. What do you know about this individual, what are his hobbies? If the account holder is not known to you, focus on accounts that

- Haven't had password changes for a long time
- Have weakly protected service accounts
- Have poorly shared accounts

- Indicate the user has never logged in
- Have information in the comment field that might be used to compromise password security

1.6 The Phases of Ethical Hacking

The process of ethical hacking can be broken down into five distinct phases. An ethical hacker follows processes similar to those of a malicious hacker. The steps to gain and maintain entry into a computer system are similar no matter what the hacker's intentions are. Figure 1.1 illustrates the five phases that hackers generally follow in hacking a computer system.

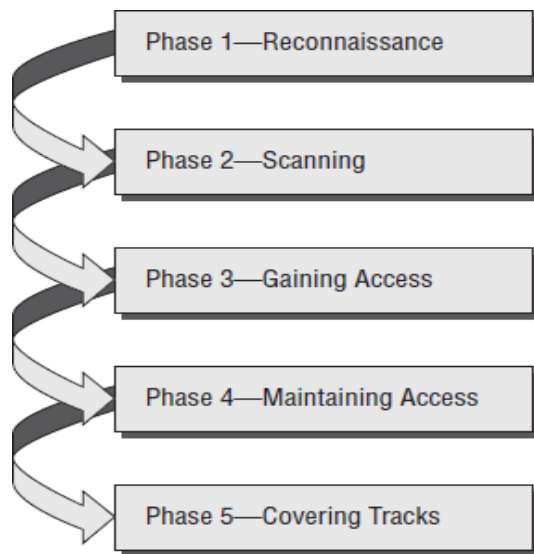


Figure 1.1 Phases of hacking.

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

✚ **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

Gaining access 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.

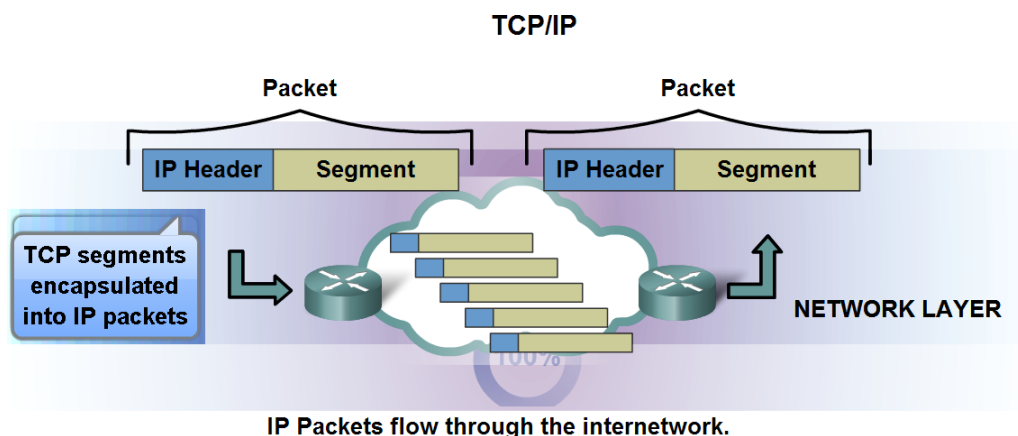
Phase 5: Covering Tracks

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

TCP/IP Model Principles

TCP/IP protocol suite is designed through a highly structured and layered approach, with each layer responsible for a different facet of communications. This hierarchical architecture makes each protocol layer possible to develop independently without affecting the adjacent layer. Data encapsulation is achieved by various headers among different transportation layers, like IP header, TCP header or application headers. These headers are critical in keeping the state information for each network connection or facilitating the multiplexing and de-multiplexing of communication messages.



- **Connectionless** - No connection is established before sending data packets.
- **Best Effort (unreliable)** - No overhead is used to guarantee packet delivery.
- **Media Independent** - Operates independently of the medium carrying the data.

1- The Internet Protocol (IP)

IP (short for Internet Protocol) specifies the technical format of packets and the addressing scheme for computers to communicate over a network. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a source and a destination.

IP by itself can be compared to something like the **postal system**. It allows you to address a package and drop it in the system, but there's no direct link between you and the recipient. TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time.

2- Transmission Control Protocol (TCP) :is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet.

TCP is built on top of IP layer, which is unreliable and connectionless. However, TCP provides the higher layer application a reliable connection-oriented service. As a tradeoff, each TCP connection requires an establishment procedure and a termination step between communication peers. Furthermore, TCP also provides sequencing and flow control.

source port number			destination port number		
sequence number					
acknowledge number					
header	reserved	urg,ack,psh,rst,syn,fin		window size	
TCP checksum			urgent pointer		
options (if any)					
data (if any)					

TCP Header

Without options, TCP header occupies 20 bytes. The source and destination port number is used to identify the sending and receiving processes. The sequence number is essential in keeping the sending and receiving datagram in proper order. There are six flag bits with the TCP header, namely URG, ACK, PSH, RST, SYN and FIN, each of them has a special use in the connection establishment, connection termination or other control purposes. Window size is advertised between communication peers to maintain the flow control. TCP establishes a connection in three steps, namely **three-way handshake**. Following figure is a typical three-way handshake procedure happened between a source host S and a destination host D.

TCP: Transmission Control Protocol

UDP :User Datagram Protocol

(SCTP) :Stream Control Transmission Protocol

(IGMP): Internet Group Message Protocol

URG: The value of the urgent pointer field is valid.

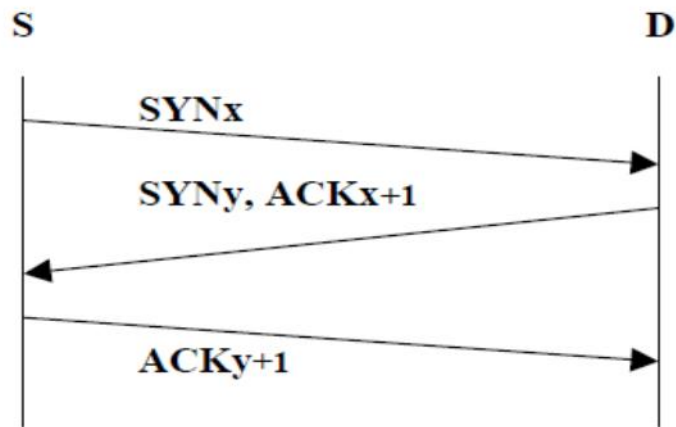
ACK: The value of the acknowledgment field is valid.

PSH: Push the data.

RST: Reset the connection.

SYN: Synchronize sequence numbers during connection.

FIN: Terminate the connection.



Three-Way handshake

First, source host sends a SYN packet to destination host, telling it the wish to establish a connection and setting its own ISN (Initial Sequence Number) in sequence number field. Upon receiving the request packet, the destination host sends back a SYN_ACK packet with its own ISN and the incremented ISN from source host. Finally, the source host will transmit an ACK packet and data transfer can take place. There is one extra point need to mention. Suppose that host S did not send any SYN packet but received a SYN_ACK packet from host D, it would just send back a RST packet to reset the connection.

3- User Datagram Protocol (UDP): is an unreliable, connectionless protocol. It is also widely used for one-shot.client-server type request-reply queries and applications in which prompt delivery is more important than accurate delivery.

Foot printing

Foot printing is defined as the process of creating a blueprint or map of an organization's network and systems. Information gathering is also known as foot printing an organization. Foot printing begins by determining the target system, application, or physical location of the target. Once this information is known, specific information about the organization is gathered using nonintrusive methods. For example, the organization's own web page may provide a personnel directory or a list of employee bios, which may prove useful if the hacker needs to use a social-engineering attack to reach the objective. The information the hacker is looking for during the foot printing phase is anything that gives clues as to the network architecture,

server, and application types where valuable data is stored. Before an attack or exploit can be launched, the operating system and version as well as application types must be uncovered so the most effective attack can be launched against the target. Here are some of the pieces of information to be gathered about a target during foot printing:

- Domain name
- Network blocks
- Network services and applications
- System architecture
- Intrusion detection system
- Authentication mechanisms
- Specific IP addresses
- Access control mechanisms
- Phone numbers
- Contact addresses

1- Foot printing Tools

Foot printing can be done using hacking tools, either applications or websites, which allow the hacker to locate information passively. By using these foot printing tools, a hacker can gain some basic information on, or “footprint,” the target. By first foot printing the target, a hacker can eliminate tools that will not work against the target systems or network. For example, if a graphics design firm uses all Macintosh computers, then all hacking software that targets Windows systems can be eliminated. Foot printing not only speeds up the hacking process by eliminating certain toolsets but also minimizes the chance of detection as fewer hacking attempts can be made by using the right tool for the job. Some of the common tools used for foot printing and information gathering are as follows:

- a) Domain name lookup
- b) Whois
- c) NSlookup
- d) Sam Spade

1- Domain Name Information

You can <http://www.whois.com/whois> website to get detailed information about a domain name information including its owner, its registrar, date of registration, expiry, name server, owner's contact information, etc.



The image shows a screenshot of the WHOIS Lookup website. At the top, it says "WHOIS Lookup" in orange. Below that, it says "Search domain name registration records". There is a search input field with the placeholder text "Enter Domain Name or IP Address" and a green "SEARCH" button with a magnifying glass icon. Below the input field, it lists examples: "Examples: qq.com, google.co.in, bbc.co.uk, ebay.ca".

1- Quick Fix: It's always recommended to keep your domain name profile a private one which should hide the above-mentioned information from potential hackers.

2-Finding IP Address: You can use **ping** command at your prompt. This command is available on Windows as well as on Linux OS. Following is the example to find out the IP address of tutorialspoint.com

```
$ping tutorialspoint.com
```

It will produce the following result –

```
PING tutorialspoint.com
(66.135.33.172) 56(84) bytes of data.
64 bytes from 66.135.33.172: icmp_seq = 1 ttl = 64 time = 0.028 ms
64 bytes from 66.135.33.172: icmp_seq = 2 ttl = 64 time = 0.021 ms
64 bytes from 66.135.33.172: icmp_seq = 3 ttl = 64 time = 0.021 ms
64 bytes from 66.135.33.172: icmp_seq = 4 ttl = 64 time = 0.021 ms
```

3- Finding Hosting Company: Once you have the website address, you can get further detail by using ip2location.com website. Following is the example to find out the details of an IP address –

	Field Name	Value
	IP Address	49.205.122.168
<input checked="" type="checkbox"/>	Country	India
<input type="checkbox"/>	Region & City	Kukatpalli, Telangana
<input type="checkbox"/>	Latitude & Longitude	17.48333, 78.41667
<input type="checkbox"/>	ZIP Code	508126
<input type="checkbox"/>	ISP	Beam Telecom Pvt Ltd
<input type="checkbox"/>	Domain	beamtele.com
<input type="checkbox"/>	Time Zone	+05:30

Here the ISP (Internet Service Provide) row gives you the detail about the hosting company because IP addresses are usually provided by hosting companies only.

4- IP Address Ranges : Small sites may have a single IP address associated with them, but larger websites usually have multiple IP addresses serving different domains and sub-domains. You can obtain a range of IP addresses assigned to a particular company using American Registry for Internet Numbers (ARIN).



You can enter company name in the highlighted search box to find out a list of all the assigned IP addresses to that company.

5- History of the Website: It is very easy to get a complete history of any website using www.archive.org.



You can enter a domain name in the search box to find out how the website was looking at a given point of time and what were the pages available on the website on different dates.

Scanning and Enumeration

Scanning is the first phase of active hacking and is used to locate target systems or networks for later attack. Enumeration is the follow-on step once scanning is complete and is used to identify computer names, usernames, and shares.

1- Scanning

After the reconnaissance and information-gathering stages have been completed, scanning is performed. It is important that the information-gathering stage be as complete as possible to identify the best location and targets to scan. During scanning, the hacker continues to gather information regarding the network and its individual host systems. Information such as IP addresses, operating system, services, and installed applications can help the hacker determine which type of exploit to use in hacking a system. *Scanning* is the process of locating systems that are alive and responding on the network. Ethical hackers use scanning to identify target systems' IP addresses. Scanning is also used to determine whether a system is on the network and available. Scanning tools are used to gather information about a system such as IP addresses, the operating system, and services running on the target computer.

1-Scanning based on purpose

- Port scanning: determines open ports and services.
- Network scanning: identifies IP addresses on a given network or subnet.
- Vulnerability scanning: discovers presence of known weaknesses on target systems.

Port Scanning: port scanning is the process of identifying open and available TCP/IP ports on a system. Port-scanning tools enable a hacker to learn about the services available on a given system. Each service or application on a machine is associated with a *well-known* port number.

Port Numbers are divided into three ranges:

- Well-Known Ports: 0-1023
- Registered Ports: 1024-49151
- Dynamic Ports: 49152-65535

For example, a port-scanning tool that identifies port 80 as open indicates a web server is running on that system. Hackers need to be familiar with well-known port numbers.

Network Scanning: network scanning is a procedure for identifying active hosts on a network, either to attack them or as a network security assessment. Hosts are identified by their

individual IP addresses. Network-scanning tools attempt to identify all the *live* or responding hosts on the network and their corresponding IP addresses.

Vulnerability Scanning : vulnerability scanning is the process of proactively identifying the vulnerabilities of computer systems on a network. Generally, a vulnerability scanner first identifies the operating system and version number, including service packs that may be installed. Then, the scanner identifies weaknesses or vulnerabilities in the operating system. During the later attack phase, a hacker can exploit those weaknesses in order to gain access to the system. Although scanning can quickly identify which hosts are listening and active on a network, it is also a quick way to be identified by an intrusion detection system (IDS). Scanning tools probe TCP/IP ports looking for open ports and IP addresses, and these probes can be recognized by most security intrusion detection tools. Network and vulnerability scanning can usually be detected as well, because the scanner must interact with the target system over the network. Depending on the type of scanning application and the speed of the scan, an IDS will detect the scanning and flag it as an IDS event. Some of the tools for scanning have different modes to attempt to defeat an IDS and are more likely to be able to scan undetected. As a CEH it is your job to gather as much information as possible and try and remain undetected.

2-Scan types:

A **port scanner** is an application designed to probe a **server** or **host** for open **ports**. Such an application may be used by **administrators** to verify **security** policies of their **networks** and by **attackers** to identify **network services** running on a host and exploit vulnerabilities.

A **port scan** is a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port; this is not a nefarious process in and of itself. The majority of uses of a port scan are not attacks, but rather simple probes to determine services available on a remote machine.

Sweep scan is to scan multiple hosts for a specific listening port. The latter is typically used to search for a specific service, for example, an **SQL-based computer worm** may sweep looking for hosts listening on **TCP** port 1433.

a. TCP scanning.

The simplest port scanners use the operating system's network functions and are generally the next option to go to when SYN is not a feasible option (described next). **Nmap** calls this mode

connect scan, named after the Unix `connect()` system call. If a port is open, the operating system completes the **TCP** three-way handshake, and the port scanner immediately closes the connection to avoid performing a **Denial-of-service attack**. Otherwise, an error code is returned. This scan mode has the advantage that the user does not require special privileges. However, using the OS network functions prevents low-level control, so this scan type is less common. This method is "noisy", particularly if it is a "*port sweep*": the services can log the sender IP address and **Intrusion detection systems** can raise an alarm.

b. SYN scanning

SYN scan is another form of TCP scanning. Rather than using the operating system's network functions, the port scanner generates raw IP packets itself, and monitors for responses. This scan type is also known as "half-open scanning", because it never actually opens a full TCP connection. The port scanner generates a SYN packet. If the target port is open, it will respond with a SYN-ACK packet. The scanner host responds with an RST packet, closing the connection before the handshake is completed.[3] If the port is closed but unfiltered, the target will instantly respond with an RST packet.

c. UDP scanning

UDP scanning is also possible, although there are technical challenges. **UDP** is a **connectionless** protocol so there is no equivalent to a TCP SYN packet. However, if a UDP packet is sent to a port that is not open, the system will respond with an **ICMP** port unreachable message. Most UDP port scanners use this scanning method, and use the absence of a response to infer that a port is open. However, if a port is blocked by a **firewall**, this method will falsely report that the port is open. If the port unreachable message is blocked, all ports will appear open. This method is also affected by **ICMP rate limiting**.

d. ACK scanning

ACK scanning is one of the more unusual scan types, as it does not exactly determine whether the port is open or closed, but whether the port is filtered or unfiltered. This is especially good when attempting to probe for the existence of a firewall and its rulesets. Simple packet filtering will allow established connections (packets with the ACK bit set), whereas a more sophisticated tasteful firewall might not.

e. Window scanning

Rarely used because of its outdated nature, window scanning is fairly untrustworthy in determining whether a port is opened or closed. It generates the same packet as an ACK scan, but checks whether the window field of the packet has been modified. When the packet reaches its destination, a design flaw attempts to create a window size for the packet if the port is open, flagging the window field of the packet with 1's before it returns to the sender. Using this scanning technique with systems that no longer support this implementation returns 0's for the window field, labeling open ports as closed.

f. FIN scanning

Since SYN scans are not surreptitious enough, firewalls are, in general, scanning for and blocking packets in the form of SYN packets. **FIN packets** can bypass firewalls without modification. Closed ports reply to a FIN packet with the appropriate RST packet, whereas open ports ignore the packet on hand. This is typical behavior due to the nature of TCP, and is in some ways an inescapable downfall.

3- The Certified Ethical Hacker (CEH) Scanning Methodology

As a CEH, you're expected to be familiar with the scanning methodology presented in Figure 1. This methodology is the process by which a hacker scans the network. It ensures that no system or vulnerability is overlooked, and that the hacker gathers all necessary information to perform an attack. Various stages of this scanning methodology, starting with the first three steps checking for systems that are live and for open ports and service identification in the following section.

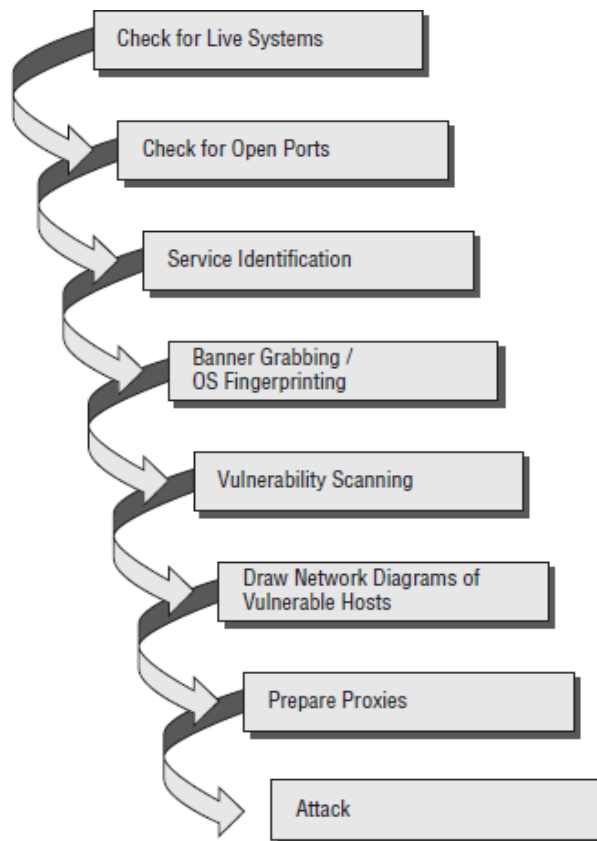


Figure 1. (CEH) Scanning Methodology.

2- Enumeration

Enumeration belongs to the first phase of Ethical Hacking, i.e., “Information Gathering”. This is a process where the attacker establishes an active connection with the victim and try to discover as much attack vectors as possible, which can be used to exploit the systems further.[3]

Enumeration can be used to gain information on –

- *TCP: Transmission Control Protocol*
- *UDP: User Datagram Protocol*
- *(SCTP): Stream Control Transmission Protocol*
- *(IGMP): Internet Group Message Protocol*
- *URG: The value of the urgent pointer field is valid.*
- *ACK: The value of the acknowledgment field is valid.*
- *PSH: Push the data.*
- *RST Reset the connection.*
- *SYN: Synchronize sequence numbers during connection.*

- Network shares
- SNMP (simple network management protocol) data, if they are not secured properly(IP tables)
- Usernames of different systems
- Passwords policies lists

Enumerations depend on the services that the systems offer. They can be –

- DNS (Domain Name System) enumeration
- NTP enumeration
- SNMP enumeration
- Linux/Windows enumeration
- SMB enumeration

Enumeration occurs after scanning and is the process of gathering and compiling usernames, machine names, network resources, shares, and services. It also refers to actively querying or connecting to a target system to acquire this information. Hackers need to be methodical in their approach to hacking. The following steps are an example of those a hacker might perform in preparation for hacking a target system[1]:

1. Extract usernames using enumeration.
2. Gather information about the host using null sessions.
3. Perform Windows enumeration using the SuperScan tool.
4. Acquire the user accounts using the tool GetAcct.
5. Perform SNMP port scanning.

The object of enumeration is to identify a user account or system account for potential use in hacking the target system. It isn't necessary to find a system administrator account, because most account privileges can be escalated to allow the account more access than was previously granted.

Many hacking tools are designed for scanning IP networks to locate NetBIOS name information. For each responding host, the tools list IP address, NetBIOS computer name, logged-in username, and MAC address information. On a Windows 2000 domain, the built-in tool net view can be used for NetBIOS enumeration. To enumerate NetBIOS names using the net view command, enter the following at the command prompt:

```
net view / domain  
nbtstat -A IP address
```

Null Sessions

A null session occurs when you log in to a system with no username or password. NetBIOS null sessions are a vulnerability found in the Common Internet File System (CIFS) or SMB, depending on the operating system.

Once a hacker has made a NetBIOS connection using a null session to a system, they can easily get a full dump of all usernames, groups, shares, permissions, policies, services, and more using the Null user account. The SMB and NetBIOS standards in Windows include APIs that return information about a system via TCP port 139. One method of connecting a NetBIOS null session to a Windows system is to use the hidden Inter-Process Communication share (IPC\$). This hidden share is accessible using the net use command. As mentioned earlier, the net use command is a built-in Windows command that connects to a share on another computer. The empty quotation marks (“”) indicate that you want to connect with no username and no password. To make a NetBIOS null session to a system with the IP address 192.21.7.1 with the built-in anonymous user account and a null password using the net use command, the syntax is as follows:

```
C: \> net use \\192.21.7.1 \IPC$ “” /u: “”
```

Once the net use command has been successfully completed, the hacker has a channel over which to use other hacking tools and techniques. As a CEH, you need to know how to defend against NetBIOS enumeration and null sessions.

NetBIOS Enumeration and Null Session Countermeasures

The NetBIOS null session uses specific port numbers on the target machine. Null sessions require access to TCP ports 135, 137,139, and/or 445. One countermeasure is to close these ports on the target system. This can be accomplished by disabling SMB services on individual hosts by unbinding the TCP/IP WINS client from the interface in the network connection's properties. To implement this countermeasure, perform the following steps:

1. Open the properties of the network connection.
2. Click TCP/IP and then the Properties button.
3. Click the Advanced button.
4. On the WINS tab, select Disable NetBIOS Over TCP/IP.

A security administrator can also edit the Registry directly to restrict the anonymous user from login. To implement this countermeasure, follow these steps:

1. Open regedt32 and navigate to HKLM\SYSTEM\CurrentControlSet\LSA.
2. Choose Edit ⇔ Add Value. Enter these values:
 - Value Name: **RestrictAnonymous**
 - Data Type: **REG_WORD**
 - Value: **2**

Sniffing

Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is a form of “tapping phone wires” and get to know about the conversation. It is also called **wiretapping** applied to the computer networks.

There is so much possibility that if a set of enterprise switch ports is open, then one of their employees can sniff the whole traffic of the network. Anyone in the same physical location can plug into the network using Ethernet cable or connect wirelessly to that network and sniff the total traffic.

In other words, Sniffing allows you to see all sorts of traffic, both protected and unprotected. In the right conditions and with the right protocols in place, an attacking party may be able to gather information that can be used for further attacks or to cause other issues for the network or system owner.

What can be sniffed?

One can sniff the following sensitive information from a network –

- Email traffic
- FTP passwords
- Web traffics
- Telnet passwords
- Router configuration
- Chat sessions
- DNS traffic

-Types of Sniffing

Sniffing can be either Active or Passive in nature.

Passive Sniffing

In passive sniffing, the traffic is locked but it is not altered in any way. Passive sniffing allows listening only. It works with Hub devices. On a hub device, the traffic is sent to all the ports. In a network that uses hubs to connect systems, all hosts on the network can see the traffic. Therefore, an attacker can easily capture traffic going through.

The good news is that hubs are almost obsolete nowadays. Most modern networks use switches. Hence, passive sniffing is no more effective.

Active Sniffing

In active sniffing, the traffic is not only locked and monitored, but it may also be altered in some way as determined by the attack. Active sniffing is used to sniff a switch-based network. It involves injecting **address resolution packets** (ARP) into a target network to flood on the switch **content addressable memory** (CAM) table. CAM keeps track of which host is connected to which port.

DNS Poisoning

DNS Poisoning is a technique that tricks a DNS server into believing that it has received authentic information when, in reality, it has not. It results in the substitution of false IP

address at the DNS level where web addresses are converted into numeric IP addresses. It allows an attacker to replace IP address entries for a target site on a given DNS server with IP address of the server controls. An attacker can create fake DNS entries for the server which may contain malicious content with the same name.

For instance, a user types `www.google.com`, but the user is sent to another fraud site instead of being directed to Google's servers. As we understand, DNS poisoning is used to redirect the users to fake pages which are managed by the attackers.

Defenses against DNS Poisoning

As an ethical hacker, your work could very likely put you in a position of prevention rather than pen testing. What you know as an attacker can help you prevent the very techniques you employ from the outside.

Here are defenses against the attacks we just covered from a pen tester's perspective –

- Use a hardware-switched network for the most sensitive portions of your network in an effort to isolate traffic to a single segment or collision domain.
- Implement IP DHCP Snooping on switches to prevent ARP poisoning and spoofing attacks.
- Implement policies to prevent promiscuous mode on network adapters.
- Be careful when deploying wireless access points, knowing that all traffic on the wireless network is subject to sniffing.
- Encrypt your sensitive traffic using an encrypting protocol such as SSH or IPsec.
- Port security is used by switches that have the ability to be programmed to allow only specific MAC addresses to send and receive data on each port.
- IPv6 has security benefits and options that IPv4 does not have.
- Replacing protocols such as FTP and Telnet with SSH is an effective defense against sniffing. If SSH is not a viable solution, consider protecting older legacy protocols with IPsec.

In the following sections, four types of hacking will be explained with details:

1. Hacking Windows
2. Linux Hacking
3. Wireless Hacking
4. Web Server Hacking

1- Hacking Windows

The primary vectors for compromising Windows systems remotely include:

- 1. Authentication spoofing:** The primary gatekeeper of access to Windows systems remains the frail password. Common brute force/dictionary password guessing and man-in-the-middle authentication spoofing remain real threats to Windows networks.
- 2. Network services:** Modern tools make it point-click-exploit easy to penetrate vulnerable services that listen on the network.
- 3. Client vulnerabilities :** Client software like Internet Explorer, Outlook, Windows Messenger, Office, and others have all come under harsh scrutiny from attackers looking for direct access to end user data.
- 4. Device drivers :** Ongoing research continues to expose new attack surfaces where the operating system parses raw data from devices like wireless network interfaces, USB memory sticks, and inserted media like CD-ROM disks.

Privilege Escalation

Once attackers have obtained a user account on a Windows system, they will set their eyes immediately on obtaining Administrator- or SYSTEM-equivalent privileges. One of the all-time greatest hacks of Windows was the so-called getadmin family of exploits

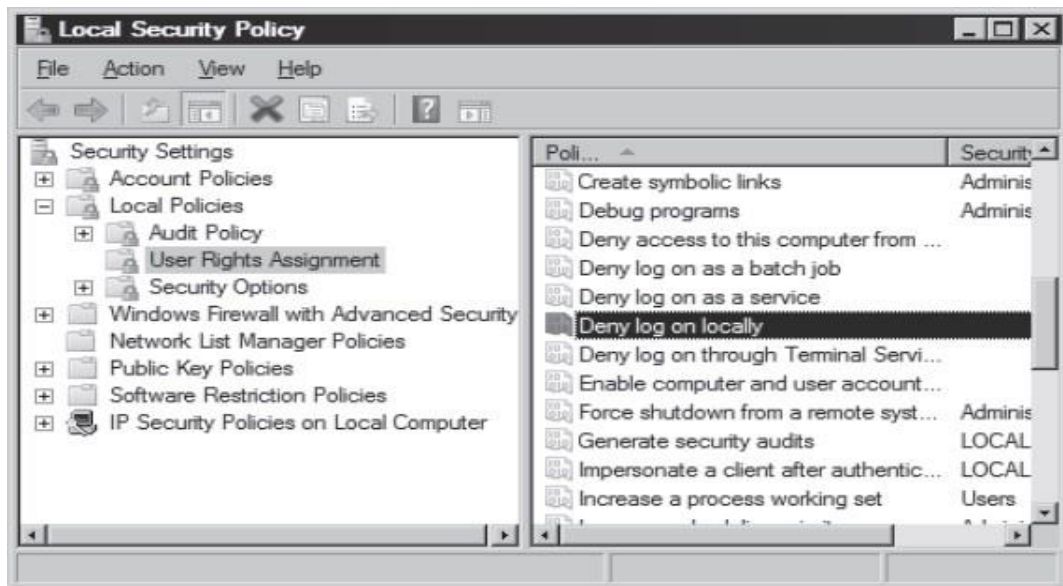
(see <http://www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=9231>).

Getadmin was the first serious privilege escalation attack against Windows NT4, and although that specific attack has been patched (post NT4 SP3), the basic technique by which it works, DLL injection, lives on and is still used effectively today. The power of getadmin was muted somewhat by the fact that it must be run by an interactive user on the target system, as must most privilege-escalation attacks. Because most users cannot log on interactively to a Windows server by default, it is really only useful to rogue members of the various built-in

Operators groups (Account, Backup, Server, and so on) and the default Internet server account, IUSR_machinename, who have this privilege. If malicious individuals have the interactive logon privilege on your server already, privilege escalation exploits aren't going to make things much worse. They already have access to just about anything else they'd want.

Preventing Privilege Escalation

First of all, maintain appropriate patch levels for your Windows systems. Exploits like getadmin take advantage of flaws in the core OS and won't be completely mitigated until those flaws are fixed at the code level. Of course, interactive logon privileges should be severely restricted for any system that houses sensitive data, because exploits such as these become much easier once this critical foothold is gained. To check interactive logon rights under Windows 2000 and later, run the Security Policy applet (either Local or Group), find the Local Policies\User Rights Assignment node, and check how the Log On Locally right is populated. New in Windows 2000 and later, many such privileges now have counterparts that allow specific groups or users to be excluded from rights. In this example, you could use the Deny Logon Locally right, as shown here:



Extracting and Cracking Passwords

Once Administrator-equivalent status has been obtained, attackers typically shift their attention to grabbing as much information as possible that can be leveraged for further system conquests. Furthermore, attackers with Administrator-equivalent credentials may have

happened upon only a minor player in the overall structure of your network and may wish to install additional tools to spread their influence. Thus, one of the first post-exploit activities of attackers is to gather more usernames and passwords, since these credentials are typically the key to extending exploitation of the entire environment, and possibly even other environments linked through assorted relationships.

2- Linux Hacking

Linux is an open source operating system for computers. Linux is a Unix-like operating system, meaning that it supports multitasking and multi-user operation. Linux is widely used for supercomputers, mainframe computers, and servers. Linux can also run on personal computers, mobile devices, tablet computers, routers, and other embedded systems. One of the most prominent examples of this is the Android mobile operating system, which is based on the Linux Kernel. Linux is capable of running many of the same applications and software as Windows and Mac OS X. Linux operating systems, software, and applications are commonly referred to as Linux distributions (distros for short).

Linux is an extremely popular operating system for hackers. There are two main reasons behind this. First off, Linux's source code is freely available because it is an open source operating system. This means that Linux is very easy to modify or customize. Second, there are countless Linux security distros available that can double as Linux hacking software.

Generally speaking, there are two types of Linux hacking: hacking done by hobbyists and hacking done by malicious actors. Hobbyists are often hackers looking for new solutions to software problems or tinkerers looking for new uses for their software/hardware. Malicious actors use Linux hacking tools to exploit vulnerabilities in Linux applications, software, and networks. This type of Linux hacking is done in order to gain unauthorized access to systems and steal data.

Linux Hacking Tools and Services

Malicious actors typically use tools such as password crackers, network and vulnerability scanners, and intrusion detection software. These Linux hacking tools all serve different purposes and are used for a wide range of attacks.

Password crackers are software developed for decoding passwords in a variety of formats, such as encrypted or hashed passwords. Many cracking distros offer additional functionality such as network detectors and wireless packet sniffing. Malicious actors use these Linux hacking tools because they offer a simple way to gain access to an organization's network, databases, directories, and more. Password cracking distros are commonly used in Linux wifi hacking (Linux hacking that targets wireless networks).

Linux network scanners are used to detect other devices on a network. In doing so, attackers are able to develop a virtual map of the network. In addition to discovering other devices, many network scanners are capable of gathering details about devices such as which operating systems, software, and firewalls are being used. Network scanners are used to discover network security holes in Linux wifi hacking. They also can be used to gather information useful for Linux distro hacking (Linux hacking that targets software, applications, operating systems, etc).

Linux vulnerability scanning software is used to detect vulnerabilities in systems and applications. Malicious parties often use vulnerability scanners as Linux hacking software in order to detect exploitable vulnerabilities, gather simple passwords, discover configuration issues, and perform denial of service attacks. Vulnerability scanners are frequently used for Linux distro hacking because of these capabilities.

Hacking Code

Before seeking out buffer overflows in code, let's take a look at what they are in the first place. As the name implies, buffer overflow vulnerabilities deal with buffers, or memory allocations in languages that offer direct, low-level access to read and write memory.

In the case of languages such as C and Assembly, reading from or writing to one of these allocations does not entail any automatic bounds checking. In other words, there is no check that the number of bytes to be written or read will actually fit in the buffer in question. Thus, the program can "overflow" the capacity of the buffer. This results in data being written past its end and overwriting the contents of subsequent addresses on the stack or heap, or extra data being read. In fact, the latter is exactly what happened in the case of the Heartbleed bug.

Detecting buffer overflow

With this definition in mind, we can explore how to detect these flaws. When working with source code, the short answer to buffer overflows is just to pay special attention to where buffers are used, modified, and accessed. Of particular note would be functions dealing with input supplied by a user or other outside source, as these would provide the easiest vector for exploitation of the overflow. For example, when asking a user a yes or no question, it seems feasible to store the user's string input in a small buffer—only large enough for the string “yes” as the following example shows:

```
void askQuestion() {
    char user_answer[4];
    printf("Is this code secure? Please answer yes or no:");
    gets(user_answer);
}
```

Looking at the code, it is clear that no bounds checking is performed. If the user enters “maybe” then the program will likely crash rather than asking the user for a valid answer and re-prompting with the question. The user's answer is simply written into the buffer, regardless of its length.

In this example, since `user_answer` is the only variable declared, the next values on the stack would be the return address value, or the location in memory to which the program will return after running the `askQuestion` function. This means that if the user enters four bytes of data (enough to fill the memory specifically set aside for the buffer), followed by a valid address in memory, the program's return address will be modified. This allows the user to force the program to exit the function at a different point in the code than originally intended, potentially causing the program to behave in dangerous and unintended ways.

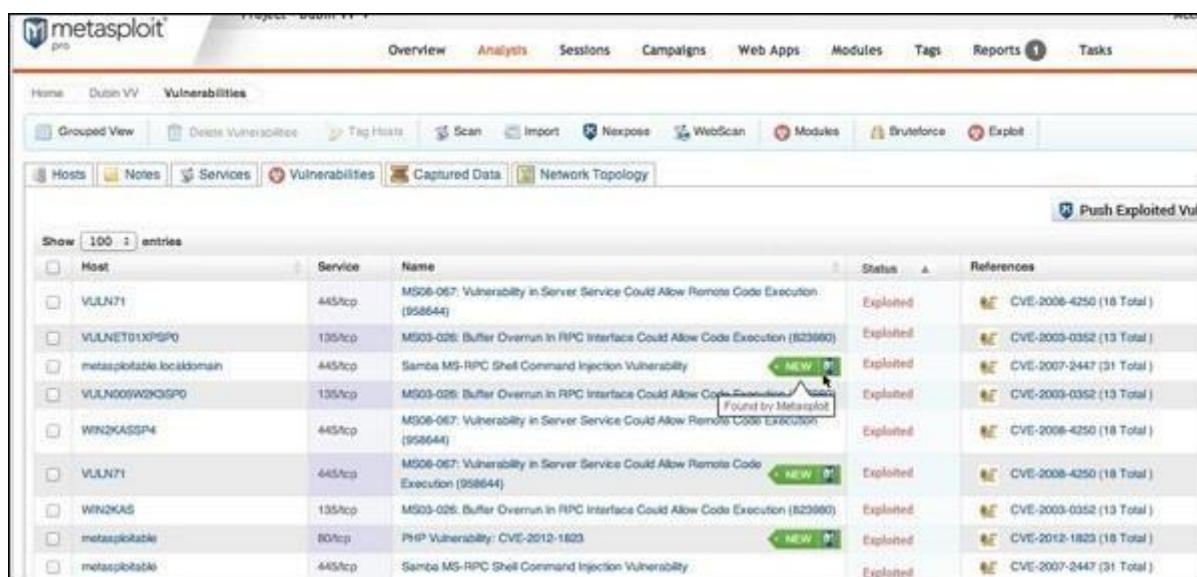
If the first step to detect buffer overflows in source code is understanding how they work, and the second step is knowing to look for external input and buffer manipulations, then the third step is to know what functions are susceptible to this vulnerability and can act as red flags for its presence. As illustrated above, the `gets` function is perfectly happy writing past the

bounds of the buffer provided to it. In fact, this quality extends to the whole family of related functions (including strcpy, strcat, and printf/sprintf). Anywhere one of these functions is used, there is likely to be a buffer overflow vulnerability.

Exploitation

Exploitation is a piece of programmed software or script which can allow hackers to take control over a system, exploiting its vulnerabilities. Hackers normally use vulnerability scanners like Nessus, Nexpose, OpenVAS, etc. to find these vulnerabilities.

Metasploit is a powerful tool to locate vulnerabilities in a system.



The screenshot shows the Metasploit web interface with a table of vulnerabilities. The table has columns for Host, Service, Name, Status, and References. Several vulnerabilities are listed, including MS08-067, MS03-026, and CVE-2012-1823. Some entries have a 'NEW' badge and a 'Found by Metasploit' tooltip.

Host	Service	Name	Status	References
VULN71	445/tcp	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	Exploited	CVE-2008-4250 (18 Total)
VULNET01XPSP0	135/tcp	MS03-026: Buffer Overrun in RPC Interface Could Allow Code Execution (823980)	Exploited	CVE-2003-0352 (13 Total)
metasploitable.localdomain	445/tcp	Samba MS-RPC Shell Command Injection Vulnerability	Exploited	CVE-2007-2447 (31 Total)
VULN009W2K0SP0	135/tcp	MS03-026: Buffer Overrun in RPC Interface Could Allow Code Execution (823980)	Exploited	CVE-2003-0352 (13 Total)
WIN2KAS2P4	445/tcp	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	Exploited	CVE-2008-4250 (18 Total)
VULN71	445/tcp	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	Exploited	CVE-2008-4250 (18 Total)
WIN2KAS	135/tcp	MS03-026: Buffer Overrun in RPC Interface Could Allow Code Execution (823980)	Exploited	CVE-2003-0352 (13 Total)
metasploitable	80/tcp	PHP Vulnerability: CVE-2012-1823	Exploited	CVE-2012-1823 (18 Total)
metasploitable	445/tcp	Samba MS-RPC Shell Command Injection Vulnerability	Exploited	CVE-2007-2447 (31 Total)

Based on the vulnerabilities, we find exploits. Here, we will discuss some of the best vulnerability search engines that you can use.

- **Exploit Database**

www.exploit-db.com is the place where you can find all the exploits related to a vulnerability.

The screenshot shows the Exploit-DB website with a navigation bar containing 'Home', 'Exploits', 'Shellcode', 'Papers', 'Google Hacking Database', 'Submit', and 'Search'. The main heading is 'Remote Exploits'. Below the heading is a table listing various exploits with columns for 'Date Added', 'D', 'A', 'V', 'Title', 'Platform', and 'Author'.

Date Added	D	A	V	Title	Platform	Author
2016-08-23	🟢	-	✔️	Phoenix Exploit Kit - Remote Code Execution (Metasploit)	PHP	Metasploit
2016-02-26	🟢	-	🟢	Microsoft Windows - SRV2.SYS SMB Code Execution Exploit (Python) (MS09-050)	Windows	ohnozzy
2016-02-26	🟢	-	🟢	Microsoft Windows - NetAPI32.dll Code Execution Exploit (Python) (MS08-067)	Windows	ohnozzy
2016-08-19	🟢	-	🟢	TOPSEC Firewalls - Remote Exploit (ELIGIBLEBACHELOR)	Hardware	Shadow Brokers
2016-08-18	🟢	-	🟢	Cisco ASA 8.x - Authentication Bypass (EXTRABACON)	Hardware	Shadow Brokers
2016-08-14	🟢	-	🟢	Samsung Smart Home Camera SNH-P-6410 - Command Injection	Hardware	PentestPartner.
2016-08-12	🟢	-	🟢	FreePBX 13 / 14 - Remote Command Execution With Privilege Escalation	Linux	pgt

- **Common Vulnerabilities and Exposures**

Common Vulnerabilities and Exposures (CVE) is the standard for information security vulnerability names. CVE is a dictionary of publicly known information security vulnerabilities and exposures. It's free for public use. <https://cve.mitre.org>.

The screenshot shows the 'CVE List Main Page' on the MITRE website. The page features a navigation bar with 'CVE LIST', 'COMPATIBILITY', 'NEWS - AUGUST 29, 2016', and 'SEARCH'. The main content area includes a 'National Vulnerability Database' section with a list of links: 'Data feeds of NVD's CVE content', 'Scoring for CVE-IDs', 'Fix information for CVE-IDs', 'Statistics for NVD's CVE content', and 'Advanced searching of NVD's CVE content'. There is also a 'CVE List Master Copy' section with links for 'Download CVE List', 'Search keywords or look-up CVE-IDs', and 'View entire CVE List (html)'. A sidebar on the right contains a 'CVE List' menu with options like 'Search Master Copy of CVE', 'Download CVE', and 'Request a CVE Identifier'.

- **National Vulnerability Database**

National Vulnerability Database (NVD) is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance. You can locate this database at – <https://nvd.nist.gov>

NVD includes databases of security checklists, security-related software flaws, misconfigurations, product names, and impact metrics.



In general, you will see that there are two types of exploits –

1. **Remote Exploits** – These are the type of exploits where you don't have access to a remote system or network. Hackers use remote exploits to gain access to systems that are located at remote places.
2. **Local Exploits** – Local exploits are generally used by a system user having access to a local system, but who wants to overpass his rights.

Quick Fix

updates, so it is recommended that you update your system on a regular basis, for example, once a week.

In Windows environment, you can activate automatic updates by using the options available in the Control Panel → System and Security → Windows Updates.

In Linux Centos, you can use the following command to install automatic update package.

```
yum -y install yum-cron
```

- **Metasploit**

is one of the most powerful exploit tools. Most of its resources can be found at: <https://www.metasploit.com>. It comes in two versions – **commercial** and **free edition**. There are no major differences in the two versions, so in this tutorial, we will be mostly using the Community version (free) of Metasploit.

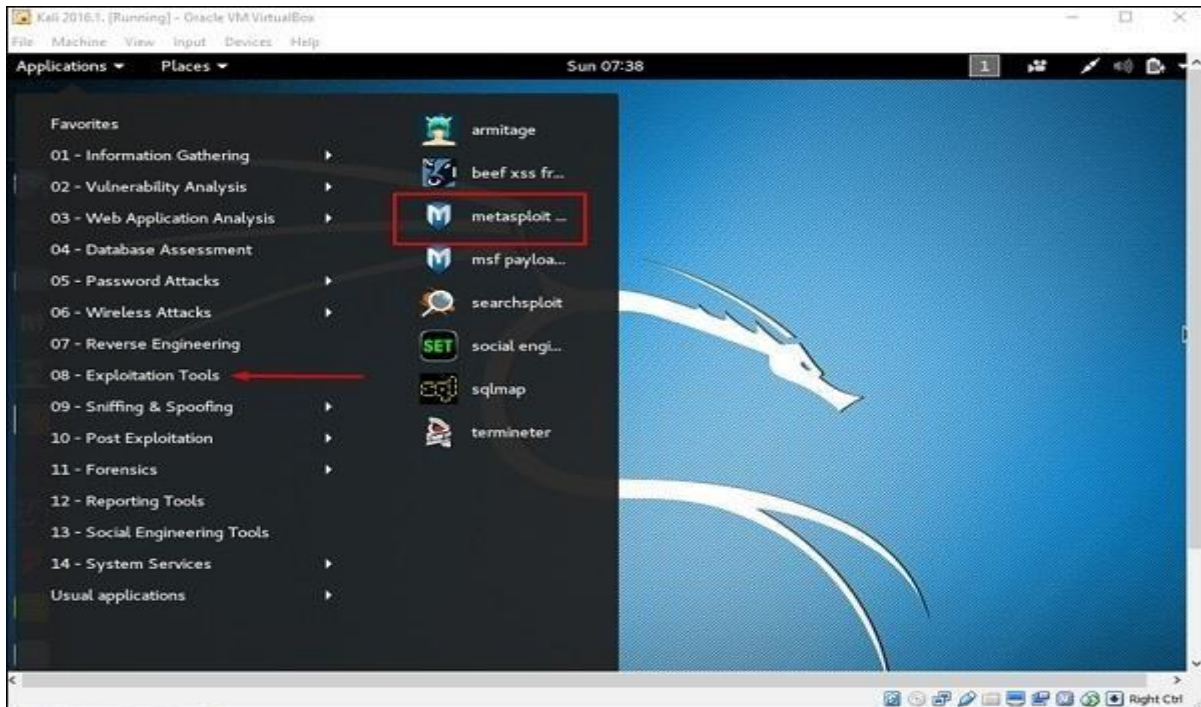
As an Ethical Hacker, you will be using “Kali Distribution” which has the Metasploit community version embedded in it along with other ethical hacking tools. But if you want to

install Metasploit as a separate tool, you can easily do so on systems that run on Linux, Windows, or Mac OS X.

The hardware requirements to install Metasploit are –

- 2 GHz+ processor
- 1 GB RAM available
- 1 GB+ available disk space

Metasploit can be used either with command prompt or with Web UI. To open in Kali, go to Applications → Exploitation Tools → metasploit.



After Metasploit starts, you will see the following screen. Highlighted in red underline is the version of Metasploit.

Email Spoofing

In email spoofing, the spammer sends emails from a known domain, so the receiver thinks that he knows this person and opens the mail. Such mails normally contain suspicious links, doubtful content, requests to transfer money, etc.

```
Delivered-To: a1 n@l./e/ .com
Received: by 10.50.1.2 with SMTP id Zcsp76020igi;
    Wed, 21 May 2014 05:34:27 -0700 (PDT)
X-Received: by 10.140.18.180 with SMTP id 49mr3109738qgf.105.1400675667586;
    Wed, 21 May 2014 05:34:27 -0700 (PDT)
Return-Path: <whitson@lifehacker.com>
Received: from iad1-shared-relay1.dreamhost.com (iad1-shr ad-relay1.dre m1.st.com.
    [208.113.157.50])
    by mx.google.com with ESMTP id c38si1162387qge.80.2014.05.21.05.34.27
    for <example@example.com>
    Wed, 21 May 2014 05:34:27 -0700 (PDT)
Received-SPF: softfail (google.com: domain of transitioning whitson@lifehacker.com
    does not designate 208.113.157.50 as permitted sender) client-ip=208.113.157.50;
```

3- Wireless Hacking

A wireless network is a set of two or more devices connected with each other via radio waves within a limited space range. The devices in a wireless network have the freedom to be in motion, but be in connection with the network and share data with other devices in the network. One of the most crucial point that they are so spread is that their installation cost is very cheap and fast than the wire networks.

Wireless networks are widely used and it is quite easy to set them up. They use IEEE 802.11 standards. A **wireless router** is the most important device in a wireless network that connects the users with the Internet. In a wireless network, we have **Access Points** which are extensions of wireless ranges that behave as logical switches.

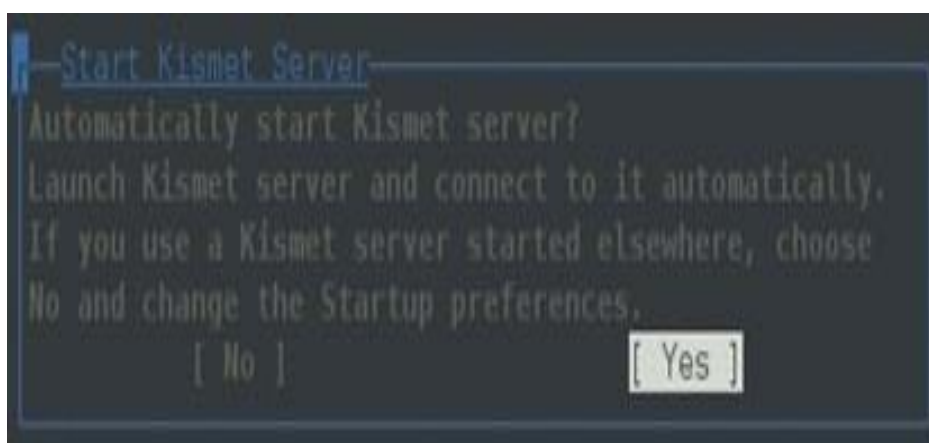


Although wireless networks offer great flexibility, they have their security problems. A hacker can sniff the network packets without having to be in the same building where the network is located. As wireless networks communicate through radio waves, a hacker can easily sniff the network from a nearby location. Most attackers use network sniffing to find the SSID and hack a wireless network. When our wireless cards are converted in sniffing modes, they are called **monitor mode**.

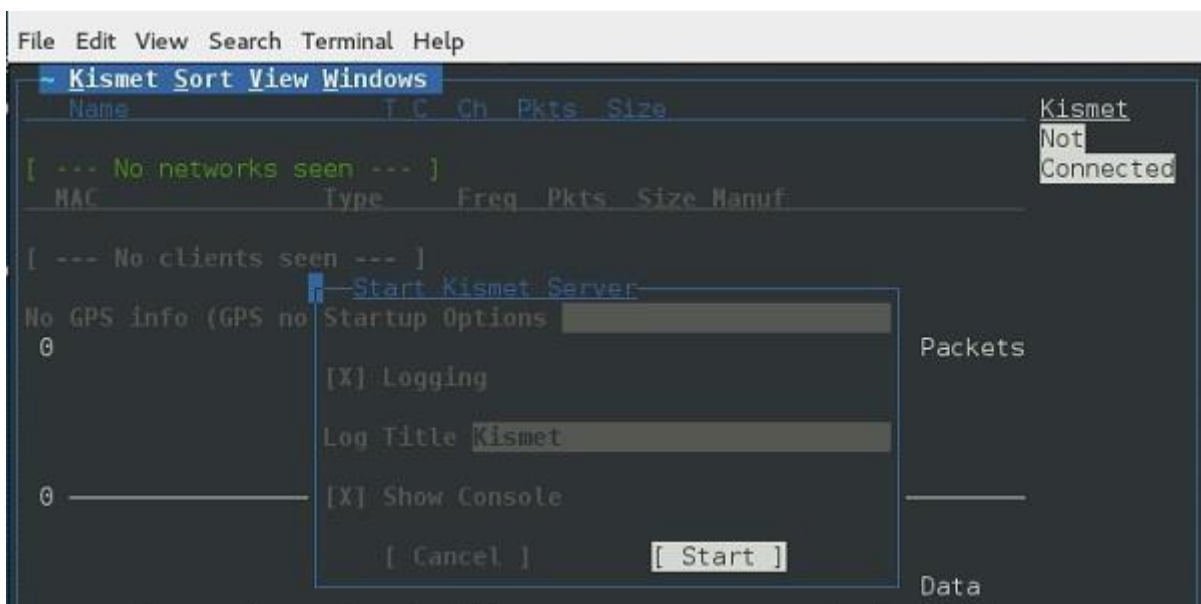
Kismet

Kismet is a powerful tool for wireless sniffing that is found in Kali distribution. It can also be downloaded from its official webpage – <https://www.kismetwireless.net/index.shtml>

Let's see how it works. First of all, open a terminal and type **kismet**. Start the Kismet Server and click Yes, as shown in the following screenshot.



As shown here, click the Start button.



Now, Kismet will start to capture data.

4- Web Server Hacking

A web server is a program that stores files (usually web pages) and makes them accessible via the network or the internet. A web server requires both hardware and software. Attackers usually target the exploits in the software to gain authorized entry to the server. Let's look at some of the common vulnerabilities that attackers take advantage of.

- **Default settings**– These settings such as default user id and passwords can be easily guessed by the attackers. Default settings might also allow performing certain tasks such as running commands on the server which can be exploited.

- **Misconfiguration** of operating systems and networks – certain configuration such as allowing users to execute commands on the server can be dangerous if the user does not have a good password.
- **Bugs in the operating system and web servers**– discovered bugs in the operating system or web server software can also be exploited to gain unauthorized access to the system.

Types of Web Servers

The following is a list of the common web servers

- **Apache**– This is the commonly used web server on the internet. It is cross platform but is it's usually installed on Linux. Most [PHP](#) websites are hosted on [Apache](#) servers.
- **Internet Information Services (IIS)**– It is developed by Microsoft. It runs on Windows and is the second most used web server on the internet. Most asp and aspx websites are hosted on IIS servers.
- **Apache Tomcat** – Most Java server pages (JSP) websites are hosted on this type of web server.
- **Other web servers** – These include Novell's Web Server and IBM's Lotus Domino servers.

Types of Attacks against Web Servers

- **Directory traversal attacks**– This type of attacks exploits bugs in the web server to gain unauthorized access to files and folders that are not in the public domain. Once the attacker has gained access, they can download sensitive information, execute commands on the server or install malicious software.
- **Denial of Service Attacks**– With this type of attack, the web server may crash or become unavailable to the legitimate users.
- **Domain Name System Hijacking** – With this type of attacker, the DNS setting are changed to point to the attacker's web server. All traffic that was supposed to be sent to the web server is redirected to the wrong one.

- **Sniffing**– Unencrypted data sent over the network may be intercepted and used to gain unauthorized access to the web server.
- **Phishing**– With this type of attack, the attack impersonates the websites and directs traffic to the fake website. Unsuspecting users may be tricked into submitting sensitive data such as login details, credit card numbers, etc.

Web server attack tools

Some of the common web server attack tools include;

- **Metasploit**– this is an open source tool for developing, testing and using exploit code. It can be used to discover vulnerabilities in web servers and write exploits that can be used to compromise the server.
- **MPack**– this is a web exploitation tool. It was written in PHP and is backed by MySQL as the database engine. Once a web server has been compromised using MPack, all traffic to it is redirected to malicious download websites.
- **Zeus**– this tool can be used to turn a compromised computer into a bot or zombie. A bot is a compromised computer which is used to perform internet-based attacks. A botnet is a collection of compromised computers. The botnet can then be used in a denial of service attack or sending spam mails.
- **Neosplit** – this tool can be used to install programs, delete programs, replicating it, etc.

How to avoid attacks on Web server?

An organization can adopt the following policy to protect itself against web server attacks.

- Patch management– this involves installing patches to help secure the server. A patch is an update that fixes a bug in the software. The patches can be applied to the operating system and the web server system.
- Secure installation and configuration of the operating system
- Secure installation and configuration of the web server software

- Vulnerability scanning system– these include tools such as Snort, NMap, Scanner Access Now Easy (SANE)
- Firewalls can be used to stop simple DoS attacks by blocking all traffic coming the identify source IP addresses of the attacker.
- Antivirus software can be used to remove malicious software on the server
- Disabling Remote Administration
- Default accounts and unused accounts must be removed from the system
- Default ports & settings (like FTP at port 21) should be changed to custom port & settings (FTP port at 5069)

Social Engineering

Social engineering can be broken into two common types:

- A. Human-Based:** - Human-based social engineering refers to person-to-person interaction to retrieve the desired information. An example is calling the help desk and trying to find out a password.
- B. Computer-Based:-** Computer-based social engineering refers to having computer software that attempts to retrieve the desired information. An example is sending a user an email and asking them to reenter a password in a web page to confirm it. This social-engineering attack is also known as *phishing*.

A. Human-Based Social Engineering

Human-based social engineering techniques can be broadly categorized as follows:

1. **Impersonating an Employee or Valid User** In this type of social-engineering attack, the hacker pretends to be an employee or valid user on the system. A hacker can gain physical access by pretending to be a janitor, employee, or contractor. Once inside the facility, the hacker gathers information from trashcans, desktops, or computer systems.
2. **Posing as an Important User** In this type of attack, the hacker pretends to be an important user such as an executive or high-level manager who needs immediate assistance to gain access to a computer system or files. The hacker uses intimidation so that a lower-level employee such as a help desk worker will assist them in gaining access

to the system. Most low-level employees won't question someone who appears to be in a position of authority.

3. **Using a Third Person** Using the third-person approach, a hacker pretends to have permission from an authorized source to use a system. This attack is especially effective if the supposed authorized source is on vacation or can't be contacted for verification.
4. **Calling Technical Support** Calling tech support for assistance is a classic social-engineering technique. Help desk and technical support personnel are trained to help users, which makes them good prey for social-engineering attacks.
5. **Shoulder Surfing** Shoulder surfing is a technique of gathering passwords by watching over a person's shoulder while they log in to the system. A hacker can watch a valid user log in and then use that password to gain access to the system.
6. **Dumpster Diving** Dumpster diving involves looking in the trash for information written on pieces of paper or computer printouts. The hacker can often find passwords, filenames, or other pieces of confidential information.

B. Computer-Based Social Engineering

Computer-based social-engineering attacks can include the following:

1. Email attachments
2. Fake websites
3. Pop-up windows

Insider Attacks

If a hacker can't find any other way to hack an organization, the next best option is to infiltrate the organization by getting hired as an employee or finding a disgruntled employee to assist in the attack. Insider attacks can be powerful because employees have physical access and are able to move freely about the organization.

Identity Theft

A hacker can pose as an employee or steal the employee's identity to perpetrate an attack. Information gathered in dumpster diving or shoulder surfing in combination with creating fake ID badges can gain the hacker entry into an organization. Creating a persona that can enter the building unchallenged is the goal of identity theft.

Phishing Attacks

Phishing involves sending an email, usually posing as a bank, credit card company, or other financial organization. The email requests that the recipient confirm banking information or reset passwords or PINs. The user clicks the link in the email and is redirected to a fake website. The hacker is then able to capture this information and use it for financial gain or to perpetrate other attacks. Emails that claim the senders have a great amount of money but need your help getting it out of the country are examples of phishing attacks. These attacks prey on the common person and are aimed at getting them to provide bank account access codes or other confidential information to the hacker.

References:

- 1- Certified Ethical Hacker, Study Guide book, Kimberly Graves, 2010
- 2- Certified Ethical Hacker, (CEH) Cert Guide book, Michael Gregg, 2014