DOMAIN 1

SECURITY+ EXAM CRAM

PROVEN FAST, EFFECTIVE & AFFORDABLE EXAM PREP

CompTIA Security+

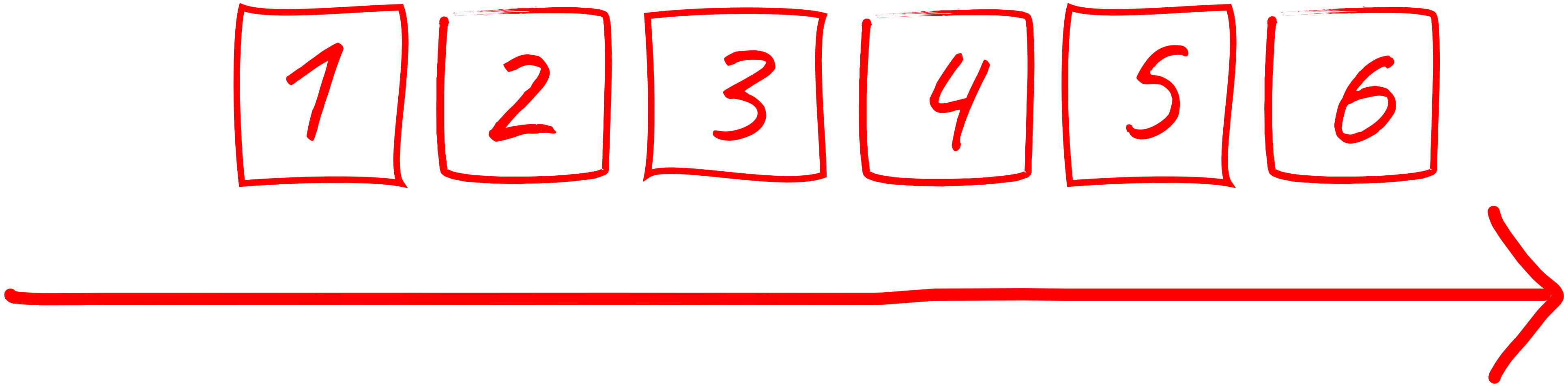
with Pete Zerger CISSP, vCISO, MVP

EXAM OBJECTIVES (DOMAINS)

DOMAIN	WEIGHT
1.0 Attacks, Threats, and Vulnerabilities	**24%**
2.0 Architecture and Design	21%
3.0 Implementation	25%
4.0 Operations and Incident Response	16%
5.0 Governance, Risk, and Compliance	14%

INTRODUCTION: SERIES OVERVIEW

LESSONS IN THIS SERIES



Intro + one lesson for each exam domain

+ 5-10 shorter supplemental lessons

ULTIMATE STRATEGY GUIDE

PROVEN *FAST, EFFECTIVE & AFFORDABLE EXAM PREP*

SECURITY+ EXAM CRAM

CompTIA Security+

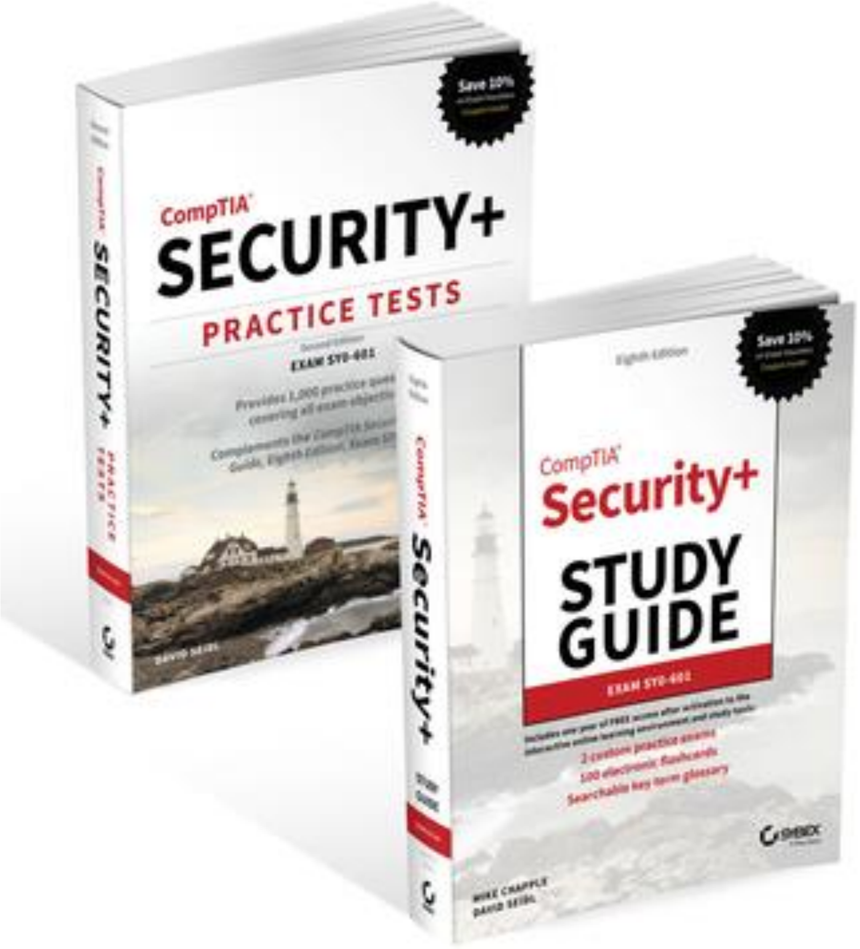
with Pete Zerger CISSP, vCISO, MVP

CompTIA Security+ Exam Cram

EXAM NUMBER: SY0-601

1.0 Threats, Attacks and Vulnerabilities

Covering all topics in the official Security+ exam objectives

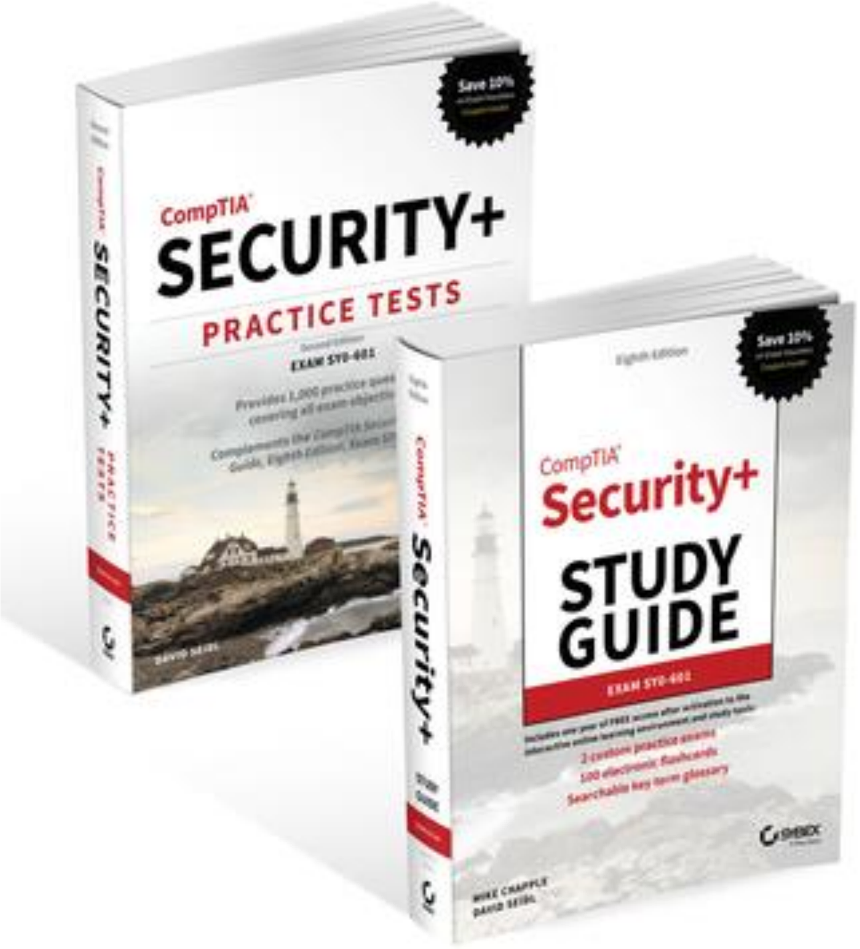


SECURITY+
EXAM STUDY GUIDE
& PRACTICE TESTS BUNDLE

1,000 flashcards

1,000 practice questions

2 practice exams



SECURITY+

EXAM STUDY GUIDE

& PRACTICE TESTS BUNDLE

1,000 flashcards

1,000 practice questions

2 practice exams

Save 10%
CompTIA
SECURITY+
PRACTICE TESTS
EXAM SY0-601
Save 10%
Eighth Edition
CompTIA
Security+
STUDY GUIDE
EXAM SY0-601
SYBEX
MIKE CHAPPLE
DAVID SEIDL

A pdf copy of the presentation is available in the video description!

SUBSCRIBE

1.0 THREATS, ATTACKS AND VULNERABILITIES

1.1 Compare and contrast different types of social engineering techniques

- **Phishing**
- **Smishing**
- **Vishing**
- **Spam**
- **Spam over instant messaging (SPIM)**
- **Spear phishing**
- **Dumpster diving**
- **Shoulder surfing**
- **Pharming**
- **Tailgating**
- **Eliciting information**
- **Whaling**
- **Prepending**
- **Identity fraud**
- **Invoice scams**
- **Credential harvesting**
- **Reconnaissance**
- **Hoax**
- **Impersonation**
- **Watering hole attack**
- **Typosquatting**
- **Pretexting**
- **Influence campaigns**
  - Hybrid warfare
  - Social media
- **Principles (reasons for effectiveness)**
  - Authority
  - Intimidation
  - Consensus
  - Scarcity
  - Familiarity
  - Trust
  - Urgency

CLASSIFYING SOCIAL ENGINEERING ATTACKS

At a high level, two categories of social engineering attacks:

Physical Attacks

- ✓ Tailgating
- ✓ Shoulder surfing
- ✓ Dumpster diving

Virtual Attacks

- ✓ Phishing
- ✓ Spear Phishing
- ✓ Whaling
- ✓ Vishing
- ✓ Hoax
- ✓ Watering hole attack

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 often 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!

SPAM AND SPIM

SPAM

Unsolicited email, generally considered an irritant

defeat with strong spam filtering

SPIM

SPAM over instant messaging, also generally considered an irritant

IM and mobile providers providing some protection here

Create cryptic usernames and do not list your ID in the IM service public directory

Not always just an irritant! Both are delivery channels for ransomware!

WHAT IS DUMPSTER DIVING

Gathering important details (intelligence) from things that people have thrown out in their trash.

Often legal, and may target individuals or organizations

SOCIAL ENGINEERING TECHNIQUES

Tailgating

when an unauthorized individual might follow you in through that open door without badging in themselves.

Usually not an accident!

Eliciting Information

aka 'elicitation'

strategic use of casual conversation to extract information without the arousing suspicion of the target

Can involve complex cover stories and co-conspirators!

SOCIAL ENGINEERING TECHNIQUES

Tailgating

when an unauthorized individual might follow you in through that open door without badging in themselves.

Usually not an accident!

Eliciting Information

aka 'elicitation'

strategic use of casual conversation to extract information without the arousing suspicion of the target

Techniques include flattery, false statements, artificial ignorance, bracketing

SOCIAL ENGINEERING TECHNIQUES

Shoulder Surfing

a criminal practice where thieves steal your personal data by spying over your shoulder

Can happen anywhere with any device

Pharming

an online scam similar to phishing, where a website's traffic is manipulated, and confidential information is stolen.

a portmanteau of the words "phishing" and "farming",

SOCIAL ENGINEERING TECHNIQUES

IDENTITY FRAUD

aka "identity theft"

use of another person's personal information, without authorization, to commit a crime or to deceive or defraud that person or other 3rd party

PREPENDING

Prepending is adding words or phrases like "SAFE" to a malicious file or suggesting topics via social engineering to uncover information of interest.

INVOICE SCAMS

fake invoices with a goal of receiving money or by prompting a victim to put their credentials into a fake login screen.

SOCIAL ENGINEERING TECHNQUES

Credential Harvesting

attackers trying to gain access to your usernames and passwords that might be stored on your local computer

This is a frequent goal of phishing attempts

Credential Harvesting

attackers trying to gain access to your usernames and passwords that might be stored on your local computer

COUNTERMEASURES: email defense, anti-malware, EDR/XDR solutions that will check URLs and block the scripts often used to execute the attack

RECONNAISSANCE

A common technique that comes in multiple forms

Passive discovery

Techniques that do not send packets to the target; like Google hacking, phone calls, DNS and WHOIS lookups

Semi-passive discovery

Touches the target with packets in a non-aggressive fashion to avoid raising alarms of the target

Active discovery

More aggressive techniques likely to be noticed by the target, including port scanning, and tools like **nmap** and **Metaspoit**

SOCIAL ENGINEERING TECHNIQUES

Hoaxes

Intentional falsehoods coming in a variety of forms ranging from virus hoaxes to fake news. Social media plays a prominent role in hoaxes today

Impersonation

A form of fraud in which attackers pose as a known or trusted person to dupe the user into sharing sensitive info, transferring money, etc.

Watering hole attack

Attack strategy in which an attacker guesses or observes which websites an organization often uses and infects one or more of them with malware

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

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.

INFLUENCE CAMPAIGNS

A social engineering attack intended to manipulate the thoughts and minds of large groups of people

Hybrid Warfare

Attack using a mixture of conventional and unconventional methods and resources to carry out the campaign

Social media

May use multiple social platforms leveraging multiple/many individuals to amplify the message, influencing credibility.

May involve creating multiple fake accounts to post content and seed the spread.

and may even include paid advertising.

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 to target with a issue, to establish a relationship.

Urgency

Time sensitivity that demands immediate action, similar to scarcity

1.0 THREATS, ATTACKS AND VULNERABILITIES

1.2 Given a scenario, analyze potential indicators to determine the type of attack

- **Malware**
  - Ransomware
  - Trojans
  - Worms
  - Potentially unwanted programs (PUPs)
  - Fileless virus
  - Command and control
  - Bots
  - Crypto-malware
  - Logic bombs
  - Spyware
  - Keyloggers
  - Remote access Trojan (RAT)
  - Rootkit
  - Backdoor
- **Password attacks**
  - Spraying
  - Dictionary
  - Brute force
  - Offline
  - Online
  - Rainbow table
  - Plaintext/unencrypted
- **Physical attacks**
  - Malicious Universal Serial Bus (USB) cable
  - Malicious flash drive
  - Card cloning
  - Skimming
- **Adversarial artificial intelligence (AI)**
  - Tainted training data for machine learning (ML)
  - Security of machine learning algorithms
- **Supply-chain attacks**
- **Cloud-based vs. on-premises attacks**
- **Cryptographic attacks**
  - Birthday
  - Collision
  - Downgrade

APPLICATION ATTACKS

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

Rootkit (escalation of privilege)

freely available on the internet and exploit known vulnerabilities in various operating systems enabling attackers to elevate privilege.

keep security patches up-to-date
anti-malware software, EDR/XDR

Back Door

undocumented command sequences that allow individuals with knowledge of the back door to bypass normal access restrictions.
often used in development and debugging.

countermeasures:
firewalls, anti-malware, network monitoring, code review

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

You should know key characteristic(s) of each for the exam!

Crypto-malware

Ransomware that encrypts files stored on a computer or mobile device in order to extort money.

Hoaxes

Virus hoaxes are a nuisance that result in wasted resources. Used to spread through "email from a friend" but have changed with social media.

Logic Bombs

Logic bombs are malicious code objects that infect a system and lie dormant until they are triggered by the occurrence of one or more conditions, such as time, program launch, website logon, etc.

WHAT IS A TROJAN HORSE

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

MALWARE

Worm

a type of malware that spreads copies of itself from computer to computer, replicating itself without human interaction.

Potentially unwanted programs (PUPs)

a program that may be an unwanted app, often delivered alongside a program the user wants. PUPs include spyware, adware, and dialers.

Keylogger

Designed to log keystrokes, creating records of everything you type on a computer or mobile keyboard.

Spyware

Malware designed to obtain information about an individual, system, or organization.

MALWARE

Fileless virus

a type of malicious software that does not rely on virus-laden files to infect a host. Instead, it exploits applications that are commonly used for legitimate and justified activity to execute malicious code in resident memory.

Command and control

a computer controlled by an attacker or cybercriminal which is used to send commands to systems compromised by malware and receive stolen data from a target network.

Remote access trojan (RAT)

a malware program that gives an intruder administrative control over a target computer.

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
- File auto-versioning

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
- User awareness training ← Most important defense!

AI-driven cloud services offer help with these

PASSWORD ATTACKS

Dictionary attacks

Use programs with built in dictionaries.

They attempt all dictionary words to try and find the correct password, in the hope that a user would have used a standard dictionary word.

Effective countermeasures include MFA, biometric authentication, limit number of attempts, force resets after certain number of failed attempts.

PASSWORD ATTACKS

Password spraying

a type of brute force attack

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

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

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

PASSWORD ATTACKS

Offline

Attempt to discover passwords from a captured database or captured packet scan.

Online

Attempts to discover a password from an online system. For example, an attacker trying to log on to an account by trying to guess a user’s password.

most web and wi-fi attacks are online attacks

Plaintext/unencrypted

Protocols and authentication methods that leave credentials unencrypted, like basic authentication and telnet.

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

PASSWORD ATTACKS

SALTS

Cryptographic

Attackers may use **rainbow tables**, which contain precomputed values of cryptographic hash functions to identify commonly used passwords

A **salt** is random data that is used as an additional input to a one-way function that hashes data, a password or passphrase.

Adding salts to the passwords before hashing them reduces the effectiveness of rainbow table attacks.

MULTI-ATTACK PREVENTION

Multi-factor Authentication

Something you **know** (pin or password)

Something you **have** (trusted device)

Something you **are** (biometric)

PREVENTS:

- Phishing
- Spear phishing
- Keyloggers
- Credential stuffing
- Brute force and reverse brute force attacks
- Man-in-the-middle (MITM) attacks

BOTS, BOTNETS, AND BOT HERDERS

represent significant threats due to the massive number of computers that can launch attacks

Botnet

a collection of compromised computing devices (often called bots or zombies).

Bot Herder

criminal who uses a command-and-control server to remotely control the zombies

often use the botnet to launch attacks on other systems, or to send spam or phishing emails

PHYSICAL ATTACKS

Malicious flash drive

Attack comes in two common forms:

Drives dropped where they are likely to be picked up.

Sometime effectively a trojan, shipped with malware installed after leaving the factory.

Malicious USB cable

Less likely to be noticed than a flash drive. May be configured to show up as a human interface device (e.g. keyboard)

Less common because it requires dedicated engineering

PHYSICAL ATTACKS

Card cloning

Focuses on capturing info from cards used for access, like RFID and magnetic stripe cards.

Skimming

Involve fake card readers or social engineering and handheld readers to capture (skim) cards, then clone so attacker may use for their own purposes

Device (skimmer) often installed at POS devices like ATM and gas pumps

ADVERSARIAL ARTIFICIAL INTELLIGENCE

A rapidly developing field targeting AI and ML

Tainted training data for machine learning (ML)

Data poisoning that supplies AI and ML algorithms with adversarial data that serves the attackers purposes, or attacks against privacy.

Security of machine learning algorithms

Validate quality and security of the data sources.

Secure infrastructure and environment where AI and ML is hosted.

Review, test, and document changes to AI and ML algorithms.

Know the difference between AI & ML for the exam

ARTIFICIAL INTELLIGENCE vs MACHINE LEARNING

Knowing the difference will help on the exam!

Artificial Intelligence | Focuses on accomplishing "smart" tasks combining machine learning and deep learning to emulate human intelligence

Machine Learning | A subset of AI, computer algorithms that improve automatically through experience and the use of data.

Deep Learning | a subfield of machine learning concerned with algorithms inspired by the structure and function of the brain called **artificial neural networks**.

SUPPLY CHAIN ATTACKS

a cyber-attack that seeks to damage an organization by targeting less-secure elements in the supply chain.

Often attempt to compromise devices, systems, or software before it reaches an organization.

Sometimes focus on compromising a vulnerable vendors in the organization's supply chain, and then attempting to breach the target organization.

Known as an "island hopping" attack

Supply chain attacks can have massive consequences for organizations upstream and downstream in the supply chain

CLOUD-BASED VS ON-PREMISES ATTACKS

Cloud-based attacks

Data center is often more secure and less vulnerable to disruptive attacks (like DDoS)

On the downside, you will not have facility-level or physical system-level audit access.

Changes (and limits) the attacks you will worry about

On-premises attacks

You do not benefit from the cloud's shared responsibility model.

You have more control but are responsible for security of the full stack.

Org has to defend a wider range of attacks and greater expense and effort to defend against them.

COMMON 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

COMMON CRYPTOGRAPHIC ATTACKS

Birthday Attack

an attempt to find collisions in hash functions.

commonly targets digital signatures

Replay Attack

an attempt to reuse authentication requests.

targets authentication (often Kerberos)

COMMON CRYPTOGRAPHIC ATTACKS

Birthday Attack

an attempt to find collisions in hash functions.

defeat with long hash output (to make it computationally infeasible)

Replay Attack

an attempt to reuse authentication requests.

defeat with date/time stamps

1.0 THREATS, ATTACKS AND VULNERABILITIES

1.3 Given a scenario, analyze potential indicators associated with application attacks

- **Privilege escalation**
- **Cross-site scripting**
- **Injections**
  - Structured query language (SQL)
  - Dynamic-link library (DLL)
  - Lightweight Directory Access Protocol (LDAP)
  - Extensible Markup Language (XML)
- **Pointer/object dereference**
- **Directory traversal**
- **Buffer overflows**
- **Race conditions**
  - Time of check/time of use
- **Error handling**
- **Improper input handling**
- **Replay attack**
  - Session replays
- **Integer overflow**
- **Request forgeries**
  - Server-side
  - Cross-site
- **Application programming interface (API) attacks**
- **Resource exhaustion**
- **Memory leak**
- **Secure Sockets Layer (SSL) stripping**
- **Driver manipulation**
  - Shimming
  - Refactoring
- **Pass the hash**

A security hole created when code is executed with higher privileges than those of the user running it.

PRIVILEGE ESCALATION

REQUEST FORGERIES

a type of injection using **malicious scripts**

Cross-site scripting (XSS)

a client-side vulnerability

A type of injection, in which malicious scripts are injected into otherwise benign and trusted websites.

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

occur when web apps contain 'reflected input'

Input validation and filtering. Validate **data length** AND **data type**. This filters out malicious input (like a <SCRIPT> tag)

REQUEST FORGERIES

exploits **user trust** to execute code

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

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

exploits trust that a user has in a website 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!

INJECTIONS (INJECTION ATTACKS)

Dynamic-link library (DLL)

Is a situation in which the malware tries to inject code into the memory process space of a library using a vulnerable/compromised DLL.

Lightweight Directory Access Protocol (LDAP)

exploits weaknesses in LDAP implementations.

This can occur when the user's input is not properly filtered, and the result can be executed commands, modified content, or results returned to unauthorized queries.

Extensible Markup Language (XML)

when users enter values that query XML (known as XPath) with values that take advantage of exploits, it is known as an **XML injection attack**.

XPath works in a similar manner to SQL, except that it does not have the same levels of access control, so exploits can return entire documents.

The best defense is to filter the user's input and sanitize it to make certain that it does not cause XPath to return more data than it should.

INJECTIONS (INJECTION ATTACKS)

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 prepared statements, and limit account privileges.

POINTER/OBJECT DEREFERENCE

An attack that consists of finding null references in a target program and **dereferencing** them, causing an exception to be generated.

Dereferencing means **taking away the reference** and giving you what it was actually referring to.

The vulnerability in memory that usually causes the applications to crash or a denial of service is a **NULL Pointer dereference**.

In this case, there is nothing at that memory address to dereference (it is empty, or NULL) and the application crashes.

Good coding is the best protection. Code should check to make sure it is not NULL **BEFORE** dereferencing it.

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.

BUFFER OVERFLOWS

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

Buffer Overflow

exist when a developer does not validate user input to ensure that it is of an appropriate size (allows Input that is too large can "overflow" memory buffer).

prevent with INPUT VALIDATION !

RACE CONDITIONS

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

Time-of-Check-to-Time-of-Use (TICTOU)

a timing vulnerability that occurs when a program checks access permissions too far in advance of a resource request.

file locking, transactions in file system or OS kernel

It becomes a bug when one or more of the possible behaviors is undesirable.

Error handling

Related to input validation is error handling

Every function that has any meaningful functionality should have appropriate error handling.

Properly done, the user will simply see an error message box

If a program crashes, it is a sign of poor error handling!

Error handling is an element of **good coding practices**

COMMON CRYPTOGRAPHIC ATTACKS

Replay Attack

an attempt to reuse authentication requests.

targets authentication (Kerberos a frequent target)

Session Replay

an attacker steals a valid session ID of a user and reuses it to impersonate an authorized user and perform fraudulent transactions or activities.

Disallow session ID reuse in web apps

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

API Attacks

Attempts to manipulate the application programming interface (API)

Include DDoS, Man in the Middle, and injection attacks focused on an API

Goals are to gain additional resource or data access, or interrupt service

Countermeasures: Transport Layer Security (TLS), OAuth, request timestamps, key/password hash

RESOURCE EXHAUSTION a form of DoS attack (when intentional)

When an application continuously allocates additional resources, exhausting machine resources, leading the system to hang or crash.

When exploited, resource exhaustion vulnerabilities in apps, software, or system security that hang, crash, or interfere with external programs perform designated tasks properly.

Memory leaks can lead to resource exhaustion (see "memory leaks" in this session).

However, these attacks can be executed by exhausting other resource subsystems, such as CPU, disk, or network.

Countermeasures: Good software development practices (e.g. preventing memory leaks), limiting what files and apps can be executed on endpoints.

MEMORY LEAK

The most common issue in memory management

Which languages are susceptible?

Many modern programming languages (such as C# and Java) don’t allow the programmer to directly allocate or deallocate memory.

Therefore, those programming languages are not prone to memory leaks.

However, certain older languages, most notably C and C++, give the programmer a great deal of control over memory management.

Cause

Memory leaks are usually caused by failure to deallocate memory that has been allocated.

A **static code analyzer** can check to see if all memory **allocation** commands (malloc, alloc, and others) have a matching **deallocation** command.

SECURE SOCKETS LAYER (SSL) STRIPPING

aka 'SSL downgrading'.

A technique by which a website is **downgraded from https to http**

This attack downgrades your connection from HTTPS to HTTP and exposes you to eavesdropping and data manipulation.

How it works

To execute an SSL strip attack, there must be three entities – victim's system, secure web server, and attacker's system.

In order to "strip" the TLS/SSL, an attacker intervenes in the redirection from HTTP to HTTPS and intercepts a request from the user to the server.

TLS has replaced SSL, so this attack affects TLS as well

Countermeasures: Enable HTTPS on ALL pages of your website. Implement a HTTP Strict Transport Security (HSTS) policy, so the browser requires HTTPS.

DRIVER MANIPULATION

Shimming

A **shim** is a small library that is created to intercept API calls transparently and do one of three things:

1) handle the operation itself, **2)** change the arguments passed, or
3) redirect the request elsewhere.

Involves creating a library (or modifying an existing) to bypass a driver and perform a function other than the one for which the API was created.

Refactoring

The name given to a set of techniques used to identify the flow and then modify the internal structure of code without changing the code's visible behavior.

In legitimate scenarios, this is done in order to improve the design, to remove unnecessary steps, and to create better code.

In malware, this is often done to look for opportunities to take advantage of weak code and look for holes that can be exploited.

PASS THE HASH

typically targets NTLM

a technique whereby an attacker captures a password hash (as opposed to the password characters) and then passes it through for **authentication and lateral access**.

Pass-the-Hash vs Pass-the-Ticket

Pass-the-ticket targets Kerberos

One primary difference between pass-the-hash and pass-the-ticket, is ticket expiration

Kerberos TGT tickets expire (10 hours by default) whereas NTLM hashes only change when the user changes their password.

A TGT ticket must be used within its lifetime, or it can be renewed for a longer period (7 days).

How to prevent the pass the hash attacks?

Enforce least privilege access, analyze applications to determine which require admin privileges, use flexible policies that allow only trusted applications to run and in specific context.

"Credential Guard" in Windows 10 encrypts hash in memory, stopping this attack

1.0 THREATS, ATTACKS AND VULNERABILITIES

1.4 Given a scenario, analyze potential indicators associated with network attacks

- **Wireless**
  - Evil twin
  - Rogue access point
  - Bluesnarfing
  - Bluejacking
  - Disassociation
  - Jamming
  - Radio frequency identification (RFID)
  - Near-field communication (NFC)
  - Initialization vector (IV)
- **On-path attack (previously known as man-in-the-middle attack/ man-in-the-browser attack)**
- **Layer 2 attacks**
  - Address Resolution Protocol (ARP) poisoning
  - Media access control (MAC) flooding
  - MAC cloning
- **Domain name system (DNS)**
  - Domain hijacking
  - DNS poisoning
  - Uniform Resource Locator (URL) redirection
  - Domain reputation
- **Distributed denial-of-service (DDoS)**
  - Network
  - Application
  - Operational technology (OT)
- **Malicious code or script execution**
  - PowerShell
  - Python
  - Bash
  - Macros
  - Visual Basic for Applications (VBA)

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.

MOBILE AND 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.

MOBILE AND WIRELESS ATTACKS

Evil Twin

A malicious fake wireless access point set up to appear as a legitimate, trusted network.

Common in airports and coffee shops

Disassociation

A type of DoS attack in which the attacker breaks the wireless connection between the victim device and the access point.

Gives attacker a window to inject an evil twin

Jamming

A DoS attack that prevents other nodes from using the channel to communicate by occupying the channel that they are communicating on.

Can be difficult to detect & often unintentional

MOBILE AND WIRELESS ATTACKS

RFID

RADIO FREQUENCY IDENTIFICATION

Vulnerable to several classes of attack, like sniffing (or eavesdropping), spoofing, cloning, replay, relay, and DoS attacks

RFID commonly used in access badge systems

NFC

NEAR FIELD COMMUNICATION

Built on RFID, often used with payment systems. Subject to many of the same vulnerabilities as RFID

The touch pay system at the grocery

Initialization Vector (IV)

modifies the initialization vector of an encrypted wireless packet during transmission. Enables attacker to compute the RC4 key stream generated by IV used and decrypt all other packets.

Fairly uncommon today (legacy)

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.

NETWORK ATTACKS

Hyperlink Spoofing

Similar to DNS spoofing

Can take the form of DNS spoofing or can simply be an alteration of the hyperlink URLs

is usually successful because people just click links!

Use same precautions used against DNS spoofing, and services that mask and test links in detonation chamber.

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

TYPES OF DDoS ATTACKS

Cloud service providers (MSFT, AWS) have DDoS protection built-in

Network

volume-based attacks targeting flaws in network protocols, often using botnets, using techniques such as UDP, ICMP flooding, or SYN flooding (TCP-based).

Application

exploit weaknesses in the application layer (Layer 7) by opening connections and initiating process and transaction requests that consume finite resources like disk space and available memory.

Operational Technology (OT)

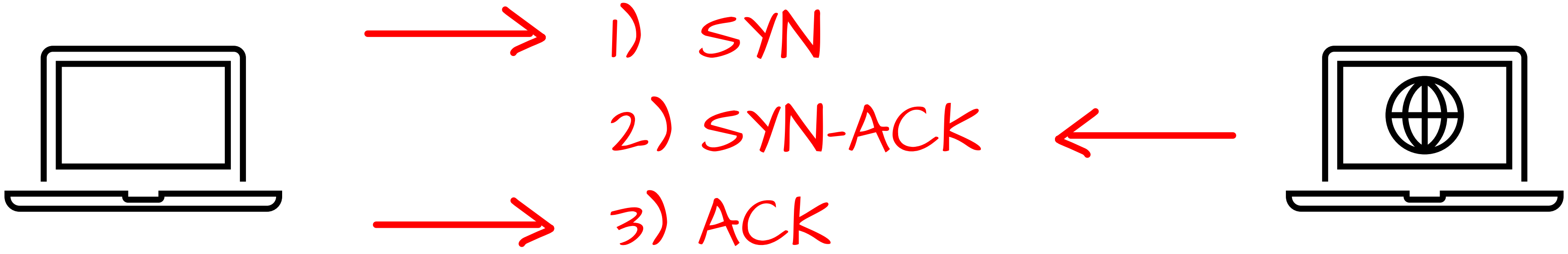
Targets the weaknesses of software and hardware devices that control systems in factories, power plants, and other industries, such as IoT devices.

Often target weaknesses using the network and application techniques described above.

COUNTERMEASURES: IDS, IPS, rate-limiting, firewall ingress/egress filters

KNOW THE ORDER OF THE 3-WAY HANDSHAKE

It comes up commonly in discussions of TCP/IP-based network attacks!



NETWORK ATTACKS

URL Redirection

a vulnerability which allows an attacker to force users of your application to an untrusted external site.

Comes in multiple forms - parameter-based, session restoration, domain-based

Domain Reputation

services and tools provide info as to whether a domain is a trusted email sender or is a source of spam email.

SPF and DMARC are all commonly used to ensure email comes from approved senders

Domain Hijacking

involves an individual changing the domain registration information for a site without the original registrant's permission.

COUNTERMEASURES: domain registration auto-renewal, privacy protection (blocking your name from WHOIS), a trusted domain provider

NETWORK ATTACKS

Layer 2 attacks (OSI model)

MAC Flooding

forcing legitimate MAC table contents out of the switch and forcing a unicast flooding behavior.

potentially sends sensitive info to areas of the network where it is not normally intended to go.

ARP Poisoning

Aka "ARP spoofing"

sending ARP packets across the LAN that contain the attacker's MAC address and the target's IP address.

NETWORK ATTACKS

Layer 2 attacks (OSI model)

MAC Cloning

Duplicates the MAC address (hardware address) of a device, allowing attacker to appear as a trusted device.

Can be difficult to detect without additional info about the device

Countermeasures: network access control (NAC) to provide a validation gate to network access.

APPLICATION ATTACKS

Malicious code or script execution

Malicious code or scripts that are not malware

Commonly PowerShell, Python, Bash, macros, and VBA

Comprehensive endpoint security (like XDR), spam/phishing defense, and user education are good countermeasures

Microsoft Defender Application Control and **Attack Surface Reduction** features are effective on Windows endpoints

1.0 THREATS, ATTACKS AND VULNERABILITIES

1.5 Explain different threat actors, vectors, and intelligence sources

- **Actors and threats**
  - Advanced persistent threat (APT)
  - Insider threats
  - State actors
  - Hacktivists
  - Script kiddies
  - Criminal syndicates
  - Hackers
    - Authorized
    - Unauthorized
    - Semi-authorized
  - Shadow IT
  - Competitors

- **Attributes of actors**
  - Internal/external
  - Level of sophistication / capability
  - Resources/funding
  - Intent/motivation
- **Vectors**
  - Direct access
  - Wireless
  - Email
  - Supply chain
  - Social media
  - Removable media
  - Cloud

1.0 THREATS, ATTACKS AND VULNERABILITIES

1.5 Explain different threat actors, vectors, and intelligence sources

- **Threat intelligence sources**
  - Open-source intelligence (OSINT)
  - Closed/proprietary
  - Vulnerability databases
  - Public/private information sharing centers
  - Dark web
  - Indicators of compromise
  - Automated Indicator Sharing (AIS)
  - Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Intelligence Information (TAXII)
  - Predictive analysis
  - Threat maps
  - File/code repositories
- **Research sources**
  - Vendor websites
  - Vulnerability feeds
  - Conferences
  - Academic journals
  - Request for comments (RFC)
  - Local industry groups
  - Social media
  - Threat feeds
  - Adversary tactics, techniques, and procedures (TTP)

ACTORS AND THREATS

Threat Actor	Skill	Description
Advanced Persistent Threat (APT)	High	Conduct sophisticated series of related attacks taking place over an extended period of time. Typically well-organized, well-funded and highly skilled.
Insider threats	Varies	people inside the targeted organization and are either responsible for the attack or are colluding with outsiders (who are responsible).
State actors	High	Well-funded, often driving warfare conducted against information processing equipment and municipal services (water, power, etc.)
Hacktivists	Varies, but often Medium-High	a group of hackers working together for a collectivist effort, usually on the behalf of some cause.
Script kiddies	Low	Individuals who use hacking techniques but have limited skills. Often rely almost entirely on automated tools they download from the Internet.

ACTORS, THREATS, SKILL, FUNDING, AND MOTIVATION

Threat Actor	Skill	Description
Criminal syndicates	High	A “structured” threat. Structured threats are conducted over a longer period of time, have more financial backing, and possibly help from insiders.
Hackers	Med/High	Skilled actor falling into various categories: **Unauthorized** (malicious), **Authorized** (Good), **Semi-authorized** (usually finding but not exploiting)
Shadow IT	Varies	The use of information technology systems, devices, software, applications, and services without explicit IT department approval, often done with good intentions.
Competitors	Varies, but often Med/High	May encourage individuals within a competitive organization to steal/sell intellectual property.

INSIDE THE HUMAN ELEMENT

Collusion, Fraud, Espionage, and Sabotage

PREVENTING FRAUD AND COLLUSION

Collusion is an agreement among multiple persons to perform some unauthorized or illegal actions.

Separation of duties

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

Job rotation

employees are rotated into different jobs, or tasks are assigned to different employees.

Implementing these policies **helps prevent fraud** by limiting actions individuals can do without colluding with others.

ESPIONAGE & SABOTAGE

Espionage

external

when a competitor tries to steal information, and they may use an internal employee.

Sabotage

insider

malicious insiders can perform sabotage against an org if they become disgruntled for some reason

ATTACK VECTORS - Methods of attack

Vector	Description
Direct access	Physical access to facilities, hardware and infrastructure. Keylogger, flash drive common here.
Wireless	Unsecure access points, rogue access points, evil twin.
Emails	SPAM, phishing, ransomware, fake invoice scams.
Supply chain	Attack on vendors in an organizations supply chain, sometimes as a precursor to direct attack.
Social media	Individuals who use hacking techniques but have limited skills. However, does factor in hybrid warfare.
Cloud	Unsecure apps, misconfigured infrastructure, shadow IT

Countermeasures

Physical security

Secure Wi-Fi netwks

User training
Phishing simulations

Vendor screening

Acceptable use policies

CASB and config management

1.0 THREATS, ATTACKS AND VULNERABILITIES

1.5 Explain different threat actors, vectors, and intelligence sources

- **Threat intelligence sources**
  - Open-source intelligence (OSINT)
  - Closed/proprietary
  - Vulnerability databases
  - Public/private information sharing centers
  - Dark web
  - Indicators of compromise
  - Automated Indicator Sharing (AIS)
  - Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Intelligence Information (TAXII)
  - Predictive analysis
  - Threat maps
  - File/code repositories
- **Research sources**
  - Vendor websites
  - Vulnerability feeds
  - Conferences
  - Academic journals
  - Request for comments (RFC)
  - Local industry groups
  - Social media
  - Threat feeds
  - Adversary tactics, techniques, and procedures (TTP)

THREAT INTELLIGENCE SOURCES

Open-source intelligence (OSINT)

Enables orgs to conduct cyber-threat intelligence gathering free of charge. Sources include threatcrowd.org, openphish.com.

Closed/proprietary

You may see these vendor-specific threat intelligence feeds limited to paying customers, which are intended to keep customers informed and secure, while not tipping off threat actors (hackers).

Vulnerability databases

such as www.shodan.io, allow you to search for vulnerabilities. The National Institute of Standards and Technology (NIST) maintains a comprehensive database of vulnerabilities. This is the National Vulnerability Database and it keeps within that database a list of CVEs or Common Vulnerabilities and Exposures.

THREAT INTELLIGENCE SOURCES

Public/private information sharing centers.

Programs, groups, and feeds to designed to share cyber intelligence in various forms to government and commercial organizations around the world.

The Cybersecurity Infrastructure and Security Agency (CISA), an agency of the US federal government, maintains a list of information sharing centers at https://www.cisa.gov/information-sharing-and-awareness .

Dark web

This is an overlay to the existing internet that requires specialized software to be able to access these private websites. There’s extensive information to gather from the dark web, including the activities of hacker groups.

Indicators of compromise

sometimes called “threat indicators” are “pieces of forensic data, such as data found in system log entries or files, that identify potentially malicious activity on a system or network.”

THREAT INTELLIGENCE SOURCES

SIEM solutions can often ingest threat intelligence feeds

Sources of shared threat intelligence

Automated Indicator Sharing (AIS)

a Cybersecurity and Infrastructure Security Agency (CISA) capability, enables the real-time exchange of machine-readable cyber threat indicators and defensive measures.

It's provided free to help protect participants of the AIS community and ultimately reduce the prevalence of cyberattacks.

Find it at https://www.cisa.gov/ais

Trusted Automated eXchange of Intelligence Information (TAXII)

short for **T**rusted **A**utomated e**X**change of **I**ntelligence **I**nformation, defines how real-time cyber threat information can be shared via services and message exchanges.

Structured Threat Information eXpression (STIX)

TAXII is designed specifically to support STIX information, which it does by defining an API that aligns with common sharing models.

Created by MITRE, maintained by OASIS

THREAT INTELLIGENCE SOURCES

Predictive analysis.

Leverages predictive intelligence, a mix of automation and human intelligence capabilities to optimize your cybersecurity program and gradually build capacity to predict and prevent attacks before they hit.

Threat maps

A cyber threat map, also known as a cyber attack map, is a real-time map of the computer security attacks that are going on at any given time.

Find cyber threat maps from Fortinet, FireEye and other in the Top 8 Cyber Threat Maps

File/code repositories.

Google searching code repositories on sources like Github can show you what threat actors are using. For example, full source code of Mimikatz is available at https://github.com/ParrotSec/mimikatz.

If you're using open-source software for your business, know that hackers often review popular open-source apps looking for vulnerabilities.

RESEARCH SOURCES

Vendor websites

There's usually a page on a vendor's website where they keep track of all of the known vulnerabilities.

Often, there's some type of notification process so they can inform you immediately when a new vulnerability is discovered.

Vulnerability feeds

It's common to supplement vulnerability databases with third party feeds from other organizations. You might roll up all of those vulnerability feeds into one central vulnerability management system.

Conferences

These are great events to network with experts, hear talks often based on experiences of others, and even hear from members of product teams talking in-depth about security of their app or service.

Academic Journals

Offer information about attack types and how others have responded or recovered from them.

Available from a variety of government, education, and community sources, often peer-reviewed!

usually results in higher quality

EXAMPLES:

Oxford Academic Journal of Cybersecurity
https://academic.oup.com/cybersecurity

MDPI Switzerland
https://www.mdpi.com/journal/jcp

Request for comments (RFC)

A publication in a series, from the principal technical development and standards-setting bodies for the Internet, most prominently the **Internet Engineering Task Force (IETF)**.

An **RFC** is authored by individuals or groups of engineers and computer scientists in the form of a memorandum describing methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems.

Request for comments (RFC)

A publication in a series, from the principal technical development and standards-setting bodies for the Internet, most prominently the **Internet Engineering Task Force (IETF)**.

The IETF adopts some of the proposals published as Internet Standards. However, many are informational or experimental in nature and are not standards.

Request for comments (RFC)

A publication in a series, from the principal technical development and standards-setting bodies for the Internet, most prominently the **Internet Engineering Task Force (IETF)**.

The IETF adopts some of the proposals published as Internet Standards.

However, many are informational or experimental in nature and are not standards.

RFCs have become official documents of Internet specifications, communications protocols, procedures, and events.

RESEARCH SOURCES

Learning from your peers and community experts

Local industry groups

You'll find local interest groups or user groups around cybersecurity (and many related topics) where you can learn from your peers and experts in your local community.

Social media

Hackers often publish recent vulnerabilities on **Twitter**

Security interest groups and certification study groups on **LinkedIn**.

Video learning content on **YouTube** on cybersecurity certification, concepts, and entertainment.

RESEARCH SOURCES

Threat feeds

automated threat feed that delivers information about the most important threats you need to know about.

TTP

Tactics, Techniques, and Procedures

the behaviors, methods, tools and strategies that cyber threat actors and hackers use to plan and execute cyber attacks on business networks.

TTPs are the "why" and "how" of cyber attacks, guidance on response and prevention.

1.0 THREATS, ATTACKS AND VULNERABILITIES

1.6 Explain the security concerns associated with various types of vulnerabilities

- **Cloud-based vs. on-premises vulnerabilities**
- **Zero-day**
- **Weak configurations**
  - Open permissions
  - Unsecure root accounts
  - Errors
  - Weak encryption
  - Unsecure protocols
  - Default settings
  - Open ports and services
- **Third-party risks**
  - Vendor management
  - System integration
  - Lack of vendor support
  - Supply chain
  - Outsourced code development
  - Data storage
- **Improper or weak patch management**
  - Firmware
  - Operating system (OS)
  - Applications
- **Legacy platforms**
- **Impacts**
  - Data loss
  - Data breaches
  - Data exfiltration
  - Identity theft
  - Financial
  - Reputation
  - Availability loss

CLOUD-BASED VS. ON-PREMISES VULNERABILITIES

A few examples

Untrained Users

User awareness training is the best defense

One type of vulnerability is an **untrained user**. It only takes one person to cause a breach.

For IT, training and formal processes

Misconfigurations

Change and release mgmt, infrastructure-as-code

An improperly configured account or service be a significant vulnerability in either model.

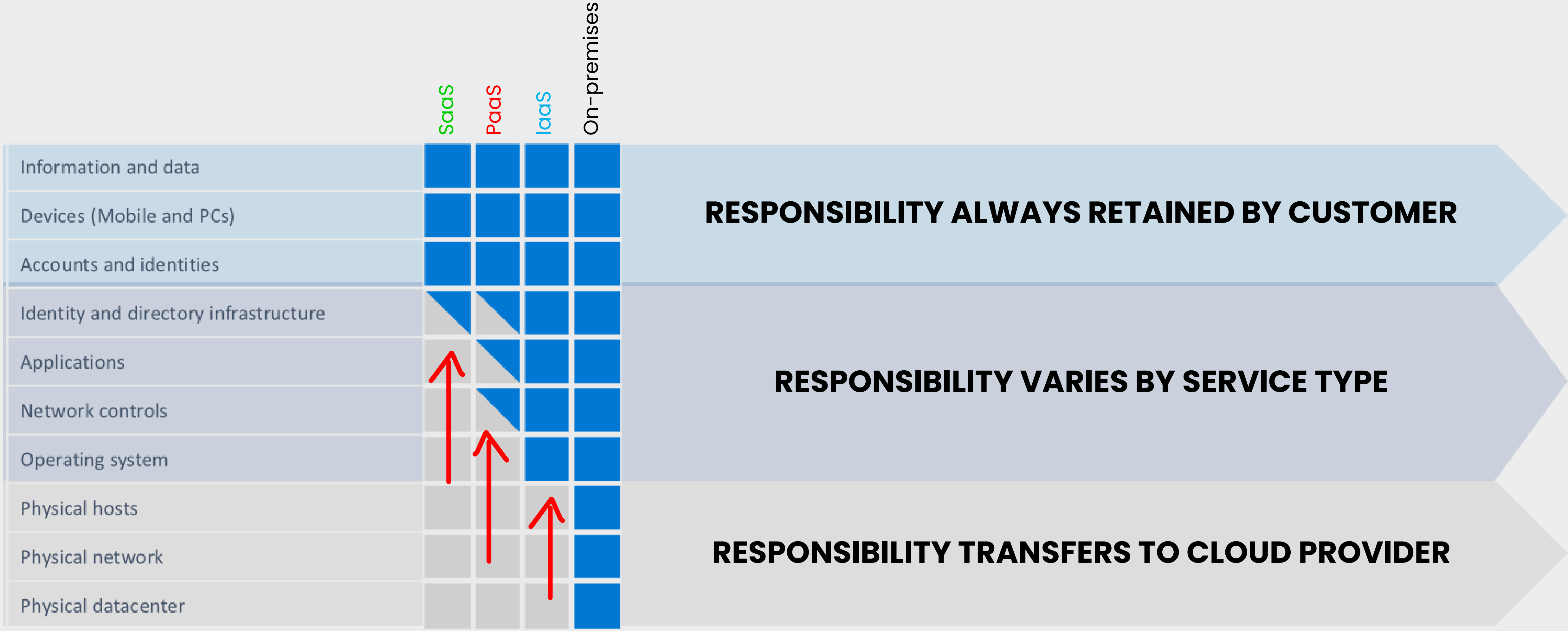
Many cloud platforms have in-built tooling to alert on current misconfigurations, open configurations, least privilege concerns, etc.

Disruptive attacks

On-premises will be more susceptible to **disruptive attacks at scale**, like DDoS.

CSPs have many infrastructure, process, and training advantages

SHARED RESPONSIBILITY MODEL



	SaaS	PaaS	IaaS	On-premises
Information and data	🟦	🟦	🟦	🟦
Devices (Mobile and PCs)	🟦	🟦	🟦	🟦
Accounts and identities	🟦	🟦	🟦	🟦
Identity and directory infrastructure	◪	◪	🟦	🟦
Applications	⬜	◪	🟦	🟦
Network controls	⬜	◪	🟦	🟦
Operating system	⬜	⬜	🟦	🟦
Physical hosts	⬜	⬜	⬜	🟦
Physical network	⬜	⬜	⬜	🟦
Physical datacenter	⬜	⬜	⬜	🟦

RESPONSIBILITY ALWAYS RETAINED BY CUSTOMER

RESPONSIBILITY VARIES BY SERVICE TYPE

RESPONSIBILITY TRANSFERS TO CLOUD PROVIDER

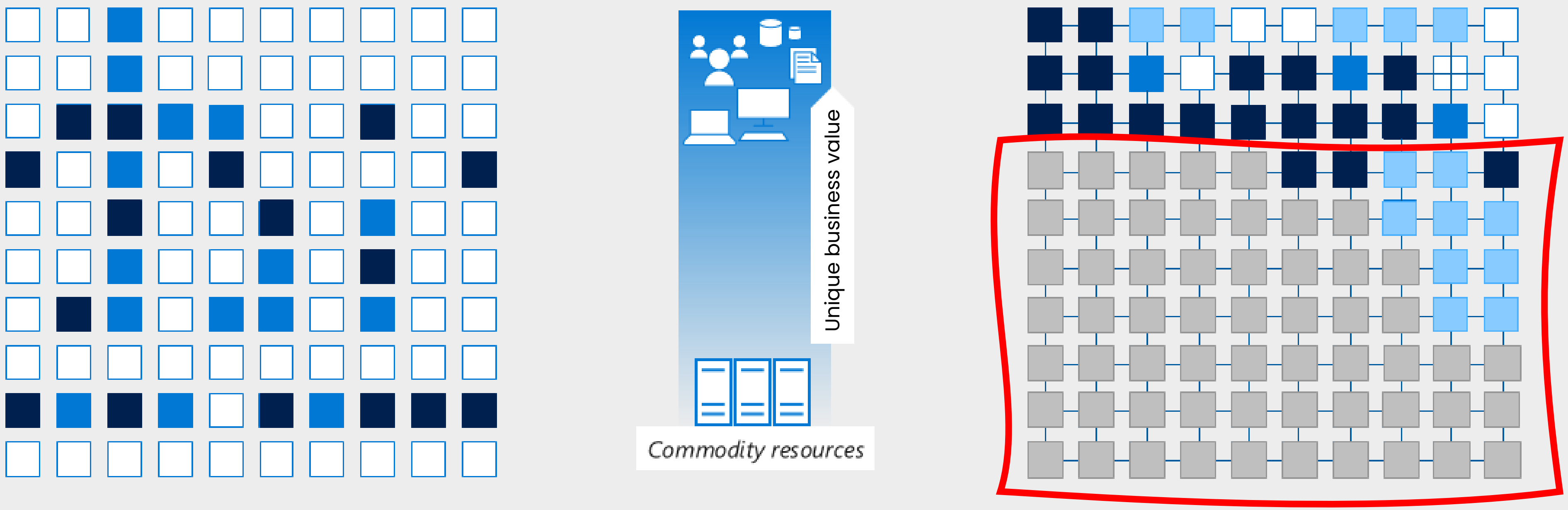
🟦 **CSP** ⬜ **CUSTOMER**

Image courtesy of Microsoft

BETTER SECURITY IN THE CLOUD?

ON-PREMISES

CLOUD-ENABLED



Security is a challenging and under-resourced function

- ■ Satisfied responsibility
- □ Unmet responsibility
- 🟦 Partially met responsibility
- ▨ Cloud provider responsibility

Cloud Technology enables security to:

- ▨ Shift commodity responsibilities to provider and re-allocate your resources
- 🟦 Leverage cloud-based security capabilities for more effectiveness
- ⊞ Use cloud intelligence to improve detection/response time

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

WEAK CONFIGURATIONS

Open permissions

Configurations that have greater than necessary permissions, failing to implement least privilege.

Unsecure default configurations, lack of standards, and human error frequently factors.

Prevent with DevOps, Infra-as-Code, change and release mgmt

Unsecure root accounts

Root accounts with default or weak passwords, or without an elevation gate (like sudo).

Similar issues have been common on Windows in the past.

Errors

Humans are the weakest link in cybersecurity

Researchers from Stanford University found that approximately 88 percent of all data breaches are caused by an employee mistake.

Open ports and services

Open ports and running services that are not actually being used increase the attack surface and risk of breach.

WEAK CONFIGURATIONS

Weak encryption

Choosing strong encryption is key here.

Some cipher suites are easier to crack than others.

Deprecated cryptographic algorithms often remain in production beyond their recommended lifespan.

Unsecure protocols

TELNET, SNMP v1 and v2, FTP

Most networks involve equipment (such as servers, routers, and switches) that support communication protocols that lack security features.

Unsecure protocols allow attackers and hackers to easily have access to your data and even to remote controls.

Default settings

Often a process issue in business scenarios

Every device that you put on your network to manage has a default username and a default password.

Often, the defaults are open and available for anybody to use. (wi-fi and IoT)

Botnets and offensive security tools will find, and exploit devices with weak default settings still in place.

THIRD-PARTY RISKS

Lack of vendor support

Vendor may end support for legacy application versions before an organization is ready to support dependent business processes on another platform.

For apps beyond mainstream support, security patches may be expensive or unavailable entirely.

Outsourced code development

Source code storage and access control will be important.

Development workstations and environments must be secured to the organization's standards. Managed virtual desktop

Data storage

Sensitive data stored in vendor repositories, such as cloud services, needs to be secured, access managed, and usage monitored.

THIRD-PARTY RISKS

Supply chain

One impacted customer can result in service impact

Supply chain security has become a significant concern for organizations.

Includes, suppliers, manufacturers, distributors, and customers.

A breach at any link in the supply chain can result in business impact.

Vendor management

Risk of "island hopping attack"

Many orgs are reducing the number of vendors they work with and requiring stricter onboarding procedures

Vendors may be required to submit to an external audit and agree to strict communication and reporting requirements in event of potential breach.

System integration

Potential for Increased risk of insider attack

System integration partners working on systems often have privileged remote or physical access, necessitating security measures and process controls.

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.

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

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.

Legacy Platforms

Legacy applications that might require an outdated version of an operating system.

May run aging business-critical applications for which staff to manage is difficult to find.

Isolation, attack surface reduction, and patching (if possible) are important to minimize exposure of legacy vulnerabilities

Sandboxing, the process of isolating legacy apps, such as in a VM, can be an effective approach.

Legacy Platforms

Legacy applications that might require an outdated version of an operating system.

May run aging business-critical applications for which staff to manage is difficult to find.

Lack of vendor support for legacy apps poses a risk.
end-of-life date, security updates may no longer be available.

Sandboxing, the process of isolating legacy apps, such as in a VM, can be an effective approach.

IMPACTS

Data breach, loss, exfiltration

Exposure of sensitive data, such as customer data is the first in a long line of consequences of an attack.

Reputation Damage

When a company suffers a data breach and it is known to the public, it can cause their damage to their brand as they lose the respect of the public.

Your domain reputation is dependent on the type of emails you send out.

An attack that results in spam from your domain can affect your domain reputation and perhaps result in it being blacklisted.

Availability Loss

Disruptive attacks like DDoS and ransomware can impact an organization's ability to conduct business, including revenue-producing activities.

IMPACTS

Identity Theft

Identity theft can have far reaching consequences for affected individuals.

If any data held on a customer is stolen and then used for identity theft, the company can be sued for damages.

Financial

Data breaches could result in lost revenue AND regulatory fines.

With GDPR, the max fine is 20 million euros or 4% of the company's annual global turnover, whichever is greater.

Intellectual Property(IP)Theft

IP theft could result in copyrighted material, trade secrets, and patents being stolen by competitors, resulting in a loss of revenue.

This data could be used in countries where a legal route to recover your data would be impossible.

1.0 THREATS, ATTACKS AND VULNERABILITIES

1.7 Summarize the techniques used in security assessments

- **Threat hunting**
  - Intelligence fusion
  - Threat feeds
  - Advisories and bulletins
  - Maneuver
- **Vulnerability scans**
  - False positives
  - False negatives
  - Log reviews
  - Credentialed vs. non-credentialed
  - Intrusive vs. non-intrusive
  - Application
  - Web application
  - Network
  - Common Vulnerabilities and Exposures (CVE)/Common Vulnerability Scoring System (CVSS)
  - Configuration review
- **Syslog/Security information and event management (SIEM)**
  - Review reports
  - Packet capture
  - Data inputs
  - User behavior analysis
  - Sentiment analysis
  - Security monitoring
  - Log aggregation
  - Log collectors
- **Security orchestration, automation, and response (SOAR)**

THREAT HUNTING

a dynamic process of seeking out cybersecurity threats inside your network from attackers and malware threats.

Intelligence Fusion

involves industry and government

Fusion centers in the US and abroad play an important role in countering cyber threats, attacks, and crime through gathering, analyzing, and sharing threat information.

Threat Feeds

Threat intelligence feeds

Enable organizations to stay informed about indicators of compromise (IoCs) related to various threats that could adversely affect the network.

THREAT HUNTING

a dynamic process of seeking out cybersecurity threats inside your network from attackers and malware threats.

Advisories and Bulletins

Advisories and security bulletins provide good advice on how to keep your company safe.

The advisories tend to be released government-funded agencies.

Bulletins tend to be released by vendors or private companies.

Maneuver

A cybersecurity maneuver, then, refers to a company's efforts to defend itself by disguising its systems, thereby making it difficult for an attacker to successfully infiltrate.

VULNERABILITY SCANS

A vulnerability scan assesses possible security vulnerabilities in computers, networks, and equipment that can be exploited.

False Positive: where the scan believes that there is a vulnerability but when physically checked, it is not there.

False Negative: When there is a vulnerability, but the scanner does not detect it.

True Positive: This is where the results of the system scan agree with the manual inspection.

Log Reviews: Following a vulnerability scan, it is important to review the log files/reports that list any potential vulnerabilities.

VULNERABILITY SCANS

A vulnerability scan assesses possible security vulnerabilities in computers, networks, and equipment that can be exploited.

Credentialed Scan: A credentialed scan is a much more powerful version of the vulnerability scanner. It has higher privileges than a non-credentialed scan.

Spot vulnerabilities that require privilege, like non-expiring PWs

Non-Credentialed Scan: A non-credentialed scan has lower privileges than a credentialed scan. It will identify vulnerabilities that an attacker would easily find.

Scans can find missing patches, some protocol vulnerabilities

VULNERABILITY SCANS

A vulnerability scan assesses possible security vulnerabilities in computers, networks, and equipment that can be exploited.

Non-Intrusive Scans: These are passive and merely report vulnerabilities. They do not cause damage to your system.

Intrusive Scans: can cause damage as they try to exploit the vulnerability and should be used in a sandbox and not on your live production system.

Configuration Review: Configuration compliance scanners and desired state configuration in PowerShell ensure that no deviations are made to the security configuration of a system.

The combination of techniques can reveal which vulnerabilities are most easily exploitable in a live environment.

VULNERABILITY SCANS

Network Scans: These scans look at computers and devices on your network and help identify weaknesses in their security.

Application Scans: Before applications are released, coding experts perform regression testing that will check code for deficiencies.

Web Application Scans:
Crawl through a website as if they are a search engine looking for vulnerabilities.

Perform and automated check for site/app vulnerabilities, such as cross-site scripting and SQL injection.

Also know difference between SAST and DAST for the exam

There are many sophisticated web application scanners available, due in part due to mass adoption of cloud computing.

VULNERABILITY SCANS

Common Vulnerabilities and Exposures (CVE) and Common Vulnerability Scoring System (CVSS)

CVSS is the overall score assigned to a vulnerability. It indicates severity and is used by many vulnerability scanning tools.

CVE is simply a list of all publicly disclosed vulnerabilities that includes the CVE ID, a description, dates, and comments.

The CVSS score is not reported in the CVE listing – you must use the **National Vulnerability Database (NVD)** to find assigned CVSS scores.

The CVE list feeds into the NVD

The National Vulnerability Database (NVD) is a database, maintained by NIST, that is synchronized with the MITRE CVE list.

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.

Packet Capture

Can capture packets and analyze them to identify threats as soon as they reach your network, providing immediate alert to security team if desired.

Data Inputs

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

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

SYSLOG/SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

User Entity Behavior Analysis (UEBA)

This is based on the interaction of a user that focuses on their identity and the data that they would normally access on a normal day.

It tracks the devices that the user normally uses and the servers that they normally visit.

Sentiment Analysis

Artificial intelligence and machine learning to identify attacks.

Cybersecurity sentiment analysis can monitor articles on social media, look at the text and analyze the sentiment behind the articles.

Over time, can identify a users' attitudes to different aspects of cybersecurity.

Security Monitoring

Real-time protection and event monitoring system that correlates the security events from multiple resources, identifies a breach, and helps the security team to prevent the breach.

UEBA, AI, ML, and threat intel feeds all factor here

ARTIFICIAL INTELLIGENCE vs MACHINE LEARNING

From section 1.2

Knowing the difference will help on the exam!

Artificial Intelligence

Focuses on accomplishing "smart" tasks combining machine learning and deep learning to emulate human intelligence

Machine Learning

A subset of AI, computer algorithms that improve automatically through experience and the use of data.

Deep Learning

a subfield of machine learning concerned with algorithms inspired by the structure and function of the brain called **artificial neural networks**.

SYSLOG/SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Event Reporting (Review Reports)

A SIEM typically includes dashboard and collects reports that can be reviewed regularly to ensure that the policies have been enforced and that the environment is compliant.

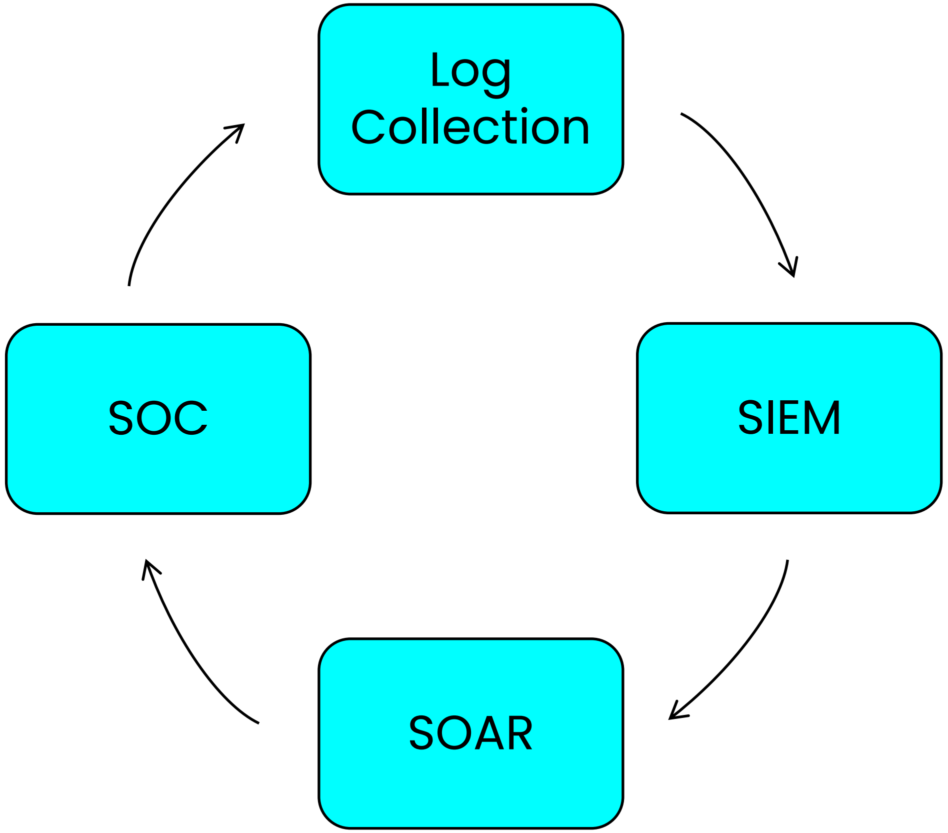
Also highlight whether the SIEM system is effective and working properly. Are incidents raised true positives?

False positives may arise because the wrong input filters are being used or the wrong hosts monitored.

For the exam, Know the difference between **UEBA**, **machine learning**, **AI**, and **deep learning**.

SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR)

Tooling that allows an organization to define incident analysis and response procedures in a digital workflow format.



Integrates your security processes and tooling in a central location.

Response automation, using machine learning and artificial intelligence

These make it faster than humans in identifying and responding to true incidents.

Reduces MTTD and accelerates response

Uses **playbooks** that define an incident and the action taken. Capabilities vary by situation & vendor

Over time, should produce faster alerting and response for the SOC team.

1.0 THREATS, ATTACKS AND VULNERABILITIES

1.8 Explain the techniques used in penetration testing

- **Penetration testing**
  - Known environment
  - Unknown environment
  - Partially known environment
  - Rules of engagement
  - Lateral movement
  - Privilege escalation
  - Persistence
  - Cleanup
  - Bug bounty
  - Pivoting

- **Passive and active reconnaissance**
  - Drones
  - War flying
  - War driving
  - Footprinting
  - OSINT

Exercise types

- Red-team
- Blue-team
- White-team
- Purple-team

PENETRATION TESTING CONCEPTS

Known environment white box test

penetration tester is given a map of target systems and networks. They go into the test with substantial/full information of the target systems and networks.

Unknown environment black box test

penetration tester knows nothing about target systems and networks. They go into the test completely blind and build out the database of everything they find as they go.

Partially known environment grey box test

limited information is shared with the tester, sometimes in the form of login credentials. Simulate the level of knowledge that a hacker with long-term access to a system would achieve through research and system footprinting.

Rules of engagement

Rules of engagement define the purpose of the test, and what the scope will be for the people who are performing this test on the network.

They ensure everyone will be aware of what systems will be considered, date and time, and any constraints all should be aware of.

PENETRATION TESTING CONCEPTS

Lateral movement

Gaining access to an initial system, then moving to other devices on the inside of the network.

Privilege escalation

A security hole created when code is executed with higher privileges than those of the user running it.

Generally, a higher-level account, but in some cases, it is a horizontal privilege escalation where a user gains access to another users' resources.

Persistence

in the context of penetration testing refers to the testers ability to achieve a persistent presence in the exploited system— long enough for a bad actor to gain in-depth access.

Enabling the ability to reconnect to the compromised host and use it as a remote access tool.

PENETRATION TESTING

Cleanup

The final stage of a penetration test, in which all work done during the testing process is cleaned up / removed.

Bug bounty

A monetary reward given to ethical hackers for successfully discovering and reporting a vulnerability or bug to the application's developer. Bug bounty programs allow companies to leverage the hacker community to improve their systems' security posture over time continuously.

Pivoting

Also known as island hopping , a compromised system is used to attack another system on the same network following the initial exploitation . If the compromise is introduced at a different time than the attack, then it is said to involve persistence.

PASSIVE AND ACTIVE RECONNAISSANCE

Passive reconnaissance one is not interacting directly with the target and as such, the target has no way of knowing, recording, or logging activity.

War driving

Gathering wireless network information while driving around the streets of the city.

Drones

Can be leveraged in multiple ways for passive reconnaissance, from assessing physical security to gathering wireless network information.

War flying

Combines war driving with a drone and simply float above all of these organizations to gather wireless details. Enables accumulation of information like SSID or wireless network names, and encryption status of these networks.

PASSIVE AND ACTIVE RECONNAISSANCE

Passive reconnaissance one is not interacting directly with the target and as such, the target has no way of knowing, recording, or logging activity.

OSINT

Much of this information in the open source can be categorized as open-source intelligence or OSINT. The data that you can gather through these open sources is extensive.

A site that gives you a base of information that you can gather is available at https://osintframework.com

PASSIVE AND ACTIVE RECONNAISSANCE

Active reconnaissance interacts directly with the target in some way and as such, the target may discover, record, or log these activities.

Footprinting

Includes active and passive methods

An ethical hacking technique used to gather as much data as possible about a specific targeted computer system, infrastructure and networks to identify opportunities to penetrate them.

Active footprinting

Ping sweep
Tracert analysis
Nmap
Extracting DNS information

Passive footprinting

Browsing target website
Google search (Google hacking)
Performing WHOIS lookup
Visiting social media profiles

Exercise Types

Red Team offense

are internal or external entities dedicated to testing the effectiveness of a security program by emulating the tools and techniques of likely attackers in the most realistic way possible.

Blue Team defense

the internal security team that defends against both real attackers and Red Teams.

Purple Team process improvement

exist to ensure and maximize the effectiveness of the Red and Blue teams.

White Team judge / referee

responsible for overseeing an engagement/competition between a Red Team of mock attackers and a Blue Team of actual defenders.

INSIDE CLOUD

AND SECURITY

THANKS

FOR WATCHING!