

# Cyber Security

## Lecture 1.1 Overview of the Course

# Lecture Agenda



- **Course Information and Protocol**
- **Cyber Security: A Bigger Picture**
- **Categories of Cyber Security**
- **History of Cyber Attacks**
- **Prerequisites of the Course**
- **A discussion on Course Modules**

# Course Info & Protocols



# About the Instructor



## Dr. Muhammad Arif Butt

Asst. Prof. at Department of Data Science  
University of Punjab, Lahore  
[arif@pucit.edu.pk](mailto:arif@pucit.edu.pk)  
<https://www.linkedin.com/in/dr-arif-butt/>  
<https://arif.phd>  
<https://arifbutt.me>

## Education:

- Graduation from Pakistan Military Academy Kakul
- MPhil CS from University of Punjab, Lahore
- PhD CS from University of Punjab, Lahore

## Experience:

- Served in field/staff/instructional posts in Pakistan Army
- Assistant Professor, Department of Data Science

## Research Interests:

- Embedded and real time operating systems
- Vulnerability research and exploit development
- Cyber Security
- AI/LLM Security





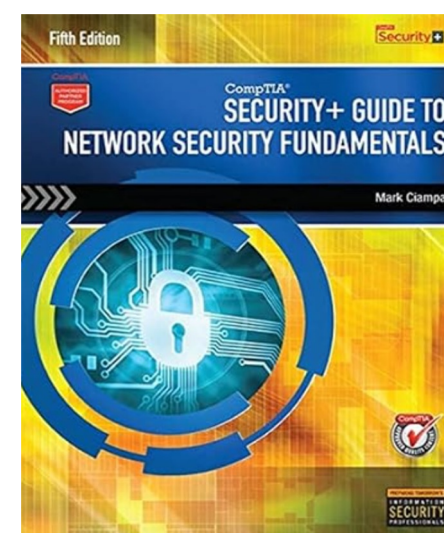
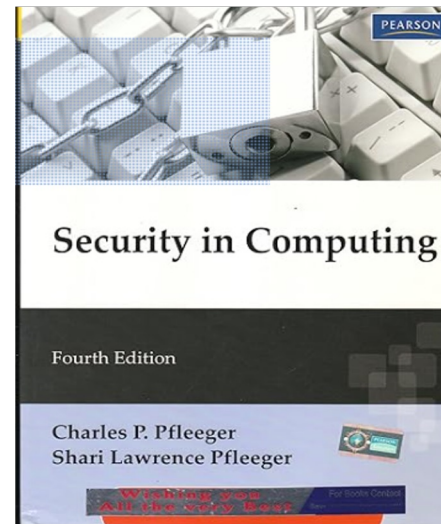
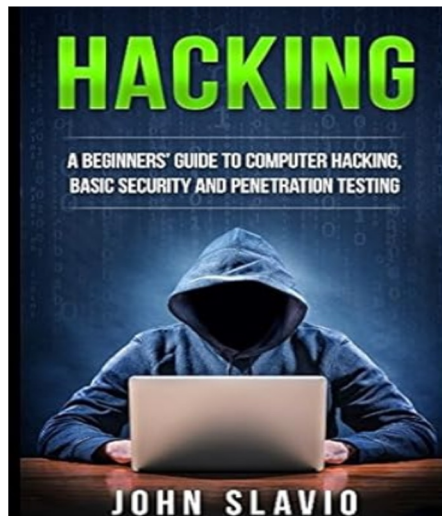
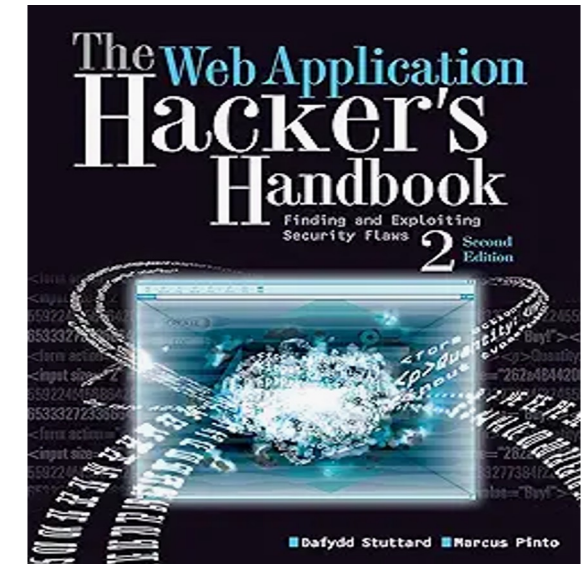
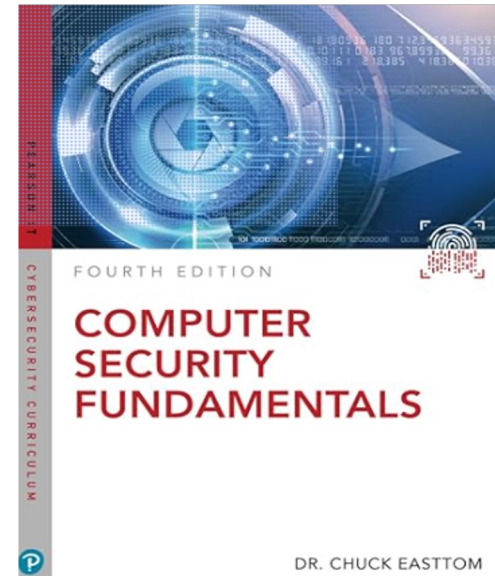
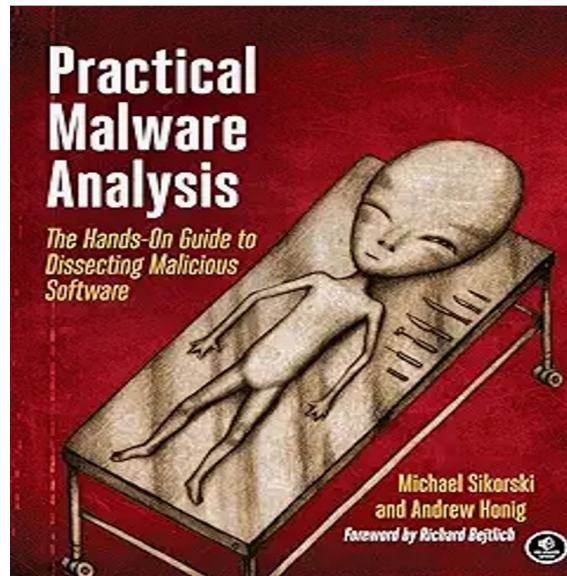
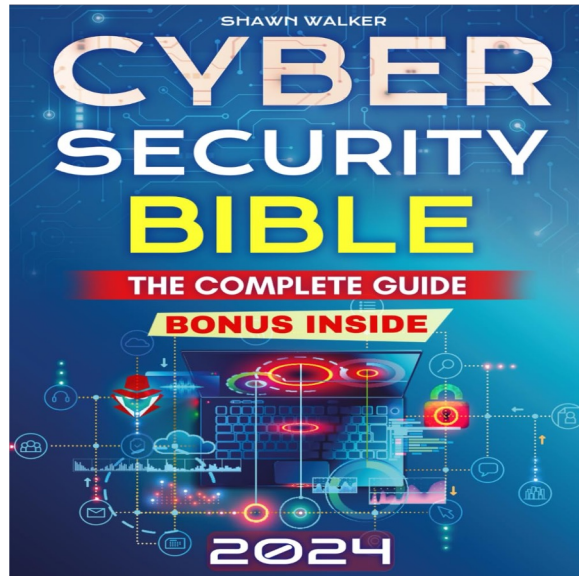
# Course Information



- Lectures Slides/Handouts Available at: <https://arifbutt.me>
- Video Lectures Available at: <https://youtube.com/learnwitharif>
- Codes Hosted at: <https://github.com/arifpucit>
- Grades Website: <https://online.pucit.edu.pk>
- Prerequisites:
  - OS and Internetworking with Linux
  - Basic programming skills in Python, C, and Assembly
- Office: Building-C, FCIT (NC)
- Students Counseling hours:
  - Mon: 0900 hrs – 1000 hrs
  - Tues: 1130 hrs – 1230 hrs
- 24 hour turnaround for email: [arif@pucit.edu.pk](mailto:arif@pucit.edu.pk)



# Text and Reference Books



Instructor(s): Muhammad Rauf Butt, Muhammad Arif Butt, PhD





# Who cares to get an A



- **Final-Term Exam:** 40
- **Mid-Term Exam:** 35
- **Sessional Activities:** 25
  - **Assignments: 30%**
  - **Quizzes: 40%**
  - **Class Activities: 30%**





# Lecture Format



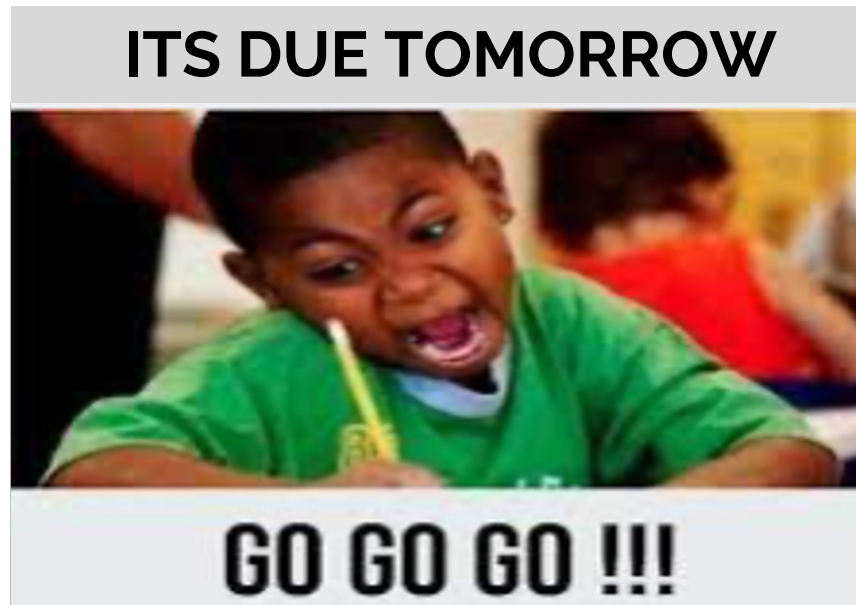
Instructor(s): Muhammad Rauf Butt, Muhammad Arif Butt, PhD



# Late submission guidelines protocol



- Late Assignment submissions will not be accepted!
- There will be no retake on exams and quizzes!



Start working on your tasks early and submit well before time.





# Cheating Policy



- Academic integrity
- Copying an Assignment with or without permission. Both the cheater and the student who aided the cheater will be held responsible for the cheating
- The instructor may take actions such as:
  - require repetition of the subject work,
  - assign '**zero**' or may be '**negative**' marks for the subject work,
  - for serious offenses, assign an **F** grade for the course



# Cyber Security

## The Big Picture

# What is Cyber Security?



- **Cybersecurity** is the practice of protecting systems, networks, devices and data from from cyber threats such as malware, ransomware, phishing, data breaches and so on to safeguard both individual and organizational digital assets.
- It encompasses a wide range of domains, including information security, network security, application security, and incident response.
- It involves the application of technologies, processes, and practices to ensure the confidentiality, integrity, and availability of information





# CIA Triad



**CIA Triad** is the foundational model in IS, representing three core principles that ensure the protection of information



**Availability** ensures that information and resources are accessible to authorized users when needed

**Confidentiality** ensures that sensitive information is accessible only to authorized users.

**Integrity** ensures the accuracy, consistency and trustworthiness of information by protecting it from unauthorized modification, deletion or corruption

## Opposite of CIA is DAD

- **Disclosure** means someone not authorized is getting access to the system.
  - **Alteration** means your data has been altered.
  - **Destruction** means your data or system have been destroyed.
- 100\$ Question:** Finding the right mix
- Ensuring too much **C**, **A** will suffer.
  - Ensuring too much **I**, **A** will suffer.
  - Ensuring too much **A**, both **C** & **I** will suffer

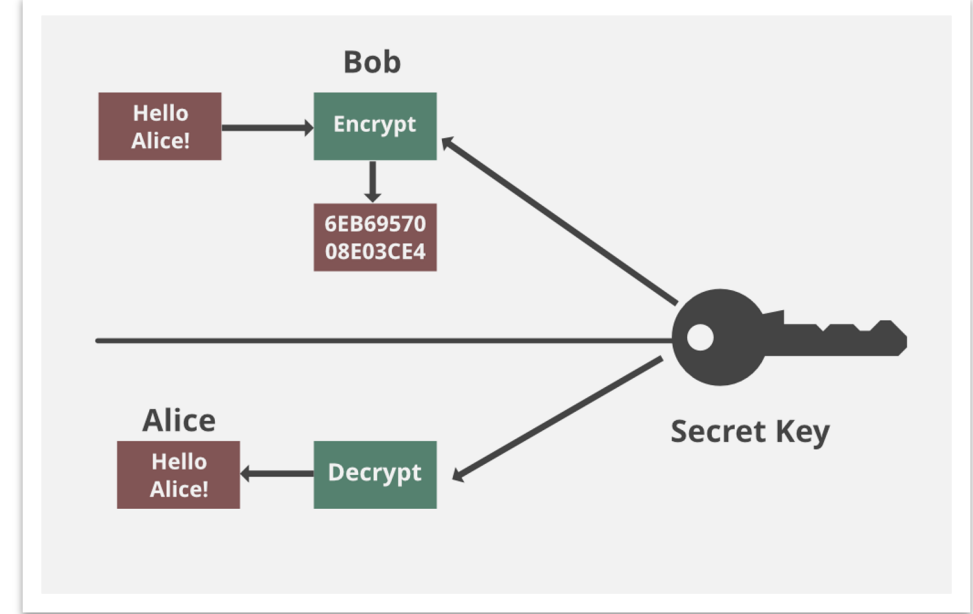
# CIA Triad: Confidentiality



**Confidentiality** ensures that sensitive information is accessible only to authorized users.

## Measures to achieve Confidentiality:

- **Encryption:** (3DES, Blowfish, AES, RSA, DSS, PGP)
- **Secure Transport Protocols:** (SSL, TLS, IPSec)
- **Access Control:** (DAC, MAC, RBAC)
- **Authentication Mechanisms:** (MFA, Biometrics)
- **NW Security Controls:** (Fire Walls, VPNs, IDS/IPS)
- **Least Privilege Principle:**
- **Physical Security:**
- **End-user Training:**



## Threats:

- Social engineering/Phishing.
- Unauthorized NW access & Port scanning.
- Eavesdropping and MitM attacks.
- Password dump stealing and attack on your encryption (cryptoanalysis).
- Authorized users may abuse their access to retrieve sensitive data.

# CIA Triad: Integrity

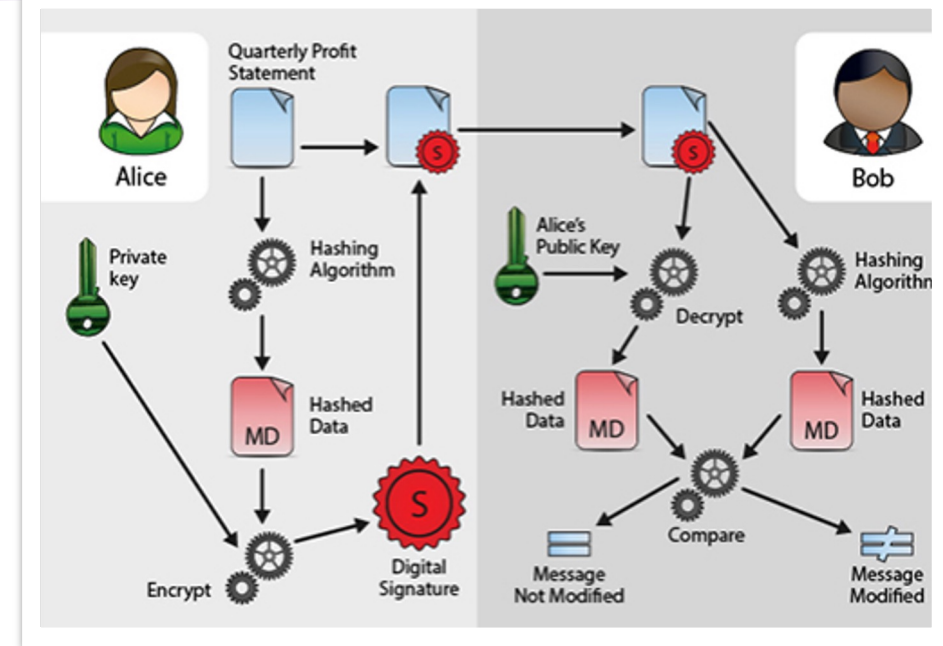


**Integrity:** ensures the accuracy, consistency and trustworthiness of information by protecting it from unauthorized modification, deletion or corruption

## Measures to achieve Integrity:

- **Hashing**, generating a fixed size hash value for data , so that any alteration is easily detectable. (MD5, SHA-256, SHA-512)
- **Checksums**, using checksums to detect errors in data communication or storage. (CRC-32, Adler32)
- **Digital Signature**, is used to verify the authenticity and integrity of a message or document. (RSA, PGP)
- **Version Control**, is used to track changes to document or code, allowing roll back if unauthorized changes are detected. (Git, SVN)
- **Active Logging**, maintaining logs that track data changes, system access and transactions (Splunk, Elastic Stack)

Instructor(s): Muhammad Rauf Butt, Muhammad Arif Butt, PhD



## Threats:

- MitM for tempering
- Data corruption by malware
- Malicious code injection
- Ransomware
- Deleting/altering DB records by SQLi
- DNS Spoofing / Cache Poisoning
- Replay attacks

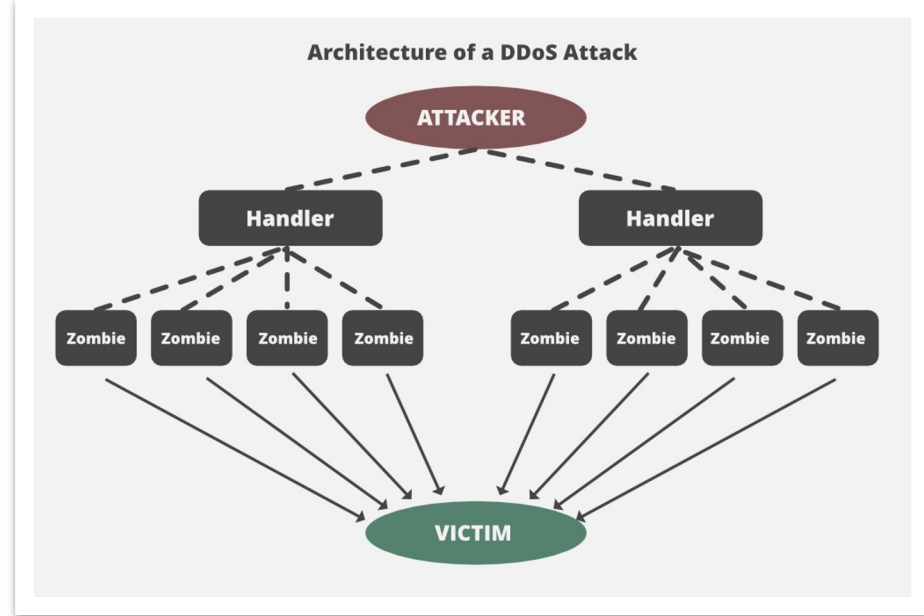
# CIA Triad: Availability



**Availability:** Achieving Availability ensures that information and resources are accessible to authorized users when needed.

## Measures to achieve Availability:

- **Redundancy and Failover**, Implementing redundant systems and automatic failover mechanisms (RAID, Load balancers, Data Center Failover)
- **DDoS Protection**, using security measures to ensure continuous availability of services. (Cloudflare, Akamai)
- **Backup and Recovery**, Regularly backing up data and maintaining recovery procedures to restore systems in case of a disaster. (Veeam, Acronis, AWS Backup)
- **High Availability Architecture**, Using HA designs in systems avoiding single points of failure. (Clustering, Virtualization, Container Orchestration (Kubernetes, Docker).
- **Patch Management**, Keeping systems and applications updated to prevent downtime caused by security vulnerabilities or bugs.



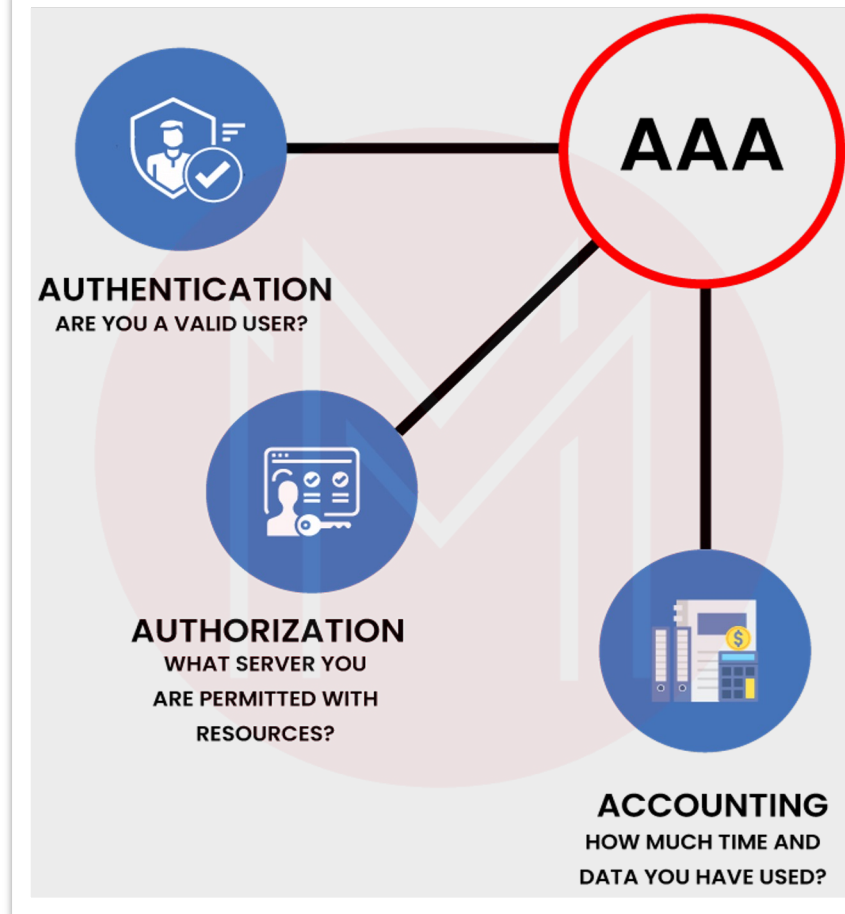
## Threats:

- DDoS
- Ransomware (for availability).
- H/W or S/W Failure.
- Natural disasters.
- Sabotage / Insider attacks.
- Resource exhaustion attacks.
- Logic bombs.

# AAA Architecture



- **Authentication** is the process of verifying the identity of a user or system trying to access a resource.
  - Something you know (password, passphrase, PIN)
  - Something you have (NIC, ATM, Passport)
  - Something you are (Biometrics)
  - Somewhere you are (Geographic location, IP, MAC address)
  - Something you do (signatures, pattern unlock)
- **Authorization** determines what an authenticated user or system is allowed to do, specifying access levels or permissions based on the user role or identity. (DAC, MAC, RBAC)
- **Accountability**, also known as auditing, involves tracking and recording user activities and resource usage. This information is used for monitoring, analysis, and compliance purposes.



# Cyber Security

## Major Categories



# Information Security



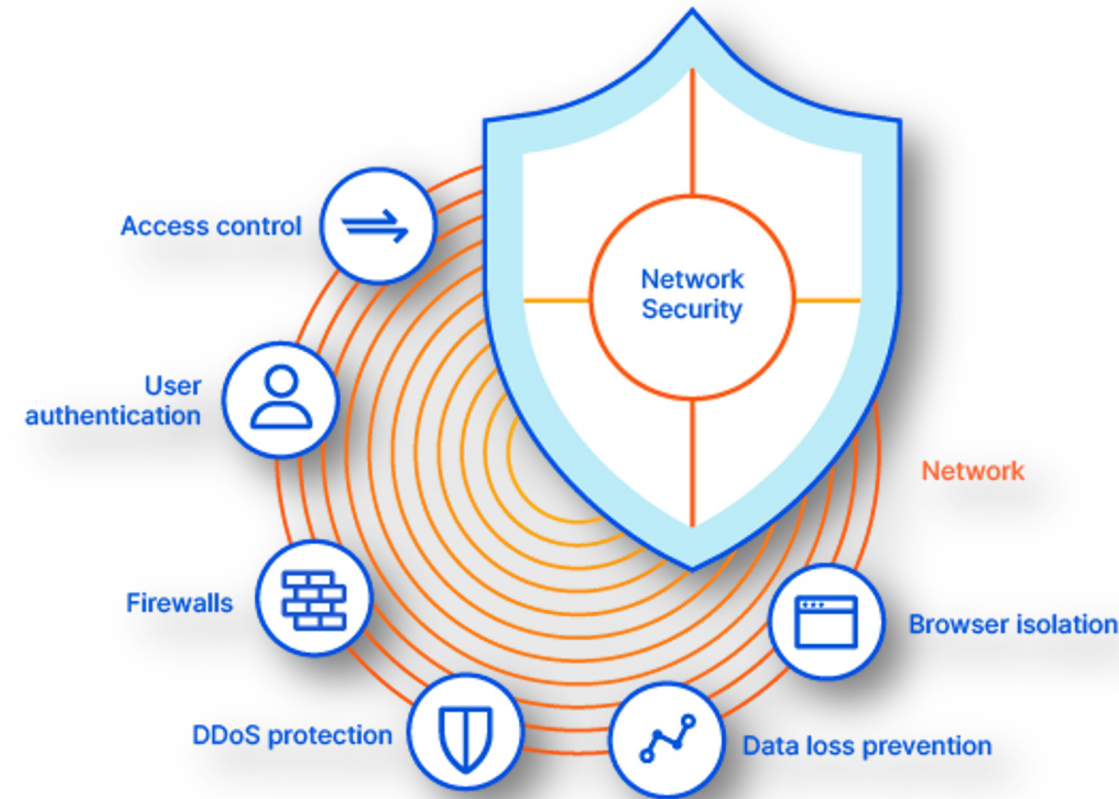
- **Information Security (InfoSec)** is the practice of protecting information from unauthorized access, disclosure, disruption, modification, or destruction.
- It aims to ensure the confidentiality, integrity, and availability (CIA Triad) of data, whether it's in storage, processing, or transit, through the use of policies, procedures, and technologies.
- Information security encompasses a wide range of security practices, including risk management, cryptography, access controls, and incident response, to protect both digital and physical information assets.



# Network Security



- **Network Security** is the practice of protecting the confidentiality, integrity, and availability of data and resources as they are transmitted or accessed across a network.
- It involves a combination of policies, procedures and technologies to prevent unauthorized access, misuse, modification, or disruption of network infrastructure.
- Network security includes measures such as encryption, security protocols, firewalls, IDS/IPS, and access controls to safeguard communication between devices and protect networks from threats like cyberattacks, malware, and data breaches.

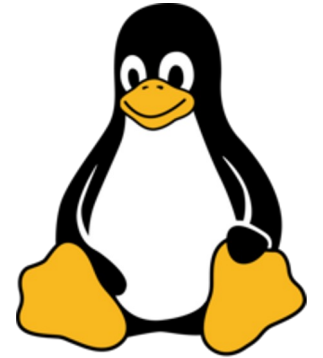
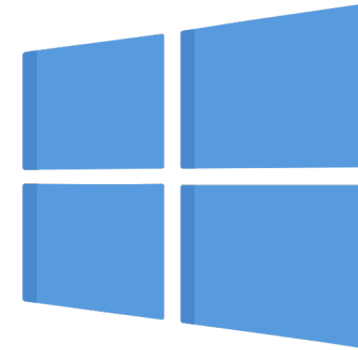




# Operating System Security



- **OS security** focuses on protecting the operating system from vulnerabilities and threats, ensuring that the system operates securely and is resistant to attacks.
- It is achieved through following steps:
  - Regularly applying updates and patches to address vulnerabilities and improve security.
  - Configuring the OS to reduce its attack surface by disabling unnecessary services and features.
  - Access Control.
  - User Authentication.
  - File System Security.



Linux™



Mac™OS



# Application Security



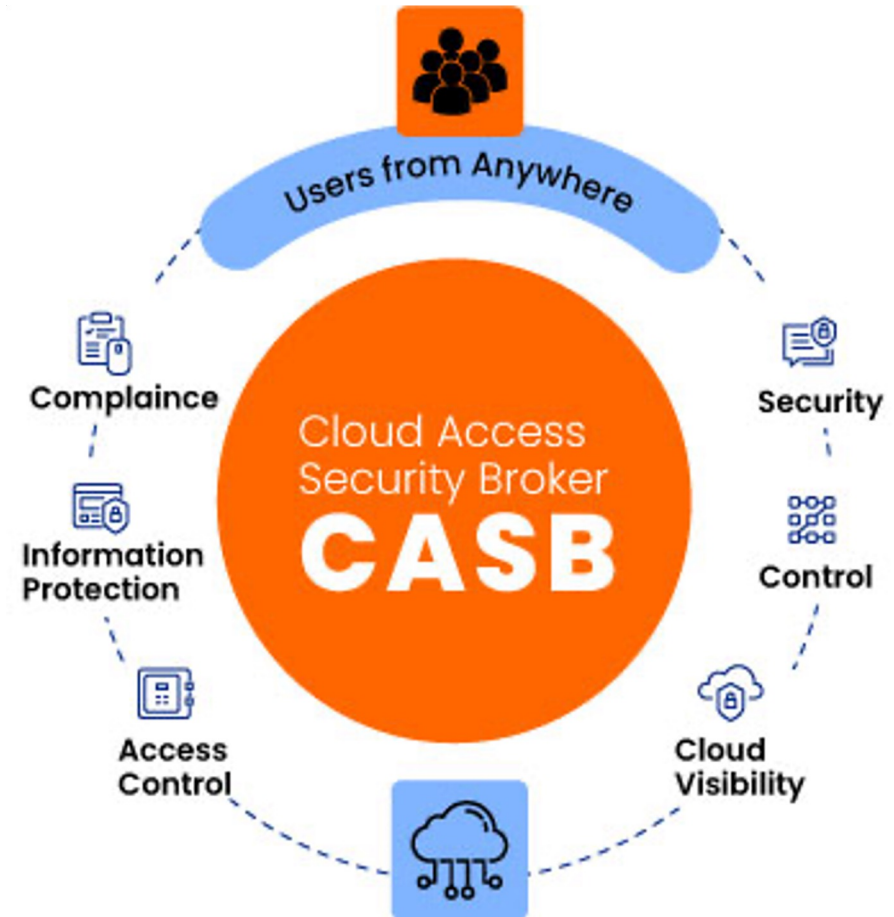
- **Application security** focuses on protecting software applications from threats and vulnerabilities that could lead to unauthorized access, data breaches, or other forms of exploitation.
- This includes techniques like secure coding, input validation, authentication, authorization, encryption, and regular security testing (such as vulnerability scanning and penetration testing).
- Application security aims to identify and fix vulnerabilities, such as SQL injection or cross-site scripting (XSS), to prevent malicious attacks.



# Cloud Security

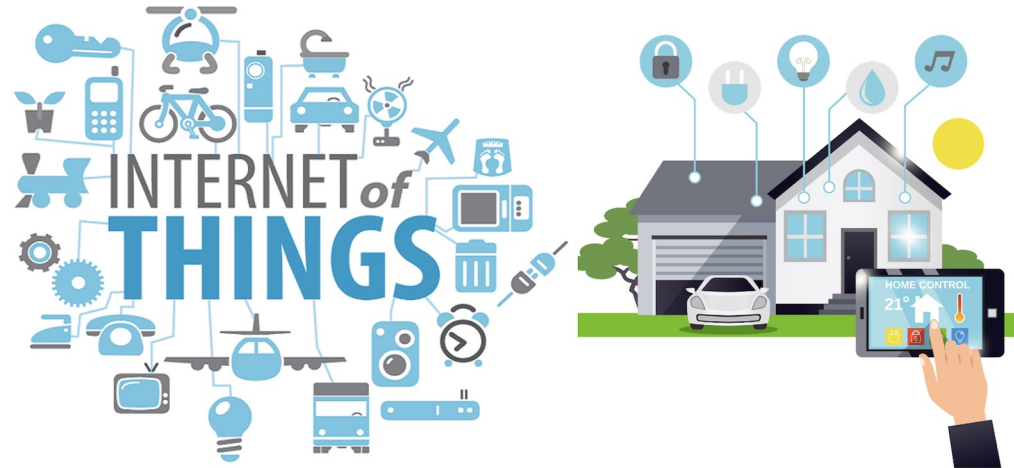


- **Cloud security** is the practice of safeguarding data, applications, and services hosted in cloud environments from unauthorized access, data breaches, and other cyber threats.
- Cloud security measures include encryption, Identity and Access Management (IAM), network security, Data Loss Prevention (DLP), and regular security monitoring.
- It addresses both the responsibilities of cloud providers (infrastructure security) and customers (secure configuration and data protection) to prevent threats like data leaks, account hijacking, and misconfigurations.



- **IoT security** is the practice of protecting Internet of Things (IoT) devices and the networks they connect to from cyber threats, unauthorized access, and vulnerabilities.
- Key IoT security practices include device authentication, encryption, secure firmware updates, network segmentation, and monitoring for unusual activity.
- IoT security is critical because these devices often have limited processing power, making them more susceptible to attacks, and they can serve as entry points for threats like malware or unauthorized control in broader network environments.

Collection of interconnected devices that communicate and transfer data through the Internet



Organizations struggle every day with the cybersecurity skills shortage. There just aren't enough qualified people to fill every role. In fact, research shows the world needs an influx of close to 3 million more cybersecurity professionals to meet demand.



ISC2

<https://www.isc2.org> › landing › throw-down-the-ladder

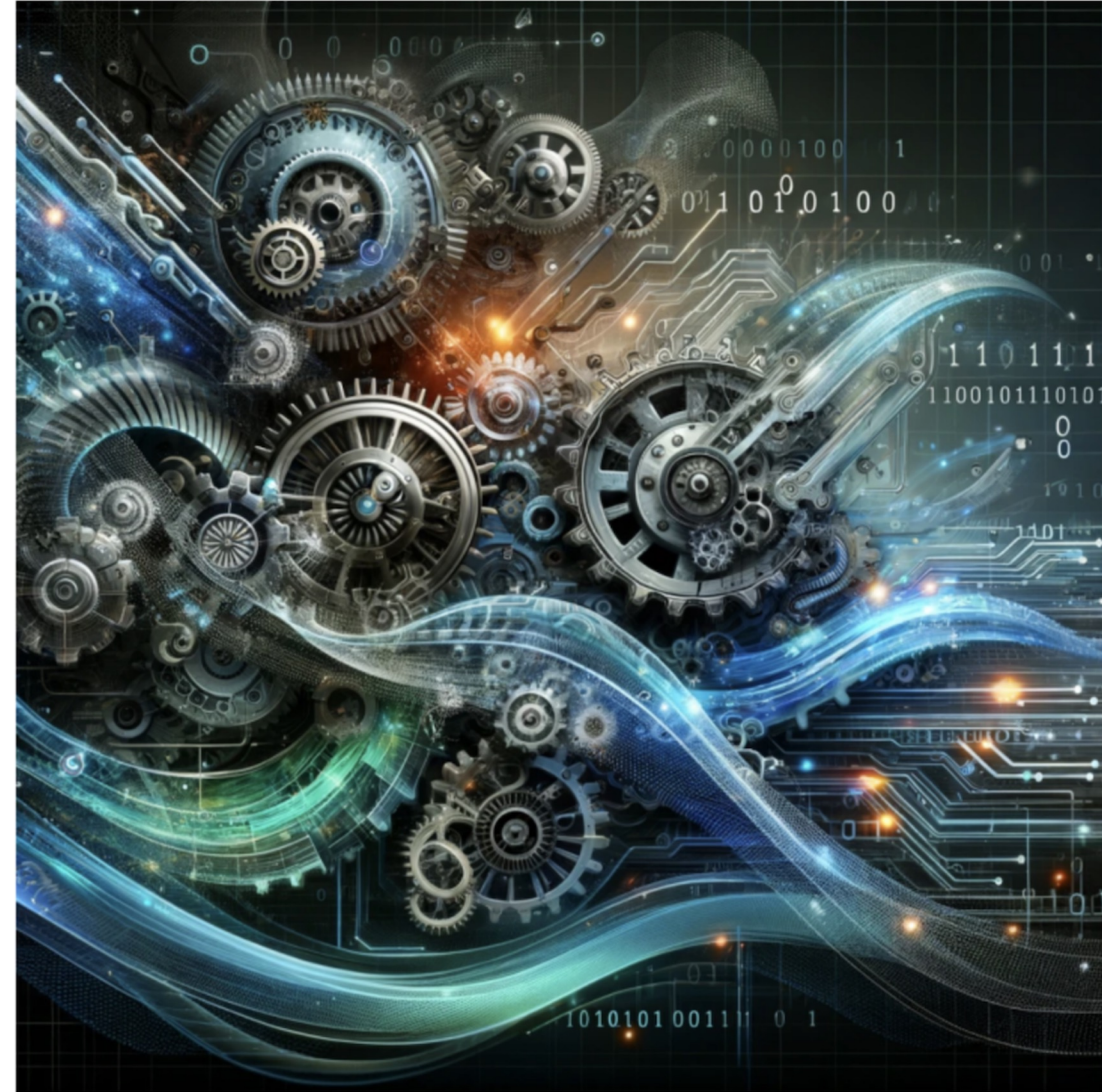


Throw Down the Ladder | ISC2 Certified in Cybersecurity



## LLM Security Threats

- Prompt injection
- Jail breaking
- Backdoor and data poisoning
- Adversarial inputs
- Insecure output handling
- Data extraction & privacy
- Data reconstruction
- Denial of service
- Privilege escalation
- Water marking and evasion
- Model theft



DALL-E: "Automation"

# History of Cyber Attacks

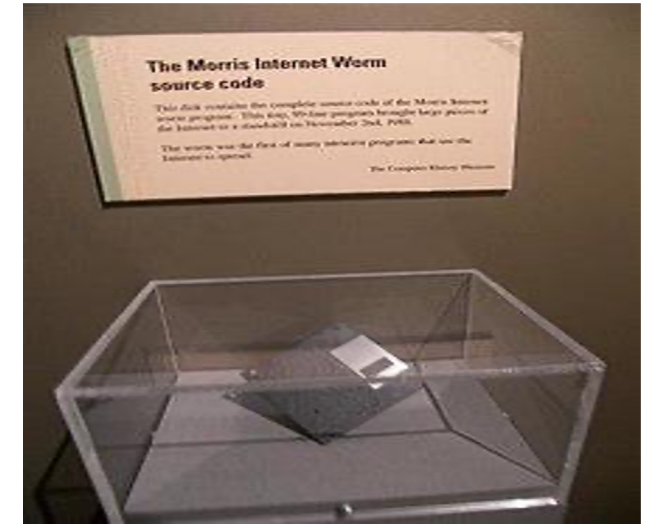
# Famous Cyber Attacks



**Morris Worm (1988):** Often considered one of the first major worms, created by Robert Tappan Morris. It exploited sendmail service to achieve RCE and exploited BoF vulnerability in the finger daemon to retrieve user information in Unix systems and spread across the internet. It infected around 6,000 computers, causing significant disruption by slowing down systems and making them unusable.

**Melissa Virus (1999):** The Melissa virus was a computer virus that spread quickly through email attachments in 1999. It primarily exploited vulnerabilities in Microsoft Word Macros and Outlook users, and was one of the first viruses to raise awareness of the risks of opening unsolicited emails.

**ILOVEYOU Worm (2000):** The ILOVEYOU Worm, also known as the Love Bug, spread through email with a subject line that read "I Love You." It used a social engineering trick to lure recipients into opening an infected attachment. It caused widespread damage, affecting 10 million computers globally, and led to billions of dollars in damages.



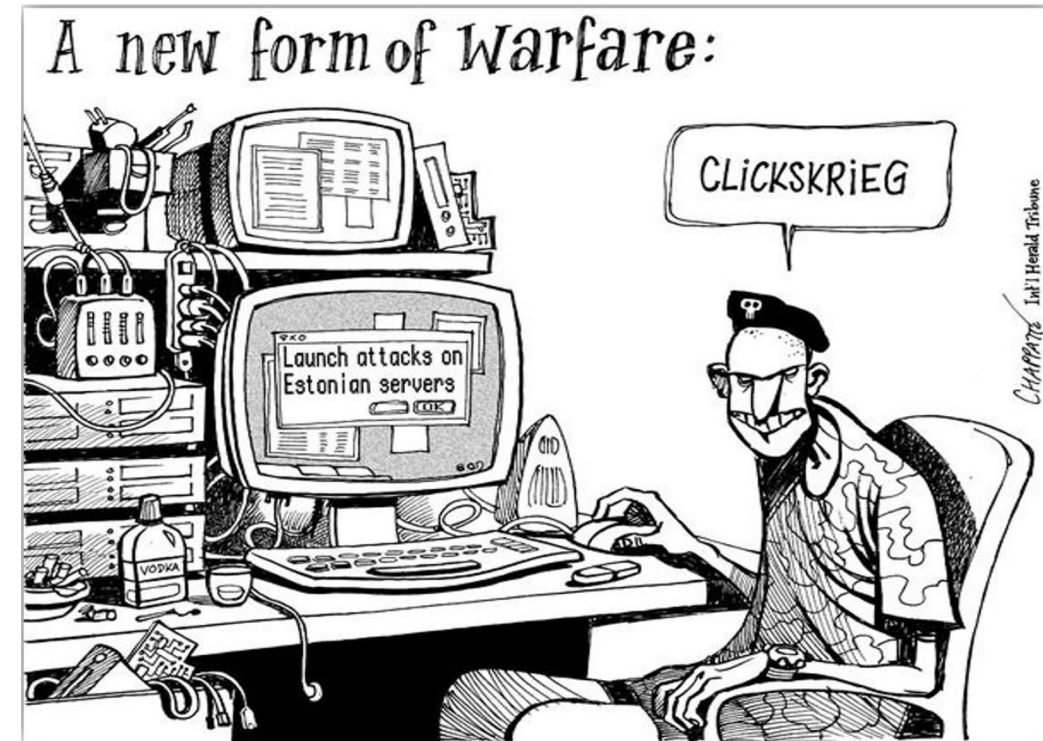


# Famous Cyber Attacks



**Cyber Attacks against Estonia (2007):** In 2007, Estonia experienced a series of major cyber attacks, widely regarded as one of the first large-scale, politically motivated, state-sponsored cyber warfare campaigns.

- These attacks targeted government institutions, banks, media outlets, and other critical infrastructure, effectively disrupting the nation's online services for several weeks.
- It involved DDoS (Distributed Denial of Service) attacks, overwhelming servers with traffic to shut down websites and services.
- Russia was widely suspected of being behind the attacks.

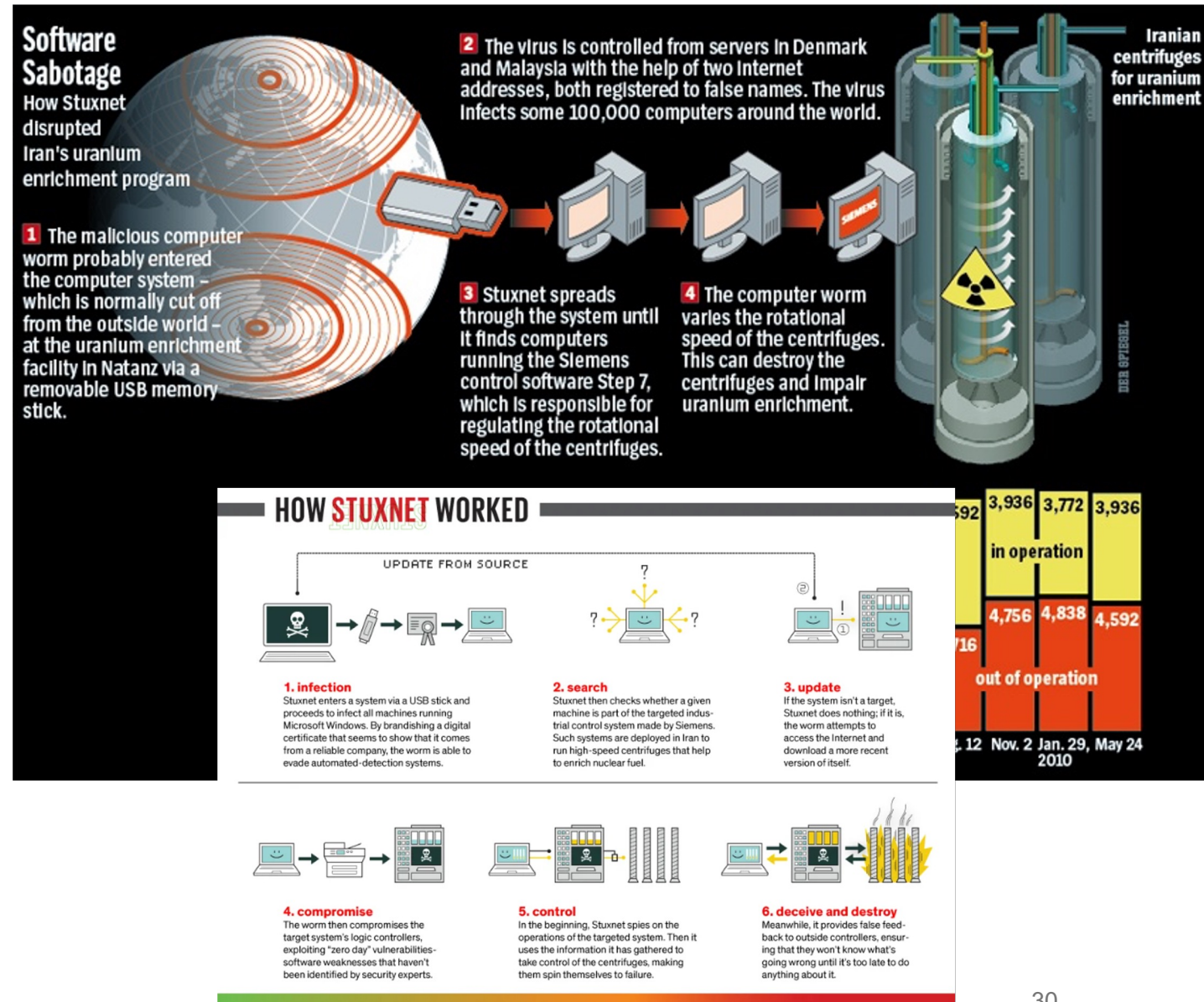


# Famous Cyber Attacks



## Stuxnet (2010):

- Stuxnet was a sophisticated worm believed to be created by the U.S. and Israeli governments to target Iran's nuclear facilities. Worm spread through Windows computers, but its primary function was to cause physical damage to the centrifuges by altering their speeds without detection, while simultaneously sending normal operating signals to monitoring systems.
- It is considered one of the first known cyber weapons and demonstrated the potential for cyber-attacks to cause physical damage.



# Famous Cyber Attacks



## Sony PlayStation Network Hack (2011):

- Attackers compromised Sony's PlayStation Network (**PSN Hack**), gaining access to personal information of around 77 million users.
- They used a combination of phishing techniques and SQL injection to gain unauthorized access to Sony's servers. Data Breach forced Sony to shut down the PSN for nearly a month.
- Sony faced financial loss of \$171 million approx., making it one of the largest security breaches of its time.
- The breach led to the suspension of the network, significant financial losses, and a major hit to Sony's reputation.





# Famous Cyber Attacks



## WannaCry Ransomware Attack (2017):

- WannaCry attacked computers worldwide by exploiting a vulnerability in Microsoft's Server Message Block protocol.
- Vulnerability ID: CVE-2017-0144
- Exploit used: EternalBlue, developed by NSA, leaked by shadow brokers hacking group.
- It encrypted users' files and demanded ransom payments in Bitcoin.
- The attack affected more than 300,000 computers across 150 countries, with total damage ranging from hundreds of millions to billions of dollars.
- Attack caused significant financial losses, halted critical services, and highlighted the dangers of outdated software and unpatched security vulnerabilities.

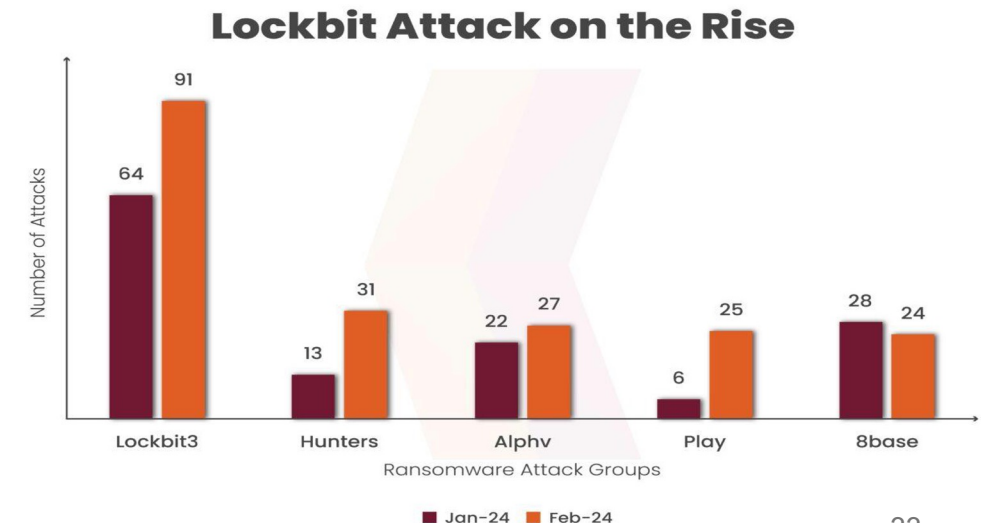


# Famous Cyber Attacks



## LockBit (2019):

- A notorious ransomware group known for its multiple versions of ransomware, including LockBit1.0 (2019), LockBit2.0 (2021), LockBit3.0 (2022) and LockBit Black (2023).
- Each version has become more sophisticated, with enhanced encryption and better evasion tactics. The group operates under a ransomware-as-a-service (RaaS) model, allowing other cybercriminals to use their software for a fee.
- Attacked financial services, healthcare and transportation sectors.
- Used in approximately 1,700 ransomware attacks in US between January 2020 to and May 2023, with US\$91 million paid as ransom.
- Also declared as the world's most prolific ransomware in 2022.



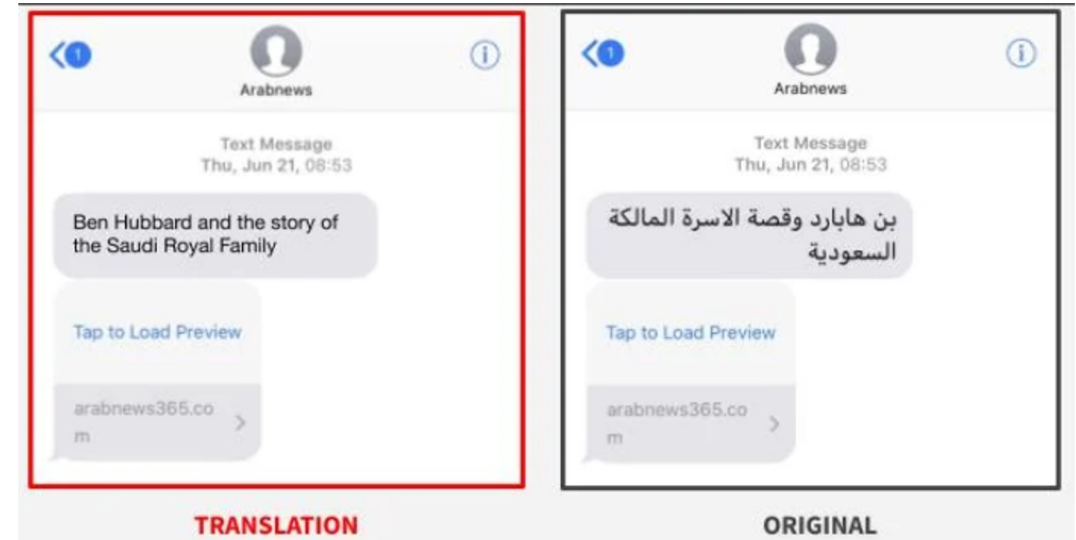
# Famous Cyber Attacks



**Pegasus (Forced Entry) (2021):** Pegasus (Forced Entry) refers to a specific exploit of the Pegasus spyware, developed by Israeli company NSO group. It explored a zero-day in Apple's iMessage, allowing the spyware to be installed on a device without any interaction from the victim. This attack didn't require the victim to click on a malicious link or open a compromised file; it could be silently triggered just by receiving a specially crafted message. Once installed, Pegasus could monitor calls, messages, emails, and even activate microphones and camera

**Operation Triangulation (2023):** This operation utilized Pegasus spyware to silently compromise mobile devices and gain access to sensitive data. Operation Triangulation is a targeted cyberattack on iOS devices conducted using a chain of four zero-day vulnerabilities.

Instructor(s): Muhammad Rauf Butt, Muhammad Arif Butt, PhD



# Famous Cyber Attacks (Cont..)



## IoT (Internet of Things) Attacks

- **Mirai Botnet (2021):** The Mirai botnet, which was initially used for DDoS attacks, continues to exploit vulnerabilities in IoT devices to launch large-scale attacks.
- IoT device vulnerabilities can lead to widespread disruptions and can be used to launch attacks on various services. It stresses the importance of securing connected devices and updating their software regularly.





# Famous Cyber Attacks (Cont..)



**Deepfake AI:** Deepfake AI poses significant challenges to cybersecurity, as it can be used to create highly convincing fake audio, video, and text content that can deceive individuals and manipulate public opinion

- Social Engineering Attacks
- Phishing and Fraud
- Reputation Damage
- Misinformation and Disinformation Campaigns
- Authentication and Trust Issues





# Famous Cyber Attacks (Cont..)



ispr.gov.pk

## Hacked By Benaam Pakistani

### Pakistan Zindabad

#### Dear Pakistani's

**In the memories of those who sacrifice their life for us,**

**It is to inform that Pakistan Armed Forces are the best in the World.**

**They've made a lot of sacrifices for this country and were the true defenders of this motherland.**

**But, they must not misuse their power against their own people.**

**They should work for the betterment of this country rather than killing it like a parasite.**

**Meanwhile, the politicians too are required to obey by their oath.**

**They should work to make the country a much better place to live in.**

**Islamic principles and teachings should be opted in every field especially in the economic aspect (interest free).**

**Moreover, the citizens are also advised to rectify their character and code of conduct. They must leave all the activities which tends out to be a harm for the country. It is time to unite!**

## Over 2 million Pakistanis' data hacked from restaurants database up for sale



**KARACHI:** Bykea, a popular ride-hailing, mobility, and delivery app used by many Pakistanis, experienced a disturbing hacking incident on Tuesday, causing widespread concern among users.

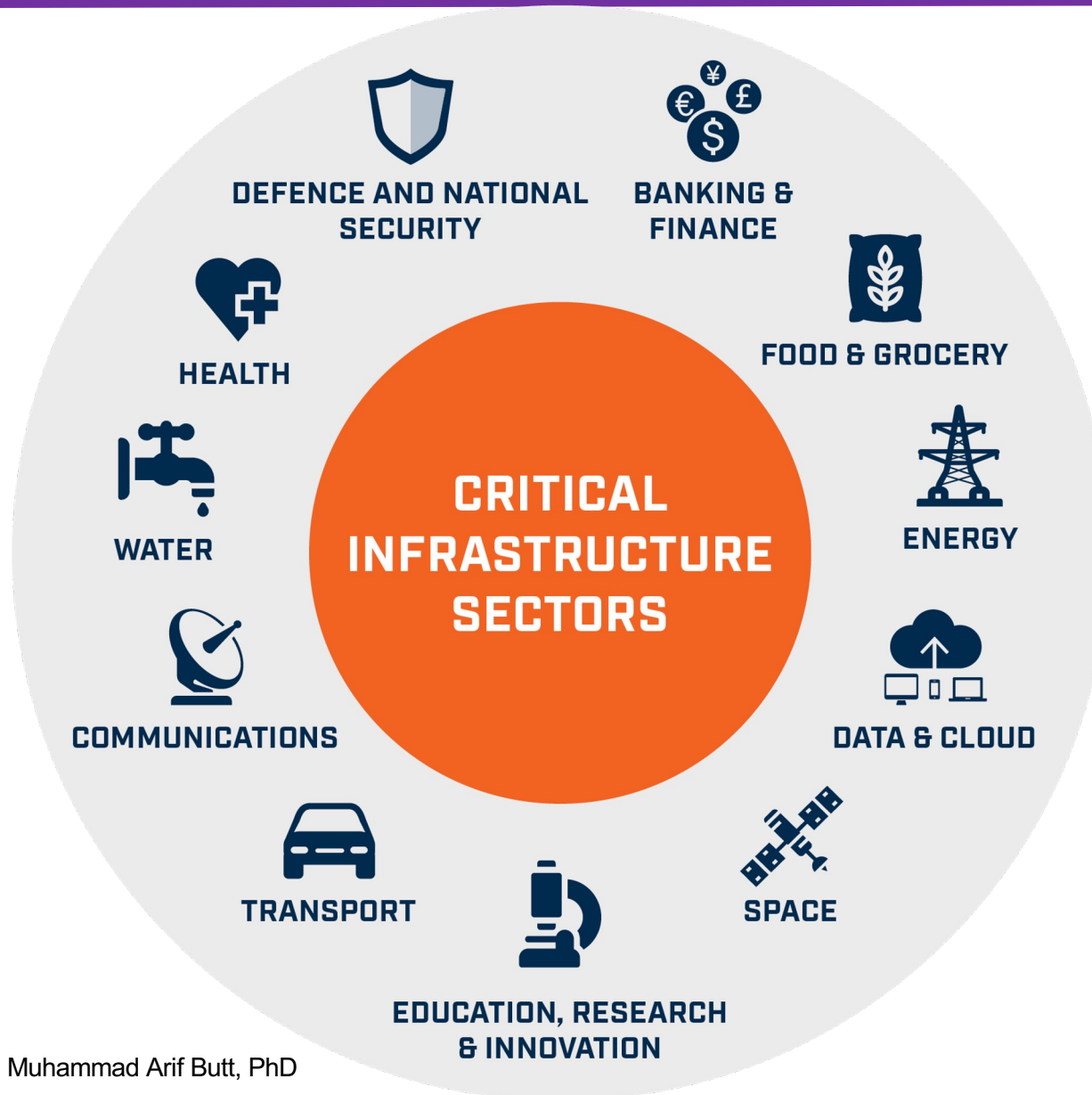
The ordeal began when users started receiving highly inappropriate text messages, alarming and unsettling them. Bykea promptly addressed the issue and issued an apology for the offensive messages.

# Impacts of Cyber Attacks



- **Financial Losses:** Direct financial losses due to theft, ransom payments, and fraud, as well as indirect costs from downtime, recovery efforts, and legal fees.
- **Operational Disruption:** Interruption of business operations, affecting productivity and service delivery. Critical infrastructure attacks can lead to widespread disruptions in essential services.
- **Reputational Damage:** Loss of customer trust and damage to the organization's reputation, which can affect future business prospects and customer relationships.
- **Data Privacy Concerns:** Exposure of personal and sensitive data, leading to increased risks of identity theft, phishing, and privacy violations.
- **Regulatory and Legal Consequences:** Increased scrutiny from regulators and potential legal actions, resulting in fines and compliance costs.
- **National Security Risks:** Espionage and attacks on critical infrastructure can have implications for national security and geopolitical stability.

# National Critical Infrastructure



# Cybersecurity Roles



# Penetration Testing (PT)



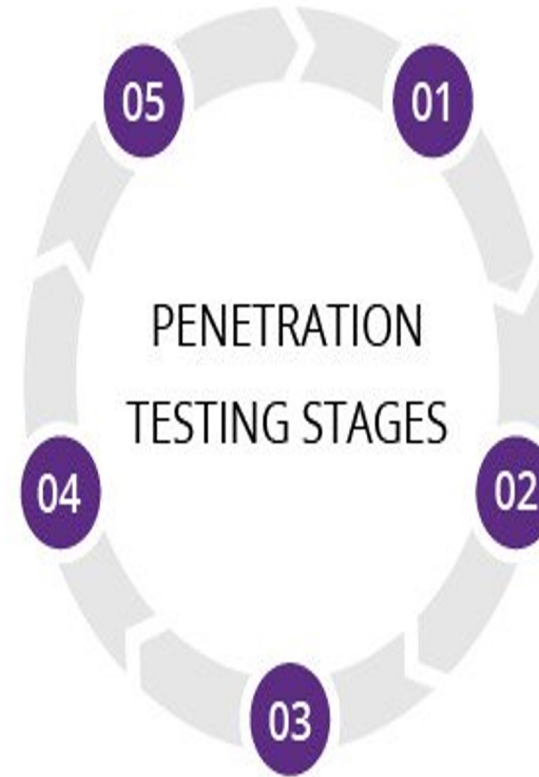
- **Networks**
- **Websites**
- **Mobile applications**
- **Cloud Services**
- **Large Language Models**

## Analysis and WAF configuration

Results are used to configure WAF settings before testing is run again.

## Maintaining access

APT's are imitated to see if a vulnerability can be used to maintain access.



## Planning and reconnaissance

Test goals are defined and intelligence is gathered.

## Scanning

Scanning tools are used to understand how a target responds to intrusions.

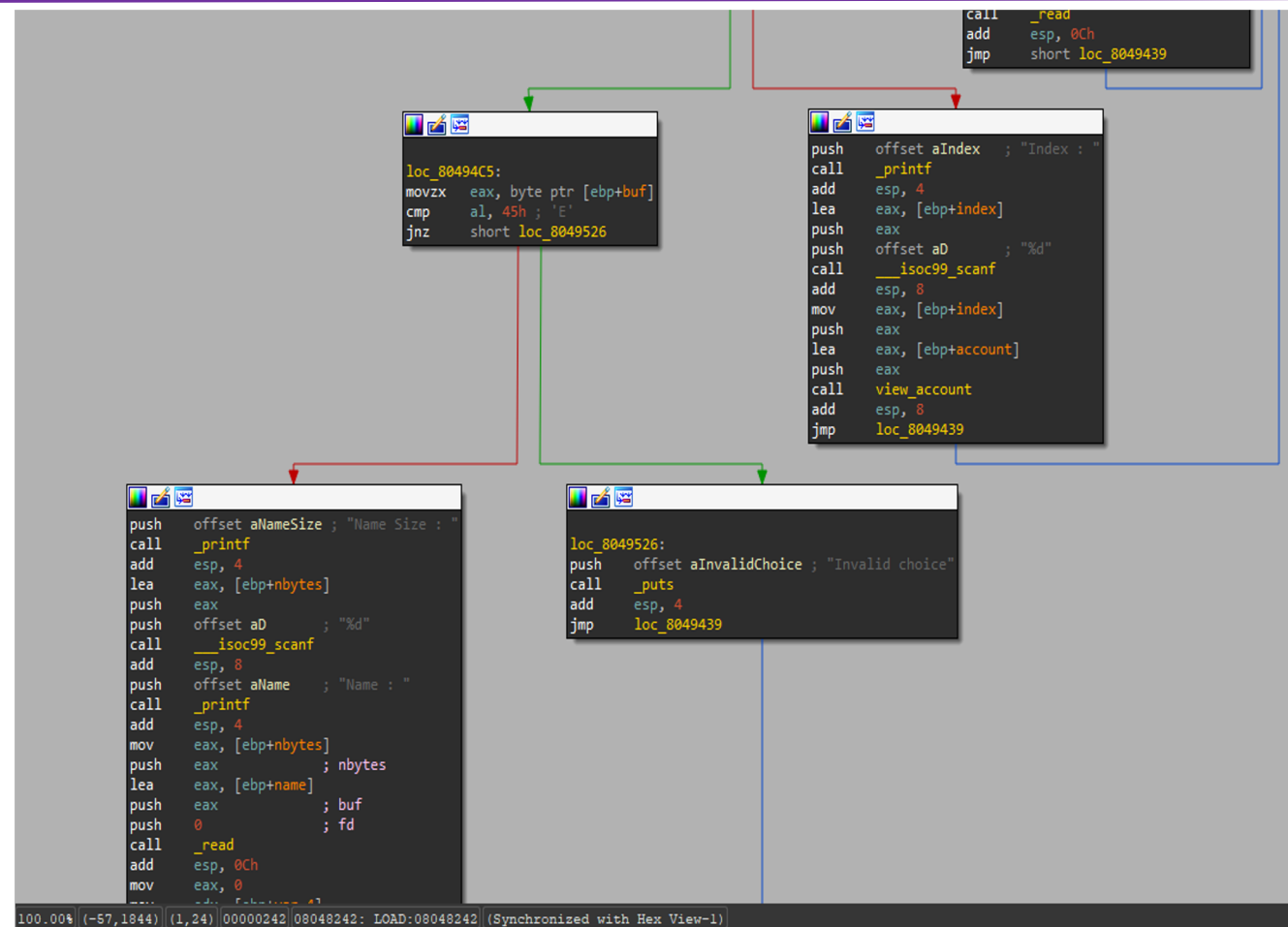
## Gaining access

Web application attacks are staged to uncover a target's vulnerabilities.

# Reverse Engineering



- Closed Source Code Analysis
- Malware Analysis
- License Reversing



- [illegible]

- **Attackers**
- **Offensive**
- **Legal Criminal Activity**
- **Website Hacking**
- **Mobile Phone Hacking**
- **Network Hacking**





# Blue Team



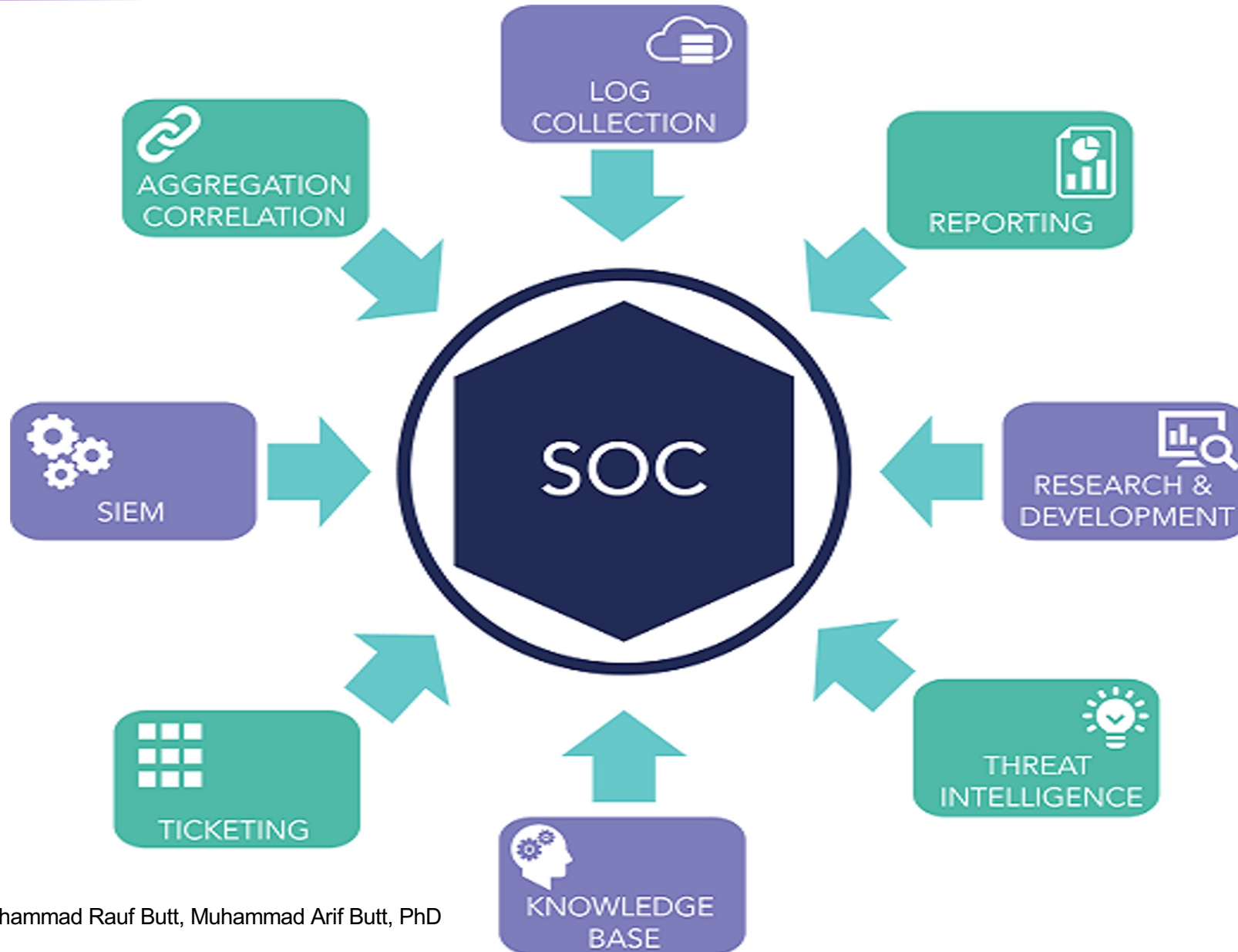
- Defenders
- Protect against Red Team



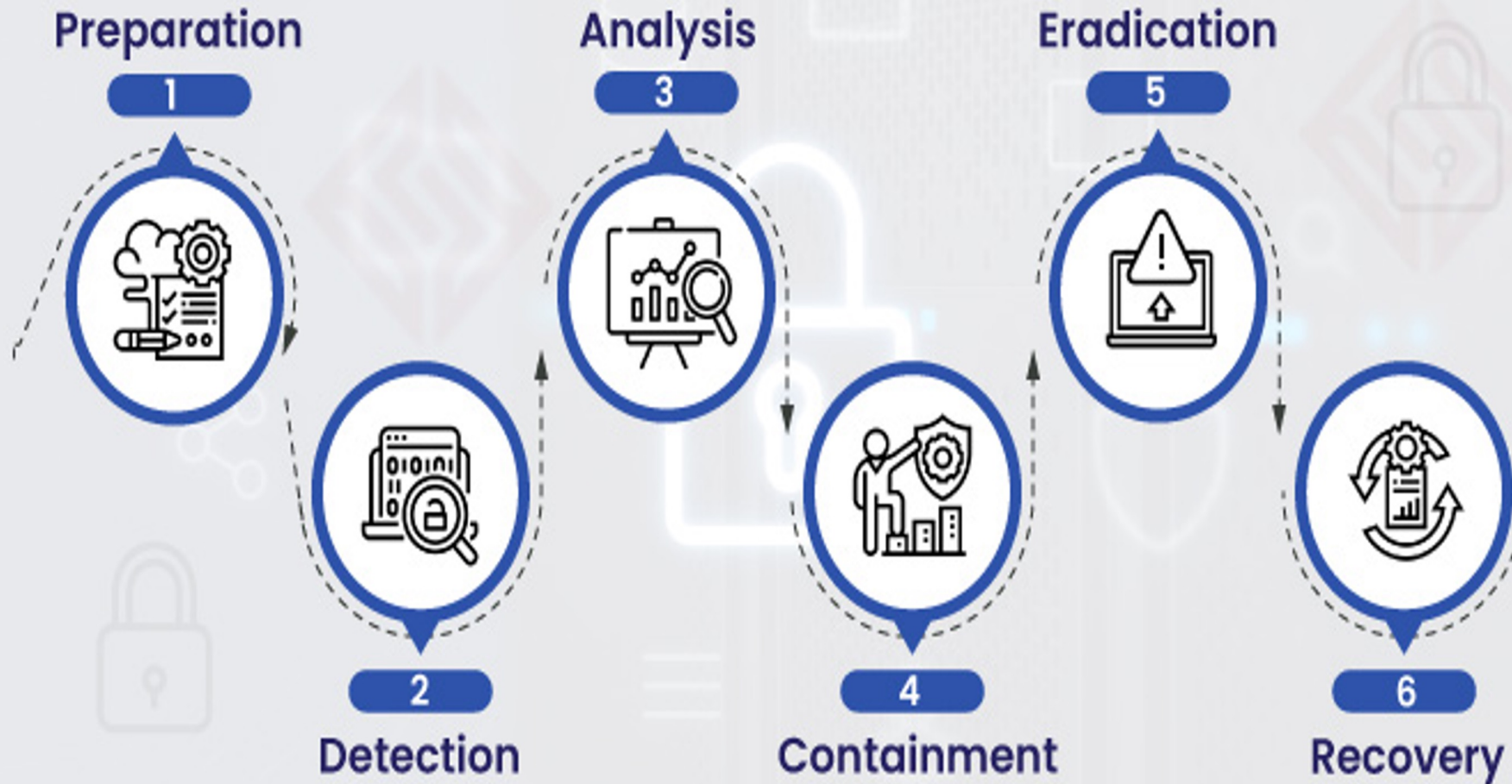
- **Governance**
- **Risk Management**
- **Compliance**
  - Secure Programming
  - Secure Assets
  - Secure Interpersonal Communication



# Security Operation Center

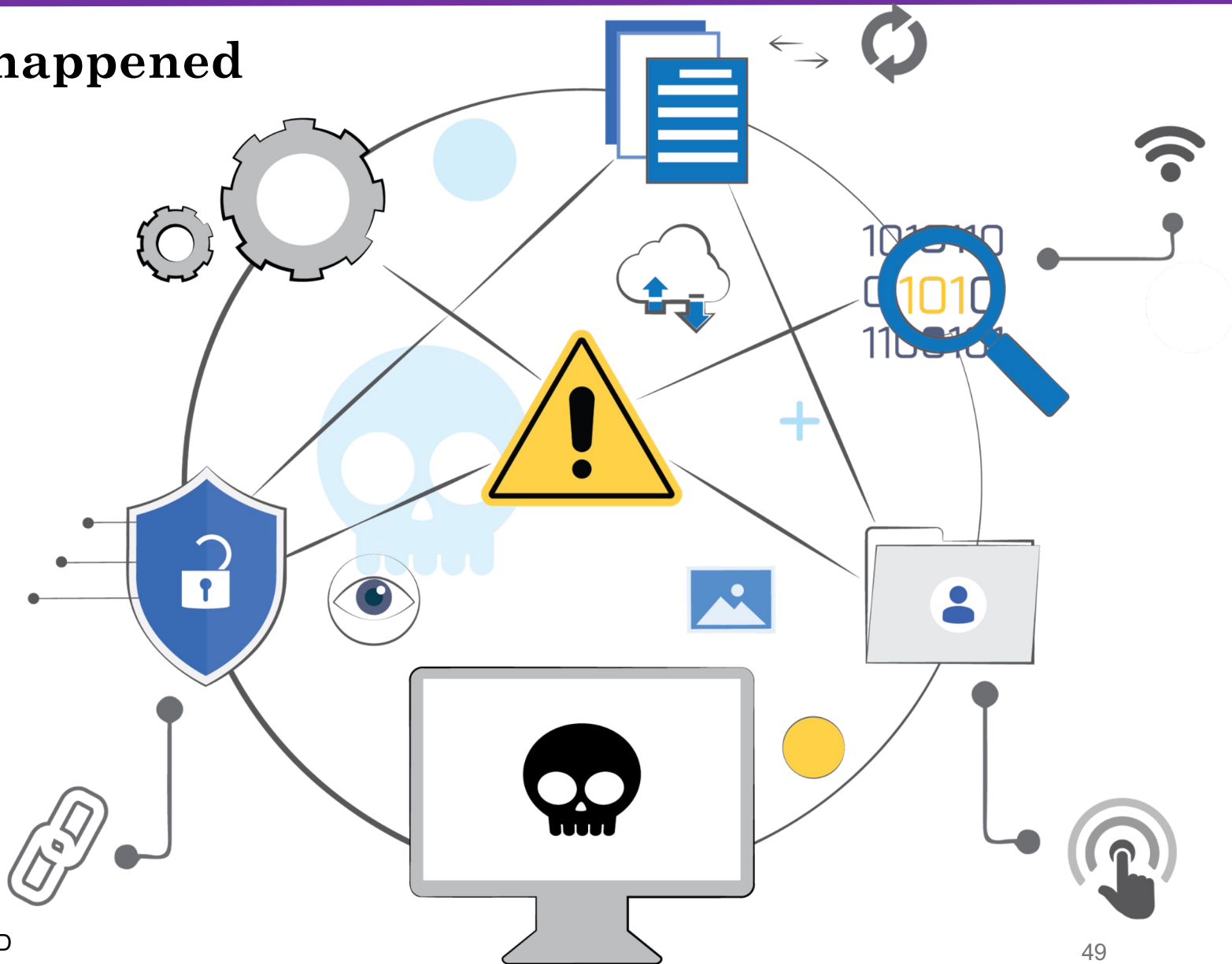


## The Six Steps of Incident Response





- **Figure out how attack happened**
- **Disk Analysis**
- **Memory Analysis**
- **Follow traces**



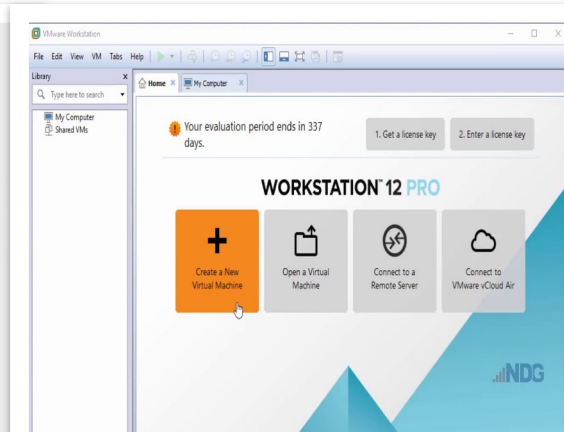
# Course Contents

# Overview of the Course



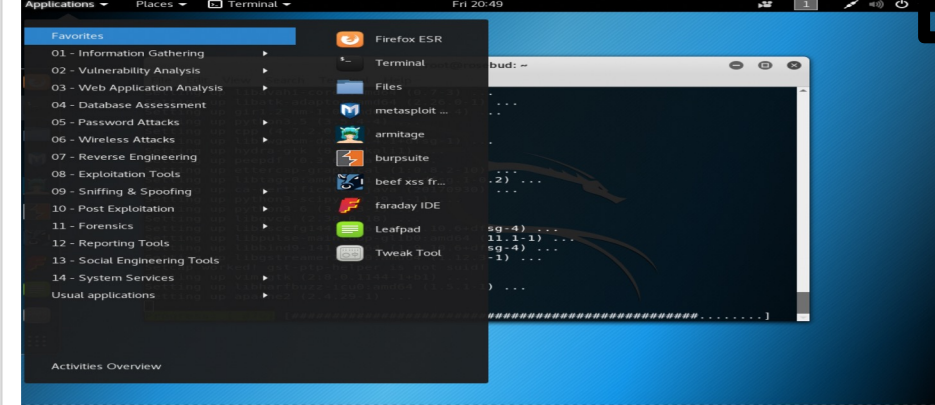
M1

## Overview and pre-requisites



## NW Attacks and Penetration Testing

M2



M3

## Reverse Engineering & Binary Exploitation



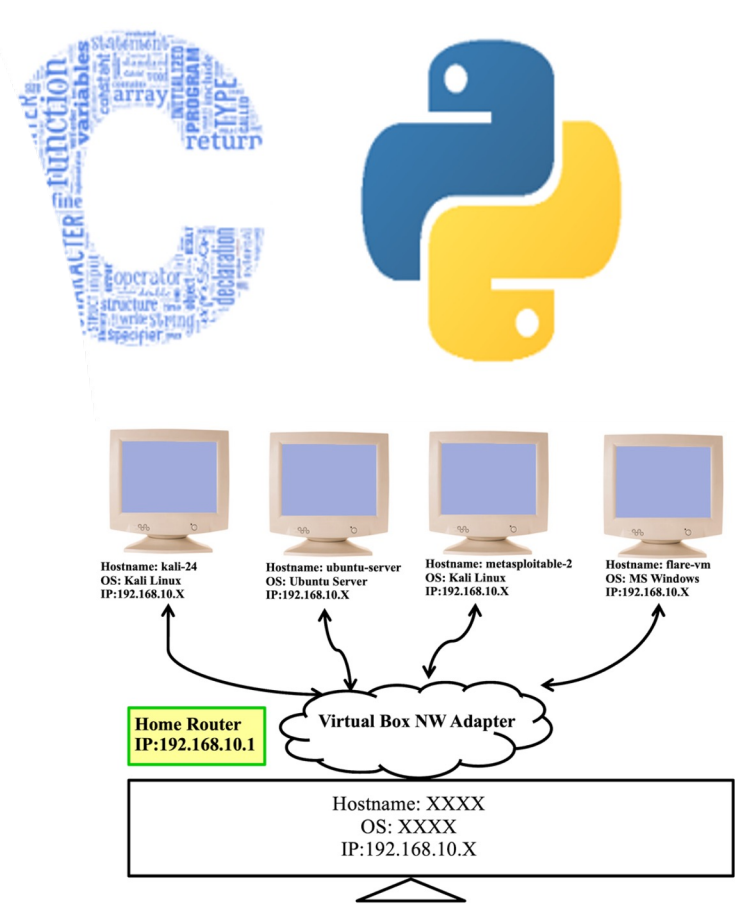
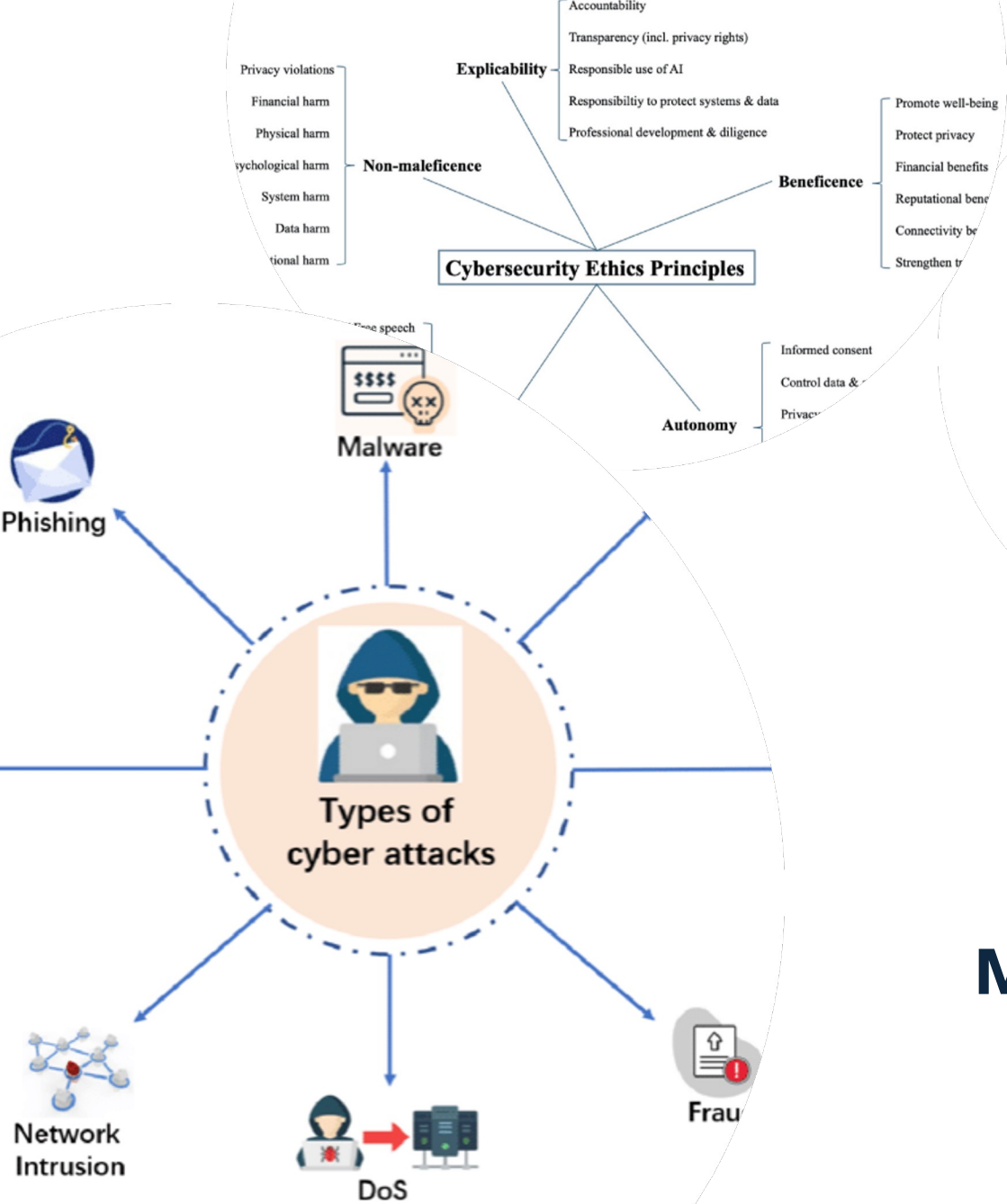
## Malware Development and Analysis

M4



# Module 01: Overview and Prerequisites





## Module 1: Overview and Prerequisites

# Prerequisites of the Course



## Operating System



Linux



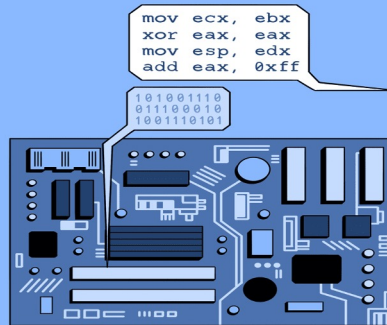
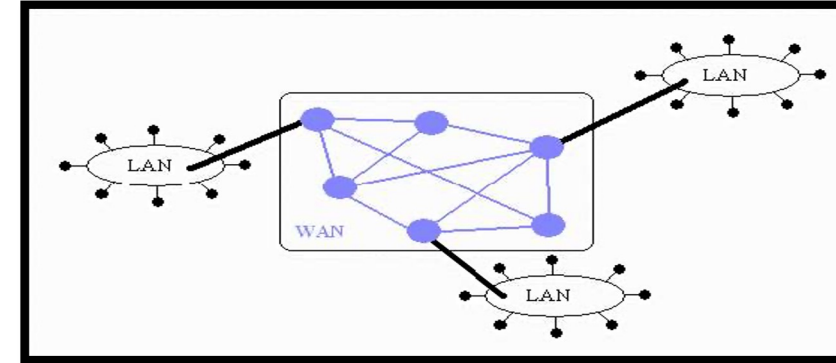
Windows



macOS



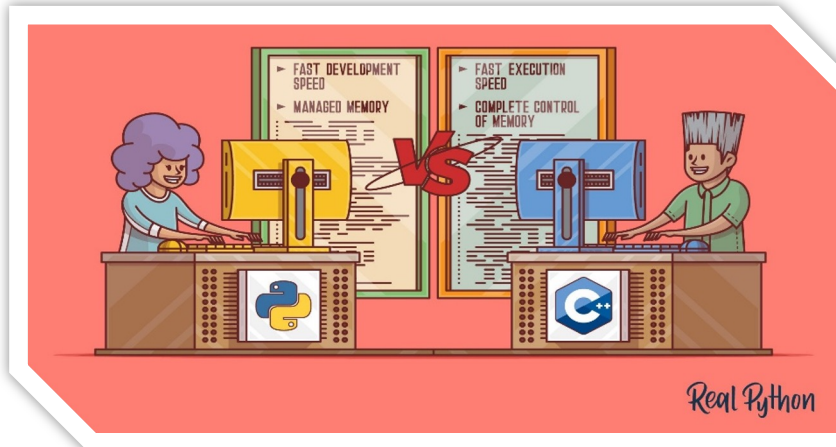
Android



## Assembly Language

[ə-'sem-blē 'lɑŋ-gwɪj]

Low-level programming language intended to communicate directly with a computer's hardware.



# **Module2: NW Attacks & Penetration Testing**

# Module 2: NW Attacks & PT



Penetration testing (pen testing) is a systematic process used to identify and exploit vulnerabilities in a system, network, or application to understand the security risks.

1

**Reconnaissance  
and Information  
Gathering**

2

**Scanning and  
Vulnerability  
Analysis**

3

**Exploitation and  
Gaining Access**

4

**Privilege  
Escalation**

5

**Maintaining  
Access and  
Persistent  
Mechanisms**

6

**Covering Tracks**

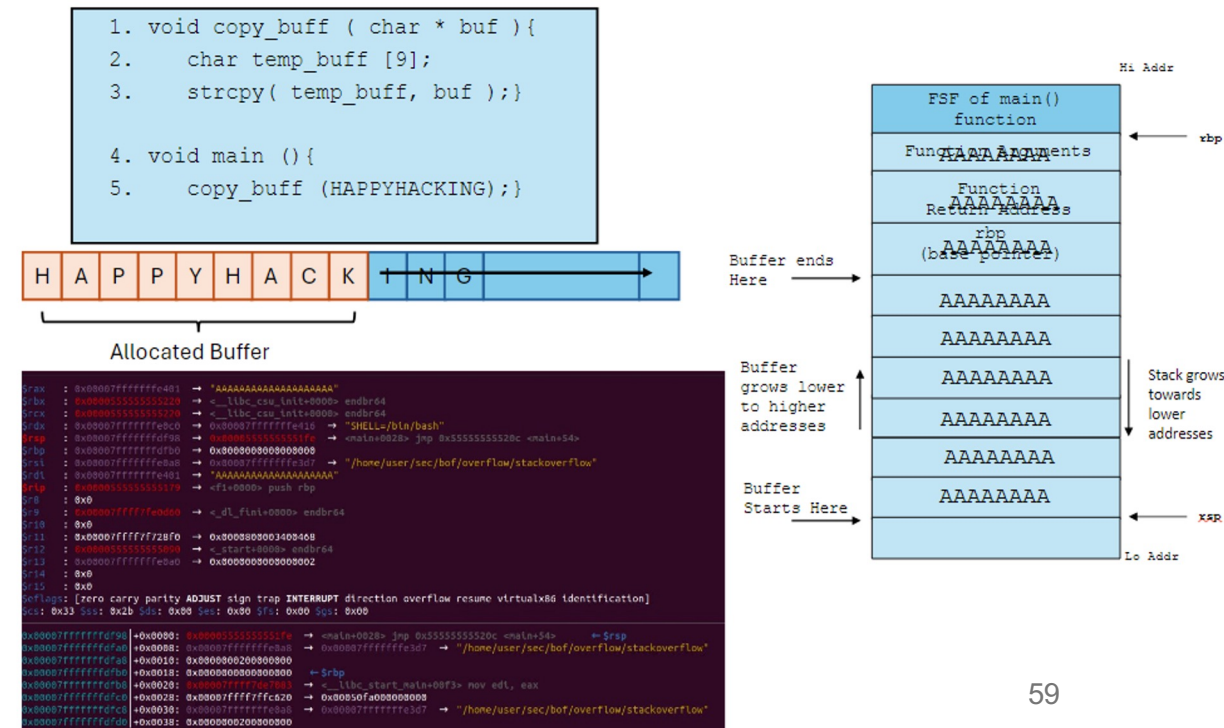


# **Module3: Reverse Engineering and Binary Exploitation**

- **Reverse engineering** in cybersecurity refers to the process of analyzing and disassembling software, hardware, or protocols to understand their inner workings, often with the goal of extracting valuable information, identifying vulnerabilities, malicious behavior or weaknesses.
- Key purposes of reverse engineering are:
  - Software cracking or protection
  - Vulnerability research
  - Malware analysis
  - Digital forensics
- Tools used in reverse engineering are:
  - GNU GDB
  - IDA Pro
  - Radare2
  - X64dbg
  - Wireshark
  - Burp Suite

- Buffer overflow
- Integer overflow
- Use after free
- Race condition
- Return oriented programming
- Format string vulnerability
- Shellshock vulnerability
- SUDO vulnerability
- COW vulnerability

Instructor(s): Muhammad Rauf Butt, Muhammad Arif Butt, PhD



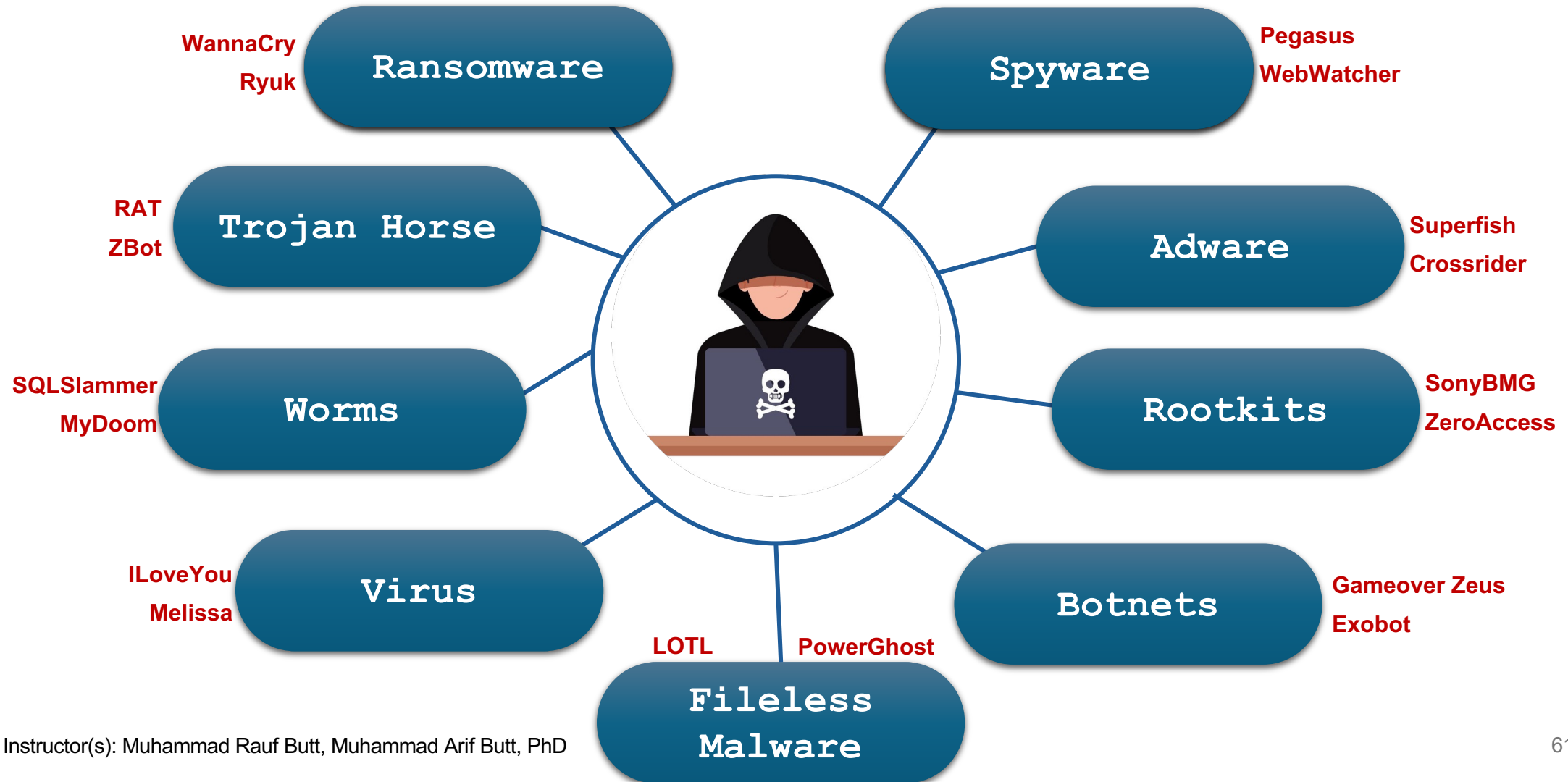
# Module4: Malware Development & Analysis



# Module 4: Malware Development & Analysis



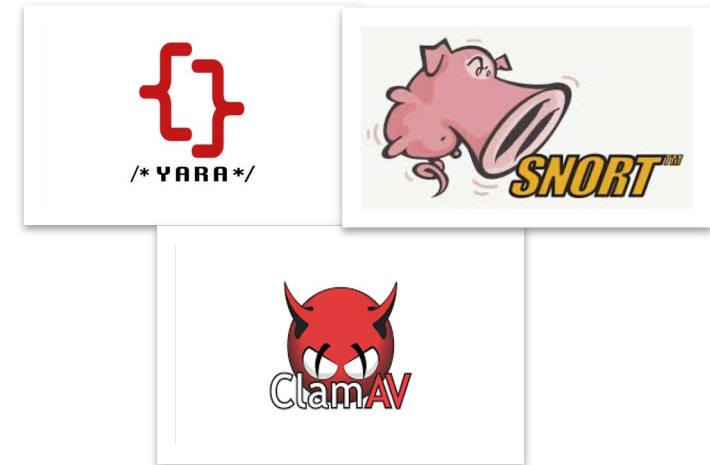
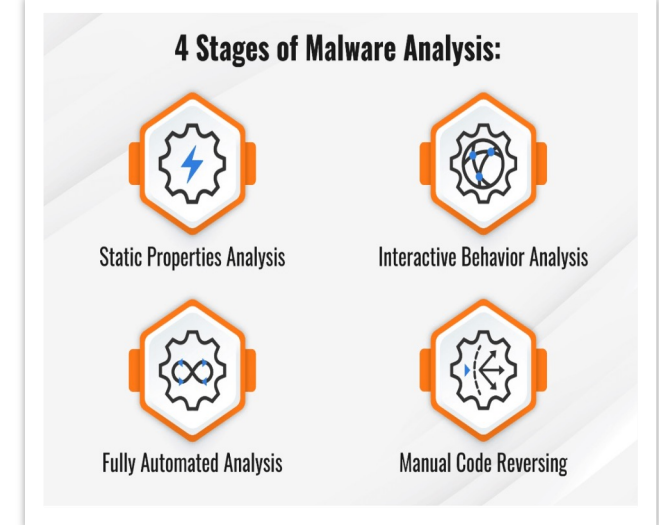
Malware development refers to the process of creating malicious software designed to infiltrate, damage or steal data from, or disrupt the operation of computers, NW or devices



# Module 4: Malware Development & Analysis



- Understanding Malwares and its types
- Building closed environment to perform analysis
- Understanding the procedure to perform the analysis
- Understanding the art of writing detection rules
- **YARA:** Yet Another Ridiculous Acronym is a versatile and powerful tool for malware detection, classification and hunting. It help writing custom rules to detect threads that might bypass traditional security solutions.
- **ClamAV:** An open-source antivirus engine used for detecting and removing malware, including viruses, trojans, and worms.
- **Snort:** An open-source IDS/IPS that helps in monitoring network traffic in real time to detect suspicious activities and potential security threats.



# Happy Hacking

## To Do:

Go through Handout # 1.2 at your own and set-up your own Virtual Hacking Lab for all the class activities and assignments using either Virtual Machines or Docker Containers or both 😊