(12th November 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.

# 6th Lab Recap Guide: Security+ (ACRONYMS)

## Recording is here

Jon covered exam questions, flash card practice, ACRONYMS and a practical on Cracking Passwords.

## Timestamps

00:00 "Job Market for Pentesters"

18:52 "Exploring Security Engineer Role"

25:13 Cybersecurity Job Market Trends

39:31 "Industrial Control Systems Explained"

43:58 ACRONYMS Practice

01:19:29  DEMO on Cracking Passwords

01:52:39 Security+ Exam Practice

## Recommended Resources

- Jon's email for 1-to-1 support jon@optima-it.co.uk
- CREST Suppliers
- Security Cleared Job Board
- Cyber Security Job Market
- FREE Entry Level Certification by ISC2
- Cheatsheet Station Folder (everything from Wireshark, NMAP, Linux etc)
- ExamCompass - Practice Security+ Exam Questions

## Other Recordings To Date

| Date | Order | Recordings | Lab Recap Guides |
|---|---|---|---|

(12th November 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.

| | | | |
|---|---|---|---|
| 12th November 2025 | Lab 6 | RECORDING | THIS ONE |
| 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 | |

## Acronyms

MSP = Managed Service Provider
MSSP = Managed Security Service Provider
ICS = Industrial Control System
SCADA = Supervisory Control and Data Acquisition
OT = Operational Technology
PPP = Point-to-Point Protocol
PPTP = Point-to-Point Tunneling Protocol
IGMP = Internet Group Management Protocol
MPLS = Multi-Protocol Label Switching
MTBF = Mean Time Between Failure
RTO = Recovery Time Objective
MTTR = Mean Time To Recover
RPO = Recovery Point Objective
PAM = Privileged Access Management
IAM = Identity and Access Management
SSO = Single Sign-On
MFA = Multi-Factor Authentication
SCAP = Security Content Automation Protocol
OVAL = Open Vulnerability Assessment Language
GPO = Group Policy Object
NTLM = New Technology LAN Manager
AD = Active Directory
SAM = Security Account Manager

(12th November 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 = Application Programming Interface
REST = Representational State Transfer
RBAC = Role-Based Access Control
DAC = Discretionary Access Control
MAC = Mandatory Access Control (Think Defence)
LDAP = Lightweight Directory Access Protocol
SCEP = Simple Certificate Enrollment Protocol
CSR = Certificate Signing Request
OCSP = Online Certificate Status Protocol
PKCS = Public Key Cryptography Standard
SAML = Security Assertion Markup Language
JWT = JSON Web Token
CSF = Cyber Security Framework
CRT = Crest Registered Tester
OSCP = Offensive Security Certified Professional
CIA = Confidentiality, Integrity, Availability

# Cybersecurity Job Roles & Certifications

Key Points:

- Junior Pentester roles expect 6+ months demonstrable experience which you get by going through Optima-IT
- Certifications such as Security+, Certified Ethical Hacker (CEH), OSCP, and Crest CPSA are valued.
- Entry roles sometimes ask for 2–5 years’ experience. Your Security+ & CPSA completion counts toward experience!

# Security+ Exam Domains Overview

Why it matters:
Security+ covers five domains—the backbone of the exam. The split helps you allocate study time efficiently.

Domains:

1. General Security Concepts
2. Threats, Vulnerabilities, and Mitigations
3. Security Architecture
4. Security Operations
5. Security Program and Oversight

- Security Operations

(12th November 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.

Exam Format Tips:

- Score Required: 750/900 (approx. 83%)
- Format: Multiple Choice, Performance-Based Questions (PBQ)

# Windows & Linux Security Concepts

- Windows:
  - NTLM & LM Hashes: Used for authentication; LM is obsolete & weak
  - GPO: Think password policy, account restrictions, etc.
  - Kerberos: Modern authentication protocol (port 88)
  - SAM File: Local user/password hash storage
- Linux:
  - Tools: Kali Linux, Ubuntu (as a safer alternative to Windows for malware resistance)
  - John the Ripper: Password hash cracking utility
  - Hashcat: Powerful hash cracker (often with rainbow tables)
  - RockYou.txt: Common password wordlist for cracking

# Authentication & Access Management

What to know:

You'll be tested on types of authentication, access control models, and practical scenarios.

- Authentication Factors:
  - Something you know (password, PIN)
  - Something you have (token, smart card)
  - Something you are (biometric, fingerprint, Face ID)
  - Location-based or risk-based factors (THINK: How can you be in the UK one minute, and China 1 hour later)
- SSO: Allows users to authenticate once and access multiple resources.
- MFA: Adds extra layer of security. NIST recommends it strongly.
- Provisioning: Creating accounts, assigning privileges, least privilege principle (THINK: Onboarding)
- Account Policies: Password history, length, complexity, password age (NIST now recommends NOT forcing regular changes unless compromised in a data breach)

# Password Policies & Hash Cracking

- Why it matters:
  Weak password policies lead to easy compromises. Expect exam items on password management, cracking, and incident response.
- Password History: Prevents re-use of old passwords.
- Password Complexity/Length: Longer passphrases

- Password Age: NIST/NSCS recommend changing only after compromise, not regular rotation.
- Hash Cracking:
  - NTLM vulnerable; John The Ripper
  - Dictionary attacks (using wordlists like RockYou.txt - a list of compromised passwords).

# Key Controls

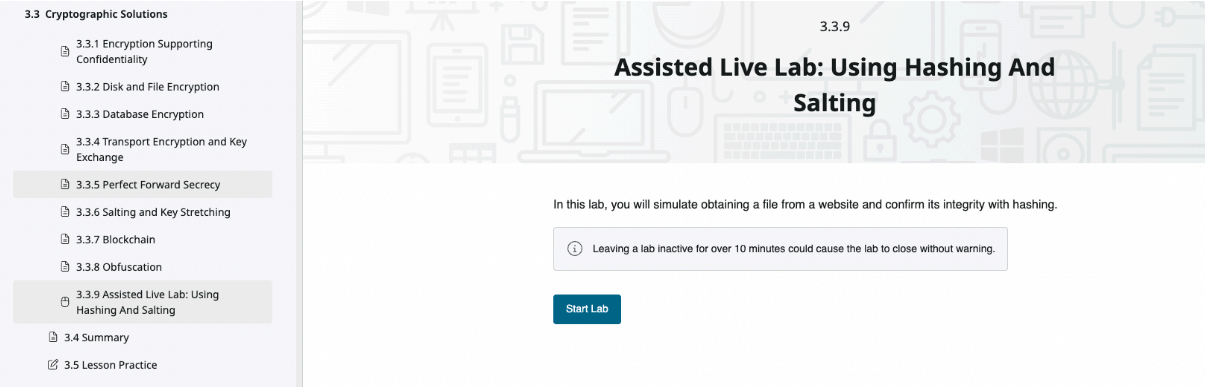
- RBAC vs. MAC vs. DAC:
  - RBAC: Assigns access by job role (least privilege).
  - MAC: Used in contexts needing security clearance (used in Defense).
  - DAC: Owner controls resource sharing (e.g., files in OS, Google Drive)**.**

# DEMO on Cracking Passwords (go to 1h 20m)

Try it out yourself in the Security Labs.

### 3.3 Cryptographic Solutions

3.3.9 Assisted Live Lab: Using Hashing And Salting


3.3 Cryptographic Solutions
3.3.1 Encryption Supporting Confidentiality
3.3.2 Disk and File Encryption
3.3.3 Database Encryption
3.3.4 Transport Encryption and Key Exchange
3.3.5 Perfect Forward Secrecy
3.3.6 Salting and Key Stretching
3.3.7 Blockchain
3.3.8 Obfuscation
3.3.9 Assisted Live Lab: Using Hashing And Salting
3.4 Summary
3.5 Lesson Practice
Start Lab

3.3.9

Assisted Live Lab: Using Hashing And Salting

In this lab, you will simulate obtaining a file from a website and confirm its integrity with hashing.

Leaving a lab inactive for over 10 minutes could cause the lab to close without warning.

(12th November 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.

## Analogy - Hollywood Blockbuster

**The Director (You)** You’re the director, the mastermind of everything happening on set, from casting to final cut. You decide who gets into the studio (network), what part they play (access levels), and who’s allowed in the editing room (admin privileges). But running a film isn’t solo work—the production crew (IT pros) keeps everything rolling.

**Casting Actors (User Roles)** The actors turn up for auditions (job market), vying for roles: Pen Tester, SOC Analyst, Vulnerability Specialist—junior or senior. Some have the right certifications (OSCP, Security+, Crest CPSA)—their IMDb profiles are glowing (“six months’ experience,” “recent placement,” “security clearance”). You only hire people with the right credentials for each role—no random walk-ons!

**Production Team Access (RBAC/DAC/MAC)** You give out backstage passes based on job—camera crew only in the studio (RBAC), make-up artists get access to the dressing rooms (DAC at the discretion of the room owner), while only the special effects team is allowed in the high-security vault where the next blockbuster script is stored (MAC—strict clearance!).

**Passwords: The Script Rewrite** Script security is key! If someone keeps leaving the script (password) in plain sight or reusing the old version, the press (hackers) might leak spoilers. That’s why the director insists on clever, unique passphrases—think “ILove-Film1-ng@-Sunset-2024” instead of “password123.” If anyone’s caught with a weak script, your production inspector (Jon Heaps and his trusty John the Ripper software) will crack those secrets faster than a TMZ headline.

**Audition Check-Ins (IAM & Multifactor Authentication)** To get on set, actors must show ID, scan their thumbprint, and say their secret catchphrase (“multi-factor authentication”). Sometimes, an actor tries to FaceTime from Beijing right after leaving the London premiere—suspicious! That’s the location-based authentication twist: you check the time and place. If it doesn’t add up, the actor’s sent home.

**Scheduling & Support (Student Support)** If an actor feels like their role’s overwhelming, you’ve got supportive production assistants (StudentSupport@Optima.it) ready to lend a hand, rewrite schedules, or offer a break between scenes.

**Cheat Sheets (Screenplay Pages)** Between takes, your cast studies the “cheat sheets” and script notes—quick references to what makes secure acting, exactly like those PDFs and guides Jon Heaps shared. The best actors aren’t just talented—they know their lines, know the roles, and never forget an acronym!

**The Big Premiere** Finally, it’s opening night—the Security+ exam! If your actors (students) worked hard in rehearsals, studied the script (acronyms, job roles, password policies), and learned the choreography (hands-on practicals), your film will earn rave reviews and top box-office results.

# Exam Question Practice

1. **What are the classic three factors of authentication?**

Something you know, something you have, something you are (password/PIN, token/smart card, biometrics)

2. **What policy prevents users from choosing old passwords again?**

Password History

3. **What’s the current NCSC/NIST guidance on password renewal/changes?**

Only change if evidence of breach; regular forced changes not recommended.

4. **What are passphrases and why are they recommended?**

Longer/more complex than passwords, harder to crack.

5. **What is a dictionary attack?**

Cracking passwords using a pre-compiled list (e.g. Rockyou.txt) of commonly used passwords.

6. **Name a popular tool for password cracking.**

John the Ripper *(also discussed: Hashcat, Hydra, Rainbow tables)*

7. **Why is just having a password not enough for authentication?**

Employees choose poor passwords; passwords alone are often insecure.

8. **Which technology must an employee use to access company’s shared drive from outside the office?**

VPN

9. **For defense contractors, which access control model should be used for strict classification/clearance requirements?**

MAC (Mandatory Access Control)

10. **Why might an accountant not have access to all accounting software sections?**

Role-Based Access Control & Principle of Least Privilege

11. **What protocol allows linking AD to third-party directory for SSO?**

LDAP (port 389; uses X.500)

12. **What SSO solution uses XML standard?**

SAML (Security Assertion Markup Language)

13. **What control should the administrator use for drive access determined by job function?**

Role-Based Access Control

14. **Which policy should a company adjust if employees are writing down passwords due to complexity?**

Password Complexity (review/reduce complexity so people don't write down passwords)

15. **How can a company add another layer to IAM? (Choose two)**

Multi-Factor Authentication, Location-Based (Geographic) restrictions

16. **What technology does an engineer need to pull data for metrics/dashboard from a ticketing system?**

API

17. **What is the process of prepping accounts/access for new employees from HR platform?**

Provisioning

18. **Which security policy aligns with updated NIST guidelines?**

Multi-Factor Authentication

19. **What technology replaced NTLM in AD?**

Kerberos

20. **How can a company restrict access to a contractor only during 9am–12pm?**

Time-Based Restrictions

21. **How do you link two directory systems from company acquisition for single account access?**

Federation

22. **If an employee can't access work email while traveling, what policy is impacting them?**

Location-Based Restrictions

23. **For one-off drives where the owner picks access, which control type is this?**

Discretionary Access Control

24. **Why can password age policy cause issues? (frequent required changes)**

Employees choose weak passwords or write them down.

## Terminology

MSP (Managed Service Provider): Outsources general IT services to companies lacking in-house expertise.

MSSP (Managed Security Service Provider): Outsources IT security management, including SOC and cyber threat intelligence.

SOC Analyst: Security Operations Center specialist, often entry-level cyber role focused on monitoring and responding to threats.

SCADA (Supervisory Control and Data Acquisition): System for monitoring and controlling industrial equipment and processes.

ICS (Industrial Control Systems): Broad category including hardware/software to manage industrial devices and operations.

OT (Operational Technology): Technology used to manage industrial operations, often alongside ICS and SCADA.

PPP (Point-to-Point Protocol): Method for establishing a connection between two networked devices.

PPTP (Point-to-Point Tunneling Protocol): Obsolete VPN protocol for secure point-to-point communications.

IGMP (Internet Group Management Protocol): Manages multicast group memberships in IP networks.

(12th November 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.

RPO (Recovery Point Objective): Maximum acceptable amount of data loss before a disaster becomes critical.

RTO (Recovery Time Objective): Amount of time allowed to restore operations after an outage.

MTTR (Mean Time to Recover): Average time it takes to repair and restore a system after failure.

MTBF (Mean Time Between Failures): Predicted time between repairs in a system's lifecycle.

PAM (Privileged Access Management): Controls and monitors privileged accounts like admin or root users.

IAM (Identity and Access Management): Framework for managing user identities and controlling resource access.

SSO (Single Sign-On): Allows users to access multiple systems with one set of login credentials.

MFA (Multi-Factor Authentication): Requires more than one type of credential for user authentication.

SCAP (Security Content Automation Protocol): Protocol for automating checks of system security baselines and compliance.

NTLM (New Technology LAN Manager): Microsoft authentication and hash protocol, now mostly replaced by Kerberos.

GPO (Group Policy Object): Centralized way to manage policies and settings in Windows networks.

Kerberos: Authentication protocol used in Active Directory, operates on port 88.

LDAP (Lightweight Directory Access Protocol): Protocol for managing user objects in directories (port 389).

SAML (Security Assertion Markup Language): XML-based standard for transmitting authentication and authorization data for SSO.

OAuth (Open Authorization): Standard for token-based authentication, often using JWT (JSON Web Token).

Provisioning: Creating user accounts and assigning appropriate access within organizations.

RBAC (Role-Based Access Control): Assigns access permissions based on job roles.

(12th November 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.

DAC (Discretionary Access Control): Resource creator/owner determines access permissions at their discretion.

MAC (Mandatory Access Control): Access is dictated by clearance levels and mandatory policies, often in defense or government.

API (Application Programming Interface): Middleware that enables integration and communication between software applications.

Password Policy: Organizational rules for password length, complexity, reuse, and history.

Risk-Based Authentication: Adjusts authentication requirements according to contextual risk factors (e.g., location, behavior patterns).

Password Hash: Encrypted version of a password, used for secure storage and verification.

John the Ripper: Tool used for offline password hash cracking.

Hashcat: Advanced password recovery tool leveraging precomputed hash tables ("rainbow tables").

REST (Representational State Transfer): Architectural style for designing networked APIs.

X500 Standard: Directory standard that dictates how LDAP entries are formatted.

SID (Security Identifier): Unique identifier for user accounts in Microsoft environments.

Keep up the great work team! You’ve got this!

All the best, Chris Cownden (fellow JAGUAR cohort team player)

Feel free to connect with me here: https://www.linkedin.com/in/chriscownden/