Interactive
Experience

Comprehensive Beginners Guide to Learn The Basics and Effective Methods of Cybersecurity

CYBER SECURITY

Fundamentals

You'll Learn:

Key terms and concept

Secure your device and personal data

Step-by-step guide- hands on (AR apps)

Mohd Hafizil Izuan

Ayu Hasnidah

Subject Matter Expert (SME)

First Edition 2026

CYBER SECURITY *Fundamentals*

https://kkpayabesar.mypolycc.edu.my
elearningkkpb@gmail.com

COURSE *Creator*

MOHD HAFIZIL IZUAN BIN MOHMAD NAZIR

Programme of Creative Multimedia Avertising (certificate), Paya Besar Community College, Pahang.
Possessing skills in Video editing, Digital Technology and Cybersecurity

Lecturer DH12

AYU HASNIDAH BINTI ZAINUDIN

Programme of Information Technology(certificate), Paya Besar Community College, Pahang.
Possessing skills in Computer and Robotic Programming, Digital Technology and Cybersecurity

Lecturer DH12

First Edition 2026

Authors:
Mohd Hafizil Izuan bin Mohmad Nazir
Ayu Hasnidah binti Zainudin

eISBN: 978 - 629 - 94331 - 4 - 9

Published by:
Kolej Komuniti Paya Besar
Kementerian Pendidikan Tinggi
Batu 19, Jalan Maran
26300 Gambang
Pahang

Email: elearningkkpb@gmail.com
Website: https://kkpayabesar.mypolycc.edu.my

COPYRIGHT

SYNOPSIS

This eBook introduces readers to the current cybersecurity threats and hazards. This course provides readers with a foundational understanding of information security theory, basic principles and techniques for designing secure systems.

Readers will explore principles and best practices in environmentally sustainable and secure computing and learn to utilize appropriate tools and technologies for managing information system environments.

CONTENTS

Click on the page number to go directly to the desired page.

TOPIC 1

INTRODUCTION TO CYBERSECURITY

TOPIC 1 A. Cybersecurity Fundamentals

Types of Cybersecurity Studies:

a) Information Security
b) Application Security
c) Network Security
d) Operational Security

A) INFORMATION SECURITY

- Protects information from unauthorized access, disclosure, alteration, and destruction.
- Focuses on data confidentiality, integrity, and availability.
- Example:
  A bank uses encryption so that even if hackers steal customer data, they cannot read it without the decryption key.

B) APPLICATION SECURITY

- Protects software and apps from threats and vulnerabilities.
- Includes secure coding, testing, and patch management.
- Example:
  Gmail uses password strength checks and Two Factor Authentication (2FA) to keep attackers out.

TOPIC 1 *A. Cybersecurity Fundamentals*

Types of Cybersecurity Studies:

a) Information Security
b) Application Security
✔c) Network Security
✔d) Operational Security

C) NETWORK SECURITY

- Ensures safe use of computer networks.
- Involves firewalls, intrusion detection systems, and secure protocols.
- Example:
  When you connect to Wi-Fi at school, a firewall prevents outsiders from accessing the internal school network.

D) OPERATIONAL SECURITY

- Deals with processes and decisions for protecting critical systems and assets.
- Focuses on user permissions, data handling, and incident response.
- Example:
  A company sets rules so only HR staff can access employee salary files.

TOPIC 1 *A. Cybersecurity Fundamentals*

The CIA Triad

The three fundamental goals of cybersecurity

Confidentiality

Only authorized people can access information

Example: WhatsApp's end-to-end encryption

Integrity

Data remains unaltered without authorization

Example: Database change logs and restoration

Availability

Information accessible when needed

Example: Amazon's backup servers

YouTube
The CIA Triad Concept (Confidentiality, Integrity, Availability)

1) White Hat

- Ethical hackers who test systems to improve security
- Good guys hired by companies

2) Black Hat

- Criminal hackers exploiting systems for personal gain
- Steal credit cards and data

3) Grey Hat

- In-between; may break rules but not always malicious
- Report bugs publicly instead of privately

4) Script Kiddies

- Inexperienced hackers using existing tools without deep knowledge

YouTube
Types of Hackers (White Hat vs Black Hat)

TOPIC 1 *B. Security and Hazards*

1) Malicious Code

- Viruses and worms
- Trojans
- Ransomware attacks

Malicious Code
is a computer program code that is written with the intent to harm, destroy or annoy.

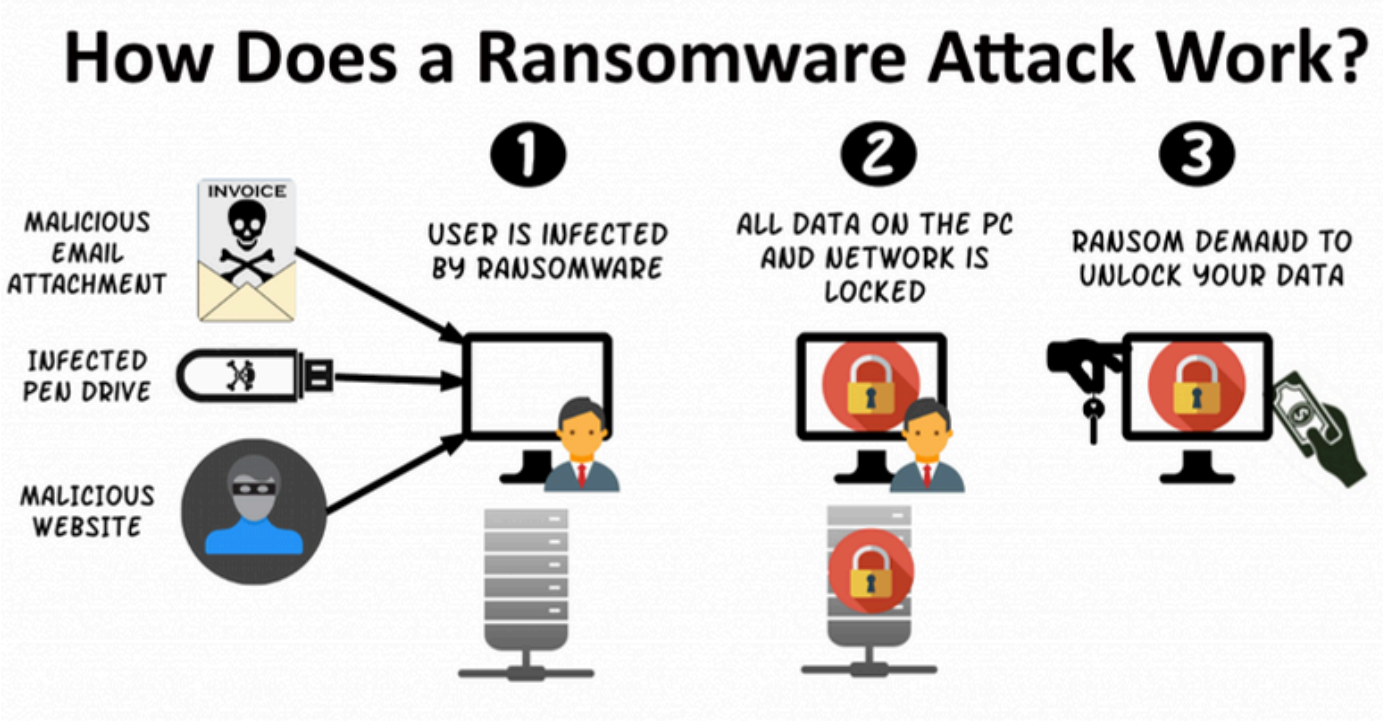
✓**Viruses and worms**
- attach to program and propagate

✓**Trojans**
- unexpected / additional functionality

✓**Ransomware attacks**
- is a type of malware that encrypts the victim's personal data until a ransom is paid

YouTube
What is Ransomware?

TOPIC 1 *B. Security and Hazards*



YouTube
Real Case: WannaCry Attack

TOPIC 1 B. Security and Hazards

2) Hacking Attacks

- Unauthorized access
- Password cracking
- System exploitation

Hacking Attacks refers to the act of compromising digital devices and networks through unauthorized access.

✓ **Unauthorized access**

- Unauthorized access occurs when someone gains entry into a system, network, or database without permission

✓ **Password cracking**

- Password cracking is the process of recovering or guessing passwords to gain unauthorized access

✓ **System exploitation**

- System exploitation refers to using software or hardware vulnerabilities to gain control of a system

TOPIC 1 *B. Security and Hazards*

3) Physical Threats

- Natural disasters
- Device theft
- Data center damage

Physical Threats
are risks that come from the real-world environment—like theft, damage, or unauthorized physical access to devices and infrastructure.

✓ **Natural disasters**
- Earthquakes, floods, hurricanes, fires, or pandemics

✓ **Device theft**
- Stolen laptops, smartphones, USB drives, or even physical servers

✓ **Data center damage**
- Fire, flooding, vandalism, or accidental damage to racks and servers

TOPIC 1 B. Security and Hazards

Threat Sources

Risk Assesment Process

1) Assets identification
   - Pinpointing all valuable resources that need protection

2) Risk identification
   - Determining potential events that could negatively affect assets

3) Threat identification
   - Recognizing sources of harm that could exploit weaknesses

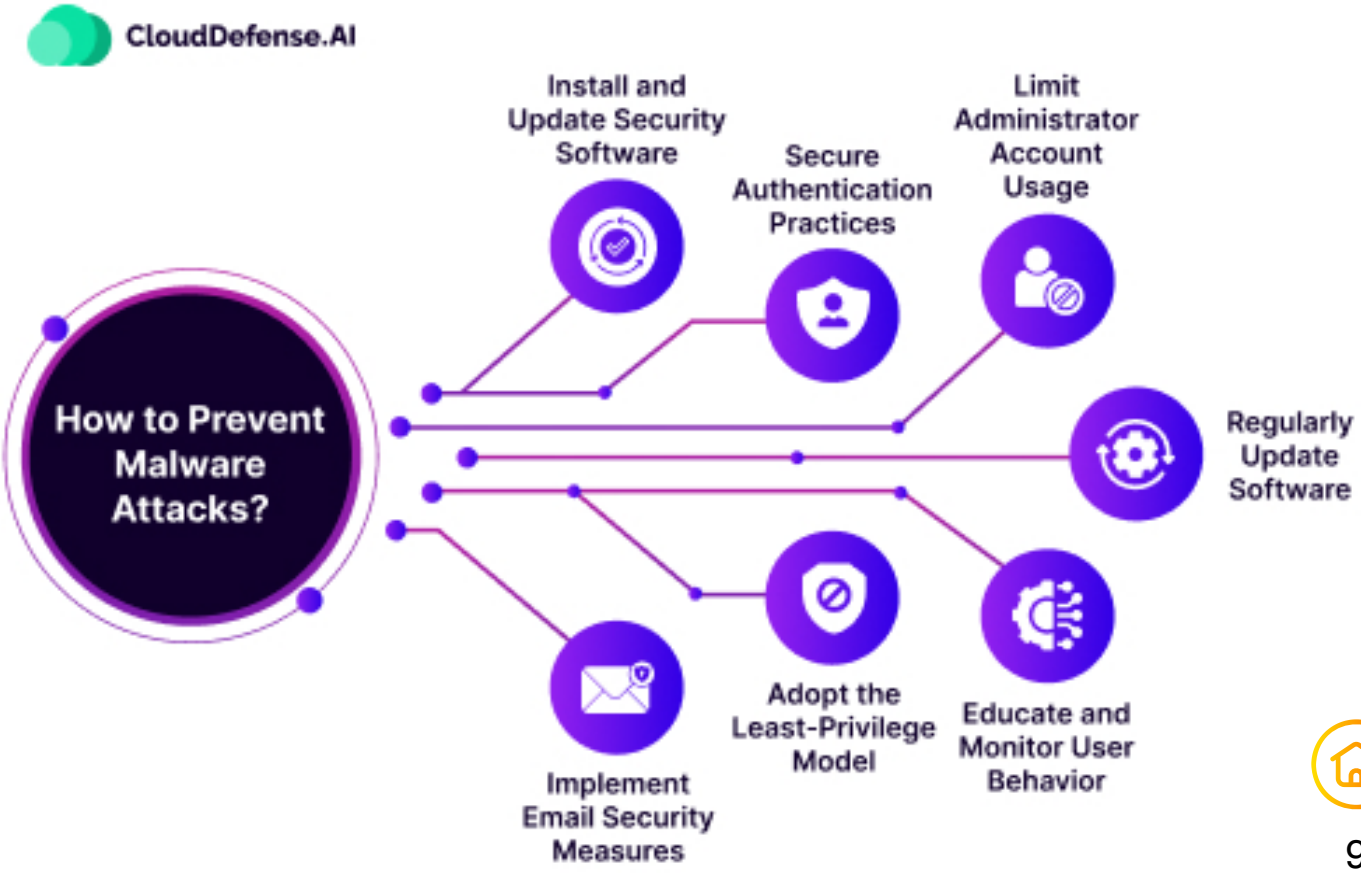
4) Vulnerability assesment
   - Evaluating weaknesses in systems, processes, or people that threats could exploit

TOPIC 1

C. Malicious Code

- Malware, or "malicious software," is an umbrella term that describes any malicious program or code that is harmful to systems.

- Hostile, intrusive, and intentionally nasty, malware seeks to invade, damage, or disable computers, computer systems, networks, tablets, and mobile devices, often by taking partial control over a device's operations. Like the human flu, it interferes with normal functioning.



TOPIC 1

C. Malicious Code

TOPIC 2

SECURITY ATTACKS AND THREATS

TOPIC 2 *A. Security attacks*

Classification of Security Attack

Passive Attacks

Attackers only monitor and gather information without altering data.
Example: Packet sniffing to capture usernames and passwords from network traffic.

Active Attacks

Attackers modify, disrupt, or damage information and systems.
Example: A hacker changes values in a database or injects malware into a system.

Insider Attacks

Attacks carried out employees, contractors, or anyone with authorized access.
Example: An employee steals customer data from the company's database.

Distribution Attacks

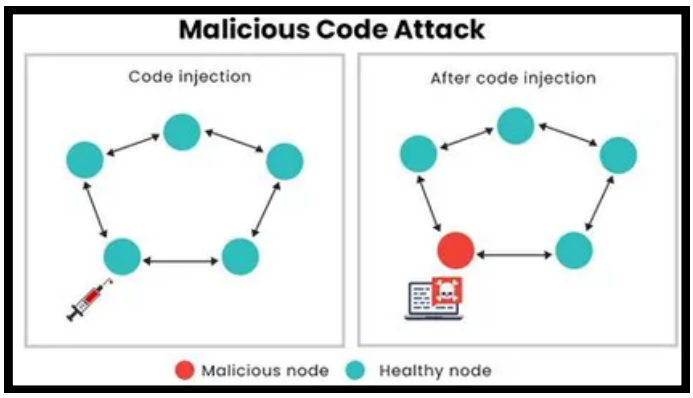
Attacks on software or hardware during its distribution process.
Example: A malicious actor installs spyware into a USB drive before it is sold.

TOPIC 2

B. Cybersecurity attacks

- Collecting information about a system before attacking
- Ex: using wireshark for sniffing and spoofing to trick users

- Overwhelms a system, making services unavailable
- Ex: A website becomes inaccessible when flooded with fake request, such as a DDoS attack on gaming servers



- Involves malware like worms, viruses, and trojan horses
- Ex: A trojan disguised as a game that secretly install spyware

- Gaining unauthorized access to systems
- Ex: A hacker cracking weak passwords to log into company accounts

TOPIC 2 C. Social Engineering

Social Engineering Attacks

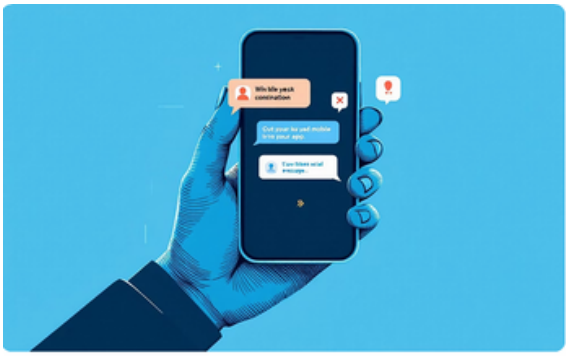
Social engineering attacks exploit human psychology to trick individuals into divulging confidential information or performing actions that compromise security. These attacks can be categorized by the method used to manipulate victims.

Impersonation-Based

Attackers deceive individuals by pretending to be someone trustworthy to gain sensitive information. This includes **vishing** (phone scams), **eavesdropping**, **shoulder surfing**, **dumpster diving**, and **reverse social engineering**.

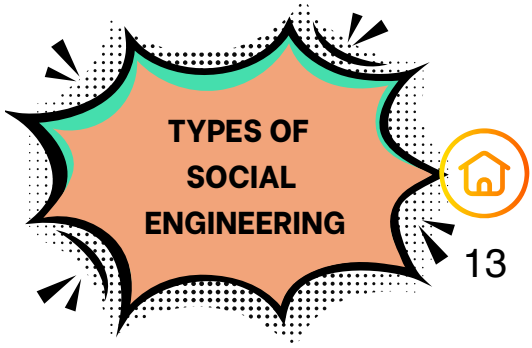
Computer-Based

These attacks leverage digital platforms, primarily email and fake websites, to trick users. **Phishing** emails often request login credentials, mimicking legitimate services like banks or payment processors (e.g., a fake PayPal email).



Mobile-Based

Targeting smartphones and tablets, these attacks utilize SMS (**smishing**), malicious apps, or deceptive updates. For example, a fraudulent text message from a "bank" prompts users to click a suspicious link.



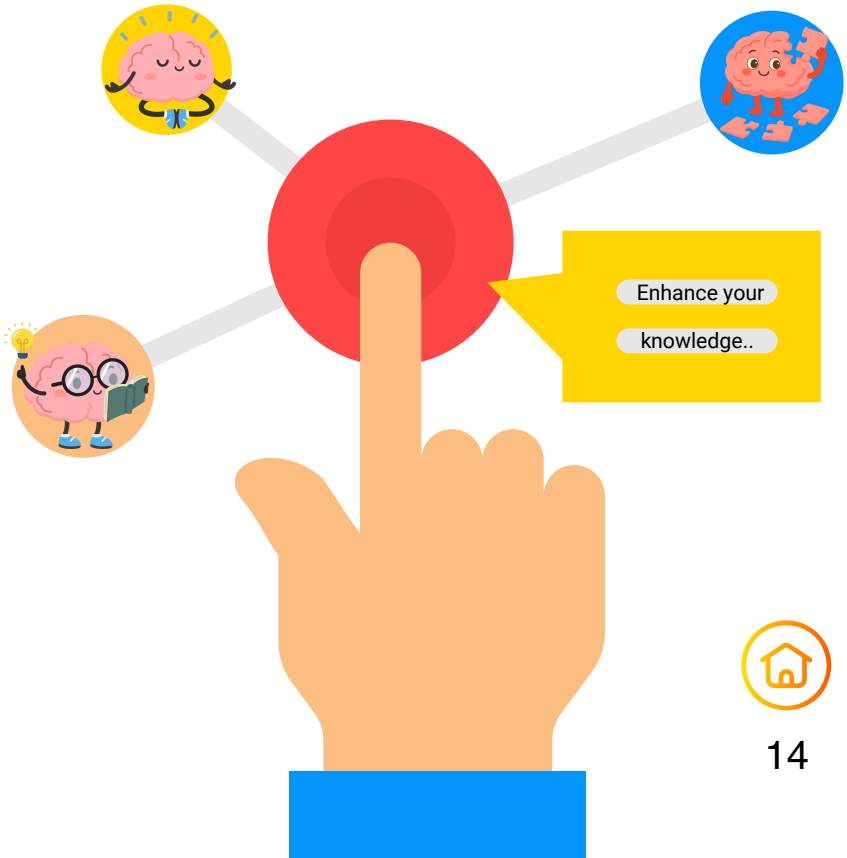
TOPIC 2

YouTube
Social Engineering Demo (Vishing - Voice Attack)

YouTube
Real Case: How Uber Was Hacked (MFA Fatigue)

YouTube
What is a DDoS Attack?

YouTube
Password Cracking Techniques (Brute Force vs Dictionary)



TOPIC 2

D. Cybersecurity Threats, Protection & Prevention

Common Cybersecurity Threats

1) Malware
   - Malicious software like viruses, worms, ransomware, and Trojans are designed to disrupt systems or steal data

2) Phishing attacks
   - Attackers impersonate trustworthy entities (e.g. banks) via fake emails or messages to trick victims into revealing sensitive information like login credentials.

3) Denial of Service (DoS) attacks
   - These attacks overwhelm a system, server, or network resource with traffic, making it unavailable to legitimate users.

4) Insider threats
   - Security risks originating from within an organization, often from current or former employees, contractors, or business partners.

5) Zero-Day Exploits
   - These exploits target a software vulnerability unknown to the vendor or public, giving developers 'zero days' to create a patch.

TOPIC 2

D. Cybersecurity Threats, Protection & Prevention

Cybersecurity *Protection* Measures

1) Firewalls
   - Block unauthorized access between networks. A company firewall prevents hackers from entering the office network, acting as a crucial barrier.

2) Encryption
   - Secures data by making it unreadable without a key. Online banking uses HTTPS encryption to protect sensitive transactions and personal information.

3) Antivirus and Anti malware Software
   - Detects and removes malicious programs from systems. For instance, Windows Defender can block a Trojan download before it can infect your computer.

4) Multi-Factor Authentication (MFA)
   - Requires two or more verification steps for access. A common example is Gmail sending a code to your phone for verification when you login.

TOPIC 2 D. Cybersecurity Threats, Protection & Prevention

Cybersecurity *Prevention* Strategies

1) User Awareness & Training
   - Educating employees and users about common cyber threats, such as phishing and malware, helps them identify and avoid potential attacks. For instance, universities train students not to click suspicious links or open attachments from unknown senders.

2) Regular Software Updates
   - Applying timely patches and updates to all software, operating systems, and applications closes known security vulnerabilities. A prime example is Microsoft's "Patch Tuesday," which regularly releases updates to fix security holes before they can be exploited.

3) Strong Password Policies
   - Implementing and enforcing policies that require complex, unique passwords and regular password changes significantly enhances account security. Systems should reject weak passwords like '123456' and enforce the use of strong combinations of characters, numbers, and symbols.

4) Access Control Policies
   - Restricting access to sensitive data and systems based on user roles and responsibilities minimizes the risk of unauthorized information access. For example, only finance department staff should have access to critical payroll systems and financial records.

5) Data Backup & Disaster Recovery
   - Regularly backing up critical data and having a robust disaster recovery plan ensures business continuity even after a successful cyberattack or system failure. Cloud-based backups allow companies to quickly restore systems and data, minimizing downtime and data loss.

TOPIC 3

SECURITY MEASURES IN CYBER THREATS

TOPIC 3

A. Classification of Infrastructure security

Classification of Infrastructure Security

1) Devices
   - Protecting servers, routers, switches, and endpoints.
   - Example: Installing endpoint protection on company laptops.

2) Media
   - Protecting storage devices like hard drives, USBs, and cloud storage.
   - Example: Encrypting a USB drive with BitLocker.

3) Security Topologies
   - Designing network structures to limit exposure.
   - Example: Using a star topology where all traffic goes through a secured router.

4) Intrusion Detection
   - Monitoring systems for suspicious activity.
   - Example: IDS alerts if multiple failed login attempts are detected.

5) Security Baseline
   - Minimum required security settings for systems.
   - Example: All devices must have updated antivirus, firewalls, and strong passwords.

6) Application hardening
   - Strengthening software against attacks.
   - Example: Disabling unused features and applying security patches.

TOPIC 3 B. Common Security Infrastructure security

Common Security Infrastructure Security

1) Firewalls
   - Block or allow traffic based on rules.
   - Example: Blocking all incoming traffic except web server ports.

2) Virtual Private Networks (VPN)
   - Encrypt data and hide user IP addresses.
   - Example: Employees use VPN to securely connect to office systems from home.

3) Intrusion Detection System (IDS)
   - Detect suspicious traffic and report it.
   - Example: Detecting unusual login attempts from foreign countries.

4) Honeypots
   - Fake systems used to attract hackers for study.
   - Example: A decoy database set up to log hacker activity.

5) Demilitarized Zone (DMZ)
   - Isolated network area that exposes external services but protects internal systems.
   - Example: Hosting a public website in the DMZ while keeping company databases safe inside.

6) Network Monitoring /Diagnostic
   - Continuous observation of traffic to detect issues.
   - Example: Monitoring tools detecting a sudden spike in traffic.

YouTube
How a Firewall Works?

TOPIC 3

C. Protection Physical Equipment

Protection Physical **Equipment**

1) Access Control
   - Restricting entry using locks, badges, biometrics.
   - Example: Using fingerprint scanners for data centre entry.

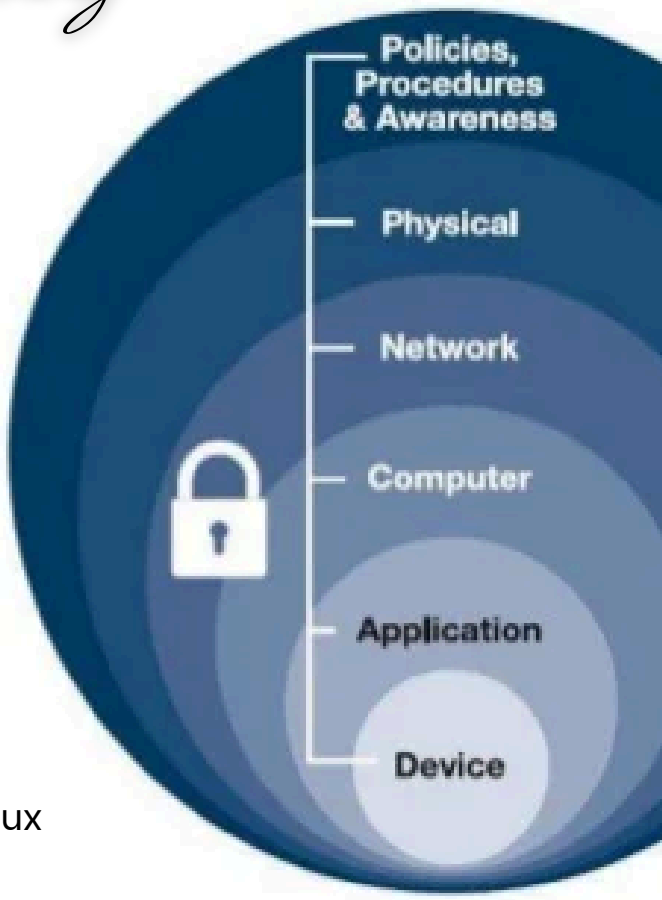
2) Environment Controls
   - Protecting equipment from environmental damage.
   - Example: Fire suppression systems, wireless shielding, climate control in server rooms.

YouTube
Physical Security (Hacking Lift & Doors)

TOPIC 3

D. Application Security Hardware Hardening

Application Security **Hardening**



1) Service packs
   - Collections of updates and improvements.
   - Example: Windows Service Packs fixing bugs and vulnerabilities.

2) Security patches
   - Fixing specific vulnerabilities in software.
   - Example: Installing monthly security patches from Microsoft or Linux distributions.

3) Hotfixes
   - Emergency fixes for critical issues.
   - Example: Applying a hotfix after discovering a severe zero-day vulnerability.

4) Cold Fixes
   - Fixes that require restarting the system.
   - Example: Restarting a server after applying a kernel patch.

5) Bug Fixes
   - Correcting errors in software.
   - Example: Updating an app to remove a coding flaw that allows SQL injection.

YouTube
Real Case: Stuxnet Virus (USB Physical Attack)

TOPIC 4

CYBERSECURITY GOVERNANCE FRAMEWORK

TOPIC 4 *A. Security Policies*

A comprehensive framework for establishing robust cybersecurity governance in educational and enterprise environments. Essential for IT managers and security practitioners building effective defence systems.

1. Information Security Policy Governance and Management

Security policies define rules and procedures for protecting data.
Example: A university IT department establishes a policy requiring all devices to use antivirus software

2. Information Classification

Classifying data based on sensitivity: Public, Internal, Confidential, Secret
Example: Student exam results = confidential; university advertisements = public.

1

Public

Information freely available to the general public

- Marketing materials
- Published research
- Public announcements

2

Internal

Information for organisational use only

- Internal policies
- Staff directories

3

Confidential

Sensitive information requiring protection

- Student exam results
- Employee records
- Financial data

4

Secret

Highly sensitive information with severe impact

- Research IP
- Security Vulnerabilities
- Strategic plans

TOPIC 4 *A. Security Policies*

3. Security Policy Document

A written policy outlining organizational security measures.
Example: A company publishes a Cybersecurity Handbook that employes must follow

4. Usernames & Password Management

Enforce robust credential standards;

- Minimum 12 characters
- Mixed case, numbers symbols
- Regular password rotation
- No password reuse

5. File & Folder Permission

Implement principle of least privilege;

- Role-based access control
- Regular permission audits
- Automated de-provisioning
- Activity monitoring

TOPIC 4 *A. Security Policies*

6. Data Protection Methods

Data Encryption

Transforms data into unreadable format, protecting sensitive communications and stored information. Essential for email security and database protection.

Biometric Authentication

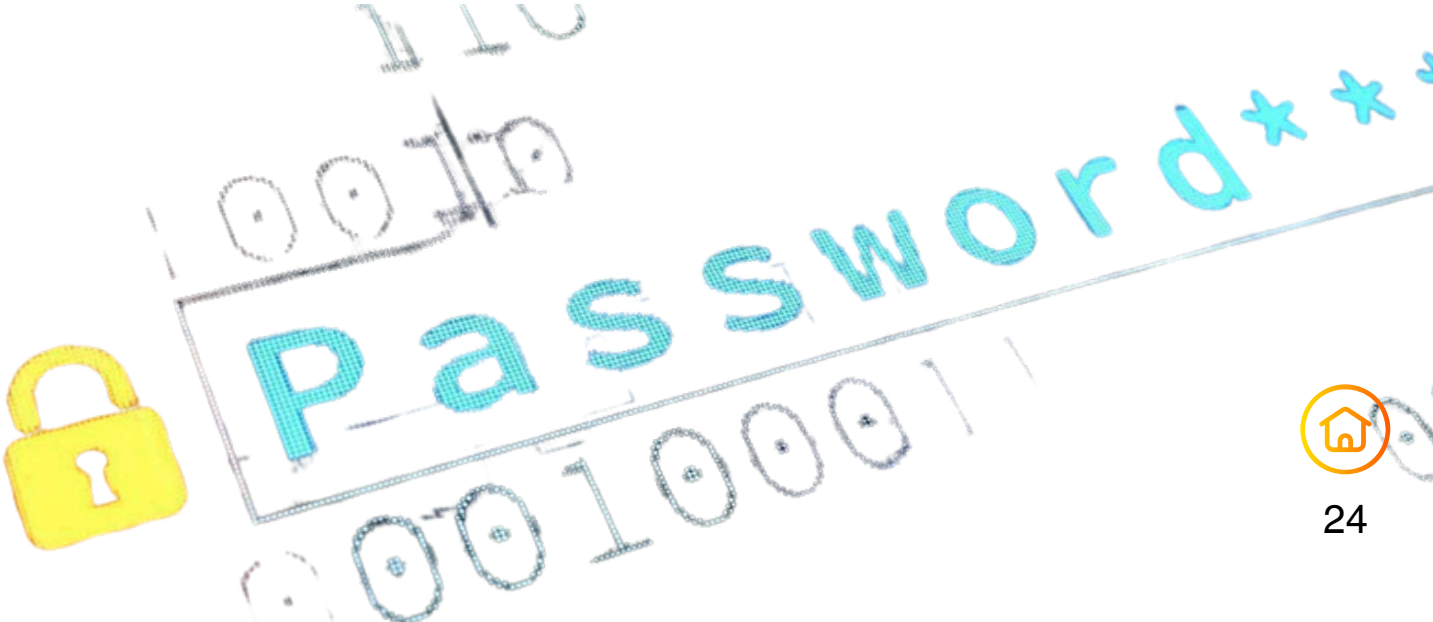
Leverages unique physical characteristics like fingerprints or facial recognition for secure, convenient user verification.

Security Tokens

Hardware and software devices generating time-based one-time passwords. Widely adopted by financial institutions for secure authentication.

Multi-Factor Authentication

Combines multiple verification methods for enhanced security. Standard practice for enterprise Gmail and critical system access.



TOPIC 4 *B. Security Procedures & Policies*

Security Procedures and Policies

Acceptable Use Policy
Clearly defines permitted and prohibited activities with IT resources, including software installation restrictions and internet usage guidelines.

Physical Access Control
Implement smart card systems, biometric scanners, and visitor management protocols to secure sensitive areas like server rooms.

TOPIC 4

C. Various Tools in Cybersecurity & Information Security

Cybersecurity Tools

Network Mapper (Nmap)
Comprehensive network discovery and security auditing tool, identifies active devices, open ports, and potential vulnerabilities across network infrastructure.

Wireshark
Industry-standard protocol analyzer for network troubleshooting and security analysis. Captures and examines network packets to detect anomalous traffic patterns.

Autopsy
Open-source digital forensic platform used by law enforcement and security professionals for investigating cyber incidents and recovering digital evidence.

TOPIC 4
D. Security Awareness & Training

Security Awareness Programme

Initial Training

Comprehensive onboarding covering basic security principles, common threats, and organisational policies.

Regular Updates

Quarterly briefings on emerging threats, new policies, and security best policies to maintain awareness levels.

Simulation Testing

Phishing simulations and social engineering tests to assess and improve staff response to real-world threats.

Continuous Improvement

Analysis of test results and incident data to refine training programmes and address knowledge gaps.

THE 7 MOST COMMON PASSWORD ATTACK & MITIGATIONS

BRUTE FORCE ATTACK

Description: Automated trial-and-error that attempts every possible password combination until the correct one is found.
Mitigation: Implement Account Lockout Policies (e.g., after 5 failed tries) and use Multi-Factor Authentication (MFA).

DICTIONARY ATTACK

Description: Uses a pre-compiled list of common words, phrases, and previously leaked passwords instead of trying all combinations.
Mitigation: Enforce complex, long passwords (12+ characters) and prevent users from setting common dictionary words.

CREDENTIAL STUFFING

Description: Uses leaked username/ password pairs from one data breach to gain unauthorized access to a user's other accounts due to password reuse.
Mitigation: Users must use a unique password for every account, ideally managed by a password manager.

PASSWORD SPRAYING

Description: Tries a small list of very common passwords against a large list of usernames to avoid triggering account lockouts on any single account.
Mitigation: Implement MFA across all users. Prohibit the use of common passwords (block lists).

THE 7 MOST COMMON PASSWORD ATTACK & MITIGATIONS

PHISHING ATTACK

Description:Social engineering where an attacker tricks the user into entering credentials on a fake website disguised as a legitimate entity (e.g., bank, IT).
Mitigation: User education on spotting phishing links and suspicious emails always verify the URL/ sender.

RAINBOW TABLE ATTACK

Description:Attack stored password hashes by using pre-computed tables hash values to quickly reverse-engineer the original password.
Mitigation: Use strong hashing algorithms (like Argon2 or bcrypt) combined with salting (adding random data before hashing).

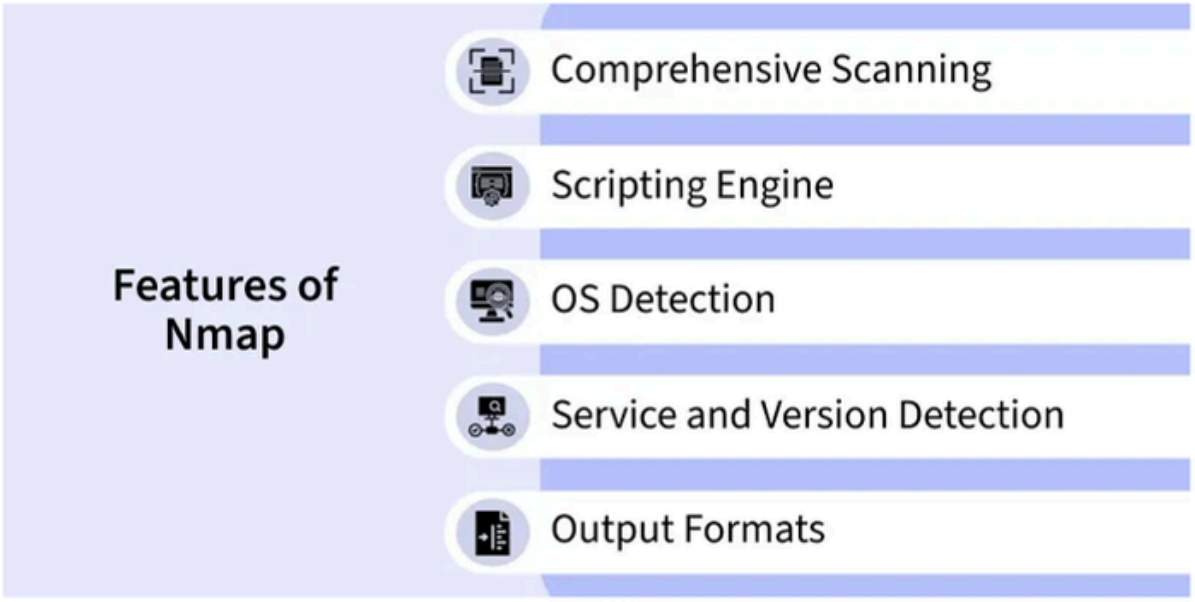
KEYLOGGER ATTACK

Description:Malicious software or a physical device that secretly records every keystoke a user makes, capturing login credentials as they are typed.
Mitigation: Use up-to-date Antivirus/ Anti-Malware software. Employ device authentication and secure startup processes.

NETWORK MAPPER (NMAP)

Features of Nmap

Nmap offers a wide range of features to its users, including:



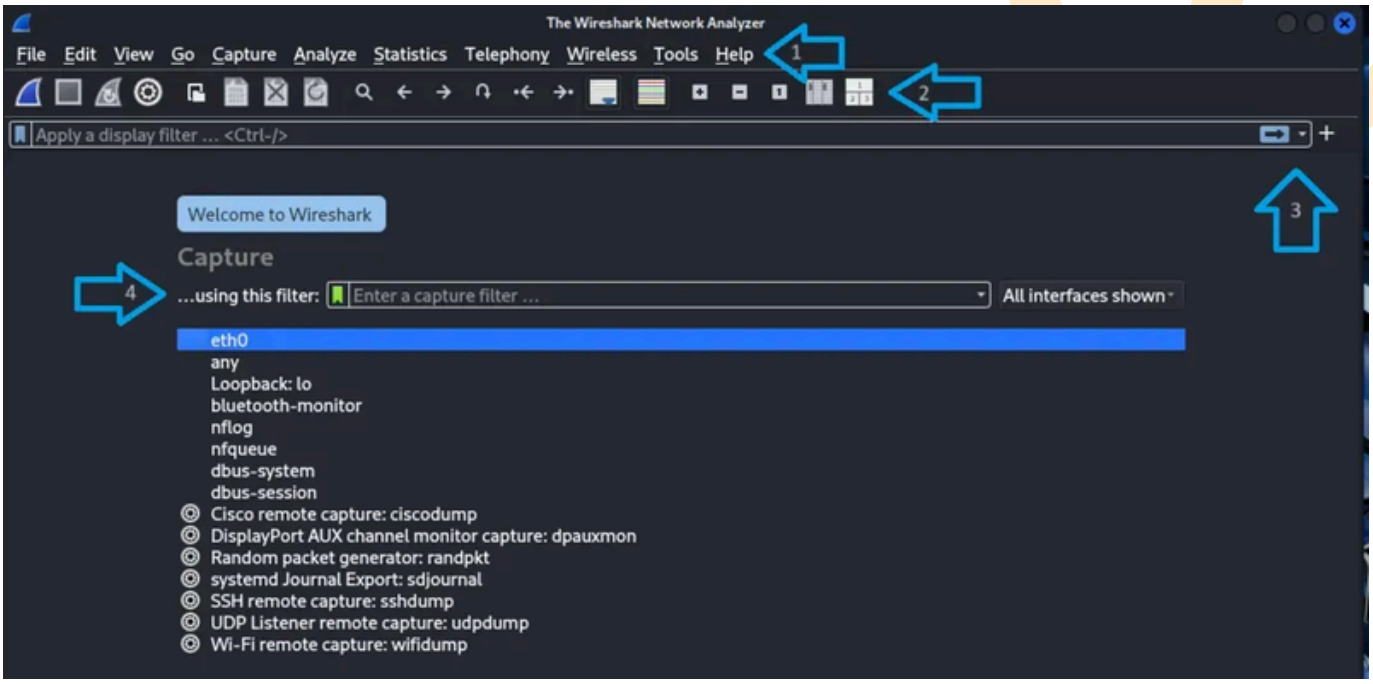
Importance of Nmap

There are a few points that reflect the work of Nmap and provide many reasons to have Nmap on your network

NETWORK MAPPER (NMAP)

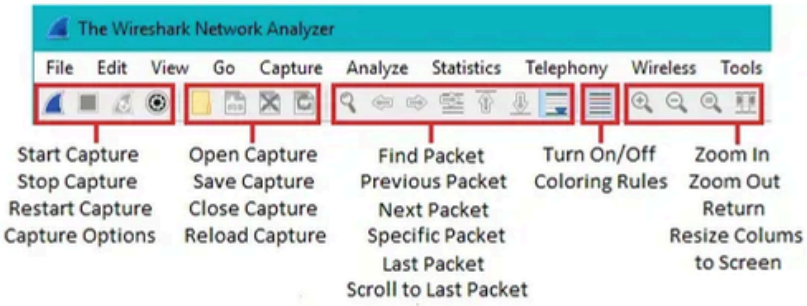
WIRESHARK

Interface Overview (Core GUI Components)



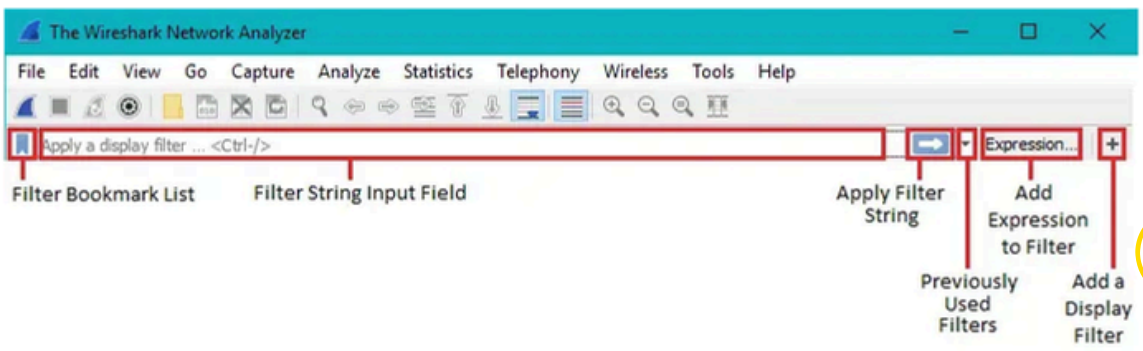
Main Toolbar

Quick button for start/ stop capture, open/save files, restart capture



Filter Toolbar

Capture filter (before capture)
Display filter (after capture) with real-time validation



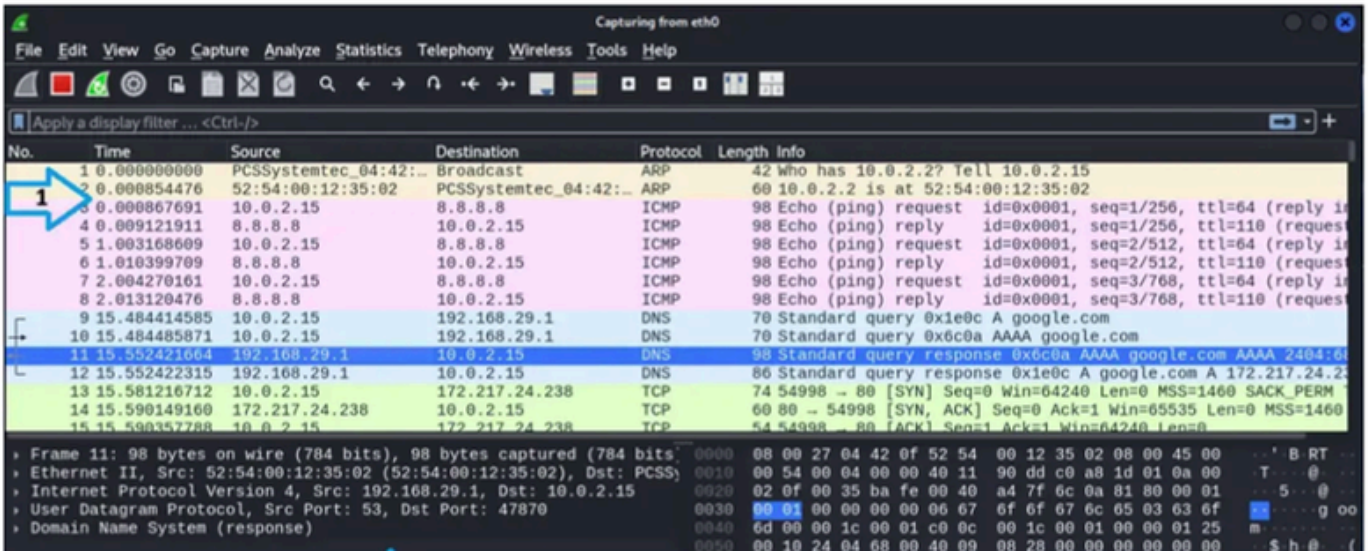
WIRESHARK

Interface List (Start Screen)

Shows available network adapters and their current traffic
Select interface + optional capture filter before starting

Main Pane Layout(post-capture)

You can also enable the Packet Diagram Pane to get a visual, textbook style representation of packet headers and payload



WIRESHARK

Autopsy® is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer.

Extensible

Autopsy was designed to be an end-to-end platform with modules that come with it out of the box and others that are available from third-parties. Some of the modules provide:

- Timeline Analysis - Advanced graphical event viewing interface (video tutorial included).
- Hash Filtering - Flag known bad files and ignore known good.
- Keyword Search - Indexed keyword search to find files that mention relevant terms.
- Web Artifacts - Extract history, bookmarks, and cookies from Firefox, Chrome, and IE.
- Data Carving - Recover deleted files from unallocated space using PhotoRec
- Multimedia - Extract EXIF from pictures and watch videos.
- Malware Scanning

Fast

Everyone wants results yesterday. Autopsy runs background tasks in parallel using multiple cores and provides results to you as soon as they are found. It may take hours to fully search the drive, but you will know in minutes if your keywords were found in the user's home folder.

Cost Effective

Autopsy is free. As budgets are decreasing, cost effective digital forensics solutions are essential. Autopsy offers the same core features as other digital forensics tools and offers other essential features, such as web artifact analysis and registry analysis, that other commercial tools do not provide.

AUTOPSY

REFERENCES

Johnson Jr, Charles H . (2022). Cybersecurity Essentials: The Beginner's Guide. Ojula Technology Innovations. (ISBN 978-5-595-90056-0)

Steinberg, Joseph. (2020). Cybersecurity Essentials: The Beginner's Guide. United States: John Wiley & Sons Inc. (ISBN 978- 1119560326)

Dalziel, Henry. (2022). Introduction to Cybersecurity. Springer. (ISBN 978-3030543321)

Cybersecurity: The beginner's Guide: A comprehensive guide to getting started in cybersecurity. (2019). Packt Publishing. (ISBN 978-1789806939)

Brian Walker. (2019). Cyber Security: Comprehensive Beginners Guide to Learn the Basics and Effective Methods of Cyber Security. (ISBN 978-1075257674)

Ajay Singh. (2023). Introduction to Cybersecurity: Concepts, Principles, Technologies and Practices. Universities Press. (ISBN 978-9393330314)

CYBER SECURITY FUNDAMENTALS

eISBN 978-629-94331-4-9

KOLEJ KOMUNITI PAYA BESAR

(online)