Information and Data Security

Mohammed Amine Merzoug

Associate Professor, University of Batna 2
amine.merzoug@univ-batna2.dz

2025/2026 - Fesdis, Batna

Brief about Me

Mohammed Amine Merzoug

Associate Professor at University of Batna 2

HDR, Ph.D., Eng. in Computer Science

Research interests

- Distributed systems
- Cybersecurity
- Artificial intelligence

amine.merzoug@univ-batna2.dz
https://staff.univ-batna2.dz/merzoug-amine

Chapter 0

Cybersecurity Overview

What Do You Know About Cybersecurity?

What Do You Know About Cybersecurity?

Concepts?

Technologies/Tools?

Environments?

Careers?

Answer this question, before moving to the next slide

What Do You Know About Cybersecurity?

Concepts: vocabulary (asset, threat, vulnerability, risk, attack), CIA Triad, ethical hacking, encryption, malware, types of attackers, etc.

Technologies/Tools: Kali Linux, Metasploitable, Metasploit, Wireshark, firewalls, IDS/IPS, WAF, EDR, XDR, SIEM, SOAR, etc.

Environments: Virtual Machines (VMs), Sandboxes, penetration testing platforms, vulnerability scanning, etc.

Careers: SOC analyst, penetration tester, security engineer, security architect, etc.

What is cybersecurity?

What is cybersecurity?

Definition: ***protection*** of systems, networks, and data from digital attacks and ***recovery*** after attacks

Why it matters? economic impact, privacy, national security, safety-critical systems.

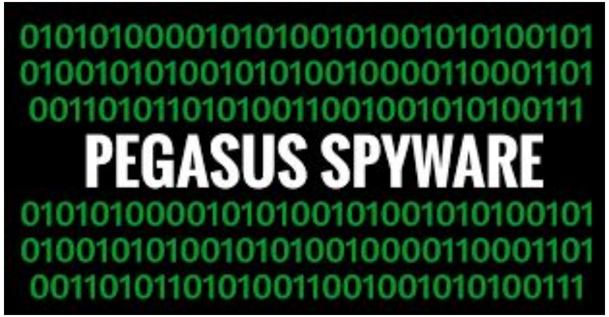
- Cybersecurity affects everyone—governments, businesses, and even **<u>you</u> (individuals)!**

Real-World Impacts (case studies)

- **WannaCry** (ransomware 2018): widespread disruption.
  - Helped by cryptocurrency
- **Pegasus spyware**: stealthy, high-impact compromise.
  - Tool bought by governments
- **NoName(16)** (operational disruption).
  - Botnets (russian)

These examples are given to show different attacker goals

- Financial gain
- Espionage
- Disruption



Core Concepts of Cybersecurity

Core concepts - Some vocabulary

This is the vocabulary we will be using throughout the course

- **Asset**: What you want to protect (data, devices, apps, servers, etc.).
- **Threat**: Anything that could harm your assets.
- **Vulnerability**: Weakness that could be exploited.
- **Attack**: When a threat actually exploits a vulnerability.
- **Risk**: The likelihood and impact of an attack. (Risk = Likelihood × Impact)
- **Countermeasure**: Defense method (tools, policies, practices, guidelines, procedures, etc.)

Core concepts - Examples of Threats

Threats (potential dangers)

- Malware (viruses, ransomware, etc.)
- Phishing emails
- DDoS attacks
- Insider misuse
- Zero-day vulnerabilities

Core concepts - Examples of Risks

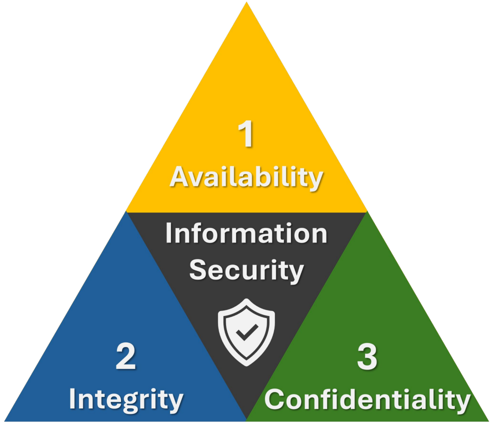
Risks (impact if threat succeeds)

- Data theft (personal info, credit cards)
- Financial loss (fraud, ransomware payments)
- Service downtime (website/app offline)
- Reputation damage (loss of customer trust)
- Legal consequences (non-compliance with GDPR, HIPAA, etc.)

Key point

- **Threat** is **what could happen**
- **Risk** is **what happens if it affects you**

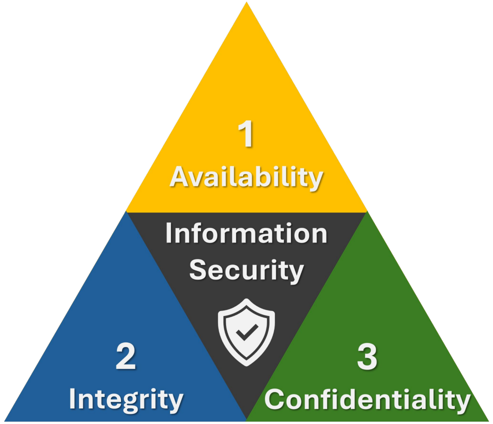
Core concepts - CIA Triad



- **Confidentiality**: data privacy and secrecy.
  - Keep data secret (encryption).
- **Integrity**: data accuracy and trustworthiness.
  - Keep data accurate (hashing, signatures).
- **Availability**: systems accessible when needed.
  - Keep systems accessible (backups, redundancy).

- **Example:** Banks vs hospitals vs commercial websites
  - How does the CIA triad apply?

Core concepts - CIA Triad

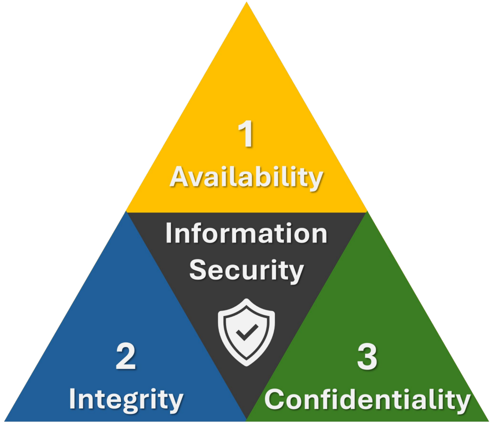


The CIA triad applies ***everywhere***, but the ***priority balance changes***.

For example:

- In **hospitals**, availability (life-or-death) and integrity are top.
- In **banks**, confidentiality and integrity dominate.
- In **e-commerce**, integrity (prices/orders) and availability (uptime) matter most.

Core concepts - CIA Triad + Proof



Sometimes the model is extended beyond CIA to include

Proof: Making sure actions can be verified.

Authentication

- Verifying *who* is accessing the system.
- Example: username/password, 2FA, digital certificates.

Non-Repudiation

- Ensuring users cannot later deny an action they performed.
- Example: digital signatures, signed transactions, logging.
- Real-world example: If you transfer money online, you can't later say, *"That wasn't me".*

Networking Foundations (must-know for cybersecurity)

Networking Foundations (must-know for cybersecurity)

- **Layers of networking**: OSI Model (Physical → Application)
  - Attacks often target specific layers
  - Example: DoS at network, SQL injection at application

- **Protocols**: TCP/IP, UDP, HTTP, HTTPS, DNS, FTP, SMTP, ICMP, ARP, RDP, etc.
  - TCP vs UDP: reliability vs speed.

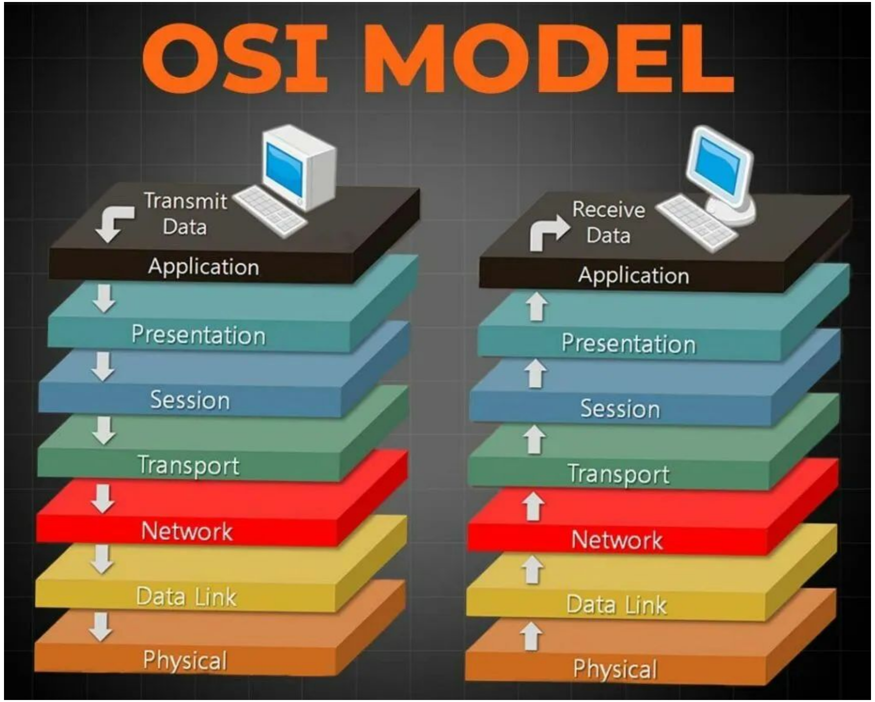
- **Ports and services**: 80 (HTTP), 443 (HTTPS), 21 (FTP), 22 (SSH), 53 (DNS), 25 (SMTP).
  - Why are open ports interesting to attackers?

- **IP addresses, MAC addresses**: identity of devices.
  - **IP address → building, ports → doors/rooms**

Networking Foundations (must-know for cybersecurity)

- **OSI model: seven layers**
  - Physical → Application

- **Real-world example**
  - HTTP request traveling down/up the stack



Networking Foundations (must-know for cybersecurity)

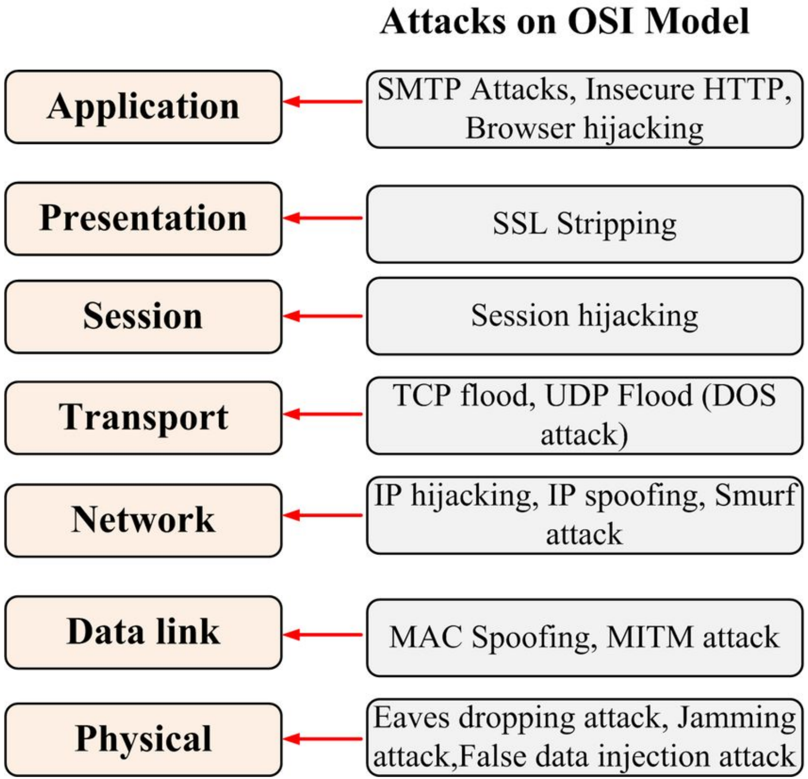
Some attacks per layer

Application?

Mac? ARP spoofing

Key point

Defense must be applied at different layers

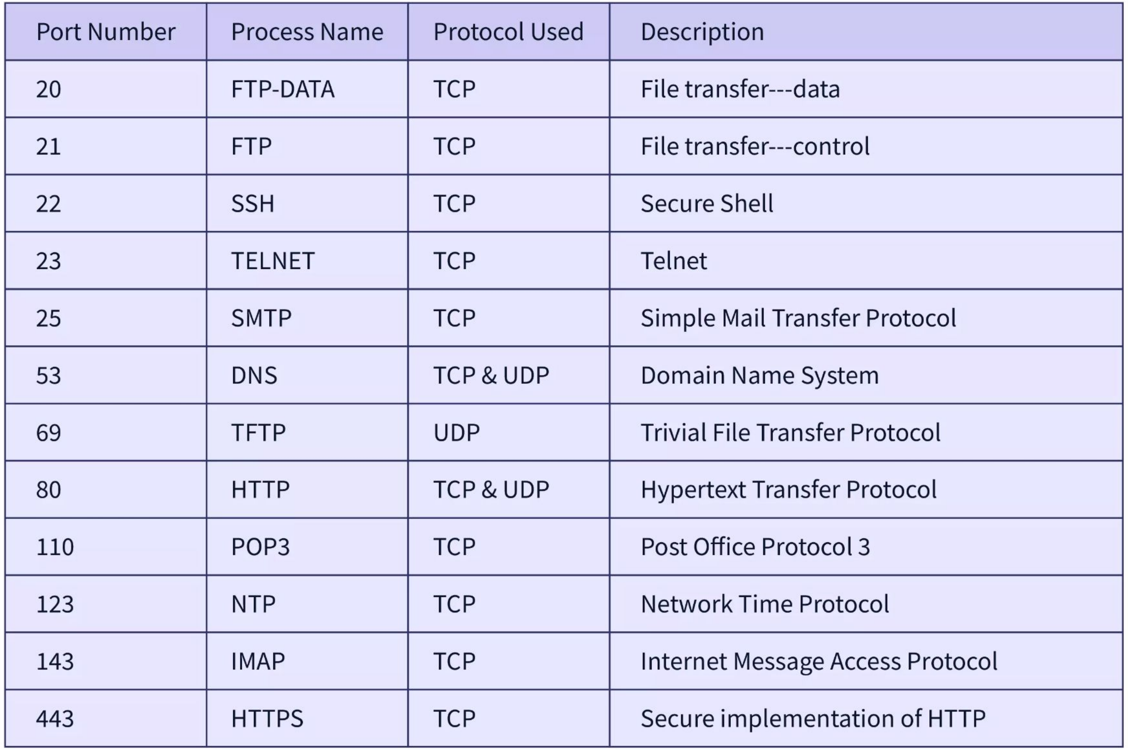


Attacks on OSI Model

Application	SMTP Attacks, Insecure HTTP, Browser hijacking
Presentation	SSL Stripping
Session	Session hijacking
Transport	TCP flood, UDP Flood (DOS attack)
Network	IP hijacking, IP spoofing, Smurf attack
Data link	MAC Spoofing, MITM attack
Physical	Eaves dropping attack, Jamming attack,False data injection attack

Networking Foundations (must-know for cybersecurity)

- **Common ports, services, and Protocols**
- Services can use **TCP**, **UDP**, or **both**



Port Number	Process Name	Protocol Used	Description
20	FTP-DATA	TCP	File transfer---data
21	FTP	TCP	File transfer---control
22	SSH	TCP	Secure Shell
23	TELNET	TCP	Telnet
25	SMTP	TCP	Simple Mail Transfer Protocol
53	DNS	TCP & UDP	Domain Name System
69	TFTP	UDP	Trivial File Transfer Protocol
80	HTTP	TCP & UDP	Hypertext Transfer Protocol
110	POP3	TCP	Post Office Protocol 3
123	NTP	TCP	Network Time Protocol
143	IMAP	TCP	Internet Message Access Protocol
443	HTTPS	TCP	Secure implementation of HTTP

Attackers

Who are the attackers?

- **Script Kiddies:** Inexperienced hackers using ready-made tools
- **Hacktivists:** Attack for political or social causes
- **Cybercriminals:** Motivated by financial gain (ransomware, fraud)
- **Insiders:** Employees or contractors abusing access
- **State-Sponsored Groups:** Advanced, well-funded attackers (APT - Advanced Persistent Threat)
- **Suicide hackers:** fame, etc.

Motivations: Money, ideology, revenge, espionage, and curiosity

Who are the attackers?

- **Black Hat Hackers:** Malicious hackers who break systems for personal gain or harm.
- **White Hat Hackers:** Ethical hackers who help organizations find and fix vulnerabilities.
- **Gray Hat Hackers:** In-between, sometimes break rules but not always with malicious intent.
- **Red Team vs Blue Team**
  - **Red Team** = offensive (simulate attackers)
  - **Blue Team** = defensive (protect and respond)
- **Purple team?**

Vulnerabilities

Vulnerabilities

Definition: Weaknesses in software, hardware, or human behavior that attackers exploit.

Examples

- Unpatched software
- Weak/default passwords
- Misconfigured servers, firewalls, IPS/IDS, etc.
- Outdated protocols (e.g., SSL, Telnet)
- Zero-day vulnerabilities

Key point: Threats become successful attacks only when they exploit vulnerabilities.

CVE and CVSS Score

CVE

Common Vulnerabilities and Exposures

- A standardized list of publicly known cybersecurity vulnerabilities
- Each CVE has a unique ID (e.g., CVE-2021-34527 – PrintNightmare).
- Discovered by academic researchers, industry professionals, hackers, etc.
- https://www.cvedetails.com/
- https://nvd.nist.gov/ - NVD (National Vulnerability Database) maintained NIST (National Institute of Standards and Technology)

CVSS Score

Common Vulnerability Scoring System

- Rates the severity of vulnerabilities on a **scale from 0.0 to 10.0**
- Categories
  - Low (0.1–3.9)
  - Medium (4.0–6.9)
  - High (7.0–8.9)
  - Critical (9.0–10.0)

Why CVE and CVSS matter? Help prioritize patching and risk management (PoC)

Types of Cyber Attacks

Some Cyber Attacks

- **Malware** (malicious software): viruses, worms, ransomware, trojans, spyware, adware, etc.
- **Social Engineering** (tricking humans): phishing, spear-phishing, whaling, smishing, vishing, spam, scam, etc.
- **Denial of Service (DoS/DDoS)**: flooding systems
- **Man-in-the-Middle (MitM)**: intercepting communication
- **SQL Injection & XSS**: targeting web apps
- **Password Attacks**: brute force, dictionary, credential stuffing, password spraying, etc.

These attacks can be categorized into classes.

Types of Cyber Attacks

1. Malicious code attacks computer viruses, worms, spyware, trojans, adware, ransomware, cryptominers, etc.

2. Network attacks

- IP Spoofing
- ARP Spoofing
- DNS Spoofing
- Fragmentation attacks
- TCP Session Hijacking
- Man-in-the-Middle (MITM)
- Denial of Service (DoS/DDoS)

3. Program attacks

- Buffer overflow
- Injection attacks
  - SQL Injection (SQLi)
  - Cross-Site Scripting (XSS)
- Website Defacement

4. Social engineering attacks phishing, spear phishing, whaling, spam, scams, vishing, smishing, etc.

Attack Lifecycle (Intrusion Phases)

Attack Lifecycle (Intrusion Phases)

1. **Reconnaissance**: gather public info about the target

2. **Network Scanning**: actively probe the target to find live hosts, open ports, and services

3. **Gaining Access**: exploit vulnerabilities or trick users to obtain an initial foothold

4. **Maintaining Access**: establish persistence so the attacker can return later

5. **Covering Tracks**: remove or alter traces to avoid detection and forensic analysis

Attack Lifecycle (Intrusion Phases) - Tools and examples

1. Reconnaissance: OSINT, Google dorking, LinkedIn profiling, Shodan searches, etc.

- https://www.shodan.io/

2. Network Scanning: nmap, ping, port sweeps, etc.

3. Gaining Access: phishing, SQL injection, exploiting unpatched software, Metasploit modules.

4. Maintaining Access: web shells, backdoors, creating hidden accounts, scheduled tasks/cron jobs, rootkits, etc.

5. Covering Tracks: log deletion/alteration, timestamping file metadata, clearing shell history, anti-forensic tools, etc.

Security Mechanisms

Security Mechanisms

- **Anti-DDoS**
- **Firewalls**: block or allow traffic
- **IDS/IPS** (Intrusion Detection/Prevention Systems)
- **Proxy** (forward proxy, reverse proxy)
- **WAF** (Web Application Firewall)
- **Antivirus/EDR** (Endpoint Detection & Response): endpoint defenses
- **DLP** (Data Loss Prevention)
- **DMZ** (Demilitarized Zone)
- **VPN**
- **PKI** (certification): public key infrastructure (proof/authentication + integrity)
- **Encryption**: protects data (AES, RSA, TLS)
- **Authentication**: passwords, MFA, biometrics
- **Access Control**: principle of least privilege
- **SIEM** (Security Information and Event Management) / **XDR** / **SOAR**

Security Principles & Architecture

Security Principles & Architecture

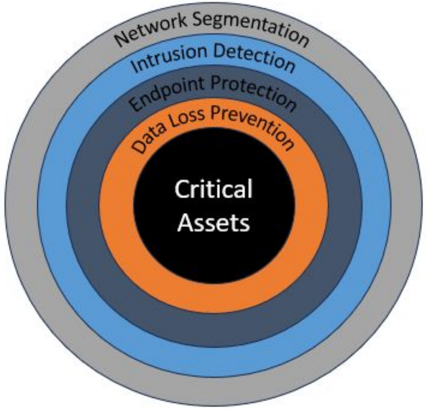
- **Secure by Design**
- **Defense in Depth**
- **Least Privilege**
- **Zero Trust**

Security Principles & Architecture

Secure by Design

- Security is integrated **from the start**, not added later.
- Systems are built with security requirements in the **architecture, design, and coding phases**.
- Goal: prevent vulnerabilities rather than patch them after deployment.

Defense in Depth



- Use **multiple layers of security controls** to protect assets.
- If one layer fails, others continue to provide protection.
- Examples: firewall ➜ intrusion detection ➜ endpoint protection ➜ data encryption.

Security Principles & Architecture

Least Privilege

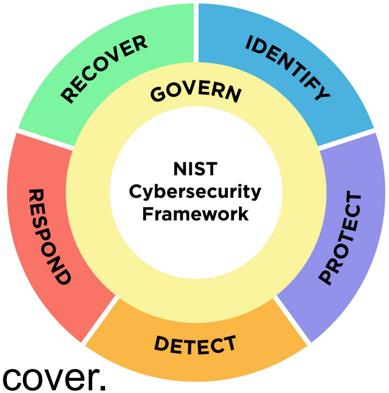
- Users, applications, and services operate with **only the permissions necessary** to perform their tasks.
- Reduces damage if an account or process is compromised.
- Principle applies to both human users and automated systems.

Zero Trust

- **Never trust, always verify**
- Every access request is authenticated, authorized, and encrypted, regardless of network location.
- Assumes no implicit trust within internal networks.

5. Cybersecurity Frameworks & Standards

5. Cybersecurity Frameworks & Standards



- **NIST Cybersecurity Framework**: Identify, Protect, Detect, Respond, Recover.
  - Set of guidelines and best practices that help organizations against cybersecurity threats

- **ISO 27001**: International security standard (basics and compliance vs security)
  - Requirements for implementing IS security

- **MITRE ATT&CK**: Matrix of adversary tactics & techniques (threat intelligence).
  - https://attack.mitre.org/

MITRE ATT&CK™

Why are frameworks useful for organizations and auditors?

Pentesting & Red Team Basics

Pentesting & Red Team Basics

- Reconnaissance → Scanning → Exploitation (gaining access) → Post-exploitation (maintaining access, covering tracks)
- In reality, the pentester stops at **phase 3** (gaining access)!
- Ethical rules: permission, scope, and non-destructive testing.
- Example: A **network architect** wanted to become a **SOC analyst**, so he **tested his hacking skills on the company's systems without permission**.
    - **Result:** Immediate dismissal and **criminal charges leading to jail time**.
    - **Lesson:** Even if your intentions are good, **unauthorized access is illegal**.
      Always obtain **explicit written authorization** before performing any security testing.

Pentesting & Red Team Basics

- Clarify legal/ethical boundaries and responsible disclosure.
  - When performing security testing or red team operations, it is essential to understand **what is allowed and what is not**.

☞ **Legal Boundaries**

- You must have **written authorization** before testing any system.
  Acting without permission is considered **illegal hacking** (even inside your organization).

☞ **Ethical Boundaries**

- Follow professional ethics: **do no harm**, **avoid unnecessary disruption**, and **protect sensitive data**.

☞ **Responsible Disclosure**

- If you discover a vulnerability, **report it responsibly** to the organization or vendor through the proper channel (not publicly or on social media) so it can be fixed securely.

Practical Skills & Tools

Practical Skills & Tools

- **Networking**
- **Commands (windows and linux)**
- **Kali Linux**: penetration testing OS
- **Metasploitable**: vulnerable VM
- **Metasploit**: exploitation framework
- **Wireshark:** packet capture and analysis
- **Nmap**: network scanning (discovery and port scanning)
- **Burp Suite**: web application testing. **Nikto**: web application scanning
- **DVWA (Damn Vulnerable Web App)**: practice web hacking safely

You will use these tools in labs and projects

Some other tools

- **Snort** (IPS/IDS)
- **Volatility** (RAM forensics tool)
- **Autopsy** (disk forensics tool)
- **SIEM** (Security Information and event management):
  - Splunk (Cisco)
  - ELK
  - QRadar (IBM)
  - Sentinel (Microsoft)
  - LogScale (CrowdStrike)
  - Wazuh
- **OpenVAS** (vulnerability scanning), **Nessus**

Some other tools

- **Open-source investigation tools**
  - virusTotal: https://www.virustotal.com/ (url, IP, hash, file)
  - IBM X-Force (hash, IP, URL like VirusTotal): https://exchange.xforce.ibmcloud.com/
  - scamDoc: https://www.scamdoc.com/ (email trust score)
  - Have I Been Pwned: https://haveibeenpwned.com/ (email)
  - URLScan.io: https://urlscan.io/ (url scan)
  - greyNoise: https://www.greynoise.io/ (IP)
  - AbuseIPDB: https://www.abuseipdb.com/ (IP)
  - JoeSandBox: https://www.joesandbox.com/ (file → malware?)
  - HybridSandBox: https://hybrid-analysis.com/
  - App.any (sandBox): https://app.any.run/
  - etc.

Career Paths in Cybersecurity

Career Paths in Cybersecurity

- **Defensive (Blue Team)**
  - Log onboarding, SOC analyst, threat intel, threat hunting, reverse engineering, security architect, etc.
  - Each company has its own policy

- **Offensive (Red Team)**
  - Penetration tester, ethical hacker (audit)

- **Purple Team**? Both

Career Paths in Cybersecurity

- **Governance, Risk, Compliance (GRC)**
  - Policies, audits, risk management.

- **Digital Forensics & Incident Response (DFIR)**
  - Investigating breaches.
  - Writes reports at the end with SOC recommendations

- **Malware Analysis & Reverse Engineering**

- **Threat intelligence (look for IoC: proofs of attacks)**

- **Threat hunting (proactive: against untraditional (next-gen) techniques)**

Career Paths in Cybersecurity

- **Suggested skills & certifications**
  - EHC: Ethical Hacking Certifications
  - CompTIA Security+
  - CISSP (Five years of experience): Certified Information Systems Security Professional
  - OSCP: Offensive Security Certified Professional

- **Interdisciplinary nature:** coding (scripting), networks, psychology (understanding hackers).

8. Learning Roadmap

8. Learning Roadmap

- **Step 1: Learn networking (OSI model, TCP/IP, ports, services)**
- **Step 2: Learn Linux and Windows commands (PowerShell/cmd, shell)**
- **Step 3: Study attacks & defenses (phishing, malware, SQLi, DDoS, etc.)**
- **Step 4: Practice with tools (Kali Linux, DVWA, Wireshark, etc.)**
- **Step 5: Study security frameworks (NIST, MITRE)**
- **Step 6: Specialize (ethical hacking, blue team, forensics, etc.)**

Networking → Linux → Tools → Web/Network/System security → Advanced topics (forensics, RE, threat intel, threat hunting, malware analysis).

Labs: Kali + Metasploitable, Nmap, Wireshark, Metasploit, Snort, DVWA, etc.

Q & A

amine.merzoug@univ-batna2.dz

https://staff.univ-batna2.dz/merzoug-amine