Foundations of Cybersecurity

Module 2

Computer Virus

Malicious code designed to interfere with computer operations and cause damage to data and software.

Malware

Software intended to harm devices or networks.

Early Malware Attacks

Brain Virus

Created in 1986 by Alvi brothers.
Intended to track illegal copies of medical software but spread unexpectedly.
Infected disks spread virus globally, impacting productivity and business operations.
Emphasized need for security and productivity plans in computing industry.

Morris Worm

Developed by Robert Morris in 1988.
Program to assess internet size but failed, causing it to replicate uncontrollably.
Affected 6,000 computers, representing 10% of the internet.
This attack cost millions of dollars in damages due to business disruptions and the efforts required to remove the worm.

Led to establishment of Computer Emergency Response Teams (CERTs).

Notable Attacks

LoveLetter Attack (2000)

Created by **Onel De Guzman** to steal internet **login credentials**.
First example of **social engineering**,
Exploited **human error** through **social engineering**, spreading rapidly via **email attachments**.
Spread rapidly via unsolicited emails with subject **I Love You** and attachment "**Love Letter For You**.
Infected 45 million computers globally, causing over **$10 billion in damages**.

Equifax Breach (2017)

Attackers infiltrate Equifax, resulting in one of the largest data breaches.
143 million customer records stolen, affecting **40%** of Americans.
Personally identifiable information, including social security numbers and credit card numbers, was stolen.
Resulted from multiple **failures** on Equifax's part, including neglecting **to fix known vulnerabilities**.
Settlement with the U.S. government resulted in over **$575 million** paid to resolve customer complaints and cover **fines**.

Common Attack Methods

Phishing

Phishing is the use of digital communications to trick people into revealing sensitive data or deploying malicious software.

Types of phishing

Business Email Compromise (BEC): A threat actor sends an email message that seems to be from a known source to make a seemingly legitimate request for information, in order to obtain a financial advantage.
Spear phishing: A malicious email attack that targets a specific user or group of users. The email seems to originate from a trusted source.
Whaling: A form of spear phishing. Threat actors target company executives to gain access to sensitive data.
Vishing: The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source.
Smishing: The use of text messages to trick users, in order to obtain sensitive information or to impersonate a known source.

Malware

Malware is software designed to harm devices or networks. There are many types of malware. The primary purpose of malware is to obtain money, or in some cases, an intelligence advantage that can be used against a person, an organization, or a territory.

Types of malware

Viruses: Malicious code written to interfere with computer operations and cause damage to data and software. A virus needs to be initiated by a user (i.e., a threat actor), who transmits the virus via a malicious attachment or file download. When someone opens the malicious attachment or download, the virus hides itself in other files in the now infected system. When the infected files are opened, it allows the virus to insert its own code to damage and/or destroy data in the system.

Worms: Malware that can duplicate and spread itself across systems on its own. In contrast to a virus, a worm does not need to be downloaded by a user. Instead, it self-replicates and spreads from an already infected computer to other devices on the same network.

Ransomware: A malicious attack where threat actors encrypt an organization's data and demand payment to restore access.

Spyware: Malware that’s used to gather and sell information without consent. Spyware can be used to access devices. This allows threat actors to collect personal data, such as private emails, texts, voice and image recordings, and locations.

Social Engineering

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. Human error is usually a result of trusting someone without question. It’s the mission of a threat actor, acting as a social engineer, to create an environment of false trust and lies to exploit as many people as possible.

Types of social engineering

Social media phishing: A threat actor collects detailed information about their target from social media sites. Then, they initiate an attack.
Watering hole attack: A threat actor attacks a website frequently visited by a specific group of users.
USB baiting: A threat actor strategically leaves a malware USB stick for an employee to find and install, to unknowingly infect a network.
Physical social engineering: A threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location.

Social engineering principles

Social engineering is incredibly effective. This is because people are generally trusting and conditioned to respect authority. The number of social engineering attacks is increasing with every new social media application that allows public access to people's data. Although sharing personal data—such as your location or photos—can be convenient, it's also a risk.

Authority: Threat actors impersonate individuals with power. This is because people, in general, have been conditioned to respect and follow authority figures.

Intimidation: Threat actors use bullying tactics. This includes persuading and intimidating victims into doing what they're told.

Consensus/Social proof: Because people sometimes do things that they believe many others are doing, threat actors use others' trust to pretend they are legitimate. For example, a threat actor might try to gain access to private data by telling an employee that other people at the company have given them access to that data in the past.

Scarcity: A tactic used to imply that goods or services are in limited supply.

Familiarity: Threat actors establish a fake emotional connection with users that can be exploited.

Trust: Threat actors establish an emotional relationship with users that can be exploited over time. They use this relationship to develop trust and gain personal information.

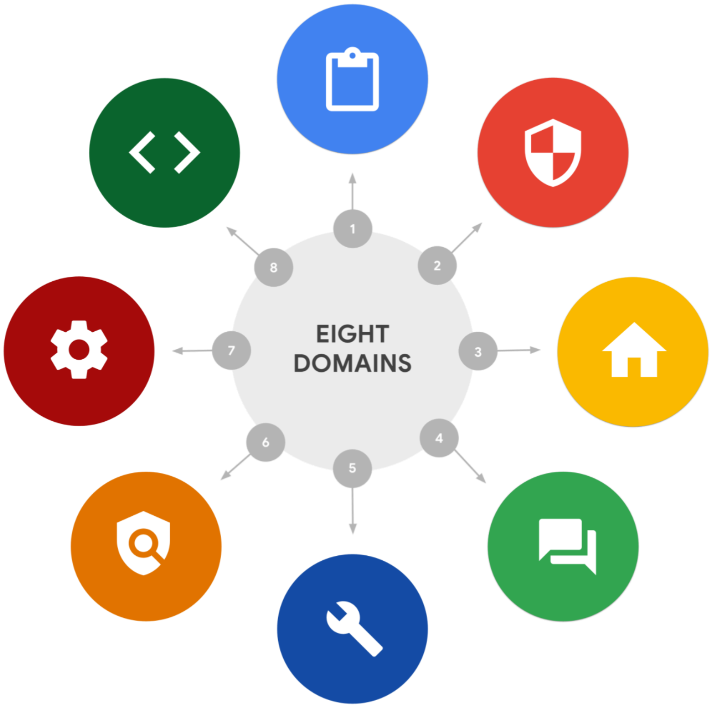
Urgency: A threat actor persuades others to respond quickly and without questioning.

CISSP Security Domains

Certified Information Systems Security Professional (CISSP) is one of the gold standard and most sought information security certification for proving knowledge in Cybersecurity. This validates the professionals for their information and experience to build and manage security architects for the organization.

Maintained by a non-profit organization, International Information System Security Certification Consortium (ISC)2 develops & maintains the CISSP Domains and conducts examinations for professionals globally.

CISSP Common Body of Knowledge (CBK) is a collection of 8 domains that covers all the comprehensive aspects of information security and CISSP domains explained



Security and Risk Management

Focuses on defining security goals and objectives, risk mitigation, compliance, business continuity, and the law.

Asset Security

Focuses on securing digital and physical assets, including the storage, maintenance, retention, and destruction of data.

Security Architecture and Engineering

Focuses on optimizing data security through effective tools, systems, and processes, such as configuring firewalls.

Communication and Network Security

Focuses on managing and securing physical networks and wireless communications, including analyzing user behavior and creating network policies.

Identity and Access Management (IAM)

Focuses on securing data by controlling and managing physical and logical assets. Validates employee identities and assigns access roles to maintain physical and digital security.

Security Assessment and Testing

Focuses on conducting security control testing, analyzing data, and conducting audits to monitor risks, threats, and vulnerabilities.
Regular audits of user permissions ensure appropriate access levels.

Security Operations

Focuses on conducting investigations and implementing preventative measures in response to security incidents.
Requires following organizational policies and procedures to address potential threats.

Software Development Security

Focuses on using secure coding practices to create secure applications and services. Security analysts collaborate with software development teams to incorporate security practices into the software development life-cycle.

Attack types based on security domain

Password attack

A **Password Attack** is an attempt to access password-secured devices, systems, networks, or data.
Brute force
Rainbow table

Password attacks fall under the **communication** and **network security** domain.

Social engineering attack

Social Engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.

Phishing
Smishing
Vishing
Spear phishing
Whaling
Social media phishing
Business Email Compromise (BEC)
Watering hole attack
USB (Universal Serial Bus) baiting
Physical social engineering

Social Engineering Attacks are related to the **Security** and **Risk Management** domain.

Physical attack

A **Physical Attack** is a security incident that affects not only digital but also physical environments where the incident is deployed.

Malicious USB cable
Malicious flash drive
Card cloning and skimming

Physical Attacks fall under the **Asset Security** domain.

Adversarial Artificial Intelligence

Adversarial Artificial Intelligence is a technique that **Manipulates Artificial Intelligence** and **Machine Learning** technology to conduct attacks more efficiently.

Adversarial Artificial Intelligence falls under both the **Communication** and **Network Security** and the **Identity And Access Management** domains.

Supply-Chain Attack

A **Supply-Chain Attack** targets systems, applications, hardware, and/or software to locate a vulnerability where malware can be deployed (**Targets The Weakest Link In A Supply Chain**). Because every item sold undergoes a process that involves third parties, this means that the security breach can occur at any point in the supply chain. These attacks are costly because they can affect multiple organizations and the individuals who work for them.

Supply-chain attacks can fall under several domains, including but not limited to the **Security And Risk Management**, **Security Architecture** and **Engineering, And Security Operations** domains.

Cryptographic Attack

A **Cryptographic Attack** affects secure forms of communication between a sender and intended recipient.

Birthday
Collision
Downgrade

Cryptographic attacks fall under the **Communication And Network Security** domain.

Understand attackers

As a reminder, a **Threat Actor** is any person or group who presents a security risk.

Threat Actor Types

Advanced Persistent Threats

Advanced Persistent Threats (APTs) have significant expertise accessing an organization's network without authorization. APTs tend to research their targets (e.g., large corporations or government entities) in advance and can remain undetected for an extended period of time.

Their intentions and motivations can include:
Damaging critical infrastructure, such as the power grid and natural resources
Gaining access to intellectual property, such as trade secrets or patents

Insider Threats

Insider Threats abuse their authorized access to obtain data that may harm an organization.

Their intentions and motivations can include:
Sabotage
Corruption
Espionage
Unauthorized data access or leaks

Hacktivists

Hacktivists are threat actors that are driven by a **Political Agenda**.

They abuse digital technology to accomplish their goals, which may include:

Demonstrations

Propaganda

Social change campaigns

Fame

Hacker Types

Six hackers on computers.

A **Hacker** is any person who uses computers to gain access to computer systems, networks, or data. They can be beginner or advanced technology professionals who use their skills for a variety of reasons. There are three main categories of hackers:

Authorized Hackers are also called **Ethical Hackers**. They follow a code of ethics and adhere to the law to conduct organizational risk evaluations. They are motivated to safeguard people and organizations from malicious threat actors.

Semi-Authorized Hackers are considered **Researchers**. They search for vulnerabilities but don’t take advantage of the vulnerabilities they find.

Unauthorized Hackers are also called **Unethical Hackers**. They are malicious threat actors who do not follow or respect the law. Their goal is to collect and sell confidential data for financial gain.

Glossary terms from module 2

Terms and definitions from Course 1, Module 2

Adversarial artificial intelligence (AI): A technique that manipulates artificial intelligence (AI) and machine learning (ML) technology to conduct attacks more efficiently

Business Email Compromise (BEC): A type of phishing attack where a threat actor impersonates a known source to obtain financial advantage

CISSP: Certified Information Systems Security Professional is a globally recognized and highly sought-after information security certification, awarded by the International Information Systems Security Certification Consortium

Computer virus: Malicious code written to interfere with computer operations and cause damage to data and software

Cryptographic attack: An attack that affects secure forms of communication between a sender and intended recipient

Hacker: Any person who uses computers to gain access to computer systems, networks, or data

Malware: Software designed to harm devices or networks

Password attack: An attempt to access password secured devices, systems, networks, or data

Phishing: The use of digital communications to trick people into revealing sensitive data or deploying malicious software

Physical attack: A security incident that affects not only digital but also physical environments where the incident is deployed

Physical social engineering: An attack in which a threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location

Social engineering: A manipulation technique that exploits human error to gain private information, access, or valuables

Social media phishing: A type of attack where a threat actor collects detailed information about their target on social media sites before initiating the attack

Spear phishing: A malicious email attack targeting a specific user or group of users, appearing to originate from a trusted source

Supply-chain attack: An attack that targets systems, applications, hardware, and/or software to locate a vulnerability where malware can be deployed

USB baiting: An attack in which a threat actor strategically leaves a malware USB stick for an employee to find and install to unknowingly infect a network

Virus: refer to "computer virus"

Vishing: The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source

Watering hole attack: A type of attack when a threat actor compromises a website frequently visited by a specific group of users