(3rd December 2025) - JAGUAR COHORT
Made by Chris Cownden
I'm creating recap guides as revision notes for future use. Please use this document as you see fit.

8th Lab Recap Guide: Security+

Recording is here

Timestamps

00:00 Cybersecurity Roles Explained

11:20 Jaguar Cyber Attack - Jira and Internal Threat Actor

31:52 Exam Practice: DES Encryption: Weak Key Space

41:41 Exam Practice: Next-Gen Firewall Explained

54:05 Exam Practice: Website Styling and Interaction Basics

01:07:35 Exam Practice: Java's Legacy vs JavaScript Evolution

01:38:57 Third-Party Authentication Explained

01:51:49 Attackers Seek Access Vulnerabilities

01:57:05 Privacy Breach Concerns Raised

02:12:50 Web App Recon Basics

Resources

- Exam Compass – Source for SEC+ acronyms and practice questions
- D Hashed – Paid service to search for exposed usernames and passwords
- Breach Directory – Free alternative to D Hashed for checking compromised credentials
- GitHub – Search for passwords or API keys leaked in public code repositories
- Security Trails – Sign up free to enumerate subdomains and attack surfaces
- Microsoft SAML/Teams – Used for enterprise authentication and team collaboration
- NCC, Sakama, CGI, BT, Pen Test Partners, ECS Security, Adama, Accenture – Top UK penetration testing and security consulting firms
- OSCP – Offensive Security Certified Professional course

(3rd December 2025) - JAGUAR COHORT
Made by Chris Cownden
I'm creating recap guides as revision notes for future use. Please use this document as you see fit.

Other Recordings To Date

Date	Order	Recordings	Lab Recap Guides
3rd December	Lab 8	RECORDING	THIS ONE
26th November 2025	Lab 7	RECORDING	RECAP GUIDE
19th November 2025	NO SESSION AS JON WAS ABSENT		
12th November 2025	Lab 6	RECORDING	RECAP GUIDE
5th November 2025	Lab 5	RECORDING	RECAP GUIDE
2nd November 2025	3rd Sunday	RECORDING	
29th October 2025	Lab 4	RECORDING	RECAP GUIDE
22nd October 2025	Lab 3	RECORDING	RECAP GUIDE
19th October 2025	2nd Sunday	RECORDING	
15th October 2025	Lab 2	RECORDING	RECAP GUIDE
8th October 2025	Lab 1	RECORDING	RECAP GUIDE
5th October 2025	1st Sunday	RECORDING	

Core Concepts

The Five Domains of Security+

General Security Concepts

- CIA Triad (Confidentiality, Integrity, Availability)
- Basic principles & how to think securely

(3rd December 2025) - JAGUAR COHORT

Made by Chris Cownden

I'm creating recap guides as revision notes for future use. Please use this document as you see fit.

Threats, Vulnerabilities, and Mitigation

- What threats/vulnerabilities are, how they're exploited, and how to control/mitigate them
- Controls/measures = things put in place to reduce risk

Security Architecture

- Secure design principles: Bake security in from the start, not as an afterthought
- Cheaper and more effective to add security early

Security Operations

- Day-to-day practices: incident response, digital forensics, monitoring
- Importance of preparation, identification, and evidence gathering

Security Program Management & Oversight

- Policies, standards, risk management, compliance
- Understand regulatory/compliance frameworks

Difference between Antivirus, Normal Firewall and NGFW

Antivirus

- Scans files, programs, and system behaviour on a device
- Detects malware, viruses, trojans, spyware, etc.
- Works on the endpoint, not the network

Normal Firewall

- Controls network traffic (allow/deny rules)
- Works mainly on IP addresses, ports, and protocols
- Does not inspect files, malware, or user behavior
  Good for perimeter control, but limited against modern threats

NGFW (Next-Generation Firewall)

- Does everything a normal firewall does plus:
  - Deep packet inspection (looks *inside* traffic)
  - Intrusion prevention (IPS)
  - App-level filtering (e.g., block TikTok, allow Slack)

- Web filtering
- Sandboxing / malware detection (this is the antivirus-like bit)

Access Control Models

- **Mandatory Access Control (MAC):**
  Usually in government/military; access requires security clearance.

- **Discretionary Access Control (DAC):**
  Resource owners set permissions.

- **Role-Based Access Control (RBAC):**
  Permissions based on job role (common in organisations/websites).

- **Attribute-Based Access Control (ABAC):**
  Permissions based on attributes: department, location, device, etc.

Least Privilege

- Users should only get the minimum access needed to complete tasks.
- Prevents overexposure & reduces risk if an account is compromised.

Separation of Duties

- Critical tasks divided among several people to prevent collusion, fraud, and single point of failure.
- E.g., bank card & PIN sent separately; multiple admins needed for sensitive operations.

Zero Trust Architecture

- Never automatically trust any device, user, or network – always verify.
- Often uses mutual authentication/certificates.

Encryption

- Symmetric: Same key for encrypt/decrypt (e.g., AES)
- Asymmetric: Public/private keys (e.g., RSA)
- PKI (Public Key Infrastructure): For managing certificates

Incident Response

- Preparation, identification, containment, eradication, recovery, lessons learned
- Digital evidence collection for possible legal action

(3rd December 2025) - JAGUAR COHORT

Made by Chris Cownden

I'm creating recap guides as revision notes for future use. Please use this document as you see fit.

Terminology

Blue Team: Defensive security professionals monitoring, detecting, and responding to security threats.
Red Team: Offensive security professionals focused on authorized attacks to test defenses.
Security Operations: Daily practices to protect IT infrastructure, including incident response and forensics.
Penetration Testing: Authorized simulated attacks to identify security weaknesses.
SOC (Security Operations Center): Centralized unit monitoring and analyzing security for an organization.
Threat: Any potential danger to information or systems (e.g., hackers, malware).
Vulnerability: A flaw that could be exploited by threats to gain unauthorized access or cause harm.
Control): Safeguard or countermeasure put in place to mitigate a vulnerability.
Compensating Control: Alternative measures to satisfy a security requirement when the preferred control can't be used.
Security Architecture: The design and organization of security controls in IT environments.
Incident Response: Procedures for detecting, responding to, and recovering from security breaches.
HIPAA: Health Insurance Portability and Accountability Act; U.S. regulation protecting health information.
CIA Triad: Security model emphasizing confidentiality, integrity, and availability of information.
Access Control List (ACL): List governing which users can access specific resources and in what ways.
MAC (Mandatory Access Control): Restrictive access system where permissions are based on regulated policies, often seen in military/government.
RBAC (Role-Based Access Control): Access granted based on user's role/job function.
ABAC (Attribute-Based Access Control): Access permissions based on user and environment attributes (e.g., location, job title).
Least Privilege: Security principle of granting users only the permissions they need and nothing more.
Separation of Duties: Policy ensuring more than one person is required to complete critical tasks to reduce fraud risk.
Zero Trust: Security model where no user or device is trusted by default—continuous verification required.
Federation: A method of authentication where third-party identity providers (e.g., Google, Microsoft) validate user identity.
Single Sign-On (SSO): A method allowing users to access multiple services with one authentication.

(3rd December 2025) - JAGUAR COHORT

Made by Chris Cownden

I'm creating recap guides as revision notes for future use. Please use this document as you see fit.

OAuth: Open standard for token-based authentication allowing third-party access without sharing passwords.
SAML: Security Assertion Markup Language, used for exchanging authentication information, often in corporate environments.
PKI (Public Key Infrastructure): System for managing digital certificates and public-key encryption.
Symmetric Encryption: Encrypts and decrypts data using the same key.
Asymmetric Encryption: Uses a paired public and private key for encryption and decryption.
AES: Advanced Encryption Standard, modern symmetric encryption replacing DES.
DES: Data Encryption Standard, an older symmetric encryption algorithm with a small key size.
RC4: Outdated stream cipher, formerly used for rapid encryption.
RSA: Asymmetric encryption algorithm named for designers Rivest, Shamir, and Adleman.
SDLC (Software Development Life Cycle): Formal process for designing, developing, testing, deploying, and maintaining software.
SaaS: Software as a Service, software delivered and accessed over the web.
OOP: Object-Oriented Programming, method of software design using "objects."
BIOS: Basic Input/Output System, firmware interface initializing hardware before booting OS.
UEFI: Unified Extensible Firmware Interface, modern BIOS replacement with enhanced features.
GPT: GUID Partition Table, disk partitioning standard.
ACPI: Advanced Configuration and Power Interface, standard for device configuration and power management.
PXE: Preboot Execution Environment, allows computers to boot from a network.
UTM (Unified Threat Management): All-in-one network security solution combining multiple functions (firewall, IDS, AV, etc.).
NGFW (Next Generation Firewall): Firewall with advanced features such as content inspection and decryption.
IDS: Intrusion Detection System, monitors networks for suspicious activity.
WAP: Wireless Access Point, device enabling Wi-Fi connection.
WLAN: Wireless Local Area Network.
HTML: HyperText Markup Language, the main language for web page structure/content.
CSS: Cascading Style Sheets, code describing website look and formatting.
JS: JavaScript, programming language enabling dynamic web features.
HTTP: Hypertext Transfer Protocol, the system for fetching web pages.
SNMP: Simple Network Management Protocol, used for monitoring/management of networked devices.
SMTP: Simple Mail Transfer Protocol, standard for email transmission.
IMAP: Internet Message Access Protocol, for retrieving emails from a mail server.
Reconnaissance: The process of gathering information about a target, especially before penetration testing.
Shodan: Search engine for internet-connected devices, used to find exposed systems/services.
DHashed/Breach Directory: Services for searching leaked credentials in data breaches.
Nmap: Network scanning tool to discover devices and open ports (mentioned as methodology in context).

(3rd December 2025) - JAGUAR COHORT

Made by Chris Cownden

I'm creating recap guides as revision notes for future use. Please use this document as you see fit.

API Key: Secret used to authenticate a program or user to an API.
Cross Site Scripting (XSS): Vulnerability allowing attackers to inject malicious code into web pages.

Acronyms

ACL = Access Control List
ACPI = Advanced Configuration and Power Interface
AES = Advanced Encryption Standard
AP = Access Point
AV = Antivirus
BIOS = Basic Input Output System
CRT = Crest Registered Tester
CSS = Cascading Style Sheets
CPSA = Crest Practitioner Security Analyst
CPIA = Crest Practitioner of Intrusion Analysis
DES = Data Encryption Standard
DV = Developed Vetting
GRC = Governance, Risk, and Compliance
GPT = GUID Partition Table
HTML = HyperText Markup Language
HTTP = HyperText Transfer Protocol
HTTPS = HyperText Transfer Protocol Secure
IAM = Identity and Access Management
IMAP = Internet Message Access Protocol
IDP = Identity Provider
IPS = Intrusion Prevention System
MFA = Multi-Factor Authentication
NGFW = Next Generation Firewall
OSCP = Offensive Security Certified Professional
OT = Operational Technology
PBQ = Performance-Based Questions
PKI = Public Key Infrastructure
PXE = Preboot Execution Environment
RBAC = Role-Based Access Control
RAD = Rapid Application Development
SAML = Security Assertion Markup Language
SAAS = Software as a Service
SC = Security Clearance
SDLC = Software Development Life Cycle
SET = Social Engineering Toolkit
SMTP = Simple Mail Transfer Protocol
SOC = Security Operations Center
SSO = Single Sign-On

(3rd December 2025) - JAGUAR COHORT

Made by Chris Cownden

I'm creating recap guides as revision notes for future use. Please use this document as you see fit.

TCP = Transmission Control Protocol
UDP = User Datagram Protocol
UEFI = Unified Extensible Firmware Interface
URL = Uniform Resource Locator
UTM = Unified Threat Management
WAP = Wireless Access Point
WLAN = Wireless Local Area Network

Analogies - Security booth checking passengers

- A normal firewall is like a security checkpoint where you poke your head out of your booth and look inside a car as it passes by, just checking if the right number of people are inside and maybe asking to see their passports.

- A next-generation firewall (NGFW), on the other hand, is like getting out of your security booth, opening the car doors, asking all the passengers to step out, inspecting them for weapons or drugs (malware), checking their arms, pockets, hair, collars, and even opening the boot and looking underneath the car.