# Unit-6 Types of Hacking

**Contents**

**6.1 Network Hacking**

- Network Infrastructure
- Network Infrastructure vulnerabilities
- Scanning-Ports
- Ping sweeping
- Scanning SNMP
- Grabbing Banners
- Analysing Network Data and Network Analyzer
- MAC-daddy attack

**Wireless LANs:**

- Implications of Wireless Network Vulnerabilities
- Wireless Network Attacks

**6.2 Operating System Hacking**

- Introduction of Windows and Linux Vulnerabilities

**6.3 Applications Hacking**

**Messaging Systems**

- Vulnerabilities,
- E-Mail Attacks- E-Mail Bombs,
- Banners,
- Best practices for minimizing e-mail security risks

**Web Applications:**

- Web Vulnerabilities,
- Directories Traversal and Countermeasures,

**Database System**

- Database Vulnerabilities
- Best practices for minimizing database security risks

## 6.1 Network Hacking

- Computer Network is one of the most fundamental communications systems in your organization. Network consists of such devices as routers, firewalls, and even generic hosts (including servers and workstations) that you must assess as part of the ethical hacking process.

- There are thousands of possible network vulnerabilities, equally as many tools, and even more testing techniques. We don’t need to test our network for every possible vulnerability, using every tool available.
- We can eliminate many well-known network vulnerabilities by simply patch-ing your network hosts with the latest vendor software and firmware patches. We can eliminate many other vulnerabilities by following some security best practices on our network.

### 6.1.2 Network Infrastructure Vulnerabilities

- Network infrastructure vulnerabilities are the foundation for all technical security issues in your information systems. These lower-level vulnerabilities affect everything running on your network. That’s why you need to test for them and eliminate them whenever possible.
- Your focus for ethical hacking tests on your network infrastructure should be to find weaknesses that others can see in your network so you can quantify your level of exposure.
- Many issues are related to the security of your network infrastructure. Some issues are more technical and require you to use various tools to access them properly. You can access others with a good pair of eyes and some logical thinking. Some issues are easy to see from outside the network, and others are easier to detect from inside your network.
- Network infrastructure security involves accessing such areas as
  - ✓ Where such devices as a firewall or IDS (Intrusion Detection System) are placed on the network and how they are configured.
  - ✓ What hackers see when they performed port scans and how they can exploit vulnerabilities in your network hosts.
  - ✓ Network design, such as internet connections, remote-access capabilities, layered defences, and placements of hosts on the network.
  - ✓ Interaction of installed security devices
  - ✓ Protocols in use.
  - ✓ Commonly attacked ports that are unprotected.
  - ✓ Network hosts configuration.
  - ✓ Network monitoring and maintenance.
- If any of these network security issue is exploited, such things can happen:
  - ✓ A DoS attack can take down your internet connection or even your entire network.
  - ✓ A hacker using a network analyser can steal confidential information in e-mails and files being transferred.
  - ✓ Backdoors into your network can be setup.
  - ✓ Specific hosts can be attacked by exploiting local vulnerabilities across the network.
- Always remember to do the following:
  - ✓ Test your systems from both the outside in and the inside out.
  - ✓ Obtain permission from partner networks that are connected to your network to check for vulnerabilities on their ends that can affect your network’s security, such as open ports and lack of a firewall or a misconfigured router.

**Network Testing and port scanning tools:**

- **Sam Spade** for windows for network queries from DNS lookups to trace routes.
- **SuperScan** for ping sweeps and port scanning
- **NetScan**Tools Pro for dozens of network security-assessment functions, including ping sweeps, port scanning, and SMTP relay testing.
- **Nmap or NMapWin** as a happy-clicky-GUI front end for host-port probing and operating-system fingerprinting.
- **Netcat** the most versatile security tool for such security checks as port scanning and firewall testing.
- **WildPacketsEtherPeek** for network analysis.

### 6.1.3 Scanning-Ports

- A port scanner is a software tool that basically scans the network to see who's there. Port scanners provide basic views of how the network is laid out. They can help identify unauthorized hosts or applications and network host configuration errors that can cause serious security vulnerabilities.
- The big-picture view from port scanners often uncovers security issues that may otherwise unnoticed. Port scanners are easy to use and can test systems regardless of what operating systems and applications they're running. The tests can be performed very quickly without having to touch individual network hosts, which would be a real pain otherwise.
- Port-scan tests take time. The length of time depends on the number of hosts you have, the number of ports you scan, the tools you see, and the speed of your network links. Also, perform the same tests with the different utilities to see whether you get different results. Not all tools find the same open ports and vulnerabilities. This is unfortunate, but it's a reality of ethical hacking tests.
- If your results don't match after you run the tests using different tools, you may want to explore the issue further. If something doesn't look right such as a strange set of open ports it probably isn't. Test it again; if you're in doubt, use another tool for a different perspective.
- As an ethical hacker, you should scan all 65,535 UDP and 65,535 TCP ports on each network host that's found by your scanner. If you find questionable ports, look for documentation that the application is known and authorized. For speed and simplicity , you can scan commonly hacked ports.

**Table 6.1: Commonly hacked ports**

| Port Nos. | Service | Protocols |
|---|---|---|
| 7 | Echo | TCP, UDP |
| 19 | Chargen | TCP, UDP |
| 20 | FTP data(File Transfer Protocol) | TCP |

| | | |
|---|---|---|
| 21 | FTP control | TCP |
| 22 | SSH | TCP |
| 23 | Telnet | TCP |
| 25 | SMTP(Simple Mail Transfer Protocol) | TCP |
| 37 | Daytime | TCP, UDP |
| 53 | DNS (Domain Name System) | UDP |
| 69 | TFTP (Trivial File Transfer Protocol) | UDP |
| 79 | Finger | TCP, UDP |
| 80 | HTTP (Hypertext Transfer Protocol) | TCP |
| 110 | POP3 (Post Office Protocol version 3) | TCP |
| 111 | SUN RPC (remote procedure calls) | TCP, UDP |
| 135 | RPC/DCE end point mapper for Microsoft networks | TCP, UDP |
| 137, 138,139 | NetBIOS over TCP/IP | TCP, UDP |
| 161 | SNMP (Simple Network Management Protocol) | TCP, UDP |
| 220 | IMAP (Internet Message Access Protocol) | TCP |
| 443 | HTTPS (HTTP over SSL) | TCP |
| 512, 513,514 | Berkeley r commands<br>(such as rsh, rexec, and rlogin) | TCP |
| 1214 | Kazaa and Morpheus | TCP, UDP |
| 1433 | Microsoft SQL Server | TCP, UDP |
| 1434 | Microsoft SQL Monitor | TCP, UDP |
| 3389 | Windows Terminal Server | TCP |
| 5631, 5632 | pcAnywhere | TCP |
| 6346, 6347 | Gnutella | TCP, UDP |
| 12345, 12346, 12631, 12632, 20034, 20035 | NetBus | TCP |
| 27444 | Trinoo | UDP |
| 27665 | Trinoo | TCP |
| 31335 | Trinoo | UDP |

| | | |
|---|---|---|
| 31337 | Back Office | UDP |
| 34555 | Trinoo | UDP |

Counter Measures (Port Scanning)

- You can implement various counter measures to typical port scanning.

✓ Traffic Restriction

- Enable only the traffic you need to access internal hosts preferably as far as possible from the hosts you're trying to protect. You apply these rules in two places: External router for inbound traffic & Firewall for outbound traffic.
- Configure firewalls to look for potentially malicious behaviour over time (such as the number of packets received in a certain period of time), and have rules in place to cut off attacks if a certain threshold is reached, such as 100 port scans in one minute. Most firewalls, IDSs, and IDPs detect port scanning and cut it off in real time.

✓ Gathering network information

- NetScanTools Pro is a great tool for general network information, such as the number of unique IP addresses, NetBIOS names, and MAC addresses found.
- The following report is an example of the NetScanner (network scanner) output of NetScanTools Pro 2000:
- Scan completion time = Sat, 7 Feb 2004 14:11:08
- Start IP address:192.168.1.1
- End IP address: 192.168.1.254
- Number of target IP addresses: 254
- Number of IP addresses responding to pings: 13
- Number of IP addresses sent pings: 254
- Number of intermediate routers responding to pings: 0
- Number of successful NetBIOS queries: 13
- Number of IP addresses sent NetBIOS queries: 254
- Number of MAC addresses obtained by NetBIOS queries: 13
- Number of successful Subnet Mask queries: 0
- Number of IP addresses sent Subnet Mask queries:254
- Number of successful Whois queries: 254

✓ Traffic denial

- Deny ICMP traffic to specific host's you're trying to protect. Most hosts don't need to have ICMP enabled especially inbound ICMP requests unless it's needed for a network management system that monitors hosts using this protocol.
- You can break applications on your network, so make sure that you analyze what's going on, and understand how applications and protocols are working, before you disable such network traffic as ICMP.

### 6.1.4 Ping sweeping

- Port sweeping is regarded by certain systems experts to be different from port scanning.
- They point out that port scanning is executed through the searching of a single host for open ports. However, they state that port sweeping is executed through the searching of multiple hosts in order to target just one specific open port.
- While Port scanning and sweeping have legitimate uses with regard to network management, unfortunately,they are used almost as frequently for the purpose of criminal activity.

**A Serious Threat**

- Any times there are open ports on one's personal computer, there is potential for the loss of data, the occurrence of a virus, and at times, even complete system compromise.
- It is essential for one to protect his or her virtual files, as new security risks concerning personal computers are discovered every day.
- Computer protection should be the number one priority for those who use personal computers.
- Port scanning is considered a series threat to one's PC, as it can occur without producing any outward signs to the owner that anything dangerous is taking place.

**Firewall Protection**

- Protection from port scanning is often achieved through the use of a firewall. A firewall monitors incoming and outgoing connections through one's personal computer.
- One technique used by firewall technology is the opening of all the ports at one time. This action stops port scans from returning any ports. This has worked in many situations in the past, however, most experts agree it is best to have all open ports investigated individually.
- Another approach is to filter all port scans going to one's computer. An individual can also choose to port scan his or her own system, which enables one to see the personal computer through the eyes of the hacker.
- Firewalls are the best protection one can invest in with regard to port scanning. Firewalls deny outside access to an individual's personal computer. With this type of protection, a personal computer is essentially hidden from unwelcome visitors and is also protected from a variety of other hacking techniques. With firewall software, an individual is assured that his or her sensitive and personal information remains protected.

- A ping sweep of all your network subnets and hosts is a good way to find out which hosts are alive and kicking on the network.
- A ping sweep is when you ping a range of addresses using Internet Control Message Protocol (ICMP) packets.
- Dozens of Nmap command-line options exist, which can be overwhelming when you just want to do a basic scan.
- You can just enter nmap on the command line to see all the options available.

- These command-line options can be used for an Nmap ping sweep:
  - sP tells Nmap to perform a ping scan.
  - ntellsNmap to not perform name resolution. You may want to omit this if you want to resolve hostnames to see which systems are responding. Name resolution may take slightly longer, tough.
  - -T 4 option tells Nmap to perform an aggressive (faster) scan.
  - 192.168.1.1-254 tells Nmap to scan the entire 192.168.1.x subnet.

### 6.1.5 SNMP (Simple Network Management Protocol) scanning

- Networks are the backbone of every business. Even in small or enterprise-level businesses, the loss of productivity during a network outage can result in hefty damages.
- Network monitoring helps you anticipate potential outages and address network problems proactively. This helps in maintaining a congestion-free network that keeps your business up and running.
- A network monitoring software helps you to monitor the performance of any IP-based device and helps businesses remotely visualize their system performance and monitor network services, bandwidth utilization, switches, routers and traffic flow.

**Vulnerabilities (SNMP)**

- The problem is that most network hosts run SNMP that isn't hardened or patched to prevent known security vulnerabilities. The majority of network devices have SNMP enabled and don't even need it.
- If SNMP is compromised, a hacker can gather such network information as ARP tables and TCP connections to attack your systems. If SNMP shows up in port scans, you can bet that a hacker will try to compromise the system.

**Countermeasures (SNMP)**

- Preventing SNMP attacks can be as simple as A-B-C:
- Always disable SNMP on hosts if you’re not using it period.
- Block the SNMP port (UDP port 161) at the network perimeter.
- Change the default SNMP community string using from public to another value that’s more difficult to guess. This makes SNMP harder to hack.

### 6.1.6 Banner Grabbing

- Banner Grabbing is the act of capturing the information provided by banners, configurable text-based welcome screens from network hosts that generally display system information. Banners are intended for network administration.
- Banner grabbing is often used for White Hat Hacking endeavors like vulnerability analysis and penetration testing as well as gray hat activities and black hat hacking. Banners screen can be accessed through telnet at the command prompt on the target system’s IP address.
- Other tools for banner grabbing include Nmap, Netcat, and SuperScan. A login screen, often associated with the banner, is intended for administrative use but can also provide access to hacker. Meanwhile, the banner data can yield information about velnerable software and services running on the host systems.

- For the sake of security, if banners are not a requirement of business or other software on a host system, the services that provide them may be disabled altogether. Banners scan can also be customized to present disinformation or even a warning message for hackers.
- Banners are the welcome screen that divulge software version numbers and other hosts information to a network hosts. This banner information may identify the operating system, the version number, and the specific service packs, so hackers know possible vulnerabilities. You can grab banners by using either plain old telnet or Netcat.
- Telnet

✓ You can telnet to hosts on the default telnet port (TCP port 23) to see whether you are presented with a login prompt or any other information.

✓ Just enter the following line at the command prompt in windows and unix:

✓ telnet ip_address

- Netcat

✓ Netcat can grab banners information from router and other network hosts such as, a wireless access point or managed Ethernet switch.

- Counter Measures (Banner Grabbing)

✓ The following steps can reduce the chance of banner-grabbing attacks:

- If there is no business need for services that offer banner information, disable those unused services on the network host.
- If there is no business need for the default banners, or if you can customized the banners displayed, configure the network host’s application or operating system to either disable the banners or remove information from the banners that could give an attacker a leg upn.

### 6.1.7 Analysing Network Data and Network Analyzer

- A network analyzer is a tool that allows you to look into a network and analyse data going across the wire for network optimization, security, and/or troubleshooting purposes. Like a microscope for a lab scientist, a network analyser is a must-have tool for any security professional.
- Network analyzers are often generically referred to as sniffers, though that’s actually the name and trademark of specific product from Network Associates, Sniffers (the original network-analysis tool).
- When assessing security and responding to security incidents, a network analyser can help you.
    - ✓ View anomalous network traffic and even track down an intruder.
    - ✓ Develop a baseline of network activity and performance before a security incident occurs, such as protocols in use, usage trends, and MAC addresses.
- A Network analyser is just software running on a computer with a network card. It works by placing the network card in promiscuous mode, which enables the card to see all the traffic on a network, even traffic not destined to the network-analyser host.
- The network analyser performs the following functions:
    - ✓ Capture all network traffic.
    - ✓ Interprets or decode what is found into a human-readable format.
    - ✓ Displays it all in chronological order.
- Here are a few caveats for using a network analyser:

- ✓ To capture all traffic, you must connect the analyser to either a hub on the network.
- ✓ A monitor/span/mirror port on a switch
- ✓ What's entering your network before the firewall filters eliminates the junk traffic.
- ✓ What's leaving your network after the traffic goes past the firewall.

- When your network behaves erratically, a network analyser can help you in
  - ✓ Track and isolate malicious network usage.
  - ✓ Detect malicious Trojan-horse applications.
  - ✓ Monitor and track downs DoS attacks.
- Different network analysing tools are:

| Sr No. | Name of Network Analyser | Supporting Operating System |
|---|---|---|
| 1 | EtherPeek by WildPackets | Windows |
| 2 | Ethereal | Windows and Unix |
| 3 | Ettercap | Windows and Unix |
| 4 | Dsniff | Unix |

Counter measures (Network Analyser)

A network analyser can be used for good or evil. All these tests can be used against you, too. A few counter measures can help prevent someone from using an unauthorized network analyser, but there is no way to completely prevent it.

- ✓ Physical Security
  - Ensure that adequate physical security is in place to prevent a hacker from plugging into your network.
  - Keep the bad guys out off your server room and closet.
  - A special monitor port on a switch where a hacker can plug in a network analyser is especially sensitive. Make sure it's extra secure.
  - Make sure that such unsupervised areas as unoccupied desks don't have live network connections.
- ✓ Network-Analyser Detection

- You can use a network-or host-based utility to determine if someone is running an unauthorised network analyser on your network.
- Some network analyser detection tools are sniffdet, PromiscDetect. These tools enable us to monitor the networks for Ethernet cards that are running in promiscuous mode.

### 6.1.8 The MAC-daddy attack

- Hackers can use ARP protocol that is running on the network to make their systems seem as your system or another allowed host on your network.
- A too much number of ARP (Address Resolution Protocol) requests can be a sign of an ARP poisoning or spoofing attack on your network. Anyone can run a program, such as dsniff tool or Cain & Abel tool, can modify the ARP tables, which are responsible for saving IP addresses to media access control (MAC) address mappings on network hosts.
- That makes the victim machines to think they require to forward traffic to the hacker's computer rather than to the correct destination machine when communicating on the

network. And this is a type of man-in-the-middle (MITM) attacks. Spoofed ARP responses can be sent to a switch, which returns the switch to broadcast mode and basically turns it into a hub. When this happens, a hacker can sniff every packet going through the switch and capture anything and everything from the network.

**ARP spoofing**

- ✓ An expensive amount of ARP requests can be a sign of an ARP poisoning attack (or ARP spoofing) on your network.
- ✓ What happens is that a client running a program such as the UNIX-based dsniff or the UNIX- and DOS/Windows –based Ettercap can change the ARP tables the tables that store IP addresses to media access control (MAC) mappings on network hosts.
- ✓ This causes the victim computers to think they need to send traffic to the attacker's computer, rather than the true destination computer, when communicating on the network. This is often referred to as a Man-in-the-Middle (MITM) attack.

**MAC-address spoofing**

- ✓ MAC-address spoofing tricks the switch into thinking you (actually, your computer) are someone else. You simply change your MAC address and masquerade as another user.
- ✓ You can use this trick to test such access controls that check for specific MAC addresses.

**Countermeasures (MAC- daddy attack)**

- ✓ A few countermeasures on your network can minimize the effects of a hacker attack against ARP and MAC addresses on your network.

- You can prevent MAC-address spoofing if your switches can enable port security to prevent automatic changes to the switch MAC address tables.
- No realistic countermeasures for ARP poisoning exist. The only way to prevent ARP poisoning is to create and maintain static ARP entries in your switches for every host on the network. This is definitely something that no network administrator has time to do.

**Detection**

- ✓ You can detect these two types of hacks through either an IDS or a stand-alone MAC address monitoring utility.
- ✓ Arp watch is a UNIX-based program alerts you via e-mail if it detects changes in MAC addresses associated with specific IP addresses on the network.

**Wireless LAN**

- A wireless LAN (or WLAN) is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection. The IEEE 802.11 group of standards specify the technologies for wireless LANs 802.11 standards use the Ethernet Protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing and include an encryption method, the Wire Equivalent Privacy algorithm.

- Implications of Wireless Network Vulnerabilities

✓ WLANs are very susceptible to hacker attacks even more so than wired networks are.

✓ They have vulnerabilities that can allow a hacker to bring your network to its knees and allow your information to be gleaned right out of thin air.

✓ If a hacker comprises your WLAN, you can experience the following problems:

1. Loss of network access, including e-mail, Web, and other services that can cause business downtime.
2. Loss of confidential information, including passwords, customer data, intellectual property, and more.
3. Legal liabilities associated with unauthorized users.

- Most of the wireless vulnerabilities are in the 802.11 protocol and within wireless access points the central hub like devices that allow wireless clients to connect to the network. Wireless clients have some vulnerability as well.
- Various fixes have come along in recent years to address these vulnerabilities, but most of these fixes have not been applied or are not enabled by default.
- You may also have employees installing rogue WLAN equipment on your network without your knowledge; this is the most serious threat to your wireless security and a difficult one to fight off, Even when WLANs are hardened and all the latest patches have been applied, you still may have some serious security problems, such as DoS and man-in-the-middle attacks (like you have on wired networks), that will likely be around for a while.
- Common Wireless Threats
  - There are a number of main threats that exists to wireless LANs, this include:

✓ Rogue access Points/Ad-Hoc Networks

✓ Denial of Service

✓ Configuration problems (Mis Configurations/Incomplete Configurations )

✓ Passive Capturing

**Wireless Network Attacks**

- Wi-Fi networks can be vulnerable to a variety of difficult attacks. Because of this, it’s important to be aware of them so you can take the necessary steps to prevent and reduce their impact.
- Different kinds of attacks are Encrypted traffic, Rogue networks, Physical security problems, vulnerable wireless workstations, Default configuration settings.

✓ **Encrypted traffic**

- Wireless traffic can be captured directly out of the airwaves, making this communications medium susceptible to malicious eavesdropping.

- Unless the traffic is encrypted, it’s sent and received in clear text just like on a standard wired network.
- On top of that, the 802.11 encryption protocol, Wired Equivalent Privacy (WEP), has its own weakness that allows hackers to crack the encryption keys and decrypt the captured traffic.

✓ **Rogue Networks**

- Watch out for unauthorized Access Points and wireless clients attached to your network that are running in ad-hoc mode.
- Using NetStumbler or your client manager software, you can test for Access Points that don’t belong on your network.
- You can also use the network monitoring features in a WLAN analyzer such as AiroPeek.
- Walk around your building or campus to perform this test to see what you can find.
- Physically look for devices that don’t belong a well-placed Access Point or WLAN client that’s turned off won’t show up in your network analysis tools.
- Search near the outskirts of the building or near any publicly accessible areas.
- Scope out boardrooms and the offices of upper level managers for any unauthorized devices. These are places that are typically off limits but often are used as locations for hackers to set up rogue Access Points.

✓ **Physical-security problems**

- Various physical-security vulnerabilities can result in physical theft, the reconfiguration of wireless devices, and the capturing of confidential information.
- You should look for the security vulnerabilities when testing your systems such as Access Points mounted on the outside of a building and accessible to the public, Poorly mounted antennas or the wrong types of antennas that broadcast too strong a signal and that are accessible to the public.
- You can view the signal strength in NetStumbler or your wireless client manager.

✓ **Vulnerable wireless workstations**

- Wireless workstations have tons of security vulnerabilities from weak passwords to unpatched security holes to the storage of WEP (Wired Equivalent Privacy) leys locally.
- One serious vulnerability is for wireless clients using the Orinoco wireless card.
- The Orinoco Client Manager software stores encrypted WEP keys in the Windows Registry even for multiple networks.

✓ **Default configuration settings**

- Similar wireless workstations, wireless Access Points have many known vulnerabilities.
- The most common ones are default SSIDs(Service Set Identifier) and admin passwords. The more specific ones occurs only on certain hardware and software versions that are posted in vulnerability databases and vendor Web sites.
- The one vulnerability that stands out above all others is that certain Access Points, including Linksys, D-Link and more, are susceptible to a vulnerability that exposes and WEP key(s), MAC (Media Access Control) address filters, and even the admin password! All that hackers have to do to exploit this is to send a broadcast packet on UDP port 27155 with a string of gstsearch.

## 6.2 Operating System hacking

- An operating system is a program that acts as an interface between the software and the computer hardware. It is an integrated set of specialized programs used to manage overall resources and operations of the computer. It is specialized software that controls and monitors the execution of all other programs that reside in the computer, including application programs and other system software. Many operating systems are available now days.
- Many securities flaws in the headlines aren't new. They're variants of vulnerabilities that have been around for a long time in UNIX and LINUX, such as the Remote Procedure Call vulnerabilities that the Blaster worm used.
- You've heard the saying "the more things change, the more they stay the same."
- That applies here, too
- Most Windows attacks are prevented if the patches were properly applied. Thus, poor security management is often the real reason.

### Windows

- ✓ The Microsoft Windows OS is the most widely used OS in the world.
- ✓ It's also the most widely hacked, because Microsoft doesn't care as much about security as other OS versions? The answer is no. Numbers security mistakes were unnoticed especially in the Windows NT days but because Microsoft products are so pervasive through networks. Microsoft is the easiest vendor to pick on, and often its Microsoft products that end up in the crosshairs of hackers. This is the same reason for many vulnerability alerts on Microsoft products. The one positive about hackers is that they're driving the requirement for better security!
- ✓ There are variants of vulnerabilities that have been around for a long time in UNIX and Linux, such as the RPC vulnerabilities that the Blaster worm used. Most Windows attacks are prevented if the patches were properly applied. Thus, poor security management is often the real reason Windows attacks are successful
  - Much vulnerability have been published for windows operating system.
  - Some of the common vulnerabilities found in all versions of windows are: DoS, Remote Code Execution, Memory Corruption, Overflow, Sql Injection, XSS, Http Response Splitting, Directory Traversal, Bypass something Gain Information/Privileges, CSRF File Inclusion etc.
  - The maximum number of vulnerabilities detected were of Gaining Privileges by which the confidentiality and integrity was highly impacted.
- **Windows Vulnerabilities**
  - ✓ Due to the ease of use of Windows, many organizations have moved to the Microsoft platform for their networking needs.
  - ✓ Many businesses especially the small to medium sized ones depend solely on the Windows OS for networks usage.
  - ✓ Many large organizations run critical servers such as Web servers and Database servers on the Windows platform.

- ✓ If security vulnerabilities aren't addressed and managed properly, they can bring a network or an entire organization to its knees.
- ✓ When Windows and other Microsoft software are attacked especially by a widespread internet-based worm or virus hundreds of thousands of organizations and millions of computers are affected.
- ✓ Many **well-known attacks against Windows** can lead to.

- Leakage of confidential information, including files being copied and credit card numbers being stolen.
- Passwords being cracked and used to carry out other attacks.
- Systems taken completely offline by DoS attacks.
- Entire databases being corrupted or deleted when insecure Windows-based systems are attacked, serious things can happen to a tremendous number of computers around the world.
- Autoplay feature came in Windows XP. This feature checks removable media/devices then identifies and launches appropriate application based on its contents. This feature is useful for authentic users but is a gateway for an attacker.
- Clipboard vulnerability can allow attacker to get access to the sensitive clipboard data. In windows clipboard is common for all applications. This may lead to access and modification in the clipboard of all applications in the operating system.
- MS-Windows stores its configuration settings and options in a hierarchical database which is known as windows Registry. Registry is used for low level operating system setting and for settings of applications running on the platform.

- **LINUX**
  - ✓ It is the latest flavour of UNIX that has really taken off in corporate networks.
  - ✓ It is the competitor Operating System for Microsoft.
  - ✓ A common misunderstanding is that Windows is the most insecure operating system. However, Linux and most of its sister variant of UNIX are prone to the same security vulnerabilities as any other operating system.
  - ✓ Hackers are attacking Linux because of its popularity and growing usage in today's network environment, because some versions of Linux are free.
  - ✓ Many organizations are installing Linux for their Web servers and e-mail servers in expectations of saving money.
  - ✓ Linux has grown in popularity for other reasons, including the following:

- Ample resources available, including books, Web sites, and consultant expertise.
- Perception that Linux is more secure than Windows.
- Unlikeliness that Linux will get hit with as many viruses (not necessarily worms) as Windows and its applications do. This is an area where Linux excels when it comes to security, but it probably won't stay that way.
- Increased buy-in from other UNIX vendors, including IBM and Sun Micro systems.
- Growing ease of use.

- **Linux Vulnerabilities**

- ✓ Vulnerabilities and hacker attacks against Linux are affecting a growing number of organizations especially e-commerce companies and ISPs that rely on Linux for many of their systems.
- ✓ When Linux systems are hacked, the victim organizations can experience the same side effects as if they were running Windows, including:
  - Leakage of confidential intellectual property and customer information.
  - Passwords being cracked.
  - Systems taken completely offline by DoS attacks.
  - Corrupted or deleted databases.

## 6.3 Applications Hacking:-

### 6.3.1 Messaging System

Messaging System Messaging systems are those e-mail and instant messaging (IM) applications that we depend on are often hacked within a network. Why? Because messaging software both at the server and client level is vulnerable because network administrators forget about securing these systems, believe that antivirus software is all that's needed to keep trouble away, and ignore the existing security vulnerabilities.

**• Messaging system Vulnerabilities**

- ✓ E-mail and instant-messaging applications are hacking targets on your network.
- ✓ In fact, e-mail systems are some of the most targeted.
- ✓ A ton of vulnerabilities are inherent in messaging systems
- ✓ The following factors can create weaknesses:
  - Security is rarely integrated into software development.
  - Convenience and usability often outweigh the need for security.
  - Many of the messaging protocols were not designed with security in mind.
  - Especially those developed several decades ago, when security wasn't nearly the issue it is today.
- ✓ Many hacker attacks against messaging systems are just minor nuisances. Others can inflict serious harm on your information and your organization's reputation. The hacker attacks against messaging systems include these:
  - Transmitting malware
  - Crashing servers
  - Obtaining remote control of workstations
  - Capturing and modifying confidential information as it traveis across the network
  - Perusing e-mails in e-mail databases on servers and workstations

  - Perusing instant-messaging log files on workstation hard drives
  - Gathering messaging trend information, via log files or network analyzer, that can tip off the hacker about conversations between people and organizations
  - Gathering internal network configuration information, such as hostname and IP addresses

- ✓ Hacker attacks like these can lead to such problems as lost business, unauthorized and potentially illegal disclosure of confidential information and loss of information.

**Email Attacks**

- Many people rely on the Internet for many of their professional, social and personal activities. But there are also people, who attempt to damage our Internet-connected computers, violate our privacy and render inoperable the internet services
- Email is a universal service used by number of people worldwide. As one of the most popular services, email has become a major vulnerability to users and organizations.
- The following e-mail attacks use the most common e-mail security vulnerabilities. Some of these attacks require the basic hacking methodologies, gathering public information, scanning and enumerating your systems, and attacking. Others can he carried out by sending e-mails or capturing network traffic.
- Different email attacks are email bomb, banner etc.
- **Email Bombs**
  - ✓ E-mail bombs can crash a server and provide unauthorized administrator access.
  - ✓ They attack by creating DoS conditions against your e-mail software and even your network and internet connection by taking up so much bandwidth and requiring so much storage space.
  - ✓ An email bomb is a form of Internet abuse which is perpetrated through the sending of massive volumes of email to a specific email address with the goal of overflowing the mailbox and overwhelming the mail server hosting the address, making it into some form of denial of service attack.
  - ✓ An email bomb is also known as a letter bomb.
  - ✓ Different email bomb attacks are as attachment overloading attack, connection attack, autoresponder attack.

1. **Attachment Overloading Attack**
   - An attacker can create an attachment-Overloading attack by sending hundreds or thousands of emails with very large attachments.
   - Attachment overloading attacks may have a couple of different goals
   - The whole email server may be targeted for a complete interruption of service with these features like storage overload and bandwidth blocking.

A. **Storage Overload**

- Multiple large messages can quickly fill the total storage capacity of an email server. If the messages aren't automatically deleted by the server or manually deleted by individual user accounts, the server will be unable to receive new messages.
- This can create a serious DOS problem for your email system, either crashing it or requiring you take your email system of line to clean up the junk that has accumulated. Eg. 100 MB file attachment sent 10 times to 80 users can take 80GB of storage space.

B. **Bandwidth Blocking**

- An attacker can crash your email service or bring it to a crawl by filling the incoming internet connections with junk. Even if your system automatically identifies and discards obvious attachments attacks, the bogus messages eat resources and delay processing of valid messages.

**Counter Measures (Attachment-Overloading Attack)**

These countermeasures can help prevent attachment-overloading attacks:

- Limit the size of either e-mails or e-mail attachment. Check for this options in e-mail server configuration options, e-mail content filtering, and e-mail clients. This is the best protection against attachment overloading.
- Limit each user's on the server. This denies large attachments from being written to disk. Limit message sizes for inbound and even outbound messages if you want to prevent a user from launching this attack inside your network.

2. **Connection Attack**

✓ A hacker can send a huge amount of e-mails simultaneously to addresses on your network.
✓ These connection attacks can cause the server to give up on servicing any inbound or outbound TCP requests.
✓ This can lead to a complete server lockup or a crash, often resulting in a condition where the attacker is allowed administrator or root access to the system!
✓ This attack is often carried out as spam attack.

**Countermeasures (Connection Attacks)**

✓ Many e-mail servers allow you to limit the number of resources used for inbound connections.
✓ It can be impossible to completely stop an unlimited amount of inbound requests.
✓ However, you can minimize the impact of the attack. This setting limits the amount of server processor time, which can help prevent a DoS attack.
✓ Even in large companies, there's no reason that thousands of inbound e-mail delivers should be necessary within a short time period.

3. **Autoresponders Attack**

- ✓ This is an interesting attack to find two or more users on the same or different e-mail systems that have autoresponder configured.
- ✓ Autoresponder is that annoying automatic e-mail response you often get back from random users when you are subscribing to mailing list.
- ✓ A message goes to the mailing list of subscribers and then users have their e-mail configured to automatically respond back, saying they're out of the office or, on vacation.
- ✓ An autoresponder attack is a pretty easy hack.
- ✓ Many unsuspecting users and e-mail administrators never know what hit them!
- ✓ The hacker sends each of the two (or more) users an e-mail from the simply by masquerading as that
- ✓ This attack can create a never-ending loop that bounces thousands of messages back and forth between users.
- ✓ This can create a DoS condition by filling either the user's individual disks space quota on the e-mail server or the e-mail server's entire disk space.

**Countermeasures (Autoresponder Attack)**

- ✓ The best countermeasure for an autoresponder attack is to make policy that no one sets up an autoresponder message.
- ✓ Prevent e-mail attacks as far considering perimeter of your network.
- ✓ The more traffic or malicious behavior you keep off, your e-mail servers and clients are better.

- **Banners**
  - ✓ One of the first orders of business for a hacker when hacking an e-mail server is performing a basic banner grab to see whether he can tell that e-mail server Software is running.
  - ✓ This is one of the most critical tests to find out what the World knows about your SMTP, POP3, and IMAP servers.
  - ✓ Gathering Information
  - When a basic telnet connection is made on port 25 (SMTP) banner displayed on an e-mail server.
  - To do this, at a command prompt, simply enter telnet IP or hostname.
  - From that we get what e-mail software type and version of the server is running. This information can give hackers some ideas about possible attacks, especially if they search a vulnerability database for known vulnerabilities of that software version.
  - If you've changed your default SMTP banner, don't think that no one can figure out the version.
  - One Linux-based tool called smtpscan determines e-mail server version information based on how the server responds to malformed SMTP requests.

**Countermeasures (Banners)**

There is not a 100 percent secure way of disguising banner information.

Following are some banner security tips for SMTP, POP3, and IMAP servers:

- Change your default banners to cover up the information.
- Make sure that you're always running the latest software patches.
- Harden your server as much as possible by using well-known best practices

**General Best Practices for minimizing email security risk**

The following countermeasure helps to keep email messages as secure as possible:-

- ✓ Use of right software can neutralize many threats such as – Use malware protection software on the e-mail server better, Apply the latest operating system and e-mail application security patches consistently.
- ✓ Use of encrypted messages or messaging system.
- ✓ Put your e-mail server behind a firewall, preferably in a DMZ that's on a different network segment from the internet and from your internal LAN.
- ✓ Disable unused protocols and services on your e-mail server.
- ✓ Run your e-mail server on a dedicated server, if possible, to help keep hackers out of other servers and information if the server is hacked.
- ✓ Log all transactions with the server in case you need to investigate malicious use in the future.
- ✓ If your server doesn't need e-mail services running (SMTP, POP3, and IMAP) disable them immediately.
- ✓ Email monitoring can detect and block messages sent from compromised accounts.
- ✓ Email filtering can block certain types of attacks that are known to carry malicious content.
- ✓ Secure email client configurations can also reduce the risk of malicious email.
- ✓ Checking to see if the email address of a questionable message matches the reply-to email address.
- ✓ Verifying that URLs in an email go to legitimate websites.

### 6.3.2 Web Applications

- Web applications, like e-mail are common hacker targets because they are everywhere and often open for anyone to poke around in.
- Basic Web sites used for marketing, contact information, document downloads and so on are a common target for hackers especially the script-kiddie's types to deface.
- However, for criminal hackers, Web sites that store valuable information, like credit-card and Social Security numbers, are especially attractive.
- Why are Web applications so vulnerable? The general consent is they're vulnerable because of poor software development and testing practices. Sound familiar? It should, because this is the name problem that affects operating systems and practically all computer systems.

- This is the side effect of relaying on software compilers to perform error checking, lack of user demand for higher-quality software and emphasizing time-to-market instead of security and stability.
- **Web application Vulnerabilities**

✓ Hacker attacks against insecure Web applications via Hypertext Transfer Protocol (HTTP) make up the majority of all Internet-related attacks.

✓ Most of these attacks can be carried out even if the HTTP traffic is encrypted (via HTTPS or HTTP over SSL) because the communications medium has nothing to do with these attacks.

✓ The security vulnerabilities actually lie within either the Web applications themselves or the Web server and browser software that the applications run on and communicate with.

✓ Many attacks against Web applications are just minor nuisances or may not affect confidential information or system availability.

✓ However, some attacks can cause destruction on your systems. Whether the Web attack is against a basic brochure ware site or against the company's most critical customer server, these attacks can hurt your organization.

✓ Some other web application security vulnerabilities are as follows

### SQL Injection

- Injection is a security vulnerability that allows an attacker to alter backend SQL statements by manipulating the user supplied data.
- Injection occurs when the user input is sent to an interpreter as part of command or query and trick the interpreter into executing unintended commands and gives access to unauthorized data.

### Cross site scripting

- Cross Site Scripting is also shortly known as XSS.
- XSS vulnerabilities target scripts embedded in a page that are executed on the client side i.e. user browser rather than at the server side. These flaws can occur when the application takes untrusted data and send it to the web browser without proper validation.
- Attackers can use XSS to execute malicious scripts on the users in this case victim browsers. Since the browser cannot know if the script is trusty or not, the script will be executed, and the attacker can hijack session cookies, deface websites, or redirect the user to an unwanted and malicious websites.
- XSS is an attack which allows the attacker to execute the scripts on the victim's browser.

### Security Misconfiguration

- Security Configuration must be defined and deployed for the application, frameworks, application server, web server, database server, and platform. If these for the application , are properly configured , an attacker can have unauthorized access to sensitive data or functionality.
- Sometimes such flaws result in complete system compromise. Keeping the software up to date is also good security

**Directory Traversals**

- ✓ A directory traversal is a really basic attack , but it can turn up interesting information about a Web site .
- ✓ This attack is basically browsing a site and looking for clues about the server ' s directory structure
- ✓ Properly controlling access to web content is crucial for running a secure web server.
- ✓ Directory traversal or Path Traversal is an HTTP attack which allows attackers to access restricted directories and execute commands outside of the web server's root directory.
- ✓ Web servers provide two main levels of security mechanisms

Access Control Lists ( ACLs )

- An Access Control List is used in the authorization process.
- It is a list which the web server ' s administrator uses to indicate which users or groups are able to access , modify or execute particular files on the server , as well as other access rights

Root directory

- The root directory is the top - most directory on the server file System.
- User access is confined to the root directory , meaning users are unable to access directories or files outside of the root

Countermeasures ( Directory Traversal Attack )

- ✓ There are two main countermeasures to having files compromised via Malicious directory traversals :
- o **Don't store old , sensitive , or otherwise nonpublic files on your web server.**
- The only files that should be in your / htdocs or Document Root folder are those that are needed for the site to function properly.
- These files should not contain confidential information that you don ' t want the world to see.
- o Ensure that your Web server is properly configured to allow public access only to those directories that are needed for the site to function.
- Minimum necessary privileges are key here , so provide access only to the bare minimum files and directories needed for the Web application to perform properly.

6.3.3 Database System Vulnerabilities

- ✓ Database management systems are nearly as complex as the operating systems on which they reside .
- ✓ As a security professional , there is need to assess and manage any potential security problems
- ✓ Following are the Vulnerabilities in database management systems
  - ➢ Loose access permissions. Like applications and operating systems , database management systems have schemes of access controls that are often designed far too

loosely , which permits more access to critical and sensitive information than is appropriate . This can also include failures to implement cryptography as an access control when appropriate.

- ➢ Excessive retention of sensitive data. Keeping sensitive data longer than necessary increases the impact of a security breach.
- ➢ Aggregation of personally identifiable information. The practice known as aggregation of data about citizens is a potentially risky undertaking that can result in an organization possessing sensitive personal information. Sometimes, this happens when an organization deposits historic data from various sources into a data warehouse, where this disparate sensitive data is brought together for the first time . The result is a gold mine or a time bomb , depending on how you look at it.

**Best practices for minimizing database security risks**

- ✓ While some attackers still focus on denial of service attacks , cyber criminals often target the database because that is where the money is.
- ✓ The databases that power web sites hold a great deal of profitable information for someone looking to steal credit card information or personal identities
- ✓ Database security on its own is an extremely in - depth copic that could never be covered in the course of one article : however there are a few best practices that can help even the smallest of businesses secure their database enough to make an attacker move on to an easier target.

**Separate the Database and Web Servers**

- Keep the database server separate from the web server.
- When installing most web software, the database is created for you. To make things easy , this database is created on the same server where the application itself is being installed , the web server . Unfortunately, this makes access to the data all too easy for an attacker to access.
- If they are able to crack the administrator account for the web server, the data is readily available to them.
- Instead, a database should reside on a separate database server located behind a firewall, not in the DMZ (Demilitarized Zone) with the web server. While this makes for a more complicated setup , the security benefits are well worth the effort.

**Encrypt Stored Files**

- Encrypt stored files.
- White Hat security estimates that 83 percent of all web sites are vulnerable to at least one form of attack.
- The stored files of a web application often contain information about the databases the software needs to connect to.
- This information, if stored in plain text like many default installations do , provide the keys an attacker needs to access sensitive data.

### Encrypt Your Backups Too

- Encrypt back-up files.
- Not all data theft happens as a result of an outside attack. Sometimes, it's the people we trust most that are the attackers.

### Use a WAF

- Employ web application firewalls.
- The misconception here might be that protecting the web server has nothing to do with the database.
- Nothing could be further from the truth. In addition to protecting a site against cross site scripting vulnerabilities and web site vandalism, a good application firewall can thwart SQL injection attacks as well.
- By preventing the injection of SQL queries by an attacker , the firewall can help keep sensitive information stored in the database away from prying eyes.

### Keep Patches Current

- Keep patches current. This is one area where administrators often come up short.
- Web sites that are rich with third-party applications, widgets, components and various other plug-ins and add-ons can easily find themselves a target to an exploit that should have been patched.

### Minimize Use of 3rd Party Apps

- Keep third-party applications to a minimum.
- We all want our website to be filled with interactive widgets and sidebars filled with cool content, but any app that pulls from the database is a potential threat.
- Many of these applications are created by hobbyists or programmers who discontinue support for them.

### Don't Use a Shared Server

- Avoid using a shared web server if your database holds sensitive information.
- While it may be easier, and cheaper, to host your site with a hosting provider you are essentially placing the security of your information in the hands of someone else.
- If you have no other choice, make sure to review their security policies and speak with them about what their responsibilities are should your data become compromised.

### Enable Security Controls

- Enable security controls on your database.
- While most databases nowadays will enable security controls by default, it never hurts for you to go through and make sure you check the security controls to see if this was done.

- Keep in mind that securing your database means you have to shift your focus from web developer to database administrator. In small businesses, this may mean added responsibilities and additional buy in from management.
- However, getting everyone on the same page when it comes to security can make a difference between preventing an attack and responding to an attack.

**References:**

1. Hacking for Dummies (5th Edition), Kevin Beaver CISSP, Wiley Publishing Inc. ISBN: 978-81-265-6554-2
2. CISSP for Dummies(5th Edition). Lawrence C. Miller, Peter H. Gregory, ISBN: 978-1-119-21023-8
3. http://www.applicure.com/blog/database-security-best-practice
4. https://thecybersecurityplace.com/database-hacking-its-prevention
5. https://www.valencynetworks.com/blogs/cyber-attacks-explained-database-hacking
6. https://www.acunetix.com/websitesecurity/directory-traversal
7. https://www.veracode.com/security/directory-traversal

**Sample Multiple Choice Questions:**

1. SNMP stands for
    a. Simple Network Messaging Protocol
    b. Simple Network Mailing Protocol
    c. Simple Network Management Protocol
    d. Simple Network Master Protocol
2. Which of the following tool is used for Network Testing and port Scanning
    a. NetCat
    b. SuperScan
    c. NetScan
    d. All of Above
3. Banner grabbing is often used for
    a. White Hat Hacking
    b. Black Hat Hacking
    c. Gray Hat Hacking
    d. Script Kiddies
4. An attacker can create an. . . . . . . . . . . attack by sending hundreds or thousands of e-mails with very large attachments.
    a. Connection Attack
    b. Auto responder Attack
    c. Attachment Overloading Attack
    d. All of the above