Catalog

4.1. Introduction to Ethical Hacking

Ethical hackers are usually security professionals or network penetration testers who use their hacking skills and toolsets for defensive and protective purposes. Ethical hackers who are security professionals test their network and systems security for vulnerabilities using the same tools that a hacker might use to compromise the network. Any computer professional can learn the skills of ethical hacking.

The term cracker describes a hacker who uses their hacking skills and toolset for destructive or offensive purposes such as disseminating viruses or performing denial-ofservice (DoS) attacks to compromise or bring down systems and networks. No longer just looking for fun, these hackers are sometimes paid to damage corporate reputations or steal or reveal credit card information, while slowing business processes and compromising the integrity of the organization.

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. This is the traditional definition of a hacker and what most people consider a hacker to be.

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.

Ethical hackers are motivated by different reasons, but their purpose is usually the same as that of crackers: they're trying to determine what an intruder can see on a targeted network or system, and what the hacker can do with that information. This process of testing the security of a system or network is known as a penetration test, or pen test.

Hackers break into computer systems. Contrary to widespread myth, doing this doesn't usually involve a mysterious leap of hackerly brilliance, but rather persistence and the dogged repetition of a handful of fairly well-known tricks that exploit common weaknesses in the security of target systems. A pen test is no more than just performing those same steps with the same tools used by a malicious hacker to see what data could be exposed using hacking tools and techniques.

Many ethical hackers detect malicious hacker activity as part of the security team of an organization tasked with defending against malicious hacking activity. When hired, an ethical hacker asks the organization what is to be protected, from whom, and what resources the company is willing to expend in order to gain protection. A penetration test plan can then be built around the data that needs to be protected and potential risks.

Documenting the results of various tests is critical in producing the end product of the pen test: the pen test report. Taking screenshots of potentially valuable information or saving log files is critical to presenting the findings to a client in a pen test report. The pen test report is a compilation of all the potential risks in a computer or system.

Ethical Hacking Terminology

Threat - An environment or situation that could lead to a potential breach of security.

Ethical hackers look for and prioritize threats when performing a security analysis. Malicious hackers and their use of software and hacking techniques are themselves threats to an organization's information security.

Exploit - A piece of software or technology that takes advantage of a bug, glitch, or vulnerability, leading to unauthorized access, privilege escalation, or denial of service on a computer system. Malicious hackers are looking for exploits in computer systems to open the door to an initial attack. Most exploits are small strings of computer code that, when executed on a system, expose vulnerability. Experienced hackers create their own exploits, but it is not necessary to have any programming skills to be an ethical hacker as many hacking software programs have ready-made exploits that can be launched against a computer system or network. An exploit is a defined way to breach the security of an IT system through a vulnerability.

Vulnerability - The existence of a software flaw, logic design, or implementation error that can lead to an unexpected and undesirable event executing bad or damaging instructions to the system. Exploit code is written to target a vulnerability and cause a fault in the system in order to retrieve valuable data.

Target of Evaluation (TOE) - A system, program, or network that is the subject of a security analysis or attack. Ethical hackers are usually concerned with high-value TOEs, systems that contain sensitive information such as account numbers, passwords, Social Security numbers, or other confidential data. It is the goal of the ethical hacker to test hacking tools against the high-value TOEs to determine the vulnerabilities and patch them to protect against exploits and exposure of sensitive data.

Attack - An attack occurs when a system is compromised based on a vulnerability. Many attacks are perpetuated via an exploit. Ethical hackers use tools to find systems that may be vulnerable to an exploit because of the operating system, network configuration, or applications installed on the systems, and to prevent an attack.

There are two primary methods of delivering exploits to computer systems:

Remote The exploit is sent over a network and exploits security vulnerabilities without any prior access to the vulnerable system. Hacking attacks against corporate computer systems or networks initiated from the outside world are considered remote. Most people think of this type of attack when they hear the term hacker, but in reality most attacks are in the next category.

Local The exploit is delivered directly to the computer system or network, which requires prior access to the vulnerable system to increase privileges. Information security policies should be created in such a way that only those who need access to information should be allowed access and they should have the lowest level of access to perform their job function. These concepts are commonly referred as “need to know” and “least privilege” and, when used properly, would prevent local exploits. Most hacking attempts occur from within an organization and are perpetuated by employees, contractors, or others in a trusted position. In order for an insider to launch an attack, they must have higher privileges than necessary based on the concept of “need to know.” This can be accomplished by privilege escalation or weak security safeguards.

The Phases of Ethical Hacking

The process of ethical hacking can be broken down into five distinct phases. Later in this book, hacking software programs and tools will be categorized into each of these steps.

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 illustrates the five phases that hackers generally follow in hacking a computer system.

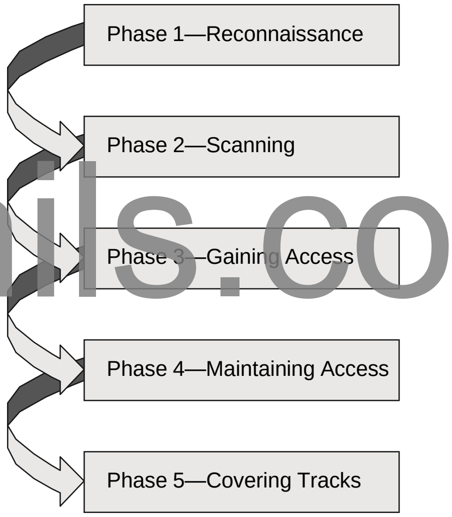


Fig : Phases of hacking

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

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

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

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

Phase 2: Scanning

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

- ✓ Dialers

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

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

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

Phase 3: Gaining Access

Phase 3 is when the real hacking takes place. Vulnerabilities exposed during the reconnaissance and scanning phase are now exploited to gain access to the target system. The hacking attack can be delivered to the target system via a local area network (LAN), either wired or wireless; local access to a PC; the Internet; or offline. Examples include stackbased buffer overflows, denial of service, and session hijacking. These topics will be discussed in later chapters. 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

Identifying Types of Hacking Technologies

Many methods and tools exist for locating vulnerabilities, running exploits, and compromising systems. Once vulnerabilities are found in a system, a hacker can exploit that vulnerability and install malicious software. Trojans, backdoors, and rootkits are all forms of malicious software, or malware. Malware is installed on a hacked system after a vulnerability has been exploited.

Buffer overflows and SQL injection are two other methods used to gain access into computer systems. Buffer overflows and SQL injection are used primarily against application servers that contain databases of information.

Most hacking tools exploit weaknesses in one of the following four areas:

Operating Systems : Many system administrators install operating systems with the default settings, resulting in potential vulnerabilities that remain unpatched.

Applications: Applications usually aren't thoroughly tested for vulnerabilities when developers are writing the code, which can leave many programming flaws that a hacker can exploit. Most application development is “feature-driven,” meaning programmers are under a deadline to turn out the most robust application in the shortest amount of time.

Shrink-Wrap Code : Many off-the-shelf programs come with extra features the common user isn’t aware of, and these features can be used to exploit the system. The macros in Microsoft Word, for example, can allow a hacker to execute programs from within the application.

Misconfigurations : Systems can also be misconfigured or left at the lowest common security settings to increase ease of use for the user; this may result in vulnerability and an attack.

Identifying Types of Ethical Hacks

Ethical hackers use many different methods to breach an organization’s security during a simulated attack or penetration test. Most ethical hackers have a specialty in one or a few of the following attack methods. In the initial discussion with the client, one of the questions that should be asked is whether there are any specific areas of concern, such as wireless networks or social engineering. This enables the ethical hacker to customize the test to be performed to the needs of the client. Otherwise, security audits should include attempts to access data from all of the following methods.

Here are the most common entry points for an attack:

Remote Network - A remote network hack attempts to simulate an intruder launching an attack over the Internet. The ethical hacker tries to break or find vulnerability in the outside defenses of the network, such as firewall, proxy, or router vulnerabilities. The Internet is thought to be the most common hacking vehicle, while in reality most organizations have strengthened their security defenses sufficient to prevent hacking from the public network.

Remote Dial-Up Network - A remote dial-up network hack tries to simulate an intruder launching an attack against the client’s modem pools. War dialing is the process of repetitive dialing to find an open system and is an example of such an attack. Many organizations have replaced dial-in connections with dedicated Internet connections so this method is less relevant than it once was in the past.

Local Network - A local area network (LAN) hack simulates someone with physical access gaining additional unauthorized access using the local network. The ethical hacker must gain direct access to the local network in order to launch this type of attack. Wireless LANs (WLANs) fall in this category and have added an entirely new avenue of attack as radio waves travel through building structures. Because the WLAN signal can be identified and captured outside the building, hackers no longer have to gain physical access to the building and network to perform an attack on the LAN. Additionally, the huge growth of WLANs has made this an increasing source of attack and potential risk to many organizations.

Stolen Equipment - A stolen-equipment hack simulates theft of a critical information resource such as a laptop owned by an employee. Information such as usernames, passwords, security settings, and encryption types can be gained by stealing a laptop. This is usually a commonly overlooked area by many organizations. Once a hacker has access to a laptop authorized in the security domain, a lot of information, such as security configuration, can be gathered. Many times laptops disappear and are not reported quickly enough to allow the security administrator to lock that device out of the network.

Social Engineering - A social-engineering attack checks the security and integrity of the organization’s employees by using the telephone or face-to-face communication to gather information for use in an attack. Social-engineering attacks can be used to acquire usernames, passwords, or other organizational security measures. Social-engineering scenarios usually consist of a hacker calling the help desk and talking the help desk employee into giving out confidential security information.

Physical Entry - A physical-entry attack attempts to compromise the organization’s physical premises. An ethical hacker who gains physical access can plant viruses, Trojans, rootkits, or hardware key loggers (physical device used to record keystrokes) directly on systems in the target network. Additionally, confidential documents that are not stored in a secure location can be gathered by the hacker. Lastly, physical access to the building would allow a hacker to plant a rogue device such as a wireless access point on the network. These devices could then be used by the hacker to access the LAN from a remote location.

4.2. Foot printing and Reconnaissance

Footprinting

Footprinting is defined as the process of creating a blueprint or map of an organization's network and systems. Information gathering is also known as ***footprinting*** an organization. Footprinting 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 footprinting 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 footprinting:

- 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

Once this information is compiled, it can give a hacker better insight into the organization, where valuable information is stored, and how it can be accessed.

Footprinting Tools

Footprinting can be done using hacking tools, either applications or websites, which allow the hacker to locate information passively. By using these footprinting tools, a hacker can gain some basic information on, or "footprint," the target. By first footprinting 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. Footprinting 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.

For the exercises in this chapter, you will perform reconnaissance and information gathering on a target company. I recommend you use your own organization, but because these tools are passive, any organization name can be used.

Some of the common tools used for footprinting and information gathering are as follows:

Domain name lookup

- ✓ Whois
- ✓ NSlookup
- ✓ Sam Spade

Before we discuss these tools, keep in mind that open source information can also yield a wealth of information about a target, such as phone numbers and addresses. Performing Whois requests, searching domain name system (DNS) tables, and using other lookup web tools are forms of open source footprinting. Most of this information is fairly easy to get and legal to obtain.

Footprinting a Target

Footprinting is part of the preparatory preattack phase and involves accumulating data regarding a target's environment and architecture, usually for the purpose of finding ways to intrude into that environment. Footprinting can reveal system vulnerabilities and identify the ease with which they can be exploited. This is the easiest way for hackers to gather information about computer systems and the companies they belong to. The purpose of this preparatory phase is to learn as much as you can about a system, its remote access capabilities, its ports and services, and any specific aspects of its security.

Reconnaissance

The term *reconnaissance* comes from the military and means to actively seek an enemy's intentions by collecting and gathering information about an enemy's composition and capabilities via direct observation, usually by scouts or military intelligence personnel trained in surveillance. In the world of ethical hacking, reconnaissance applies to the process of information gathering. Reconnaissance is a catchall term for watching the hacking target and gathering information about how, when, and where they do things. By identifying patterns of behavior, of people or systems, an enemy could find and exploit a loophole.

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.

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

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

Active reconnaissance involves probing the network to discover individual hosts, IP addresses, and services on the network. This process involves more risk of detection than passive reconnaissance and is sometimes called rattling the doorknobs. Active reconnaissance can give a hacker an indication of security measures in place, 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.

4.3. Scanning Networks

Scanning

Scanning is the first phase of active hacking and is used to locate target systems or networks for later attack. 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.

Types of scanning:

Three types of scanning are ,

S.No	Scanning type	Purpose
1	Port scanning	Determines open ports and services
2	Network scanning	Identifies IP addresses on a given network or subnet
3	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.

Common port Numbers

On Windows systems, well-known port numbers are located in the C:\windows\system32\drivers\etc\services file. Services is a hidden file. To view it, show hidden files in Windows Explorer, and double-click the filename to open it with Notepad. The CEH exam expects you to know the well-known port numbers for common applications; familiarize yourself with the port numbers for the following applications:

- ✓ FTP, 21
- ✓ Telnet, 23
- ✓ HTTP, 80
- ✓ SMTP, 25
- ✓ POP3, 110
- ✓ HTTPS, 443

The following list contains additional port numbers not necessarily on the CEH exam but useful for real-world penetration testing:

- ✓ Global Catalog Server (TCP), 3269 and 3268
- ✓ LDAP Server (TCP/UDP), 389
- ✓ LDAP SSL (TCP/UDP), 636
- ✓ IPsec ISAKMP (UDP), 500
- ✓ NAT-T (UDP), 4500
- ✓ RPC (TCP), 135
- ✓ ASP.NET Session State (TCP), 42424
- ✓ NetBIOS Datagram Service (UDP), 137 and 138
- ✓ NetBIOS Session Service (TCP), 139

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.

The CEH (Certified Ethical Hacker)Scanning Methodology

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.

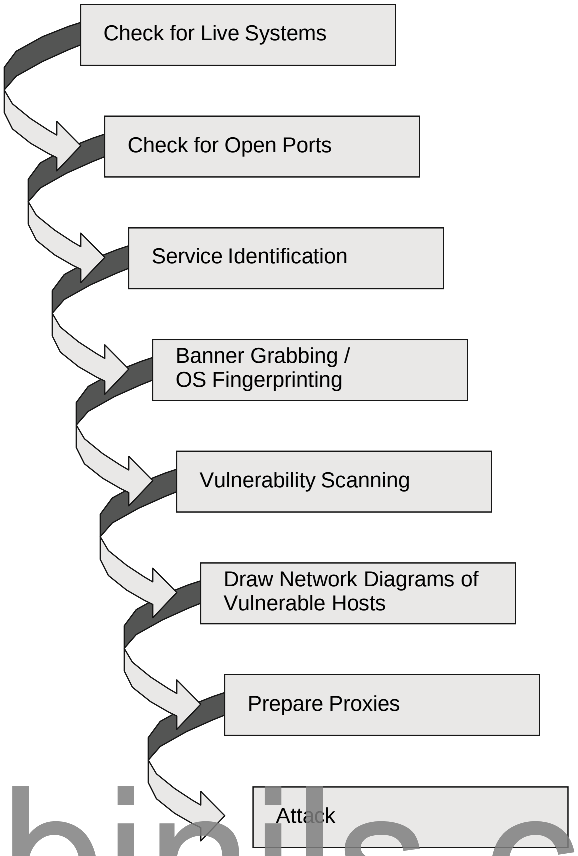


Fig:CEH scanning methodology

Ping Sweep Techniques

The CEH scanning methodology starts with checking for systems that are live on the network, meaning that they respond to probes or connection requests. The simplest, although not necessarily the most accurate, way to determine whether systems are live is to perform a *ping sweep* of the IP address range. All systems that respond with a ping reply are considered live on the network. A ping sweep is also known as Internet Control Message Protocol (ICMP) scanning, as ICMP is the protocol used by the ping command.

ICMP scanning, or a ping sweep, is the process of sending an ICMP request or ping to all hosts on the network to determine which ones are up and responding to pings. ICMP began as a protocol used to send test and error messages between hosts on the Internet. It has evolved as a protocol utilized by every operating system, router, switch or Internet Protocol (IP)-based device. The ability to use the ICMP Echo request and Echo reply as a connectivity test between hosts is built into every IP-enabled device via the ping command. It is a quick and dirty test to see if two hosts have connectivity and is used extensively for troubleshooting.

A benefit of ICMP scanning is that it can be run in *parallel*, meaning all systems are scanned at the same time; thus it can run quickly on an entire network. Most hacking tools include a ping sweep option, which essentially means performing an ICMP request to every host on the network. Systems that respond with a ping response are alive and listening on the network.

One considerable problem with this method is that personal firewall software and network-based firewalls can block a system from responding to ping sweeps. More and more systems are configured with firewall software and will block the ping attempt and notify the user that a scanning program is running on the network. Another problem is that the computer must be on to be scanned.

Scanning Ports and Identifying Services:

Port scanning is the method used to check for open ports. The process of port scanning involves probing each port on a host to determine which ports are open. Port scanning generally yields more valuable information than a ping sweep about the host and vulnerabilities on the system.

Service identification is the third step in the CEH scanning methodology; it’s usually performed using the same tools as port scanning. By identifying open ports, a hacker can usually also identify the services associated with that port number.

Port-Scan Countermeasures:

Countermeasures are processes or toolsets used by security administrators to detect and possibly thwart port scanning of hosts on their network. The following list of countermeasures should be implemented to prevent a hacker from acquiring information during a port scan:

- Proper security architecture, such as implementation of IDS and firewalls, should be followed.
- Ethical hackers use their toolset to test the scanning countermeasures that have been implemented. Once a firewall is in place, a port-scanning tool should be run against hosts on the network to determine whether the firewall correctly detects and stops the port-scanning activity.
- The firewall should be able to detect the probes sent by port-scanning tools. The firewall should carry out stateful inspections, which means it examines the data of the packet and not just the TCP header to determine whether the traffic is allowed to pass through the firewall.
- Network IDS should be used to identify the OS-detection method used by some common hackers tools.
- Only needed ports should be kept open. The rest should be filtered or blocked.

- The staff of the organization using the systems should be given appropriate training on security awareness. They should also know the various security policies they’re required to follow.

nmap Command Switches:

Nmap is a free, open source tool that quickly and efficiently performs ping sweeps, port scanning, service identification, IP address detection, and operating system detection. Nmap has the benefit of scanning a large number of machines in a single session. It's supported by many operating systems, including Unix, Windows, and Linux.

The state of the port as determined by an nmap scan can be open, filtered, or unfiltered. *Open* means that the target machine accepts incoming request on that port. *Filtered* means a firewall or network filter is screening the port and preventing nmap from discovering whether it's open. *Unfiltered* mean the port is determined to be closed, and no firewall or filter is interfering with the nmap requests.

Nmap supports several types of scans

S.No	Nmap scan type	Description
1	***TCP connect***	The attacker makes a full TCP connection to the target system. The most reliable scan type but also the most detectable. Open ports reply with a SYN/ACK while closed ports reply with a RST/ACK.
2	***XMAS tree scan***	The attacker checks for TCP services by sending XMAS-tree packets, which are named as such because all the "lights" are on, meaning the FIN, URG, and PSH flags are set (the meaning of the flags will be discussed later in this chapter). Closed ports reply with a RST flag.
3	***SYN stealth scan***	This is also known as half-open scanning. The hacker sends a SYN packet and receives a SYN-ACK back from the server. It's stealthy because a full TCP connection isn't opened. Open ports reply with a SYN/ACK while closed ports reply with a RST/ACK.
4	***Null scan***	This is an advanced scan that may be able to pass through firewalls undetected or modified. Null scan has all flags off or not set. It only works on Unix systems. Closed ports will return a RST flag.
5	***Windows scan***	This type of scan is similar to the ACK scan and can also detect open ports.
6	***ACK scan***	This type of scan is used to map out firewall rules. ACK scan only works on Unix. The port is considered filtered by firewall rules if an ICMP destination unreachable message is received as a result of the ACK scan.

Scan Types

As a CEH (Certified Ethical Hacker), you need to be familiar with the following scan types and uses:

SYN : A SYN or stealth scan is also called a half-open scan because it doesn't complete the TCP three-way handshake. (The TCP/IP three-way handshake will be covered in the next section.) A hacker sends a SYN packet to the target; if a SYN/ACK frame is received back, then it's assumed the target would complete the connect and the port is listening. If an RST is received back from the target, then it's assumed the port isn't active or is closed. The advantage of the SYN stealth scan is that fewer IDS systems log this as an attack or connection attempt.

XMAS: X MAS scans send a packet with the FIN, URG, and PSH flags set. If the port is open, there is no response; but if the port is closed, the target responds with a RST/ACK packet. XMAS scans work only on target systems that follow the RFC 793 implementation of TCP/IP and don't work against any version of Windows.

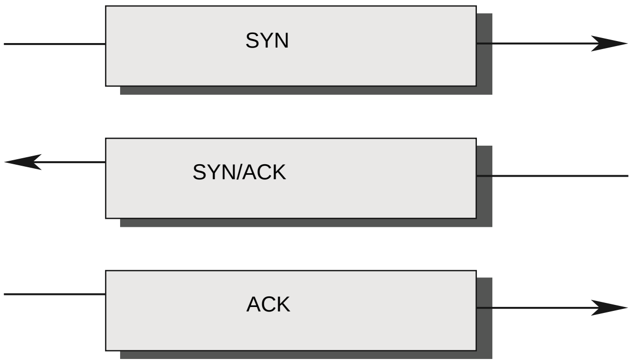
FIN : A FIN scan is similar to an XMAS scan but sends a packet with just the FIN flag set. FIN scans receive the same response and have the same limitations as XMAS scans.

NULL : A NULL scan is also similar to XMAS and FIN in its limitations and response, but it just sends a packet with no flags set.

IDLE : An IDLE scan uses a spoofed IP address to send a SYN packet to a target. Depending on the response, the port can be determined to be open or closed. IDLE scans determine port scan response by monitoring IP header sequence numbers.

TCP Communication Flag Types

TCP scan types are built on the *TCP three-way handshake*. TCP connections require a three-way handshake before a connection can be made and data transferred between the sender and receiver. Figure shows the steps of the TCP three-way handshake.



To complete the three-way handshake and make a successful connection between two hosts, the sender must send a TCP packet with the synchronize (SYN) bit set. Then, the receiving system responds with a TCP packet with the synchronize (SYN) and acknowledge (ACK) bit set to indicate the host is ready to receive data. The source system sends a final packet with the ACK bit set to indicate the connection is complete and data is ready to be sent.

Because TCP is a connection-oriented protocol, a process for establishing a connection (three-way handshake), restarting a failed connection, and finishing a connection is part of the protocol. These protocol notifications are called *flags*. TCP contains ACK, RST, SYN, URG, PSH, and FIN flags. The following list identifies the function of the TCP flags:

SYN Synchronize. Initiates a connection between hosts.

ACK Acknowledge. Established connection between hosts.

PSH Push. System is forwarding buffered data.

URG Urgent. Data in packets must be processed quickly.

FIN Finish. No more transmissions.

RST Reset. Resets the connection.

A hacker can attempt to bypass detection by using flags instead of completing a normal TCP connection.

TCP scan types

S.No	**XMAS scan**	**Flags sent by hacker**
1	XMAS scan	All flags set (ACK, RST, SYN, URG, PSH, FIN)
2	FIN scan	FIN
3	NULL scan	No flags set
4	TCP connect/full-open scan	SYN, then ACK
5	SYN scan / half-open scan	SYN, then RST

4.4. 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. 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. We’ll discuss that in the following section.

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:
3. Value Name: RestrictAnonymous
   - Data Type: REG_WORD
   - Value: 2

Finally, the system can be upgraded to Windows XP and the latest Microsoft security patches, which mitigates the NetBIOS null session vulnerability from occurring.

SNMP Enumeration

SNMP enumeration is the process of using SNMP to enumerate user accounts on a target system. SNMP employs two major types of software components for communication: the SNMP agent, which is located on the networking device, and the SNMP management station, which communicates with the agent.

Almost all network infrastructure devices, such as routers and switches and including Windows systems, contain an SNMP agent to manage the system or device. The SNMP management station sends requests to agents, and the agents send back replies. The requests and replies refer to configuration variables accessible by agent software. Management stations can also send requests to set values for certain variables. Traps let the management station know that something significant has happened in the agent software, such as a reboot or an interface failure. Management Information Base (MIB) is the database of configuration variables that resides on the networking device.

SNMP has two passwords you can use to access and configure the SNMP agent from the management station. The first is called a read community string. This password lets you view the configuration of the device or system. The second is called the read/write community string; it’s for changing or editing the configuration on the device. Generally, the default read community string is public and the default read/write community string is private. A common security loophole occurs when the community strings are left at the default settings: a hacker can use these default passwords to view or change the device configuration

SNMP Enumeration Countermeasures

The simplest way to prevent SNMP enumeration is to remove the SNMP agent on the potential target systems or turn off the SNMP service. If shutting off SNMP isn't an option, then change the default read and read/write community names.

In addition, an administrator can implement the Group Policy security option Additional Restrictions For Anonymous Connections, which restricts SNMP connections.

Windows 2000 DNS Zone Transfer

In a Windows 2000 domain, clients use service (SRV) records to locate Windows 2000 domain services, such as Active Directory and Kerberos. This means every Windows 2000 Active Directory domain must have a DNS server for the network to operate properly.

A simple zone transfer performed with the nslookup command can enumerate lots of interesting network information. The command to enumerate using the nslookup command is as follows:

```
nslookup ls -d domainname
```

Within the nslookup results, a hacker looks closely at the following records, because they provide additional information about the network services:

- ✓ Global Catalog service (_gc._tcp_)
- ✓ Domain controllers (_ldap._tcp)
- ✓ Kerberos authentication (_kerberos._tcp)

As a countermeasure, zone transfers can be blocked in the properties of the Windows DNS server.

An Active Directory database is a Lightweight Directory Access Protocol (LDAP)-based database. This allows the existing users and groups in the database to be enumerated with a simple LDAP query. The only thing required to perform this enumeration is to create an authenticated session via LDAP. A Windows 2000 LDAP client called the Active Directory Administration Tool (ldp.exe) connects to an Active Directory server and identifies the contents of the database. You can find ldp.exe on the Windows 2000 CD-ROM in the

Support\Reskit\Netmgmt\Dstool folder.

To perform an Active Directory enumeration attack, a hacker performs the following steps:

1. Connect to any Active Directory server using ldp.exe on port 389. When the connection is complete, server information is displayed in the right pane.
2. On the Connection menu, choose Authenticate. Type the username, password, and domain name in the appropriate boxes. You can use the Guest account or any other domain account.
3. Once the authentication is successful, enumerate users and built-in groups by choosing the Search option from the Browse menu.

4.5. System Hacking

The Simplest Way to Get a Password

Many hacking attempts start with getting a password to a target system. Passwords are the key piece of information needed to access a system, and users often select passwords that are easy to guess. Many reuse passwords or choose one that's simple—such as a pet's name—to help them remember it. Because of this human factor, most password guessing is successful if some information is known about the target. Information gathering and reconnaissance can help give away information that will help a hacker guess a user's password.

Once a password is guessed or cracked, it can be the launching point for escalating privileges, executing applications, hiding files, and covering tracks. If guessing a password fails, then passwords may be cracked manually or with automated tools such as a dictionary or brute-force method

Types of Passwords

Several types of passwords are used to provide access to systems. The characters that form a password can fall into any of these categories:

- Only letters
- Only numbers
- Only special characters
- Letters and numbers
- Only letters and special characters
- Only numbers and special characters
- Letters, numbers, and special characters

A strong password is less susceptible to attack by a hacker. The following rules, proposed by the EC-Council, should be applied when you're creating a password, to protect it against attacks:

- ➢ Must not contain any part of the user's account name
- ➢ Must have a minimum of eight characters
- ➢ Must contain characters from at least three of the following categories:
  - ✓ Nonalphanumeric symbols ($,:"%@!#)
  - ✓ Numbers
  - ✓ Uppercase letters
  - ✓ Lowercase letters

A hacker may use different types of attacks in order to identify a password and gain further access to a system.

The types of password attacks are as follows:

Passive Online : Eavesdropping on network password exchanges. Passive online attacks include sniffing, man-in-the-middle, and replay attacks.

Active Online : Guessing the Administrator password. Active online attacks include automated password guessing.

Offline : Dictionary, hybrid, and brute-force attacks.

Nonelectronic : Shoulder surfing, keyboard sniffing, and social engineering.

Passive Online Attacks

A passive online attack is also known as sniffing the password on a wired or wireless network. A passive attack is not detectable to the end user. The password is captured during the authentication process and can then be compared against a dictionary file or word list. User account passwords are commonly hashed or encrypted when sent on the network to prevent unauthorized access and use. If the password is protected by encryption or hashing, special tools in the hacker's toolkit can be used to break the algorithm.

Another passive online attack is known as man-in-the-middle (MITM). In a MITM attack, the hacker intercepts the authentication request and forwards it to the server. By inserting a sniffer between the client and the server, the hacker is able to sniff both connections and capture passwords in the process.

A replay attack is also a passive online attack; it occurs when the hacker intercepts the password en route to the authentication server and then captures and resends the authentication packets for later authentication. In this manner, the hacker doesn't have to break the password or learn the password through MITM but rather captures the password and reuses the password-authentication packets later to authenticate as the client.

Active Online Attacks

The easiest way to gain administrator-level access to a system is to guess a simple password assuming the administrator used a simple password. Password guessing is an active online attack. It relies on the human factor involved in password creation and only works on weak passwords.

Performing Automated Password Guessing

To speed up the guessing of a password, hackers use automated tools. An easy process for automating password guessing is to use the Windows shell commands based on the standard NET USE syntax. To create a simple automated password-guessing script, perform the following steps:

1. Create a simple username and password file using Windows Notepad. Automated tools such as the Dictionary Generator are available to create this word list. Save the file on the C: drive as credentials.txt.
2. Pipe this file using the FOR command:

```
C:\> FOR /F “token=1, 2*” %i in (credentials.txt)
```

3. Type net use \\targetIP\IPC$ %i /u: %j to use the credentials.txt file to attempt to log on to the target system’s hidden share.

Defending Against Password Guessing

Two options exist to defend against password guessing and password attacks. Both smart cards and biometrics add a layer of security to the insecurity that’s inherent when users create their own passwords.

A user can also be authenticated and validated using biometrics. Biometrics use physical characteristics such as fingerprints, hand geometry scans, and retinal scans as credentials to validate users.

Both smart cards and biometrics use two-factor authentication, which requires two forms of identification (such as the actual smart card and a password) when validating a user. By requiring something the user physically has (a smart card, in this instance) and something the user knows (their password), security is increased, and the authentication process isn’t susceptible to password attacks.

Offline Attacks

Offline attacks are performed from a location other than the actual computer where the passwords reside or were used. Offline attacks usually require physical access to the computer and copying the password file from the system onto removable media. The hacker then takes the file to another computer to perform the cracking. Several types of offline password attacks exist

Type of attack	Characteristics	Example password
Dictionary attack	Attempts to use passwords from a list of dictionary words	Administrator
Hybrid attack	Substitutes numbers of symbols for password characters	Adm1n1strator
Brute-force attack	Tries all possible combinations of letters, numbers, and special characters	Ms!tr245@F5a

A dictionary attack is the simplest and quickest type of attack. It's used to identify a password that is an actual word, which can be found in a dictionary. Most commonly, the attack uses a dictionary file of possible words, which is hashed using the same algorithm used by the authentication process. Then, the hashed dictionary words are compared with hashed passwords as the user logs on, or with passwords stored in a file on the server. The dictionary attack works only if the password is an actual dictionary word; therefore, this type of attack has some limitations. It can't be used against strong passwords containing numbers or other symbols.

A hybrid attack is the next level of attack a hacker attempts if the password can't be found using a dictionary attack. The hybrid attack starts with a dictionary file and substitutes numbers and symbols for characters in the password. For example, many users add the number 1 to the end of their password to meet strong password requirements. A hybrid attack is designed to find those types of anomalies in passwords.

The most time-consuming type of attack is a brute-force attack, which tries every possible combination of uppercase and lowercase letters, numbers, and symbols. A brute-force attack is the slowest of the three types of attacks because of the many possible combinations of characters in the password. However, brute force is effective; given enough time and processing power, all passwords can eventually be identified.

Nonelectronic Attacks

Nonelectronic—or nontechnical attacks—are attacks that do not employ any technical knowledge. This kind of attack can include social engineering, shoulder surfing, keyboard sniffing, and dumpster diving. Social engineering is the art of interacting with people either face to face or over the telephone and getting them to give out valuable information such as passwords. Social engineering relies on people's good nature and desire to help others. Many times, a help desk is the target of a social-engineering attack because their job is to help people—and recovering or resetting passwords is a common function of the help desk.

The best defense against social-engineering attacks is security-awareness training for all employees and security procedures for resetting passwords. Shoulder surfing involves looking over someone's shoulder as they type a password. This can be effective when the hacker is in close proximity to the user and the system. Special screens that make it difficult to see the computer screen from an angle can cut down on shoulder surfing. In addition, employee awareness and training can virtually eliminate this type of attack. Dumpster diving hackers look through the trash for information such as passwords, which may be written down on a piece of paper. Again, security awareness training on shredding important documents can prevent a hacker from gathering passwords by dumpster diving.

Cracking a Password

Manual password cracking involves attempting to log on with different passwords. The hacker follows these steps:

1. Find a valid user account (such as Administrator or Guest).
2. Create a list of possible passwords.
3. Rank the passwords from high to low probability.
4. Key in each password.
5. Try again until a successful password is found.

A hacker can also create a script file that tries each password in a list. This is still considered manual cracking, but it's time consuming and not usually effective.

A more efficient way of cracking a password is to gain access to the password file on a system. Most systems hash (one-way encrypt) a password for storage on a system. During the logon process, the password entered by the user is hashed using the same algorithm and then compared to the hashed passwords stored in the file. A hacker can attempt to gain access to the hashing algorithm stored on the server instead of trying to guess or otherwise identify the password. If the hacker is successful, they can decrypt the passwords stored on the server.

Redirecting the SMB Logon to the Attacker

Another way to discover passwords on a network is to redirect the Server Message Block (SMB) logon to an attacker's computer so that the passwords are sent to the hacker. In order to do this, the hacker must sniff the NTLM responses from the authentication server and trick the victim into attempting Windows authentication with the attacker's computer. A common technique is to send the victim an email message with an embedded link to a fraudulent SMB server. When the link is clicked, the user unwittingly sends their credentials over the network.

SMBRelay : An SMB server that captures usernames and password hashes from incoming SMB traffic. SMBRelay can also perform man-in-the-middle (MITM) attacks.

SMBRelay2 : Similar to SMBRelay but uses NetBIOS names instead of IP addresses to capture usernames and passwords.

pwdump2 : A program that extracts the password hashes from a SAM file on a Windows system. The extracted password hashes can then be run through L0phtCrack to break the passwords.

Samdump : Another program that extracts NTLM hashed passwords from a SAM file.

C2MYAZZ A spyware program that makes Windows clients send their passwords as cleartext. It displays usernames and their passwords as users attach to server resources.

SMB Relay MITM Attacks and Countermeasures

An SMB relay MITM attack is when the attacker sets up a fraudulent server with a relay address. When a victim client connects to the fraudulent server, the MITM server intercepts the call, hashes the password, and passes the connection to the victim server.

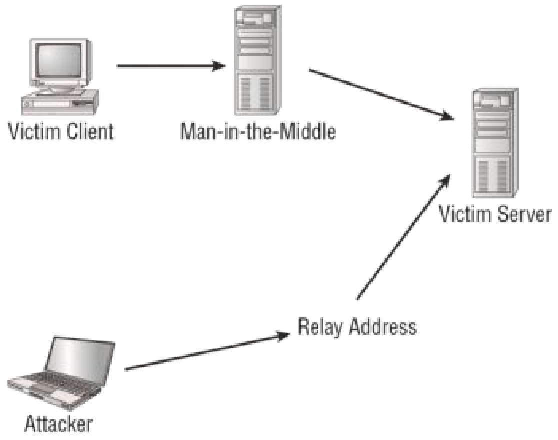


Fig: SMB relay MITM attack

SMB relay countermeasures include configuring Windows 2000 to use SMB signing, which causes it to cryptographically sign each block of SMB communications.

NetBIOS DoS Attacks

A NetBIOS denial-of-service (DoS) attack sends a NetBIOS Name Release message to the NetBIOS Name Service on a target Windows systems and forces the system to place its name in conflict so that the name can no longer be used. This essentially blocks the client from participating in the NetBIOS network and creates a network DoS for that system.

Password-Cracking Countermeasures

The strongest passwords possible should be implemented to protect against password cracking. Systems should enforce 8–12-character alphanumeric passwords

To protect against cracking of the hashing algorithm for passwords stored on the server, you must take care to physically isolate and protect the server. The system administrator can use the SYSKEY utility in Windows to further protect hashes stored on the server’s hard disk. The server logs should also be monitored for brute-force attacks on user accounts.

A system administrator can implement the following security precautions to decrease the effectiveness of a brute-force password-cracking attempt:

- ✓ Never leave a default password.
- ✓ Never use a password that can be found in a dictionary.

- ✓ Never use a password related to the hostname, domain name, or anything else that can be found with Whois.
- ✓ Never use a password related to your hobbies, pets, relatives, or date of birth.
- ✓ As a last resort, use a word that has more than 21 characters from a dictionary as a password.

Understanding Keyloggers and Other Spyware Technologies

If all other attempts to gather passwords fail, then a keystroke logger is the tool of choice for hackers. Keystroke loggers (keyloggers) can be implemented either using hardware or software. Hardware keyloggers are small hardware devices that connect the keyboard to the PC and save every keystroke into a file or in the memory of the hardware device. In order to install a hardware keylogger, a hacker must have physical access to the system.

Software keyloggers are pieces of stealth software that sit between the keyboard hardware and the operating system so that they can record every keystroke. Software keyloggers can be deployed on a system by Trojans or viruses.

4.6. Malware Threats

Trojans and backdoors are two ways a hacker can gain access to a target system. They come in many different varieties, but they all have one thing in common: they must be installed by another program, or the user must be tricked into installing the Trojan or backdoor on their system. Trojans and backdoors are potentially harmful tools in the ethical hacker's toolkit and should be used judiciously to test the security of a system or network.

Viruses and worms can be just as destructive to systems and networks as Trojans and backdoors. In fact, many viruses carry Trojan executables and can infect a system, then create a backdoor for hackers. This chapter will discuss the similarities and differences among Trojans, backdoors, viruses, and worms. All of these types of malicious code or malware are important to ethical hackers because they are commonly used by hackers to attack and compromise systems.

Trojans and Backdoors

Trojans and backdoors are types of malware used to infect and compromise computer systems. A ***Trojan*** is a malicious program disguised as something benign. In many cases the Trojan appears to perform a desirable function for the user but actually allows a hacker access to the user's computer system. Trojans are often downloaded along with another program or software package. Once installed on a system, they can cause data theft and loss, as well as system crashes or slowdowns. Trojans can also be used as launching points for other attacks, such as distributed denial of service (DDoS). Many Trojans are used to manipulate files on the victim computer, manage processes, remotely run commands, intercept keystrokes, watch screen images, and restart or shut down infected hosts. Sophisticated Trojans can connect themselves to their originator or announce the Trojan infection on an Internet Relay Chat (IRC) channel.

Trojans ride on the backs of other programs and are usually installed on a system without the user's knowledge. A Trojan can be sent to a victim system in many ways, such as the following:

- An instant messenger (IM) attachment
- IRC
- An email attachment
- NetBIOS file sharing
- A downloaded Internet program

Many fake programs purporting to be legitimate software such as freeware, spyware removal tools, system optimizers, screensavers, music, pictures, games, and videos can install a Trojan on a system just by being downloaded. Advertisements on Internet sites for free programs, music files, or video files lure a victim into installing the Trojan program; the program then has system-level access on the target system, where it can be destructive and insidious.

Common Trojan programs are,

Trojan	**Protocol**	**Port**
BackOrifice	UDP	31337 or 31338
Deep Throat	UDP	2140 and 3150
NetBus	TCP	12345 and 12346
Whack-a-Mole	TCP	12361 and 12362
NetBus 2	TCP	20034
GirlFriend	TCP	21544
Master's Paradise	TCP	3129, 40421, 40422, 40423, and 40426

A ***backdoor*** is a program or a set of related programs that a hacker installs on a target system to allow access to the system at a later time. A backdoor can be embedded in a malicious Trojan. The objective of installing a backdoor on a system is to give hackers access into the system at a time of their choosing. The key is that the hacker knows how to get into the backdoor undetected and is able to use it to hack the system further and look for important information.

Adding a new service is the most common technique to disguise backdoors in the Windows operating system. Before the installation of a backdoor, a hacker must investigate the system to find services that are running. Again the use of good information-gathering techniques is critical to knowing what services or programs are already running on the target system. In most cases the hacker installs the backdoor, which adds a new service and gives it an inconspicuous name or, better yet, chooses a service that's never used and that is either activated manually or completely disabled.

This technique is effective because when a hacking attempt occurs the system administrator usually focuses on looking for something odd in the system, leaving all existing services unchecked. The backdoor technique is simple but efficient: the hacker can get back into the machine with the least amount of visibility in the server logs. The backdoored service lets the hacker use higher privileges—in most cases, as a System account.

Remote Access Trojans *(RATs)* are a class of backdoors used to enable remote control over a compromised machine. They provide apparently useful functions to the user and, at the same time, open a network port on the victim computer. Once the RAT is started, it behaves as an executable file, interacting with certain Registry keys responsible for starting processes and sometimes creating its own system services. Unlike common backdoors, RATs hook themselves into the victim operating system and always come packaged with two files: the client file and the server file. The server is installed in the infected machine, and the client is used by the intruder to control the compromised system.

RATs allow a hacker to take control of the target system at any time. In fact one of the indications that a system has been exploited is unusual behavior on the system, such as the mouse moving on its own or pop-up windows appearing on an idle system.

Overt and Covert Channels

An ***overt channel*** is the normal and legitimate way that programs communicate within a computer system or network. A *covert channel* uses programs or communications paths in ways that were not intended.

Trojans can use covert channels to communicate. Some client Trojans use covert channels to send instructions to the server component on the compromised system. This sometimes makes Trojan communication difficult to decipher and understand. An unsuspecting intrusion detection system (IDS) sniffing the transmission between the Trojan client and server would not flag it as anything unusual. By using the covert channel, the Trojan can communicate or “phone home” undetected, and the hacker can send commands to the client component undetected.

Some covert channels rely on a technique called *tunneling*, which lets one protocol be carried over another protocol. **Internet Control Message Protocol** (ICMP) tunneling is a method of using ICMP echo-request and echo-reply to carry any payload an attacker may wish to use, in an attempt to stealthily access or control a compromised system. The ping command is a generally accepted troubleshooting tool, and it uses the ICMP protocol. For that reason, many router, switches, firewalls, and other packet filtering devices allow the ICMP protocol to be passed through the device. Therefore, ICMP is an excellent choice of tunneling protocols.

Types of Trojans

Trojans can be created and used to perform different attacks. Here are some of the most common types of Trojans:

Remote Access Trojans (RATs) Used to gain remote access to a system.

Data-Sending Trojans Used to find data on a system and deliver data to a hacker.

Destructive Trojans Used to delete or corrupt files on a system.

Denial-of-Service Trojans Used to launch a denial-of-service attack.

Proxy Trojans Used to tunnel traffic or launch hacking attacks via other systems.

FTP Trojans Used to create an FTP server in order to copy files onto a system.

Security Software Disabler Trojans Used to stop antivirus software.

How Reverse-Connecting Trojans Work

Reverse-connecting Trojans let an attacker access a machine on the internal network from the outside. The hacker can install a simple Trojan program on a system on the internal network, such as the reverse WWW shell server. On a regular basis (usually every 60 seconds), the internal server tries to access the external master system to pick up commands. If the attacker has typed something into the master system, this command is retrieved and executed on the internal system. The reverse WWW shell server uses standard HTTP. It's dangerous because it's difficult to detect: it looks like a client is browsing the Web from the internal network.

Wrappers are software packages that can be used to deliver a Trojan. The wrapper binds a legitimate file to the Trojan file. Both the legitimate software and the Trojan are combined into a single executable file and installed when the program is run.

Generally, games or other animated installations are used as wrappers because they entertain the user while the Trojan in being installed. This way, the user doesn't notice the slower processing that occurs while the Trojan is being installed on the system—the user only sees the legitimate application being installed.

Trojan Construction Kit and Trojan Makers

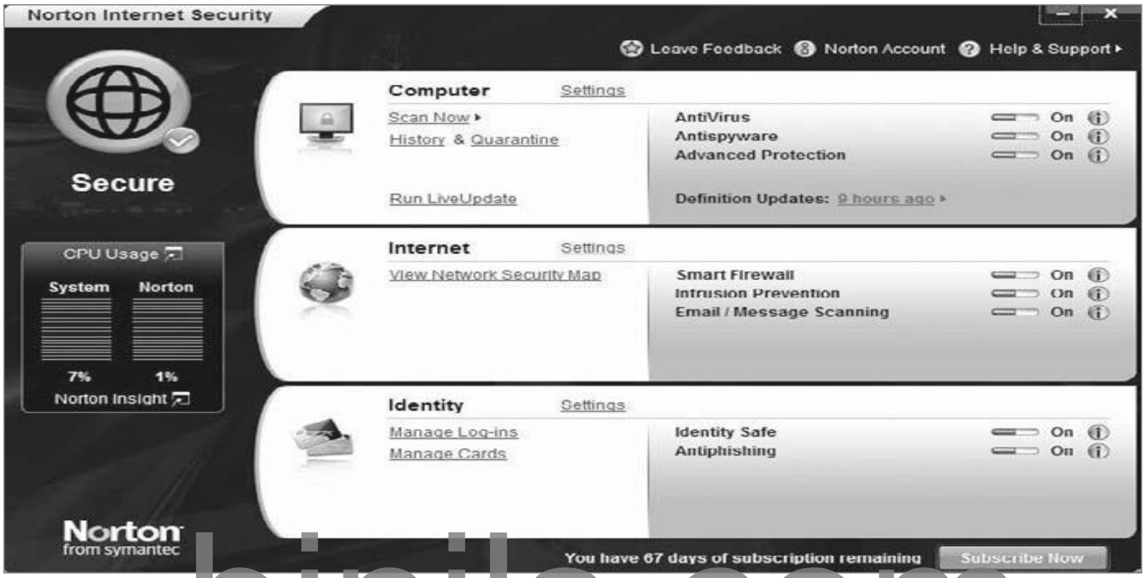
Several Trojan-generator tools enable hackers to create their own Trojans. Such toolkits help hackers construct Trojans that can be customized. These tools can be dangerous and can backfire if not executed properly. New Trojans created by hackers usually have the added benefit of passing undetected through virus-scanning and Trojan-scanning tools because they don't match any known signatures.

Some of the Trojan kits available in the wild are Senna Spy Generator, the Trojan Horse Construction Kit v2.0, Progenic Mail Trojan Construction Kit, and Pandora's Box.

Trojan Countermeasures

Most commercial antivirus program have anti-Trojan capabilities as well as spyware detection and removal functionality. These tools can automatically scan hard drives on startup to detect backdoor and Trojan programs before they can cause damage. Once a system is infected, it's more difficult to clean, but you can do so with commercially available tools.

Although several commercially antivirus or Trojan removal tools are available, my personal recommendation is Norton Internet Security (Figure below). Norton Internet Security includes a personal firewall, intrusion detection system, antivirus, antispyware, antiphishing, and email scanning. Norton Internet Security will clean most Trojans from a system as well.



Norton Internet Security

Leave Feedback | Norton Account | Help & Support ▸

Secure

CPU Usage

System	Norton
7%	1%

Norton Insight

Computer Settings

Scan Now ▸
History & Quarantine
Run LiveUpdate

AntiVirus	On
Antispyware	On
Advanced Protection	On

Definition Updates: 9 hours ago ▸

Internet Settings

View Network Security Map

Smart Firewall	On
Intrusion Prevention	On
Email / Message Scanning	On

Identity Settings

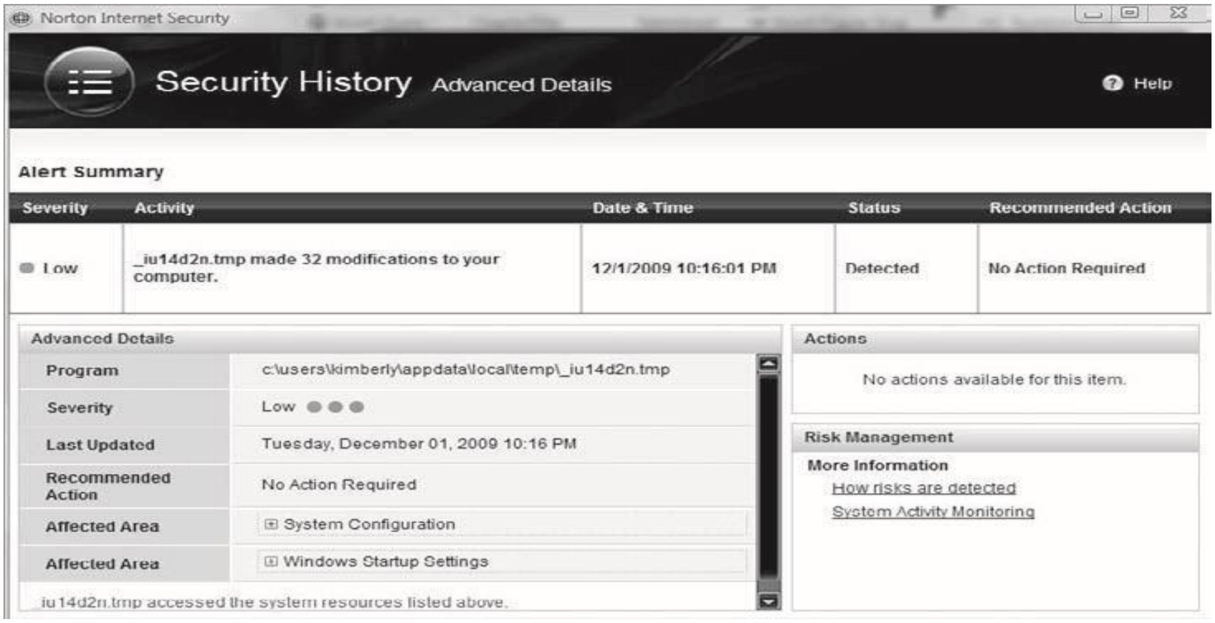
Manage Log-ins
Manage Cards

Identity Safe	On
Antiphishing	On

Norton from symantec

You have 67 days of subscription remaining | Subscribe Now

Fig: Norton Internet Security



Norton Internet Security

Security History Advanced Details

Help

Alert Summary

Severity	Activity	Date & Time	Status	Recommended Action
● Low	_iu14d2n.tmp made 32 modifications to your computer.	12/1/2009 10:16:01 PM	Detected	No Action Required

Advanced Details

Program	c:\users\kimberly\appdata\local\temp_iu14d2n.tmp
Severity	Low ● ● ●
Last Updated	Tuesday, December 01, 2009 10:16 PM
Recommended Action	No Action Required
Affected Area	⊞ System Configuration
Affected Area	⊞ Windows Startup Settings

iu14d2n.tmp accessed the system resources listed above.

Actions

No actions available for this item.

Risk Management

More Information

How risks are detected
System Activity Monitoring

The security software works by having known signatures of malware, such as Trojans and viruses. The repair for the malware is made through the use of definitions of the malware. When installing and using any personal security software or antivirus and anti-Trojan software, you must make sure that the software has all the current definitions. To ensure the latest patches and fixes are available, you should connect the system to the Internet so the software can continually update the malware definitions and fixes.

It’s important to use commercial applications to clean a system instead of freeware tools, because many freeware removal tools can further infect the system. In addition, a lot of commercial security software includes an intrusion detection component that will perform port monitoring and can identify ports that have been opened or files that have changed.

The key to preventing Trojans and backdoors from being installed on a system is to educate users not to install applications downloaded from the Internet or open email attachments from parties they don’t know. Many system administrators don’t give users the system permissions necessary to install programs on their system for that very reason. Proper use of Internet technologies should be included in regular employee security awareness training.

Checking a System with System File Verification

Windows 2003 includes a feature called Windows File Protection (WFP) that prevents the replacement of protected files. WFP checks the file integrity when an attempt is made to overwrite a SYS, DLL, OCX, TTF, or EXE file. This ensures that only Microsoft-verified files are used to replace system files.

Viruses and Worms

Viruses and worms can be used to infect a system and modify a system to allow a hacker to gain access. Many viruses and worms carry Trojans and backdoors. In this way, a virus or worm is a carrier and allows malicious code such as Trojans and backdoors to be transferred from system to system much in the way that contact between people allows germs to spread.

A *virus* and a *worm* are similar in that they’re both forms of malicious software (*malware*). A virus infects another executable and uses this carrier program to spread itself. The virus code is injected into the previously benign program and is spread when the program is run. Examples of virus carrier programs are macros, games, email attachments, Visual Basic scripts, and animations.

A worm is similar to a virus in many ways but does not need a carrier program. A worm can self-replicate and move from infected host to another host. A worm spreads from system to system automatically, but a virus needs another program in order to spread. Viruses and worms both execute without the knowledge or desire of the end user.

Types of Viruses

Viruses are classified according to two factors: what they infect and how they infect. A virus can infect the following components of a system:

- ✓ System sectors
- ✓ Files
- ✓ Macros (such as Microsoft Word macros)
- ✓ Companion files (supporting system files like DLL and INI files)
- ✓ Disk clusters
- ✓ Batch files (BAT files)
- ✓ Source code

A virus infects through interaction with an outside system. Viruses need to be carried by another executable program. By attaching itself to the benign executable a virus can spread fairly quickly as users or the system runs the executable. Viruses are categorized according to their infection technique, as follows:

Polymorphic Viruses These viruses encrypt the code in a different way with each infection and can change to different forms to try to evade detection.

Stealth Viruses These viruses hide the normal virus characteristics, such as modifying the original time and date stamp of the file so as to prevent the virus from being noticed as a new file on the system.

Fast and Slow Infectors These viruses can evade detection by infecting very quickly or very slowly. This can sometimes allow the program to infect a system without detection by an antivirus program.

Sparse Infectors These viruses infect only a few systems or applications.

Armored Viruses These viruses are encrypted to prevent detection.

Multipartite Viruses These advanced viruses create multiple infections.

Cavity (Space-Filler) Viruses These viruses attach to empty areas of files.

Tunneling Viruses These viruses are sent via a different protocol or encrypted to prevent detection or allow it to pass through a firewall.

Camouflage Viruses These viruses appear to be another program.

NTFS and Active Directory Viruses These viruses specifically attack the NT file system or Active Directory on Windows systems.

An attacker can write a custom script or virus that won't be detected by antivirus programs. Because virus detection and removal is based on a signature of the program, a hacker just needs to change the signature or look of the virus to prevent detection. The virus signature or definition is the way an antivirus program is able to determine if a system is infected by a virus. Until the virus is detected and antivirus companies have a chance to update virus definitions, the virus goes undetected. Additional time may elapse before a user updates the antivirus program, allowing the system to be vulnerable to an infection. This allows an attacker to evade antivirus detection and removal for a period of time. A critical countermeasure to virus infection is to maintain up-to-date virus definitions in an antivirus program.

One of the most longstanding viruses was the Melissa virus, which spread through Microsoft Word Macros. Melissa infected many users by attaching to the Word doc and then when the file was copied or emailed, the virus spread along with the file.

Virus Hoaxes are emails sent to users usually with a warning about a virus attack. The Virus Hoax emails usually make outlandish claims about the damage that will be caused by a virus and then offer to download a remediation patch from well-known companies such as

Microsoft or Norton. Other Hoaxes recommend users delete certain critical systems files in order to remove the virus. Of course, should a user follow these recommendations they will most certainly have negative consequences.

Common Virus Hoaxes

Name	**Executable**	**Description**
Antichrist	(none)	This is a hoax that warned about a supposed virus discovered by Microsoft and McAfee named "Antichrist", telling the user that it is installed via an email with the subject line: "SURPRISE?!!!!!!!!!!" after which it destroys the zeroth sector of the hard disk, rendering it unusable.
Budweiser Frogs	BUDSAVER.EXE	Supposedly would erase the user's hard drive and steal the user's screen name and password.
Goodtimes virus	(none)	Warnings about a computer virus named "Good Times" began being passed around among Internet users in 1994. The Goodtimes virus was supposedly transmitted via an email bearing the subject header "Good Times" or "Goodtimes," hence the virus's name, and the warning recommended deleting any such email unread. The virus described in the warnings did not exist, but the warnings themselves, were, in effect, virus-like.

Virus Detection Methods

The following techniques are used to detect viruses:

- Scanning
- Integrity checking with checksums
- Interception based on a virus signature

The process of virus detection and removal is as follows:

1. Detect the attack as a virus. Not all anomalous behavior can be attributed to a virus.
2. Trace processes using utilities such as handle.exe, listdlls.exe, fport.exe, netstat.exe, and pslist.exe, and map commonalities between affected systems.
3. Detect the virus payload by looking for altered, replaced, or deleted files. New files, changed file attributes, or shared library files should be checked.
4. Acquire the infection vector and isolate it. Then, update your antivirus definitions and rescan all systems.

4.7. Sniffing

A sniffer is a packet-capturing or frame-capturing tool. It basically captures and displays the data as it is being transmitted from host to host on the network. Generally a sniffer intercepts traffic on the network and displays it in either a command-line or GUI format for a hacker to view. Most sniffers display both the Layer 2 (frame) or Layer 3 (packet) headers and the data payload. Some sophisticated sniffers interpret the packets and can reassemble the packet stream into the original data, such as an email or a document.

Sniffers are used to capture traffic sent between two systems, but they can also provide a lot of other information. Depending on how the sniffer is used and the security measures in place, a hacker can use a sniffer to discover usernames, passwords, and other confidential information transmitted on the network. Several hacking attacks and various hacking tools require the use of a sniffer to obtain important information sent from the target system. This chapter will describe how sniffers work and identify the most common sniffer hacking tools.

Understanding Host-to-Host Communication

All Host-to-Host network communications is based upon the TCP/IP Data Communications Model. The TCP/IP Model is a 4 layer model. The TCP/IP Model maps to the older OSI model with 7 layers of data communication. Most applications use the TCP/IP suite for host-to-host data communications.

In normal network operations, the application layer data is encapsulated and a header containing address information is added to the beginning of the data. An IP header containing source and destination IP address are added to the data as well as a MAC header containing source and destination MAC addresses. IP addresses are used to route traffic to the appropriate IP network, and the MAC addresses ensure the data is sent to the correct host on the destination IP network. In this manner, traffic is sent from source host to destination host across the Internet and delivery to the correct host is ensured. The postal system works much the same way. Mail is routed to the appropriate area using the zip code, and then the mail is delivered within the zip code to the street and house number. The IP address is similar to the zip code to deliver mail to the regional area, and the street and house numbers are like the MAC address of that exact station on the network.

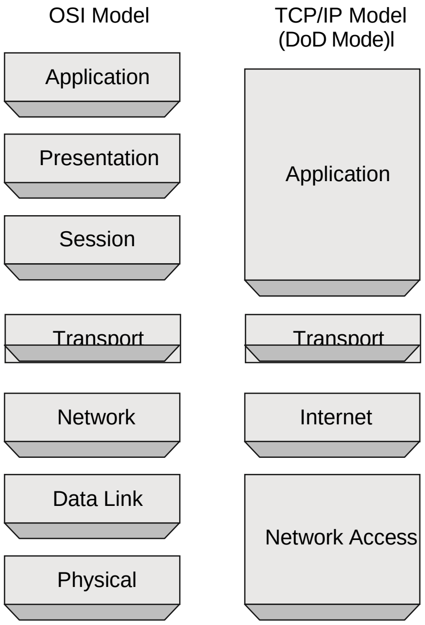
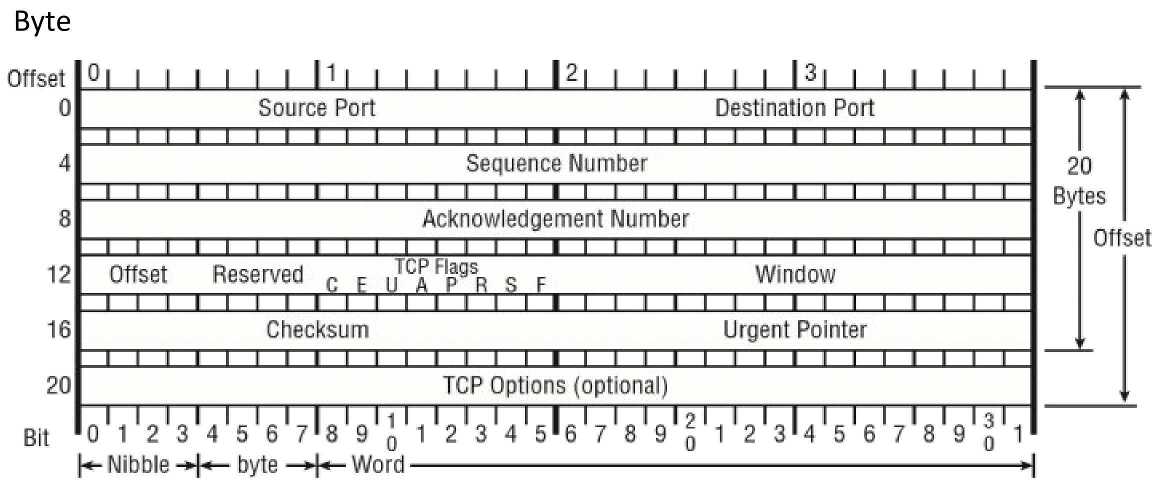


Fig: TCP/IP Model

The address system ensures accurate delivery to the receiver. In normal network operations, a host should not receive data intended for another host as the data packet should only be received by the intended receiver. Simply said, the data should only be received by the station with the correct IP and MAC address. However, we know that sniffers do receive data not intended for them.

In addition to understanding network addresses, it is also important to understand the format of the TCP Header. Figure shows the TCP Header format.



Understanding Host-to-Host Communication

Fig: TCP Header Format

The TCP Header is comprised of the following fields:

Source Port: 16 bits The source port number.

Destination Port: 16 bits The destination port number.

Sequence Number: 32 bits The sequence number of the first data octet in this segment (except when SYN is present). If SYN is present the sequence number is the initial sequence number (ISN) and the first data octet is ISN+1.

Acknowledgment Number: 32 bits If the ACK control bit is set this field contains the value of the next sequence number the sender of the segment is expecting to receive.

Data Offset: 4 bits The number of 32 bit words in the TCP Header. This indicates where the data begins.

Reserved: 6 bits Reserved for future use. Must be zero.

Control Bits: 6 bits

- ✓URG: Urgent Pointer field significant
- ✓ACK: Acknowledgment field significant
- ✓PSH: Push Function

- ✓RST: Reset the connection
- ✓SYN: Synchronize sequence numbers
- ✓FIN: No more data from sender

Window: 16 bits The number of data octets beginning with the one indicated in the acknowledgment field which the sender of this segment is willing to accept.

Checksum: 16 bits The checksum field is a computation of all fields to ensure all data was received and the data was not modified in transit.

Urgent Pointer: 16 bits This field communicates the current value of the urgent pointer as a positive offset from the sequence number in this segment. The urgent pointer points to the sequence number of the octet following the urgent data. This field is only be interpreted in segments with the URG control bit set.

Options: variable Options may occupy space at the end of the TCP header and are a multiple of 8 bits in length.

When referring to the length of the fields in the TCP Header, 8 bits comprises a single byte. A Nibble is less than a byte and a Word is more than a byte.

How a Sniffer Works

Sniffer software works by capturing packets not destined for the sniffer system’s MAC address but rather for a target’s destination MAC address. This is known as *promiscuous mode*. Normally, a system on the network reads and responds only to traffic sent directly to its MAC address. However, many hacking tools change the system’s NIC to promiscuous mode. In promiscuous mode, a NIC reads all traffic and sends it to the sniffer for processing. Promiscuous mode is enabled on a network card with the installation of special driver software. Many of the hacking tools for sniffing include a promiscuous-mode driver to facilitate this process. Not all Windows drivers support promiscuous mode, so when using hacking tools ensure that the driver will support the necessary mode.

Any protocols that don’t encrypt data are susceptible to sniffing. Protocols such as HTTP, POP3, Simple Network Management Protocol (SNMP), and FTP are most commonly captured using a sniffer and viewed by a hacker to gather valuable information such as usernames and passwords.

There are two different types of sniffing: passive and active. *Passive sniffing* involves listening and capturing traffic, and is useful in a network connected by hubs; *active sniffing* involves launching an Address Resolution Protocol (ARP) spoofing or traffic-flooding attack against a switch in order to capture traffic. As the names indicate, active sniffing is detectable but passive sniffing is not detectable.

In networks that use hubs or wireless media to connect systems, all hosts on the network can see all traffic; therefore, a passive packet sniffer can capture traffic going to and from all hosts connected via the hub. A switched network operates differently. The switch looks at the data sent to it and tries to forward packets to their intended recipients based on MAC address. The switch maintains a MAC table of all the systems and the port numbers to which they're connected. This enables the switch to segment the network traffic and send traffic only to the correct destination MAC addresses. A switch network has greatly improved throughput and is more secure than a shared network connected via hubs.

Another way to sniff data through a switch is to use a span port or port mirroring to enable all data sent to a physical switch port to be duplicated to another port. In many cases, span ports are used by network administrators to monitor traffic for legitimate purposes.

Sniffing Countermeasures

The best security defense against a sniffer on the network is encryption. Although encryption won't prevent sniffing, it renders any data captured during the sniffing attack useless because hackers can't interpret the information. Encryption such as AES and RC4 or RC5 can be utilized in VPN technologies and is commonly used to prevent sniffing on a network.

Bypassing the Limitations of Switches

Because of the way Ethernet switches operate, it is more difficult to gather useful information when sniffing on a switched network. Since most modern networks have been upgraded from hub to switches, it takes a little more effort to sniff on a switched network. One of the ways to do that is to trick the switch into sending the data to the hackers' computer using ARP poisoning.

How ARP Works

ARP allows the network to translate IP addresses into MAC addresses. When one host using TCP/IP on a LAN tries to contact another, it needs the MAC address or hardware address of the host it's trying to reach. It first looks in its ARP cache to see if it already has the MAC address; if it doesn't, it broadcasts an ARP request asking, "Who has the IP address I'm looking for?" If the host that has that IP address hears the ARP query, it responds with its own MAC address, and a conversation can begin using TCP/IP.

ARP poisoning is a technique that's used to attack an Ethernet network and that may let an attacker sniff data frames on a switched LAN or stop the traffic altogether. ARP poisoning utilizes ARP spoofing, where the purpose is to send fake, or spoofed, ARP messages to an Ethernet LAN. These frames contain false MAC addresses that confuse network devices such as network switches. As a result, frames intended for one machine can be mistakenly sent to another (allowing the packets to be sniffed) or to an unreachable host (a denial-ofservice, or DoS, attack). ARP spoofing can also be used in a man-in-the-middle attack, in which all traffic is forwarded through a host by means of ARP spoofing and analyzed for passwords and other information.

ARP Spoofing and Poisoning Countermeasures

To prevent ARP spoofing, permanently add the MAC address of the gateway to the ARP cache on a system. You can do this on a Windows system by using the ARP -s command at the command line and appending the gateway's IP and MAC addresses. Doing so prevents a hacker from overwriting the ARP cache to perform ARP spoofing on the system but can be difficult to manage in a large environment because of the number of systems. In an enterprise environment, port-based security can be enabled on a switch to allow only one MAC address per switch port.

Understanding MAC Flooding and DNS Spoofing

A packet sniffer on a switched network can't capture all traffic as it can on a hub network; instead, it captures traffic either coming from or going to the system. It's necessary to use an additional tool to capture all traffic on a switched network. There are essentially two ways to perform active sniffing and make the switch send traffic to the system running the sniffer:

ARP Spoofing This method involves using the MAC address of the network gateway and consequently receiving all traffic intended for the gateway on the sniffer system. A hacker can also *flood* a switch with so much traffic that it stops operating as a switch and instead reverts to acting as a hub, sending all traffic to all ports. This active sniffing attack allows the system with the sniffer to capture all traffic on the network.

DNS Spoofing (or DNS Poisoning) This is a technique that tricks a DNS server into believing it has received authentic information when in reality it hasn't. Once the DNS server has been poisoned, the information is generally cached for a while, spreading the effect of the attack to the users of the server. When a user requests a certain website URL, the address is looked up on a DNS server to find the corresponding IP address. If the DNS server has been compromised, the user is redirected to a website other than the one that was requested, such as a fake website.

To perform a DNS attack, the attacker exploits a flaw in the DNS server software that can make it accept incorrect information. If the server doesn't correctly validate DNS responses to ensure that they come from an authoritative source, the server ends up caching the incorrect entries locally and serving them to users that make subsequent requests.

This technique can be used to replace arbitrary content for a set of victims with content of an attacker's choosing. For example, an attacker poisons the IP address's DNS entries for a target website on a given DNS server, replacing them with the IP address of a server the hacker controls. The hacker then creates fake entries for files on this server with names matching those on the target server. These files may contain malicious content, such as a worm or a virus. A user whose computer has referenced the poisoned DNS server is tricked into thinking the content comes from the target server and unknowingly downloads malicious content.

The types of DNS spoofing techniques are as follows:

Intranet Spoofing Acting as a device on the same internal network

Internet Spoofing Acting as a device on the Internet

Proxy Server DNS Poisoning Modifying the DNS entries on a proxy server so the user is redirected to a different host system

DNS Cache Poisoning Modifying the DNS entries on any system so the user is redirected to a different host