Chapter 4
Computer Forensics Technology

10 hrs

Er. Shiva Ram Dam

Assistant Professor

Gandaki University

Content:

1. **Overview of Computer Forensics and Forensic Tools**
   - ❑ Introducing Kali Linux
   - ❑ Nmap, Wireshark, Metasploit, FTK Imager, Autopsy, e.tc.
   - ❑ Data Recovery Tools (Photorec, AccessData, TSK, e.tc.)
2. **Rules of Evidence (Admissible, Authentic, Complete, Reliable, Believable)**
3. **Good Forensic Practices (Identification, Securing the evidence, Collecting, Packaging, Preserving the evidence, Documenting the evidence, Documenting all changes)**
   - ❑ Getting Familiar with command line tools (SSH, Telnet)
   - ❑ Password-protected and Password-less SSH
   - ❑ Network Monitoring tools, Live Threat Maps, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Packet Sniffing

4.1 Overview of Computer Forensic and Forensic Tools

1. **Overview of Computer Forensics and Forensic Tools**
   - ❑ **Introducing Kali Linux**
   - ❑ **Nmap, Wireshark, Metasploit, FTK Imager, Autopsy, e.tc.**
   - ❑ **Data Recovery Tools (Photorec, AccessData, TSK, e.tc.)**

Computer Forensic

- Aka Digital forensic.
- is **the process of methodically examining computer media** (hard disks, diskettes, tapes, etc.) for evidence.
- A thorough analysis by a skilled examiner can result in the reconstruction of the activities of a computer user.
- In other words, computer forensics is **the collection, preservation, analysis, and presentation of computer related evidence**.
- Computer evidence can be useful in criminal cases, civil disputes, and human resources/employment proceedings.

Background:

- The continuing technological revolution in communications and information exchange has created an entirely new form of crime: cyber crime or computer crime.
- Computer crime has forced the computer and law enforcement professions to develop new areas of expertise and avenues of collecting and analyzing evidence.
- This is what has developed into the science of computer forensics.
- The process of acquiring, examining, and applying digital evidence is crucial to the success of prosecuting a cyber criminal.
- With the continuous evolution of technology, it is difficult for law enforcement and computer professionals to stay one step ahead of technologically savvy criminals.
- **To effectively combat cyber crime, greater emphasis must be placed in the computer forensic field of study**, including but not limited to financial support, international guidelines and laws, and training of the professionals involved in the process.

Roles of a computer in a crime

- A computer can play one of three roles in a computer crime.
  - A computer **can be the target of the crime**,
  - it can be the **instrument of the crime**, or
  - it **can serve as an evidence repository** storing valuable information about the crime.
- In some cases, the computer can have multiple roles. It can be the **"smoking gun"** serving as the instrument of the crime.
- It **can also serve as a file cabinet** storing critical evidence.
  - For example, a hacker may use the computer as the tool to break into another computer and steal files, then store them on the computer.
- When investigating a case, it is important to know what roles the computer played in the crime and then tailor the investigative process to that particular role.

- **Applying information about how the computer was used** in the crime also helps when searching the system for evidence.
  - **If the computer was used to hack into a network password file, the investigator will know to look for password cracking software and password files**.
  - **If the computer was the target of the crime, such as an intrusion, audit logs and unfamiliar programs should be checked.**
- Knowing **how the computer was used** will help narrow down the evidence collection process.
  - **With the size of hard drives these days, it can take a very long time to check and analyze every piece of data a computer contains.**

Concerns in Digital forensics

- **The Computer Forensic Objective:**
  - The objective in computer forensics is to **recover, analyze, and present computer-based** material in such a way that it is useable as evidence in a court of law.
- **The Computer Forensic Priority:**
  - In computer forensics, the absolute priority **is accuracy.**
  - One talks of completing work as efficiently as possible, that is, as fast as possible without sacrificing accuracy.
- **Accuracy versus Speed:**
  - Pressure is heaped upon you to work as fast as possible.
  - Working under such pressure to achieve deadlines may induce people to **take shortcuts in order to save time.**
  - In computer forensics, as in any branch of forensic science, the **emphasis must be on evidential integrity and security.**

The Computer Forensics Specialist

- A computer forensics specialist is the **person responsible for doing computer forensics.**
- The computer forensics specialist will **take several careful steps to identify and attempt to retrieve possible evidence** that may exist on a subject computer system.

Roles of Computer Forensic Specialist

1. **Protect the subject computer system** during the forensic examination from any possible alteration, damage, data corruption, or virus introduction.
2. **Discover all files** on the subject system. This includes existing normal files, deleted yet remaining files, hidden files, password-protected files, and encrypted files.
3. **Recover** all (or as much as possible) of discovered **deleted files.**
4. **Reveal** (to the extent possible) **the contents of hidden files** as well as temporary or swap files used by both the application programs and the operating system.
5. **Accesses** (if possible and if legally appropriate) the contents of protected or **encrypted files.**
6. **Analyze all possibly relevant data** found in special (and typically inaccessible) areas of a disk.
7. **Print out an overall analysis** of the subject computer system, as well as a listing of all possibly relevant files and discovered file data.
8. **Provide expert consultation** and/or testimony, as required.

Who Can Use Computer Forensic Evidence?

Many types of criminal and civil proceedings can and do make use of evidence revealed by computer forensics specialists.

1. **Criminal Prosecutors** use computer evidence in a variety of crimes where in-criminating documents can be found: homicides, financial fraud, drug and embezzlement record-keeping, and child pornography.
2. **Civil litigations** can readily make use of personal and business records found on computer systems that bear on fraud, divorce, discrimination, and harassment cases. Insurance companies may be able to mitigate costs by using discovered computer evidence of possible fraud in accident, arson, and workman's compensation cases.
3. **Corporations** often hire computer forensics specialists to find evidence relating to sexual harassment, embezzlement, theft or misappropriation of trade secrets, and other internal/confidential information.
4. **Law enforcement officials** frequently require assistance in pre-search warrant preparations and post seizure handling of the computer equipment. The use of computer forensics in law enforcement is discussed in detail in the next section and throughout the book.
5. **Individuals** sometimes hire computer forensics specialists in support of possible claims of wrongful termination, sexual harassment, or age discrimination.

Computer Forensic services

- No matter how careful they are, when people attempt to steal electronic information (everything from customer databases to blueprints), they leave behind traces of their activities.
- Likewise, when people try to destroy incriminating evidence contained on a computer (from harassing memos to stolen technology), they leave behind vital clues.
- In both cases, those traces can prove to be the smoking gun that successfully wins a court case.
- Thus, **computer data evidence is quickly becoming a reliable and essential form of evidence** that should not be overlooked.
- **A computer forensics professional does more than turn on a computer, make a directory listing, and search through files.**
- You, as forensics professionals, should be able to successfully perform complex evidence recovery procedures with the skill and expertise that lends credibility to your case.

- Some of the computer forensics services are as listed below:
  a) Data Seizure
  b) Data duplication and preservation
  c) Data recovery
  d) Document searches
  e) Media conversion
  f) Expert witness services
  g) Computer evidence service options
  h) Other miscellaneous services

a) Data Seizure

- Data seizure in computer forensics refers to the **process of identifying, collecting, and preserving digital evidence from electronic devices** for use in legal investigations.
- Federal rules of civil procedure let a party or their representative inspect and copy designated documents or data compilations that may contain evidence.

b) Data Duplication and Preservation

- When one party must seize data from another, two concerns must be addressed: the **data must not be altered in any way,** and the **seizure must not put an undue burden on the responding party.**
- Your computer forensics experts should acknowledge both of these concerns by making an exact duplicate of the needed data.
- Because duplication is fast, the responding party can quickly resume its normal business functions, and,
- because your experts work on the duplicated data, the integrity of the original data is maintained.

c) Data Recovery

- **Using proprietary tools,** your computer forensics experts should be able to safely recover and analyze otherwise inaccessible evidence.
- The ability to recover lost evidence is made possible by the **expert's advanced understanding of storage technologies.**
  - **For example, when a user deletes an email, traces of that message may still exist on the storage device.**
- Although the message is inaccessible to the user, your experts should be able to recover it and locate relevant evidence.

d) Document Searches:

- Your computer forensics experts **should also be able to search over 200,000 electronic documents in seconds rather than hours.**
- The speed and efficiency of these searches make the discovery process less complicated and less intrusive to all parties involved.

e) Media Conversion

- Some clients need to obtain and investigate computer data stored on old and un-readable devices.
- Your computer forensics experts should extract the relevant data from these devices, convert it into readable formats, and place it onto new storage media for analysis.

f) Expert Witness Services

- Computer forensics experts should be able to explain complex technical processes in an easy-to-understand fashion.
- This should help judges and juries comprehend how computer evidence is found, what it consists of, and how it is relevant to a specific situation

Digital Forensic Process

1. **Identification**
   - Identifying digital evidence ensures that investigators collect the right evidence and that it's not contaminated by other data sources.
   - It involves identifying who or what is involved in the crime by looking at metadata related to the digital evidence (e.g., a video file).
2. **Preservation**
   - Digital information can easily be altered or destroyed if mishandled, so it must be preserved to keep it safe from tampering. This maintains the integrity of the evidence.
3. **Analysis**
   - This involves reviewing the identified evidence to determine the accuracy of the results. Analysts then look for any additional data that might help answer questions about the case.
4. **Documentation**
   - Digital forensic analysts need to document their findings in court as evidence. Other investigators or supervisors within the organization may also request access to this information for their purposes.
5. **Presentation**
   - After documentation, experts summarize and present their findings to a court or any other investigating authority.

Digital Forensic Tools

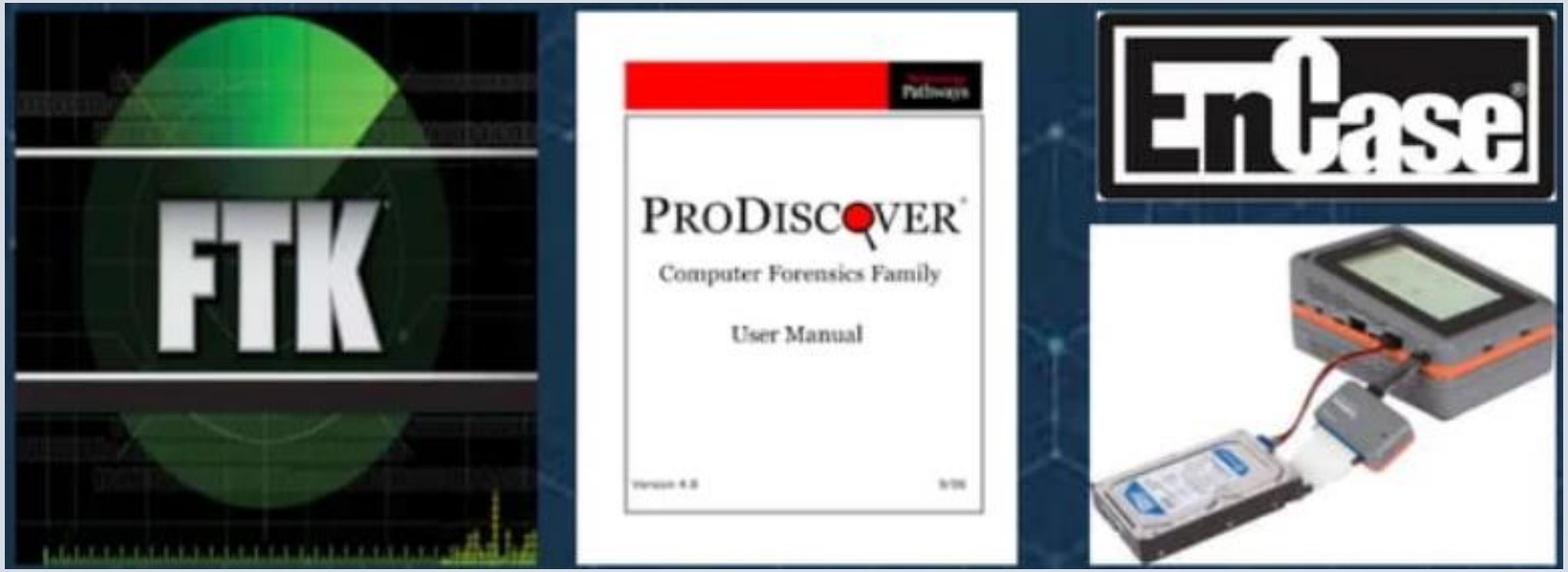
- Forensic tools are software or hardware solutions designed to assist investigators in handling digital evidence.
- Some of the Forensic tools are:

Tools	Purpose	Examples
Data Acquisition Tools	Capture a forensic image of digital storage devices..	• FTK Imager. • EnCase. • dd (Unix/Linux command-line tool).
Data Recovery Tools	Recover deleted, corrupted, or hidden files.	• Recuva. • R-Studio. • TestDisk.
Analysis Tools	Examine and interpret digital evidence.	• Autopsy (open-source forensic tool). • EnCase Forensic. • X-Ways Forensics.
Network Forensic Tools	Monitor and analyze network traffic for malicious activity.	• Wireshark. • tcpdump. • Network Miner.
Mobile Forensic Tools	Extract and analyze data from mobile devices.	• Cellebrite UFED. • Oxygen Forensic Suite. • Magnet AXIOM.
Specialized Tools	• Perform niche functions like memory analysis, steganography detection, or password recovery.	• Volatility (memory analysis). • Hashcat (password cracking). • StegDetect (steganography detection).

Tools	Purpose	Examples
Data Acquisition Tools	Capture a forensic image of digital storage devices..	• FTK Imager. • EnCase. • dd (Unix/Linux command-line tool).
Data Recovery Tools	Recover deleted, corrupted, or hidden files.	• Recuva. • R-Studio. • TestDisk.
Analysis Tools	Examine and interpret digital evidence.	• Autopsy (open-source forensic tool). • EnCase Forensic. • X-Ways Forensics.
Network Forensic Tools	Monitor and analyze network traffic for malicious activity.	• Wireshark. • tcpdump. • Network Miner.
Mobile Forensic Tools	Extract and analyze data from mobile devices.	• Cellebrite UFED. • Oxygen Forensic Suite. • Magnet AXIOM.
Specialized Tools	• Perform niche functions like memory analysis, steganography detection, or password recovery.	• Volatility (memory analysis). • Hashcat (password cracking). • StegDetect (steganography detection).

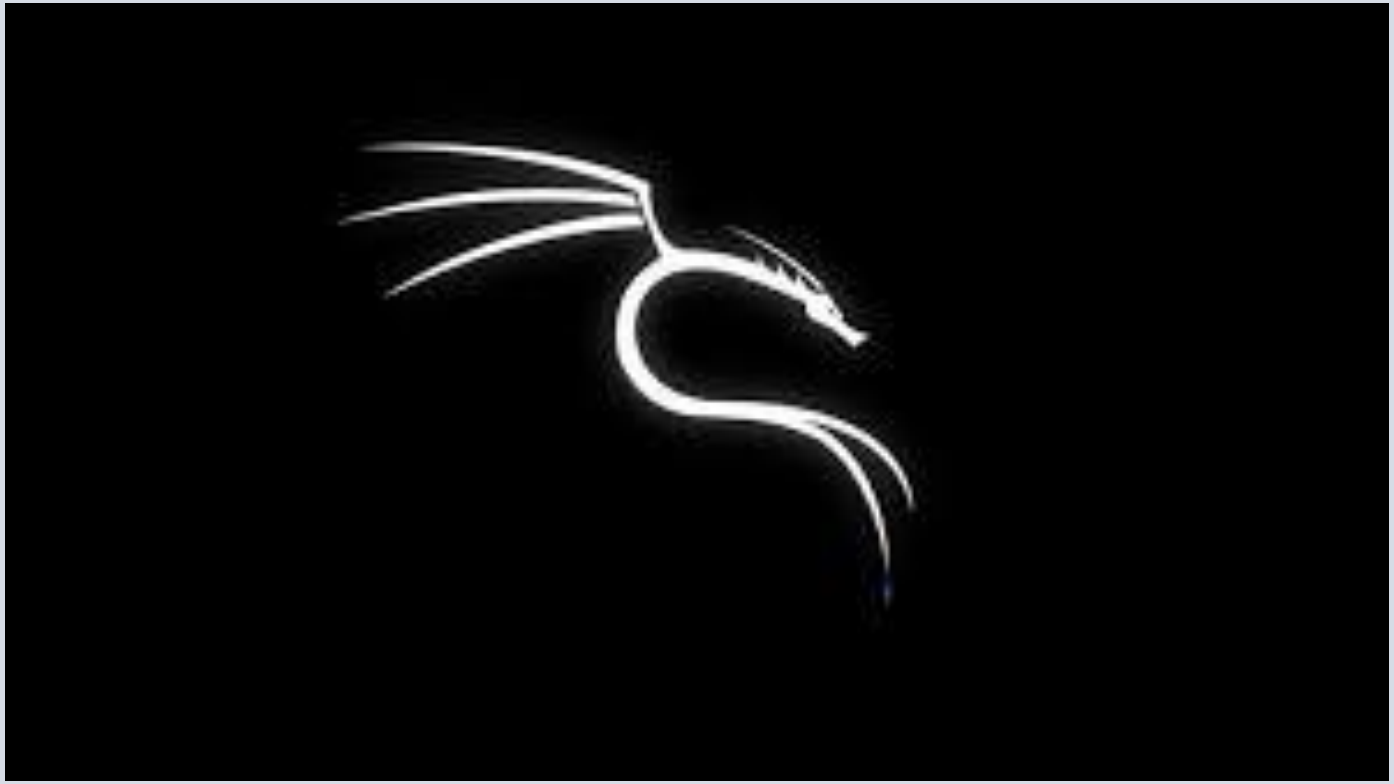
Digital Forensic Tools

- Forensic Imaging Tools:
  - A forensic image (forensic copy) is a bit-by-bit, sector-by-sector direct copy of a physical storage device, including all files, folders and unallocated, free and slack space.



- **Recovery Forensic Tools:**
  - Forensic data recovery is the extraction of data from damaged evidence sources in a forensically sound manner.
  - It can be done with the help of tools such as Recuva, Disk Drill ,etc.

Kali Linux



For download and installation:

https://www.youtube.com/watch?v=sAMnXte56yY

Introduction to Kali Linux

- Kali Linux is a Debian-based Linux distribution designed for digital forensics and penetration testing.
- Developed by Offensive Security, it is a powerful toolset for security professionals and ethical hackers.
- Kali Linux is widely used in computer forensics due to its comprehensive toolset for data acquisition, analysis, and reporting.

Key features of Kali-Linux

1. **Pre-installed Tools:**
   - Kali Linux comes with over 600 pre-installed penetration testing tools, covering various aspects of security and digital forensics.
2. **Customizable and Extensible:**
   - Users can customize their Kali Linux installation to suit their specific needs.
3. **Wide Range of Platforms:**
   - Kali Linux can be installed on a wide range of hardware, including x86, x64, and ARM architectures.
4. **Security and Updates:**
   - Regular updates ensure that Kali Linux users have access to the latest security tools and patches.
5. **Documentation and Community Support:**
   - Extensive documentation and tutorials are available on the official Kali Linux website, helping users get started and learn advanced techniques.

Applications in Forensics:

1. **Data Recovery:** Use tools like TestDisk to recover lost partitions and files.
2. **Network Analysis:** Analyze network traffic with tools such as Wireshark.
3. **File Analysis:** Examine and recover deleted files and metadata.

Some common tools in Kali Linux

1. **Information Gathering :**
   - Information gathering tools are used to collect data about systems, networks, and organizations.
   - Common tools are: ***Nmap****, Maltego, Recon-ng*
2. **Vulnerability Analysis**
   - Vulnerability analysis tools are essential in identifying and assessing security vulnerabilities within systems, applications, and networks.
   - Common tools are: *Nikto, OpenVAS, Lynis, Nessus*
3. **Exploitation Tools:**
   - These tools help security professionals test the effectiveness of security defenses by simulating real-world attacks.
   - Common tools are: **Metasploit** Framework, BeEf (browser Exploitation Framework), SQLmap, etc

4. Forensics Tools:

- Forensic tools are essential for the collection, preservation, analysis, and presentation of digital evidence in a legally sound manner
- Some common tools are : ***Autospy***, *Volatility, Foremost, etc.*

5. Social Engineering Tools:

- These tools are valuable for penetration testers and security professionals to assess and improve the resilience of organizations against social engineering attacks.
- Some common tools are: *Social Engineering Toolkit (SET), Creepy, etc.*

6. Network Sniffers:

- Network sniffers are tools used to capture and analyze network traffic. They are essential for network administrators, security analysts, and penetration testers to monitor and troubleshoot network activity, identify security threats, and perform various network-related tasks.
- Some common tools are : ***Wireshark***, *Tcpdump, etc.*

Nmap

- Nmap (Network Mapper)
- is a powerful, open-source tool **used for network discovery and security auditing.**
- It is widely used by network administrators and security professionals to:
  - map out networks,
  - discover hosts and services, and
  - perform vulnerability assessments.
- Nmap supports various scanning techniques and provides detailed information about network devices, making it an essential tool in the toolkit of anyone responsible for network security.
- Key features of Nmap:
  - Host Discovery
  - Port Scanning
  - OS Detection:
  - Vulnerability Detection
  - Service and Version Detection
  - Network Mapping

Features of Nmap

1. **Network Scanning**:
   - Detects live hosts on a network.
   - Identifies open ports and services running on those ports.
   - Maps the network topology.

2. **Service and Version Detection**:
   - Determines the type of service (e.g., HTTP, FTP) running on a port.
   - Detects the version of the software or service.

3. **Operating System Detection**:
   - Attempts to determine the operating system and its version running on a target machine.

4. **Vulnerability Detection**:
   - Can integrate with NSE (Nmap Scripting Engine) to detect specific vulnerabilities.

5. **Host Discovery**:
   - Discovers devices on a network, even those that might not be actively communicating.

6. **Flexible Output**:
   - Provides results in multiple formats like plain text, XML, or HTML for reporting and analysis.

- Nmap can be run from the command line with various options to perform different types of scans and gather information.
- Syntax:
  - **nmap [scan Types] [options] <target>**
  - Eg: **nmap –sS –p 22 192.168.1.0**
- where
- Some of the scan options and Target options can be like as:

- Some basic commands are:

nmap -sn 192.168.1.0/24	**Performs a ping scan to find live hosts on the network**
nmap 192.168.1.1	**Scans the target host for the most common 1,000 ports.**
nmap -p- 192.168.1.1	**Scans all 65,535 TCP ports on the target host.**
nmap -O 192.168.1.1	**Attempts to determine the operating system of the target host.**

More understanding: https://www.youtube.com/watch?v=W7076RPIgfQ

Wireshark

- Wireshark is a widely-used **open-source network protocol analyzer** that **enables users to capture and interactively browse the traffic running on a computer network.**
- It is an open-source **network sniffing** software, which is designed to **track network packets.**
- It is an essential tool for network administrators, security analysts, and developers to **diagnose network issues**, analyze network performance, and **troubleshoot security problems.**
- Usecases:
  - To analysis network packets
  - Troubleshoot networks issues
  - Check malicious and hacking possibilities

- Some commands in wireshark:

http	**Shows only HTTP protocol traffic.**
ip.addr == 192.168.1.1	**Shows packets to or from the specified IP address 192.168.1.1**
tcp.port == 80	**Shows packets using TCP port 80.**

- Reference Videos:
  - https://www.youtube.com/watch?v=Lb-PJl9u3z8
  - What is Wireshark? Cyberwings Security: https://www.youtube.com/watch?v=hGV8wsiCF28

Metasploit

- Metasploit is a widely used open-source framework for developing, testing, and executing exploits against computer systems.
- **Exploits** are Code that takes advantage of a vulnerability.
- It is primarily employed by security professionals, ethical hackers, and penetration testers to identify vulnerabilities in networks and applications.
- Metasploit is a **widely used penetration testing framework** that
  - provides information about known **security vulnerabilities,**
  - helps in developing and testing exploit code, and
  - enables security assessments.
- It's an essential tool for ethical hackers and security professionals.

Common Uses of Metasploit:

1. **Penetration Testing**: Simulates real-world attacks to assess the security posture of a system or network.
2. **Vulnerability Assessment**: Identifies and validates vulnerabilities in software and configurations.
3. **Security Research**: Provides a platform for security professionals to test and understand new exploits and techniques.
4. **Educational Purposes**: Used for teaching and learning about cybersecurity concepts.

Example : Exploiting a Vulnerability

1. **Launch Metasploit Console**:
   msfconsole
2. **Search for an Exploit**:
   search eternalblue
3. **Select the Exploit**:
   use exploit/windows/smb/ms17_010_eternalblue
4. **Set Target Options**:
   set RHOST 192.168.1.10
   set LHOST 192.168.1.20
5. **Run the Exploit**:
   exploit

Reference Video:

- https://www.youtube.com/watch?v=HWbEbxSaaoA
- https://www.youtube.com/watch?v=5m4KF9XbkzU

FTK Imager

- FTK Imager is **a forensic imaging tool developed by AccessData.**
- It is widely used by digital forensic investigators **to acquire, analyze, and preserve digital evidence** from various storage media and file systems.
- **Key Features**
  1. **Disk Imaging**: Creates bit-by-bit forensic images of hard drives, USB drives, optical discs, and other storage media.
  2. **File System Support**: Supports various file systems including NTFS, FAT, exFAT, HFS+, EXT, and more.
  3. **Logical and Physical Imaging**: Can create logical images (specific files/folders) or physical images (entire drive).
  4. **Memory Dump**: Captures live memory (RAM) from a running system.
  5. **Evidence Analysis**: Allows viewing and analysis of the content within images, including files, folders, and deleted data.
  6. **File Carving**: Recovers deleted files that do not have an active file system record.

More understanding: https://www.youtube.com/watch?v=y80Zk5pUZN8

Autopsy

- Autopsy, **also known as The Sleuth Kit,**
- is a digital forensic tool used for analyzing and investigating digital media.
- Autopsy is a powerful **open-source digital forensic tool** that helps investigators **analyze and extract valuable information from various types of digital media**
- It is used in different fields like law, military, corporate investigation, enforcement, etc.
- Autopsy is **a fast and efficient hard drive solution for investigation** that is majorly used by cybersecurity professionals.
- It is an open-source platform that runs on Windows, Linux, and macOS, making it accessible to a wide range of users.
- Autopsy supports the analysis of various file systems, including NTFS, FAT, HFS+, and Ext2/3/4, and can handle disk images, mobile devices, and network packet captures.

Reference Video for Autopsy

- https://www.youtube.com/watch?v=ifRoOMKRjas&list=PL0fjgIGwLMWQcfUJzpRieduGGsIz8VEq_
- Manual: https://security.packt.com/why-using-the-autopsy-tool-is-best-for-digital-forensics/
- Download Autopsy: https://www.autopsy.com/download/

Data Recovery Tools

- Data recovery tools are essential for retrieving lost or corrupted data from various storage devices.
- Some notable Data recovery tools are:
  1. Photorec
  2. AccessData (FTK-Forensic Toolkit)
  3. The Sleuth Kit (TSK)
  4. Recuva
  5. R-Studio
  6. EaseUS Data Recovery Wizaed
  7. Test Disk
  8. GetDataBack
  9. Stellar Data Recovery

1. Photorec

- **Purpose:** Photorec is designed **to recover lost files, including videos, documents, archives from hard disks**, CD-ROMs, and lost pictures from camera memory.
- **Key Features:**
  - Can recover more than 480 file extensions (about 300 file families).
  - Works with hard drives, CD-ROMs, memory cards, USB drives.
  - Ignored the filesystem and goes after the underlying data.

2. AccessData (FTK - Forensic Toolkit)

- **Purpose:** FTK is a comprehensive forensic tool used primarily **for digital investigations** but also supports data recovery.
- **Key Features:**
  - Provides disk imaging, analysis, and data carving capabilities.
  - Advanced email analysis and password cracking.
  - Can handle large data sets and maintain case integrity.

3. The Sleuth Kit (TSK)

- **Purpose:** TSK is a library and collection of command-line tools **used to investigate disk images and recover data.**
- **Key Features:**
  - Supports file system analysis (NTFS, FAT, exFAT, ext2/3/4, HFS+).
  - Provides tools for file system and volume analysis, file extraction, and data recovery.
  - Includes a graphical interface called Autopsy for easier use.

4. Recuva

- **Purpose:** Recuva is a user-friendly tool **for recovering deleted files** from hard drives, memory cards, and other storage devices.
- **Key Features:**
  - Supports recovery from damaged or newly formatted drives.
  - Deep scan mode for thorough search.
  - Simple and intuitive interface suitable for non-experts.

Rules of Evidence

(Admissible, Authentic, Complete, Reliable, Believable)

Rules of Evidence

- Digital evidence is the information stored or transmitted in binary form that may be relied upon in the court of law.
- Courtrooms rely more and more on the digital information.
- Prevailing evidence in court requires a good understanding of the rules of evidence.
- There are five general rules of evidence that apply to digital forensics and need to be followed in order for evidence to be useful.
- Ignoring these rules makes evidence inadmissible, and your case could be thrown out.
- These five rules are—
  - admissible,
  - authentic,
  - complete,
  - reliable, and
  - believable.
- The rules of evidence are guidelines that govern the admissibility of evidence in legal proceedings.

a) Admissible

- The **evidence must be preserved and gathered** in such a way that it can be used in court or elsewhere.
- Many errors can be made that could cause a judge to rule a piece of evidence as inadmissible.
- For example, evidence that is gathered using illegal methods is commonly ruled inadmissible.

b) Authentic

- The **evidence must be tied to the incident in a relevant way to prove something**.
- The forensic examiner must be accountable for the origin of the evidence.

c) Complete

- When evidence is presented, it must be **clear and complete** and should reflect the whole story.
- It is not enough to collect evidence that just shows one perspective of the incident.
- Presenting incomplete evidence is more dangerous than not providing any evidence at all as it could lead to a different judgment.

d) Reliable

- **Evidence collected from the device must be reliable**. The techniques used and evidence collected must not cast doubt on the authenticity of the evidence.

e) Believable

- A forensic examiner must be able to **explain, with clarity and conciseness**, what processes they used and the way the integrity of the evidence was preserved.
- The evidence presented by the examiner must be clear, easy to understand, and believable by jury.

Good Forensic Practices

- Good forensic practices apply to the collection and preservation of evidence.
- Following the good forensic practices **ensures that evidence will be accepted in a court** as being authentic and accurate.
- Modification of evidence, either intentionally or accidentally, can affect the case.
- So, understanding the best practices is critical for forensic examiners.

1. Securing the evidence

- **Isolate the digital device from all the network** so as to secure the evidence.
- For example: With isolation, the phone is prevented from receiving any new data that would cause active data to be deleted.

2. Preserving the evidence

- As evidence is collected, it **must be preserved in a state that is acceptable in court.**
- Working directly on the original copies of evidence might alter it.
- So, as soon as you recover a raw disk image or files, create a read-only master copy and duplicate it.
- All further processing or **examination should be performed on copies of the evidence.**

3. Documenting the evidence

- Be sure to **document all the methods and tools that are used to collect and extract the evidence.**
- **Detail your notes** so that another examiner could reproduce them.
- Your work must be **reproducible**; if not, a judge may rule it inadmissible.

4. Documenting all changes

- It's important to document the entire recovery process, including all the changes made during the acquisition and examination.
- For example, if the forensic tool used for the data extraction sliced up the disk image to store it, this must be documented.
- All changes to the mobile device, including power cycling and syncing, should be documented in your case notes.

Command line tools (SSH, Telnet)

- A Command-Line Interface (CLI) is a user interface (UI) that is text based.
- Windows has a CLI called Command Prompt and for Mac computers, there's the Terminal.app.
  - Both are pre-installed.
- These are **text-based tools used by investigators to find, copy, and examine data from computers, phones, or storage devices during a digital investigation.**

a) Secure Socket Shell (SSH)

- Secure Shell or Secure Socket Shell (SSH) **is a protocol used to securely connect** to an otherwise insecure computer, or server.
  - It provides a secure channel over an unsecured network by using encryption for both authentication and data transmission.
- SSH (Secure Shell) is a cryptographic network protocol **used for operating network services securely over an unsecured network**.
- **SH (Secure Shell)** is a command-line tool that allows to **securely connect** to another computer (usually over the internet or a local network).
- The best-known application of SSH is for remote login to computer systems by users.
- We can use SSH to **access, investigate, and collect evidence** from remote machines without being physically there.

Some basic SSH commands:

1. **Connecting to a remote server**:
   - **ssh user@hostname**
   - **Eg: ssh username@192.168.1.5**
   - Connects to the remote server ‘hostname’ with the username ‘user’.
2. **Specifying a different port**:
   - **ssh -p port user@hostname**
   - Connects to the remote server ‘hostname’ on a specified port ‘port’.
3. **Copying a file to a remote server using SCP**:
   - **scp /path/to/local/file user@hostname:/path/to/remote/directory**
   - Copies a local file to a directory on the remote server.
4. **Copying a file from a remote server using SCP**:
   - **scp user@hostname:/path/to/remote/file /path/to/local/directory**
   - Copies a file from the remote server to a local directory.
5. **Listing files in a remote directory using SFTP**:
   - **sftp user@hostname**
   - fter connecting, you can use typical file commands like ‘ls’, ‘cd’, ‘get’ and ‘put’.

Password-protected SSH

- When using password-protected SSH, each time you connect to a remote server, you will be **prompted to enter the password** for the remote account. This is the default method when no SSH keys are set up.
  - Basic Command: **ssh username@hostname**
  - Example: **ssh user@example.com**
- After running the command, you will be prompted to enter the password for **user** and **example.com**

Password-less SSH

- Password-less SSH allows you to connect to a remote server without entering a password each time.

More understanding on SSH: https://www.youtube.com/watch?v=v45p_kJV9i4

b) Teletype Network (Telnet)

- A **Teletype Network** (TTY) originally referred to a system of **text-based communication devices** used before modern computers.
  - It allowed people to **send and receive typed messages** over telephone lines using machines like typewriters.
- In modern computing, **TTY** refers to:
  - A **terminal interface** where a user types commands and sees output (like the Command Prompt or Terminal).
  - A **virtual terminal session** on Linux/Unix systems.
- When you open the **Terminal** or **Command Prompt**, you are using a TTY.

Role of TTY in Digital Forensics:

1. Session Tracing

- Forensic analysts can **track user activity** on different TTY sessions.
- For example, if a hacker accessed a system via tty1 and ran commands, the logs may show this.

2. Log Analysis

- TTY usage is often logged in system files like /var/log/auth.log or /var/log/wtmp.
- Tools like last, who, and w show TTY sessions and login history.
- Last: Shows who logged in and from where, including which TTY they used.

3. Live Forensics

- When analyzing a live system, forensic investigators can check **active TTYs** to find:
- Who is logged in
- What session is being used
- Possibly see ongoing commands

4. Malicious Access Detection

- If an attacker gains access via a TTY session, forensic tools may show:
  - TTY ID (e.g., pts/0)
  - Login time
  - Origin of the connection (IP address)
- This helps investigators build a timeline of the attack.

Role of TTY in Digital Forensics:

1. Session Tracing

- Forensic analysts can **track user activity** on different TTY sessions.
- For example, if a hacker accessed a system via tty1 and ran commands, the logs may show this.

2. Log Analysis

- TTY usage is often logged in system files like /var/log/auth.log or /var/log/wtmp.
- Tools like last, who, and w show TTY sessions and login history.
- Last: Shows who logged in and from where, including which TTY they used.

3. Live Forensics

- When analyzing a live system, forensic investigators can check **active TTYs** to find:
- Who is logged in
- What session is being used
- Possibly see ongoing commands

4. Malicious Access Detection

- If an attacker gains access via a TTY session, forensic tools may show:
  - TTY ID (e.g., pts/0)
  - Login time
  - Origin of the connection (IP address)
- This helps investigators build a timeline of the attack.

More Understanding : https://www.youtube.com/watch?v=tZop-zjYkrU

Assignment:

- Differentiate between Telnet and SSH.

Network Monitoring tools

- Network monitoring tools are **essential for maintaining network health, security, and performance.**
- Network monitoring tools are software applications designed to observe, track, and manage the performance and health of a network.
- They help network administrators detect and resolve issues, ensure optimal network performance, and maintain network security.
- Some of the popular Network monitoring tools are: Wireshark, Nagios, PRTG Network monitor, Cacti, Splunk, Icinga, NetFlow Nalyzer, and so on.

Key functions of Network monitoring tools:

1. **Traffic Analysis**: Monitor and analyze data traffic to understand usage patterns and identify bottlenecks.
2. **Device Monitoring**: Track the performance and status of network devices like routers, switches, servers, and firewalls.
3. **Bandwidth Monitoring**: Measure the bandwidth usage to identify excessive consumption by devices or applications.
4. **Alerting and Notifications**: Generate alerts for abnormal activities, outages, or performance issues.
5. **Security Monitoring**: Detect security threats, unauthorized access, and vulnerabilities within the network.
6. **Historical Data Analysis**: Store historical data to identify trends, perform root cause analysis, and plan for future capacity

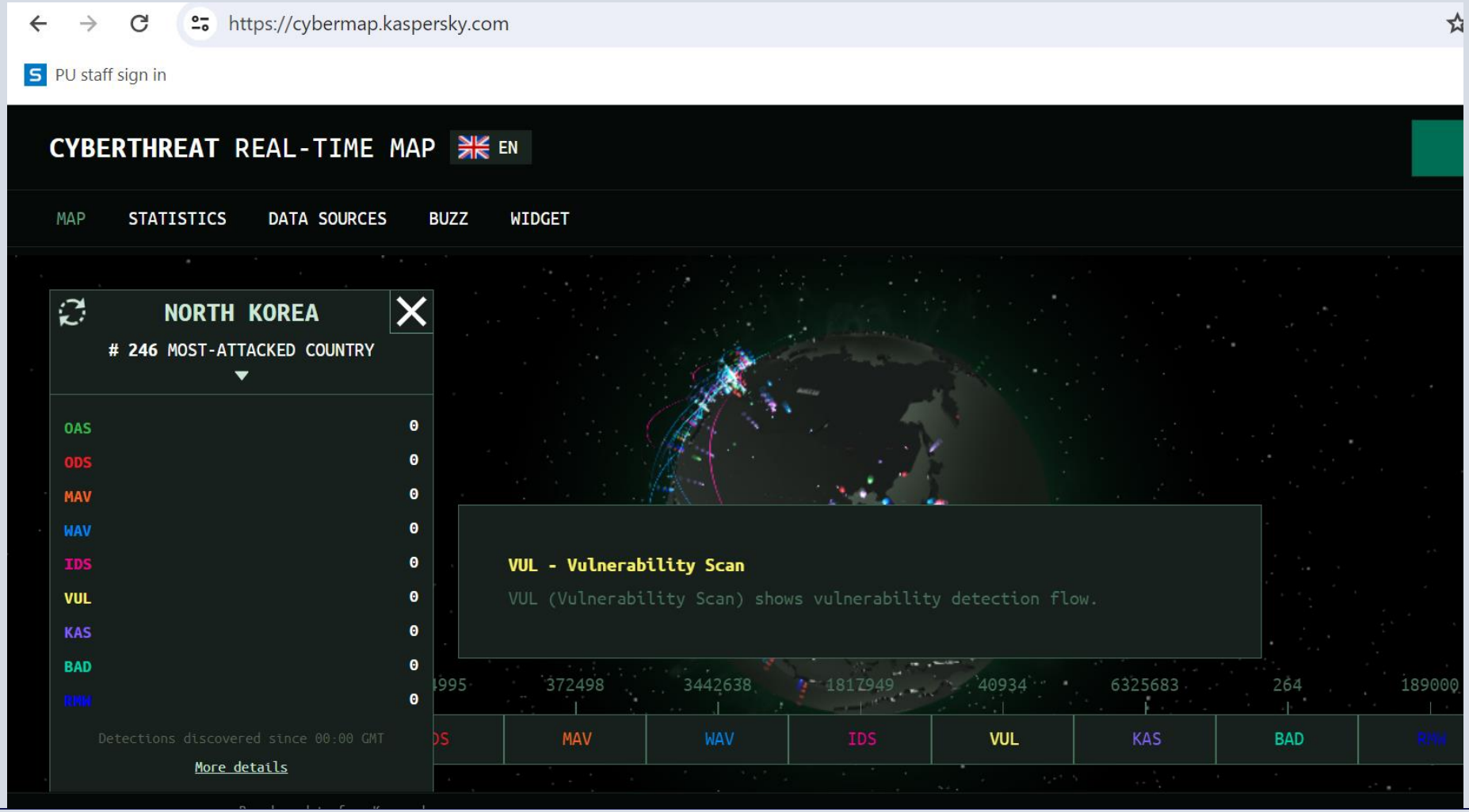
Live Threat Maps

- Live threat maps are **real-time visual representations of cyber threats and attacks occurring across the globe.**
- They provide a dynamic view of ongoing malicious activities, such as hacking attempts, malware infections, and distributed denial-of-service (DDoS) attacks.
- These maps are used by cybersecurity professionals **to monitor and analyze current threats,** helping them to respond quickly and effectively.
- Live threat maps are a valuable tool in the cybersecurity arsenal, providing real-time insights and helping to keep networks and data secure from emerging threats.
- Some popular Live Threat Maps are: Norse Attack Map, Kaspersky Cyberthreat Real-Time Map, FireEye Threat Map, Fortinet Threat Map, Check Point ThreatCloud Map, Digital Attack Map, Trend Micro Threat Connect, etc.

Key features :

1. **Real-Time Data**: Live threat maps update continuously to show the latest cyber threats as they happen.
2. **Geographical Visualization**: They display threats on a global map, often highlighting the origin and target locations of attacks.
3. **Threat Types**: Different types of attacks, such as phishing, malware, ransomware, and DDoS, are often categorized and displayed with distinct icons or colors.
4. **Attack Details**: Some maps provide detailed information about each threat, including the type of attack, IP addresses involved, and the time of occurrence.
5. **Traffic Analysis**: Visualize the volume and patterns of malicious traffic.
6. **Historical Data**: Some threat maps allow users to view past data and analyze trends over time.
7. **Alerts and Notifications**: Many maps can generate alerts for significant or unusual activity.

https://cybermap.kaspersky.com/



Intrusions

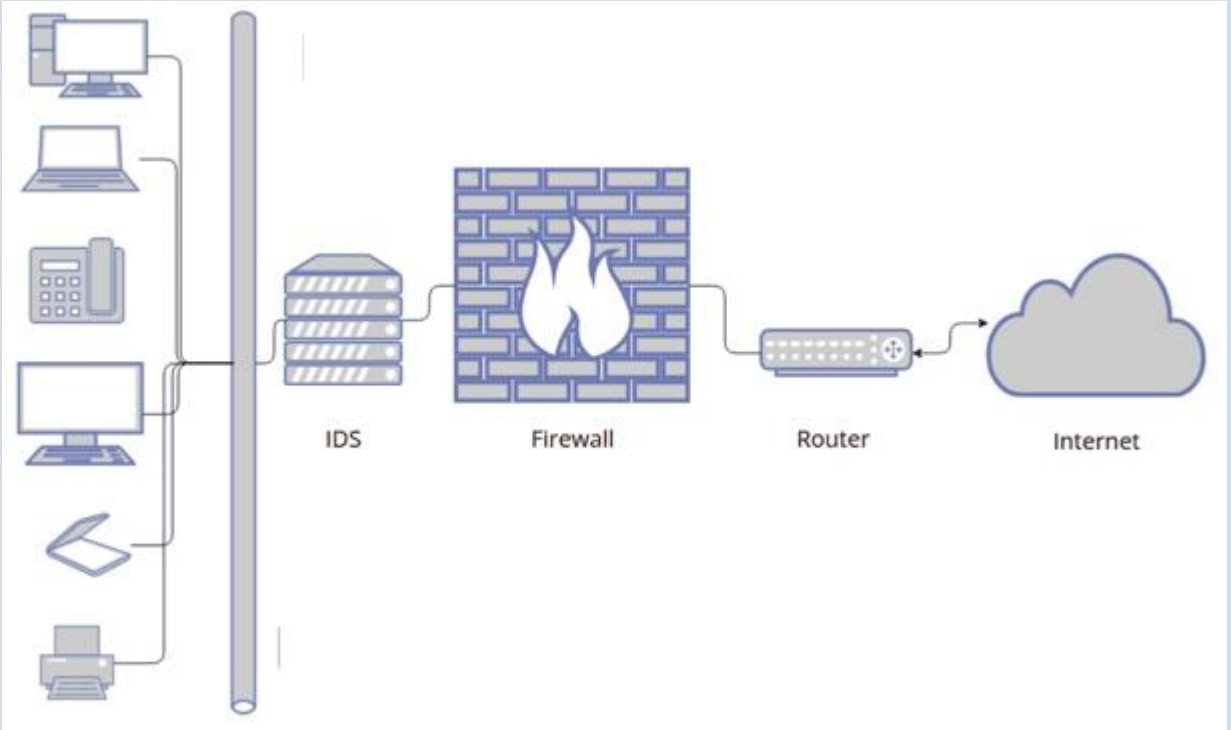
- Intrusion is typically an attacker gaining **unauthorized access to a device**, network, or system.
- Cyber criminals use increasingly sophisticated techniques and tactics to infiltrate organizations without being discovered.
- This includes common techniques like:
  a) **Address spoofing:** The source of an attack is hidden using spoofed, misconfigured, and poorly secured proxy servers, which makes it difficult for organizations to discover attackers.
  b) **Fragmentation:** Fragmented packets enable attackers to bypass organizations' detection systems.
  c) **Pattern evasion:** Hackers adjust their attack architectures to avoid the patterns that IDS solutions use to spot a threat.
  d) **Coordinated attack:** A network scan threat allocates numerous hosts or ports to different attackers, making it difficult for the IDS to work out what is happening.

Intrusion Detection System (IDS)

- An Intrusion Detection System (IDS) is **a security tool that monitors a computer network or systems for malicious activities or policy violations**.
- It helps detect unauthorized access, potential threats, and abnormal activities by analyzing traffic and alerting administrators to take action.
- An IDS is crucial for maintaining network security and protecting sensitive data from cyber-attacks.
- The IDS is also a listen-only device.
- The IDS monitors traffic and reports results to an administrator.
- It cannot automatically take action to prevent a detected exploit from taking over the system.
- Popular Open Source Intrusion Detection Systems are : **OSSEC, SNORT, BRO, SURICATA, SECURITY ONION, SAGAN, AIDE**

How IDS works?

- An IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity.
- It analyzes the data flowing through the network to look for patterns and signs of abnormal behavior.
- The IDS compares the network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion.
- If the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator.
- The system administrator can then investigate the alert and take action to prevent any damage or further intrusion.



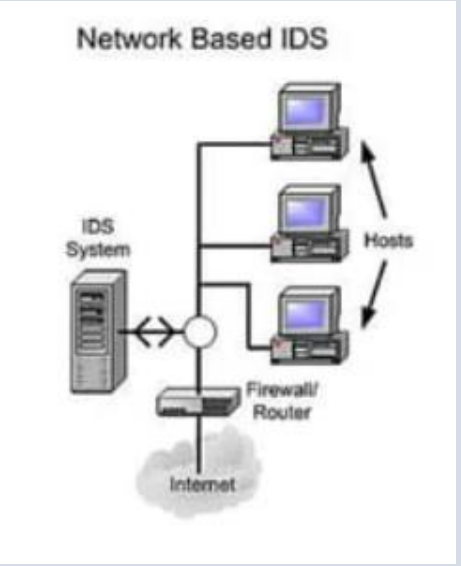
Benefits of IDS:

- Understanding risk
- Shaping security strategy
- Regulatory compliance
- Faster response time

Types of IDS:

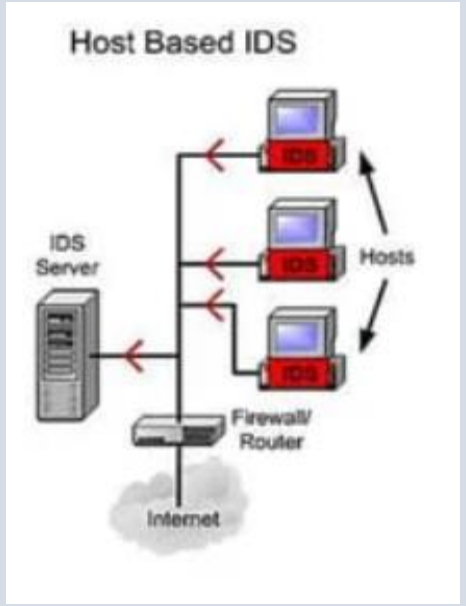
1. Network-based intrusion detection system (NIDS)

- A network IDS monitors a complete protected network.
- It is deployed across the infrastructure at strategic points, such as the most vulnerable subnets.
- The NIDS monitors all traffic flowing to and from devices on the network, making determinations based on packet contents and metadata.



2. Host-based intrusion detection system (HIDS)

- A host-based IDS monitors the computer infrastructure on which it is installed.
- It is deployed on a specific endpoint to protect it against internal and external threats.
- The IDS accomplishes this by analyzing traffic, logging malicious activity and notifying designated authorities.



3. Protocol-based (PIDS)

- A protocol-based intrusion detection system is usually installed on a web server.
- It monitors and analyzes the protocol between a user/device and the server.
- A PIDS normally sits at the front end of a server and monitors the behavior and state of the protocol.

4. Application protocol-based (APIDS)

- An APIDS is a system or agent that usually sits inside the server party.
- It tracks and interprets correspondence on application-specific protocols.
- For example, this would monitor the SQL protocol to the middleware while transacting with the web server.

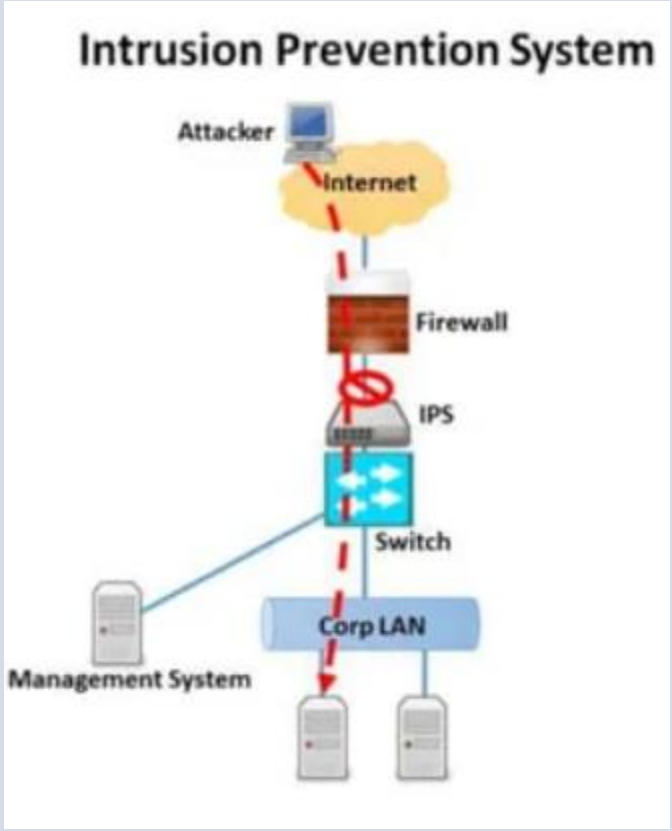
5. Hybrid intrusion detection system

- A hybrid intrusion detection system combines two or more intrusion detection approaches.
- Using this system, system or host agent data combined with network information for a comprehensive view of the system.
- The hybrid intrusion detection system is more powerful compared to other systems.
- One example of Hybrid IDS is Prelude.

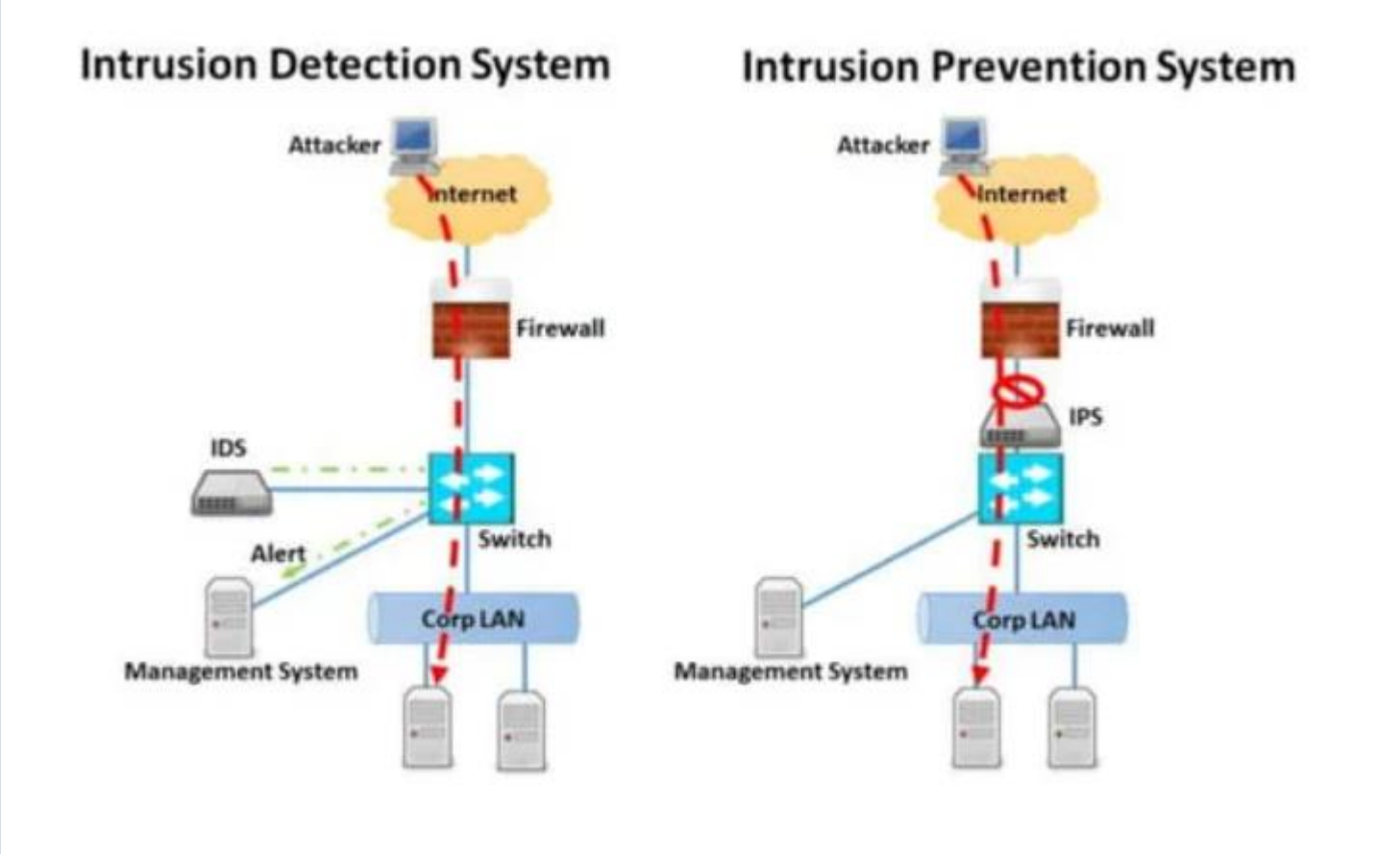
NIDS	HIDS
1. Broad in scope (watches all network activities)	1. Narrow in scope (watches only specific host activities)
2. Easier setup, less expensive to implement	2. More complex setup, more expensive to implement
3. Better for detecting attacks from the outside	3. Better for detecting attacks from the inside
4. Detection is based on what can be recorded on the entire network	4. Detection is based on what any single host can record.
5. Examines packet headers	5. Does not see packet headers
6. Detects network attacks as payload is analyzed	6. Detects local attacks before they hit the network
7. Detects unsuccessful attack attempts	7. Verifies success or failure of attacks
8. Near real-time response	8. Usually only responds after a suspicious log entry has been made
9. OS-independent	9. OS-specific

Intrusion Prevention System (IPS)

- An **intrusion prevention system (IPS)** goes beyond IDS by blocking or preventing security risks.
- An IPS can both monitor for malicious events and take action to prevent an attack from taking place.
- IPS solutions help businesses take a more proactive cybersecurity approach and mitigate threats as soon as possible.
- They constantly monitor networks in search of anomalies and malicious activity, then immediately record any threats and prevent the attack from doing damage to the company's data, networks, resources, and users.
- An IPS will also send insight about the threat to system administrators, who can then perform actions to close holes in their defenses and reconfigure their firewalls to prevent future attacks.



IDS vs IPS


Intrusion Detection System
Attacker
Internet
Firewall
IDS
Switch
Alert
Management System
Corp LAN
Intrusion Prevention System
Attacker
Internet
Firewall
IPS
Switch
Management System
Corp LAN

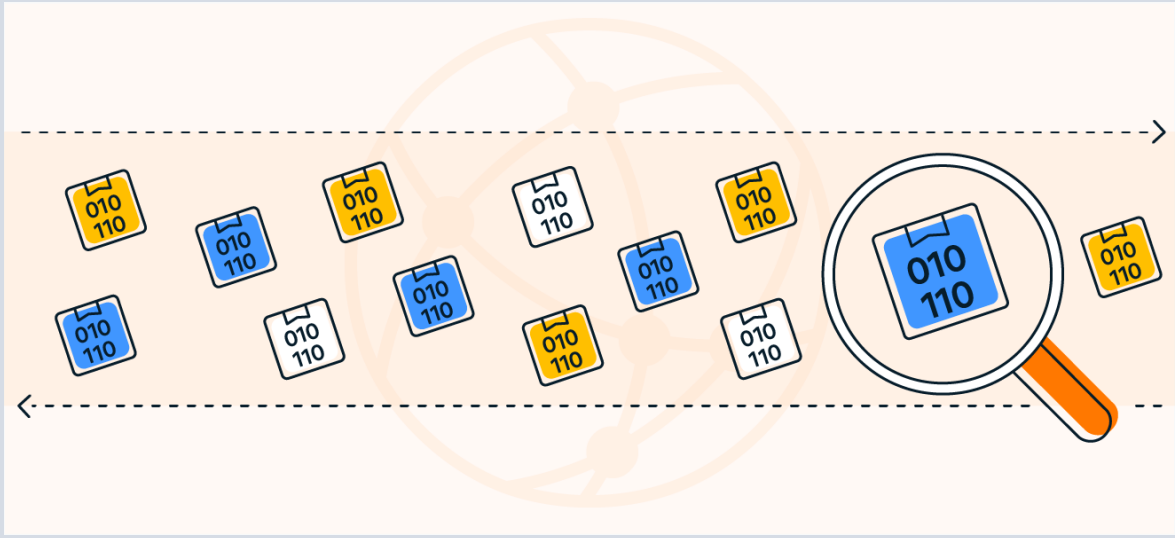
IDS vs IPS

IDS	IPS
Installed on network segments (NIDS) and on hosts (HIDS)	Installed on network segments (NIPS) and on hosts (HIPS)
Sits on network passively	Sits inline (not passive)
Cannot parse encrypted traffic	Better at protecting applications
Central management control	Central management control
Better at detecting hacking attacks	Ideal for blocking web defacement
Alerting product (reactive)	Blocking product (proactive)

Source: https://www.slideshare.net/slideshow/ids-001-ids-vs-ips/249873804

Packet Sniffing

- When any data has to be transmitted over the computer network, it is broken down into smaller units at the sender's node called ***data packets*** and reassembled at receiver's node in original format.
- It is the *smallest unit* of communication over a computer network. It is also called a block, a segment, a datagram or a cell.



- The **act of capturing data packet across the computer network** is called **packet sniffing**.
  - It is similar to as wire tapping to a telephone network.
  - It is mostly used by *crackers and hackers* to collect information illegally about network.
- Packet sniffing is a **method of detecting and assessing packet data sent over a network**.
  - It can be used by administrators for network monitoring and security.
  - However, packet sniffing tools can also be used by hackers to spy or steal confidential data.
- The packet sniffing process is achieved by analyzing data packets sent through TCP/IP protocol that connects devices to wired or wireless networks.
  - These data packets can include different types of traffic sent across a network, such as login details and passwords, as well as technical data like IP addresses.

Assignment:

1. Mention the methods used for Packet Sniffing attacks.
2. Why and how ISPs, Advertising agencies and Government agencies use packet sniffing?
3. What are the advantages and disadvantages of Packet sniffing?

End of Chapter