Introduction to Cyber Security

"To outsmart a hacker, you need to think like one."

♠ Introduction to Cybersecurity

Cybersecurity is typically divided into **two** main approaches:

1. Offensive Security

Offensive security involves actively testing systems by:

- Breaking into computer systems (ethically)
- Exploiting software bugs
- Finding loopholes in applications
- Gaining unauthorized access (with permission)

The goal is to understand hacker tactics to enhance system defenses.

Offensive Security Careers:

- **Penetration Tester**: Tests technology products to find exploitable vulnerabilities
- **Red Teamer**: Plays the role of an adversary, attacking an organization and providing feedback
- **Security Engineer**: Designs, monitors, and maintains security controls, networks, and systems

Practical Example: Using Gobuster

Gobuster is a command-line tool for brute-forcing websites to find hidden directories and pages:

```
gobuster -u http://example.com -w wordlist.txt dir
```

This command helps identify potentially hidden admin pages or sensitive content by:

- -u: Specifying the target website
- -w: Using a wordlist to check for existing pages
- dir: Indicating directory/path brute forcing mode

☠ Tips:

Gobuster works with both HTTP and HTTPS as long as the URL matches the site's supported protocol.

If the site uses HTTPS with **a self-signed certificate**, you may need to add -k (skip TLS verification) to avoid errors:

```
gobuster -u https://example.com -w wordlist.txt -k dir
```

P.T.O

2. Defensive Security

Defensive security focuses on protecting systems and includes:

Key Tasks:

- User cybersecurity awareness training
- Documenting and managing assets
- Updating and patching systems
- Setting up preventative security devices (firewalls, IPS)
- Implementing logging and monitoring systems

Defensive Security Areas:

- **Security Operations Center (SOC)**: Centralized team monitoring and responding to threats
- **Threat Intelligence**: Collecting and analyzing data about emerging threats
- **Digital Forensics and Incident Response (DFIR)**: Analyzing breaches and recovering systems
- **Malware Analysis**: Dissecting malicious software to understand its behavior

Defensive Security Careers:

- **Security Analyst**: First line of defense, monitoring alerts in a SOC
- **Security Engineer**: Designs and maintains security infrastructure
- **Incident Responder**: Contains and investigates active attacks
- **Digital Forensics Examiner**: Investigates cybercrimes through digital evidence
- **Malware Analyst**: Studies malicious software

♦ Practical Example: Alert Investigation

As a SOC analyst, you would review security alerts like:

Date	Message
undefined 8th 2025, 03:57:13:124	Successful SSH authentication attempt to port 22 from IP address 143.110.250.149
undefined 8th 2025, 03:54:24:078	Unauthorized connection attempt detected from IP address **143.110.250.149** to port 22
undefined 8th 2025, 01:37:09:250	The user John Doe logged in successfully (Event ID 4624)
undefined 8th 2025, 01:37:01:291	Multiple failed login attempts from John Doe

undefined 8th 2025, 01:27:42:284	Logon Failure: Specified Account's Password Has Expired (Event ID 535)

Investigation would involve:

1. Checking IP reputation using tools like AbuseIPDB or Cisco Talos
2. Analyzing the pattern of failed and successful login attempts
3. Escalating concerns to the appropriate person

- **Incident Escalation Question:**

Choose to whom you would escalate this event?

1. Sales Executive
2. Security Consultant
3. Information Security Architect
4. SOC Team Lead

Answer: 4. SOC Team Lead

Why? The SOC Team Lead is the appropriate choice because they directly oversee the Security Operations Center team and have the authority to coordinate immediate response actions. They understand the technical details and operational context of security alerts, can mobilize the necessary resources, and know the proper escalation paths if the incident requires broader attention. Other options like Sales Executive (non-security role), Security Consultant (typically external advisor), or Information Security Architect (focuses on design rather than operations) don't have the direct operational responsibility needed for immediate incident response.

♠ Cybersecurity Career Paths

The cybersecurity industry offers diverse career options with high demand and competitive salaries:

1. **Security Analyst**: Monitors systems and responds to alerts
2. **Security Engineer**: Designs and builds security infrastructure
3. **Incident Responder**: Contains and investigates active threats
4. **Digital Forensics Examiner**: Analyzes digital evidence
5. **Malware Analyst**: Studies malicious software
6. **Penetration Tester**: Ethically hacks systems to find vulnerabilities
7. **Red Teamer**: Simulates full-scale attacks to test defenses

♦ Cybersecurity Mindset Quiz

This quiz reveals personality traits that align with cybersecurity roles:

A. If I was stranded on an island, the first thing I would do is...

1. Try and build a raft home
2. Scope the landscape for potential threats
3. Gather food and plan next steps
4. Find a way to send an SOS
5. Build a secure shelter to prevent potential attacks

Answer: 4. Find a way to send an SOS

Why? The survival priority order typically follows the "rule of threes" - you can survive 3 minutes without air, 3 hours without shelter in harsh conditions, 3 days without water, and 3 weeks without food. While shelter might seem urgent based on this, sending a distress signal as early as possible maximizes your chances of rescue before other survival concerns become critical.

B) In my spare time, I like to...

1. Tinker with new technology and understand how it works
2. Watch crime-solving TV shows
3. Keep busy by learning something new
4. Find geocaches in my neighborhood
5. Upkeep and maintain my home through DIY projects

Answer: 1. Tinker with new technology and understand how it works

Why? This is most aligned with hacker culture and mindset. The curiosity to take things apart, understand their inner workings, and potentially repurpose or modify them is a fundamental trait of successful cybersecurity professionals. This hands-on approach to technology demonstrates the exploratory thinking needed to anticipate security vulnerabilities.

C) My favorite game is...

1. Battleships
2. Cluedo
3. Chess
4. Hide and seek
5. Risk

Answer: 3. Chess

Why? Chess represents strategic thinking at its finest, and the skills valued in chess directly parallel those used in cybersecurity and ethical hacking. Both require thinking several moves ahead, understanding your opponent's strategy, planning multiple approaches, adapting to changing circumstances, and recognizing patterns. Chess players, like cybersecurity professionals, must balance offensive tactics and defensive positioning.

D) I'm best described as...

1. Curious
2. Strategical
3. Calm under pressure
4. Mischievous
5. Practical

Answer: 1. Curious

Why? Curiosity is the foundational trait of successful cybersecurity professionals. It drives the continuous exploration of how systems work, what vulnerabilities might exist, and how attackers think. Curious individuals are more likely to discover unconventional attack vectors, dig deeper into anomalies, question assumptions, and maintain the lifelong learning mindset essential in the constantly evolving cybersecurity landscape.

E) My favorite movie is...

1. Back to the Future
2. Matrix
3. Terminator

4. Indiana Jones
5. Jurassic Park

Answer: 2. Matrix

Why? The Matrix is particularly relevant to cybersecurity professionals as it explores themes of digital reality, system vulnerabilities, hacking, and the relationship between humans and technology. It portrays a world where understanding the underlying code allows for manipulation of the system—a direct parallel to how cybersecurity professionals must understand systems to protect or exploit them. The film's emphasis on questioning reality and seeing beyond surface appearances mirrors the analytical mindset needed in cybersecurity.

Key Terminology

- **SSH Authentication**: Secure Shell protocol for secure remote access
- **Firewall**: Controls network traffic entering and leaving a system
- **IPS**: Intrusion Prevention System that blocks malicious network traffic
- **SIEM**: Security Information and Event Management tool for centralized monitoring
- **IP Address**: A unique identifier for devices on a network
- **Flag:** A token or data piece used in cybersecurity challenges to show a vulnerability is found or a task completed.

---------- X----------