Cisco: Introduction to Cybersecurity

My Knowledge Check Result

> Before completing the course, I answered the initial questions to check my current knowledge at the time. I did this to be able to compare it with the final exam and measure the skills I gained during the course.

Module 1: Introduction to Cybersecurity

What is Cybersecurity?

> An ongoing effort to protect individuals, organizations, and governments from digital attacks.

- How can hackers access your personal data? Through Medical records, Educational records & Employment and financial records.

What do hackers want?

Example (Phishing Attack):
A phishing scam targeted users of an online bank. Victims received an email that looked like a real notification warning of "suspicious activity" and asked them to click a link to verify their identity.
The link led to a **fake login page**. When users entered their credentials, attackers stole the data and accessed their accounts.

Identity Theft (is not a joke, Jim):

- Used to incur high medical bills (especially in systems without universal healthcare).
- Used to steal money or take out loans under another person's name.

Who else wants my data?

- **ISPs (Internet Service Providers):** Track your online activity and may sell it to advertisers.
- **Advertisers:** Use online habits and preferences for targeted ads.
- **Search engines & social media:** Collect gender, location, phone number, ideologies, etc.
- **Websites:** Use cookies to track and sell user data trails.

Types of Organizational Data

- **Traditional:** Transactional data, intellectual property, financial data

- **IoT:** Devices connected to the internet that collect and share data

The Security Cube (3D Framework)

CIA Triad – Core Principles of Cybersecurity:

- **Confidentiality:** Encryption, identity proofing, two-factor authentication
- **Integrity:** Use of hash functions or checksums
- **Availability:** Hardware maintenance, updates, backups

Data States:

- **Data in process:** Actively being used (e.g., updating a database)
- **Data at rest:** Stored on disk or memory
- **Data in transit:** Moving between systems or networks

Protection Measures:

- **People:** Awareness, training, education
- **Technology:** Firewalls, antivirus, secure hardware
- **Policies and Procedures:** Rules and frameworks to govern access and response

Data Security Breaches – Examples

- **Persirai Botnet:** Exploited IoT cameras via open ports for DDoS attacks
- **Equifax Breach:** US credit reporting agency compromised due to web exploit

Consequences of Security Breaches

- **Reputational Damage:** Loss of trust, compensation, slow recovery
- **Vandalism:** Inserting false info (e.g., fake phone number on website)
- **Theft:** Personal data used for fraud or identity theft
- **Loss of Revenue:** Direct financial impact and business disruption
- **Damaged Intellectual Property:** Leaked trade secrets hurt competitiveness

Practical Case 1: - Data: Massive data breach in an hotel chain the hackers couldn´t access account or financial info. - Vulnerability: hackers gained access via customer database by using employees login details - Result: The hackers stole the personal information of over three million hotel guests. This included their names, email addresses and phone numbers. **Practical Case 2**: - Data: bad management of clients information - can be used for phising malware and fraud - Vulnerability: leaving it at the public site - bad security practice (control your access via 2fa or smt!) - Result: Hackers are targeting the increasing numbers of organizations who are migrating to the cloud or using cloud-based services and resources. In this scenario, hackers were able to take advantage of an organization's poor security practices. Unsecured cloud databases left exposed on the Internet present a huge vulnerability and one that attackers will seek to exploit to gain easy access to valuable organizational data.

In both cases, the organizations need to invest in improved security practices.

This might include:

- investing in cybersecurity training for all staff so that they are aware of and able to spot a cyber attack
- enforcing two factor authentication for employees accessing files and applications that contain sensitive data
- maintaining log files and ongoing monitoring to identify anomalous behavior that might indicate a data breach
- storing the passwords of customers using a combination of salting and robust hashing algorithms
- separating cloud-based resources from the public Internet into an isolated private network segment
- granting employee access to personal data and internal systems only via a secure VPN connection.

https://www.netacad.com/content/i2cs/7.1/courses/content/m1/en-US/assets/m1-lab-what-was-taken.pdf -> https://github.com/nievesnu/cybersecurity-portfolio/courses/Introduction to Cybersecurity/breach-examples.md

Types of Attackers

- Script kiddies: amateurs
- White hat: breaks in prior permission to look for vulnerabilities to improve the security of a network or system
- Grey hat: similar to white but biased can published vulnerabilities they found or report to the owner
- Black hat: takes advantage of vulnerability for gain
- Organized hackers (Anonymus): have cyber criminals, hacktivists(awareness about issues) terrorist and state sponsored hackers (pigs, commits sabotage on behalf of their government, well funded)

Internal Threats: Employees => clumsy **External Threats**: Outsiders =>

have to gain access

Stuxnet malware was designed not just to hijack targeted computers but to actually cause physical damage to equipment controlled by computers Non-Trivial distribution, Sophistication, Modular coding, Unique Target(patience), Motive. **The Purpose of Cyberwarfare** gain advantage over adversaries via compromised info via espionage = disruption & chaos.

Module 1 Quiz Result:

Module 2: Attacks, Concepts and Techniques

Types of Malware

- **Spyware**: Tracks and logs your activity (keystrokes, data, online behavior). Often bundled with legitimate software or trojans.
- **Adware**: Displays unwanted ads, usually in browsers. Often paired with spyware.
- **Backdoor**: Bypasses normal authentication to give remote access to a system. Hard to detect.
- **Ransomware**: Encrypts your data and demands payment to restore access. Spread via phishing or system vulnerabilities.
- **Scareware**: Uses fake warnings to trick users into installing malware.
- **Rootkit**: Alters OS to allow remote access. Very stealthy, often requires full system reinstall.
- **Virus**: Replicates and attaches to files. Needs user interaction. Can be destructive or harmless. Often spreads via USB, email, or network shares.
- **Trojan Horse**: Disguises as legit software. Doesn't self-replicate but opens a door for malware.
- **Worms**: Self-replicate and spread independently. Don't need user interaction. Used in major historical attacks like Code Red (2001).

Infiltration Techniques

- **Social Engineering**: Human manipulation to gain access (e.g., tailgating, quid pro quo).

- **DoS (Denial-of-Service)**: Overwhelms target with traffic or malformed packets.

- **DDoS (Distributed DoS)**: Same as DoS but from multiple sources.

- **Botnet**: Network of infected machines controlled via a C&C server.

- **On-Path Attacks**: Intercept or alter communications (Man-in-the-Middle/Mobile).

- **SEO Poisoning**: Ranks malicious sites higher using search optimization.

- **Wi-Fi Password Cracking**
- **Password Attacks**:
  - **Password Spraying**: Tries common passwords on many users.
  - **Dictionary Attack**: Uses lists of common passwords.
  - **Brute Force**: Tries every combination.
  - **Rainbow Table**: Uses precomputed hash tables.
  - **Traffic Interception**: Reads passwords stored or transmitted in plain text.
- **APT (Advanced Persistent Threats)**: Long-term, stealthy, highly targeted attacks, often nation-state sponsored.

Hardware Vulnerabilities

- Result from design flaws in specific device models.
- **Example**: *SYNful Knock* on Cisco IOS (2015) allowed attackers to gain control of enterprise-grade routers, such as the legacy Cisco ISR routers, from which they could monitor all network communication and infect other network devices. This vulnerability was introduced into the system when an altered IOS version was installed on the routers.
- **Prevention**: Verify firmware integrity and restrict physical access. Verify the integrity of the downloaded IOS image and limit the physical access of such equipment to authorized personnel only.

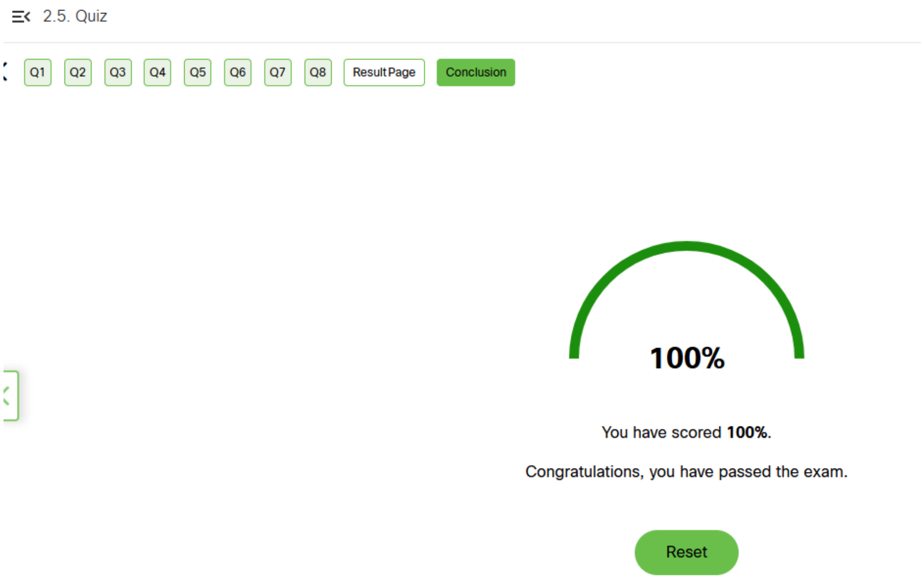
Categorizing Software Vulnerabilities

- **Buffer Overflow**: Writes data beyond buffer limits, can cause crashes or privilege escalation.
- **Non-Validated Input**: Malicious data input exploits program behavior (e.g., malformed image files).
- **Race Conditions**: Execution timing flaws can create vulnerabilities.
- **Weak Security Practices**: Avoid using custom security code. Use proven libraries.
- **Access Control Issues**:
  - Improper access settings can be exploited.
  - Physical access can override software protections — use encryption.

Cryptocurrency & Cryptojacking

- **Cryptocurrency**: Digital money secured via encryption.
- **Cryptojacking**: Malware mines crypto using your device's resources without your consent.

Module 2 Quiz Result



You have scored **100%**.

Congratulations, you have passed the exam.

Figure 1: Module 2 Quiz Result

Module 3: Protecting Your Data and Privacy

Protect computer device: Turn the firewall on - Install antivirus and antispyware - Manage your operating system and browser - Set up password protection Wireless Network Security at home with WPA2 encryption.

Password 1. Do not use dictionary words or names in any lenguages 2. Do not use common misspelling of dictionary words 3. Use special characters 4. Do not use computer names or account names 5. Use a p with >10 characters *NIST guidelines are stronger

- **Encryption:** converting information into a form in which unauthorized parties cannot read it How? -> choose a folder > properties > advanced

> Encrypt contents to secure data = EFS encription

- **BackupData:** at home, secondary location and in the cloud.
- **Delete Data Permanently:** It must be overwritten, to do so we have to use specific tools. Windows: SDelete, Linus Shred, MacOS X empty trash. The only way to be certain that data or files are not recoverable is to physically destroy the hard drive or storage device.

Data Ownership The Terms of Service are a legally binding contract that governs the rules of the relationship between you, the service provider and others who use the service. Before agreeing to use an online service, read the privacy policy and terms of service to understand how your data will be used. Use strong, unique passwords and enable two-factor authentication (2FA) to protect your account. Avoid sharing sensitive information unless necessary. Regularly update your software and review account activity. Be cautious of phishing attempts and only access services from secure networks. To protect your data and safeguard your account, you should: always read the Terms of Service when registering for a new service and decide whether the service is worth waiving your rights to your data for select your privacy settings rather than accepting the default, limit the group of people you share content with, review the service provider's security policy to understand what they are doing to protect your data, change your passwords periodically, use a complex password and two factor authentication to secure your account.

Two Factor Authentication adds an extra layer of security for account logins. - OAuth is an open standard protocol that allows you to use your credentials to access third-party applications without exposing your password. - Social sharing rule: the less the best - Dont get Spoofed - Private browsing = less data of yourself trhough the internet bcs disabled cookies & traces of your roundabouts.

Password manager applications can protect passwords by saving them in a secure encrypted form. They enable random passwords to be generated and managed easily, averting the need for users to have the same password for multiple accounts, which presents a security risk.

Quiz Module 3 Result:

Module 4: Protecting the Organization

Security Appliances

Security appliances can be standalone devices (e.g., routers) or software tools that run on a network device. They are generally categorized as follows:

Routers Primarily used to connect network segments. They also offer basic traffic filtering, helping control communication between different segments.

Firewalls Firewalls inspect network traffic for malicious behavior and apply security policies to allow or block traffic. Types include:

- **Network layer firewall**: Filters by IP addresses.
- **Transport layer firewall**: Filters by data ports and connection states.
- **Application layer firewall**: Filters by applications or services.
- **Context-aware layer firewall**: Filters by user, device, role, and threat profile.
- **Proxy server**: Filters web content requests.
- **Reverse proxy server**: Protects and manages access to web servers.
- **NAT firewall**: Hides internal IP addresses.
- **Host-based firewall**: Filters traffic on individual systems.

Intrusion Prevention Systems (IPS) Use traffic signatures to detect and block malicious activities in real-time.

Virtual Private Networks (VPNs) Create secure encrypted tunnels for remote access and interconnect branch offices securely.

Antimalware/Antivirus Identify and block malicious code using signature and behavior-based analysis.

Other Security Devices Include web/email security appliances, decryption tools, access control servers, and management systems.

Port Scanning

Each application uses a port number for communication. Port scanning probes for open ports, which can:

- Reveal running services and the OS (used in attacks)
- Help network admins verify firewall configurations

Example using Nmap:

```
Nmap my ip: https://hackertarget.com/nmap-online-port-scanner/
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-16 10:27 UTC
Nmap scan report for **.***.***.**.dyn.user.ono.com (**.***.***.**)
Host is up (0.12s latency).

PORT     STATE    SERVICE       VERSION
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   closed   telnet
80/tcp   filtered http
110/tcp  closed   pop3
143/tcp  closed   imap
443/tcp  filtered https
```

```
3389/tcp closed   ms-wbt-server

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 2.66 seconds
```

IDS vs IPS

- **Intrusion Detection System (IDS)**: Monitors and alerts on suspicious traffic.
- **Intrusion Prevention System (IPS)**: Monitors and actively blocks malicious traffic.

Image: Cisco's Threat Grid

Teams Involved

- **SOC team**: Secure Operations Center collects actionable security data.
- **Incident Response team**: has access to forensically sound information then analyzes behavior for faster mitigation.
- **Threat Intelligence team**: enhances defense through analysis, improving the organization's security infrastructure..
-

  ## Engineering team: is able to consume and act on threat information faster, often in an automated way.

Security Best Practices

- **Risk assessment**: Identify valuable assets and risks.
- **Security policies**: Define rules, roles, and responsibilities.
- **Physical security**: Restrict access to equipment.
- **HR security**: Perform background checks.
- **Backups**: Regularly back up and test data recovery.
- **Patching**: Keep systems updated.
- **Access control**: Use role-based permissions and strong authentication.
- **Incident response**: Employ and drill response teams.
- **Monitoring tools**: Use integrated analytics tools.
- **Network security devices**: Use next-gen routers/firewalls.
- **Endpoint security**: Use enterprise antimalware.
- **User education**: Train staff on security.
- **Data encryption**: Encrypt all sensitive data.

Behavior-Based Security

- **Honeypots**: Decoy systems that trap attackers and log their behavior.
- **Cisco Cyber Threat Defense**: Uses behavior-based detection to identify the who/what/when/where/how of attacks.

NetFlow Technology Collects metadata about network traffic, showing who, when, and how devices access the network.

Penetration Testing

A controlled attack to identify and fix vulnerabilities:

1. **Planning**: Information gathering and footprinting.
2. **Scanning**: Port/vulnerability scanning and enumeration.
3. **Gaining Access**: Exploiting systems via payloads, social engineering, or misconfigurations.
4. **Maintaining Access**: Staying undetected using backdoors, Trojans, and rootkits.
5. **Reporting**: Share findings to improve defenses.

Impact Reduction

- **Communicate**: Internally and externally, be transparent.
- **Accountability**: Own up and respond sincerely.
- **Details**: Disclose what happened and what was compromised.
- **Cause**: Investigate and identify the breach vector.
- **Apply Lessons**: Improve systems based on findings.
- **Recheck**: Ensure no backdoors remain.
- **Educate**: Train staff and stakeholders.

Risk Management

Risk management is the formal process of continuously identifying and assessing risk in an effort to reduce the impact of threats and vulnerabilities. You cannot eliminate risk completely but you can determine acceptable levels by weighing up the impact of a threat with the cost of implementing controls to mitigate it. The cost of a control should never be more than the value of the asset you are protecting.

1. **Frame the risk**: Identify the threats that increase risk. Threats may include processes, products, attacks, potential failure or disruption of

services, negative perception of an organization's reputation, potential legal liability or loss of intellectual property.
2. **Assess the risk**: Determine the severity that each threat poses. For example, some threats may have the potential to bring an entire organization to a standstill, while other threats may be only minor inconveniences. Risk can be prioritized by assessing financial impact (a quantitative analysis) or scaled impact on an organization's operation (a qualitative analysis).
3. **Respond to the risk**: Develop an action plan to reduce overall organization risk exposure, detailing where risk can be eliminated, mitigated, transferred or accepted.
4. **Monitor the risk**: Continuously review any risk reduced through elimination, mitigation or transfer actions. Remember, not all risks can be eliminated, so you will need to closely monitor any threats that have been accepted.

Cisco CSIRT

Cisco's Computer Security Incident Response Team works with global partners (FIRST, NSIE, DSIE, DNS-OARC) to stay updated on threats.

Security Tools & Practices:

- **Playbooks**: Provide case-based response guides.
- **Detection/Prevention**: Use tools like SIEM and DLP.
- **Cisco Identity Services Engine (ISE)/TrustSec**: Enforce role-based access to resources.

- An IPS can block or deny traffic based on a positive rule or signature match.
- An IDS scans data against a database of rules or attack signatures, looking for malicious traffic.
- A DLP system is designed to stop sensitive data from being stolen from or escaping a network.
- A SIEM system collects and analyzes security alerts, logs and other real-time and historical data from security devices on the network.

Exam Result

Module 5: Will Your Future Be in Cybersecurity?

Legal & Ethical Issues

- **Personal Legal Issues vs Corporate Legal Issues** If you are unsure whether an action or behavior might be illegal, **assume it is illegal and do not do it**. Always check with the organization's legal or HR department. International law and cybersecurity is a constantly evolving field. There are no traditional geographic boundaries in cyberspace.
- **Information Systems Security Association (ISSA)** An organization that has published **Codes of Ethics** to help guide employee actions and behaviors.

Download Ethics Decision Tree (PDF)

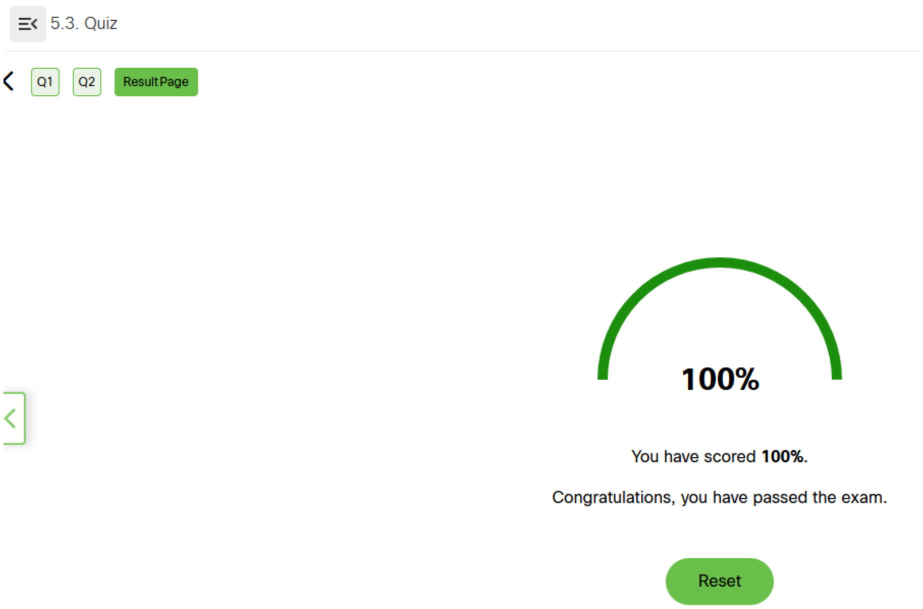
Education & Careers

Professional certifications are a great way to verify your skills and knowledge and can also boost your career.

- **Cisco Certified Support Technician (CCST) Cybersecurity** Entry-level certification for newcomers preparing to start their cybersecurity career. Ideal for high school, early college students, or career changers. No expiration or recertification required. **Cost:** $125 More info
- **CompTIA Security+** Entry-level security certification meeting U.S. Department of Defense Directive 8570.01-M requirements — important for IT security roles in federal government. **Cost:** $340 More info
- **EC Council Certified Ethical Hacker (CEH)** Tests knowledge of identifying system weaknesses and vulnerabilities using the same tools as malicious hackers, but lawfully. **Cost:** $1,759.00 before tax More info
- **(ISC)² Certified Information Systems Security Professional (CISSP)** One of the most recognized security certifications. Requires at least five years of relevant experience to sit for the exam. **Cost:** €191.04 – €719.04 More info
- **Cisco Certified CyberOps Associate** Validates skills for associate-level cybersecurity analysts in Security Operations Centers (SOC). **Cost:** $300 (exam only) More info

---

Result quiz module 5



You have scored **100%**.

Congratulations, you have passed the exam.

Figure 2: Module 5 Quiz Result

Final Exam: Course Completion

Notes

This pdf serves as a study log and reference for key cybersecurity principles learned through the Cisco "Introduction to Cybersecurity" course.