CompTIA Security+

SECURITY+ EXAM CRAM

THE COMPLETE COURSE

2024 EDITION

DOMAIN 2

Coverage of every topic in the official exam syllabus!

with **Pete Zerger** vCISO, CISSP, MVP

2.0 THREATS, VULNERABILITIES, AND MITIGATIONS

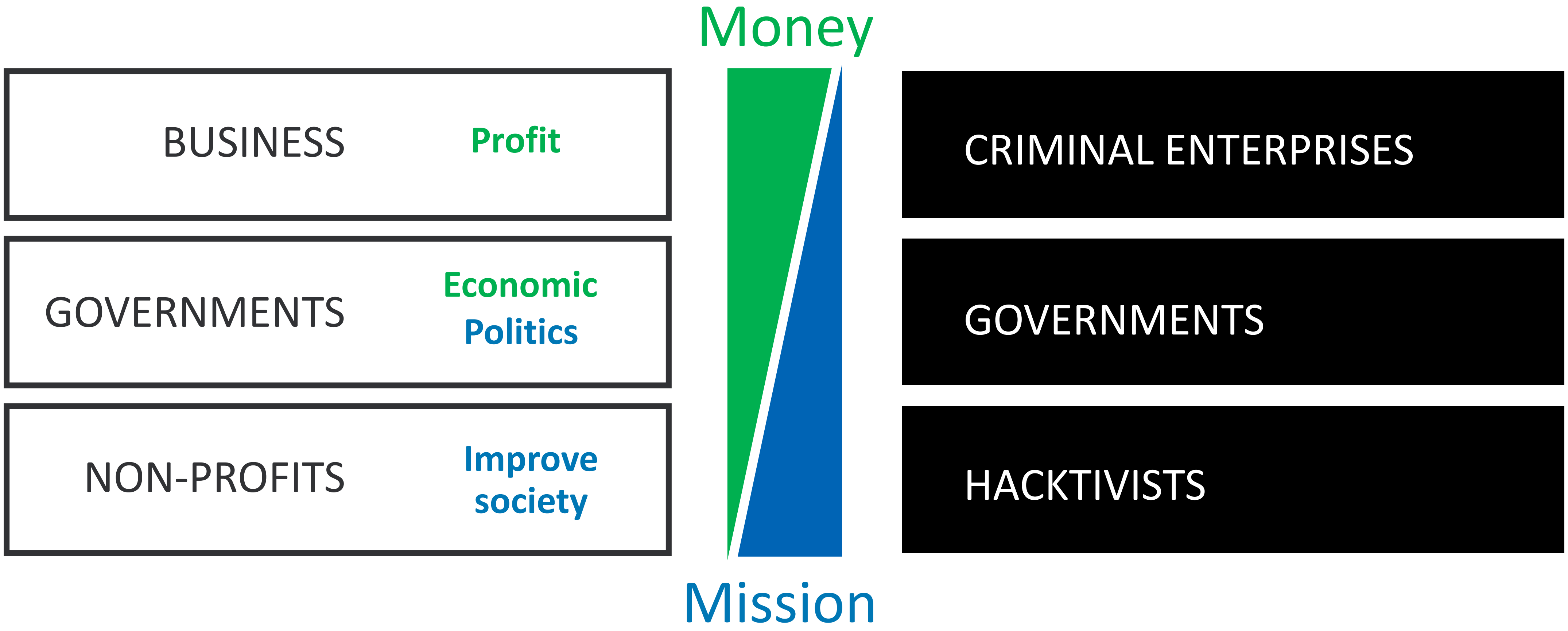
2.1 Compare and contrast common threat actors and motivations

- **Threat actors**
  - Nation-state
  - Unskilled attacker
  - Hacktivist
  - Insider threat
  - Organized crime
  - Shadow IT
- **Attributes of actors**
  - Internal/external
  - Resources/funding
  - Level of sophistication/capability

- **Motivations**
  - Data exfiltration
  - Espionage
  - Service disruption
  - Blackmail
  - Financial gain
  - Philosophical/political beliefs
  - Ethical
  - Revenge
  - Disruption/chaos
  - War

THREAT ACTORS, ATTRIBUTES, AND MOTIVATIONS

Categorical perspective



Money

BUSINESS — Profit

GOVERNMENTS — Economic, Politics

NON-PROFITS — Improve society

CRIMINAL ENTERPRISES

GOVERNMENTS

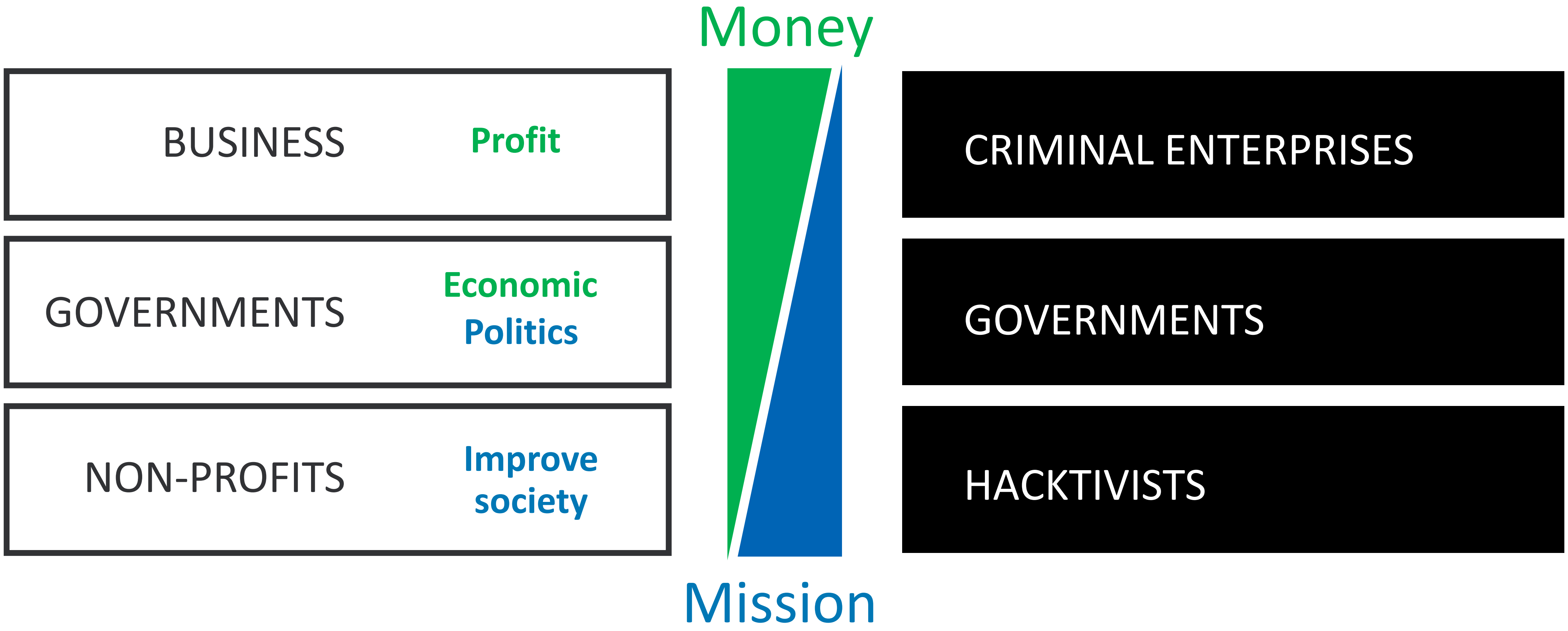
HACKTIVISTS

Mission

The motivations and incentives for different types of attacker's mirror those of legitimate organizations.

THREAT ACTORS, ATTRIBUTES, AND MOTIVATIONS

Categorical perspective



Money

BUSINESS — Profit

GOVERNMENTS — Economic, Politics

NON-PROFITS — Improve society

CRIMINAL ENTERPRISES

GOVERNMENTS

HACKTIVISTS

Mission

Understanding attackers' motivations reveals probabilities and potential impacts, so you can establish priorities

THREAT ACTORS, ATTRIBUTES, AND MOTIVATIONS

Nation-state: A country's government that uses cyberattacks to disrupt or steal information from another country.

Unskilled attacker: Someone with limited technical knowledge who may launch attacks out of curiosity or malice.

Hacktivist: An individual or group that uses cyberattacks to promote a political or social cause.

Insider threat: An authorized internal user who intentionally or unintentionally misuses their access to harm a system or organization.

Organized crime: A criminal syndicate that uses cyberattacks for financial gain, such as stealing money or data.

Shadow IT: Employees leveraging unauthorized or unmanaged IT resources used within an organization, which can create security vulnerabilities.

While not exactly an actor itself, it creates an exploitable risk.

MOTIVATIONS

Data Exfiltration

The unauthorized removal of sensitive or proprietary information from a computer system.

Espionage

Cyberattacks conducted by organizations, including nation-states or corporations, with the goal of stealing confidential information from another organization.

Service Disruption

Attacks aimed at taking down or significantly hindering critical systems or networks, causing outages or disruptions to essential services.

MOTIVATIONS

Blackmail

Attacks that threaten to expose sensitive information or launch further attacks unless the victim submits to a demand, typically for money or other concessions.

Financial Gain

Attacks motivated by the desire to steal money or valuables through fraudulent activities.

Philosophical/Political Belief

Cyberattacks driven by ideological or political motivations, such as promoting a cause or ideology.

MOTIVATIONS

Ethical Hacking

Authorized simulated attacks conducted by security researchers or ethical hackers to identify vulnerabilities in a computer system and improve its overall security posture.

Revenge

Cyberattacks motivated by a desire to retaliate against an individual or organization for perceived wrongs, often causing public embarrassment or operational disruption.

Disruption/Chaos

Attacks aimed at causing widespread disruption and hindering normal operations of a system or network.

May be driven by personal satisfaction or furthering another agenda.

MOTIVATIONS

War

The use of cyberattacks by military forces or civilian groups to disrupt enemy military operations and gain an advantage in an armed conflict.

War waged through cyberattacks is often called 'cyberwarfare'

2.1 THREAT ACTORS, ATTRIBUTES, AND MOTIVATIONS

These are insiders (employees)

Threat Actor	Skill Level	Primary Motivation
Nation-State	High	Varies (Espionage, Disruption, Power)
Organized Crime	High	Financial Gain (Extortion, Fraud)
Insider Threat	Varies	Varies (Financial Gain, Disgruntled Employee, Espionage)
Hacktivist	Varies	Values (Social/Political Causes)
Unskilled Attacker	Low	Varies (Curiosity, Malice, Financial Gain)
Shadow IT	Varies	Varies (Productivity, Avoiding Bureaucracy)

2.1 THREAT ACTORS, ATTRIBUTES, AND MOTIVATIONS

Threat Actor	Attributes	Motivations	Example
Nation-State	- Advanced capabilities - Extensive resources - Government backing	- Espionage (stealing secrets) - Disrupting critical infrastructure - Developing cyber weapons	Stealing intellectual property from a foreign competitor
Unskilled Attacker	- Limited knowledge - Often use automated tools	- Curiosity - Malice (causing disruption) - Financial gain (through scams)	Launching a phishing campaign against random email addresses
Hacktivist	- Strong ideological beliefs - Technical skills vary	- Promoting a social/political cause - Disrupting orgs they disagree with	Leaking sensitive data from a corporation they believe is unethical
Insider Threat	- Authorized access to systems/data	- Disgruntled employee - Financial gain - Espionage for a competitor	Selling customer data on the black market
Organized Crime	- High level of organization - Sophisticated tools and techniques	- Financial gain (thru extortion, fraud) - Power and control	Ransomware attack on a major hospital chain
Shadow IT	- Unapproved use of technology	- Increased productivity (perceived) - Avoiding bureaucracy	Creating a cloud storage account outside of IT department control, exposing sensitive data

IMPACT OF SKILL AND FUNDING

How do threat actor **skill** and **funding level** impact the threat to the organization?

Skill Level

High Skill: Highly skilled attackers, can exploit complex vulnerabilities, bypass security measures, and remain undetected for extended periods.

They can target specific systems or individuals within an organization, making them highly dangerous.

Low Skill: Unskilled attackers are less likely to launch sophisticated attacks. They may rely on readily available tools or exploit well-known vulnerabilities.

However, even unskilled attackers can be dangerous if they target a vulnerable system or trick employees into compromising security (e.g., phishing attacks).

IMPACT OF SKILL AND FUNDING

How do threat actor **skill** and **funding level** impact the threat to the organization?

Funding Level

High Funding: Well-funded actors, like nation-states and organized crime groups, can invest in advanced tools, hire skilled attackers, and develop custom malware.

This allows them to target a wider range of organizations and launch more complex attacks.

Low Funding: Low-funded attackers may rely on free or readily available tools. This can limit their capabilities, but it doesn't eliminate the threat.

They can still exploit basic vulnerabilities or launch social engineering attacks that don't require significant resources.

Patch hygiene, employee awareness, and layered defense all help mitigate

IMPACT OF SKILL AND FUNDING

COMBINED IMPACT

Skill Level	Funding Level	Danger to Organization
High	High	Most Dangerous
High	Low	Dangerous
Low	High	Moderately Dangerous
Low	Low	Less Dangerous, but Still a Threat

IMPACT OF SKILL AND FUNDING

COMBINED IMPACT

The combination of high skill and high funding creates the most dangerous threat actors.

Skill Level	Funding Level	Danger to Organization
High	**High**	**Most Dangerous**
High	Low	Dangerous
Low	High	Moderately Dangerous
Low	Low	Less Dangerous, but Still a Threat

They have the resources to develop and launch sophisticated attacks that are difficult to defend against.

2.0 THREATS, VULNERABILITIES, AND MITIGATIONS

2.2 Explain common threat vectors and attack surfaces.

- **Message-based**
  - Email
  - Short Message Service (SMS)
  - Instant messaging (IM)
- **Image-based**
- **File-based**
- **Voice call**
- **Removable device**
- **Vulnerable software**
  - Client-based vs. agentless
- **Unsupported systems and applications**

- **Unsecure networks**
  - Wireless
  - Wired
  - Bluetooth
- **Open service ports**
- **Default credentials**
- **Supply chain**
  - Managed service providers (MSPs)
  - Vendors
  - Suppliers

- **Human vectors/social engineering**
  - Phishing
  - Vishing
  - Smishing
  - Misinformation/disinformation
  - Impersonation
  - Business email compromise
  - Pretexting
  - Watering hole
  - Brand impersonation
  - Typosquatting

THREAT VECTOR vs ATTACK SURFACE Definitions

Threat Vector

A method or combination of methods that attackers use to gain unauthorized access to a computer system, network, or data.

Think of it as the pathway an attacker takes to exploit a vulnerability.

EXAMPLES:
Phishing emails, malware in attachments, unpatched software vulnerabilities, social engineering tactics.

THREAT VECTOR vs ATTACK SURFACE Definitions

Attack Surface

The sum total of all the possible entry points that an attacker can exploit to gain access to a system.

It's the broader landscape of weaknesses an organization or individual presents.

A larger attack surface means there are more potential threat vectors attackers can utilize

EXAMPLES:
Unsecured devices, weak passwords, open service ports, outdated software, reliance on untrusted sources.

THREAT VECTOR vs ATTACK SURFACE An analogy

Imagine a castle

The **threat vector** would be a specific way to breach the castle, like scaling a weak wall or bribing a guard.

The **attack surface** would be the entire castle itself, including all its walls, gates, and potential weaknesses.

RELATIONSHIP

The *stronger* the castle's defenses, the *smaller* the attack surface will be.

And the *fewer effective ways* (threat vectors) attackers will have to breach it.

THREAT VECTOR vs ATTACK SURFACE

TYPE: Message-based

Email:

Threat Vectors

Phishing emails with malicious attachments or links, spam containing malware, email spoofing for social engineering attacks.

Attack Surfaces

Unprotected email accounts, weak passwords, lack of multi-factor authentication (MFA), poorly configured email filters.

Modern email security will evaluate/execute URLs and attachments

THREAT VECTOR vs ATTACK SURFACE

TYPE: Message-based

SMS (Short Message Service):

Threat Vectors

Smishing attacks with malicious links, SIM swapping for account takeover.

Attack Surfaces

Unsecured mobile devices, weak SMS verification processes, lack of awareness about smishing threats.

Mobile providers offer free software to reduce this threat

THREAT VECTOR vs ATTACK SURFACE

TYPE: Message-based

Instant Message:

Threat Vectors

Malicious links or files shared within IM chats, social engineering attacks impersonating contacts.

Attack Surfaces

Unencrypted IM platforms, lack of user access controls within IM applications.

THREAT VECTOR vs ATTACK SURFACE

TYPE: Image-based

Threat Vectors

Steganography (hiding malware within images), phishing attacks using fake images to lure victims.

Attack Surfaces

Downloading images from untrusted sources, opening image attachments without proper scanning.

Image-based generative AI is fueling an expansion of fake image threat

THREAT VECTOR vs ATTACK SURFACE

TYPE: File-based

COUNTERMEASRES
user awareness training, good software hygiene and email security

Threat Vectors

Malware hidden within files (e.g., documents, executables), zero-day vulnerabilities exploited through file attachments.

Attack Surfaces

Downloading files from untrusted sources, opening attachments without proper scanning, outdated software with unpatched vulnerabilities.

THREAT VECTOR vs ATTACK SURFACE

TYPE: Voice Call

Threat Vectors

Vishing attacks where attackers attempt to steal information over the phone by impersonating legitimate callers.

Attack Surfaces

Lack of awareness about vishing threats, weak user authentication processes over the phone.

AI-based voice deep fakes make 'stop and verify' a necessity!

THREAT VECTOR vs ATTACK SURFACE

TYPE: Vulnerable Software

Client-based:

Threat Vectors

Unpatched software with known vulnerabilities, outdated applications with security flaws.

Attack Surfaces

Outdated operating systems and applications, lack of automated software update processes.

Good software hygiene is the fix. Keep up with version upgrades and security patches

THREAT VECTOR vs ATTACK SURFACE

TYPE: Vulnerable Software

Agentless:

Threat Vectors

Exploiting vulnerabilities in the main software that doesn't require a separate agent for infection.

Attack Surfaces

While attack surface is less, less configurability, limited patching options, and increased reliance on vendor security are risks.

Discuss these concerns with the software vendor

THREAT VECTOR vs ATTACK SURFACE

TYPE: Unsupported Systems and Applications

Threat Vectors

Attackers targeting known vulnerabilities in unsupported software without security patches.

Attack Surfaces

Using outdated and unsupported operating systems or applications due to lack of upgrade options.

Network segmentation and/or isolation important in this case

THREAT VECTOR vs ATTACK SURFACE

TYPE: Unsecure Networks

Wireless:

Threat Vectors

Man-in-the-middle attacks on unencrypted Wi-Fi networks, eavesdropping on network traffic.

Attack Surfaces

Connecting to public Wi-Fi networks without a VPN, using weak encryption protocols on wireless networks.

Minimize use of public wi-fi, and keep access points updated and patched

THREAT VECTOR vs ATTACK SURFACE

TYPE: Unsecure Networks

Wired:

Threat Vectors

Physical access to a wired network for unauthorized access, malware spreading through the network.

Attack Surfaces

Weak network segmentation, lack of physical security measures for network equipment.

Network segmentation or micro-segmentation are key defenses

THREAT VECTOR vs ATTACK SURFACE

TYPE: Unsecure Networks

Bluetooth:

Threat Vectors

Bluetooth hijacking for data theft or malware infection.

Attack Surfaces

Unidentified or unsecured Bluetooth connections, leaving Bluetooth enabled on devices even when not in use.

THREAT VECTOR vs ATTACK SURFACE

TYPE: Open Service Ports

Threat Vectors

Attackers exploiting vulnerabilities in exposed services running on specific ports.

Attack Surfaces

Unnecessary services running on a system, failure to disable unused ports, inadequate network access control.

THREAT VECTOR vs ATTACK SURFACE

TYPE: Default Credentials

Threat Vectors

Brute-force attacks to guess default usernames and passwords for system access.

Attack Surfaces

Leaving devices or applications with factory default credentials, lack of strong password policies.

THREAT VECTOR vs ATTACK SURFACE

TYPE: Supply Chain

Managed Service Providers (MSPs), Vendors, Suppliers

Threat Vectors

Compromised systems, software, or services within a supplier's network leading to attacks on their clients.

Attack Surfaces

Lack of vendor risk management, limited visibility into vulnerabilities and security practices of third-party providers.

Direct or Indirect exposure to all of a vendor’s vulnerabilities

PRINCIPLES OF SOCIAL ENGINEERING

Principles of social engineering success

Authority

Citing position, responsibility, or affiliation that grants the attacker the authority to make the request.

Intimidation

Suggesting you may face negative outcomes if you do not facilitate access or initiate a process.

Consensus

Claiming that someone in a similar position or peer has carried out the same task in the past.

Scarcity quantity

Limited opportunity, diminishing availability that requires we get this done in a certain amount of time, similar to urgency.

PRINCIPLES OF SOCIAL ENGINEERING

Principles of social engineering success

Familiarity

aka 'liking'

Attempting to establish a personal connection, often citing mutual acquaintances, social proof.

Trust

Citing knowledge and experience, assisting the target with an issue, to establish a relationship.

Urgency

Time sensitivity that demands immediate action, similar to scarcity

SOCIAL ENGINEERING TECHNIQUES

Best defense for both is security awareness training (user education)

Social Engineering

an attempt by an attacker to convince someone to provide info (like a password) or perform an action they wouldn't normally perform (such as clicking on a malicious link)

Social engineers may try to gain access to the IT infrastructure or the physical facility.

Phishing

commonly used to try to trick users into giving up personal information (such as user accounts and passwords), click a malicious link, or open a malicious attachment.

Spear phishing targets specific groups of users

Whaling targets high-level executives

Vishing (voice phishing) phone-based

Smishing uses sms(text) messaging on mobile

phishing is #1 cyber attack!

An entry point for ransomware!

Know all these variants!

THREAT VECTOR vs ATTACK SURFACE

TYPE: Human Vectors/Social Engineering

Phishing, Vishing, Smishing:

Threat Vectors

Deceptive emails, phone calls, or SMS messages tricking users into revealing sensitive information or clicking malicious links.

Attack Surfaces

Lack of user awareness about social engineering tactics, susceptibility to pressure or urgency tactics.

TWO DEFENSES: Show user less malicious content AND reduce the likelihood they will click or respond to requests within the malicious content.

THREAT VECTOR vs ATTACK SURFACE

TYPE: Human Vectors/Social Engineering

Misinformation/Disinformation:

Threat Vectors

Spreading false or misleading information to manipulate public opinion or disrupt decision-making.

Attack Surfaces

Reliance on unverified sources of information, difficulty in discerning truth from fiction online.

User education/awareness training will reduce this risk.

THREAT VECTOR vs ATTACK SURFACE

TYPE: Human Vectors/Social Engineering

Impersonation/Business Email Compromise:

Threat Vectors

Attackers and their creativity in leveraging social engineering principles are the primary threat vectors.

Attack Surfaces

User vulnerability to emotional manipulation, deceptive content, as well as exploitation of their trust.

Generative AI has made attacks more difficult to detect

PRETEXTING

an attacker tries to convince a victim to give up information of value, or access to a service or system.

The distinguishing feature…
Is that the attacker develops a story, or pretext, in order to fool the victim.

The pretext often leans on establishing authority for the attacker as someone who should have access to information.

The pretext often includes a ***character*** played by the scam artist, and a ***plausible situation*** in which that character needs access to information.

THREAT VECTOR vs ATTACK SURFACE

TYPE: Human Vectors/Social Engineering

Pretexting:

Threat Vectors

Deceptive communication where an attacker invents a scenario (pretext) to gain a victim's trust and extract information or access.

Attack Surfaces

Lack of verification procedures for callers or requests, user willingness to help without proper caution.

Teaching users to 'pause and verify' can reduce risk

THREAT VECTOR vs ATTACK SURFACE

TYPE: Human Vectors/Social Engineering

Brand Impersonation:

Threat Vectors

Attackers create websites, social media accounts, or emails that closely resemble those of a legitimate brand to trick victims into revealing personal information or clicking malicious links.

Attack Surfaces

Lack of attention to detail when interacting with online content, not verifying the legitimacy of a website or sender.

TYPOSQUATTING

Typosquatting

aka "URL hijacking"

a form of cybersquatting (sitting on sites under someone else's brand or copyright) targeting users who type an incorrect website address

Often employ a **drive-by download** that can infect a device even if the user does not click anything

THREAT VECTOR vs ATTACK SURFACE

TYPE: Human Vectors/Social Engineering

Typosquatting:

Threat Vectors

Attackers register domain names with slight misspellings of popular websites (e.g., googel.com instead of google.com).

When users mistype the address, they are directed to a malicious website that might steal login credentials or infect their device.

Attack Surfaces

Mistyping website addresses, not checking the URL carefully before entering login information.

2.0 THREATS, VULNERABILITIES, AND MITIGATIONS

2.3 Explain various types of vulnerabilities.

- **Application**
  - Memory injection
  - Buffer overflow
  - Race conditions
    - Time-of-check (TOC)
    - Time-of-use (TOU);
  - Malicious update
- **Operating system (OS)-based**
- **Web-based**
  - Structured Query Language injection (SQLi)
  - Cross-site scripting (XSS)
- **Hardware**
  - Firmware
  - End-of-life
  - Legacy
- **Virtualization**
  - Virtual machine (VM) escape
  - Resource reuse
- **Cloud-specific**
- **Supply chain**
  - Service provider
  - Hardware provider
  - Software provider
- **Cryptographic**
- **Misconfiguration**
- **Mobile device**
  - Side loading
  - Jailbreaking
- **Zero-day**

IMPORTANT TERMS AND CONCEPTS

4 terms you must know before we begin

IMPORTANT TERMS AND CONCEPTS

Vulnerability

a weakness in a system, application, or infrastructure that can be exploited to gain unauthorized access or cause damage.

It's a flaw or gap in security that could be taken advantage of

Threat

a potential event that could exploit a vulnerability and cause harm.

It's the possibility of something bad happening

Exploit

a specific method or tool used to take advantage of a vulnerability.

It's like a recipe for hacking that leverages the system's weakness

Attack

the actual attempt to exploit a vulnerability to achieve a malicious goal.

How they relate

Think of these terms as steps in a potential security breach:

1 A **vulnerability** exists in a system.

2 A malicious actor identifies this **threat** and sees an opportunity.

3 The attacker develops or uses an existing **exploit** to take advantage of the vulnerability.

4 If successful, this becomes a full-blown **attack**, causing harm to the system or its data.

An analogy

Here’s an analogy that may be a helpful example:

Imagine a house with a weak lock (**vulnerability**).

A burglar (**threat**)…

sees this and uses a crowbar (**exploit**)…

to break in (**attack**).

By understanding these terms and their relationship, you can better identify and address security risks in your systems.

BUFFER OVERFLOWS

Attacks attackers use to exploit **poorly written software**.

Buffer Overflow

Exists when a developer writes code that does not validate user input to ensure it does not allow Input that is too large for its memory space

When this occurs, code or related data can "overflow" memory buffer

PREVENT with input validation

IDENTIFY with appropriate software testing

Maliciously inserting information into memory is known as **memory injection,** and is the primary goal of a buffer overflow attack.

INTEGER OVERFLOW

Putting too much information into too small of a space that has been set aside for numbers.

A type of arithmetic overflow error when the result of an integer operation does not fit within the allocated memory space.

Instead of an error handled in the program, it usually causes the result to be unexpected.

Often lead to buffer overflows, and generally ranked as one of the most dangerous software errors.

Error messages may include 'overflow' or 'arithmetic overflow'

Countermeasures: Secure coding practices, appropriate typing of variables, using larger variable types, like long (Java) or long int (C)

RACE CONDITIONS

A condition where the system's behavior is dependent on the **sequence or timing** of other uncontrollable events.

Time-of-Check (TOC) moment a system verifies access permissions or other security controls.

Time-of-Use (TOU) moment when the system accesses the resources or uses granted permissions.

Time-of-Check/Time-of-Use (TOCTOU)
a timing vulnerability that occurs when a program checks access permissions too far in advance of a resource request.

Malicious Updates

Where an attacker attempts to deploy a fake patch that designed to compromise the security of an application or operating system

And if systems only accept signed updates, the threat is mitigated

Software publishers can protect against this threat with **code signing**

OS-based vulnerabilities

Default settings

Many OSes today aim for 'secure defaults'

Default passwords, insecure settings, unneeded apps and services are all potential paths for attackers

Configurations/Misconfigurations

Are often intentional but may not be secure.

Use secure configuration baselines

Privilege escalation

Require auth to elevate (UAC, SUDO)

Vulnerabilities that allow attackers to gain higher privileges on a system than they should have, allowing access sensitive data or to install malware.

Zero-day

May target other apps, systems, data, and infra

Vulnerabilities that are unknown to the software or hardware vendor, and very dangerous because there is no patch available to fix them

Defense-in-depth with AI and next-gen capabilities (XDR, IDPS, CASB, etc.)

An OS has many features. Enabled features = greater attack surface!

WEB-BASED THREATS

Improper input handling

used to compromise web front-end and backend databases

SQL injection attacks

Use unexpected input to a web application to gain unauthorized access to an underlying database.

NOT new and can be prevented through good code practices

Countermeasures: Input validation, use stored procedures, and limit account privileges.

WEB-BASED THREATS

Exploits client-side trust, but the server plays a role

a type of injection using **malicious scripts**

Cross-site scripting (XSS)

A type of injection, in which malicious scripts are injected into otherwise benign and trusted websites (often thru input field).

Occurs when an attacker uses a web application to send malicious code to a different end user.

occurs when web apps contain 'reflected input'

DEFENSE: Input validation and filtering to catch malicious inputs. Validate **data length** AND **data type**.

An analogy

Here’s an analogy for XSS that may be helpful:

> Imagine a bakery accidentally mixing broken glass into a batch of cookies (**server-side vulnerability**).
>
> If someone eats those cookies (**client-side execution**), they'll get hurt.
>
> The bakery (**server**) is responsible for ensuring safe ingredients (**validated user input**).

2.3 HARDWARE

Hardware vulnerabilities require attention in the **design phase** because some compensating controls are hardware-based.

Firmware

Prevent with a TPM to facilitate a secure boot process

Firmware attacks can occur through the update process or one-off malicious downloads, impacting the boot process

End-of-life

Aging equipment that has some usable lifespan left. You should have a timeline for replacement in advance.

Replacement will require budget for new hardware, and project time and effort.

Legacy

Definition a bit less clear, but for the exam, is used to describe hardware, software, or devices that are unsupported.

2.3 VIRTUALIZATION

Virtualization

Server virtualization the process of dividing a physical server into multiple unique and isolated virtual servers by means of a software application (hypervisor).

related concepts indicate server virtualization is the focus

VM Escape

where an attacker gains access to a VM, then attacks either the host machine that holds all VMs, the hypervisor, or any of the other VMs.

Protection: ensure patches for hypervisor and VMs are always up to date, guest privileges are low. Server-level redundancy and HIPS/HIDS protection also effective.

Resource reuse

When cloud providers take hardware resources originally assigned to one customer and reuse them with another customer. Risk of data remanence due to incomplete erasure

Avoidance: make sure you encrypt your sensitive data so it cannot be recovered by the next customer through forensic techniques.

CLOUD-SPECIFIC VULNERABILITIES

The primary vulnerability in the cloud is that it is an Internet-based model

Organizations could be at risk if the CSP's public-facing infrastructure comes under attack

Any attack on your CSP or cloud vendor may be unrelated to you as an organization

Threat actors may be targeting the CSP or another tenant of the CSP

Risks can come from the other tenants as well.

Customers may be "collateral damage" of an attack on the CSP!

CLOUD-SPECIFIC VULNERABILITIES

Cloud-Specific Risks

The Cloud Security Alliance details the top cloud-specific security threats in their list titled "**The CSA Egregious 11**"

1. Data Breaches
2. Misconfiguration and inadequate change control
3. Lack of cloud security architecture and strategy
4. Insufficient identity, credential access and key management
5. Account hijacking
6. Insider threat
7. Insecure interfaces and APIs
8. Weak control plane
9. "Metastructure" and "applistructure" failures
10. Limited cloud usage visibility
11. Abuse and nefarious use of cloud services

The "CSA Egregious 11"

Data breaches Unintentional loss/oversharing is a "data leak"

Loss of sensitive data (PII, PHI, intellectual property) due to security breach.

Misconfiguration and inadequate change control

Software can offer the most secure configuration options, but if it is not properly set up, then the resulting system will have security issues.

Remediate risk through change and configuration management

Lack of cloud security, architecture, and strategy

As organizations migrate to the cloud, some overlook security, or fail to consider their obligations in the shared responsibility model.

Insufficient identity, credential access, and key management

The public cloud offers benefits over legacy on-premises environments but can also bring additional complexities.

Well-architected identity and access management (IAM), encryption, secret and key management are different than on-prem and essential

The "CSA Egregious 11"

Account hijacking ← Phishing is the most common approach

Credential theft, abuse, and/or elevation to carry out an attack.

Insider threat

Disgruntled employees, employee mistakes, and unintentional over-sharing.

Job rotation, privileged access management, auditing, security training

Insecure interfaces and APIs

Customers failing to secure access to systems gated by APIs, web consoles, etc.

Controls include MFA, RBAC, and key-based API access

Weak control plane

Weaknesses in the elements of a cloud system that enable cloud environment configuration and management (web console, CLI, and APIs)

Most CSPs offer reference architectures to ensure customers secure and isolate their dev/test/prod environments and data

DEMO

Insider threat protections offered by CSPs

EXAMPLE FOR CONTEXT:
Capabilities will vary by CSP

The "CSA Egregious 11"

Metastructure and applistructure failures
Vulnerabilities in the operational capabilities that CSPs make available, like APIs for accessing various cloud services.

If the CSP has inadequately secured these interfaces, any resulting solutions built on top of those services will inherit these weaknesses.

Metastructure. The protocols and mechanisms that provide the interface between the cloud layers, enabling management and configuration.

Applistructure. Applications deployed in the cloud and the underlying application services used to build them.

e.g. PaaS features like message queues, functions, and message services

Responsibility? Mitigation?
Mitigating risks in this area is the responsibility of the CSP. Customers should verify the CSP has implemented their own SSDLC to ensure service security.

The "CSA Egregious 11"

Limited cloud usage visibility
Refers to when organizations experience a significant reduction in visibility over their information technology stack.

This is because in some models, the CSP own the stack!

Abuse and nefarious use of cloud services
While the low cost and high scale of compute in the cloud is an advantage to enterprises, it is an opportunity for attackers to execute disruptive attacks at scale.

Makes executing DDoS and phishing attacks easier, so CSPs must implement mitigating security controls for these risks

RISK MITIGATION STRATEGIES

There are several approaches to risk mitigation in cloud environments.

Selecting a qualified CSP is an essential first step.

The next step is designing and architecting with security in mind.

Security should be considered at every step starting with design!

The next risk mitigation tool is encryption, and data should be encrypted at rest and in-transit.

Storage and database encryption at rest, TLS and VPN in-transit

Finally, ongoing monitoring and management to maintain posture.

Major CSPs provide the ability to manage and monitor configuration security, and to monitor changes to cloud services, and track usage

CompTIA Security+

SECURITY+ EXAM CRAM

THE COMPLETE COURSE

DEMO

Ongoing monitoring to maintain security posture

EXAMPLE FOR CONTEXT:
Capabilities will vary by CSP

INSIDE CLOUD AND SECURITY

2.3 SUPPLY CHAIN

Sophisticated attackers may attempt to indirectly interfere with an organizations business through their **supply chain**

Attackers may gain access to **hardware devices** at the manufacturer or while in transit from the manufacturer to the end user.

They may install backdoors or other malware for device control

Attackers may also target **software providers**, inserting vulnerabilities into software before it is released

Attackers may compromise **managed service providers (MSPs)** to gain access to their network and by association, the customers they service

PREVENTION: Effective vendor management practices that uncover service providers security posture and practices reduce risk.

2.3 CRYPTOGRAPHIC VULNERABILITIES

Cryptographic Vulnerabilities

The weaknesses or flaws in a cryptographic system that can be exploited to compromise system security.

1. Weak encryption
2. Improper key management
3. Inadequate randomness
4. Inadequate authentication
5. Key lifetimes
6. Public key length
7. Symmetric key length
8. Strength of implementation

Vulnerabilities can lead to severe consequences, like exposure of sensitive data, unauthorized system access, and other security breaches

2.3 CRYPTOGRAPHIC VULNERABILITIES

Examples of **cryptographic vulnerabilities** explained

Weak encryption

Using an encryption algorithm no longer considered secure, such as DES or RSA with a small key size, can make it easier for an attacker to decrypt information.

Make sure you select algorithms well-suited to the use case and widely accepted as secure

Improper key management

Failing to protect access to encryption keys adequately can compromise the sensitive information they protect.

Keys should be stored in an access-restricted store or vault

Inadequate randomness

Some cryptographic algorithms, such as generating session keys, require a source of valid random numbers.

Use a True Random Number Generator (TRNG), not a Pseudo Random Number Generator (PRNG), which can weaken encryption

2.3 CRYPTOGRAPHIC VULNERABILITIES

Examples of **cryptographic vulnerabilities** explained

Inadequate authentication

Failing to authenticate parties properly in a cryptographic exchange can lead to man-in-the-middle attacks, where an attacker intercepts and alters communications.

Key Lifetimes

The length of time a key is used for encryption can affect the security of the cryptographic system.

For example, client and server certificates should typically have a lifespan of no more than approximately one year

Public key length

Given a key of the same length, public key cryptography is generally more vulnerable to attacks than symmetric key cryptography.

2048-bit key length is suggested for x.509 certificates

2.3 CRYPTOGRAPHIC VULNERABILITIES

Examples of **cryptographic vulnerabilities** explained

Symmetric key length

The length of the symmetric key can also affect the security of the cryptographic system, even with a currently accepted algorithm.

AES with 256-bit key length is required in some U.S. gov't scenarios

Strength of implementation

Ensuring cryptographic solutions are properly implemented is as important as selection of secure solutions.

It's crucial to implement cryptographic systems as recommended and keep them updated to protect against these vulnerabilities.

Misconfiguration

Occurs when a configuration mistake is made, (human error), for which impact may vary.

PREVENT WITH

- Infrastructure-as-code
- Configuration management tools
- Continuous Integration/Continuous Delivery (CI/CD)
- Checklists and templates
- Change management (that requires test/review)
- Regular security audits and vulnerability scans

MOBILE DEVICE

Rooting/jailbreaking

Custom firmware downloads are used to root an Android mobile device.

Gives user a higher level of permissions on that device and removes some elements of vendor security.

Jailbreaking is the Apple's iOS equivalent of rooting on Android:

it allows you to run unauthorized software and remove device security restrictions.

You can still access the Apple App Store even though jailbreaking has been carried out.

For the exam: Rooting and jailbreaking remove the vendor restrictions on a mobile device to allow unsupported software to be installed.

MOBILE DEVICE

Third-party application stores

There is a danger of downloading apps from third-party app stores as there is no guarantee of the security of the app being installed.

This could pose a security risk, as vetting process for mobile apps in third-party stores may be less rigorous than official app stores.

Sideloading

Enables installing an application package in .apk format on a mobile device.

Useful for developers to run trial of third-party apps, but also allows unauthorized software to be run on a mobile device.

ZERO-DAY EXPLOITS

an attack that uses a vulnerability that is either unknown to anyone but the attacker or known only to a limited group of people.

basic security practices can often prevent!

ZERO-DAY EXPLOITS

an attack that uses a vulnerability that is either unknown to anyone but the attacker or known only to a limited group of people.

Today, AI, ML, and UEBA driven antivirus, SIEM, IDPS, and EDR/XDR solutions offer some defense

2.0 THREATS, VULNERABILITIES, AND MITIGATIONS

2.4 Given a scenario, analyze indicators of malicious activity.

- **Malware attacks**
  - Ransomware
  - Trojan
  - Worm
  - Spyware
  - Bloatware
  - Virus
  - Keylogger
  - Logic bomb
  - Rootkit
- **Physical attacks**
  - Brute force
  - Radio frequency identification (RFID) cloning
  - Environmental
- **Network attacks**
  - Distributed denial-of-service (DDoS)
    - ○ Amplified
    - ○ Reflected
  - Domain Name System (DNS) attacks
  - Wireless
  - On-path
  - Credential replay
  - Malicious code
- **Application attacks**
  - Injection
  - Buffer overflow
  - Privilege escalation
  - Forgery
  - Directory traversal
  - Replay
- **Cryptographic attacks**
  - Downgrade
  - Collision
  - Birthday
- **Password attacks**
  - Spraying
  - Brute force
- **Indicators**
  - Account lockout
  - Concurrent session usage
  - Blocked content
  - Impossible travel
  - Resource consumption
  - Resource inaccessibility
  - Out-of-cycle logging
  - Published/documented
  - Missing logs

IMPORTANT TERMS AND CONCEPTS

Indicators of Malicious Activity

Indicators

signs that something suspicious might be happening on a system or network.

can be technical (unusual login attempts, data exfiltration) or behavioral (employees downloading suspicious files)

Don't necessarily mean an attack is underway, but they warrant investigation

Malicious Activity

a potential event that could exploit a vulnerability and cause harm.

Can be detected by indicators, but some may be more subtle and require deeper investigation

Cyber Attack

a deliberate and focused attempt to exploit a system or network vulnerability to achieve a specific goal.

The actual execution of malicious activity with a specific goal in mind

An analogy

Here’s an analogy that may be a helpful example:

Indicators are like smoke detectors.

They might go off because of burning toast (***false positive***) or a real fire (***true positive***).

Malicious Activity is like seeing flames flickering in a window.

It suggests something bad is happening, but it could be an unattended candle or a full-blown fire.

Attack is the actual fire spreading through the house.

It's the most damaging event, confirming malicious intent and causing significant harm.

INDICATORS

Account lockouts

This happens when someone repeatedly fails to login with the correct credentials, suggesting brute-force attacks or stolen passwords.

Concurrent session usage

If someone has access from geographically impossible locations at the same time, it could indicate account compromise and someone else being logged in simultaneously.

Blocked content

Security systems might block access to malicious websites or files.

Frequent attempts to access blocked content could be a sign of malware trying to phone home.

INDICATORS

Impossible Travel Time

Login attempts from locations too far apart in a short time span might indicate stolen credentials being used elsewhere.

Resource Consumption

A sudden spike in resource usage (CPU, memory, network) could be malware running or a hacker trying to exploit system vulnerabilities.

Resource Inaccessibility

Critical resources being inaccessible could be a sign of a denial-of-service attack or malware tampering with systems.

INDICATORS

Out-of-Cycle Logging

Security systems typically log events on a schedule.

Unscheduled or unexpected logging activity could indicate tampering or an attempt to cover tracks.

Published/Documented

If a specific exploit or malware is well-known, security professionals might track instances where it's being used.

Missing Logs

Security logs are crucial for investigating incidents.

Missing logs could be a sign of tampering to avoid detection.

WHAT IS RANSOMWARE?

infects a target machine and then uses encryption technology to encrypt documents, spreadsheets, and other files stored on the system with a key known only to the malware creator.

WHAT IS RANSOMWARE?

user is then unable to access their files and receives an ominous pop-up message warning that the files will be permanently deleted unless a ransom is paid within a short period of time.

ransomware is a trojan variant

RANSOMWARE COUNTERMEASURES & PREVENTION

There are a number of countermeasures and prevention techniques:

COUNTERMEASURES

- Back up your computer
- Store backups separately
- User awareness training

cloud-hosted email and file storage ease this process!

RANSOMWARE COUNTERMEASURES & PREVENTION

There are a number of countermeasures and prevention techniques:

PREVENTION

- Update and patch computers
- Use caution with web links
- Use caution with email attachments
- Verify email senders
- Preventative software programs

AI-driven cloud services offer help with these

TROJAN

a software program that appears good and harmless but carries a malicious, hidden payload that has the potential to wreak havoc on a system or network.

good defense? 1) only allow software from trusted sources. 2) don't let users install software

2.4 INDICATORS OF MALWARE ATTACKS

Ransomware, Trojan, Spyware

Account lockout: Possible if malware attempts brute-force logins to gain access to additional systems.

Blocked content: May occur if security blocks malware upload or download attempts.

Resource consumption: High CPU, memory, or network usage due to malware processes.

Missing logs: Malware might try to tamper with logs to avoid detection.

MALWARE

Spyware

Software designed to monitor and steal a user's activity without their knowledge.

Can capture keystrokes, passwords, browsing habits, and other sensitive information.

HOW TO MITIGATE

Install and update anti-spyware software.

Be cautious of free software downloads that may contain spyware.

Adjust browser privacy settings to limit tracking.

Be mindful of what information you share online.

Use strong passwords and avoid using them on multiple websites.

MALWARE

Worm

A self-replicating program that spreads itself across a network, infecting other computers.

Can exploit vulnerabilities in software or hardware to propagate.

can consume resources, steal data, or disrupt system operations

HOW TO MITIGATE

Apply security patches promptly to close vulnerabilities.

Disable unnecessary network services and ports.

Use firewalls to control network traffic.

Educate users about not opening suspicious emails or attachments.

Regularly scan systems for malware infections.

2.4 INDICATORS OF MALWARE ATTACKS

Worm

Resource consumption: Worms can consume resources while replicating.

Network inaccessibility: Worms can overload networks making resources inaccessible.

Out-of-cycle logging: Security systems might log worm propagation attempts.

Published/documented: If a specific worm is known, security professionals might track its activity.

MALWARE

Bloatware

Unnecessary software pre-installed on a device that consumes resources and reduces performance.

not technically malicious but can be unwanted and difficult to remove.

HOW TO MITIGATE

- Research devices before purchase to understand pre-installed software.
- Look for options to remove bloatware during device setup.
- Use third-party uninstaller tools with caution (risk of removing critical software).

Bloatware, Keylogger

Resource consumption: Bloatware might consume moderate resources.

Missing logs: Keyloggers might try to hide their activity by tampering with logs.

MALWARE

Keylogger

Software or hardware that records every keystroke typed on a computer.

Can be used to steal login credentials, credit card information, and other sensitive data.

HOW TO MITIGATE

Use a virtual keyboard for sensitive information entry (prevents hardware keyloggers).

Enable two-factor authentication for added login security.

Be cautious of suspicious software downloads.

Update your operating system and applications regularly.

WHAT IS A COMPUTER VIRUS?

a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another.

a class of threat with many types

TYPES OF VIRUSES

A few examples of computer viruses

Multipartite Viruses

Multipartite viruses use more than one propagation technique in an attempt to penetrate systems that defend against only one method or the other.

Stealth Viruses

Stealth viruses hide themselves by actually tampering with the operating system to fool antivirus into thinking that everything is functioning normally.

Polymorphic Viruses

Polymorphic viruses actually modify their own code as they travel from system to system.

Know basic virus definition, indicators, and mitigation for exam

MALWARE

Logic Bomb

Malicious code designed to trigger a specific action at a predetermined time or event.

Can erase data, corrupt files, or disable systems.

HOW TO MITIGATE

- Implement strong access controls to prevent unauthorized code installation.
- Regularly review system logs for suspicious activity.
- Conduct security audits to identify vulnerabilities.
- Maintain backups of critical data for recovery in case of attack.

MALWARE

Rootkit

A stealthy program that provides an attacker with privileged access to a computer system.

Can hide files, processes, and network activity, and thus difficult to detect and remove.

HOW TO MITIGATE

Implement strong user authentication and access controls.

Regularly scan systems for rootkit infections using specialized tools.

Keep your operating system and applications up to date.

Be cautious of suspicious software downloads and attachments.

Monitor system logs for unusual activity.

Logic Bomb, Rootkit

Resource consumption:
Logic bombs might use resources before detonation, rootkits might use resources to maintain stealth.

Resource inaccessibility:
Logic bombs might detonate and render resources inaccessible;
Rootkits might hide critical resources.

Out-of-cycle logging:
Security systems might log suspicious activity related to logic bomb detonation or rootkit installation.

Missing logs:
Logic bombs and rootkits might tamper with logs to avoid detection.

2.4 INDICATORS OF PHYSICAL ATTACKS

Indicators of physical attack are obvious in retrospect, but prevention generally requires physical security controls

Brute-force attacks (but of the physical variety)

This means breaking locks, breaching locked doors and gates, or other means of unauthorized physical entry.

Alarms, physical barriers, patrols, inspections, high-security locks

2.4 INDICATORS OF PHYSICAL ATTACKS

Brute Force

Resource inaccessibility: Physical damage from breaking in might render resources inaccessible (e.g., servers in a damaged room).

Out-of-cycle logging: Security systems might log unusual activity related to the break-in, like triggered alarms or door sensor malfunctions.

Missing logs: An attacker might tamper with physical security logs or security cameras to hide evidence.

2.4 INDICATORS OF PHYSICAL ATTACKS

Indicators of physical attack are obvious in retrospect, but prevention generally requires physical security controls

Brute-force attacks (but of the physical variety)

This means breaking locks, breaching locked doors and gates, or other means of unauthorized physical entry.

Alarms, physical barriers, patrols, inspections, high-security locks

Radio frequency identification (RFID) cloning

These attacks work by cloning an RFID card, which can be difficult to detect if the RFID is the only identifier used.

Encryption, shielded badge holder, anomaly detection

RFID Cloning

Impossible travel:
This is a key indicator if a cloned RFID card is used from a location significantly different from the authorized user's typical location.

Missing logs:
An attacker might tamper with logs to hide unauthorized access via a cloned RFID tag

2.4 INDICATORS OF PHYSICAL ATTACKS

Indicators of physical attack are obvious in retrospect, but prevention generally requires physical security controls

Brute-force attacks (but of the physical variety)

This means breaking locks, breaching locked doors and gates, or other means of unauthorized physical entry.

Alarms, physical barriers, patrols, inspections, high-security locks

Radio frequency identification (RFID) cloning

These attacks work by cloning an RFID card, which can be difficult to detect if the RFID is the only identifier used.

Encryption, shielded badge holder, anomaly detection

Environmental attacks

May include attacks on HVAC, triggering a fire alarm/suppression, or physical tampering, like cutting cables.

Security cameras, alarms, and controlled access points

2.4 INDICATORS OF PHYSICAL ATTACKS

Environmental

Resource inaccessibility: Environmental attacks can render resources inaccessible (e.g., flooded server room, high heat damaging equipment).

Out-of-cycle logging: Security systems might log unusual environmental sensor readings (e.g., sudden temperature spikes, water leaks).

Missing logs: An attacker might tamper with security logs to hide their activity after causing environmental damage.

NETWORK ATTACKS

these are a class of attacks

Denial of-Service

is a resource consumption attack intended to prevent legitimate activity on a victimized system.

Distributed **Denial of-Service**

a DoS attack utilizing multiple compromised computer systems as sources of attack traffic.

COUNTERMEASURES: firewalls, routers, intrusion detection (IDS), SIEM, disable broadcast packets entering/leaving, disable echo replies, patching

NETWORK ATTACKS

The two main variants of DDoS

Reflected DDoS

involves the attacker sending requests to a third-party server with a spoofed source IP address (address of the target of the attack).

sends the response to the target instead of the attacker, overwhelming the target with unsolicited traffic.

Amplified DDoS

uses reflection techniques in combination with a technique called amplification.

a small request from the attacker generates a much larger response from the third-party server.

DDoS

Resource consumption: A massive spike in network traffic is a telltale sign of a DDoS attack.

Resource inaccessibility: Flooded networks can become inaccessible to legitimate users.

Out-of-cycle logging: Security systems might log unusual traffic patterns indicative of a DDoS attack.

Published/documented: If a large DDoS attack is underway, security professionals might be tracking it.

DNS ATTACKS

DNS Poisoning

attacker alters the domain-name-to-IP-address mappings in a DNS system

may redirect traffic to a rogue system OR perform denial-of-service against system.

DNS Spoofing

attacker sends false replies to a requesting system, beating the real reply from the valid DNS server.

COUNTERMEASURES: allow only authorized changes to DNS, restrict zone transfers, verified forwarders and log all privileged DNS activity.

DNS ATTACKS

Domain Hijacking

changes the registration of a domain through technical means, like exploiting a vulnerability with a domain registrar.

or through nontechnical means such as social engineering.

Enables domain's settings and configuration to be changed by the attacker

COUNTERMEASURES: using a secure domain registrar, use secure protocols like DNSSEC, strong access controls for DNS record mgmt.

DNS Attacks

Resource consumption:
DNS servers under attack might experience high resource usage.

Resource inaccessibility:
A successful attack might render internet resources inaccessible by redirecting traffic.

Out-of-cycle logging:
Security systems might log suspicious queries or attempts to modify DNS records.

Published/documented:
If a widespread DNS attack is happening, security professionals might track its activity.

Missing logs:
Attackers might tamper with logs to hide their activity.

WIRELESS ATTACKS

to prevent, use long pin, 2FA, and disable discovery mode

Bluejacking

annoyance

pranksters push unsolicited messages to engage or annoy other nearby Bluetooth through a loophole in Bluetooth messaging options

Bluesnarfing

data theft

data theft using Bluetooth. Vulnerable devices are those using bluetooth in public places with device in discoverable mode.

Bluebugging

eavesdropping or hacking

developed a year after bluejacking, creates a backdoor attack before returning control of the phone to its owner.

WIRELESS ATTACKS

Evil Twin

a malicious access point set up to appear to be a legitimate, trusted network.

Once a client connects to the evil twin, the attacker will typically provide Internet connectivity.

ROGUE Access Points

APs added to your network either intentionally or unintentionally.

Once connected, they can offer a point of entry to attackers or other unwanted users.

COUNTERMEASURES: Network monitoring, network segmentation, strong network protocols (WPA2, WPA3), periodic network scans.

Wireless Attacks

Blocked content: Security systems might block unauthorized access attempts on wireless networks.

Concurrent session usage: If unauthorized devices are accessing the network concurrently with legitimate ones.

Out-of-cycle logging: Security systems might log suspicious activity on wireless networks (e.g., rogue access points).

Missing logs: An attacker might tamper with logs to hide unauthorized wireless access.

ON-PATH (MAN-IN-THE-MIDDLE) ATTACK

Attacker sits in the middle between two endpoints and is able to intercept traffic, capturing (and potentially changing) information.

Fools both parties into communicating with the attacker (in between the two) instead of directly with each other.

Different versions of the attack exist, some affecting websites, email communications, DNS lookups, or Wi-Fi networks.

Countermeasures: only use secured Wi-Fi, VPN, HTTPS, and use multi-factor authentication.

On-Path Attacks

Blocked content: Security systems might block suspicious traffic patterns indicative of a man-in-the-middle attack.

Missing logs: Attackers might tamper with logs to hide their activity.

Credential Replay

Involves stealing or capturing legitimate login credentials (username and password, session token, etc.) and then reusing them to gain unauthorized access to a system or account.

RESULT: If successful, the attacker gains **unauthorized access** to the compromised account or system you can attempt account takeover, lateral movement, privilege escalation, etc.

Credential Replay

Involves stealing or capturing legitimate login credentials (username and password, session token, etc.) and then reusing them to gain unauthorized access to a system or account.

COUNTERMEASURES: Multi-Factor Authentication (MFA), regular password rotation, secure login protocols, session and idle timeout, security awareness training, and monitoring logs.

Credential Replay

Impossible travel: If stolen credentials are used from a location very different from the authorized user's typical location.

Account lockout: Multiple login attempts from various locations could trigger lockouts.

Concurrent session usage: Multiple logins from unexpected locations could indicate credential replay.

Higher likelihood of account lockout vs other network attacks

Malicious Code

Several malicious code attacks fall into the network category, target the communication channels and exploit vulnerabilities within the network itself, rather than individual devices.

EXAMPLES: Denial-of-Service (DoS/DDoS), On-path, credential replay

Malicious Code

Impossible travel: If stolen credentials are used from a location very different from the authorized user's typical location.

Account lockout: Multiple login attempts from various locations could trigger lockouts.

Concurrent session usage: Multiple logins from unexpected locations could indicate credential replay.

Out-of-cycle logging: A sudden increase in failed login attempts, unusual access times, or a significant rise in data transfer outside of normal usage patterns could indicate unauthorized access.

DIRECTORY TRAVERSAL

Gaining access to restricted directories

If an attacker is able to gain access to restricted directories through HTTP, it is known as a **directory traversal attack**.

One of the simplest ways to perform directory traversal is by using a ***command injection attack*** that carries out the action.

If successful, may allow attacker to get to site's root directory,

Most vulnerability scanners will check for weaknesses with directory traversal/command injection and inform you of their presence.

To secure your system, you should run a scanner and keep the web server software patched.

INJECTION

Improper input handling

used to compromise web front-end and backend databases

SQL injection attacks

Use unexpected input to a web application to gain unauthorized access to an underlying database.

NOT new and can be prevented through good code practices

Countermeasures: Input validation, use stored procedures, and limit account privileges, WAF.

BUFFER OVERFLOWS

Attacks attackers use to exploit **poorly written software**.

Buffer Overflow

Exists when a developer writes code that does not validate user input to ensure it does not allow Input that is too large for its memory space

When this occurs, code or related data can “overflow” memory buffer

PREVENT with input validation

IDENTIFY with appropriate software testing

Maliciously inserting information into memory is known as **memory injection,** and is the primary goal of a buffer overflow attack.

Injection, Buffer Overflow, Directory Traversal

Resource consumption:
Exploitation attempts might consume resources during the attack.

Resource inaccessibility:
A successful attack could render resources inaccessible by corrupting data or crashing applications.

Out-of-cycle logging:
Security systems might log suspicious activity related to the exploit attempt.

Published/documented:
If a specific vulnerability is known, security professionals might track exploit attempts.

Missing logs:
Attackers might try to tamper with logs to hide their activity.

Session Replay

Attack that targets web applications that rely on session tokens or cookies to identify and authenticate users.

CAPTURE: The attacker intercepts a legitimate user's login session with the application.

REPLAY: The attacker then uses the stolen token or cookie to replay the captured session

If successful, attacker gains access through a fake session that appears legitimate

COUNTERMEASURES: Short-lived session tokens, invalidate session on logout, CSRF protection, MFA, server-side validation

Session Replay

Concurrent session usage:
If a user has multiple login sessions happening simultaneously, especially from geographically distant locations, it could be a strong sign of a session replay attack.

Impossible travel:
Similar to concurrent session usage, seeing login activity from a location very far away from the user's usual location in a short timeframe can indicate a replay attack. Attackers might use stolen session tokens from anywhere in the world.

Out-of-cycle logging:
A sudden increase in successful logins from unusual locations or a significant rise in data transfer outside of normal usage patterns could suggest unauthorized access through a replayed session.

APPLICATION

Privilege Escalation

Vulnerability that allows attackers to gain higher privileges on a system than they should have

Potentially allows access sensitive data or to install malware.

To mitigate, require authentication to elevate (user access control on Windows, SUDO on Linux)

Privilege Escalation

Account lockout:
Possible if the attack involves brute-forcing privileged accounts.

Account lockout more likely for P.E. than other app attacks

Concurrent session usage:
Might occur if an attacker establishes a new privileged session alongside a legitimate one.

Resource consumption:
Exploitation attempts or privilege escalation might consume resources.

Out-of-cycle logging:
Security systems might log suspicious activity related to privilege escalation attempts.

Missing logs:
Attackers might try to tamper with logs to hide their activity.

REQUEST FORGERIES

exploits **website trust** to execute code

Cross-site request forgery (XSRF or **CSRF)**

similar to cross-site scripting attacks but exploits a different trust relationship.

exploits trust a website has for your browser to execute code on the user's computer.

create web apps that **use secure tokens**, and sites that **check the referring URL** in requests to ensure it came from local site!

REQUEST FORGERIES

Web App Firewalls (WAFs) can detect and block malicious requests

exploits the server's functionality to make **unintended requests**

Server-Side Request Forgery (SSRF)

A type of injection in which attacker targets a web application that fetches data from URLs provided by users.

The vulnerability lies in the server trusting the user-provided URL and acting upon it.

The server assumes the URL is safe because it originates from within the application itself (provided by the user).

DEFENSE: Input validation and sanitation, allowlist/denylist approach limiting the URLs accepted as input

Forgery

Blocked content: Security systems might block forged requests.

Out-of-cycle logging: Security systems might log suspicious activity related to forgery attempts (e.g., unusual login attempts).

Published/documented: If a specific forgery technique is known, security professionals might track its use.

CRYPTOGRAPHIC ATTACKS

Collision Attack

attack on a cryptographic hash to find two inputs that produce the same hash value

beat with collision-resistant hashing algorithms

2.4 INDICATORS OF CRYPTOGRAPHIC ATTACK

Collision Attack

Resource consumption: Large-scale collision attacks might consume significant resources during the calculation phase. (Less likely for most systems)

Published/documented: If a specific hashing algorithm is vulnerable to collisions and actively exploited, security professionals might track its use.

CRYPTOGRAPHIC ATTACKS

Collision Attack

attack on a cryptographic hash to find two inputs that produce the same hash value

beat with collision-resistant hashes

Downgrade Attack

when a protocol is downgraded from a higher mode or version to a low-quality mode or lower version.

commonly targets TLS

Downgrade Attack

Out-of-cycle logging: Security systems might log unusual attempts to negotiate weaker cryptographic protocols.

Published/documented: If a specific downgrade vulnerability exists, security professionals might track instances where it's being exploited.

CRYPTOGRAPHIC ATTACKS

Birthday Attack

an attempt to find collisions in hash functions.

based on a statistical phenomenon (called the ‘birthday paradox)

makes the brute forcing of one-way hashes easier

commonly targets digital signatures

Applies to hashing as it’s much harder to find something that collides with a given hash than it is to find any two inputs that hash to the same value.

Birthday Attack

Resource consumption: Large-scale birthday attacks might consume significant resources during the calculation phase. (Less likely for most systems).

Published/documented: If a specific hashing algorithm is vulnerable to birthday attacks and actively exploited, security professionals might track its use.

Additional Insights

Account lockout, concurrent session usage, blocked content, impossible travel, missing logs, and **resource inaccessibility…**

are unlikely indicators for these specific cryptographic attacks themselves in most cases.

These attacks often happen behind the scenes without directly affecting user accounts or system functionality.

And often target weaknesses in the underlying algorithms or implementations (logs may or may not help)

PASSWORD ATTACKS

a type of brute force attack

Password spraying

Attacker tries a password against many different accounts to avoid lockouts that typically come when brute forcing a single account.

Succeeds when an admin or an application sets a default password for new users.

Effective countermeasures include MFA, CAPTCHA, and forcing password change on first login.

Spraying

Account lockout: A high volume of failed login attempts from various accounts can trigger lockouts.

Resource consumption: A moderate increase in resource consumption by login processes might occur during a spraying attack.

Out-of-cycle logging: Security systems might log unusual login attempt patterns indicative of spraying.

Published/documented: If a large spraying campaign is underway, security professionals might be tracking it.

PASSWORD ATTACKS

Brute Force Attack

Attempts to randomly find the correct cryptographic key attempting all possible combinations (trial and error)

Password complexity and attacker resources will determine effectiveness of this attack.

rainbow tables and powerful compute resources make this attack more effective

Effective countermeasures include cryptographic salts, Captcha, throttling the rate of repeated logins, and IP blocklists

Brute Force

Account lockout: Repeated failed login attempts from a single account are highly likely to trigger lockouts.

Resource consumption: Brute-force attacks can consume resources as login attempts are processed.

Out-of-cycle logging: Security systems might log excessive login attempts from a single source.

Published/documented: If a large brute-force attack is underway, security professionals might be tracking it.

2.0 THREATS, VULNERABILITIES, AND MITIGATIONS

2.5 Explain the purpose of mitigation techniques used to secure the enterprise

- **Segmentation**
- **Access control**
  - Access control list (ACL)
  - Permissions
- **Application allow list**
- **Isolation**
- **Patching**
- **Encryption**
- **Monitoring**
- **Least privilege**
- **Configuration enforcement**
- **Decommissioning**
- **Hardening techniques**
  - Encryption
  - Installation of endpoint protection
  - Host-based firewall
  - Host-based intrusion prevention system (HIPS)
  - Disabling ports/protocols
  - Default password changes
  - Removal of unnecessary software

Many mitigation techniques in this list are security controls, so we'll begin with a comparison of terms

Mitigation Technique

Mitigation refers to the process of reducing the severity or seriousness of the potential consequences of a risk.

Mitigation is a form of security control but is more about managing and minimizing risks rather than eliminating them.

Security Control

Security controls are **safeguards** or **countermeasures** implemented to protect an organization's assets.

Safeguards are proactive, and countermeasures reactive.

Segmentation

Security of services that are permitted to access or be accessible from other zones involves a strict set of rules controlling this traffic.

Rules are enforced by the IP address ranges of each subnet.

Within a private subnet, segmentation can be used to achieve departmental, infrastructure, app, or data isolation.

Physical = with hardware

Logical = software/configuration

ON-PREM: Segmentation may be **physical or logical**.

IN THE CLOUD: Segmentation is usually **logical**.

SEGMENTATION

Reasons for segmentation

Boosting Performance

can improve performance through an organizational scheme in which systems that often communicate are located in the same segment

Systems that rarely or never communicate are located in separate segments.

Reducing Communication Problems

reduces congestion and contains communication problems, such as broadcast storms, to individual subsections of the network.

Providing Security

can also improve security by isolating traffic and user access to those segments where they are authorized, protecting sensitive data and resources.

Reduces the scope of a potential security breach

Micro-segmentation

Taking the concept of logical segmentation to a more granular level by further dividing apps or workloads.

The small segments or 'microsegments' contain a specific workload or functionally similar/identical nodes.

Polices and controls are then targeted to these microsegments

Further limits scope of impact, outage, or breach (lateral movement, etc.)

SEGMENTATION In the public cloud

Virtual networks, public and private subnets, segmentation, and API inspection and integration are important elements of **cloud network security**

Virtual Private Cloud (VPC)

A virtual network that consists of cloud resources, where the VMs for one company are isolated from the resources of another company.

Separate VPCs can be isolated using public and private networks or segmentation. VPCs in the cloud are typically isolated each other by default

Subnets are configured within VPCs, which can communicate by default

The concept exists in all major public clouds:

In Amazon Web Services (AWS), the term is **VPC**

In Microsoft Azure, it's called a **virtual network (VNET)**

In Google Cloud Platform (GCP), it's also a **VPC**

NETWORK SECURITY

(Network) security groups provide an additional layer of security for cloud resources

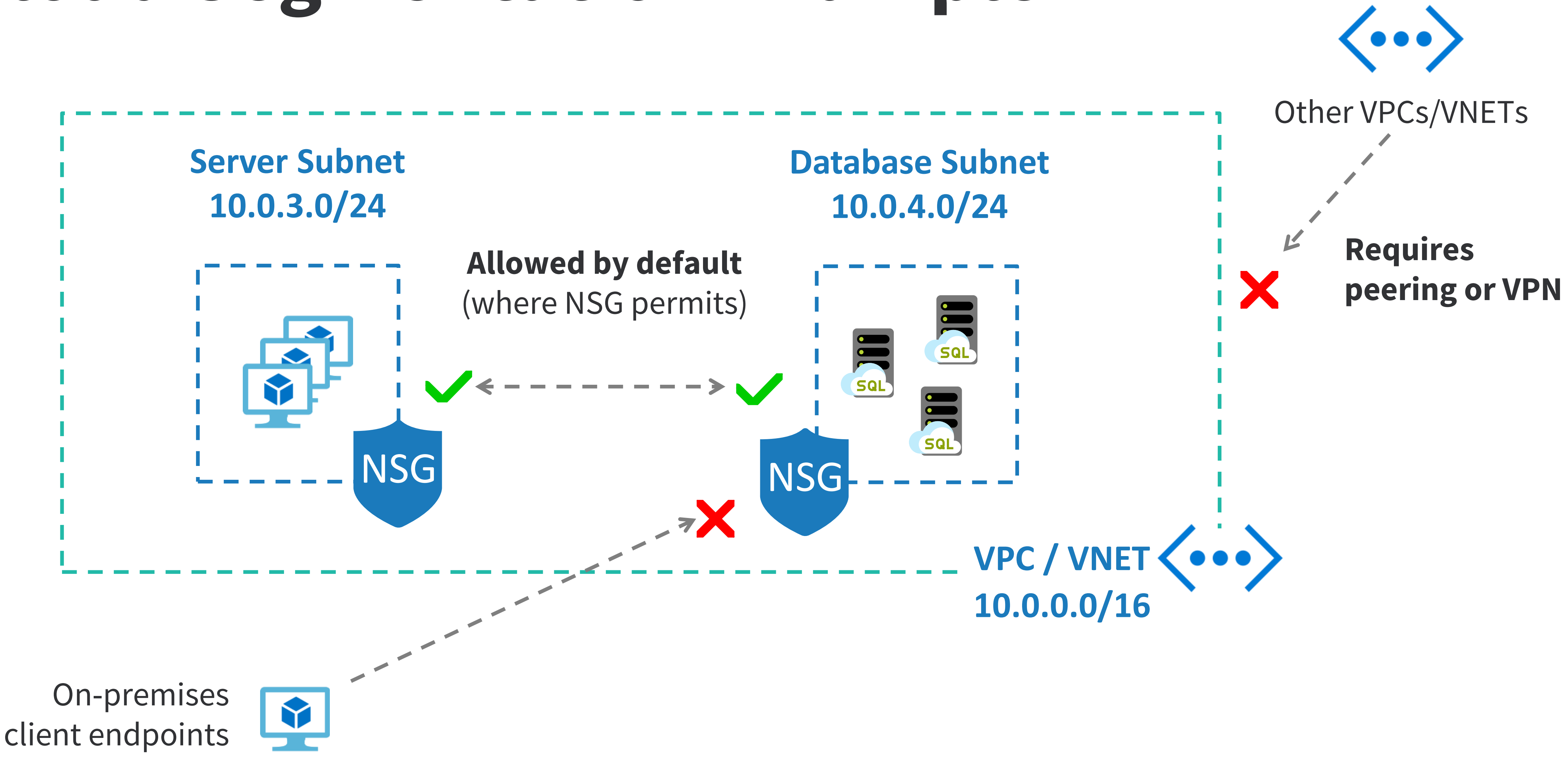
Acts as a virtual firewall for VPCs, VNETs and resource instances. (e.g. VMs, databases, subnets)

Carries a list of security rules (IP and port ranges) that allow or deny network traffic to resource instances.

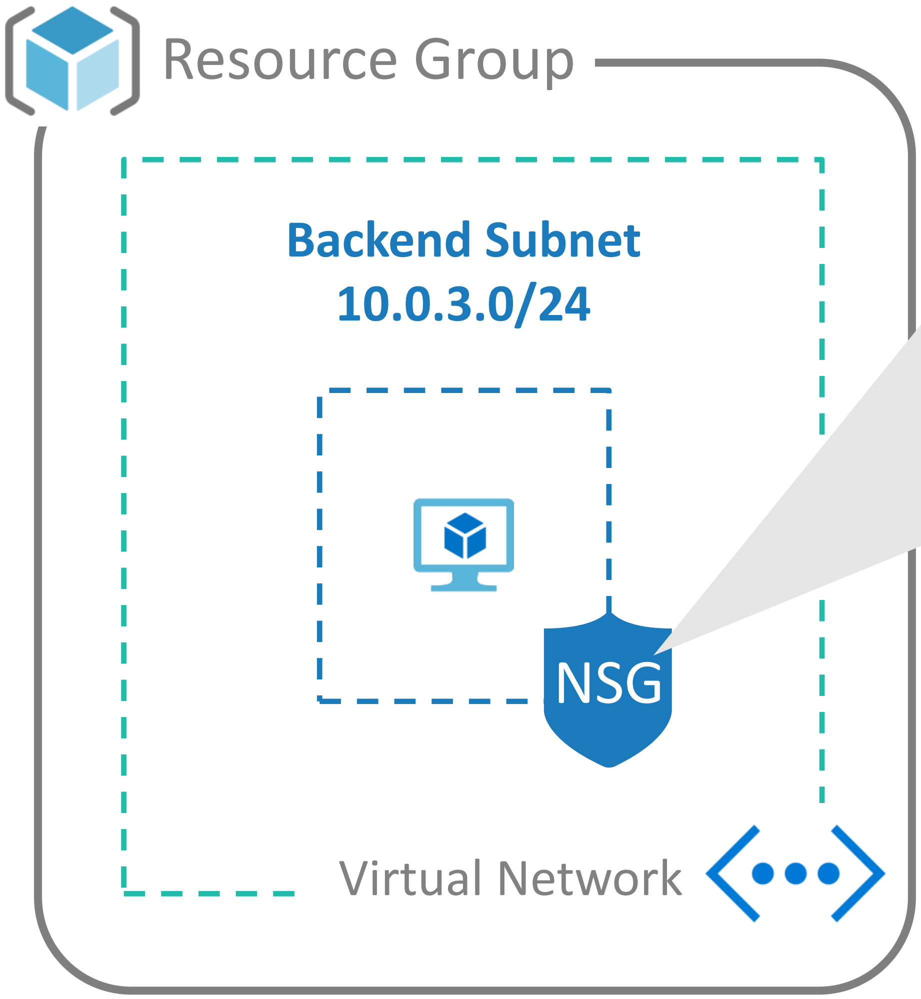
Provides a layer 4 virtual firewall for a collection of cloud resources with the same security posture.

Exists in multiple CSPs. Details may vary slightly with each.

Cloud Segmentation Example



(Network) Security Group Example



Priority	Name	Port	Protocol	Source	Dest	Action
200	SQL	1433	TCP	Any	Any	Allow
65000	AllVNetInbound	Any	Any	VNET	VNET	Allow
65500	DenyAllInbound	Any	Any	Any	Any	Deny

Action determines if the rule allows or denies traffic.

SEGMENTATION

There are several ways to look at segmentation

Mobile device management. in a BYOD mobile device scenario, mobile app management (MAM) will keep personal and business data separate.

Can prevent business data from leaking into personal apps

Endpoints. segment devices that have become vulnerable, such as an unpatched printer where there are no updates.

You could place these printers in a VLAN.

Non-compliant devices can be quarantined until remediated.

This is possible with network access control (NAC)

Applications. Within a private subnet, VLANs can be used to carry out segmentation and traffic filtering for sensitive apps and data.

These rules could be enforced with subnets and firewalls

2.5 ACCESS CONTROL

Mandatory Access Control (MAC)

Enforces an access policy that is determined by the system, not the object owner. Relies on classification labels that are representative of security domains and realms.

Discretionary Access Control (DAC) NTFS file permissions (Windows)

Permits the owner or creator of an object to control and define its accessibility, because the owner has full control by default.

Non-discretionary Access Control A form of MAC

Enables the enforcement of system-wide restrictions that override object-specific access control.

Rule-based Access Control

Defines specific functions for access to requested objects. Commonly found in firewall systems.

RULE-BASED ACCESS CONTROL

Routers and firewalls use rules within access control lists (ACLs).

These rules define the traffic the devices allow into the network

ROLE-BASED ACCESS CONTROL

Uses a well-defined collection of **named job roles** to endow each one with specific permissions

Aims to ensure that users who occupy such roles can access what they need to get their jobs done.

Used on Windows and public cloud platforms

Implementing application security controls can prevent attacks.

Application Allow List

An application allow list enables only explicitly allowed applications to run.

Firewalls, IDS/IPS, and EDR systems can have an allow list

Application Deny List

Restricts traffic in the opposite way of an allow list.

Essentially any application not explicitly denied is allowed.

Less restrictive (more permissive) than an application allow list

ISOLATION

Isolation means blocking access altogether

Air gap endpoints are used to view classified data to isolate the endpoint from the network to protect against a network-based attack.

Air gap eliminates all network connectivity (wired, wi-fi)

The only way to add or extract data from an air gapped computer is by using a removable device such as a USB drive.

Requiring users entering an area for confidential meetings or to view secret research to place their phones in a faraday cage.

It blocks electromagnetic signals from entering or exiting the cage, rendering cellular signals useless

Isolation of ICS/OT systems is common due to their critical nature

PATCHING

Patch Management

aka "update management"

ensures that systems are kept up-to-date with current patches.

will evaluate, test, approve, and deploy patches.

system audits verify the deployment of approved patches to system

Patch both native OS and 3rd party apps

Apply out-of-band updates promptly.

Orgs without patch management will experience outages from **known vulnerabilities** that could have been prevented

IMPROPER OR WEAK PATCH MANAGEMENT

Firmware

Commonly overlooked in IoT devices and other embedded systems, like VoIP phones.

Operating system (OS)

Windows has historically been (and continues to be) the biggest target, but we need to keep Mac and Linux patched also.

In the age of the smartphone, mobile systems are a common target of threat actors. Not rooted/jailbroken, min OS version, and managed

Applications

In many environments, non-Microsoft applications (commonly called third-party apps) get overlooked for patching.

Due in part because many management tools (and software vendors) do not offer the same level of automation.

Hardware Root of Trust

A line of defense against executing unauthorized firmware on a system

And when certificates are used in FDE, they use a hardware root of trust for key storage.

It verifies that the keys match before the secure boot process takes place

The **Trusted platform module (TPM)** is an implementation of a hardware root of trust.

Trusted Platform Module

A chip that resides on the motherboard of the device.

Multi-purpose, like storage and management of keys used for full disk encryption (FDE) solutions and secure boot of device operating system.

Provides the operating system with access to keys, but prevents drive removal and data access

If an encrypted drive is removed from the system, data is inaccessible since the encryption keys are in the TPM

BOOT INTEGRITY

Boot integrity ensures host is protected during the boot process, so all protections are in place when system is fully operational.

Unified Extensible Firmware Interface (UEFI)

a modern version of the Basic Input/Output System (BIOS) that is more secure and is needed for a secure boot of the OS. The older BIOS cannot provide secure boot.

Measured Boot

where all components from the firmware, applications, and software are measured and information stored in a log file

The log file is on the Trusted Platform Module (TPM) chip on the motherboard.

Trusted Secure Boot and Boot Attestation

Operating Systems such as Windows 10 can perform a secure boot at startup where the OS checks that all of the drivers have been signed.

If they have not, the boot sequence fails as the system integrity has been compromised.

This can be coupled with *attestation*, where the software integrity has been confirmed.

Bitlocker implements attestation and its keys are stored on the TPM

DRIVE ENCRYPTION

FDE

Full Disk Encryption

Full Disk Encryption is built into the Windows operating system.

Bitlocker is an implementation of FDE.

Keys are stored on the TPM

SED

Self-Encrypting Device

encryption on a SED is built into the hardware of the drive itself.

anything that's written to that drive is automatically stored in encrypted form.

A good SED should follow the Opal Storage Specification

PROTECTING DATA AT REST

Full Disk Encryption (FDE) “under the hood”

Trusted Platform Module (TPM): is on the motherboard and is used to store the encryption keys so when system boots, it can compare keys and ensure that the system has not been tampered with.

Hardware Root of Trust: When using certificates for FDE, they use a hardware root of trust that verifies that the keys match before the secure boot process takes place.

Self-Encrypting Drives (SEDs)

The OPAL storage specification is the industry standard for self-encrypting drives. This is a hardware solution, and typically outperform software-based alternatives.

They don't have the same vulnerabilities as software and therefore are more secure.

SEDs are **Solid State Drives (SSDs)** and are purchased already set to encrypt data at rest. The encryption keys are stored on the hard drive controller.

They are immune to a cold boot attack and are compatible with all operating systems

SED is effective in protecting the data on lost or stolen devices (such as a laptop). Only the **user** and **vendor** can decrypt the data.

MONITORING PRIVILEGED OPERATIONS

Privileged entities are trusted, but they can abuse their privileges.

It’s important to monitor all assignment of privileges and the use of privileged operations.

Goal

To ensure that trusted employees do not abuse the special privileges they are granted.

Monitoring these operations can also detect many attacks because attackers commonly use special privileges

MONITORING

Log Monitoring

Logs from various systems, services and devices record details of activity on systems and networks.

Takes multiple logs get the full view of a breach

By monitoring these logs, it's possible to detect security incidents.

Automated log monitoring can automatically detect and investigate potential incidents.

Centralizing log collection (for cloud and on-prem) and automating investigation is the norm in the enterprise today

SIEM AND SOAR

uses AI, ML, and threat intelligence

SIEM

Security Information Event Management

system that collects data from many other sources within the network.

provides real-time monitoring, analysis, correlation & notification of potential attacks.

SOAR

Security Orchestration Automation, & Response

centralized alert and response automation with threat-specific playbooks.

response may be fully automated or single-click.

Many providers deliver these capabilities together

SYSLOG/SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Log Collectors

SIEM has built-in log collector tooling that can collect information from both the syslog server and multiple other servers. An agent is placed on the device that can collect log information, parse and restructure data, and pass to SIEM for aggregation.

Ingestion may be with via an agent, syslog, or API

Log Aggregation

Can correlate and aggregate events so that duplicates are filtered and a better understanding network events is achieved to help identify potential attacks.

Data Inputs

The SIEM system collects a massive amount of data from various sources.

May include network devices, IDM, MDM, CASB, XDR, and more

LIMITING ACCESS & DAMAGE

Need-to-know and the **principle of least privilege** are two standard IT security principles implemented in secure networks.

They limit access to data and systems so that users and other subjects have access only to what they require.

They help prevent security incidents

They help limit the scope of incidents when they occur.

When these principles are not followed, security incidents **result in far greater damage** to an organization.

LIMITING ACCESS & DAMAGE

Separation of Duties | a basic security principle that ensures that no single person can control all the elements of a critical function or system.

Reduces likelihood of collusion amongst employees

Least Privilege | a subject should be given only those privileges necessary to complete their job-related tasks.

Can prevent or limit scope of security incidents and data theft

Need to Know | limiting access to information to only those who genuinely require it to perform their job duties.

Minimizes risk of data leak and increases accountability

Configuration & Change Management

Can prevent security related incidents and outages

Configuration Management

ensures that systems are configured similarly, configurations are known and documented.

Baselining ensures that systems are deployed with a common baseline or starting point, and imaging is a common baselining method.

Change Management

helps reduce outages or weakened security from changes.

Versioning uses a labeling or numbering system to track unauthorized changes in updated versions of software.

requires changes to be requested, approved, tested, and documented.

Configuration Management

Diagrams: detailed diagrams to show the relationship of all the interconnected devices ensuring security team have visibility of the security in place.

Standard Naming Conventions: standard naming convention make identifying device type (router, server, printer) easier.

Naming prefixes (e.g. rtr, svr, prt) can help

Asset Management: Maintain an up-to-date asset register to ease the process of tracking and maintaining assets.

Scan for unknown devices, ensure devices are patched

Baseline Configurations: It is vital that each type of device being placed on the network has a secure baseline configuration.

Image-based deployment, infrastructure-as-code (IaC)

Firewall Rules: Firewalls can be used to block traffic and we can use either an MDM solution or group policy to change the configuration on endpoint devices.

Standardize and automate configuration, IaC and CI/CD

2.5 CONFIGURATION ENFORCEMENT

Configuration Management

Mobile Device Management (MDM): An MDM solution can be used to push configuration changes to mobile devices.

Min iOS/Android version, 6-digit pin, no rooted devices, app management

Content Filter/URL Filter: Blocking harmful content with filtering appliances like Unified Threat Management (UTM) or Next Generation (NG) firewalls.

UTM bundles features (URL, email, AV, IPS), NG use threat intel feeds

Update or Revoke Certificates: Certificates facilitate authentication and secure connectivity (TLS/HTTPS web, IPSec VPN connectivity).

Track certificate expiration and ensure minimum TLS version support.

Decommissioning

Hardware being retired must be disposed of securely, so data it hosts is not recoverable through forensic means.

Crypto-shredding is a data deletion method that involves discarding the encryption keys of encrypted data.

If data is recoverable through forensic tools and techniques the system has not been properly decommissioned or recycled

EOL hardware is often recycled for reuse. Secure data deletion is critical.

2.5 HARDENING TECHNIQUES

Know these **4 types of endpoint protection** for the exam

Antivirus software

Scans endpoints for the presence of malware like viruses, worms, trojans, and other malicious code.

When an infection is detected, it can generally remediate automatically through quarantine or removal of detected malware.

Originally relied in AV signatures (of known threats), but today relies on AI and threat intelligence to detect malicious behaviors.

Endpoint detection and response (EDR)

a security technology that focuses on detecting and responding to threats at the endpoint level.

often uses behavioral analysis techniques to identify suspicious activity and contain threats before they can cause damage.

prevents unauthorized access, tampering, or other types of attacks.

2.5 HARDENING TECHNIQUES

Know these **4 types of endpoint protection** for the exam

Extended detection and response (XDR)

a next generation security technology that goes beyond the endpoint to include other types of devices and systems…

such as network devices, cloud infrastructure, and IoT devices,

provides a broader view of the entire IT environment and enabling faster, more accurate threat detection and response.

Host intrusion prevention systems (HIPS)

intrusion prevention local to a single host or endpoint

uses techniques such as behavior analysis, file integrity monitoring, and application control to detect threats

and when possible, will take action to stop identified threats

Software-based, so may be easier for attacker to disable

HOST-BASED IDS AND IPS

IDS/IPS in software form, installed on a host (often a server)

HIDS

Host-based Intrusion Detection System

Analyzes whole packets, both header and payload, looking for known events.

When a known event is detected, a **log message is generated.**

HIPS

Host-based Intrusion Prevention System

Analyzes whole packets, both header and payload, looking for known events.

When a known event is detected, **packet is rejected**.

HARDENING TECHNIQUES

Host-based Firewall

an application firewall that is built into desktop operating systems, like Windows or Linux.

because it is an application, it is more vulnerable to attack in some respects (versus hardware FW).

restricting service/process access to ensure malicious parties cannot stop/kill is important.

Host-based and network-based firewalls are often used together in a layered defense

2.5 HARDENING TECHNIQUES

Close open ports and disable services

listening ports should be restricted to those necessary, filtered to restrict traffic, and disabled entirely if unneeded

unused services should be disabled

Block through firewalls or disabling underlying service.

Registry

access should be restricted, and updates controlled through policy where possible

always take a backup of the registry before you start making changes.

OS (Operating System)

OS hardening can often be implemented through security baselines

Can be applied through group policies or management tools (like MDM)

Baselines can implement all the above

2.5 HARDENING TECHNIQUES

Default password changes

any services, apps, or OS with pre-created users with a default password should be change before deployment

Removal of unnecessary software

Any software that is definitely unneeded should be removed to reduce the attack surface and patching burden

Use OS imaging over third party uninstallers when dealing with bloatware or other PUA

INSIDE CLOUD
AND SECURITY

THANKS

FOR WATCHING!