CyberSecurity
CSCS
Introduction

Today's Agenda

- A basic intro of
  - —Hacker and its types
  - —Vulnerability
  - —Cyber Attack
  - —Malicious Software and its types
  - —Anonymity
  - —Deep Web
  - —Dark Web
  - —Penetration Testing Life Cycle

Compliance to HEC academic standards

- This course has been designed according to the HEC BS Revised Curriculum for Computing Disciplines (CS, SE, IT, DS, CE, AI and Cyber Security), dated February 16, 2023
- Revised Curriculum – Computing Disciplines of HEC can be found at following link:

https://nceac.org.pk/Documents/Curriculums/BS%20Curriculm%20Computing%20Disciplines-2023.pdf

Course Overview

- Overview and pre-requisite
- Network Attacks and Penetration Testing
- Vulnerability Research and Exploit Development
- Malware Analysis (Optional)

```
fffdd38|+0x0000: "jaaaaaaa"    ← $rsp
fffdd40|+0x0008: 0x00007fffffffde00  →  0x0000000000000000
fffdd48|+0x0010: 0x00000001f7fca000
fffdd50|+0x0018: 0x0000000000400698  →   push rbp
fffdd58|+0x0020: 0x00007fffffffe199  →  0x480d4cb2d09d0269
fffdd60|+0x0028: 0x0000000000400720  →   push r15
fffdd68|+0x0030: 0x1aedd050d0c1aeaf
fffdd70|+0x0038: 0x00000000004005a0  →   xor ebp, ebp

070b                    call   0x400580 <gets@plt>
0710                    mov    eax, 0x0
0715                    leave
00716                   ret
not disassemble from $PC

d 1, Name: "pwn1", stopped 0x400716 in ?? (), reason: SIGSEG

0x400716 → ret

  pattern search jaaa
Searching 'jaaa'
] Found at offset 69 (little-endian search) likely
+] Found at offset 72 (big-endian search)
gef➤
```

FEW BASIC TERMS USED IN THE FIELD OF CYBER SECURITY

Hacker

- Person skilled in computer systems and programming who uses their expertise to explore, understand, and manipulate technology.

White Hat Hacker

- Intentions:
  - —Positive, with the aim of improving security.
- Activities:
  - —Conduct authorized penetration testing, vulnerability assessments, and security audits.
- Example:
  - —Security professionals who work for companies to secure their networks.

Black Hat Hacker

- Intentions:
  - —Malicious, often motivated by personal gain, causing harm, or disrupting systems.
- Activities:
  - —Unauthorized access to systems, data theft, malware distribution, and other illegal activities.
- Example:
  - —Cybercriminals who perform malicious activities like stealing credit card information or deploy ransomware etc.

Gray Hat Hacker

- Intentions:
  - —Ambiguous;
  - —they may break into systems without permission but without malicious intent.
- Activities:
  - —Often exploit vulnerabilities and then inform the system owner, sometimes expecting a reward.
- Example:
  - —Hackers who find and disclose vulnerabilities in software without explicit permission but without harmful intent.

Vulnerability

- A weakness or flaw in a
  —system,
  —application,
  —network, or
  —device
- Can be exploited to gain
  —unauthorized access,
  —cause damage, or
  —perform unauthorized actions.

Vulnerability

- Vulnerabilities can arise from various sources, including:
  - —software bugs
  - —Misconfigurations
  - —Design flaws
  - —Human errors

Exploit

- An exploit is a program, or piece of code
- Designed to find and take advantage of a security flaw or vulnerability in an application or computer system
- An exploit is not malware itself
- Rather it is a method to deliver malware.

Payload

- Payload is a piece of malicious code
- Designed to execute a specific action on a target system.
- This code can take various forms, such as a virus, worm, or Trojan
- Delivered to the target system through a vulnerability or security flaw.
- Once the payload is executed, it can perform a wide range of actions, such as stealing sensitive information, disrupting system operations, or taking control of the target system.

Vulnerability

Vs

Exploit

Vs

Payload

Cyber Attack

- A cyber-attack is a malicious attempt by individuals or groups to compromise, or damage
  - —computer systems,
  - —networks, or
  - —information.
- Some of the impacts of cyber-attacks have been listed below:
  - —Financial Loss
  - —Reputation Damage
  - —Data Breach
  - —Operational Disruption

Malicious Software -- Malware

- Virus
  - —A virus is a piece of code that inserts itself (or is inserted) into an application and executes when the app is run.
  - —Once inside a network, a virus may be used to steal sensitive data, launch DDoS attacks or conduct ransomware attacks.

Malicious Software -- Malware

- Worm
  - —Worms target vulnerabilities in operating systems to install themselves into networks.
  - — They may gain access in several ways:
    - through backdoors built into software
    - through unintentional software vulnerabilities
    - through flash drives

Malicious Software -- Malware

- Worm Vs Virus
  - —Worms
    - Standalone, and therefore donot need host program for execution
  - —Virus
    - Attaches itself to a host file
    - Remains dormant until host is executed

Malicious Software -- Malware

- Trojan Horse
  - — Disguises itself as legitimate software or files to deceive users into executing or installing it on their systems.
  - —Need some form of user interaction to download and install these on the system.
  - —These are not self replicating.

Malicious Software -- Malware

- Ransomware
  - —Designed to encrypt files on a victim's computer or entire network, rendering them inaccessible until a ransom is paid.
  - —It is a form of extortion where attackers demand payment in exchange for decrypting the files and restoring access to the affected system.

Malicious Software -- Malware

- Spyware
  - —Designed to secretly gather information about a user's activities on their computer or device without their knowledge or consent.
  - —The purpose of spyware ranges from tracking browsing habits for advertising purposes to stealing sensitive information such as passwords, credit card numbers, and personal data.
  - —For example, installing a keylogger after gaining access to a system.

Malicious Software -- Malware

- Adware
  - —Display advertisements on a user's device, often in a disruptive or intrusive manner.
  - —While not always malicious, adware can become a significant nuisance, affecting user experience and system performance.
  - —Adware is often bundled with free software and gets installed without the user's full awareness or consent.

Malicious Software -- Malware

- Rootkit
  - —A rootkit is designed primarily for concealment.
  - — It hides the presence of other malware or malicious activity on a system.
  - —By doing so, it allows an attacker to maintain control over a system without being detected.
  - —Rootkits modify the operating system or use other techniques to hide files, processes, network connections, and system logs.
  - —They can operate at different levels, such as user mode, kernel mode.

Malicious Software -- Malware

- Botnets
  - —A botnet is a network of compromised computers, known as "bots" or "zombies," that are controlled remotely by an attacker, often called a "botmaster" or "bot herder."
  - —Botnets are typically used to conduct large-scale cyber-attacks and other malicious activities.

Malicious Software -- Malware

- Fileless Malware
  - —Conventional malware relies on executable files or scripts stored on the disk.
  - —Fileless malware executes its payload directly in the system's memory (RAM).
  - —It may also use legitimate system tools like pwer shell, system scripts, MS Office macros.

Achieving Anonymity

- Anonymity refers to the state of being unidentified or untraceable within a digital environment.
- This concept is often associated with privacy and security measures designed to protect an individual's identity and activities from being discovered or tracked by others.

Achieving Anonymity

- Connecting to the internet can be done in various ways, each offering different levels of privacy, security, and complexity.
  - Local area network
  - Using a Proxy Server
  - Using VPN
  - Using some browser like
    - Tor Browsers like
      - DuckDuckGo Browser
      - Brave Browser

The Deep Web

- The deep web refers to all parts of the internet that are not indexed by traditional search engines like Google, Bing, or Yahoo.
- This means that these pages cannot be found through standard search queries.
- Examples:
  - —Academic databases like JSTOR or IEEE Xplore.
  - —Government databases and resources not intended for public access.
  - —Corporate intranets and internal systems.

The Dark Web

- The dark web is a small portion of the deep web that has been intentionally hidden and is inaccessible through standard web browsers.
- It requires specific software, configurations, or authorization to access.
- Access:
  - —Requires special software like Tor (The Onion Router) or I2P (Invisible Internet Project) to access.
  - —These tools anonymize user activity by routing traffic through multiple nodes.

The Dark Web

- Purpose:
  - —Provides a platform for anonymous communication and transactions.
  - —It is used by those seeking privacy and anonymity, such as political activists, journalists, and individuals living under oppressive regimes.
  - —It is also exploited by criminals for illicit activities.

LIFE CYCLE OF PENETRATION TESTING

Pen Testing

- A systematic process used to identify and exploit vulnerabilities in a system, network, or application to understand the security risks.
- The life cycle of a pen test typically follows a series of phases designed to mimic the steps an attacker might take to compromise a target.
- An overview of the pen testing life cycle with the key phases is discussed in upcoming slides.

Pen Testing Phases

- Information Gathering
- Scanning
- Gaining Access
- Privilege Escalation
- Maintaining Access
- Covering Tracks

Reconnaissance and Information Gathering

- Objective:
  - —To collect as much information as possible about the target to identify potential vulnerabilities.
- Activities:
  - —Passive Reconnaissance:
    - Gathering information without direct interaction with the target, such as using public sources (websites, social media, WHOIS databases).
  - —Active Reconnaissance:
    - Directly interacting with the target to gather information, such as pinging the network, querying DNS records, or using tools like Nmap for network mapping.

Reconnaissance and Information Gathering

- Tools:
  - —Ping
  - —Nslookup
  - —Whatweb
  - —TheHarvestor
  - —Reverse IP Lookup
  - —Hunter.io

Scanning

- Objective:
  - To identify open ports, services, and vulnerabilities in the target systems.
- Activities:
  - Port Scanning:
    - Identifying open ports and the services running on them.
  - Vulnerability Scanning:
    - Identifying known vulnerabilities in the target's services and applications.
  - Network Scanning:
    - Mapping the network to identify active devices and their IP addresses.

Scanning

- Tools and Techniques:
  - —Nmap
  - —Nessus
  - —OpenVAS
  - —Nikto
  - —Burp Suite

Gaining Access

- Objective:
  - —To exploit identified vulnerabilities to gain unauthorized access to the target systems.
- Activities:
  - —Exploiting Vulnerabilities:
    - Using the information gathered to exploit vulnerabilities in services, applications, or network configurations.
  - —Brute Force Attacks:
    - Attempting to gain access by guessing passwords or using automated tools to try multiple combinations.

Gaining Access

- Tools and Techniques:
  - —Metasploit Framework
  - —Exploit databases (e.g., Exploit-DB)
  - —Hydra (for brute force attacks)
  - —SQL injection
  - —Buffer overflow exploits

Privilege Escalation

- Objective:
  - —To gain higher levels of access within the target system to fully control the environment.
- Activities:
  - —Local Exploits:
    - Exploiting local vulnerabilities to elevate privileges.
  - —Password Cracking:
    - Cracking passwords of higher-privileged accounts.
  - —Misconfigurations:
    - Exploiting misconfigurations that allow privilege escalation.

Privilege Escalation

- Tools and Techniques:
  - —Metasploit
  - —Privilege escalation scripts (e.g., PowerSploit, LinEnum)
  - —Password cracking tools (e.g., John the Ripper, Hashcat)

Maintaining Access

- Objective:
  - —To ensure continued access to the target system, even if initial vulnerabilities are patched.
- Activities:
  - —Installing Backdoors:
    - Deploying backdoors or rootkits to maintain access.
  - —Creating Accounts:
    - Creating new user accounts with administrative privileges.
  - —Persistence Mechanisms:
    - Setting up persistence mechanisms that re-establish access after reboots.

Maintaining Access

- Tools and Techniques:
  - —Netcat
  - —Metasploit payloads
  - —Creating scheduled tasks or cron jobs
  - —Modifying startup scripts

Covering Tracks

- Objective:
  - To remove any evidence of the penetration test to avoid detection by the target's security measures.
- Activities:
  - Log Clearing:
    - Deleting or modifying system logs to remove traces of the attack.
  - File Removal:
    - Removing any files or tools that were uploaded during the test.
  - Hiding Evidence:
    - Using tools and techniques to conceal the presence of malware or changes made to the system.

Covering Tracks

- Tools and Techniques:
  —Log-cleaning scripts
  —Secure file deletion tools (e.g., shred, sdelete)
  —Rootkits that hide files and processes
  —Modifying timestamps of files to avoid detection

INFORMATION SECURITY
VS
NETWORK SECURITY
VS
CYBER SECURITY

Information Security

- Protects data in all forms, whether electronic or physical or any other form.
- Focuses on

  —confidentiality,

  —integrity, and

  —availability.

Network Security

- Protects data as it moves across networks
- focuses on securing network infrastructure and data flow.

Cybersecurity

- Protects data that is in electronic form ONLY.
- Broadly protects against cyber threats, encompassing both information and network security, with a focus on defending against attacks from the digital realm.