Identify and Analyze Cyber Threats

Malware
Definition: Software that is intentionally designed to harm a computer or network, typically designed to steal data, damage systems, or gain unauthorized access.

Function: Malware typically enters a system through phishing emails, malicious downloads, or infected USB drives. Once inside, it can execute harmful actions such as stealing data, encrypting files, or creating backdoors for unauthorized access.

Real-World Example: The 2017 WannaCry ransomware attack used a vulnerability in outdated Windows systems to encrypt files and demanded Bitcoin payments for decryption.

Impact: Data loss, financial loss, disruption of systems.

Social Engineering
Definition: Social engineering manipulates individuals into giving up sensitive information.

Function: Using tactics like phishing, baiting or pretexting to gain access to confidential information by tricking users

Real-World Example: Twitter Bitcoin same used bots to social engineer employee credentials

Impact: Led to Unauthorized access to systems, data breaches, loss of reputation

Advanced Persistent Threats (APTs)
Definition: APTs are prolonged and targeted cyberattacks where attackers gain unauthorized access to a network and remain undetected to steal sensitive data over time.

Function: APTs use techniques, such as custom malware, spear-phishing, and exploiting system vulnerabilities. Attackers prioritize stealth to avoid detection while exfiltrating data or gaining persistent access.

Real-World Example: The SolarWinds attack (2020) was an APT where attackers inserted malicious code into a software update, compromising numerous organizations, including U.S. government agencies.

Impact: Data breaches, compromise of sensitive information

Insider Threats

Definition: Insider threats arise from individuals within an organization, such as employees, contractors, or business partners, who misuse their access to harm the organization.

Function: Insiders can intentionally or unintentionally compromise security by stealing data, leaking sensitive information, or damaging systems

Real-World Example: The 2013 Edward Snowden leaks revealed classified information about NSA surveillance programs, significantly impacting national security

Impact: Exposure of confidential data, loss of customer trust

Zero- Day Exploits
Definition: Zero-day exploits take advantage of vulnerabilities in software or hardware that are unknown to the vendor and unpatched.

Function: Attackers identify and exploit these flaws before they are discovered and patched, often using custom malware or scripts to infiltrate systems.

Real-World Example: The Stuxnet worm exploited zero-day vulnerabilities to sabotage Iran's nuclear centrifuges, highlighting its potential for cyber warfare.

Impact: Compromise of Infrastructure, Loss of System Control.

Apply Vulnerability Assessment Techniques

```
┌──(shuwhits㉿Shuwhits)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fd00::f829:9c55:f79:2cad  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::a00:27ff:fe70:e04c  prefixlen 64  scopeid 0x20<link>
        inet6 fd00::a00:27ff:fe70:e04c  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:70:e0:4c  txqueuelen 1000  (Ethernet)
        RX packets 30  bytes 5824 (5.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 558  bytes 36820 (35.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(shuwhits㉿Shuwhits)-[~]
└─$ sudo nmap -sn 10.0.2.15/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-15 16:35 EST
Nmap scan report for 10.0.2.2
Host is up (0.00042s latency).
MAC Address: 52:55:0A:00:02:02 (Unknown)
Nmap scan report for 10.0.2.3
Host is up (0.00038s latency).
MAC Address: 52:55:0A:00:02:03 (Unknown)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.37 seconds

┌──(shuwhits㉿Shuwhits)-[~]
└─$ nmap -sV -p- 10.0.2.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-15 16:35 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.26 seconds
```

```
┌──(shuwhits㉿Shuwhits)-[~]
└─$ nmap -sV --script vuln 10.0.2.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-15 16:59 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 13.47 seconds
```