UNIT III

CHAPTER 3

Ethical Hacking : Enterprise Security

Syllabus Topics

Phases : Gaining and Maintaining Access : Systems hacking – Windows and Linux – Metasploit and Kali Linux, Keylogging, Buffer Overflows, Privilege Escalation, Network hacking - ARP Poisoning, Password Cracking, WEP Vulnerabilities, MAC Spoofing, MAC Flooding, IPSpoofing, SYN Flooding, Smurf attack, **Applications hacking** : SMTP/Email-based attacks, VOIP vulnerabilities, Directory traversal, Input Manipulation, Brute force attack, Unsecured login mechanisms, SQL injection, XSS, Mobile apps security, **Malware analysis** : Netcat Trojan, wrapping definition, reverse engineering

Phases : Covering your tracks : Steganography, Event Logs alteration

Additional Security Mechanisms : IDS/IPS, Honeypots and evasion techniques, Secure Code Reviews (Fortify tool, OWASP Secure Coding Guidelines)

Syllabus Topic : Phases : Gaining and Maintaining Access

3.1 Phases : Gaining and Maintaining Access

GQ. 3.1.1 Explain Gaining Access& Maintaining Access Phases.

Gaining Access

- In Gaining Access phase, the real hacking takes place.
- Vulnerabilities discovered during the reconnaissance and scanning phase are now utilized to gain access phase.
- The hacker uses method of connection for an exploit can be a internet, local area network (LAN, either wired or wireless), local access to a PC, or offline.
- Examples include denial of service (DoS), stack-based buffer overflows, and session hijacking.
- In the hacker world, gaining access is known as owning the system.

Maintaining Access

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

Syllabus Topic : Systems hacking

3.1.1 Systems Hacking

GQ. 3.1.2 Explain in detail System Hacking.

- System hacking is hacking the different software based technological systems such as desktops, laptops, etc.
- It is defined as the compromise of computer systems and software to gain access to the target computer and theft or misuse their sensitive information.
- Here the malicious hacker uses the weaknesses in a computer system or network to gain unauthorized access of its data or take illegal advantage of it.
- The system hacker is able to hack the computer system because the hacker knows the actual work of computer systems and software which is present inside the system.
- For such attacks, a hacker has information about the systems, networking and knowledge of other areas related to computer science.
- Anyone who is using a computer and is connected to the internet is vulnerable to the threats of malicious hackers.
- These online attackers generally use viruses, Trojans, malware, worms, phishing techniques, email spamming, social engineering, exploit operating system vulnerabilities, or port vulnerabilities to get access to any victim's system.
- When victim's PC gets connected to the internet, the hacker may execute malware on victim's PC and quietly transmits the personal, financial and essential information without victims knowledge consent.

- Then these hackers can blackmail the victim for the money, by stealing that sensitive information from victim's computer which he/she don't want to reveal.
- The hacker can do these following things After compromising the victim's system:
  1. Run the victim's data by deleting the files.
  2. Theft files and folders.
  3. Hijack username and password of victims.
  4. Steal money and credit card details while the victim is doing e-marketing or online transaction.
  5. Sell victim's information to third parties who may use this information for illicit purposes.
  6. Create traffic to shut down victim's website.
  7. Get access to the servers and manipulate the files, programs, etc.

Syllabus Topic : Windows and Linux - Metasploit and Kali Linux,

3.1.2 Windows and Linux

UQ. 3.1.3 Compare windows and Linux operating System on the basis of following points: a. Customizable b. Security c. Efficiency (MU - April 2018)

Linux System Hacking

- Linux is an Operating System (OS) assembled user the model of open-source software development and distribution and is based on Unix OS created by Linus Torvalds.
- We have to know the basic file structure of Linux to hack a Linux based computer system and get access to a password protected Linux system.
- Linux is considered to be the most secure Operating System to be hacked or cracked, but in the world of Hacking means nothing is 100% secured.
- Hackers usually use the following techniques to hack the Linux system.
  1. Hack Linux using SHADOW file.
  2. To bypass the user password option in Linux.
  3. Detects the error or bugs on Linux distribution and tries to take advantage of it.

Windows System Hacking

- The user's password of Windows OS which appears after the Windows starts logging in lets users to protect computer from getting unauthorized access.
- Always choosing a strong password of more than eight digits is an excellent practice.
- However, we can protect our files and folders from the hands of malicious users.
- There are several tricks and techniques used to crack a windows password. But, as per the hacker's point of view, if you able to social engineer your victims and finds a Windows computer open, you can easily modify the existing password and gave a new password which will be unaware of the victim or the owner of the computer.

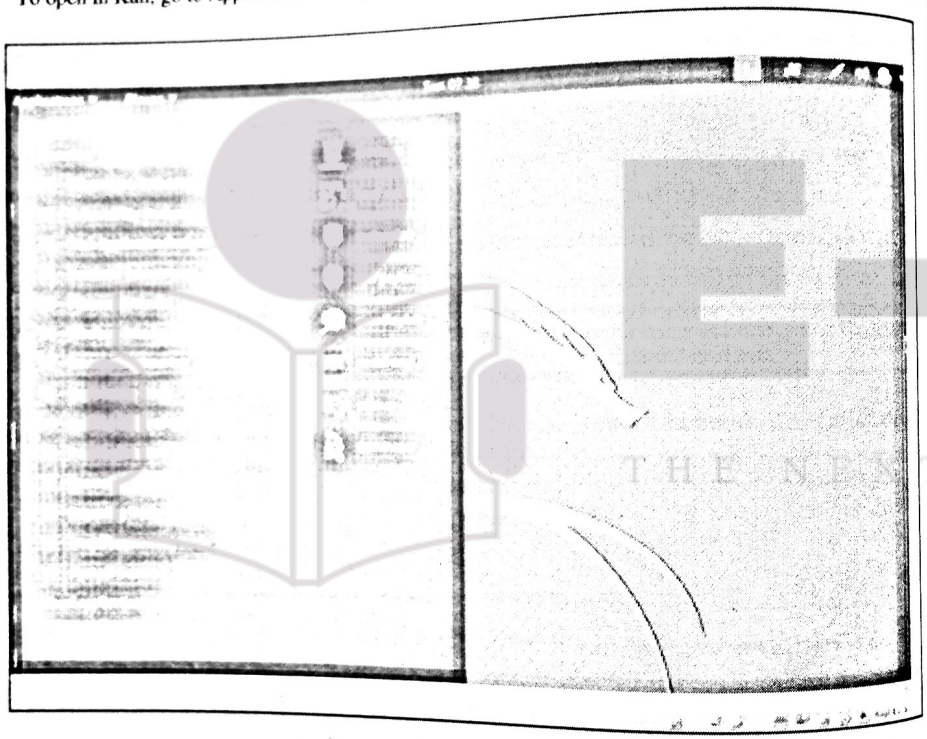
Syllabus Topic : Metasploit and Kali Linux

3.1.3 Metasploit and Kali Linux

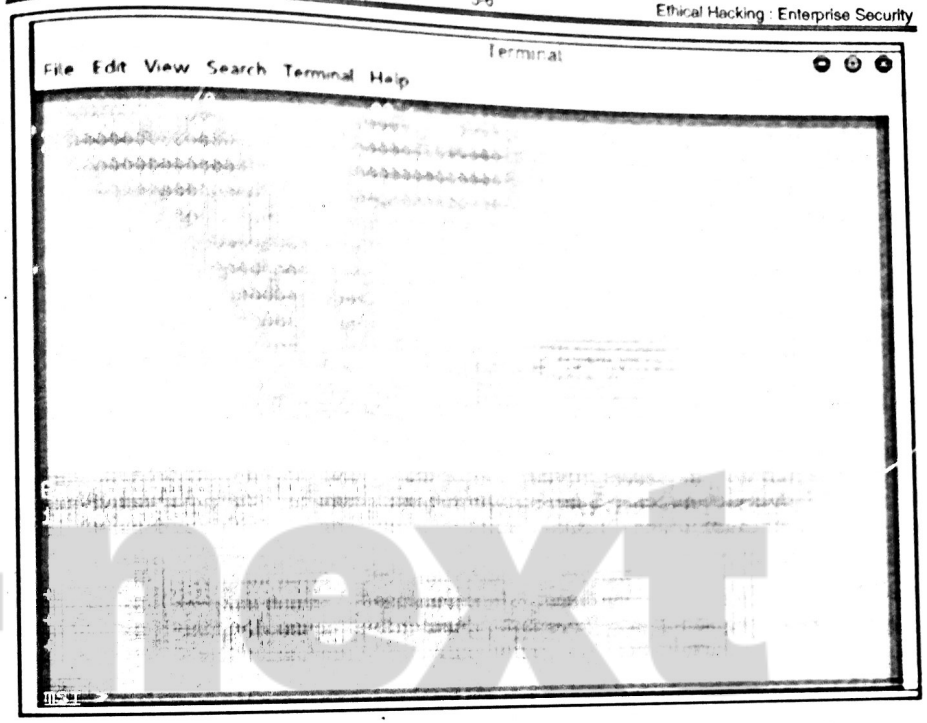
UQ. 3.1.4 Explain in detail Metasploit Framework. (MU - April 2018)

- Metasploit is one of the most powerful utilized tools.
- Metasploit comes in two versions - commercial and free edition.

- An Ethical Hacker uses kali Distribution which has the Metasploit community version embedded in it along with other ethical hacking tools.
- But if you want to install Metasploit as a separate tool, you can easily do so on systems that runs on Windows, Linux, or Mac OS X.
- The hardware requirements to install Metasploit are :
  1. 2 GHz + processor
  2. 1 GB RAM available
  3. 1 GB + available disk space
- It can be either used with command prompt or with Web UI.
- To open in Kali, go to Applications → Exploitation Tools → Metasploit.

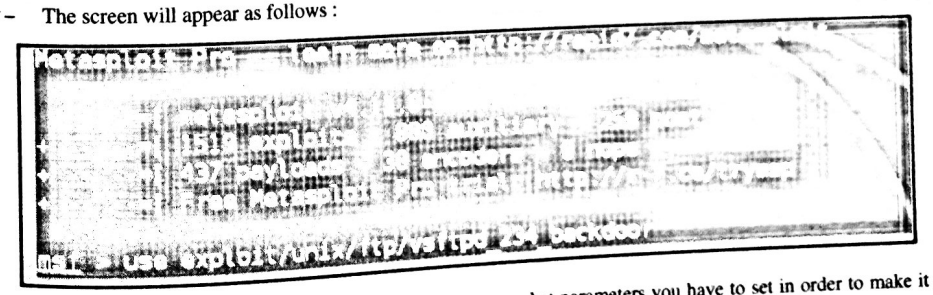


- After Metasploit starts, the following screen will appear. On that screen, the text that highlighted in red underline is the version of Metasploit.

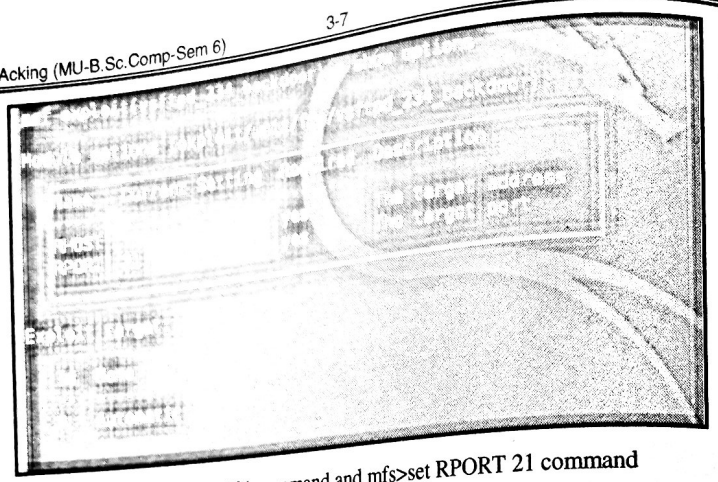


☞ Exploits of Metasploit

- We found that the Linux machine that we have for test is vulnerable to FTP service from Vulnerability Scanner. Now use the exploit that can work for us. The command is - use "exploit path"
- The screen will appear as follows :

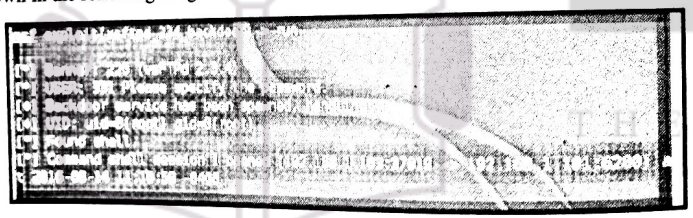


- Then type mfs> show options command in order to see what parameters you have to set in order to make it functional. As shown in the following image, we have to set RHOST as the "target IP address"



- We type mfs> set RHOST 192.168.1.101 command and mfs>set RPORT 21 command

- Then, type mfs>run command. If the exploit is successful, then it will open one session that we can intera with, as shown in the following image.



Syllabus Topic : Key Logging

3.1.4 Key logging

GQ. 3.1.5 Describe Key Logging.

- A keystroke logger is the tool of choice for hackers if all other attempts to gather passwords fail.
- Keystroke loggers (key loggers) can be implemented either using software or hardware.

Hardware key loggers

- It is small hardware devices that connect b keyboard to the PC and save every keystroke in a file or in the memory of the hardware device.
- A hacker must have physical access to the syst in order to install a hardware key logger.

Software key loggers

- It is pieces of stealth software that sit between keyboard hardware and the os, so they can rec every keystroke.
- It can be deployed on a system by Trojans viruses.

Syllabus Topic : Buffer Overflows

3.1.5 Buffer Overflows

GQ. 3.1.6 Explain Buffer Overflow

- Buffer overflows are hacking attempts that exploit weaknesses in an application's code.
- The buffer overflow attack sends too much information to a field variable in an application, which can create an application error.
- Most of times, the application doesn't aware what action to perform next because it's been overwritten with the overflow data.
- So it can either executes the command in the overflow data or drops out a command prompt to allow the user to enter the next command.
- The command prompt is the key for a hacker and it can be used to execute other applications.

Syllabus Topic : Privilege Escalation

3.1.6 Privilege Escalation

GQ. 3.1.7 Explain Privilege Escalation with example.

- Privileges Escalating is the third step in the hacking cycle.
- Privileges Escalating basically means adding more rights or permissions to a user account.
- Privileges Escalating makes a regular user account into an administrator account. Administrator accounts have stronger password requirements, and their passwords are more closely guarded. If it is not possible to find a username and password with Administrator privileges account, then a hacker may choose to use with lower privilege account.
- In this scenario, the hacker must then escalate that account's privileges. This is accomplished by first gaining access using a non admin user account typically by gathering the username and password through one of the previously discussed methods and then increasing the privileges on the account to the level of an Administrator.
- As hacker has a valid user account and password the next step is to execute applications.
- Mostly the hacker needs to have an account with Administrator level access in order to install programs and that is why escalating privileges is so important. In the following sections, we'll see what hackers can do with your system once they have Administrator privileges.
- **For example :** GetAdmin.exe is a small program that adds a user to the local administrators group. This tool uses a low-level NT kernel routine to allowing access to any running process.
- A logon to the server console is needed to execute the program. GetAdmin.exe is run either from the command line or from a browser.
- It works only with Windows NT 4.0 Service Pack 3. The Hk.exe utility exposes a Local Procedure Call flaw in Windows NT. A non admin user can be escalated to the administrators group using this tool.

Syllabus Topic : Network Hacking

3.2 Network Hacking

The following are Networking Hacking Mechanism :

1. ARP Poisoning.
2. Password Cracking
3. WEP Vulnerabilities
4. MAC Spoofing
5. MAC Flooding
6. IP Spoofing
7. SYN Flooding
8. Smurf attack

Syllabus Topic : ARP Poisoning

3.2.1 ARP Poisoning

GQ. 3.2.1 Write a short note on ARP Poisoning.

- Address Resolution Protocol(ARP) allows the network to translate IP addresses into MAC addresses.
- When one host using TCP/IP on a LAN tries to communicate with another, it needs the MAC address or hardware address of the host which is trying to reach.
- Firstly it looks in its ARP cache to see whether it already has the MAC address; if it does not have then it broadcasts an ARP request asking, "Who has the IP address I am looking for?"
- If the host that has that IP address looking in the ARP query, host responds with its own MAC address, and a conversation can begin using TCP/IP.
- ARP poisoning is a technique that is used to attack an Ethernet network and that let an attacker sniff data frames on a switched LAN or stop the traffic altogether.
- ARP poisoning uses ARP spoofing where the purpose is to send fake, or spoofed, ARP messages to an Ethernet LAN.
- These frames contain wrong MAC addresses that confuse network devices such as network switches.
- As a result, frames intended for one machine can be mistakenly sent to another or to an unreachable host.
- ARP spoofing can 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.
- To prevent ARP spoofing, we have to permanently add the MAC address of the gateway to the ARP cache on a system.
- We 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.
- This can used to prevent from a hacker to overwriting the ARP cache to perform ARP spoofing on the system but it can be difficult to manage in a large environment because of the number of systems.
- Port-based security can be enabled in an enterprise environment on a switch to allow only one MAC address per switch port.

Syllabus Topic : Password Cracking

3.2.2 Password Cracking

GQ. 3.2.2 How to crack password? Explain.

- Many hacker attempts start with attempting to crack passwords.
- Passwords are the key of information needed to access a system.
- When user creates passwords, he often selects passwords that are prone to being cracked. Many reuse passwords or choose one that is simple, such as a "name" to help them remember it.
- Because of this most password cracking is successful to crack passwords, it can be the launching point for escalating privileges, hiding files, executing applications, and covering tracks.
- Passwords may be cracked manually or with automated tools like a dictionary or brute-force method.
- In manual password cracking involves attempting to log on with different passwords.
- The hacker follows these steps :
  1. They find a valid user account (such as Admin or Guest).
  2. They create a list of possible passwords.
  3. They rank the passwords from high to low probability.
  4. Key in each password.
  5. They try again and again until a successful password is found.
- A hacker can create a script file that tries each password in a list. This is still considered manual cracking, but it is 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 directly.
- Most systems encrypt a password for storage on a system. During the logon process, the password entered by the user is encrypted using the same algorithm and then compared to the hashed passwords stored in the file.
- A hacker can attempt to gain access to the encrypting algorithm stored on the server instead of trying to guess or otherwise identify the password.
- If the hacker is successful then they can decrypt the passwords stored on the server.

Syllabus Topic : WEP Vulnerabilities

3.2.3 WEP Vulnerabilities

GQ. 3.2.3 Write a short note on WEP Vulnerability.

- There are two methods exist for authenticating wireless LAN clients to an access point: open system or shared key authentication.
- **Open system :** It does not provide any security mechanisms but is simply a request to make a connection to the network. Shared key: Its authentication has the wireless client hash a string of challenge text with the WEP key to authenticate to the network.
- Wired Equivalent Privacy (WEP) was the first security option for 802.11 WLANs.
- It is used to encrypt data on the WLAN and can optionally be paired with shared key authentication to authenticate WLAN clients.
- It uses an RC4 64-bit or 128-bit encryption key to encrypt the layer 2 data payload.
- To making the WEP key either 64- or 128-bit, WEP key comprises a 40-bit or 104-bit user-defined key combined with a 24-bit Initialization Vector (IV),
- The process by which RC4 uses IVs is the real weakness of WEP which allows a hacker to crack the WEP key.

- The FMS attack is the method uses to encrypted output bytes to determine the most probable key bytes.
- It was incorporated into products like AirSnort, WEPCrack, and aircrack to exploit the WEP vulnerability.
- Although a hacker can attempt to crack WEP by brute force attack and the most common technique is the FMS attack.
- It employs the Temporal Key Integrity Protocol (TKIP) which is a safer RC4 implementation for data encryption and either WPA Personal or WPA Enterprise for authentication.
- WPA Personal uses an ASCII passphrase for authentication and WPA Enterprise uses a RADIUS server to authenticate users.
- WPA Enterprise is a more secure robust security option than WPA Personal but it relies on the creation and more complex setup of a RADIUS server.
- TKIP rotates the data encryption key to prevent the vulnerabilities of WEP and simultaneously cracking attacks.
- WPA2 is similar to 802.11i and it uses the Advanced Encryption Standard (AES) to encrypt the data payload, which is considered an uncrackable encryption algorithm. WPA2 also allows for the use of TKIP during a transitional period called mixed mode security.
- In this transitional mode both TKIP and AES can be used to encrypt data.
- WPA Personal and WPA2 Personal both uses a passphrase to authentication WLAN clients.
- WPA Enterprise and WPA2 Enterprise both authenticate WLAN users via a RADIUS server using the 802.1X/Extensible Authentication Protocol (EAP) standards.
- 802.11i and WPA2 both use the same encryption and authentication mechanisms as WPA2. But WPA2 doesn't require vendors to implement preauthorization.
- Table summarizes the authentication and encryption options for WLANs.

	Encryption	Authentication	Weakness
Original IEEE 802.11 standard	WEP	WEP	IV weakness allows the WEP key to be cracked. The same key is used for encryption and authentication of all clients to the WLAN
WPA	TKIP	Passphrase or RADIUS (802.1x/EAP)	Passphrase is susceptible to a dictionary attack.
WPA2	AES (can use TKIP while in mixed mode)	Passphrase or RADIUS (802.1x/EAP)	Passphrase is susceptible to a dictionary attack.
IEEE 802.11i	AES (can use TKIP while in mixed mode)	Passphrase or RADIUS (802.1x/EAP)	Passphrase is susceptible to a dictionary attack.

- For Example: Aircrack is a WEP-cracking software tool. This doesn't capture packets but used to perform the cracking after another tool has captured the encrypted packets.

Syllabus Topic : MAC Spoofing

3.2.4 MAC Spoofing

GQ. 3.2.4 Explain MAC Spoofing.

- Media Access Control (MAC) spoofing is a method used to change the factory-assigned MAC address of a network interface on a networked device.
- The MAC address that is hard coded on a network interface controller cannot be changed but many drivers enable the MAC address to be changed.
- This address of a computer is a unique identifier assigned to network interfaces for communications at the data link layer of a network segment.
- MAC address is a very common defence mechanism for wireless networks, where you configure your APs to enable only wireless clients with known MAC addresses to connect to the network.
- So a very common hack against wireless networks is MAC address spoofing.
- The hackers can simply spoof MAC addresses in UNIX by using the if config command, and in Windows, by using the SMAC utility or any other tools.
- However MAC address based access controls are another layer of protection and better than nothing at all.
- If hacker spoofs one of your MAC addresses, the only way to discover malicious behaviour is through contextual awareness by spotting the same MAC address being used in two or more places on the WLAN, which can be difficult.

Syllabus Topic : MAC Flooding

3.2.5 MAC Flooding

GQ. 3.2.5 Explain MAC Flooding in details.

- A packet sniffer on a switched network cannot capture all traffic as it can on a hub network but it captures either traffic coming from or traffic going to the system.
- It is necessary to use an additional tool to capture all traffic on a switched network.
- There are two ways to perform active sniffing and make the switch send traffic to the system running the sniffer i.e. ARP spoofing and ARP flooding.
- ARP spoofing takes the MAC address of the network gateway and simultaneously receiving all traffic intended for the gateway on the sniffer system.
- A hacker can 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 sniffing attack allows the system with the sniffer to capture all traffic on the network.

Syllabus Topic : IPSpoofing

3.2.6 IPSpoofing

GQ. 3.2.6 Explain IP Spoofing.

- A hacker may spoof an IP address when scanning target systems to minimize the chance of detection. One drawback of IP spoofing is that a TCP session cannot be successfully completed.
- Source routing notify an attacker specify the route that a packet takes through the Internet. It can also minimize the chance of detection by bypassing

IDS and firewalls that may block or detect the attack.

- Source routing uses a reply address in the IP header to return the packet to a spoofed address instead of the attacker's real address.
- To detect IP address spoofing, you can compare the time to live (TTL) values (The attacker's TTL will be different from the spoofed address's real TTL).

Syllabus Topic : SYN Flooding

3.2.7 SYN Flooding

GQ. 3.2.7 *Elaborate the term SYN Flooding.*

- A SYN flood attack sends TCP connection requests faster than any machine can process them.
- The hacker creates a random source address for each packet and sets the SYN flag to request a new connection to the server from the spoofed IP address.
- Then victim responds to the spoofed IP address and then waits for the TCP confirmation that never arrives.
- Simultaneously, the victim's connection table fills up waiting for replies, as the table is full, all new connections and legitimate users are ignored as well as can't access the server.
- Some of the methods to prevent SYN Flood attacks are SYN cookies, Micro Blocks, RST cookies, and Stack Tweaking.

Syllabus Topic : Smurf attack

3.2.8 Smurf attack

GQ. 3.2.8 *Explain Smurf attack in details.*

- A smurf attack is sends large amount of ICMP echo (ping) traffic to a broadcast IP address with the spoofed source address of a victim.
- Each secondary victim's host on that IP network replies to the ICMP echo request with an echo reply, multiplying the traffic by the number of hosts responding.
- Hundreds of machines might reply to each packet on a multi-access broadcast network.
- It creates a magnified DoS attack of ping replies flooding the primary victim.
- On the Internet, IRC servers are the primary victim of smurf attacks.

Syllabus Topic : Applications Hacking

3.3 Applications Hacking

- The following are Application Hacking Mechanisms:
- SMTP/Email-based attacks

Syllabus Topic : SMTP/Email-Based Attacks

3.3.1 SMTP/Email-Based Attacks

GQ. 3.3.1 *Elaborate the term Email-based Attack.*

- The sender of an e-mail to know whether the recipient reads, forwards, modifies, or deletes an e-mail because of e-mail tracking programs.
- Most e-mail tracking programs work by appending a domain name to e-mail address, such as abcRead.com.
- A single-pixel graphic file that is not noticeable to the recipient is attached to the e-mail. Then, the graphic file connects back to the server and notifies the sender of the action when an action is performed on the e-mail.

- MailTracking.com and eMailTracking Pro are tools that allow an ethical hacker to track e-mail messages.
- When using these tools to send an e-mail, modify an e-mail, forward an e-mail, or reply to an e-mail, the resulting actions and tracks of the original e-mail are logged.
- The sender is getting notification of all actions performed on the tracked e-mail by an automatically generated e-mail.
- Spammers and anyone else who interested in collecting e-mail addresses from the Internet can use web spiders.
- A web spider combs websites collecting certain information such as email addresses. They uses syntax such as the @ symbol to locate email addresses then copies them into a list. These addresses are then added to a database and may be used later to send unsolicited e-mails. They can be used to locate all kinds of information on the Internet.
- A hacker can use a web spider to automate information gathering process. To prevent from web spidering of your website is to put the robots.txt file in the root of your website with a listing of directories that you want to protect from crawling.

Syllabus Topic : VOIP vulnerabilities

3.3.2 VOIP vulnerabilities

UQ. 3.3.2 *What is VOIP? Explain in details any two VOIP vulnerability.* (MU - April 18)

- VoIP stands for Voice over Internet Protocol, is a technology that allows to make voice calls using a broadband Internet connection instead of a regular phone line.

There are following kinds of VOIP vulnerabilities occur :

1. **Insufficient verification of data :** In VoIP implementations insufficient verification of data can enable man-in the-middle attacks.
2. **Execution flaws :** Standard databases are used as the backbone of VoIP services and registrations. The majority of problems arise to execution flaws result from bad input filtering and insecure programming practices.
3. **String manipulation flaws :** Malware formed packets with unexpected structures and content can exist in any protocol messages, including SIP, H.323, SDP, RTP,MGCP, and SRTP. Mostly malformed messages include buffer-overflow attacks and other boundary-value conditions. The result is that the input given by attacker is written over other internal memory content, such as registers and pointers, which will let the attacker take full control of the vulnerable process.
4. **Low resources :** The resources that VoIP implementations especially in embedded devices can use can be scarce. Low memory and processing capability makes it easy for an attacker to shut down VoIP services in embedded devices.
5. **Low bandwidth :** This service has to be built so that it will withstand the load even if every caller makes a call at the same time. When the number of subscribers to a VoIP service is low that's not big problem. But when a service is intentionally flooded with thousands of bot clients the result might be a shutdown of the whole service.
6. **File manipulation flaws :** These flaws are typical implementation mistakes, programming errors from using insecure programming constructs that result in security problems. These flaws include insecure access to files.

7. **Password management :** The only identifier a VoIP consumer has is telephone number or SIP URL and possible password for the service. The passwords are stored in both the client and server. If passwords are storied in the server in a format that can be reversed, anyone with access to that server can collect the username and password pairs.
8. **Permissions and privileges :** Resources have to be protected both from the OS and platform perspective and from the network perspective. VoIP services running on the platform have to consider privileges they run with. A VoIP service does not necessarily require a rootor privilege to administrative run.
9. **Crypto and randomness :** In VoIP signalling, confidential data needs to be protected from eavesdropping attacks. The common vulnerability in this category is to fail to encrypt at all, even if the encryption mechanisms are available.
10. **Authentication and certificate errors :** Both users and devices need to be authenticated. Also other services, like device management, exist in VoIP devices that need user authentication.

Syllabus Topic : Directory Traversal

3.3.3 Directory Traversal

GQ. 3.3.3 Explain Directory Traversal.

- Windows 2000 systems running IIS are susceptible to a directory traversal attack, also known as the Unicode exploit.
- The vulnerability inIIS allows for the directory traversal/Unicode exploit, occurs only in unpatched Windows 2000 systems and affects CGI scripts and ISAPI extensions such as .ASP.
- The vulnerability exists which allowing hackers system level access because the IIS parser was not properly interpreting Unicode.
- Unicode converts characters of any language to a universal hexadecimal code specification. However, it is interpreted twice, and the parser only scanned the resultant request once.
- Therefore Hackers could sneak file requests through IIS. For example, utilizing %c 0% af instead of a slash in a relative pathname exploits the IIS vulnerability..
- The Unicode directory traversal vulnerability allows a hacker to add, change, or upload or delete files, and run code on the server.
- The ability to add or run files on the system allows a hacker to install a Trojan or backdoor on the system

Syllabus Topic : Input Manipulation

3.3.4 Input Manipulation

GQ. 3.3.4 Explain the term Input Manipulation

- The input Parameter manipulation attack is based on the manipulation of parameters exchanged between client and server in order to modify application data like user details and permissions, quantity of products and price
- This information is stored in the form of cookies, hidden form fields, or URL Query Strings which is used to increase application functionality and control.
- This attack can be performed by a malicious hacker who wants to utilize the application for their own benefit, or an attacker who wishes to attack a third-person using a Man-in-the-middle attack.

- For above given cases tools likes Web scarab and Paros proxy are mostly used.
- The attack success depends on lack in integrity and logic validation mechanism errors, and its utilization can result in other consequences including SQL Injection, XSS, file inclusion, and path disclosure attacks.

Syllabus Topic : Brute Force Attack

3.3.5 Brute Force Attack

GQ. 3.3.5 What is Brute Force attack? Explain.

- In a brute-force attack, the hacker uses all possible combinations of letters, numbers, special characters, and capital and small letters to break the password.
- Brute force attack has a high probability of success, but it requires an enormous amount of time to process all the combinations.
- This attack is slow and the hacker requires a system with high processing power to perform all those permutations and combinations faster.
- John the Ripper(Johnny) is one of the powerful tools to set a brute-force attack and it comes bundled with the Kali distribution of Linux

Syllabus Topic : Unsecured login mechanisms

3.3.6 Unsecured Login Mechanisms

GQ. 3.3.6 Explain in detail unsecure login mechanism.

- Many websites can't give permission to do anything with application until they log in to website. These can be a great help to hackers. These login mechanisms often don't handle wrong user IDs or passwords gracefully.
- An Attacker often reveals too much information that an attacker can use to gather valid user IDs and passwords.
- Browse to your application and log in to test for unsecured login mechanisms :
  1. Use an invalid user ID with a valid password and check
  2. Use a valid user ID with an invalid password and check
  3. Using an invalid user ID and invalid password and check
- After you enter such kind of credentials, the web application will probably respond with a message similar to 'Your user ID is invalid' or' Your password is invalid'.
- The web application might return a generic error message, such as 'user ID and password combination is invalid' and, returns different error codes at the same time in the URL for invalid user IDs and passwords.

Syllabus Topic : SQL injection

3.3.7 SQL Injection

GQ. 3.3.7 Explain SQL injection

- In SQL injection attack, malicious code is inserted into a web form field or the website's code to make a system execute a command shell or other arbitrary commands.
- Just as Unauthorized user enters queries and additions to SQL database via a web form, the hacker can insert commands to the SQL server with the same web form field.
- For example, a random command from a hacker might open a command prompt or display a table from the database. A database table may contain

personal information such as passwords, credit /debit card numbers, or social security numbers.

- SQL servers are common database servers and used by many organizations to store confidential data. This will makes a SQL server a high value target and therefore a system that is very attractive to hackers.
- The hacker determines whether the configuration of the database and related tables and variables is vulnerable to understand the Steps to Conduct SQL Injection before launching a SQL injection attack.
- The steps to determine the SQL server's vulnerability are as follows:

1. Using web browser, search for a website that uses a login page or other database input or query fields (like an "I forgot my password" form).
2. Look for web pages that display the POST or GET HTML commands by checking the site's source code.

Syllabus Topic : XSS

3.3.8 XSS

GQ. 3.3.8 Write a short note on XSS

- A Cross-site scripting(XSS) vulnerabilities occur when web applications allow users to add custom code into a url path or onto a website that will be seen by other users.
- It can be exploited to run malicious JavaScript code on a victim's browser.
- For example, an attacker could send an email to a user that appears to be from a trusted bank, with a link to that bank's website. This link have some malicious JavaScript code tagged onto the end of the url so if the bank's site is not properly protected against cross-site scripting, then that malicious code will be run in the user's web browser when they click on the link.
- Prevention strategies for cross-site scripting include escaping untrusted HTTP requests as well as validating and sanitizing user-generated content.
- We can use modern web development frameworks like ReactJS and Ruby on Rails also provides some built-in cross-site scripting protection.

Syllabus Topic : Mobile apps Security

3.3.9 Mobile Apps Security

GQ. 3.3.9 How to secure Mobile apps? Explain.

- Mobile app security is measure and means of defending mobile device apps from digital fraud in the form of hacking, malware, and other criminal manipulation.
- It can be implemented by both technological means alongside personal responses and corporate processes intended to safeguard digital integrity on mobile devices.

The Threat of Mobile Apps

- Mobile apps are major channel for security threats, especially when they are connected to business brands.

- They are targeted by criminal elements searching to profit from companies and employees who use mobile devices but do not engage in proper mobile app security processes.
- When a mobile app is compromised by malware or a device user downloads an unauthorized rogue app that is not actually officially launched, it stands a high risk of being a victim of digital fraud.

This following are more common or currently popular scams and schemes in play with mobile apps :

1. Financial login credentials being stolen
2. Credit card details stolen and resold
3. Giving hackers access to their business network
4. Wholesale identity theft
5. Device being used to spread malware to uninfected devices
6. Having SMS or TXT messages copied and scanned for private info

The consequences can be severe, when this occurs, including :

1. Negative end-user experiences
2. Negative, potentially permanent impact on the brand's reputation
3. Ngoing financial losses

Mobile Application Security Best Practices

- To defend your brand and your employees from the threat posed by mobile app security fraud and online attacks following points to be consider :

1. **Enact Digital Security Training :** Train your employees about the risk mobile apps can present. Teach them how to recognize malware sites, potential attacks, and phishing attempts, and put proper response procedures in place.
2. **Proactively Monitor for Rogue Apps :** Keep eye on both authorized and unauthorized app download platforms for any apps that carry your logo, brand name, or messaging that may have been posted to lure in unsuspecting customers.
3. **Only Download from Trusted Sources :** Provide a list of verified app download sites to both your employees and customers and even then, suggest high caution whenever downloading a new app and reporting of any suspicious activity.
4. **Improve Data Security :** Initiate brand specific data security strategy and policy that enforces active compiling and resolving all possible data breaches. Having your development team implements solid encryption whenever data is transferred between any devices.
5. **Avoid Saving Passwords :** Many app require a login with a username and password, Discourage the use of such apps that save passwords on your system or in the cloud, as these can allow the private credentials to be harvested and used to hack other devices or networks.
6. **Force User Session End :** Never let a user's session to remain active after they have logged out or closed your app. Require them to close the session on every logout and to log back in to regain access. Also, after predetermined inactivity period, log out user for extra safety.
7. **Go Beyond Anti-Malware :** Mobile app security resources Firstly scan devices for known malware and alert user with the option to remove

anything found. It is an excellent precaution that your corporate digital security measures should not stop here. Behavioural analysis tools, Incorporate encryption routines, traffic monitoring, and more.

8. **Invest in Mobile App Security Services :** Your team can only do too much to get the best mobile app security. To further defensive strength you can also engage mobile app security suite that handle much of data analysis, the app monitoring, and rogue app takedown for you.

Syllabus Topic : Malware Analysis

3.4 Malware Analysis

GQ. 3.4.1 Define Malware Analysis.

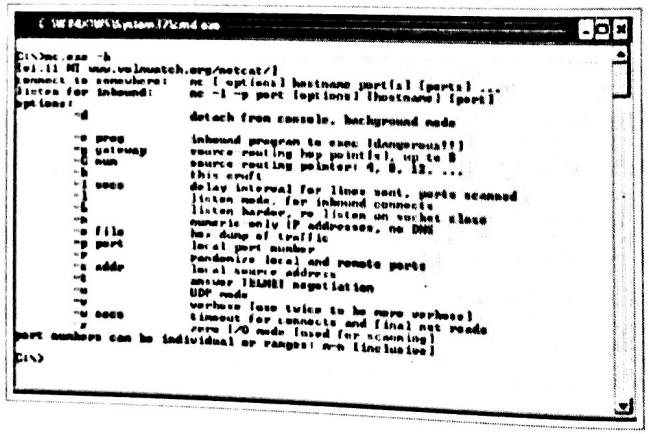
- Malware analysis is a process of learning how malware functions and any potential outcomes of a given malware.
- Malware code can differ radically, and it is essential to know that malware can have many functionalities.
- These may come in the form of worms, viruses, spyware, and Trojan horses.
- Each type of malware . assembled information about the infected device without the knowledge, or authorization of the user.

Syllabus Topic : Netcat Trojan

3.4.1 Netcat Trojan

GQ. 3.4.2 Explain Netcat Trojan.

- A Netcat is Trojan that uses a command-line interface to open TCP or UDP ports on a target system.
- A hacker can then telnet to those open ports and gain shell access to target system.
- Firstly download a version of Netcat for your system.There are many versions of Netcat for all Windows Operating Systems and also, Netcat was originally developed for the Unix system and that is available in many Linux distributions, including BackTrack.



- It needs to run on both a client and the server. The server side connection enabled by the -l attribute and it is used to create a listener port.
- For example, use following command to enableNetcat listener on the server:

```
nc -L -p 123 -t -e cmd.exe
```

- On Netcat client, run following command to connect to Netcat listener on the server:

```
nc<ip address of the server><listening port on the server>
```

Syllabus Topic : Wrapping definition

3.4.2 Wrapping Definition

GQ. 3.4.3 Elaborate Wrapping in Malware Analysis with example.

- Wrappers are software packages which are used to deliver a Trojan.
- The wrapper binds an authorized file to the Trojan file. Both authorized software and Trojan are combined into a single executable file and installed when the program is executed.
- Mostly games or other animated installations are used as wrappers because they entertain to user while the Trojan in being installed.
- In this way user doesn't notice the slower processing that occurs when the Trojan is being installed on the system, the user only sees the authorized application being installed.

For examples

1. **Graffiti** is an animated game that can be wrapped with Trojan. Graffiti entertains the user with an animated game while the Trojan is being installed in background.
2. **Silk Rope 2000** is wrapper that combines the Back Orifice server and any other specified application.
3. **ELITeWrap** is an advanced .exe wrapper used for installing and running programs for Windows. It can create setup program to extract files to a directory and run programs or batch files that display help menus or copy files on to the target system.

Syllabus Topic : Reverse Engineering

3.4.3 Reverse Engineering

GQ. 3.4.4 Describe Reverse Engineering.

- Reverse engineering is a process that taking apart an object to see how it works in order to duplicate or enhance the object.
- The best practice that it taken from older industries which are now frequently used on computer hardware and software.
- **Software reverse engineering** : It involves reversing a program's machine code back into source code that it was written in, using program language statements.
- In Software reverse engineering, it is done to retrieve source code of a program because the source code was lost, to study how program performs such operations, to improve performance of a program, to fix the bug , to identify malicious content in a code such as a virus or to adapt a program written for use with one microprocessor for use with another.
- Reverse engineering used for copying or duplicating programs may constitute copyright violation.
- The licensed use of software specifically prohibits reverse engineering in some cases.
- In Software reverse engineering, may use several tools to disassemble a program.

- For example, a hexadecimal dumper is the tool, which prints or displays binary numbers of a program in hexadecimal format. Reverse engineer can identify certain portions of a program to see how it works by understanding bit patterns that represent the processor instructions and the instruction lengths.
- **Hardware reverse engineering :** It involves taking apart a device to see how it works.
- For example, if a processor manufacturer wants to see how competitor's processor works, they can first purchase competitor's processor, analysed it, and then make a processor similar to it. But this process is illegal in many countries.
- In hardware reverse engineering, it requires a great deal of expertise and which is quite expensive.
- There are another type of reverse engineering involves to producing 3-D images of manufactured parts when a blueprint is not available in order to remanufacture the part. In part reverse, it is measured by a coordinate measuring machine (CMM). As part is measured, a 3-D wire frame image is generated and displayed on a monitor. As the measuring is complete, wire frame image is created. Any part reverse engineered can be using these methods.
- Sometimes, the term forward engineering is used in contrast to reverse engineering.

Syllabus Topic : Phases : Covering your Tracks

3.5 Phases : Covering your Tracks

GQ. 3.5.1 How to cover your tracks?

- Once hacker has successfully gained Administrator access on a system then they try to cover their tracks to prevent detection of their presence (either pastor current) on system.
- They may also try to remove evidence of their identity or any activities performed on the system to prevent tracing of their identity or location by authorities.
- They usually erase any error messages or security events that have been logged, to prevent detection.
- There are two methods used by a hacker to cover their tracks and avoid detection: disabling auditing and clearing the event log.

Disabling Auditing

- The first thing hackers do after gaining Administrator privileges is to disable auditing. In the Windows Event Viewer, Windows auditing records certain events in a log file that is stored. Events can be logging in to the system, an application, or an event log.
- An administrator can select level of logging implemented on a system. A hacker wants to examine level of logging implemented to see whether they need to clear events which indicates their presence on the system.

Syllabus Topic : Steganography

3.5.1 Steganography

GQ. 3.5.2 Explain in brief Steganography with respect to hacking

- Steganography is a process of hiding data in other types of data such as text files or images.
- The most popular way of hiding data in files is to use graphic images as hiding places. Using steganography, hackers can embed any information in a graphic file.
- They can hide directions on a secret bank account number, making a bomb, or answers to a test. Really any text imaginable can be hidden in an image.

For examples

- The Image Hide is a steganography program that hides large amounts of text in images. There is no increase in the image size even after adding bytes of data.
- The image looks same in a normal graphics programs. This loads and saves to files and therefore is able to bypass most e-mail sniffers.
- The Blindside is a steganography application that hides information inside BMP images. It is a command-line utility.
- The MP3Stego tool hides information in MP3 files during the compression process. The data is encrypted, compressed, and then hidden in the MP3 bit stream.
- It is difficult to detect Steganography, but can be detected by some programs.
- Firstly locate files with hidden text, which can be done by analysing patterns in the images and changes to colour palette.

For example

- The Stegdetect is an automated tool for detecting steganography content in images. It is capable of detecting different steganography methods to embed hidden information in JPEG images.
- The Dskprobe is a tool on Windows 2000 installation CD. It is a low-level hard-disk scanner that can detect steganography.

Syllabus Topic : Event Logs alteration

3.5.2 Event Logs alteration

GQ. 3.5.3 Explain Event logs alteration

- Hackers can easily clear out the security logs in the Windows Event Viewer. An event log which contains one or few events is suspicious because it usually indicates that other events have been cleared.
- It is still necessary to clear event log after disabling auditing, because using Audit Pol tool places an entry in the event log indicating that auditing has been disabled.
- Several tools exist to clear the event log, or a hacker can do so manually in the Windows Event Viewer.
- For example: elsave.exe utility is a simple tool used for clearing the event log. It is command-line based.
- The Win Zapper is a tool that an hacker can use to erase event records selectively from the security log in Windows 2000.

Syllabus Topic : Additional Security Mechanisms

3.6 Additional Security Mechanisms

Syllabus Topic : IDS/IPS

3.6.1 IDS/IPS

UQ. 3.6.1 Describe Intrusion Detection System. **(MU - April 2018)**

- **Intrusion detection systems (IDSs)** : They are systems that inspect traffic and look for known signatures of attacks or unusual behaviour patterns.
- Packet-sniffer views and monitors traffic and then a built-in component of IDS.
- IDS modify a command center or system administrator by e-mail, pager or cell phone when an event listed on the company's security event list is triggered.
- **Intrusion prevention systems (IPSs) :** It initiates countermeasures such as blocking traffic when suspected traffic flow is detected.

- This system automate response to an intrusion attempt and allow you to automate the deny-access capability.
- **There are two main types of IDS :** Host-based and Network Based.

1. Host-based IDSs (HIDSs):

- They are applications that reside on a single system or host and filter traffic or events based on a known signature list for that specific operating system.
- It includes Norton Internet Security and Cisco Security Agent (CSA).
- Many Trojans and worms can turn off an HIDS.

2. Network-based IDSs (NIDSs):

- They are software-based appliances that present on the network. They are used solely for ID purposes to detect all types of malicious network traffic and computer usage that cannot be detected by a conventional firewall.
- NIDSs includes network attacks against vulnerable services, data attacks on applications, host based attacks such as unauthorized logins and access to sensitive files, privilege escalation, and malware. They are passive systems
- The IDS sensor detects a logs the information, potential security breach, and signals an alert on the console.
- It can perform either signature analysis or anomaly detection to determine if traffic is a possible attack.
- Signature detection IDSs matches traffic with known signatures and patterns of misuse.
- A signature is a pattern which is used to identify either a single packet or a series of packets that, when combined, execute an attack.
- When there is an anomaly in the behaviour of access to systems, files, logins, and so on, IDS can employs anomaly detection looks for intrusion attempts based on a person's normal business patterns and alerts.
- A hacker can evade IDS by changing traffic so that it does not match a known signature. This may involve using a different protocol like UDP instead of TCP or HTTP instead of ICMP to deliver an attack.
- Hacker can break an attack up into several smaller packets to pass through IDS but when reassembled at receiving station will result in a compromise of the system, is known as session splicing.
- Some other methods of evading detection involve obfuscating addresses or data, inserting extra data by using encryption, or desynchronizing and taking over a current client's session.

Syllabus Topic : Honey Pots and Evasion Techniques

3.6.2 Honey Pots and Evasion Techniques

GQ. 3.6.2 Write a short note on Honey pots.

- A honey pot is a decoy box residing inside your network Demilitarized Zone (DMZ),
- It set up by a security professional to trap or aid in locating hackers, or to draw them away from real target system.
- The honey pot is a decoy system that a malicious attacker might try to attack like software on the system can log information about the attacker such as IP address. This information can be used to try and locate the hacker either during or after the attack.
- The best location for a honey pot is in front of the firewall on the DMZ which making it very attractive to hackers.
- A honey pot with a static address looks similar like a real production server.

Syllabus Topic : Secure Code Reviews (Fortify tool, OWASP Secure Coding Guidelines)

3.6.3 Secure Code Reviews (Fortify tool, OWASP Secure Coding Guidelines)

GQ. 3.6.3 Elaborate Secure Code Review.

- Security code review(SCR) is a process of auditing the source code for an application to verify that the proper security controls are present, that they work as intended, and that they have been invoked in all right places.
- Code review is a way of ensuring that application has been developed so as to be self-defending in its given environment.
- SCR is a method of assuring secure application developers are following secure development techniques.
- A general rule of thumb is that a penetration test should not discover any additional application vulnerabilities relating to developed code after application has undergone a proper SCR.
- All SCR's are a combination of human effort and technology support.
- At one end of the spectrum is an inexperienced person with a text editor and at the other end of the scale is a security expert with an advanced static analysis tool.
- It takes a fairly serious level of expertise to use current application security tools effectively.
- Tools can be used to perform such task but they always need human verification. Tools do not understand context, which is the keystone of SCR.
- Tools are good at assessing large amounts of code and pointing out possible issues, but a person needs to verify every single result to determine if it is a real issue, if it is actually exploitable, and calculate risk to the enterprise.
- Human reviewers are also necessary to fill in for significant blind spots where automated tools simply cannot check.

Fortify Tool

GQ. 3.6.4 Explain working of Fortify Tool.

- The Fortify Source Code Analyzer (FSCA) created by Fortify Software.
- It is a software security vendor of choice of government and Fortune 500 companies in a wide variety of industries.
- Fortify tool provide products that identify and remediate security vulnerabilities in software in order to mitigate enterprise security risks.
- The FSCA tool attempts to protect systems from security flaws in business-critical software applications.
- It drives down cost and risk by automating and enhancing key software audit, development, testing and deployment processes.
- FSCA strengthens software applications themselves so that hackers and malicious insiders cannot access vital assets or disrupt business processes.

Working of Fortify Tools

- FSCA is a static analysis tool and it processes code in a manner similar to a code compiler.
- FSCA uses build tool that runs on source code file or set of files which converts it into an intermediate model that is optimized for security analysis by Fortify.
- FSCA model is put through a series of analyzers (Semantic, Data flow, Control Flow, Configuration, and Structural).
- FSCA also uses Fortify Secure Coding Rule Packs to analyze the code base for violations of secure coding practices.
- Fortify Rules Builder allows to expand and extend analysis capabilities to include custom rules.
- The outputs can be viewed in a number of ways using the Audit Workbench and the Fortify Manager.

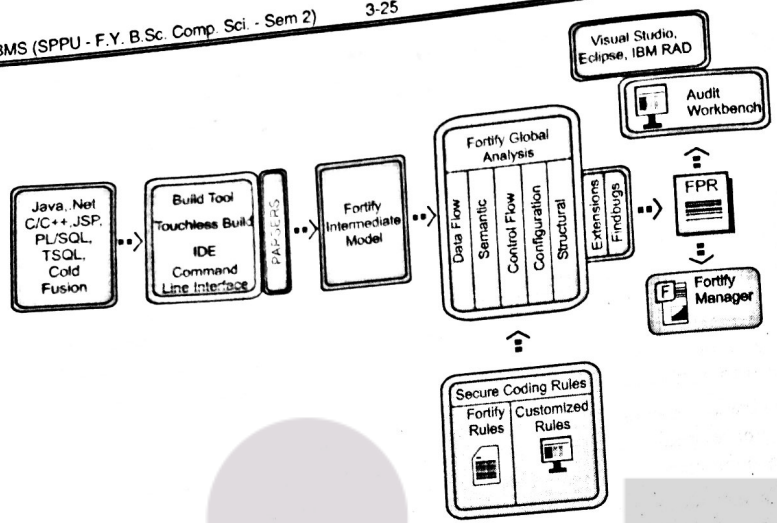


Fig. 3.6.1

☞ Features

1. Used to find and fix following software vulnerabilities at root cause such as Command Injection, Buffer Overflow, Cross-Site Scripting, Denial of Service, Format String, Integer Overflow, Log Forging, Privacy Violation, Path Manipulation, Race Conditions, Session Fixation, SQL Injection, System Information Leak, and Unreleased Resource.
2. FSCA sorts, filters, prioritizes Analysis of Software Artifacts April 24, 2007 3 and categorizes issues found in various forms for easy viewing and analysis through Audit Workbench and Fortify Manager.
3. The results can also be exported as a report in formats like html and xml.

GQ. 3.6.5 Enlist OWASP Secure Code Review? Explain any 4 in details.

☞ OWASP Secure Code Reviews

The following is OWASP SCR checklist :

1. Input Validation
2. Output Encoding
3. Authentication and Password Management
4. Session Management
5. Access Control
6. Cryptographic Practices
7. Error Handling and Logging
8. Communication Security
9. System Configuration
10. Database Security
11. File Management
12. Memory Management
13. General Coding Practices

1. Input Validation

- You should conduct all data validation on a trusted system (For Example: server)
- First Identify all data sources and classify them into trusted and untrusted. Validate all data from untrusted sources (For Example: Databases, file streams, etc.)
- There should be centralized input validation routine for application
- State proper character sets (for example:"UTF-8" for all input sources.
- Before validating encode data to a common character set
- All validation failures should result in input rejection
- Validate for expected data types
- Validate data range
- Validate data length
- Whenever possible, validate all input against a white list of allowed characters.

2. Output Encoding

- Run all encoding on a trusted system (For example: The server)
- Exploit a standard, tested routine for each type of outbound encoding
- Contextually output encode all data returned to client that originated outside the application's trust boundary. (For example: HTML entity encoding), but does not work in all cases
- Encode all characters unless they are known to be safe for the intended interpreter
- Contextually sanitize all output of untrusted data to queries for SQL, XML, and LDAP
- Sanitize all output of un-trusted data to OS commands

3. Authentication and Password Management

- Require authentication for all pages and resources, except those specifically intended to be public
- All authentication controls must be enforced on a trusted system (e.g., The server)
- Establish and utilize standard, tested, authentication services whenever possible
- Use a centralized implementation for all authentication controls, including libraries that call external authentication services
- Segregate authentication logic from the resource being requested and use redirection to and from the centralized authentication control
- All authentication controls should fail securely
- All administrative and account management functions must be at least as secure as the primary authentication mechanism
- Password hashing must be implemented on a trusted system (e.g., The server).
- Use only HTTP POST requests to transmit authentication credentials
- Notify users when a password reset occurs
- Prevent password re-use
- Disable "remember me" functionality for password fields
- Re-authenticate users prior to performing critical operations

4. Session Management

- Use the server or framework's session management controls.
- Session identifier creation must always be done on a trusted system (e.g., The server)
- Session management controls should use well vetted algorithms that ensure sufficiently random session identifiers

- Set the domain and path for cookies containing authenticated session identifiers to an appropriately restricted value for the site
- Logout functionality should fully terminate the associated session or connection
- Logout functionality should be available from all pages protected by authorization
- If a session was established before login, close that session and establish a new session after a successful login
- Generate a new session identifier on any re-authentication
- Do not allow concurrent logins with the same user ID
- Set cookies with the Http Only attribute, unless you specifically require client-side scripts within your application to read or set a cookie's value

5. Access Control

- Use only trusted system objects, for example: server side session objects for making access authorization decisions.
- Use a single site-wide component to check access authorization. This includes libraries that call external authorization services.
- Access controls should fail securely.
- Deny all access if the application cannot access its security configuration information.
- Segregate privileged logic from other application code.
- Restrict access to files or other resources, including those outside the application's direct control, to only authorized users.
- Restrict access to protected URLs to only authorized users
- Restrict direct object references to only authorized users.
- Restrict access to services to only authorized users
- Restrict access to application data to only authorized users.
- Restrict access to user and data attributes and policy information used by access controls

6. Cryptographic Practices

- All cryptographic functions used to protect secrets from the application user must be implemented on a trusted system (e.g., The server)
- Protect master secrets from unauthorized access
- Cryptographic modules should fail securely
- All random numbers, random file names, random GUIDs, and random strings should be generated using the cryptographic module's approved random number generator when these random values are intended to be un-guessable
- Establish and utilize a policy and process for how cryptographic keys will be managed

7. Error Handling and Logging

- Do not disclose sensitive information in error responses, including system details, session identifiers or account information
- Use error handlers that do not display debugging or stack trace information
- Implement generic error messages and use custom error pages
- The application should handle application errors and not rely on the server configuration
- Properly free allocated memory when error conditions occur
- Error handling logic associated with security controls should deny access by default
- Log all input validation failures
- Log all authentication attempts, especially failures
- Log all access control failures
- Log all system exceptions

- Do not store passwords, connection strings or other sensitive information in clear text or in any non-cryptographically secure manner on the client side
- Do not include sensitive information in HTTP GET request parameters
- Implement appropriate access controls for sensitive data stored on the server.

8. Communication Security

- Implement encryption for the transmission of all sensitive information
- TLS certificates should be valid and have the correct domain name, not be expired, and be installed with intermediate certificates when required
- Failed TLS connections should not fall back to an insecure connection
- Utilize TLS connections for all content requiring authenticated access and for all other sensitive information
- Utilize TLS for connections to external systems that involve sensitive information or functions
- Utilize a single standard TLS implementation that is configured appropriately
- Specify character encodings for all connections

9. System Configuration

- Ensure servers, frameworks and system components are running the latest approved version
- Ensure servers, frameworks and system components have all patches issued for the version in use
- Turn off directory listings
- Restrict the web server, process and service accounts to the least privileges possible
- When exceptions occur, fail securely
- Remove all unnecessary functionality and files
- Remove test code or any functionality not intended for production, prior to deployment
- Define which HTTP methods, Get or Post, the application will support and whether it will be handled differently in different pages in the application
- Implement a software change control system to manage and record changes to the code both in development and production

10. Database Security

- Use strongly typed parameterized queries
- Utilize input validation and output encoding and be sure to address meta characters.
- Ensure that variables are strongly typed
- The application should use the lowest possible level of privilege when accessing the database
- Use secure credentials for database access
- Close the connection as soon as possible
- Remove or change all default database administrative passwords. Utilize strong passwords/phrases or implement multi-factor authentication
- Remove unnecessary default vendor content
- The application should connect to the database with different credentials for every trust distinction (e.g., user, read-only user, guest, administrators)

11. File Management

- Do not pass user supplied data directly to any dynamic include function
- Require authentication before allowing a file to be uploaded
- Limit the type of files that can be uploaded to only those types that are needed for business purposes

- Validate uploaded files are the expected type by checking file headers.
- Prevent or restrict the uploading of any file that may be interpreted by the web server.
- Turn off execution privileges on file upload directories
- Do not pass user supplied data into a dynamic redirect.
- Do not pass directory or file paths, use index values mapped to pre-defined list of paths
- Never send the absolute file path to the client
- Scan user uploaded files for viruses and malware

12. Memory Management

- Utilize input and output control for un-trusted data
- Double check that the buffer is as large as specified
- Check buffer boundaries if calling the function in a loop and make sure there is no danger of writing past the allocated space
- Truncate all input strings to a reasonable length before passing them to the copy and concatenation functions
- Use non-executable stacks when available
- Avoid the use of known vulnerable functions (e.g., printf, strcat, strcpy etc.)
- Properly free allocated memory upon the completion of functions and at all exit points

13. General Coding Practices

- Use tested and approved managed code rather than creating new unmanaged code for common tasks
- Use checksums or hashes to verify the integrity of interpreted code, libraries, executables, and configuration files
- Utilize locking to prevent multiple simultaneous requests or use a synchronization mechanism to prevent race conditions
- Protect shared variables and resources from inappropriate concurrent access
- Do not pass user supplied data to any dynamic execution function
- Restrict users from generating new code or altering existing code
- Review all secondary applications, third party code and libraries to determine business necessity and validate safe functionality, as these can introduce new vulnerabilities
- Implement safe updating

Chapter Ends...

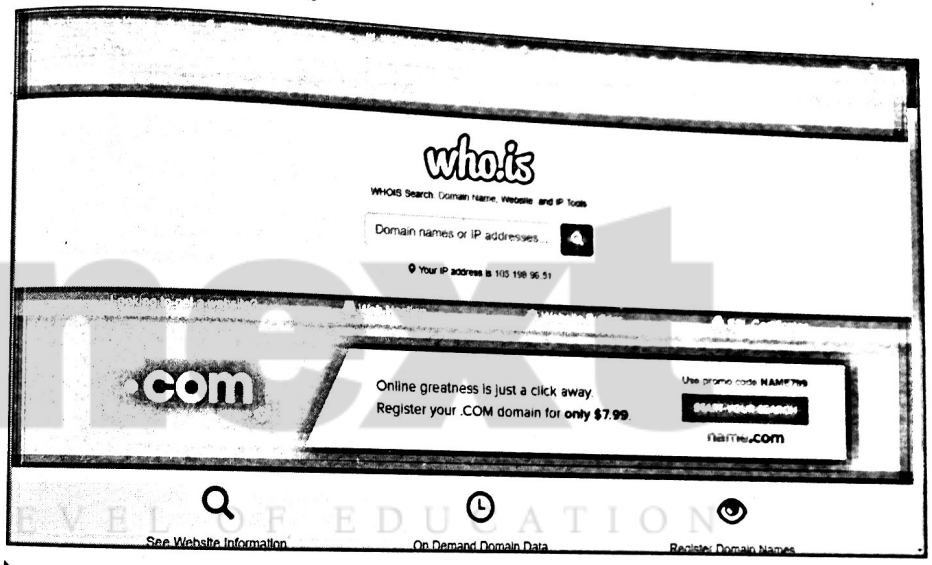
❑❑❑

LAB MANUAL

Practical No 1 : Use Google and Whois for Reconnaissance

Using who.is

Step 1: Open the "WHO.is" website



Step 2 : Enter the website name and click on the "Enter button".