Cyber Security

Lecture 1.0
Overview of the Course

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

Lecture Agenda

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

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
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 at different field in Pakistan Army
- Assistant Professor, Department of Data Science

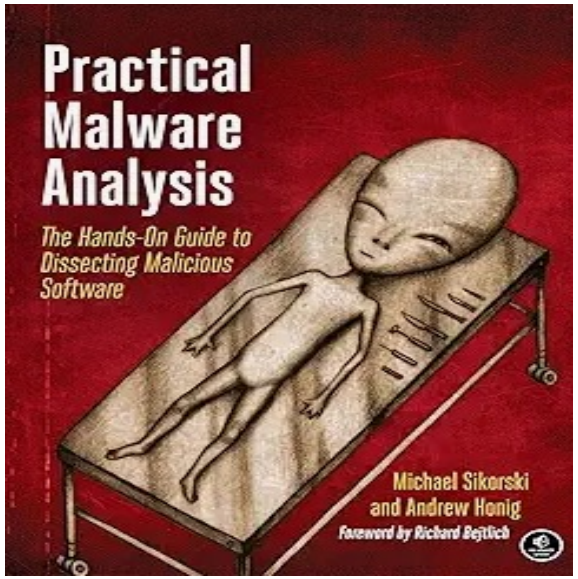
Research Interests:

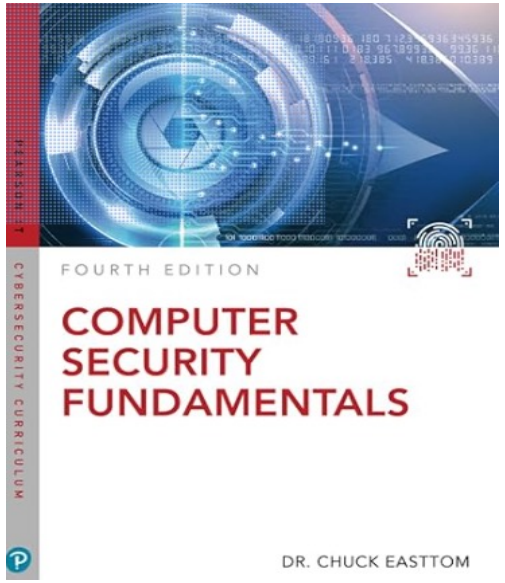
- Embedded and real time operating systems
- Generative AI
- AI/LLM Security

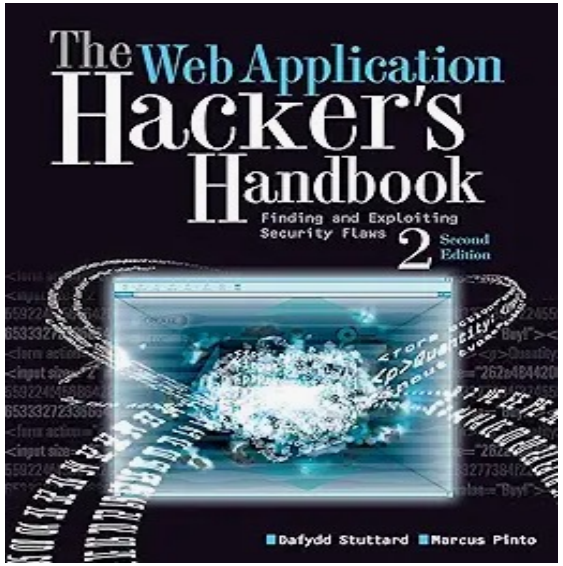
Course Information

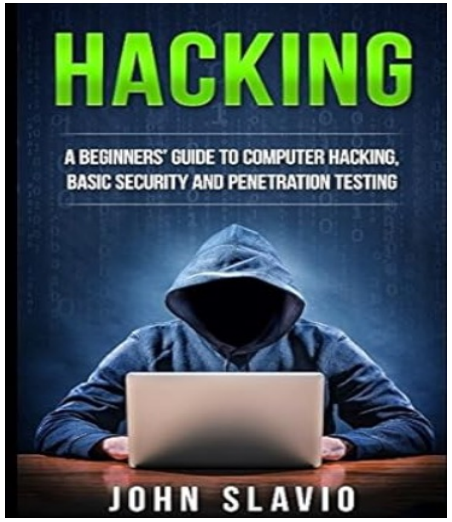
- Lectures Slides/Handouts Available at: https://arifbutt.me
- Video Lectures Available at: https://youtube.com/learnwitharif
- Codes Hosted at: https://github.com/arifpucit
- Grades Website: https://online.pucit.edu.pk
- Prerequisites:
  - OS and Internetworking with Linux
  - Basic programming skills 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

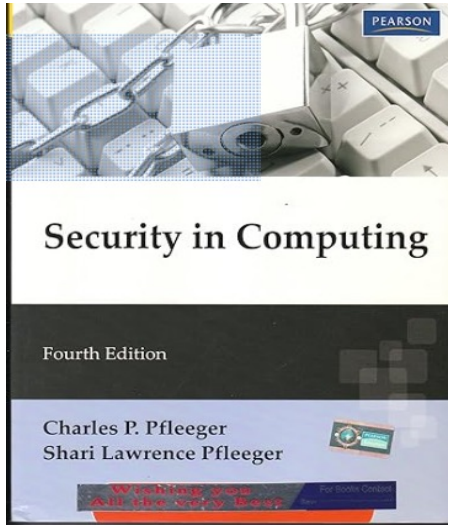
Text and Reference Books

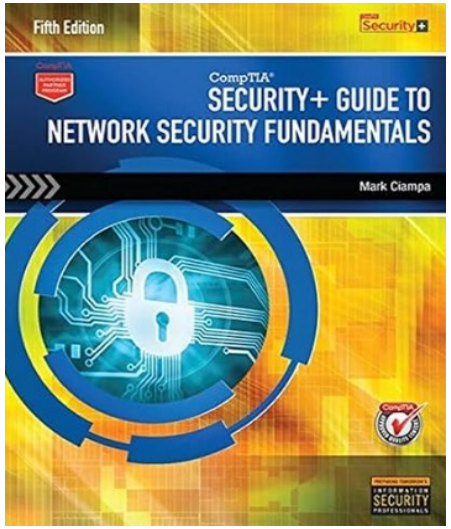












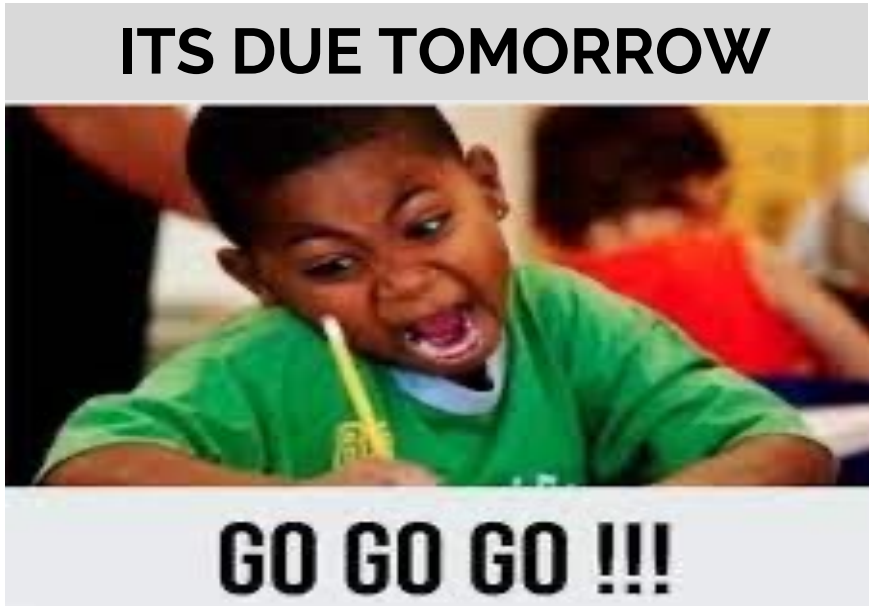
Who cares to get an A

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

Lecture Format

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
- 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

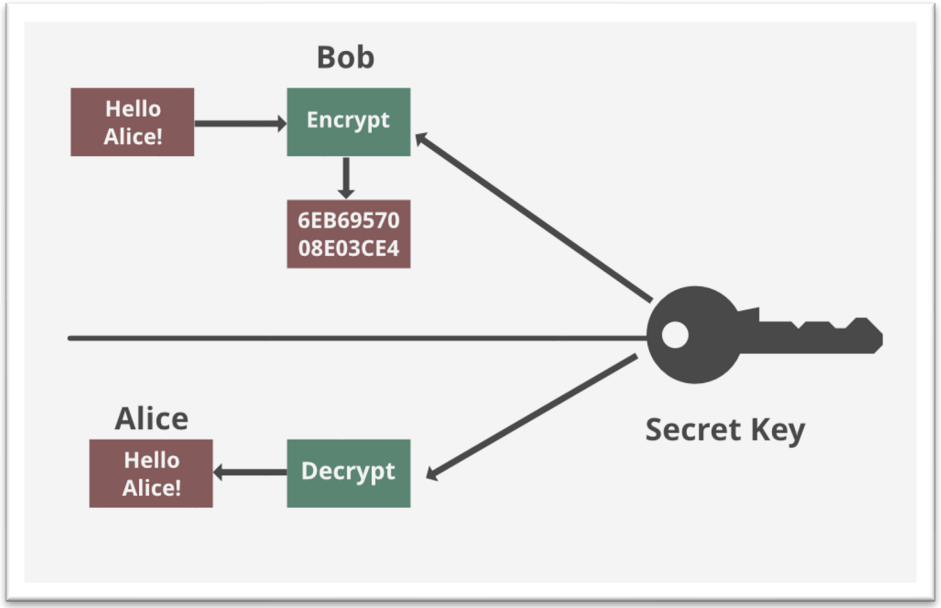
- Ensuring too much **C**, → A will suffer.
- Ensuring too much **I**, → A will suffer.
- Ensuring too much **A**, → both C & I will suffe

CIA Triad: Confidentiality

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

Measures to achieve Confidentiality:

- **Encryption:** (AES, RSA)
- **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:

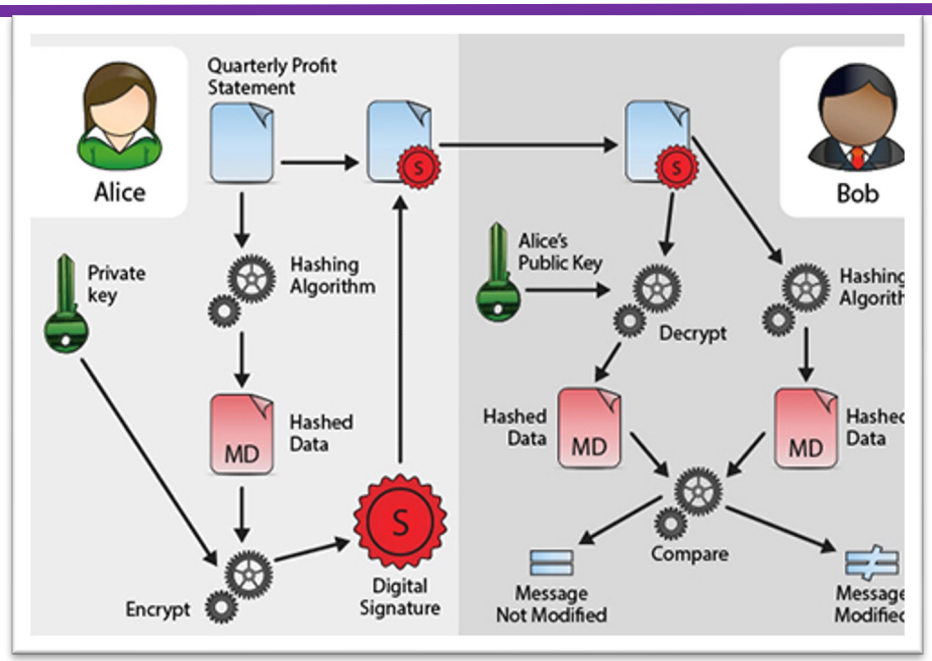
- Social engineering/Phishing.
- Unauthorized NW access & Port scanning.
- Eavesdropping and MitM attacks.
- Password dump stealing and attack on your encryption (cryptoanalysis)
- Authorized users may abuse their access to retrieve sensitive data.

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. (PGP, RSA)
- **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)



Threats:

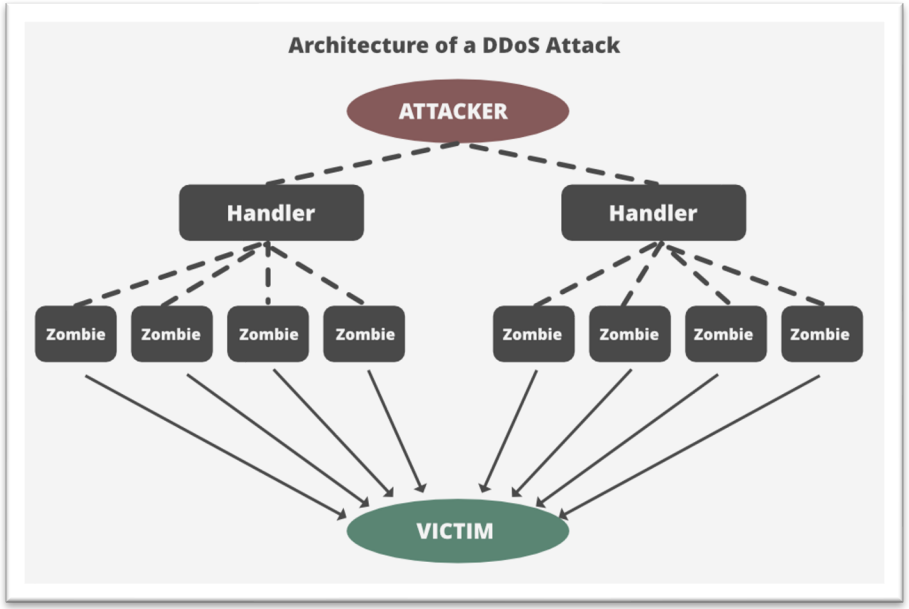
- MitM for tempering
- Data corruption by malware
- Malicious code injection
- Ransomware
- Deleting/altering DB records by SQLi
- DNS Spoofing / Cache Poisoning
- Replay attacks

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:

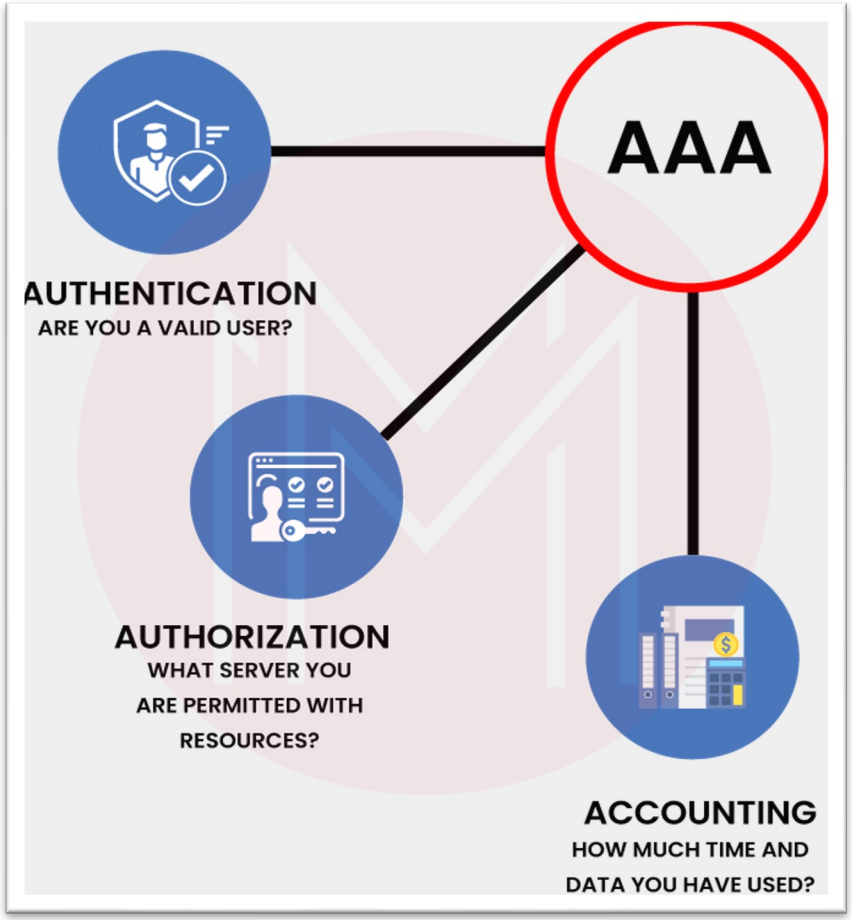
- DDoS
- Ransomware (for availability).
- H/W or S/W Failure.
- Natural disasters.
- Sabotage / Insider attacks.
- Resource exhaustion attacks.
- Logic bombs.

AAA Architecture

- **Authentication** is the process of verifying the identity of a user or system trying to access a resource. (Multi-Factor)
  - 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

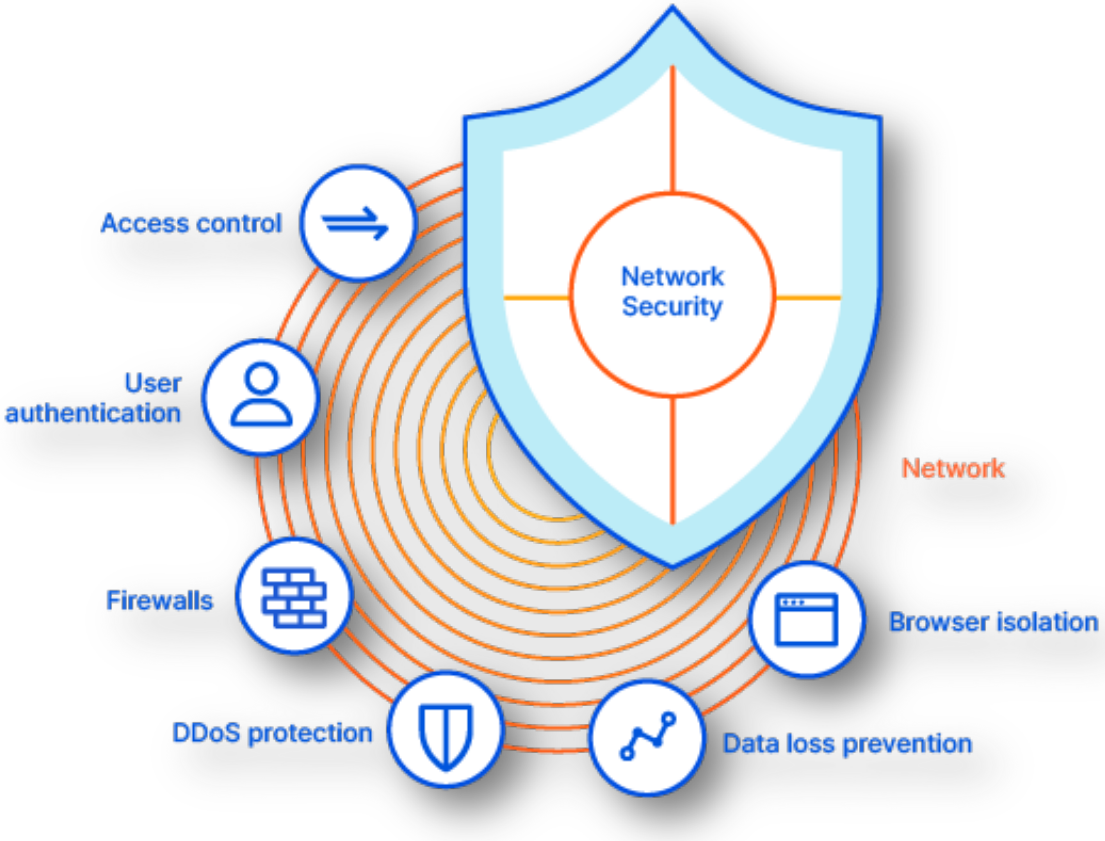
Major Categories

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.

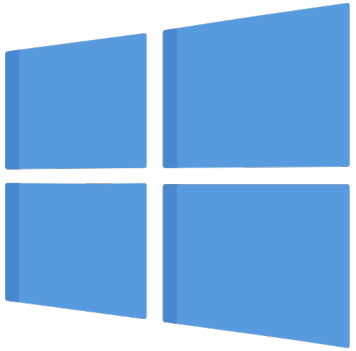
Network Security

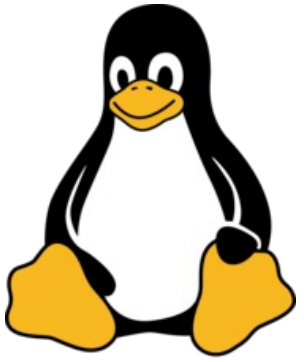
- **Network Security** is the practice of protecting the confidentiality, integrity, and availability of data and resources as they are transmitted or accessed across a network.
- It involves a combination of policies, procedures and technologies to prevent unauthorized access, misuse, modification, 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.



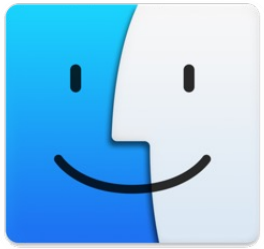
Operating System Security

- **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





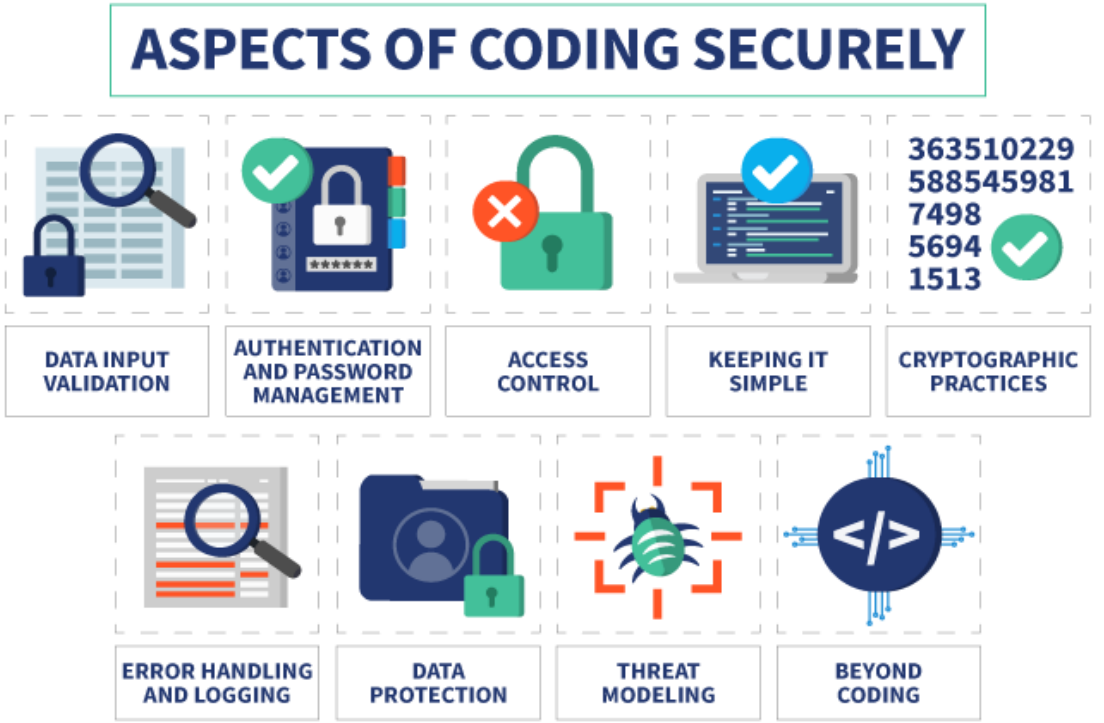
Linux™



MacOS

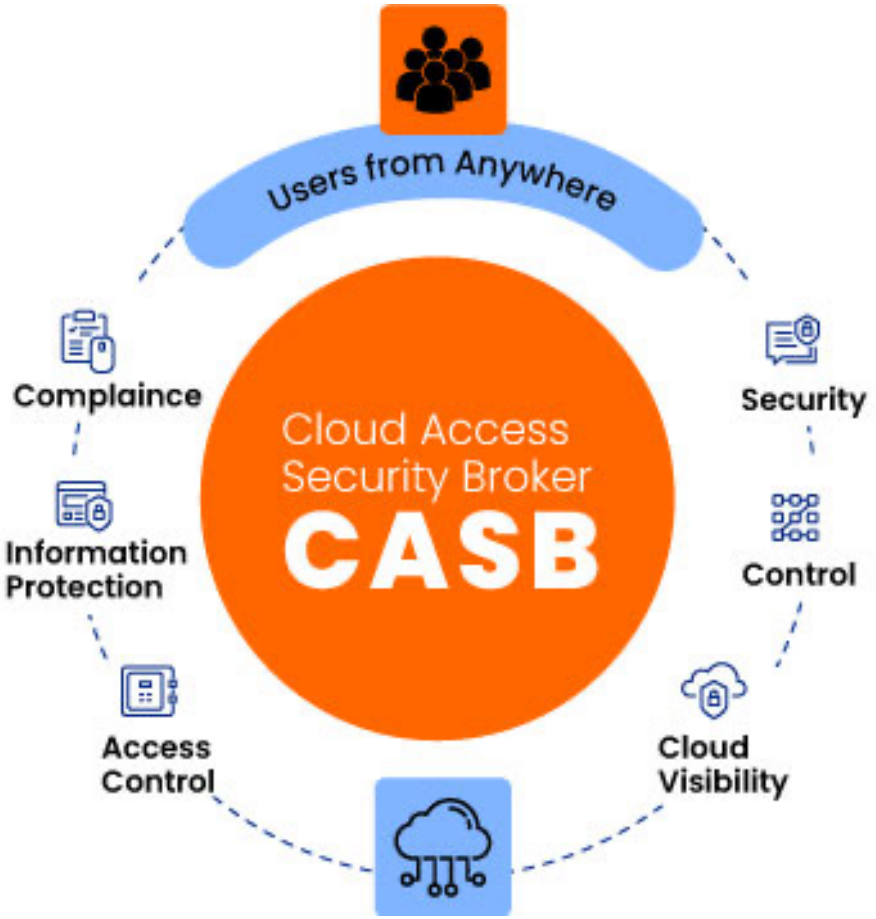
Application Security

- **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

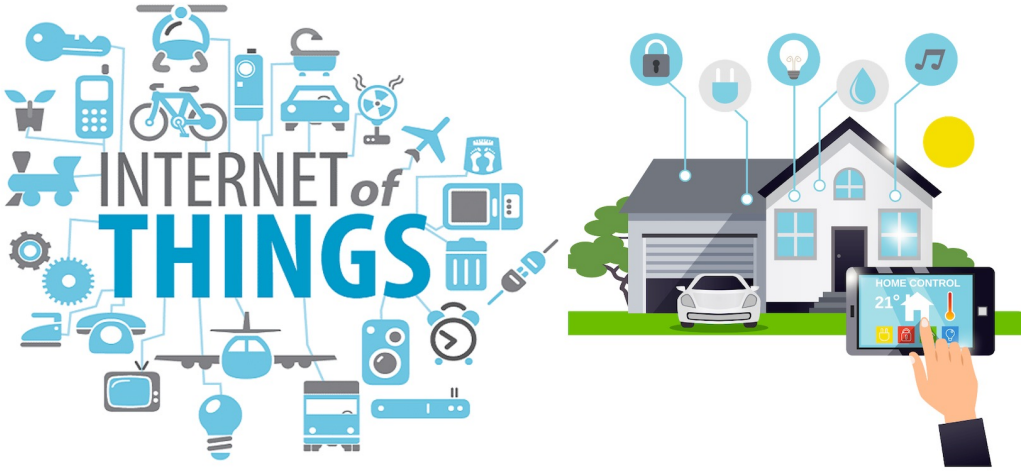
- **Cloud security** is the practice of safeguarding data, applications, and services hosted in cloud environments from unauthorized access, data breaches, and other cyber threats.
- Cloud security measures include encryption, identity and access management (IAM), network security, data loss prevention (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

- **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.

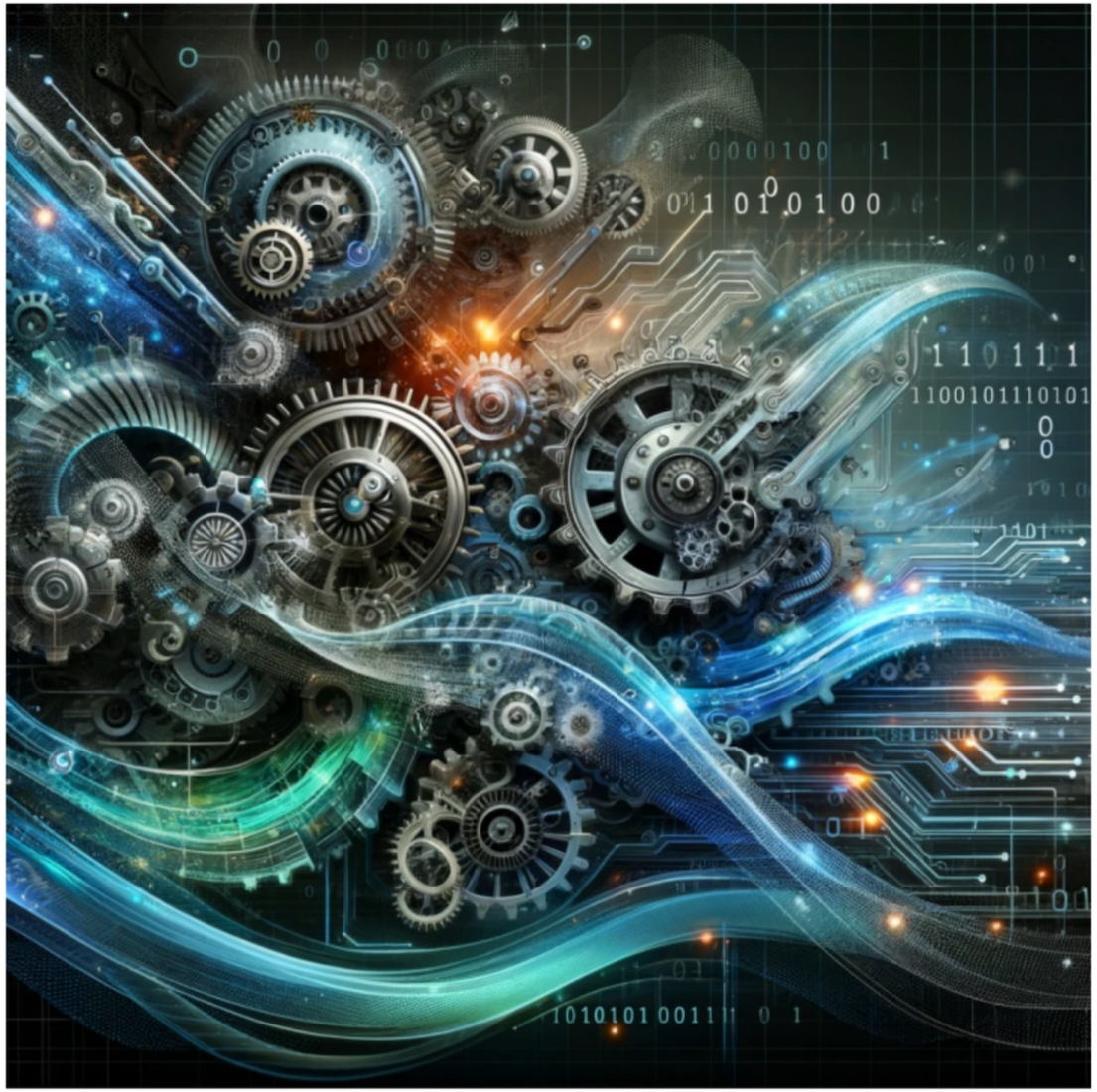
Collection of interconnected devices that communicate and transfer data through the Internet



The Future: Security of Gen-AI Models

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"

LLM Prompt Injection

- **Prompt Injection** attack is a new attack technique specific to LLMs that enables attackers to manipulate the output of the model by using carefully crafted prompts that make the model ignore previous instructions or perform unintended actions.
- **Potential threats:**
  - Access to sensitive data from databases.
  - Stealing application prompts.
  - Executing unauthorized LLM functions.
- **Examples of attacks:**
  - Bypassing content filters using specific language patterns or tokens.
  - Crafting the prompt to trick the LLM into revealing sensitive info, such as user credentials, internal system details, by making the model think that the request is legitimate.

LLM Jail Breaking

- A **Jail Break** attack on a Large Language Model (LLM) refers to manipulating or hijacking the initial prompt of an LLM to direct it towards malicious or unintended outputs.
- **Prompt Level Jail Breaks** involve semantically meaningful deception and social engineering to force LLMs to generate hostile content. They are interpretable but requires considerable human effort, limiting their scalability.
- **Token-Level Jail Breaks** manipulate LLMs outputs by optimizing the prompt through the addition of arbitrary tokens. This method can be automated using algorithmic tools but often results in uninterpretable jail breaks due to the unintelligible tokens added to the prompt.

History of Cyber Attacks

Famous Cyber Attacks

Morris Worm (1988): Often considered one of the first major worms, the Morris Worm was created by Robert Tappan Morris. It was designed to exploit vulnerabilities in Unix systems and spread across the internet.

- **Impact:** 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 macro virus that spread through Microsoft Word documents. It was created by David L. Smith and was distributed via email.

- **Impact**: It infected hundreds of thousands of computers, causing email systems to become overloaded and leading to significant financial losses.

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.

- **Impact:** It caused widespread damage, affecting millions of computers globally, and led to billions of dollars in damages.

Famous Cyber Attacks (Cont..)

SQL Slammer (2003): The SQL Slammer worm targeted vulnerabilities in Microsoft SQL Server and spread rapidly across the internet.

- **Impact**: It caused significant network congestion and service disruptions, affecting a wide range of services including emergency response systems.

Stuxnet (2010): Stuxnet was a sophisticated worm believed to be created by the U.S. and Israeli governments to target Iran's nuclear facilities. It was designed to sabotage uranium enrichment by causing centrifuges to malfunction.

- **Impact**: It is considered one of the first known cyber weapons and demonstrated the potential for cyber-attacks to cause physical damage.

Sony PlayStation Network Hack (2011): Attackers compromised Sony's PlayStation Network, gaining access to personal information of around 77 million users.

- **Impact**: The breach led to the suspension of the network, significant financial losses, and a major hit to Sony's reputation.

Famous Cyber Attacks (Cont..)

Target Data Breach (2013): Cyber attackers gained access to Target's network through a third-party vendor and stole credit card information and personal details of approximately 40 million customers.

- **Impact**: The breach resulted in substantial financial losses for Target, legal costs, and a decline in customer trust.

WannaCry Ransomware Attack (2017): WannaCry ransomware attacked computers worldwide by exploiting a vulnerability in Microsoft Windows. It encrypted users' files and demanded ransom payments in Bitcoin.

- **Impact**: The attack affected more than 200,000 computers across 150 countries, disrupting services in hospitals, businesses, and government agencies.

SolarWinds Hack (2020): The SolarWinds cyber attack involved a sophisticated supply chain attack that compromised the Orion software used by thousands of organizations. The attackers, believed to be state-sponsored, inserted malicious code into updates of the software.

- **Impact**: The breach affected numerous high-profile organizations, including U.S. government agencies, and highlighted vulnerabilities in supply chain security.

Cyber Attacks in 2024

Phishing and Social Engineering Attacks

- **Twitter Employee Breach (2020)**: Attackers used social engineering to gain access to Twitter's internal tools, leading to a high-profile phishing attack on several prominent accounts, including those of Elon Musk and Barack Obama.
  - **Impact**: The attack resulted in the posting of fraudulent messages and demonstrated the effectiveness of social engineering tactics. It emphasized the importance of training employees to recognize and respond to phishing attempts.

Cryptocurrency Theft

- **BitMart Hack (2021)**: BitMart, a cryptocurrency exchange, suffered a hack resulting in the theft of approximately $150 million worth of cryptocurrencies.
  - **Impact**: The theft affected investors and users of the exchange, causing financial losses and impacting confidence in cryptocurrency platforms. It highlighted the need for robust security practices in handling digital assets.

Cyber Attacks in 2024 (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.
  - **Impact**: 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.

Cyber Attacks in 2024 (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

Impacts of Cyber Attacks

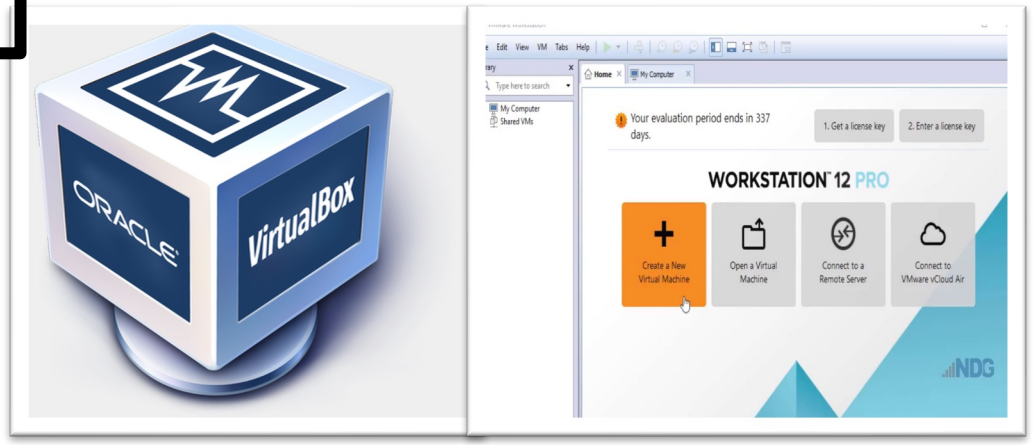
- **Financial Losses**: Direct financial losses due to theft, ransom payments, and fraud, as well as indirect costs from downtime, recovery efforts, and legal fees.
- **Operational Disruption**: Interruption of business operations, affecting productivity and service delivery. Critical infrastructure 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.

Course Contents

Overview of the Course

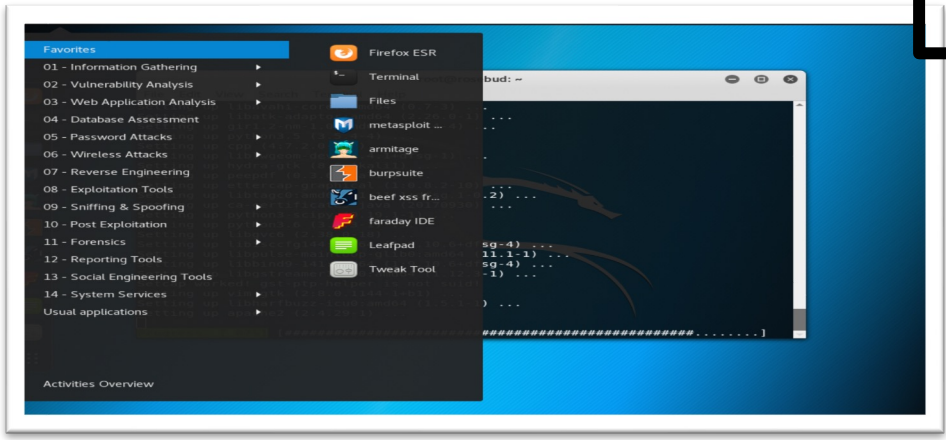
M1

Overview and pre-requisites



M2

NW Attacks and Penetration Testing



M3

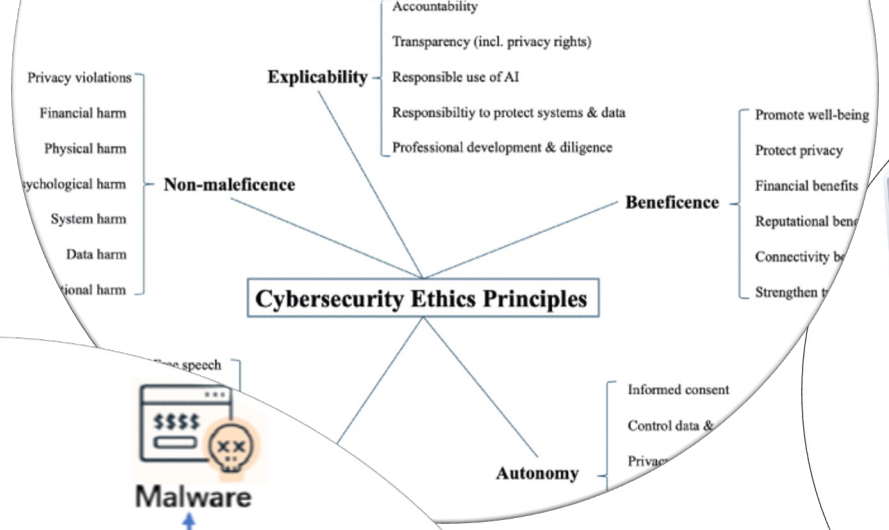
Vulnerability Research & Malware Development

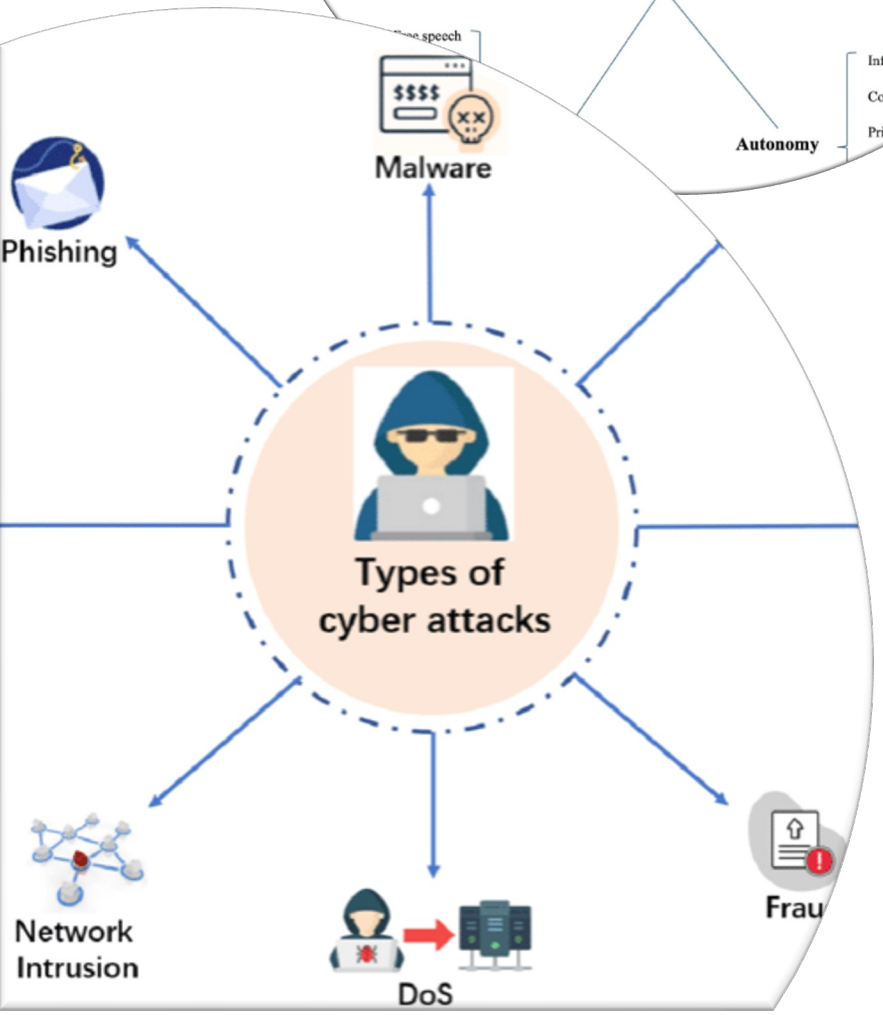
Malware Analysis

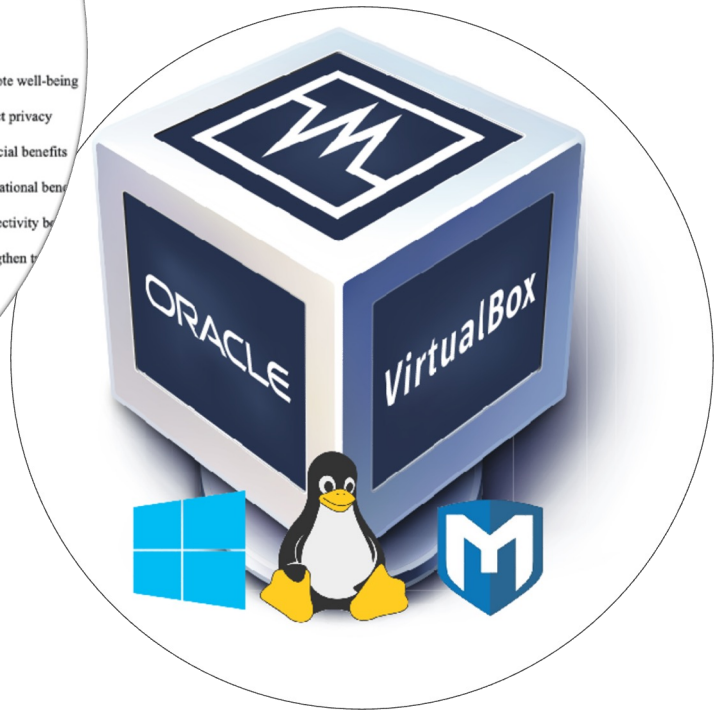
M4

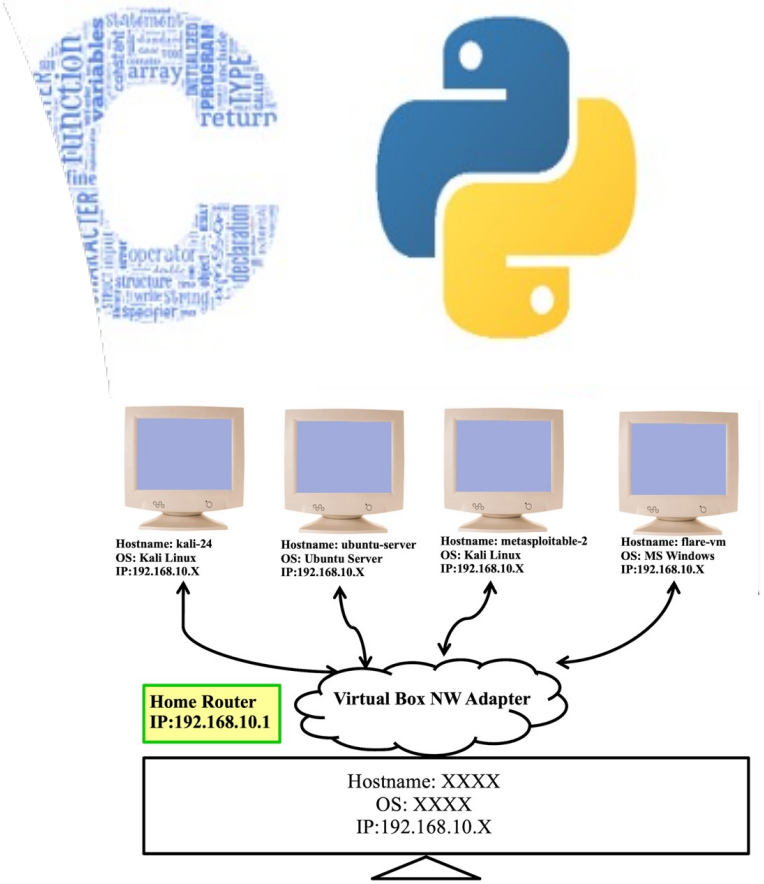
Instructor(s): Muhammad Rauf Butt, Muhammad Arif Butt, PhD

Module 01: Overview and Prerequisites



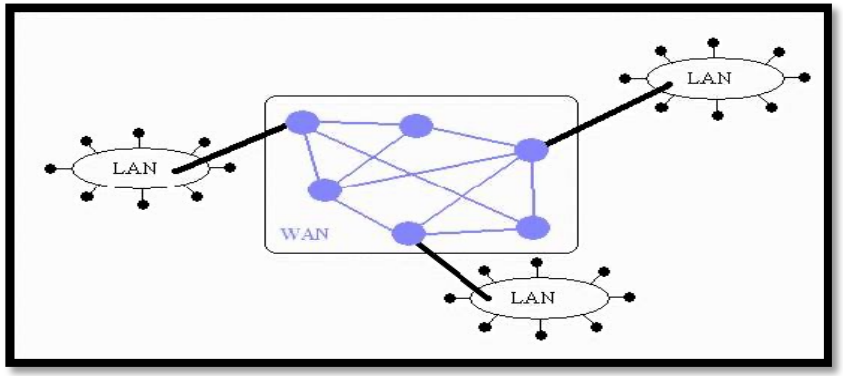


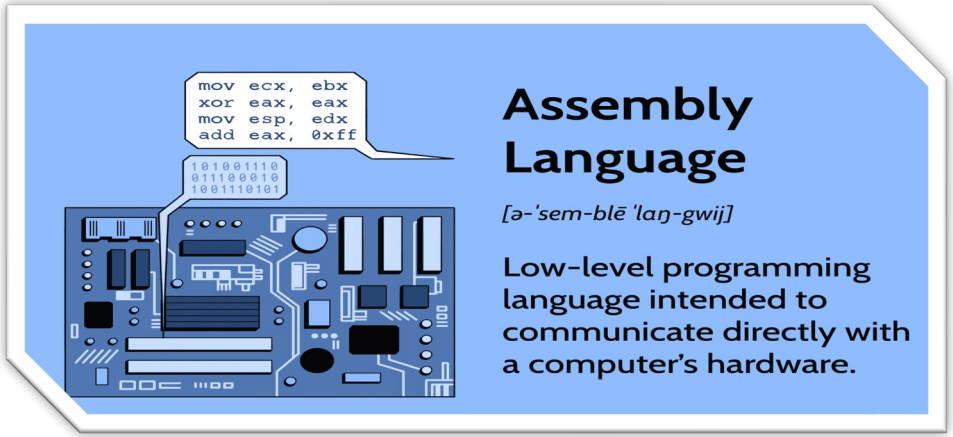


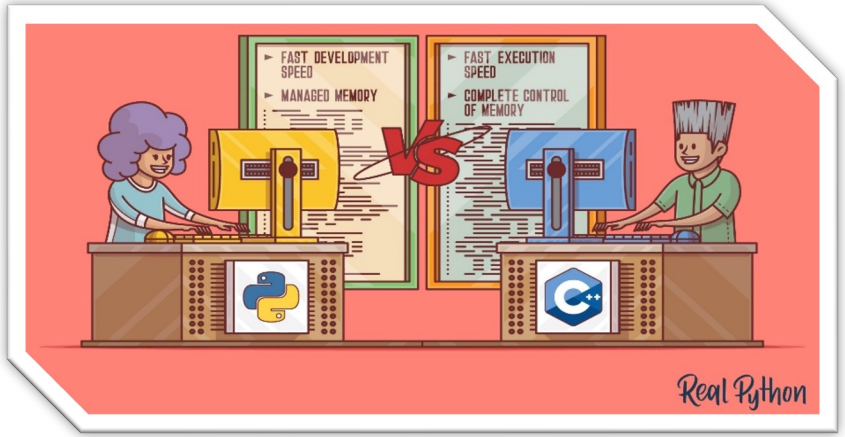


Module 1: Overview and Prerequisites

Prerequisites of the Course







Module2:
NW Attacks & Penetration Testing

Module 2: NW Attacks & PT

Reconnaissance and Information Gathering

Scanning and Vulnerability Analysis

Exploitation and Gaining Access

Privilege Escalation

Maintaining Access and Persistent Mechanisms

Covering Tracks

Phase 1: Reconnaissance and Info Gathering

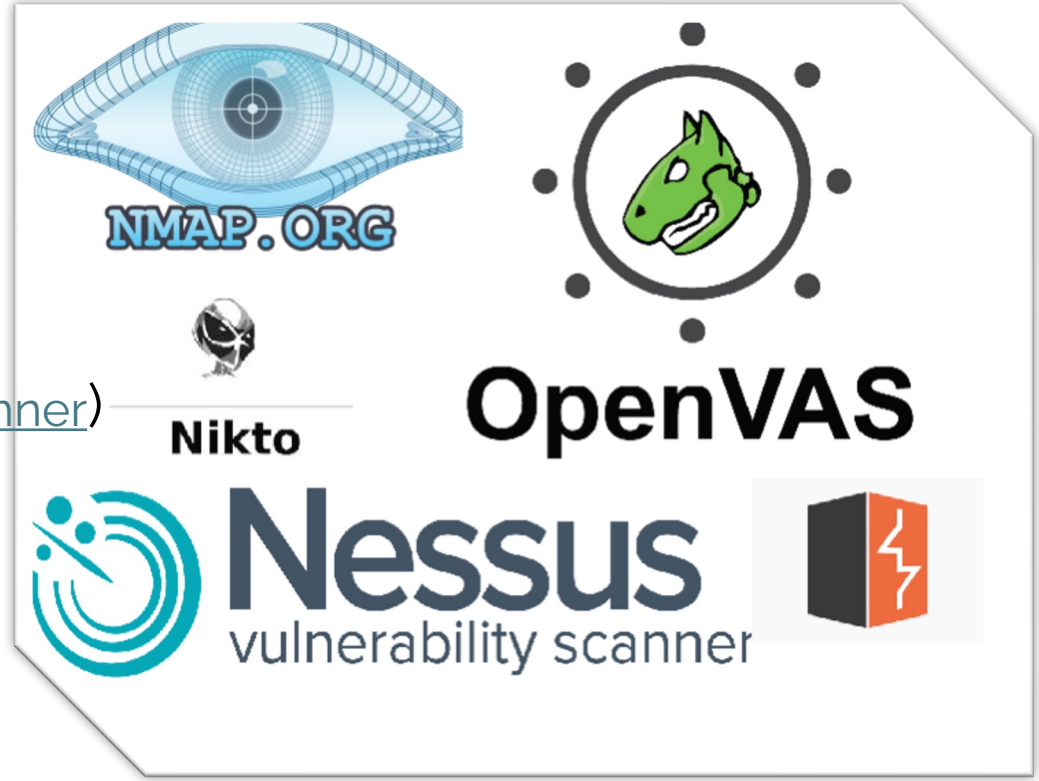
Reconnaissance and information gathering is the initial step in the penetration testing lifecycle. This phase involves collecting as much public information as possible about the target organization, systems, networks, applications and employees to identify potential vulnerabilities and formulate a strategy for further testing.

- Netdiscover (https://github.com/netdiscover-scanner/netdiscover)
- Whatweb (https://whatweb.net/)
- Nslookup (https://www.nslookup.io/)
- Whois (https://www.whois.com/)
- Ipinfo.info (https://ipinfo.info/)
- TheHarvester (https://github.com/laramies/theHarvester)
- Hunter.io (https://hunter.io/)
- Sherlock (https://github.com/sherlock-project/sherlock)
- Google Dorking
- OSINT (https://osintframework.com)

Phase 2: Scanning and Vulnerability Analysis

Scanning and vulnerability analysis involves directly interacting with the target network, hosts, ports, employees and so on to collect data. This can include open ports, services, vulnerabilities and other critical details about the target. The tools used in this phase often leaves traces or logs on the target systems, making it more detectable.

- Nmap (https://nmap.org/download)
- Searchsploit (https://www.exploit-db.com/searchsploit)
- Nessus (https://www.tenable.com/products/nessus)
- OpenVAS (https://github.com/greenbone/openvas-scanner)
- Nikto (https://github.com/sullo/nikto)
- Burpsuite (https://portswigger.net/burp)



Phase 3: Exploitation and Gaining Access

In this phase, the pentester take the advantage of the identified weaknesses like vulnerable applications and default configurations/credentials running on the target machine to gain unauthorized entry into the target system. Other than exploiting the known vulnerabilities, the pentester may use brute force, social engineering and phishing attacks to gain the initial entry to the target system.

- MSF (https://www.metasploit.com/download)
- Exploit DB (https://www.exploit-db.com/)
- SQLmap (https://sqlmap.org/)
- Cobalt Strike (https://www.cobaltstrike.com/)

- Social Engineering Toolkit (https://github.com/trustedsec/social-engineer-toolkit)
- BeEF (Browser Exploitation Framework) (https://beefproject.com/)
- PowerSploit (https://github.com/PowerShellMafia/PowerSploit)

Phase 4: Privilege Escalation

After gaining initial access to the target machine, you may find that your session has only limited user rights. This severely limits the actions that one can perform on the remote systems such as dumping passwords, manipulating registry, and installing backdoors or keyloggers. So Privilege Escalation is a critical phase in penetration testing where the tester attempts to gain elevated access rights beyond initial compromises.

- MSF (msfconsole, msfvenom)
(https://www.metasploit.com/download)

- Privilege Escalation Scripts(e.g., powersploit, LinEnum)
(https://github.com/PowerShellMafia/PowerSploit)

- Password Cracking Tools (e.g., John the Ripper, Hashcat)
(https://github.com/openwall/john)

- LinPEAS (Linux Privilege Escalation Awesome Script)
(https://github.com/peass-ng/PEASS-ng)

Phase 5: Maintaining Access and Persistent Mechanisms

Maintaining access and persistent mechanisms are crucial in penetration testing for ensuring that an attacker can retain control over a compromised system and re-access it even after initial detection or remediation efforts. Some common techniques to maintain access are installing a backdoor, keylogger or a RAT on the target system

- Installing backdoors
- Creating new accounts
- Persistence mechanisms
- MSF (https://www.metasploit.com/download)
- powersploit (https://github.com/PowerShellMafia/PowerSploit)
- BeEF (Browser Exploitation Framework) (https://beefproject.com/)
- Cobalt Strike (https://www.cobaltstrike.com/)

Phase 6: Covering Tracks

Covering tracks is important in penetration testing as it demonstrates the methods attackers use to evade detection and hide their activities. To do this the attacker delete or modifies log entries, or do log spoofing (creating false trails). He may also clear command history, perform timestomping, and erase evidence of persistence mechanisms.

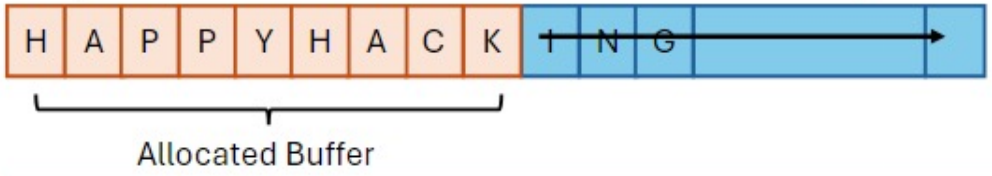
- Log cleaning scripts
- Secure file deletion tools (shred, sdelete)
- Rootkits that hide files and processes
- Modifying timestamps of files to avoid detection
- MSF (https://www.metasploit.com/download)
- Sysinternals Suite (https://learn.microsoft.com/en-us/sysinternals/downloads/)

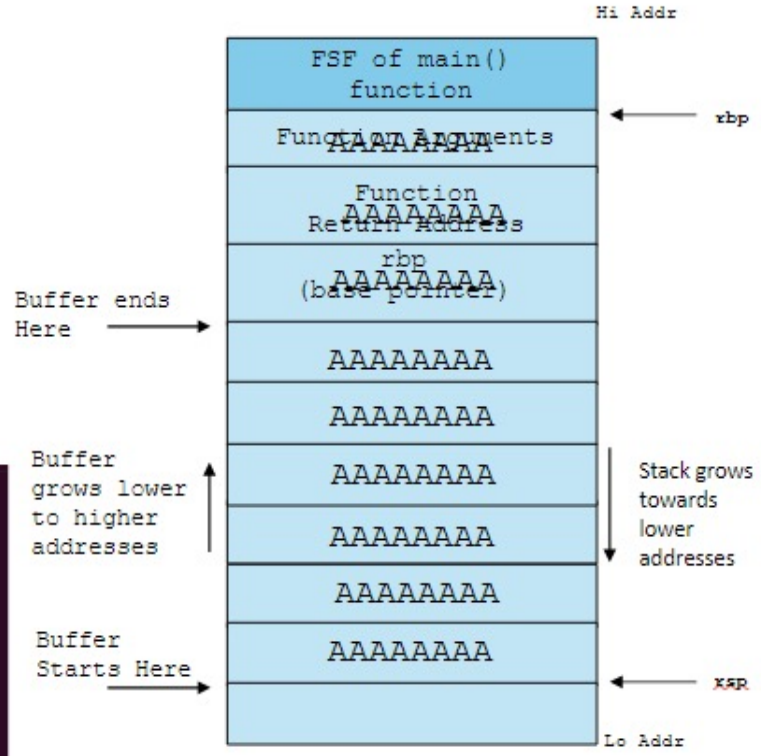
Module3: Vulnerability Research and Malware Development

Module 3: Vulnerability Research

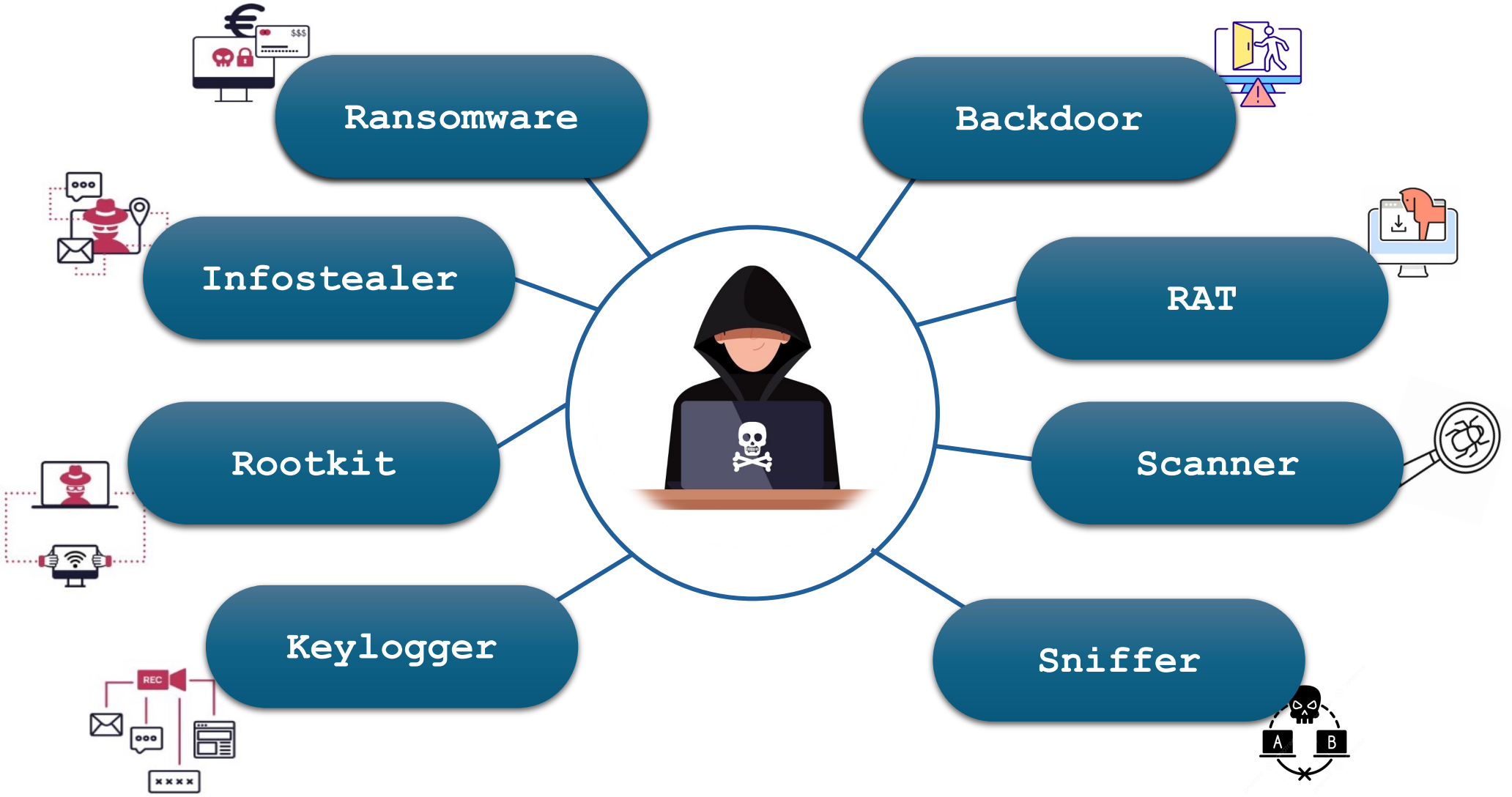
```
1. void copy_buff ( char * buf ){
2.     char temp_buff [9];
3.     strcpy( temp_buff, buf );}

4. void main (){
5.     copy_buff (HAPPYHACKING);}
```





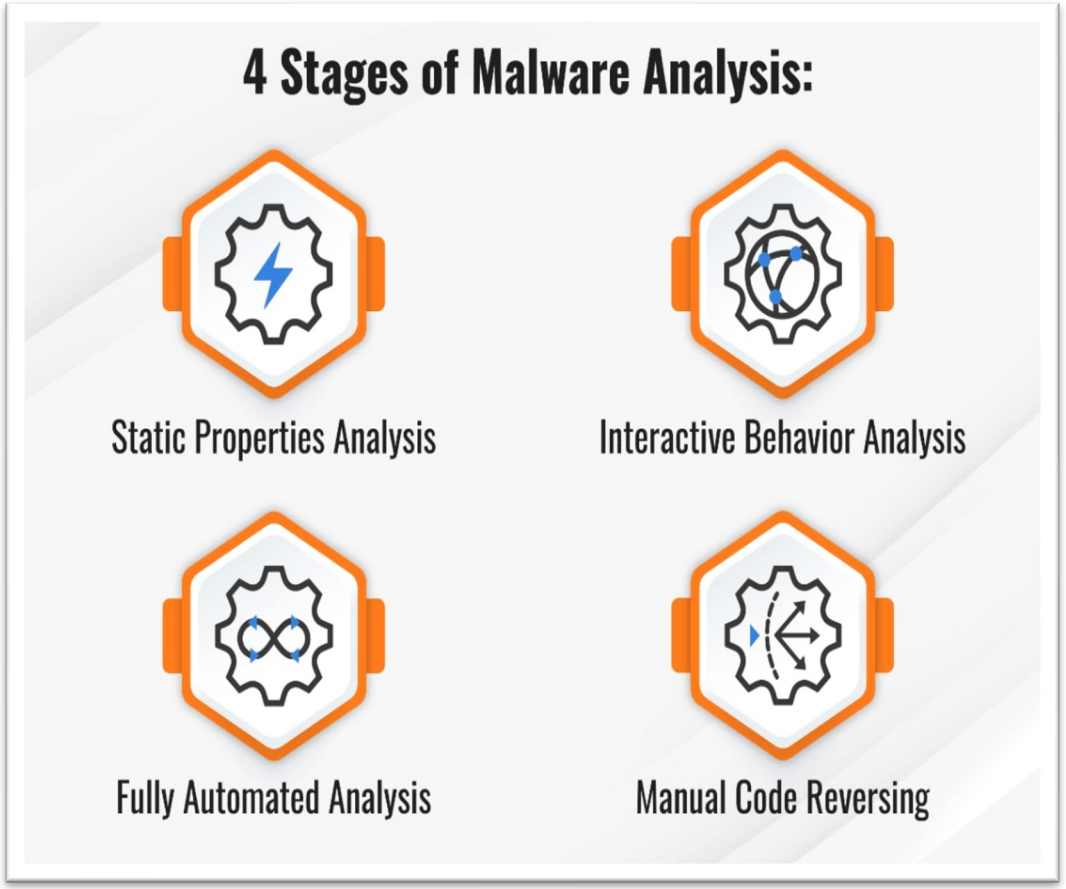
Module 3: Malware Development



Module 4: Malware Analysis

Module 4: Malware 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



Module 4: Malware Analysis: Detection

- **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.

Scope of Cyber Security in Pakistan in 2024

Cyber Security in Pakistan

- **NADRA:** Offers various services such as CNIC applications, registration, and verification (https://www.nadra.gov.pk/)
- **Pakistan Citizen Portal:** Offering a centralized platform for complaints, service requests, and feedback (https://web.citizenportal.gov.pk/)
- **e-Sahulat** Offers a range of services designed to facilitate transactions and interactions between citizens and government institutions (https://e-sahulat.nadra.gov.pk/)
- **Punjab Transport Department:** Facilitates vehicle registration, driving license applications, and transport-related inquiries (https://punjabtransport.org/)
- **PTA Device Verification System DIRBS:** Offering services such as device registration, verification, and reporting of lost or stolen devices (https://dirbs.pta.gov.pk/)
- **ePay** enables users to make payments for a variety of services online, including utility bills, government fees, and other financial transactions (https://epay.punjab.gov.pk/)

Happy Hacking