BlackHack Academy

Security+ SY0-701

Enrichment Program

10-Week Intensive Bootcamp | Purple Team Edition

"Home for Ethical Hackers"

BlackHack Society

CompTIA Security+ SY0-701 Certification Preparation

Complete Beginners to Exam-Ready in 10 Weeks

root@blackhack:~# ./start_curriculum.sh

Table of Contents

Program Overview

Course Philosophy: The Purple Team Way

The BlackHack Academy Security+ program is built on a foundational principle: every topic is taught through both offensive AND defensive lenses. We call this the Purple Team Mentality. Red teams attack. Blue teams defend. Purple teams do both — because the best defenders think like attackers, and the best attackers understand the defender's playbook.

This is not a passive certification prep course. You will build attack labs, crack passwords, exploit vulnerable applications, and launch network scans. Then you will immediately pivot to the defensive side — configuring firewalls, tuning SIEM alerts, hardening systems, and responding to the very attacks you just executed. This dual perspective creates security professionals who truly understand the threat landscape.

Target Audience

This program is designed for complete beginners with no prior IT or cybersecurity background. If you can use a computer and are willing to learn, you belong here. By the end of 10 weeks, you will have the knowledge to pass the CompTIA Security+ SY0-701 exam and the practical skills to contribute on day one in a security role.

Program Details

Parameter	Details
Duration	10 weeks intensive bootcamp
Exam Alignment	CompTIA Security+ SY0-701
Format	Lectures + Labs + Case Studies + Practice Exams
Prerequisites	None — complete beginners welcome
Lab Environment	VirtualBox + Kali Linux + Target VMs (all free)
Certification	CompTIA Security+ (vendor-neutral, DoD 8570 compliant)

Tools Needed (All Free)

All labs use exclusively free and open-source tools. Required accounts:

- VirtualBox — virtualization platform for your attack/defense lab
- Kali Linux — penetration testing operating system
- Any.Run — interactive malware analysis sandbox (free tier)
- Splunk Free — SIEM for log analysis (up to 500MB/day)

- Shodan — internet-connected device search engine (free account)
- VirusTotal — file/URL scanning service (free account)

Source Philosophy

BlackHack Academy draws from two streams of knowledge, clearly labeled throughout all materials:

[OFFICIAL] Accredited Sources	[UNDERGROUND] Bleeding Edge Sources
CompTIA Official Materials NIST Publications (SP 800 series) SANS Reading Room MITRE ATT&CK Framework CISA Advisories OWASP Documentation RFC Documents	Reddit (r/netsec, r/cybersecurity, r/hacking) YouTube (NetworkChuck, John Hammond, IppSec, TheCyberMentor) DEF CON / Black Hat talks Security researcher blogs Exploit-DB Hacker conference proceedings Underground community knowledge

SY0-701 Exam Domain Map

The CompTIA Security+ SY0-701 exam covers five domains. The table below maps each domain to its exam weight and the weeks in this program where it is covered.

Domain	Weight	Weeks	Visual Weight
1.0 General Security Concepts	12%	1–2	||||||
2.0 Threats, Vulnerabilities, and Mitigations	22%	3–5	||||||||||
3.0 Security Architecture	18%	6–7	||||||||
4.0 Security Operations	28%	8–9	||||||||||||
5.0 Security Program Management and Oversight	20%	10	||||||||

Study Priority by Domain Weight

Focus your study time proportionally to exam weight. Domain 4 (Security Operations) at 28% deserves the most attention, while Domain 1 (General Concepts) at 12% is foundational but carries the least weight.

WEEK 1

Foundations & The Hacker Mindset

SY0-701 Objectives: 1.1: Compare and contrast various types of security controls | 1.2: Summarize fundamental security concepts

PURPLE TEAM FRAMING

This week establishes the BlackHack philosophy: every defender must think like an attacker, and every attacker must understand the defender's playbook. We examine security controls not just as protective measures, but as obstacles an adversary must bypass — and then we flip the script to understand why those controls exist. The CIA triad is explored through both the lens of an attacker trying to violate confidentiality, integrity, and availability, and a defender working to preserve them.

Learning Objectives

1. Classify security controls by category (technical, managerial, operational, physical) and type (preventive, detective, corrective, compensating, deterrent, directive)
2. Explain the CIA triad and apply it to real-world security scenarios
3. Describe the AAA framework (Authentication, Authorization, Accounting) and its role in access management
4. Articulate Zero Trust architecture principles including control plane and data plane components
5. Differentiate between deception technologies: honeypots, honeynets, honeyfiles, and honeytokens
6. Set up a virtualized attack/defense lab environment using VirtualBox and Kali Linux
7. Adopt the purple team mindset — understanding security from both offensive and defensive perspectives

Lecture Topics

- Introduction to the Purple Team Philosophy — why BlackHack trains both offense and defense
- Brief History of Hacking: From phone phreaking to nation-state APTs
- Security Controls Deep Dive:
  - Categories: Technical (firewalls, encryption), Managerial (policies, risk assessments), Operational (training, change management), Physical (locks, cameras)
  - Types: Preventive vs. Detective vs. Corrective vs. Compensating vs. Deterrent vs. Directive
  - Layered defense: How controls overlap to create defense-in-depth
- The CIA Triad — Confidentiality, Integrity, Availability:
  - Real-world mapping: encryption = confidentiality, checksums = integrity, redundancy = availability
  - How attackers target each pillar (data theft, tampering, DDoS)
- Non-Repudiation: Digital signatures, audit logs, and why they matter legally
- AAA Framework:
  - Authentication: something you know/have/are, multi-factor concepts
  - Authorization: RBAC, ABAC, MAC, DAC overview

  - Accounting: logging, auditing, SIEM introduction
- Zero Trust Architecture:
  - 'Never trust, always verify' — the end of perimeter-based security
  - Control Plane: Policy Engine, Policy Administrator, adaptive identity
  - Data Plane: Policy Enforcement Point, implicit trust zones, subject/system
- Physical Security Controls: Bollards, access control vestibules, fencing, video surveillance, sensors (IR, pressure, microwave, ultrasonic)
- Deception Technologies: Honeypots, honeynets, honeyfiles, honeytokens — how defenders use them to detect and study attackers
- Setting Up Your Lab: VirtualBox installation, Kali Linux VM, Windows target VM, network configuration

Official Sources

[OFFICIAL] CompTIA Security+ SY0-701 Certification Guide, 3rd Edition — Chapters 1-2

[OFFICIAL] NIST SP 800-53 Rev. 5 — Security and Privacy Controls for Information Systems
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[OFFICIAL] NIST SP 800-207 — Zero Trust Architecture
https://csrc.nist.gov/publications/detail/sp/800-207/final

[OFFICIAL] CISA Zero Trust Maturity Model
https://www.cisa.gov/zero-trust-maturity-model

[OFFICIAL] SANS Reading Room — 'Defense in Depth: An Impractical Strategy?'
https://www.sans.org/white-papers/defense-in-depth/

Underground / Bleeding Edge Sources

[UNDERGROUND] r/netsec — 'Zero Trust is not a product, it's a philosophy' discussion thread

[UNDERGROUND] NetworkChuck — 'You need to learn Virtual Machines RIGHT NOW!' video

[UNDERGROUND] John Hammond — 'Setting Up Your First Hacking Lab' tutorial series

[UNDERGROUND] DEF CON 27 — 'Honeypots: The Good, The Bad, and The Ugly' talk

[UNDERGROUND] r/cybersecurity — 'Best free resources for Security+ SY0-701' mega-thread

[UNDERGROUND] TheCyberMentor — 'Ethical Hacking in 15 Hours' full course (free on YouTube)

CASE STUDY: Kevin Mitnick & SolarWinds — From Social Engineering Pioneer to Nation-State Supply Chain Attack

Kevin Mitnick, once the FBI's most-wanted hacker, pioneered social engineering attacks in the 1980s-90s. He compromised Pacific Bell, Nokia, Motorola, and Sun Microsystems — not through sophisticated code exploits, but by manipulating people. He impersonated IT staff, dumpster-dived for passwords, and exploited the human element that no firewall could stop. His arrest in 1995 and subsequent 5-year prison sentence became a watershed moment for cybersecurity awareness. Mitnick later became a respected security consultant, proving that understanding the attacker mindset is the best defense.

Fast-forward to 2020: The SolarWinds Orion attack demonstrated how nation-state actors (Russian SVR/APT29 — Cozy Bear) compromised the software supply chain. Attackers inserted malicious code into SolarWinds' Orion IT monitoring platform update (SUNBURST malware), which was then distributed to approximately 18,000 organizations including the U.S. Treasury, Department of Homeland Security, and Fortune 500 companies.

What the attackers did right (from their perspective): They targeted the supply chain — a single point of trust that bypassed traditional perimeter defenses. They operated with extreme patience, remaining undetected for 9+ months. They mimicked legitimate Orion traffic patterns to avoid detection.

What the defenders did wrong: SolarWinds had weak build-process security. The update server password was reportedly 'solarwinds123'. Many organizations failed to apply the principle of least privilege to their monitoring tools — Orion had broad network access by design. Detection mechanisms were inadequate for supply chain attacks.

What was done right: FireEye (now Mandiant) detected the breach when they noticed unauthorized access to their own Red Team tools. Their transparent disclosure accelerated the response across the entire industry.

Lessons learned: Zero Trust is not optional — even trusted software must be verified. Supply chain security requires continuous validation. The purple team approach matters: defenders who think like attackers would have questioned why a monitoring tool needed such broad access.

HANDS-ON LAB: Build Your Attack/Defense Lab

Objective

Set up a fully functional virtualized security lab with Kali Linux (attacker) and a Windows/Linux target, establishing the foundation for all future hands-on exercises.

Tools Required

VirtualBox (free), Kali Linux ISO (free), Ubuntu Server ISO (free)

Step-by-Step Instructions

1. Download and install VirtualBox from https://www.virtualbox.org/
2. Download Kali Linux ISO from https://www.kali.org/get-kali/ (select 'Installer' for VirtualBox)
3. Create a new VM in VirtualBox: Name='Kali-Attack', Type=Linux, Version=Debian 64-bit, RAM=4GB, Disk=40GB
4. Mount the Kali ISO and install. Default credentials: kali/kali
5. Download Ubuntu Server ISO from https://ubuntu.com/download/server
6. Create a second VM: Name='Target-Ubuntu', Type=Linux, Version=Ubuntu 64-bit, RAM=2GB, Disk=20GB
7. Configure both VMs on an 'Internal Network' (VirtualBox > Network > Attached to: Internal Network, Name: 'hacklab')
8. Also add a NAT adapter to Kali for internet access (Adapter 2 > NAT)
9. Boot both VMs. On Kali, run 'ip addr' to confirm network interfaces
10. On Ubuntu target, install SSH server: 'sudo apt install openssh-server'
11. From Kali, verify connectivity: 'ping [Ubuntu-IP]'
12. Run your first scan: 'nmap -sV [Ubuntu-IP]' — observe open ports
13. Document your lab configuration: IP addresses, network topology, VM specs

Expected Outcomes

A working two-VM lab environment with network connectivity. Kali can reach the Ubuntu target. You've performed your first network scan and identified open services.

Purple Team Debrief

As an ATTACKER, you now have a platform to launch reconnaissance and exploits in a safe environment. As a DEFENDER, consider: what did that Nmap scan look like from the target's perspective? Check Ubuntu's auth.log and syslog. This is the core purple team exercise — always see both sides.

Key Terms & Definitions

CIA Triad
The three pillars of information security: Confidentiality (preventing unauthorized access), Integrity (ensuring data accuracy and trustworthiness), and Availability (ensuring authorized access when needed)

Zero Trust
A security model that requires strict verification for every person and device trying to access resources, regardless of whether they are inside or outside the network perimeter

AAA
Authentication, Authorization, and Accounting — the three-step framework for controlling access to network resources

Defense in Depth
A layered security strategy that uses multiple security controls at different levels to protect assets

Honeypot
A decoy system designed to attract attackers, allowing security teams to study attack methods and detect intrusions

Honeynet
A network of honeypots that simulates an entire production environment to trap and observe attackers

Honeytoken
A piece of fake data (credentials, files) planted to detect unauthorized access or data exfiltration

Non-Repudiation
The assurance that a party cannot deny the authenticity of their signature or the sending of a message

Compensating Control
An alternative security measure implemented when a primary control is not feasible

Policy Enforcement Point (PEP)
In Zero Trust architecture, the component that enables, monitors, and terminates connections between subjects and resources

Policy Engine
The Zero Trust component that makes access decisions based on policy and input from external sources

Gap Analysis
The process of comparing current security posture against desired or required standards to identify deficiencies

Bollard
A physical security barrier (short vertical post) designed to prevent vehicle-borne attacks on buildings

Access Control Vestibule
A physical security mechanism (formerly called a mantrap) using two interlocking doors to control entry

Purple Team
A collaborative security approach combining offensive (Red Team) and defensive (Blue Team) techniques to improve overall security posture

Practice Questions — Multiple Choice

Q1. A company implements a policy requiring all employees to wear ID badges. This is an example of which type of security control?

A. Technical

B. Managerial

C. Operational

D. Physical

Answer: C — Requiring employees to wear ID badges is an operational control — it's a procedure carried out by people in day-to-day operations.

Q2. Which component of Zero Trust architecture makes the final decision on whether to grant access to a resource?

A. Policy Enforcement Point

B. Policy Engine

C. Policy Administrator

D. Implicit Trust Zone

Answer: B — The Policy Engine evaluates requests against policies and makes the ultimate access decision. The Policy Administrator communicates the decision, and the PEP enforces it.

Q3. An organization deploys a fake database server containing fabricated customer records to detect insider threats. This is an example of:

A. Honeypot

B. Honeyfile

C. Honeypot with honeytoken

D. Honeynet

Answer: C — The fake database is a honeypot (decoy system), and the fabricated records within it are honeytokens (fake data designed to trigger alerts when accessed).

Q4. A security architect needs to ensure that data has not been tampered with during transmission. Which element of the CIA triad is being addressed?

A. Confidentiality

B. Integrity

C. Availability

D. Non-repudiation

Answer: B — Integrity ensures that data remains accurate and unaltered. Hash functions and digital signatures are common integrity controls.

Q5. After a firewall fails, it continues to allow all traffic through. This is an example of:

A. Fail-closed

B. Fail-open

C. Fail-safe

D. Fail-secure

Answer: B — Fail-open means the system allows all traffic when it fails, prioritizing availability over security. Fail-closed (fail-secure) would block all traffic.

Practice Questions — Performance-Based (PBQ)

PBQ1. SCENARIO: You are a security administrator tasked with classifying the following controls for a new data center. Drag each control to its correct CATEGORY and TYPE. Controls: (1) Installing security cameras, (2) Creating an acceptable use policy, (3) Deploying a firewall, (4) Requiring security awareness training, (5) Installing bollards around the building. Categories: Technical, Managerial, Operational, Physical Types: Preventive, Detective, Deterrent

> Answer: (1) Physical/Detective+Deterrent, (2) Managerial/Preventive, (3) Technical/Preventive, (4) Operational/Preventive, (5) Physical/Deterrent+Preventive. Security cameras are physical controls that detect and deter. An AUP is a managerial preventive control. A firewall is a technical preventive control. Training is an operational preventive control. Bollards are physical controls that deter and prevent vehicle attacks.

PBQ2. SCENARIO: Your organization is migrating to a Zero Trust architecture. The CISO asks you to diagram the key components. Identify and describe the role of each component: Policy Engine, Policy Administrator, Policy Enforcement Point. Then explain how a user request to access a file server flows through these components.

> Answer: Flow: (1) User requests access to file server → (2) Request arrives at Policy Enforcement Point (PEP), which intercepts the connection → (3) PEP forwards the request to the Policy Administrator → (4) Policy Administrator consults the Policy Engine → (5) Policy Engine evaluates the request against policies (user identity, device health, location, time, behavior analytics) → (6) Policy Engine makes grant/deny decision → (7) Policy Administrator instructs the PEP → (8) PEP either establishes or denies the connection. The key principle: no implicit trust — every request is verified regardless of network location.

WEEKLY CHALLENGE

Build a 'Security Control Matrix' for a fictional small business (a coffee shop with a website and POS system). Identify at least 15 security controls across all four categories (technical, managerial, operational, physical) and all six types. For each control, explain how an attacker might attempt to bypass it (offensive perspective) and how to strengthen it (defensive perspective). Document in a spreadsheet or table format.

WEEK 2

Cryptography — Locks, Keys, and How to Break Them

SY0-701 Objectives: 1.4: Explain the importance of using appropriate cryptographic solutions

PURPLE TEAM FRAMING

Cryptography is the backbone of all digital security — and breaking it is the holy grail of offensive hacking. This week, we learn how encryption protects data from the defender's perspective, then immediately switch to the attacker's view: how do you crack hashes, exploit weak implementations, and downgrade protocols? Every student will both protect and attack cryptographic systems.

Learning Objectives

1. Differentiate between symmetric and asymmetric encryption algorithms and their appropriate use cases
2. Explain PKI components: certificates, certificate authorities, CRLs, OCSP, and the chain of trust
3. Demonstrate hashing concepts including salting, key stretching, and digital signatures
4. Identify cryptographic attack techniques: birthday attacks, collision attacks, downgrade attacks
5. Use OpenSSL to generate certificates and inspect SSL/TLS configurations
6. Crack password hashes using Hashcat to understand why strong hashing matters
7. Explain blockchain fundamentals and their role in non-repudiation

Lecture Topics

- Cryptography Fundamentals:
  - Symmetric encryption: AES, DES, 3DES — shared secret, fast, used for data at rest/transit
  - Asymmetric encryption: RSA, ECC, Diffie-Hellman — key exchange, digital signatures, PKI
  - Key exchange: How Diffie-Hellman enables secure key sharing over insecure channels
  - Key length matters: AES-128 vs AES-256, RSA-2048 vs RSA-4096
- Encryption Levels and Applications:
  - Full-disk, partition, file, volume, database, record-level encryption
  - Transport encryption: TLS 1.3, IPSec, VPN tunnels
- Hashing and Integrity:
  - Hash functions: SHA-256, SHA-3, MD5 (broken), SHA-1 (deprecated)
  - Salting: preventing rainbow table attacks
  - Key stretching: PBKDF2, bcrypt, scrypt — slowing down brute force
  - Digital signatures: how they provide integrity + non-repudiation + authentication
- PKI Deep Dive:
  - Certificate Authorities (CAs): root CA, intermediate CA, chain of trust
  - Certificate lifecycle: CSR generation, issuance, revocation
  - CRL vs OCSP: checking certificate validity

  - Certificate types: wildcard, self-signed, third-party, root of trust
- Obfuscation Techniques:
  - Steganography: hiding data in images, audio, video
  - Tokenization: replacing sensitive data with tokens
  - Data masking: showing partial data (e.g., credit card ***1234)
- Cryptographic Tools:
  - TPM: hardware-based key storage
  - HSM: enterprise-grade cryptographic processing
  - Key management systems and secure enclaves
- Blockchain and Open Public Ledger: distributed trust without central authority
- Cryptographic Attacks (Offensive Perspective):
  - Birthday attack, collision attack, downgrade attack
  - Pass-the-hash, rainbow tables, brute force, dictionary attacks
  - Why MD5 and SHA-1 are dead (demonstrated collisions)

Official Sources

[OFFICIAL] CompTIA Security+ SY0-701 Certification Guide, 3rd Edition — Chapter on Cryptography

[OFFICIAL] NIST SP 800-175B — Guideline for Using Cryptographic Standards
https://csrc.nist.gov/publications/detail/sp/800-175b/rev-1/final

[OFFICIAL] NIST SP 800-57 Part 1 Rev. 5 — Recommendation for Key Management
https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

[OFFICIAL] OWASP Cryptographic Storage Cheat Sheet
https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html

[OFFICIAL] RFC 8446 — TLS 1.3 Specification
https://datatracker.ietf.org/doc/html/rfc8446

Underground / Bleeding Edge Sources

[UNDERGROUND] Computerphile (YouTube) — 'How AES Encryption Works' and 'Public Key Cryptography' videos

[UNDERGROUND] John Hammond — 'Cracking Passwords with Hashcat' tutorial

[UNDERGROUND] IppSec — 'HTB Walkthrough: Exploiting Weak Cryptography' video

[UNDERGROUND] r/netsec — 'The definitive guide to password hashing in 2025' thread

[UNDERGROUND] DEF CON 28 — 'Exploiting Crypto Bugs for Fun and Profit' talk

[UNDERGROUND] CrackStation.net — Rainbow table lookup service (educational resource)

CASE STUDY: Heartbleed (CVE-2014-0160) & The LastPass Breach (2022)

Heartbleed (CVE-2014-0160) was a catastrophic vulnerability in OpenSSL's implementation of the TLS heartbeat extension, disclosed in April 2014. The bug allowed attackers to read up to 64KB of server memory per request — potentially exposing private keys, user credentials, and session tokens. An estimated 17% of all SSL-enabled web servers (around 500,000) were affected at disclosure.

How the attack worked: The TLS heartbeat protocol sends a payload and expects the same data echoed back. The vulnerable code failed to validate the payload length field. An attacker could claim their payload was 64KB while sending only a tiny request, causing the server to read and return 64KB of adjacent memory — which could contain anything from private keys to user passwords.

What defenders did wrong: The vulnerability existed in OpenSSL for over two years before discovery. Many organizations were slow to patch even after disclosure. Some never revoked and reissued their SSL certificates after patching, meaning stolen private keys remained valid.

The LastPass Breach (2022): In August 2022, attackers compromised a LastPass developer's workstation, stealing source code and proprietary technical information. In November, they used this to target a LastPass engineer's home computer, exploiting a vulnerable Plex media server to install a keylogger. They captured the engineer's master password to access LastPass corporate vault backups. The stolen encrypted vaults were protected by customers' master passwords — but weak master passwords could be brute-forced offline.

Lessons learned: (1) Cryptographic implementations must be audited continuously — not just algorithms, but code. (2) Private keys must be rotated after any suspected compromise. (3) Password vaults are only as strong as the master password. (4) Defense in depth matters: the LastPass breach chained multiple compromises together. (5) From the attacker's perspective: patience and persistence in chaining small vulnerabilities leads to catastrophic access.

HANDS-ON LAB: Crack Hashes & Inspect Certificates

Objective

Use Hashcat to crack password hashes (understanding why weak hashing is dangerous) and OpenSSL to generate/inspect SSL certificates (understanding PKI from the inside).

Tools Required

Hashcat (pre-installed on Kali), OpenSSL (pre-installed on Kali), wordlist: rockyou.txt (included in Kali)

Step-by-Step Instructions

1. Open a terminal on your Kali VM
2. Create a test hash file: echo '5f4dcc3b5aa765d61d8327deb882cf99' > hashes.txt (this is MD5 of 'password')
3. Add more hashes: echo '482c811da5d5b4bc6d497ffa98491e38' >> hashes.txt (MD5 of 'password123')
4. Run Hashcat: hashcat -m 0 -a 0 hashes.txt /usr/share/wordlists/rockyou.txt
5. Observe: '-m 0' = MD5 mode, '-a 0' = dictionary attack. Watch the speed — millions of hashes per second
6. Now try SHA-256: echo -n 'letmein' | sha256sum, save the hash, crack with hashcat -m 1400
7. Create a self-signed certificate with OpenSSL:
8. openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem -days 365 -nodes
9. Inspect the certificate: openssl x509 -in cert.pem -text -noout
10. Examine a live website's certificate: openssl s_client -connect google.com:443 | openssl x509 -text -noout
11. Identify: issuer, subject, validity dates, signature algorithm, public key size
12. Compare: How does the self-signed cert differ from Google's CA-signed cert?
13. Generate a CSR: openssl req -new -key key.pem -out request.csr
14. Inspect the CSR: openssl req -in request.csr -text -noout

Expected Outcomes

Successfully cracked MD5 and SHA-256 hashes using dictionary attacks. Generated a self-signed certificate, inspected live website certificates, and understood the PKI chain of trust. Observed the dramatic speed

difference in cracking weak vs. strong hashes.

Purple Team Debrief

As an ATTACKER: you've seen how trivially weak hashes fall. MD5 cracks in seconds. This is why password databases are targeted. As a DEFENDER: you now understand why salting, key stretching (bcrypt), and strong algorithms matter. You've also seen PKI from the inside — understanding certificate validation helps you detect MitM attacks using fake certificates.

Key Terms & Definitions

Symmetric Encryption
Encryption using a single shared key for both encryption and decryption (e.g., AES, 3DES)

Asymmetric Encryption
Encryption using a key pair — public key encrypts, private key decrypts (e.g., RSA, ECC)

PKI
Public Key Infrastructure — the framework of policies, hardware, software, and procedures for managing digital certificates and encryption keys

Certificate Authority (CA)
A trusted entity that issues and manages digital certificates, verifying the identity of certificate holders

CRL
Certificate Revocation List — a list of certificates that have been revoked before their expiration date

OCSP
Online Certificate Status Protocol — a real-time method to check if a specific certificate has been revoked

Hashing
A one-way mathematical function that converts data into a fixed-length value (digest) that cannot be reversed

Salting
Adding a random value to data before hashing to prevent rainbow table attacks and ensure identical passwords produce different hashes

Key Stretching
A technique (PBKDF2, bcrypt, scrypt) that makes hash computation deliberately slow to resist brute-force attacks

Digital Signature
A cryptographic value that provides authentication, integrity, and non-repudiation by signing data with a private key

TPM
Trusted Platform Module — a hardware chip that securely stores cryptographic keys and performs encryption operations

HSM
Hardware Security Module — a dedicated physical device for managing and protecting cryptographic keys

Steganography
The practice of hiding secret data within ordinary, non-secret data (e.g., embedding text in image files)

Key Escrow
The arrangement where cryptographic keys are held in escrow by a third party for later retrieval

Birthday Attack

A cryptographic attack that exploits the mathematics of the birthday problem to find hash collisions faster than brute force

Rainbow Table

A precomputed table for reversing cryptographic hash functions, used for cracking password hashes

Blockchain

A distributed, immutable ledger technology that chains blocks of transactions together using cryptographic hashes

CSR

Certificate Signing Request — a message sent to a Certificate Authority to apply for a digital identity certificate

Practice Questions — Multiple Choice

Q1. A company needs to encrypt large volumes of data at rest with maximum performance. Which approach is MOST appropriate?

A. RSA-4096

B. AES-256

C. ECC P-384

D. Diffie-Hellman

Answer: B — AES-256 is a symmetric algorithm optimized for speed and is the standard for encrypting data at rest. Asymmetric algorithms (RSA, ECC, DH) are too slow for bulk data encryption.

Q2. An administrator discovers that a CA has been compromised. Which mechanism should be used to immediately invalidate all certificates issued by that CA?

A. Certificate Signing Request

B. Key escrow

C. Certificate Revocation List

D. OCSP stapling

Answer: C — A CRL lists all certificates revoked by a CA. When a CA is compromised, the CRL is updated to invalidate affected certificates. OCSP checks individual certificates but a CRL handles mass revocation.

Q3. A developer stores user passwords using MD5 without salting. Which attack would be MOST effective?

A. Brute force attack

B. Rainbow table attack

C. Birthday attack

D. Downgrade attack

Answer: B — Unsalted MD5 hashes are directly vulnerable to rainbow table attacks — precomputed tables that map hashes to plaintext. Salting would defeat rainbow tables by making each hash unique.

Q4. Which cryptographic concept ensures that a sender cannot deny having sent a message?

A. Confidentiality

B. Integrity

C. Non-repudiation

D. Availability

Answer: C — Non-repudiation ensures the sender cannot deny sending the message. Digital signatures provide non-repudiation by binding the sender's private key to the message.

Q5. An organization wants to protect credit card numbers in its database while still allowing the last four digits to be visible. Which technique is MOST appropriate?

A. Encryption

B. Hashing

C. Data masking

D. Steganography

Answer: C — Data masking replaces sensitive data with obfuscated values while preserving format (e.g., ****-****-****-1234). This allows partial visibility without exposing the full number.

Practice Questions — Performance-Based (PBQ)

PBQ1. SCENARIO: Your company's web server certificate is expiring in 7 days. Walk through the complete certificate renewal process, identifying each step and the PKI components involved. Include: CSR generation, CA interaction, certificate installation, and verification.

Answer: Step 1: Generate a new private key (if rotating) or reuse existing. Step 2: Create a CSR using OpenSSL: openssl req -new -key server.key -out server.csr. Step 3: Submit CSR to Certificate Authority (public CA like DigiCert, or internal CA). Step 4: CA validates domain ownership (DV) or organization identity (OV/EV). Step 5: CA signs the certificate with their private key and issues it. Step 6: Install the new certificate on the web server along with the intermediate CA chain. Step 7: Verify: openssl s_client -connect yoursite.com:443 — check chain of trust, expiration, and algorithm. Step 8: Test OCSP response and ensure old cert is not cached by clients.

PBQ2. SCENARIO: Match each cryptographic solution to its BEST use case: Solutions: AES-256, RSA-2048, SHA-256, bcrypt, Diffie-Hellman, Steganography Use Cases: (A) Encrypting a hard drive, (B) Establishing a shared secret over the internet, (C) Verifying file integrity, (D) Storing user passwords, (E) Signing a software update, (F) Hiding a message inside an image

Answer: AES-256 → (A) Encrypting a hard drive (symmetric, fast bulk encryption). RSA-2048 → (E) Signing a software update (asymmetric, digital signatures). SHA-256 → (C) Verifying file integrity (hashing produces fixed-length digest). bcrypt → (D) Storing user passwords (key stretching resists brute force). Diffie-Hellman → (B) Establishing a shared secret over the internet (key exchange protocol). Steganography → (F) Hiding a message inside an image (obfuscation technique).

WEEKLY CHALLENGE

Create a 'Crypto Attack Cheat Sheet' documenting at least 8 cryptographic attacks (birthday, collision, downgrade, brute force, dictionary, rainbow table, pass-the-hash, replay). For each, explain: how it works, what it targets, real-world example, and the defensive countermeasure. Then use CyberChef (https://gchq.github.io/CyberChef/) to encode a secret message using at least 3 different methods (Base64, XOR, AES) and share the recipe with a classmate to decode.

WEEK 3

Threat Actors, Vectors & Social Engineering

SY0-701 Objectives: 2.1: Compare and contrast common threat actors and motivations | 2.2: Explain common threat vectors and attack surfaces

PURPLE TEAM FRAMING

Social engineering is the most exploited attack vector because it targets the weakest link — humans. This week, students learn to think like a social engineer (crafting pretexts, identifying targets via OSINT) and simultaneously build defenses (awareness training, email filtering, reporting procedures). Understanding how threat actors operate and their motivations is essential for predicting and preventing attacks.

Learning Objectives

1. Categorize threat actors by type (nation-state, organized crime, hacktivist, insider, unskilled attacker, shadow IT) and their motivations
2. Identify and explain common threat vectors: message-based, file-based, supply chain, human vectors
3. Demonstrate OSINT reconnaissance techniques using free tools
4. Analyze social engineering tactics: phishing, vishing, smishing, pretexting, watering hole, BEC
5. Explain supply chain attack vectors including MSP, vendor, and supplier risks
6. Craft and identify phishing emails in a controlled lab environment

Lecture Topics

- Threat Actor Classification:
  - Nation-state: APT groups (APT28/Fancy Bear, APT29/Cozy Bear, Lazarus Group), motivations (espionage, war, disruption)
  - Organized crime: Ransomware gangs (LockBit, BlackCat/ALPHV, Cl0p), financial motivation
  - Hacktivists: Anonymous, political/philosophical motivations
  - Insider threats: malicious insiders, negligent employees, shadow IT risks
  - Unskilled attackers: script kiddies, purchased exploit kits
  - Actor attributes: internal/external, resources/funding, sophistication level
- Threat Vectors and Attack Surfaces:
  - Message-based: email phishing, SMS (smishing), instant messaging
  - Image-based and file-based vectors
  - Voice calls (vishing)
  - Removable devices (USB drop attacks)
  - Vulnerable software: client-based vs agentless
  - Unsupported systems and unsecure networks (wireless, wired, Bluetooth)
  - Open service ports and default credentials

  - Supply chain vectors: MSPs, vendors, suppliers
- Social Engineering Deep Dive:
  - Phishing: spear phishing, whaling, clone phishing
  - Vishing and smishing campaigns
  - Pretexting: building a false narrative
  - Business Email Compromise (BEC): CEO fraud, invoice fraud
  - Watering hole attacks: compromising trusted websites
  - Brand impersonation and typosquatting
  - Misinformation and disinformation campaigns
- OSINT Reconnaissance:
  - Passive recon: Google dorking, WHOIS, DNS enumeration, social media analysis
  - Tools: Maltego CE, theHarvester, Shodan, Recon-ng
  - OSINT frameworks: what data is publicly available about your organization?
- MITRE ATT&CK Framework Introduction:
  - Initial Access techniques mapping
  - Tactic-Technique-Procedure (TTP) model

Official Sources

[OFFICIAL] MITRE ATT&CK Framework — Initial Access Tactics
https://attack.mitre.org/tactics/TA0001/

[OFFICIAL] CISA — Understanding and Responding to Social Engineering
https://www.cisa.gov/topics/cybersecurity-best-practices/phishing-and-social-engineering

[OFFICIAL] NIST SP 800-63B — Digital Identity Guidelines
https://pages.nist.gov/800-63-3/sp800-63b.html

[OFFICIAL] SANS Reading Room — 'Social Engineering: Attacking the Weakest Link'
https://www.sans.org/white-papers/social-engineering/

[OFFICIAL] FBI IC3 — Internet Crime Report (BEC statistics)
https://www.ic3.gov/

Underground / Bleeding Edge Sources

[UNDERGROUND] TheCyberMentor — 'OSINT in 5 Hours' full course (free on YouTube)

[UNDERGROUND] NetworkChuck — 'Ethical Hacking: Social Engineering' video

[UNDERGROUND] r/OSINT — 'Best free OSINT tools for beginners' pinned thread

[UNDERGROUND] DEF CON Social Engineering Village — Annual social engineering CTF talks

[UNDERGROUND] John Hammond — 'Phishing Analysis: How to Identify Malicious Emails' video

[UNDERGROUND] r/netsec — 'MGM hack: How Scattered Spider used a phone call' analysis thread

CASE STUDY: The MGM Resorts Hack (2023) — Scattered Spider's Phone Call That Cost $100M

In September 2023, the Scattered Spider threat group (also known as UNC3944/0ktapus) brought MGM Resorts International to its knees with a social engineering attack that began with a single phone call. The group identified an MGM employee on LinkedIn, called the MGM IT help desk, impersonated that employee, and convinced the help desk to reset the employee's MFA credentials. Total call time: approximately 10 minutes.

With those credentials, Scattered Spider gained access to MGM's Okta identity platform and then pivoted to the Azure cloud environment. They deployed the ALPHV/BlackCat ransomware across MGM systems, encrypting critical infrastructure. The result: slot machines went dark, hotel room keys stopped working, check-in systems failed, and the MGM website went offline. The estimated financial impact exceeded $100 million.

For contrast, consider the Twitter hack of July 2020. A 17-year-old from Florida and two accomplices used phone-based social engineering to target Twitter employees, gaining access to internal admin tools. They hijacked high-profile accounts (Barack Obama, Elon Musk, Apple) to promote a Bitcoin scam that netted approximately $120,000. While the financial damage was small, the reputational damage and the demonstration of insider tool access was massive.

What the attackers did right: Scattered Spider invested in OSINT reconnaissance to identify employees and organizational structure. They exploited the human element — help desk procedures that prioritized customer service over security verification. They moved quickly from initial access to ransomware deployment.

What defenders did wrong: MGM's help desk lacked robust identity verification procedures for MFA resets. There was insufficient monitoring of admin-level credential changes. Network segmentation between IT management systems and operational technology was inadequate.

Lessons learned: Help desk social engineering is a critical attack vector that technical controls alone cannot address. Identity verification procedures must be rigorous, especially for privileged operations like MFA resets. OSINT awareness is essential — if attackers can find your employees on LinkedIn, they can impersonate them. Purple team exercises should include social engineering simulations.

HANDS-ON LAB: OSINT Reconnaissance & Phishing Analysis

Objective

Conduct OSINT reconnaissance on a target organization (use your own or a designated practice target) and analyze real phishing emails to identify indicators of social engineering.

Tools Required

theHarvester (pre-installed on Kali), Maltego CE (free), Shodan (free account), Google Dorking

Step-by-Step Instructions

PART A — OSINT Reconnaissance:

2. Choose a target (your own organization or use 'megacorpone.com' — a legal practice target)
3. Run theHarvester: theHarvester -d megacorpone.com -b google,bing,linkedin -l 200
4. Document findings: email addresses, subdomains, employee names discovered
5. Use Google Dorking: site:megacorpone.com filetype:pdf (look for exposed documents)
6. Search Shodan: shodan search hostname:megacorpone.com (identify exposed services)
7. Open Maltego CE: create a new graph, add domain entity, run transforms to map relationships
8. Compile an OSINT report: what could an attacker learn before ever touching the target's systems?

PART B — Phishing Analysis:

10. Download sample phishing emails from PhishTank (https://phishtank.org/)
11. For each sample, identify: sender spoofing, urgency tactics, malicious links, attachment types

12. Check email headers for: SPF/DKIM/DMARC results, originating IP, relay path
13. Use VirusTotal (https://www.virustotal.com/) to check any URLs or file hashes found
14. Create a phishing identification checklist based on your analysis

PART C — Craft a Controlled Phishing Email:

16. Write a phishing email targeting a fictional company (DO NOT SEND — analysis only)
17. Apply social engineering principles: authority, urgency, social proof, familiarity
18. Have a classmate review it: could they identify it as phishing? What gave it away?

Expected Outcomes

A comprehensive OSINT report demonstrating passive reconnaissance capabilities. A phishing analysis showing ability to identify social engineering indicators. Understanding of how easily public information can be weaponized.

Purple Team Debrief

As an ATTACKER: OSINT is free and devastating. You found email formats, employee names, technologies in use — all without triggering a single alert. As a DEFENDER: review what your organization exposes publicly. Implement email authentication (SPF, DKIM, DMARC). Train employees to verify identity through out-of-band channels before processing sensitive requests.

Key Terms & Definitions

APT
Advanced Persistent Threat — a prolonged and targeted cyberattack by a well-funded threat actor (typically nation-state) that remains undetected for extended periods

Social Engineering
The psychological manipulation of people into performing actions or divulging confidential information

Phishing
A fraudulent attempt to obtain sensitive information by disguising as a trustworthy entity in electronic communication

Spear Phishing
Targeted phishing aimed at a specific individual or organization using personalized information

Vishing
Voice phishing — social engineering conducted over phone calls

Smishing
SMS phishing — social engineering via text messages

BEC
Business Email Compromise — a scam where attackers impersonate executives or business partners to trick employees into transferring money or data

Pretexting
Creating a fabricated scenario (pretext) to engage a victim and gain their trust for information extraction

Watering Hole Attack
Compromising a website frequently visited by the target group to infect their systems

Typosquatting

Registering domains that are common misspellings of popular websites to capture misdirected traffic

OSINT

Open Source Intelligence — collecting information from publicly available sources for intelligence purposes

Shadow IT

Technology systems and solutions used within an organization without explicit IT department approval

Insider Threat

A security risk that originates from within the targeted organization, typically current or former employees

Supply Chain Attack

Compromising a target by attacking less-secure elements in their supply chain (vendors, MSPs, software providers)

Threat Vector

The path or means by which an attacker gains access to a target system

Attack Surface

The total number of possible entry points for unauthorized access into any system

MITRE ATT&CK

A globally-accessible knowledge base of adversary tactics and techniques based on real-world observations

Practice Questions — Multiple Choice

Q1. A well-funded group conducts a targeted attack against a government agency over several months, remaining undetected while exfiltrating classified data. This threat actor is BEST classified as:

A. Hacktivist

B. Insider threat

C. Nation-state

D. Organized crime

Answer: C — Nation-state actors are well-funded, target government/critical infrastructure, conduct prolonged campaigns (APTs), and focus on espionage/data exfiltration.

Q2. An attacker registers the domain 'arnazon.com' to capture traffic from users who mistype 'amazon.com'. This is an example of:

A. Watering hole attack

B. Brand impersonation

C. Typosquatting

D. DNS poisoning

Answer: C — Typosquatting exploits common typing errors by registering similar-looking domain names to redirect users to malicious sites.

Q3. An employee receives a phone call from someone claiming to be from the IT department, asking for their password to 'fix a system issue.' This is an example of:

A. Phishing

B. Vishing

C. Smishing

D. Tailgating

Answer: B — Vishing (voice phishing) uses phone calls to manipulate victims into revealing sensitive information.

Q4. Which threat actor motivation is MOST commonly associated with organized crime groups?

A. Espionage

B. Philosophical beliefs

C. Financial gain

D. Disruption/chaos

Answer: C — Organized crime groups are primarily motivated by financial gain through ransomware, fraud, data theft, and other monetizable attacks.

Q5. A company discovers that employees have been using an unapproved cloud storage service to share files. This is an example of:

A. Data exfiltration

B. Insider threat

C. Shadow IT

D. Supply chain attack

Answer: C — Shadow IT refers to technology used within an organization without IT department knowledge or approval, creating unmanaged security risks.

Practice Questions — Performance-Based (PBQ)

PBQ1. SCENARIO: You are a security analyst who receives a suspicious email forwarded by an employee. The email claims to be from the CFO, requesting an urgent wire transfer to a new vendor. Analyze this email and identify all social engineering techniques used. Determine if this is a legitimate request or BEC attack. Describe your investigation steps.

Answer: Investigation: (1) Check sender address carefully — is it the CFO's actual email or a spoofed/similar domain? (2) Examine email headers for SPF/DKIM/DMARC failures. (3) Look for urgency tactics ('must be done today'), authority exploitation ('direct from CFO'), and bypass of normal procedures ('skip the usual approval'). (4) Verify through out-of-band channel — call the CFO directly on their known phone number. (5) Check if the vendor is in the approved vendor list. (6) Review email for grammatical/formatting inconsistencies. Red flags: unusual urgency, new/unknown vendor, request to bypass procedures, reply-to address different from sender. This is a classic BEC attack using authority and urgency.

PBQ2. SCENARIO: Map the following threat actors to their MOST LIKELY motivation, typical sophistication level, and a known real-world example: (1) Lazarus Group, (2) LockBit, (3) Anonymous, (4) A disgruntled former employee, (5) A teenager using Metasploit

Answer: (1) Lazarus Group: Nation-state (North Korea), high sophistication, motivated by financial gain and espionage. Example: Bangladesh Bank SWIFT heist ($81M). (2) LockBit: Organized crime, high sophistication, financially motivated. Example: LockBit ransomware-as-a-service affecting thousands of organizations. (3) Anonymous: Hacktivist, moderate sophistication, motivated by philosophical/political beliefs. Example: DDoS attacks against governments during the Arab Spring. (4) Disgruntled employee: Insider threat, variable sophistication, motivated by revenge. Example: Internal sabotage, data theft before departure. (5) Teenager: Unskilled attacker (script kiddie), low sophistication, motivated by curiosity/disruption. Example: Using pre-built tools without understanding the underlying exploits.

WEEKLY CHALLENGE

Conduct a full OSINT assessment of yourself (or a willing friend/colleague). Document everything publicly discoverable: social media profiles, email addresses, phone numbers, workplace info, photos with metadata, forum posts. Create a 'Personal Attack Surface Report' with recommendations for reducing your digital footprint. This is a real-world skill both attackers and defenders need.

WEEK 4

Vulnerabilities & Malware Deep Dive

SY0-701 Objectives: 2.3: Explain various types of vulnerabilities | 2.4: Given a scenario, analyze indicators of malicious activity

PURPLE TEAM FRAMING

Vulnerabilities are the battlefield where attackers and defenders clash daily. This week, we dissect vulnerabilities from both sides: attackers learn to find and exploit them, defenders learn to detect, prioritize, and patch them. We perform live malware analysis in sandboxes — studying the enemy's weapons to build better shields. Every ransomware sample we examine teaches us both how attacks succeed and how detection fails.

Learning Objectives

1. Classify vulnerability types: application, OS, web, hardware, virtualization, cloud, supply chain, cryptographic, mobile, zero-day
2. Identify and describe major malware categories: ransomware, trojans, worms, spyware, rootkits, logic bombs, keyloggers
3. Analyze indicators of malicious activity including network attacks, application attacks, and cryptographic attacks
4. Navigate the CVE/CVSS system to assess and prioritize vulnerabilities
5. Perform basic malware analysis in a sandboxed environment
6. Use vulnerability scanning tools (Nmap, Nessus Essentials) to identify system weaknesses

Lecture Topics

- Vulnerability Taxonomy:
  - Application vulnerabilities: memory injection, buffer overflow, race conditions (TOC/TOU), malicious updates
  - OS-based vulnerabilities: privilege escalation, kernel exploits
  - Web vulnerabilities: SQLi, XSS (stored, reflected, DOM-based)
  - Hardware: firmware vulnerabilities, end-of-life, legacy systems
  - Virtualization: VM escape, resource reuse attacks
  - Cloud-specific: misconfiguration, insecure APIs, shared responsibility gaps
  - Supply chain: software/hardware/service provider compromises
  - Cryptographic: weak algorithms, implementation flaws
  - Mobile: side-loading, jailbreaking risks
  - Zero-day: the unknown unknowns
- Malware Classification:
  - Ransomware: encryption, double extortion (Akira, Qilin, LockBit, BlackCat families)
  - Trojans: RATs, banking trojans, dropper trojans
  - Worms: self-propagating, network worms

  - Spyware and keyloggers: data exfiltration tools
  - Rootkits: kernel-level persistence
  - Logic bombs: time/event-triggered payloads
  - Viruses: file infectors, boot sector, polymorphic, metamorphic
  - Bloatware: PUPs and their security implications
- Indicators of Malicious Activity:
  - Network attacks: DDoS (amplified, reflected), DNS attacks, wireless attacks, on-path attacks, credential replay
  - Application attacks: injection, buffer overflow, replay, privilege escalation, forgery, directory traversal
  - Cryptographic attacks: downgrade, collision, birthday
  - Password attacks: spraying, brute force
  - Physical attacks: brute force entry, RFID cloning, environmental
  - Indicators: account lockout, concurrent sessions, impossible travel, resource consumption, missing logs
- CVE/CVSS System:
  - CVE numbering and database navigation
  - CVSS scoring: base, temporal, environmental metrics
  - Prioritizing vulnerabilities by CVSS score and business context

Official Sources

[OFFICIAL] MITRE CVE Database
https://cve.mitre.org/

[OFFICIAL] NIST National Vulnerability Database (NVD)
https://nvd.nist.gov/

[OFFICIAL] OWASP Top 10 Web Application Security Risks
https://owasp.org/www-project-top-ten/

[OFFICIAL] CISA Known Exploited Vulnerabilities Catalog
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[OFFICIAL] MITRE ATT&CK — Malware Techniques
https://attack.mitre.org/software/

Underground / Bleeding Edge Sources

[UNDERGROUND] John Hammond — 'Malware Analysis for Beginners' series (YouTube)

[UNDERGROUND] IppSec — Hack The Box walkthroughs demonstrating vulnerability exploitation

[UNDERGROUND] r/malwareanalysis — community-sourced malware samples and analysis writeups

[UNDERGROUND] Exploit-DB (https://exploit-db.com) — public exploit database

[UNDERGROUND] DEF CON 31 — 'Ransomware: Behind the Curtain' talk on ransomware gang operations

[UNDERGROUND] Marcus Hutchins (MalwareTech) blog — WannaCry kill switch discovery and analysis

CASE STUDY: WannaCry, NotPetya & The MOVEit Catastrophe

WannaCry (May 2017): The WannaCry ransomware worm exploited EternalBlue (CVE-2017-0144), an SMBv1 vulnerability in Windows allegedly developed by the NSA and leaked by the Shadow Brokers group. In a single day, it infected over 230,000 computers across 150 countries. The UK's National Health Service was devastated — hospitals turned away patients, surgeries were cancelled, and ambulances were diverted. Microsoft had released a patch (MS17-010) two months prior, but many organizations had not applied it.

The kill switch: Security researcher Marcus Hutchins (MalwareTech) discovered that WannaCry checked if a specific domain was registered before executing. By registering that domain for $10.69, he accidentally activated a kill switch that stopped the global spread. This saved countless organizations but highlighted how close we came to far worse damage.

NotPetya (June 2017): Just weeks after WannaCry, NotPetya appeared, also using EternalBlue. But NotPetya was not ransomware — it was a Russian cyberweapon disguised as ransomware, targeting Ukraine through a compromised update mechanism for M.E.Doc (Ukrainian tax software). NotPetya's encryption was irreversible by design; paying the ransom was pointless. Total global damages exceeded $10 billion. Maersk lost its entire IT infrastructure and rebuilt 45,000 PCs and 4,000 servers in just 10 days. Merck, FedEx, and Mondelez suffered billions in losses.

MOVEit (2023): The Cl0p ransomware gang exploited a zero-day SQL injection vulnerability (CVE-2023-34362) in Progress Software's MOVEit Transfer file-sharing platform. Unlike traditional ransomware, Cl0p didn't encrypt files — they exfiltrated data and threatened to publish it. Over 2,600 organizations and 77 million individuals were affected, including Shell, British Airways, the BBC, and numerous U.S. government agencies.

Lessons learned: (1) Patching is not optional — WannaCry exploited a vulnerability patched months earlier. (2) Supply chain attacks (NotPetya via M.E.Doc, MOVEit as a shared service) multiply impact exponentially. (3) Attribution matters — NotPetya masquerading as ransomware hid its true destructive purpose. (4) Zero-day vulnerabilities in widely-used file transfer tools are gold for attackers. (5) Defenders must monitor for indicators of compromise beyond just encryption behavior.

HANDS-ON LAB: Malware Analysis & Vulnerability Scanning

Objective

Analyze malware samples in a sandbox environment and scan for vulnerabilities using industry-standard tools.

Tools Required

Any.Run (free tier), Nmap (pre-installed on Kali), Nessus Essentials (free), VirusTotal

Step-by-Step Instructions

PART A — Malware Analysis:

2. Create a free account at https://any.run/

3. Browse the public submissions to find recent malware samples (DO NOT download to your host)

4. Select a ransomware sample and observe the sandbox analysis: process tree, network connections, file system changes, registry modifications

5. Document the malware's behavior: What files does it create? What network connections does it make? What processes does it spawn?

6. Use VirusTotal (https://www.virustotal.com/) to look up the sample hash — how many AV engines detect it?

7. Identify MITRE ATT&CK techniques used by the malware

PART B — Vulnerability Scanning:

9. On your Kali VM, run a comprehensive Nmap scan against your Ubuntu target:

10. nmap -sV -sC -O -A [target-IP] -oN full_scan.txt

11. Analyze results: open ports, service versions, OS detection, script results

12. Install Nessus Essentials on Kali (free for up to 16 IPs): https://www.tenable.com/products/nessus/nessus-essentials
13. Run a basic vulnerability scan against your Ubuntu target VM
14. Review Nessus results: identify vulnerabilities by CVSS score, categorize by severity
15. For the highest-severity finding, look up the CVE in NVD (https://nvd.nist.gov/) — what's the attack vector?
16. Create a vulnerability report: prioritize findings and recommend remediation steps

Expected Outcomes

Analyzed real malware behavior in a sandbox without risk. Identified malware techniques mapped to MITRE ATT&CK. Performed vulnerability scanning and created a prioritized remediation report.

Purple Team Debrief

As an ATTACKER: you've seen how malware operates and evades detection. You understand what vulnerability scanners miss (zero-days, logic flaws). As a DEFENDER: you've used the same tools SOC analysts use daily. You know how to prioritize vulnerabilities by real risk, not just CVSS score. The sandbox analysis teaches you what to look for in endpoint detection alerts.

Key Terms & Definitions

Zero-Day
A vulnerability unknown to the vendor with no available patch, actively exploited by attackers

CVE
Common Vulnerabilities and Exposures — a standardized system for identifying and naming vulnerabilities

CVSS
Common Vulnerability Scoring System — a framework for rating the severity of vulnerabilities on a 0-10 scale

Buffer Overflow
A vulnerability where a program writes data beyond the allocated memory buffer, potentially allowing code execution

SQL Injection
An attack that inserts malicious SQL code into application queries to manipulate or extract database data

XSS
Cross-Site Scripting — injecting malicious scripts into web pages viewed by other users

Ransomware
Malware that encrypts victim data and demands payment for the decryption key

Rootkit
Malware that provides continued privileged access while hiding its presence from detection tools

Trojan
Malware disguised as legitimate software that performs malicious actions once executed

Worm
Self-replicating malware that spreads across networks without user interaction

Logic Bomb
Malicious code that triggers when specific conditions are met (date, event, action)

VM Escape

An exploit that allows code running inside a virtual machine to break out and interact with the host operating system

DDoS

Distributed Denial of Service — overwhelming a target with traffic from multiple sources to make it unavailable

Race Condition

A vulnerability where system behavior depends on the timing of events, creating exploitable windows (TOC/TOU)

Indicator of Compromise (IoC)

Evidence that a security breach has occurred — file hashes, IP addresses, domain names, behavioral patterns

EternalBlue

An SMBv1 exploit (CVE-2017-0144) allegedly developed by the NSA, used in WannaCry and NotPetya attacks

Practice Questions — Multiple Choice

Q1. A security analyst observes that a user account has logged in from New York and Tokyo within a 30-minute window. This is an indicator of:

A. Concurrent session usage

B. Impossible travel

C. Resource consumption anomaly

D. Out-of-cycle logging

Answer: B — Impossible travel occurs when a user appears to log in from geographically distant locations within a time frame that makes physical travel impossible.

Q2. An attacker exploits a web application by inserting ' OR 1=1 -- into a login form. This is an example of:

A. Cross-site scripting

B. Buffer overflow

C. SQL injection

D. Directory traversal

Answer: C — SQL injection manipulates database queries by inserting SQL code. ' OR 1=1 -- is a classic SQLi payload that bypasses authentication by making the WHERE clause always true.

Q3. Malware that encrypts files and demands Bitcoin payment, while also threatening to publish stolen data, is BEST described as:

A. Ransomware with single extortion

B. Ransomware with double extortion

C. A wiper disguised as ransomware

D. Spyware with ransomware capabilities

Answer: B — Double extortion ransomware both encrypts data (demanding payment for decryption) and exfiltrates data (threatening to publish it), creating two leverage points.

Q4. A vulnerability exists in a widely-used library, but the vendor is unaware and no patch exists. This is classified as:

A. Known vulnerability

B. Zero-day vulnerability

C. Misconfiguration

D. Legacy vulnerability

Answer: B — A zero-day vulnerability is one that is unknown to the vendor with no available patch. It may or may not be actively exploited.

Q5. An attacker forces a TLS connection to downgrade from TLS 1.3 to TLS 1.0 to exploit known weaknesses. This is a:

A. Birthday attack

B. Collision attack

C. Downgrade attack

D. Replay attack

Answer: C — A downgrade attack forces the use of a weaker protocol version that has known vulnerabilities, allowing the attacker to exploit those weaknesses.

Practice Questions — Performance-Based (PBQ)

PBQ1. SCENARIO: Your SIEM alerts show the following indicators on a workstation: (1) Unusual outbound traffic to a known C2 IP on port 443, (2) Multiple failed login attempts to domain controller, (3) New scheduled task created at 3 AM, (4) Large volume of files being renamed with .encrypted extension. Analyze these indicators, identify the likely attack stage, and recommend immediate response actions.

Answer: Analysis: This indicates an active ransomware infection in the lateral movement and encryption phases. (1) C2 traffic confirms malware communication with attacker infrastructure. (2) Failed DC logins suggest attempted privilege escalation/lateral movement. (3) Scheduled task indicates persistence mechanism. (4) File renaming with .encrypted extension confirms ransomware execution. Immediate actions: (1) Isolate the affected workstation from the network immediately. (2) Block the C2 IP at the firewall. (3) Disable the compromised user account. (4) Check other workstations for the same IoCs. (5) Preserve forensic evidence before remediation. (6) Activate incident response plan. (7) Check backups for integrity — do NOT connect backup systems to the network.

PBQ2. SCENARIO: Match each malware type to its PRIMARY behavior and one real-world example: Malware types: Ransomware, Worm, Rootkit, Trojan, Logic Bomb, Keylogger Provide: behavior description, propagation method, detection difficulty (1-5), and a real example.

Answer: Ransomware: Encrypts files, demands payment. Propagates via phishing/exploits. Detection: 3/5 (behavioral detection possible). Example: LockBit 3.0. Worm: Self-replicates across networks. Propagates automatically via network vulnerabilities. Detection: 2/5 (network anomalies visible). Example: WannaCry. Rootkit: Hides in OS kernel, provides persistent hidden access. Propagates via initial exploit then installs. Detection: 5/5 (extremely difficult, modifies OS). Example: Necurs rootkit. Trojan: Disguises as legitimate software. Propagates via social engineering/downloads. Detection: 3/5 (behavioral analysis). Example: Emotet. Logic Bomb: Triggers on specific condition/date. Pre-planted by insider or via prior access. Detection: 4/5 (dormant until triggered). Example: South Korean banking logic bomb (2013). Keylogger: Records keystrokes. Propagates via phishing or physical access. Detection: 3/5 (behavior/process monitoring). Example: Olympic Vision keylogger targeting BEC.

WEEKLY CHALLENGE

Set up DVWA (Damn Vulnerable Web Application) on your Ubuntu target VM using Docker: 'docker run --rm -it -p 80:80 vulnerables/web-dvwa'. Then attempt to find and document at least 3 different vulnerability types (SQLi, XSS, command injection, file upload, etc.). For each vulnerability: document how you found it, how you exploited it, what the impact could be in a real environment, and how a developer should fix it. Screenshot your work.

WEEK 5

Attacks, Mitigations & Hardening

SY0-701 Objectives: 2.4: Given a scenario, analyze indicators of malicious activity (continued — network/application/cryptographic/password attacks) | 2.5: Explain the purpose of mitigation techniques used to secure the enterprise

PURPLE TEAM FRAMING

This week is where offense meets defense head-on. We launch real attacks against DVWA and then immediately pivot to implementing the defenses that would stop those attacks. Every exploit demonstrates a defensive failure; every mitigation technique is tested against a real attack. Students experience the full attack-defend cycle in a single lab session, building intuition for how both sides operate.

Learning Objectives

1. Demonstrate common network and application attacks: SQL injection, XSS, DDoS, password attacks in a controlled environment
2. Explain and apply mitigation techniques: segmentation, ACLs, allow lists, isolation, patching, encryption, monitoring
3. Apply system hardening techniques using CIS Benchmarks
4. Configure host-based firewalls and endpoint protection
5. Understand the principle of least privilege and its implementation across systems
6. Develop a hardening checklist for Linux and Windows systems

Lecture Topics

- Attack Demonstrations and Analysis:
  - SQL Injection: UNION-based, blind, error-based — from input to database compromise
  - Cross-Site Scripting: stored, reflected, DOM-based — session hijacking, cookie theft
  - DDoS attacks: volumetric, protocol, application layer — amplification and reflection
  - Password attacks: spraying, brute force, credential stuffing
  - DNS attacks: poisoning, tunneling, zone transfer exploitation
  - On-path (man-in-the-middle) attacks: ARP spoofing, SSL stripping
  - Wireless attacks: evil twin, deauthentication, WPA cracking
  - Replay attacks and credential replay
  - Privilege escalation: horizontal and vertical
  - Directory traversal: accessing files outside intended directories
- Mitigation Techniques Deep Dive:
  - Network segmentation: VLANs, subnets, microsegmentation
  - Access control: ACLs, permissions, role-based access
  - Application allow listing: only approved software runs
  - Isolation: sandboxing, air-gapping, network isolation

  - Patching: patch management programs, testing, deployment
  - Encryption: data at rest, in transit, in use
  - Monitoring: continuous monitoring, alerting, SIEM integration
  - Least privilege: minimum necessary access for each role
  - Configuration enforcement: Group Policy, MDM, SCAP
  - Decommissioning: secure disposal of old systems
- Hardening Techniques:
  - Endpoint protection installation and configuration
  - Host-based firewalls: iptables, Windows Firewall
  - Host-based IPS (HIPS)
  - Disabling unnecessary ports/protocols/services
  - Changing default passwords and credentials
  - Removing unnecessary software
  - CIS Benchmarks: automated hardening assessment
- Defense in Depth Architecture:
  - Layering controls across network, host, application, and data layers
  - Why single points of failure are unacceptable

Official Sources

[OFFICIAL] CIS Benchmarks (free PDF downloads)
https://www.cisecurity.org/cis-benchmarks

[OFFICIAL] OWASP Testing Guide
https://owasp.org/www-project-web-security-testing-guide/

[OFFICIAL] NIST SP 800-123 — Guide to General Server Security
https://csrc.nist.gov/publications/detail/sp/800-123/final

[OFFICIAL] CISA — Best Practices for Securing Your Enterprise
https://www.cisa.gov/cybersecurity-best-practices

[OFFICIAL] SANS — CIS Critical Security Controls
https://www.sans.org/critical-security-controls/

Underground / Bleeding Edge Sources

[UNDERGROUND] IppSec — Hack The Box walkthroughs demonstrating SQL injection and privilege escalation chains

[UNDERGROUND] TheCyberMentor — 'Web Application Penetration Testing' full course (free on YouTube)

[UNDERGROUND] NetworkChuck — 'Linux Hardening in 10 Minutes' video

[UNDERGROUND] r/netsec — 'DDoS mitigation strategies that actually work' discussion

[UNDERGROUND] DEF CON 30 — 'Breaking and Fixing Web Applications Live' talk

[UNDERGROUND] Exploit-DB — searchable database of public exploits for educational analysis

CASE STUDY: Equifax (2017), Capital One (2019) & Log4Shell (2021)

Equifax (2017): One of the largest data breaches in history exposed personal information of 147 million Americans. The root cause was a known Apache Struts vulnerability (CVE-2017-5638) that had been patched two months before the breach. Equifax failed to apply the patch to a public-facing web application. Attackers exploited the vulnerability to gain initial access, then moved laterally through the

network for 76 days undetected, exfiltrating Social Security numbers, birth dates, addresses, and driver's license numbers.

What went wrong: (1) Patch management failure — the vulnerability was known and patched, but not applied. (2) No network segmentation — attackers moved freely between systems. (3) Expired SSL certificates on security monitoring tools — making the IDS blind to encrypted traffic. (4) Inadequate monitoring — 76 days of undetected data exfiltration.

Capital One (2019): A former AWS employee, Paige Thompson, exploited a Server-Side Request Forgery (SSRF) vulnerability in Capital One's web application firewall (WAF) to access AWS metadata services. She obtained IAM role credentials, which allowed access to S3 buckets containing 100+ million customer records. The breach demonstrated that cloud misconfigurations can be as devastating as traditional vulnerabilities.

Log4Shell (CVE-2021-44228): Discovered in December 2021, this critical vulnerability in Apache Log4j (a ubiquitous Java logging library) allowed Remote Code Execution (RCE) by simply sending a specially crafted string that the library would interpret and execute. The CVSS score was 10.0 — maximum severity. Because Log4j was embedded in thousands of applications and services, the attack surface was enormous. Organizations scrambled for weeks to identify all affected systems.

Lessons learned: (1) Patch management is not glamorous but it's the #1 defense against known vulnerabilities. (2) Network segmentation limits blast radius — Equifax's flat network let attackers roam freely. (3) Cloud security requires understanding the shared responsibility model — Capital One's WAF misconfiguration was their responsibility, not AWS's. (4) Software supply chain awareness is critical — most organizations didn't even know they were running Log4j. (5) Defense in depth: no single control would have prevented all three, but layered controls dramatically reduce risk.

HANDS-ON LAB: Attack DVWA & Harden Linux

Objective

Exploit vulnerabilities in DVWA using Burp Suite Community, then apply CIS-aligned hardening to your Linux target to prevent those same attacks.

Tools Required

DVWA (Docker), Burp Suite Community (free, pre-installed on Kali), CIS Benchmark PDFs (free)

Step-by-Step Instructions

PART A — Web Application Attacks:

2. Start DVWA on your target VM: docker run --rm -it -p 80:80 vulnerables/web-dvwa
3. Access DVWA in Kali browser: http://[target-IP]/. Default creds: admin/password. Set security to 'Low'
4. Configure Burp Suite as browser proxy (127.0.0.1:8080) — intercept traffic
5. SQL Injection: Navigate to SQLi page. Enter: 1' OR '1'='1 in the User ID field. Observe the full user table returned
6. Advance: use UNION-based injection to enumerate database tables and columns
7. XSS (Reflected): Navigate to XSS Reflected page. Enter: <script>alert('XSS')</script>. Observe script execution
8. XSS (Stored): Navigate to XSS Stored. Post a comment with JavaScript payload — it persists and executes for all visitors

9. Command Injection: Navigate to Command Injection. Enter: 127.0.0.1; cat /etc/passwd. Observe OS command execution

10. Document each vulnerability: what you did, what happened, and the potential real-world impact

PART B — System Hardening:

12. On your Ubuntu target VM, apply the following hardening steps:

13. Disable unnecessary services: sudo systemctl disable [service] for any non-essential services

14. Configure UFW firewall: sudo ufw default deny incoming && sudo ufw allow ssh && sudo ufw enable

15. Set password policy: install libpam-pwquality, configure /etc/security/pwquality.conf (minlen=12, dcredit=-1, ucredit=-1)

16. Disable root SSH login: edit /etc/ssh/sshd_config, set PermitRootLogin no

17. Enable automatic security updates: sudo apt install unattended-upgrades

18. Remove unnecessary packages: sudo apt autoremove

19. Verify hardening: re-scan with Nmap from Kali — compare results to pre-hardening scan

Expected Outcomes

Successfully exploited SQLi, XSS, and command injection in DVWA. Applied Linux hardening measures that demonstrably reduced the attack surface (fewer open ports, stricter access controls). Before/after Nmap scans show measurable improvement.

Purple Team Debrief

As an ATTACKER: web application vulnerabilities give you a direct path to the underlying system. Command injection is essentially remote code execution. As a DEFENDER: input validation stops injection attacks. Firewalls limit network exposure. Least privilege prevents lateral movement. You've now experienced both sides of the same vulnerability.

Key Terms & Definitions

Segmentation
Dividing a network into smaller, isolated segments to limit lateral movement and contain breaches

ACL
Access Control List — a set of rules that define which users or systems are allowed or denied access to resources

Application Allow List
A security measure that only permits pre-approved applications to execute, blocking all others

Least Privilege
The principle of granting users and systems only the minimum access rights needed to perform their functions

CIS Benchmark
A set of best-practice security configuration guidelines published by the Center for Internet Security for hardening systems

Patch Management
The systematic process of identifying, acquiring, testing, and deploying software updates to fix vulnerabilities

HIPS
Host-based Intrusion Prevention System — software that monitors and blocks suspicious activity on a single host

Defense in Depth

A layered security approach using multiple controls at different levels to protect against various attack vectors

Input Validation
The process of verifying that user-supplied data meets expected formats before processing, preventing injection attacks

Hardening
The process of reducing a system's attack surface by removing unnecessary features, applying security configurations, and patching vulnerabilities

Decommissioning
The secure process of retiring old systems, including data sanitization and proper disposal

Configuration Enforcement
Automated mechanisms (Group Policy, SCAP, MDM) that ensure systems maintain their security baseline

Microsegmentation
Granular network segmentation that creates secure zones around individual workloads, limiting lateral movement

Sandboxing
Isolating applications in a controlled environment to prevent them from affecting the rest of the system

Endpoint Protection
Security software installed on endpoints (workstations, servers) that includes antivirus, anti-malware, and behavioral analysis

Practice Questions — Multiple Choice

Q1. After a breach, investigators discover the attacker moved freely between the web server, database, and internal file server. Which mitigation would have MOST effectively limited this movement?

A. Encryption

B. Patching

C. Network segmentation

D. Application allow listing

Answer: C — Network segmentation limits lateral movement by isolating systems into separate zones. Even if one segment is compromised, the attacker cannot freely access others.

Q2. An administrator configures a system to only run approved executables. This is an example of:

A. Sandboxing

B. Application allow listing

C. Access control list

D. Configuration enforcement

Answer: B — Application allow listing (whitelisting) only permits pre-approved applications to execute, blocking all unauthorized software including malware.

Q3. A web application accepts user input and directly incorporates it into SQL queries without sanitization. This vulnerability is BEST mitigated by:

A. Network segmentation

B. Input validation and parameterized queries

C. Full-disk encryption

D. Host-based firewall

Answer: B — SQL injection is prevented by input validation (sanitizing user input) and parameterized queries (prepared statements) that separate code from data.

Q4. Which hardening technique involves removing pre-installed software that is not required for the system's function?

A. Patching

B. Configuration enforcement

C. Removal of unnecessary software

D. Decommissioning

Answer: C — Removing unnecessary software reduces the attack surface by eliminating potential vulnerability points and reducing system complexity.

Q5. A company's security team discovers that a recently decommissioned server's hard drives were discarded without being wiped. This violates which principle?

A. Least privilege

B. Data sanitization during decommissioning

C. Patch management

D. Configuration enforcement

Answer: B — Proper decommissioning requires data sanitization (wiping, degaussing, or destroying) of storage media before disposal to prevent data recovery.

Practice Questions — Performance-Based (PBQ)

PBQ1. SCENARIO: You are tasked with creating a hardening checklist for a new Ubuntu web server. List at least 10 specific hardening steps in priority order, explaining why each step matters and what attack it prevents.

Answer: Priority order: (1) Apply all security updates — prevents known vulnerability exploitation. (2) Configure firewall (UFW) to allow only ports 80, 443, 22 — reduces attack surface. (3) Disable root login via SSH — prevents direct root compromise. (4) Set up SSH key-based authentication, disable password auth — prevents brute force. (5) Install and configure fail2ban — blocks repeated failed logins. (6) Remove unnecessary packages and services — reduces attack surface. (7) Set strong password policies — prevents weak credential exploitation. (8) Enable automatic security updates — ensures ongoing patching. (9) Configure file permissions (chmod/chown) restrictively — prevents unauthorized access. (10) Install HIDS (AIDE or OSSEC) — detects unauthorized file changes. (11) Disable unnecessary network protocols (IPv6 if unused) — reduces attack surface. (12) Configure logging to remote syslog server — preserves evidence if compromised.

PBQ2. SCENARIO: A web application has been compromised via SQL injection. As the incident responder, determine: (1) What evidence to collect, (2) How the attack likely progressed, (3) What immediate mitigations to apply, and (4) What long-term fixes to recommend.

Answer: (1) Evidence: web server access logs (look for SQLi patterns like UNION, OR 1=1, -- comments), database query logs, WAF logs, application error logs, network traffic captures. (2) Attack progression: Attacker probed input fields → found unvalidated parameter → injected SQL to enumerate DB → extracted sensitive data (and possibly wrote web shell via INTO OUTFILE). (3) Immediate mitigations: Take application offline, block attacker IP at WAF/firewall, reset all database passwords, check for web shells, review database for unauthorized changes, notify affected users. (4) Long-term: Implement parameterized queries throughout the application, deploy WAF rules for SQLi patterns, conduct application security code review, implement input validation framework, set up regular penetration testing, apply database least privilege (app account should not have DBA rights).

WEEKLY CHALLENGE

Download the CIS Benchmark for Ubuntu Linux (free from https://www.cisecurity.org/cis-benchmarks). Apply at least 20 hardening recommendations to your Ubuntu target VM. Document each change: before state, change made, after state, and verification method. Create a compliance scorecard showing your hardening progress percentage.

WEEK 6

Security Architecture & Network Defense

SY0-701 Objectives: 3.1: Compare and contrast security implications of different architecture models | 3.2: Given a scenario, apply security principles to secure enterprise infrastructure

PURPLE TEAM FRAMING

Network defense is the traditional battlefield of cybersecurity. This week, we build enterprise-grade defenses — firewalls, IDS/IPS, VPNs — and then immediately test them from the attacker's perspective. Students learn firewall evasion techniques so they can build rules that actually stop real threats. We bypass our own IDS to understand why signature-based detection has blind spots, then tune the rules to close those gaps.

Learning Objectives

1. Compare architecture models: cloud, on-premises, hybrid, IaC, serverless, microservices, containerization
2. Explain network infrastructure security: physical isolation, air-gapping, SDN, logical segmentation
3. Configure network security appliances: firewalls (WAF, NGFW, UTM), IDS/IPS, proxy servers, jump servers, load balancers
4. Implement secure communication: VPN, TLS tunneling, IPSec, SD-WAN, SASE
5. Understand failure modes (fail-open vs fail-closed) and device placement strategies
6. Set up a home network defense lab with pfSense and Snort/Suricata

Lecture Topics

- Architecture Models and Security Implications:
  - Cloud models: IaaS, PaaS, SaaS — shared responsibility matrix
  - Hybrid cloud considerations and third-party vendor risks
  - Infrastructure as Code (IaC): security benefits and risks
  - Serverless and microservices: expanded attack surface, API security
  - Containerization (Docker, Kubernetes): isolation vs VM-based virtualization
  - IoT and ICS/SCADA security challenges
  - Embedded systems and RTOS security considerations
  - Architecture considerations: availability, resilience, cost, scalability, risk transference
- Network Infrastructure Security:
  - Physical isolation and air-gapped networks
  - Logical segmentation: VLANs, subnets, security zones
  - Software-Defined Networking (SDN): programmable security
  - Centralized vs decentralized architectures

- Network Security Appliances:
  - Firewalls: packet filtering, stateful inspection, WAF, NGFW, UTM, Layer 4/Layer 7
  - IDS vs IPS: signature-based, anomaly-based, inline vs passive
  - Proxy servers: forward proxy, reverse proxy, transparent proxy
  - Jump servers (bastion hosts): secure administrative access
  - Load balancers: distributing traffic and preventing overload
  - Port security: 802.1X, EAP authentication
  - Sensors: network taps, SPAN ports
- Secure Communication:
  - VPN types: site-to-site, remote access, split vs full tunnel
  - Tunneling protocols: TLS, IPSec (IKE, ESP, AH)
  - SD-WAN: software-defined wide area networking
  - SASE: Secure Access Service Edge
- Failure Modes and Device Placement:
  - Fail-open vs fail-closed: when and why
  - Active vs passive devices, inline vs tap/monitor
  - DMZ architecture and screened subnets
- Firewall Evasion and IDS Bypass (Offensive Perspective):
  - Fragmentation attacks, protocol manipulation
  - Encrypted tunnel abuse, DNS tunneling
  - Why signature-based detection fails against novel attacks

Official Sources

[OFFICIAL] NIST SP 800-41 Rev. 1 — Guidelines on Firewalls and Firewall Policy
https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final

[OFFICIAL] NIST SP 800-77 Rev. 1 — Guide to IPsec VPNs
https://csrc.nist.gov/publications/detail/sp/800-77/rev-1/final

[OFFICIAL] CISA — Securing Network Infrastructure Devices
https://www.cisa.gov/news-events/news/securing-network-infrastructure-devices

[OFFICIAL] MITRE ATT&CK — Lateral Movement Tactics
https://attack.mitre.org/tactics/TA0008/

[OFFICIAL] SANS — Network Security Architecture Best Practices
https://www.sans.org/white-papers/network-security/

Underground / Bleeding Edge Sources

[UNDERGROUND] NetworkChuck — 'Build Your Own Firewall with pfSense' tutorial

[UNDERGROUND] John Hammond — 'IDS Evasion Techniques' video

[UNDERGROUND] r/homelab — 'My home network security setup' showcase threads

[UNDERGROUND] DEF CON 29 — 'Bypassing Next-Gen Firewalls' talk

[UNDERGROUND] IppSec — 'HTB: Pivoting and Lateral Movement' walkthrough

[UNDERGROUND] r/netsec — 'SD-WAN security: the good, bad, and ugly' analysis

CASE STUDY: Target POS Breach (2013) & Marriott Breach (2018) — Network Segmentation Failures

Target (2013): During the 2013 holiday season, attackers stole 40 million credit/debit card numbers and 70 million customer records from Target. The attack began when Fazio Mechanical (Target's HVAC vendor) fell victim to a phishing email. Attackers used Fazio's VPN credentials to access Target's network — but here's the critical failure: Target's vendor network was not segmented from the payment processing network. Attackers installed RAM-scraping malware on POS terminals to capture card data in transit (before encryption). The malware exfiltrated data to external servers, triggering FireEye alerts that Target's security team ignored.

What went wrong: (1) No network segmentation between vendor access and POS systems. (2) Third-party vendor had excessive network access. (3) Security alerts from FireEye were ignored by the SOC team. (4) POS terminals were running embedded Windows XP — outdated and vulnerable. The total cost exceeded $200 million in settlements and remediation.

Marriott/Starwood (2018): Marriott disclosed that its Starwood reservation system had been compromised since 2014 — four years before detection. When Marriott acquired Starwood in 2016, they inherited the breach along with the IT infrastructure. Attackers used Remote Access Trojans (RATs) and Mimikatz for credential harvesting, moving laterally through the network. 500 million guest records were exposed including passport numbers.

What went wrong: (1) Due diligence during the acquisition did not include thorough security assessment of Starwood's infrastructure. (2) The Starwood network had insufficient segmentation and monitoring. (3) Attackers used legitimate tools (Mimikatz, RATs) that blended with normal admin activity. (4) Lateral movement went undetected for four years — a catastrophic monitoring failure.

Lessons learned: (1) Network segmentation is not optional — every zone should be isolated with strict inter-zone rules. (2) Vendor access must be tightly controlled and segmented from critical systems. (3) M&A cybersecurity due diligence is essential — you inherit their vulnerabilities. (4) Alerts are useless if no one responds to them. (5) Lateral movement detection requires behavioral analytics, not just signature-based IDS.

HANDS-ON LAB: Build a Network Defense Lab with pfSense & IDS

Objective

Configure pfSense as a network firewall with granular rules and set up Snort or Suricata as an IDS to detect network attacks.

Tools Required

pfSense (free ISO), Snort or Suricata (free, integrated with pfSense), WireGuard (free)

Step-by-Step Instructions

1. Download pfSense CE ISO from https://www.pfsense.org/download/
2. Create a new VM in VirtualBox: Name='pfSense-FW', RAM=1GB, Disk=10GB, two network adapters
3. Adapter 1: Bridged (WAN), Adapter 2: Internal Network 'hacklab' (LAN)
4. Install pfSense, configure WAN (DHCP) and LAN (192.168.1.1/24) interfaces
5. Access pfSense web GUI from Kali: https://192.168.1.1 (default: admin/pfsense)
6. Configure firewall rules: Block all inbound by default, allow LAN to WAN for HTTP/HTTPS/DNS only
7. Create an alias for 'Blocked_IPs' — add known malicious IP ranges

8. Install Snort package: System > Package Manager > search 'snort' > install
9. Configure Snort on the LAN interface: enable ET Open rules (free)
10. From Kali, run a port scan against a target: nmap -sS -T4 [target] — observe Snort alerts
11. Try an aggressive scan: nmap -A -T5 [target] — how does Snort respond?
12. Review Snort alerts in the pfSense GUI — identify true positives vs false positives
13. Configure WireGuard VPN on pfSense for secure remote access
14. Test: Can Kali reach the LAN through the VPN tunnel? Verify encryption with Wireshark

Expected Outcomes

A working pfSense firewall with customized rules protecting the lab network. Snort IDS detecting and alerting on port scans and suspicious network activity. A functional WireGuard VPN tunnel providing encrypted remote access.

Purple Team Debrief

As an ATTACKER: you've seen that standard Nmap scans trigger IDS alerts. Advanced evasion techniques (fragmentation, slow scans, decoys) might bypass detection. As a DEFENDER: you've configured layered network defenses and understand alert tuning. Not every alert is real — false positive management is a critical SOC skill.

Key Terms & Definitions

NGFW
Next-Generation Firewall — combines traditional firewall capabilities with advanced features like application awareness, IPS, and threat intelligence

WAF
Web Application Firewall — specifically protects web applications by filtering and monitoring HTTP/HTTPS traffic

IDS
Intrusion Detection System — monitors network traffic for suspicious activity and generates alerts

IPS
Intrusion Prevention System — monitors and actively blocks detected malicious traffic inline

SDN
Software-Defined Networking — decouples the network control plane from the data plane, enabling programmatic network management

SASE
Secure Access Service Edge — a cloud-delivered framework combining network security and WAN capabilities

SD-WAN
Software-Defined Wide Area Network — uses software to manage WAN connections, optimizing performance and security

DMZ
Demilitarized Zone — a network segment between internal and external networks that hosts public-facing services

Jump Server
A hardened intermediary server used to access systems in a different security zone (also called bastion host)

802.1X
: An IEEE standard for port-based Network Access Control, providing authentication for devices connecting to a LAN

IPSec
: Internet Protocol Security — a suite of protocols for securing IP communications through authentication and encryption

Air Gap
: A physical isolation security measure where a computer or network is not connected to any other network, including the internet

IaC
: Infrastructure as Code — managing IT infrastructure through machine-readable configuration files rather than physical hardware or interactive tools

Fail-Open
: A failure mode where a security device allows all traffic when it malfunctions, prioritizing availability

Fail-Closed
: A failure mode where a security device blocks all traffic when it malfunctions, prioritizing security

UTM
: Unified Threat Management — a single appliance combining multiple security functions: firewall, IDS/IPS, antivirus, content filtering

Practice Questions — Multiple Choice

Q1. A company needs a firewall solution that can inspect encrypted HTTPS traffic and identify specific applications being used. Which type is MOST appropriate?

A. Packet-filtering firewall

B. Stateful inspection firewall

C. Next-generation firewall (NGFW)

D. Web application firewall (WAF)

Answer: C — NGFWs combine traditional firewall capabilities with application awareness, SSL/TLS inspection, and integrated IPS — able to inspect encrypted traffic and identify applications.

Q2. A security architect places an IDS sensor on a network TAP rather than inline. This makes the IDS:

A. Active and able to block traffic

B. Passive and able to only alert

C. More effective at preventing attacks

D. A replacement for a firewall

Answer: B — A TAP provides a copy of network traffic to the IDS without the IDS being inline. This makes it passive — it can detect and alert but cannot block traffic. An IPS would be placed inline.

Q3. An organization is designing its cloud architecture and wants to ensure that a failure at one cloud provider doesn't take down all services. This is BEST achieved by:

A. Hybrid cloud

B. Multi-cloud

C. Private cloud

D. Community cloud

Answer: B — Multi-cloud distributes services across multiple cloud providers, ensuring that a single provider failure doesn't cause total service disruption.

Q4. Which protocol provides both authentication and encryption for VPN tunnels at the network layer?

A. TLS

B. SSH

C. IPSec

D. PPTP

Answer: C — IPSec operates at the network layer (Layer 3) and provides both authentication (AH) and encryption (ESP) for VPN tunnels.

Q5. A critical network firewall fails. Traffic is now flowing through without any inspection. This firewall was configured in:

A. Fail-closed mode

B. Fail-open mode

C. Passive mode

D. Inline mode

Answer: B — Fail-open allows all traffic when the device fails. Fail-closed would block all traffic — more secure but impacts availability.

Practice Questions — Performance-Based (PBQ)

PBQ1. SCENARIO: Design a network architecture for a medium-sized company with the following requirements: public web server, internal database, employee workstations, and remote worker access. Draw/describe the architecture including: network zones, firewall placement, IDS/IPS placement, VPN configuration, and segmentation strategy.

Answer: Architecture: (1) WAN connection through edge router to NGFW. (2) DMZ zone behind NGFW containing web server — only ports 80/443 open from WAN. (3) Internal zone with two segments: Database VLAN (only accessible from web server and admin workstations) and Employee VLAN (general workstations). (4) IDS sensor on network TAP between DMZ and internal zone. (5) IPS inline between employee VLAN and database VLAN. (6) VPN concentrator in DMZ for remote workers — authenticates with MFA, provides access only to employee VLAN. (7) Jump server in admin segment for database access. (8) Firewall rules: DMZ web server → database (specific port only), employees → internet (filtered), remote VPN → employee VLAN only. (9) All inter-VLAN traffic inspected by NGFW.

PBQ2. SCENARIO: Your IDS has generated 500 alerts in the past 24 hours. Categorize and prioritize the following alerts, and determine which are likely false positives: (1) Port scan from internal IP, (2) SQL injection attempt on web server, (3) DNS query to known C2 domain, (4) SSH brute force from internet, (5) Large file transfer to cloud storage during business hours.

Answer: Priority 1 (CRITICAL): (3) DNS query to known C2 domain — indicates possible active compromise, investigate immediately. Priority 2 (HIGH): (2) SQL injection attempt — active attack on web server, verify WAF is blocking, check for successful exploitation. Priority 3 (HIGH): (4) SSH brute force — active attack, verify fail2ban is blocking, check for successful logins. Priority 4 (MEDIUM): (1) Port scan from internal IP — could be legitimate IT scanning or compromised internal host, investigate source. Priority 5 (LOW/likely false positive): (5) Large file transfer to cloud storage during business hours — likely normal business activity, verify against approved cloud services. Tuning recommendations: Create allow list for approved cloud storage, set threshold for SSH alerts, correlate internal port scans with scheduled vulnerability scans.

WEEKLY CHALLENGE

Build a complete network diagram for a fictional company 'CyberShield Corp' with 200 employees across two offices. Include: WAN connectivity, firewalls, DMZ, internal segmentation (at least 4 VLANs), IDS/IPS placement, VPN for remote workers, Wi-Fi security, and a jump server. Document all firewall rules between zones. Use draw.io (https://app.diagrams.net/ — free) to create the diagram.

WEEK 7

Data Protection, Cloud Security & Resilience

SY0-701 Objectives: 3.3: Compare and contrast concepts and strategies to protect data | 3.4: Explain the importance of resilience and recovery in security architecture

PURPLE TEAM FRAMING

Data is the ultimate target — whether you're an attacker trying to exfiltrate it or a defender trying to protect it. This week explores cloud security from the attacker's perspective (finding misconfigured S3 buckets, exploiting cloud APIs) and the defender's perspective (proper configuration, encryption, access controls). We also build resilience — because the question isn't IF you'll be breached, but how fast you can recover.

Learning Objectives

1. Classify data types (regulated, trade secret, IP, legal, financial) and apply appropriate data classifications
2. Implement data protection methods: encryption, hashing, masking, tokenization, segmentation, geographic restrictions
3. Understand data states: at rest, in transit, in use — and protection strategies for each
4. Explain cloud security concepts: shared responsibility, misconfiguration risks, cloud attack surfaces
5. Design resilient architectures: high availability, disaster recovery sites (hot/warm/cold), backups, replication
6. Conduct backup/recovery exercises and understand RPO/RTO concepts

Lecture Topics

- Data Classification and Types:
  - Regulated data: PII, PHI, PCI-DSS, FERPA
  - Trade secrets, intellectual property, legal information, financial data
  - Classification levels: public, private, sensitive, confidential, restricted, critical
  - Human-readable vs non-human-readable data
- Data States and Protection:
  - Data at rest: full-disk encryption, database encryption, file-level encryption
  - Data in transit: TLS, IPSec, VPN tunnels
  - Data in use: secure enclaves, memory encryption
  - Data sovereignty and geolocation requirements
- Data Protection Methods:
  - Encryption (symmetric/asymmetric), hashing, masking, tokenization
  - Obfuscation, segmentation, permission restrictions
  - Geographic restrictions and data residency
  - DLP (Data Loss Prevention) strategies

- Cloud Security Deep Dive:
  - Shared responsibility model: what the provider secures vs what you secure
  - Cloud attack surfaces: misconfigured storage, exposed APIs, identity issues
  - S3 bucket enumeration (offensive), S3 bucket policies (defensive)
  - Cloud Security Posture Management (CSPM) tools
  - Multi-cloud and hybrid cloud security challenges
- Resilience and Recovery:
  - High availability: load balancing vs clustering
  - DR sites: hot (fully operational), warm (partially ready), cold (infrastructure only)
  - Geographic dispersion and platform diversity
  - Continuity of operations planning
  - Capacity planning: people, technology, infrastructure
- Testing Resilience:
  - Tabletop exercises, failover testing, simulations, parallel processing
- Backup Strategies:
  - Onsite vs offsite, frequency, encryption, snapshots
  - Recovery, replication, journaling
  - The 3-2-1 backup rule: 3 copies, 2 different media, 1 offsite
- Power Resilience: generators, UPS systems

Official Sources

[OFFICIAL] NIST SP 800-88 Rev. 1 — Guidelines for Media Sanitization
https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final

[OFFICIAL] CSA (Cloud Security Alliance) — Security Guidance v4.0
https://cloudsecurityalliance.org/research/guidance/

[OFFICIAL] NIST SP 800-144 — Guidelines on Security and Privacy in Public Cloud Computing
https://csrc.nist.gov/publications/detail/sp/800-144/final

[OFFICIAL] AWS Shared Responsibility Model
https://aws.amazon.com/compliance/shared-responsibility-model/

[OFFICIAL] NIST SP 800-34 Rev. 1 — Contingency Planning Guide
https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final

Underground / Bleeding Edge Sources

[UNDERGROUND] Rhino Security Labs Blog — 'Exploiting AWS Misconfigurations' series

[UNDERGROUND] NetworkChuck — 'Cloud Security for Beginners' video

[UNDERGROUND] r/aws — 'We left an S3 bucket public and here's what happened' post-mortem

[UNDERGROUND] DEF CON Cloud Village — annual talks on cloud exploitation techniques

[UNDERGROUND] TheCyberMentor — 'Practical Cloud Penetration Testing' course content

[UNDERGROUND] grayhatwarfare.com — Public S3 bucket search engine (educational/awareness)

CASE STUDY: Capital One S3 Breach (2019) & The Uber 2022 Hack

Capital One (2019): Former AWS employee Paige Thompson exploited a Server-Side Request Forgery (SSRF) vulnerability in Capital One's WAF to access the AWS Instance Metadata Service (IMDS). This gave her

temporary credentials for an IAM role that had excessive permissions to S3 buckets. She exfiltrated records of 100+ million customers, including Social Security numbers and bank account numbers.

Technical details: The SSRF vulnerability allowed Thompson to query http://169.254.169.254 (the AWS metadata endpoint) from the WAF. The metadata service returned IAM role credentials with S3 access. Capital One had not restricted the IAM role's permissions to only necessary buckets, nor had they implemented IMDSv2 (which requires a token, mitigating SSRF). The data in S3 was not encrypted with customer-managed keys.

Uber (2022): An 18-year-old hacker breached Uber by purchasing stolen credentials from the dark web, then bombarding an Uber employee with MFA push notifications until they accepted (MFA fatigue attack). Once inside, the attacker found a PowerShell script on a network share containing hardcoded admin credentials for Uber's Privileged Access Management (PAM) system. This gave them access to virtually all of Uber's internal systems including AWS, GCP, Slack, SentinelOne EDR console, and HackerOne bug bounty reports.

What defenders did wrong: Capital One — overly permissive IAM roles, no IMDSv2, unencrypted sensitive data in S3. Uber — MFA without phishing-resistant methods (FIDO2), hardcoded credentials in scripts, insufficient monitoring of PAM access, no alerting on anomalous MFA behavior.

Lessons learned: (1) Cloud IAM policies must follow least privilege — no IAM role should have blanket access to all S3 buckets. (2) Use IMDSv2 on all AWS instances. (3) Encrypt sensitive data with customer-managed keys, not just default encryption. (4) MFA fatigue attacks are real — use number matching or FIDO2 hardware keys. (5) Never store credentials in scripts or code. (6) Monitor and alert on anomalous access patterns, especially to PAM systems.

HANDS-ON LAB: Cloud Security Audit & Backup Recovery

Objective

Use ScoutSuite to audit cloud security configurations and practice backup/recovery procedures to understand disaster recovery.

Tools Required

ScoutSuite (free), AWS Free Tier or LocalStack (free), rsync, tar, cron

Step-by-Step Instructions

PART A — Cloud Security Auditing:

2. Install ScoutSuite on Kali: pip install scoutsuite
3. If you have an AWS Free Tier account, configure AWS CLI: aws configure
4. Run ScoutSuite: scout aws --no-browser (generates HTML report)
5. If no AWS account, use the ScoutSuite sample report at: https://github.com/nccgroup/ScoutSuite
6. Review the report: identify misconfigured S3 buckets, overly permissive IAM policies, unencrypted resources
7. For each finding: document the risk, CVSS-equivalent severity, and remediation steps
8. Create a 'Cloud Security Scorecard' based on findings

PART B — Backup and Recovery Exercise:

10. On your Ubuntu target VM, create test data: mkdir -p /home/user/important_data && echo 'critical business data' > /home/user/important_data/financials.txt

11. Create additional files to simulate a real environment with various file types
12. Perform a full backup: tar czf /backup/full_backup_$(date +%Y%m%d).tar.gz /home/user/important_data/
13. Simulate data loss: rm -rf /home/user/important_data/ (this simulates ransomware encryption)
14. Restore from backup: tar xzf /backup/full_backup_*.tar.gz -C /
15. Verify restoration: diff the restored files against expected content
16. Set up automated backups with cron: crontab -e, add daily backup job
17. Calculate RPO: if backups run daily, maximum data loss = 24 hours. Discuss acceptable RPO for different data types
18. Document your backup strategy: frequency, retention, encryption, offsite copy plan

Expected Outcomes

A cloud security audit report identifying misconfigurations with remediation recommendations. A working backup/recovery process with automated scheduling. Understanding of RPO/RTO trade-offs.

Purple Team Debrief

As an ATTACKER: misconfigured cloud resources are low-hanging fruit. S3 bucket enumeration is trivial, and overly permissive IAM roles are everywhere. As a DEFENDER: cloud security requires continuous auditing. Backups must be tested — untested backups are not backups. The 3-2-1 rule (3 copies, 2 media, 1 offsite) is your ransomware insurance policy.

Key Terms & Definitions

Data at Rest
Data stored on a device or medium that is not currently being transmitted or processed

Data in Transit
Data actively moving between locations — across networks, between devices, or between services

Data in Use
Data currently being processed, accessed, or read by a system or application in memory

Data Sovereignty
The concept that data is subject to the laws and governance structures of the country where it is collected or stored

Tokenization
Replacing sensitive data with a non-sensitive token that maps back to the original data through a secure lookup system

DLP
Data Loss Prevention — technologies and policies that prevent unauthorized data exfiltration from an organization

Shared Responsibility Model
A cloud security framework defining which security tasks the cloud provider handles and which the customer must manage

RPO
Recovery Point Objective — the maximum acceptable amount of data loss measured in time (how old can restored data be?)

RTO
Recovery Time Objective — the maximum acceptable downtime before services must be restored

Hot Site
A fully operational disaster recovery facility with real-time data replication, ready for immediate failover

Warm Site
A DR facility with hardware and connectivity but requiring data restoration before becoming operational

Cold Site
A DR facility with basic infrastructure (power, cooling, connectivity) but no pre-installed hardware or data

High Availability
System design that ensures a high level of operational continuity, typically through redundancy and failover mechanisms

3-2-1 Backup Rule
Best practice: maintain 3 copies of data, on 2 different storage media, with 1 copy stored offsite

CSPM
Cloud Security Posture Management — automated tools that continuously monitor cloud configurations for security risks

SSRF
Server-Side Request Forgery — a vulnerability where an attacker tricks a server into making requests to unintended internal resources

Practice Questions — Multiple Choice

Q1. A company stores customer credit card numbers. To reduce PCI-DSS compliance scope, they replace card numbers with random tokens that map to the actual numbers in a secure vault. This technique is:

A. Encryption

B. Hashing

C. Tokenization

D. Data masking

Answer: C — Tokenization replaces sensitive data with non-sensitive tokens. Unlike encryption, the token has no mathematical relationship to the original data, reducing compliance scope.

Q2. An organization's business continuity plan specifies that they can tolerate a maximum of 4 hours of data loss. This defines their:

A. RTO

B. RPO

C. MTTR

D. MTBF

Answer: B — RPO (Recovery Point Objective) defines maximum acceptable data loss in time. An RPO of 4 hours means backups must occur at least every 4 hours.

Q3. In the AWS shared responsibility model, which of the following is the CUSTOMER'S responsibility?

A. Physical security of data centers

B. Hypervisor patching

C. IAM policy configuration

D. Network infrastructure maintenance

Answer: C — IAM policy configuration is the customer's responsibility. AWS manages physical security, hypervisor, and network infrastructure. The customer manages what they put IN the cloud.

Q4. A disaster recovery facility has hardware installed and network connectivity but requires data to be restored from backups before operations can resume. This is a:

A. Hot site

B. Warm site

C. Cold site

D. Mobile site

Answer: B — A warm site has hardware and connectivity pre-installed but is not running live data replication. It requires data restoration before becoming operational.

Q5. Data stored in a database is classified as data:

A. In transit

B. In use

C. At rest

D. In processing

Answer: C — Data at rest is data stored on a device or medium — databases, file systems, archives. It's not being actively transmitted or processed.

Practice Questions — Performance-Based (PBQ)

PBQ1. SCENARIO: Your company is migrating to AWS. Design a data protection strategy that addresses: (1) Data classification for customer PII, (2) Encryption for data at rest and in transit, (3) Access controls following least privilege, (4) Backup and disaster recovery with RPO of 1 hour and RTO of 4 hours.

Answer: (1) Classification: PII marked as 'Confidential', stored only in designated encrypted S3 buckets with versioning enabled. Tag all PII resources. (2) Encryption at rest: S3 SSE-KMS with customer-managed keys (CMK), RDS encryption enabled, EBS volumes encrypted. In transit: enforce TLS 1.2+ for all API calls, VPC endpoints for internal service communication. (3) Access: IAM policies with least privilege, no wildcard permissions, MFA required for console access, service accounts use IAM roles (not access keys), S3 bucket policies deny public access. (4) DR: RPO 1hr = RDS automated backups every hour with Multi-AZ deployment, S3 cross-region replication. RTO 4hr = warm site in secondary region with CloudFormation templates ready to deploy, Route 53 health checks for automated DNS failover. Regular DR testing quarterly.

PBQ2. SCENARIO: A cloud security audit reveals the following findings. Prioritize them and recommend remediation: (A) 3 S3 buckets with public read access, (B) Root account used for daily operations, (C) CloudTrail logging disabled in 2 regions, (D) Security groups allowing 0.0.0.0/0 on port 22, (E) Unencrypted RDS instance containing customer data.

Answer: Priority 1 (CRITICAL): (B) Root account used for daily operations — root has unrestricted access, no accountability. Remediation: create individual IAM users immediately, enable MFA on root, lock root credentials. Priority 2 (CRITICAL): (A) Public S3 buckets — data exposure risk. Remediation: enable S3 Block Public Access at account level, review bucket policies. Priority 3 (HIGH): (E) Unencrypted RDS with customer data — compliance violation. Remediation: enable RDS encryption (requires snapshot, restore to encrypted instance). Priority 4 (HIGH): (C) CloudTrail disabled — no audit trail, attacker activity invisible. Remediation: enable CloudTrail in all regions, send to centralized S3 bucket. Priority 5 (MEDIUM): (D) SSH open to internet — brute force risk. Remediation: restrict to specific admin IP ranges, implement bastion host.

WEEKLY CHALLENGE

Create a complete Disaster Recovery Plan for a fictional e-commerce company. Include: (1) Business Impact Analysis identifying critical systems and their RTO/RPO, (2) DR site strategy (hot/warm/cold with justification), (3) Backup strategy with 3-2-1 rule implementation, (4) Communication plan during a disaster,

(5) Recovery procedures step-by-step, (6) Testing schedule. Aim for a professional-quality document that could be presented to management.

WEEK 8

Security Operations — Detection, Monitoring & IAM

SY0-701 Objectives: 4.1: Given a scenario, apply common security techniques to computing resources | 4.2: Explain the security implications of proper hardware, software, and data asset management | 4.3: Explain various activities associated with vulnerability management | 4.4: Explain security alerting and monitoring concepts and tools | 4.5: Given a scenario, implement and maintain identity and access management

PURPLE TEAM FRAMING

Security operations is where the rubber meets the road — this is what defenders do every single day. But we teach it the BlackHack way: for every detection technique, we show the evasion technique. For every IAM control, we demonstrate the identity attack that bypasses it. Students set up Splunk and immediately try to generate activity that evades their own detection rules. Kerberoasting and Pass-the-Hash attacks are performed so students understand why PAM and monitoring matter.

Learning Objectives

1. Establish and maintain secure baselines for servers, workstations, and mobile devices
2. Implement asset management practices: acquisition, tracking, disposal, sanitization
3. Execute vulnerability management lifecycle: identification, analysis, remediation, validation
4. Configure SIEM solutions (Splunk/Wazuh) for log aggregation, alerting, and monitoring
5. Implement IAM: SSO (SAML, OAuth, LDAP), MFA, RBAC, privileged access management
6. Perform identity-based attacks (Kerberoasting, Pass-the-Hash) and defend against them
7. Configure email security: SPF, DKIM, DMARC

Lecture Topics

- Secure Baselines and Hardening Targets:
  - Establishing baselines: CIS Benchmarks, STIG, vendor hardening guides
  - Deploying and maintaining baselines across: mobile devices, workstations, switches, routers, cloud, servers, ICS/SCADA, IoT
  - Wireless security: WPA3, site surveys, heat maps, RADIUS
  - Mobile solutions: MDM, BYOD/COPE/CYOD, Bluetooth/cellular/Wi-Fi security
  - Application security: input validation, secure cookies, static code analysis, code signing, sandboxing
- Asset Management:
  - Acquisition/procurement, assignment/accounting, ownership, classification
  - Monitoring/tracking: inventory, enumeration
  - Disposal: sanitization, destruction, certification, data retention
- Vulnerability Management Lifecycle:

  - Identification: vulnerability scans, static/dynamic analysis, package monitoring, threat feeds (OSINT, proprietary, dark web), pen testing, bug bounties
  - Analysis: confirmation (false positive/negative), prioritization, CVSS, CVE, classification
  - Response: patching, insurance, segmentation, compensating controls, exceptions
  - Validation: rescanning, audit, verification
  - Reporting and metrics
- Security Monitoring and SIEM:
  - Log aggregation from systems, applications, infrastructure
  - SIEM platforms: Splunk, Wazuh, ELK
  - Alerting, scanning, reporting, archiving
  - Alert response: quarantine, tuning, remediation
  - Tools: SCAP, benchmarks, agents vs agentless, antivirus, DLP, SNMP traps, NetFlow, vulnerability scanners
- Identity and Access Management:
  - SSO: LDAP, OAuth, SAML
  - MFA: biometrics, tokens, security keys, factors (know/have/are/somewhere)
  - Access controls: MAC, DAC, RBAC, rule-based, ABAC, time-of-day
  - Privileged Access Management: JIT permissions, password vaulting, ephemeral credentials
  - Password concepts: complexity, managers, passwordless
  - Identity attacks (Offensive): Kerberoasting, Pass-the-Hash, Golden Ticket, credential stuffing
- Enterprise Security Capabilities:
  - Firewalls, IDS/IPS, web filters, DNS filtering
  - Email security: DMARC, DKIM, SPF, gateways
  - File integrity monitoring, DLP, NAC, EDR/XDR
  - User behavior analytics

Official Sources

[OFFICIAL] NIST SP 800-137 — Information Security Continuous Monitoring
https://csrc.nist.gov/publications/detail/sp/800-137/final

[OFFICIAL] NIST SP 800-63B — Digital Identity Guidelines (Authentication)
https://pages.nist.gov/800-63-3/sp800-63b.html

[OFFICIAL] MITRE ATT&CK — Credential Access Tactics
https://attack.mitre.org/tactics/TA0006/

[OFFICIAL] CIS Controls v8
https://www.cisecurity.org/controls/v8

[OFFICIAL] SANS — SIEM and Log Management Best Practices
https://www.sans.org/white-papers/siem/

Underground / Bleeding Edge Sources

[UNDERGROUND] John Hammond — 'Active Directory Attacks for Beginners' video

[UNDERGROUND] IppSec — 'Kerberoasting and Pass-the-Hash' HTB walkthroughs

[UNDERGROUND] r/blueteamsec — 'Setting up Wazuh SIEM at home' guide

[UNDERGROUND] TheCyberMentor — 'Practical Ethical Hacking: Active Directory' module

[UNDERGROUND] DEF CON 32 — 'Abusing Active Directory: A Red Teamer's Guide' talk

[UNDERGROUND] 13Cubed (YouTube) — 'Splunk for Security Analysts' tutorial series

CASE STUDY: SolarWinds Orion Detection Failures & The Okta Breach (2023)

SolarWinds Orion — Detection Perspective: The SolarWinds SUNBURST attack (discovered December 2020) remained undetected for approximately 9 months. The attackers' tradecraft was specifically designed to evade detection: the malicious code mimicked legitimate Orion traffic patterns, used IP addresses in the same country as the victim, and only activated after a 12-14 day dormancy period. The malware checked for security tools (antivirus, EDR) before executing.

Detection failures: (1) Network monitoring didn't flag the C2 communications because they used legitimate Orion API patterns. (2) Endpoint detection tools were specifically evaded — the malware checked for security products. (3) The software supply chain was trusted — nobody inspected SolarWinds updates. (4) Lateral movement used legitimate admin tools (PowerShell, WMI). FireEye finally detected the breach when they noticed unauthorized access to their own Red Team tools — not through automated detection but through manual investigation triggered by a suspicious MFA enrollment.

Okta Breach (2023): The Okta support system was compromised in October 2023 when attackers used stolen credentials to access Okta's customer support case management system. Attackers could view HAR (HTTP Archive) files uploaded by customers for troubleshooting, which contained session tokens. Using these tokens, attackers accessed customer Okta tenants including BeyondTrust and Cloudflare.

What makes this significant for IAM: Okta is an identity provider for thousands of organizations. Compromising the identity provider gives access to all connected services. BeyondTrust detected the breach within 24 hours because they had robust anomaly detection on their Okta integration — showing that monitoring works when done right.

Lessons learned: (1) Supply chain monitoring requires behavioral analysis, not just signature detection. (2) SIEM correlation rules should detect anomalous patterns in trusted software. (3) Identity providers are high-value targets — extra monitoring is essential. (4) Session token management must include rotation and anomaly detection. (5) SOC teams need threat hunting capabilities to find what automated tools miss.

HANDS-ON LAB: SIEM Setup & Active Directory Attack/Defend

Objective

Set up Splunk Free for log analysis and Wazuh for monitoring, then perform and detect Active Directory identity attacks using BloodHound.

Tools Required

Splunk Free (free), Wazuh (free), BloodHound (free), Mimikatz (on Kali)

Step-by-Step Instructions

PART A — SIEM Configuration:

2. Install Splunk Free on your Kali or Ubuntu VM: download from https://www.splunk.com/en_us/download.html
3. Start Splunk: /opt/splunk/bin/splunk start (set admin password)
4. Access web interface: http://localhost:8000
5. Configure data inputs: monitor /var/log/auth.log and /var/log/syslog
6. Generate some events: attempt SSH logins (successful and failed) from your Kali VM
7. Create a search query: index=main sourcetype=syslog 'Failed password' | stats count by src_ip

8. Build a dashboard: failed logins over time, top source IPs, event severity distribution
9. Create an alert: trigger when failed logins exceed 10 from a single IP in 5 minutes

PART B — Identity Attack Simulation:

11. Install BloodHound on Kali: apt install bloodhound
12. If you have an AD lab (or use a practice environment like DVAD/GOAD):
13. Run SharpHound collector to map AD relationships
14. Import data into BloodHound and identify attack paths to Domain Admin
15. Find Kerberoastable accounts: look for SPNs on user accounts
16. If no AD lab available, use BloodHound's sample database to analyze attack paths
17. Study the attack path: initial access → Kerberoasting → privilege escalation → domain compromise
18. For each attack path node, document: the attack technique AND the defensive control that would block it

Expected Outcomes

A working SIEM with custom dashboards and alerts detecting security events in real-time. Understanding of Active Directory attack paths and how identity-based attacks chain together. Defensive recommendations for each attack technique discovered.

Purple Team Debrief

As an ATTACKER: Active Directory is often the keys to the kingdom. Kerberoasting, Pass-the-Hash, and lateral movement through trust relationships are standard red team techniques. As a DEFENDER: SIEM monitoring, service account hardening (long random passwords, managed service accounts), and PAM (just-in-time access) significantly reduce identity attack risk. BloodHound should be run by defenders regularly to find and eliminate dangerous attack paths before adversaries do.

Key Terms & Definitions

SIEM
Security Information and Event Management — centralized platform for collecting, correlating, and analyzing security logs from across the enterprise

EDR
Endpoint Detection and Response — security solution that monitors endpoints for suspicious activity, provides investigation capabilities, and enables rapid response

XDR
Extended Detection and Response — extends EDR across multiple security layers (network, cloud, email, identity) for correlated threat detection

RBAC
Role-Based Access Control — access permissions assigned based on a user's role within the organization

SAML
Security Assertion Markup Language — an XML-based standard for exchanging authentication and authorization data between identity providers and service providers

OAuth
Open Authorization — a standard protocol for token-based authorization, commonly used for API access

LDAP

Lightweight Directory Access Protocol — a protocol for accessing and managing directory services (e.g., Active Directory)

Kerberoasting
An attack technique that extracts service account ticket-granting tickets from Active Directory for offline password cracking

Pass-the-Hash
An attack where stolen password hashes are used to authenticate without knowing the actual password

NAC
Network Access Control — technology that enforces security policies on devices connecting to the network

SCAP
Security Content Automation Protocol — a method for using security standards to automate vulnerability management and configuration compliance

MDM
Mobile Device Management — software for managing, monitoring, and securing mobile devices in an enterprise environment

SSO
Single Sign-On — authentication mechanism allowing users to access multiple applications with one set of credentials

MFA Fatigue
An attack where the adversary sends repeated MFA push notifications hoping the user will approve one to stop the alerts

Privileged Access Management
Solutions that secure, manage, and monitor privileged accounts and access, including JIT permissions and password vaulting

DMARC
Domain-based Message Authentication, Reporting and Conformance — email authentication protocol that uses SPF and DKIM to detect email spoofing

Practice Questions — Multiple Choice

Q1. A security analyst configures the SIEM to alert when a user account logs in from two different countries within one hour. This is monitoring for:

A. Brute force attack

B. Impossible travel

C. Privilege escalation

D. Account lockout

Answer: B — Impossible travel detection alerts when a user appears to log in from geographically distant locations within a timeframe that makes physical travel impossible.

Q2. An attacker extracts service account TGTs from Active Directory and cracks them offline. This technique is called:

A. Pass-the-Hash

B. Golden Ticket

C. Kerberoasting

D. Credential stuffing

Answer: C — Kerberoasting targets Kerberos Ticket Granting Tickets (TGTs) for service accounts, which can be requested by any authenticated domain user and cracked offline.

Q3. Which MFA factor type does a fingerprint scanner represent?

A. Something you know

B. Something you have

C. Something you are

D. Somewhere you are

Answer: C — Biometrics (fingerprint, retina, facial recognition) represent 'something you are' — an inherence factor.

Q4. A company wants to ensure that employees can only access applications relevant to their job function. Which access control model is MOST appropriate?

A. Discretionary Access Control

B. Mandatory Access Control

C. Role-Based Access Control

D. Rule-Based Access Control

Answer: C — RBAC assigns access based on organizational roles. Employees are assigned roles, and roles have predefined permissions — ensuring job-function-aligned access.

Q5. After decommissioning a server, the security team must ensure data cannot be recovered. Which sanitization method provides the HIGHEST assurance?

A. Formatting the drive

B. Deleting all files

C. Degaussing

D. Physical destruction

Answer: D — Physical destruction (shredding, incineration) provides the highest assurance that data cannot be recovered. Degaussing works for magnetic media but not SSDs. Formatting and deletion are insufficient.

Practice Questions — Performance-Based (PBQ)

PBQ1. SCENARIO: Your SIEM shows the following sequence of events for user 'jsmith': (1) Login at 3 AM (outside normal hours), (2) Access to HR file share (outside jsmith's role), (3) Large data transfer to external IP, (4) VPN login from unusual country. Analyze these events, determine the likely scenario, and describe your incident response steps.

Answer: Analysis: This pattern strongly suggests a compromised account being used for data exfiltration. Events indicate: (1) Off-hours login = avoiding detection during low-staffing periods. (2) HR file access = lateral movement to sensitive data outside user's normal role. (3) Large external transfer = data exfiltration. (4) Foreign VPN = attacker operating from outside the country. Response: (1) Immediately disable jsmith's account and active sessions. (2) Block the external IP at the firewall. (3) Preserve all SIEM logs as evidence. (4) Contact jsmith directly to verify if activity was legitimate. (5) Analyze the data transferred to determine scope of exposure. (6) Check for persistence mechanisms (new scheduled tasks, modified startup scripts). (7) Review jsmith's access history for the past 30 days. (8) Initiate incident response plan. (9) Determine if the account was compromised via phishing, credential stuffing, or other means.

PBQ2. SCENARIO: Implement an IAM strategy for a company migrating to cloud. Define: (1) Authentication approach (SSO protocol choice and justification), (2) MFA implementation, (3) Access control model, (4) Privileged access management, (5) Account lifecycle (provisioning to decommissioning).

Answer: (1) SSO via SAML 2.0 with a cloud IdP (Okta/Azure AD) — SAML provides enterprise SSO across web applications with federation. OAuth 2.0 for API access. (2) MFA: FIDO2 security keys for admins (phishing-resistant), authenticator app (TOTP) for regular users, number-matching push (not simple approve). (3) RBAC with ABAC enhancements — base roles defined per job function, attribute-based conditions for sensitive data (location, device trust, time). (4) PAM: JIT permissions (admin rights granted only when needed, auto-revoked), password vaulting for service accounts (CyberArk/BeyondTrust), ephemeral credentials for cloud access. (5) Lifecycle: automated provisioning from HR system (hire → account creation with role), quarterly access reviews, automated deprovisioning on termination (revoke within 1 hour of HR notification), annual certification of all access.

WEEKLY CHALLENGE

Set up a complete Wazuh SIEM deployment (https://wazuh.com/) with at least 2 agents (Kali + Ubuntu target). Configure custom rules to detect: (1) SSH brute force, (2) File integrity changes in /etc/, (3) New user account creation, (4) Rootkit detection. Create a dashboard showing all alerts and write a SOC analyst playbook for responding to each alert type.

WEEK 9

Incident Response, Forensics & Automation

SY0-701 Objectives: 4.6: Given a scenario, modify enterprise capabilities to enhance security | 4.7: Explain the importance of automation and orchestration related to secure operations | 4.8: Explain appropriate incident response activities | 4.9: Given a scenario, use data sources to support an investigation

PURPLE TEAM FRAMING

Incident response is where the purple team philosophy comes full circle. We study real breaches from both the attacker's and responder's perspectives. Students develop IR playbooks, then test them against simulated attacks. Forensic analysis reveals how attackers cover their tracks — and how defenders can still find evidence. Automation isn't just about efficiency; it's about ensuring consistent response when humans are stressed and sleep-deprived during a real incident.

Learning Objectives

1. Execute the complete incident response lifecycle: preparation, detection, analysis, containment, eradication, recovery, lessons learned
2. Apply digital forensics procedures: legal hold, chain of custody, acquisition, preservation, e-discovery
3. Identify and use investigation data sources: firewall logs, application logs, endpoint logs, packet captures
4. Explain automation and orchestration benefits: efficiency, baseline enforcement, scaling, reaction time
5. Develop incident response playbooks and conduct tabletop exercises
6. Perform basic forensic analysis using Autopsy and log analysis with ELK

Lecture Topics

- Incident Response Process:
  - Preparation: IR plans, team formation, communication procedures, tools readiness
  - Detection: monitoring, alerting, user reports, threat intelligence
  - Analysis: triage, severity classification, scope determination
  - Containment: short-term (isolate) and long-term (temporary fix)
  - Eradication: remove threat actor presence, patch vulnerabilities, reset credentials
  - Recovery: restore systems, verify integrity, return to operations
  - Lessons learned: post-incident review, IR plan updates, security improvements
- IR Training and Testing:
  - Tabletop exercises: walkthrough scenarios without hands-on
  - Simulations: controlled exercises in production-like environments
  - Root cause analysis: finding the true origin, not just symptoms

- Threat Hunting:
  - Proactive search for threats that evade automated detection
  - Hypothesis-driven hunting, IoC-based hunting, behavior-based hunting
- Digital Forensics:
  - Legal hold: preserving relevant data for potential legal proceedings
  - Chain of custody: documenting evidence handling from collection to court
  - Acquisition: forensic imaging (bit-for-bit copy), write blockers
  - Preservation: evidence integrity, hashing for verification
  - Reporting: documenting findings for legal and technical audiences
  - E-discovery: identifying and collecting electronically stored information
- Investigation Data Sources:
  - Log data: firewall, application, endpoint, OS security, IPS/IDS, network logs, metadata
  - Other sources: vulnerability scans, automated reports, dashboards, packet captures (PCAP)
- Automation and Orchestration:
  - Use cases: user provisioning, resource provisioning, guard rails, security groups, ticket creation, escalation, enabling/disabling services
  - CI/CD integration and API-based automation
  - Benefits: efficiency, baseline enforcement, standard configs, secure scaling, reaction time
  - Considerations: complexity, cost, single point of failure, technical debt, supportability
  - SOAR platforms: Security Orchestration, Automation, and Response overview
- Security Scripting (Intro):
  - Python basics for security: parsing logs, automating scans, API integration
  - Bash scripting: automating system checks, alerting

Official Sources

[OFFICIAL] NIST SP 800-61 Rev. 2 — Computer Security Incident Handling Guide
https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

[OFFICIAL] NIST SP 800-86 — Guide to Integrating Forensic Techniques
https://csrc.nist.gov/publications/detail/sp/800-86/final

[OFFICIAL] SANS Incident Response Process (PICERL)
https://www.sans.org/incident-response/

[OFFICIAL] MITRE ATT&CK — Collection and Exfiltration Tactics
https://attack.mitre.org/tactics/TA0009/

[OFFICIAL] CISA — Incident Response Playbooks
https://www.cisa.gov/incident-response-playbooks

Underground / Bleeding Edge Sources

[UNDERGROUND] 13Cubed (YouTube) — 'Digital Forensics with Autopsy' complete tutorial series

[UNDERGROUND] John Hammond — 'Incident Response: Real World Scenarios' video

[UNDERGROUND] r/computerforensics — 'Getting started with DFIR' resource compilation

[UNDERGROUND] DFIR Diva blog — practical forensics walkthroughs and case studies

[UNDERGROUND] DEF CON DFIR Village — annual forensics challenges and talks

[UNDERGROUND] TheCyberMentor — 'Python for Cybersecurity' scripting tutorials

CASE STUDY: Sony Pictures (2014) vs. Norsk Hydro (2019) — IR Failures and Gold Standard Response

Sony Pictures (2014) — IR Failure: In November 2014, the 'Guardians of Peace' (attributed to North Korea's Lazarus Group) devastated Sony Pictures Entertainment. The attack wiped hard drives across the network, leaked unreleased films, exposed employee personal data, salary information, embarrassing executive emails, and confidential business plans. Sony's incident response was widely criticized.

What went wrong in the response: (1) Sony had no effective incident response plan — their reaction was chaotic and slow. (2) Communication was poor: employees learned about the breach from news media before internal notification. (3) The company initially tried to contain media coverage rather than contain the breach. (4) Forensic investigation was hampered because the attackers had destroyed evidence on compromised systems. (5) There was no established chain of custody for digital evidence. (6) The company's backup and recovery capabilities were insufficient — staff resorted to using paper and pencil.

Norsk Hydro (2019) — Gold Standard Response: In March 2019, Norwegian aluminum manufacturer Norsk Hydro was hit by LockerGoga ransomware. The attack encrypted systems across 170 sites in 40 countries. Unlike many victims, Norsk Hydro's response is studied as a model of excellence.

What they did right: (1) They refused to pay the ransom — a principled decision supported by robust backups. (2) They immediately switched to manual operations at aluminum plants, keeping production running. (3) They were radically transparent: daily press conferences, public website updates, and a YouTube channel documenting the recovery process. (4) They had practiced incident response procedures and had an IR retainer with external forensics firms. (5) Their IT team worked methodically: isolating affected systems, rebuilding from known-good backups, and verifying integrity before reconnecting. (6) Total recovery took several weeks, but the company estimated losses at $71 million — compared to their resilience, this was manageable.

The CrowdStrike/Falcon Incident (2024): In July 2024, a faulty CrowdStrike Falcon sensor update caused millions of Windows systems worldwide to enter BSOD boot loops. While not a cyberattack, it became one of the largest IT incidents in history, grounding flights, disrupting hospitals, and taking financial systems offline. It demonstrated how security tools themselves can become single points of failure, and why update testing, rollback procedures, and resilience planning are critical.

Lessons learned: (1) IR planning and practice (tabletop exercises) separate good responses from catastrophic ones. (2) Transparency during incidents builds trust — trying to hide a breach always makes it worse. (3) Backups are the #1 defense against ransomware — but only if they're tested and offline/immutable. (4) Manual fallback procedures keep operations running during digital outages. (5) Security tools must be tested as rigorously as the systems they protect.

HANDS-ON LAB: Incident Response Tabletop & Forensic Analysis

Objective

Conduct an IR tabletop exercise based on a ransomware scenario, then perform forensic analysis on a disk image using Autopsy.

Tools Required

Autopsy (free), ELK Stack or grep/awk for log analysis, IR playbook template

Step-by-Step Instructions

PART A — IR Tabletop Exercise:

SCENARIO: At 6 AM Monday, your SOC receives alerts: 5 workstations showing file encryption activity, one server unreachable, a ransom note found on affected machines

3. Document your response for each IR phase:
4. Preparation: What IR resources do you need? Who do you call first?
5. Detection: What additional data do you collect? What logs do you check?
6. Analysis: How do you determine scope? What IoCs do you search for?
7. Containment: What systems do you isolate? How do you prevent spread?
8. Eradication: How do you remove the ransomware? What do you patch?
9. Recovery: How do you restore from backups? In what order?
10. Lessons Learned: What changes would prevent recurrence?
11. Write up your complete response as an IR report

PART B — Forensic Analysis:

13. Download Autopsy from https://www.autopsy.com/ (pre-installed on some Kali builds)
14. Download a practice forensic image (e.g., from https://cfreds.nist.gov/ or https://digitalcorpora.org/)
15. Create a new Autopsy case: provide case number, examiner name
16. Add the forensic image as a data source
17. Run ingest modules: hash lookup, keyword search, recent activity, web artifacts
18. Investigate: look for recently accessed files, deleted files, browser history, email artifacts
19. Document findings: timeline of activity, evidence of suspicious behavior, recovered deleted files
20. Create a forensic report: chain of custody documentation, findings, evidence hashes, conclusions

PART C — Log Analysis Challenge:

22. Download sample security logs (auth.log, apache access.log) or use your lab VM logs
23. Use grep/awk to identify: failed login attempts, successful brute force, suspicious user agents, SQL injection attempts in web logs
24. Create a timeline of attacker activity from log correlation

Expected Outcomes

A complete IR report for the tabletop scenario following NIST IR framework. Forensic analysis findings from a practice disk image with proper chain of custody documentation. Log analysis identifying attacker activity patterns.

Purple Team Debrief

As an ATTACKER: understanding IR procedures helps you anticipate defender response and design attacks that are harder to detect and respond to (e.g., destroying logs, anti-forensics). As a DEFENDER: practicing IR through tabletop exercises builds muscle memory for real incidents. Forensic analysis skills help you understand the full scope of a breach and prevent the attacker from maintaining persistence.

Key Terms & Definitions

Incident Response

The organized approach to addressing and managing the aftermath of a security breach or cyberattack

Chain of Custody
A chronological documentation trail showing the collection, transfer, and handling of digital evidence

Legal Hold
A process that requires an organization to preserve all forms of relevant information when litigation is reasonably anticipated

E-Discovery
The process of identifying, collecting, and producing electronically stored information in response to legal proceedings

SOAR
Security Orchestration, Automation, and Response — platforms that automate incident response workflows

Forensic Image
A bit-for-bit copy of a storage device that preserves all data including deleted files and slack space

Write Blocker
A hardware or software tool that prevents any writes to a storage device during forensic acquisition

Threat Hunting
The proactive search for cyber threats that are present in a network but have not been detected by automated security tools

Root Cause Analysis
A systematic process for identifying the fundamental cause of an incident, not just the symptoms

PICERL
Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned — the SANS IR framework

Tabletop Exercise
A discussion-based IR exercise where participants walk through a simulated incident scenario without hands-on activity

IOC
Indicator of Compromise — artifacts observed on a network or system that indicate a potential security breach

Volatile Data
Data that exists only in RAM or system state and is lost when the system is powered off (must be collected first in forensics)

PCAP
Packet Capture — a file containing recorded network traffic for analysis

Guard Rails
Automated constraints that prevent users or systems from making configurations that violate security policies

Technical Debt
The implied cost of future rework caused by choosing quick-fix solutions over more robust approaches

Practice Questions — Multiple Choice

Q1. During incident response, what is the FIRST action after detecting a confirmed ransomware infection on a workstation?

A. Pay the ransom

B. Wipe and reimage the machine

C. Isolate the affected system from the network

D. Begin forensic imaging

Answer: C — Containment (isolation) is the immediate priority to prevent the ransomware from spreading to other systems. Forensic imaging follows after containment.

Q2. A forensic investigator needs to collect evidence from a running system. Which type of data should be collected FIRST?

A. Hard drive contents

B. Network logs

C. Volatile memory (RAM)

D. Email archives

Answer: C — Volatile data (RAM) must be collected first because it's lost when the system is powered off. The order of volatility: registers → cache → RAM → disk → removable media → remote logs.

Q3. Which automation benefit DIRECTLY addresses the challenge of maintaining consistent security configurations across thousands of servers?

A. Employee retention

B. Enforcing baselines

C. Workforce multiplier

D. Reaction time

Answer: B — Enforcing baselines through automation ensures every server maintains the same security configuration, eliminating configuration drift across large environments.

Q4. After resolving a security incident, the security team conducts a meeting to discuss what happened, what worked, and what needs improvement. This is the:

A. Root cause analysis

B. Tabletop exercise

C. Lessons learned phase

D. Threat hunting session

Answer: C — The lessons learned phase (post-incident review) occurs after recovery, analyzing the incident and response to improve future procedures.

Q5. Which data source would be MOST useful for investigating suspected data exfiltration over the network?

A. Endpoint logs

B. Packet captures (PCAP)

C. Vulnerability scan results

D. Application logs

Answer: B — Packet captures record all network traffic content, providing the most detailed view of what data left the network, to where, and via what protocol.

Practice Questions — Performance-Based (PBQ)

PBQ1. SCENARIO: You are the IR lead. A ransomware attack has encrypted 30% of your file servers. The ransom demand is $500,000 in Bitcoin. Your CEO asks for your recommendation. Create a complete IR brief covering: (1) Should we pay? (2) What are our recovery options? (3) What's the timeline? (4) What do we communicate externally?

Answer: (1) Recommendation: Do NOT pay. Reasons: no guarantee of decryption, funds criminal operations, may violate OFAC sanctions if attacker is sanctioned entity, paying doesn't address root cause. (2) Recovery options: restore from last known-good backups (verify integrity first), rebuild compromised systems from gold images, prioritize systems by business criticality. If no viable backups exist, consult with specialized decryption services (NoMoreRansom.org). (3) Timeline: 24-48 hours for containment and assessment, 3-5 days for critical system recovery, 2-4 weeks for full recovery. (4) External communications: notify law enforcement (FBI IC3), engage legal counsel for regulatory notification requirements, prepare customer communication if PII is involved, issue public statement acknowledging the incident and response steps. Do NOT reveal technical details that could help the attacker.

PBQ2. SCENARIO: Create a Python script that automates basic log analysis. The script should: (1) Read an auth.log file, (2) Identify all failed SSH login attempts, (3) Count attempts per source IP, (4) Flag IPs with more than 5 failures, (5) Output a simple report. Write the script and explain each section.

Answer: ```python import re from collections import Counter def analyze_auth_log(filepath): failed_pattern = re.compile(r'Failed password.*from (\d+\.\d+\.\d+\.\d+)') failed_ips = Counter() with open(filepath) as f: for line in f: match = failed_pattern.search(line) if match: failed_ips[match.group(1)] += 1 print('=== SSH Brute Force Detection Report ===') print(f'Total unique source IPs with failures: {len(failed_ips)}') print(f'Total failed attempts: {sum(failed_ips.values())}') print('\n--- FLAGGED IPs (>5 failures) ---') for ip, count in failed_ips.most_common(): if count > 5: print(f' [ALERT] {ip}: {count} failed attempts') analyze_auth_log('/var/log/auth.log') ``` Explanation: regex extracts IPs from failed password lines, Counter tallies per-IP, threshold of 5 flags potential brute force. This is a foundation for automated security monitoring.

WEEKLY CHALLENGE

Develop a complete Incident Response Playbook for ransomware. Include: (1) Detection criteria and SIEM alert rules, (2) Severity classification matrix, (3) Step-by-step response procedures for each IR phase, (4) Communication templates (internal, executive, legal, customer, media), (5) Recovery checklists, (6) Post-incident review template. Then conduct a tabletop exercise with a friend/colleague using your playbook — document what worked and what needs revision.

WEEK 10

GRC, Compliance & Exam Domination

SY0-701 Objectives: 5.1: Summarize elements of effective security governance | 5.2: Explain elements of the risk management process | 5.3: Explain the processes associated with third-party risk assessment and management | 5.4: Summarize elements of effective security compliance | 5.5: Explain types and purposes of audits and assessments | 5.6: Given a scenario, implement security awareness practices

PURPLE TEAM FRAMING

GRC might sound dry, but it's the strategic layer that directs all tactical security operations. From the attacker's perspective, compliance gaps are attack vectors — organizations that fail audits often have the same vulnerabilities that attackers exploit. From the defender's perspective, GRC frameworks provide the structure to justify budgets, prioritize investments, and measure security posture. This week, we build a security program from scratch and then run a mock penetration test against it.

Learning Objectives

1. Explain governance structures, policies, standards, and procedures for security programs
2. Apply risk management concepts: risk identification, assessment (qualitative/quantitative), SLE, ALE, ARO, risk register
3. Evaluate third-party risk through vendor assessments, due diligence, and agreement types (SLA, MOA, MOU, NDA, BPA)
4. Understand compliance frameworks: regulatory, legal, industry standards — and consequences of non-compliance
5. Differentiate audit types: internal, external, regulatory, self-assessment, penetration testing
6. Design and implement security awareness programs: phishing campaigns, user training, anomalous behavior recognition
7. Develop comprehensive exam preparation strategy for SY0-701

Lecture Topics

- Security Governance:
  - Policies: AUP, information security, business continuity, DR, IR, SDLC, change management
  - Standards: password, access control, physical security, encryption
  - Procedures: change management, onboarding/offboarding, playbooks
  - Guidelines: advisory documents, best practice recommendations
  - Governance structures: boards, committees, centralized vs decentralized
  - Roles: data owners, controllers, processors, custodians/stewards
  - External considerations: regulatory, legal, industry, local/regional/national/global
- Risk Management:
  - Risk identification and risk register maintenance

  - Risk assessment: ad hoc, recurring, one-time, continuous
  - Qualitative vs quantitative analysis
  - Quantitative metrics: SLE, ALE, ARO, probability, likelihood, exposure factor, impact
  - Risk tolerance, appetite: expansionary, conservative, neutral
  - Risk strategies: transfer (insurance), accept, avoid, mitigate
  - Business Impact Analysis: RTO, RPO, MTTR, MTBF
- Third-Party Risk Management:
  - Vendor assessment: pen testing, right-to-audit, internal audits, independent assessments, supply chain analysis
  - Vendor selection: due diligence, conflict of interest
  - Agreement types: SLA, MOA, MOU, MSA, WO/SOW, NDA, BPA
  - Vendor monitoring and questionnaires
- Compliance:
  - Compliance reporting: internal and external
  - Consequences: fines, sanctions, reputational damage, license loss, contractual impacts
  - Compliance monitoring: due diligence/care, attestation, automation
  - Privacy: GDPR, CCPA, data subjects, controllers/processors, right to be forgotten
  - Frameworks: SOC 2, ISO 27001, NIST 800-171, PCI-DSS, HIPAA
- Audits and Assessments:
  - Internal: compliance, audit committee, self-assessments
  - External: regulatory, examinations, independent third-party
  - Penetration testing: physical, offensive, defensive, integrated, known/partially known/unknown environment
  - Reconnaissance: passive and active
- Security Awareness:
  - Phishing campaigns and simulations
  - User training: policy/handbooks, situational awareness, insider threat, password management, social engineering, OpSec, remote work
  - Anomalous behavior recognition: risky, unexpected, unintentional
  - Reporting and monitoring programs
- EXAM PREPARATION:
  - SY0-701 exam format: 90 questions, 90 minutes, passing ~750/900
  - Question types: multiple choice and performance-based (PBQ)
  - Study strategies, time management, PBQ approach
  - Domain weight allocation and study prioritization

Official Sources

[OFFICIAL] NIST Risk Management Framework (RMF)
https://csrc.nist.gov/projects/risk-management/about-rmf

[OFFICIAL] NIST SP 800-171 Rev. 3 — Protecting CUI in Nonfederal Systems
https://csrc.nist.gov/publications/detail/sp/800-171/rev-3/final

[OFFICIAL] ISO 27001 Information Security Management (overview)
https://www.iso.org/isoiec-27001-information-security.html

[OFFICIAL] CompTIA Security+ SY0-701 Exam Objectives
https://www.comptia.org/certifications/security

[OFFICIAL] GDPR Official Text
https://gdpr.eu/

Underground / Bleeding Edge Sources

[UNDERGROUND] Professor Messer — 'CompTIA Security+ SY0-701 Course' (free on YouTube, full course)
[UNDERGROUND] r/CompTIA — 'I passed SY0-701! Here's how' success story threads
[UNDERGROUND] Jason Dion — Security+ practice exams and study tips (YouTube)
[UNDERGROUND] r/cybersecurity — 'Compliance is not security' debate threads
[UNDERGROUND] DEF CON Policy Village — talks on bridging the gap between security and governance
[UNDERGROUND] Black Hills Information Security (YouTube) — GRC from a pen tester's perspective

CASE STUDY: GDPR Mega-Fines & The SEC Cyber Disclosure Rules

GDPR Enforcement Actions: Since the EU's General Data Protection Regulation took effect in May 2018, regulators have imposed billions in fines. Meta (Facebook) received a record €1.2 billion fine in 2023 for transferring EU user data to the US without adequate protections. Amazon was fined €746 million in 2021 for processing personal data without proper consent. These fines demonstrate that compliance failures have massive financial consequences.

The Anthem Breach (2015) and Compliance Failure: Anthem, the second-largest US health insurer, suffered a breach exposing 78.8 million records including SSNs, medical IDs, and employment information. Investigation revealed multiple compliance failures: PHI was stored unencrypted (violating HIPAA best practices), there was no security monitoring on the compromised database, and access controls were insufficient. Anthem paid $115 million in settlement — the largest data breach settlement at the time. Additional HHS HIPAA penalty: $16 million.

SEC Cyber Disclosure Rules (2023): The U.S. Securities and Exchange Commission adopted new rules in July 2023 requiring public companies to disclose material cybersecurity incidents within four business days of determining materiality. Companies must also describe their processes for assessing, identifying, and managing cybersecurity risks in annual reports. This fundamentally changes how organizations treat cybersecurity — it's now a board-level and investor concern, not just an IT issue.

Impact: SolarWinds' CISO Timothy Brown was charged by the SEC for misleading investors about the company's cybersecurity practices prior to the breach. This was groundbreaking — personal liability for security executives who misrepresent their organization's security posture.

Lessons learned: (1) Compliance is the floor, not the ceiling — meeting minimum requirements doesn't mean you're secure. (2) Data privacy regulations have real financial teeth — GDPR fines can reach 4% of global annual revenue. (3) Healthcare data requires encryption and access controls (HIPAA). (4) Cybersecurity is now a board-level and regulatory concern. (5) Personal liability for security leaders is becoming real — misrepresenting security posture can result in SEC charges. (6) Third-party risk management is essential — many compliance failures trace back to vendor relationships.

HANDS-ON LAB: Risk Assessment & Mock Exam

Objective

Conduct a formal risk assessment using NIST RMF methodology and complete a timed mock Security+ exam to prepare for certification.

Tools Required

NIST RMF documentation (free), risk assessment template, practice exam questions

Step-by-Step Instructions

PART A — Risk Assessment Exercise:

2. Choose a scenario: a small healthcare clinic with 50 employees, patient records, and a public-facing website
3. Step 1 — Categorize: identify information systems and classify data (PHI = High Confidentiality/Integrity)
4. Step 2 — Select Controls: using NIST 800-53, select appropriate security controls for the system categorization
5. Step 3 — Implement: describe how each selected control would be implemented
6. Step 4 — Assess: identify gaps between current state and required controls
7. Step 5 — Authorize: prepare a risk-based decision document for the clinic director
8. Step 6 — Monitor: define ongoing monitoring procedures
9. Calculate quantitative risk for one scenario:
10. Asset: Patient database. AV (Asset Value) = $500,000
11. Threat: Ransomware. EF (Exposure Factor) = 80%
12. SLE = AV × EF = $400,000
13. ARO (Annualized Rate of Occurrence) = 0.5 (once every 2 years)
14. ALE = SLE × ARO = $200,000
15. Use ALE to justify security investment: if a $50,000/year solution reduces risk by 90%, the ROI is clear
16. Create a Risk Register with at least 10 risks, rated by likelihood and impact

PART B — Timed Mock Exam:

18. Set a 90-minute timer
19. Complete all practice questions from Weeks 1-10 (PBQs first, then MC)
20. Score yourself and identify weak domains
21. Create a targeted study plan for your weakest areas
22. Review every question you got wrong — understand WHY the correct answer is correct

Expected Outcomes

A complete risk assessment document for the healthcare clinic using NIST RMF. A quantitative risk analysis with ROI justification for security investment. Mock exam results with a personalized study plan targeting weak areas.

Purple Team Debrief

As an ATTACKER: compliance gaps are your reconnaissance gold. Organizations that fail audits often have exploitable vulnerabilities. Healthcare targets are especially lucrative because PHI sells for more than credit card numbers on the dark web. As a DEFENDER: GRC provides the strategic framework to prioritize security investments, justify budgets to leadership, and build a sustainable security program. The risk assessment exercise teaches you to speak the language of business — not just security.

Key Terms & Definitions

GRC

Governance, Risk, and Compliance — the integrated framework for aligning IT with business objectives, managing risk, and meeting regulatory requirements

SLE
Single Loss Expectancy — the expected monetary loss from a single occurrence of a risk event (AV × EF)

ALE
Annualized Loss Expectancy — the expected yearly monetary loss from a risk (SLE × ARO)

ARO
Annualized Rate of Occurrence — the estimated frequency with which a risk event occurs per year

Risk Register
A documented list of identified risks with their assessment, owner, and treatment plan

Risk Appetite
An organization's willingness to accept risk in pursuit of its objectives (expansionary, conservative, neutral)

SLA
Service Level Agreement — a contract defining the expected level of service between a provider and customer

MOU
Memorandum of Understanding — a non-binding agreement outlining terms and intentions between parties

NDA
Non-Disclosure Agreement — a legal contract preventing parties from sharing confidential information

BPA
Business Partners Agreement — a legal arrangement that defines the relationship, responsibilities, and liabilities between business partners

Due Diligence
The research and analysis conducted before entering into an agreement to ensure informed decision-making

GDPR
General Data Protection Regulation — EU regulation governing personal data protection, with fines up to 4% of global annual revenue

PCI-DSS
Payment Card Industry Data Security Standard — security standard for organizations handling credit card data

HIPAA
Health Insurance Portability and Accountability Act — US law protecting the privacy and security of health information

SOC 2
Service Organization Control 2 — an auditing standard measuring a service organization's controls for security, availability, processing integrity, confidentiality, and privacy

Penetration Testing
An authorized simulated cyberattack performed to evaluate the security of a system or network

Risk Transference
Shifting the financial burden of a risk to another party, typically through insurance or contractual agreements

Practice Questions — Multiple Choice

Q1. An organization calculates: Asset Value = $1,000,000, Exposure Factor = 50%, ARO = 0.2. What is the ALE?

A. $100,000

B. $200,000

C. $500,000

D. $1,000,000

Answer: A — SLE = AV × EF = $1,000,000 × 0.50 = $500,000. ALE = SLE × ARO = $500,000 × 0.2 = $100,000.

Q2. A company discovers a vendor has access to customer data without a formal agreement in place. Which agreement should be established FIRST?

A. SLA

B. NDA

C. BPA

D. MOU

Answer: B — An NDA should be established first to legally prevent the vendor from disclosing or misusing the customer data. SLAs and other agreements can follow.

Q3. A European company collects personal data from EU citizens and stores it on US servers. Under GDPR, the company must:

A. Delete all data immediately

B. Ensure adequate data protection standards for cross-border transfers

C. Only store data on paper

D. Get approval from each EU member state

Answer: B — GDPR requires that cross-border data transfers maintain adequate protection standards, typically through Standard Contractual Clauses, BCRs, or adequacy decisions.

Q4. A penetration test is conducted where the testers have no prior knowledge of the target environment. This is a:

A. Known environment test

B. Partially known environment test

C. Unknown environment test

D. Integrated test

Answer: C — Unknown environment (formerly 'black box') testing simulates a real attacker with no prior knowledge of the target's infrastructure.

Q5. An employee repeatedly clicks on phishing simulation emails despite training. The security team's BEST response is:

A. Terminate the employee

B. Restrict the employee's email access

C. Provide additional targeted training and coaching

D. Implement email allow listing

Answer: C — Security awareness is about behavior change through education. Additional targeted training addresses the specific knowledge gap. Punitive measures create a culture of fear, not security.

Practice Questions — Performance-Based (PBQ)

PBQ1. SCENARIO: You are building a security program from scratch for a startup. Create a comprehensive governance framework including: (1) Three critical policies to establish first, (2) Risk management approach, (3) Compliance requirements for a SaaS company handling customer data, (4) Third-party risk management process, (5) Security awareness program.

Answer: (1) Critical policies: (a) Information Security Policy — overarching policy defining security objectives, roles, responsibilities. (b) Acceptable Use Policy — employee expectations for using company resources. (c) Incident Response Policy — procedures for detecting, responding to, and recovering from incidents. (2) Risk management: adopt NIST RMF, establish risk register, quarterly risk assessments, define risk appetite (likely conservative as a startup), identify top risks (data breach, insider threat, supply chain), calculate ALE for top risks. (3) Compliance: SOC 2 Type II (required by enterprise customers), GDPR if handling EU data, potentially CCPA. Start with SOC 2 readiness assessment. (4) Third-party risk: vendor questionnaire for all SaaS tools, require SOC 2 reports from critical vendors, NDA before sharing any data, annual vendor reviews, right-to-audit clauses in contracts. (5) Awareness: onboarding security training, monthly phishing simulations, quarterly security awareness sessions, reporting mechanism for suspicious activity, gamification (leaderboard, rewards for reporting phishing).

PBQ2. SCENARIO: Calculate the ROI of a proposed security investment. Current state: ransomware ALE = $400,000/year. Proposed solution: advanced EDR + backup improvements costing $120,000/year, estimated to reduce ransomware risk by 85%. Should the company invest? Show your work and present the business case.

Answer: Current ALE = $400,000/year. Proposed solution cost = $120,000/year. Risk reduction = 85%. New ALE = $400,000 × (1 - 0.85) = $60,000/year. Annual savings = $400,000 - $60,000 = $340,000. ROI = (Annual savings - Solution cost) / Solution cost = ($340,000 - $120,000) / $120,000 = 183%. Net annual benefit = $340,000 - $120,000 = $220,000. Recommendation: INVEST. The solution pays for itself 2.8x over. Beyond financial ROI, consider: reduced business disruption, regulatory compliance improvement, customer trust, and reputational protection. Present to leadership with: 'For every dollar spent, we save $2.83 in expected losses, plus immeasurable benefits to business continuity and reputation.'

WEEKLY CHALLENGE

Build a complete 'Security Program in a Box' for a fictional company: (1) Write an Information Security Policy (2-3 pages), (2) Create a Risk Register with 15+ risks, (3) Design a vendor assessment questionnaire (20+ questions), (4) Build a 12-month security awareness training calendar, (5) Write an executive security brief summarizing the company's security posture for the board. This is your capstone project — it synthesizes everything from the entire course.

Appendix A: Complete SY0-701 Exam Objectives Checklist

Use this checklist to track your mastery of each exam objective. Mark each objective as you study and review it.

Domain 1.0 — General Security Concepts (12%)

- [ ] 1.1 — Compare and contrast various types of security controls
- [ ] 1.2 — Summarize fundamental security concepts
- [ ] 1.3 — Explain the importance of change management processes and the impact to security
- [ ] 1.4 — Explain the importance of using appropriate cryptographic solutions

Domain 2.0 — Threats, Vulnerabilities, and Mitigations (22%)

- [ ] 2.1 — Compare and contrast common threat actors and motivations
- [ ] 2.2 — Explain common threat vectors and attack surfaces
- [ ] 2.3 — Explain various types of vulnerabilities
- [ ] 2.4 — Given a scenario, analyze indicators of malicious activity
- [ ] 2.5 — Explain the purpose of mitigation techniques used to secure the enterprise

Domain 3.0 — Security Architecture (18%)

- [ ] 3.1 — Compare and contrast security implications of different architecture models
- [ ] 3.2 — Given a scenario, apply security principles to secure enterprise infrastructure
- [ ] 3.3 — Compare and contrast concepts and strategies to protect data
- [ ] 3.4 — Explain the importance of resilience and recovery in security architecture

Domain 4.0 — Security Operations (28%)

- [ ] 4.1 — Given a scenario, apply common security techniques to computing resources
- [ ] 4.2 — Explain the security implications of proper hardware, software, and data asset management
- [ ] 4.3 — Explain various activities associated with vulnerability management
- [ ] 4.4 — Explain security alerting and monitoring concepts and tools
- [ ] 4.5 — Given a scenario, implement and maintain identity and access management
- [ ] 4.6 — Given a scenario, modify enterprise capabilities to enhance security
- [ ] 4.7 — Explain the importance of automation and orchestration related to secure operations
- [ ] 4.8 — Explain appropriate incident response activities
- [ ] 4.9 — Given a scenario, use data sources to support an investigation

Domain 5.0 — Security Program Management and Oversight (20%)

- [ ] 5.1 — Summarize elements of effective security governance
- [ ] 5.2 — Explain elements of the risk management process
- [ ] 5.3 — Explain the processes associated with third-party risk assessment and management
- [ ] 5.4 — Summarize elements of effective security compliance
- [ ] 5.5 — Explain types and purposes of audits and assessments
- [ ] 5.6 — Given a scenario, implement security awareness practices

Appendix B: Recommended Free Tools List

All tools listed below are free for personal/educational use. Download links are current as of publication.

Tool	Description	Download URL
VirtualBox	Virtualization platform	https://www.virtualbox.org/
Kali Linux	Penetration testing OS	https://www.kali.org/
Nmap	Network scanner	https://nmap.org/
Wireshark	Packet analyzer	https://www.wireshark.org/
Burp Suite Community	Web app security testing	https://portswigger.net/burp/communitydownload
Metasploit Framework	Exploitation framework	https://www.metasploit.com/
Hashcat	Password recovery	https://hashcat.net/hashcat/
John the Ripper	Password cracker	https://www.openwall.com/john/
DVWA	Damn Vulnerable Web App	https://github.com/digininja/DVWA
Maltego CE	OSINT and recon	https://www.maltego.com/ce/
theHarvester	Email/subdomain OSINT	https://github.com/laramies/theHarvester
Autopsy	Digital forensics	https://www.autopsy.com/
Splunk Free	SIEM (up to 500MB/day)	https://www.splunk.com/en_us/download.html
Wazuh	Open-source SIEM/XDR	https://wazuh.com/
pfSense	Firewall/router	https://www.pfsense.org/
Snort	IDS/IPS	https://www.snort.org/
Suricata	IDS/IPS	https://suricata.io/
WireGuard	VPN	https://www.wireguard.com/
OpenSSL	Crypto toolkit	https://www.openssl.org/
ScoutSuite	Cloud security auditing	https://github.com/nccgroup/ScoutSuite
BloodHound	AD attack path mapping	https://github.com/BloodHoundAD/BloodHound
Any.Run	Interactive malware sandbox	https://any.run/
REMnux	Malware analysis distro	https://remnux.org/
Nessus Essentials	Vulnerability scanner (free)	https://www.tenable.com/products/nessus/nessus-essentials
CyberChef	Data transformation tool	https://gchq.github.io/CyberChef/

Shodan	Internet device search	https://www.shodan.io/
ELK Stack	Log management	https://www.elastic.co/elastic-stack
SET (Social Engineering Toolkit)	Social engineering	https://github.com/trustedsec/social-engineer-toolkit

Appendix C: Exam Day Strategy Guide

EXAM FORMAT: The CompTIA Security+ SY0-701 exam consists of a maximum of 90 questions to be completed in 90 minutes. The passing score is 750 on a scale of 100-900. Questions include both multiple choice (single and multiple answer) and performance-based questions (PBQs).

Test-Taking Tactics

- 1. PBQ Strategy: PBQs appear first. If a PBQ is complex, FLAG IT and move on. Return after completing all multiple-choice questions. PBQs are worth more but shouldn't eat all your time.
- 2. Time Management: You have exactly 1 minute per question on average. Spend no more than 90 seconds on any single MC question. If stuck, flag it and move on.
- 3. Elimination Method: Even if you don't know the answer, eliminate obviously wrong choices. Going from 4 options to 2 gives you a 50% chance.
- 4. Read the ENTIRE question: CompTIA loves 'BEST' and 'MOST' qualifiers. Multiple answers may be technically correct, but one is BEST.
- 5. Domain Weighting Study Strategy:

- Domain 4 (Security Operations) = 28% — study this the MOST

- Domain 2 (Threats/Vulnerabilities) = 22% — second priority

- Domain 5 (GRC) = 20% — third priority

- Domain 3 (Security Architecture) = 18% — fourth priority

- Domain 1 (General Concepts) = 12% — foundational, usually easiest

- 6. Acronym Mastery: Make flashcards for ALL acronyms. The exam loves testing acronym knowledge.
- 7. Know Your Ports: Common ports (22-SSH, 23-Telnet, 25-SMTP, 53-DNS, 80-HTTP, 443-HTTPS, 3389-RDP, etc.) appear frequently.
- 8. Scenario Practice: Many questions are scenario-based. Practice identifying the KEY requirement in each scenario.
- 9. Don't Overthink: If an answer seems obviously correct, it probably is. CompTIA isn't trying to trick you — they're testing knowledge.
- 10. Review Flagged Questions: Use remaining time to review flagged questions. Change answers ONLY if you have a clear reason.

Common Port Numbers to Memorize

Port	Service	Protocol
20/21	FTP (Data/Control)	TCP
22	SSH / SFTP / SCP	TCP
23	Telnet (insecure)	TCP
25	SMTP (email sending)	TCP

53	DNS	TCP/UDP
67/68	DHCP (Server/Client)	UDP
80	HTTP	TCP
88	Kerberos	TCP/UDP
110	POP3	TCP
143	IMAP	TCP
161/162	SNMP	UDP
389	LDAP	TCP
443	HTTPS	TCP
445	SMB / CIFS	TCP
514	Syslog	UDP
636	LDAPS	TCP
993	IMAPS	TCP
995	POP3S	TCP
1433	MS SQL	TCP
1723	PPTP VPN	TCP
3306	MySQL	TCP
3389	RDP	TCP
5060/5061	SIP / SIPS (VoIP)	TCP/UDP
8080	HTTP Proxy / Alt HTTP	TCP

Appendix D: Glossary of All Key Terms

Consolidated glossary of all key terms from the 10-week curriculum, alphabetically organized.

3-2-1 Backup Rule
Best practice: maintain 3 copies of data, on 2 different storage media, with 1 copy stored offsite

802.1X
An IEEE standard for port-based Network Access Control, providing authentication for devices connecting to a LAN

AAA
Authentication, Authorization, and Accounting — the three-step framework for controlling access to network resources

Access Control Vestibule
A physical security mechanism (formerly called a mantrap) using two interlocking doors to control entry

ACL
Access Control List — a set of rules that define which users or systems are allowed or denied access to resources

Air Gap
A physical isolation security measure where a computer or network is not connected to any other network, including the internet

ALE
Annualized Loss Expectancy — the expected yearly monetary loss from a risk (SLE × ARO)

Application Allow List
A security measure that only permits pre-approved applications to execute, blocking all others

APT
Advanced Persistent Threat — a prolonged and targeted cyberattack by a well-funded threat actor (typically nation-state) that remains undetected for extended periods

ARO
Annualized Rate of Occurrence — the estimated frequency with which a risk event occurs per year

Asymmetric Encryption
Encryption using a key pair — public key encrypts, private key decrypts (e.g., RSA, ECC)

Attack Surface
The total number of possible entry points for unauthorized access into any system

BEC
Business Email Compromise — a scam where attackers impersonate executives or business partners to trick employees into transferring money or data

Birthday Attack
A cryptographic attack that exploits the mathematics of the birthday problem to find hash collisions faster than brute force

Blockchain
A distributed, immutable ledger technology that chains blocks of transactions together using cryptographic hashes

Bollard
A physical security barrier (short vertical post) designed to prevent vehicle-borne attacks on buildings

BPA
Business Partners Agreement — a legal arrangement that defines the relationship, responsibilities, and liabilities between business partners

Buffer Overflow
A vulnerability where a program writes data beyond the allocated memory buffer, potentially allowing code execution

Certificate Authority (CA)
A trusted entity that issues and manages digital certificates, verifying the identity of certificate holders

Chain of Custody
A chronological documentation trail showing the collection, transfer, and handling of digital evidence

CIA Triad
The three pillars of information security: Confidentiality (preventing unauthorized access), Integrity (ensuring data accuracy and trustworthiness), and Availability (ensuring authorized access when needed)

CIS Benchmark
A set of best-practice security configuration guidelines published by the Center for Internet Security for hardening systems

Cold Site
A DR facility with basic infrastructure (power, cooling, connectivity) but no pre-installed hardware or data

Compensating Control
An alternative security measure implemented when a primary control is not feasible

Configuration Enforcement
Automated mechanisms (Group Policy, SCAP, MDM) that ensure systems maintain their security baseline

CRL
Certificate Revocation List — a list of certificates that have been revoked before their expiration date

CSPM
Cloud Security Posture Management — automated tools that continuously monitor cloud configurations for security risks

CSR
Certificate Signing Request — a message sent to a Certificate Authority to apply for a digital identity certificate

CVE
Common Vulnerabilities and Exposures — a standardized system for identifying and naming vulnerabilities

CVSS
Common Vulnerability Scoring System — a framework for rating the severity of vulnerabilities on a 0-10 scale

Data at Rest
Data stored on a device or medium that is not currently being transmitted or processed

Data in Transit
Data actively moving between locations — across networks, between devices, or between services

Data in Use
Data currently being processed, accessed, or read by a system or application in memory

Data Sovereignty
The concept that data is subject to the laws and governance structures of the country where it is collected or stored

DDoS
Distributed Denial of Service — overwhelming a target with traffic from multiple sources to make it unavailable

Decommissioning
The secure process of retiring old systems, including data sanitization and proper disposal

Defense in Depth
A layered security strategy that uses multiple security controls at different levels to protect assets

Digital Signature
A cryptographic value that provides authentication, integrity, and non-repudiation by signing data with a private key

DLP
Data Loss Prevention — technologies and policies that prevent unauthorized data exfiltration from an organization

DMARC
Domain-based Message Authentication, Reporting and Conformance — email authentication protocol that uses SPF and DKIM to detect email spoofing

DMZ
Demilitarized Zone — a network segment between internal and external networks that hosts public-facing services

Due Diligence
The research and analysis conducted before entering into an agreement to ensure informed decision-making

E-Discovery
The process of identifying, collecting, and producing electronically stored information in response to legal proceedings

EDR
Endpoint Detection and Response — security solution that monitors endpoints for suspicious activity, provides investigation capabilities, and enables rapid response

Endpoint Protection
Security software installed on endpoints (workstations, servers) that includes antivirus, anti-malware, and behavioral analysis

EternalBlue
An SMBv1 exploit (CVE-2017-0144) allegedly developed by the NSA, used in WannaCry and NotPetya attacks

Fail-Closed
A failure mode where a security device blocks all traffic when it malfunctions, prioritizing security

Fail-Open
A failure mode where a security device allows all traffic when it malfunctions, prioritizing availability

Forensic Image
A bit-for-bit copy of a storage device that preserves all data including deleted files and slack space

Gap Analysis
The process of comparing current security posture against desired or required standards to identify deficiencies

GDPR
General Data Protection Regulation — EU regulation governing personal data protection, with fines up to 4% of global annual revenue

GRC
Governance, Risk, and Compliance — the integrated framework for aligning IT with business objectives, managing risk, and meeting regulatory requirements

Guard Rails
Automated constraints that prevent users or systems from making configurations that violate security policies

Hardening
The process of reducing a system's attack surface by removing unnecessary features, applying security configurations, and patching vulnerabilities

Hashing
A one-way mathematical function that converts data into a fixed-length value (digest) that cannot be reversed

High Availability
System design that ensures a high level of operational continuity, typically through redundancy and failover mechanisms

HIPAA
Health Insurance Portability and Accountability Act — US law protecting the privacy and security of health information

HIPS
Host-based Intrusion Prevention System — software that monitors and blocks suspicious activity on a single host

Honeynet
A network of honeypots that simulates an entire production environment to trap and observe attackers

Honeypot
A decoy system designed to attract attackers, allowing security teams to study attack methods and detect intrusions

Honeytoken
A piece of fake data (credentials, files) planted to detect unauthorized access or data exfiltration

Hot Site
A fully operational disaster recovery facility with real-time data replication, ready for immediate failover

HSM
Hardware Security Module — a dedicated physical device for managing and protecting cryptographic keys

IaC
Infrastructure as Code — managing IT infrastructure through machine-readable configuration files rather than physical hardware or interactive tools

IDS
Intrusion Detection System — monitors network traffic for suspicious activity and generates alerts

Incident Response
The organized approach to addressing and managing the aftermath of a security breach or cyberattack

Indicator of Compromise (IoC)
Evidence that a security breach has occurred — file hashes, IP addresses, domain names, behavioral patterns

Input Validation
The process of verifying that user-supplied data meets expected formats before processing, preventing injection attacks

Insider Threat
A security risk that originates from within the targeted organization, typically current or former employees

IOC
Indicator of Compromise — artifacts observed on a network or system that indicate a potential security breach

IPS
Intrusion Prevention System — monitors and actively blocks detected malicious traffic inline

IPSec

Internet Protocol Security — a suite of protocols for securing IP communications through authentication and encryption

Jump Server
A hardened intermediary server used to access systems in a different security zone (also called bastion host)

Kerberoasting
An attack technique that extracts service account ticket-granting tickets from Active Directory for offline password cracking

Key Escrow
The arrangement where cryptographic keys are held in escrow by a third party for later retrieval

Key Stretching
A technique (PBKDF2, bcrypt, scrypt) that makes hash computation deliberately slow to resist brute-force attacks

LDAP
Lightweight Directory Access Protocol — a protocol for accessing and managing directory services (e.g., Active Directory)

Least Privilege
The principle of granting users and systems only the minimum access rights needed to perform their functions

Legal Hold
A process that requires an organization to preserve all forms of relevant information when litigation is reasonably anticipated

Logic Bomb
Malicious code that triggers when specific conditions are met (date, event, action)

MDM
Mobile Device Management — software for managing, monitoring, and securing mobile devices in an enterprise environment

MFA Fatigue
An attack where the adversary sends repeated MFA push notifications hoping the user will approve one to stop the alerts

Microsegmentation
Granular network segmentation that creates secure zones around individual workloads, limiting lateral movement

MITRE ATT&CK
A globally-accessible knowledge base of adversary tactics and techniques based on real-world observations

MOU
Memorandum of Understanding — a non-binding agreement outlining terms and intentions between parties

NAC
Network Access Control — technology that enforces security policies on devices connecting to the network

NDA
Non-Disclosure Agreement — a legal contract preventing parties from sharing confidential information

NGFW
Next-Generation Firewall — combines traditional firewall capabilities with advanced features like application awareness, IPS, and threat intelligence

Non-Repudiation
The assurance that a party cannot deny the authenticity of their signature or the sending of a message

OAuth

Open Authorization — a standard protocol for token-based authorization, commonly used for API access

OCSP
Online Certificate Status Protocol — a real-time method to check if a specific certificate has been revoked

OSINT
Open Source Intelligence — collecting information from publicly available sources for intelligence purposes

Pass-the-Hash
An attack where stolen password hashes are used to authenticate without knowing the actual password

Patch Management
The systematic process of identifying, acquiring, testing, and deploying software updates to fix vulnerabilities

PCAP
Packet Capture — a file containing recorded network traffic for analysis

PCI-DSS
Payment Card Industry Data Security Standard — security standard for organizations handling credit card data

Penetration Testing
An authorized simulated cyberattack performed to evaluate the security of a system or network

Phishing
A fraudulent attempt to obtain sensitive information by disguising as a trustworthy entity in electronic communication

PICERL
Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned — the SANS IR framework

PKI
Public Key Infrastructure — the framework of policies, hardware, software, and procedures for managing digital certificates and encryption keys

Policy Enforcement Point (PEP)
In Zero Trust architecture, the component that enables, monitors, and terminates connections between subjects and resources

Policy Engine
The Zero Trust component that makes access decisions based on policy and input from external sources

Pretexting
Creating a fabricated scenario (pretext) to engage a victim and gain their trust for information extraction

Privileged Access Management
Solutions that secure, manage, and monitor privileged accounts and access, including JIT permissions and password vaulting

Purple Team
A collaborative security approach combining offensive (Red Team) and defensive (Blue Team) techniques to improve overall security posture

Race Condition
A vulnerability where system behavior depends on the timing of events, creating exploitable windows (TOC/TOU)

Rainbow Table
A precomputed table for reversing cryptographic hash functions, used for cracking password hashes

Ransomware
Malware that encrypts victim data and demands payment for the decryption key

RBAC

Role-Based Access Control — access permissions assigned based on a user's role within the organization

Risk Appetite
An organization's willingness to accept risk in pursuit of its objectives (expansionary, conservative, neutral)

Risk Register
A documented list of identified risks with their assessment, owner, and treatment plan

Risk Transference
Shifting the financial burden of a risk to another party, typically through insurance or contractual agreements

Root Cause Analysis
A systematic process for identifying the fundamental cause of an incident, not just the symptoms

Rootkit
Malware that provides continued privileged access while hiding its presence from detection tools

RPO
Recovery Point Objective — the maximum acceptable amount of data loss measured in time (how old can restored data be?)

RTO
Recovery Time Objective — the maximum acceptable downtime before services must be restored

Salting
Adding a random value to data before hashing to prevent rainbow table attacks and ensure identical passwords produce different hashes

SAML
Security Assertion Markup Language — an XML-based standard for exchanging authentication and authorization data between identity providers and service providers

Sandboxing
Isolating applications in a controlled environment to prevent them from affecting the rest of the system

SASE
Secure Access Service Edge — a cloud-delivered framework combining network security and WAN capabilities

SCAP
Security Content Automation Protocol — a method for using security standards to automate vulnerability management and configuration compliance

SD-WAN
Software-Defined Wide Area Network — uses software to manage WAN connections, optimizing performance and security

SDN
Software-Defined Networking — decouples the network control plane from the data plane, enabling programmatic network management

Segmentation
Dividing a network into smaller, isolated segments to limit lateral movement and contain breaches

Shadow IT
Technology systems and solutions used within an organization without explicit IT department approval

Shared Responsibility Model
A cloud security framework defining which security tasks the cloud provider handles and which the customer must manage

SIEM

Security Information and Event Management — centralized platform for collecting, correlating, and analyzing security logs from across the enterprise

SLA
Service Level Agreement — a contract defining the expected level of service between a provider and customer

SLE
Single Loss Expectancy — the expected monetary loss from a single occurrence of a risk event (AV × EF)

Smishing
SMS phishing — social engineering via text messages

SOAR
Security Orchestration, Automation, and Response — platforms that automate incident response workflows

SOC 2
Service Organization Control 2 — an auditing standard measuring a service organization's controls for security, availability, processing integrity, confidentiality, and privacy

Social Engineering
The psychological manipulation of people into performing actions or divulging confidential information

Spear Phishing
Targeted phishing aimed at a specific individual or organization using personalized information

SQL Injection
An attack that inserts malicious SQL code into application queries to manipulate or extract database data

SSO
Single Sign-On — authentication mechanism allowing users to access multiple applications with one set of credentials

SSRF
Server-Side Request Forgery — a vulnerability where an attacker tricks a server into making requests to unintended internal resources

Steganography
The practice of hiding secret data within ordinary, non-secret data (e.g., embedding text in image files)

Supply Chain Attack
Compromising a target by attacking less-secure elements in their supply chain (vendors, MSPs, software providers)

Symmetric Encryption
Encryption using a single shared key for both encryption and decryption (e.g., AES, 3DES)

Tabletop Exercise
A discussion-based IR exercise where participants walk through a simulated incident scenario without hands-on activity

Technical Debt
The implied cost of future rework caused by choosing quick-fix solutions over more robust approaches

Threat Hunting
The proactive search for cyber threats that are present in a network but have not been detected by automated security tools

Threat Vector
The path or means by which an attacker gains access to a target system

Tokenization

Replacing sensitive data with a non-sensitive token that maps back to the original data through a secure lookup system

TPM
Trusted Platform Module — a hardware chip that securely stores cryptographic keys and performs encryption operations

Trojan
Malware disguised as legitimate software that performs malicious actions once executed

Typosquatting
Registering domains that are common misspellings of popular websites to capture misdirected traffic

UTM
Unified Threat Management — a single appliance combining multiple security functions: firewall, IDS/IPS, antivirus, content filtering

Vishing
Voice phishing — social engineering conducted over phone calls

VM Escape
An exploit that allows code running inside a virtual machine to break out and interact with the host operating system

Volatile Data
Data that exists only in RAM or system state and is lost when the system is powered off (must be collected first in forensics)

WAF
Web Application Firewall — specifically protects web applications by filtering and monitoring HTTP/HTTPS traffic

Warm Site
A DR facility with hardware and connectivity but requiring data restoration before becoming operational

Watering Hole Attack
Compromising a website frequently visited by the target group to infect their systems

Worm
Self-replicating malware that spreads across networks without user interaction

Write Blocker
A hardware or software tool that prevents any writes to a storage device during forensic acquisition

XDR
Extended Detection and Response — extends EDR across multiple security layers (network, cloud, email, identity) for correlated threat detection

XSS
Cross-Site Scripting — injecting malicious scripts into web pages viewed by other users

Zero Trust
A security model that requires strict verification for every person and device trying to access resources, regardless of whether they are inside or outside the network perimeter

Zero-Day
A vulnerability unknown to the vendor with no available patch, actively exploited by attackers

root@blackhack:~# echo "End of curriculum. Now go hack (ethically)."

"The best way to learn security is to break things — then fix them." — BlackHack Society