Syllabus Topic : Incident Verification and System Identification

Q. 4 What is Incidence? What are the goals of incidence response ? *(Refer section 1.2.1)* **(5 Marks)**

Q. 5 Explain the Incidence Response methodology or explain the components of Initia Response or explain the steps of initial response ? *(Refer section 1.2.2)* **(5 Marks)**

Q. 6 Explain the phase after detection of incident. *(Refer section 1.2.4)* **(5 Marks)**

Syllabus Topic : Recovery of Erased and Damaged Data

Q. 7 Explain the techniques used to recover erased or damaged data. *(Refer section 1.3)* **(5 Marks)**

Q. 8 How Linux tools use to recover files on FAT file systems. *(Refer section 1.3.1)* **(5 Marks)**

Q. 9 How deleted files recover on Windows systems ? *(Refer section 1.3.1)* **(5 Marks)**

Syllabus Topic : Disk Imaging and Preservation

Q. 10 What is disk imaging ? *(Refer section 1.4)* **(5 Marks)**

Q. 11 What is mirror image ? *(Refer section 1.4)* **(5 Marks)**

Q. 12 What are the forensic duplication tool requirements ? *(Refer section 1.4.1)* **(5 Marks)**

Q. 13 How to create a forensic duplicate of hard drive ? *(Refer section 1.4.2)* **(5 Marks)**

Q. 14 How to create a qualified forensic duplicate of hard drive ? *(Refer section 1.4.3)* **(5 Marks)**

Syllabus Topic : Data Encryption and Compression

Q. 15 Explain data encryption and compression. *(Refer section 1.5)* **(5 Marks)**

Syllabus Topic : Automated Search Techniques

Q. 16 Write short note on automated search techniques. *(Refer section 1.6)* **(5 Marks)**

Syllabus Topic : Forensics Software

Q. 17 Explain the forensic softwares. *(Refer section 1.7)* **(5 Marks)**

Chapter Ends

Unit I

CHAPTER 2

Network Forensic

Syllabus Topic : Introduction to Network Forensics and Tracking Network Traffic

2.1 Introduction to Network Forensics and Tracking Network Traffic

Q. 2.1.1 What is network forensics ? *(Ref. Sec. 2.1)* **(5 Marks)**

Q. 2.1.2 What is mean by securing a network ? *(Ref. Sec. 2.1)* **(5 Marks)**

- **Network forensics** is the process of collecting and analyzing raw network data and tracking network traffic systematically to find out how an attack was carried out or how an event occurred on a network.
- Network attacks are increasing day by day. Few of the attacks are unintentional which happens because of lack of knowledge. 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 mention particular computer crimes.
- 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 inspite of the fact that the individuals who get access and then destroy information or plant viruses are legitimately called by both names.
- Network forensic helps you to find out that the attacks on the network are done intentionally or unintentionally.
- When the intruders attack the network they leave a trace behind. So, it is necessary to find out the variation in network traffic to track the intrusions. It is important to know the typical pattern of your network, for example, the peak hours of using internet in the city are between 6 a.m. and 6 p.m.

- If anything wrong or suspicious occur during night then the network administrator would find out it as an unusual activity and do the investigation
- The network forensics examiners have to set standard procedures to acquire data after an attack or intrusion incident.
- Normally, the network administrators desire to find compromised machines, get them offline, and restore them as fast as possible to reduce downtime.
- It is necessary to take time to follow the standard procedure to make sure that all the compromised systems are tracked and find out attack methods in an attempt to prevent them from happening again.

Securing a network

- Network forensics is used to find out the security breach due to attacks, Viruses and other incidents. Hardening contains a series of tasks, like applying the latest patches, using a layered network defense strategy, which sets up layers of protection to hide the most valuable data at the deepest part of the network. It make sure that if the attacker goes deeper then the access become more difficult and the more safeguard are in place.
- The National Security Agency (NSA) developed a similar approach, called the Defense in Depth (DiD) strategy. DiD has the following three modes of protection:

1. People
2. Technology
3. Operations

- If any of the mode out of 3 fails the other mode is used to prevent the attack. Posting people as a mode of protection implies organizations must hire very much qualified individuals and treat them well so they have no motivation to look for revenge.
- Train the employees adequately in security procedures and the organizations security policy. This mode includes Physical as well as personnel security measures.
- The technology mode consists of, selection strong network architecture and using tested tools, for example, firewalls and Intrusion Detection Systems (IDSs).
- Regular penetration testing combined with risk assessment will help you to enhance network security, too. Having set up that permit speedy and exhaustive examination when a security break happens is likewise part of the technology mode of protection.
- At last, the operations mode tends to everyday activities. Updating antivirus software security patches, and OSs falls into this class, as does evaluation and monitoring methods and disaster recovery plans.

Syllabus Topic : Reviewing Network Logs

2.2 Reviewing Network Logs

Q. 2.2.1 What is mean by reviewing logs? *(Ref. Sec. 2.2)* **(5 Marks)**

- The incoming and the outgoing traffic of network is recorded by the Network logs. Network servers, firewalls, routers, and other devices record the activities and events that go through them.
- Running the Tcpdump program is the common method to examine the network traffic. It generates the Hundreds or thousands of lines of records. A example output is shown here :

```
TCP log from 2010-12-16:15:06:33 to 2010-12-16:15:06:34
Wed Doc 15 15:06:33 2010; TCP; eth0; 1296 bytes; from
204.146.114.10:1916 to 156.26.62.201:126
Wed Dec 15 15:06:33 2010; TCP; eth0; 625 bytes; from
192.168.114.30:289 to 188.226.173.122:13
Wed Dec 15 15:06:33 2010; TCP; eth0; 2401 bytes; from
192.168.5.41:529 to 188.226.173.122:31
Wed Dec 15 15:06:33 2010; TCP; eth0; 1296 bytes; from
206.199.79.28:1280 to 10.253.170.210:168; first packet
END
```

- The first line is the header and the remaining lines follow the format time; Protocol; interface; size; source and destination addresses.
- The second line given below, shows that the data was transmitted on Wednesday, December 15, 2010 at 15:06:33. The packet sent was TCP packet through the Ethernet 0 interface of 1296 bytes.
- The packet was sent from the IP address 204.146.114.10:1916 to IP address 156.26.62.201:126. In the IP address the port number is given after the colon.

```
Wed Dec 15 15:06:33 2010; TCP; eth0; 1296 bytes; from
204.146.114.10:1916 to 156.26.62.201:126
```

- When you view the network log, the port information gives you hint for investigation, such as you can observe that a specific IP address is coming very frequently on a unusual port.
- The ports above 1024 raise a flag. You can check the assigned ports from internet assigned numbers Authority Web site (www.iana.org/assignments/port-numbers).
- If you wanted to generate a list of translation he top 10 Web sites users in your network are visiting, use the Ethereal tool. This tool will give you the list of 10 websites along with the information like, the number of bytes transferred followed by the IP address. For example, *4897 110.150.70.190*. You can also create a list o top 10 internal users, for example, *2401 204.146.114.50*.
- Network logs also show you the patterns, like an employee is sending information frequently from a particular IP address. If you investigate it, you will come to know that, the employee was doing the online shopping during company timing. After the investigation, keep the preserved evidenced in your mind, your investigation may edge other companies that have been compromised. You should not reveal the findings about the other companies.
- The solution to this is, contact the companies and enlist their aid in tracking down network intruders or you can report the incident to federal authorities.

Syllabus Topic : Network Forensic Tools

2.3 Network Forensic Tools

Q. 2.3.1 Write a short note on network forensic tools? *(Ref. Sec. 2.3)* **(5 Marks)**

There are different types of tools available for network administrator or forensic. By using these tools one can perform remote shutdowns, monitor device use and more.

Windows Operating System Network Tools

- Sysinternals is a collection of freeware tools for examining windows products. These tools are created by Mark Russinovich and Bryce Cogswell and acquired by Microsoft.
- These tools are very helpful for monitoring the network traffic thoroughly and efficiently. You can monitor your network and shutdown machines or processes that could be harmful.
- Table 2.3.1 will give the information about the tools. All the tools mentioned in the tables are freeware.

Table 2.3.1

Tools	Description
RegMon	It Shows all registry data in real time
Process explorer	Shows what files, Registry keys, and dynamic link libraries (DLLs) are loaded at a specific time.
Handle	Shows what files are open and which processes are using these files.
Filemon	Shows file system activity.
PsExec	Runs processes remotely
PsGetSid	Displays the security identifier (SID) of a computer or user
PsKill	Kills processes by name or process ID
PsList	Lists detailed information about processes
PsLoggedOn	Displays who's logged on locally
PsPasswd	Allows you to change account passwords
PsService	Enables you to view and control services
PsShutdown	Shuts down and optionally restarts a computer
PsSuspend	Allows you to suspend processes

UNIX/ Linux operating System Network Tools

- Knoppix Security Tools Distribution is a bootable Linux CD intended for computer and network forensics.
- Before using this tool one has to adjust the BIOS of the system you are using and make sure that it is booting from your CD.
- The Knoppix Security Tools Distribution is made by Klaus Knopper and maintained and updated by knoppix users.

- When you view the network log, the port information gives you hint for investigation, such as you can observe that a specific IP address is coming very frequently on a unusual port.
- The ports above 1024 raise a flag. You can check the assigned ports from internet assigned numbers Authority Web site (www.iana.org/assignments/port-numbers).
- If you wanted to generate a list of translation he top 10 Web sites users in your network are visiting, use the Ethereal tool. This tool will give you the list of 10 websites along with the information like, the number of bytes transferred followed by the IP address. For example, 4207 110.150.70.190. You can also create a list o top 10 internal users, by example, 2401 204.146.114.50.
- Network logs also show you the patterns, like an employee is sending information frequently from a particular IP address. If you investigate it, you will come to know that the employee was doing the online shopping during company timing. After the investigation, keep the preserved evidenced in your mind, your investigation may edge other companies that have been compromised. You should not reveal the findings about the other companies.
- The solution to this is, contact the companies and enlist their aid in tracking down network intruders or you can report the incident to federal authorities.

Syllabus Topic : Network Forensic Tools

2.3 Network Forensic Tools

Q. 2.3.1 Write a short note on network forensic tools? (Ref. Sec. 2.3) (5 Marks)

There are different types of tools available for network administrator or forensic. By using these tools one can perform remote shutdowns, monitor device use and more.

Windows Operating System Network Tools

- Sysinternals is a collection of freeware tools for examining windows products. These tools are created by Mark Russinovich and Bryce Cogswell and acquired by Microsoft.
- These tools are very helpful for monitoring the network traffic thoroughly and efficiently. You can monitor your network and shutdown machines or processes that could be harmful.
- Table 2.3.1 will give the information about the tools. All the tools mentioned in the table are freeware.

Table 2.3.1

Tools	Description
RegMon	It Shows all registry data in real time
Process explorer	Shows what files, Registry keys, and dynamic link libraries (DLLs) are loaded at a specific time.
Handle	Shows what files are open and which processes are using these files.
Filemon	Shows file system activity.
PsExec	Runs processes remotely
PsGetSid	Displays the security identifier (SID) of a computer or user
PsKill	Kills processes by name or process ID
PsList	Lists detailed information about processes
PsLoggedOn	Displays who's logged on locally
PsPasswd	Allows you to change account passwords
PsService	Enables you to view and control services
PsShutdown	Shuts down and optionally restarts a computer
PsSuspend	Allows you to suspend processes

UNIX/ Linux operating System Network Tools

- Knoppix Security Tools Distribution is a bootable Linux CD intended for computer and network forensics.
- Before using this tool one has to adjust the BIOS of the system you are using and make sure that it is booting from your CD.
- The Knoppix Security Tools Distribution is made by Klaus Knopper and maintained and updated by knoppix users.

- Knoppix offers tools of various categories like authentication, firewalls, password tools, wireless tools, encryption, IDS's, honeynets, forensics, packet sniffers, Vulnerability, assessment etc.

Table 2.3.2

Tools	Description
dcfldd	The U.S. DOD computer forensics lab version of the dd command
memfetch	Forces a memory dump
photorec	Retrieves files from a digital camera
snort	A popular IDS that performs packet capture and analysis in real time
oinkmaster	Helps manage snort rules so that you can specify what items to ignore as regular traffic and what items should raise alarms
john	The latest version of John the Ripper, a password cracker
chntpw	Enables you to reset passwords on a Windows computer, including the administrator password
tcpdump and ethereal	Packet sniffers

Using PACKET SNIFFERS

- "PACKET SNIFFERS" are device and/or software placed network to monitor traffic.
- Network administrators use sniffers for increasing security and tracking bottlenecks.
- Attackers use sniffers to obtain information illegally.
- On TCP/IP networks, sniffers examine packets. Thus termed as "Packet sniffers".
- In OSI model, Packet sniffers work at Layer 2 or Layer 3.
- Some sniffers perform packet captures. Sniffers are used for analysis. Some of the sniffers are used for both the purpose.
- Your organization needs to have policies about network sniffing to comply with new federal laws or digital evidence.

- As in windows, they have many sniffing tools capable of capturing and analyzing packets. But can't feed data (they collect directly into other tools).
- Most of tools can read anything captured in Pcap (Packet capture) format (LibPcap is for LINUX/UNIX and WinPcap is for Windows).
- As forensics experts, you must choose tools that best suit your purpose.
- **For Example :** If your network is being hit by SYN flood attacks. You need to find packet with SYN flag set.
- To find these packets, TCP dump Tethereal and SNORT can be programmed to examine TCP headers to SYN flag (Flag areas contains several flags and SYN flag is one of them).

Table 2.3.3

Tools	Description
Tcpslice	It is a good tool for extracting information from large Libpcap files; you specify the time frame you want to examine. Also Capable of combining files.
Tcpreplay	A suite of tools which can be used to replay network traffic recorded in libpcap format, this information used to test network devices such as routers , switches, etc.
Ngrep	It is used to examine Email headers or IRC logs .It collects and hashes data for Verification.
Ethereal	Tool used for viewing Network traffic graphically.
Netdude	It's a GUI tool, which are designed as an easy-to-use interface for inspecting and analyzing large Tcpdump files.
Argus	It is a session data probe , collector and analysis tool
Ethereal	It is used in a real-time environment to open saved trace files from packet capture. It also used to rebuild session.

Examining the Honeynet Project

- The main aim this project is to make the information available was developed to make the information available in an attempt to thwart internet and network attackers. Worldwide

there are many people who participate in the project. The main aim behind it is to create awareness, information and tools.

- The first step is making people and organizations aware that threats exist and they might be targets.
- The second is to provide information on how to protect against these threats, including how attackers operate, how they communicate, and what tactics they use. Finally, for people who want to do their own research, the Honey net Project offers tools and methods.
- The recent major threats to a network are Distributed denial-of-service (DDoS) attacks and zero day attacks. In DDoS attacks, the attacker uses hundreds or even thousands of machines.
- These machines are known as zombies because they have unwittingly become part of the attack. When the first DDoS attacks began, the main concerns were the high monetary impact and the amount of time it took to track down these attacks.
- In **Zero day attacks** attackers look for holes in networks and OSs and try to exploit these weaknesses before patches are available.
- The honeynet project set up as a resource to help network administrators' deal with DDoS and other attacks. It involves installing honeypots and Honeywalls at various locations in the world.
- A Honeypot is a computer set up to look like any other machine on your network; its purpose is to lure attackers to your network, but the computer contains no information of real value. In this way, you can take the Honeypot offline and not affect the running of your network.
- Honeywalls are computers set up to monitor what's happening to honeypots on your network and record what attackers are doing.
- The principle behind honey pots is that they aren't used on the network; they are simply set out to act as bait.
- The original machine is loaded with the standard software used on that part of the network, a forensic image of it is created, and then the machine is deployed on the network. If the machine is compromised, its taken offline and another image of it is made.
- The software then compares the two images to determine what method of attack was used and what files were altered or added. Both images are stored in the database.

Syllabus Topic : Performing Live Acquisitions

2.4 Performing Live Acquisitions

Q. 2.4.1 What is the general procedure given for live acquisition ? *(Ref. Sec. 2.4)* **(5 Marks)**

- Live acquisitions are mainly useful when you are dealing with active network attacks or intrusions or you have doubt that employees are accessing network areas that they should not have to access.
- Live acquisitions is performed before the system go offline and it has also become necessity as attack may left footprint or evidence only in running processes or RAM; for instance, there are some malware which get disappeared when the system is restarted.
- The information in RAM gets lost when the suspects system is turned off. After the live acquisition, there is change in the information on the system
- Information because your actions have affected the RAM and the running processes, so, the information cannot be produced again. As a result, live acquisitions don't follow typical forensics procedures.
- The following is the general procedure given for live acquisition, the steps are :

1. Create/download a bootable forensic CD, before using it test on the suspected drive. If the suspected system is on your network and you can access it remotely, add the suitable forensic tools to your computer. Otherwise insert the bootable forensics CD in the suspected system.
2. Ensure that you are keeping the log of all of your actions. Documenting the actions and reasons for these actions is important.
3. A network drive is perfect as a place to send the data you gather. In the event that you don't have one accessible, interface a USB thumb drive to the suspect system for gathering information. Ensure that you have noted this step in your log.
4. Now copy the physical memory (RAM).
5. The next step is depends on the incident you are investigating. For example, you want to shut down the system and make the static acquisition later; you want to see whether a rootkit is present by using a tool such as RootKit Revealer; You may also want to access the firmware to check it is changed or not.

6. Be confident that you will get the forensically sound digital hash value of all files you have recovered in the live acquisition to ensure that they are not modified later

Performing a Live Acquisition in Windows

To perform the live acquisitions many tools are available for capturing RAM, for example, network sniffers, password crackers, and freeware forensics tools.

Tools available to capture RAM for performing a live acquisition in windows

Win32dd	This tools runs on command line for performing memory dump on windows.
BackTrack 3	It combines the tools from White Hat Hackers CD and The Auditor CD. This tool is popular with penetration testers
Mantech Memory DD	It acquires up to 4 GB Ram in standard DD format
Winen.exe from guidance software	It is a standalone RAM acquisition tool.

You can also use the GUI tools, but it needs many resources. Few GUI tools may get the false readings from Windows Oss. As compare to GUI tool, Command-line tools give you more control.

Syllabus Topic : Order of Volatility

2.5 Order of Volatility

Q. 2.5.1 What is order of volatility ? *(Ref. Sec. 2.5)* **(5 Marks)**

- The investigators faces the problem of the Order Of Volatility (OOV), it means how long a part of information lasts on a system.
- Data such as RAM and running processes might exist for only milliseconds; other data such as files stored on the hard drive, might last for years.
- While collecting the evidences related to network based on the volatility a proper order collecting the evidence have to follow, this is known as order of volatility.

- The OOV is given as follows :
  1. Registers, Cache
  2. Routing Table, ARP Cache, Process Table, Kernel Statistics
  3. Memory
  4. Established network connections
  5. Running processes
  6. Temporary File Systems
  7. Media in use : Disk
  8. Remote Logging and Monitoring Data
  9. Backup media : tapes, disks not in use
  10. Archival Media
  11. WOM: CD ROMs, DVD's.
- After this you can separately collect the analogue material like physical configuration and network topology, paper, figure prints and DNA.

Syllabus Topic : Standard Procedures

2.6 Developing Standard Procedures for Network Forensics

Q. 2.6.1 What is the standard procedure used in network forensics? *(Ref. Sec. 2.6)* **(5 Marks)**

Network forensics is a long and, tiresome process. A standard procedure is used in network forensics is as follows :

1. Every time use the standard installation image for systems on a network. This image is not a bit-stream image but an image containing all the standard applications used. For all the applications and OS files you should have the MD5 and SHA-1 hash values.
2. In case, intrusion incident occurs, ensure the vulnerability has been fixed to avoid other attacks from taking advantage of the opening.
3. Try to recover all the volatile data by performing the live acquisition before the system turns off, for example, RAM and running processes.

4. Acquire and make the forensic image of the compromised drive.
5. Perform the comparison between files on forensic image and the original installatio image. Also compare the common files hash values, such as Win.exe and standard DLL and find out whether they have altered.

2.7 Exam Pack (Review Questions)

☛ **Syllabus Topic : Introduction to Network Forensics and Tracking Network Traffic**

Q. 1 What is network forensics ? *(Refer section 2.1)* (5 Marks)

Q. 2 What is mean by securing a network ? *(Refer section 2.1)* (5 Marks)

☛ **Syllabus Topic : Reviewing Network Logs**

Q. 3 What is mean by reviewing logs? *(Refer section 2.2)* (5 Marks)

☛ **Syllabus Topic : Network Forensic Tools**

Q. 4 Write a short note on network forensic tools? *(Refer section 2.3)* (5 Marks)

☛ **Syllabus Topic : Performing Live Acquisitions**

Q. 5 What is the general procedure given for live acquisition ? *(Refer section 2.4)* (5 Marks)

☛ **Syllabus Topic : Order of Volatility**

Q. 6 What is order of volatility ? *(Refer section 2.5)* (5 Marks)

☛ **Syllabus Topic : Standard Procedures**

Q. 7 What is the standard procedure used in network forensics ? *(Refer section 2.6)* (5 Marks)

Chapter End

Unit I

CHAPTER 3

Cell Phone and Mobile Device Forensics

Syllabus Topic : Overview

3.1 Overview

Q. 3.1.1	What type of information does the mobile phone contains ? *(Ref. Sec. 3.1)*	**(5 Marks)**
Q. 3.1.2	Explain the digital networks for mobile phones. *(Ref. Sec. 3.1)*	**(5 Marks)**
Q. 3.1.3	Explain the technologies where the 4G network can be used. *(Ref. Sec. 3.1)*	**(5 Marks)**
Q. 3.1.4	What are the main components used with cell phone for communication ? *(Ref. Sec. 3.1)*	**(5 Marks)**
Q. 3.1.5	Explain SIM card *(Ref. Sec. 3.1)*	**(5 Marks)**

- Cell phone and mobile device forensics is a fast changing field as maximum work is done by mobile device.
- In cell phone people save lots and lots of data, so if in case you lose your mobile phone, the data stored in the cell phone also get lost and it may be used for wrong purposes. It is observed that many people do not secure their cell phones, though they regularly lock and secure laptops or desktops.
- Now a day's maximum transactions are done via mobile like people log into their bank accounts and transfer the funds and perform other banking work. Your mobile phone contains the following information.
- Incoming calls, outgoing calls, and missed calls
  - Text and Short Message Service (SMS) messages