MODULE 04 – NETWORK FORENSICS

Q. Explain techniques of tracing an email message. ⇒ HBSNS²

Ans.

Email tracing is a technique to reveal exact time & date when an email was received or opened as well as IP address of the recipient, detailed record of email transaction, intent of the sender etc. Various approaches used for tracing an email are briefly defined below:

1. Header Analysis:

Metadata in the email message in the form of control information i.e envelope & headers including headers in the message body contain information about the sender and/or the path along which the message has traversed.

A detailed analysis of these headers & their correlation is performed in header analysis.

2. Bait Tactics:

In these technique investigations of an email is done with http: "Error! Filename not specified." tag having image source at some computer monitored by the investigation is send to the sender of an email containing real e-mail address.

When the email is opened, a log entry containing IP address of recipient is recorded on http server hosting the image & thus sender is tracked.

3. Server Investigation:

In this investigation, copies of delivered emails and server logs are investigated to identify source of an email message.

Emails purged from clients (senders or receivers) whose recovery is impossible may be requested from servers as most of them store a copy of all emails after their deliveries.

Further, logs maintained by servers can be studied to trace the address of the computer responsible for making the e-mail transaction.

4. Network Device Investigation:

In this form of e-mail investigation, logs maintained by the network devices such as routers, firewalls and switches are used to investigate the source of an e-mail message.

This form of investigation is complex and is used only when the logs of servers (Proxy or ISP) are unavailable due to some reason, e.g. when ISP or proxy does not maintain a log or lack of cooperation by ISP's or failure to maintain chain of evidence.

5. Software Embedded Identifiers:

Some information about the creator of e-mail, attached files or documents may be included with the message by the e-mail software used by the sender for composing e-mail.

This information may be included in the form of custom headers or in the form of MIME content as a Transport Neutral Encapsulation Format (TNEF).

6. Sender Mailer:

Fingerprints Identification of software handling e-mail at server can be revealed from the Received header field and identification of software handling e-mail at client can be ascertained by using different set of headers like "X-Mailer" or equivalent.

Shaunashree . V . More .

Q. Explain the procedure to investigate routers.

Ans.

Steps in router investigation:

1. **Establishing a router connection:**

It is used in accessing a router from the console port & whenever router connection is established at that time to make sure to log the entire session.

2. **Record System time:**

It helps in the cross referencing the data.

3. **Determining who is logged on:**

It helps in finding who is logged on the router.

4. **Determine the routers uptime:**

It is nothing but the time that shows when the system has been online since the last reboot session.

5. **Determine the listening sockets:**

It is used to determine which ports are listening on the router & uses an external port to detect which services are running on the router.

6. **Save the router Configuration:**

Here the information is stored in NVRAM & router boots uses this stored configuration.

It is possible to change the configuration of router without modifying the file stored in NVRAM.

7. **Review the routing table:**

This table contains the blueprint of how the router forwards packets & if an attacker does the changes to the table then the attacker also changes the packets which are sending location.

8. *Check interface configurations:*

The information of every routers interface which is available in configuration file should be checked.

9. *View the ARP (Address Resolution Protocol) Cache:*

This maps the IP addresses & MAC addresses, so this ARP cache is useful when investigating attacks happen.

Q. Short note on Internet Fraud.

Ans.

Internet fraud is the use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them. Tools which are used for internet fraud are such as follows:

1. Email
2. Chat rooms
3. Websites
4. Message Boards
5. Portals
6. Web Application

Types of frauds are: SPAM SCI SIP ISS

1. **Spam:** It is used to describe electronic 'junk mail' or unwanted messages, which are sent to your email account or mobile phone. These are irrelevant messages sent typically to a large number of users for purpose of advertising, phishing etc.

2. **Scams:** It refers to the scheme that is fraudulent & intents to make gains out of fraudulent schemes.

3. **Phishing:** It is a technique used to gain victim's personal information for the purpose of identity theft. It involves targeting online banking customers, sending phishing emails or other online payment facilities.

4. **Identity Theft:** It is an identity fraud which refers to the theft of personal data of victim & using the same to create a false identity.

5. **Internet banking fraud:** This fraud is committed using online technology to illegally remove money from a bank account or transfer money to an account in a different bank.

6. **Spyware:** These are the software that are installed on victim's computer secretly & steals data from victim's computer without victim's permission or knowledge.

i) IDS used for monitoring both user & system activities
2) detect attack which may harm the system by continuously monitoring it.
3) Provides cross platform protection
4) To track user policy violations
5) Performs analysis of abnormal activity pattern in order to secure a n/w.

Q. Short note on Intrusion Detection.

Ans.

An intrusion detection system (IDS) is a type of security software designed to automatically alert administrators when someone or something is trying to compromise information system through malicious activities or through security policy violations.

An IDS works by monitoring system activity through examining vulnerabilities in the system, the integrity of files and conducting an analysis of patterns based on already known attacks. It also automatically monitors the Internet to search for any of the latest threats which could result in a future attack.

Types of IDS:

1. Network based Intrusion Detection System:

Network Intrusion Detection Systems (NIDS) usually consists of a network appliance (or sensor) with a Network Interface Card (NIC) operating in promiscuous mode and a separate management interface.

The IDS is placed along a network segment or boundary and monitors all traffic on that segment.

NIDS is used to monitor & analyze n/w traffic & protect sys from n/w based threat.

2. Host based Intrusion Detection System:

A Host Intrusion Detection Systems (HIDS) and software applications (agents) installed on workstations which are to be monitored.

The agents monitor the operating system and write data to log files and/or trigger alarms.

A host Intrusion detection systems (HIDS) can only monitor the individual workstations on which the agents are installed and it cannot monitor the entire network.

Host based IDS systems are used to monitor any intrusion attempts on critical servers.

capable of monitoring & analyzing the internals of a comp sys as well as the n/w packets on its n/w interface.

Advantages:

1. IDS recognize constantly developing the number of issues.
2. Less expensive
3. Simpler to control

3) Signature based IDS:-
- simple pattern matching
- Maintains database of signature.
- Signature based IDS monitors the packet on the network and compare them against a database of signatures.

Types :- Host, NIW, Anomaly, Protocol Based, Signature based, Hybrid IDS.

Disadvantages:

1. Not very much protected which makes it useless.
2. IDD's does not run itself, somebody needs to monitor its record & react to its alarm.
3. Sensitivity is restricted by IDS & so finding the best possible balance is critical.

④ Anomaly based IDS

- It is based on behaviour of user.
- Monitors the system activity & classifies them as either normal or anomalous based on heuristic rather than signature.

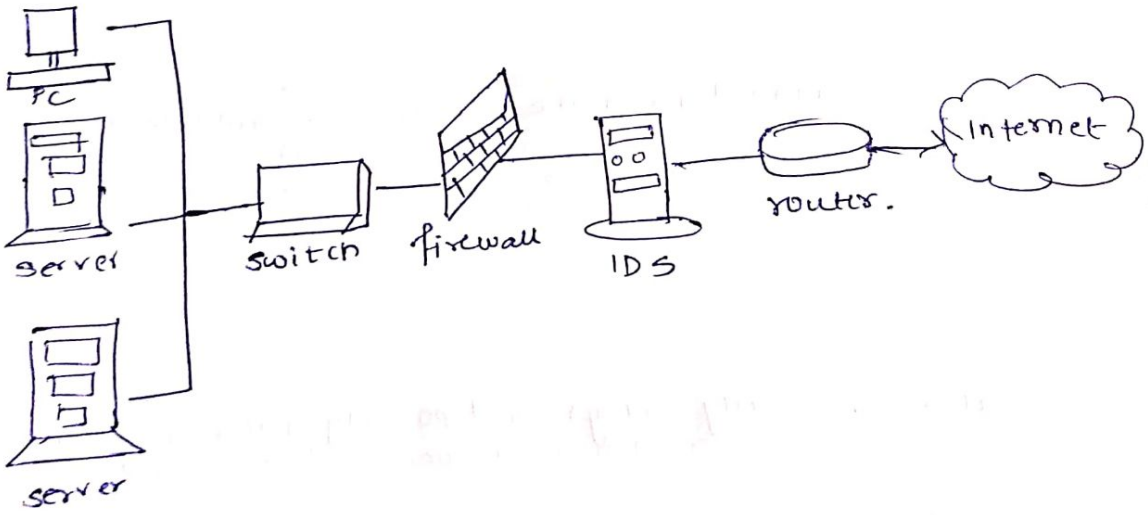

Diagram.

Q. Explain the attacks of the network & its prevention.

Ans.

Computer Network Attack is an attempt to destroy, steal and gain unauthorized access from web services or network and make unofficial use of information.

Some attacks are passive means in this attack data would be analyzed and monitored to gain authorized information like password and it results in leakage the data files to the attacker without authorization of users.

While some are an active attack where data may be altered through worms, viruses or Trojan horse in order to corrupt or destroy information or network itself.

Let's look at common network attacks:

1. **Eavesdropping:** Eavesdrop means to listen private conversation secretly as per meaning in Eavesdropping data exposed by the capturing data packets which transforms between computers on the network.

2. **Daniel of service (DoS) attack:** Daniel of service attack is network attack with intend to prevent the use of the computer and the web services from the authorized users.

   intented to make resource unavailable to authorized users.

3. **Man in the Middle attack:** It is an attack in eavesdropping form where attackers steal the private information of users from computer network.

   Decrypted transformation on server gets high chances of sniffing, user gets any information on the web.

   Attacker uses the public key of the user and steals private information like credit card number, email addresses etc.

   attacker secretly relays and possibly alters the comm^n bet^n 2 parties who believe they are directly communicating with each other

4. **IP Spoofing:** Every computer system on the internet has ip address that reveals its identification. IP Address spoofing also known as ip address forgery, it is a hijacking technique that highjack the host browser to gain the access of the network.

5. **Sniffer Attack:** sniffer is a device or function that capture data packets on the network and attacker get the important information among them like Password, credit card number, email address etc.

6. DNS (Domain Name System) Spoofing: Domain name system is an organized way of naming computer and services connected to the web or private network. It translates the name in to the IP address because the Domain names are in alphabetical so it is easy to memorize.

How to prevent network attacks

It is hard to detect and prevent network attack once the virus built and further, we do not know the type of virus but we could prevent same if take some actions regarding that.

1. Chang your password frequently to prevent password hacking.
2. Take a backup of important files and programs regularly.
3. Do not open the unknown or spam email without security.
4. Use antivirus program to detect and prevent from the viruses.
5. Uses strong encryption to perform daily transaction on the web when you transfer your personal information, can use SSL (Digital Certificate) which being hard for intruders.
6. Using firewall, it is a machine between your system's network and internet that filtering the traffic which might be unsafe.

There are various types of network attacks to harm the system one or another way like some attacks intend to theft the information for make money and some to corrupt or control the system or server. So best practice is to use strong encryption or take above steps to detect and prevent computer network attack.

MODULE 05 – SYSTEM INVESTIGATION

Q. What are various hacking tools? Explain any two in detail.

Ans.

Ethical hacking tools help in information gathering, creating backdoors & payloads, cracking passwords and an array of other activities.

1- Metasploit Framework

The tool that turned hacking into a commodity in which the Metasploit Framework made cracking known vulnerabilities as easy as point and click. Although sold as a penetration testing tool, Metasploit's free version is still where most neophyte hackers cut their teeth.

2 – OpenSSH

OpenSSH is a suite of low-level tools that rights many of the wrongs built into the original network-level utilities in most Internet operating systems. Created as an integral part of the bulletproof OpenBSD UNIX implementation, OpenSSH was useful enough and solid enough that it was quickly adopted by other UNIX forks and made available as portable packages for other operating systems.

3 – Nessus

Nessus is the world's most popular vulnerability scanner, a battle-scarred champion that has held that throne for decades even as new challengers have crowded the arena in recent years.

1. NMAP

Description:

Nmap is a security scanner, port scanner, as well as a network exploration tool.

It is an open source software and is available for free.

It supports cross-platform.

It can be used for network inventory, managing service upgrade schedules, and for monitoring host & service uptime.

It can work for a single host as well as large networks. It provides binary packages for Linux, Windows, and Mac OS X.

Features:

- **Nmap suite has:**

o Data transfer, redirection, and debugging tool(Ncat),

- Scan results comparing utility(Ndiff),
- Packet generation and response analysis tool (Nping),
- GUI and Results viewer (Nping)

- **Using raw IP packets it can determine:**

- The available hosts on the network.
- Their services offered by these available hosts.
- Their OS.
- Packet filters they are using.
- And many other characteristics.

Nmap uses raw IP packets to determine –

what hosts are available on the network,

what services those hosts are offering,

what operating systems they are running on,

what type of firewalls are in use, and other such characteristics

Nmap runs on all major computer operating systems such as Windows, Mac OS X, and Linux.

Advantages:

1. Scans for open ports, giving you the option of how aggressively or lightly to scan.

2. Can help determine which OS and services are running on a device, again, giving the option of how aggressively to scan a device.

3. Nmap has a unique process of fingerprinting applications/devices to help us identify their communications patterns quicker.

4. Nmap can be used for network auditing by specifying whole subnets that you would like to scan for open/closed ports.

5. Nmap has a diverse presence and can be used from most operating systems.

Disadvantages:

1. A number of shortcuts and GUI options are available in Zenmap to simplify the process, but perhaps a more visual interface can help simplify the selection process prior to executing the Nmap command.

2. Since Nmap is a free software, new and updated versions don't pop up regularly.

It's rather complete as it is, but technologies advance quickly and it would benefit NMAP to try to keep up.

3. Nmap is currently offered as graphical and command line programs. Not sure if a web-based version would be something the developers would consider.

4. Nmap does not appear to offer commercial support so you are at the mercy of the community and developers if you have a particular problem you need to find a resolution for in a short amount of time.

2. Wireshark

1. **Wireshark** is a free and open-source packet analyzer.

2. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

3. Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows.

4. There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU General Public License.

Features

1. Wireshark has a rich feature set which includes the following:

2. Deep inspection of hundreds of protocols, with more being added all the time

3. Live capture and offline analysis

4. Standard three-pane packet browser

5. Multi-platform: Runs on Windows, Linux, OS X, FreeBSD, NetBSD, and many others

6. Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility

7. The most powerful display filters in the industry

8. Rich VoIP analysis

9. Capture files compressed with gzip can be decompressed on the fly

Advantages:

1. Free software

2. Available for multiple platforms

3. Can see detailed information about packets within a network

Disadvantages:

1. Notifications will not make it evident if there is an intrusion in the network

2. Can only gather information from the network but cannot send it

Dhanashree . V . More ,

Q. Explain techniques used to recover deleted files

Ans.

Many a times we want to clear the unallocated space on a restored image in order to undelete or recover as many files or file fragments as possible.

To recover the file on windows system we use the following tools:

1. Windows based tools: Encase, FTK

a. It is used to recover files on FAT file systems & have built-in capability and automatically recover any files they can

2. Linux tools: Fatback, TASK & Foremost

Here three utilities are used to recover data they are as follows:

a. FatBack to Recover Deleted Files

1. Fatback is used to recover deleted files from the FAT system.
2. It also performs file recovery on FAT12, FAT16, and FAT32 file systems on linux platform
3. Following are the features of FatBack:
4. It supports the long filename.
5. There is recursive undeletion of directories.
6. Lost cluster chain recovery.
7. To recover the files following commands are used:

    -a option runs fatback in automatic undelete mode

    -o option places recovered files into the specified directory.

    -s option tells fatback to treat the input file evidencefloppy.bin as a single partition

b. Using task to recover deleted files

It is an open source forensic toolkit which is used to analyze microsoft and unix file systems.

This can recover files from different file systems including FAT12, FAT16 and FAT32, etc

Task can work on binary images which do not have embedded checksum values and works with only single partition so that image in drive separately use this tool.

c. Using Foremost to recover lost files

This recovers file based on headers and footers.

Foremost is portable and exceptional tool for data recovery.

It works on file generated by dd, safeback, or directly on a device.

Q. Explain various ethical issues concern in computer forensics.

Ans.

1. Ethics: "The science of morals, the department of study concerned with the principles of human duty, the moral principles by which a person is guided."

Some of the ethical issues are briefly defined below:

2. Repositories and processors of information: Unauthorized utilization of generally unused computer services or of data put away in computers brings up issues of suitability or fairness.

3. Producers of new forms and types of assets: Computer programs are combinedly new types of assets, potentially not subject to the same ideas of ownership as other assets.

4. Instruments of acts: To what extents must computer services and users of computers information & programs be responsible for integrity and suitableness of computer output.

5. Technology instruction: Internal and external privacy to the firm, computer observation. Employee monitoring hacking

6. Ownership issues: Moonlighting, software copyrights theft of information, etc.

7. Personal issues: This issue covers the Employee harm and human components to keep away from job obsolescence.

MODULE 06 – BODIES OF LAW

Q. Explain the term DMCA, CFAA, CANspam

Ans.

DMCA:

The Digital Millennium Copyright Act (DMCA) was signed into law by President Clinton on October 28, 1998. The DMCA is divided into five titles which are briefly described below:

TITLE 1: WIPO TREATY IMPLEMENTATION

1. It makes certain technical amendments to provide appropriate references and links. It creates two prohibitions:

2. To avoid copyrights and protect their works

3. To add civil remedies and criminal penalties for violating the prohibitions

Technical amendments cover:

1. National Eligibility (Section 102(b))

2. Restoration of Copyright Protection (Section 102(c))

3. Registration as a Prerequisite to Suit (Section 102(d))

Technological Protection and Copyright Management Systems This includes:

1. General approach

2. No mandate

3. Savings clauses

The five additional exceptions are as follows:

1. Reverse Engineering Exceptions

2. Exceptions for Law Enforcement and Intelligence

3. Encryption research exceptions

4. Security testing exceptions

5. Exceptions for non profit Libraries, archives and educational institutions

TITLE 2: ONLINE COPYRIGHT INFRINGEMENT LIABILITY LIMITATION

This adds a new section 512 to copyright act to create new limitations which are listed below:

1. Transitory communication
2. System caching
3. Information location tools
4. Storage of information on systems or network at direction of users, etc

TITLE 3: COMPUTER MAINTENANCE OR REPAIR

This expands the existing exemption related to our computer programs in section 117 of the copyright act.

This allows the owner of a copy of a program to make reproductions whenever necessary to use the programs.

This permits the owner to make authorize copy of program in that computer.

This permission is accepted only when the computer is activated.

TITLE 4: MISCELLANEOUS PROVISIONS

This includes:

Ephemeral Recordings for broadcasters

Distance Education Study

Exemption for non profit libraries and activities

Webcasting Amendments to the digital performance right in sound recordings

Assumptions of contractual Obligations upon transfers of rights in motion pictures

TITLE 5: PROTECTION OF CERTAIN ORIGINAL DESIGNS

Title of DMCA, entitled the vessel hull design protection act.

It creates new systems for protecting original designs.

Useful articles are limited to the hulls.

Protection is lost if an application for registration is not made within two years after a design is made public.

CFAA:

The **Computer Fraud and Abuse Act (CFAA)** is a United States cyber security bill that exist in computer fraud law as Comprehensive Crime Control Act of 1984.

The law prohibits accessing a computer without authorization, or in excess of authorization.

The original 1984 bill was enacted in response to concern that computer-related crimes might go unpunished.

The CFAA was written to increase the scope limiting, where computers of the federal government or certain financial institutions are involved or where the crime itself is interstate in nature."

CANspam:

CAN-SPAM (Controlling the Assault of Non-Solicited Pornography And Marketing) is an act that was passed in 2003.

That act is a law that establishes the rules for commercial email and commercial messages, gives recipients the right to have a business stop emailing them, and outlines the penalties incurred for those who violate the law.

The Bureau of Consumer Protection notes that CAN-SPAM doesn't *just* apply to bulk email but also covers all commercial messages, which the law defines as 'any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service,' including email that promotes content on commercial websites.

The law makes no exception for business-to-business email." It does, however, exempt transactional and relationship messages.

Rules to Follow for CAN-SPAM Compliance

In order to be CAN-SPAM compliant, it's important your email messages follow these rules,

DO's

1. Do include your valid physical postal address in every email you send out.

2. Do provide a clear and obvious way to opt out of every email you send out, and honor the unsubscribe within 10 business days.

3. Do use clear "From," "To," and "Reply to" language that accurately reflects who you are. This applies to the person or business sending the message, as well as the domain name and email address.

DONT's

1. Don't sell or transfer any email addresses to another list.

2. Don't make it hard to unsubscribe from emails.

3. You cannot;

   1) Charge a fee

   2) Require a recipient to provide personally identifying information beyond an email address, or

   3) Make recipients take extensive steps other than simply replying to an email or visiting a single page on a website to unsubscribe themselves from your emails.

   4) Don't use deceptive subject lines in your emails that misrepresent the contents of your message.

Q. Explain bodies of law.

Ans.

Criminal law :

Criminal law is the body of law that deals with crime and the legal punishment of criminal offenses.

To maintain the stability of the state and society by punishing offenders and deterring them and others from offending. "Innocent until proven guilty":

The prosecution must prove defendant guilty.

A guilty defendant is subject to Custodial (imprisonment) or Non-custodial punishment (fines or community service).

In exceptional cases, the death penalty.

Example - Theft, assault, robbery, trafficking in controlled substances, murder, etc

Civil Law :

Civil law deals with the disputes between individuals, organizations, or between the two, in which compensation is awarded to the victim.

To deal with the disputes between individuals, organizations, or between the two, in which compensation is awarded to the victim.

Claimant must give proof however, the burden may shift to the defendant in situations of Res Ipsa Loquitur (The thing speaks for itself).

Compensation (usually financial) for injuries or damages, or an injunction in nuisance.

Example - Landlord/tenant disputes, divorce proceedings, child custody proceedings, property disputes, personal injury, etc.

Administrative/Regulatory law:

It is the third body of law which is often overloaded in discussion of criminal & civil law.

It consists of rules & regulations that are approved by government agency under authority given to it by the legislative body & that applies to a particular field.

Example- Environmental Protection Agency regulations

Dhanashree . V . More .

Q. Explain levels of laws

Ans:

Responsibilities

Representatives are elected to federal and state/territory parliaments and local councils, so that all Australians have someone to represent them at each level of government.

Parliaments and councils make laws; governments put these laws into action.

Some of the responsibilities of federal, state/territory and local governments overlap, but generally each level of government provides different services to Australians:

The federal government has broad national powers. Among other things, it administers (puts into action) laws in relation to defence, immigration, foreign affairs, trade, postal services and taxation.

State/territory governments have the power to look after laws not covered by the federal government; for instance, hospitals, schools, police and housing services.

The powers of local councils are defined by Acts of Parliament passed by state parliaments and include responsibility for building regulations, rubbish collection, local roads and pet control.

All levels of government raise money, through collecting taxes, to pay for services provided to Australians. State/territory and local governments also receive some money from the federal government, and states fund local councils.

FEDERAL LAW: [National Law] Bill passed

The federal government raises money to run the country by collecting taxes on incomes, goods and services and company profits and spends it on national matters: for example, trade, defence, immigration and the environment.

STATE/TERRITORY:

State/territory governments also raise money from taxes but receive more than half their money from the federal government and spend it on state/territory matters: for example, schools, housing and hospitals, roads and railways, police and ambulance services.

LOCAL:

Local councils collect taxes (rates) from all local property owners and receive grants from federal and state/territory governments and spend this on local matters: for example, town planning, rubbish collection, water and sewerage, local roads and pet control.

Territories

Local councils in the Northern Territory (NT) are established by the NT Legislative Assembly under a local government law. The Australian Capital Territory (ACT) does not have local councils, as the ACT Legislative Assembly combines both state and local government functions.

The Australian Constitution

Section 51 of the Australian Constitution details the powers of the federal Parliament to make laws in relation to national matters. These laws are administered by the federal government.

Issues not listed in section 51 are the responsibility of state governments.

Under section 109 of the Constitution, if a state Parliament and the federal Parliament pass conflicting laws on the same subject, then the federal law overrides the state law.

Section 122 of the Constitution allows the federal Parliament to override a territory law at any time.