Unit II

CHAPTER 4

Internet Forensic

Syllabus Topic : Introduction to Internet Forensics

4.1 Introduction to Internet Forensics

Q. 4.1.1 What is internet forensics ? List out the internet crimes ?

(Ref. Secs. 4.1 and 4.2) **(5 Marks)**

- ***In Computer forensics*** we study how computers are involved in the crimes. We get the information from the hard drive related to the cases fraud, to blackmail, identity theft, and child pornography. In ***Internet forensics*** the focus is the Internet at large rather than the individual machine. It is challenging to identify criminal activity and people around the globe.
- Internet spawn crimes are the crimes that are internet oriented. Internet is used as center of crime by criminals to do their bidding.
- Many times these criminals take advantage of certain situation having heavy impact thus leading many people to get trapped into their fraudulent plans. Internet spawn crimes are hard to detect since after earning enough gains or completing their tasks these cyber-criminals wash off their cyber-footprints and return to shadows until next event hits.
- Internet is used as a means of communication for many types of criminal activity.
- Spam is one of the activity were unwanted emails are the burdens on many servers each day. Companies are spending huge amount to control it to increase the productivity. As computer savvy people focus on spam mail and it results in wastage of time. People may look into the contents which involved scam. The aim of this spam is to get your credentials like credit card number.

- ***Phishing*** is the type of activity; it is a fraud that involves fake web sites. These fake web sites look like those of banks or credit card companies. A phishing email is sent away like most other spam, but it attempts to attract victims by appearing to come from a well-known, legitimate business like HDFC bank or Amazon.

- The message tells you to click the URL and then direct you to the fake website which looks like the original web site. This website then asks the user to enter the account information and personal data online.

- Computer ***viruses*** and ***worms*** is another activity, initially it was regarded as the malicious creations of people who wanted to show off their programming skills and wanted to "get in the face" of computer users around the world. It infects the computer. Today's Viruses affects the antivirus software and stop such tools from being installed on an already infected system.

4.2 Internet Crime

Q. 4.2.1 What is internet forensics ? List out the internet crimes ?

(Ref. Secs. 4.1 and 4.2) **(5 Marks)**

- Internet crime is stated as – An illegal activity that involves a computer system, where the system as a whole is used as a device for committing a crime.

- The following are the types of Internet Crime :

1. Password trafficking
2. Trademark counterfeiting
3. Data transfer theft
4. Computer intrusion (i.e. hacking)
5. Computer output theft
6. Desktop forgery
7. Wrongful programming
8. Child Pornography or Exploitation
9. Internet Fraud
10. Internet harassment
11. Information transfer theft.

➜ **1. Password trafficking**

Misusage and illegal selling of individual's password.

➜ **2. Trademark counterfeiting**

Stealing other individuals' thoughts and whatever else that could be copyrighted, and offering them or abusing them for individual addition.

➜ **3. Data Transfer theft**

It includes Public and private representatives who uses organization's chance and cash, surf the PC or play diversions without appropriate approval. This sort of conduct in numerous occasions is not acknowledged by directors, but rather there's little approach to manage it.

➜ **4. Computer Intrusion**

Stated as "it is an illegal access by any person using a computer and any other communications tool to break computer security or avoid it to enter into a system."

➜ **5. Computer Output theft**

Thieves take data that originate from individual or organization PCs for the sole purpose of discovering mystery or individual data. They do this by taking PC printouts, mailing records, client records, and so forth.

➜ **6. Desktop Forgery**

With PC innovation and desktop distributed projects, hoodlums duplicate authority letterhead, records, and travel permits, conception endorsements, and money receipts for individual increase.

➜ **7. Wrongful Programming**

Wrongful programming violations happen when somebody changes a PC program and guides it to control data on the system or somebody's close to home data. This is a more entangled wrongdoing than most others

➜ **8. Child Pornography or Exploitation**

Illegally setting a small child obscenity on the web so as to make a benefit, or taking a gander at small child erotic entertainment for joy.

9. **Internet Fraud**

Any type of fraud blueprint that uses internet for example chat rooms, emails, or Web sites - to present fraudulent proposals to prospective victims, to organize fraudulent transactions, or to send the proceeds of fraud to financial institutions.

10. **Internet Harassment**

Stalking or badgering any individual through the utilization of the web.

11. **Information Transfer Theft**

Tapping so as to steal of individual data into a telephone line outside one's home and running a line straightforwardly into one's own PC. This should frequently be possible without one notwithstanding knowing it through split lines.

Syllabus Topic : World Wide Web Threats, Hacking and Illegal Access

4.3 World Wide Web Threats, Hacking and Illegal Access

1. There are many forms of intrusion and attacks. As compare to internal threats external threats get the more attention. Attacker may or may not have computer knowledge and skills to launch an attack.
2. The hackers learn the details of the computer system by performing attacks. To access the system illegally they try to get the user credentials.
3. Few of the attacks are unintentional which happens because of lack of knowledge.
4. Attacks can be done without gaining entry to the network or system, for example DoS attacks. The DoS attacks overload network resources to make the network unavailable to genuine users, but the attacker never gains access to any computer on the network. It's imperative, then, to be exact when we allude to particular computer crimes.
5. DoS attackers ought not to be referred to as intruders when no interruption happens. In like manner, not all intruders can precisely be named attackers in spite of the fact that the individuals who get access and then destroy information or plant viruses are legitimately called by both names.

Attack types

The attack types are relying on upon how an intruder get passage to your computer or network and what things the attacker does once he or she has get entry. The classification of attack is done as follows :

1. Pre-intrusion/attack activities
2. Password-cracking techniques
3. Technical exploits
4. Malicious code attacks

Let's see the types of attacks that fit into each category.

4.3.1 Pre-intrusion/Attack Activities

Q. 4.3.1 Explain pre-intrusion/attack activities? *(Ref. Sec. 4.3.1)* (5 Marks)

- The attack procedure is break into the following steps :
  1. Pre-attack
  2. Initial access
  3. Full system access
  4. Planting back doors for future access
  5. Covering tracks.
- The pre-attack phase focuses on gathering information. Pre-attack information gathering contains the goal of the hack, target of attack and finding the flaws of the target which can be exploited to do the hack. The pre attack phase also include few steps to hide the attackers identity or put some introduction program or devices in place to collect the information or make it easy to access the system when they want to carry out attack. Some particular pre attack activities include:
- To identify potential targets and their flaws
  - Perform Port scanning
  - IP spoofing to hide the attacker's identity.
  - Inserting Trojans on the target system.
  - Inserting tracking devices and software on the target system
  - Placing sniffers in place to capture transmissions to and from the target system.

Port Scans

- A port is a point where data enters or leaves a computer.
- When the port scanning is performed the attacker will get the information about the standard ports and services are running and responding on the target system, operating systems are installed on the target system, and applications and versions of an application are present.
- Port scanner is a software program used to determine the TCP/UDP ports are open on a given system. The port scanners are sometimes used by the administrator to check the vulnerabilities in their own system. If they found any vulnerability they will correct it before the intruder come to know about it. The SATAN (Security Administrator's Tool for Analyzing Networks) tool is used for the port scanning.
- Scanning is used for many purposes before penetration or attack :
  1. **Target enumeration :** Locate the host system which is open to attack.
  2. **Service identification :** It is also used to identify vulnerable ports and services on the target system
  3. **Target identification :** It is used to identify the target system.
- There are three type of port scan :

1. TCP Connect
2. TCP SYN/Half-Open
3. FIN

➜ 1. TCP Connect

The TCP connect scanning make use of TCP open system call. The TCP open system call is provided by the operating system kernel to connect to particular ports on the target host. The TCP connect scan completes the three way handshake and the application on destination port will reply to the connection attempt.

➜ 2. TCP SYN/Half-Open

TCP SYN scanning is responsible for sending the SYN packet to the target host. The target host then respond with the SYN+ACK. In case when the target host is not listening to a specific port but it is alive then RST packet will be received. As this technique do not complete the three way handshake so it is mysterious and not logged by the target host.

3. FIN

FIN packet is send to the target machine to close the connection. When FIN packet is send and the target host is alive but not listening on a specific port then it reply with RST packet.

Address Spoofing

- Address spoofing means the hacker use spoofed addresses to con other computers and fool them into thinking a message originated from a different machine.
- The most popular spoofing is IP spoofing, there are some other spoofing method used by hackers which are ARP spoofing, Web spoofing, and DNS spoofing.

IP Spoofing

- IP spoofing means changing the header of message; this indicates that message is not come from the true source. The attacker computer impersonates another machine and makes the recipient to accept messages which come from the attacker machine. Trusted ports are spoofed and it permits the hacker to get a message from the firewall or router.
- Proper configuration of firewall is necessary to protect from the IP spoofing. The IP spoofing is used in combination with one of the other types of attacks. For example, a spoofed address is used to hide the true IP address of the attacker in Ping of Death, Teardrop, and other attacks.
- Remote Procedure Call (RPC) services, the X Window system, the UNIX services (rlogin, rsh, and so on) and any service that uses IP address authentication are all susceptible to IP spoofing.
- Finding the address of the trusted host is the goal of the attacker. Normally the communication between the sender and the receiver is intercepted by the attacker. The attackers frequently perform a DoS attack against the trusted host to prevent trusted host from communicating on the network.
- Then next step is to change the packet headers to make it look as though the attacker's messages are coming from the trusted host, and the packets are sent to a service or port that uses address authentication.
- The biggest difficulty of IP spoofing is that the attacker must guess the proper sequence number of the trusted machine.

ARP Spoofing

- At the time of deriving frames from packets, the Ethernet header knows only the destination IP not the MAC address. The header needs to determine the MAC address, given the IP of the machine. This is where ARP comes in. The Address Resolution Protocol (ARP) maintains the ARP cache. ARP table maps unique network IP of the machine to unique MAC addresses.
- This cache is necessary because the MAC address is used at the physical level to locate the destination computer to which a message should be delivered.
- ARP spoofing involves changing the MAC to IP address entries, causing traffic to be redirected from legitimate system to unauthorized system of the attacker's choice.
- For a particular IP address if there is no entry in the ARP cache then ARP sends a broadcast message to all the computers on the subnet and request that the machine with the IP address in question respond with its MAC address. This mapping then gets added to the ARP cache. ARP spoofing, also known as ARP poisoning.

DNS Spoofing

- DNS spoofing attack is based on the concept of domain name server. A DNS is a table that converts the domain names like XYZ.com into network addresses like 211.217.74.130; this process is known as resolving the domain.
- DNS spoofing refers to two methods of causing a DNS server to direct users incorrectly :
  1. Poisoning of the DNS cache results caching the false entries and servers' direct users to the wrong Web sites or e-mail being sent to the wrong mail servers.
  2. Predicting the DNS server's send request by using the recursive mechanism of DNS and respond to it with fake information.
- Either of these techniques permits the attacker to capture the victim's mail or to set up spoofed Web pages that give clients inaccurate data. This technique can even be utilized to con the victim into giving individual data through Web form.

Placement of Trojans

- Trojans are also known as Trojan horse. This software is programs that appear as legitimate and does something else in addition to or instead of their ostensible purposes.
- In the pre-attack phase, a hacker can plan a Trojan program on the victim's machine, this program installs keystroke-logging programs to gather information for the main attack or later the attacker will use that information to get into victims machine.

Placement of Tracking Devices and Software

- Another way to attack is place a physical tracking device on a system if an attacker has onsite access to the victim system. The device is very small and can be installed in less than a minute.
- We just have to unplug the keyboard from PC and then plug the logger into the PC's keyboard port. This device is not noticeable to most users. Inside the logger there are a microchip and a non-volatile memory chip. Depending on the memory size it can record the pages of keystroke.
- There is no need to install software for the logger to work. The loggers are compatible to work with different operating systems. This device draws the power from the computer so no battery is required. After capturing the strokes the attacker remove the device and attach it to different computer.
- The captured data is password protected and after entering the correct password it can be read in notepad or any other text editor and then save the data to a file. Now attacker can erase the data in the device to use it again.

Placement of Packet Capture and Protocol Analyzer Software

- Network monitors are also known as protocol analyzers. These protocol analyzers allow the administrators to capture and analyze the network traffic for troubleshooting purposes or to monitor network activity.
- To capture the packets secretly the hackers use this tool and then hacker read the information from the packets. The network sniffers are also used to listen the activity on the wire.
- Hackers use this tool to collect the network data and analyze it on the spot. Some triggers can also be set for some events or data across the wire.
- For example, when some particular keywords in the mail communication move through the network, the tool allows user to capture only those frames that they are interested in.

Prevention and Response

The preventions for the preattack activities are:

1. Use scanner to find open doors to their networks, as such there is no way to prevent port scanning.
2. Do the address verification on the router to prevent the IP spoofing. After address verification do encrypted authentication and configure the router to reject the messages which comes from outside but appear as internal.

3. Use static ARP tables to prevent ARP spoofing. Another way prevent ARP spoofing is MAC binding. MAC binding can be enabled on the network switches. It allows the automatic updating. But if there is IP address with associated MAC address then the association between them cannot be changed except the administrative action.
4. There are some tools available which monitors the changes to the cache and provides the automatic notification to administrators so they will be aware of any attempts to use ARP spoofing.
5. Use latest version of DNS software on DNS server to prevent the DNS spoofing.
6. Configure the firewalls properly so that Trojan will be kept outside the network or use the Trojan removal software.
7. Do proper physical examination of the cable to prevent from the Keystroke-logging devices or use Antikeystroke logger programs to scan for keystroke logging activity and detect software-based loggers.

4.3.2 Understanding Password Cracking

Q. 4.3.2 Explain password cracking techniques? *(Ref. Sec. 4.3.2)* **(5 Marks)**

Many times people use name and password to get the access of particular system. Passwords can be cracked by the attacker and the attacker can use that password to impersonate the legitimate user. There are many ways to crack the password:

1. Use the Brute Force
2. Recover and exploit the password stored on the system.
3. Make use of password decryption software
4. Social engineering

➜ **1. Brute Force**

- In the brute force attack the attacker will try all the possible combinations to crack the password until the attacker get the success. The brute force attack is performed manually. This attack is also known as dictionary attack. Password cracking is also used for legitimate use, for example, an employee make left the job suddenly, an employee may die and it may be possible an employee may forget his/her password.
- So, to retrieve the important file password cracking is used. This is also known as password recovery. It is advised to create ling and complex password. There are some tools available which allow dividing the task into parts and also using many machines simultaneously to work on it, this technique is called distributed attack.

2. Recover and Exploit the password Stored on the system

- Guessing a password is a tedious job. If the attacker's list of the password which may be on the hard disk of a computer. Some people use different password in the organization for different purposes so they store there password on the system's hard disk or somewhere, where they can get it in case if they lost the stored copy on the system. The cracker just has to acquire these files.
- Some people do not store the password in the plain text format; they store the password in encrypted or hashed format. If the cracker can get the encrypted password file, then the attacker use a software program. This program uses all the hash function the system uses and encrypts possible passwords, then compare the result with the encrypted passwords in the password file. This method is known as *comparative analysis.*

Interception of Passwords

- Crackers every time do not capture the password file or guess the password. When the password send across the network through the remote access connection in the form of plain text, then that password may get intercepted by the attacker. They use sniffer software for interception.
- Another technique to intercept the password is keystroke logger. The keystroke logger is hardware device or a software program, it captures and records the every character including password.
- A device time domain reflect meter (TDR) is used to detect the unauthorized packet sniffer on the wire. It sends the pulse down the cable and generates a graph of reflections that are returned.
- By reading the graph we can find where the unauthorized devices are attached to the cable.
- There are also some techniques like PING, DNS and ARP also help to catch the unauthorized sniffers.

3. Make use of Password Decryption Software

- One byte patching : The one byte patching technique is used to decrypt the program. It decrypts the password simply by changing one byte in the program.
- Known plain-text method : In this technique is used with algorithms. The attackers already have obtained one or more decrypt files the attacker use same methods to decrypt the other files which contains the same algorithm. This technique is used to attack the password protected files like .zip, .rar, and .arj files.

4. Social Engineering

- Social engineering requires the social abilities and the individual communication to make somebody to uncover security related data and maybe even to accomplish something that allows an attack.
- The fundamental thought process behind the social engineering is to convince the victim to be useful.

Prevention and Response

Password is the main and the first line of defence in some system and networks. To prevent the password from cracking:

- Use long password
- Use special characters
- Avoid actual names and words
- Do not tell your password to anyone
- Do not write the password
- Change the password regularly.

Protecting the Network against Social Engineers

- Social engineering is a big challenge to the administrator. Some people on the network are vulnerable to the network. The intruder may woe the user by telling the stories of extra cost will incur if the user spends extra time for verifying their identity.
- The attacker may impose himself as a top authority of the company and he may threaten the employee with loss of job or any other action if the employee doesn't cooperate. In social engineering prevention comes through the education rather than technical solution.

4.3.3 Understanding Technical Exploits

Q. 4.3.3 Explain technical exploits? *(Ref. Sec. 4.3.3)* **(5 Marks)**

The attacker uses various techniques to get the access of system and network. The techniques used by the attacker exploits the characteristics of protocol, operating system and the application software used on the targeted network or the system. There are many technical exploits which the hacker uses to get the access of network.

Protocol Exploits

- The important characteristic of a protocol is the handshake method which is used by TCP to establish the connection for communication.
- The attacker exploits this characteristic by flooding the targeted system to the point so that the system is unable to communicate with authorized user. They also manipulate the network protocol and flood the network server so that no authorized user can communicate.

DoS Attacks That Exploit TCP/IP

There are many attacks which exploit a variety of characteristics of the TCP/IP protocol suite. We are going to see in this section how DoS attacks work and the attack types like:

1. **DNS DoS attacks :** This attack exploit the DNS protocols.
2. **SYN/LAND attack :** This attack exploit the TCP handshake process.
3. **The Ping of Death :** This attack uses a killer packet to flood a system
4. **Ping flood, fraggle, and smurf attacks :** These are the methods used to flood the network or server.
5. **UDP bomb and UDP snork :** This attack exploit the User Datagram Protocol
6. **Teardrop attacks :** This attack exploit the IP packet header fields.
7. **Exploits of SNMP :** This SNMP exploits are included with most TCP/IP implementations.

What Is Denial of Service ?

- A Denial of Service attack do not does any damage or not steals any information. This attack brings down the network and denies the services to the legitimate users. The software for DoS attacks is easily available.
- The purpose of the DoS attack is to make the network inaccessible by generating the network traffic that crashes the server, floods the router or make the network devices functions improper. DoS attack can be performed by tying up the servers resources like flooding the memory and CPU.
- Distributed DoS (DDoS) attacks use mediator computers, called agents. On this computer programs called as zombies have been secretly installed. Then the hacker activates these zombie programs remotely, causing the mediator computers to simultaneously launch the actual attack. The attack comes from the mediator computers running the zombie programs on the network. So, the hacker can easily hide the true origin of the attack.

DDoS attacks poses two layer threats, it not only attack the network but also crashes the servers and prevents the servers incoming and outgoing traffic.

1. DNS DoS

- The difference between the DNS query and the DNS response is exploited by the DNS DoS attack. In this attack the networks all the bandwidth is tied up by bogus DNS queries. To multiply the traffic the attacker uses the DNS servers as amplifiers.
- The attackers begin the attack by sending small DNS queries that contains the spoofed IP address of the intentional victim to each DNS server.
- In response to the small queries much larger size data/response is sent. Because of this the link becomes congested and DoS take place.

2. SYN/LAND Attacks

- The TCP's three way handshake connection establishment process between two computers is exploited by the SYN attacks. The TCP handshake has the following steps :
  1. Client sends the SYN request.
  2. The server sends an acknowledgement and SYN, it means client's machine request is acknowledged and SYN request is send to client. The client and the server must have to synchronize the sequence numbers.
  3. The client sends the ACK to server to acknowledge the server synchronization request.
- When client and server acknowledge each other's request, the handshake is successfully completed.
- A SYN attack sends the multiple SYN packets to the targeted system whose IP addresses are bad. They flood the target system with these SYN packets. As a result this makes the system to send the response as SYN/ACK messages.
- The main problem arrives when the system wait for the ACK message from the client who comes in response to SYN/ACK message, but the SYN/ACK messages are waiting in the queue. The queue size is limited for the no of messages.
- When the queue become full, all subsequent incoming SYN packets get ignored. In order for a SYN/ACK to be removed from the queue, an ACK message must have to be returned from the client. Otherwise, the time interval run out and terminates the three-way handshake process. So the request queue remains full and the services to the legitimate users are denied.

- The LAND attack is little bit different from the SYN attack. In this attack SYN packets flood from the same spoof IP address is send to the targeted system. If the source IP address of computer is from the internal network then the LAND attack can be prevented by filtering out incoming packets.

➜ 3. The Ping of Death

In the ping of death attack the attacker creates the IP packets larger than the 10MB, which is the maximum allowed size by IP specifications. So, these packets may crash, hang or reboot the target system.

➜ 4. Ping Flood/Fraggle/Smurf

- The ping flood attack is also known as ICMP flood. The attacker sends the number of ping packets to the Winsock which floods the server. This causes the server not to respond to server ping activity responses and the connections will be time out. If we found a huge amount of modem activity then there may be chances of ping flood attack or you can also called it as ping storm.
- The fraggle attack is related to the ping flood. In the fraggle attack the attacker sends the ping packets to a subnet using a spoofed IP address. This action causes all the computers on the subnet to respond to the spoofed addresses and results in flood of echo reply messages.
- The smurf attack is a type of brute-force attack and also a variation of the ping attack. This attack uses a ping packet, but with the two twist. First the attacker selects the network of innocent victims.
- The attacker spoofs the source IP address in the ping packet so that it appears to come from the victim. After this attacker sends this request to the network in broadcast mode by setting the last byte of the address to all 1's. Then the broadcast mode packets are distributed to all the hosts on the network. Smurf attack does more damage than other forms of DoS like SYN flood.

➜ 5. UDP Bomb/UDP Snork

- In UDP Bomb an attacker uses UDP and few of the services that echo packets on receipt to make service-denying network congestion by creating a flood of UDP packets between two target systems. The UDP chargen is a testing tool that generates a series of characters for each packet that it receives.
- Then it sends packets to another system's UDP echo service, which echoes every character it receives.

- The port for UDP chargen is 10. This testing tool is exploited by sending the flow of echoes goes back and forth between the two systems, and it causes the congestion in the network. This is called UDP Bomb or Packet Strom.
- Use firewall to filter the ports of service to prevent and protect from attack. Also disable unnecessary UDP services on each computer.
- The snork attack is like the UDP bomb. It uses a UDP frame that has a source port 9(chargen) or 7 (echo,) with a destination port of 135(Microsoft location service).The result of this attack is same as the UDP bomb. It is a flood of unnecessary transmissions that can slow performance or crash the systems that are involved.

➜ 6. Teardrop Attacks

- The teardrop attack misuses the features designed to improve the network communication. As we know network IP datagram is variable in length. The datagram protocol allows sending single data unit to fragment and transmit separately.
- Every fragment indicates its length and relative position within the data unit. So the receiving end is responsible for reassembling the fragment into a single data unit. In teardrop attack, the attacker sends series of datagram that cannot fit together properly. It may happen that the operating system locks with the partial data units and cannot reassemble the data and causes DoS.

➜ 7. SNMP(Simple Network Management Protocol) Exploits

- To monitor network devices and manage networks SNMP tool is used. SNMP is a set of protocols and it uses PDU (protocol Data Units) messages over the network to different machines or devices that have SNMP agent software installed.
- The SNMP agent software maintains Management Information Bases (MIBs). These MIBS contains information about the device. So, after receiving the PDUs by agent, they respond with information from the MIB.
- In some SNMP Vulnerabilities have been discovered, it provides a means for attackers to disable the devices or create a DoS.

☛ Source Routing Attacks

- The source routing attacks are supported by TCP/IP, it permit the sender of network data to route the packets through a specific point on the network.
- Source routing is of two types :

1. **Strict source routing :** The exact route is specified by the sender of data.

2. **Loose source record route (LSRR) :** The sender can specify certain routers (hops) through which the packet must pass.

- The IP headers contain an option called source root. This option allows the sender to dominate the routing decisions that are usually taken by the routers between the source and destination machines. The source routing is used by Network administrators :

1. To map the network.
2. Troubleshooting routing and communications problems.
3. To force traffic through a route that will give the best performance.

- Hacker exploit the source routing, they use it to reach private internal addresses on the LAN that usually would not be reachable from the Internet. So, they route the traffic through another machine that is reachable from both the Internet and the internal machine. Most of the routers prevent this attack by disabling the source routing.

Other Protocol Exploits

The hackers can also exploits the protocols like DNS, HTTP, CGI and other commonly used protocols.

Application Exploits

- Application programs have some weaknesses and application software exploits take advantage of this weaknesses.
- The weaknesses of the application programs are often called bugs. The intruder use application exploits to get unauthorized access to computers or networks or to crash or congest up the systems to deny service to others.

UNIX Exploits

- The main aim of many UNIX/Linux exploits is gaining root access. Unix root account is equal to the Administrator account on a Windows system. If a user will logged on to the root account then the user will have full control of the system.
- The user can also clear the logs to cover his tracks or the user can get the access of Super user ID (SUID) file which contains super user permissions. The user may run the script or exploit the bugs in Send mail or some other services.

Rootkit Attacks

- Rootkit attack is a group of programs which install a Trojan login replacement with a back door along with packet sniffer on UNIX boxes.

- The sniffer captures the network traffic, including user identification. The attacker gets the root account access with user identification.

NFS Exploits

- The Network File System (NFS) permits users to remotely mount disks on other computers one by one to access the files on the remote system. It makes the files on the remote disk available across the network.
- The nfsbug program is used to try out various techniques of mounting an NFS disk to determine if the remote computer is configured in such a manner as to permit remote mounting. If it will become successful, it allows the attacker full access to the remote file system and the attacker can then read or write to all the files.

Other UNIX Exploits

The other UNIX exploits are buffer overflow insecure default configuration and the flaws in the programming that hacker can use to compromise the network and system.

Router Exploits

- Now a day's many routers comes with the default administrator password. If the administrator does not change that password then the attacker may obtain that password. The attacker can alter the router configuration table.
- The routers also have backdoor password which will be used by the vendor's tech support personnel in case if the administrator forget the password so by using this password the vendor will help to get back it.
- The attacker can also create the DoS attack by altering the routing table entries to send the entire message to one destination.
- The attacker will send the spoofed RIP messages if the router is using the RIP (Routing Information Protocol) to dynamically update the routing table.
- The RIP messages can change the routing table entries without accessing the router directly. DoS attack causes the router to shut down.

Bug Exploits

The bugs are of following type :

- **Buffer overflows :** Buffer overflow occurs when the character input exceeds the buffer size.
- **Unexpected input :** Programmers do not consider what happens when invalid input is entered. This may cause the program to crash or open a door to the system.

- **Configuration bugs :** Configuration bugs are nothing but the ways of configuring the software that leaves it vulnerable to penetration. Software's like IIS, MSIE and MSOE are hackers favourite. Hackers always look for the ways to exploit it. ActiveX controls, JavaScript, and VBScript can be used to add animations or applets to Web sites or e-mail messages, but hackers can exploit these features, they write controls or scripts that permit them to plant the virus remotely, access data, or change or delete files on the hard disk of unaware users who visit the page or open the mail and run the script.

Mail Bombs

- A mail bomb is a means of flooding a mail server. This causes the mail server to stop functioning, which results in denying services to the users. This is a simple form of attack accomplished by sending an enormous quantity of e-mail to a specific user or system.
- Now days many programs are available on hacking website on internet to easily launch a mail bomb attack. It automatically sends floods of e-mail to a specified address. A number of types of mail-bombing methods are used against the Sendmail program. The methods are chain bombs, error message bombs, covert distribution channel and abuse of mail exploders.
- List linking is the mail bomb program. This program subscribes the targeted user to thousands of high volume internet mailing list; this mailing list fills the user's mailbox or mail server. Examples of list linking attacks are Voodoo, Unabomber. To avoid the mail bomb attack solution is block traffic from the originating network using packet filters.

Browser Exploits

- Web browsers are client software programs like MSIE, Netscape etc. These web browsers connect to the servers running Web server software such as IIS or Apache. Then it request Web pages through URL. The URL is a friendly address which represents an IP address and particular files on the server at that address.
- The browser receives the encoded file and interprets the code which determines how the page will be displayed on the user's monitor. There are many attacks preformed on the browsers.

Exploitable Browser Characteristics

- The browsers contain images, text sounds, and movies and also run the executable codes. The browser software also stores information of the computer and the user. This information gets uploaded to web server by the user or in response to code on a Web site.

These characteristics help to support for running code, allows Web designers to create pages to interact with users.

- Cookies help the user to set the preferences on sites which will be retained the next time they visit the site. The hackers exploit these characteristics. The hacker can program a Web site to run code that transfers a virus to the client computer via browse. This program erases key system files and plants a back door program which allows the hacker to take control of the user's system.

Web Spoofing

- Web Spoofing means the attacker can see or make the changes to the web pages that are transmitted from one machine to other machine. The web pages may contain important information like credit card details, passwords used to access the website.
- The attacker may use the JavaScript to route the web pages and information via the attacker's computer, which impersonates the destination Web server. The attacker can send a mail to the victim. The mail contains the link to the forged page or the attacker may put the link into the popular search engine. The SSL do not verify the hyperlinks that the user follows.

Web Server Exploits

- Web server is a program which stores the Web pages. These web pages are available to others across Internet. Public Web servers are always on risk because they are available to the internet to do what they want to do.
- Clients send transmission to request for the web pages. The web servers should be isolated from the network as they are vulnerable to the attack. Web server applications may contain bugs.
- For example, in 2001, in Microsoft's IIS software an error was discovered. This error exploited the code used for indexing feature, where the components get installed by default.
- When the code was running the hackers created the buffer overflows to take control of server and to change the web pages and bring down the system In Apache Web server the error was found in PHP scripting language that if exploited by an attacker, the attacker runs the arbitrary code on the system.

Buffer Overflows

- Buffer is a temporary memory with small size which holds the data. Many software programs use buffer memory to speed up processing. Buffer is also used to store changes

to data, the information in the buffer is copied to the disk. Buffer overflow occurs when more information is put into the buffer than its capacity to handle. The hacker deliberately overflows the buffer and exploits to run the malicious code.

- Overflows are of two types :

  1. Stack overflow 2. Heap overflow

- The stack and the heap are two areas of the memory structure. These are allocated when a program is run. Stack stores the function call and heap stores the dynamically allocated variables. Buffers have also allocated specific amount of memory. To attack the heap attacker uses buffer overflow attacker and tries to overwrite a password, file name or any other data. If the filename is overwritten then the user can open a different file and run it which was not intended to be run.

- In Unix system the command interpreter allows the attacker to execute the command with Super user privileges. In windows system overflow code is used to send a HTTP request for downloading malicious code of attacker's choice.

☞ Operating System Exploits

Some operating system or family of operating system exploits is unique. These attacks exploit particular characteristics of operating system code. Every operating system has its own vulnerabilities.

☞ The WinNuke Out-of-Band Attack

The out of band attack exploits the vulnerability of some Microsoft networks, thus this attack is also known as *Windows OOB bug*. The WinNuke program and variations like Sinnerz and Muerte create an OOB data transmission that crashes the machine to which it is sent. It works like this :

1. It establishes a TCP/IP connection using port 139 with a target system IP address.
2. The program uses the flag MSG_OOB in the packet header to send the data. The MSG_OOB flag instructs the computer's Winsock to send data called *out-of-band data*.
3. When this flag is received , the targeted Windows server anticipates that a pointer will the position in the packet where the urgent information closes, with typical information taking after, yet the OOB pointer in the packet made by WinNuke focuses to the end of the frame, with no information taking after.
4. The Windows machine does not know how to handle this situation and ceases communicating on the network. Service is denied to any users who subsequently attempt to communicate with it.

5. A WinNuke attack usually needs a reboot of the affected system to re-establish network communications.

☞ Windows Registry Attacks

The Windows Registry stores the critical information like system and application configuration and initialization information. This information is centralized but is vulnerable to hacker and attacker. The hacker can exploit the Windows registry by altering the information which may result in bringing down the system.

☞ Prevention and Response

The preventions which are taken to prevent the application, operating system and protocol exploits are :

- Make sure that the systems have latest security patches.
- Build the kernel with SYN cookies to protect the Linux system from the SYN attack. Some Unix systems have built in protection and edit the windows registry to protect against the SYN attack.
- Configure the routers against the smurf attack.
- Configure the router in such a way that it to filter out the incoming packets with a source IP address that comes from the local network.
- Configure a system in such a way that it ignore the router redirect.
- Configure the DNS server to respond with the refuse response against the suspicious query and DNS DoS attacks.
- Disable the SNMP when it is not needed.
- Disable ActiveX, JavaScript, Java and other active content in the Web browser.
- Use firewall and application gateway.
- Modify the routers default password and disable the backdoor password.

4.3.4 Attacking with Trojans, Viruses and Worms

Q. 4.3.4 Explain malicious code attacks? *(Ref. Sec. 4.3.4)* **(5 Marks)**

The attacker can damage the network and system by putting the various types of malicious program.

These programs are also known as virus. The more destructive malicious code also referred as malware. Some malware are:

1. **CIH/Chernobyl :** This malware infects the executable files and spread by running an infected file on a Windows 95/98 system. There are several variants of CHI. These are time bomb viruses which activated on predefined date and time when the defined date triggers the virus start overwriting the first 2048 sectors of every hard disk in the computer and wipe out the file allocation table and cause the hard disk appear to be erased. This virus also attempted to write to BIOS boot block to make the computer unbootable.

2. **Melissa :** Melissa virus distributed through e-mail. This virus was written in Visual Basic Application and embedded in Microsoft Word document. When anyone opened the infected document, the macro runs and sends itself to the first 50 address entries in every Microsoft Outlook MAPI. So these addresses were the mailing list addresses and result in rapid propagation of the virus. This virus produces mails in huge volume and causes the Denial of service on some email server.

3. **Code Red :** Code red was more than a worm. This virus spreads itself on the web servers running Microsoft's Internet Information Server software. Code red takes two steps infection and the propagation. The code red takes the advantage of the internet information server's vulnerability and overflows the buffer in the DLL (Dynamic Link library) to live in server's memory. Then to spread Code Red checks the IP address on port 80 of the computer to see if that web server is vulnerable.

4. **Nimda :** The Nimda virus made modifications to Web documents and executable files on the infected systems. This virus made different duplicates of itself and spread by means of email, network shares, and through getting to infected Websites. This virus exploited vulnerabilities in IIS versions 4 and 5. It spread from client machines to Web servers through the back doors left by the Code Red II worm. Nimda allows attackers to execute random commands on IIS machines that had not been fixed, and results in denials of service.

There are three broad categories of the malware :

1. Trojans
2. Viruses
3. Worms

➜ **1. Trojans**

– Trojan is program that appears to be something that it is not. When the Trojan is installed the hacker can exploit the security and get the unauthorized access. Trojan programs can delete or modify the files.

- They transmit the file across the network to the attackers and they can also install viruses and other programs. It may be possible that an executable script on a website may install a Trojan. When the user access a web site that site can initiate the installation of a program to run automatically if and only if the web browser is configured to allow such programs to run. Trojans use default behaviour of Windows to masquerade their true nature.
- As the file extension is hidden by default, a hacker can name a file like flower.jpg and it will be shown in Windows Explorer as flower.jpg. It seems like an innocent graphics file when it is really an executable program. When we double click on the picture it will run the program. Trojans that are intended to permit a programmer unapproved access over the system is now and then called remote access Trojans, or RATs.

2. Virus

- Virus is a piece of self-replicating code embedded within another program (host). Viruses are associated with program files like Hard disks, floppy disks, CD-ROMS and Email attachments.
- Virus spread through Diskettes or CDs, Email or Files downloaded from Internet. Virus deletes or modifies files. Sometimes a virus also changes the location of files. Virus is slower than worm.
- Some types of viruses are :
  - **Boot sector viruses :** These viruses spread through a diskette. Virus is written to the master boot record on the hard drive and then it is loaded into the computer's memory every time the system is booted.
  - **Application or program viruses :** Application programs are executable programs. When the application program runs they infect the system. Viruses are also attached with some harmless program, when these programs get installed at the same time the desirable program gets installed.
  - **Macro viruses :** Macro viruses are embedded in documents which are using macros, for example Microsoft Word documents.
  - Viruses that are programmed to "go off " or are activated and destroy data or files on a mentioned date are called **time bombs or logic bombs.**

3. Worms

- The worm is code that replicate itself in order to consume resources to bring it down through computer network. It exploits security holes in networked computers. It exploits a weakness in an application or operating system by replicating itself.

- For spreading it can use a network to replicate itself to other computer systems without user intervention. Usually it does not infect files, Worms usually only monopolize the CPU and memory. Worm is faster than virus.

Prevention and Response

Take the following precautions to prevent your system from damage caused by Trojans, viruses, and worms.

- Turn off the Preview and/or HTML mail options in your e-mail client program.
- Avoid running the .exe that is executable files from unidentified sources including those attached to email or downloaded from Web destinations.
- From the unknown resources do not open the Microsoft Office documents without first disabling macros.
- Be careful while using the floppy which is used on other computer.
- Install and use firewall software.
- Install antivirus software and configure it such a way that it would run scans automatically at predefined times and updating the description files frequently.
- Use behaviour blocker tool which is used to prevent from the intrusion. These tools deny programs that have the ability to execute operations that have not been explicitly permitted.
- Use behaviour detection solutions for analyzing the executable files and assess whether they are likely to be hostile.
- To scan the system for changes use integrity checker software.

Syllabus Topic : Obscene and Incident Transmission

4.4 Obscene and Incident Transmission

Q. 4.4.1 Write a short note on obscene and incident transmission ? *(Ref. Sec. 4.4)* **(5 Marks)**

- Obscenity is considered as offence. Transmitting obscene data means transfer, pass, communicate a medium for transmitting, signal etc. Obscenity as "anything which is appears to the prurient interest or if its effect is tend to degrade and corrupt persons. Example of obscenity is child pornography.

- Punishment for Transmitting or Publishing Obscene Information in Electronic Form.
- In Section 67 of Information Technology Act, 2008, whoever transmits or causes to be transmitted in the electronic form any information which contains sexually expressive act or direct might be refused on first belief with detainment of either depiction for a term which may reach out to five years and with fine which may stretch out to ten lakh rupees and in case of second or resulting conviction with detainment of either portrayal for a term which may reach out to seven years and furthermore with fine which may stretch out to ten lakh rupees.

Punishment for Transmitting or Publishing of Data or Information Containing Sexually Expressive Act in Electronic Form

In Section 67 of Information Technology Act, 2008, whoever transmits or causes to be distributed or transmitted in the electronic frame, any material which contains sexual expressive act or lead, should be rebuffed on first conviction with detainment of either portrayal for a term which may stretch out to five years and with fine which may stretch out to ten lakh rupees. In case of second or ensuing conviction with detainment of either portrayal for a term, that may stretch out to seven years and furthermore with fine, which may stretch out to ten lakh rupees.

Punishment for Transmitting or Publishing of Data or Any Information Depicting Children in Sexually Expressive Act in Electronic Form

As per Section 67 of Information Technology (Amendment) Act, 2008[12], whoever

(a) Transmits or publishes or causes to be transmitted or published material in any electronic media form which portrays children engaged in sexually expressive act or behavior, or

(b) Creates, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes text or digital images or material in any electronic media form portraying children in any obscene or indecent or sexually expressive behavior, or

(c) Induces, Entices, cultivates children to online relationship with one or more children for any sexually expressive act or in a behavior that may offend a reasonable adult on the computer resource, or

(d) Facilitates Child abuse on online platform, or

(e) If any recordings are made on own abuse or that with others relating to sexually expressive act with children.

He shall be punished on first conviction with detainment for a term which may extend to five years along with a fine which may extend to ten lakh rupees. In the event of second or subsequent conviction with imprisonment of a term which may extend to seven years along with fine which may extend to ten lakh rupees.

As per Section 6 of the Indecent Representation of Women (Prohibition) Act 1986, any person who contravenes the provisions of this Act shall be punishable on first conviction with detainment which may extend to two years, along with fine which may extend to two thousand rupees. In case of a second or subsequent conviction with imprisonment for a term of not less than six months which may extend to five years along with a fine not less than ten thousand rupees but which may extend to one lakh rupees.

Syllabus Topic : Domain Name Ownership

4.5 Domain Name Ownership

Q. 4.5.1 Write short note on domain name ownership ? *(Ref. Sec. 4.5)* **(5 Marks)**

Domain name :

- Domain name is a string of characters. It is used as Internet identifier to simplify the Internet location of an entity's web site, for example ebay.com. The URL (Uniform resource locator) includes the domain name, for example http://www.yahoo.com. The server access the domain name.
- There are following concepts related to the domain:

1. **Registrar**

   It is a company that sells the domain name which is available to the clients to its relationship with one or more domain name registries.

2. **Registry**

   It is an entity that is responsible for giving out unique domain names within a particular country code or top level domain.

3. **WHOIS record**

   It is a record that gives detailed information for a particular domain name, which usually includes a registrant and an administrative contact.

   If you want to check the availability of the domain name then use the WHOIS record for the required domain name. you can also use the automated tools like gTLDs and ccTLDs.

DOMAIN NAME OWNERSHIP

- The Domain name ownership is obtained by accessing the WHOIS record for the domain name. There are few registrars who use the automated tools that create domain names including one or more terms and related WHOIS records.
- The registrant is the real domain owner, though he/she/it is not the person using the domain name. The administrative contact has the authority to alter the domain name, as well as changing registrant information and accepting change of registrars.

OBTAINING A WHOIS RECORD

- There are two types of domain extensions, centralized and decentralized. The centralized domains have extensions such as .us, .info, and .biz and the decentralized domain names have the extensions like .com and .Net.
- To get the WHOIS records for decentralized extensions, visit the registry to first identify the registrar associated with the domain name, after that visit the registrar to get the WHOIS record. To get the centralized extensions visit the registry.
- There are some sites that have the WHOis record, for example ALLWhois.com where you will get WHOIS records from a variety of registries and registrars.

STEPS FOR DOMAIN NAME INVESTIGATIONS

1. Determine ownership of the domain name.
2. Retain copies of the WHOIS record and content.
3. Check whether the entity is associated with additional domain names.
4. View prior versions of the domain name content.
5. Check metatags and keywords.
6. Perform a brand/trademark search.
7. Check for prior UDRP and court decisions.

Syllabus Topic : Reconstructing Past Internet Activities and Events

4.6 Reconstructing Past Internet Activities and Events

Q. 4.6.1 How to reconstruct past internet activities and events? *(Ref. Sec. 4.6)* (5 Marks)

Event Reconstruction

- Search techniques are used to find the incriminating information as it is considered as the suspect contains the all the data. It is also possible that the owner of the computer may not responsible for putting some data; an intruder may have done this by planting the virus, so the data may get generated automatically.
- To find out who is responsible, the investigator must reconstruct events in the past that caused presence of the objects. To reconstruct the event it is important to understand the computer functionality.
- There are many techniques for reconstructing the events; they are categorized according to the primary object of analysis. The two major classes are:

1. Log file analysis
2. File system analysis

1. Log file analysis

- A log file is a purposefully generated record of past events in a computer system; organized as a sequence of entries. An entry usually consists of a timestamp, an identifier of the process that generated the entry, and some description of the reason for generating an entry. It is common to have multiple log files on a single computer system. Different log files are usually created by the operating system for different types of events. In addition, many applications maintain their own log files.
- Log file entries are generated by the system processes when something important (from the process's point of view) happens. For example, a TCP wrapper process may generate one log file entry when a TCP connection is established and another log file entry when the TCP connection is released.
- The knowledge of circumstances, in which processes generate log file entries, permits forensic scientist to infer from presence or absence of log file entries that certain events happened. For example, from presence of two log file entries generated by TCP wrapper for some TCP connection X, forensic scientist can conclude that
  - TCP connection X happened.
  - X was established at the time of the first entry.
  - X was released at the time of the second entry.
- This reasoning suffers from implicit assumptions. It is assumed that the log file entries were generated by the TCP wrapper, which functioned according to the expectations of

the forensic scientist; that the entries have not been tampered with; and that the timestamps on the entries react real time of the moments when the entries were generated.

- It is not always possible to ascertain these assumptions, which results in several possible explanations for appearance of the log file entries. For example, if possibility of tampering cannot be excluded, then forgery of the log file entries could be a possible explanation for their existence.
- To combat uncertainty caused by multiple explanations, forensic analyst seeks corroborating evidence, which can reduce number of possible explanations or give stronger support to one explanation.
- Determining temporal order with timestamps.
  - Timestamps on log file entries are commonly used to determine temporal order of entries from different log files. The process is complicated by two time related problems, even if the possibility of tampering is excluded.
  - First problem : If the log file entries are recorded on different computers with different system clocks. Apart from individual clock imprecision, there may be an unknown skew between clocks used to produce each of the timestamps. If the skew is unknown, it is possible that the entry with the smaller timestamp could have been generated after the entry with the bigger timestamp.
  - Second problem: if resolution of the clocks is too coarse. As a result, the entries may have identical timestamps, in which case it is also not possible to determine whether one entry was generated before the other.

2. File system analysis

- In most operating systems, a data storage device is represented at the lowest logical level by a sequence of equally sized storage blocks that can be read and written independently.
  - Most file systems divide all blocks into two groups. One group is used for storing user data, and the other group is used for storing structural information.
  - Structural information includes structure of directory tree, file names, locations of data blocks allocated for individual les, locations of unallocated blocks, etc. Operating system manipulates structural information in a certain well-defined way that can be exploited for event reconstruction.
  - Detection of deleted files.
  - Information about individual files is stored in standardized file entries whose organization diers from file system to file system.

- In Unix file systems, the information about a file is stored in a combination of i-node and directory entries pointing to that i-node.
- In Windows NT File System (NTFS), information about a file is stored in an entry of the Master File Table.
- When a disk or a disk partition is first formatted, all such file set to initial "unallocated" value.
- When a file entry is allocated for a file, it becomes active. Its fields are filled with proper information about the file.
- In most file systems, however, the file entry is not restored to the "unallocated" value when the file is deleted. As a result, presence of a file entry whose value is different from the initial "unallocated" value, indicates that that file entry once represented a file, which was subsequently deleted.
- File attribute analysis.

– Every file in a file system is either active or deleted; has a set of attributes such as name, access permissions, timestamps and location of disc blocks allocated to the file.

– File attributes change when applications manipulate files via operating system calls.

– File attributes can be analyzed in the same way as log file entries.

- Timestamps are a particularly important source of information for event reconstruction.

– In most file systems a file has at least one timestamp. In NTFS, for example, every active (i.e. non-deleted) file has three timestamps, which are collectively known as MAC-times.

- Time of last Modification (M)
- Time of last Access (A)
- Time of Creation (C)

– Imagine that there is a log file that records every file operation in the computer.

– In this imaginary log file, each of the MAC-times would correspond to the last entry for the corresponding operation (modification, access, or creation) on the file entry in which the timestamp is located.

– To visualize this similarity between MAC-times and the log file, the mactimes tool from the coroner's toolkit sorts individual MAC-times of files; both active and deleted; and presents them in a list, which resembles a log file.

- Signatures of different activities can be identified in MAC-times like in ordinary log files.
- Following are several such signatures, which have been published.

Reconstructing past internet activities

To rebuild the past internet there are two methods :

1. Use DNS cache to find deleted browsing history
2. To recover lost browsing history files
3. To recover deleted history by using Google history.

These methods are used to recover the history from all the browsers like Chrome, Firefox, IE Edge etc.

1. Use DNS Cache to find deleted browsing history

DNS is Domain Name System, it is faster method to restore searches or history. The problem in this is, if the computer is restarted, it will not be able to help you find browsing history. DNS cache will work only when about everything is connected to the internet. So do not shut down the computer if you want to restore deleted browsing history for an app or video game Perform the following steps to restore the browsing history.

Press Windows + R,

type cmd and click OK. Or you can also type cmd in Windows search bar

Open Command Prompt, type ipcongif/displaydns and click Enter.

Then all your recently visited websites will be displayed. You can view all your recent browsing history and find those important websites back.

2. Use data recovery software to recover lost browsing history files

If you are not aware where the browsing history is saved then follow next path to check that the history file is deleted or not.

Internet Explorer: *C:\Users\(username)\AppData\Local\Microsoft\Windows\History*

Google Chrome :

C:\Users\(username)\AppData\Local\Google\Chrome\User Data\Default\local storage

Mozilla Firefox: *C:\Users\(username)\AppData\Roaming\Mozilla\Firefox\Profiles*

You can use the data recovery software to recover the deleted history files, for example, EaseUS Data Recovery Wizard, it recovers all deleted files including the browsing history data saved in your computer without any obstructions.

The following are the steps to recover the data :

launch software > choose file types(browser history files)

Scan device > recover found browser/internet history data.

➜ 3. Recover deleted history by using Google history

The Google history is not deleted if you delete the history from browser; it stores all browsing history, including all pages visited and all devices attached to your Google Account. This means, you can also recover that history from your Android phone.

The following are steps :

Go to Google History and sign in with the Google account

It will display the date and time, calendar that you use. Go to the date at which you would like to see the browsing history.

4.7 Exam Pack (Review Questions)

☞ Syllabus Topic : Introduction to Internet Forensics

Q. 1 What is internet forensics? List out the internet crimes? *(Refer sections 4.1 and 4.2)* **(5 Marks)**

☞ Syllabus Topic : World Wide Web Threats, Hacking and Illegal Access

Q. 2 Explain pre-intrusion/attack activities ? *(Refer section 4.3.1)* **(5 Marks)**

Q. 3 Explain password cracking techniques ? *(Refer section 4.3.2)* **(5 Marks)**

Q. 4 Explain technical exploits ? *(Refer section 4.3.3)* **(5 Marks)**

Q. 5 Explain malicious code attacks? *(Refer section 4.3.4)* **(5 Marks)**

☞ Syllabus Topic : Obscene and Incident Transmission

Q. 6 Write a short note on obscene and incident transmission ? *(Refer section 4.4)* **(5 Marks)**

Syllabus Topic : Domain Name Ownership

Q.7 Write short note on domain name ownership ? *(Refer section 4.5)* **(5 Marks)**

Syllabus Topic : Reconstructing Past Internet Activities and Events

Q.8 How to reconstruct past internet activities and events ? *(Refer section 4.6)* **(5 Marks)**

❑❑❑

Chapter Ends...

Unit II

CHAPTER 5

E-mail Forensics

Introduction

- Email is used to communicate with the two parties. Where file transfer taken place between the two servers on a particular port number. A client side application is required to compose an e-mail.
- The examples of client side application are yahoo mail, Web Client, MS Outlook, hotmail. It requires a Sender's identity, stores it as a file and then delivered to a destination user address through one or more number of servers.
- The Email communication makes the things simple, powerful and efficient. Email writing and communication have been under the focus of malicious intruders over the last few decades. Emails can be forged easily.
- Email abuse is also increasing day by day. Email crimes like spam, threatening mails, narcotic trafficking etc are also increased.

5.1 Email Clients and Servers

Q. 5.1.1 Write a short note on email forensics? *(Ref. Secs. 5.1 and 5.2)* **(5 Marks)**

- Email client message is made up of two parts that are header and the body. The header contains the information about the email origin, like the address from where it comes, how it reached to the destination and who send it. The body contains the message and attachment if any.
- Many organizations have their own mail server. Some Users dials for the internet service provider. When this user sends the mail that mail first go to the ISP server then ISP send that mail to receivers mail server.
- The message stays on the receiver server till the recipient retrieve it. An email server is a computer which runs on Unix, Windows or any other operating system. The server contains the software to manage the transmission and holds the messages.

- When we investigate the email crime, the internal corporate emails are easy to trace. They use Universal Naming Conventions (UNC) coupled with central authentication and controls. So it makes easy to find the sender and receiver of email.
- The email client performs task like listing all the messages in mailbox by displaying message header as well as the time and date of the messages. It also tells the senders and the size of the message. The client can view, compose or delete the message.
- The email server is having the list of all the accounts. It have text file for each account. When a person click the send button to send the mail. It passes the mail to the mail server with sender and receiver name and message. The server formats this information and appends it to the bottom of the recipients text file. To interact with the server the following email protocols are required.
  - **Post Office Protocol (POP) :** It stores only incoming messages. Investigation is done at the workstation.
  - **Internet Message Access Protocol (IMAP) :** This protocol stores all the messages. Copies of incoming and the outgoing messages are stored on the server or workstation or both.
  - **Microsoft's Mail API (MAPI) :** This protocol also work same as IMAP.
  - **HTTP :** This protocol is used for web based send and receives.
  - **Simple mail transfer protocol (SMTP) :** It is responsible for sending and receiving the email. It uses TCP port 25. It is easy to spoof SMTP and send the fake mail.

Syllabus Topic : E-mail Analysis

5.2 E-mail Analysis

Q. 5.2.1 Write a short note on email forensics? *(Ref. Secs. 5.1 and 5.2)* **(5 Marks)**

Q. 5.2.2 Explain the steps involved in email analysis/investigation? *(Ref. Sec. 5.2)* **(5 Marks)**

Email crime investigation or analysis contains the following steps:

1. Examine the email message
2. Copy the email message
3. Print the email message
4. View the mail headers
5. Examine the email headers
6. Examine attachment if it is there in email
7. Trace the Email.

➜ **1. Examine the email**

When it is come into the light that email crime has happened then it is necessary to collect the evidence which is required to prove the crime in the court of law. Evidence may be gathers from the victim's computer. Evidence is the mail which the victim received.

- First take the image of machines hard drive.
- Obtain the victims machine password to open the encrypted file.
- Take the printed copy of the crime mail (including header).
- Examine the IP address of the sender's server.

➜ **2. Copy the email message into the USB key.**

➜ **3. Take the printout of the email message by using the print option available in the mail program.**

➜ **4. View the mail header**

- To check the mail header
- Open your mail.
- Right click on your mail.
- After right click menus will display. Click on view full header.
- The file header will get opened.

➜ **5. Examine the email header**

The email header contains the message header and the subject body. The email header contains the information of the email origin. You can see in the given message that the IP address of the sender's machine is sent i.e. X-originating- IP: [200.85.213.54]. It also gives the return path, and the receiver mail id.

From Suvarna Pansambal Tue Feb 2 12:16:14 2016

X-Apparently-To : suvarnashirke@yahoo.com; Tue, 02 Feb 2016 12:16:15 +0000

Return-Path : <suvarna.atharv@gmail.com>

Received-SPF : pass (domain of gmail.com designates 209.85.213.54 as permitted sender)

X-Originating-IP : [209.85.213.54]

Authentication-Results : mta1073.mail.gq1.yahoo.com from=gmail.com; domainkeys=neutral (no sig); from=gmail.com; dkim=pass (ok)

Received : from 127.0.0.1 (EHLO mail-vk0-f54.google.com) (209.85.213.54) by mta1073.mail.gq1.yahoo.com with SMTPS; Tue, 02 Feb 2016 12:16:15 + 0000

Received : by mail-vk0-f54.google.com with **SMTP id** n1so95500114vkb.3 for <suvarnashirke@yahoo.com>; Tue, 02 Feb 2016 04:16:14 -0800 (PST)

DKIM-Signature : v=1; a=rsa-sha256; c=relaxed/relaxed; d=gmail.com; s=20120113;

h=mime-version:date:message-id:subject:from:to:content-type;

bh=7AWYrxUKcsQ8uhNfa2cJrervIPR8oNJDId+M28otZas=;
b=TFIL3/WMYu9aLdGKBoSoYoWqerdG+Wjmmckw/kKA7tNfNncm1xvyqlRpOYMI O05LIq

X-Google-DKIM-Signature : v=1; a=rsa-sha256; c=relaxed/relaxed;

d=1e100.net; s=20130820;

h=x-gm-message-state:mime-version:date:message-id:subject:from:to:content-type;

bh=7AWYrxUKcsQ8uhNfa2cJrervIPR8oNJDId+M28otZas=;-Gm-Message-State: AG10YOT91xCYmn4COfUybd9MEb6HEtEU+MiOY99sDZQ6PbFlgE09G/boN2F9x MBQSk6aAFVx74W0+hLMbo5SJg==

MIME-Version : 1.0

X-Received : by 10.31.16.197 with SMTP id 66mr16543831vkq.41.1454415374794; Tue, 02 Feb 2016 04:16:14 -0800 (PST)

Received : by 10.31.151.147 with HTTP; Tue, 2 Feb 2016 04:16:14 -0800 (PST)
Date : Tue, 2 Feb 2016 17:46:14 +0530

Message-ID :
<CAL1VNuOeJv075FDfSN=ENDdg_KhGNmQGizVsi9y9eA8OcX401w@mail.gmail.com>

Subject : Threat mail

From : Suvarna Pansambal suvarna.atharv@gmail.com

To : suvarnashirke suvarnashirke@yahoo.com

Content-Type : multipart/alternative; boundary=001a11436378c545c7052ac877ff

Content-Length : 542

Fig. 5.2.1 : Email Message header

➜ **6. Examine the attachments**

If the mail contains any attachment then copy that attachment and also take the print of the attachment.

➜ **7. Trace the Email**

- The IP address of the origination computer machine tells the owner of the email address which has been used in the possible crime that is being investigated. It may be possible that this information may be fake. So it's important to validate the evidence which you uncover. There are many sites which tell the owner associated with the domain name. For example: suvarna@yahoo.com , everything after the @ sign is the domain name.
- The examples of the site which tells the owner of the mail associated with the sites are :

1. **www.arin.net**

   The ARIN (American Registry for Internet Numbers) is used to find the domain name from the IP addresses. It also gives the contact personal listed against the domain name.

2. **www.freeality.com**

   This website provides many different searching options like names, phone number and mail address. This websites permit the users to reverse email searches. This may help to reveal the subjects original identity.

Syllabus Topic : e-Mail Headers and Spoofing

5.3 e-mail Headers and Spoofing

We have studied the E-mail headers in the previous section. Email spoofing is the forgery of an email header. The message which you receive is actually originated from someone else than the actual user.

☛ **Email Spoof with PHP function mail ()**

The mail () function allows you to send mail.

- Bool mail (string $to, string $subject, string $message [, string $additional_headers [, string $additional parameters]])

- Example: www.rootspot.com/jose/mai

Email Spoof with telnet

- Open command prompt and type telnet 25
- mail from: your email id @ blah.com
- rcpt to: recipient email id @ blah.com

Email Recovery Tools

The list of the email recovery tools is as follows:

- FINALeMAIL
- Email Examiner
- Network E-mail Examiner
- R-mail

Syllabus Topic : Laws against e-mail Crime

5.4 Laws Against e-mail Crime

Q. 5.4.1 Write short note on CAN-SPAM act. *(Ref. Sec. 5.4)*	**(5 Marks)**
Q. 5.4.2 Explain the Law against email crimes? *(Ref. Sec. 5.4)*	**(5 Marks)**

1. The CAN-SPAM Act

- The CAN-SPAM Act, a law that sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations.
- Despite its name, the CAN-SPAM Act doesn't make a difference just to mass email. It covers every single business message, which the law characterizes as "any electronic mail message the basic role of which is the business ad or advancement of a business item or administration," including email that advances content on business sites.
- The law makes no special case for business-to-business email. That implies all email – for instance, a message to previous clients declaring another product offering – must obey the rules to the law.

- Each separate email infringing upon the CAN-SPAM Act is liable to penalties of upto $16,000, so rebelliousness can be expensive. In any case, following the law isn't confounded.

☞ **Here's a rundown of CAN-SPAM's main requirements :**

1. Try not to utilize false or deceiving header data. Your "From," "To," "ReplyTo," and directing data – including the beginning space name and email address – must be exact and distinguish the individual or business who initiated the message.
2. Try not to utilize tricky titles. The headline should precisely reflect the content of the message.
3. Recognize the message as a promotion. The law gives you a great deal of space in how to do this, however you should reveal unmistakably and prominently that your message is an ad.
4. Tell recipients where you are located. Your message must incorporate your substantial physical postal address. This can be your present street address, a post office box you have registered with the Postal Service, or a private mailbox you have registered with a business mail accepting office set up under Postal Service directions
5. Advise recipients how to quit accepting future email from you. Your message must incorporate a reasonable and prominent clarification of how the recipients can quit getting email from you later on. Specialty the notice in a way that is simple for a customary individual to perceive, read, and get it. Innovative utilization of sort size, shading, and area can enhance lucidity. Give an arrival email address or another simple Internet based approach to enable individuals to impart their decision to you. You may make a menu to enable a recipients to quit specific sorts of messages, however you should incorporate the choice to prevent every single business message from you. Ensure your spam channel doesn't shut these quit requests.
6. Respect quit asks for immediately. Any quit component you offer must have the capacity to process quit demands for no less than 30 days after you send your message. You should respect a recipient's quit demand inside 10 business days. You can't charge an expense, require the recipient to give you any specifically recognizing data past an email address, or make the recipient make any stride other than sending an answer email or visiting a solitary page on an Internet site as a condition for respecting a quit demand. When individuals have revealed to you they would prefer not to get more messages from you, you can't move or exchange their email addresses, even as a mailing list.

   The main special case is that you may exchange the addresses to an organization you have procured to enable you to conform to the CAN-SPAM Act.

7. Monitor what others are doing on your behalf. The law clarifies that regardless of whether you employ another organization to deal with your email advertising, you can't contract away your lawful duty to conform to the law.

   Both the organization whose item is advanced in the message and the organization that really sends the message might be considered lawfully dependable.

5.5 Section 66A

- Sending offensive messages through communication service, causing irritation etc through an electronic communication or sending an email to mislead or deceive the recipient about the origin of such messages (commonly known as IP or email spoofing) are all covered here.
- Punishment for these acts is imprisonment upto three years or fine. If anyone get booked under Section 66A, then that person has to face upto 3 years of imprisonment along with a fine.

Syllabus Topic : Messenger Forensics : Yahoo Messenger

5.6 Messenger Forensics : Yahoo Messenger

Q. 5.6.1 Write a short note on messenger forensics? *(Ref. Sec. 5.6)* **(5 Marks)**

Yahoo Messenger Overview

- Yahoo! Messenger is one of the popular instant messaging clients from Yahoo. By using the yahoo messenger you can send messages, photos, videos, files. You can do video chat as well as internet phone calls.
- Yahoo messenger has some default preferences such as alerts, sounds and signing into Yahoo Messenger. In yahoo messenger by default chat messages are archived and saved but these messages are cleared out once the user signs out of Yahoo Messenger. If you do not log out then it is possible to view these archived messages.
- One can also change the default setting option. If user wants to Yahoo messenger chat sessions then they can do it.

Data Analysis

- Investigation of the evidence start from the registry structure for Windows Vista and Windows 7 using the built in registry editor for Windows. The registry is examined with respect to the Yahoo Messenger files.

- Windows registry structure is quite similar to Yahoo Messenger registry structure for Windows XP. The data is found in the given locations as shown in Table 5.6.1.

Table 5.6.1 : Yahoo registry evidence for Windows XP, Windows Vista and Windows 7.

File	Location	Description	XP	Vista	Windows 7
HKEY_CURRENT_USER	Software\yahoo\Pager	Gives user ID	Yahoo User ID	Yahoo User ID	Yahoo User ID
		Gives the Installed Version	N/A	Version	Version
		Gives the version revisions	N/A	VersionRev	VersionRev
		Show if the password is saved		Save password	Save password
		Shows if auto sign in is on or off	N/A	Auto login	Auto login
		Number of P2P users	N/A	P2P count	N/A
HKEY_CURRENT_USER	Software\yahoo\Pager\Profiles\screenname\Chat		Chat(rooms visited or created)	Chat	chat
HKEY_CURRENT_USER	Software\yahoo\Pager\Profiles\screennname\Chat\Favorite Rooms		N/A	Favorite rooms	Favorite rooms
HKEY_CURRENT_USER	Software\yahoo\Pager\Profiles\screenname\FT	Location of last received file and last sent transferred file.	File transfer	FT	FT
HKEY_CURRENT_USER	Software\yahoo\Pager\Profiles\screenname\FriendIcons	Location of user icon displayed to friends.	N/A	Friend Icons	Friend Icons

- The investigator try to find out the Yahoo user ID of the person who is using the account, version of the Yahoo Messenger installed on the computer, all the revisions made to the YM version, if the save password option is turned on and also if the Auto sign in has been enabled. There is one extra feature in Windows Vista that is P2P count. P2P count is the number of allowed P2P users who can send huge data among each other.
- **User\Software\Yahoo\Pager\profiles\profile_name\chat** location shows the last selected chat room category, but not essentially the correct chat room entered. Y using this information investigator can understand chat room category that the predators potentially use. **User\Software\Yahoo\Pager\profiles\profile_name\chat\favorite_rooms** location provides the list of saved favourite rooms for the user. This information is important to understand the different chat rooms that the predator uses.
- **User\Software\Yahoo\Pager\profiles\profile name\FT** location provides the last saved location of a received file as well the last sent location of a transferred file, that is, the location from where the last sent file was uploaded. This information is useful when validating whether a user has been sharing or receiving files. Please refer to Table 5.6.1 for further detail. **User\Software\Yahoo\Pager\profiles\profile_name\FriendIcons** location provides the icon that the user has set for himself, that is displayed to the user's friends. The name of the file used will be visible in the path as well as where it is located on the hard drive.
- Photo Sharing: Creation of the "S" folder

In the Yahoo Messenger whenever a photo sharing session is initiated r from a Vista machine, a photo sharing folder starting with the letter "S" is created in the Program Data folder. In addition random assigned numbers and alphanumeric characters are appended to the end of the naming structure. The following is the path for the created "S" folder:

C:\ProgramData\Yahoo!\Messenger\PhotoSharing\Sc8b0

- The "S" folder is created when the user initiates the photo sharing session. Once the session is initiated, immediately the other yahoo user accepts the photo sharing invite, the "S" folder is created in the Photo Sharing folder on the initiator's side.
- The "S" folder is empty until a picture is shared. As soon as an image is shared or sent, a thumbs file '_t.jpg' is created followed by the image file '_m.jpg'. The name of this file is displayed as randomly assigned series of alphanumeric characters.
- If there are multiple chat sessions and photo sharing sessions open on users machine then at the same time with different users, a different "S" folder is created for each chat session.

5.6.1 File Transfer

- Yahoo Messenger has two ways of sharing a photo:
  1. Yahoo Photo Sharing
  2. File transfer option.
- For the photo sharing the "S" folder creation is applicable but it is not applicable to file transfer. If the user wants to save the photos through Photo Sharing, the default folder where these pictures will be saved is in the 'Picture' folder.
- The 'Picture' folder is a shortcut located under 'Libraries'. The full path is **'C:\Users\UserName\Pictures'**. The user can save the photos to any location they wish on the computer.
- The file transfer is used to transfer all types of media such as, photos, music, documents etc. The default location for saving a file during a file transfer is "Documents". The Documents folder is a shortcut located under 'Libraries'.
- The full path is **'C:\Users\UserName\Documents'**. The user can save the file anywhere on the computer as per his wish. The default file name and the original file is same. The date-time stamp of the saved file is same as local machine when the file was saved.

Syllabus Topic : Social Media Forensics: Social Media Investigations

5.7 Social Media Forensics : Social Media Investigations

Q. 5.7.1 Write a short note on social media forensics? *(Ref. Sec. 5.7)* **(5 Marks)**

- Social Media Investigations is now a days is a common feature of any investigation effort. The police uses social media to collect the evidences and build cases. Investigators use photos posted on the social media. The personal information on social media helps the investigator to ascertain someone's character, check for illegal or wrong behavior, to find someone, or to prove (or disprove) an explanation.
- Social media investigation is powerful as more that 80% people is using social media and people are posting to much information online. There are many popular social media sites, few are listed below.
  - Facebook
  - LinkedIn

- Twitter
- Youtube
- Instagram
- LinkedIn
- Tumblr
- Reddit

- Social media is a rich wellspring of data for pretty much any examination. In the event that your objectives incorporate get-together data about somebody's developments, partners, or character, social media investigations are an incredible fit.

5.7.1 Gathering Evidence for Court

- For court cases social media is a great source. Evidences are collected to prove someone's character, prove or disprove defense, or collect other various supporting evidence. Investigator collects the more information from statuses, photos, tweets from social media.
- The metadata attached with the post is used to determine where someone was at a given time. It also provides information about someone's behaviours and habits over time. This sort of evidence can discredit or support someone's claims, or even establish their reliability as a witness.
- Social media evidences should be collected methodologically, with proper metadata and other validating information intact. If the evidence is not collected properly then it won't be considered in the court.

Types of Evidence Typically Collected for Court Cases

- Relevant statements or comments.
- Metadata from posts establishing time and location of posting.
- Posts relating to past illegal activity.
- Photos.
- Content establishing character (for example, attitudes to police, past sentiments, racist or sexist content etc).
- List of social media profiles and screen names associated with target individual.

Employment Checks

- The social media is also used in employment where the employer can assess your character, work experience, and education.

- Social media investigations helps to find the past illegal behaviour, provide evidence to support or discredit claims about education and employment, and assess whether they are probable to conduct themselves in a manner befitting your organization. Before conducting a social media investigation on an employee , you should know that these types of background checks are subject to the Fair Credit Reporting Act. It means applicants consent is needed.

☞ Types of Evidence Typically Collected

- Posts and photos relating to illegal activity or **drug use.**
- Posts relating to objectionable content (e.g. **racist or sexist** content).
- Posts supporting or discrediting past **education and employment.**
- Relevant statements and comments.
- List of social media profiles and screen names associated with target individual.

☞ Person Location

Social media posts contains location data. It will be helpful you to find your long lost friend then social media is useful. Social media investigations merge social connections and biographical information to find people.

☞ Types of Evidence Typically Collected

- Location metadata from posts.
- Location metadata from images.
- Relevant statements and claims.
- Photo analysis.
- Leads from interviews and social connections.

The same way social media is used in custody cases, divorce cases.

☞ Tools used for Social Media Investigation

Screencast-O-Matic

Screencast-O-Matic tool is used to record the screen. This tool record the social media screen as evidence. It record the posts, comments, photos and videos posted on the social media.

5.8 Browser Forensics

Q. 5.8.1 Write a short note on browser forensics ? *(Ref. Sec. 5.8)* (5 Marks)

Web browsers overview

- Nowadays there are many web browsers available in the market like Internet Explorer, Google Chrome, and Mozilla etc.
- These all web browsers are slightly different in web services. To display the same website faster on future occasions, web browsers maintain the Downloaded web site data, so that it remains available on the computer even if the user closes the browser or shuts down the machine. This is a useful feature.
- The downloaded web files are known as caches, cached history or temporary files. Based on the operating system and browser applications they are in different locations.

Internet Explorer

The most famous web browser is Internet Explorer (IE) as it is a component of the Windows operating system. IE is very and is frequently used as a default web browser. In windows 10 IE is replaced with Microsoft EDGE (ME).IE and ME both work in InPrivate mode, without storing information about web resources visited by the user.

Google Chrome

- Google Chrome is browser by provided by Google. It has incorporation with Google services. It allows the Synchronization of user passwords between devices. One can use the extensions and plug-in. Google Chrome performs fast operations and collects user data but it Consumes large amounts of memory.
- The impposrtant feature of google chrome is that it works in Incognito mode, which prevents the browser from permanently storing any history information, cookies, site data or form inputs.
- There are many web browsers created by the third party developers based on Chrome Engine, like Chromodo, Amigo, Sputnik, Uran, Epic Browser, SafeZone, Comodo Dragon, Flock, Rockmelt, Sleipnir SRWare Iron, Titan Browser, Torch Browser, 360 Extreme Explorer, Avast Chromium, CoolNovo, Cốc Cốc, Vivaldi, Yandex.Browser, Opera, Orbitum, Breach, Nihrome, Perk, QIP Surf, Baidu Spark, etc. All of these borrowers function like Google Chrome and create web browser artifacts like Google Chrome and also support most of Google Chrome's extensions and plugins.

Opera

The Opera web browser is also a famous web browser. It was the first web browser to introduce features that other web browsers adopted, like; pop-up blocking, Speed Dial, private browsing and tabbed browsing re-opening recently closed pages. Opera have a free Virtual Private Network (VPN) service, which permits users to surf the web incognito.

Firefox

Firefox is also one of the popular web browsers. It is more secure as compare to other browsers. It has advanced Incognito mode, disabling tracking of user's locations and advertisements. Firefox has its own extensions.

Difficulties of web browsers forensic analysis

There are following difficulties faced by the forensic examiner while analyzing the web browsers :

- Many web browsers are available with lots of data. Different data.
- To protect the data Encryption is used.
- If the user is using the Incognito mode (private mode) then computer do not contain the browser artifacts.

Web browser forensic artifacts

Each web browser has its own artifacts in operating system. The artefacts are depend on the version of the web browser. Usually one can get the following artefacts:

- History
- Cache
- Cookies
- Typed URLs
- Sessions
- Most visited sites
- Screenshots
- Financial info
- Form values (Searches, Autofill)
- Downloaded files (Downloads)
- Favorites.

Syllabus Topic : Browser Forensics : Cookie Storage and Analysis

5.8.1 Cookie Storage and Analysis

- Cookies are the text files. These files are used to feedback from the user to the server. When performing some actions with a web resource like viewing web links, downloading files, etc, these actions are registered in a cookie that is secretly sent by the server to the user's computer. By using this web resource, the server can find out what actions the user has taken on previous visits to this web resource.
- The cookies are stored in cookies folder, but the location of the cookies folder is based on the web browser and the operating system .The following table illustrate the location of the cookies based on the browser and operating system.

Browser	Operating System	location
Internet Explorer	Windows 98	\Windows\Cookies\
	Windows 2000, Windows XP	\Documents and Settings\Administrator\Cookies
	Windows 7	\Users\%userprofile%\AppData\Roaming\Microsoft\Windows\Cookies
	Windows 7	\Users\Default\AppData\Roaming\Microsoft\Windows\Cookies
Firefox, Windows		\Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\cookies.sqlite
Google Chrome, Windows		\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Cookies.db

Syllabus Topic : Browser Forensics : Analyzing Cache and Temporary Internet Files

5.8.2 Analyzing Cache and Temporary Internet Files

Cache Files

- The cache folder contains the browser history and it automatically creates the profile folder at start. This folder is the storage place for the browsing history.

- The following table shows the cache locations of the different browsers :

Firefox	Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\cache2\entries
Google Chrome, Windows	\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Cache\ \Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\GPUCache\ \Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Media Cache\
Opera	\Users\%userprofile%\AppData\Roaming\Opera Software\Opera Stable\ShaderCache\GPUCache\data_3
Safari, MacOS	\Users\%userprofile%\Library\Caches\com.apple.Safari\Cache.db

Windows Temporary Internet Files

- Temporary Internet Files (C:\Windows\Temporary Internet Files) are immediate downloads from the Internet, more often than not containing realistic pictures in Windows bitmap (bmp), jpeg, gif, or .art format. There will likewise be html and htm files for website home page components, and so forth. Approaching Yahoo and Hotmail messages may likewise exist as files in the Temporary Internet Files folder.
- Downloaded movies, mpegs, avi files, and Adobe PDF files will be found in Temporary Internet Files.

Temporary files

- Windows Temp files (C:\Windows\Temp) are temporary files made by Windows as different programs are running and diverse processes are occurring. They are regularly exact copy of files put away somewhere else on the PC. At different occasions they are exact duplicates of files which are waiting to be handled by the PC.
- For instance, a print work heading off to a laser printer will make a temporary document called an EMF (enhanced windows metafiles). EMF's (smaller than normal photos of the original) can frequently be found in the Temp index a very long time after laser printer was utilized.
- Numerous different sorts of files can be found in the Temp registry too (e.g., programmed report recuperation files).

How is the data stored?

- Internet Explorer and Windows Explorer store most of the data in index.dat files. INDEX.DAT files are used by Internet Explorer to store information about visited pages, cookies and the time they are used.
- To this end, Internet Explorer indexes files that are located in folders that are browser caches and maps these files to the network resource from which these files were downloaded. In addition, INDEX.DAT files contain such information as the decryption of HTTP-header packets, in which the file was transferred, the date of creation and last access to the file, the number of calls to it, and much more.
- The following are the locations for index.dat file.

1	\Documents and Settings\%userprofile%\Local Settings\Temporary Internet Files\Content.IE5\index.dat
2	\Users\%userprofile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
3	\Documents and Settings\%userprofile%\Cookies\
4	\Documents and Settings\%userprofile%\Local Settings\History\History.IE
5	\Documents and Settings\%userprofile%\Local Settings\ History\History.IE\MSHist[timestamps]

Syllabus Topic : Browser Forensics : Web Browsing Activity Reconstruction

5.8.3 Web Browsing Activity Reconstruction

- To reconstruct the web browsing activity, you have to reconstruct it from cached file in users computer. Examine Cached files created by web browsers.
- The browsing activities are internet shopping, downloading, browsing and searching etc. you can perform web browsing activity reconstruction using any open source or freeware tool.
- The following are the steps to reconstruct the web browsing activity :

1. **First check the cookies folder, here we are considering browser Firefox, and operating system is windows xp. So you get the cache file at the location given below:**

   \Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\ cookies.sqlite

2. Check the cache file at the given location

Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\cache2\entries)

3. Check the favorites at the given location

Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\places.sqlite

4. For session recover check the following location

\Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\sessionstore.js

5. Check the downloaded file given at the following location

\Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\places.sqlite

6. Check the URL's visited in the location given below

\Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\places.sqlite

7. Check the form value

\Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\formhistory.sqlite (Firefox, Windows)

8. Check the typed URL's

\Users\%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxxx.default\places.sqlite

9. Check the session restore artifacts

\Users\%userprofile%\Library\Safari\Local Storage\

\Users\%userprofile%\AppData\Roaming\Opera Software\Opera Stable\Last Tabs (Opera, Windows)

- Google Chrome, Safari, Firefox, Opera store most of the data in SQLite databases. Manual analysis of these databases and carving will allow you to extract the maximum amount of data.

When analyzing SQLite data bases, remember :

- Some deleted records can be found in Freelist – unused tables that can contain deleted data.

Where can I find the Web Browsers artifacts?

- Physical dumps of mobile devices.
- File systems of mobile devices.
- Backups of mobile devices.
- Data, which can be extracted from Clouds.
- Hard drives.
- Images of hard drives.
- Memory dumps.
- Hibernation and page files.

5.9 Exam Pack (Review Questions)

Syllabus Topic : E-mail Analysis

Q. 1 Write a short note on email forensics ? *(Refer sections 5.1 and 5.2)* **(5 Marks)**

Q. 2 Explain the steps involved in email analysis/investigation. *(Refer section 5.2)* **(5 Marks)**

Syllabus Topic : Laws against e-mail Crime

Q. 3 Write short note on CAN-SPAM act ? *(Refer section 5.4)* **(5 Marks)**

Q. 4 Explain the Law against email crimes ? *(Refer section 5.4)* **(5 Marks)**

Syllabus Topic : Messenger Forensics : Yahoo Messenger

Q. 5 Write a short note on messenger forensics ? *(Refer section 5.6)* **(5 Marks)**

Syllabus Topic : Social Media Forensics : Social Media Investigations

Q. 6 Write a short note on social media forensics ? *(Refer section 5.7)* **(5 Marks)**

Q. 7 Write a short note on browser forensics ? *(Refer section 5.8)* **(5 Marks)**

❑❑❑

Chapter Ends...