



Course 446

CompTIA Security+ Certification Exam Preparation

by

Randy W. Williams

Technical Editor: Jay Hickman



Copyright

© LEARNING TREE INTERNATIONAL, INC.
All rights reserved.

All trademarked product and company names are the property of their
respective trademark holders.

No part of this publication may be reproduced, stored in a retrieval system, or
transmitted in any form or by any means, electronic, mechanical, photocopying,
recording or otherwise, or translated into any language, without the prior written
permission of the publisher.

Copying software used in this course is prohibited without the express
permission of Learning Tree International, Inc. Making unauthorized copies of
such software violates federal copyright law, which includes both civil and
criminal penalties.

Acknowledgements

The author would like to acknowledge the following for contributions to this course

- ▶ Heidi Foster
- ▶ Jay Hickman
- ▶ Mitch Garvis
- ▶ The Herndon PD Lab





Introduction and Overview

Course Objectives

- ▶ **Introduce the Security+ Objectives and outline testing procedures**
- ▶ **Review the basic elements of cybersecurity**
- ▶ **Inspect security program oversight and management**
- ▶ **Investigate threats, attacks, and mitigations**
- ▶ **Apply secure architecture and design principles**
- ▶ **Utilize secure protocols and defenses**
- ▶ **Inspect identity management and cryptography**
- ▶ **Assess readiness for the exam**



PKI = public key infrastructure

Course Contents

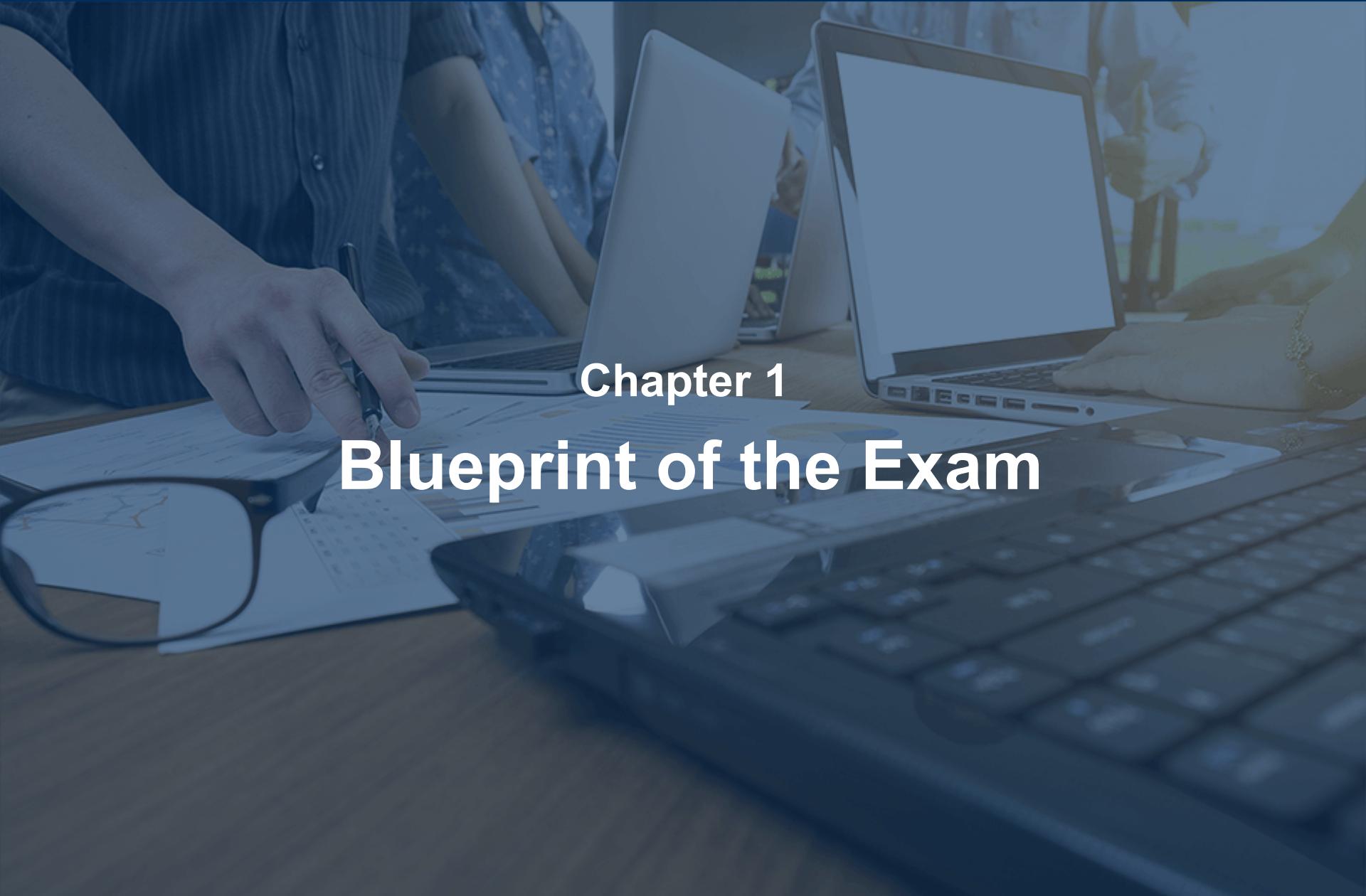
Introduction and Overview

- Chapter 1 Blueprint of the Exam**
- Chapter 2 Domain 1: General Security Concepts**
- Chapter 3 Domain 5: Security Program Management and Oversight**
- Chapter 4 Domain 2: Threats, Vulnerabilities, and Mitigations**
- Chapter 5 Domain 3: Security Architecture**
- Chapter 6 Domain 4: Security Operations**
- Chapter 7 Final Preparation and Review**
- Chapter 8 Course Summary**
- Next Steps**

Ground Rules

To encourage a positive course experience, let's observe the following ground rules

- ▶ Be open to new ideas or approaches
- ▶ Participate actively
 - Very important to extract maximum value
- ▶ Recognize that, in this class, we must focus on the *right* answer
 - “Right” is the answer that will get you the mark for a question
- ▶ Embrace a “discovery approach” to learning
- ▶ Have some *fun!*

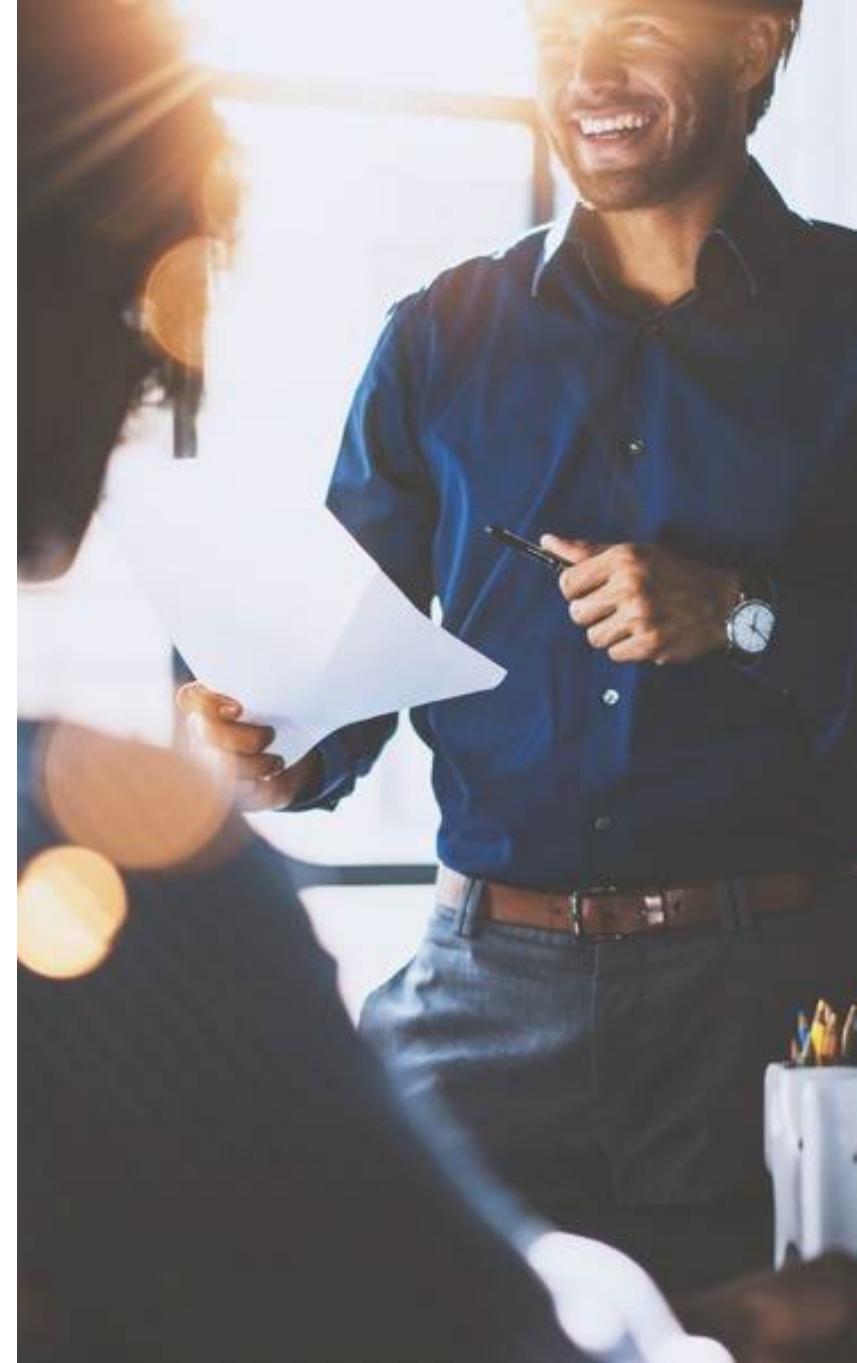


Chapter 1

Blueprint of the Exam

Objectives

- ▶ **Outline the goals of the CompTIA Security+ test**
- ▶ **Present the test procedures and parameters**
- ▶ **Inspect the domains of knowledge**



Contents

The CompTIA Security+ Test

- Domains of Knowledge



CompTIA Security+ Certification

- ▶ A well-recognized examination of computer security technical and policy knowledge
- ▶ For DoD personnel
 - Needed for personnel in IAT-2 and IAM-1 positions
 - DoD 8140/8570.1 requirements <https://public.cyber.mil/wid/cwmp/dod-approved-8570-baseline-certifications/>
 - For IAT-3 and IAM-2, additional certifications are needed (e.g., CISSP)
 - General certification and test information available at
 - <https://www.comptia.org/certifications/security#examdetails>
- ▶ Often required or recommended for other government and business positions

CISSP = Certified Information System Security Professional

DoD = U.S. Department of Defense

IAM = Information Assurance Management

IAT = Information Assurance Technical

Continuing Education

- ▶ **CompTIA Security+ requires 50 CEUs to renew for three years**
 - This certification is valid for three years
 - You may also take the new full exam
 - A \$50 USD annual maintenance fee is also required
- ▶ **These activities are eligible for continuing education credit**
 - Teaching, lecturing, or presenting on relevant industry topics
 - Participating in non-degree courses or computer-based training
 - Attending relevant industry conferences
 - Publishing articles or blogs
 - Work experience
 - Participation in IT events
- ▶ **See <https://www.comptia.org/continuing-education/learn/earn-continuing-education-units> for numbers of credits granted for activities**

CEU = Continuing Education Unit
USD = United States dollars

The CompTIA Security+ Certification Exam

► **Measures skills and knowledge for**

- Terms and concepts
- Communication protocols
- Best practices
- Devices
- Alerts, logs, and output
- Policies and frameworks
- Some tools and techniques
- Risk management strategies

► **Weighted for these domains**

• 1.0 General Security Concepts	12%
• 2.0 Threats, Vulnerabilities, and Mitigations	22%
• 3.0 Security Architecture	18%
• 4.0 Security Operations	28%
• 5.0 Security Program Management and Oversight	20%

The CompTIA Security+ Certification Exam

- ▶ The 2023 revision exam code: SY0-701
- ▶ 72 to 90 questions during a 90-minute exam
 - Multiple choice, many indicate choosing the *best* answer
 - Mostly single answers
 - Expect 5-8 multiple answer items
 - Many multiple-sentence questions
 - Many require acronym mastery
 - Expect several exhibits or simulations worth multiple points
 - Each examination session draws from a large pool
 - Question count balanced for each domain
- ▶ Commonly requires higher levels of knowledge
 - Explain/Summarize Basic definitional understanding
 - Compare/Differentiate Broad knowledge
 - Implement/Install/Configure Detailed knowledge <<
 - Analyze/Interpret Exhibits <<
 - Troubleshoot Simulations <<

Exhibits typically have multiple tasks, each worth about 1 percentage point. It seems partial credit is given.

The CompTIA Security+ Certification Exam

► Scoring

- 750 is the minimum passing score
 - 100–900 point range
- 81.25 percent needed

► Most questions weighted evenly

- Multiple-choice questions all count the same
- Simulations count more, worth 5 percent to 15 percent on each question
- Blank answers scored as incorrect answers

► Question quality

- Poor overall
 - Some questions are inaccurately written and ambiguous
 - There may be a few single-select questions with 2 or more correct answers
- Expect
 - Some confusing questions or vaguely wrong sets of answers
 - Anticipate many questions with the correct answer being borderline wrong

This Course

- ▶ **A boot-camp course**
 - A full week
 - Full breadth of all domains
 - Practical testing strategies
 - Practice examinations
- ▶ **Discussion will cover all published Security+ Objectives**
- ▶ **Demonstrations of difficult concepts**
- ▶ **Match the items**
 - About midway in each chapter, a vocabulary quiz will be administered
 - A list of topics is shown on the left part of the slide
 - A mixed listing of corresponding terms or definitions is on the right part of the slide
 - Match the items to the terms and definitions
 - The real exam is likely to have several of these
- ▶ **Review at the end of each chapter**

This Course

- ▶ **Vouchers for the test**
 - Your test voucher will be sent once you request it
 - Contact Customer Service 1-800-THE-TREE
 - Will be emailed
- ▶ **When you are ready for your CompTIA exam, register at**
 - <http://vue.com>
 - You can select from test centers in your area or other centers worldwide
 - Online remote testing is possible
- ▶ **Broad coverage**
 - The exam is considered difficult
- ▶ **Topics match the Security+ Objectives, including the obscure areas**
 - Backup strategies
 - General policy
 - Physical security

Contents

- The CompTIA Security+ Test

Domains of Knowledge



The Chapters and Domains

- ▶ **Chapter 2—Domain 1: General Security Concepts**
 - Types of concepts and controls
 - Change management
 - Cryptography
- ▶ **Chapter 3—Domain 5: Security Program Management and Oversight**
 - Effective governance
 - Risk management process
 - Third-party risk assessment and management
 - Compliance and audits
 - Security awareness

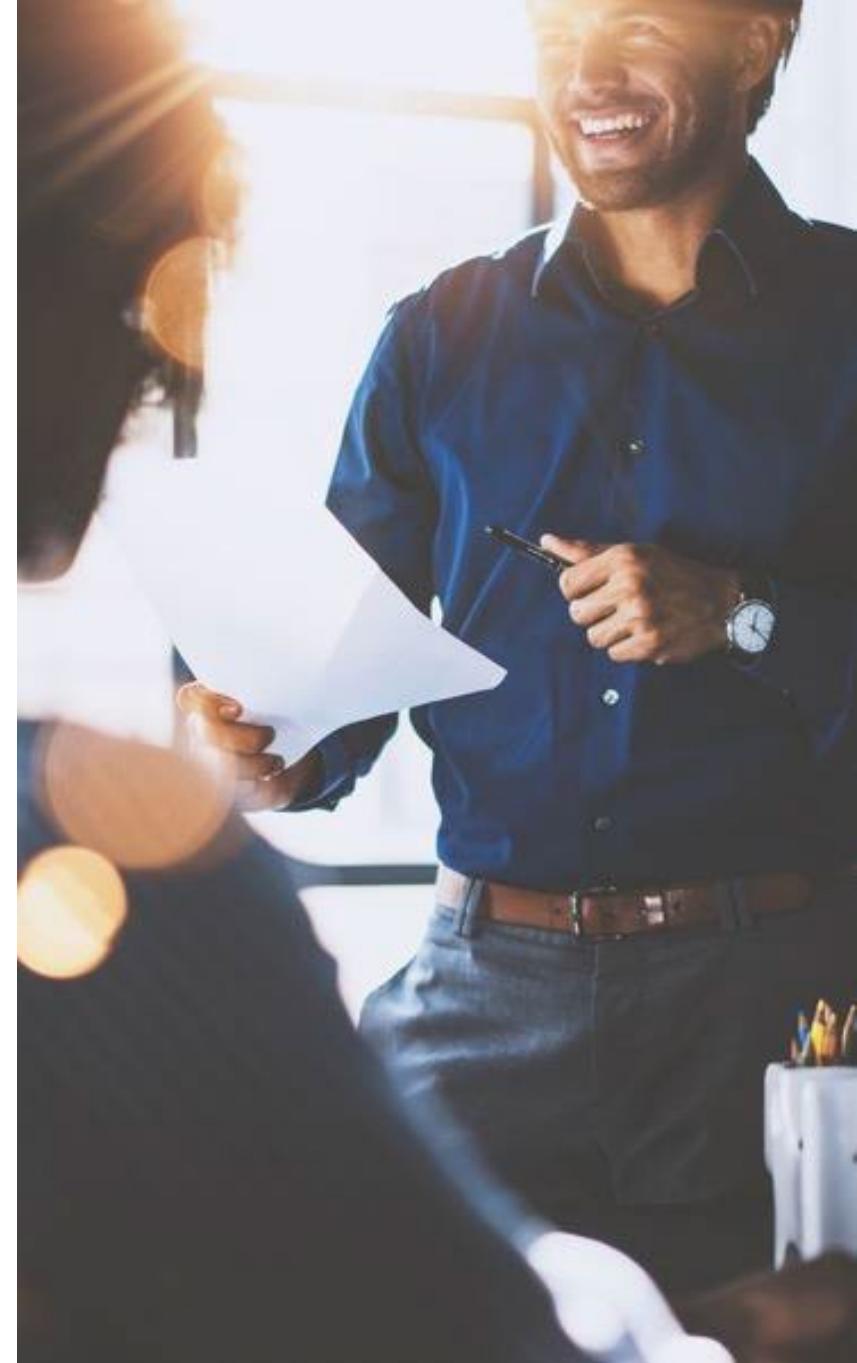
The domains will be taught in an order to best build upon knowledge and prerequisites

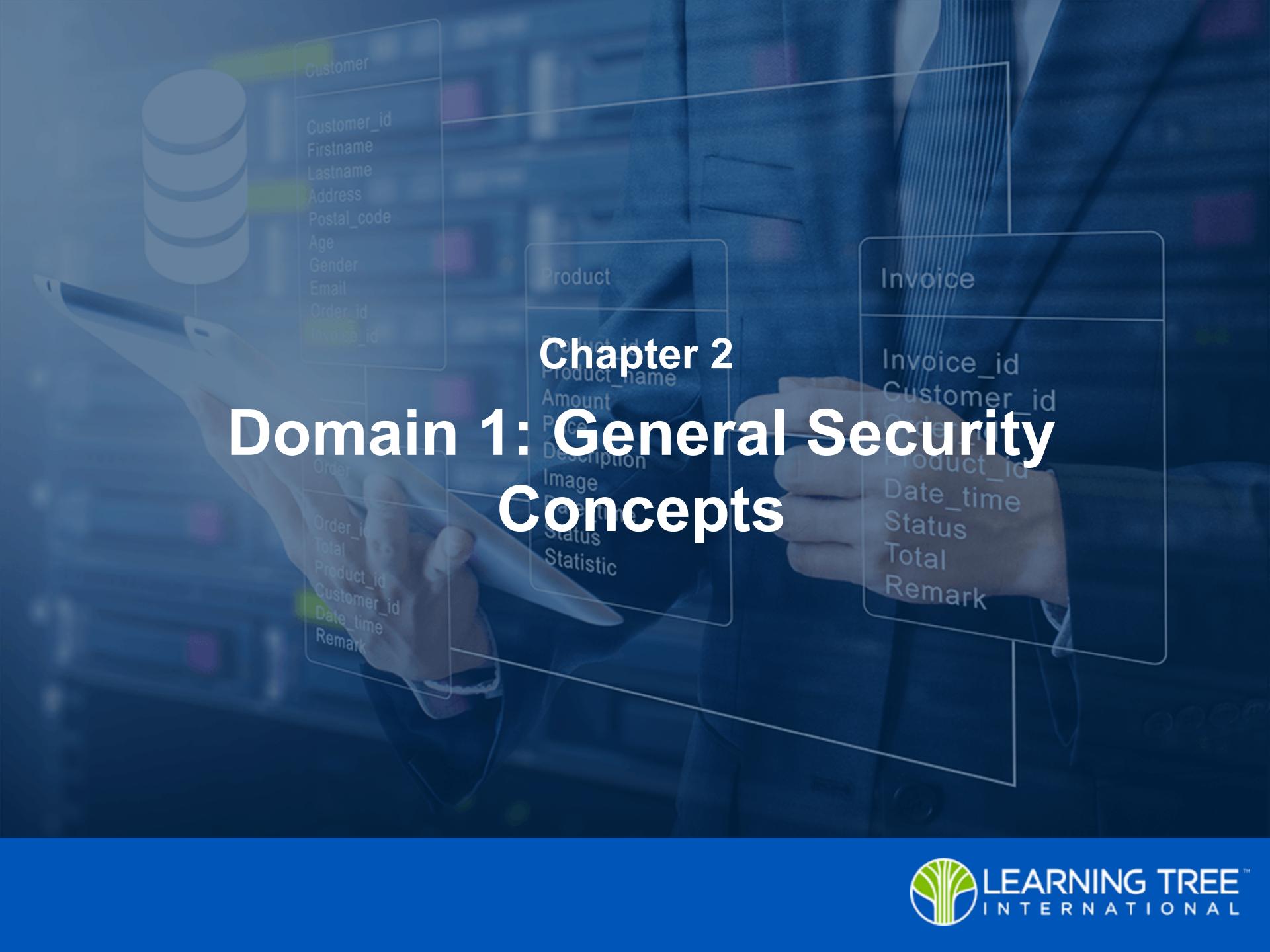
The Chapters and Domains

- ▶ **Chapter 4—Domain 2: Threats, Vulnerabilities, and Mitigations**
 - Threat actors
 - Vectors and attack surfaces
 - Vulnerabilities and malicious activities
 - Mitigation techniques
- ▶ **Chapter 5—Domain 3: Security Architecture**
 - Comparing security architectures
 - Securing the enterprise
 - Protecting data
 - Resilience and recovery
- ▶ **Chapter 6—Domain 4: Security Operations**
 - Hardware, software, and data asset management
 - Vulnerability management
 - Automation, alerting and monitoring
 - Identity and Access Management
 - Incident response activities and investigations

Objectives

- ▶ **Outline the goals of the CompTIA Security+ test**
- ▶ **Present the test procedures and parameters**
- ▶ **Inspect the domains of knowledge**





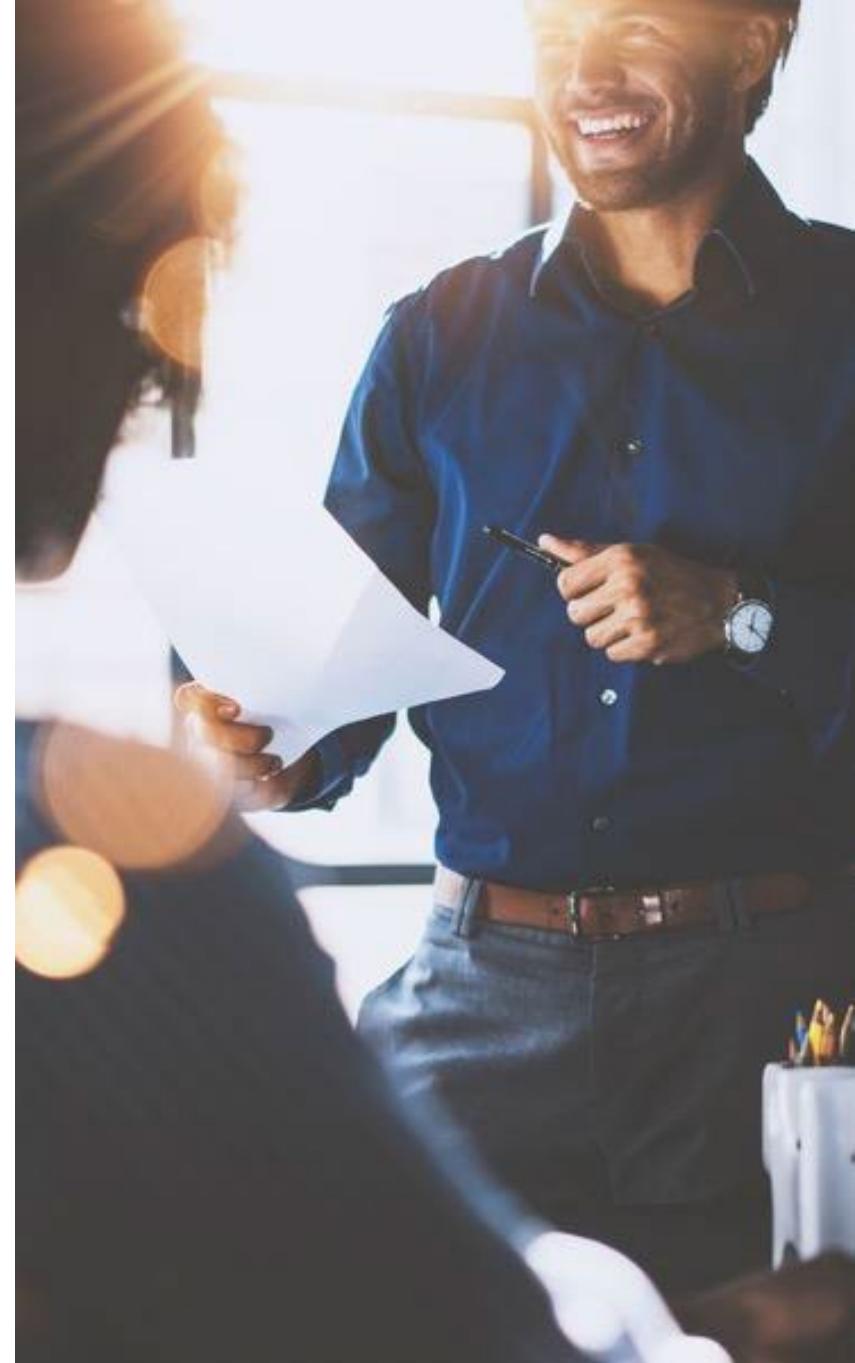
Chapter 2

Domain 1: General Security Concepts

Objectives

- ▶ **Identifying security fundamentals**
- ▶ **Comparing and contrast security controls**
- ▶ **Understanding the importance of change management**
- ▶ **Applying secure cryptographic principles**

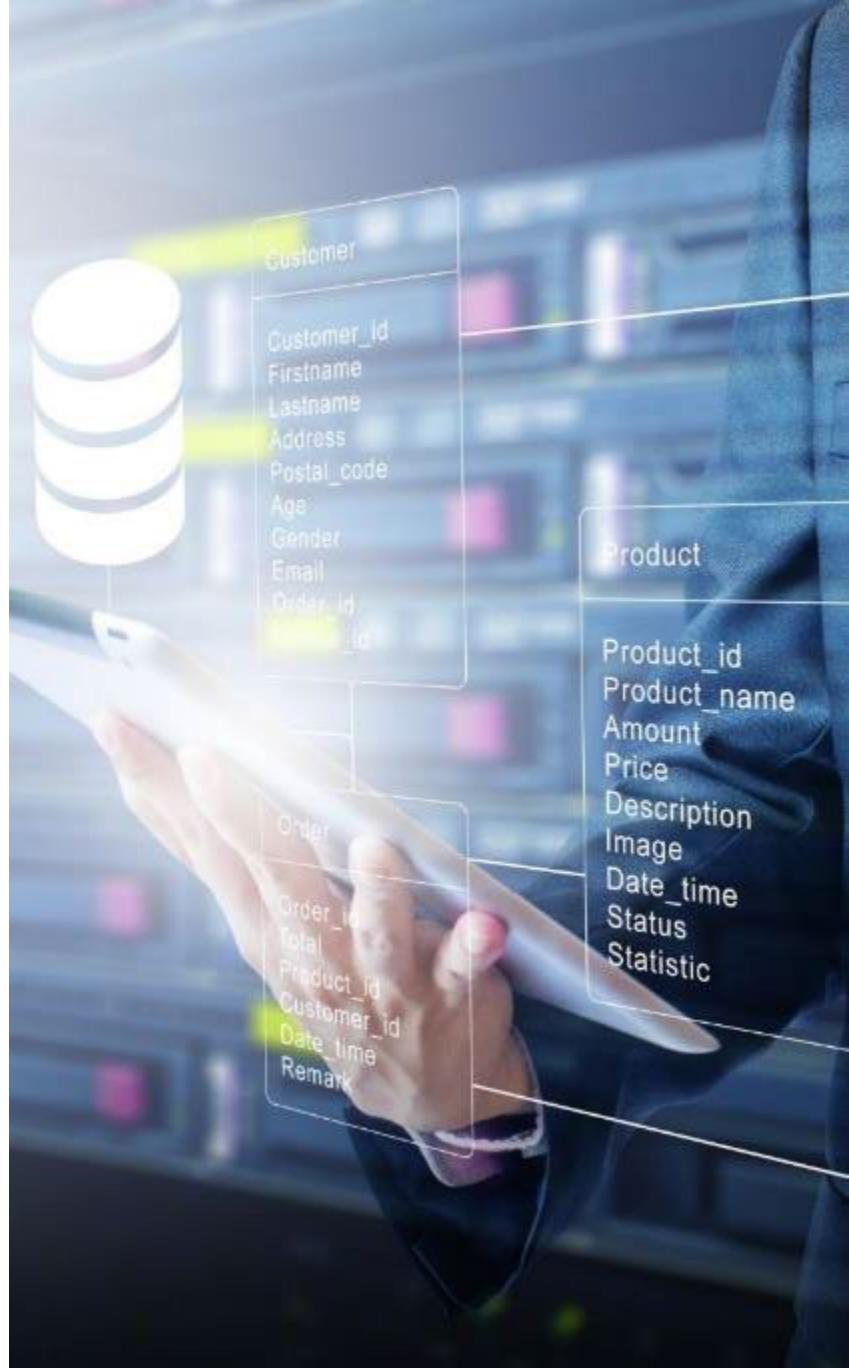
12%



Contents

Fundamentals of Security

- ▶ **Security Controls**
- ▶ **Change Management**
- ▶ **Cryptography**



Organizational Security Goals: CIA

- ▶ **Confidentiality**
 - Goals: “*Ensuring that information is accessible only to those authorized to have access*”*
 - Threats: Eavesdropping, system compromise, and access
 - Defenses: Cryptosystems, access controls
- ▶ **Integrity**
 - Goals: “*Data integrity is having assurance that the information has not been altered in transmission, from origin to reception*”*
 - Threats: Spoofing, system compromise, and access
 - Defenses: Digital signatures and hashing
- ▶ **Availability**
 - Goals: “*Assurance in the timely and reliable access to data services for authorized users*”*
 - Threats: Denial of Service (DoS)
 - Defenses: Redundancy, fault tolerance, and patching

*Source: www.iso.org

Measures to Achieve Security Goals

► AAA

- Authentication
 - Confirming identity
- Authorization
 - Permission to use resources
- Accountability
 - Verifying that authorized use has been proper
 - Enforced with auditing and logging

► Nonrepudiation

- Being certain of message origin (able to undeniably confirm that a message was sent by a party at a given time)
- E.g., digital signature

Authentication and Authorization

- ▶ **Authentication may be applied to**
 - People—username/password, tokens, Kerberos
 - Systems—certificates, Kerberos, IP address
- ▶ **Authorization models**
 - MAC—Mandatory Access Control
 - DAC—Discretionary Access Control
 - RBAC—Role-Base Access Control
 - RBAC—**Rule**-Base Access Control
 - ABAC—Attribute-Based Access Control
- ▶ **These identity and access management models will be discussed in detail in Domain 4**

Physical Security Measures

- ▶ Logical security can be no better than the physical defenses
- ▶ These should include
 - Guards in places where judgment is required or where cameras cannot reach
 - Cameras have the advantage of being always on and recording
 - Secured areas, such as wiring centers and data centers
 - Swipe card, inexpensive cipher locks with door codes, or biometric access control
 - Lock types include: Pin/tumbler, high-security—Medeco, Wafer
 - Locking cabinets and enclosures
 - Security screws
 - Safes or vaults to store small or critical devices
 - HSM, TPM, critical media
 - Cable locks attached to systems
 - Master keying systems
 - Emergency access



HSM = Hardware Security Module
TPM = Trusted Platform Module

Physical Security Measures

- ▶ **Logical security is no better than the physical security provided to devices**
 - Signs
 - Lighting
 - Fencing, gates for people
 - Bollards, and barricades as anti-vehicle measures
 - Air gaps—are the most secure, no connectivity
 - Access control vestibules, mantraps and turnstiles—screening areas that regulate access
 - Access badges/CAC/PIV and access control lists
 - Video/cameras to monitor employees and unguarded areas
 - Protected wiring centers and cabling systems
 - Proximity card and RFID readers
 - Screen filters and polarizers—to prevent eavesdropping
- ▶ **Be prepared to select any of these controls based upon a scenario**



CCTV = closed-circuit television
RFID = radio-frequency identification

CAC = Common Access Card
PIV = Personal Identity Verification

Sensors

► **Infrared**

- Often used at doorways to detect body heat and motion

► **Pressure**

- Weight sensitive and commonly used for doors

► **Microwave**

- Similar to radio wave and detects via reflections and movement

► **Ultrasonic**

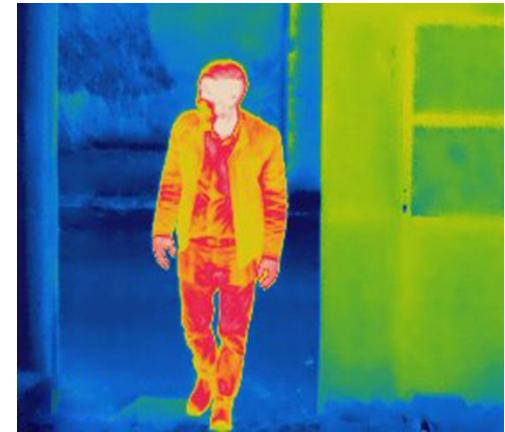
- Sound reflections detect via sonar-like methods

► **Humidity/moisture**

- Highly sensitive to changes in the environment

► **Sound detection**

- Glass breaking sensors are usually tuned to listen for the high-pitched sound of glass breaking



Deception and Disruption

- ▶ **Honeypots are often used by antivirus companies to gather samples**
 - A *honeynet* is a simulated network of honeypots
 - Honeypots may not be useful for prosecution
 - Samples analyzed with Cuckoo—a popular analysis tool
- ▶ **Honeyfiles:**
 - Closely monitored files that will set off alarms when accessed to identify intrusions
- ▶ **Honeytokens**
 - Unique or fictitious words/phrases added to communications streams to track data leaks
- ▶ **Goals**
 - Discover new threats—zero-days
 - And new viruses
 - Divert an attacker from real assets
 - Observe the attacker
 - Identify source, methods and areas of interest



Contents

- ▶ Fundamentals of Security

Security Controls

- ▶ Change Management
- ▶ Cryptography



Achieving Security With Controls

- ▶ **Based upon assessments of risk and gaps, controls are assigned**
 - NIST SP 800-53 is an excellent catalog of controls
- ▶ **Technical**
 - Security controls that the computer system executes (e.g., firewalls, IDS, and deploying whitelisting)
- ▶ **Management (also called Administrative)**
 - The management of the computer security program and risk within the organization (e.g., creating a risk management process for implementing job rotation or conducting a penetration test)
- ▶ **Operational**
 - Defenses that regard people and are executed by them
 - Training
 - Security awareness
 - Disaster preparation
- ▶ **Physical**

IDS = intrusion detection system

Pop Quiz: Controls



Indicate the type of control: Management, Technical, Operational

- 1. John is a CISO and has ordered a technical penetration test of the externally facing IT assets.**
- 2. Mary has been hired to social engineer her way beyond the front door vestibule.**
- 3. Amad has decided to perform a virus scan of his computer.**
- 4. Jason is implementing a firewall between accounting and the Call Center.**

Security Controls

- ▶ These are defensive methods that implement a risk management strategy
- ▶ Detective
 - Lights and surveillance cameras
 - SIEMs
 - E.g., mail server Logs and other audits
- ▶ Preventative
 - Firewalls
 - Door access controls
- ▶ Corrective
 - Backups
 - Redundant servers
 - Cross-training
 - Invoked after an incident



PTZ = pan, tilt, zoom

Security Measures

► Deterrent

- Clean desk and closed-door policy
- Highly visible guards
- Warning signs (“Use of lethal force authorized”)

► Compensating

- Fire extinguishers
- Cross-training of personnel
- Invoked during an incident

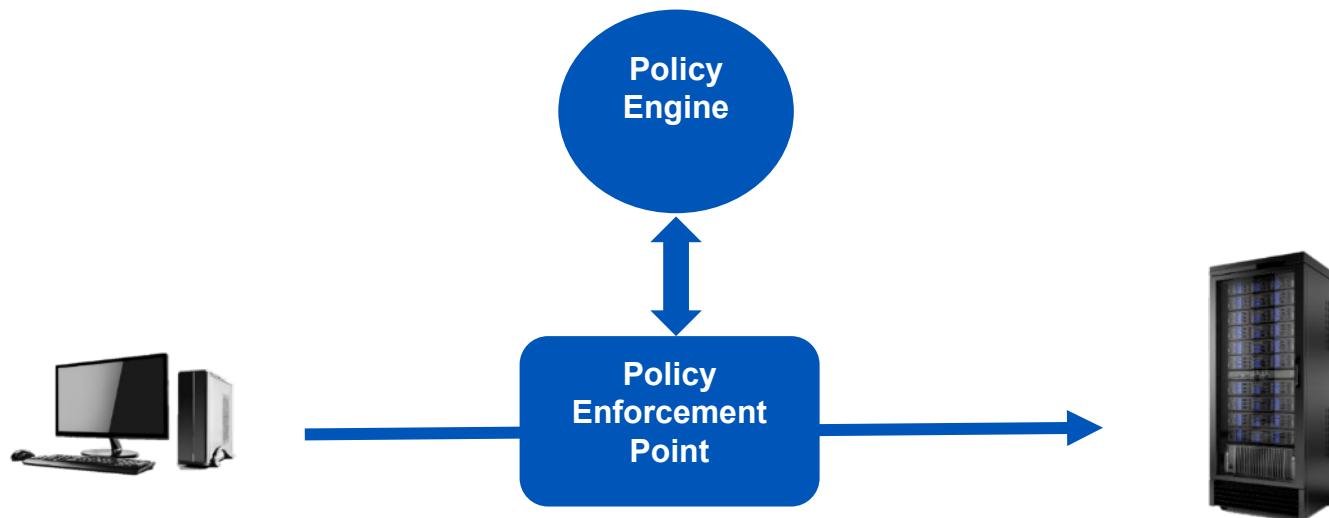
► Directive

- Implementing policies, standards, procedures and guidelines
- E.g.: Devising acceptable use policies



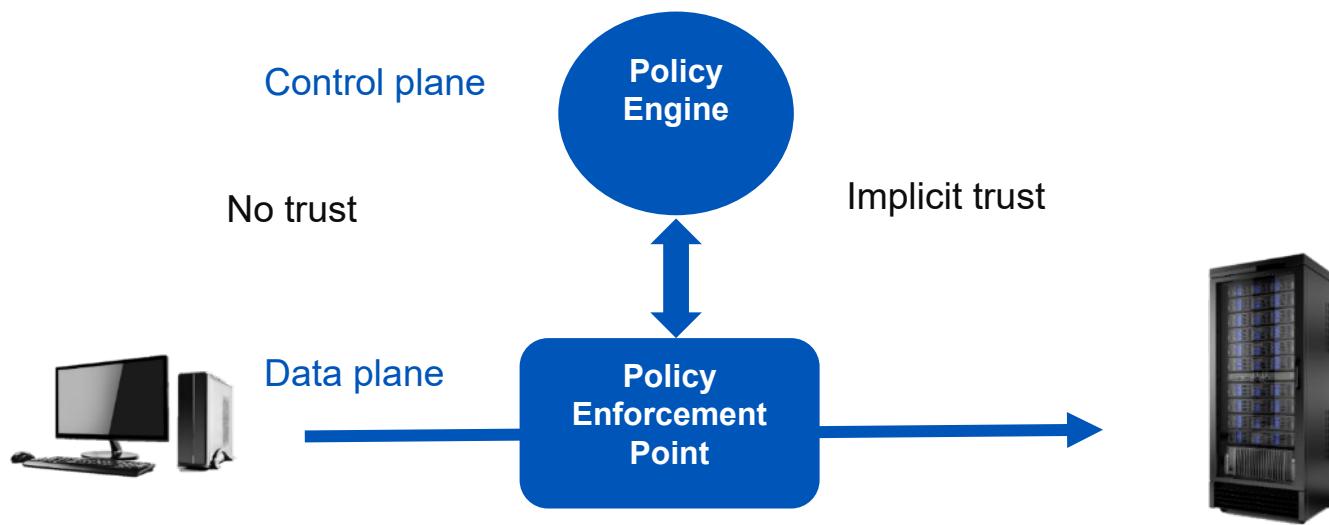
Zero Trust Network Access (ZTNA)

- ▶ **Zero Trust Network Access (ZTNA) is a security model that assumes no implicit trust within a network**
 - Instead, it verifies the identity of subjects (users, devices, and applications) before granting access to objects (resources)
 - Firewalls are largely based upon a source/destination paradigm
- ▶ **ZTNA is based on the principle of "never trust, always verify"**
 - Every user, device, and application must be authenticated and authorized before being granted access
 - Regardless of whether it is inside or outside the network perimeter.



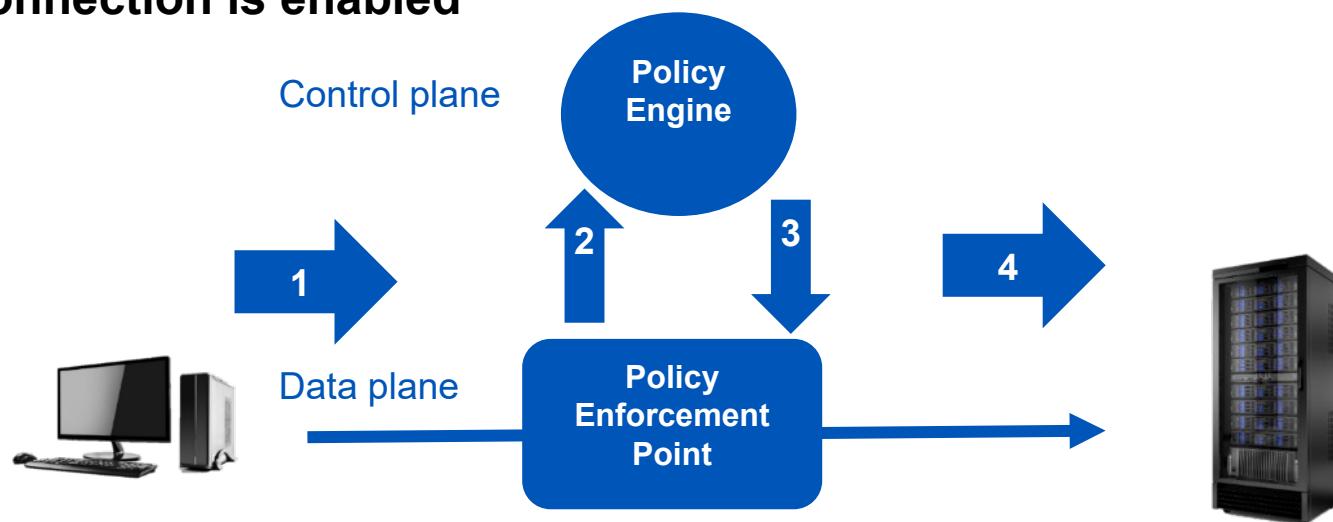
Planes

- ▶ **The Control plane defines and enforces security policies**
 - It includes adaptive identity management (who), threat scope reduction (are they healthy), the policy engine (access rules), policy-driven access control and administration
- ▶ **The ZTNA data plane is responsible for implementing the security policy**
 - It includes the policy enforcement point (PEP)
 - Firewalls and intrusion detection and prevention systems
 - Secure web gateways
 - Everything behind the PEP is implicitly trusted



ZTNA Example

- 1. A user or device attempts to access a resource**
 - The request is initially handled by a PEP
- 2. The control plane verifies the identity of the user or device and determines whether access should be granted and the level of authorization**
- 3. If access is granted, the control plane provides the data plane needed instructions**
 - E.g., issue a valid session ID
- 4. The connection is enabled**



Contents

- ▶ Fundamentals of Security
- ▶ Security Controls

Change Management

- ▶ Cryptography



Processes Impacting Security Operations



► Approval process

- Identify the change
- Assess risk
- Develop mitigation plan
- Review/approve
- Implement and monitor

► Ownership

- Has ultimate responsibility

► Stakeholders

- Must be consulted or be involved

Analysis

► Impact analysis

- Assessing the potential impacts of a proposed change on the organization
 - Benefits and risks

► Test results

- Where possible the results of testing should be reviewed
- Identify possible risk factors

► Gap analysis

- When regular patching or mitigation is unavailable, a risk gap exists
 - Legacy systems
- Gap analysis determines the extent and identifies potential work-arounds



Implementing Change

- ▶ **Backout plans**
 - Patches may be well-tested, but later prove to have side-effects
 - A methodology should be created to reverse changes
- ▶ **Maintenance windows**
 - Systems may have required hours of operation
 - Some mission critical systems may dictate extremely short down-time periods
- ▶ **Standard operating procedures**
 - Standard operating procedures (SOPs) are step-by-step instructions on how to perform a task or process in a desired, consistent and efficient manner



Technical Considerations

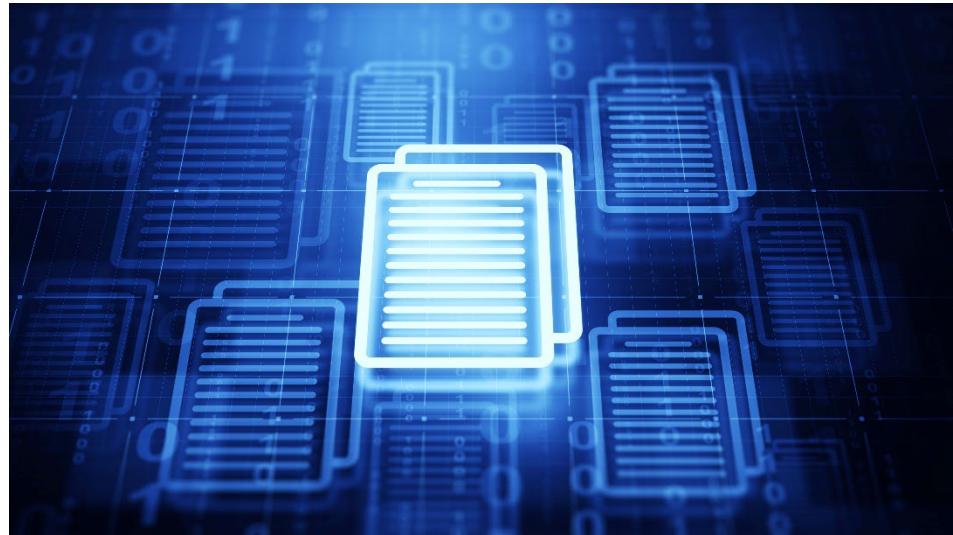
- ▶ **Allow lists/deny lists**
 - An allow list is a list of approved changes that can be implemented without going through the full change approval process
 - Deny lists are automatically disapproved
- ▶ **Restricted activities**
 - Changes that require special approval
 - Must check with stakeholders
- ▶ **Downtime / service restart / application restart**
- ▶ **Legacy applications**
 - May have special procedures, due to patch unavailability
 - End of Life—the product is no longer sold/produced
 - End of Service Life—no more support, patches or updates
- ▶ **Dependencies**
 - Changes may have a cascading effect

|| Changes →



Change Management Documentation

- ▶ In a mature organization, activities are systematic and documented
- ▶ Documentation
 - Updating diagrams
 - Updating policies/procedures
- ▶ Version control
 - May be manual or automated



Domain 1: Match the Items to the Topics

Do Now

Item	Answer	Topic
Always verify		A. Detective
Penetration test		B. Gap analysis
When patch no longer available		C. Management
Reporting suspicious behavior		D. Honeytoken
Performing an audit		E. Application restart
Protecting cables		F. Operational
Using a unique or secret phrase		G. STP
May delay patching		H. ZTNA

For each item on the left, write in the corresponding letter from a topic on the right

Contents

- ▶ Fundamentals of Security
- ▶ Security Controls
- ▶ Change Management

Cryptography



Algorithm Types

► Hashing

- A one-way function that converts data into a fixed-length output
- Provides the integrity security goal
- Not reversible
- Output is called a *message digest* and is typically 128, 160, or 256 bits long

► Encryption

- Primarily for obscuring data to achieve confidentiality
- Should employ seasoned and well-tested algorithms
- Reversible
- Symmetric: sender and receiver use the same key
 - Bulk encryption
- Asymmetric: also called *public key*—sender and receiver use different keys
 - Keys are generated as pairs—public and private
 - Often used to negotiate keys for symmetric encryption

Other Terms

- ▶ **Nonce**
 - A number that may only be used once
- ▶ **Random/Pseudorandom numbers**
 - Values created by a process that appears to be random
 - Keystroke/mouse movement, disk I/O, least significant bits in voltage measurements
- ▶ **Encoding is the simple conversion of data to another format, such as turning binary data into ASCII (ROT-13 or Base64)**
 - Does not involve a key and is called obfuscation (ROT-13 is security through obscurity)
- ▶ **Diffusion**
 - The principle that a change to the input will be reflected throughout the output, and not in the same locale
- ▶ **Confusion**
 - The principle that it should be difficult to understand or reverse

ROT-13 = rotate by 13 places

Diffusion and Confusion

Demo

Encode a file and observe changes

1. Open Cryptool
2. Select Encrypt/Decrypt | Symmetric (classic) | Caesar/ROT-13
3. Choose ROT-13 and then Encrypt
4. Return to the original opening document and edit the first word from ‘Starting’ to ‘Ending’
5. Perform the ROT-13 conversion again and compare the two outputs
6. Note that only the first word in the ciphertext has changed—it lacks diffusion
7. Neither is it hard to figure out—poor confusion
8. Later, when hashing is demonstrated, diffusion will be seen

Hashing

- ▶ A mathematical function that produces different results with each differing set of input data
- ▶ It is often necessary to ensure the integrity of information
 - Has a file been modified?
 - Does a downloaded file match the published hash value?
 - Check that a message has not changed in transit
 - The hash function is computed for data before and after transmission
 - The hash output results are compared to verify that the data has not changed



Hash Functions Are One-Way

- ▶ **Unlike encryption, hashing cannot be reversed**

- The output is called a message digest
- The data *cannot* be directly recovered from the digest
- A collision occurs when two different inputs hash to the same output
 - MD5 and SHA have documented problems with this
- Collision resistance is the ability to prevent two differing inputs from resulting in identical output



- ▶ **A hash function has these features**

- It is computationally difficult to discover the input from the digest
- The size of the hash is small with respect to the input data
 - The digest is always the same size
- A change in input must result in a significant change in the output value

Using Hashing

Hash a file using the SHA-1 algorithm and observe the results

- 1. Open a command prompt**
- 2. Type cd \secret, then press <Enter>**
- 3. Use a utility to calculate a hash for a file with:
`sha1sum myfile.txt` and press <Enter>**
- 4. Edit `myfile.txt`**
 - Edit it with this command: `notepad myfile.txt`, then press <Enter>
- 5. Change the file in any small way, save it and repeat the hashing from the previous steps**
- 6. Explore a collision by hashing these two different files with `md5sum.exe` and `sha1sum`**
 - `sha1sum *.ps` Note differing hashes
 - `md5sum *.ps` Note identical hashes—a collision

Hashes

- ▶ **SHA series: SHA-1 (deprecated), SHA-2, SHA-3, SHA-4, SHA-5**
- ▶ **MD hashes: Several algorithms (e.g., MD2, MD4, MD5, MD6)**
 - MD2-5 are deprecated
 - Output is 128 bits
- ▶ **RIPEMD (RACE Integrity Primitives Evaluation Message Digest)**
 - 160 bits; designed like MD4, and has similar performance to SHA-1



RACE = Research and Development in Advanced Communications Technologies in Europe

- ▶ **SHA-2 has up to 256/512-bit output**
 - Has replaced SHA-1
- ▶ **SHA-1 is the Secure Hash Algorithm 1**
 - A deprecated U.S. government standard
 - Generates a 160-bit hash result
- ▶ **SHA-2 is a family consists of six hash functions**
 - The digest lengths are
 - SHA-224
 - SHA-256
 - SHA-384
 - SHA-512
 - SHA-512/224
 - SHA-512/256

Hashed Message Authentication Code (HMAC)

- ▶ **If two parties each know a secret, they may**
 - Periodically hash it
 - Send it to the other party
- ▶ **If the receiver hashes their secret value, and it matches what was received, then it means the sender was authentic**
 - Achieves the authenticity and provides the message integrity
 - Exchanges a hash of the message and the secret key to verify the identity
 - Does an integrity check to verify a message has not changed
- ▶ **Used by SSL and TLS to defend against MITM attacks**
 - A MITM would not be able to replicate the hash
 - Does not know the secret

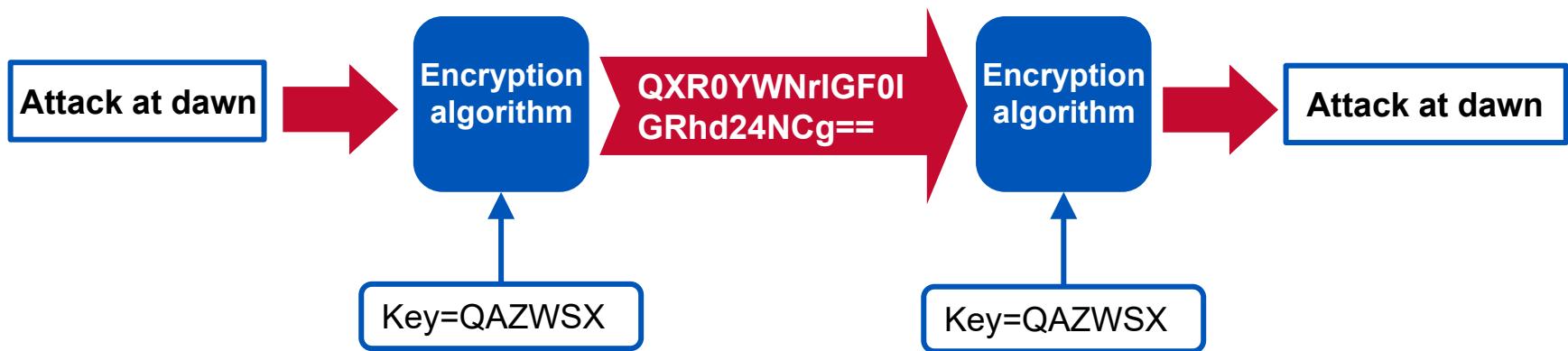
Encryption Overview

- ▶ **Encryption is a process designed to exchange confidential information**
 - Obscures information so that it cannot be understood by a third party
- ▶ **Information entering the encryption algorithm is known as *cleartext* or *plaintext***
- ▶ **Cleartext is encrypted into ciphertext**
 - Decryption reverses the process
- ▶ **There are two families of encryption**
 - Symmetric
 - Asymmetric



Symmetric Key Cryptography

- ▶ Symmetric cryptography is a system in which the *same key* is used for both encryption and decryption
- ▶ Symmetric key cryptography algorithms are designed to be fast and efficient
 - Ideally suited to encrypting large amounts of bulk data
 - Hard drives, data streams



Other Ciphers

- ▶ **One-Time Pad (OTP): a message is encrypted using a special key**
 - Key is equal to the message length and may be used once and is essentially unbreakable
 - Both sender and receiver must possess the key
- ▶ **Homomorphic encryption**
 - A cryptographic technique that allows computations and analysis to be performed on encrypted data without the need to decrypt it first
 - E.g., determining if a password has required complexity
- ▶ **Blockchain**
 - A series of linked and hashed transactions
 - Currency transfers recorded in a public ledger
 - Can provide nonrepudiation for anonymized transactions
 - Blockchains are commonly used to record crypto currency transactions
 - Bitcoin uses a blockchain system

Symmetric Algorithms: AES

- ▶ **The Advanced Encryption Standard is designed as a replacement for DES**
 - U.S. government standard (FIPS-197)
- ▶ **Uses the Rijndael algorithm**
 - Designed by Joan Daemen and Vincent Rijmen
- ▶ **Key and block lengths are multiples of 32 bits**
 - Usually 128-bit, 192-bit, or 256-bit key and block length
 - Any combination of block and key lengths is acceptable
 - A block cipher
- ▶ **Stream ciphers are ideal for streaming audio and video**
 - AES in CTR mode is a stream cipher
 - GCM has high performance characteristics

Enhancing Cryptographic Keys

► Key stretching and salting

- A technique used to make a possibly weak key (like a common word or passphrase) more resistant to a brute-force attack
- Salting improves resistance to rainbow tables
 - By increasing the time it takes to test each possible key combination
- The first key is processed by an algorithm that creates an enhanced key
 - The length of this second key should be beyond practical brute-force cracking methods
 - Password-Based Key Derivation Function 2 (PBKDF2)
 - Bcrypt

► Cryptographic system resilience

- Systems that stay secure even if characteristics of the secret key is leaked
- Leaked via memory side-channel attack or social engineering (e.g., learning about a key when intelligence informs you they never use vowels in a key)

Symmetric Encryption

Demo

- 1. Run CrypTool from the desktop**
 - There is a message open by default that can be encrypted
- 2. Select Crypt | Symmetric (Modern) | IDEA**
- 3. Enter a very simple key: 01**
- 4. Select Encrypt**
 - The resulting message has been encrypted
- 5. Select Crypt | Symmetric (Modern) | IDEA**
- 6. Enter the same simple key: 01**
- 7. Select Decrypt**
 - The resulting message has now been decrypted

Disk, Device, and File Encryption

- ▶ **Device and whole-disk encryption should be applied to any device that has an excessive risk of physical theft**
 - Especially laptops
 - BitLocker is a popular whole disk encryption product
 - Requires a TPM
- ▶ **Database fields should encrypt data-sensitive information**
 - Applications accessing the encrypted fields must have the key to reveal the data
 - Hashed passwords are more secure than encryption
- ▶ **Cell phones with storage and email access**
 - Protect with encryption of data



Hardware-Based Encryption Devices

► **Hardware Security Modules (HSMs)**

- Can generate and store keys
- Creates a hardware Root of Trust
- Often used with payment gateways and certificate authorities
 - Largely associated with automated use of private keys

► **Level or type**

- Selective file/folder encryption—Microsoft EFS
 - Selectee files and folders
- Volume encryption—VeraCrypt
 - A portion of a disk is set aside for encryption
- Full-disk encryption (FDE)—BitLocker
- Full database encryption—entire database
- Record encryption in a database
 - Specific record columns



Hardware Roots of Trust (RoT)

- ▶ A set of core functions in trusted computing that can always be trusted by the operating system
- ▶ Secure enclave
 - Designed to protect this data from unauthorized access, even if the rest of the system is compromised
 - Integrated into the processor
- ▶ TPMs are a similar implementation in PCs
 - Dedicated hardware security chips that provide a platform-wide root of trust
 - Needed for FDE
- ▶ A secure system will also have
 - Trusted supply chain
 - Trust that components upstream delivered to an organization have integrity



Symmetric Modes of Operation

- ▶ A mode of operation is an explicit method by which you use a block cipher (DES, AES, Blowfish) to do more than encrypt a single data block (e.g., a fixed 128-bit block of text)
- ▶ ECB and CBC allows encryption of multiple blocks of data in one cycle
 - ECB should not be used if encrypting more than one block of data with the same key
- ▶ CTR is used if parallel processing and/or speed are desired
 - A form of stream cipher
- ▶ GCM can perform *authentication* and *encryption*
- ▶ XTS is method applicable to encrypting disc storage
 - Optimized to securely encrypt disk sectors

ECB = Electronic Code Book
GCM = Galois/Counter Mode
CTR = Counter

CBC = Cipher Block Chaining
XTS = XEX Tweakable Block Cipher with Ciphertext Stealing

Encryption Strength

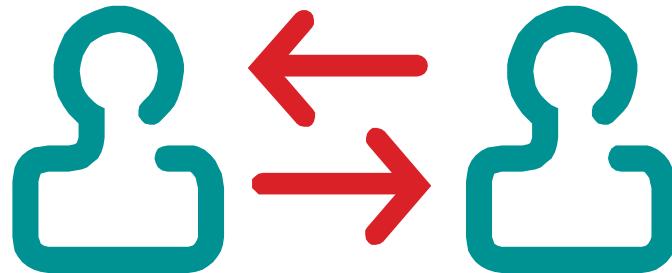
- ▶ **The safety of cryptography rests in the key**
- ▶ **The key length is expressed as a power of 2**
 - DES is 56 bits $2^{56} = 72,057,594,037,927,936$
 - Triple DES (3DES) is typically 112 bits
 - $5.1 * 1,000,000,000,000,000,000,000,000,000,000$
 - AES will not fit on the page ($1.1 * 10^{77}$)
 - As computing power progresses, the safe key length rises
- ▶ **In earlier years, the complexity of the algorithm was most important**
 - The German Enigma machine
 - Captured May 9, 1941
 - Allowed Allies to read German Naval traffic



Issues With Symmetric Encryption Systems

► **The most difficult parts of symmetric key encryption are**

- Distributing the key to all parties
 - It must be communicated in secret



- Managing the keys
 - Repeated use of a key makes it vulnerable to analysis techniques

Asymmetric Encryption

- ▶ Asymmetric encryption is also known as public key encryption
- ▶ One technique to handle the symmetric key distribution issue is to use asymmetric encryption to negotiate the later use of symmetric encryption
 - Can serve security goals other than just confidentiality
- ▶ Asymmetric encryption involves two different keys, generated as a pair
 - Public: Anyone may possess it
 - Private: It must be guarded; only the owner may possess it



Asymmetric Encryption Algorithms

- ▶ **The two keys are generated as a pair using an algorithm**
 - First the private key, then the public key (a mistaken idea from CompTIA)
- ▶ **Data encrypted with the one key can be decrypted *only* with the other key**
 - For example, data encrypted with the private key can be decrypted only with the corresponding public key
 - The key chosen for encryption depends on the security goal
- ▶ **A party's public key must be possessed by other parties who want to send confidential messages**
 - Decryption can only be performed by the private key holder
 - The private key must remain secret



Creating Asymmetric Keys

Demo

1. Open a command prompt
2. Run gpg --gen-key and press <Enter>

Prompt

Please select what kind of key do you want:

What keysize do you want? (2048)

Key is valid for? (0)

Is this correct? (Y/N)

Real name:

Email address:

Comment:

Change

Enter passphrase:

Repeat passphrase:

Response

1

2048

0

y

instructor

instructor@ltree.com

my identity

0 (for okay)

adminpw123

adminpw123

3. Run gpg --list-keys <Enter> to see the public keys held
4. Run gpg --list-secret-keys <Enter> to view secret keys

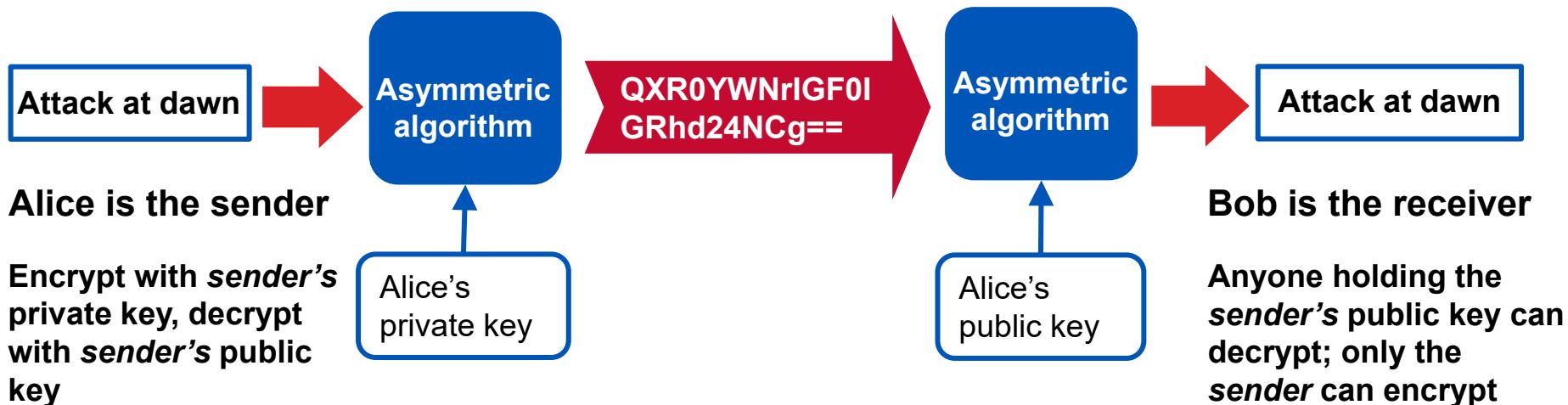
Using Asymmetric Cryptography for Confidentiality

- If Alice wants to send a confidential message to Bob, she encrypts it with *Bob's public key*
 - Then it can be decrypted only with *Bob's private key*
 - This provides confidentiality



Using Asymmetric Cryptography for Authentication

- ▶ If Alice wants to send a message to Bob such that he can verify that Alice sent it, she encrypts it with *Alice's private key*
 - Anyone with *Alice's public key* can decrypt the message
- ▶ In a PKI, the owner of the private key and the private key are assumed to be one; they are bound together
 - The private key is used by smart cards and CACs for authentication
 - This is the process used by a digital signature



Examples of Encryption Key Exchange Methods

- ▶ **Typically used to negotiate later symmetric encryption**
 - Used for securely negotiating authentication and later symmetric encryption
- ▶ **Out Of Band (OOB)**
 - Used with a separate method to exchange keys (e.g., using SMS messages or a phone call to distribute keys)
- ▶ **Rivest, Shamir, and Adleman (RSA)**
 - Based on the difficulty in discovering large factored prime numbers
 - Used by SSL and TLS
 - Used with a specified key length (minimum 512 bits)
- ▶ **Digital Signature Algorithm (DSA)**
 - U.S. standard—can only encrypt using the private key
- ▶ **Diffie-Hellman (D-H)**
 - A key exchange algorithm based upon modulus math
 - Used with SSH

SMS = Short Message Service

Other Asymmetric or Key Exchange Methods

- ▶ **Perfect forward secrecy (PFS)**
 - An aspect of key-agreement protocols that ensures that a session key created by a set of long-term keys cannot be discovered even if the long-term key is learned in the future
 - A key breach today cannot be used to reveal future or past encrypted data
- ▶ **DHE**
 - An implementation of DH that provides an ephemeral key
- ▶ **Elliptic Curve Cryptography (ECC)**
 - Based on the math used to represent elliptical curves and is more CPU-efficient than RSA—smaller keys, but same security as RSA
 - Often seen in use with embedded devices
- ▶ **ECDHE**
 - A key agreement protocol that allows two parties each with an elliptic curve public-private key pair to share an ephemeral secret or a symmetric key

DHE = Diffie-Hellman Ephemeral

RSA Asymmetric Encryption

- ▶ **RSA is the first public key algorithm to encrypt using either the public or the private key**
 - The most popular asymmetric encryption algorithm
 - Encrypts with either the public or private key
- ▶ **RSA can use keys of varying lengths**
 - Keys are 512 bits or longer
 - Shorter keys make encryption faster
 - Longer keys are more secure
- ▶ **Public key encryption is slow when compared with symmetric key algorithms**
 - Rather than using it for encrypting the entire message, it is often used to encrypt a symmetric key that is regularly and automatically changed
 - That key is called a *session key* or *ephemeral key*
 - Used for encrypting the body of the message

Email Encryption

► Relatively easy to use cryptosystems

- Pretty Good Privacy (PGP) was developed by Phil Zimmermann to be a widely deployed cryptosystem
 - Although PGP involves the use of secret and public key encryption, CompTIA Security+ identifies only the public key aspect
 - Initially designed for encryption of email messages
- GNU Privacy Guard (GPG or GnuPG)
 - Similar operation and free
 - Compatible with PGP
 - www.gnupg.org

► Corporate email format

- Secure Multipurpose Internet Mail Extensions (S/MIME)
 - Originally created by RSA Security
 - Supported by most email clients
- Encrypts the message, not the headers
 - SMTP sends data as cleartext

Encryption Summary

► Symmetric ciphers

- Encrypt the *data* with low latency
- Do not handle key exchange
- Are fast
- AES, Blowfish, DES, 3DES

► Asymmetric ciphers

- Protect the *key exchange*
- Easy key management
- Are slow
- RSA, ECC, DH

► Hashes

- Handle integrity checking
- Are one-way
- Create a message digest
- MD series, SHA series

Deprecated Algorithms

- ▶ **These algorithms have been labeled as deprecated**
 - Not safe for use
- ▶ **Hashes**
 - SHA-1—superseded by SHA-256 or SHA-512
 - MD2, MD4, and MD5
- ▶ **Asymmetric encryption**
 - 1024-bit RSA or DSA—too low bit length—weak keys
 - 160-bit ECDSA—too low bit length—weak keys
- ▶ **Symmetric encryption**
 - DES and 3DES—superseded by AES
 - RC4—a lack of randomness

Asymmetric Encryption

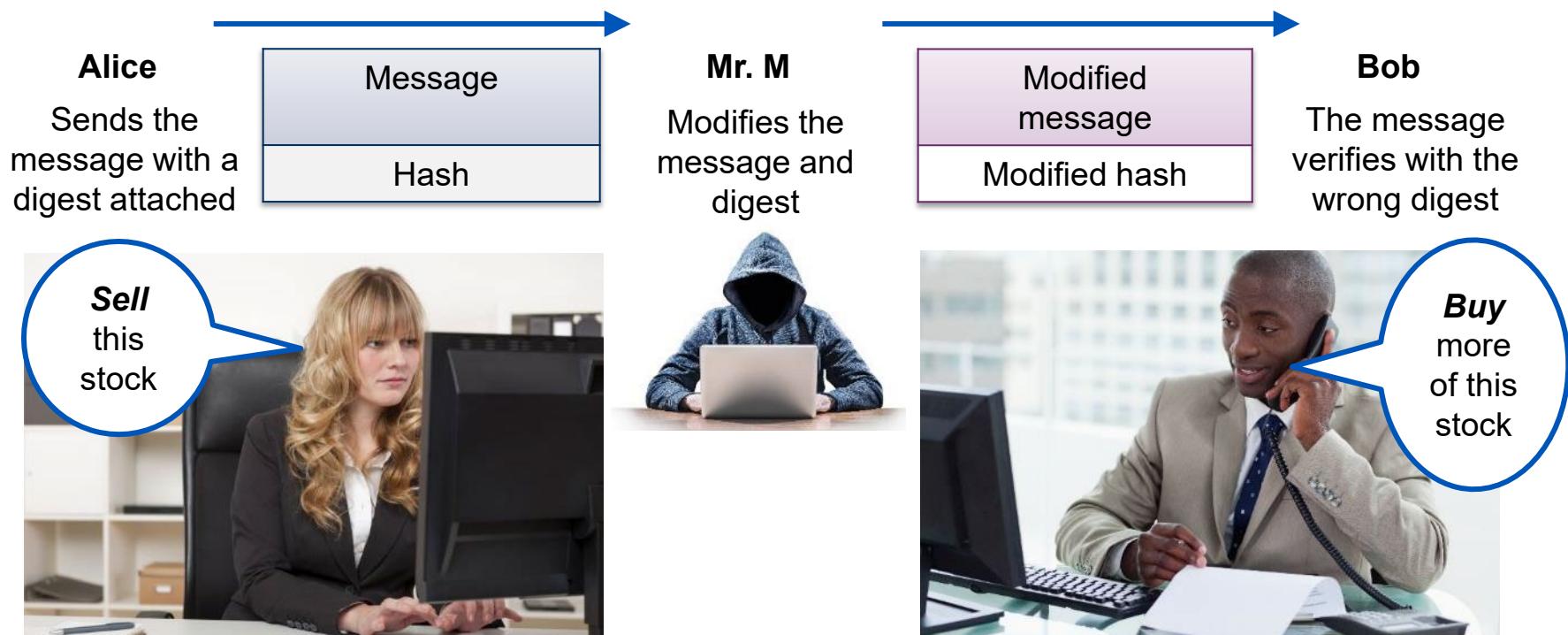
Demo

1. Open a command prompt and enter cd \secret, then press <Enter>
2. Display a cleartext file: type secret.txt, then press <Enter>
3. Encrypt a message:
gpg -e -r instructor secret.txt, then press <Enter>
4. Run type secret.txt.gpg, then press <Enter>
 - This is the encrypted message
5. Decrypt a message gpg -d secret.txt.gpg, then press <Enter>
6. Enter the passphrase for instructor: adminpw123

Failing to Protect a Message in Motion

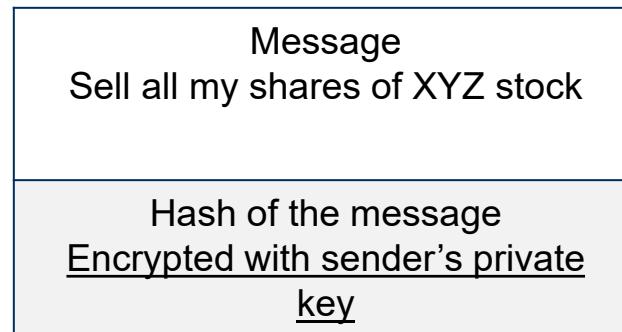
► Alice sends a message to Bob

- Alice adds a hash to the message so that Bob can check it; a man-in-the-middle (Mr. M) modifies the message and creates a new digest
- Bob verifies modified message with the fraudulent digest
- *The problem is that the message digest could be modified*



Creating the Digital Signature

- ▶ If Alice had encrypted the hash with *her private key*, Bob could have verified that Alice (or someone with her key) had hashed the message
 - Mr. M could not have modified the hash
 - He could read it with Alice's public key
 - He could not re-encrypt it because *he does not have Alice's private key*
- ▶ The encrypted hash Alice created is known as a *digital signature*
 - Encrypted with a private key; decrypted with a public key
- ▶ Digital signatures may also be used to sign code, such as ActiveX
 - Called Authenticode by Microsoft



This is able to verify the message and its origin

Digital Signatures

1. Open a command prompt, cd \secret, then press <Enter>
2. Display a cleartext file: type signature.txt, then press <Enter>
3. Digitally sign the file:
gpg --clearsign signature.txt, then press <Enter>
4. Run type signature.txt.asc, then press <Enter>
 - This is the signed version of the message
5. Why can the content be read?
6. Edit the file and change any character in the message:
notepad signature.txt.asc, then press <Enter>
7. Save the file and exit Notepad
8. Verify the file integrity:
gpg --verify signature.txt.asc, then press <Enter>
9. Note the result

Public Key Infrastructure

- ▶ **Public and private keys**
 - Commonly used for authentication, as well as confidentiality
 - Private keys are always kept secret
 - Managing public keys poses certain challenges
 - In what form is a public key sent or processed?
 - What happens if a private key is stolen?
 - How are those who possess copies of the public key notified?
 - Should a key be used forever?
 - Over time, is there a growing chance that the key would be compromised?
 - How can a recipient be sure that a public key belongs to a particular party?
 - What manages all of this?
- ▶ **The answers are**
 - PKI
 - X.509 certificates
 - Certificate authorities

X.509v3 Certificates

- ▶ **Electronic documents that contain standardized information**
- ▶ **Should be obtained from a commercial CA, if applications are public-facing**
- ▶ **They contain**
 - Key owner's name (called subject)
 - Name of the private key owner (e.g., the website name or person to whom the certificate was issued)
 - Subject's public key
 - Issuer name and digital signature
 - Thumbprint—a hash of the public key
 - Serial number assigned by the issuer
 - Dates
 - Issuance
 - Inception
 - Expiration (may be set to never expire)
 - Version (currently 3)
 - Enhancements allow for creation of custom attributes

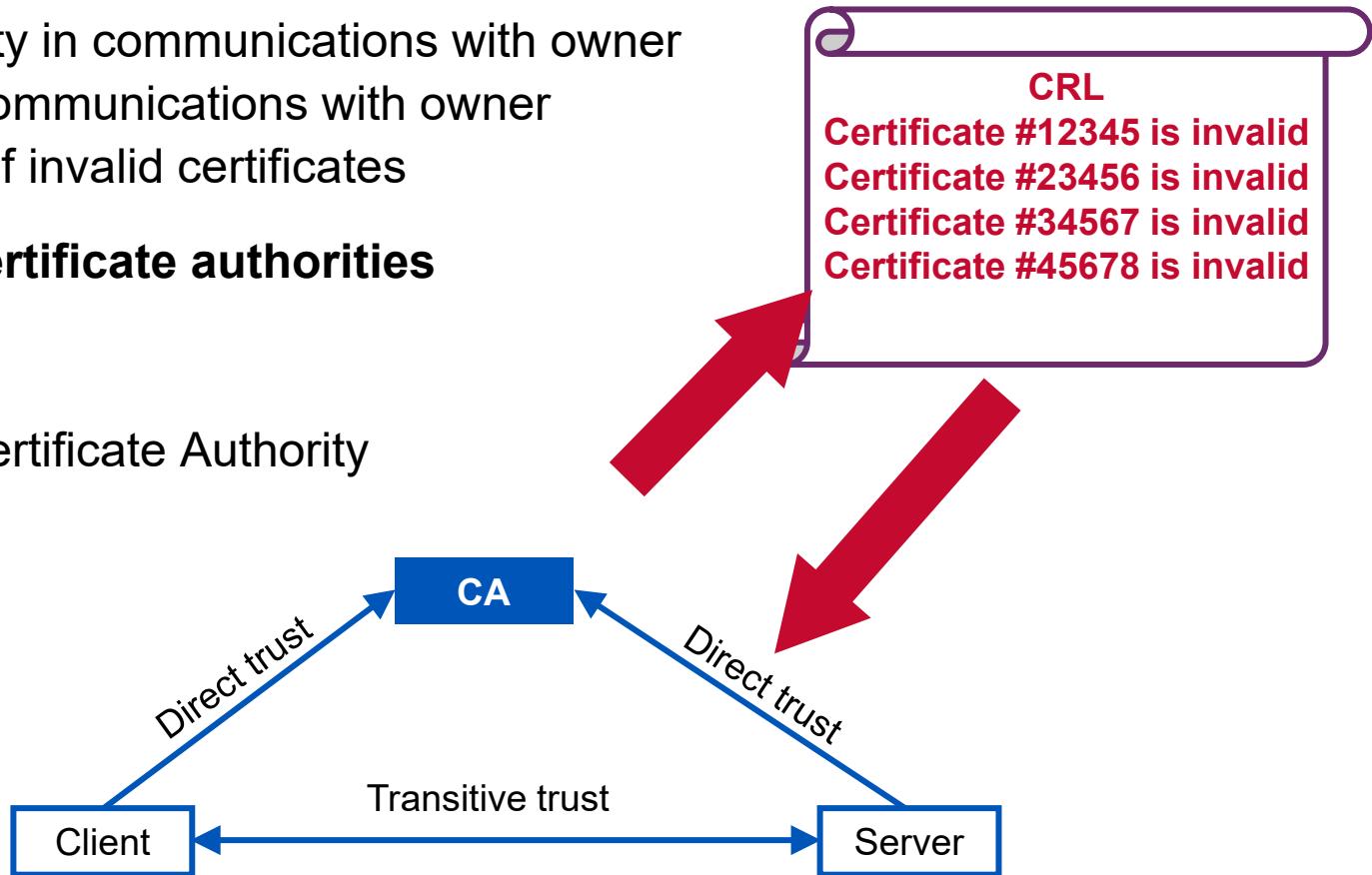
Creating/Renewing an X.509 Certificate

- 1. Owner authenticates with a registration authority**
- 2. Owner generates a public and private key pair**
- 3. Owner sends CSR and public key to a certificate authority**
 - Owner proves identity to the Certificate Authority (CA) per CA requirements
 - Certificate Practices Statement
- 4. CA software creates a certificate with these attributes**
 - A. Digitally signed owner's public key with CA's private key
 - B. Serial number for use in Certificate Revocation List (CRL)
 - C. Data about the subject (owner of the public key)
 - D. Dates (inception, expiration, etc.)
 - E. Other fields
- 5. Returns completed X.509 certificate to original sender**
- 6. To be used, the new certificate must first be published to a global access list**

CSR = certificate-signing request

Public Key Infrastructure (PKI)

- ▶ PKI is the ability to manage and verify public key ownership and validity
- ▶ Assurance of ownership of a public key allows
 - Authentication of owner
 - Confidentiality in communications with owner
 - Integrity in communications with owner
 - Publication of invalid certificates
- ▶ Examples of certificate authorities
 - Entrust
 - Godaddy
 - DoD Root Certificate Authority



Viewing Browser CA Certificates

Demo

1. Open Firefox
2. Select <Alt> Tools | Options | Advanced
3. Go to the Certificates tab
4. Click View Certificates
5. Go to the Authorities tab
6. These are organizations that commercially distribute certificates
7. These certificates and their public keys are used to validate any certificate opened by your browser
 - Issuers publish their public key as a trusted root CA

Certificate Types

- ▶ **Certificate Authority (CA)**—for issuing certificates
- ▶ **Server**—HTTP and other servers
- ▶ **Personal**—people, CAC, and PIV
- ▶ **Code signing**—code integrity and authentication (e.g., Authenticode)
- ▶ **Email and Digital Signing**
- ▶ **Wildcard**—allows unlimited sub-domains under a domain and easier management
 - ftp.learningtree.com
 - www.learningtree.com
 - www2.learningtree.com
 - Servers may be added with no change in certificates
- ▶ **Subject Alternative Name (SAN)**—Useful for multiple names in differing domains such as **www.learningtree.com** and **www.learningtree.net**
 - Only the names specifically added to the certificate are covered

Certificate Formats

- ▶ **Distinguished Encoding Rules (DER)**
 - Typically saved with .cer and .crt extensions, binary encoding
- ▶ **Privacy Enhanced Email (PEM)**
 - Base64 ASCII and saved with .pem extensions
 - Most commonly used by CAs
- ▶ **CER and CRT**
 - .cer extension—common to Microsoft
 - .crt extension—common with Linux
- ▶ **PFX**
 - Replaced by PKCS #12—common to Windows
 - Only used if sharing a private key, too
- ▶ **P12 (PKCS #12)**
 - Used to share public and private keys
 - Uses .p12 extensions—common to Windows
- ▶ **P7B: Uses Base64 encoding and .p7b extension**

Certificate Authorities

- ▶ **The issuer of certificates is usually a third-party, called a certificate authority (CA)**
 - Entrust, Thawte, DoD Root certificate authority
 - CAs are often arranged in a hierarchical tree-structured manner
- ▶ **Certificates issues**
 - Certificates from a CA must be present in a browser or OS or else they will generate an error indicating a certificate cannot be trusted
 - Self-signed certificates may cause this as well
 - Name mismatch errors are indicative of a man-in-the-middle attack or of going to a site by IP address alone, not DNS
- ▶ **Keys for terminated employees and lost/stolen key pairs are published in a certificate revocation list (CRL) that is always available**
 - Clients may check CRLs with Online Certificate Status Protocol (OCSP)
 - CRLs indicate: Good, Unknown, or Revoked status

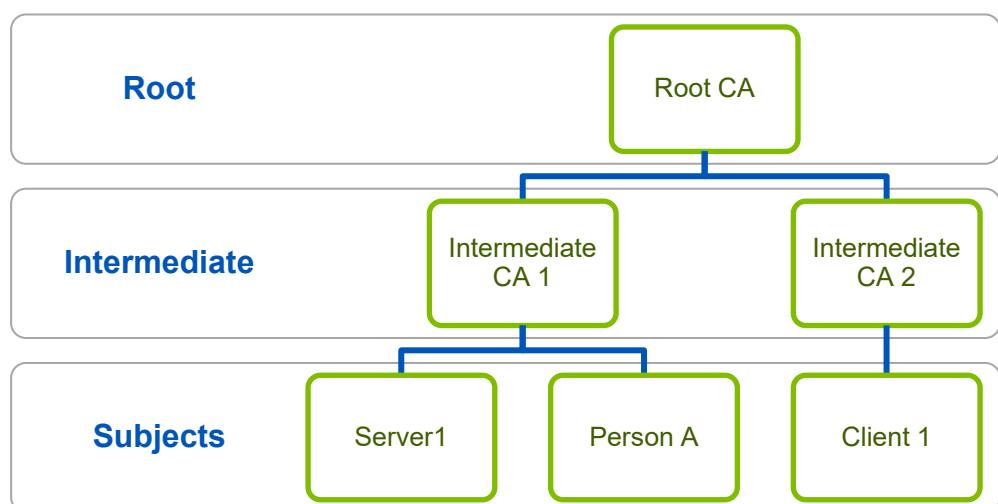


This Connection is Untrusted

You have asked Firefox to connect securely to **159.53.74.11**,
is secure.

Other Certificate Concepts

- ▶ **Certificate stapling**
 - Also called TLS Certificate Status Request
 - Allows the origin of a certificate to handle the resource cost in OCSP responses by “stapling” a time-stamped CA-signed OCSP response

 - ▶ **Certificate chaining**
 - Establishing and linking trust from the bottom to the top
 - Subordinate certificates are issued and signed by the superior
 - Inferior subjects are identified by public keys of superiors
- 

Key Escrow

- ▶ **Used to ensure encrypted data may always be recovered**
 - Otherwise, old, encrypted data is not recoverable
- ▶ **Recovery agents (RAs) may keep a backup copy of private keys by a trusted third party and recover them if a private key is lost**
 - Not used for stolen private keys



Active private key
held by owner



Copy of private key held by certificate
authority and recovery agent

Steganography Tools

► Steganography

- Hiding a program or message inside an image
- Uses encoding such as manipulating the least significant bits
- Results in some image degradation

► Types of Steganography

- White on white text
- Cover image
- Whitespace encoding
- Micro dots
- Audio
- Video



1
2
3
4
5
6
7
8
9

Hidden Communication

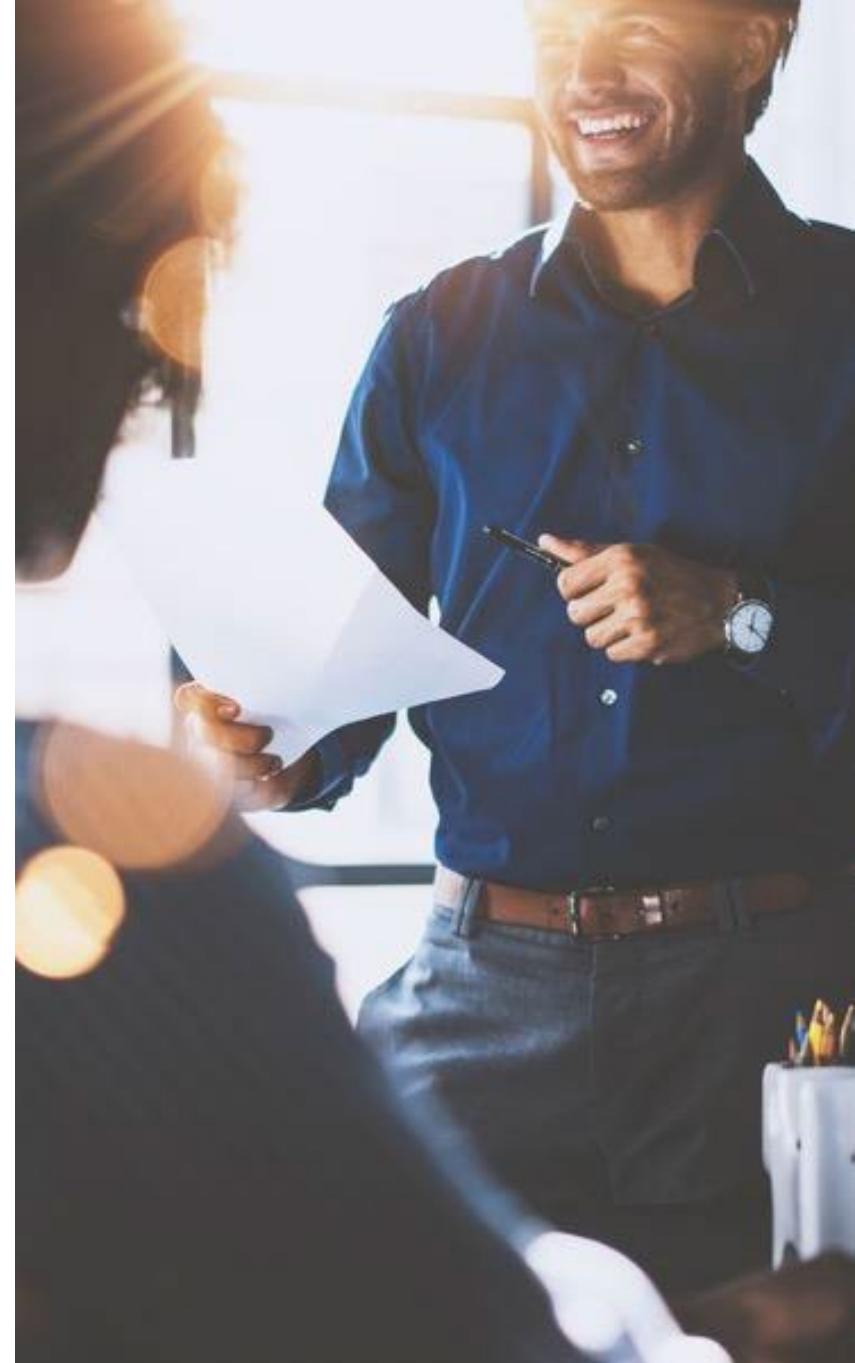
Demo

- **Information may be hidden**
 - Steganography is hiding a message, image, or file within another message, image, or file
1. **Launch SilentEye from the desktop**
 2. **Choose File | Open | c:\secret\ltree.bmp**
 3. **Select Encode**
 - a. Change the media encoding format to BMP
 - b. Ensure c:\secret\stego\ is the output directory
 - c. Enter: **attack at dawn** as the message; then press **Encode**
 4. **Choose File | Close current; then, File Open | c:\secret\stego\ltree.bmp**
 5. **Press Decode**
 6. **Select BMP as the Media encoding format and then Decode to view the secret message**
 7. **Close SilentEye**

Objectives

- ▶ **Identifying security fundamentals**
- ▶ **Comparing and contrast security controls**
- ▶ **Understanding the importance of change management**
- ▶ **Applying secure cryptographic principles**

12%





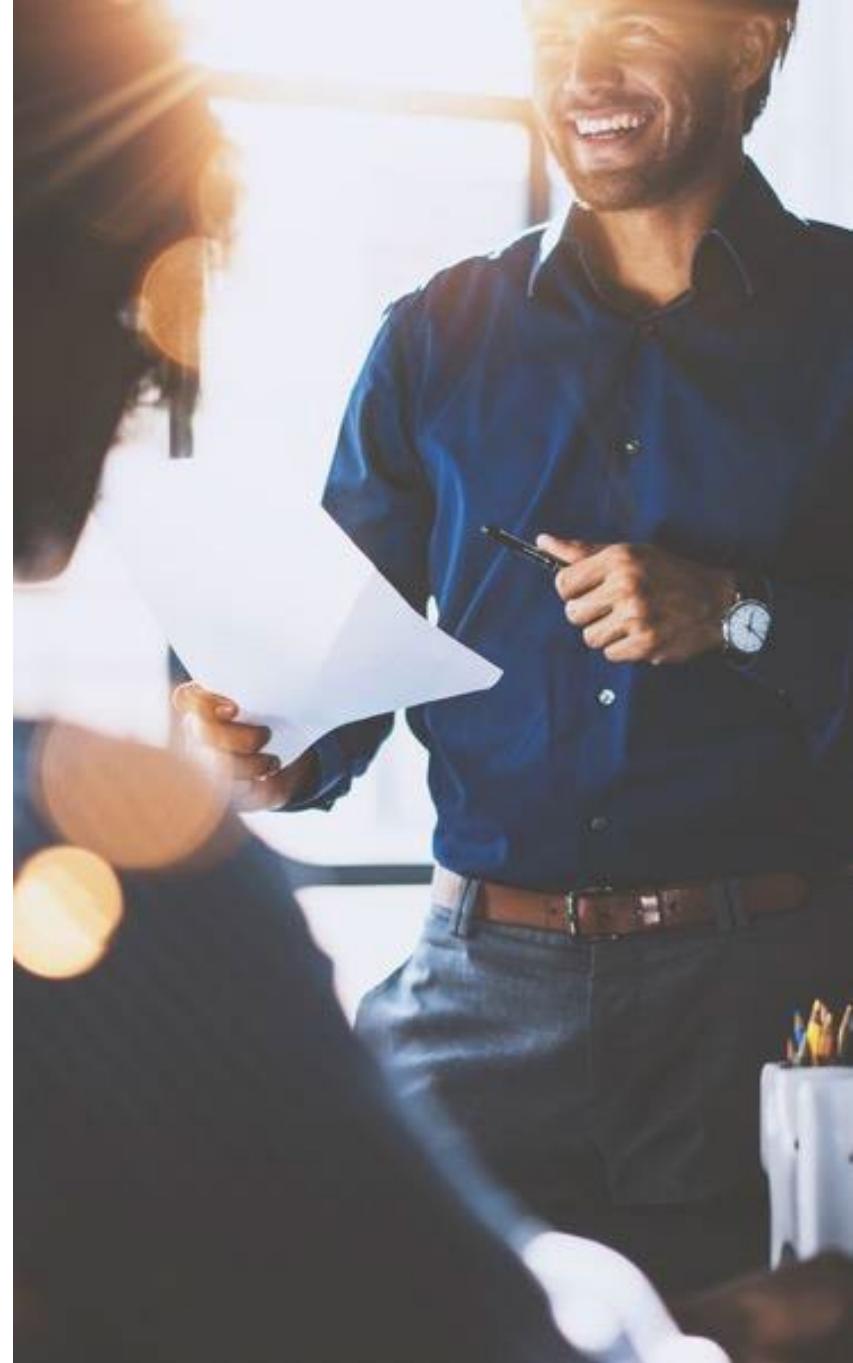
Chapter 3

Domain 5: Security Program Management and Oversight

Objectives

- ▶ Identify effective governance
- ▶ Analyze compliance measures
- ▶ Understand risk management
- ▶ Explain third-party risk management
- ▶ Examine audits and assessments
- ▶ Implement security awareness

20%



Contents

Effective Governance

- ▶ Risk Management
- ▶ Compliance Measures
- ▶ Third-Party Risk
- ▶ Audits and Assessments
- ▶ Security Awareness



Governance Bodies

- ▶ **Governance is the process of setting rules, policies, and procedures to ensure that an organization is managed effectively and efficiently**
- ▶ **Governance may be internal**
 - Boards
 - Committees
- ▶ **As well, it may be external**
 - Regulatory agencies
 - Legal
 - Industry, such as PCI DSS
 - Local/regional
 - National and international
- ▶ **Adhering to rules and policies is a large component of information security**



Data Roles and Responsibilities

- ▶ **Data custodians are responsible for**
 - Backup, recovery, availability, and physical security
- ▶ **Data owners/stewards handle**
 - Accuracy, integrity, accountable for legal requirements and classification
 - Logical access controls
- ▶ **Data processor**
 - Processing systems, servers
- ▶ **Data controller**
 - Determines the purposes for which data may be processed
- ▶ **Data protection officer**
 - Reports to senior management
 - Compliance for policies, regulations, and laws



Policies, Standards, and Procedures

► Policies

- Policies are higher-level goals and provide direction
- They are seldom very specific in nature as to how they are achieved
 - The organization wants systems to be used in-line with organization purposes

► Standards

- These are ways of achieving a policy goal
- It does not endorse a specific solution, but may focus on a technology
 - URL-blocking and auditing software will be implemented

► Procedures

- These are detailed and related to a specific solution or product
 - Software from XYZ will be installed/configured as shown below ...

► Guidelines

- Generally recommended, but not required
 - Check NIST SP 800-83 for useful information about blocking ransomware

Key Security-Related Policies

- ▶ **Acceptable use policy (AUP)**
- ▶ **Information security policies**
- ▶ **Business continuity**
- ▶ **Disaster recovery**
- ▶ **Incident response**
- ▶ **Software development lifecycle (SDLC)**
- ▶ **Change management**



Acceptable Use, Social Media, and Rules of Behavior

► Acceptable use policy

- Users must be told what they should and should not do
 - Enforce with education and content/URL filtering

► Social media analysis

- Reviewing employee behavior on social media platforms
- May require employee consent and *liking*

► Rules of behavior

- Including a social media policy
- Preventing information leaks
- Disparaging discussions



URL = uniform resource locator

Business Continuity vs. Disaster Recovery

► Business continuity

- Longer term: Three to four days and onward
- The focus is on the ongoing operation of the business
- Continuity of operations testing (e.g., powering off a key server to verify how well the alternates can take over the role)
 - Succession planning: Identifying the assets to take over a key function

► Disaster recovery

- Safety of personnel is the foremost concern
- The continuous and immediate functioning of the business is key
- Focus on immediate recovery/restoration of operations



Incident Response

- ▶ An incident response plan should document
 - Team members and assignments
 - Escalation requirements
 - Types and definitions of incidents
 - Reporting requirements
 - The seriousness and scope
 - Incident response teams
 - Tabletop exercises, walk throughs and simulations
- ▶ NIST SP 800-61*
 - Prepare Create policy and implement detection systems
 - Detect and analyze Sensors generate an alert
 - Contain Device removal or isolation, application shutdown
 - Eradicate Cleanup, repair, or replacement
 - Recover Restoring functionality
 - Lesson learned Forensics and revise policies



*<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

Information Security Policies

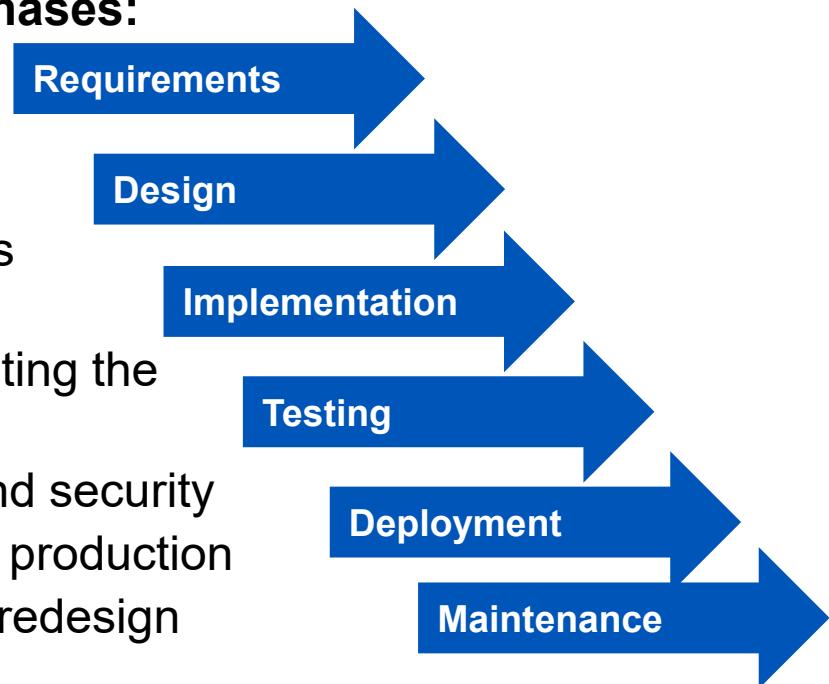
- ▶ **Information security policies should be tailored to the specific needs of the organization**
- ▶ **Common elements of information security policies include:**
 - Asset classification
 - This involves identifying and classifying the organization's information assets based on their sensitivity and importance
 - Access control
 - Defining who is authorized to access each information asset and what they are allowed to do with it
 - Data protection
 - Implementing security measures to protect information assets from unauthorized access, use, disclosure, modification, or destruction
 - Incident response
 - Defining a plan for responding to security incidents, such as data breaches and malware infections

Software Development Lifecycle (SDLC)

- The Secure Software Development Lifecycle (SDLC) is a process that integrates security into all phases of the software development lifecycle

- The SDLC consists of the following phases:

- **Requirements gathering:** Identifying customer requirements for the software, including security
- **Design:** Planning the software and its elements, including security
- **Implementation:** Securely implementing the software components
- **Testing:** Verifying the functionality and security
- **Deployment:** Moving the software to production
- Maintenance: Ongoing software and redesign



Change Management

- ▶ **Change management applies to many aspects of an organization**
 - Development
 - Cabling
 - System maintenance
- ▶ **Change management is the process of planning, implementing, and sustaining changes**
 - Changes to an organization's systems and processes can both fix and introduce security risks
- ▶ **Best practices for change management**
 - Involve the security team to identify and assess security risks associated with changes
 - The change management process should include security considerations
 - Communicate throughout the change processes

Pop Quiz: Change Management Policies



- 1. Arthur is a programmer and has discovered a serious flaw in the main web application for his company. He is the team leader in charge of the code. If exploited, this could cost the company 6,000 USD per incident, with a likelihood of 10 such problems per year. What is his best course of action?**
 - a) Discreetly repair the code and alert the change review board
 - b) Alert the change review board and then make the change
 - c) Report the issue and best recommendations to the change review board and wait
 - d) Task one of his team members with the issue and delegate it

Standards

- The following are common security standards for an organization

- Password
- Access control
- Physical security
- Encryption



Password Strength

- ▶ **Length**
 - A longer password means more guessing would have to be done to exhaust all possibilities
- ▶ **Complexity—password crackers have a tougher time with higher combinations**
 - qwertyasdf is weaker than abcde1234 is weaker than asdf321#@
- ▶ **Not using known words**
 - A cracking technique called a *dictionary attack* can quickly reveal hashed or encrypted passwords (weak passwords: flower and f10w3r)
- ▶ **Reuse/history**
 - Limiting the ability to change a password back to a previous value
 - One-time passwords (OTPs) involve passwords that may be used only once
- ▶ **Age**
 - Minimum age prevents users from changing back to an old password



Characteristics of a Good Secret

- 1. Go to this site to determine how long it would take to crack using brute force:
<http://lastbit.com/pswcalc.asp>**

- 2. Use these parameters:**
 - Password length 10
 - Keys/second 1000
 - Number of computers 1
 - Characters are: upper, lower, digits, common punctuation

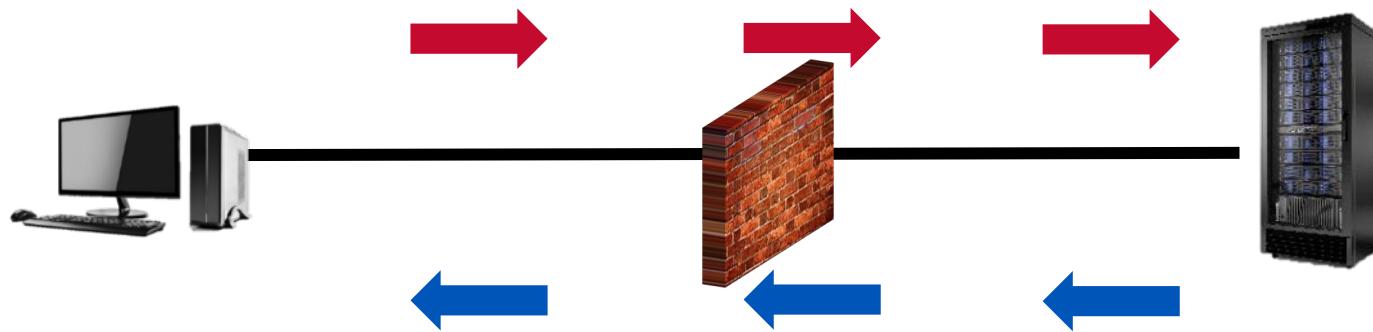
- 3. Examine when only length is considered**
 - Password length 15
 - Keys/second 1000
 - Number of computers 1
 - Characters are: lower only

Account Standards

- ▶ **These are best enforced with a domain or group policy**
- ▶ **Disablement**
 - Turning off access for an account, such as when an employee is terminated
- ▶ **Account lock-out threshold**
 - Determines the number of times invalid passwords may be submitted before crippling an account to mitigate brute-force, dictionary, and cognitive word attacks
 - Cognitive word attacks employ target-specific words that might be learned from Facebook or LinkedIn
- ▶ **Account lock-out duration**
 - The time an account is forced to be inactive before login may again be attempted

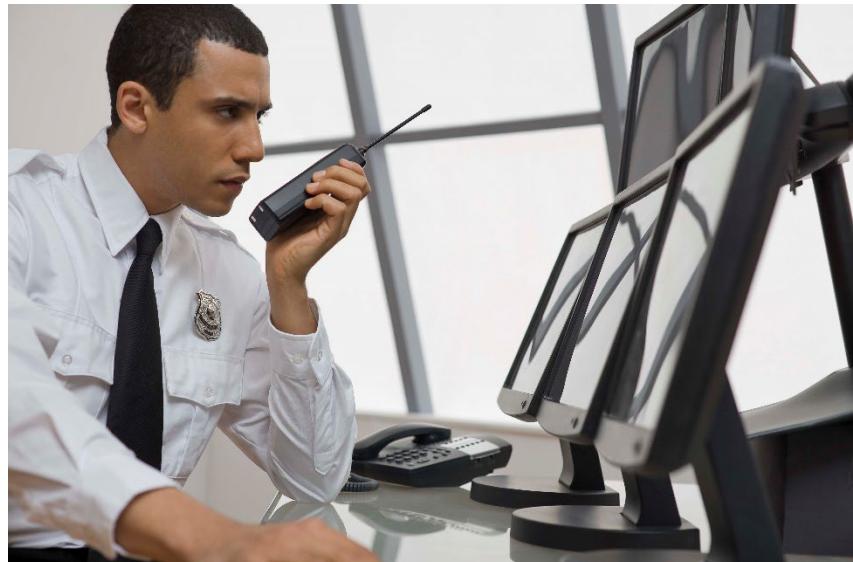
Access Control Policies

- ▶ **Access control policies are important and should address both information and physical security**
 - To protect the organization's information assets, such as customer data, financial information, and intellectual property
 - To reduce the risk of security incidents, such as data breaches and malware infections
 - To comply with industry regulations and standards



Access Control Elements

- **Access Control Policies** are critical for safeguarding an organization's digital assets. They define who can access what resources and under what conditions. Key components include
 - Authentication Verifying identity
 - Authorization Specifying permissions
 - Enforcement Mechanisms to restrict access
 - Audit and Monitoring Tracking access events
 - Documentation Clear policy guidelines
 - Access control policies apply to information assets and physical assets



Organization Encryption Standards

- ▶ In many cases, encryption standard are mandated by laws and regulation
- ▶ To securely manage information encryption standards, define:
 - Scope
 - Which data and devices must be encrypted?
 - Encryption methods
 - What encryption algorithms and key management practices must be used?
 - Responsibilities
 - Who is responsible for encrypting and decrypting data?
 - Key management
 - How will encryption keys be generated, stored, and distributed?
 - Audit and reporting
 - How will encryption compliance be monitored and reported?
- ▶ Failing to adopt and enforce good standards can lead to inconsistent use and losses of confidentiality and integrity

Procedures

- ▶ **Procedures are specific instructions**
 - Documenting and publishing procedures helps to ensure accuracy and consistency for policy goals and implementations of standards
- ▶ **Some key areas are:**
 - Change management
 - Onboarding/offboarding and employee agreements
 - Playbooks



Change Management Procedures

- ▶ **Based upon importance and impact to the organization procedures should be created for important or common activities**
 - Changes, even well-intentioned ones, can introduce new vulnerabilities and security risks
 - Detailed procedures help to identify and assess these risks before changes are implemented, and to mitigate or eliminate them as much as possible
 - Collections of these are commonly referred to as Playbooks
- ▶ **Detailed procedures also help to ensure that changes are implemented in a consistent and repeatable manner**
 - This is important for both overall security and compliance

Hiring and Employment-Related

► Onboarding

- The HR and information assurance steps for the addition of a new employee/contractor/partner to an organization and its systems including other required agreements

► Offboarding

- The HR and information assurance processes for the removal of an identity for an employee who has left the organization (covers post-separation agreements)
- Helps to ensure rogue ex-employees do not cause incidents

► Non-Disclosure Agreements (NDA)

- A legal contract that outlines sharing restrictions on confidential material, knowledge, or information
- Also known as a confidentiality agreement

► Non-Compete Agreement

- An agreement wherein a party (typically an employee) agrees not to become employed or start a business in a similar profession or trade in deemed competition against the employer

Playbooks

- ▶ **There are many kinds of security playbooks**
 - These provide necessary detail for common or important activities
- ▶ **Playbooks are detailed instructions on how to approach or respond to various issues, such as:**
 - Incident response playbooks
Instructions for responding to specific security incidents, such as ransomware attacks, data breaches, and malware infections
 - Compliance playbooks
These help organizations comply with mandated regulations and requirements, such as GDPR, HIPAA, and PCI DSS
 - Threat-specific playbooks
Focused on responding to specific attacks, such as phishing, denial-of-service attacks, and insider threats
 - Recovery playbooks
Document roles, requirements and steps for various kinds of system backups

Guidelines Examples

- ▶ **NIST and other organization publish guidelines for several types of platforms**
 - Web server
 - Operating system
 - Application servers
 - Network infrastructure devices
 - Routers
 - Switches
- ▶ **There are also general-purpose guides for**
 - Desktops
 - File servers
- ▶ **Vendor-specific guides may be available**
- ▶ **In case of conflicting instructions, follow the organization policy over the vendor's recommendations**

Contents

- Effective Governance

Risk Management

- Compliance Measures
- Third-Party Risk
- Audits and Assessments
- Security Awareness



The Risk Management Process

- ▶ It is a systematic process of identifying, assessing, prioritizing, and mitigating risks to reduce risk to an acceptable level
- ▶ These steps are typically performed in a cycle
 - Identification
 - Assessment
 - Analysis
 - Management
 - Monitoring
- ▶ NIST Risk Management Framework
 - RMF is the comprehensive information security framework for FISMA
 - A highly centralized approach to security
 - NIST SP 800-53 is a catalog of security controls
- ▶ Risk identification
 - Risk identification is the process of recognizing and documenting realistic potential threats and incidents that could impact an organization
 - E.g., protected health information could be stolen or inappropriately revealed



The Risk Management Process

► Risk assessment

- The systematic evaluation of the likelihood and potential impact of identified risks
 - E.g., a purchased device has a rating of 30,000 hours for mean time between failures and it is a single point of failure for internet access
- Frequency
 - Ad hoc As needed
 - Recurring Periodic
 - One-time Single assessment
 - Continuous Ongoing or real-time
- It starts with an inventory of hardware, software, and IP assets

► Risk analysis/prioritization

- Ranking identified risks based on their potential impact and likelihood
- Based upon the assessment, priorities may be set

Risk Analysis

- ▶ **Business Impact Analysis (BIA) provides useful data for risk analysis**
- ▶ **Matrix/heat map—scoring risks for prioritization**
 - A table with Likelihood x Impact indexes
 - Creates a visually meaningful representation

	Low	Medium	High	Very High
Critical				
High				
Medium				
Low				

- ▶ **Useful definitions**
 - *Probability* is the possibility of an event happening based on facts or assumptions that are currently known
 - *Likelihood* is the chance of a particular event given a certain hypothesis

Quantitative Risk Measurement

- ▶ A quantitative way of measuring risk is to assess IT assets
 - Assessing annual loss, likelihood of threat, and asset cost/value
- ▶ Asset Value (AV)
 - Typically measured in monetary terms
- ▶ Exposure Factor (EF)
 - The percentage of an asset you expect to be damaged by each occurrence of a particular risk event
- ▶ Single Loss Expectancy (SLE) = AV x EF
 - The anticipated loss each time risk is realized
- ▶ Annualized Rate of Occurrence (ARO)
 - The number of times it is expected that a given risk would occur in a year
- ▶ Annualized Loss Expectancy (ALE) = SLE x ARO

Risk Measurement Example

- ▶ Scenario: You are studying a project to use an online application that performs transactions to be the web front-end for your business
- ▶ The assets being handled by the system will be worth \$100,000 in revenue each year—this is the AV
- ▶ By exposing it to online threat, you could lose up to 5 percent of its value, if hacked—this is the EF
- ▶ The SLE = AV x EF, or \$5,000
- ▶ You predict that three successful attacks could occur each year—ARO
- ▶ SLE x ARO = ALE
- ▶ $\$5,000 \times 3 = \$15,000$
- ▶ You may have to perform one to two calculations

Qualitative Risk

- ▶ **People are typically assessed with a qualitative measurement**
 - Systems are measured quantitatively
- ▶ **Qualitative risk measurement is descriptive vs. measurable**
 - Can be performed in a shorter period of time and with less data
 - Typically performed through interviews
 - Requires personal assessment and judgments to be made



VS.



Quantitative

Qualitative

Risk Mitigation and Handling

► Risk mitigation

- If risk is excessive, it must be addressed

► It may be handled in five ways

1. Risk acceptance
 - Deciding to accept the consequences
 - We accept the \$15,000 loss, as we are making \$85,000 beyond it
 - The residual risk is the most important element
2. Risk transference
 - Shifting the loss to another party
 - Outsourcing the function for a cost of \$10,000
 - Still less than the \$15,000 loss
 - They accept all losses; we receive \$100,000 guaranteed
3. Risk avoidance
 - Deciding not to be involved in activities due to the potential loss
 - Our profit margin is only \$15,000
 - Drop the project

Exceptions are applied when the policies cannot be applied



Risk Management Strategies

4. Risk deterrence

- Removing factors that may become threats
- Threatening potential attackers
- Offering a reward for identifying individuals who have attacked the site
- Microsoft had several \$250,000 bounties for hackers who have created malware

5. Risk mitigation

- Implementing defensive measures and upgrades at a cost of \$5,000 and defending it
- We still make a profit of \$10,000

► **The overall goal is to reduce risk to an acceptable level**

- Risk threshold: The level at which decision is made to accept or avoid a risk
- Risk tolerance: How high or low the risk threshold is set
- Risk appetite: How much risk is acceptable before risk reduction is needed
 - May be: High/expansionary, Medium/Neutral, Low/conservative
- Risk Control Self-Assessment is a process for identifying and assessing operational risks and the effectiveness of risk management controls

Pop Quiz: Calculations and Change Management



- 1. Mary has discovered that one of her servers has failed. It costs the organization \$1000 for any day it is off-line. The technician assigned to repair it bills 85 USD per hour. It is estimated the work will take 4 hours. It is likely that two failures could happen each month.**
 - A. What is the SLE?**

 - B. Calculate the ARO**

 - C. What is the value of the ALE?**

Discussion

Risk Mitigation and Monitoring

► Risk Monitoring

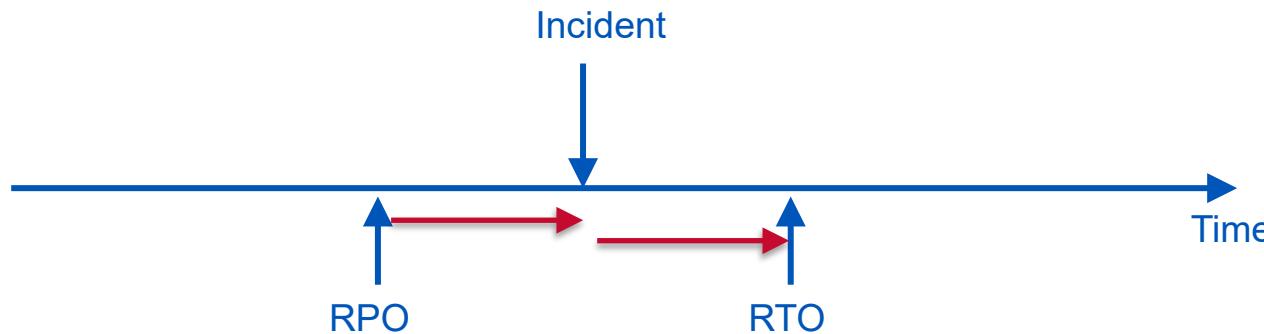
- These steps are involved in recurring and continuous risk analysis
 - Data Collection
 - Risk Analysis
 - Comparative Analysis—past vs. present
 - Reporting
 - Adjustment
 - Communication
 - Documentation

► Risk Register

- This document is key to monitoring
- A Risk Register is a list of risks identified, key risk indicators (KRI), affected owners, severity and mitigations used to track risk handling and mitigation

Risk Metrics

- ▶ **Recovery time objective (RTO)**
 - Goal for restoring normal operation or use
- ▶ **Recovery point objective (RPO)**
 - The goal for maximum loss after a recovery
 - How much data loss is acceptable
- ▶ **Mean time to repair (MTTR) replace/repair/recover/resolve**
 - Measured time (actual) for restoring normal operation or use
- ▶ **Mean time between failures (MTBF)**
 - Measured reliability is average time (actual) to a critical failure



Domain 5: Match the Items to the Topics

Do Now

Item	Answer	Topic
Likelihood x Impact		A. Custodian
Specifying permissions		B. Authorization
Longest SDLC phase		C. Maintenance
Before eradication		D. Standards
Performs backups		E. Contain
Detailed instructions		F. Heat Map
Does not specify exact solution		G. Risk Register
Tracking risk		H. Playbook

For each item on the left, write in the corresponding letter from a topic on the right

Contents

- ▶ Effective Governance
- ▶ Risk Management

Compliance Measures

- ▶ Third-Party Risk
- ▶ Audits and Assessments
- ▶ Security Awareness



Compliance

- ▶ **Defined**
 - Adhering to the applicable rules and laws
- ▶ **Compliance failures are often very expensive**
 - Fines
 - Sanctions
 - Reputational damage
 - Loss of license
 - Contractual impacts



Demonstrating Compliance

- ▶ **Compliance may be demonstrated by**
 - Attestation and acknowledgement
 - Internal and external audits
 - Automation
- ▶ **Reporting compliance**
 - Attestation
 - Issuing a statement that requirements have been met
 - Such as an internal PCI DSS audit by Qualified Security Assessor issuing a Report of Compliance
 - Automation
 - Using application suites to inspect and validate adherence to rules and regulations
 - A feature of many cloud service providers

Privacy

- ▶ **Protection varies according to the jurisdiction, organization, and use**
 - Personal information
 - Health data
 - Employee monitoring
- ▶ **Proper and safe storage of sensitive information with encryption**
 - Personally Identifiable Information (PII) uniquely specifies an individual and should be protected with special handling and retention policies
 - PHI is Protected Health Information and requires special handling and accountability
 - Data in transit—HTTPS or VPN
 - Data at rest—disk encryption
 - Data transfers between organizations must conform to data ownership and nondisclosure agreements

Contents

- ▶ **Effective Governance**
- ▶ **Risk Management**
- ▶ **Compliance Measures**

Third-Party Risk

- ▶ **Audits and Assessments**
- ▶ **Security Awareness**



Third-Party Risk Management (TPRM)

- ▶ **The process of analyzing and minimizing risks associated with**
 - Penetration tests and audits
 - Outsourcing to third-party vendors
- ▶ **Due to the highly specialized technical skills required, penetration tests are commonly performed by external third-parties**
 - May be sought for having independence as well
- ▶ **It is important to establish these contract-related parameters**
 - Right-to-audit clause
 - Documenting and showing all work
 - Independent assessments and no conflict in interest
 - Attest to independence of findings
 - E.g., not selling security products
 - Supply chain risk analysis
 - Vendors themselves and their contractors pose no excessive risk
 - Show due care—showing the same care as a reasonable person
 - Show due diligence—research issues thoroughly

Typical Vendor Agreements/Contracts

► Statement of Work

- Details of the task to be performed, project deliverables, timelines, work location

► Rules of Engagement

- Methods and types of simulated attacks allowed

► Master Services Agreement

- Delivery requirements, payment terms, intellectual property rights, warranties, dispute resolution and termination

► Service-Level Agreement (SLA) should document expectations

- The agreed commitments detailing the specific minimum levels of support/quality to be provided end to end



Additional Vendor Agreements

► **BPA (Business Partnership Agreement)**

- For larger efforts
- An arrangement in which business parties agree to work together to share benefits and risks
- Includes onboarding provisions
 - Initial briefings and enrollment in identity-management systems
 - Off-boarding briefing and Non-Disclosure Agreements (NDAs)

► **Memorandum Of Understanding (MOU)**

- A non-binding document outlining common actions of the parties and reporting

► **Memorandum Of Agreement (MOA)**

- Identifies specific ground rules for a cooperative effort or agreement
- Does not outline all responsibilities
 - A legal working agreement

► **NDAs and NCAs (discussed earlier)**

Contents

- ▶ Effective Governance
- ▶ Risk Management
- ▶ Compliance Measures
- ▶ Third-Party Risk

Audits and Assessments

- ▶ Security Awareness

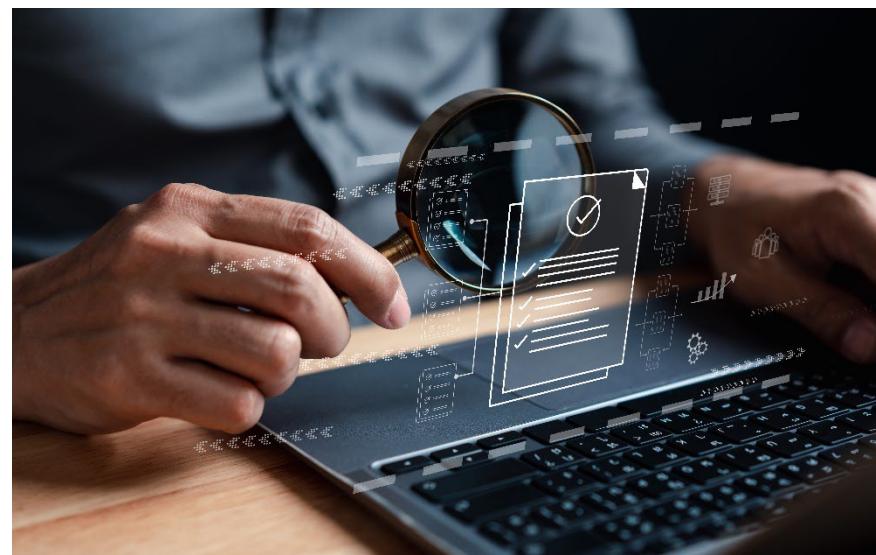


Security Assessments and Audits

- ▶ **A mandate to assess or audit may be**
 - Internal—supervisory committee
 - External—a regulatory agency
- ▶ **The motivations for these may be**
 - Compliance Typically an external agency mandates it
 - Performance A competition between attackers and defenders
 - Goal-oriented Setting an objective, such as validating an application
- ▶ **An assessment may be performed by internal or a third-party**
- ▶ **There are three ways to audit or assess**
 - Attest/interview—ask the responsible party
 - Inspect—observe the controls in place
 - Test—verify the functionality of a control

External SOC Audits

- ▶ **SOC 2 reports come in two varieties: SOC 2 Type 1 and SOC 2 Type 2**
 - The difference between the two lies in the duration of the assessment period for systems and control designs
- ▶ **SOC 2 Type 1**
 - SOC Type 1 examines an organization's systems and control designs at a specific moment in time
 - This enables a more rapid demonstration of an organization's control implementation
- ▶ **SOC 2 Type 2**
 - SOC Type 2, on the other hand, assesses the effectiveness those controls over a defined period
 - Typically ranging from 6 to 12 months



Security Assessments and Audits

- ▶ A vulnerability assessment gathers information and determines the current exposure to threats via misconfiguration or vulnerabilities
 - Performed with automated tools
 - Passively tests controls
 - Identifies the vulnerability, missing controls, or misconfiguration
- ▶ Penetration testing is a focused form of vulnerability assessment
 - Physical/site assessments
 - Social engineering
 - Offensive vs. defensive personnel
 - Performance-based
 - Integrated
 - Systems that combine a multitude of tools and data sources in a focused attack



Black, Gray, White Hats, and Boxes

- ▶ **The people who test security are generally referred to as**
 - *Black hat*: Illegal security testers (hackers) who seek illicit personal gain
 - *Gray hat*: Illegal security testers who notify the victim when they discover a vulnerability (it is still illegal)
 - *White hat*: Security testers who are authorized to perform hacking and report the results to their client
- ▶ **Methods of testing**
 - *Black box*: Unknown environment. An application is tested with inputs from the outside to see how it handles real-world interaction
 - Testers have no experience/knowledge of the application's inner workings
 - Fuzzing is a form of black box testing
 - Sends an array of information to test input validation and error handling
 - *Gray box*: Partially known environment. Having partial or limited documentation/knowledge of a system to test it
 - *White box*: Known environment. Tester has all knowledge; tests internal data flows, structures, or workings of an application

Teams and Exercises

- ▶ Coordinated drills may be performed involving an organization's defensive and offensive elements
- ▶ Red team
 - White hat offensive hacking groups
- ▶ Blue team
 - Defensive personnel, firewalls, intrusion detection endpoint security
- ▶ White team
 - Judges and umpires in an exercise
- ▶ Purple teams
 - A coordination of efforts between red and blue teams to maximize defensive capabilities

Contents

- ▶ Effective Governance
- ▶ Risk Management
- ▶ Third-party Risk
- ▶ Compliance Measures
- ▶ Audits and Assessments

Security Awareness



Security Awareness

- ▶ **Personnel should be provided with resources to combat a number of issues**
 - Social engineering
 - Insider threats and abuse
- ▶ **Operational security elements**
 - Situational awareness training
 - Policy, guides and playbooks
 - Password management
- ▶ **Today, it is especially important to address hybrid/remote work environments**

Social Engineering

- ▶ **Manipulation of personnel and users is difficult to prevent**
 - Almost any attack that involves talking or observing
 - It works even when technical controls are perfect
- ▶ **The vulnerability is the gullibility of personnel**
 - Education is the best way to prevent social engineering
- ▶ **Awareness and training are the keys**
 - Training should address
 - Recognizing phishing campaigns and spear phishing attempts
 - Reporting suspected social engineering attempts
 - Identifying anomalous behavior
 - Risky
 - Unexpected
 - Unintentional

User Training

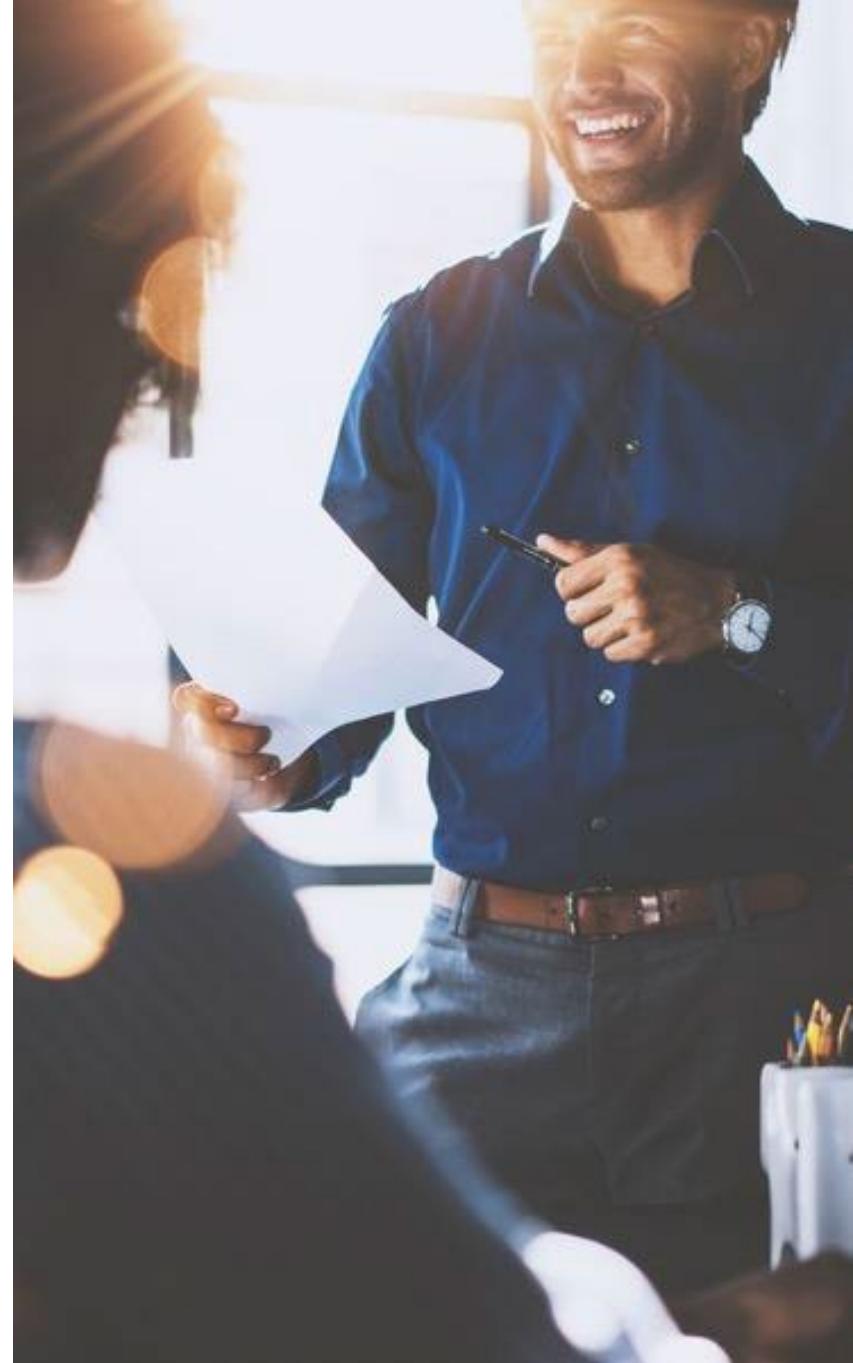
- ▶ **Testing and training should be annual and role-based**
 - Performed annually
 - Metrics tracked
- ▶ **Periodic awareness training**
 - Gamification
 - Capture the Flag (CTF)
 - Phishing simulation
 - Computer-based
- ▶ **These will help to improve the development and execution of training efforts**
- ▶ **More on social engineering in Domain 2**



Objectives

- ▶ Identify effective governance
- ▶ Analyze compliance measures
- ▶ Understand risk management
- ▶ Explain third-party risk management
- ▶ Examine audits and assessments
- ▶ Implement security awareness

20%





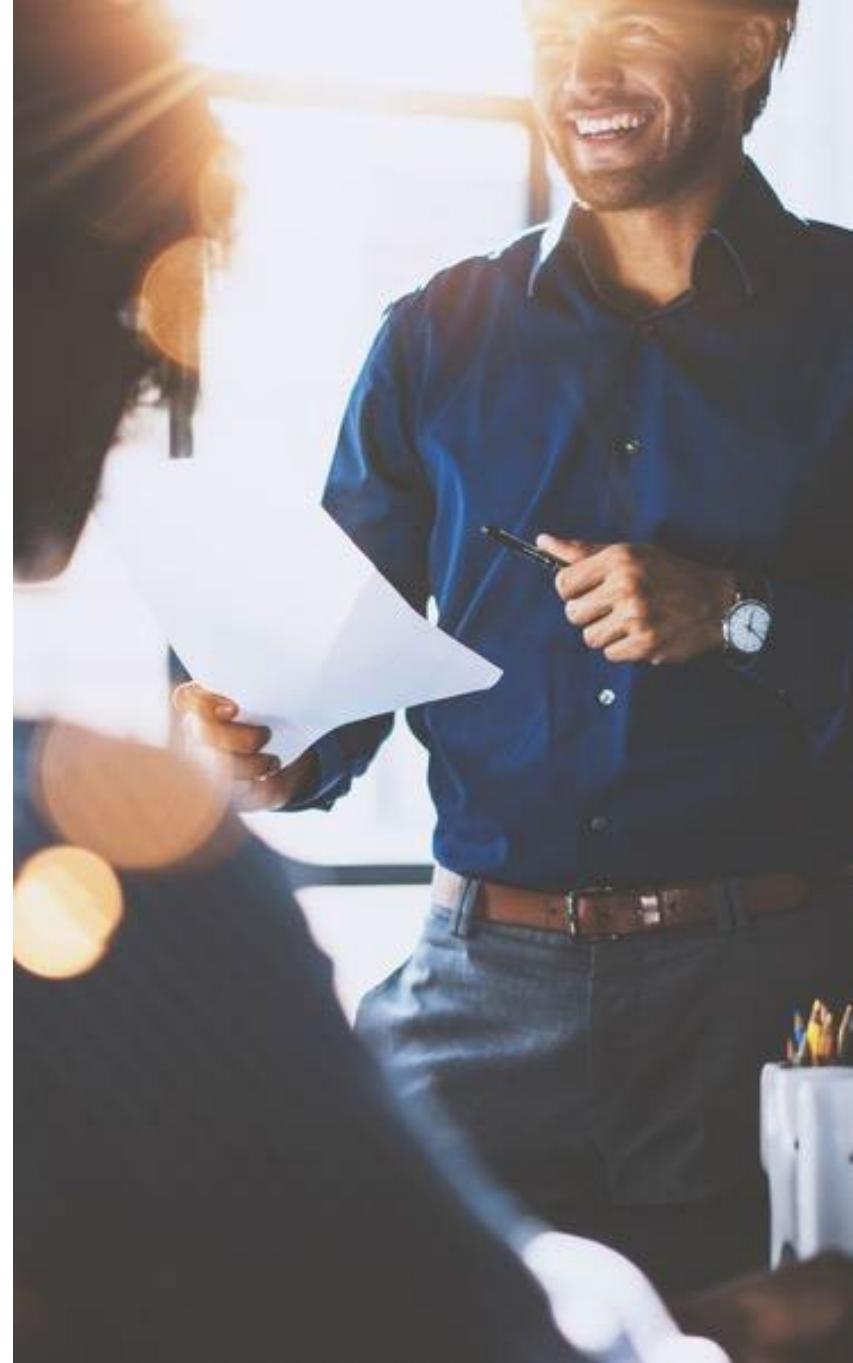
Chapter 4

Domain 2: Threats, Vulnerabilities, and Mitigations

Objectives

- ▶ Comparing threat actors
- ▶ Analyzing vectors and the attack surface
- ▶ Understanding vulnerabilities
- ▶ Identifying malware
- ▶ Specifying appropriate indicators and mitigation

22%



Contents

Threat Actors

- ▶ **Vectors and the Attack Surface**
- ▶ **Vulnerabilities and Attacks**
- ▶ **Malware**
- ▶ **Indicators and Mitigation**



Threat Actors: Script Kiddies and Hacktivists

► Script Kiddies

- Location External
- Sophistication Low
- Funding Low
- Motive Curiosity, Fame
- Use of Open sources Low

► Hacktivists

- Location External
- Sophistication Medium/High
- Funding Medium
- Motive Political, Social
- Use of Open sources High

Threat Actors: Organized Crime and Nation/State

► Organized Crime

- Location External
- Sophistication High
- Funding High
- Motive Financial
- Use of Open sources High

► Nation/State

- Location External
- Sophistication High
- Funding High
- Motive Political, Information Warfare
- Use of Open sources High

► Advanced Persistent Threat

- Sophistication High
- Coordination High
- Skill High

Threat Actors: Insiders and Competitors

► Insiders

- Location Internal
- Sophistication Medium
- Funding Low
- Motive Revenge, Financial, Personal
- Use of Open sources Low

► Competitors

- Location External
- Sophistication Medium, High
- Funding High
- Motive Financial
- Use of Open sources High

► Shadow IT

- Individuals who run their own IT systems or rogue help desks within an organization

Contents

- ▶ Threat Actors

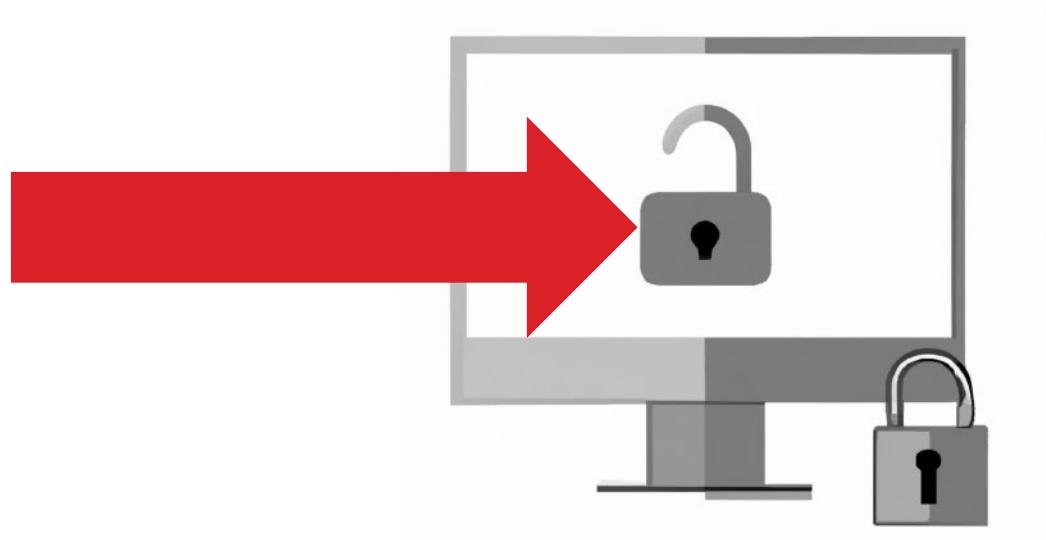
Vectors and the Attack Surface

- ▶ Vulnerabilities and Attacks
- ▶ Malware
- ▶ Indicators and Mitigation



Vectors

- ▶ A vector is a means of access to a target
- ▶ These include
 - Images and Files
 - Messaging
 - Voice calls
 - Removeable devices
 - Vulnerable software
 - Unsupported applications
 - Non-secure networks
 - Open ports
 - Default credentials
 - Social engineering



Messaging and Calls

- ▶ **Nearly all social engineering attacks involve some form of impersonation**
 - Periodic awareness training and incident alerts are best defenses
- ▶ **Phishing**
 - Commonly used to solicit banking and personal information
 - “*... an email fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients*”*
- ▶ **Spear phishing**
 - Well-researched and well-written emails that target an individual
 - Not the typical Nigerian scam
 - New trends are for email messages followed up with calls and text messages
- ▶ **Whaling**
 - Sending targeted and forged emails to high-value targets
 - Business owners, executives, CEOs, wealthy individuals

*Source: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci916037,00.html

Messaging and Voice Calls

► **Vishing**

- Anything using the telephone system to connect to a victim (a mark), commonly using Voice over IP (VoIP)
- Caller ID is easily spoofed with VoIP

► **Piggybacking or Tailgating**

- Tailgating is closely following someone through a doorway without their knowledge
- Piggybacking is entering with them, with their knowledge perhaps in a conversation

► **Spam, Smishing, and SPIM**

- Attempts at social engineering using email, SMS or Instant Messaging

► **Pretexting**

- A guided dialogue that has a plot and goals based upon a plausible scenario

► **Influence campaigns and intimidation**

- Organized attempts to influence masses

Images and Files

► Images

- Are commonly used in conjunction with social engineering
- It may be an offer, warning, or a threat



► Files

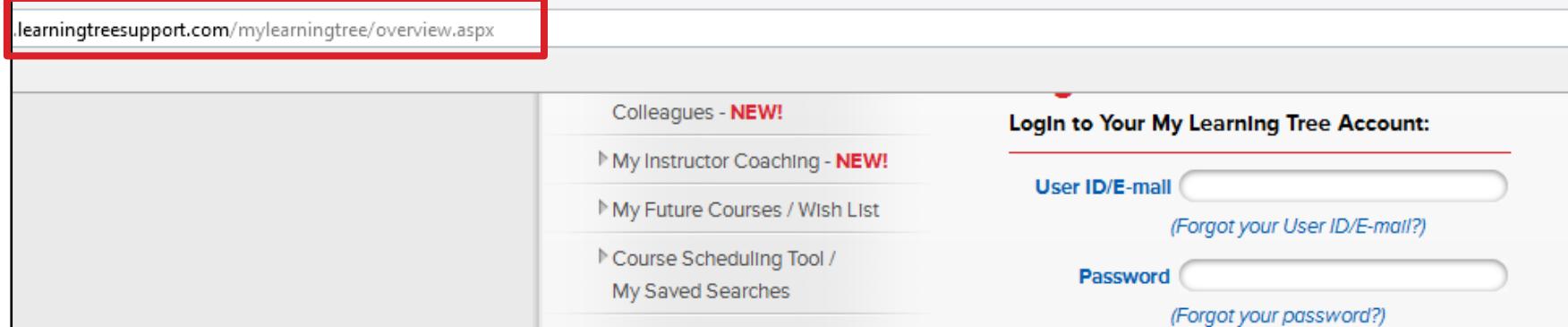
- Usually conveyed via a link sent with email or other messaging
- The file is actually a malicious payload
 - Providing remote access—command and control (c2)
 - Planting spyware or other malicious code
 - Shown below is a Metasploit session from its console

```
msf5 exploit(multi/handler) > sessions

Active sessions
=====
Id  Name    Type
--  --     --
1   meterpreter x86/windows
                               Information Connection
                               -----  -----
                               127.0.0.1:1337 -> 127.0.0.1:56!
```

Password and Identity Theft Techniques

- ▶ **Supply chain issues**
 - Brand impersonation—pretending to be authentic
- ▶ **Malicious insider threat**
 - Insiders that have access to passwords and may make use of them
 - Email compromise
- ▶ **Typo squatting/URL hijacking**
 - Login at www.learingtree.com/myhistory
- ▶ **Watering hole attack**
 - Staging a realistic site that pretends to offer help
 - Prompts for user name and password



Removeable Devices

► Malicious uses

- Keylogging
- Tracking individuals
- System access and control

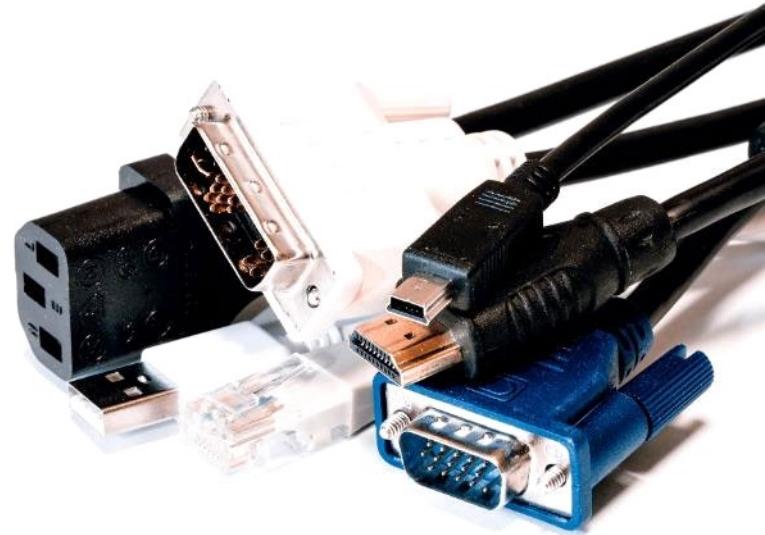


► USB Drops

- A technique where an attacker drops USB devices in trafficked areas
- Eventually a person may pick it up and access it, launching the contained payload

► Keyloggers are easily disguised as simple devices and cables

- Fobs
- Cables
- Charging stations



Unsupported or Vulnerable Software

- ▶ **Unsupported software may be dangerous and is not maintained**
 - This commonly results in vulnerable versions being preset
 - The software may itself be malicious, acting as a Trojan
- ▶ **Vulnerable software acts as a point of access for attackers**
 - Some software brands are more vulnerable than others

[CVE-2023-38248](#) Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.

[CVE-2023-38247](#) Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.

[CVE-2023-38246](#) Adobe Acrobat Reader versions 23.003.20244 (and earlier) and 20.005.30467 (and earlier) are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.

Open Port and Unfiltered Services

- ▶ Attacks typically require initial recon to be performed
 - Learn the underlying OS
 - Discover the type of database used
 - Reveal version numbers to look up in a vulnerability database
- ▶ Banner grabs



```
Administrator: Windows Command Processor - nc 10.200.11.143 21
C:\Windows\System32>nc 10.200.11.143 21
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse <Tim.Kosse@gmx.de>
220 Please visit http://sourceforge.net/projects/filezilla/
```

- ▶ Some services should not be exposed to the internet or untrusted access
 - SMB and NetBIOS TCP/135, TCP/139, TCP /445,
 - Portmapper TCP/111

XSS = cross-site scripting

A close-up photograph of a person's hands typing on a white computer keyboard. The hands are positioned in the center, with fingers pressing the keys. The background is slightly blurred.

Do Now

Examine Open Ports

- 1. On the Windows PC, open a command prompt**
- 2. Run: nmap -n -T5 -sV -O 10.1.1.125**
- 3. This will perform a port scan to elicit information about the target (Kali Linux)**

Wireless and Bluetooth

- ▶ **Bluetooth attacks are common against cell phones**
 - Bluejacking: the sending of unsolicited messages over Bluetooth
 - Bluesnarfing: using Bluetooth to pilfer information, contacts, and pictures
- ▶ **Intentional jamming or accidental interference from channel conflicts on nearby WLANs to disassociate from endpoints**
- ▶ **Wardriving involves locating wireless 802.11 LAN connections**
 - By driving around a city or other populous or industrial area to find access points and analyze network security of an unsecured wireless network
 - Aided by DHCP
- ▶ **War chalking is writing symbols near a wireless network to describe access**
- ▶ **Mitigated by shielding and disabling SSID broadcast and changing default passwords**



DHCP = Dynamic Host Configuration Protocol

LAN = local area network

Contents

- ▶ Threat Actors
- ▶ Vectors and the Attack Surface

Vulnerabilities and Attacks

- ▶ Malware
- ▶ Indicators and Mitigation



Vulnerabilities

- ▶ **Types**
 - Physical
 - General applications
 - Web applications
 - Hardware
 - Virtualization
 - Cloud
 - Supply chain
 - Cryptographic
 - Mobile devices
- ▶ **Their threat and deployment varies according to the type of vulnerability and location of the attacker, as well as the characteristics of the targets**

Physical

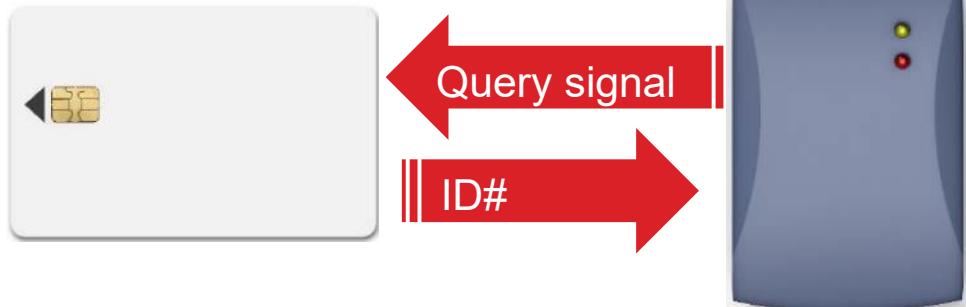
- ▶ **RFID Skimming/Cloning**
- ▶ **Environment**
- ▶ **Barrier bypass**
- ▶ **Shoulder surfing**
- ▶ **Access cards and codes**



RFID and Magnetic Cards

► Radio-Frequency IDentification (RFID): passive are easily skimmed

- May be used to steal credit card information
- The reader emits a query signal
- RFID responds with a unique ID number
- Commercial skimmers can read from several meters
- RFID tags can be read and then cloned at distances from a few inches to several meters
- RFID signals are not encrypted



RFID reader
continuously sends
querying signal

► Magnetic-stripe cards

- Common to credit cards and hotel keys
- Magnetic card must be swiped through a reader device
- Forgery may be easily performed if card is passed near a skimmer



Environment

- ▶ **The environmental controls relate to some areas outside of the security realm**
 - Site, building, and media shielding
 - HVAC, humidity, electrical support, and fire suppression
- ▶ **Air gaps**
- ▶ **Site and media shielding**
 - Very secure sites may need to implement Faraday cages to prevent sniffing and monitoring traffic, as well as preventing inbound transmissions
- ▶ **Data cabling may also be shielded**
 - Heavy electrical environments (machinery and medical imaging equipment) may cause interference with UTP and STP
 - Fiber-optic cabling is largely immune to EMI and RFI issues

HVAC = heating, ventilation, and air conditioning

STP = shielded twisted pair

UTP = unshielded twisted pair

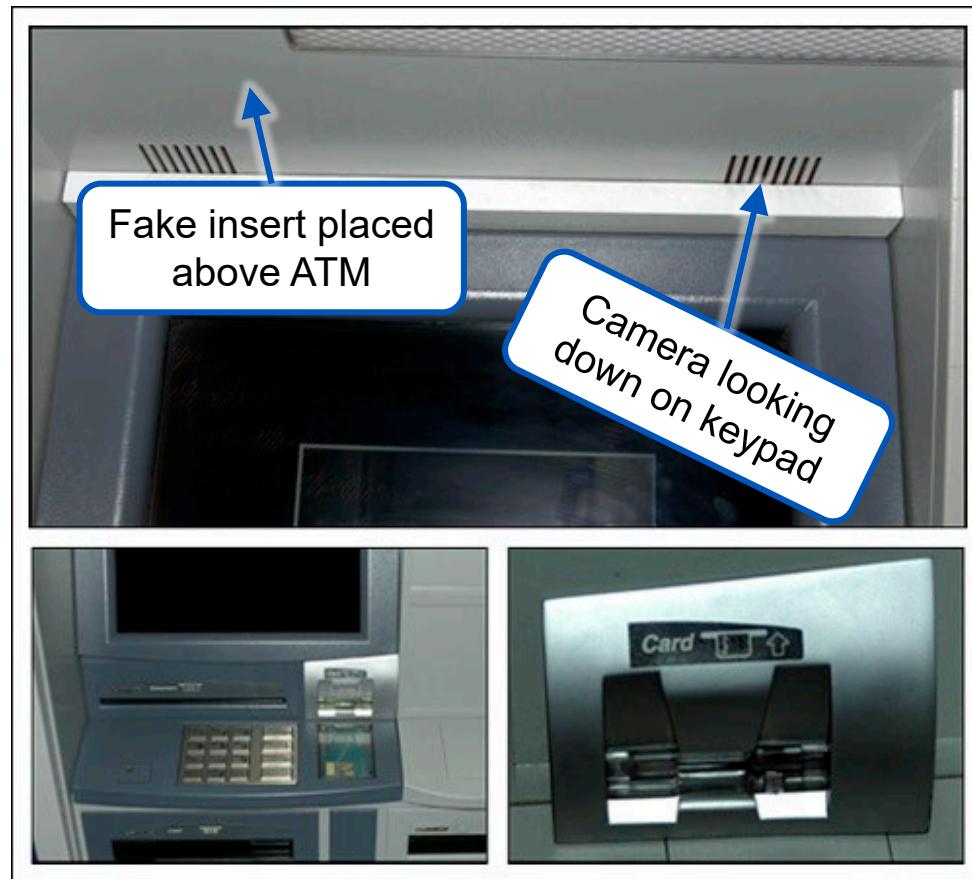
Barrier Bypass

- ▶ **Lockpicking**
- ▶ **Piggybacking or tailgating**
 - Following an authorized person through a door in high traffic areas
 - Mantraps to separate secure and insecure areas are a defense



Shoulder Surfing

- ▶ Shoulder surfing has progressed well beyond sneaking a peek over a victim's shoulder
- ▶ Cameras and illicit card readers are skillfully concealed in and around devices that require passwords and PIN codes
 - ATMs
 - Door controls
 - Computers



ATM = automatic teller machine

PIN = personal identification number

Source: "Taking a Trip to the ATM? Beware of 'Skimmers.'" Federal Bureau of Investigation, U.S. Department of Justice. <https://www.fbi.gov/news/stories/atm-skimming>.

General Application Vulnerabilities

- ▶ **Programming weaknesses**
 - Race conditions
 - Privilege escalation
 - Memory corruption/injection
 - Integer and buffer overflows
- ▶ **Change management**
 - DLL injection
 - Malicious updates
- ▶ **Network**
 - Replay



Race Conditions

► An error in programming involving competing processes

- Occurs when software is dependent on the sequence or timing
- It is a vulnerability when events do not happen in the order the programmer intended
- An issue commonly associated with multi-threaded applications
- Authentication should occur before authorization
 - What if authentication could be slowed, and then authorization completes first?
 - Perhaps system or other rights could be granted



► In software security, this involves testing a value (checking) with an issue, such as authentication; then, acting on the authentication

- Meanwhile, the state can change between the time of check (TOC) and the time of use (TOU)
- Another process changed the state

Privilege Escalation

- ▶ **Run code or perform techniques that allows any unauthorized access**
 - May be lateral or vertical
- ▶ **Attackers may steal credentials with a protocol analyzer and capture admin credentials**
- ▶ **Not all attacks result in root or administrative compromise**
- ▶ **Administrators should have two accounts: normal and privileged**
 - Web browsing should be done with an unprivileged account to prevent escalation of privileges by an attacker
- ▶ **Gaining full rights to a host is called “owning” it**
- ▶ **Any process or technique that illicitly boosts the rights is called privilege escalation**

DLL Injection and Malicious Updates

► **Malicious updates**

- A form of social engineering that introduces malware
- Fake Malvertising promotes a patch or add-on



► **DLL Injection**

- A process by which malicious instructions are inserted into an application via a malicious DLL
- The malicious code has the same name as a DLL used by the application
 - Malicious code redirects how the application works
- Vulnerability is caused by how DLLs are named and loaded

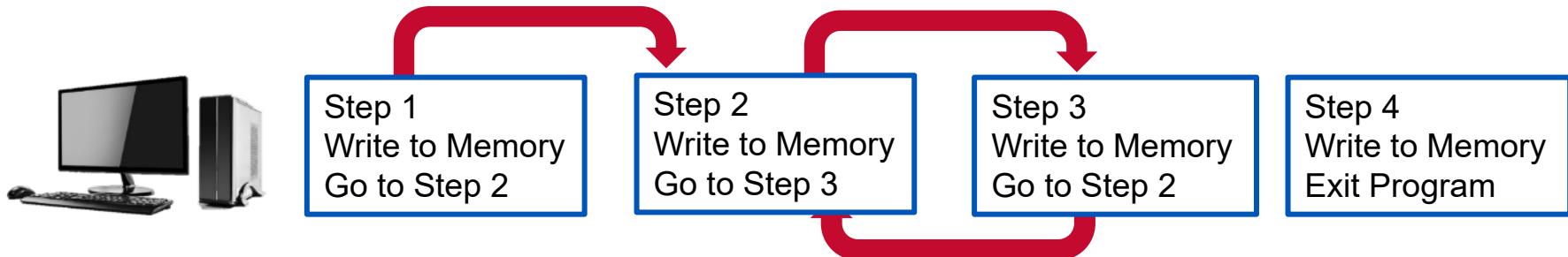
Memory Corruption

- ▶ **Typically, a programming error**

- Memory leak
- Integer overflow
- Buffer overflow

- ▶ **Memory leak**

- May also be called a recursion error
- Due to poor programming, memory is allocated in small segments
 - But, never released with `free()` consuming all memory causing a crash
 - In C, `malloc()` takes memory, `free()` releases it

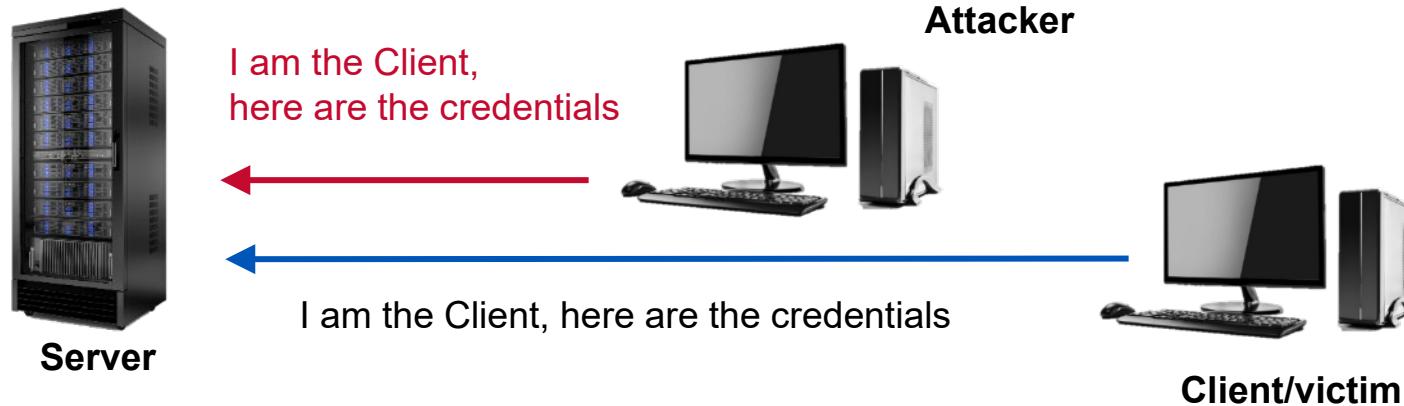


Integer and Buffer Overflow

- ▶ These are techniques that can allow new instructions to be injected into memory
- ▶ Buffer overflow is also memory corruption
 - Data is submitted to an application that does not check the amount
 - If a 20-byte buffer accepts 1,000 bytes, then the extra 980 bytes would overwrite other areas of memory
 - Causing crash or injecting malicious code
 - Defended with input validation
 - IF (VAR1.LENGTH > VAR1.BUFFERSIZE) THEN EXIT
- ▶ Integer overflow
 - Like a buffer overflow
 - When a 64-bit number is stored in the space of a 32-bit value (e.g., odometer rolling over to 000000 miles; the Y2K bug)

Replay

- ▶ **Successful logon password is captured by a protocol analyzer (sniffer)**
 - Client logging in to a server
 - Telnet and FTP protocols send passwords without encoding or encryption
 - Same packet is sent with recorded credentials embedded in new packets
- ▶ **Some wireless attacks use replay of ARP packets to break encryption**
 - Called an IV attack
- ▶ **Defense is to use Kerberos, a challenge (CHAP), or one-time passwords**



CHAP = Challenge Handshake Authentication Protocol

IV = initialization vector

Web Application Vulnerabilities

- ▶ Cross-site scripting (XSS)
- ▶ SQL Injection (SQLi)
- ▶ Command Injection
- ▶ Traversal
- ▶ Cross-site Request Forgery



Session Hijacking and XSS

- ▶ **Cross-site scripting (XSS) is a web security vulnerability that allows an attacker to**
 - Inject malicious code into a trusted website
 - This code can then be executed by the victim's browser, giving the attacker control over the victim's session
 - XSS attacks can be used for a variety of malicious purposes, such as stealing sensitive information, redirecting victims to malicious websites, and even taking control of the victim's computer
- ▶ **Stealing Session Cookies have security implications**
 - May be read by spyware to ascertain and report user browsing
 - Cross-site scripting (XSS) is an attack that may allow attackers to steal cookies and may allow webmail accounts to be *session hijacked*
 - XSS typically has malicious <script> tags embedded in a popular page

XSS

- 1. Go to the Instructor Demo PC**
- 2. Open Firefox and click the bookmark link for XSS**
- 3. Enter any words in the blog page, plus:**
`<script>alert("XSS
vulnerable!")</script>`
- 4. A popup will appear**
- 5. This demonstrates the server does not sanitize the user input. A remote user can inject a rogue JavaScript into this application**

Demo

SQL Injection

- ▶ Vulnerable web front-ends insert user-provided text directly into SQL queries
 - Consider what would happen if the username entered was ' OR 1=1 --

Credit Card User Login
Please log in

Username :

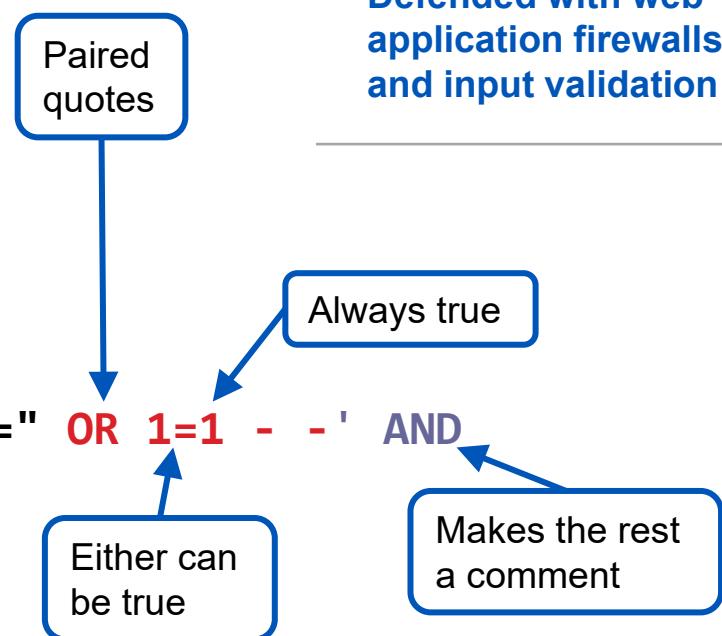
Password

```
SELECT * FROM ccards WHERE username=" OR 1=1 --"
passwd = "
```

- This could return all of the credit cards

▶ Validate input server side

- Client validation cannot be trusted



SQL Injection

- 1. Go to the Instructor Demo PC**
- 2. Open Firefox and click the bookmark link for SQL Injection**
- 3. In the username field, enter:
‘ or 1=1 -- (be sure to add a space after --)**
- 4. Why did this return all of the users?**
- 5. Mutillidae is a hacking practice application**

Command Injection

- ▶ Happens when an application passes a user value to the operating system directly
- ▶ What if a web application accepted a user-supplied value to ping an address?

```
http://server.com?app.php?name=cnn.com
```

Enter a site to ping:

- ▶ But a malicious attacker enters:

```
http://server.com?app.php?name=cnn.com%20&%20format c:
```

Enter a site to ping:

- ▶ It would ping the site, then attempt to format the C: drive

OS Command Injection

- 1. Go to the Instructor Demo. Open Firefox and chose the bookmark for: Mutillidae**
- 2. In Mutillidae, log in as adrian/somepassword**
- 3. Click the menu options for: OWASP 2017 > Injection (Other) > Command Injection >DNS Lookup**
- 4. Enter 8.8.8.8 as the IP Address and then Submit**
- 5. Change the entry to 8.8.8.8 & whoami and then Submit**
- 6. What new thing happened?**
- 7. Enter: 8.8.8.8 | dir c:\ and submit it**

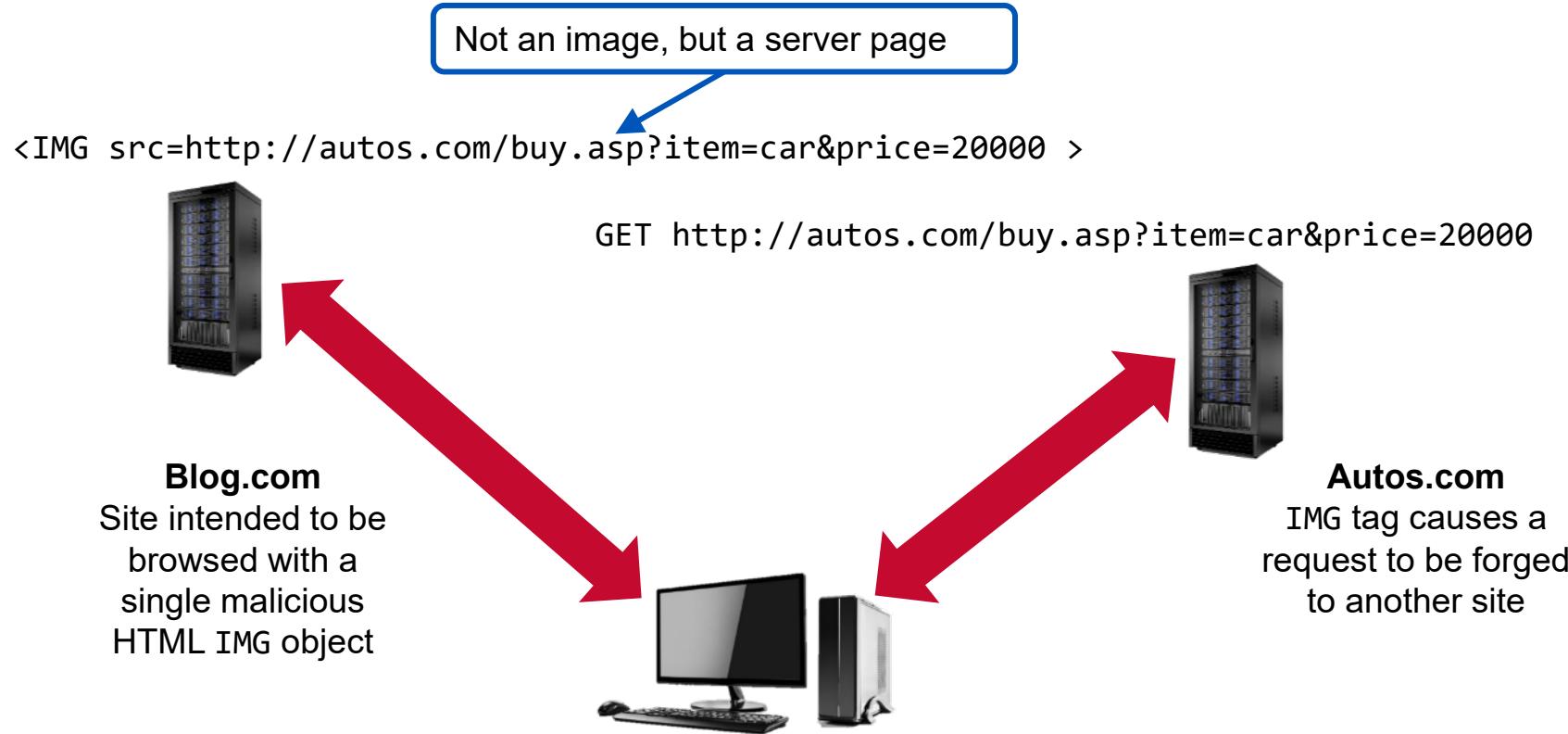
Directory Traversal

- ▶ Directory Traversal means to be able to wander throughout a file system, bypassing access controls
- ▶ Consider these normal requests
 - GET /file.html A request to retrieve a file in the working directory
 - GET ../../file.html A request to retrieve a file two directories up from the working directory
- ▶ An intruder may try a request like this
 - GET ../../../../../../etc/shadow
 - It might fetch the encrypted passwords file
 - This could be obfuscated as
 - GET %2e%2e%2f%2e%2e%2f%2e%2e%2e%2e%2fetc/shadow

Defended with web application firewalls and input validation

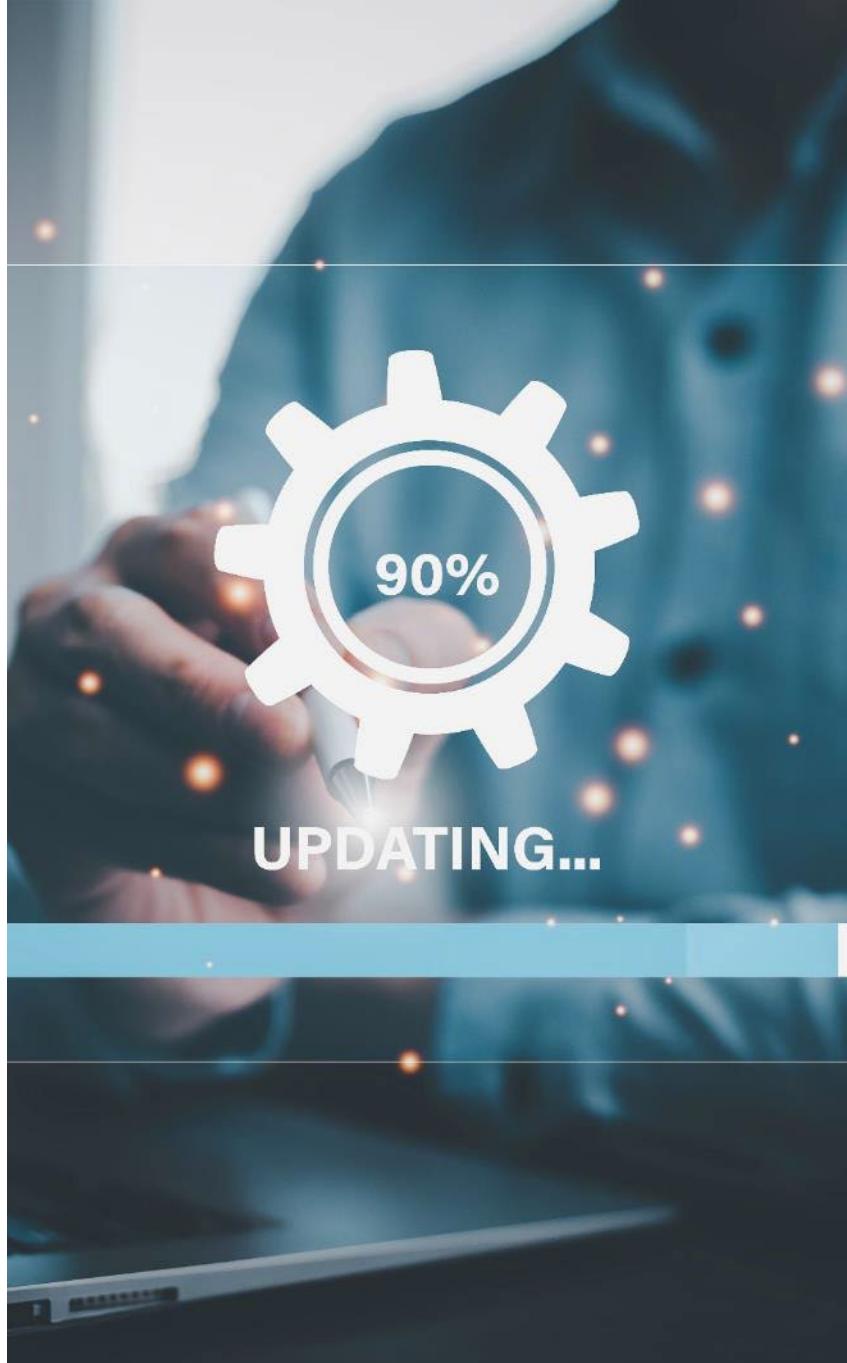
Cross-Site Request Forgery (XSRF)

- ▶ First, the client reads a page from the blog site
 - It has a malformed HTML IMG object in it
- ▶ Next, the client loads the buy.asp transaction from Autos.com
 - This causes the client to run a forged transaction to buy a car



Hardware and Firmware

- ▶ Default and hard-coded credentials
- ▶ Not designed with security in mind
- ▶ No defensive mechanisms



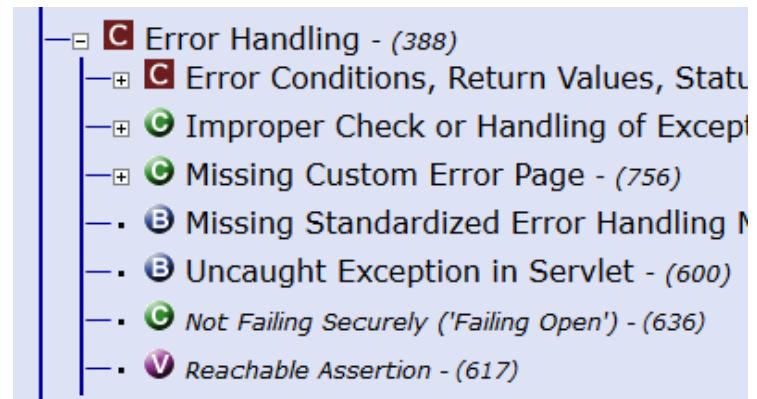
Defaults and Misconfiguration

► Default Configuration

- Nearly any system's default access controls is published somewhere (e.g., Diebold CSP 200 ATMs have the default management code of 626243)

► Misconfiguration

- Thousands of common errors may be committed
- On the right is an example of Common Weakness enumeration*



*Source: Published database with open use <https://cwe.mitre.org/about/termsofuse.html>

Specialized Systems

- ▶ Some computing environments are nontraditional and may be directly or indirectly linked to the cloud
- ▶ Beside the traditional computer-based environment, other areas must be addressed
 - Supervisory control and data acquisition (SCADA) and industrial controls (IDC)
 - Vehicles and aircraft/UAV
 - Robotics (RTOS)
 - Medical devices
 - System on a Chip (SoC)
 - Game consoles and wearable technology (first-person view)
 - Fire Control, HVAC, and residential technology
- ▶ Often these devices cannot load or use defensive software
 - The perimeter must be defended
 - Poor encryption
 - Little logging or auditing

RTOS = Real-Time Operating System

UAV = Unmanned Aerial Vehicles

Difficult to Defend

- ▶ **Embedded Systems**
 - Largely defenseless, no anti-malware exists for them
- ▶ **Attacker can gain control of**
 - Industrial controls in oil refineries
 - SCADA for building fire controls
 - Aircraft and vehicle navigation computers
- ▶ **Constraints**
 - Power availability
 - Network range limitations—Bluetooth
 - CPU limitations—cryptography
 - Access and patching limitations—wind farms
 - Medium—Ethernet, 5G, NFC, Zigbee

Virtual Machines Issues

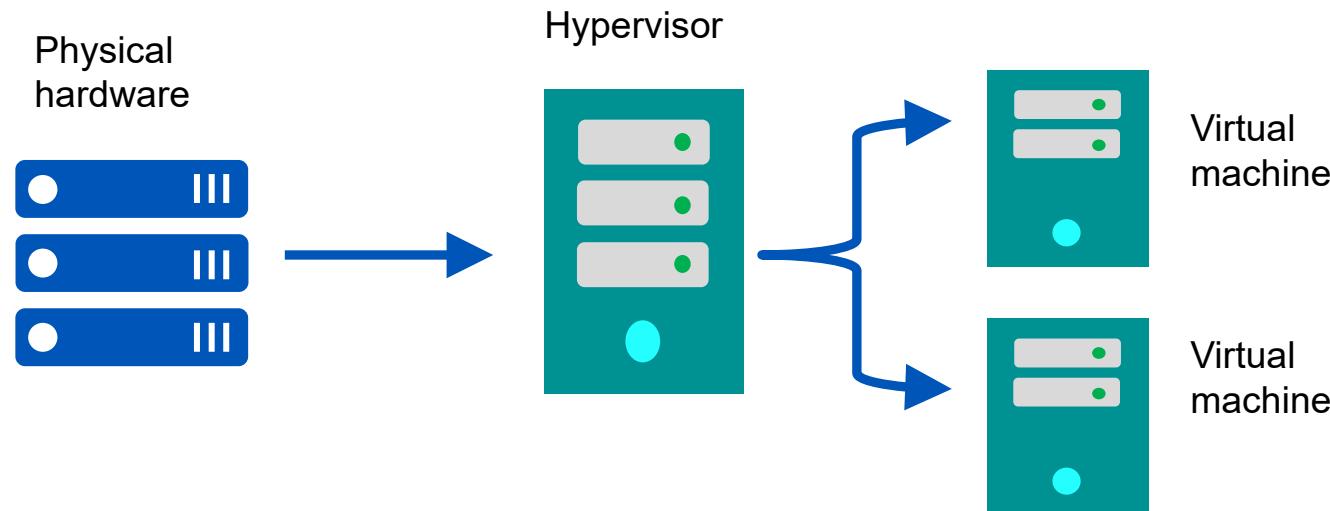
- ▶ **The emulation of a computer in software**
- ▶ **VMs are based on popular hardware computer architectures**
 - Provide nearly the same functionality as a physical computer
 - Smaller physical footprint
 - May be created in hardware or software
 - Run on hypervisors
- ▶ **VM-specific vulnerabilities**
 - VMEscape
 - VMSprawl



Virtual Machines (VMs)

► Hypervisors

- The software, firmware, or hardware that hosts virtual machines
- Type 1, also known as *bare metal*
 - Run directly off the hosting machine's hardware
- Type 2, also known as *hosted hypervisors*
 - Run on top of a conventional OS with the assistance of an application, such as VMware Player

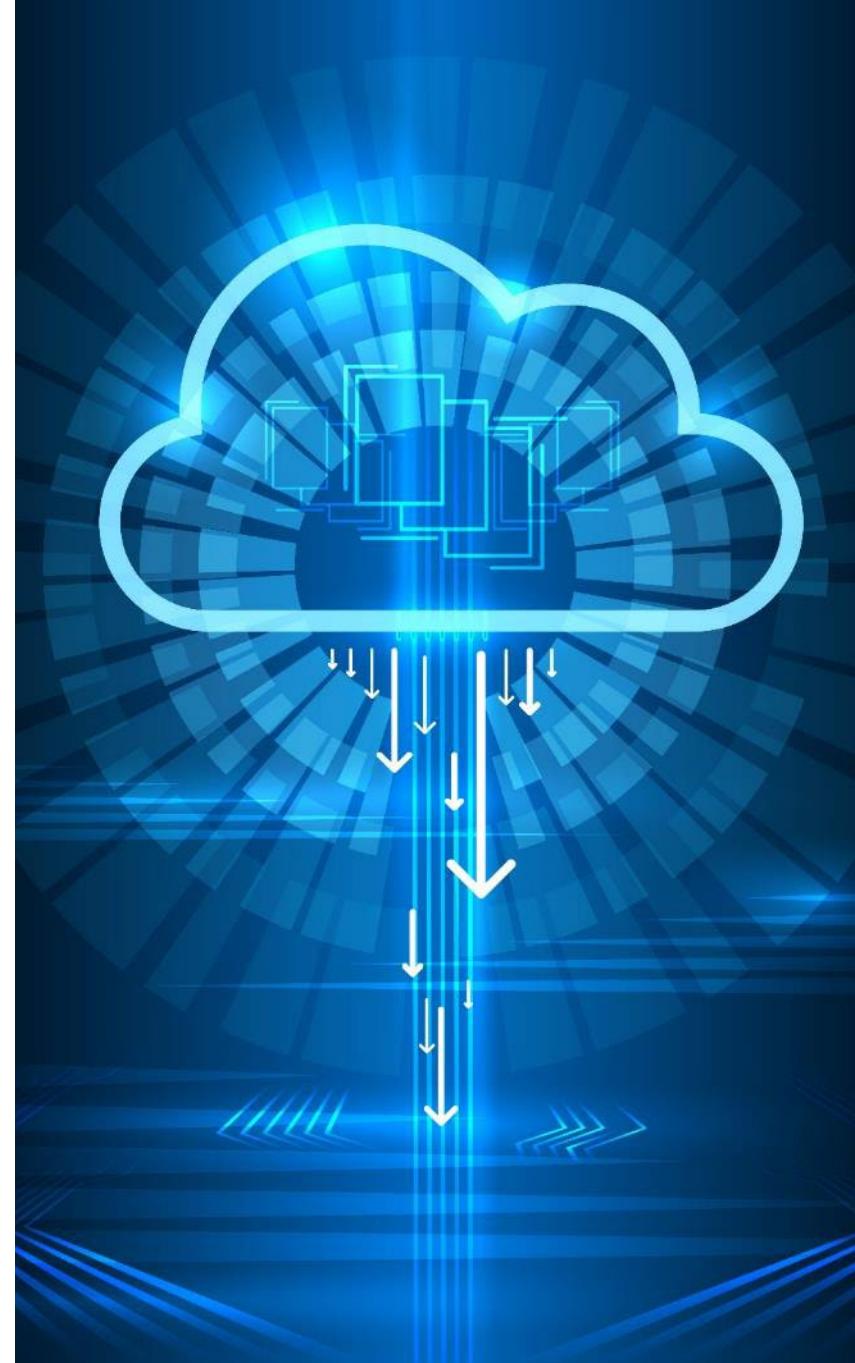


VM Issues

- ▶ **Virtual guests and hosts must be patched against threats, just like other OSes**
- ▶ **Attackers can leverage virtualization**
 - VM Escape techniques may allow VM users to gain access to the host
 - If the malware is running on the host at a higher administrative level than the guest system, then malicious code can evade detection
 - Controlling the host controls the virtual machines
- ▶ **VM Escape protection**
 - Sandboxing and segmentation
 - Implementing least privilege for guest operating systems and the hypervisors
- ▶ **Avoid VM Sprawl—creating more VMs than can be effectively managed**
 - Use standard libraries of images
 - Manage and track provisioning and deprovisioning with VM lifecycle management tools

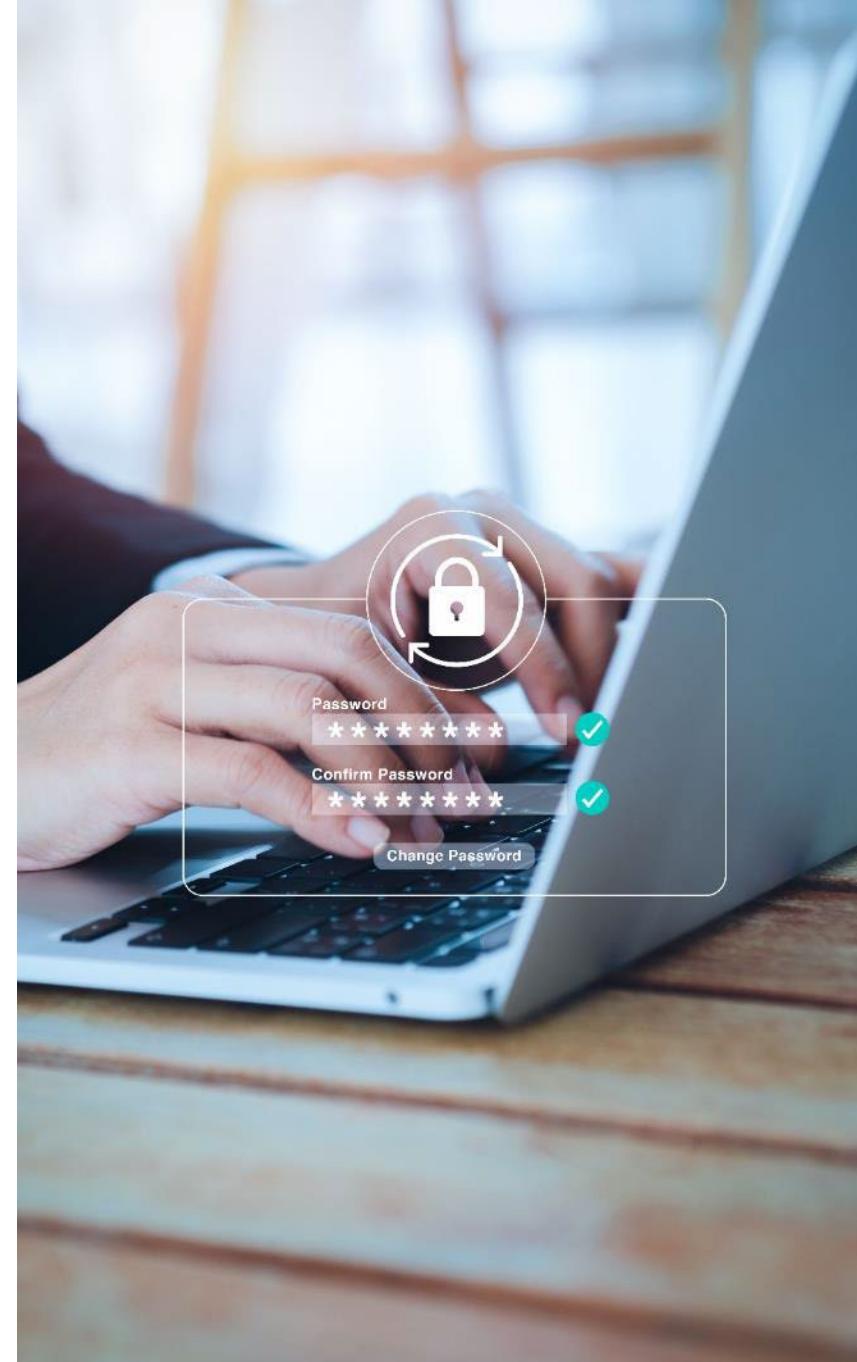
Cloud-Specific Vulnerabilities

- ▶ Inadequate Identity and Access Management
 - ▶ Data exposure
 - ▶ Shared technology
- * Note that cloud systems typically have most of the same vulnerabilities as traditional environments



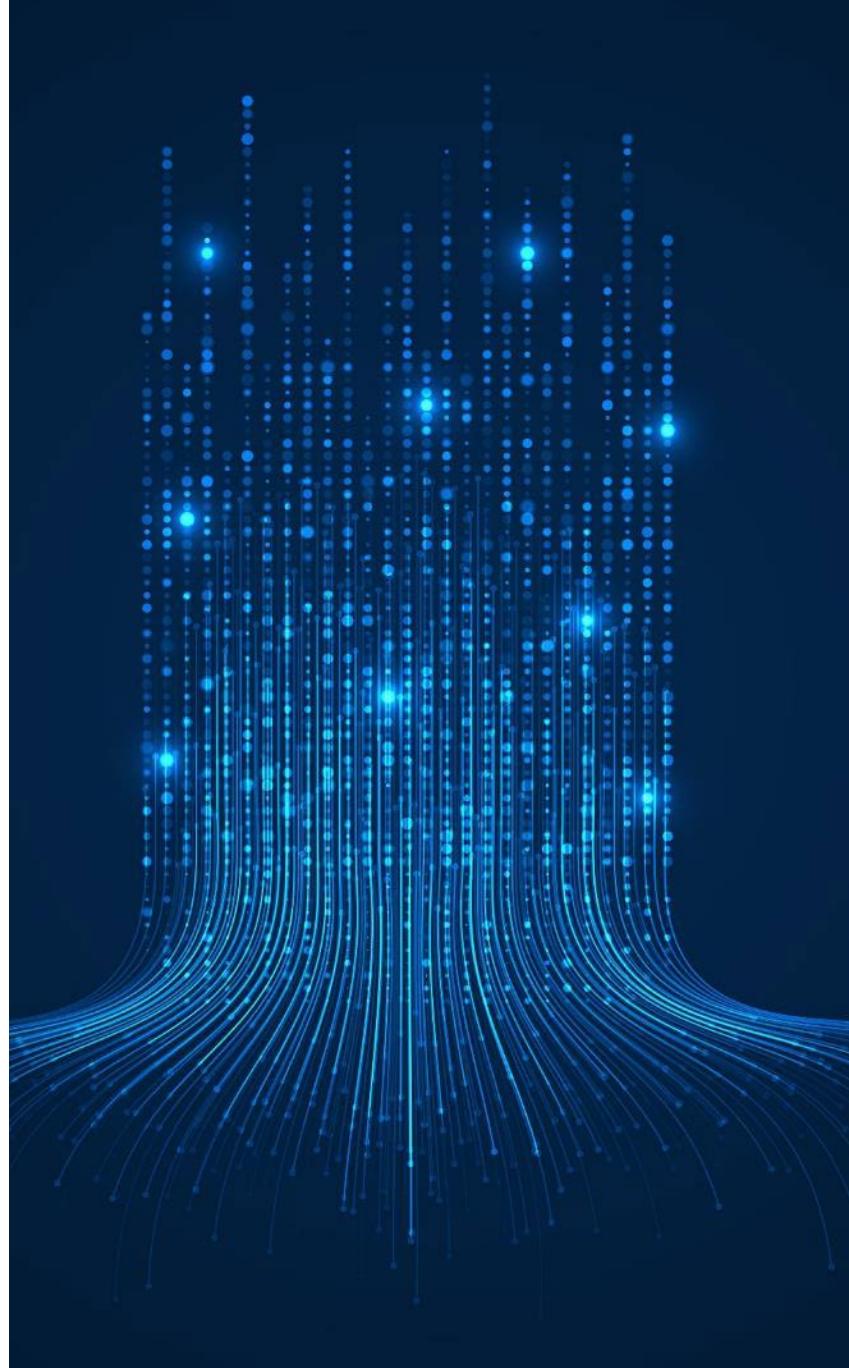
Identity and Access Management

- ▶ **Improperly configured access controls can lead to overprivileged users**
 - Allowing them to access sensitive data or resources they shouldn't have access
- ▶ **Weak passwords, lack of multi-factor authentication (MFA),**
 - This can make it easier for attackers to compromise cloud accounts



Data Exposure

- ▶ **The APIs used by customers to manage their cloud resources may introduce risk**
 - Insecure APIs can be exploited to gain unauthorized access or control
- ▶ **Poorly configured storage services, misconfigured cloud storage can lead to the exposure of sensitive data to the public internet**
 - It's essential to set proper access controls, encryption, and regular auditing of cloud storage configurations



Data Exposure

Demo

- 1. Go to the Demo PC**
- 2. In Firefox, connect to the Login Bookmark**
- 3. Ensure you are logged in as Adrian/somepassword**
- 4. Activate Firebug by pressing F12**
- 5. Move to the lower tab and choose Cookies**
- 6. Edit the one called UID and change the values from 1 to 3, to 4, to 5**
 - Meanwhile, refresh the browser between changes
- 7. What happens to the name of the account shown as logged in?**

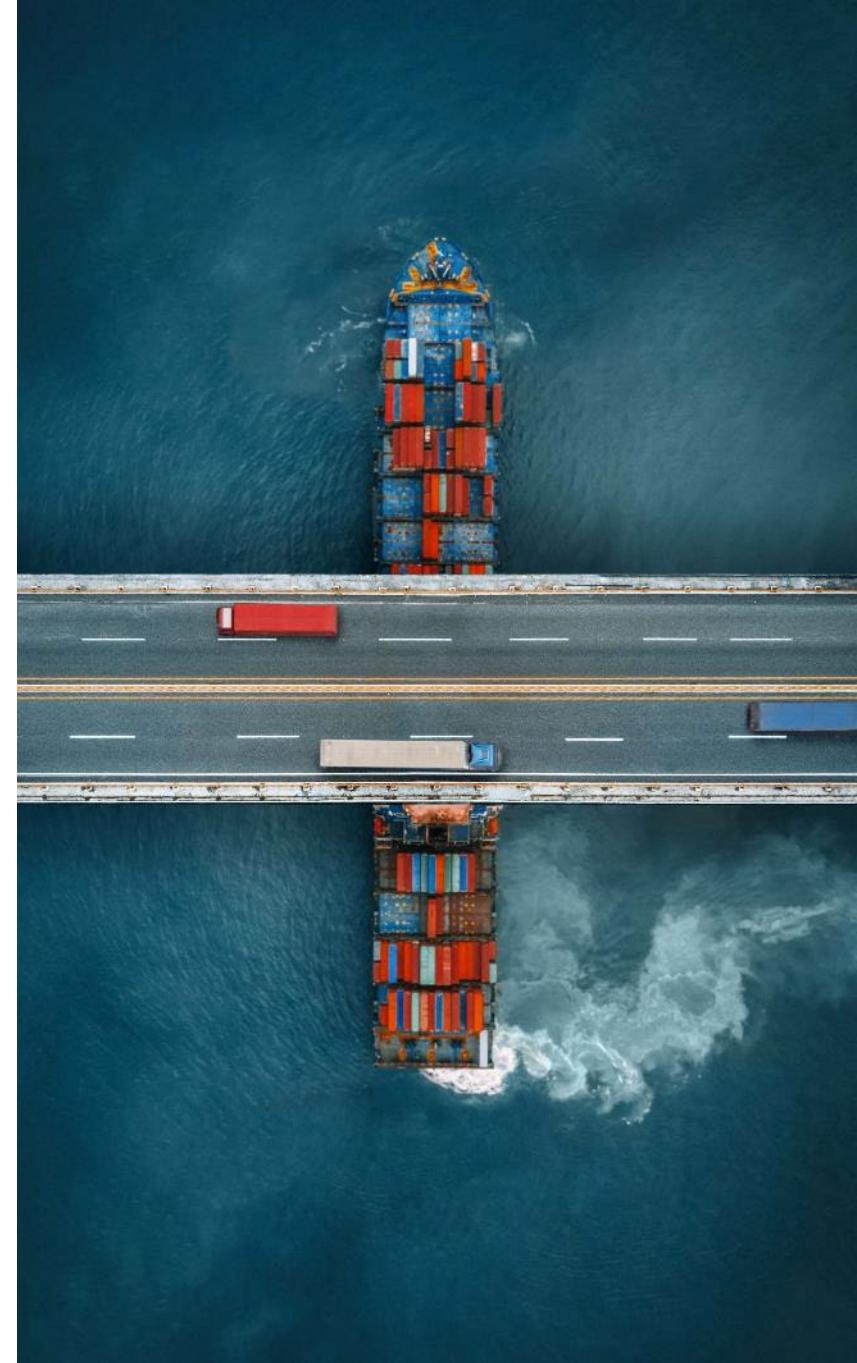
Shared Technology

- ▶ In a multi-tenant cloud environment, the use of shared resources can introduce issues
 - Vulnerabilities in the hypervisor can potentially be exploited to gain access to other's data and applications
- ▶ Virtualization vulnerabilities
 - Improper sandboxing or permissions may allow improper access or VM Escape
 - Audits, security patch management and hardening are essential to mitigate the risks

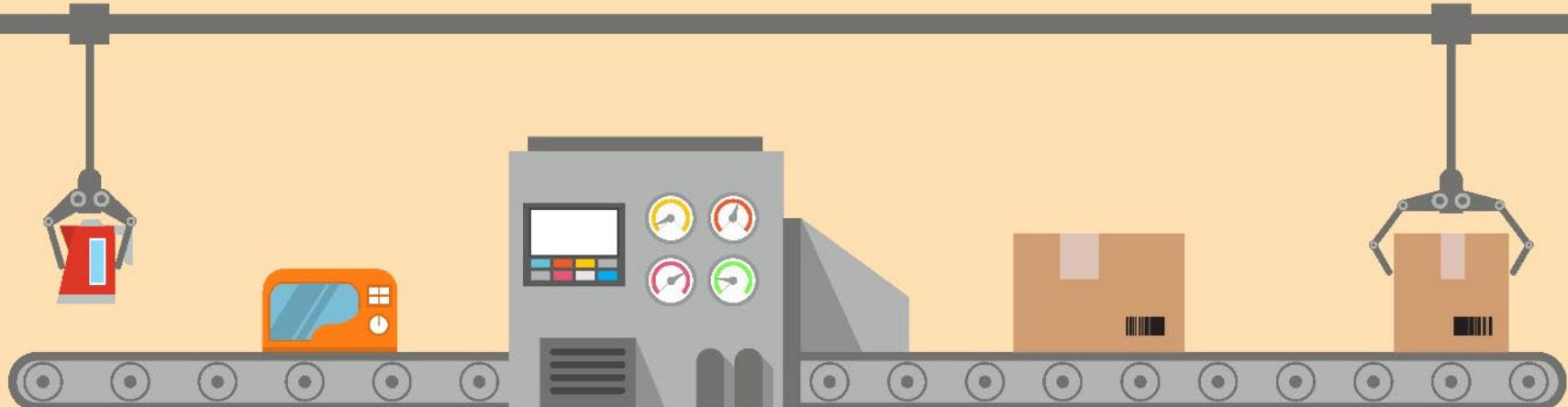


Supply Chain Concerns

- ▶ Espionage
- ▶ Vendor breach
- ▶ Poor patching or unresponsive vendors
- ▶ End of life



Espionage



► Breaches may occur due to:

- Product tampering by a supplier used by a vendor of a product or service you use
 - Target was breached via stolen credentials from an HVAC contractor
- Product tampering by the vendor itself
- Mistakes or malicious actions by consultants used by any suppliers
 - In 2015 OPM was breached due to lost credentials from a background check company
- Mistakes or malicious actions by your own staff or contractors
- Breaches at service providers, such as security, cloud, hosting, APIs

Improper and Weak Patching

► Patching may be complicated for

- 3rd parties that have gone out of business
- Unresponsive vendors
- Firmware that requires on-site or manual patching
- Legacy operating systems and applications often have no patching
- Complicated code



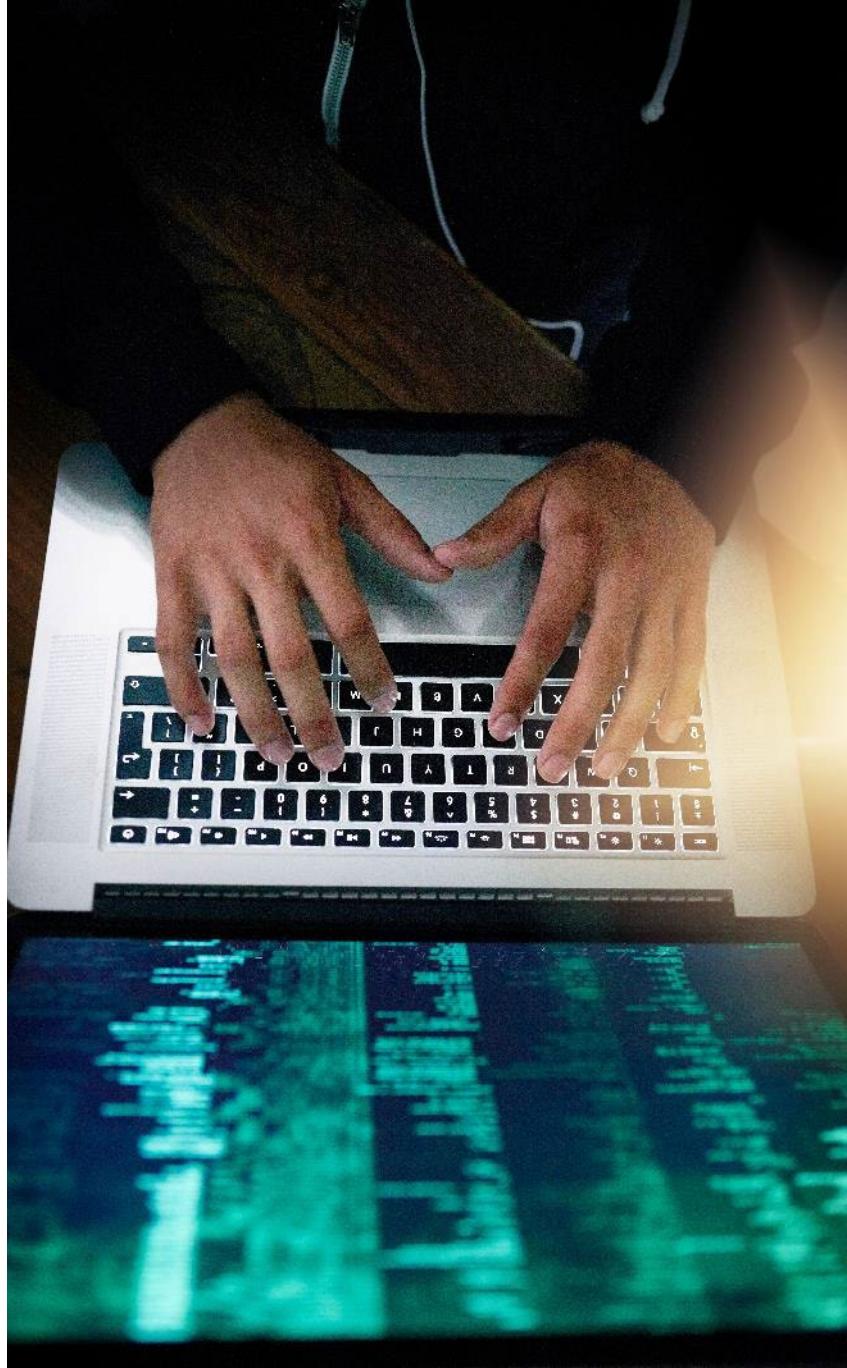
Third-party Software Risk

- ▶ **End-of-Life (EOL)**
 - No longer sold
 - When a product has reached the limit of its being useful to the vendor
- ▶ **End of Service Life (EOSL)**
 - When a product is no longer supported or maintained
- ▶ **Eventually software is phased out and patches no longer available**
 - Many banks used Windows 7 when other Windows versions were available (EOL)
 - They continued to use it, even though no patching was available (EOSL)



Cryptographic Failures

- ▶ Weak cipher suites
- ▶ Collision (shown earlier)
- ▶ Downgrade
- ▶ Replay
- ▶ Physical access and theft
- ▶ Password cracking



Weak Cipher Suites and Certificate Issues

- ▶ **Encryption and hashing algorithms are regularly deprecated due to errors, predictability, growing CPU strength**
- ▶ **Certificate and Key Management Issues**
 - Access, confidentiality and integrity failures may result
 - WEP has no key management, only a long-term key
 - WPA uses RC4, which is deprecated
 - Certificates and certificate authorities may use
 - Weak hash algorithms
 - MD5
 - SHA1
 - Servers and endpoints may support
 - SSL
 - RC4

Password Cracking Techniques

► Collision

- Fault in an algorithm, wherein the hash of two different files matches
- Show in Domain 1

► Downgrade

- SSL downgrade or SSL Stripping forces cleartext HTTP
 - Defended with HSTS
- At right, the PC Network Program 1.0 uses cleartext

```
+ Transmission Control Protocol, Src Port: 49
+ NetBIOS Session Service
- SMB (Server Message Block Protocol)
  + SMB Header
  - Negotiate Protocol Request (0x72)
    Word Count (WCT): 0
    Byte Count (BCC): 120
  - Requested dialects
    + Dialect: PC NETWORK PROGRAM 1.0
    + Dialect: LANMAN1.0
    + Dialect: Windows for Workgroups 3.1a
    + Dialect: LM1.2X002
    + Dialect: LANMAN2.1
    + Dialect: NT LM 0.12
    + Dialect: SMB 2.002
    + Dialect: SMB 2.???
```

Theft and Reuse Techniques

► Replay

- Encrypted credentials may be sniffed and captured and resent
- The attacker does not need to know the username or password

► Physical theft

- USB devices disguised as cables
- USB/flash drive keyloggers
- Access card cloning for doorways and cellular phones
- RFID and magnetic stripe card skimming



Password Cracking Techniques

- ▶ **Brute force**
 - Testing all combinations
 - ▶ **Dictionary attacks**
 - Using a large word list
 - ▶ **Hybrid**
 - Dictionary plus prepending and appending characters
 - ▶ **Spraying**
 - Using a single password across a wide range of accounts
 - ▶ **Birthday attacks**
 - A technique that involves many-to-many guessing to resolve a secret (e.g., if you ask 23 people their birthday, the odds are 50:50 that two will have the same date)
 - ▶ **Rainbow tables**
 - Use of precomputed password lists
 - Can guess even system-generated and random passwords
- 
- Defeated by intruder lock-out**

Pop Quiz: Identify the Attack

Access log

`https://server.com/?usr=john&pass=ltree`

`https://server.com/?usr=mary&pass=ltree`

`https://server.com/?usr=sue&pass=ltree`

`https://server.com/?usr=josef&pass=ltree`

`https://server.com/?usr=jason&pass=ltree`

`https://server.com/?usr=amy&pass=ltree`



Online Cracking vs. Offline Cracking

- ▶ **Online cracking involves connecting to a system and submitting credentials to test them**
 - Also called grinding and interactive
 - Very time-consuming
 - Easily defeated by intruder lock-out settings
 - No need to sniff to steal ciphertext credentials
- ▶ **Offline cracking involves sniffing or recording the ciphertext and testing it in another location**
 - Extremely fast
 - No intruder lock-out
 - Attacker must have a sample of the ciphertext credentials

Offline Hybrid Password Cracking

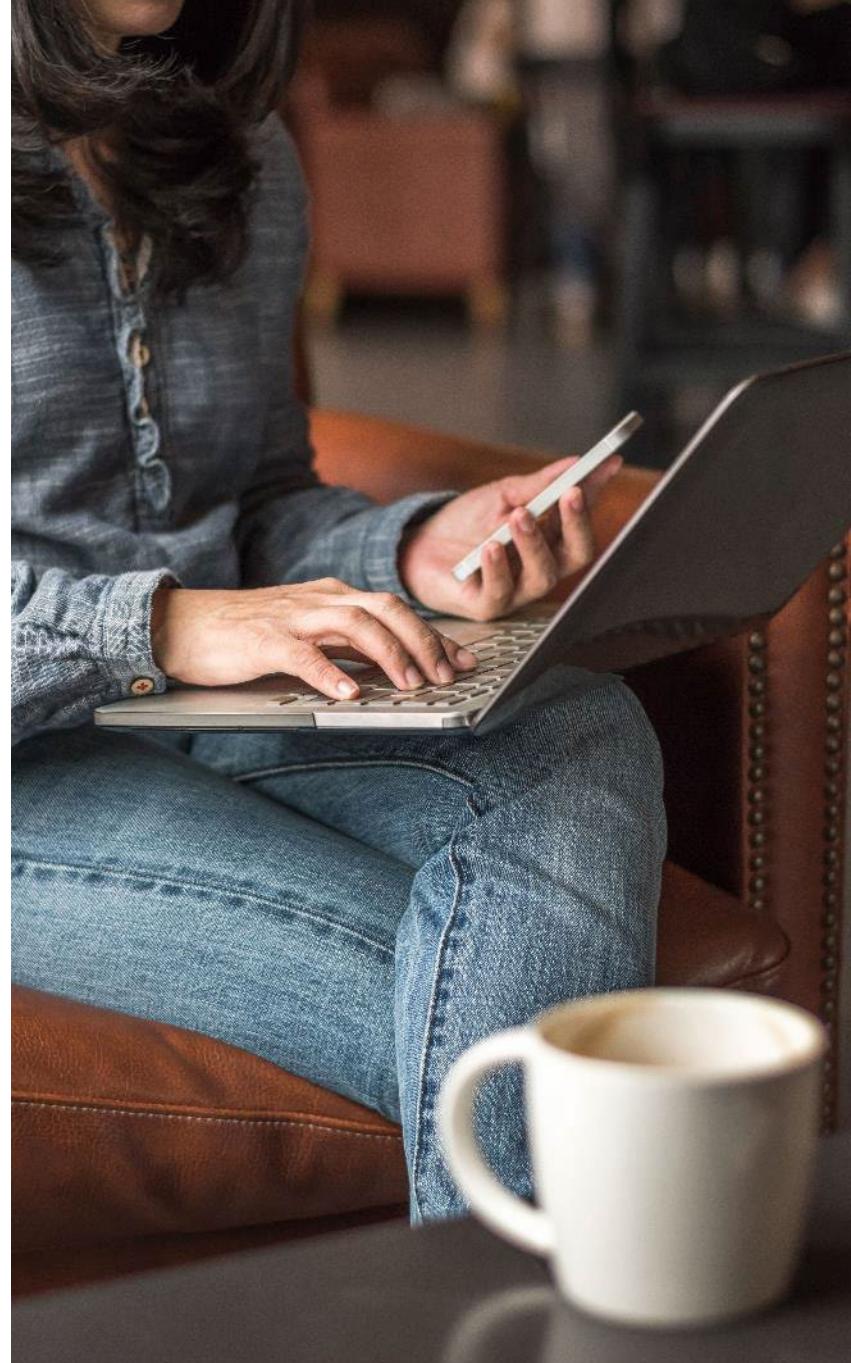
Demo

LCP is a password cracker—it guesses passwords by using a list, common suffixes/prefixes, and brute force

1. Credentials from another system have been saved to this machine for offline cracking. They include LANMAN passwords
2. Run LCP from the desktop
3. Select Import | Import from .LC File and choose PW-Dump-LANMAN.lc
4. Select Session | Options
5. On the “Dictionary attack” tab, make sure the Enabled checkbox is selected
6. If needed, place check marks next to “double word” and “reverse order” to ensure they are selected
7. On the “Hybrid attack” tab, make sure the Enabled checkbox is selected and click OK
8. Select Session | Begin Audit

Mobile Issues

- ▶ Loss/Theft
- ▶ Social engineering
- ▶ Rooting/Jailbreaking
- ▶ Sideload



Mobile

- ▶ To deploy mobile devices securely, many factors must be considered
- ▶ Mobile device threats
 - Loss, theft, tracking
 - Casual eavesdropping
 - Wiping
 - Applications
 - Intermingling organization and personal apps and data
- ▶ Social engineering is commonly performed using mobile devices as the vector
- ▶ BYOD will be discussed in Domain 4



Tablets, iOS, Android, and Smartphones

- ▶ **Cell phones have the potential for viruses, theft, eavesdropping, and interacting with internal networks**
 - Geo-tagging—using metadata in photos to track user activity and location
 - Infection by malware in smartphone apps
 - Cell phones may retrieve and store confidential emails
 - Intruders may connect rogue systems to internal networks to tap or interact with the local environment

Rooting and Jailbreaking

- ▶ **Gaining root or superuser-level access to an Android phone**
 - The user/owner no longer has restrictions for which apps to load or uninstall
 - May be used to
 - Install custom OS
 - Delete bloatware
 - May result in warranty being voided
 - Rogue software install/infestation
 - Poor performance
- ▶ **Jailbreaking is an IOS term for removing software restrictions imposed by Apple**
 - Allows unapproved apps
 - Additional customization
 - May allow insecure or dangerous applications to run

Sideload

- ▶ **Sideload** is often used for
 - Installing apps from third-party sources
 - Bypassing existing security controls
 - Installing hacking tools
- ▶ Organizations may detect or prevent this by implementing defensive tools
 - Mobile Device Management (MDM) software
 - Mobile Application Management (MAM)



Network Vulnerabilities

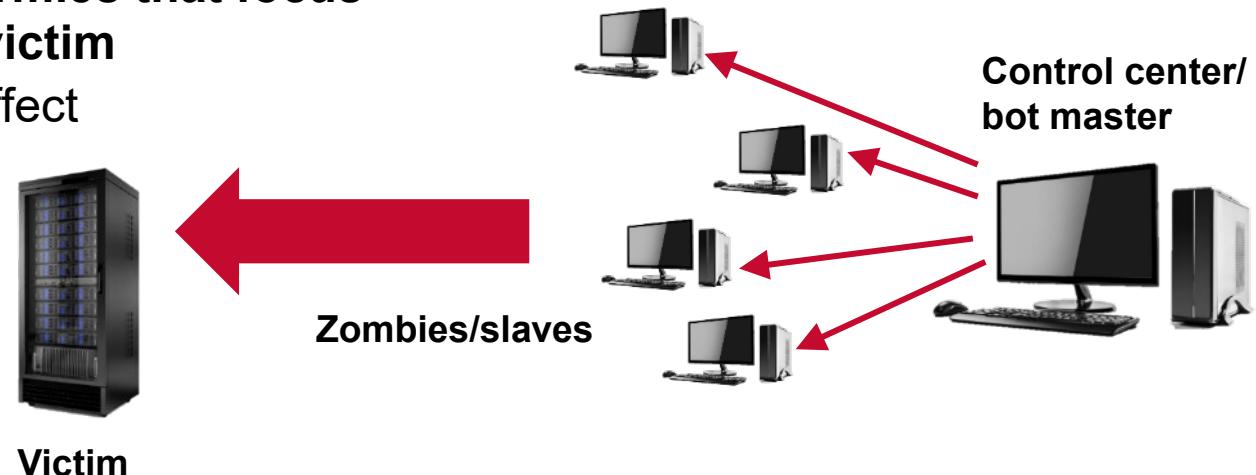
- ▶ **DoS and DDoS**
- ▶ **DNS and name resolution**
- ▶ **Wireless**
- ▶ **On-path, sniffing and flooding**
- ▶ **Replay**

DoS/DDoS

- ▶ **Denial of service is one-on-one attack**
 - Often by barrages of data and traffic
 - May be by a crafted packet that disables a service
 - SYN floods with half-open handshakes

- ▶ **Distributed denial of service**
 - Many-to-one relationship
 - The attacker controls armies of so-called agents, bots, or zombies
 - Often use IRC to communicate

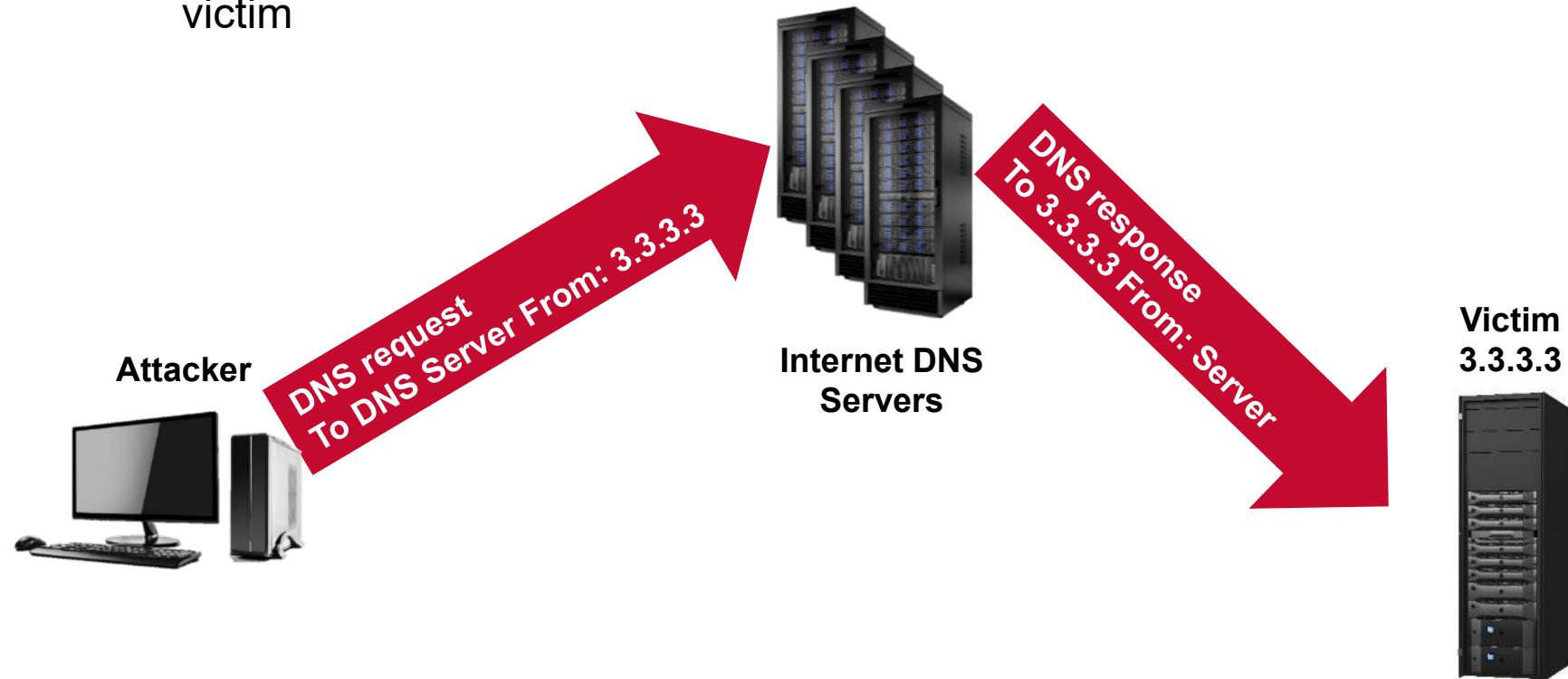
- ▶ **The botnets are armies that focus their attack on a victim**
 - Multiplies the effect



SYN = synchronize

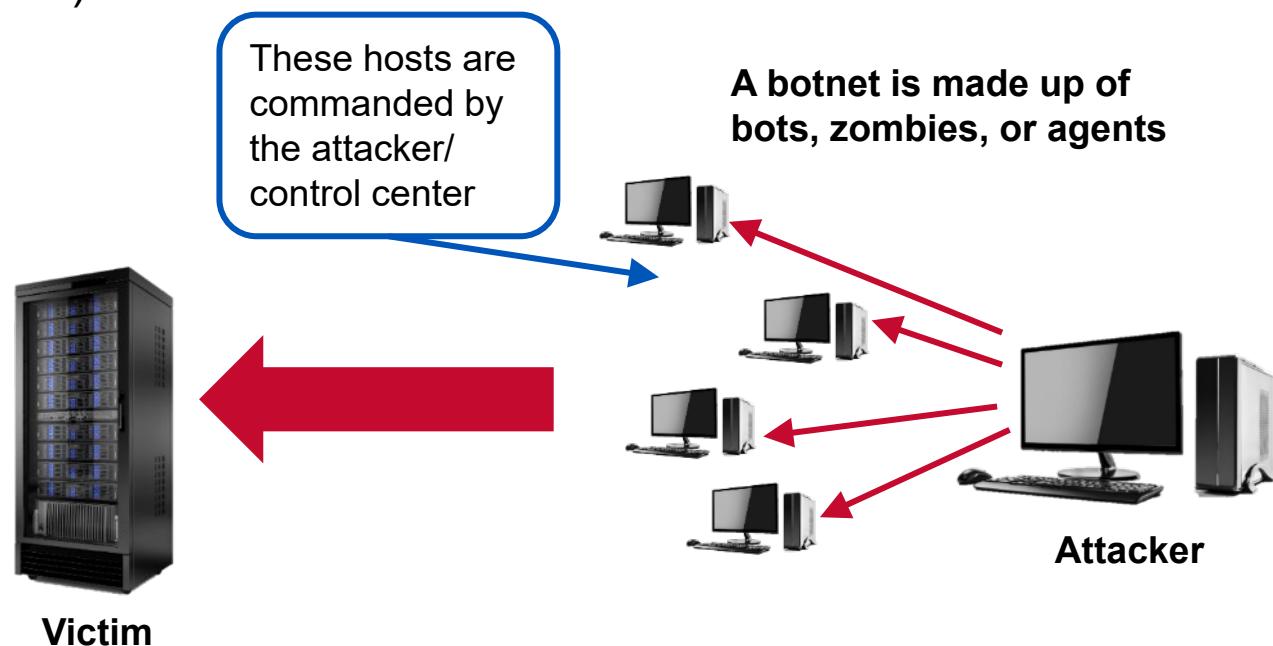
Amplification and Reflection

- An attack in which the attacker sends numerous small DNS requests for large results to a large range in Internet DNS servers
 - But the source IP address is the victim
 - Internet servers reply, sending a deluge of DNS responses that flood the victim



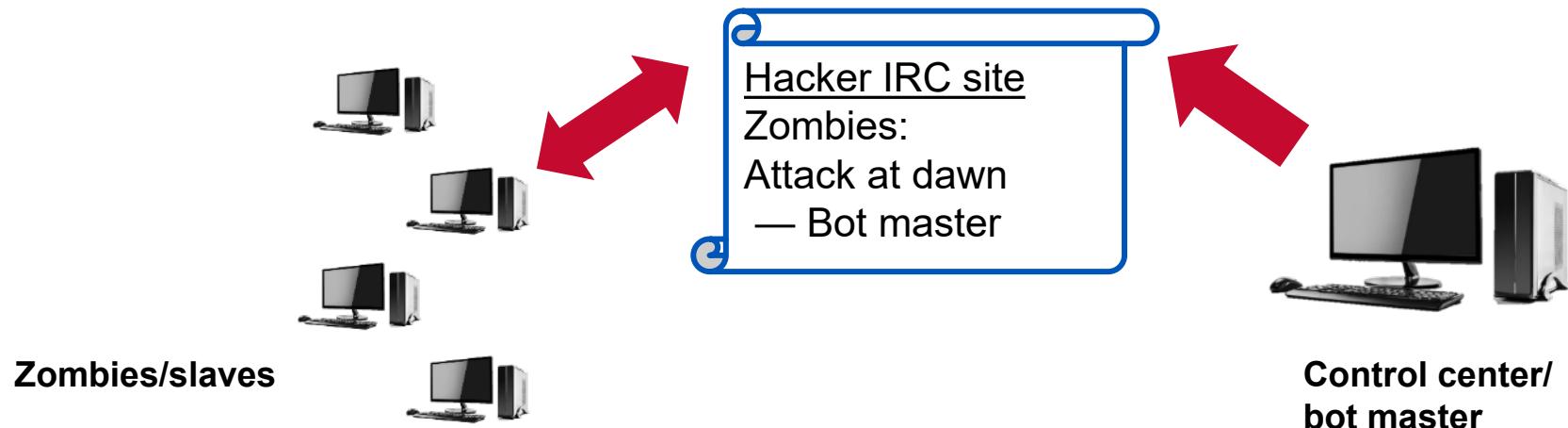
Backdoors, Zombies, and Botnets

- ▶ A backdoor is an illicit server that allows remote control of a host
 - Attackers often use covert or encrypted communication
 - Tunneling messages through DNS or HTTPS at odd hours of the day
 - Remote Access Tool (RAT) is another term for a backdoor
- ▶ May perform
 - Spamming (SPAMbot)
 - DDoS
- ▶ Examples
 - Poison Ivy
 - Storm
 - Conficker
 - Zeus



Zombie and Botnet Communication

- **Zombies and botnets receive instructions by covert messages from a control center or from a bot master, and act as a group**
 - Zombies connect to IRC or even to Google Docs sites periodically
 - Download new instructions
 - Covert communication may be tunneled over a protocol like DNS
 - Often off-hours
 - Covert messages are sometimes disguised to look like replies to bypass firewalls



IRC = Internet Relay Chat

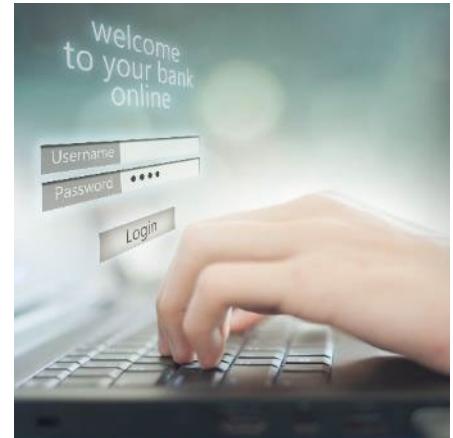
Domain Name Service

- The function of DNS is typically to resolve a name to an IP address
 - IP packets use addresses, not names
- We trust DNS implicitly to guide us to a desired site
 - What would happen if DNS could be controlled by an attacker?



Hacker running a
rogue server

<http://www.bank.com/>



Your online bank



DNS Threats

- ▶ **DNS may be compromised and cause users to be redirected to bogus sites and once there, they may reveal their credentials**
 - This is called *pharming*
- ▶ **Attacks**
 - Domain hijacking or domain theft is falsely changing the registrations of a domain name without the permission
 - Perform malicious redirection of many users
 - DNS poisoning and pharming
 - Poisoning an organization's server can redirect all of its users and systems. Can be mitigated with DNSSEC
 - Modified hosts file
 - Overrides DNS and can point a client to an incorrect address
 - URL redirection
 - Redirecting users to a watering hole page
 - Domain reputation
 - A scoring system that, if manipulated, can cause DoS and mail to be classified as Spam

Name Resolution Attack

- 1. Go to the instructor machine**
- 2. Open a command prompt and ping cnn.com
*(Note the address shown)***
- 3. On the Desktop, double-click the shortcut to the host's file**
- 4. Add to the end:
10.1.1.254 cnn.com
Save the file.**
- 5. Repeat the ping to cnn.com and note the new address.**

Wireless Attacks

► Rogue wireless Access Point (AP)

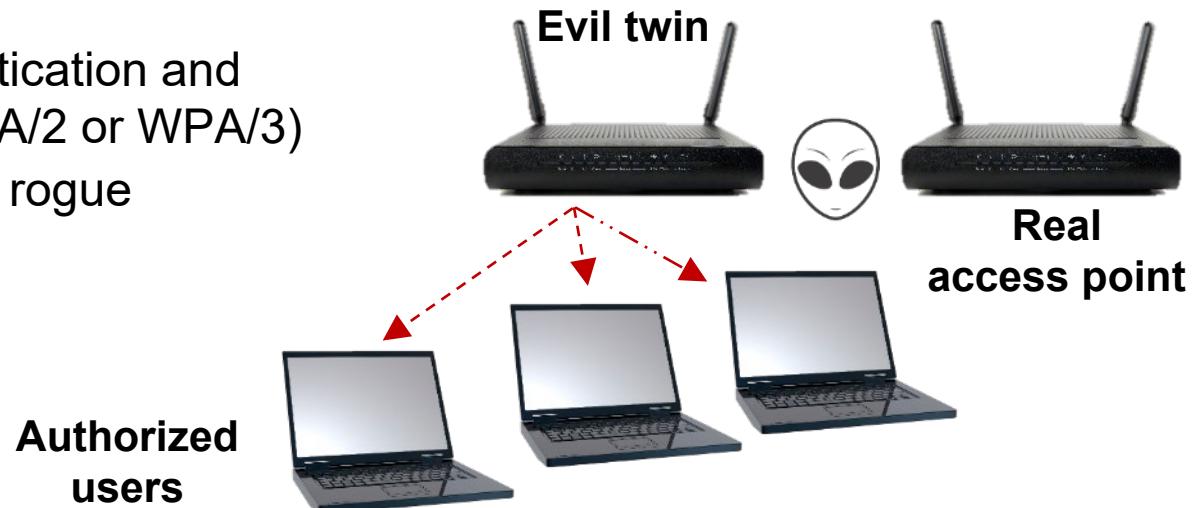
- An AP set up by rebellious employees, likely with poor security settings

► Evil twin

- A fake access point used to redirect, intercept, and eavesdrop on traffic
- Sends Disassociate messages to bounce users from real access point
- Provides a stronger signal to attract them

► Defenses

- Require authentication and encryption (WPA/2 or WPA/3)
- Track down the rogue access point



WPA = Wi-Fi protected access

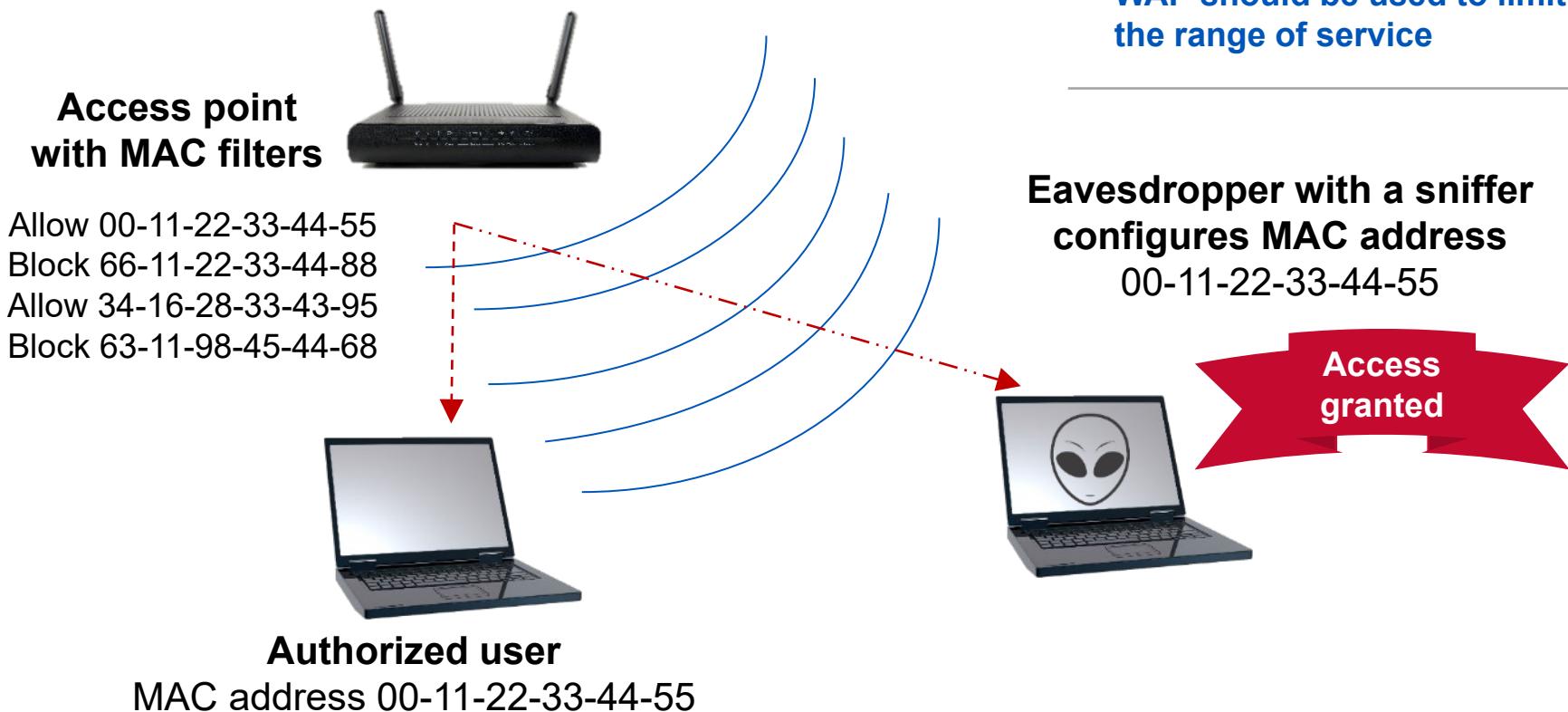
Jamming and Disassociation

- ▶ Jammers for cellular and 802.11 signals are relatively easy to obtain
 - Homemade kits
 - Stand-alone devices
 - Smartphone apps
 - Illegal without a license
- ▶ Disassociation is used to gain access to credentials for later cracking
 - The attacker sends a signal to the wireless clients to disassociate—disconnect from the WLAN
 - Each node detaches
 - The attacker sniffs and looks for new authentication exchanges
 - Clients re-connect, sending their encrypted credentials
 - The secrets are recorded and cracked later off-line at high-speed



Sniffing and Cloning MAC Addresses

- ▶ Without encryption, attackers are able to easily sniff the network with a protocol analyzer to identify the Media Access Control (MAC) address of an authentic client and spoof that address
- ▶ This allows the attacker to gain full access



Switch Flooding

- ▶ A wide array of attacks can be staged against clients, servers, and the infrastructure
 - MAC flooding
 - Sniffing
 - Man-in-The-Middle (On-path attack)
 - DoS and DDoS
- ▶ MAC flooding fills a switch table till new messages are sent to all ports

Switch Interface table

Port/VLAN	Physical Address	Type
IF 1 VLAN 2	45-de-12-09-46-fe	dynamic
IF 1 VLAN 2	98-de-76-cd-46-ac	dynamic
IF 1 VLAN 2	08-56-23-98-46-be	dynamic
IF 1 VLAN 2	28-de-89-cd-46-ea	dynamic
IF 1 VLAN 2	94-de-d0-73-46-0a	dynamic
IF 1 VLAN 2	97-de-d0-ed-46-3b	dynamic
IF 1 VLAN 2	68-de-d0-ac-46-ec	dynamic

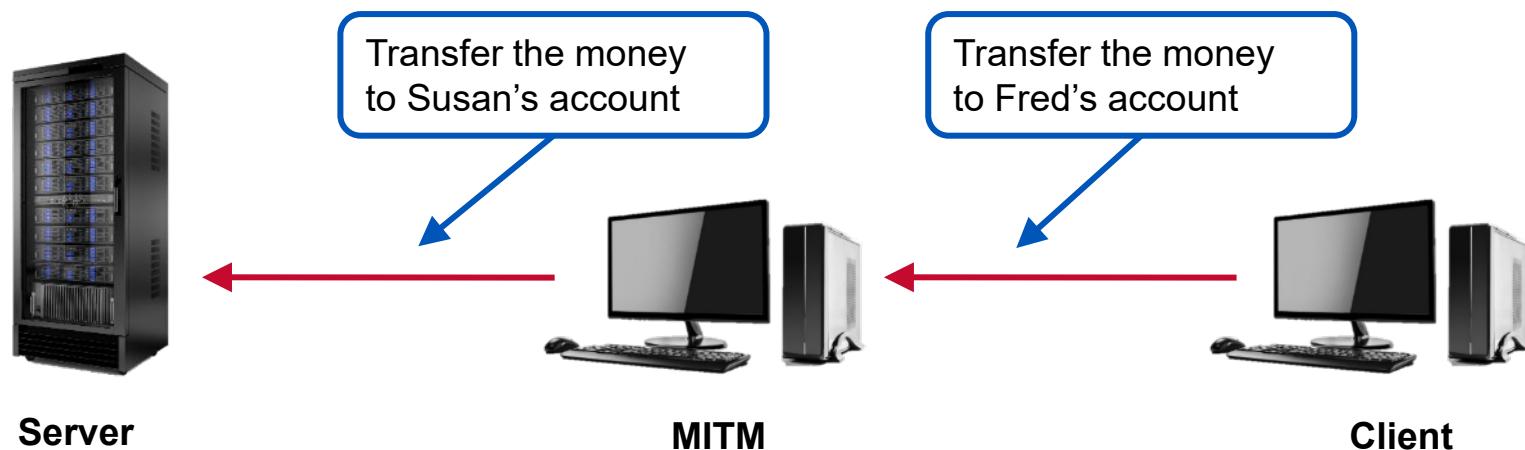
Sniffing FTP

Demo

- 1. Start Wireshark and begin capturing data**
- 2. Enter ftp as the filter and Apply**
- 3. Open a command prompt**
- 4. Enter: ftp 10.1.1.254**
- 5. Enter any username and password
(They may not work)**
- 6. Return to Wireshark**
- 7. What were the credentials entered by the instructor?**

Man-in-the-Middle (On-path)

- ▶ **Attacker sniffs the network, then intercepts and modifies packets in a conversation**
 - Convinces the client and the server to send packets to the attacker
 - Commonly used to attack Telnet, HTTP, FTP, and wireless networks
- ▶ **The MITM spoofs being the client and server to accomplish TCP hijacking**
- ▶ **Use of Message Authentication Codes (MACs), encryption, certificates, and other strong authentication makes attacking more difficult**

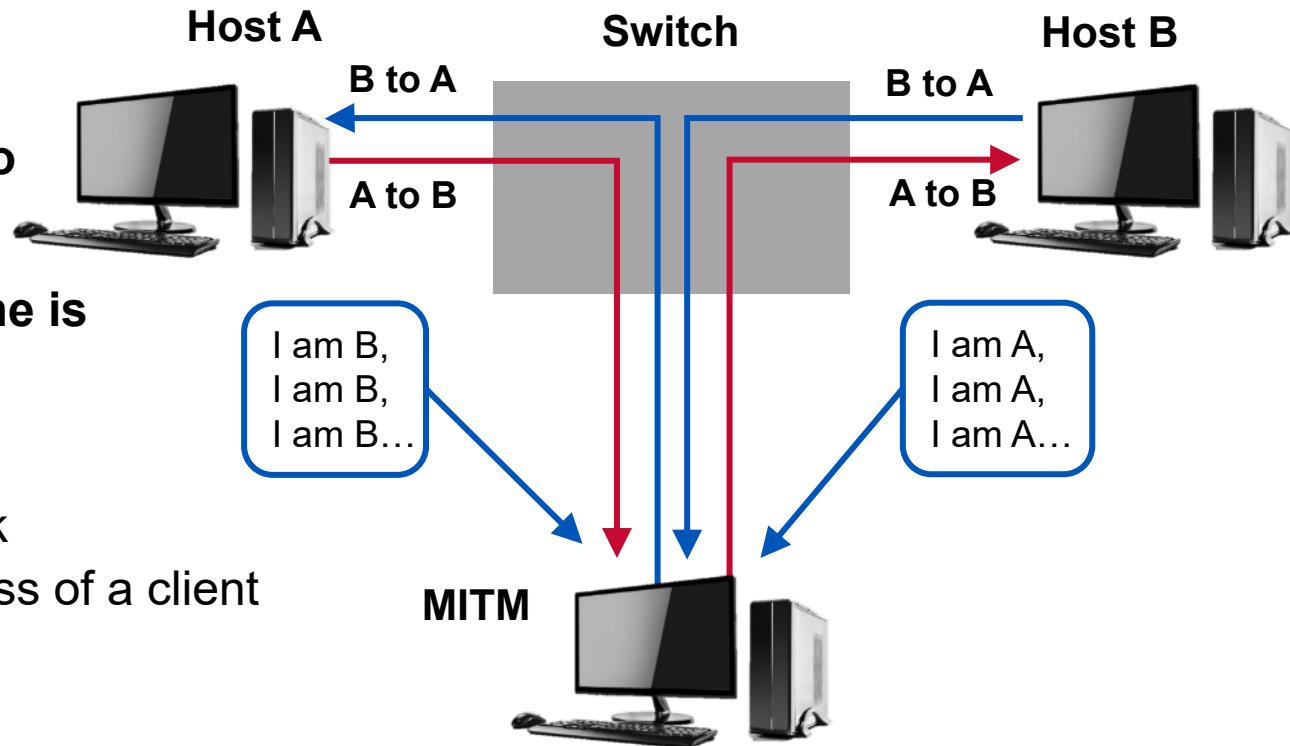


HTTP = Hypertext Transfer Protocol
MITM = man-in-the-middle

TCP = Transmission Control Protocol

ARP Poisoning/Spoofing

- ▶ Numerous ARP resolution messages are sent to endpoints
 - Poisoning switch ARP can allow data hijacking
- ▶ Data forwarded to the MITM is under its control
 - Eavesdropping
 - Modification
 - DoS
- ▶ Repeating frames to the wrong ports
- ▶ Disabling ARP cache is a form of defense
- ▶ This MITM attack
 - Sniffs the network
 - Spoofs the address of a client and server



VLAN = virtual local area network

Domain 2: Match the Items to the Topics

Do Now

Item	Answer	Topic
Fake AP		A. C2
Target breach		B. Keylogger
Defenseless		C. Jailbreak
Distributed Denial of Service		D. Traversal
.../.../.../.../...		E. Malicious update
Discovered via malvertisizing		F. Evil twin
IOS Unapproved		G. Supply chain
Found USB		H. Embedded systems

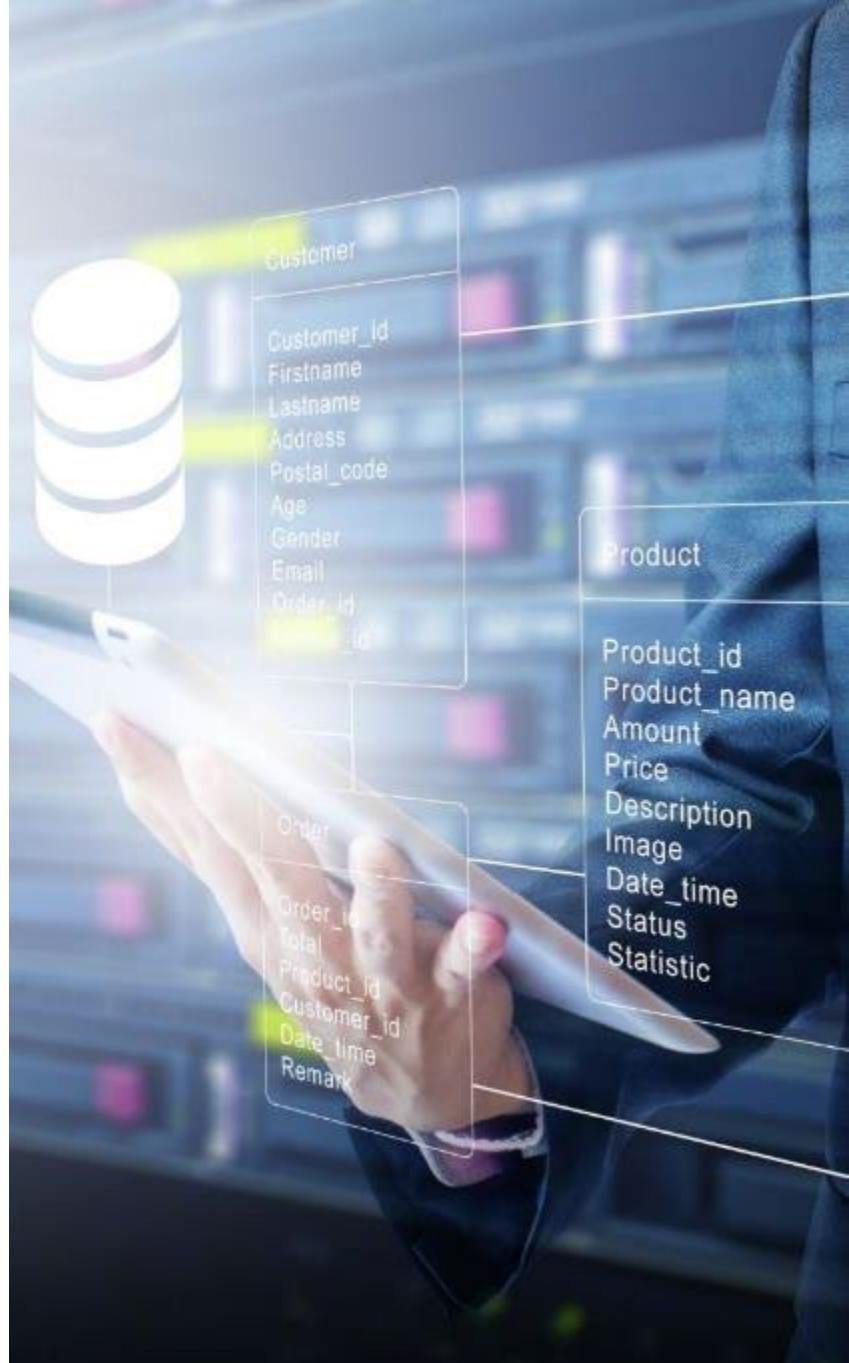
For each item on the left, write in the corresponding letter from a topic on the right

Contents

- ▶ Threat Actors
- ▶ Vectors and the Attack Surface
- ▶ Vulnerabilities and Attacks

Malware

- ▶ Indicators and Mitigation



Malware Threats to Security

- The following represents an array of software threats and types of exploits (the list is not comprehensive)
 - Ransomware
 - Trojan
 - Worm
 - Spyware
 - Bloatware
 - Virus
 - Keylogger
 - Logic bomb
 - Rootkits
- They vary in terms of
 - Typical actions
 - Intent
 - Spreading
 - Maliciousness



Ransomware

► Ransomware

- Removes or encrypts data, to be returned when a ransom is paid
- Made via Bitcoin (e.g., WannaCry, CryptoLocker)

► Depending on the attacker

- Paid ransom typically results in data access being returned
- No guarantee

► Once a recovery has been made, all systems should be scanned for residual malware

► Hoaxes

- May use false or alarming messages to extort money from a victim
- A hoax designed to obtain money



Trojan Horses

- ▶ **Malicious code that is inserted into good or benign code**
 - The content is *assumed* to be trustworthy, but it is not
 - A cool screen saver that destroys files
- ▶ **Malicious browser add-ons are a common vector to install malware and requires a user to activate it**
 - USB drives
 - Free games
 - Wallpapers
 - Customized image content viewers
 - Browser search-bar tools
- ▶ **Spyware and adware are commonly installed via this method**



Worms

- ▶ **Processes that self-replicate and spread from one computer to another via a network**
 - Morris Internet worm
 - Code Red
 - SQL Slammer
 - MSBlaster
- ▶ **Typically require no user interaction**
 - Self-activating, self-propagating
- ▶ **Usually do no direct harm, but they replicate at enormous speed**
 - Saturating bandwidth with emails or packets, creating a denial of service (DoS)



SQL = structured query language

Worm Propagation

- 1. Double-click the desktop icon nachi-worm.cap**
 - A. Wireshark will open and display more than 2,000 frames
- 2. Go to the bottom of the trace file**
- 3. Note that these frames were all sent within 14.17 seconds (second column)**
- 4. There are two systems in the trace file, each sending a series of ICMP ping messages**

ICMP = Internet Control Message Protocol

Spyware/Adware

► Spyware

- Typically installed on a user's machine via browser
 - Much of it is user-installed, with voracious license conditions
 - Results in dramatic CPU utilization increase
- Reads persistent cookies to spy on browsing history
- Highly evasive—polymorphic
- Can be difficult or impossible to remove

► Crimeware: steals account data

► Adware

- Results in recurrent browser pop-ups and numerous email solicitations



Bloatware

- ▶ **Bloatware is unwanted software that is**
 - Pre-installed
 - Of limited or insufficient use
 - Not easily removed
- ▶ **Most associated with Windows and Mobile devices**
 - A source of frustration
 - May introduce malware or vulnerability
- ▶ **Some users will attempt to jailbreak or root their devices to remove it**

Viruses

- ▶ **Require user interaction for activation and replication**
- ▶ **Spread code that resides on a medium**
 - Often delivered by download or removable media
- ▶ **Cause damage or alteration to occur to a single host (they attempt to spread)**
- ▶ **Armored viruses are designed to resist reverse engineering and analysis**
- ▶ **Fileless viruses first appeared in 2017 and would take advantage of an existing application, manipulating memory to perform actions**
 - No written trace—low observable characteristics
- ▶ **Defend with antivirus to stop spreading**

Rootkits and Covert Activities

► Steganography

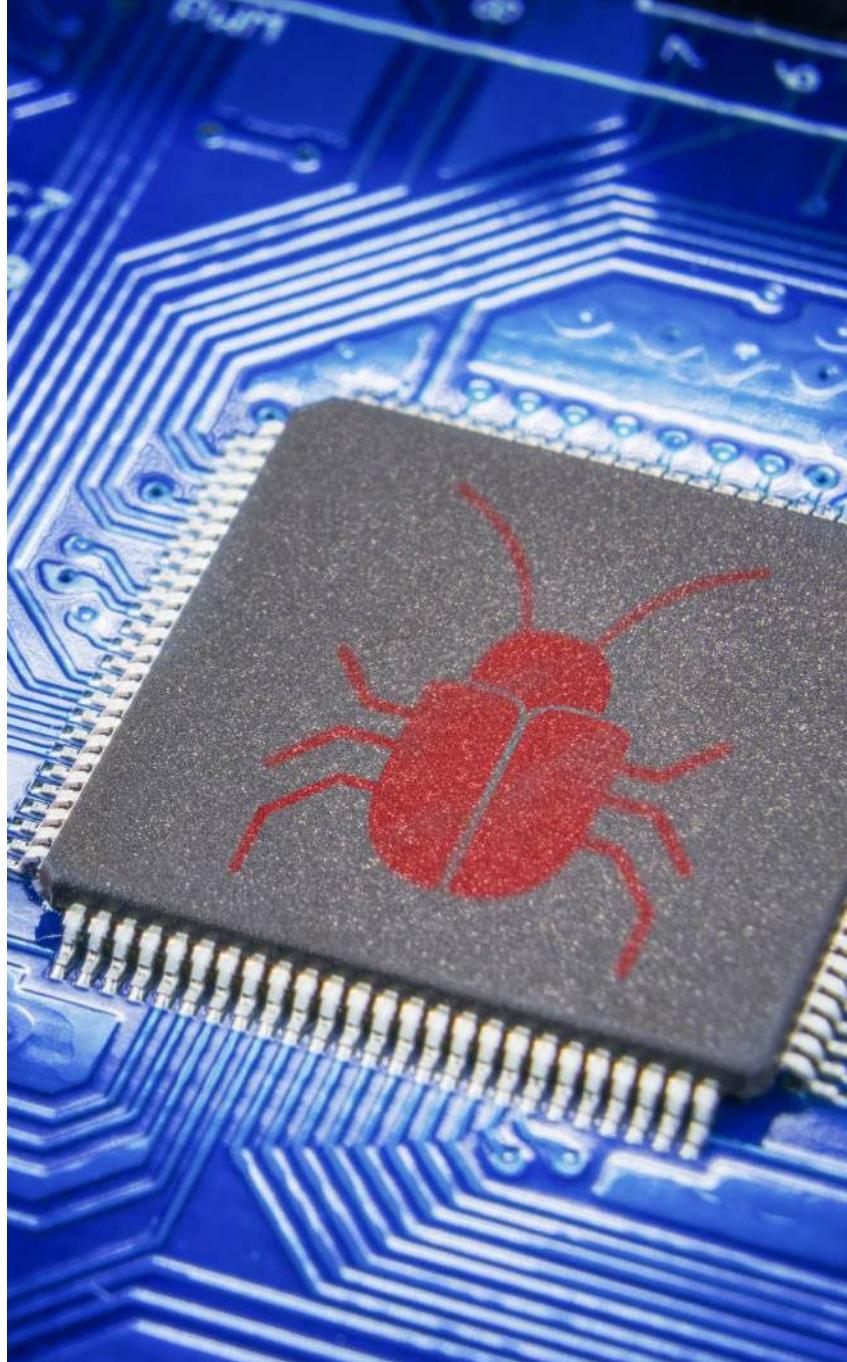
- Hiding a program or message inside an image
- Encoding message or a malicious program into the least significant bits
- Results in some image degradation

► Keyloggers

- May be hardware or software based

► Rootkit

- A program that allows attackers to hide or mask files, processes, and accounts from defensive applications
- Does not spread; installed individually



DLL = dynamic link library

Logic Bombs

- ▶ **Can be specialized code or virus-like**
 - Wait for a particular activity or date/time
- ▶ **Execute the payload or start spreading**
 - For example, a bank programmer could insert code that steals money every time interest is calculated—a rounding rip-off (e.g., Friday the 13th virus family)
- ▶ **Logic bombs do not require communication with the attacker, backdoors do**
 - These are inserted by malicious insiders
 - The greatest area of threat



Contents

- ▶ Threat Actors
- ▶ Vectors and the Attack Surface
- ▶ Vulnerabilities and Attacks
- ▶ Malware

Indicators and Mitigation



Indicators

► The term best applied is Indicator of Compromise (IoC)

- Account lockout
- Concurrent session usage
- Impossible travel
- Resource consumption
- Resource inaccessibility
- Blocked content
- Out-of-cycle logging
- Missing logs
- Published/document signatures



► Depending on the attack and target, these may appear in

- Network traffic
- Logs
- Page content

IoC: Account-Related

► **Account lockout**

- Defends against all online password guessing
 - But, not spraying

► **Concurrent session usage and impossible travel**

- Account password compromise
- XSS session theft
- Pass the Hash attack against SMB with:
 - Mimikatz
 - Crackmapexec
- Using anonymizer or proxy

► **Blocked content—by proxy or secure web gateway**

- Insider abuse
- Hacking attempts
- Attempting exfiltration

IoC: Resources

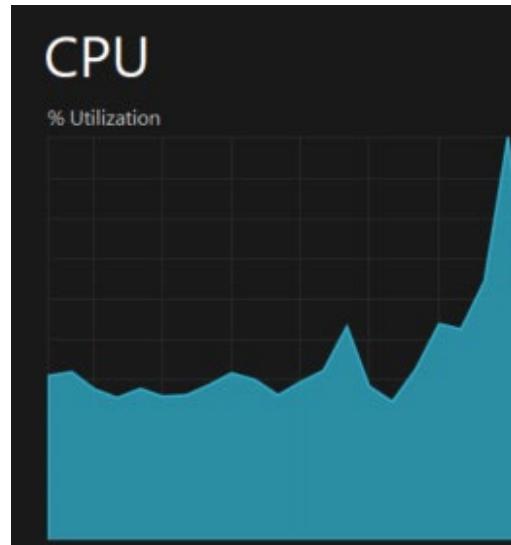
► Resource consumption (Disk, bandwidth, network, TCP connections)

- Spyware
- DoS/DDoS

► Resource inaccessibility

- DoS/DDoS
- Ransomware

```
C:\Users\fred> netstat -an | findstr "EST"
TCP    192.168.1.125:49411      20.25.241.18:443      ESTABLISHED
TCP    192.168.1.125:49793      52.109.8.89:443      ESTABLISHED
TCP    192.168.1.125:49799      52.109.4.19:443      ESTABLISHED
TCP    192.168.1.125:51376      44.209.24.18:443      ESTABLISHED
TCP    192.168.1.125:51440      31.13.66.4:443      ESTABLISHED
TCP    192.168.1.125:51452      31.13.66.4:443      ESTABLISHED
TCP    192.168.1.125:51826      34.117.65.55:443      ESTABLISHED
TCP    192.168.1.125:51830      20.25.241.18:443      ESTABLISHED
TCP    192.168.1.125:52134      44.227.32.98:443      ESTABLISHED
TCP    192.168.1.125:52216      3.162.112.51:443      ESTABLISHED
TCP    192.168.1.125:52229      20.42.73.24:443      ESTABLISHED
TCP    192.168.1.125:52246      52.109.16.96:443      ESTABLISHED
TCP    192.168.1.125:52266      13.107.6.158:443      ESTABLISHED
TCP    192.168.1.125:52267      20.75.60.91:443      ESTABLISHED
TCP    192.168.1.125:52268      20.42.73.26:443      ESTABLISHED
TCP    192.168.1.125:52272      18.210.53.80:443      ESTABLISHED
TCP    192.168.1.125:52276      3.93.126.174:443      ESTABLISHED
```



IoC: Logging

- ▶ **Out-of-cycle logging**
 - A defensive measure where logging is triggered (manually or automatically) in response to an event
 - After-hours/insider abuse
 - Attempts at stealth
- ▶ **Missing logs**
 - System compromise
 - Attempts at stealth
 - Insider abuse
 - Outsider abuse



IoC: Published or Known

► Buffer overflow

- 0x90 0x90 0x90 0x90 0x90 0x90
- Multiple Hex 90 (Assembler NOP pattern) in data

► Syn Flood

- Rapid, no replies,
single destination port

No.	Time	Source	Destination	Protocol	Length	Info	Seq=0 Win=512 Len=0
1	0.0000000000	1.2.3.4	10.10.1.254	TCP	54	2294 → 80 [SYN]	Seq=0 Win=512 Len=0
2	0.000041700	1.2.3.4	10.10.1.254	TCP	54	2295 → 80 [SYN]	Seq=0 Win=512 Len=0
3	0.000053212	1.2.3.4	10.10.1.254	TCP	54	2296 → 80 [SYN]	Seq=0 Win=512 Len=0
4	0.000062604	1.2.3.4	10.10.1.254	TCP	54	2297 → 80 [SYN]	Seq=0 Win=512 Len=0
5	0.000071692	1.2.3.4	10.10.1.254	TCP	54	2298 → 80 [SYN]	Seq=0 Win=512 Len=0
6	0.000088785	1.2.3.4	10.10.1.254	TCP	54	2299 → 80 [SYN]	Seq=0 Win=512 Len=0
7	0.000087615	1.2.3.4	10.10.1.254	TCP	54	2300 → 80 [SYN]	Seq=0 Win=512 Len=0
8	0.001762919	1.2.3.4	10.10.1.254	TCP	54	2301 → 80 [SYN]	Seq=0 Win=512 Len=0
9	0.001766397	1.2.3.4	10.10.1.254	TCP	54	2302 → 80 [SYN]	Seq=0 Win=512 Len=0
10	0.001769572	1.2.3.4	10.10.1.254	TCP	54	2303 → 80 [SYN]	Seq=0 Win=512 Len=0
11	0.001770239	1.2.3.4	10.10.1.254	TCP	54	2304 → 80 [SYN]	Seq=0 Win=512 Len=0
12	0.001772624	1.2.3.4	10.10.1.254	TCP	54	2305 → 80 [SYN]	Seq=0 Win=512 Len=0

► On-Path/MiTM

- ARP table shows two IP sharing one MAC address

192.168.1.1	f8-ac-78-1e-12-a5	dynamic
192.168.1.101	f8-ac-78-1e-12-a5	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static

► Switch Flooding

- Switch MAC tables show 1,000,000s of entries on one port

Port/VLAN	Physical Address	Type
IF 1 VLAN 2	45-de-12-09-46-fe	dynamic
IF 1 VLAN 2	98-de-76-cd-46-ac	dynamic
IF 1 VLAN 2	08-56-23-98-46-be	dynamic
IF 1 VLAN 2	28-de-89-cd-46-ea	dynamic
IF 1 VLAN 2	94-de-d0-73-46-0a	dynamic
IF 1 VLAN 2	97-de-d0-ed-46-3b	dynamic
IF 1 VLAN 2	68-de-d0-ac-46-ec	dynamic

IoC: Well-known Indicators

- ▶ Certain attacks display known patterns or leave identifiable artifacts
- ▶ Web
 - Directory traversal Logs or network traffic
.../.../.../.../.../ or %2e%2e%2f%2e%2e%2f
 - CSRF Page content or network traffic
https://server.com?account=1234&action=buy
Look for a URL that indicates a transaction is underway
 - XSS Page content or URL with
<script> tags where user data should be
 - SQLi Logs or network traffic:
' or 1=1 ; drop table accounts --
Look for:
'
Condition 1=1 or similar constant
Action: drop, select update delete
Two dashes --



Review of Handout 2

- ▶ **Tools and Indicators of Compromise**
- ▶ **Your instructor will perform a review of the exhibits listed in HO-2**
- ▶ **Knowing these is important**
 - For overall security knowledge
 - Understanding exam exhibits
 - Identifying attacks and tools used

Pop Quiz

1. A co-worker was working in their cubical
2. You noticed this on their desktop. What activity was happening?



```
[Metasploit] msf6 exploit(mscrls) > use exploit/multi/handler
[*] Starting persistent handler(s) ...
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/shell_reverse_tcp
payload => windows/x64/shell_reverse_tcp
msf6 exploit(multi/handler) > [REDACTED]
```

Mitigations

► **This list covers a wide array of measures across an enterprise**

- Segmentation
 - Dividing networks
 - VLANs
- Access control and filtering
 - Using access control lists (ACL)
- Least privilege
 - Permissions set to minimum required
- Application allow list software
- Isolation
- Patching and hardening
- Encryption
- Monitoring
- Configuration enforcement
- Decommissioning

Patch Management and Hardening

- ▶ **Compliance managed by patch management systems**
 - Automating patching and deployment policies
 - Ensuring consistent and timely distribution of patches preventing unexpected reboots
 - Locking down the Registry and closing unnecessary ports
 - Creating and maintaining baselines
 - Directed by change management policy
 - Implement policy settings on managed hosts
 - Identify unwanted/forbidden software
 - Alert for missing security software
 - Verify and audit licensing
- ▶ **Integrate into 802.1x to assess and strengthen security posture prior to LAN/WLAN admission**

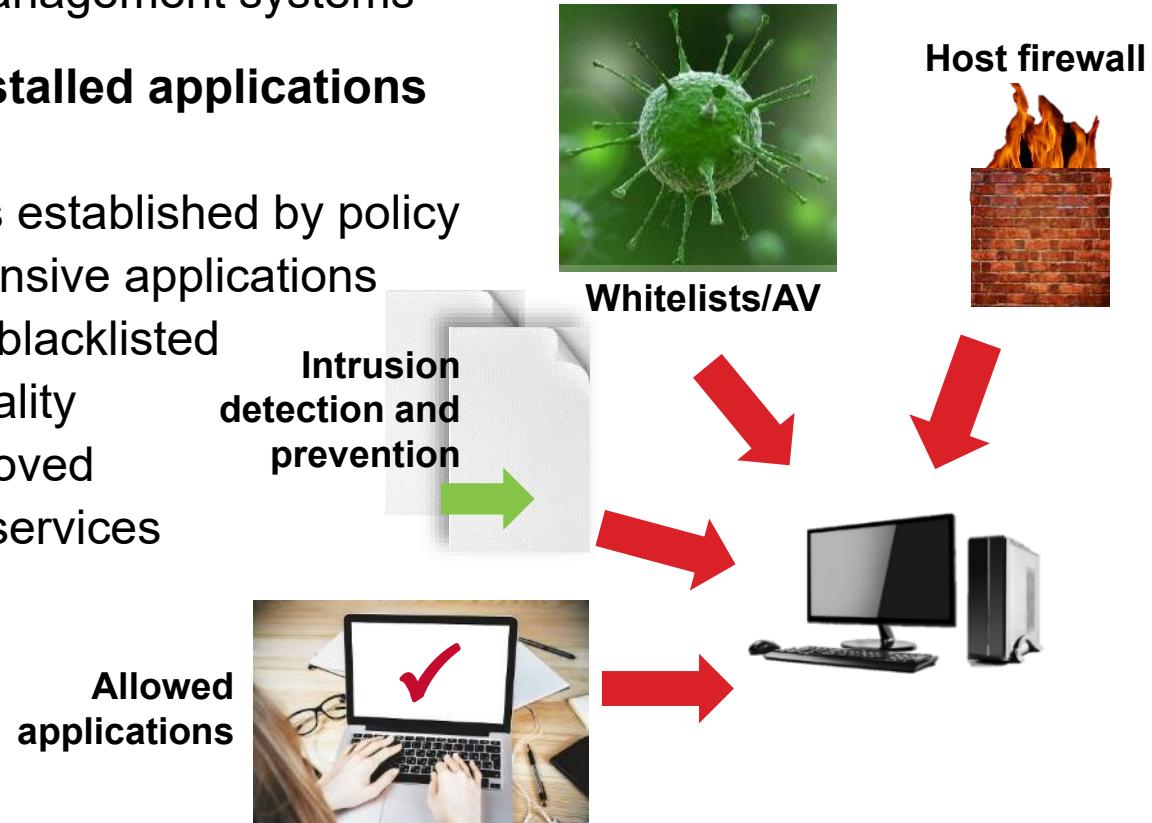
Set Least Privilege

- ▶ The most effective prevention of fraud
- ▶ Also known as minimal privilege and least authority
- ▶ Requires that a person is only accorded rights, capabilities, or access necessary to perform a task or job (e.g., web developers can modify code, but not manage the application)
- ▶ Should be set for
 - Services
 - Users



Hardened Baselines

- ▶ **Part of configuration management and systems hardening**
 - Maintained by patch-management systems
- ▶ **Regulate settings and installed applications**
 - Trusted OS
 - Secure configuration as established by policy
 - Required endpoint defensive applications
 - Forbidden applications blacklisted
 - Least privilege/functionality
 - Default passwords removed
 - Disabled unnecessary services
 - Full disk encryption
- ▶ **It serves to reduce risk by enforcing defensive measures**



AV = Antivirus

Provisioning and Deprovisioning

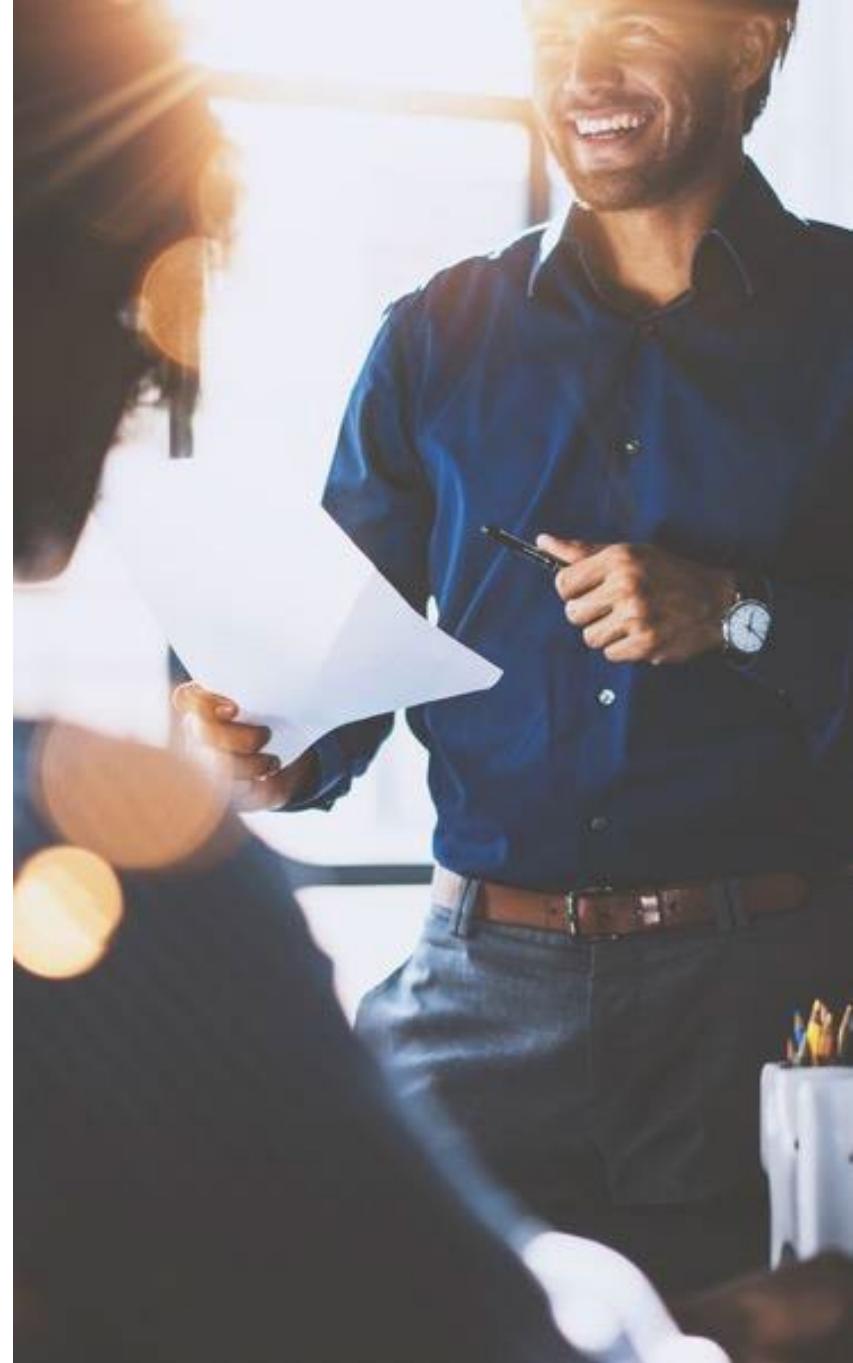
- ▶ Applications are staged on servers, and these must be created and managed
- ▶ Provisioned
 - Hardened
 - Configured
 - Adequate storage and RAM
 - Match the policy baseline
- ▶ Deprovisioned when no longer used
 - Addresses
 - Data remnants
 - VM Sprawl

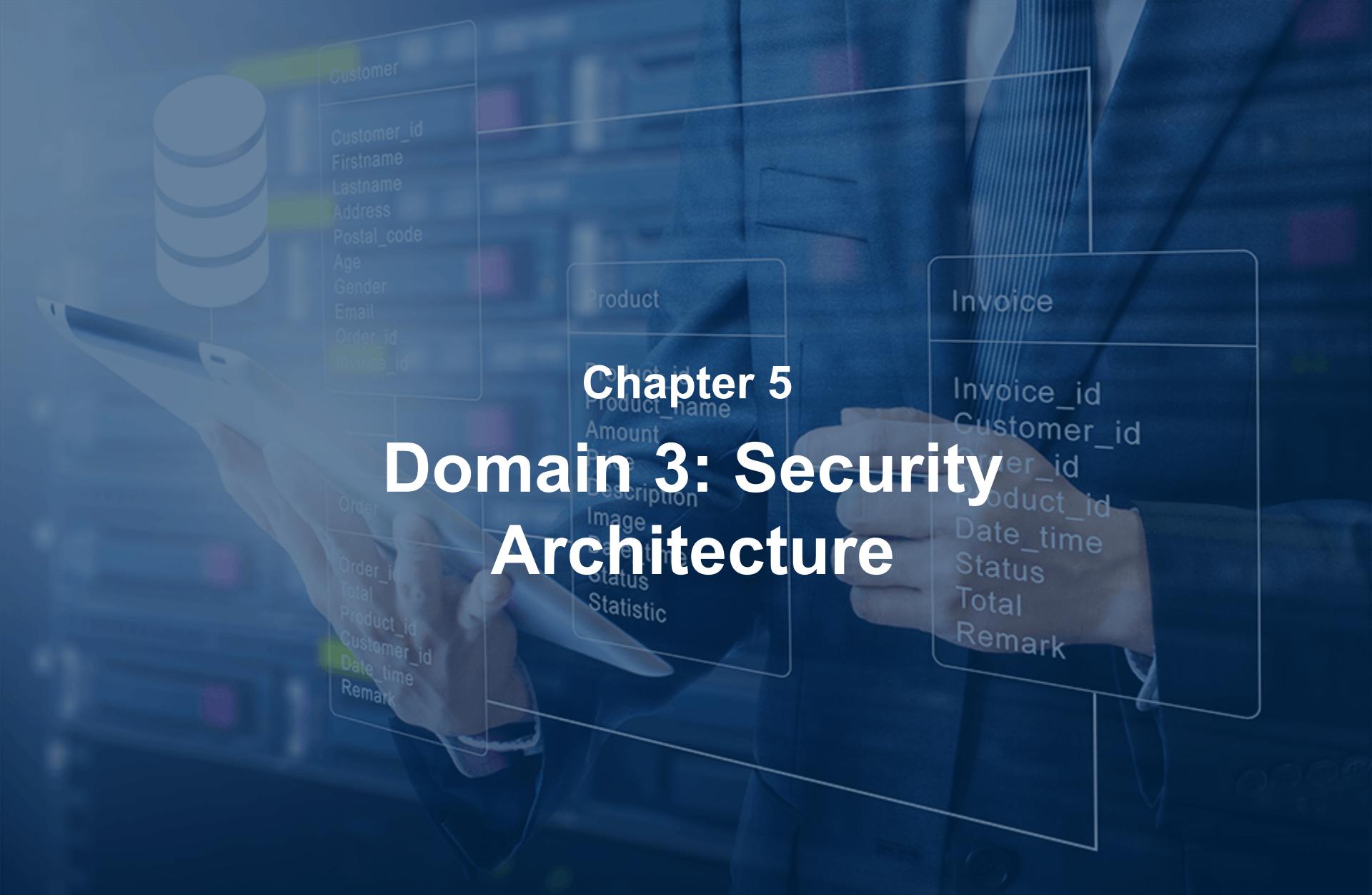


Objectives

- ▶ Comparing threat actors
- ▶ Analyzing vectors and the attack surface
- ▶ Understanding vulnerabilities
- ▶ Identifying malware
- ▶ Specifying appropriate indicators and mitigation

22%





Chapter 5

Domain 3: Security

Architecture

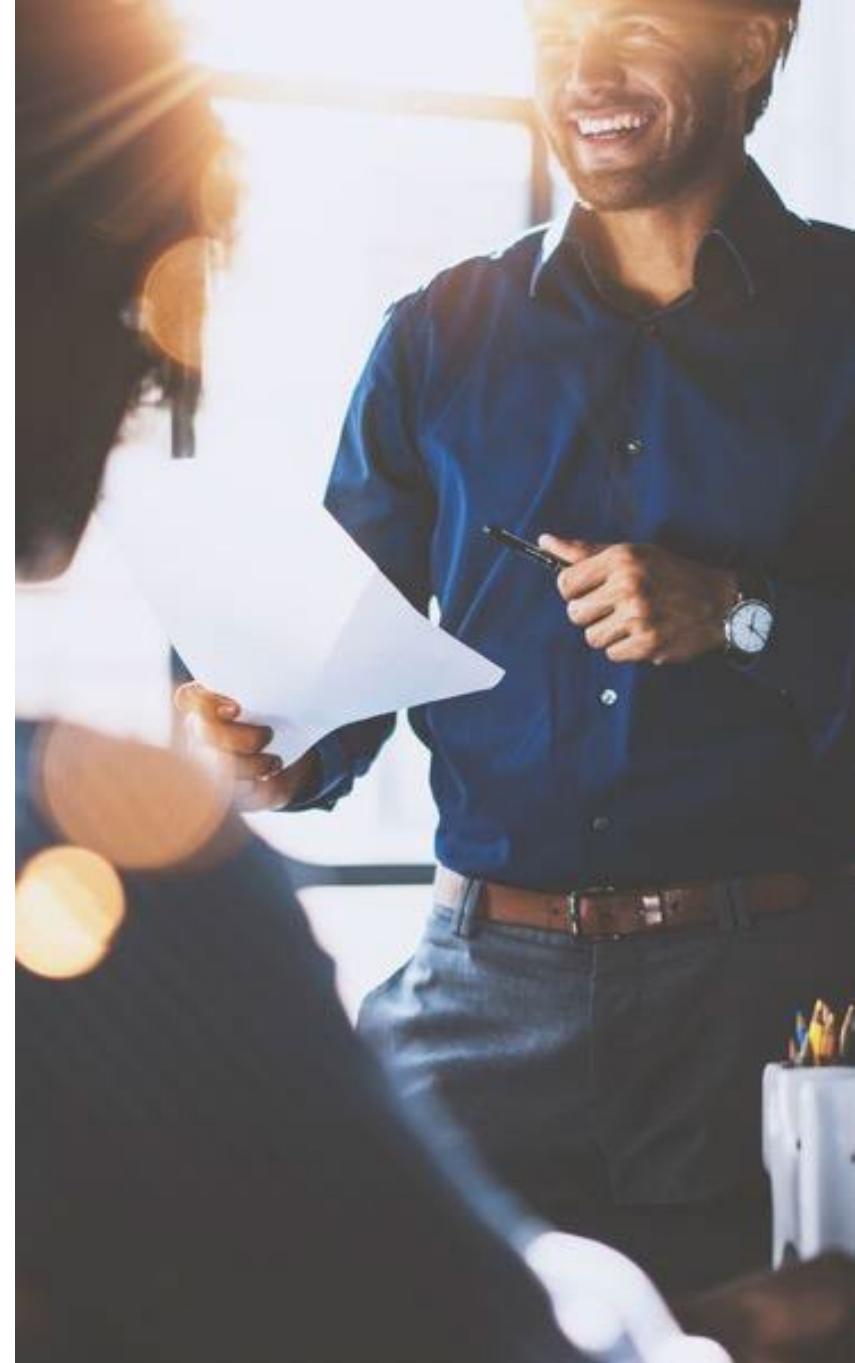


LEARNING TREE™
INTERNATIONAL

Objectives

- ▶ **Understanding infrastructure security models**
- ▶ **Securing the infrastructure**
- ▶ **Protecting data**
- ▶ **Implementing resilience and recovery**

18%



Contents

Infrastructure Security Models

- ▶ **Implementing Infrastructure Security**
- ▶ **Data Protection Measures**
- ▶ **Implementing Recovery and Resilience**



Cloud Computing Infrastructure

- ▶ **Cloud computing involves connecting to computing resources that are**
 - Physically placed in one or many locations across the Internet
 - Easily staged and taken down
 - Available in small or large numbers
 - On-demand heavy computing services
 - Multitenant and able to provide varying levels of protection
 - Greatly enhances availability
- ▶ **Supports**
 - Thin clients that run from the resources of a central cloud-based server
 - Containers that systems that it can be run anywhere, whether it be on desktop, mobile or thin client
 - Highly scalable and can be centrally monitored
- ▶ **Physical protection and backup/recovery functions are transferred to the cloud provider**

Types of Cloud Services

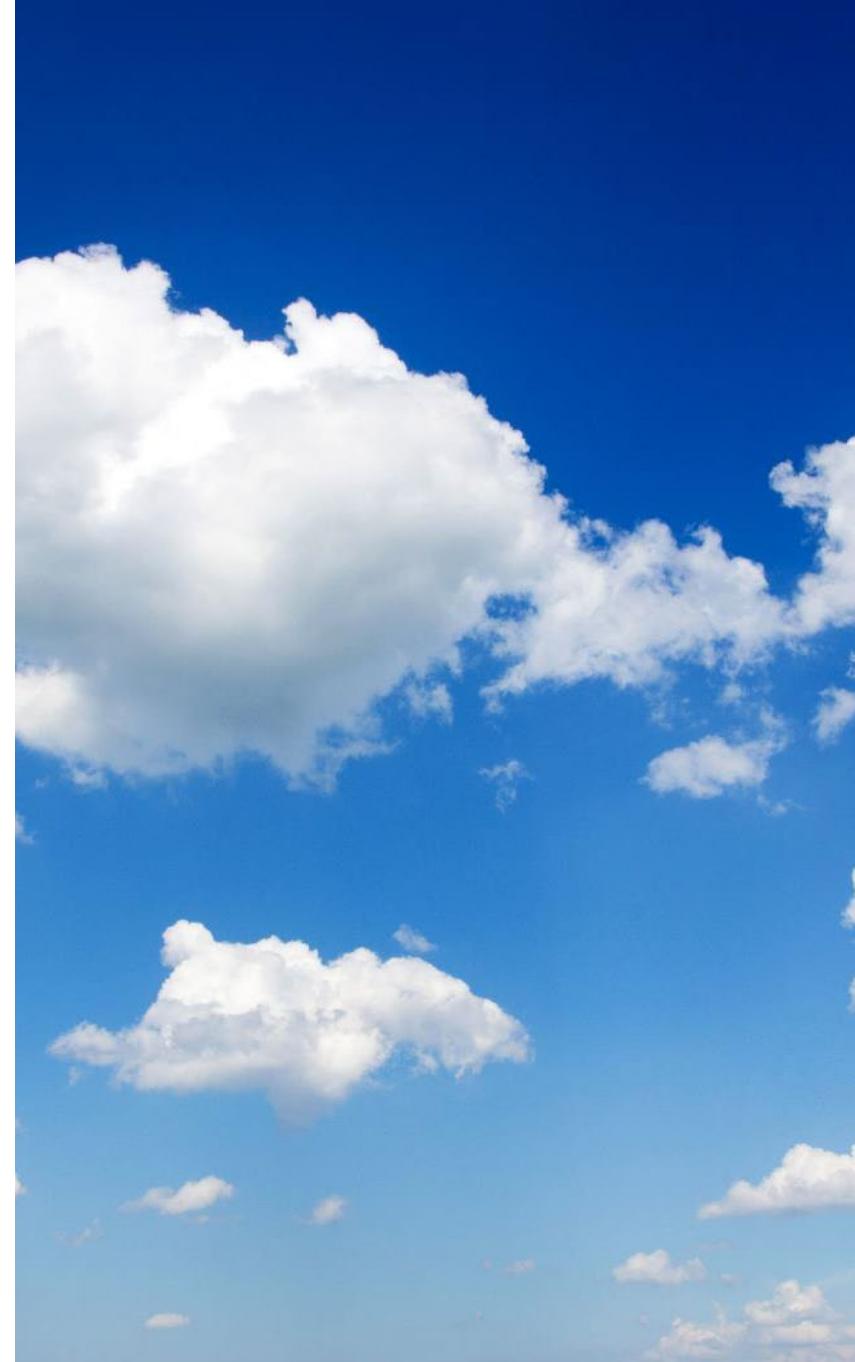
- ▶ **Software as a Service (SaaS)**
 - Delivers *one application*, like web e-mail or a database (e.g., cloud-hosted webmail service)
- ▶ **Platform as a Service (PaaS)**
 - Delivers a *plain operating system* as a service
 - The customers build their own applications to run on the cloud infrastructure
 - Used for customer-developed applications
- ▶ **Infrastructure as a Service (IaaS)**
 - Sometimes called “data center in the cloud”
 - The cloud provides services, storage and networks and access to the OS
- ▶ **Function as a Service (FaaS)**
 - Also called *serverless architecture*
 - Applications are divided into individual functions, which may be centralized or dispersed across many servers or the Internet.
 - The developer does not have to create or manage the server

Other Cloud Concepts

- ▶ **Managed Security Service Providers, such as Host Based Security System (HBSS)**
 - Complex or sophisticated application that manages security (may be cloud-based)
- ▶ **Anything as a Service (XaaS)**
 - Also called Everything as a Service
 - A generic term referring to the wide array of cloud-based services
- ▶ **Fog computing and Edge computing**
 - The utilization of edge processing and computing devices to facilitate interactions between clients and the cloud
 - The computing resources may be dispersed geographically
 - Highly associated with the Internet of Things (IoT) concept
- ▶ **Microservices**
 - An application created from numerous small services
 - Often composed of collections of interacting APIs

Other Cloud Topics

- ▶ **Cloud location**
 - Private/On-premises: fully purchased, operated and maintained by an organization/consumer
 - Hosted: Cloud provider company provides the systems
 - Virtual Private Cloud: Hosted, but isolated from other hypervisors, like a VPN
- ▶ **Cloud Access Security Broker (CASB)**
 - A service that resides between users and the cloud
 - Monitors and regulates interactions and enforces security policies, provide visibility and management



Cloud Access Types

- ▶ **Public cloud**
 - Most popular clouds are public: Services available to the public on a commercial basis (e.g., Amazon Web Services)
- ▶ **Private cloud**
 - A cloud computing environment that is implemented within the corporate security perimeter and is run by the IT department (e.g., a cloud setup for the abc.com organization alone)
- ▶ **Community**
 - A cloud infrastructure shared between several organizations from a specific community or interest group with common goals
- ▶ **Hybrid**
 - Combination of private, public, and community cloud services from different service providers

Cloud Security Measures

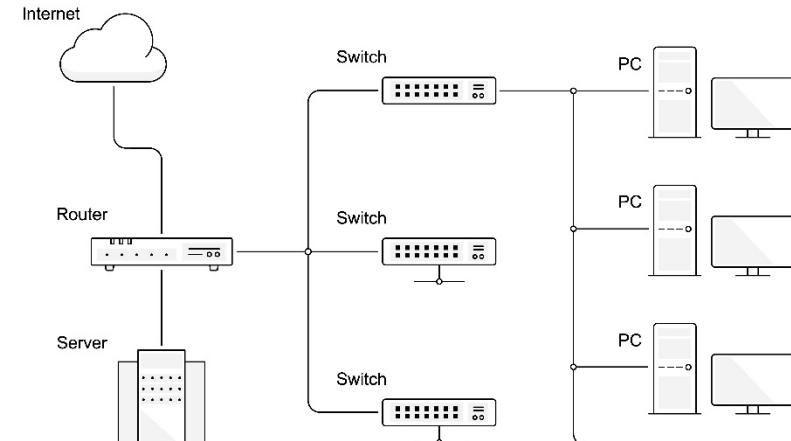
- ▶ **Implementing cloud-based systems allows for a range of measures**
 - Resource utilization policies
 - High availability
 - Application and data replication across wide distances
 - Virtual networking
 - Software defined network
 - Software defined visibility
 - The ability to view and inspect traffic and packet data
- ▶ **Solutions**
 - Cloud Access Security Brokers (CASB) for monitoring and security access
 - Zero-Trust network Access

Zones and Compartmentalization

- ▶ In any infrastructure segregation or isolation is important
- ▶ Traffic flows are susceptible to eavesdropping attacks
 - Rogue sniffers installed on hosts
 - Unauthorized media taps
- ▶ Involves proper network planning and management
 - Surveys and network maps of critical areas
 - Initial design should reflect the need for separation
- ▶ Zones identify areas of common use and can be secured by
 - Virtualization
 - Using VM technology to isolate hosts and resources
 - Air gaps—no connectivity allowed
 - Creating unique infrastructures for varying security needs
 - Logical separation
 - Subnetting with a router
 - VLANs and filters

Software-Defined Networking (SDN)

- ▶ **SDN is a network architecture that decouples the network control plane from the data plane**
 - This allows network administrators to programmatically configure and monitor the network
 - It more flexible, less costly and easier to manage
- ▶ **Components of SDN are**
 - Controller, which is responsible for configuring devices
 - Switches are responsible for forwarding traffic between devices on the network and are managed by a controller
 - Applications are used to control and automate the network
- ▶ **Infrastructure as Code**
 - Can be used to provision and manage an SDN infrastructure
 - Implementing and provisioning virtual routers, switches



Virtualization

- ▶ **The use of software that can allow a single host to run processes that allow other operating systems to run simultaneously**
 - Called a virtualized sandbox
 - Each virtual host emulates a unique hardware-based system
 - Snapshots allow the OS to immediately revert to an earlier version
 - Ideal for repetitive testing of patches and hardening
 - *Virtual switches and virtual routers* may be used to isolate VM traffic and to prevent eavesdropping
- ▶ **Advantages**
 - One hardware host may allow multiple instances of other operating systems to be present and run simultaneously
 - A significant cost and space savings—not a security advantage
 - The virtual or “guest” operating systems are isolated from the host and other virtual systems
 - Backing up a virtual host is easy—improved availability
 - Smallest footprint; takes up the least space

Virtual Machines (VMs)

- ▶ **The emulation of a computer in software**
- ▶ **VMs are based on popular hardware computer architectures**
 - Provide nearly the same functionality as a physical computer
 - Smaller physical footprint
 - May be created in hardware or software
 - Run on hypervisors
- ▶ **Hypervisors**
 - The software, firmware or hardware that hosts virtual machines
 - Type 1, also known as *bare metal*
 - Run directly off the hosting machine's hardware
 - Type 2, also known as *hosted hypervisors*
 - Run on top of a conventional OS with the assistance of an application, such as VMware Player

Other Specialized Environments

- ▶ Some computing environments are non-traditional and may be directly or indirectly linked to the cloud
- ▶ Beside the traditional computer-based environment, other areas must be addressed
 - Supervisory control and data acquisition (SCADA) and industrial controls (IDC)
 - Vehicles and aircraft/UAV
 - Robotics (RTOS)
 - Game consoles and medical devices
 - System on a Chip (SoC)
 - Wearable technology (Google Glasses)
 - Fire Control, HVAC, and residential technology
- ▶ Often these devices cannot load or use defensive software
 - The perimeter must be defended
 - Poor encryption
 - Little logging or auditing

RTOS = Real-Time Operating System

UAV = Unmanned Aerial Vehicles

Security Considerations

Feature	Traditional	Cloud	Specialized
Availability	Normal	High	Variable/Low
Resilience	Normal	High	Low
Cost	Low	High	Variable
Responsiveness	Variable	High	High
Scalability	Medium	High	N/A
Deployment ease	Medium	High	High
Risk transference	Low	High	Low
Ease of recovery	Medium	High	Low
Patch availability	Medium	N/A	Low
Ability to patch	High	N/A	Low
Computing power	Medium	High	Low

Contents

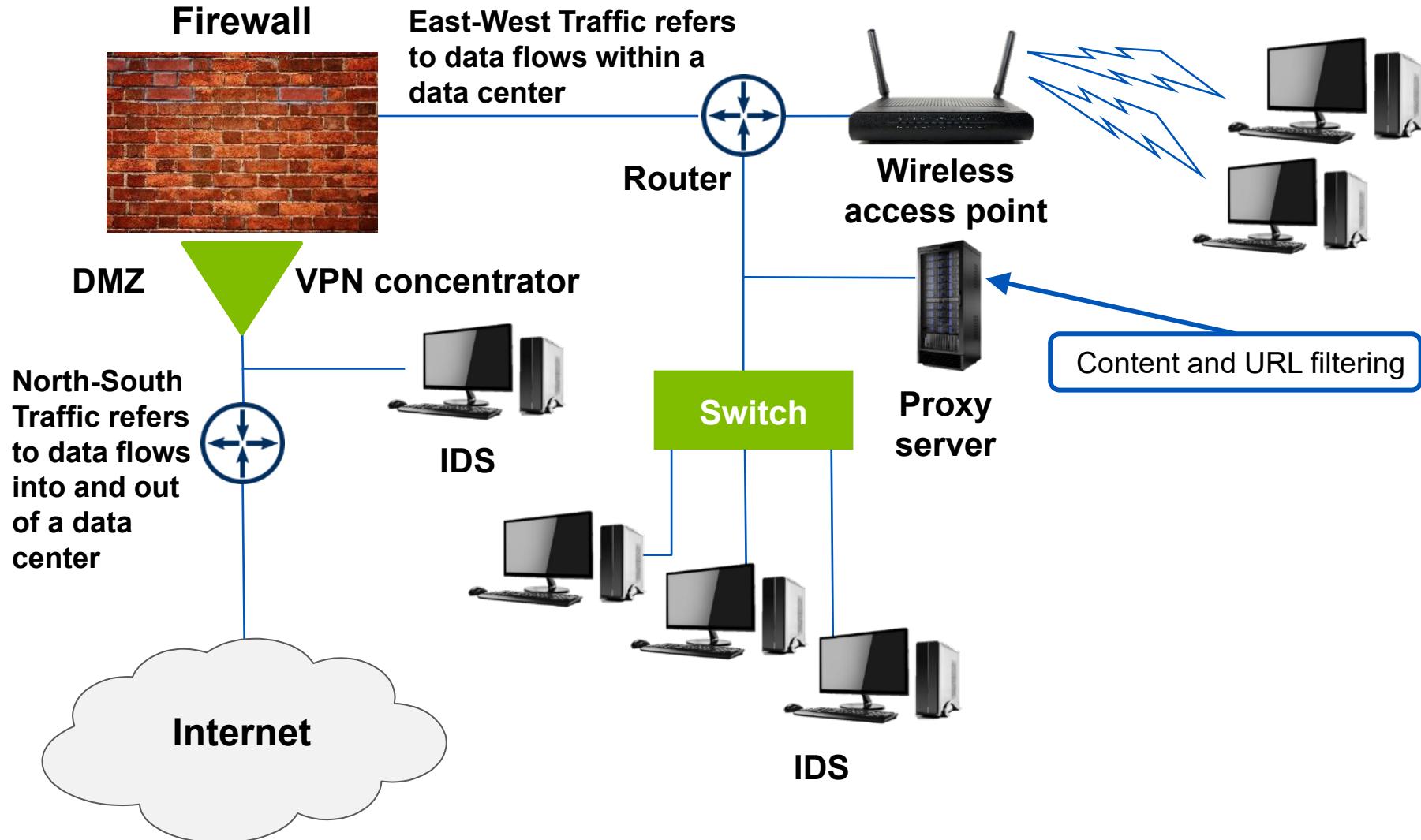
- ▶ Infrastructure Security Models

Implementing Infrastructure Security

- ▶ Data Protection Measures
- ▶ Implementing Recovery and Resilience



The Infrastructure



DMZ = demilitarized zone

VPN = virtual private network

Zones and Compartmentalization

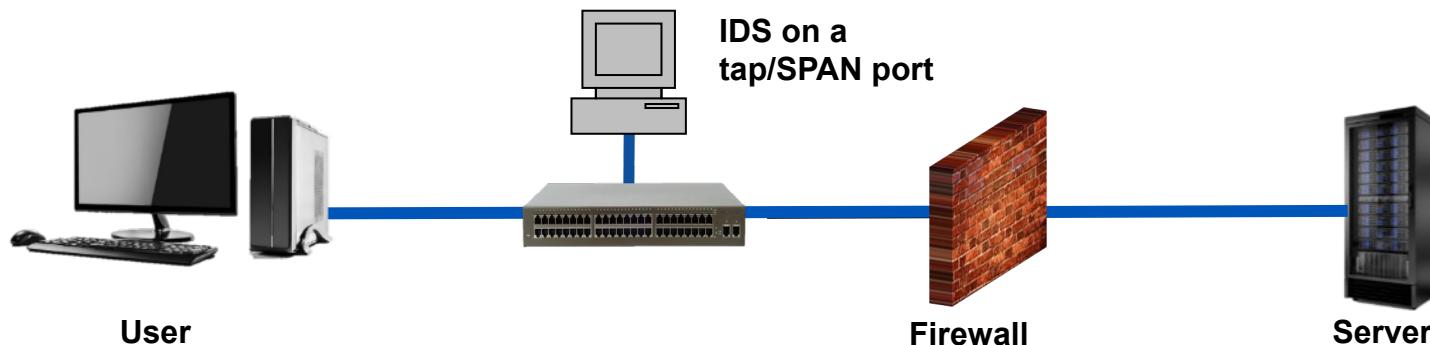
- ▶ **Traffic flows are susceptible to eavesdropping attacks**
 - Rogue sniffer installed on hosts
 - Unauthorized media taps
- ▶ **Involves proper network planning and management**
 - Surveys and network maps of critical areas
 - Initial design should reflect the need for separation
- ▶ **Zones identify areas of common use and can be secured by**
 - Virtualization
 - Using VM technology to isolate hosts and resources
 - Air gaps—no connectivity allowed
 - Creating unique infrastructures for varying security needs
 - Logical separation
 - Subnetting with a router
 - VLANs and filters

Attack Surface

- ▶ **The attack surface is the sum of all the ways an attacker can gain unauthorized access to a system or network**
 - It includes all components of a system that are exposed to potentially hostile parties or misuse
- ▶ **An attack surface can be divided into three main categories:**
 - Network attack surface
 - This includes all of the accessible devices and systems that are connected to the network, such as servers, workstations, routers, and firewalls
 - Application attack surface
 - This includes all of the applications that are running on the network, such as web applications, databases, and email
 - Data attack surface
 - The data that is transacted or stored, such as customer data, financial data, and intellectual property
- ▶ **Attackers can exploit vulnerabilities in any of these categories to gain access to a system or network**

Infrastructure Device Considerations

- ▶ **Failure modes**
 - Fail-open—availability is most important
 - Fail-closed—security is most important
- ▶ **Device attribute or placement**
 - Active vs. passive
 - Protocol analyzers are passive
 - Port scanners are active
- ▶ **Inline vs. tap/monitor**
 - Most firewalls are inline
 - Network intrusion detection uses a monitor port or tap



Logical Separation

► VLANs

- A technology that allows segregation of data between different VLAN groups
- A VLAN is a subnet and different VLANs are connected by a router
- VLAN membership may be assigned by
 - Port on a switch, IP address, MAC address
 - 802.1x authentication
- Each VLAN is a broadcast domain
 - Limiting opportunity for ARP spoofing
- Trunking protocols handle inter-switch traffic
 - Should be enabled only for inter-switch ports

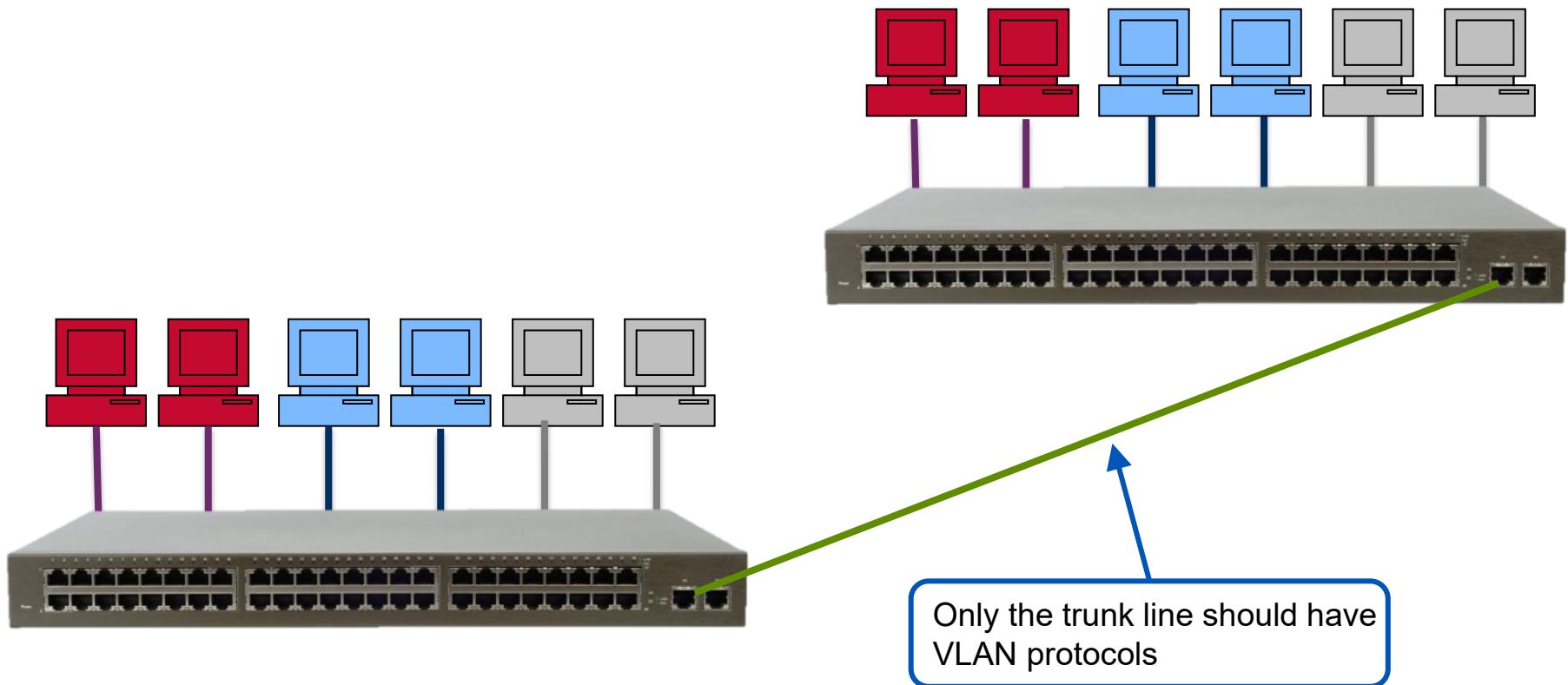
► Use a router with ACLs as the best way to control inter-VLAN traffic

► Encryption

- Where VLAN and physical separation are impractical and yield no gain

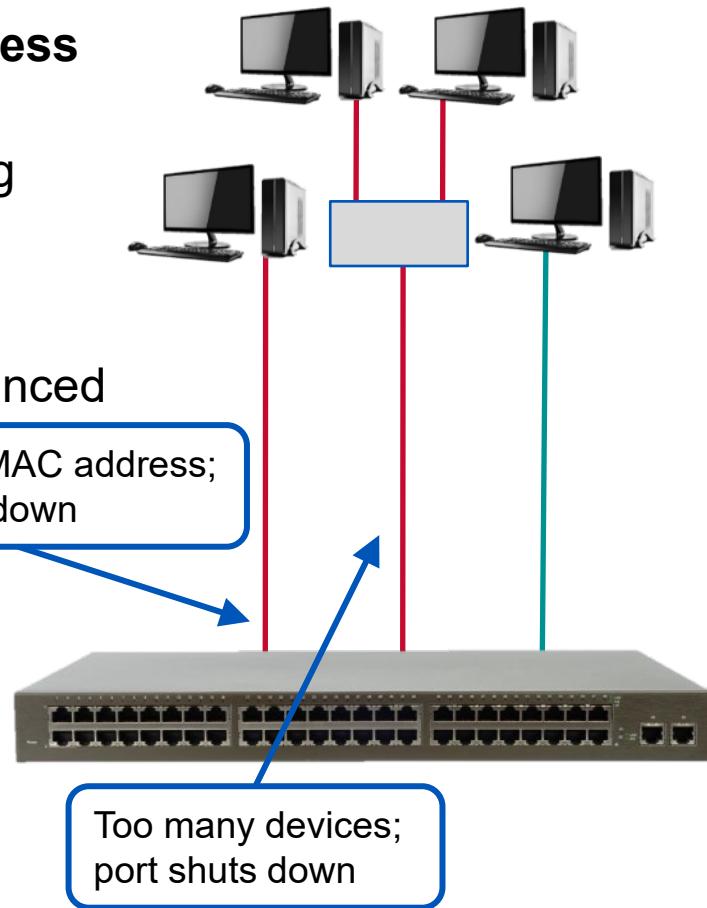
VLANs Illustrated

- ▶ Switches are interconnected via a trunk line
- ▶ Each VLAN is its own broadcast domain



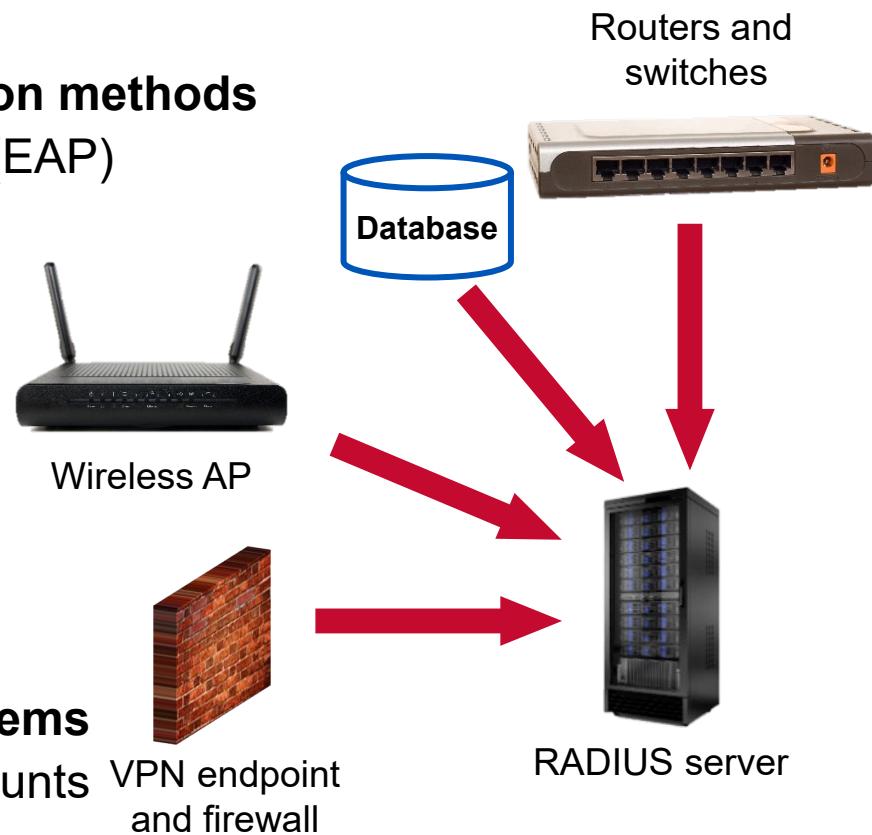
Port Security

- ▶ **A primitive form of network access control (NAC)**
 - Regulating whether a device can connect to the intranet at the switch
 - Shuts down the port when illegal devices are attached
- ▶ **Set ports to allow just one specific MAC address**
 - MAC filters are easily bypassed with a sniffer
 - Prevents rogue hubs and switches from being attached
- ▶ **Better**
 - Authenticate with 802.1x, which is more advanced
 - Implement zero trust access control
- ▶ **Prior to admission**
 - Prompt for credentials/certificates
 - Check antivirus signatures
 - Verify patching
 - May be agent-based or agentless



Centralized Authentication Services

- ▶ The primary utility of Kerberos, RADIUS, LDAP, and other authentication services is that they may act as a central authentication server
- ▶ Single-point control of accounts
- ▶ Handles many different authentication methods
 - Extensible Authentication Protocol (EAP)
 - Hashed
 - Encrypted
 - Challenges
 - Kerberos
- ▶ RADIUS implements AAA
 - Authentication, authorization, and accounting
- ▶ Privileged access management systems
 - Restricts use of administrative accounts



Wireless Security and Encryption

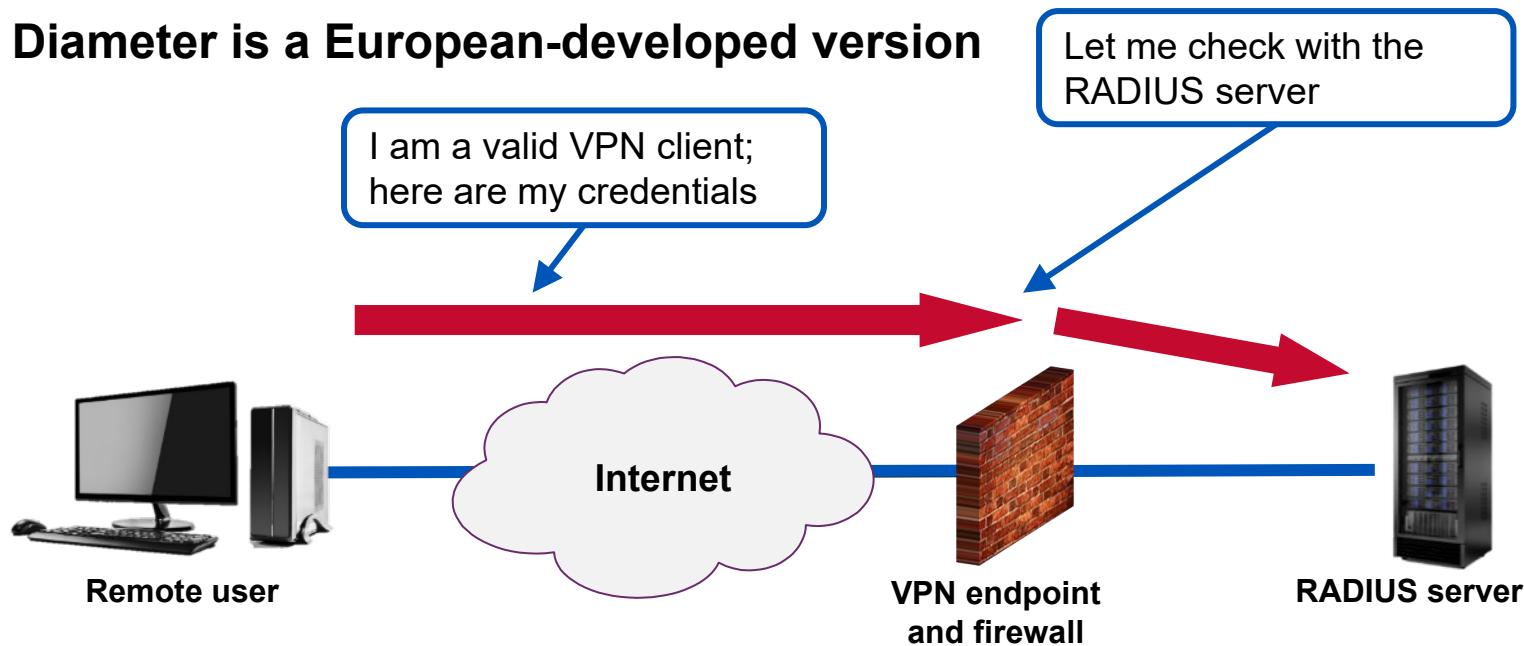
- ▶ **Wireless networks can be configured in two ways**
 - Ad-hoc
 - Peer to peer, allowing another access to your system with your rights
 - WLANs
 - Hosts transmit and receive data via a wireless access point (WAP)
 - This is the normal mechanism—infrastructure mode
- ▶ **Wireless authentication may be**
 - Physical—pressing a button on the AP for passwordless access
 - Open system or captive portal for use in a low-security environment with a disparate user base (hotels)
 - No encryption is enabled on the network; any device that knows the SSID may join the network—called a captive portal
 - Most useful for public venues and hotspots
 - Pre-Shared Key (PSK)—use in a small environment where a key can be shared and changed easily
 - Enterprise
 - Using WPA/2, WPA/3, and central authentication, such as RADIUS

RADIUS = Remote Authentication Dial-In User Service

RADIUS

- **Remote Authentication Dial-In User Service (RADIUS)**
 - Originally created in the days of modems
 - Now used as a standard third-party authentication service
 - Must have a valid certificate to be integrated with 802.1x
 - Can handle a variety of authentication protocols
 - Only encrypts credentials from client to server
 - Uses UDP/1812

- **Diameter is a European-developed version**



EAP Framework

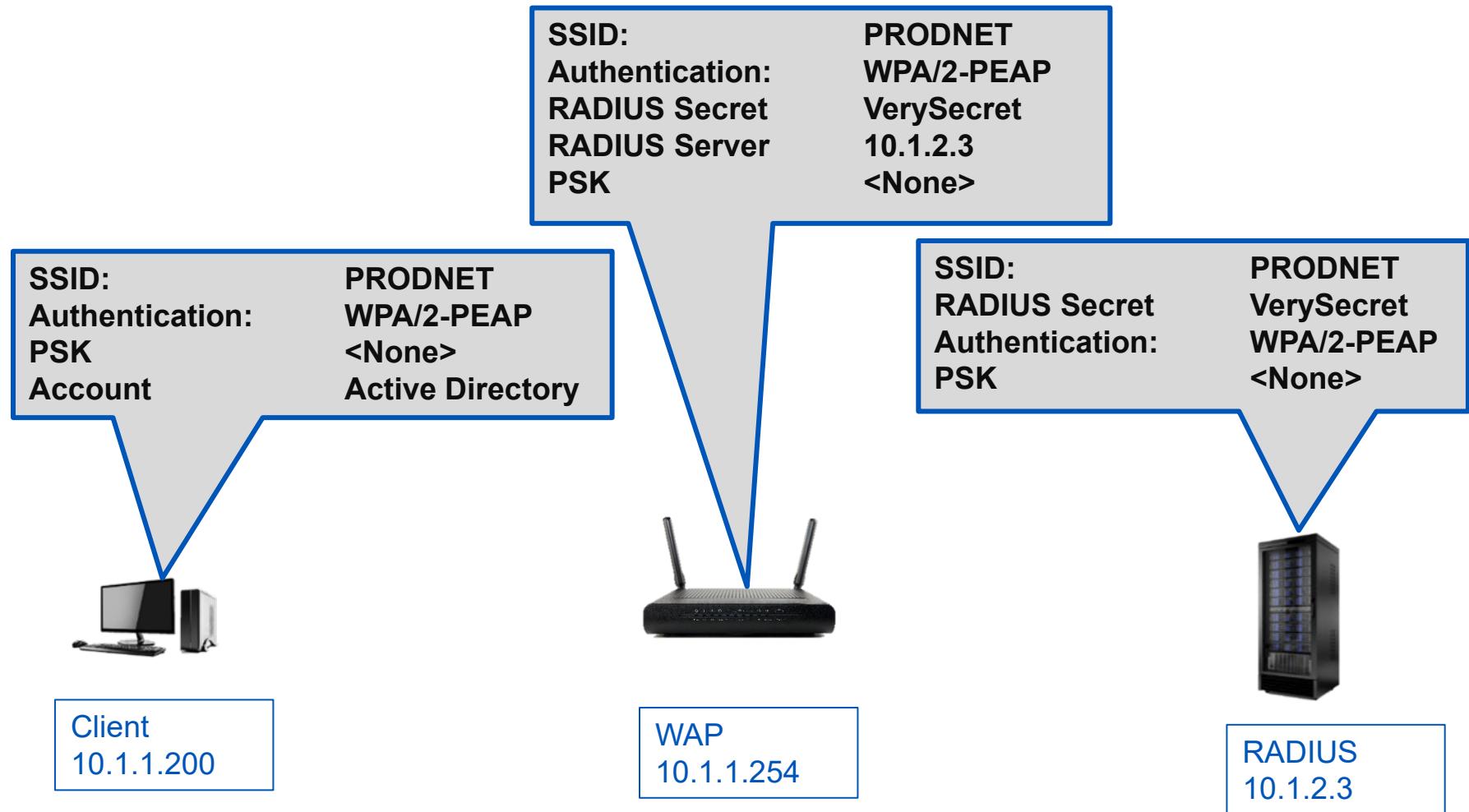
- ▶ **EAP allows authentication to occur with a variety of mechanisms**
 - It is an Internet standard (RFC-3748)
 - EAP is an authentication *framework*, not a specific authentication mechanism like Kerberos or CHAP
- ▶ **EAP defines how to send other specific authentication protocol data and receive responses**
 - EAP-TLS—PKI and certificate-based authentication
 - EAP-TTLS—Tunneled Transport Layer Security
 - The client is not required to have a certificate (which simplifies the setup)
 - EAP-FAST—Flexible Authentication via Secure Tunneling
 - Cisco developed for wireless
 - PEAP—Protected EAP implements mutual authentication with Transport Layer Security (TLS), CAs, and PKI
 - Often used to encapsulate and protect MS-CHAPv2
 - Can prompt for username and password, not just certificates

CA = Certificate Authority

MS-CHAP = Microsoft Challenge Handshake Authentication Protocol

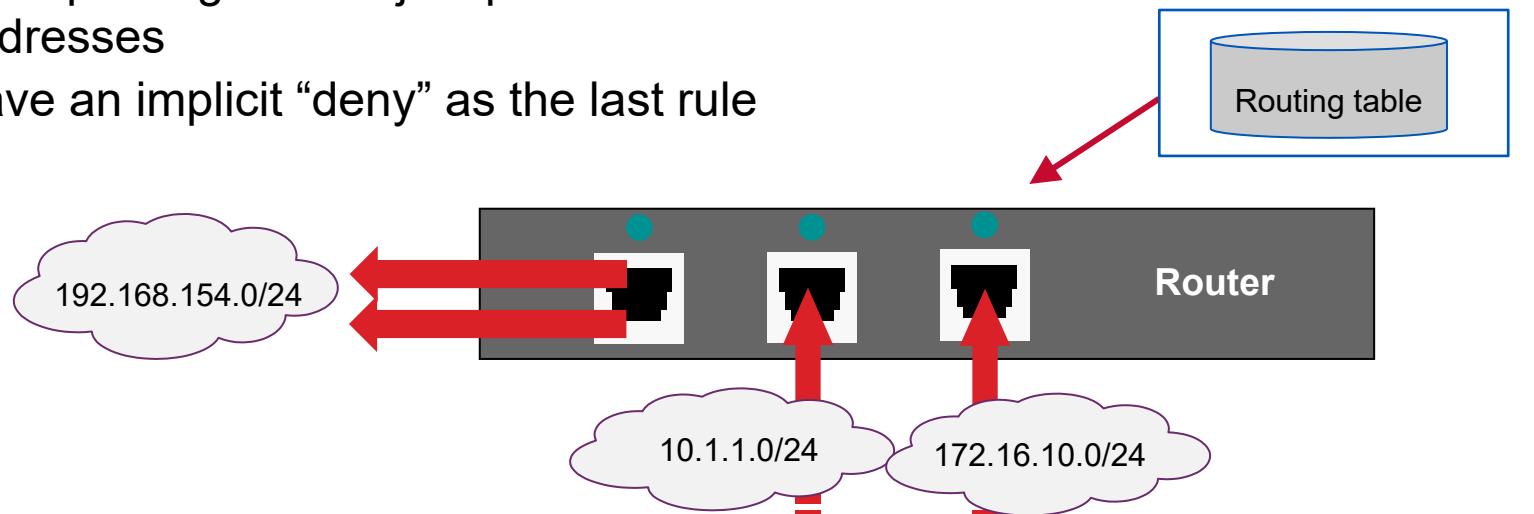
RFC = request for comments

Configuring Wireless and RADIUS



Routers

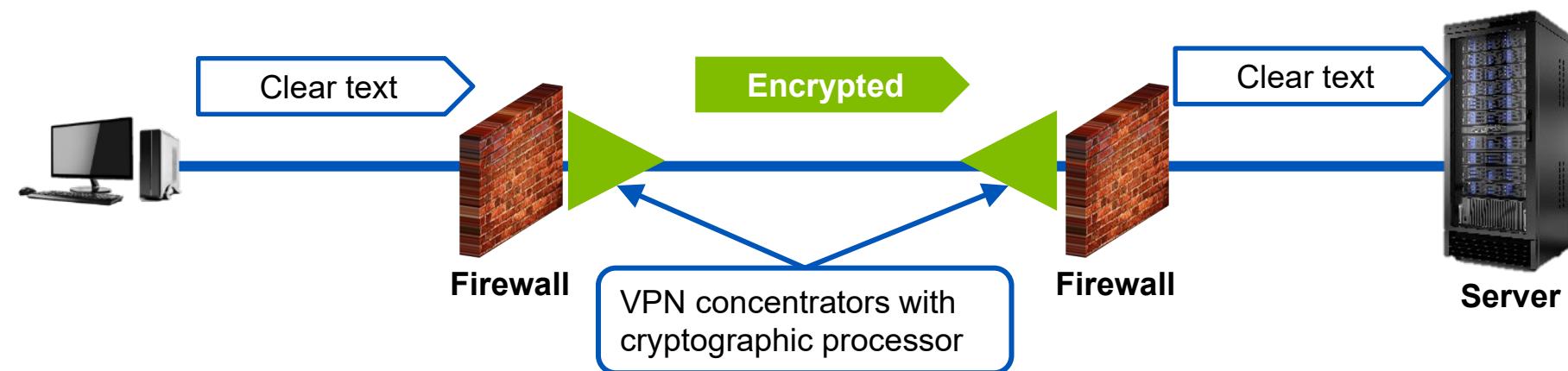
- ▶ Layer 3 protocols provide routable addressing
 - IP is a Layer 3 protocol
- ▶ Routers forward traffic between IP subnets
 - Traffic is never flooded out to all ports
 - Router relies on routing table to direct packets
 - Router updates should use secure protocols to prevent spoofing
- ▶ Most routers can filter traffic
 - Access control lists (ACLs)
 - Anti-spoofing rules reject packets from the outside that have internal source addresses
 - Have an implicit “deny” as the last rule



ACL = access control list

VPN Concentrator

- ▶ **VPN Concentrator is also known as a VPN server**
 - Commonly integrated into firewalls
 - Firewall ACLs must still allow VPN ports and protocols
 - Permits secure remote access
- ▶ **Handles encryption and decryption of traffic for remote access**
 - These activities are very CPU intensive and can impair performance
 - May have high availability features



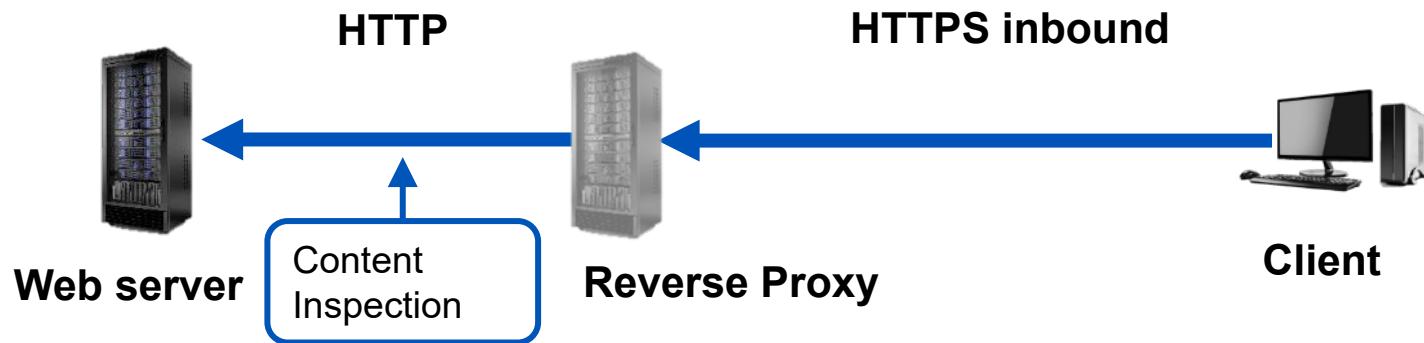
Proxies: Content and URL Filtering

- ▶ **Content filters examine data messages**
 - OSI Layer 7
 - Pass or block based on content
 - Obscene language
 - Key phrases: “top secret”
 - Blocking potentially dangerous applications and malware
- ▶ **URL/DNS filters sift through DNS and IP addresses in browsers**
 - Filters by categories:
 - Sex
 - Gambling
 - Anarchy
 - Increase productivity by blocking time-wasting
- ▶ **Next-generation Secure Web Gateway (SWG)**
 - Defends intranet against user-initiated attacks and policy violations
- ▶ **Malware inspection—antivirus on the firewall**
 - Help enforce an authorized use policy



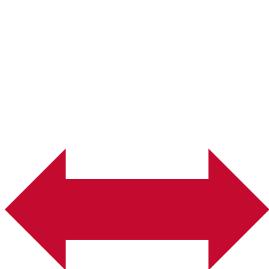
Reverse Proxies

- ▶ Servers that may be used to reduce HTTPS to HTTP, so that WAF, IDS and firewalls may inspect the data
 - Alternatively, a decryption certificate could be used
- ▶ Off loads SSL/TLS functions from servers
- ▶ Act as central point for caching and certificates
- ▶ Performs load balancing
- ▶ A web application firewall



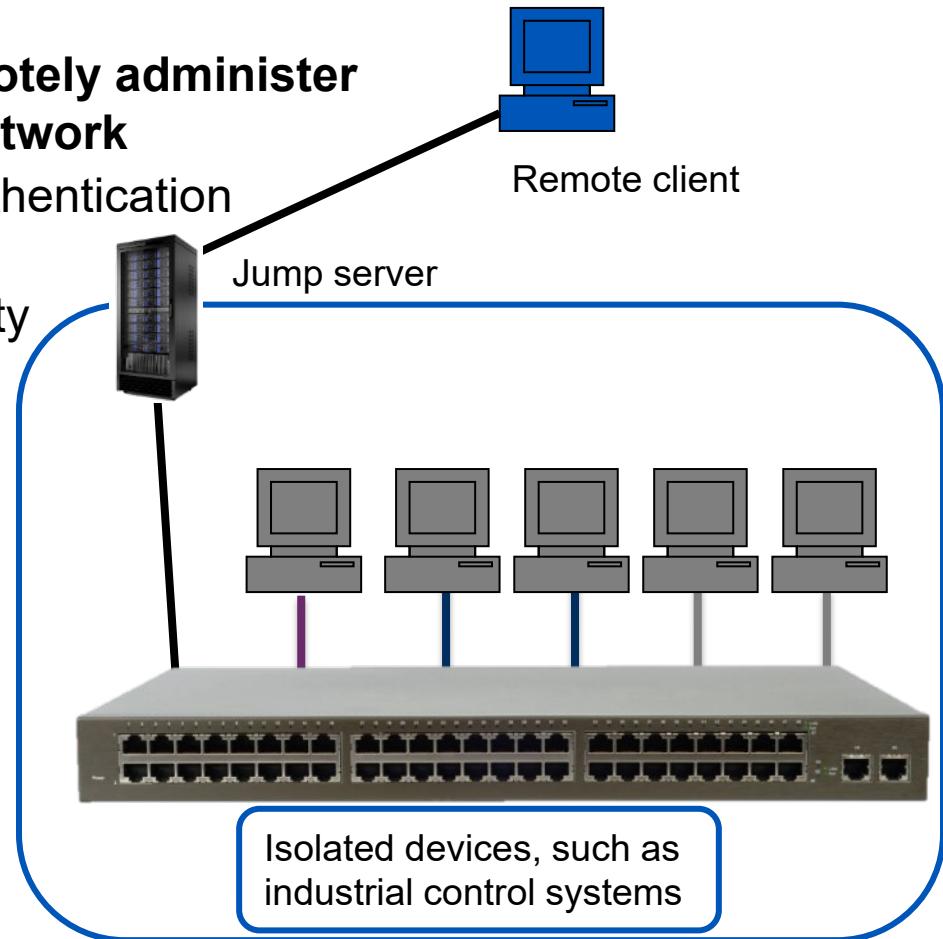
Types of Firewalls: Web Application Firewall (WAF)

- ▶ WAFs are Layer-7 defensive systems that may be hardware or software based and protect web clients and web servers against
 - XSS
 - XSRF
 - SQL injection
- ▶ Implement web-specific content filtering
- ▶ A WAF may use a reverse proxy or a special decryption certificate to inspect HTTPS



Jump Servers

- ▶ Also called jump boxes
- ▶ Jump servers can be used to remotely administer systems on a private or secure network
 - Typically, will have enhanced authentication and authorization and/or 2FA
 - They can be used to audit security logs and other system activity
- ▶ Use cases
 - Industrial controls
 - Remote or hazardous areas
 - Highly secure systems



Network Intrusion Detection Systems

- ▶ **Passively monitors network traffic**
- ▶ **Monitors network activity**
 - A *network IDS* (NIDS) detects malware or attacks in *packet data*
- ▶ **It monitors all traffic forwarded to the *sensor* or *collector***
 - Through a tap
 - SPAN or mirror ports on a switch
 - Must use TLS inspection for HTTPS data
- ▶ **IDS errors**
 - False positive: generating an alert when none should have been announced
 - False negative: failing to generate an alert when an intrusion existed
 - Alerts are validated by using a protocol analyzer
 - May be evaded by HTTPS, VPNs, or not mirroring ports

SPAN = statistical port analysis

Methods of Intrusion Detection

- ▶ **Rule-, signature-, or knowledge-based detection**
 - Compares well-known attack *signatures* or *models* to traffic
 - Signatures require frequent updates
 - Can identify only known attack patterns and must be updated frequently
 - Can be programmed to detect information leaks and transfer of forbidden documents by embedding special strings within
- ▶ **Behavior-based**
 - “Learns” the environment and generates alerts when activity established matches patterns common to attacks or abuse (e.g., worms have an exaggerated one-to-many relationship)
 - Requires building a baseline of normal activity
 - Known to be flexible, but generate more false positives initially
 - Can detect previously unknown types of attacks



Methods of Intrusion Detection

► Anomaly-based

- Like behavior-based, but examines traffic for exceptions or broken protocol rules
 - Bursts in traffic levels
 - ICMP echo reply with no earlier echo request
- Requires building a baseline of normal activity
- Can detect previously unknown types of attacks



► Intrusion Prevention System (IPS) is an active defense that can stop a malware activity or handle zero-day attacks

- If it takes action to stop or send a message about an attack, it is
 - A Network Intrusion Prevention System (NIPS)
 - An active defense
 - An inline (or in band) device, detecting, and filtering

If it only alerts, it is NIDS; if it can stop an attack, it is NIPS

Using Snort to Discover a Port Scan

Demo

- 1. On the desktop, double-click Runsnort**
 - This will start Snort Intrusion Detection
- 2. Open a command prompt**
- 3. Type nmap 10.1.1.254 -T 5 -n, then press <Enter>**
- 4. Return to the Snort window**
 - Note the alert that was posted
- 5. Snort was alerted on the number of attempted TCP three-way handshakes**

Firewalls

- ▶ **A firewall system can make pass/block decisions on packets**
 - Has an implicit “deny” as the last rule
 - Deny Any Source -> Any Destination
 - Uses a rule list to determine pass or block decisions
 - To allow public access to HTTP, inbound TCP/80 must be allowed
 - Decides based on packet headers and payload
 - Controls traffic flow between a trusted and untrusted network
- ▶ **Most firewalls are “dual homed”**
 - May have two (or more) network cards
- ▶ **May be installed**
 - On virtual machine
 - Easiest to procure and install
 - General-purpose OS
 - Must be hardened by owner
 - Appliance
 - Pre-hardened by vendor



Stateless and Stateful Packet Inspection

► Stateless packet inspection

- Typically implemented by routers
- Network layer
- Fastest operation
- Rules must be created specifically for inbound and outbound flow
- Simple filtering rules that are processed from the top down
- May pass or block according to headers, but not application data
 - IP address, port, or other packet field

► Stateful packet inspection

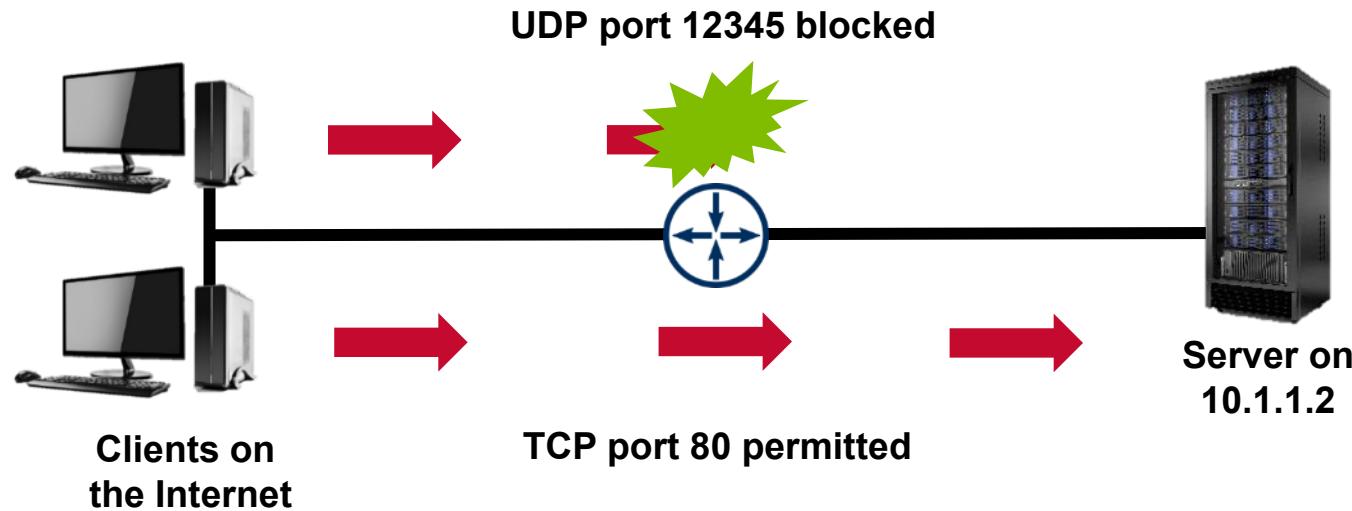
- Examines each packet, but in the context of previous packets
 - Cisco ASA
 - FireWall-1
- A rule is created for one direction
 - Firewall dynamically creates the return-trip rule
- Able to stop DoS attacks that involve fragmentation or segmentation

Stateless Packet Inspection

- ▶ Simple rules that permit or deny based on
 - IP address (source or destination)
 - TCP/UDP port (source or destination)
 - Other fields
- ▶ Called access control list (ACL)

Deny UDP from anywhere to 10.1.1.0/24 where Port = 12345

Permit TCP from anywhere to 10.1.1.0/24 where Port = 80



Stateful Packet Inspection

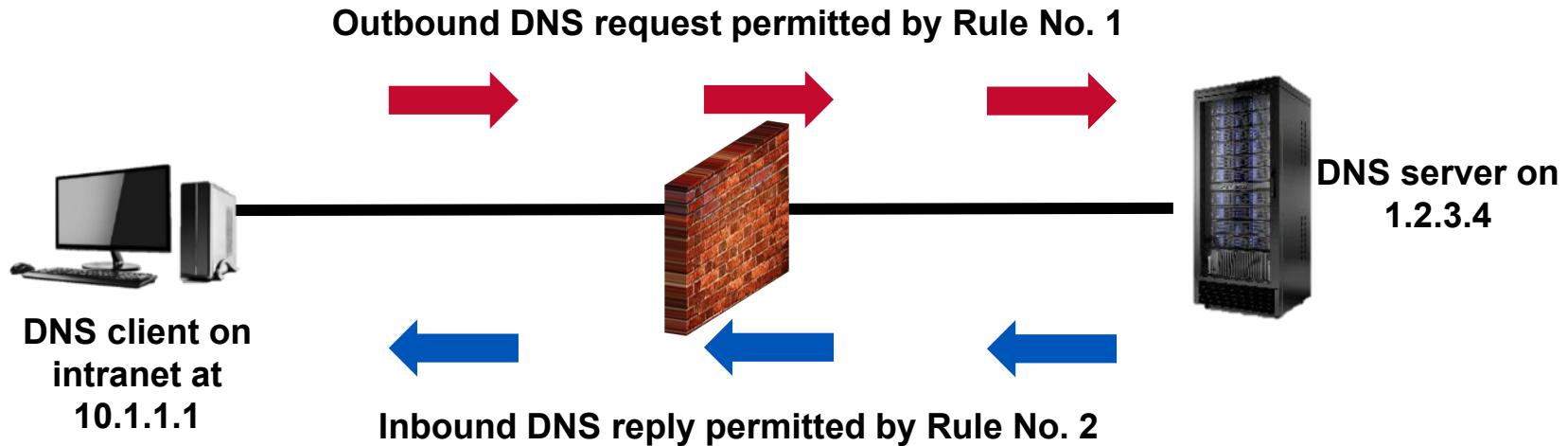
- ▶ Like stateless, but creates a dynamic rule to allow the return data
 - Operate and Layers 4-7 of the OSIRM
- ▶ Checks fragments and segments to make sure they add up properly
 - Stopping some DoS attacks

Rule No. 1 created by administrator:

Permit from intranet to 1.2.3.4/32 where packet is DNS request

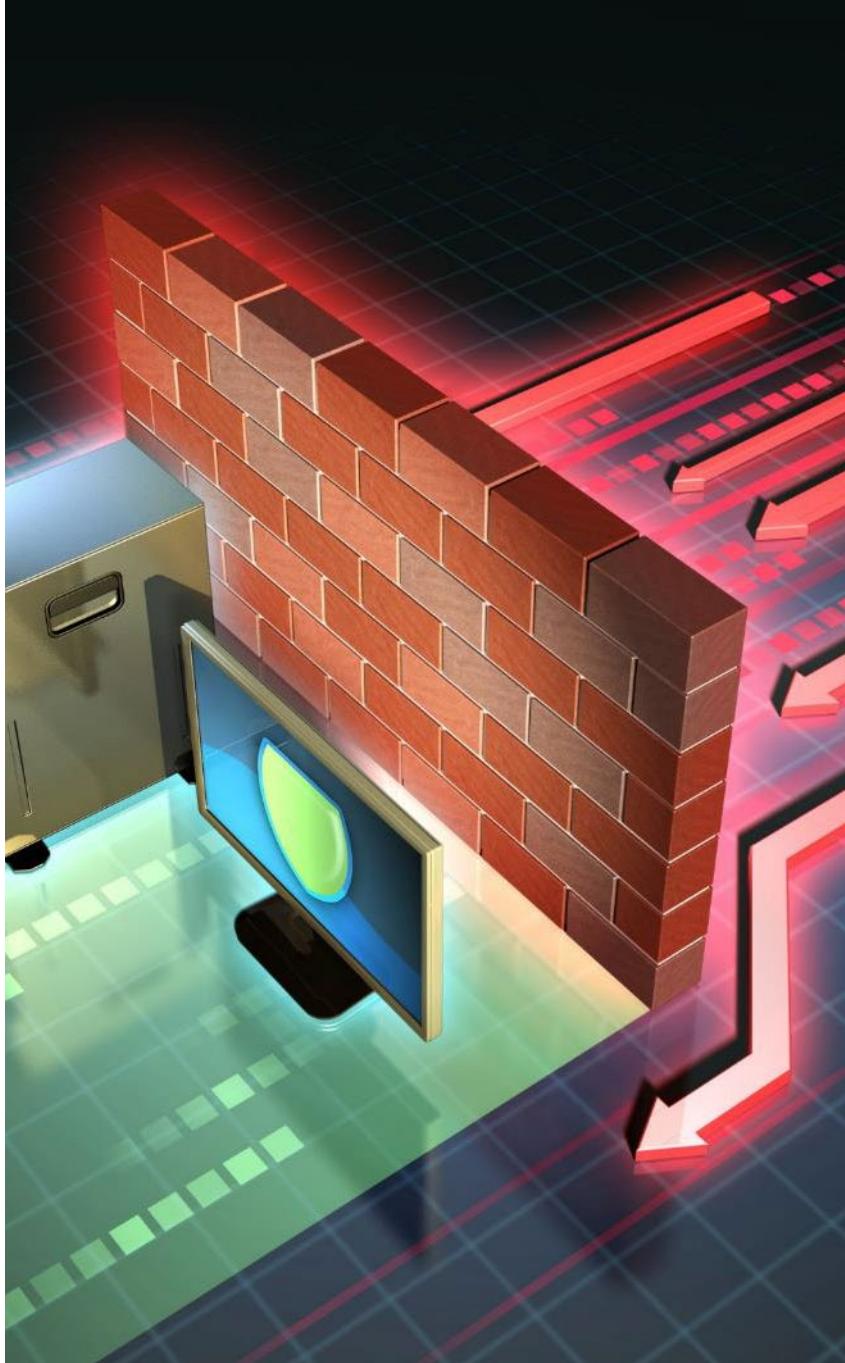
Rule No. 2 created by firewall after the request is permitted inbound:

Permit from 1.2.3.4 to 10.1.1.1/32 where packet is DNS reply



Types of Firewalls: Application

- ▶ Application proxies operate at Layer 7
- ▶ Slowest, but strongest security controls
- ▶ Receives requests and tests whether it should perform them
- ▶ Able to filter application commands and data (e.g., deny GET, allow PUT in FTP)
 - Can be equipped to filter viruses and spam



UTM and Next Generation Firewalls

- ▶ **Unified Threat Management (UTM) simply combines multiple security functions in one box for ease of management and reporting**
- ▶ **Next Generation Firewalls (NGFW)**
 - NGFW is a more advanced security solution that focuses on deep packet inspection (DPI) to identify and block malicious traffic
 - DPI allows NGFWs to inspect the contents of packets, not just the headers
- ▶ **Features common to both**
 - Firewall
 - VPN concentrator
 - IPS/IDS
 - Data-loss prevention
 - Antivirus
 - E-mail and spam filtering
 - Web application security
 - Regulate use of browsing and access to social media
 - May become single points of failure
 - Many are implemented as virtual appliances

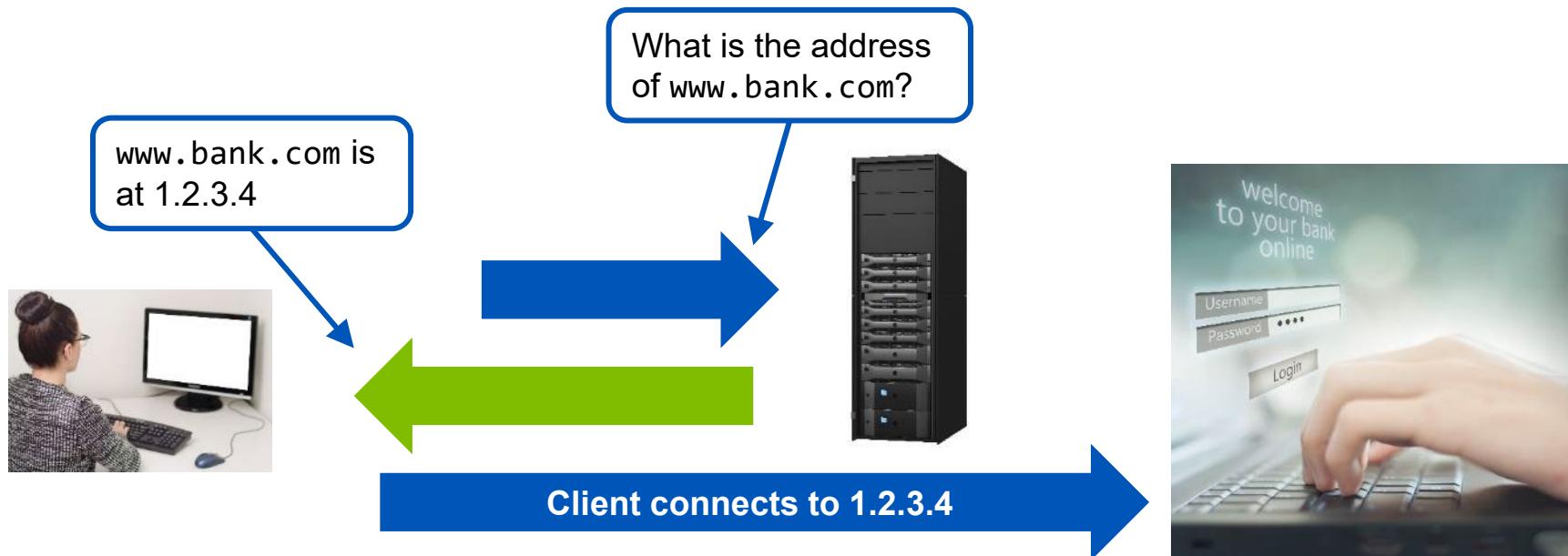


Well-Known Ports and Services

Protocol	Full Name	Port/Number
DNS	Domain Name Service	TCP & UDP/53
FTP	File Transfer Protocol	21/20
HTTP	Hypertext Transfer Protocol	80
HTTPS	HTTP over SSL/TLS	443
SMB	Server Message Block	135, 139, 445
LDAP	Lightweight Directory Access Protocol	389
RDP	Remote Desktop Protocol	3389
SSH	Secure Shell	22
SFTP	Secure FTP	22
SCP	Secure Copy	22
DHCP	Dynamic Host Configuration Protocol	UDP/67 & UDP/68

Domain Name Service

- ▶ **UDP/53 for queries and TCP/53 for zone transfers**
 - Most popular software is called BIND (Berkeley Internet Name Domain)
- ▶ **Clients connect to servers by IP address, not domain name**
 - DNS servers resolve the name to an address
 - Primaries and secondaries provide load balancing and high availability
 - Primaries should only synchronize with known secondaries
 - Enforce with router ACLs



Domain Name System Security Extensions (DNSSEC)

- ▶ **DNSSEC is an addition to DNS**
 - Allows DNS responses to be validated
 - Validates registration of dynamic DNS in DNS servers
 - Uses TSIG records with PKI data
 - Provides
 - Origin authority
 - Data integrity
 - Authentication
 - Denial of existence
- ▶ **A resolver can use public key cryptography to prove the integrity and authenticity of the DNS data received**

TSIG = Transaction signature

File Transfers

- ▶ **TCP/21 and 20**
 - Port mode uses TCP/21 and TCP/20
 - Passive mode uses TCP/21
- ▶ **TFTP involves no authentication and uses UDP/69**
- ▶ **A simple protocol that allows upload and download**
 - Cleartext—credentials may be seen with a protocol analyzer

Source	Destination	Protocol	Info
10.1.1.216	10.1.1.200	FTP	Response: 220 3Com 3CDaemon FTP Server Ve
10.1.1.200	10.1.1.216	FTP	Request: USER quasimoto
10.1.1.216	10.1.1.200	FTP	Response: 331 User name ok, need password
10.1.1.200	10.1.1.216	FTP	Request: PASS notredame



- ▶ **Use encrypted versions for confidentiality**
 - FTP over SSL/TLS (FTPS) TCP/990
 - Secure File Transfer Protocol (SFTP) and Secure Copy (SCP) are based on SSH—TCP/22

Telnet and Secure Shell

► **Telnet is an old protocol**

- TCP/23
- Cleartext
- Character-based

► **Secure Shell (SSH) is a preferred replacement**

- Used for accessing UNIX systems, routers, and switches
- TCP/22
- Incorporates SFTP and SCP over the same ports
- SCP is non-interactive

```
c:>telnet 1.2.3.4  
Connecting to 1.2.3.4  
  
[connecting]
```

```
Linux (00:49 Saturday, 23 January 2011)  
Login: fred  
Password: fredpw [password not shown]  
Last Login: Fri Jan 23 23:17:52 from  
4.5.6.7
```

```
fred@1.2.3.4 $ pwd <CR>  
/files/home/
```

```
fred@1.2.3.4 $ exit <CR>  
Logout
```

Connection to host lost.

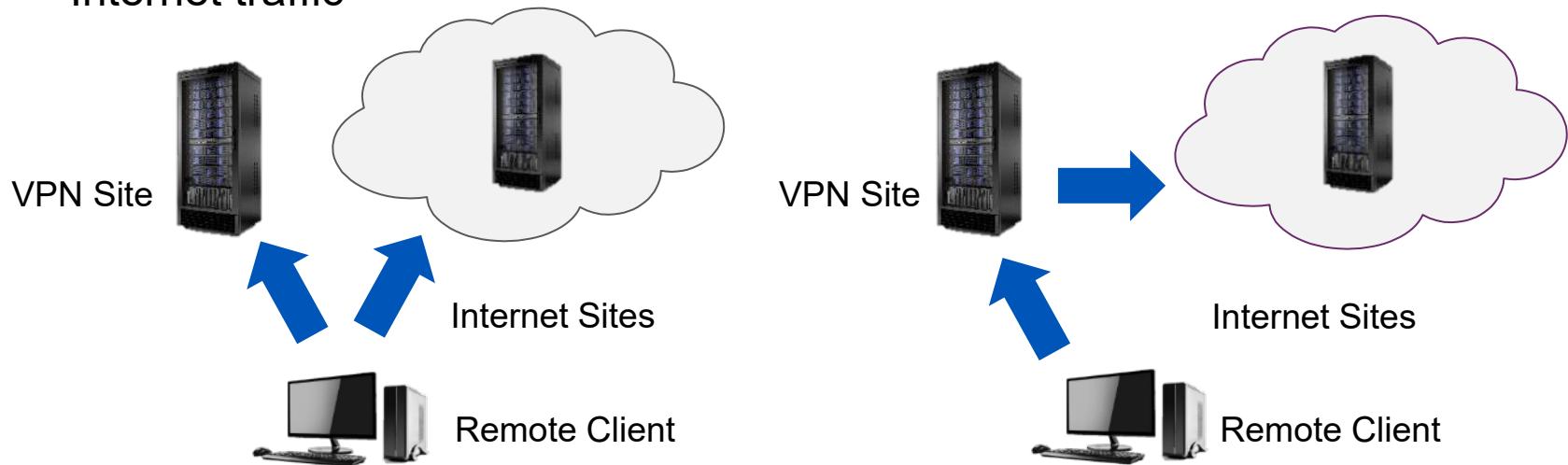
```
c:>
```

Configure SSH for Certificates

- 1. Go to the Instructor125 machines running Kali Linux**
- 2. Open a command prompt and generate a pair of public and private keys**
`ssh-keygen -t rsa`
- 3. Copy your public key to the authorized list for the server and account**
`cat /root/.ssh/id_rsa.pub > /root/.ssh/authorized_keys`
- 4. Note: In a production environment, this would likely have to be sent to a remote server, E.g.: ssh-copy-id <user>@<server IP>**
Not needed here
- 5. Reload the SSH server**
`service ssh restart`
- 6. Test by connecting to it and accept any warnings**
`ssh root@10.1.1.125`
- 7. This account can now perform passwordless authentication**

Transport Security

- ▶ For remote access and telecommuting, encryption should be used
 - Mitigates eavesdropping threat
- ▶ A VPN may involve
 - Tunneling
 - Encrypting and authenticating packets
- ▶ Split Tunnel vs. Full Tunnel
 - Split tunnel allows traffic to go to a VPN site or other Internet sites
 - Full tunnel (mandatory) requires all traffic to pass through a VPN site, even Internet traffic

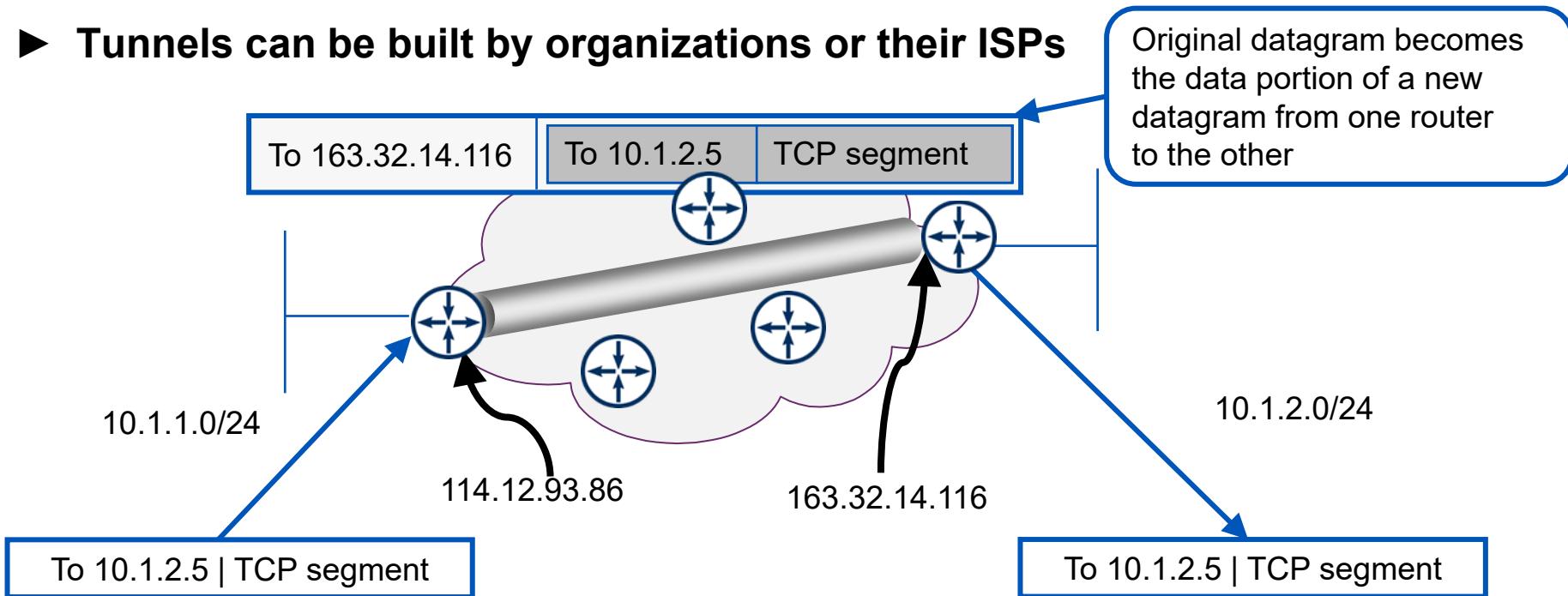


Virtual Private Network (VPN) Overview

- ▶ **A VPN helps enforce security with transport encryption and authentication**
 - Confidentiality
 - By encrypting data
 - Nonrepudiation
 - No modification
 - Authenticity
- ▶ **The basic steps involved in using a VPN are to**
 - Create a tunnel
 - Authenticate the endpoints
 - Negotiate the encryption/integrity parameters
 - Commence sending the protected data
- ▶ **Always On VPN**
 - Where a client is configured to authenticate and establish a VPN immediately after local logon
 - No delay in accessing remote sites or servers via VPN

Tunneling (Encapsulation)

- ▶ **Carrying a protocol layer over the same or a higher protocol layer**
 - The encapsulated packets may or may not be encrypted
- ▶ **Allows traffic from a private network to be sent over public network**
- ▶ **Tunnels can be built by organizations or their ISPs**



Tunneling Protocols

- ▶ Tunneling requires that a header be added after IP, which tells the receiver that the packet has another packet within
- ▶ Layer 2 Tunneling Protocol (L2TP)*
 - Can tunnel IP, as well as other protocols
 - Creates just the tunnel, not encrypted
- ▶ Transport Layer Security / Secure Sockets Layer (SSL)
 - May be used to encrypt payloads of a tunneled protocol
- ▶ IP Security (IPsec)
 - Used for remote access
 - Considered the most secure
 - Provides a Layer 3 encrypted VPN *between networks* (router to router)
 - Individual systems can connect to remote networks in *transport mode*
 - Only the IP data is encrypted
 - The headers are unchanged

*Does not automatically perform encryption; left to IPsec or other protocols

Encrypting Payloads With SSL and TLS

► **TLS**

- Newer and succeeds the older SSL v3
 - Note many still refer to this as SSL
- Encryption is applied to Layer 7 data
- Port TCP/443 is the well-known port for secure web pages
- Uses RSA to encrypt negotiations and key exchanges
- Has more advanced encryption and hashing with AES, SHA-2

► **SSL—now deprecated**

- Vulnerable to POODLE and Heartbleed attacks

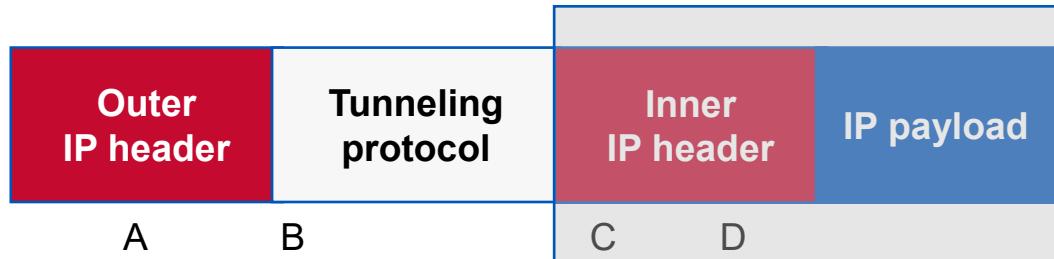
► **Enforce with HSTS and HTTPS redirects for sensitive pages**

► **Used with online transactions and VPNs**

- Can be used for any TCP-based protocol (POPS, LDAPS, FTPS)

VPN Tunneling

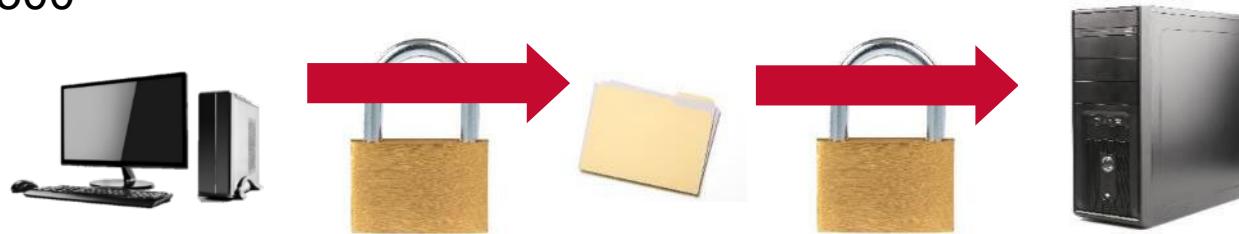
- ▶ With a VPN, the inner packet is encrypted and/or protected against modification
 - Tunneling is typically for site-to-site traffic
- ▶ Packet goes through Layer 3 twice
 - The original packet (C)
 - The packet delivered across the Internet (A)



- A. Outer IP routes over the public IP network
- B. Tunneling protocol: GRE, PPTP, IPsec, or L2TP
- C. Encrypted: Inner IP delivers between private networks
- D. Encrypted: Payload delivered between private networks

IPsec

- ▶ **Designed by the IETF for IPv6, but retrofitted to work over IPv4**
 - Considered by CompTIA as the most secure VPN protocol
 - A mandatory component of IPv6
- ▶ **Secures communication with**
 - Encapsulating Security Payloads (ESP) encryption, and/or
 - IP protocol 50
 - Can provide replay and integrity measures as well
 - Authentication Header (AH) a secure hash of content
 - IP protocol 51
- ▶ **Negotiates and authenticates with Internet Key Exchange (IKE)**
 - UDP/500

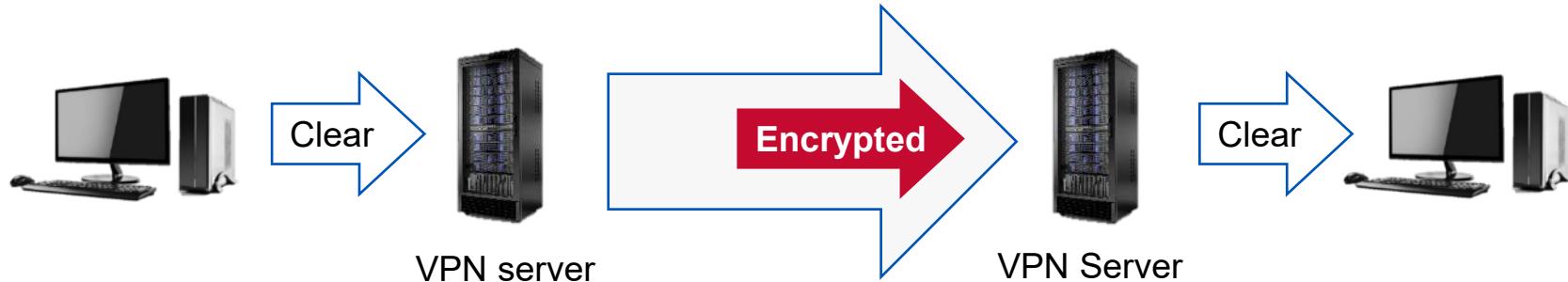


IETF = Internet Engineering Task Force

Tunnel vs. Transport Mode

► IPsec has two modes

- Tunnel is used for putting one packet inside another for data between two perimeters over the Internet
- For site-to-site traffic



- Transport mode is used point-to-point, such as a secure connection between two routers
- For remote workers connecting into the site



Securing Communication

- ▶ **Software-defined wide area network (SD-WAN)**
 - A network architecture that uses software to control and manage the network path between different locations
 - Well-suited for organizations with distributed locations
 - Performance
 - Cost
 - Agility
- ▶ **Secure access service edge (SASE)**
 - Secure access service edge (SASE) is a cloud-based security framework that combines network security and wide area network (WAN) capabilities into a single service, including
 - CASB
 - SWG
 - ZTNA

Domain 6: Match the Items to the Topics

Do Now

Item	Answer	Topic
WAN Security		A. VLAN
No Sex, Gambling, Anarchy		B. Split tunnel
Hard to see, not encrypted		C. SDN
Scalable cloud apps		D. Inline
Least secure VPN		E. NGFW
IaC		F. Jump box
Access to a restricted area		G. Containers
More than a UTM		H. SASE
IPS		I. Obfuscation
Secured access by 802.1x		J. DNS filter

For each item on the left, write in one letter from the corresponding letter from a topic on the right

Contents

- ▶ Infrastructure Security Models
- ▶ Implementing Infrastructure Security

Data Protection Measures

- ▶ Implementing Recovery and Resilience



Privacy Technologies

- ▶ **Hashing**
 - A one-way calculation to create a relatively unique message digest
- ▶ **Encryption**
 - Obscuring information such that it cannot be read without special knowledge
- ▶ **Data masking**
 - Redacting identity or meaningful, but unnecessary information
- ▶ **Tokenization**
 - Using a large value to represent a session of communication, like a session ID
- ▶ **Segmentation**
 - Dividing or segregating assets and their access
- ▶ **Permissions**
 - Granting access or a right or authorization to do something
- ▶ **Obfuscation**
 - Confusing or disguising communication, such as by using encoding

A professional woman with blonde hair, wearing a black blazer over a light blue shirt, stands next to a whiteboard. She is smiling and holding a blue marker. The whiteboard behind her has various handwritten terms and arrows: 'REQUEST' at the top left, 'PORT' with an arrow pointing to 'CUSTOMER' in an oval, 'SPECIFICATION' with an arrow pointing to 'CUSTOMER', and 'DEVELOP' partially visible at the bottom left. There is also a network diagram at the bottom.

Demo

Do Now: Obfuscation

- 1. Will these pings work?**
 - a. Ping 127.0.0.1
 - b. Ping 127.233.67.199
 - c. Ping 2145993671
 - d. Ping 0x7FE943C7
 - e. Ping 127.0351.0x43.254
- 2. The last 3 are examples of camouflaged IP addresses**

Data Sensitivity Labels

- ▶ **Data and information systems should be graded to assess the relative importance of the information contained**
 - Critical—data that is essential to the operation of an organization
 - Sensitive—could cause harm to individuals or organizations if it were compromised
 - Confidential—data that is not sensitive, but that still needs to be protected
 - Restricted—only accessible to authorized individuals
 - Private—only accessible to the individual or organization to which it belongs
 - Public—is data that is freely available to the public
- ▶ **These above do no align cleanly with government sensitivity levels**

Data Types

► Regulated

- Personally identifiable information/personal information
- Legal information
- Financial information
- Medical data (protected health information)

► Intellectual property

- Protection associated with original creations of the mind
- Trade secret—requires registration
 - Gives a company a competitive advantage (formulas, processes) and may be protected by law
- Copyright—optional registration
- Trademark—requires registration
- Patent—requires registration

► Human and non-human readable

- Non-human-readable requires special hardware or software to use or interpret

Pop Quiz: Define the Data Type

Based upon the previous page identify the data type

1. BBQ sauce product recipe
2. Your name and address
3. Company logo
4. Binary data with health records



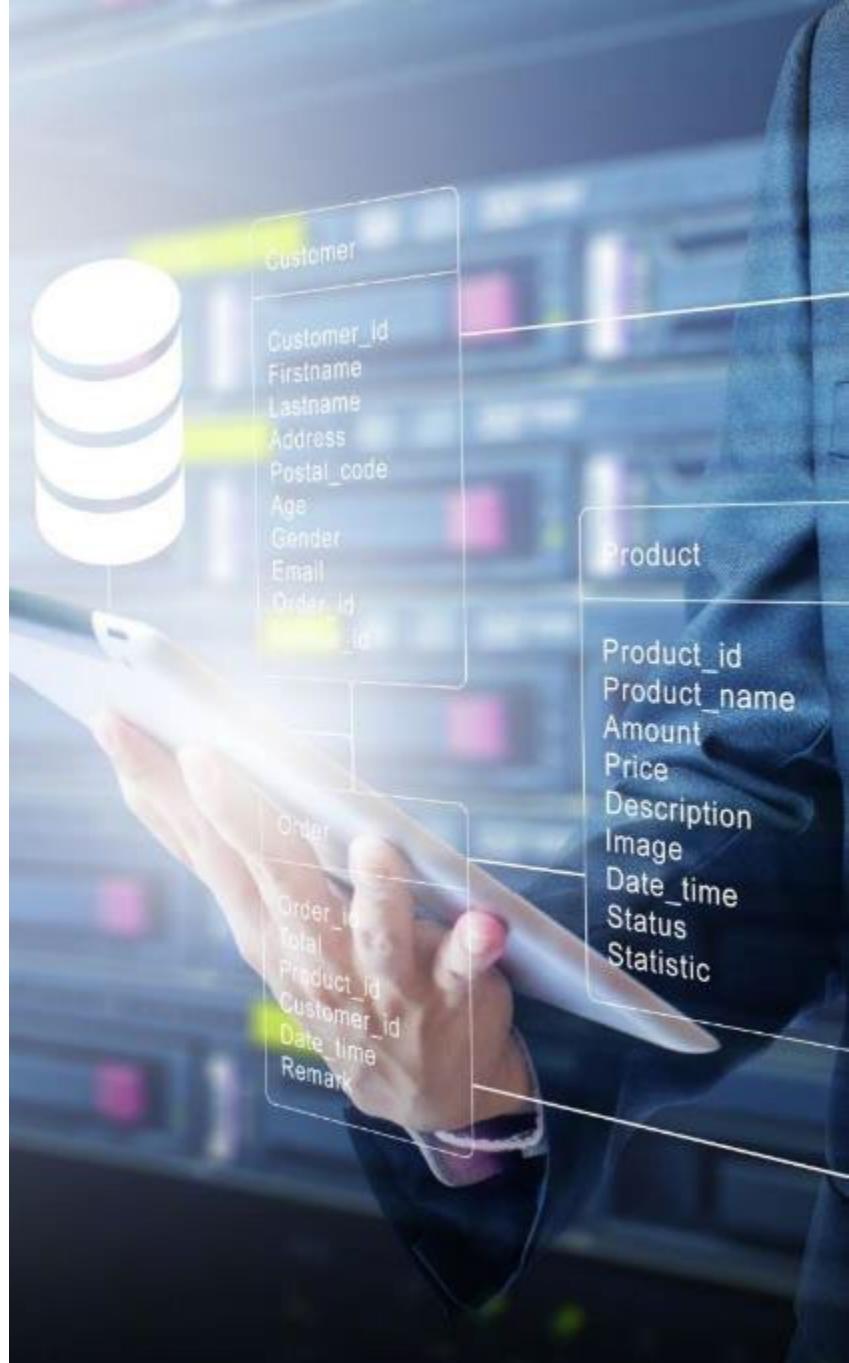
Data Loss Prevention (DLP)

- ▶ **These defensive applications protect**
 - Data in motion—*Being transmitted*
 - Placed near network egress points at the perimeter and analyzes network traffic to detect sensitive data
 - Data at rest—*Stored on disk*
 - Located in data centers to discover if confidential data is moved to or stored on unsecured media
 - Data in use—*Being processed by endpoints*
 - Endpoint-based protection regulates use, as well as internal and external traffic between groups or types of users
- ▶ **Commonly first deployed in monitor mode**
 - Allows testing and detection
 - Exception lists can be built
 - Implement blocking mode when tuned properly

Contents

- ▶ Infrastructure Security Models
- ▶ Implementing Infrastructure Security
- ▶ Data Protection Measures

Implementing Recovery and Resilience



Business Continuity and Disaster Recovery

► Disaster recovery

- The immediate restoration for functioning of the business is key
- Focus on immediate recovery/restoration of operations

► Business continuity

- Longer term: Three to four days and onward
- The focus is on the ongoing operation of the business
- Continuity of operations testing (e.g., powering off a key server to verify how well the alternates can take over the role)

► Succession planning:

- Identifying the assets to take over a key function

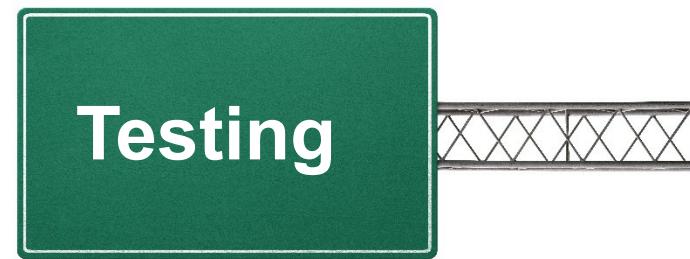


Business Continuity

- ▶ **Business Continuity Plan (BCP)**
 - Identifies the organization's vulnerability to threats
 - Specifies effective prevention and recovery
 - Takes input from Business Impact Analysis
- ▶ **Continuity Of Operations Planning (COOP)**
 - Plans made to ensure ongoing operations even in the midst of unanticipated events
 - Includes requirements for planned service interruptions
- ▶ **Planning should include**
 - Tabletop exercises
 - Reviewing previous Lessons-learned
- ▶ **Contingency planning**
 - A plan created for a specific adverse situation
 - Designating alternate sites means of conducting business

Testing Methods

- ▶ **Tabletop exercises**
 - These are time-efficient tests that involve simulating an incident or emergency
 - Used to train personnel and test procedures
- ▶ **Failover testing**
 - A type of test that verifies that a system or application can fail over to a designated secondary in the event of a failure
- ▶ **Simulations are a type of**
 - This uses computer simulations to emulate the behavior of the subject of the test
 - Simulations may be created/configured to test a wide variety of scenarios
- ▶ **Parallel testing**
 - Involves running a on two or more identical environments.
 - This allows a comparison of the results



Capacity Planning Factors

- ▶ **People—typically the most expensive aspect**
 - Current staffing levels
 - Anticipated demand/needs
 - Lead time for hiring
 - Turnover
- ▶ **Technology**
 - Current capabilities vs needs
 - Refresh cycle
- ▶ **Infrastructure**
 - Current capabilities vs. needs
 - Scalability



Cybersecurity Resilience

► Key areas

- RAID
- Load balancing
- UPS
- Replication
- Backups
- Geography
- Non-persistence
- High-availability
- Diversity

► Redundant Array of Independent Disks (RAID)

- Also called Redundant Array of Inexpensive Disks
- Fault tolerance involves striping—spreading data across one or more disks
- May interfere with disk forensics
- Least expensive way to provide fault tolerance at the disk level

Resilience: Alternate Sites

Be able to differentiate between these types of alternate sites:

- ▶ **Cold site—greater than one-week readiness**
 - Just a location, may include minimal equipment
 - Still needed: Data synchronization, communication lines, and personnel
 - Least expensive
- ▶ **Warm site—less than one-week readiness**
 - Includes some office equipment and computer systems
 - Will not be fully synchronized, configured, or include up-to-date configurations
- ▶ **Hot site—immediate readiness**
 - A copy of the original site
 - Includes communications, computer systems, and data replication
 - The most expensive
- ▶ **Geographic dispersion/geo-redundancy**
 - Storing backup data in multiple locations

Diversity

- ▶ **A defense in depth strategy that implements products from multiple vendors**
- ▶ **Vendor diversity**
 - A mono-culture of a single vendor is far easier to bypass than one made of multiple vendors
 - Varying defense techniques
 - Uncertainty bypass techniques for the attacker
- ▶ **Diversity helps to ensure there is no single point of failure**
 - Technology
 - Vendors
 - Cryptography
 - Security controls and measures
 - Multi-cloud systems
 - Computing systems that use resources from multiple cloud providers

Power Availability

- ▶ **Dual power supplies**
 - Components within a system that control and condition power
 - Two units allows for redundancy and greater power supply range
- ▶ **Uninterruptable power supplies**
 - Widely varying devices that provide short term recovery, depending on stored energy and load
 - Provides power conditioning
 - May be in-line or cut-over
- ▶ **Generators**
 - More expensive solution and needed for long term supply of power

Backup Types

- ▶ **Imaging**
 - Copies the entire disk as an image (ghosting), used for forensic examinations
 - Full system backup, archive attribute *not* reset
- ▶ **Snapshots**
 - A virtualization term associated with Last Known Good
- ▶ **Full**
 - Full system backup, archive attribute reset
- ▶ **Incremental**
 - Goes back to last incremental or full backup
 - Only files with the archive attribute set
 - Archive attribute reset

Fastest to back up,
slowest to restore
- ▶ **Differential**
 - Goes back to last full backup only—archive attribute *not* reset Only files with the archive attribute set (since the last full backup)

Slowest to back up,
fastest to restore

Additional Backup Types and Considerations

► **Journaling**

- A method of tracking changes to a system so that only the changes need to be backed up
 - Reducing the amount of data that needs to be transferred

► **Replication**

- Duplicating the data to another location
- May be performed by journaling, snapshots, full table or transactions

► **Other factors**

- Frequency—dependent on the RPO and RTO
- Encryption—security for the data

► **Recovery**

- Speed
- Complexity
- Reliability



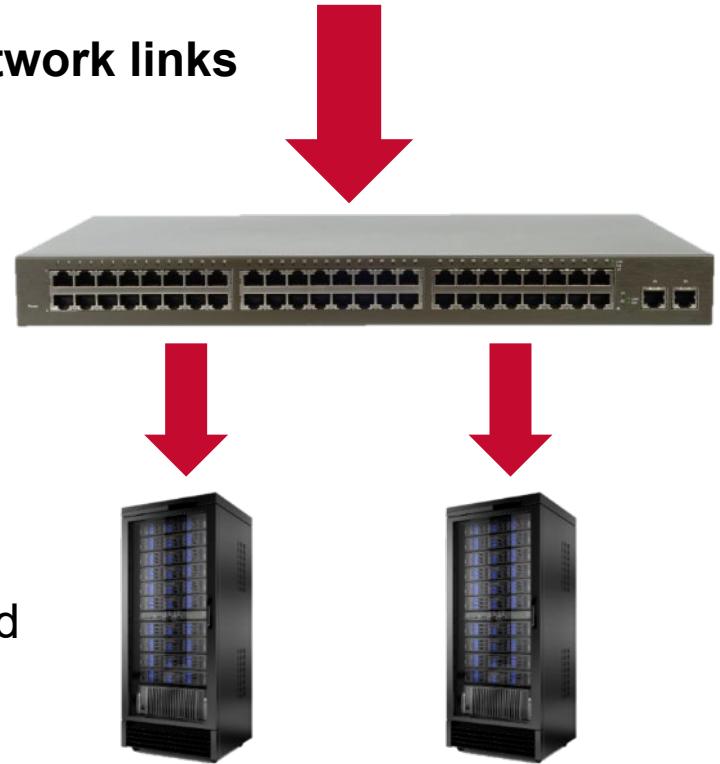
Geographic Considerations

- ▶ **Off-site backups and replication**
 - Distance—can the data be accessed in a timely manner?
 - Location selection—is the new location safe from the same disaster?
- ▶ **Legal implications**
 - Data sovereignty
 - The destination may have differing privacy laws
 - Control/access to the data may change
 - Privacy
 - There may be legal issues with moving certain data (PII) to another jurisdiction



Load Balancers, Teaming, and Clusters

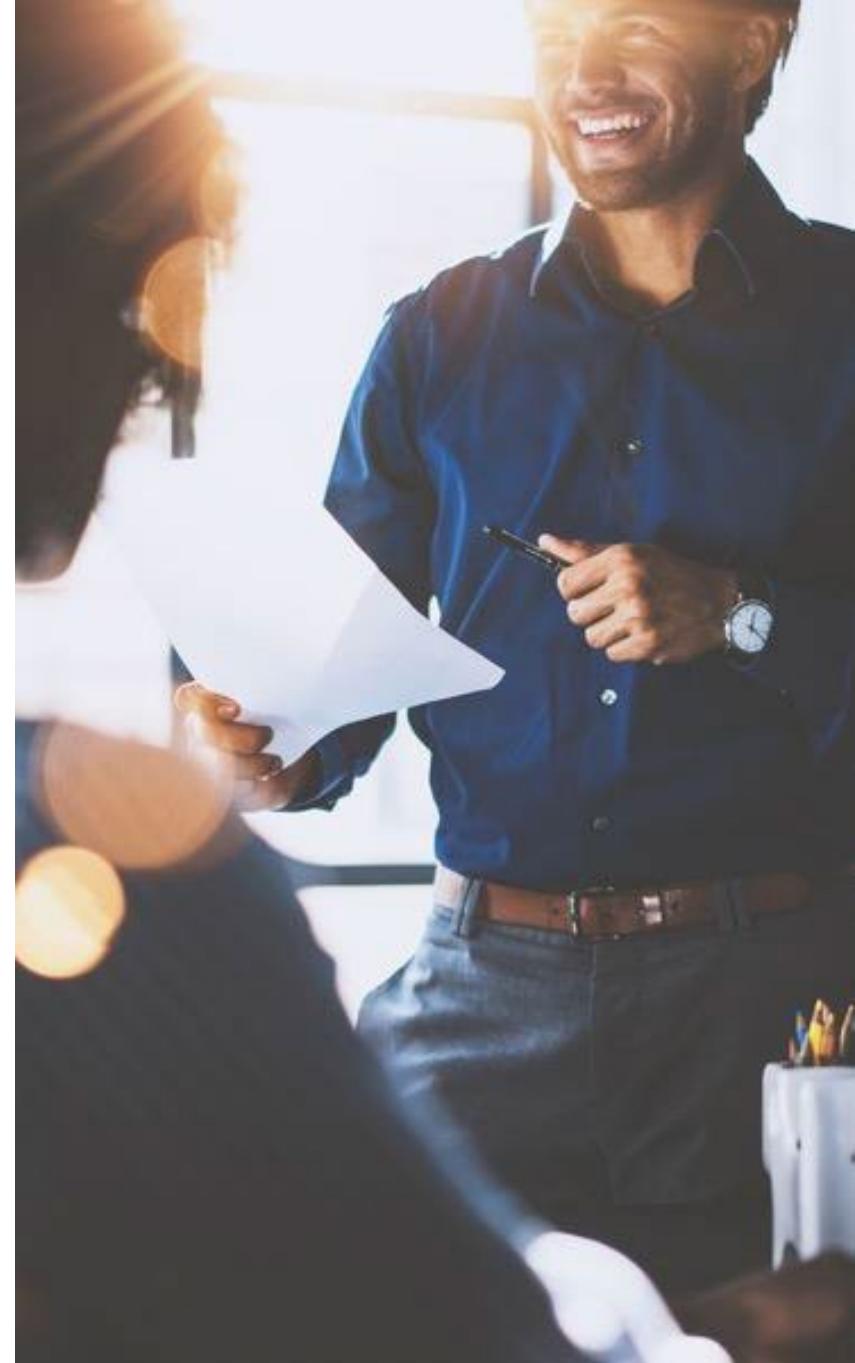
- ▶ Systems that distribute workload across network links
- ▶ They will implement
 - Caching and compression
 - TCP pooling and distributing
 - SSL/TLS offloading
 - Content routing
- ▶ Clustering
 - Grouping of multiple computers together to work as a single system, providing increased performance, availability, and scalability
- ▶ NIC Teaming
 - Provides dual connections and failover for servers
- ▶ Implemented with
 - Dedicated hardware
 - Simple algorithms, like Domain Name System—Round Robin



Objectives

- ▶ **Understanding infrastructure security models**
- ▶ **Securing the infrastructure**
- ▶ **Protecting data**
- ▶ **Implementing resilience and recovery**

18%

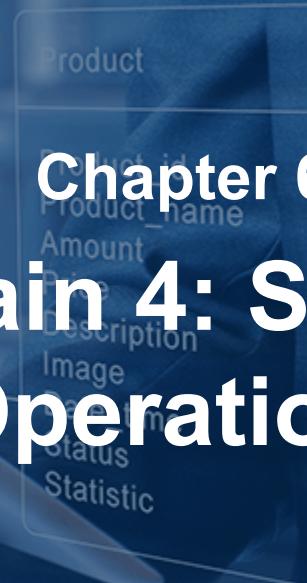




Chapter 6

Domain 4: Security

Operations

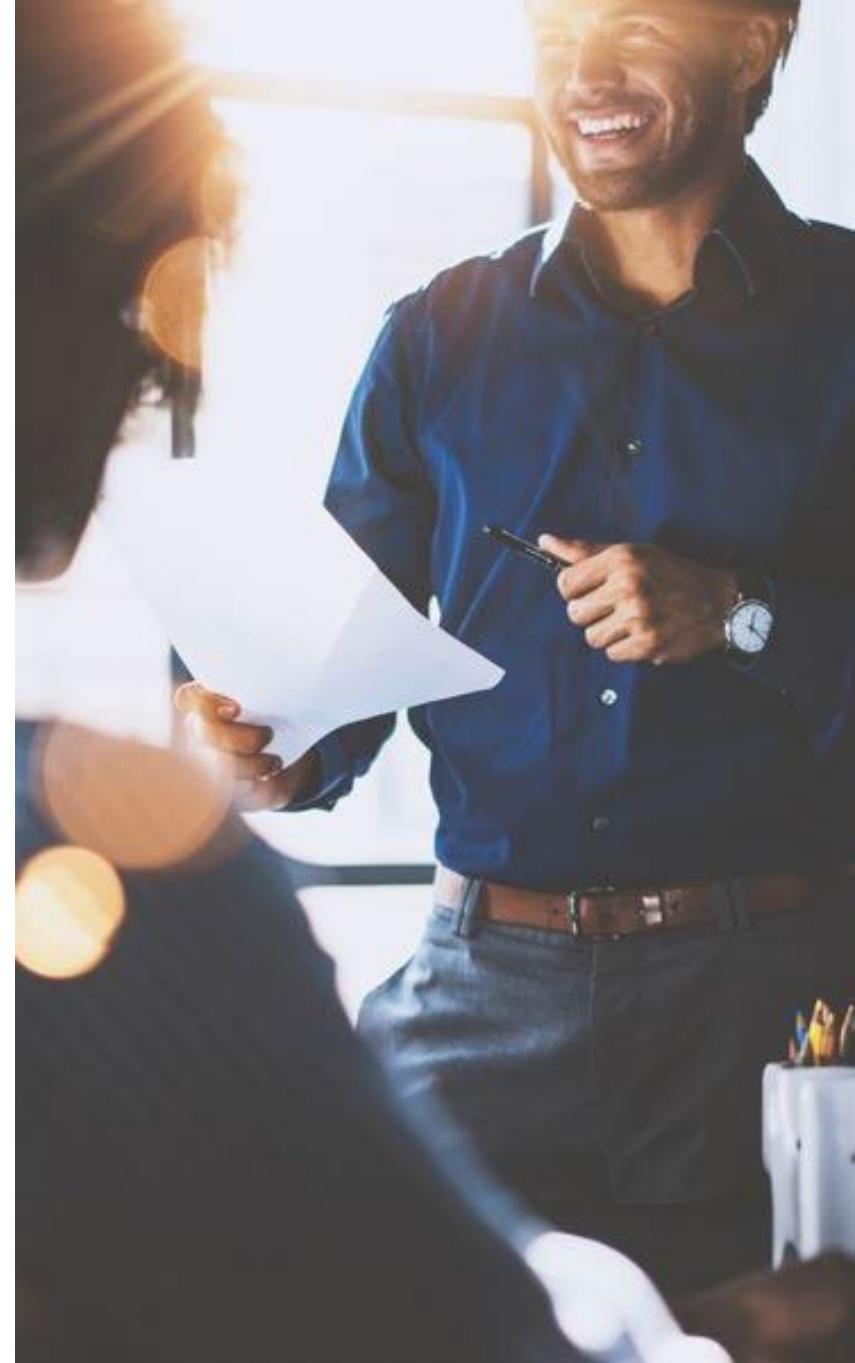


LEARNING TREE™
INTERNATIONAL

Objectives

- ▶ **Inspect common security measures**
- ▶ **Identify proper asset management**
- ▶ **Manage vulnerability in the enterprise**
- ▶ **Monitor and alert for security incidents**
- ▶ **Implement strong enterprise security**
- ▶ **Select the appropriate identity and access management**
- ▶ **Understand how to automate security**
- ▶ **Respond to incidents and investigations**

28%



Contents

Common Security Measures

- ▶ Asset Management
- ▶ Vulnerability Management
- ▶ Monitoring Security
- ▶ Enhancing Enterprise Security
- ▶ Identity and Access Management
- ▶ Security Automation
- ▶ Incidents and Investigations



Best Practices and Policies

- ▶ **Follow a baseline lifecycle**
 - Provision
 - Harden
 - Configure
 - Adequate storage and RAM
 - Match the policy baseline
 - Scan for vulnerability
 - Deploy
 - Maintain
 - Deprovision when no longer used
- ▶ **Industry standards recommend the following practices be implemented as policy to secure an organization's assets against misuse and fraud**
 - Least privilege
 - Separation of duties
 - Job rotation
 - Mandatory vacation
 - Clean desk audits, background checks, and account and rights reviews

Fraud Prevention Policies

► **Least Privilege**

- Also known as minimal privilege and least authority
- Requires that a person is only accorded rights, capabilities, or access necessary to perform a task or job (e.g., web developers can modify code but not manage the application)

► **Separation of duties**

- Ensuring that no one person has privileges that allow one to commit and conceal illicit acts
- Prevents fraud (e.g., one person manages configurations and a different person tests and validates them)

Fraud Prevention Policies

► Job rotation

- Users are less likely to misuse resources, knowing that someone else will be periodically doing their job
- Giving others cross-training mitigates single-point-of-failure issues and prevents burnout

► Mandatory vacations

- This ensures a different person will be performing a function and may notice signs of improper activity
- Management has an opportunity to look for signs of fraud
- Most recommendations are for at least one full week away each year

Fraud Prevention Policies

► Clean desk

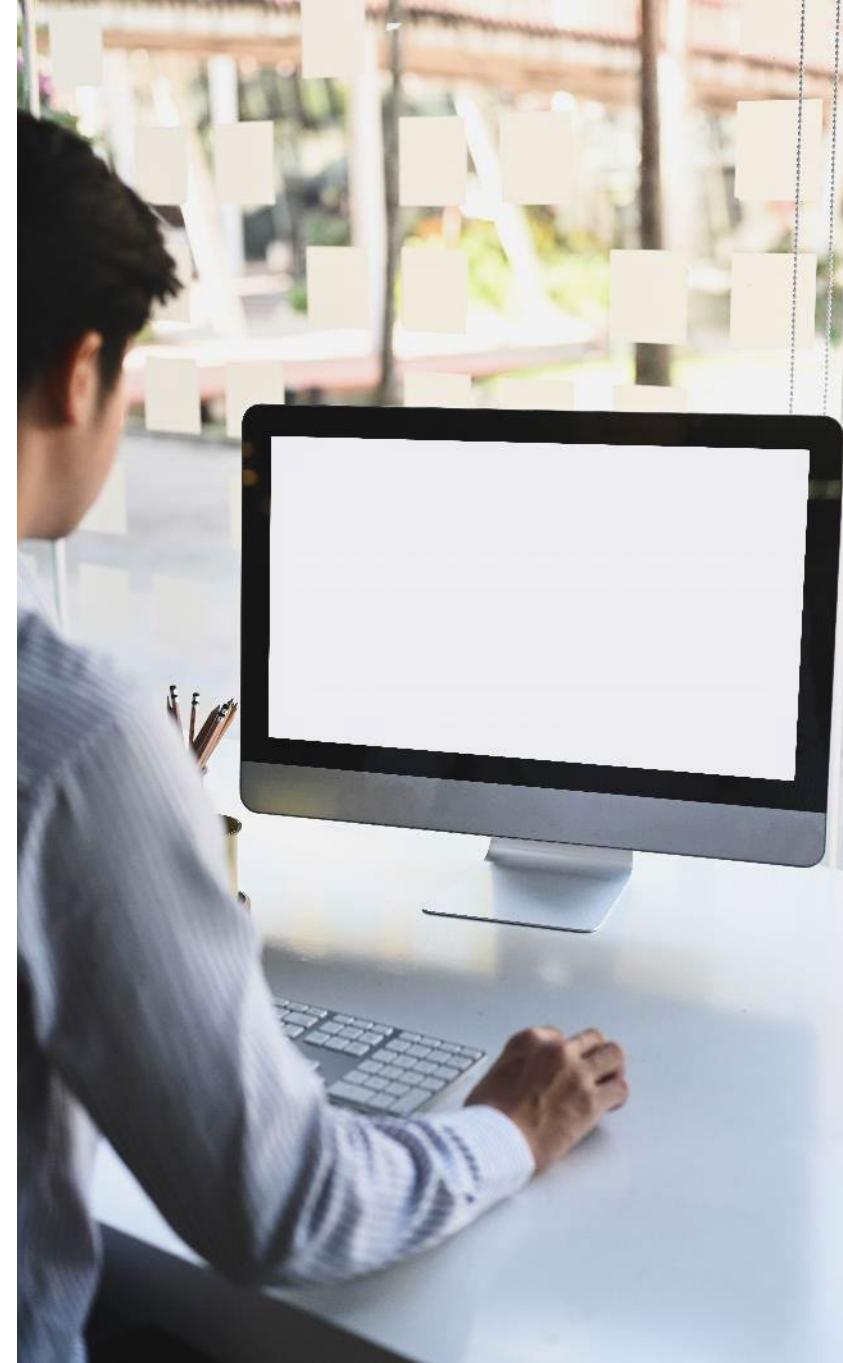
- Eavesdropping and need to know failures may be mitigated with this policy
- Information theft, fraud, or a breach could occur when sensitive information is easily in view

► Background checks

- Credit checks for possible financial issues
- Criminal check for behavioral or work history problems
- Address and travel information may reveal undesired associations

Hardening

- ▶ **General purpose systems**
 - Workstations
 - Servers
 - Mobile devices
- ▶ **Infrastructure**
 - Switches
 - Routers
- ▶ **Cloud infrastructure**
- ▶ **Specialized systems**
 - ICS/SCADA
 - Embedded systems
 - RTOS
 - IoT devices



General Purpose Systems

- ▶ **User account**
 - A standard account for use of a system
- ▶ **Privileged accounts (for Admins)**
- ▶ **Guest accounts**
 - Minimal rights
- ▶ **Shared and generic**
 - Generally forbidden, as accountability is lost
 - May be necessary for some access controls (doorway cipher locks)
- ▶ **Service accounts**
 - For servers and applications
 - Passwords seldom change
 - Privileges are fixed
 - No interaction generally possible

Policy should determine the strength, type and complexity of required credentials for any account



Account Management

► Periodic recertification and audits

- Scripting and automation should be used to efficiently and reliably remove privileges and users
- Validates the purpose of the account
- Certifies privileges and memberships in groups
- Discovers terminated employees with access and those without valid use
- Audits usage levels

► Standardized account naming

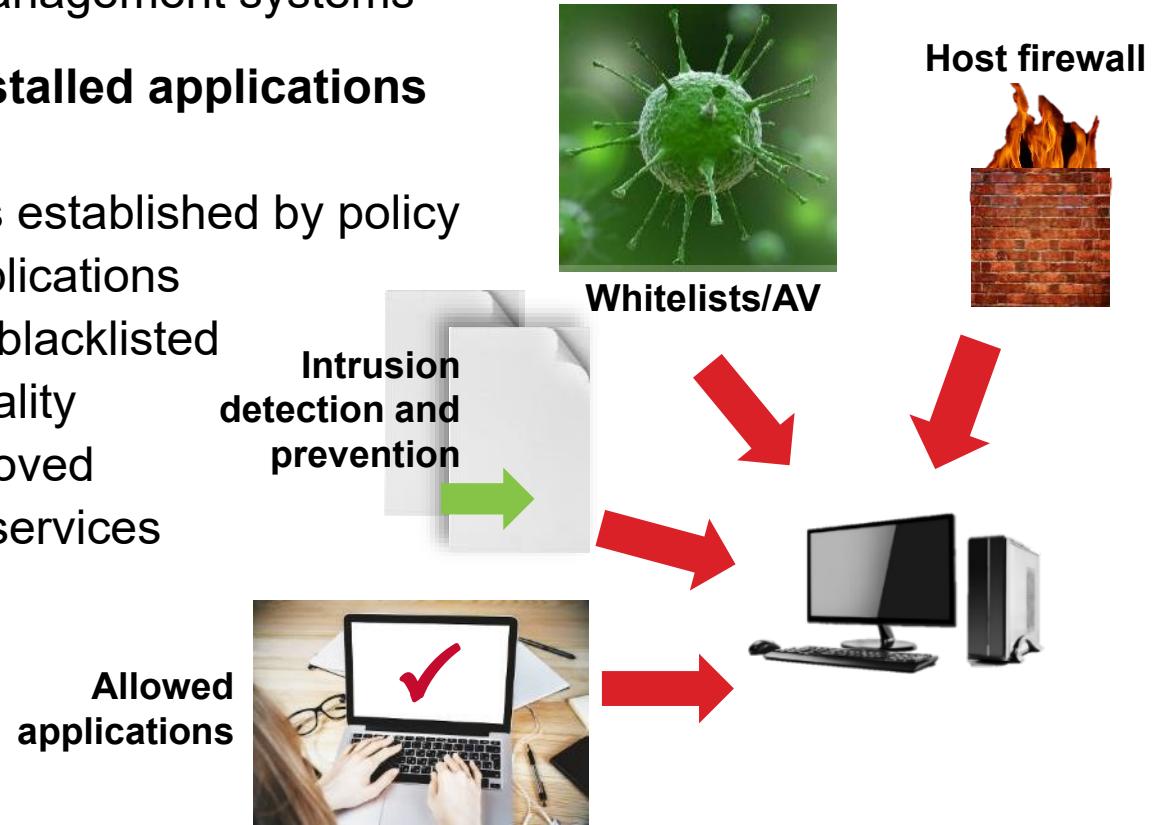
- Creates a naming structure that allows for logical and memorable IDs
- Allows for identical and near identical names
- Can be used to easily sort and recognize types of accounts
- Helps to identify rogue accounts

► Regular maintenance and auditing

- Typically, annual, or after incidents

Host Software Baselines

- ▶ **Part of configuration management and systems hardening**
 - Maintained by patch-management systems
- ▶ **Regulate settings and installed applications**
 - Trusted OS
 - Secure configuration as established by policy
 - Required defensive applications
 - Forbidden applications blacklisted
 - Least privilege/functionality
 - Default passwords removed
 - Disabled unnecessary services
- ▶ **It serves to reduce risk by enforcing defensive measures**



AV = Antivirus

Mobile

- ▶ To deploy mobile devices securely, many factors must be considered
- ▶ Mobile device threats
 - Loss
 - Theft
 - Casual eavesdropping
 - Tracking
 - Wiping
 - Applications
 - Intermingling organization and personal apps and data



Deployment Models

- ▶ **Bring Your Own Device (BYOD)**
 - Allowing or encouraging employees to use their own phones, tablets, and laptops at work
- ▶ **Choose Your Own Device (CYOD)**
 - Employees choose from a limited selection of approved, corporate-owned devices
 - The MDM must handle the security differences in various types of devices
- ▶ **Corporate Owned, Personally Enabled (COPE)**
 - A smartphone chosen and paid for by the organization
 - Employees may use the device for personal purposes
 - Allows tighter control, simpler for MDM
- ▶ **Virtual Desktop Infrastructure (VDI)**
 - Users connect to the virtual server that then directs them to their personal files and applications
 - The server hosts and updates all applications and stores all data
 - May be accessed from many types of devices

Bring Your Own Device (BYOD)

- ▶ This can reduce costs and increase morale by leveraging existing equipment
- ▶ BYOD concerns
 - Handling noncompliant systems
 - Maintaining diverse assets to support the owner
 - Intermingling corporate and personal data on an asset
 - Unsafe or unwanted applications
 - Registration and identification
 - Ensuring encryption and access control
 - Managing and auditing BYOD devices on the corporate network
- ▶ Many security vendors are offering MDM
 - MDM tools attempt to remediate the above issues
 - Implement security features across smartphones, laptops, and tablets



Mobile Connections

► Cellular

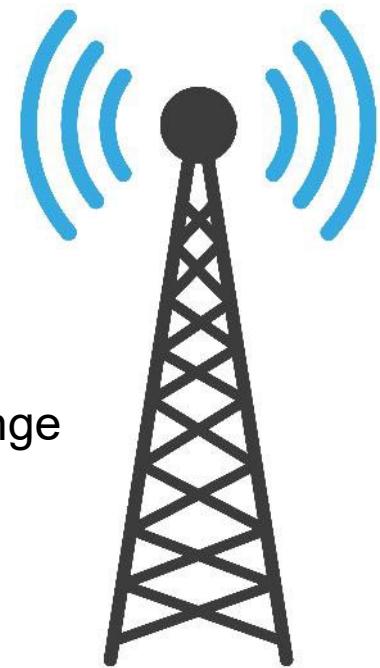
- Ubiquitous, world-wide, and may or may not be encrypted

► Wi-Fi

- Using 802.11 protocols
- Subject to WLAN security

► Bluetooth

- Short range
- Low security
- Various classes up to 25 mbps speed and 10m-100m range



Other Mobile Connections and Protocols

► NFC

- 4cm range, 424 Mbps speed
- For close-proximity transactions

► ANT

- Proprietary, commonly used with sensors (Garmin), 30M range, 12.8 kbps speed

► Infrared

- Range 1- several meters, speed 2.4 Kbps to 1 Gbps

► USB

- Manual insertion
- Varying storage amounts

Pop Quiz: Connection Protocol



- 1. At a high-security organization, it is desired to implement turnstile security**
- 2. A requirement is that a mobile devices be possessed by an individual that broadcasts a signal to perform the authentication**
- 3. Which protocol should be used?**

Tablets, iOS, Android, and Smartphones

- ▶ **Cell phones have the potential for viruses, theft, eavesdropping, and interacting with internal networks**
 - Geo-tagging—using metadata in photos to track user activity and location
 - Infection by malware in smartphone apps
 - Cell phones may retrieve and store confidential e-mails
 - Intruders may connect rogue systems to internal networks to tap or interact with the local environment
- ▶ **Device and data security may be addressed by**
 - Mobile Device Management (MDM) software
 - Mobile Application Management (MAM)

Management of Mobile

- ▶ **Whitelisting allowed applications**
 - Allowing only known good applications to execute
- ▶ **Content filtering**
 - Stored and network
- ▶ **Screen lock with PIN access and device lockout**
 - Basic defense against eavesdropping and intrusion
- ▶ **Biometrics**
 - Most secure authentication factor
- ▶ **Device data encryption**
 - Enhanced defense to prevent exposure of sensitive information
- ▶ **Remote wiping and sanitizing**
 - Best prevention against data exposure
- ▶ **GPS tracking**
 - Recovery of device

Hardening Infrastructure Devices

- ▶ **Configuring and managing infrastructure devices, such as switches and routers, to reduce the risk**
 - Using strong passwords
 - Passwords for infrastructure devices should be strong and complex and should be changed regularly.
 - Enabling SSH and disabling Telnet
 - Only secured protocols should be used for management
 - Disabling unused ports and services
 - Any ports or services that are not needed should be disabled to reduce the attack surface of the device
 - Restrict access with access control lists (ACLs)
 - Restrict access to users and devices
 - Keeping OS/firmware up to date
 - To date to mitigate known vulnerabilities
 - Establish a dedicated management network
 - Implement intrusion monitoring



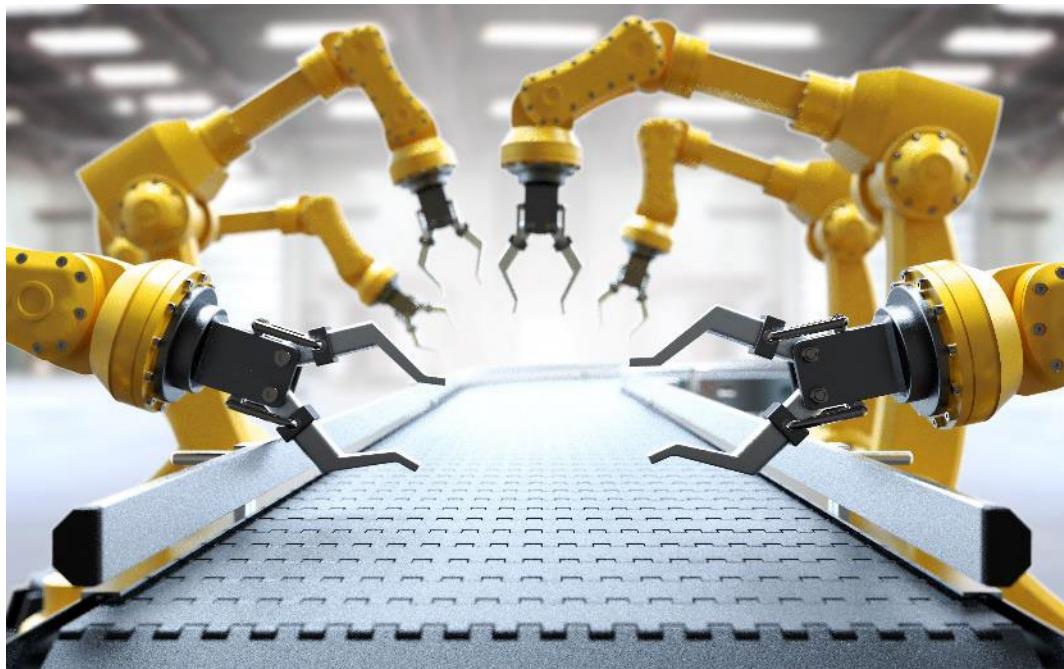
Cloud Infrastructure Hardening

- ▶ **Involves implementing a variety of security controls and practices**
 - Identity and access management (IAM)
 - IAM controls define who has access to cloud resources and what they can do with them
 - Data encryption
 - Data encryption protects data at rest and in transit
 - Network security
 - Network security controls protect cloud resources from unauthorized access
 - Logging and monitoring
 - Logging and monitoring controls collect and analyze data to identify and respond to security incidents
 - Security patching
 - Security patching involves applying security updates to cloud resources to mitigate known vulnerabilities
- ▶ **This reduces risk and helps with compliance**



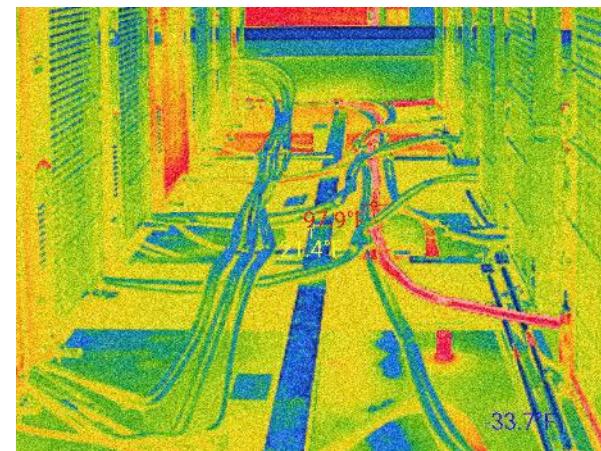
Hardening Specialized Systems

- ▶ **IoT, Operational Technology, SCADA, Embedded systems**
 - Notoriously difficult to defend
- ▶ **The devices themselves are simple and have no defensive capabilities**
 - Isolate in a perimeter/zone
 - Remote access via jump boxes
 - Implement intrusion detection systems



Wireless

- ▶ **Wireless security is essential for protecting your data and devices from unauthorized access and attacks**
- ▶ **Security may be augmented with**
 - MAC filtering—easily bypassed
 - 802.1x and EAP authentication
 - Separate guest from production by VLANs
 - Placement in the center of coverage area
 - Maps help ensure proper placement
 - Perform regular site surveys and scan for rogue devices
- ▶ **Heatmaps can be used for a variety of purposes, including:**
 - Identifying weak coverage
 - Highlighting excessive coverage



EAP = Extensible Authentication Protocol

SSID = Service Set Identifier

WLAN = Wireless Local Area Network

Wireless Defenses

- ▶ **Wi-Fi protected access WPA/2 or WPA/3 should be used**
 - Part of the 802.11i standard for WPA/2-Enterprise
- ▶ **WPA/2-Enterprise uses EAP for authentication and AES-CCMP for encryption**
 - It is considered the best wireless encryption
- ▶ **WPA/3**
 - Backwards compatibility device issues exist
 - Password protection implemented
 - Resistance to dictionary attacks
 - SAE—Simultaneous Authentication of Equals
 - Using an improved security handshake called Dragonfly
 - Prevents Key Reinstallation attacks

AES = Advanced Encryption Standard

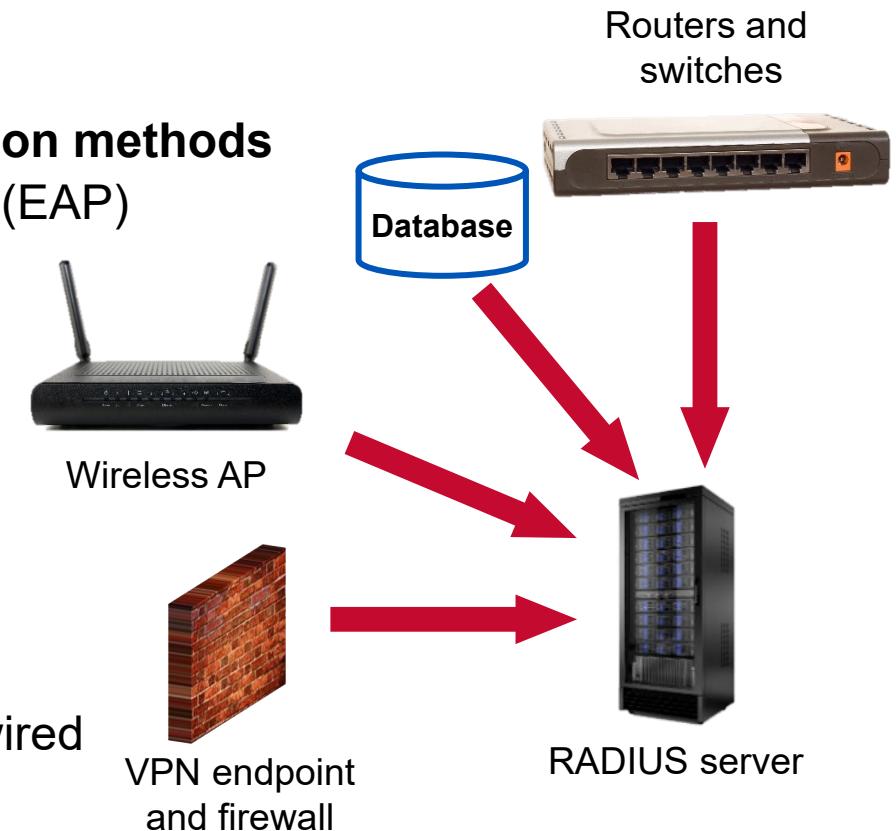
CCMP = Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

EAP = Extensible Authentication Protocol

1. On the instructor demo machine, open a command prompt in the `c:\secret` directory
2. Change to the aircrack directory: `cd aircrack`
3. There are several wireless capture files present in the current directory; we will use these three:
 - `wpa.cap`
 - `wpa2.eapol.cap`
 - `wpa2-psk-linksys.cap`
4. There is also a dictionary file named `password.lst`
5. The dictionary cracking of these files is done with this syntax:
`aircrack-ng.exe capture-file-name -w password.lst`
6. Try cracking the three files

Centralized Authentication Services

- ▶ Network access control can be managed via central authentication and authorization
 - Wired
 - Wireless
- ▶ Single-point control of accounts
- ▶ Handles many different authentication methods
 - Extensible Authentication Protocol (EAP)
 - Hashed
 - Encrypted
 - Challenges
 - Kerberos
- ▶ RADIUS implements AAA
 - Authentication, authorization, and accounting
 - Commonly used for wireless and wired access control



EAP Framework

- ▶ **EAP allows authentication to occur with a variety of mechanisms**
 - It is an Internet standard (RFC-3748)
 - EAP is an authentication *framework*, not a specific authentication mechanism like Kerberos or CHAP
- ▶ **EAP defines how to send other specific authentication protocol data and receive responses**
 - EAP-TLS—PKI and certificate-based authentication
 - EAP-TTLS—Tunneled Transport Layer Security
 - The client is not required to have a certificate (which simplifies the setup)
 - EAP-FAST—Flexible Authentication via Secure Tunneling
 - Cisco developed for wireless
 - PEAP—Protected EAP implements mutual authentication with Transport Layer Security (TLS), CAs, and PKI
 - Often used to encapsulate and protect MS-CHAPv2
 - Can prompt for username and password, not just certificates

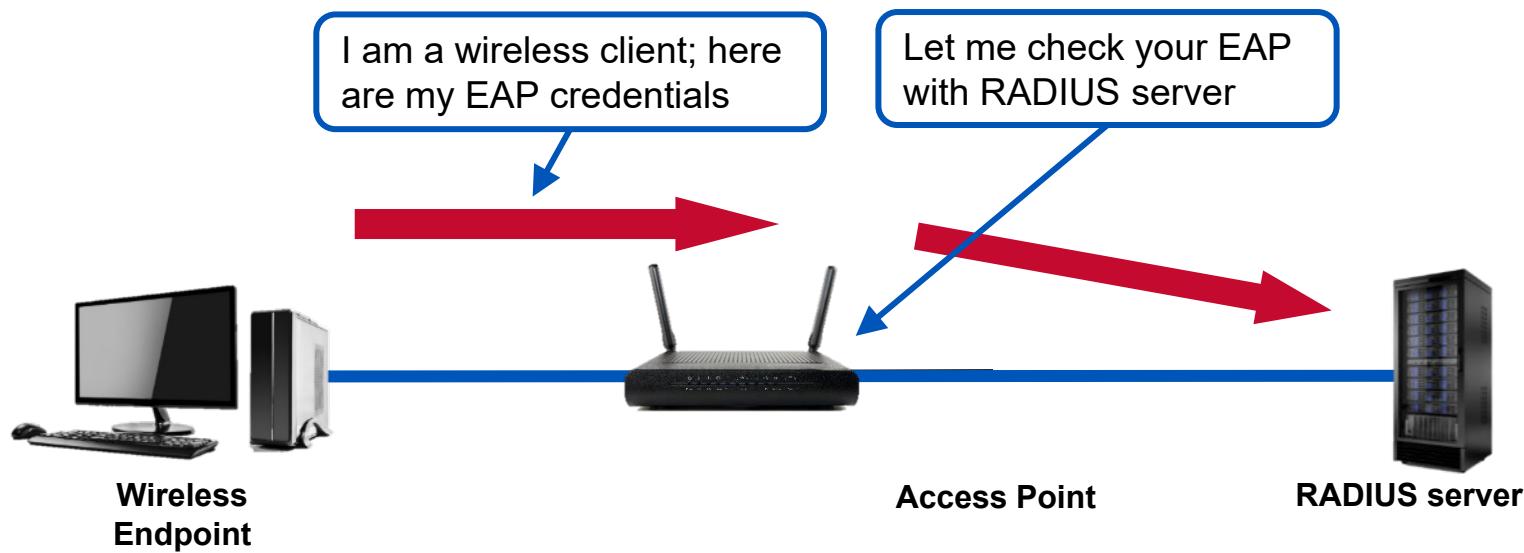
CA = Certificate Authority

MS-CHAP = Microsoft Challenge Handshake Authentication Protocol

RFC = request for comments

RADIUS

- ▶ **Remote Authentication Dial-In User Service (RADIUS)**
 - Originally created in the days of modems
 - Now used as a standard third-party authentication service
 - Must have a valid certificate to be integrated with 802.1x
 - Can handle a variety of authentication protocols
 - Only encrypts credentials from client to server
 - Uses UDP/1812
- ▶ **Diameter is a European-developed version**



Application Security

► Secure development

- Implemented code should have appropriate controls
- The Open Web Application Security Project (OWASP) is commonly referenced

► Secure Cookies

- When set by the server, it will only accept requests via HTTPS, not HTTP

► Version control

- A key aspect of change management
- Stakeholders must approve all changes

► Proper input validation and sanitation

- It may be important to validate data according to:
 - Size: Quantity of data
 - Type: Numbers, letters
 - Range: 0-9, A-Z, Valid Zip Codes
 - Format: ASCII, Hex, Octal

The screenshot shows a configuration dialog for a cookie. The fields are as follows:

- Domain: asafaweb.com
- Path: /
- Expiration: 25/03/2014 05:33 PM
- HostOnly:
- Session:
- Secure:
- HttpOnly:

Below the fields, there is a list item: __utma | .asafaweb.com.

Handling Errors and Exceptions

- ▶ **Errors are to be expected in applications**
 - None are perfect
 - Do not have a contingency for every input or circumstance
- ▶ **Programming techniques exist to handle errors and exceptions**
 - With errors—displays a standard error page
 - Prevents unexpected application crashes
- ▶ **Error pages should not leak technical information, such as error codes**
 - The information should be plain and standard
- ▶ **Data leaks, program crashes, or unexpected behavior indicates a failure**

Login Error:
This user account or password does not
exist.

Correct

Login Error:
This user does not exist.

Incorrect

Improper Error Handling

Demo

- 1. Go to the Instructor Demo PC**
- 2. Open Firefox and click the bookmark link for SQL Injection**
- 3. In the username field, enter:
‘ (a single quote)**
- 4. This displays an error**
- 5. What can the attacker learn?**

Code and Application Testing

► Scanners

- Static Analyzers
 - Perform syntax checking and look for coding errors
 - Typically, slow performance
 - Input source code
 - The output is error and omission results
- Dynamic testing
 - Fuzzing
 - Potentially dangerous to live data or production code

► Credentials

- Some scanning techniques require credentials to be effective
 - Typically administrator/root
- Non-credentialed scans can only probe the anonymous attack surface and may miss items

► Agent-based/agentless

- Mobile devices are usually scanned via installed agents

Other Testing

► Stress testing

- Can take many forms
 - Network loading
 - Data and database access
 - Transactions
 - Scaling upward of client base

► Sandboxing

- Thorough testing can identify sandbox failures
- Determines if processes and data access are confined properly

► Monitoring



Contents

- ▶ Common Security Measures

Asset Management

- ▶ Vulnerability Management
- ▶ Monitoring Security
- ▶ Enhancing Enterprise Security
- ▶ Identity and Access Management
- ▶ Security Automation
- ▶ Incidents and Investigations



Acquisitions and Procurement

- ▶ **Establish an acquisition/procurement process**
 - Procedures and that protects the information security posture
- ▶ **The steps**
 - Identify and document security requirements
 - Develop a security risk assessment process
 - Select vendors and products/services
 - Negotiate and finalize contract
 - Monitor and enforce security compliance
- ▶ **The Capability Maturity Model Integration is one framework with 5 levels of maturity**
 - Initial
 - Managed
 - Defined
 - Quantitatively managed
 - Optimized

Asset Ownership

- ▶ **Implement a tracking system**
 - This system can be as simple as a spreadsheet or as complex as a custom application
- ▶ **Identify all assets**
 - The first step is to identify all of the assets that the organization owns or manages. This includes physical, software, and intellectual property assets
- ▶ **Classify assets**
 - They should be classified according to type, value, location, and sensitivity
- ▶ **Assign ownership**
 - Once assets have been classified, ownership needs to be assigned
- ▶ **Maintain and update the system**
 - The asset tracking system needs to be maintained and updated on a regular basis to ensure that it is accurate and up-to-date. This includes adding new assets, removing assets that have been disposed of

Monitoring and Tracking Assets

► Useful features

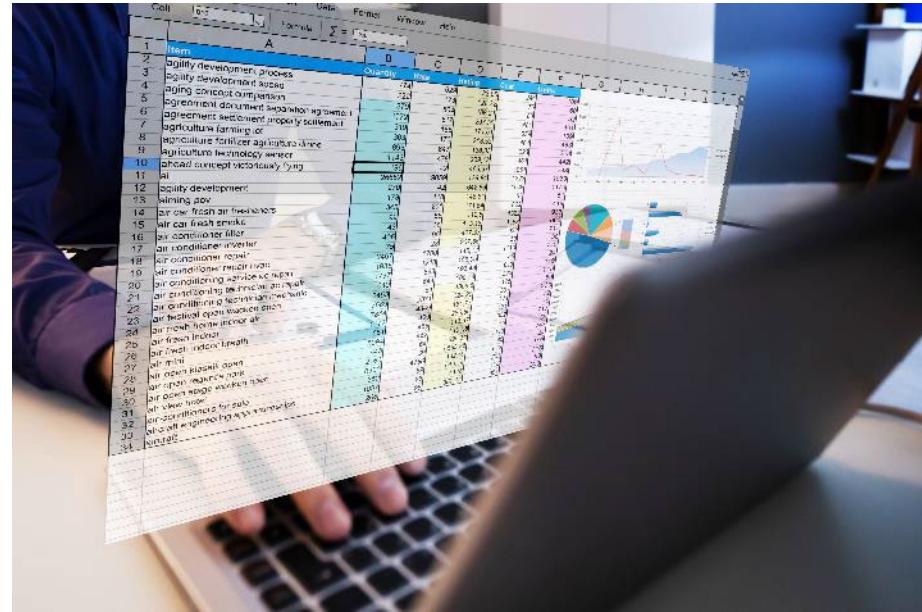
- Real-time data
- Alerts
- Reporting

► Inventory tracking

- Identifier
- Type
- Location/geofencing
- Owner
- Special use conditions
- Historical records

► Enumeration

- OS/patching
- Services
- Applications installed



► Benefits

- Improved compliance
- Loss and cost reduction
- Better utilization

Disposal and Decommissioning

- ▶ **May involve referencing these policies and procedures**

- Data retention
 - Sanitization
 - Destruction
 - Certification



- ▶ **A disposal certification is a document that certifies that an asset has been disposed of in a proper manner**

- Issued by the organization that disposed of the asset, and it may be required by law or by regulatory bodies
 - Disposal certifications typically include the following information:
 - The asset(s) that were disposed of
 - The date of disposal
 - The method of disposal
 - The name of the company that disposed of the asset
 - Attestation certifying that the asset was disposed of in a safe and responsible manner

Sanitization and Destruction

► Sanitization

- The process by which data is irreversibly removed from media or the media and data are completely destroyed

► Destruction

- Rendering plastic media utterly destroyed and data being non-recoverable

► Techniques

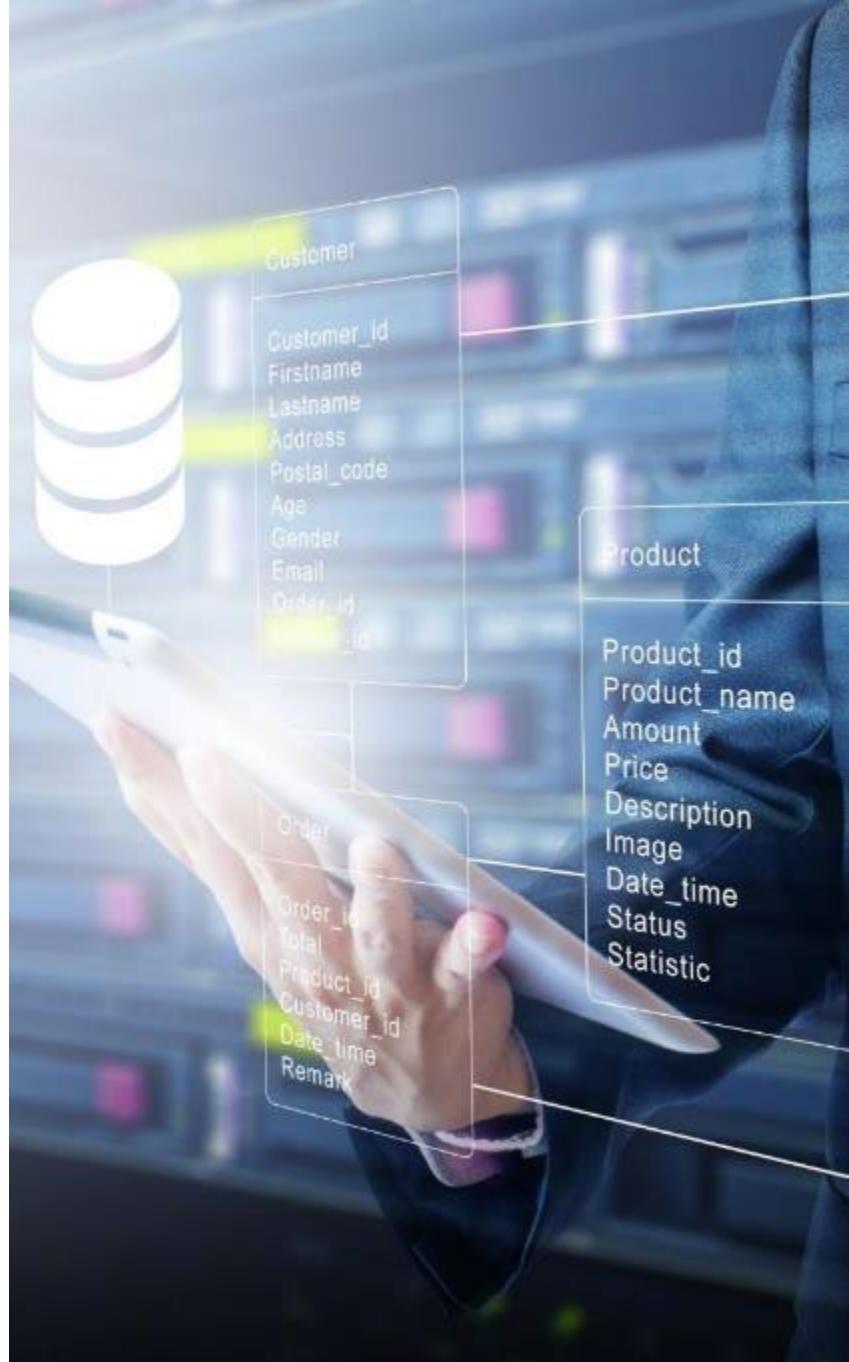
- Burning—heat destruction
- Shredding—physically tearing or splitting the media. Cross-cutting is most effective
- Pulping—dissolving media into a paste-like substance using chemicals
- Pulverizing—reducing media to a dust-like substance
- Degaussing—electronic jumbling of the binary values
- Disposal—discarding media without sanitizing
- Purging—protects confidentiality of information against laboratory attack
- Wiping or clearing—protects confidentiality of information against keyboard recovery

Contents

- ▶ Common Security Measures
- ▶ Asset Management

Vulnerability Management

- ▶ Monitoring Security
- ▶ Enhancing Enterprise Security
- ▶ Identity and Access Management
- ▶ Security Automation
- ▶ Incidents and Investigations



Vulnerability Management

- A range of tools and techniques are available to manage vulnerabilities

- Scanners
- Application security
- Threat feeds
- Penetration testing
- Disclosure programs
- Audits

- They vary widely in terms of intrusiveness and methods

<input type="checkbox"/>	CRITICAL	O... Web Servers
<input type="checkbox"/>	HIGH	A... Web Servers
<input type="checkbox"/>	MEDIUM	S... Misc.
<input type="checkbox"/>	LOW	P... CGI abuses
<input type="checkbox"/>	INFO	N... Settings
<input type="checkbox"/>	INFO	P... General

Vulnerability Scanning

- ▶ **Operation**
 - Usually, automated
 - Considered *non-intrusive* because they do not harm targets
 - Look for old, weak, or unpatched applications to identify vulnerability
 - Identify missing security controls and incorrect configurations
 - Typically require administrative credentials to probe a host
 - Considered non-intrusive, usually do not require agents installed on targets
 - False positives may arise when it misidentifies installed software
- ▶ **Some are specialized and intrusive**
 - Web application scanners
 - Database scanners
- ▶ **Typically followed up with**
 - Rescan
 - Audit to verify

Code and Application Testing

► Scanners

- Static Analyzers
 - Perform syntax checking and look for coding errors
 - Typically, slow performance
 - Input source code
 - The output is error and omission results
- Dynamic testing
 - Fuzzing
 - Black box testing tools
 - Potentially dangerous to live data or production code

► Peer review

- Best practice is to regularly have code examined by others
- Identify faults

Inspecting a Vulnerability Scan

- 1. On Instructor Windows, double-click the file:**
Demo-Vuln-Report.pdf
- 2. This is a scan performed against a Kali Linux machine**
- 3. Note:**
 - Executive Summary
 - Discovered Systems
 - Vulnerabilities, CVE and CVSS (In description)
- 4. Close the report**

Application Package Monitoring

- ▶ **Application Package Monitoring (APM) monitoring**
 - Performance
 - Availability
 - Health
- ▶ **Denial of service and brute force attacks may be identified by examining**
 - Response time
 - The amount of time it takes for an application package to respond to a request
 - Throughput
 - The number of requests that an application package can process in a given period of time
 - Error rate
 - The percentage of requests that fail, perhaps indicative of DoS
 - Resource utilization
 - The amount of CPU, memory, and disk space that an application package is using

Intelligence and Research Resources

► Threat hunting and intelligence resources

- Digging through old logs
- Search engines (OSINT)
- Proprietary and third-party
- Vulnerability databases and vendor bulletins
- Indicators of compromise (IOC) and the Dark web
 - AIS—automated indicator sharing
 - Structure Threat Information eXpression
 - Language for sharing cyber threat data
 - TAXII—Trusted Automated eXchange of Indicator Information
 - Application specification

► Research tools

- Vendors
- Vulnerability feeds
- Meeting and conferences
- Industry groups and social media
- RFCs

Attack Frameworks

► MITRE ATT&CK Framework

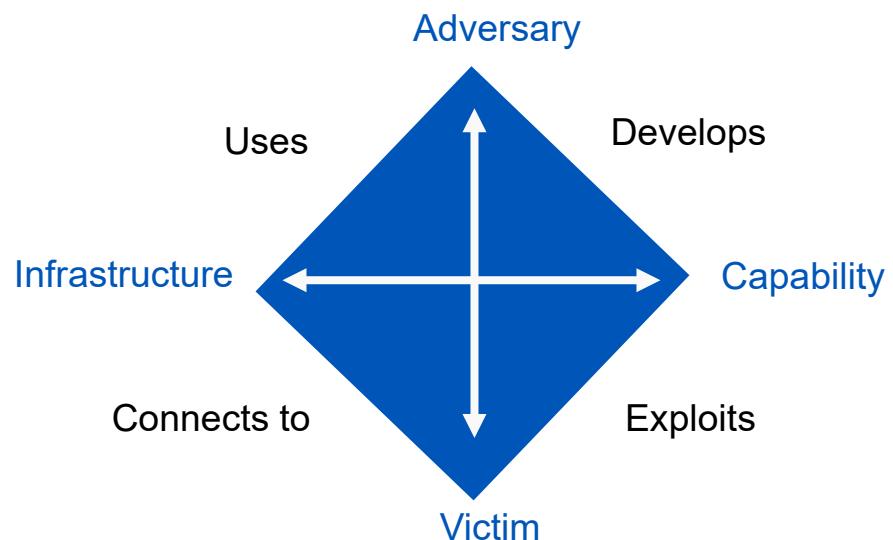
- A database base attack tactics derived from historical and documented successful attacks

► Cyber Kill Chain

- Developed by Lockheed Martin
- 7 steps from recon to compromise
 - Reconnaissance
 - Weaponization
 - Delivery
 - Exploitation
 - Installation
 - Command and control
 - Achieve goals

► Diamond Model

- Intrusion analysis



Security Assessments and Audits

- ▶ **Penetration testing is a focused form of vulnerability assessment**
 - Physical/site assessments
 - Social engineering
 - Offensive vs Defensive personnel
 - Performance-based
 - Integrated
 - Systems that combine a multitude of tools and data sources in a focused attack
- ▶ **These assessments may be**
 - Highly invasive, or
 - Inspection-driven (white box)



Black, Gray, White Hats, and Boxes

- ▶ **The people who test security are generally referred to as**
 - *Black hat*: Illegal security testers (hackers) who seek illicit personal gain
 - *Gray hat*: Illegal security testers who notify the victim when they discover a vulnerability (it is still illegal)
 - *White hat*: Security testers who are authorized to perform hacking and report the results to their client
- ▶ **Methods of testing**
 - *Black box*: Unknown environment. An application is tested with inputs from the outside to see how it handles real-world interaction
 - Testers have no experience/knowledge of the application's inner workings
 - Fuzzing is a form of black box testing
 - Sends an array of information to test input validation and error handling
 - *Gray box*: Partially known environment. Having partial or limited documentation/knowledge of a system to test it
 - *White box*: Known environment. Tester has all knowledge; tests internal data flows, structures, or workings of an application

Audits and Bounties

- ▶ **Audits are conducted by a qualified personnel to evaluate the effectiveness of the organization's IT controls and to identify any areas where improvement is needed**
- ▶ **Three means may be employed**
 - Interview
 - Observe
 - Test
- ▶ **A bug bounty is a program that rewards individuals for finding and reporting security vulnerabilities in software**
- ▶ **Bug bounty programs are typically run by software vendors, but they can also be run by other organizations, such as governments and nonprofits.**
 - Improved security posture
 - Reduced costs
 - Better visibility into flaws

Vulnerability Analysis

► The steps are

- Verification
- Prioritization
- Classification

► These tools can help

- CVE
 - Common Vulnerabilities and Exposures
 - A dictionary of vulnerabilities
- CWE
 - Common Weakness Enumeration
 - A dictionary of weakness
- CVSS
 - Common Vulnerability Scoring System
 - A vulnerability severity scoring system

Search Results

There are **2470** CVE Records that match your search.

Name

[CVE-2023-46288](#)

Exposure of Sensitive Information to an Unauthorized Actor. Apache Airflow 2.4.0 to 2.7.0. Sensitive configuration information has been exposed via the Airflow REST API for configuration even when the expose is by default. It is recommended to upgrade to a version that fixes this configuration. This is a different error than CVE-2023-45348. Values in 2.7.* are exposed by specially crafting their request (solved the issue and additionally fixes CVE-2023-45348).

[CVE-2023-46227](#)

Deserialization of Untrusted Data Vulnerability in Apache InLong 1.4.0 through 1.8.0, the attacker can use \t to bypass. To solve it. [1] <https://github.com/apache/inlong/pull/8814>

- ▶ **Common Vulnerabilities and Exposures is the best identifier for vulnerabilities—each entry is a specific instance**
- ▶ **Records first appear in <https://cve.mitre.org/>**
 - And shortly afterward at <https://nvd.nist.gov/>
- ▶ **Naming**
 - The entries always begin with CVE-
 - The next number is the year of publication
 - Last entry (4-6) digits is a unique number for the year
 - Given out in ranges to various vendors
- ▶ **Content**
 - Name/number
 - Description of the vulnerability—not the exploits
 - References
 - Party who created the entry
 - Other deprecated information

CVE-ID	Learn • CVSS S Mapping:
CVE-2023-46227	
Description	Deserialization of Untrusted Data Vulnerability issue affects Apache InLong: from 1.4.0 advised to upgrade to Apache InLong's https://github.com/apache/inlong/pull/
References	<p>Note: References are provided for the convenience; it is not intended to be complete.</p> <ul style="list-style-type: none">• MISC:https://lists.apache.org/thread/12345• URL:https://lists.apache.org/thread/12345
Assigning CNA	Apache Software Foundation

- ▶ Common Weakness Enumeration is a listing of common types of vulnerabilities at cwe.mitre.org
 - Their category
- ▶ Naming is CVE-<number>
- ▶ CWE entries are useful for categorizing root cause
 - E.g.: CWE-502 is Deserialization of Untrusted Data
 - A fault common to many applications
- ▶ Entries provide
 - Description and other names
 - Related flaws
 - Typical impact
 - Examples
 - Other examples in CVE entries

CWE-502: Deserialization of Untrusted Data

Weakness ID: 502

Abstraction: Base

Structure: Simple

View customized information:

Conceptual

Operational

Mapping
Friendly

▼ Description

The product deserializes untrusted data without sufficiently

▼ Extended Description

It is often convenient to serialize objects for communication or code can often be modified without using the provided ac protect itself. Furthermore, any cryptography would still be c assumption.

Data that is untrusted can not be trusted to be well-formed.

- ▶ An empirical score for the severity of a vulnerability
 - 0 to 10
 - ▶ Base metrics
 - Basic characteristics of a vulnerability that do not change over time or from one organization to another
 - ▶ Temporal metrics
 - Values that can change based on the exploit lifecycle, remediation, and reliability of reported vulnerability
 - ▶ Environmental metrics (includes the base metrics and temporal metrics)
 - Local considerations unique to each organization
 - If exploited, how much damage could be done
- CVSS Base Score:** 7.5
Impact Subscore: 3.6
Exploitability Subscore: 3.9
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 7.5

CVE, CWE, and CVSS



- Go to <https://cve.mitre.org/>
 1. Select Search CVE List and seek CVE-2023-46227
 2. Click the hyperlink under the name for more detail
 3. Near the top, click the link for Learn more at National Vulnerability Database to go to <https://nvd.nist.gov/>
 4. Examine the CWE entry ear the bottom
 5. Follow the CVE link to <https://CWE.mitre.org>
 6. Return to CVE
 7. Near the top, follow the link to Base Score: it will take you to the calculator
 8. Show the base values and how they change

Response and Remediation

- ▶ **The final stages of vulnerability management deals with how issues are handled. These methods are commonly accepted**
 - Accept
 - No action needed—proceed
 - See below (Exceptions and Exemptions) for special circumstances
 - Transfer
 - Insure or transfer responsibility to another party—insurance
 - Mitigate
 - Take action to reduce risk—install a patch
 - Avoid
 - Discontinue use or cancel plans—decide to deny the system or sue
- ▶ **Exceptions and Exemptions**
 - Exceptions—a temporary deviation from a security policy or procedure
 - Exemption—a security exemption is a permanent deviation from a security

Contents

- ▶ Common Security Measures
- ▶ Asset Management
- ▶ Vulnerability Management

Monitoring Security

- ▶ Enhancing Enterprise Security
- ▶ Identity and Access Management
- ▶ Security Automation
- ▶ Incidents and Investigations



Monitoring and Alerting Tools

- ▶ There are a wide variety of tools, frameworks and standards available to perform monitoring and generate alerts
 - Frameworks
 - CIS Benchmarks
 - NIST CSF
 - Protocols
 - SCAP
 - SNMP and traps
 - Tools
 - SIEM
 - Antivirus
 - DLP
- ▶ Some are defensive applications
 - Others are standards and best practices that may be referenced for comparison



CIS Benchmarks

- ▶ CIS Benchmarks are a set of best practices for secure configuration of systems
 - Operating systems
 - Infrastructure
 - Cloud
 - Compliance regulations
- ▶ They are typically downloaded in the form of a checklist, consisting of industry security best practices
 - FedRAMP cloud compliance
 - PCI DSS compliance
 - Microsoft Windows
 - Cisco IOS infrastructure
 - VMware ESXi
 - Amazon Web Services
 - Microsoft Azure



NIST CSF

- The NIST Cybersecurity Framework (CSF) is a voluntary framework that provides organizations with a set of standards, guidelines, and best practices
 - It is designed to be flexible enough to be used by organizations of all sizes and industries
- The Core Activities are divided into five functions
 - Identify assets
 - Protect with proper controls
 - Detect security incidents
 - Respond with a plan
 - Recover and resume functions
- These are further refined into 23 (currently) categories of activities
- NIST SP 800-53 provides a catalog of controls to achieve various security levels



Graphic source: <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>

- ▶ **NIST CSF recognizes implementation tiers and profiles**
- ▶ **The implementation tiers**
 - Describe how well an organization is performing Core activities
 - Partial
 - Risk-Informed
 - Repeatable
 - Adaptive
- ▶ **Profiles are self-assessments that organizations can use to measure their cybersecurity posture against the CSF**
 - These can be used to identify
 - Areas for improvement
 - Prioritize security investments
 - Communicating cybersecurity risk to stakeholders

ISO 27000 Series

- ▶ ISO 27001 is an international standard that outlines the requirements for an Information Security Management System (ISMS)
- ▶ It provides an organizational framework for:
 - Establishing security
 - Implementing controls and policies
 - Maintaining a security posture
 - Continually improving an information security management system
- ▶ It helps managing information risks, including risk identification, risk assessment, risk treatment, risk monitoring, and risk with:
 - Guidelines and
 - Best practices
- ▶ Much of it is based upon based on the principle of a Plan-Do-Check-Act (PDCA) cycle

- ▶ **The Security Content Automation Protocol (SCAP) is a suite of open standards that include**
 - Automating security assessment
 - Configuration management
 - Vulnerability management
 - Vulnerability severity assessment
- ▶ **Element of SCAP**
 - Extensible Configuration Checklist Description Format (XCCDF)
 - Open Vulnerability and Assessment Language (OVAL)
 - Software Identification (SWID) Tagging
 - SWID is used to identify software products and versions
 - Can be used to discover software integrity failures
 - Common Platform Enumeration (CPE)
 - A language for configuration management tools to identify hardware and software
 - CVE, CWE, CVSS
 - Discussed earlier

SCAP Uses

- Tools that embrace SCAP protocols are standardized and can be used to automate a wide range of security tasks, such as:
 - XCCDF
 - Used to define security policies and checklists.
 - OVAL
 - is used to describe and assess vulnerabilities in a non-proprietary manner
 - SWID
 - Used to identify software products and versions
 - Can detect unauthorized changes as well
 - Can be used to discover software integrity failures
 - CPE
 - Discovering backdated or incorrect versions of software
 - CVE, CWE, CVSS
 - Discussed earlier

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 [\(hide\)](#)

 cpe:2.3:a:apache:felix_health_checks:*\:*:*\:*:*\:*:*

Up to (including)
2.0.2

[Show Matching CPE\(s\) ▾](#)

Common Platform Enumeration

- ▶ Structure of a CPE Well-Formed Name (WFN)
- ▶ A CPE name is a URL that encodes seven ordered fields:
`cpe:/<part>:<vendor>:<product>:<version>:<update>:<edition>:<language>`
- ▶ Some of the fields may be left blank, and empty fields may be left off the end of the URL. The main division of CPE names is in the <part> field
- ▶ First is CPE and optionally its schema version
- ▶ Next, the Part; this can currently take on only three values:
 - a for applications
 - h for hardware platforms
 - o for operating systems

 **cpe:2.3:a:apache:felix_health_checks:***:*:*:*:*:*

A photograph showing two individuals from a side-on perspective, focused on writing in their notebooks with pens. They are seated at a dark-colored conference table. In the foreground, the edge of a white coffee cup is visible. The background is slightly blurred.

Do Now

Examining CPE in Output

1. In the Linux host, open a terminal prompt, run:

```
nmap -n -T5 -O 10.1.1.25 | grep  
cpe
```

2. Next, run:

```
nmap -n -T5 -sV 10.1.1.25
```

- ▶ CPE provides a standardized output to describe the system
- ▶ The –sV parameter instructs nmap to display application version information discovered

Do Now

Antivirus and Malware Scanning

- ▶ **Assume that antivirus can detect, prevent, and remove any infection or malware**
 - A classic blacklist defense
- ▶ **Signature-based**
 - Matches an exact pattern found only in the exploit code that should not be present elsewhere
 - Can identify only *known* malware
- ▶ **Behavioral-based or heuristic-based**
 - Can detect unknown viruses and zero-day attacks
 - Looks for suspicious code patterns or activities commonly seen in exploits
 - Needs multiple instances to decide
- ▶ **May be set to delete, deny or quarantine suspected malware**
- ▶ **Updates should be obtained as soon as the publisher makes them available**

Application Whitelisting

- ▶ Commonly a part of Endpoint Detection and Response (EDR)
- ▶ Identifying approved software is permitted to be present and run on a system
- ▶ Operates by
 - Building a list of known good applications and scripts
 - Name
 - Attributes
 - Hash
 - Locking down files that can execute
 - Checking executing at run-time files to verify being “whitelisted”
 - Allowing updates only by authorized users or applications
 - Rejecting any execution or modification not specifically approved



HIDS and HIPS

- ▶ Commonly a part of Endpoint Detection and Response (EDR)
- ▶ Monitors
 - Logs
 - Registry setting
 - File and directories
- ▶ Protects itself only
- ▶ Can generate alerts for
 - Zero-day attacks
 - Attacks that attempt to modify host files and executables
 - Local users' misuse or policy violations
- ▶ May affect CPU use and performance
- ▶ A HIDS that prevents damage may be called a HIPS
 - Prevents file and program alteration
 - A Host intrusion prevention system

If it only alerts, it is HIDS; if it can stop an attack, it is HIPS



Data Loss Prevention (DLP)

- ▶ Commonly a part of Endpoint Detection and Response (EDR)
- ▶ These defensive applications protect
 - Data in motion—*Being transmitted*
 - Placed near network egress points at the perimeter and analyzes network traffic to detect sensitive data
 - Data at rest—*Stored on disk*
 - Located in data centers to discover if confidential data is moved to or stored on unsecured media
 - Data in use—*Being processed by endpoints*
 - Endpoint-based protection regulates use, as well as internal and external traffic between groups or types of users

Simple Network Management Protocol (SNMP)

► SNMP is a device management protocol

- Uses TCP and UDP/161 and 162
- SNMPv3 is best; it implements encryption and TCP
 - AuthPriv security is set up with hashing (Auth) and encryption (Priv)
- Designed to discover or set device configuration
- Most commonly used version has a cleartext community string (password)
 - To read: public
 - To set: private
- Cleartext and default strings may allow reconnaissance and reconfiguration
- SNMP traps are alerts and log records sent by managed devices to an NMS



NMS = network management station

Security Automation

► **SIEM and Syslog**

- These are detective measures
- Syslog-ng is TCP-based and uses TLS
- Collect and aggregate logs and performance information across multiple systems
- Correlate using event Correlation dashboards to detect trends
- Perform deduplication to enhance accuracy
- Perform packet capture

► **Security Orchestration Automation and Response (SOAR)**

- Fast and automated handling of alerts and incidents
- Can be set to follow a playbook



Networking Information

- ▶ **Investigative support may also be gathered from**
 - Netflow
 - Cisco tools for collecting truncated header information on a collector
 - Flow exporter—routers and switches
 - Flow Collector—aggregation system
 - Analysis application to examine and detect threats
 - Sflow—Sampled Flow
 - Industry de facto standard—not IETF
 - Alternative to Netflow
 - Can implement a variety of sampling techniques
 - Uses sampling to increase scalability
 - IPFIX
 - IP Flow Information eXport
 - IETF standard
 - Metering process collects data
 - Exporters gather data and forward to collection points

Domain 4: Match the Items to the Topics

Do Now

Item	Answer	Topic
Traffic collection		A. Reducing/lessening damage
Standards, guidelines, and best practices		B. Bug bounty
Centralized		C. Interview
Compensating		D. Static scanner
Reads code		E. Secure cookies
Audit method		F. Netflow
HTTPS only		G. RADIUS
Paid to hack		H. NIST CSF

For each item on the left, write in the corresponding letter from a topic on the right

Contents

- ▶ Common Security Measures
- ▶ Asset Management
- ▶ Vulnerability Management
- ▶ Monitoring Security

Enhancing Enterprise Security

- ▶ Identity and Access Management
- ▶ Security Automation
- ▶ Incidents and Investigations



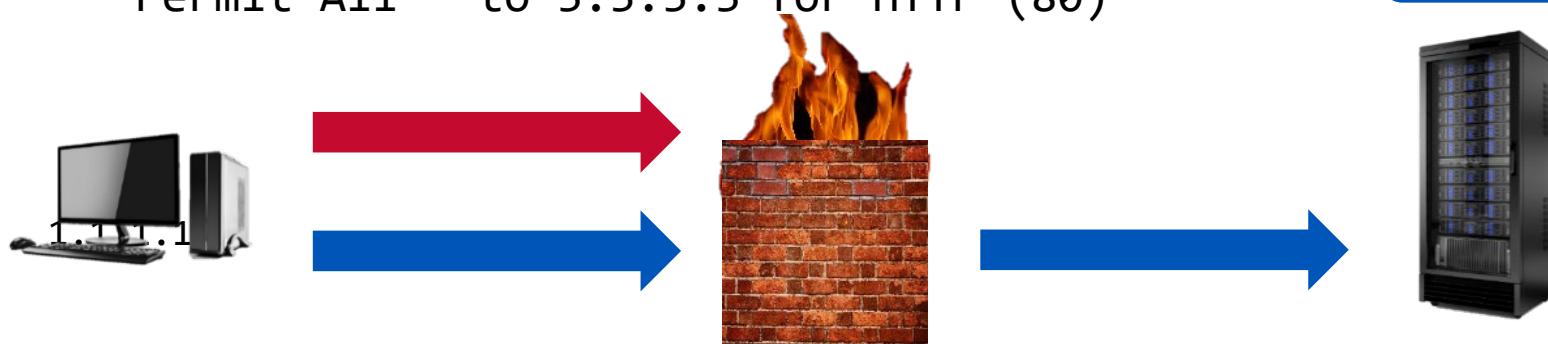
Firewall Rules Management

- ▶ Firewalls are edge devices that regulate traffic flow, ports, protocols, and addresses to the intranet with Rule-Based Access Control (RBAC)
 - The order matters
 - Have an implicit deny as the last rule to handle all other traffic
- ▶ Incorrect for blocking 1.1.1.1 access to web servers
 - Permit All to 3.3.3.3 for HTTP (80)
 - Deny 1.1.1.1 to 3.3.3.3 for HTTP (80)
- ▶ Correct
 - Deny 1.1.1.1 to 3.3.3.3 for HTTP (80)
 - Permit All to 3.3.3.3 for HTTP (80)

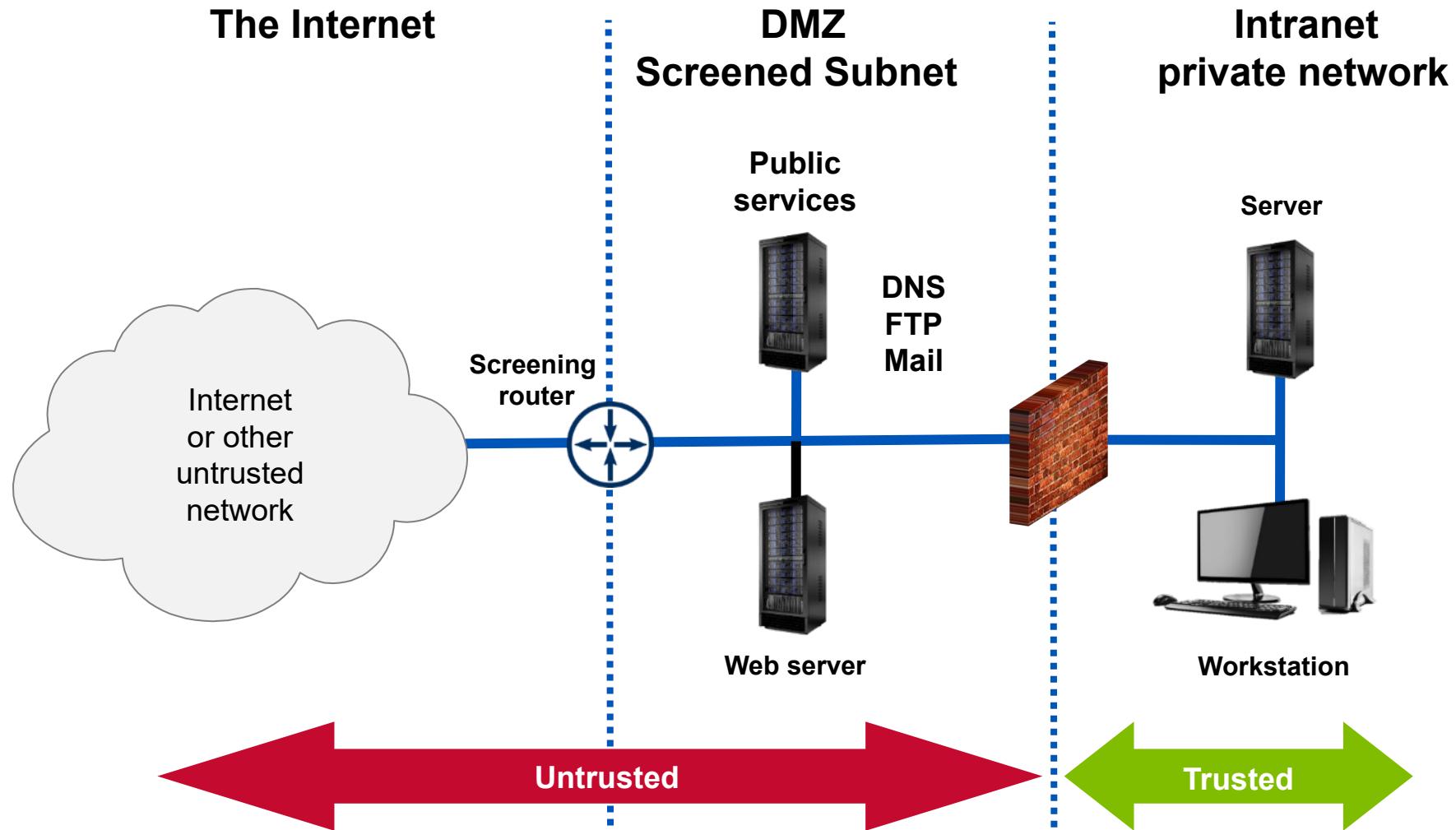
Permit All allows even 1.1.1.1 to access the web server



1.1.1.1 is blocked; others allowed



Basic DMZ



The design should create *defense in depth*, with edge ACLs on routers, rules on the firewalls, and other defenses stacked on the inside.

Web Filters

- ▶ **Block rules**
 - The rules can be based on a variety of factors, such as the website's content, category, or domain and reputation.
- ▶ **Content filters examine data messages**
 - OSI Layer 7
 - Pass or block based on content
 - Obscene language
 - Key phrases: “top secret”
 - Blocking potentially dangerous applications and malware
- ▶ **URL filters sift through DNS and IP addresses in browsers**
 - Filters by categories:
 - Sex, gambling, anarchy,
- ▶ **Reputation**
 - These analyze web site behavior and assign a reputation score to a URL to determine the likelihood that it contains URL-based malware or undesired content



Proxy Servers

► These devices provide several basic services

- Caching previously requested web pages
- Hiding internal clients' addresses
- Acting as a central point for authentication, throttling and filtering
- Preferred location for authentication and content filtering

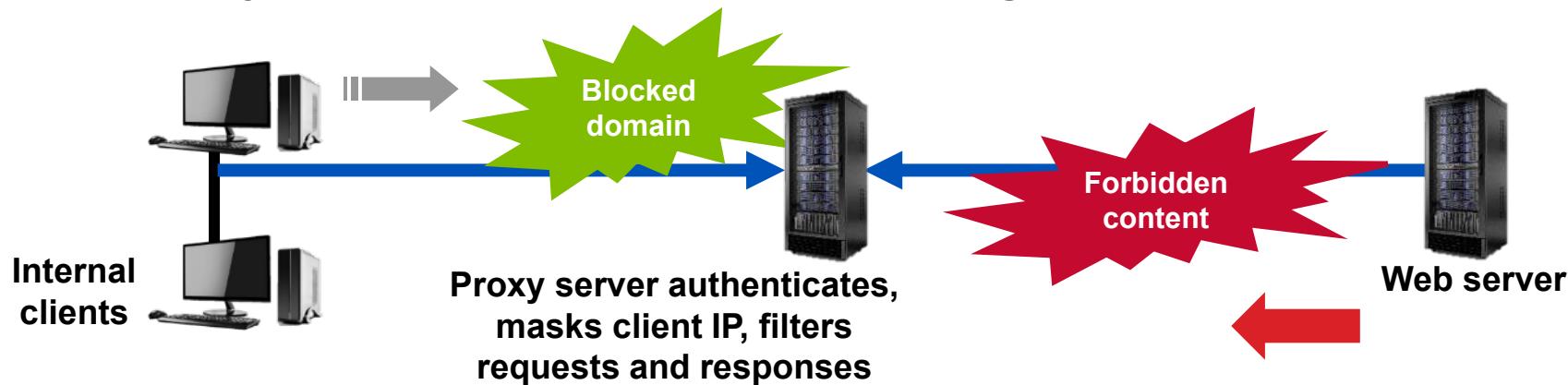
► Proxies may be accessed transparently, or clients may be required to have specific settings

Configure Proxies to Access the Internet

No proxy
 Auto-detect proxy settings for this network
 Use system proxy settings
 Manual proxy configuration:

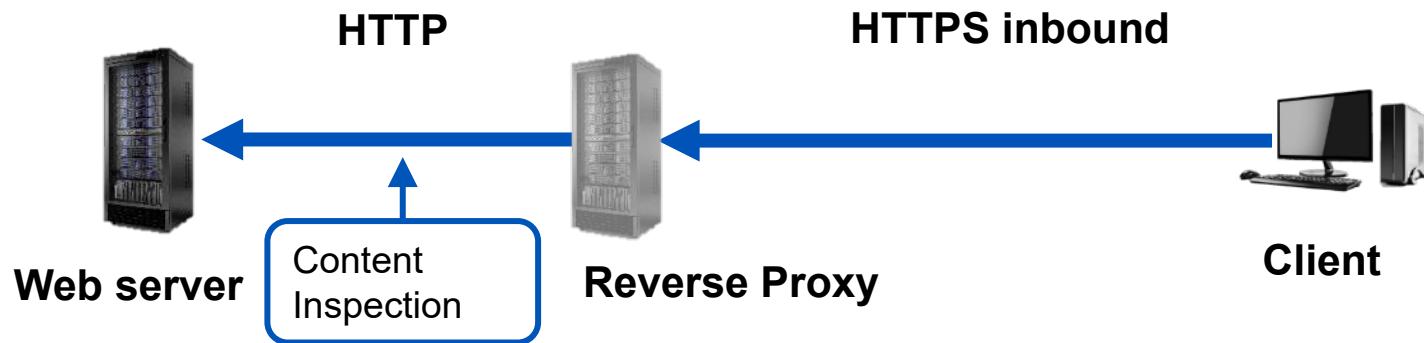
HTTP Proxy:
 Use this proxy server

SSL Proxy:



Reverse Proxies

- ▶ Servers that may be used to reduce HTTPS to HTTP, so that IDS and firewalls may inspect the data
 - Alternatively, decryption certificates could be used to allow cleartext inspection
- ▶ Off loads SSL/TLS functions from servers
- ▶ Act as central point for caching and certificates
- ▶ Performs load balancing



Hardened OS

- ▶ **Operating system security established and maintained**
 - Settings and configuration
 - Patching
 - Applications
- ▶ **Group Policy**
 - The best way to enforce domain-wide settings and configuration
- ▶ **SELinux**
 - SELinux is a Linux kernel security module that adds Mandatory Access Control capabilities to tightly control processes and users
- ▶ **Implement secure protocols**
 - Protocol selection
 - Encrypted and/or integrity checked
 - Port selection
 - For movement through a firewall
 - Transport method—TCP is usually preferred over UDP

Email and Messaging Security

- ▶ **DomainKeys Identified Mail (DKIM)**
 - An email authentication protocol that helps to verify the identity of the sender of an email
 - It does this by adding a digital signature to the email header
- ▶ **Sender Policy Framework (SPF)**
 - SPF works by adding a TXT record to the DNS record for the domain
- ▶ **Domain-based Message Authentication Reporting and Conformance (DMARC)**
 - DMARC works by building on two other email authentication protocols, SPF and DKIM
 - Publishes a policy that specifies what should happen to emails that fail SPF and DKIM
- ▶ **Gateway or Secure Email Gateway**
 - A secure email gateway (SEG) is a system that is positioned at the perimeter and inspects all incoming and outgoing email traffic for malicious content

File Integrity Checkers

- ▶ Tools that verify system and file integrity
- ▶ Inventory files and registry
- ▶ Hash files
- ▶ Record hashes in digitally signed database
- ▶ Run verification periodically or at run-time (e.g., Tripwire and FCIV)

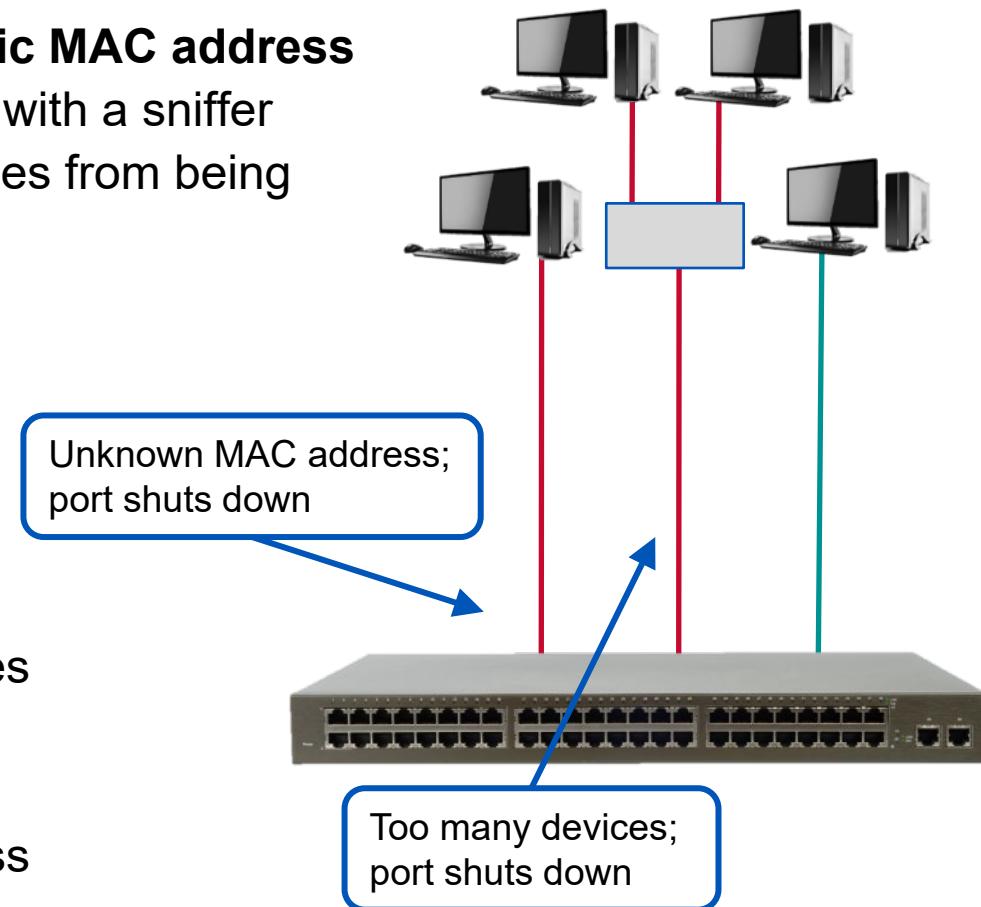
Integrity
Integrity .
actions, v
principles
In ethics
honesty
one's ac

Data Loss Prevention (DLP)

- ▶ Commonly a part of Endpoint Detection and Response (EDR)
- ▶ These defensive applications protect
 - Data in motion—*Being transmitted*
 - Placed near network egress points at the perimeter and analyzes network traffic to detect sensitive data
 - Data at rest—*Stored on disk*
 - Located in data centers to discover if confidential data is moved to or stored on unsecured media
 - Data in use—*Being processed by endpoints*
 - Endpoint-based protection regulates use, as well as internal and external traffic between groups or types of users

Port Security

- ▶ **A primitive form of network access control (NAC)**
 - Regulating whether a device can connect to the intranet at the switch
 - Shuts down the port when illegal devices are attached
- ▶ **Set ports to allow just one specific MAC address**
 - MAC filters are easily bypassed with a sniffer
 - Prevents rogue hubs and switches from being attached
- ▶ **A better solution is 802.1x**
 - Wired and wireless
 - Implement zero trust access control
- ▶ **Prior to admission**
 - Prompt for credentials/certificates
 - Check antivirus signatures
 - Verify patching
 - May be agent-based or agentless



EDR and XDR

- ▶ **Cybersecurity tools that detect and respond to cyber threats**
 - EDR is focused on protecting endpoints, such as laptops, desktops, and mobile devices
 - XDR Extends the capabilities of EDR to protect other aspects of an organization's IT environment, such as networks, cloud applications, and email

Feature	EDR	XDR
Focus	Endpoints	Endpoints, networks, cloud applications, and email
Data sources	Endpoint data	Endpoint data, network data, cloud application data, and email data
Capabilities	Threat detection, threat response, and endpoint remediation	Threat detection, threat response, endpoint remediation, network security, cloud security, and email security

User Behavioral Analysis

- ▶ **User behavior analysis (UBA) involves collecting, analyzing, and interpreting data about user behavior**
 - It can be used to identify patterns and trends in user behavior,
- ▶ **These tools can**
 - Improve the user experience,
 - Increase engagement, and
 - Detect fraud and other malicious activity
- ▶ **UBA gathers information from**
 - Website logs and analytics
 - CRM systems
 - network logs
- ▶ **It may use a variety of techniques to analyze data, including machine learning and artificial intelligence**



Contents

- ▶ Common Security Measures
- ▶ Asset Management
- ▶ Vulnerability Management
- ▶ Monitoring Security
- ▶ Enhancing Enterprise Security

Identity and Access Management

- ▶ Security Automation
- ▶ Incidents and Investigations



Access Phases

► Identification or registration

- It allows an account to be provisioned for use in a system and should have robust documentation and policies (e.g., registering for an account)
 - Called identity proofing
- Deprovisioning when there is no certifiable reason for the account

► Authentication is verified by

- Something you know (e.g., password)—the weakest
- Something you have (e.g., a token or an aircraft with a transponder*)
- Something you are (e.g., fingerprint)—the strongest
- Somewhere you are, often GPS/geofencing used to locate or ensure a party is close by

► Authorization

- Granting privileges, based on a confirmed identity

*A transponder is a proximity authentication system.

Something You Know

- ▶ **The most common form of authentication for users**
 - Hosts may also send these values
- ▶ **The password/secret should not be shared to enhance accountability**
- ▶ **Passphrases are the best reusable credentials with adequate complexity**
- ▶ **These combined values are the credentials**
 - May be cleartext (PAP, FTP, HTTP)
 - Passphrases and passwords may be reusable
 - Hardware tokens with changing values may be submitted for every authenticated session
 - One-Time Passwords (OTPs), such as with new accounts
 - TOTP: time is included in the exchange; time must be synchronized
 - HOTP: involves a shared secret and a counter that increments with each use
 - SMS Push notification—often considered the least secure
- ▶ **Credential managers and password vaults are recommended**

HOTP = HMAC-based One-time Password

HMAC = Hashed-based Message Authentication Code

PAP = Password Authentication Protocol

TOTP = Time-based One-time Password

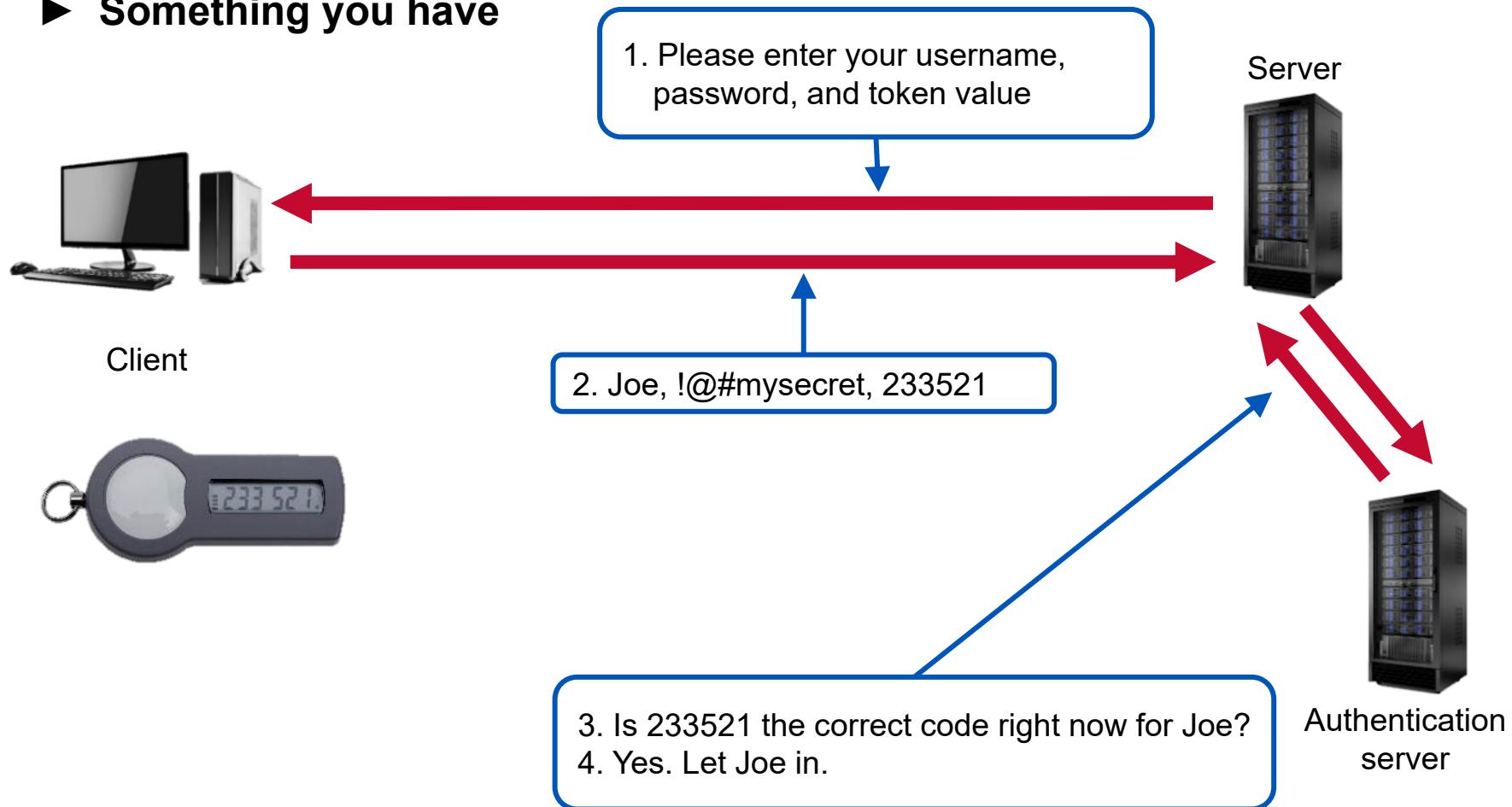
Something You Have

- ▶ **Tokens and Smartcards**
 - RSA SecurID tokens—devices that generate a one-time password for each authentication event
 - Common Access Cards (CACs), Personal Identity Verification (PIV), and smartcards that have photo ID and *private keys* embedded into them to authenticate
 - Smartcards with photo ID that have *crypto-processors*,
 - Allows for passwordless authentication
 - Proximity devices and readers: transponders, RFID chips, and radio beacons
 - RFID chips can be used to track important assets and prevent theft
- ▶ **Typically combined with “something you know” to provide two-factor authentication**
 - May contain information about level of access
- ▶ **One mechanism is to synchronize the token with a central device that knows the values on every token**
 - Secrets change frequently—say, every 60 seconds



Electronic Tokens

- ▶ Something you know
- ▶ Something you have



Biometrics: “Something You Are”

- ▶ **A third type of authentication is biometrics**
 - Generating authentication information for a person by digitizing measurements of a physical characteristic
 - Iris pattern and retina are the most accurate
 - Fingerprint
 - Voiceprint
 - No enrollment required
 - Facial
 - Gait analysis
- ▶ **Biometric authentication is typically most expensive**
 - Generally considered difficult to impersonate
 - Cannot be lost or shared or easily spoofed
- ▶ **Accuracy measurements**
 - False rejections rate (FRR): Ratio of mistakenly blocking access—Type I
 - False acceptance rate (FAR): Ratio of mistakenly allowing access—Type II

Crossover is the point at which false accepts = false rejections



Password Strength

- ▶ **Length**
 - A longer password means more guessing would have to be done to exhaust all possibilities
- ▶ **Complexity—password crackers have a tougher time with higher combinations**
 - qwertyasdf is weaker than abcde1234 is weaker than asdf321#@
- ▶ **Expiration**
 - Usually set to last day of work/contract
- ▶ **Age**
 - Maximum age a secret is allowed to remain static
- ▶ **Reuse/history**
 - Limiting the ability to change a password back to a previous value
 - One-time passwords (OTPs) involve passwords that may be used only once
- ▶ **Credential managers and password vaults are recommended**

Privileged Access Management Tools

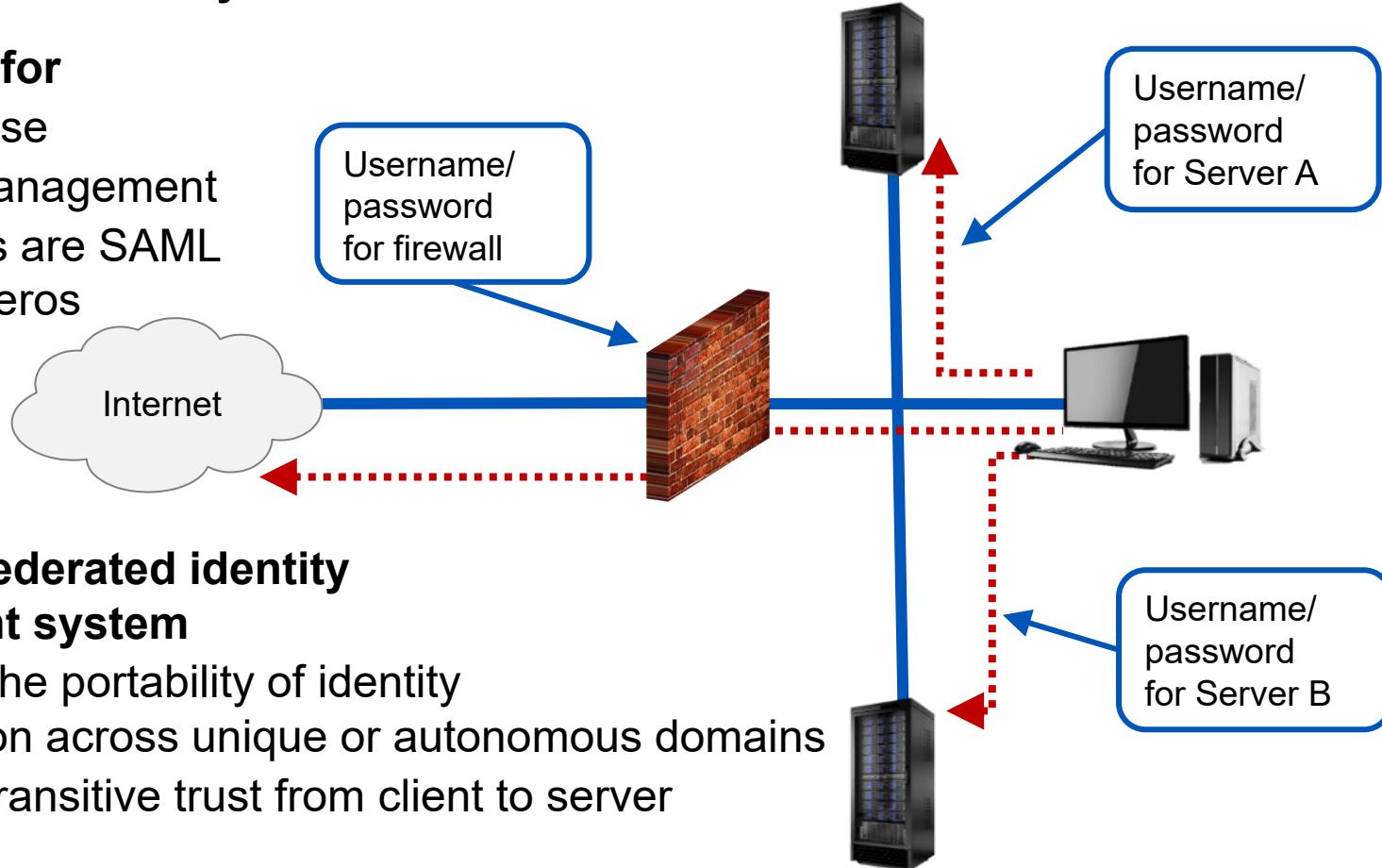
- ▶ **Just-in-time permissions (JIT)**
 - Just-in-time permissions is a security model that grants users access to resources or systems only when needed and only for the duration needed
- ▶ **Password vaulting**
 - Work by encrypting and storing all of your passwords
 - Assist with password creation, storage, rotation and 2FA
- ▶ **Ephemeral credentials**
 - Short-lived access credentials that are valid for only a short period of time
 - typically used in cloud computing and other environments where it is important to limit the time that users have access to resources
 - Ephemeral credentials can be generated by creating a short-lived certificate that is signed by a trusted certificate authority

Single Sign-On (SSO)

- ▶ In the early days of networking and security, users would have to authenticate to each system

- ▶ SSO allows for

- Ease of use
- Global management
- Examples are SAML and Kerberos



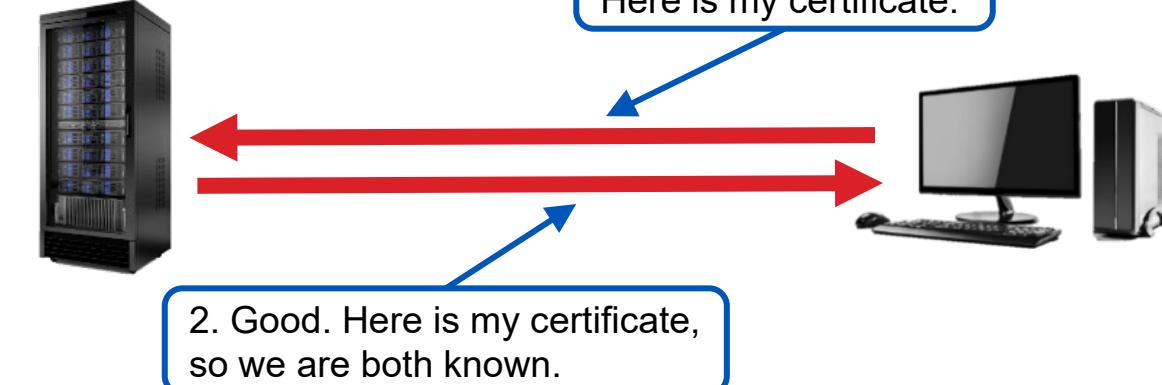
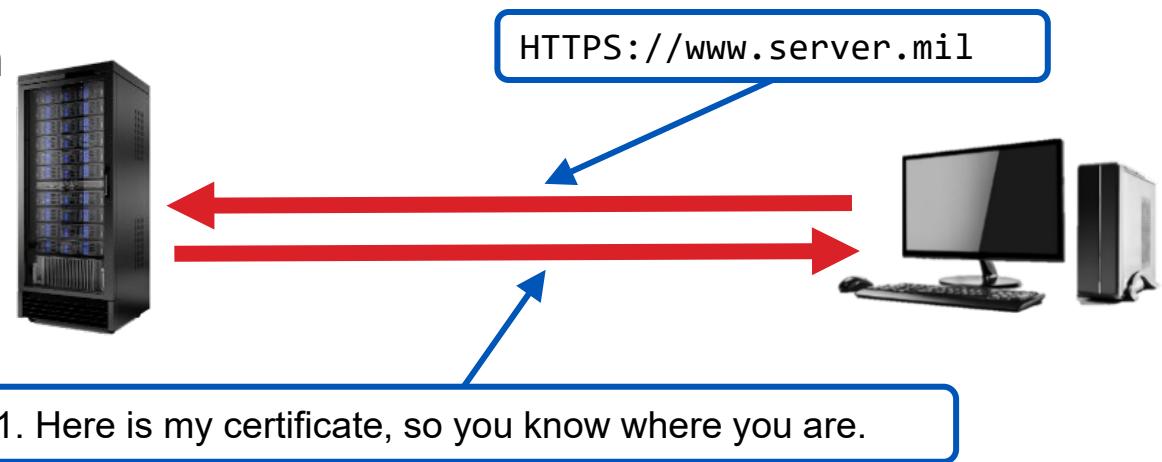
- ▶ Involves a federated identity management system

- Enables the portability of identity information across unique or autonomous domains
- Creates transitive trust from client to server

Mutual Authentication

► One-way authentication

- Logging in to an FTP server
- Going to an HTTPS site
- Which system is authenticated depends on the service



► Mutual authentication

- Client authenticates to server
- Server authenticates to client

Multifactor Authentication

- ▶ **Using multiple forms of authentication**
- ▶ **Accessing your e-mail may require only a username and password**
- ▶ **Some assets are restricted and require**
 - Username and password, plus
 - Electronic token value
 - SMS text value
 - Phone call
 - Push notification to smartphone are easiest for users
- ▶ **Cloud-based systems may not be able to implement some authentication protocols**
 - Hardware access may be required
- ▶ **For optimal results, different forms of authentication should be used**
 - Username/password plus smartcard is appropriate
 - Username/password plus username/password is not secure

Pop Quiz: Multi-Factor Authentication



How many factors?

- 1. John authenticates with**
 - A. Username/password
 - B. Additional PIN, because he is an admin

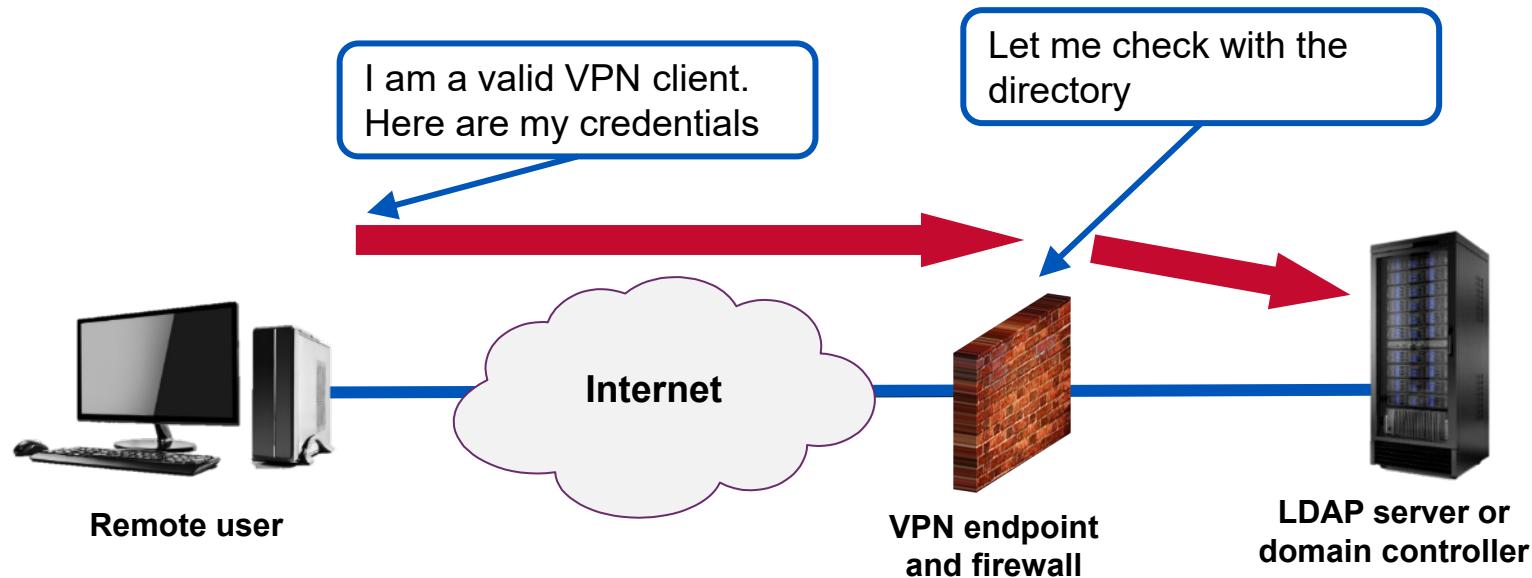
- 2. Jane authenticates with**
 - A. Hardware token
 - B. CAC with private key

- 3. Joe can access a room with**
 - A. PIN
 - B. An access code with a number written by his boss

- 4. Fred is granted access with**
 - A. Retinal scan
 - B. PIN

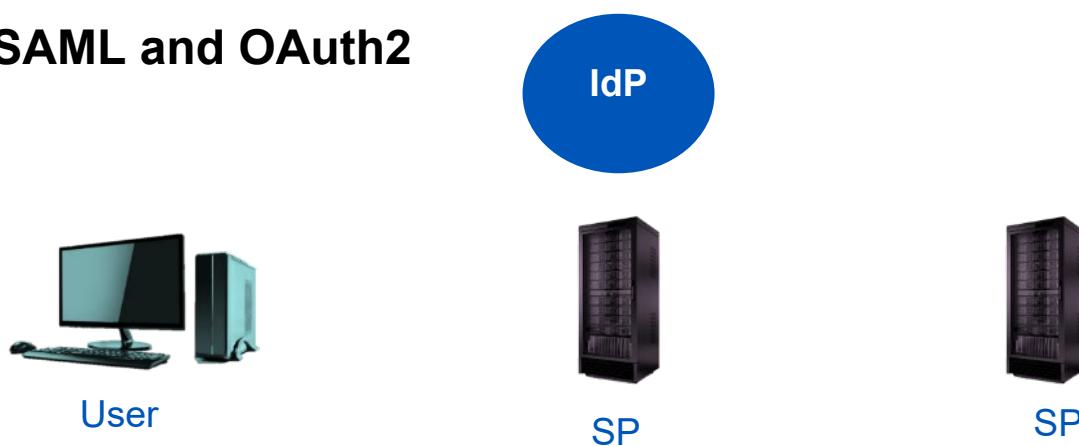
LDAP

- ▶ **Lightweight Directory Access Protocol (LDAP)**
- ▶ **Credentials are checked against a single central directory tree that contains authentication information from across the organization**
 - May be encrypted with LDAPS (Port TCP/636)
- ▶ **May integrate with many platforms: Mac, Windows, Linux**



Identity Federation

- ▶ An Identity Federation is a framework that allows users to access multiple applications and services using a single set of credentials
 - By establishing trust relationships between the different entities involved, such as the user, the server, and the identity provider
- ▶ The roles
 - The Identity provider (IdP) is responsible for authenticating the user and providing them with a digital identity
 - The Service Provider (SP) provides access to the application or service that the user seeks
 - The user is the entity that is trying to access the application or service
- ▶ E.g., SAML and OAuth2



Security Assertion Markup Language (SAML)

- ▶ **Designed to facilitate single sign-on between different organizations**
- ▶ **Three roles are defined**
 - Principal: A user
 - Identity Provider (IdP): The entity that centrally authenticates
 - Service Provider (SP): The service or site to be accessed
- ▶ **SAML operation**
 - The principal requests access from a service provider, providing credentials
 - The SP passes the credentials to an IdP
 - The IdP evaluates the credentials and replies that they are valid or invalid
 - The SP can make an access-control decision
- ▶ **SAML does not limit or specify the method of authentication or protocols that may be used**

Oauth2

- ▶ **Open Authorization 2.0 is an open standard for authorization**
 - An HTTPS-based application that allows users to grant third-party applications access to their resources without revealing their credentials
 - E.g., a social media site want to give an advertiser access to your contact information
 - Without disclosing your credentials
- ▶ **OAuth Operation**
 - UserA wants to use a third-party photo app to edit Facebook photos
 - UserA clicks on the *Edit with App* button on Facebook
 - Facebook asks UserA to authorize the editing app to access photos
 - UserA agrees
 - Facebook generates a unique token or value and sends it to the editing app
 - The editing app uses the token to access UserA's photos without knowing the password

Access Control Models

- ▶ A general concept of how access to any system may be managed
- ▶ **Mandatory Access Control (MAC)**
 - Strongest and strictest access control model
 - Uses labels to identify objects as “Confidential,” “Secret,” “Top Secret”
 - Implemented on a trusted OS, such as SELinux
 - A strict, government-oriented form of allowing access where an administrator grants and denies access, not the owner
 - Ensures no read-up or write-down
 - System developers must follow strict guidelines for configuration
- ▶ **Discretionary Access Control (DAC)**
 - A loose form of allowing access where owners may control access, as well as grant access to others
 - Ownership determines allowed access (e.g., the creator of a file may allow others to read or write to it)

*Source: <http://csrc.nist.gov/publications/history/bell76.pdf>

Access Control Models

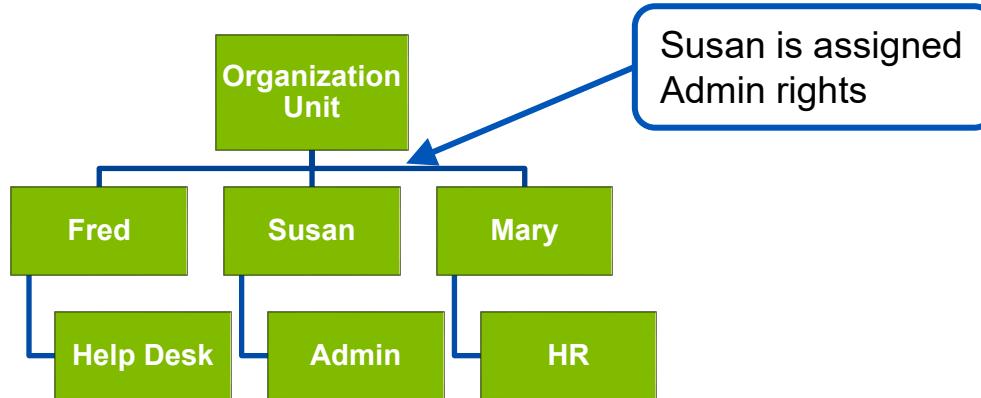
- ▶ **Role-based access control (RBAC)**
 - Easy and hierarchical way to enforce least privileges
 - Manages job rotation
 - Needs a matrix of required privileges to assign rights
 - Access is granted/denied based on the role membership of an individual (e.g., some users may change a record because they are in the Power_users group, not because they have individual rights)
- ▶ **Role-based access control is supported by creating and managing roles composed of user rights and object permission settings; roles may be assigned by**
 - Role in the organization
 - Tasks commonly performed by the role
 - Makes management of job rotation easier
- ▶ **Requires an operating system that provides for multilevel security**

Access Control Models

► Rule-based access control (RBAC)

- Access is allowed or denied to objects based on rules defined by the system administrator
- Specific rules are written for who has access to services or objects
- There is usually an “implicit deny” rule to handle all exceptions
- Firewalls

► Attribute-based access control (ABAC)



Contents

- ▶ Common Security Measures
- ▶ Asset Management
- ▶ Vulnerability Management
- ▶ Monitoring Security
- ▶ Enhancing Enterprise Security
- ▶ Identity and Access Management

Security Automation

- ▶ Incidents and Investigations



Automation and Scripting

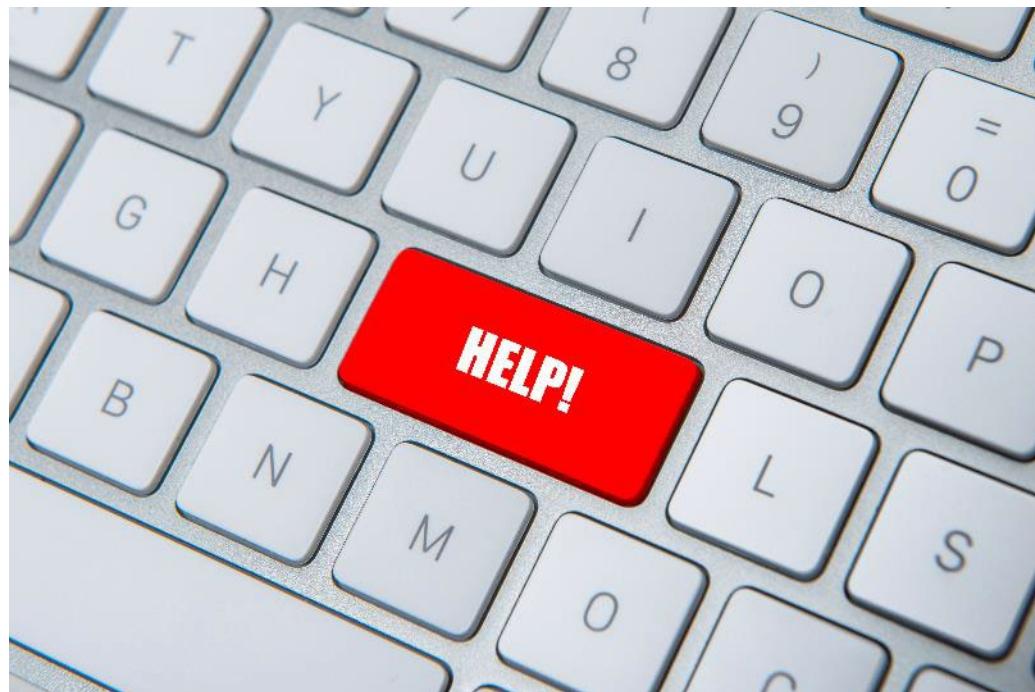
- ▶ **Commonly implemented with SOAR**
 - Security orchestration, automation, and response
- ▶ **Scripts and automation should be used to optimize use and security**
 - More reliable, consistent, accurate and faster than manual changes
 - Provisioning
 - Guardrails
 - Limits and restrictions
 - Tickets
 - Escalation
 - Service management
 - Continuous integration and monitoring
- ▶ **Benefits are**
 - Efficiency/time saving
 - Enforcing baselines
 - Standard infrastructure configurations
 - Scaling in a secure manner
 - Employee retention
 - Reaction time
 - Workforce multiplier

Provisioning and Deprovisioning

- ▶ **Applications are staged on servers, and these must be created and managed**
 - Provisioned
 - Hardened
 - Configured
 - Adequate storage and RAM
 - Match the policy baseline
 - Deprovisioned when no longer used
- ▶ **Automated scripting should be used to enable or disable services**
 - Faster and more consistent
- ▶ **Guardrails**
 - Policies or rules that are used to ensure that resources are provisioned in a secure and compliant manner
 - A guardrail could be used to prevent users from provisioning resources in a public cloud environment without first obtaining approval from a security team

Ticketing and Escalation

- ▶ By automating tasks such as ticket creation, routing, and assignment, organizations can reduce the time it takes to respond to security incidents
- ▶ One common approach is to use a security orchestration, automation, and response (SOAR) platform
 - SOAR platforms provide a platform for managing security incidents and automating task
- ▶ SOAR can automate
 - Incident identification
 - Notification
 - Ticket generation
 - Escalation
 - Responses
 - Defensive measures



Continuous Integration and Testing

- ▶ A set of practices that automates the software development and release process
 - Continuous integration
 - Developers frequently commit their code changes to a central repository frequently, and the code is automatically built and tested
 - Continuous testing
 - Code changes are automatically tested against a variety of scenarios
 - Continuous delivery
 - Once code changes have been integrated and tested, they are automatically deployed to a staging environment
 - Continuous deployment
 - Once the software has been tested and approved in the staging environment, it is automatically deployed to production
- ▶ Best practices
 - Automate Everything
 - Isolate Environments
 - Monitor and Measure
 - Version Control
 - Parallel Testing
 - Test Early and Often

Other Automation Considerations

- ▶ **Complexity**
 - Of the systems
 - Of the automation scripts
- ▶ **Single point of failure**
 - Automation can become a SPoF
- ▶ **Cost**
 - A cost/benefits analysis should be done before committing to scripting and automation initiatives
- ▶ **Technical debt**
 - Failing to account and plan for needed future efforts and maintenance
 - The implied cost incurred when businesses do not fix problems that will have impact in the future
- ▶ **Ongoing supportability**
 - Can onboard personnel maintain, or does it require external support



Pop Quiz: Automation



- 1. The CISO of an organization is concerned that system provision and maintenance automation may go too far and result in costly mistakes. What is the best solution?**
- 2. An organization decided to abandon a software project, due to costs and excessive labor involved in maintenance. As the project expanded, the teams were not able to work in sync and manual updates were continually required. What term describes this situation?**

Contents

- ▶ Common Security Measures
- ▶ Asset Management
- ▶ Vulnerability Management
- ▶ Monitoring Security
- ▶ Enhancing Enterprise Security
- ▶ Identity and Access Management
- ▶ Security Automation

Incidents and Investigations



Incident Response Steps

- NIST document SP 800-61 describes well-accepted response steps
 - Preparation
 - Establish responses capabilities, policies and detection systems
 - Detection and analysis
 - Occurs via automated (IDS) or manual means (audit) and identified, then responses are triggered. Scanning to verify incident and vulnerability
 - Containment
 - As needed to prevent an incident from escalating in severity
 - Eradication
 - Threat removal
 - Recovery
 - Returning to normal operation
 - Lessons learned
 - Documenting measures that would mitigate another instance of the incident



Incident Testing and Preparation

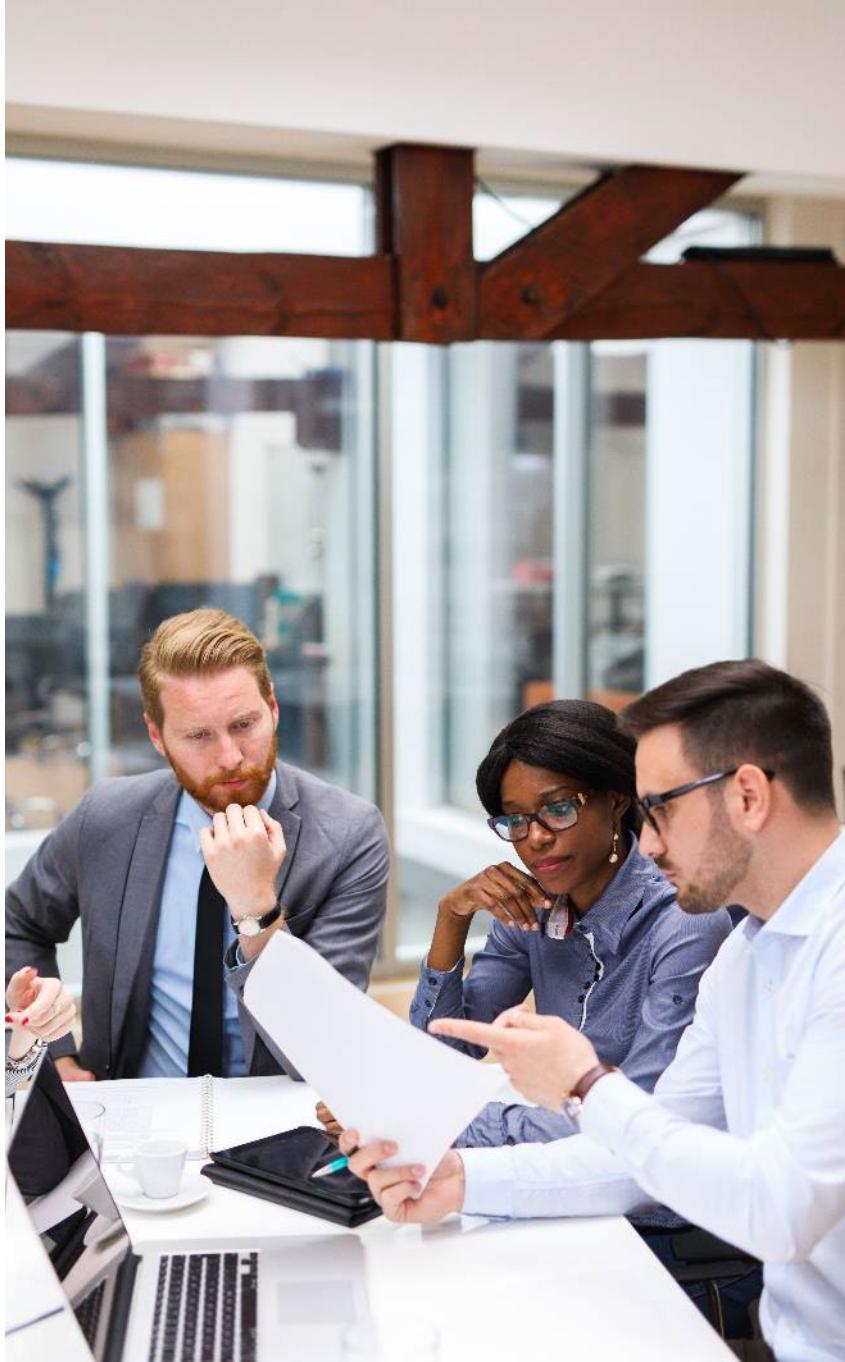
- ▶ **Annual training to ensure the effectiveness of personnel and plans**
 - Disaster recovery
 - Business continuity

- ▶ **Planning should include**
 - Communications plans for stakeholders
 - Tabletop exercises
 - Time-efficient
 - Simulations
 - Good for what-if and changing scenarios
 - Most realistic
 - Periodic reviews of policies
 - Evaluating systems and personnel



Post-Incident Activities

- ▶ **Root cause analysis (RCA)**
 - Determining the basic mistakes or conditions that led to an incident
- ▶ **Threat hunting**
- ▶ **Digital forensics**
- ▶ **Legal hold**
- ▶ **Acquisition**
- ▶ **Chain of custody**
- ▶ **Preservation**
- ▶ **Reporting**
- ▶ **E-discovery**



Threat Hunting and Research

► Threat hunting and intelligence resources

- Digging through old logs
- Search engines (OSINT)
- Threat feeds and fusion of information
- Vulnerability databases and vendor bulletins
- Indicators of compromise (IOC) and the Dark web
 - AIS—automated indicator sharing
 - Structure Threat Information eXpression
 - Language for sharing cyber threat data
 - TAXII—Trusted Automated eXchange of Indicator Information
 - Application specification

► Research tools

- Vendors
- Vulnerability feeds
- Meeting and conferences
- Industry groups and social media
- RFCs

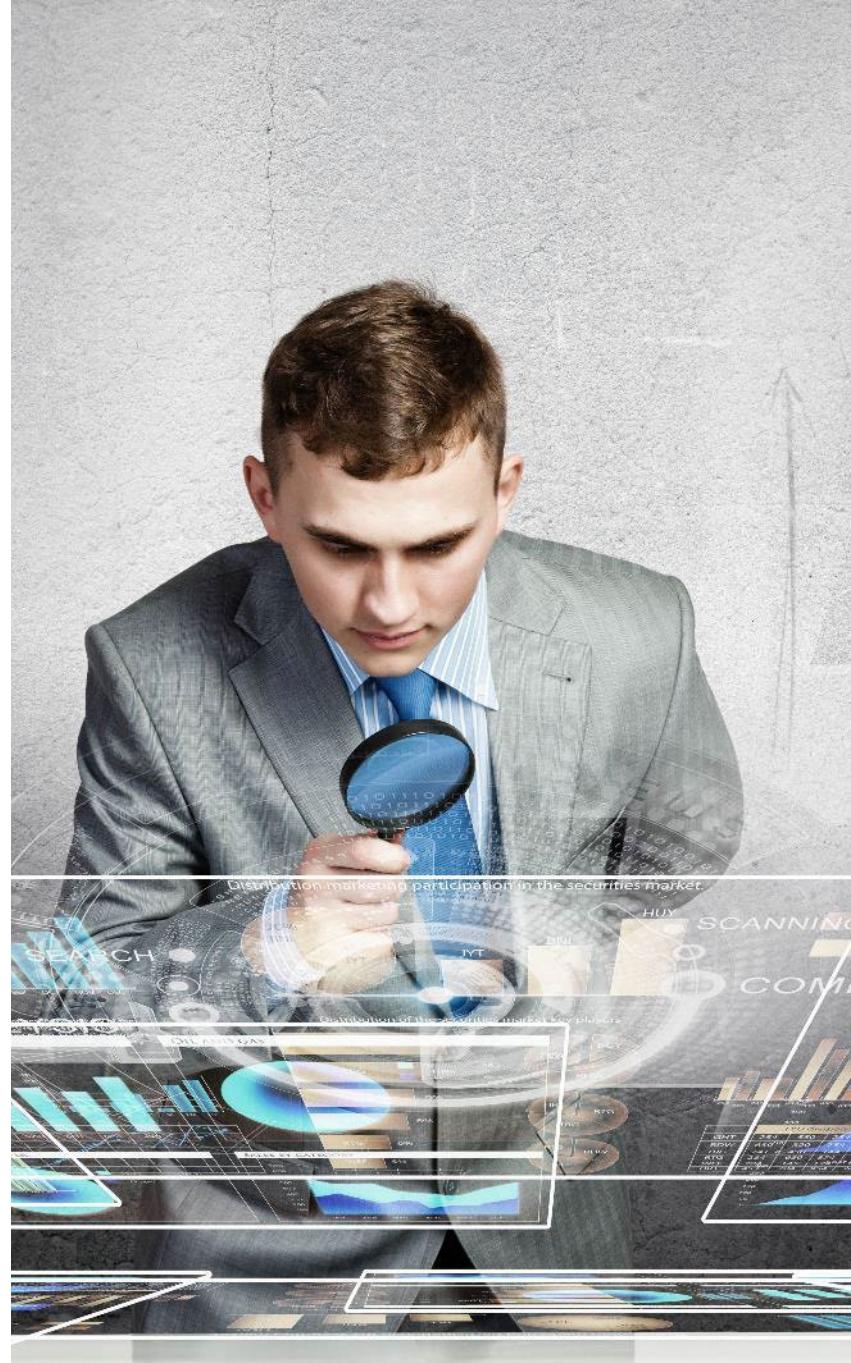
Digital Forensics

- ▶ **Forensics is a form of incident response**
 - It is an investigation of the incident
- ▶ **IT details**
 - Agent of attack
 - Attack objective
 - Methods used
 - Scope: What did it affect?
 - Severity
 - Intelligence gathered
- ▶ **Primary focus of first responders is on minimal interaction and preserving evidence**
- ▶ **Legal hold established**
 - A notice that is issued by an authorized party to require the recipient to preserve all relevant electronic data



Capturing Forensic Information

- ▶ **Information to be captured**
 - System image hashed
 - Memory dumps of keystrokes and last applications run
 - Network traffic and logs
 - Screenshots
 - MAC addresses (most uniquely identifies a host)
 - Witness interviews
- ▶ **Document**
 - Techniques, time, and effort spent
 - Record methods used to capture and preserve evidence and time spent



MAC = Media Access Control

Chain of Custody and Preservation

- ▶ **The chain of custody should be implemented immediately upon gathering evidence**
- ▶ **Evidence has no validity**
 - Unless the point of collection can be established
 - Unless the method of collection is documented
 - Unless the handling and transferring of evidence from the crime scene to the courtroom are proven
- ▶ **The chain of custody identifies**
 - All handlers
 - Preservation techniques
 - Failure to preserve a chain of custody renders the evidence useless
- ▶ **Data capture with dd and write blocking controller or other approved tools**
 - Must be documented
 - Show provenance—a certifiable history
 - Have Non-repudiation
 - Hashing and digital signatures

E-discovery

- ▶ **Identifying, collecting, processing, and producing electronically stored information in response to a legal proceeding**
- ▶ **It is made complex by**
 - The potential volume of information to be searched and retrieved
 - Multiple locations across systems, sites and the cloud
 - Numerous format
 - Multiple jurisdictions



Sources of Incident Information

► Logs

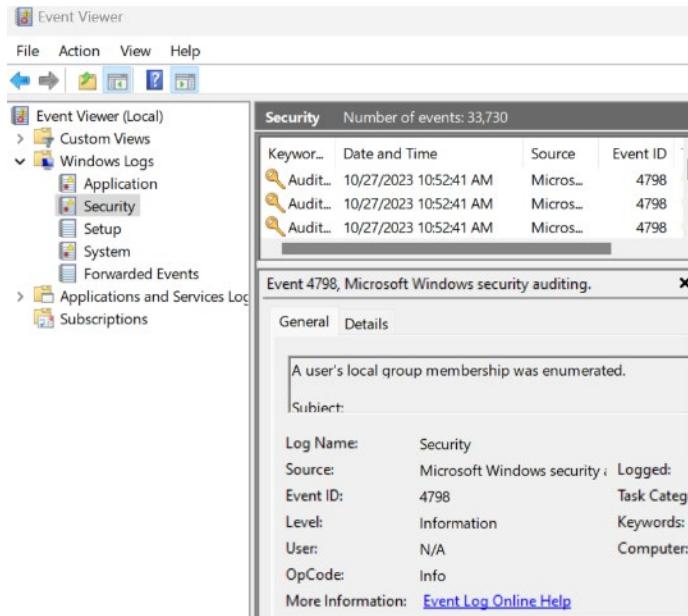
- Firewalls
- Applications
- Endpoints and managers
- OS logs

► Defensive systems

- SIEM
- Vulnerability scans

► Infrastructure

- Packet captures
- Netflow



Domain 4: Match the Items to the Topics

Do Now

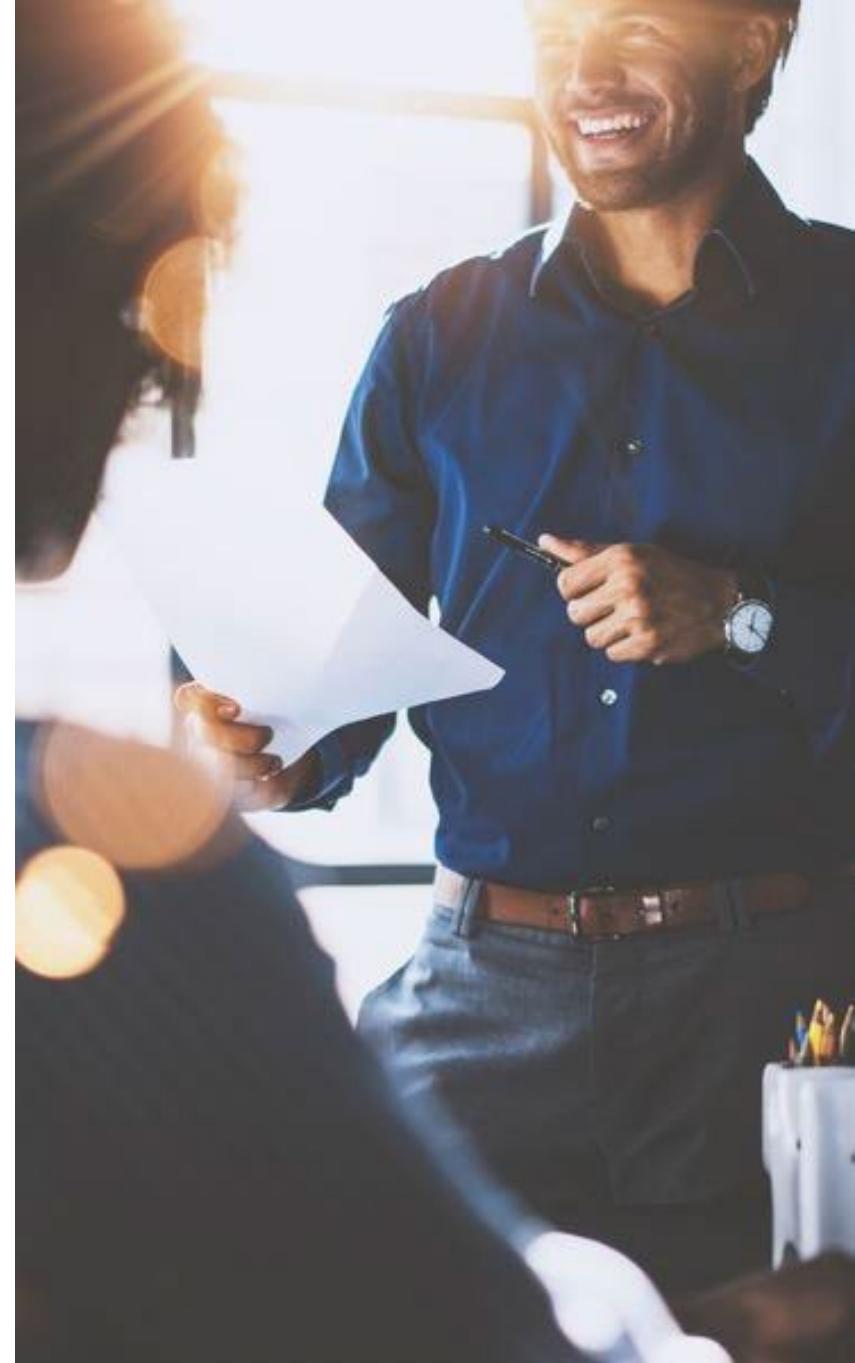
Item	Answer	Topic
Saving code changes frequently		A. IoC
Email and DNS		B. SOAR
Opposite of MAC		C. Recovery
Follows eradication		D. SPF
A rogue user created		E. Discretionary
Authorized when needed		F. Continuous integration
Automated ticketing		G. OAuth2
Authorized app		H. JIT permissions

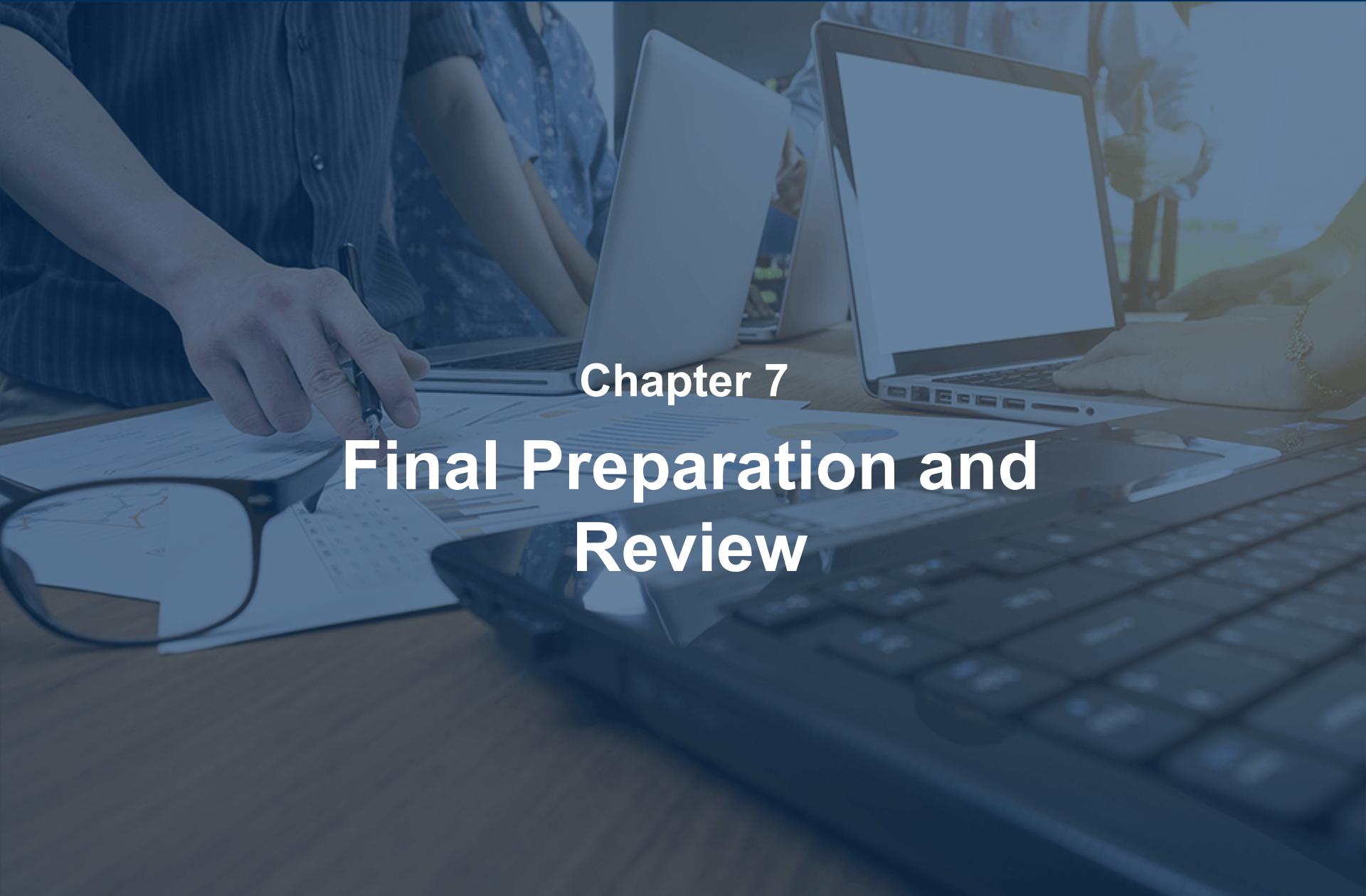
For each item on the left, write in the corresponding letter from a topic on the right

Objectives

- ▶ **Inspect common security measures**
- ▶ **Identify proper asset management**
- ▶ **Manage vulnerability in the enterprise**
- ▶ **Monitor and alert for security incidents**
- ▶ **Implement strong enterprise security**
- ▶ **Select the appropriate identity and access management**
- ▶ **Understand how to automate security**
- ▶ **Respond to incidents and investigations**

28%



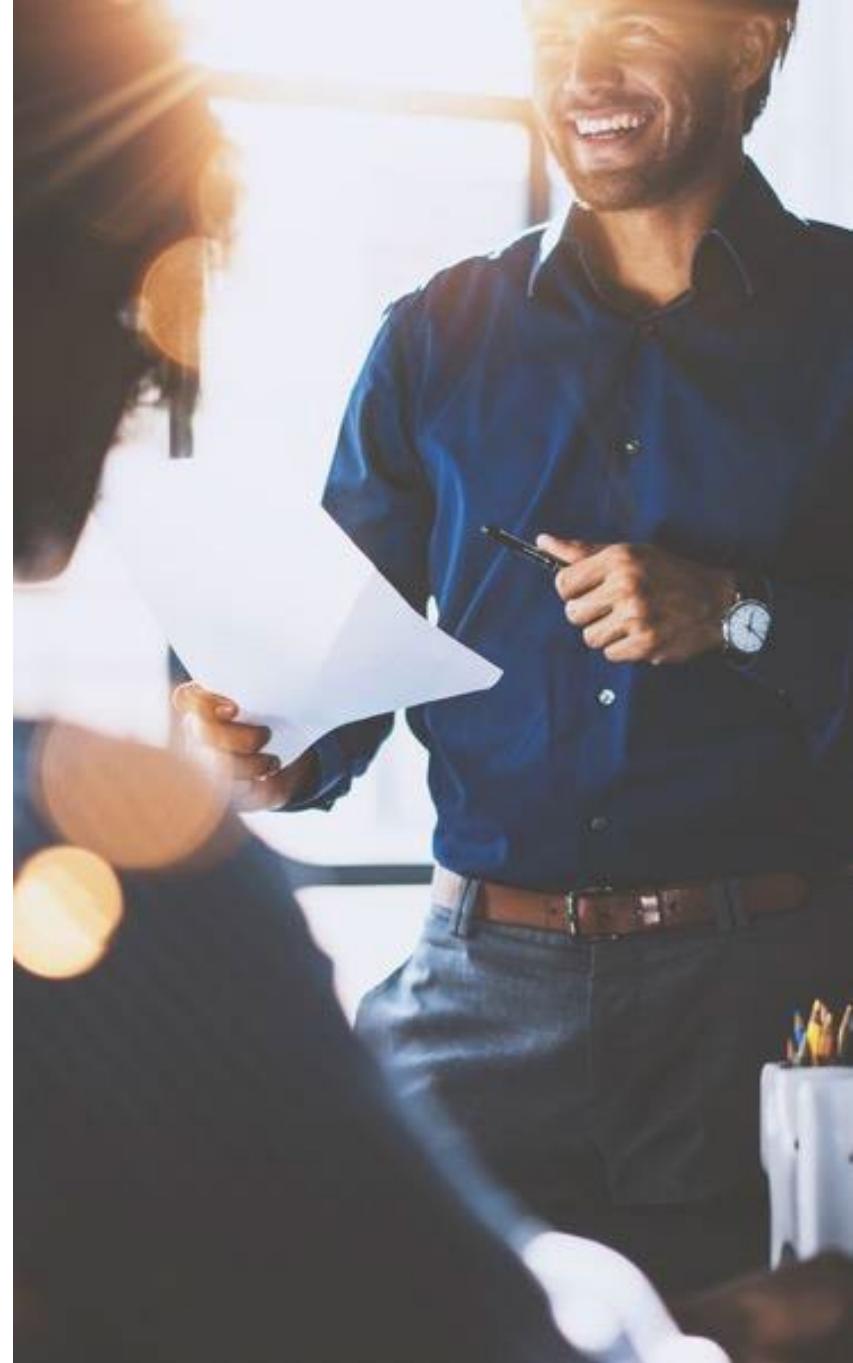


Chapter 7

Final Preparation and Review

Objectives

- ▶ **Review the SY0-701 examination procedures**
- ▶ **Enumerate the composition of the exam**
- ▶ **Prepare to handle out-of-date topics**
- ▶ **Discover strategies for examination time management**
- ▶ **Learn to choose the “correct” right answer**



Contents

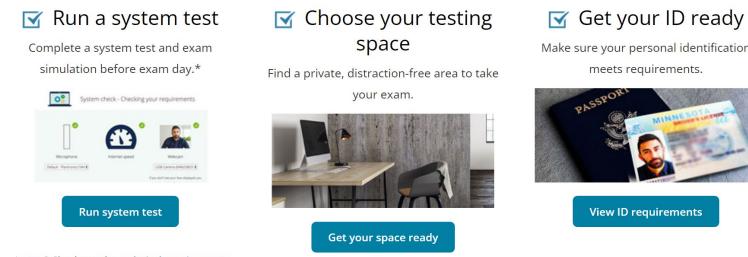
Examination Procedures

- ▶ General Guidelines
- ▶ Examination Time Management
- ▶ The “Correct” Right Answer



Exam Procedures

- See <https://home.pearsonvue.com/> to register
 - Go to this link for options on taking the exam remotely
 - <https://home.pearsonvue.com/comptia/onvue>
 - Remote procedures may vary from the procedures noted below



- Be sure to have two valid forms of ID, one government-issued with photo
 - Another with a signature, such as a payment card
- Arrive at least 15 minutes early
 - If you are late, your voucher/payment may be forfeited
 - A two-hour slot is allocated for your 90-minute test session
 - 15-minute check-in and check-out

Exam Procedures

- ▶ **Surrender all books, notes, and electronic devices**
 - Request separate secure storage for your items
 - They are commonly all locked in a group cabinet
- ▶ **Your seat may be pre-assigned**
 - Possible choice
 - But you may request ample seating and that hardware be appropriately placed
- ▶ **Request additional pads and pens before starting**
 - You may make notes on an erasable tablet during the exam
 - Difficult to make requests once the exam has begun
 - Must be turned in at the end
- ▶ **Upon starting the exam**
 - Immediately use your notes to recompose any mnemonics or difficult-to-remember items

Contents

- ▶ Examination Procedures

General Guidelines

- ▶ Examination Time Management
- ▶ The “Correct” Right Answer



Composition and Grading

- ▶ **Approximately 72 to 90 questions are selected for each candidate**
- ▶ **Questions may occur in any order**
 - Not necessarily Domain 1, Domain 2, etc.
 - Exhibits are presented first (five to seven items)
- ▶ **Expect**
 - Unique questions are drawn from the entire CompTIA outline
 - Few repeated topics
 - Many questions are verbose and require time to assess
 - Some may involve a calculation
- ▶ **You will receive a grade after completing the test and a demographic survey**
- ▶ **Results will show Pass/Fail and a 100-900 scale score**
- ▶ **Incorrectly answered items will reference the CompTIA Outline**
 - Each incorrect answer will have a reference to the Security+ outline

Guidelines

- ▶ **Questions will initially be presented in sequence**
 - Exhibits are typically presented at the beginning
 - You may mark items and choose to go back
 - At the end, you may review all or just marked questions
 - Multiple answer questions with insufficient answers are flagged
- ▶ **Remember, you may**
 - Spend any amount of time on any question
 - Make notes
 - Mark questions for review and change any answer
 - Review in any order
 - Review only marked questions with a simple selection
- ▶ **Complete the full exam and review your answers**
 - Consider marking and reviewing in several cycles, as time allows
 - Do not rush, as swift (less than 45 minutes) passing scores may be red-flagged as suspicious

Read the Questions Very Carefully

- ▶ **Leave nothing blank or unanswered**
 - Blank = wrong
- ▶ **Be careful when the item asks for the *best* solution**
- ▶ **Expect many questions to be long or complex**
 - Multiple sentences
 - Much reading and analysis
 - Time-consuming
- ▶ **Failing to spot “*not*” or “*except*” in a stem will cause you to find the first matching choice**
 - Most likely a distracter
 - Probably not the correct answer
- ▶ **Read *all* possible answers before selecting**
 - Some questions require the *best* answer
 - The first answer could be correct, but not as good as the last

Tough Questions

- ▶ **CompTIA periodically inserts questions that do not count**
 - Beta testing for future tests
 - You may not have been briefed on the topic
 - Do not panic if you have not heard of the issue—it might be a question being previewed for future exams
- ▶ **Many questions ask for the *best* or *first* thing to do out of an incomplete list**
 - For example: Which is the first or best thing to do when starting something?
 - A. Step 8
 - B. Step 5
 - C. Step 7
 - D. Step 3
- ▶ **The answer is Step 3**
 - Do not expect a full set of options for each test item
 - Step 1 may not be present

Beware of the Word **And**

- ▶ Some items may incorporate compound selections
- ▶ The word **and** requires all components to be true and exist
- ▶ Example
 - Choose the *best* fire response or suppression system for general combustibles
 - A. Spread foam and thermite at the base of the fire
 - B. Spray nitrogen tetroxide and leave the location
 - C. Trigger the alarm system and use ThermoSafe
 - D. Yell “*Fire!*” and run out of the room
- ▶ The best answer is D
 - While not very brave or technical-sounding, the others are worse
 - Thermite is an incendiary
 - Nitrogen tetroxide is a rocket fuel
 - ThermoSafe sounds good, but does not exist

What Is Sought?

- ▶ **Examine the wording**
 - Does it seek to identify a problem or solution?
 - Provide only enough to identify a solution—not more
- ▶ **Do not “over-answer” the question**
- ▶ **The *best* way to achieve confidentiality is:**
 - A. Use symmetric encryption and authenticate <<<< Too much
 - B. *Use symmetric encryption*** <<<< *The correct choice*
 - C. Authenticate <<<< Wrong choice
 - D. Digitally sign <<<< Wrong choice

Contents

- ▶ Examination Procedures
- ▶ General Guidelines

Examination Time Management

- ▶ The “Correct” Right Answer



Time Is Critical

- ▶ You will have 90 minutes on the real examination
 - Up to 100 actions or answer selections
 - Simulations count for multiple actions and points
 - 72 to 90 questions
- ▶ Each selection/answer counts as a point
- ▶ Practice with the set of four questions on the next four slides
 - You have three minutes



Time Management Question 1

- Circle the exact location of the Caucasus Mountains on this map



Time Management Question 2

- An administrator logs on to her workstation and sees that the time is not correct. She then checks her watch and confirms that the time is likely incorrect. The organization uses a time server located in Boulder, Colorado. Lately, there has been severe weather activity across the Midwest that has caused *intermittent* Internet connectivity with the atomic clock in Boulder. What should the administrator do?
(Choose one)
- A. Fix the problem
 - B. Escalate the issue to the next level of support
 - C. Alert the appropriate group
 - D. Wait until lunch

Time Management Question 3

- Which standards actually exist? (Select all correct answers)
 - A. PKCS #19
 - B. PKCS #10
 - C. PKCS #5
 - D. PKCS #11(a)

Time Management Question 4

► Identify a mobile deployment model

- A. BYoC
- B. MDM
- C. MaaS
- D. COPE

If you are not reading this after 45 seconds,
you are either a genius or are not managing time well

Time and Questions

- ▶ **Expect to take 20-35 minutes initially for exhibits and simulations**
- ▶ **All actions count nearly the same**
 - A short, single answer counts as much as a long scenario
 - Answer the questions that can be managed easily first
 - Get all the low hanging fruit
- ▶ **You have no way to know if the remaining questions are lengthy and difficult or easy with single choices**
- ▶ **Handle the easier items first**
 - Mark the rest

Contents

- ▶ Examination Procedures
- ▶ General Guidelines
- ▶ Examination Time Management

The “Correct” Right Answer

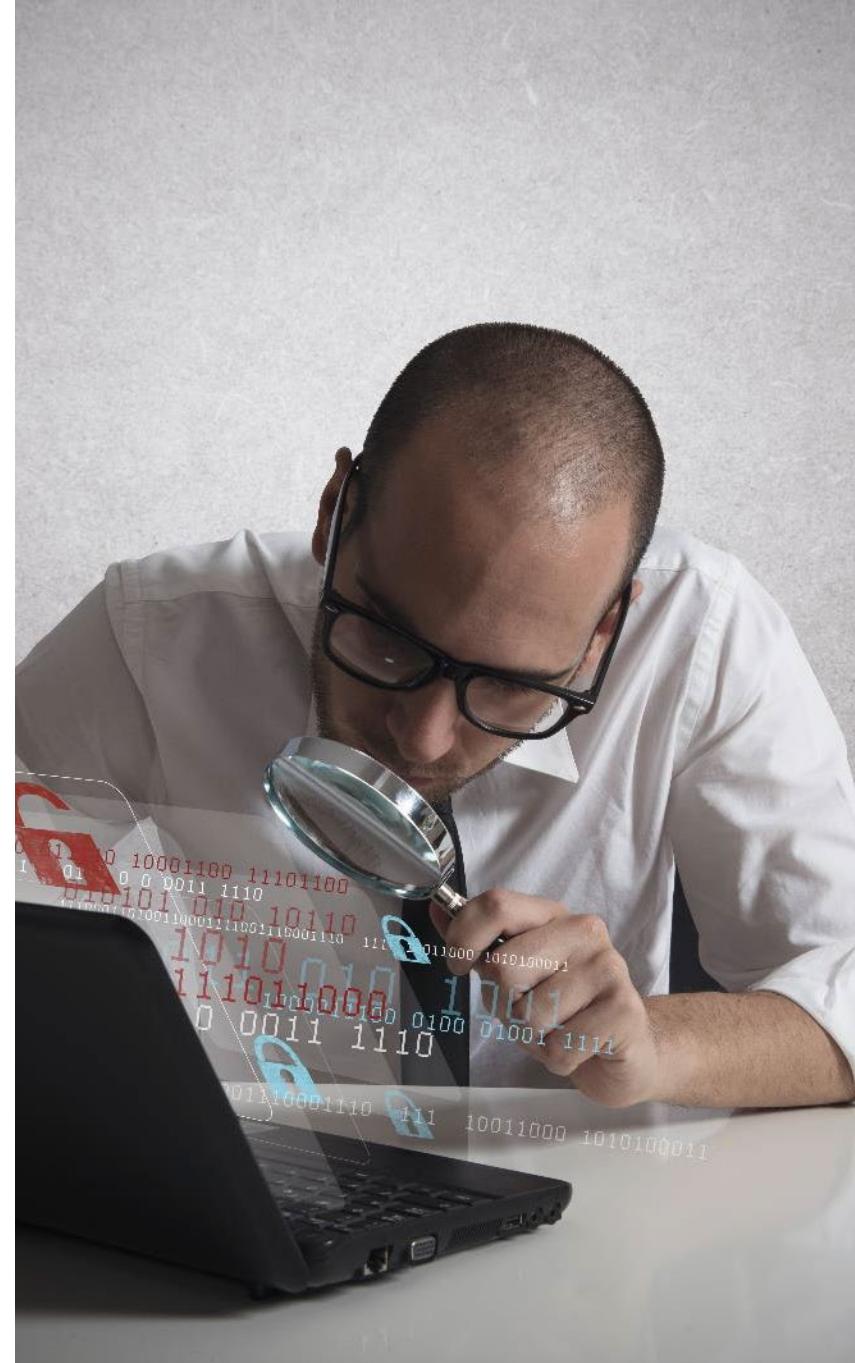


Knowledge Is Best, But...

- ▶ **Knowing the material is the best way to achieve a passing score**
 - Still, some questions will be difficult
 - Very wordy with superfluous information
 - Obscure terminology
- ▶ **The following may help when you have no idea about the correct answer**
 - Interpret in the most common and ordinary way
 - When in doubt, an answer with “policy” is a good choice
 - Cross-reference other similar questions (Take notes!)
- ▶ **Using logical problem-solving techniques may reduce the possibilities**
- ▶ **Most tests are balanced among choices**
 - Infamous answer “C” probably does not apply

Most Common and Ordinary

- ▶ **Generally, you may expect the correct answer to involve the most common and ordinary conditions**
- ▶ **Many issues may be dissected to the point where several answers could be correct**
 - You could penalize yourself by overanalyzing
 - Resist adding conditions and circumstances to create your own answer
 - Choose a simple situation or interpretation that fits



Choose the Common or Ordinary Answer

- 1. Firewalls perform the following function (choose one)**
 - A. May detect and alert on attempted intrusions
 - B. Perform network address translation
 - C. Set up tunnels for VPNs
 - D. Block intruders from gaining access to internal networks

Choose the Common or Ordinary Answer

1. The primary purpose of a firewall is to protect the internal network as well as to regulate inside-to-out connections
- The other choices are additional functions that they *may* perform
- A. May detect and alert on attempted intrusions
 - B. Perform network address translation
 - C. Set up tunnels for VPNs
 - D. *Blocking intruders from gaining access to internal networks*

Follow Policy and Procedures

- ▶ **Some questions will often have excellent distractors, with “Policy” as another option**
 - Distractors may
 - Reference sound published research
 - Promote excellent standards
 - Following “Policy” may seem absurd compared to the other options
- ▶ **No matter how good the options, following “Policy” is nearly always correct**



Follow Policy and Procedures

- ▶ **What should you do when a virus outbreak occurs?**
 - A. Contain and eradicate the infection <<<< Good, but wrong
 - B. Alert your superiors <<<< Good, but wrong
 - C. Shut down the machine <<<< Good, but wrong
 - D. Follow established policy* <<<< *The correct choice*

- ▶ **Which of these is best when doing a forensic analysis**
 - A. Follow NIST standards <<<< U.S.-centric
 - B. Comply with the Computer Criminality Act <<<< U.K.-centric
 - C. Adhere to organizational standards* <<<< *The correct choice*
 - D. Avoid contaminating the crime scene <<<< Good, but wrong

Look for Answers in Other Questions

- ▶ A common strategy for creating a base of examination questions is to reverse the stem and distracters
- ▶ It requires a good memory or notes
 - It can isolate the correct answer

Reversed Questions

1. What is the meaning of this unknown concept?

- A. It uses ABC protocol
- B. The XYZ system is in flux
- C. It implements ABD protocol
- D. It guides spaceships

25. XYZ flux protocols is:

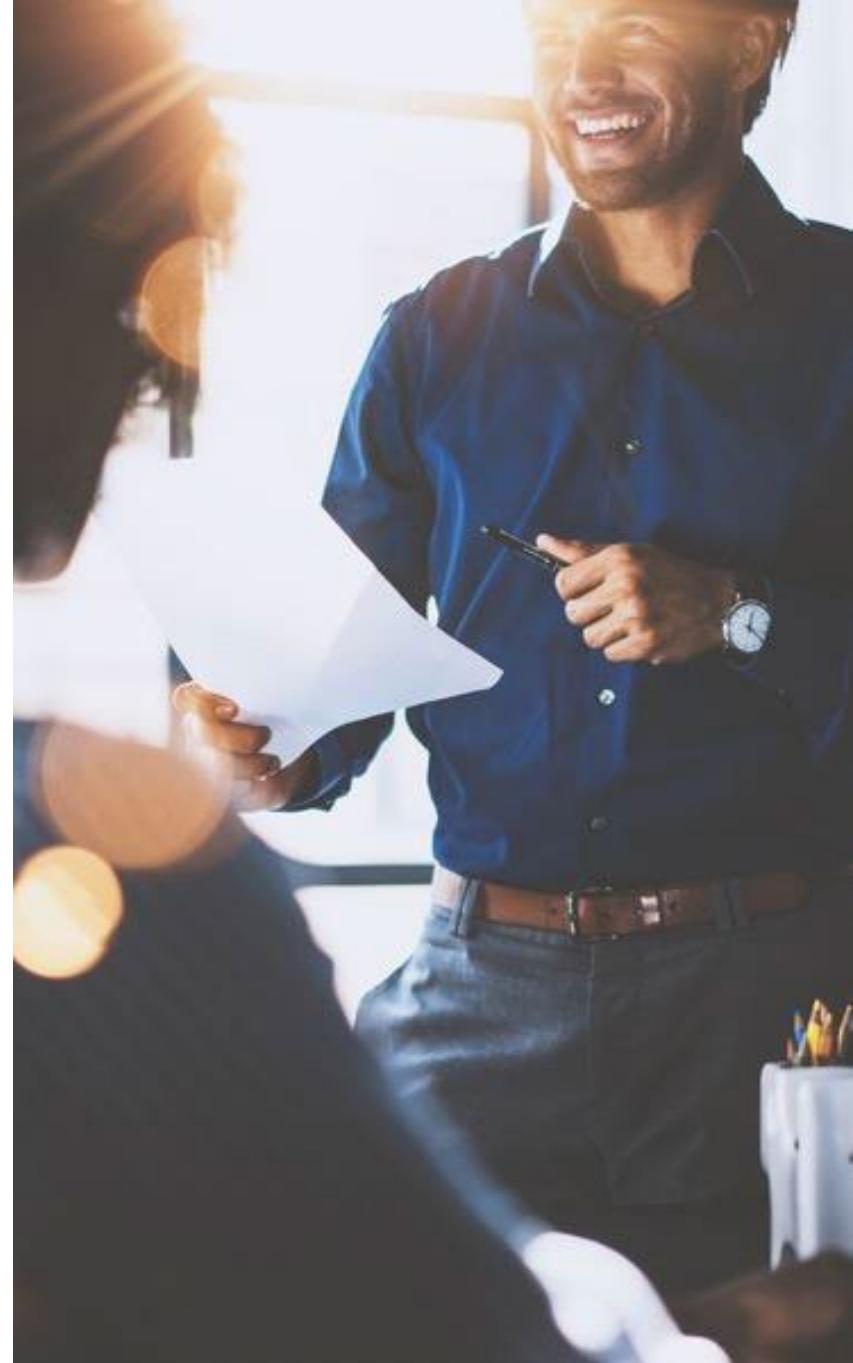
- A. Internationally recognized
- B. Nonexistent
- C. An unknown concept
- D. Used to guide spaceships

Reversed Answers

- ▶ In the two questions, only two answers overlapped
 - *The XYZ system is in flux* <<<<
 - Nonexistent
 - *An unknown concept* <<<<
 - Used to guide spaceships
- ▶ The “unknown concept” and “XYZ flux” had the best relationship of stems and distractors

Objectives

- ▶ **Review the SY0-701 examination procedures**
- ▶ **Enumerate the composition of the exam**
- ▶ **Prepare to handle out-of-date topics**
- ▶ **Discover strategies for examination time management**
- ▶ **Learn to choose the “correct” right answer**





Chapter 8

Course Summary

Course Objectives

- ▶ **Introduce the Security+ Objectives and outline testing procedures**
- ▶ **Review the basic elements of cybersecurity**
- ▶ **Inspect security program oversight and management**
- ▶ **Investigate threats, attacks, and mitigations**
- ▶ **Apply secure architecture and design principles**
- ▶ **Utilize secure protocols and defenses**
- ▶ **Inspect identity management and cryptography**
- ▶ **Assess readiness for the exam**

