# Aaron Higham

Cardinal Newman College

Total Labs Completed: **10** | Total Points: **100** | Total Time: **56 minutes**

## Labs Completed:

* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)

# Aayan Ahmed

Blackburn College

Total Labs Completed: **108** | Total Points: **3560** | Total Time: **16 hours 45 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)

# Adil Ali

Blackburn College

Total Labs Completed: **57** | Total Points: **1160** | Total Time: **2 hours 55 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Guidance on Remote Working (Fundamentals)
* History of Information Security (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Incident Response in the Workplace (Fundamentals)
* Information Security: Starting at the Beginning (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* OSI Model (Fundamentals)
* Personal Devices in the Workplace (Fundamentals)
* Physical Security (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Privileged Access (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Security On The Go (Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* The Internet (Fundamentals)
* What Is Information Security? (Fundamentals)

# Agmada Asa

Cardinal Newman College

Total Labs Completed: **113** | Total Points: **6690** | Total Time: **13 hours 54 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* C++: Hardcoded Secrets (Application Security)
* C++: Introduction (Application Security)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.10 – Demonstrate Your Knowledge (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.3 – Weaponization Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.4 – Delivery Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.5 – Exploitation Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.6 – Installation/Persistence Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.7 – What is the Command and Control (C2) Phase? (Offensive Cyber)
* Cyber Kill Chain: Ep.8 – Actions on Objectives Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.9 – Adversary Simulation (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Elliptic Curve Cryptography (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction To Elastic: Ep.1 – What is Elastic? (Defensive Cyber)
* Introduction To Elastic: Ep.2 – Querying Data (Defensive Cyber)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Hashing (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Kerberos: Ep.2 – Enumeration (Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Microsoft Azure Basics: Navigating the Web Portal (Cloud Security)
* Microsoft Azure Basics: Storage Accounts (Cloud Security)
* Modern Encryption: RSA (Fundamentals)
* Nessus: Ep.1 – Introduction to Nessus (Offensive Cyber)
* Nessus: Ep.2 – Network Scanning (Offensive Cyber)
* Nessus: Ep.3 – Authenticated Scanning (Offensive Cyber)
* Nessus: Ep.4 – Scan Results (Offensive Cyber)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* Nmap: Ep.2 – Using Nmap (Offensive Cyber)
* Nmap: Ep.3 – Host Discovery (Offensive Cyber)
* Nmap: Ep.4 – Port Scanning (Offensive Cyber)
* Nmap: Ep.5 – OS and Version Detection (Offensive Cyber)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* PKI (Public Key Infrastructure) Practical (Fundamentals)
* Packet Analysis: Packet Capture Basics (Defensive Cyber)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Protocols: ARP (Fundamentals)
* Protocols: DHCPv4 (Fundamentals)
* Protocols: DHCPv6 (Fundamentals)
* Protocols: DNS (Fundamentals)
* Protocols: FTP (Fundamentals)
* Protocols: HTTP (Fundamentals)
* Python: Code Comments (Application Security)
* Python: Hardcoded Secrets (Application Security)
* SQL Injection: UNION (Offensive Cyber)
* Scanning: Network Scanning (Defensive Cyber, Offensive Cyber)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Web Log Analysis: Ep.3 – Access Logs (Defensive Cyber)
* Web Log Analysis: Ep.4 — Error Logs (Defensive Cyber)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wireshark: Display Filters – Introduction to Filters (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)

# Ahmed Abdelrahman

Cardinal Newman College

Total Labs Completed: **65** | Total Points: **3120** | Total Time: **3 hours 45 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Git Security: Git History (Application Security)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Modern Encryption: Demonstrate Your Skills (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Threat Research: Dependency Confusion (Application Security, Cyber Threat Intelligence)
* Web Log Analysis: Ep.3 – Access Logs (Defensive Cyber)
* Web Log Analysis: Ep.4 — Error Logs (Defensive Cyber)
* Web Log Analysis: Ep.5 – Searching Web Server Logs using Linux CLI (Defensive Cyber)
* Web Log Analysis: Ep.6 — The Tomcat's Out Of The Bag (Defensive Cyber)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)

# Aleena Joseph

Runshaw College

Total Labs Completed: **95** | Total Points: **2680** | Total Time: **14 hours 31 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cookies (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Fake News (Fundamentals)
* Cyber 101: Geolocation (Fundamentals)
* Cyber 101: Information Security (Fundamentals)
* Cyber 101: Keylogging (Fundamentals)
* Cyber 101: Rogue USB Devices (Fundamentals)
* Cyber 101: Security Champions (Fundamentals)
* Cyber 101: Virtual Card Numbers (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Networking: Ep.6 — Domain Name System (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to Penetration Test Programs: Ep.2 – Cybersecurity Frameworks (Fundamentals)
* Introduction to Penetration Test Programs: Ep.3 – Defining your Testing Program (Fundamentals)
* Introduction to Penetration Test Programs: Ep.4 – Choosing a Supplier (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Linux CLI: Ep.5 – File Permissions (Fundamentals)
* Modern Encryption: RSA (Fundamentals)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* Physical Security (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Physical Security: Ep.2 – Physical Security in Your Workplace (Fundamentals)
* Physical Security: Ep.3 – Physical Security When Working Remotely (Fundamentals)
* Physical Security: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Social Engineering: Ep.3 – How Is It Used? (Fundamentals)
* Social Engineering: Ep.4 – Protecting Yourself (Fundamentals)
* Social Engineering: Ep.5 – Demonstrate Your Skills (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* Tactics: Initial Access (Defensive Cyber, Offensive Cyber)
* Tactics: Reconnaissance (Defensive Cyber, Offensive Cyber)
* Tactics: Resource Development (Defensive Cyber, Offensive Cyber)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* What is Digital Forensics? (Defensive Cyber, Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)

# Alex Lawrence

Blackpool and the Fylde College

Total Labs Completed: **64** | Total Points: **1750** | Total Time: **17 hours 0 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* AI: Prompt Injection Attacks (Application Security, Defensive Cyber, Fundamentals)
* Authentication: Ep.1 – What is Authentication? (Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Compliance: General Data Protection Regulation (GDPR) (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Data Privacy: Ep.1 – Key Concepts (Fundamentals)
* Data Privacy: Ep.2 – Data Privacy Regulations (Fundamentals)
* Data Privacy: Ep.3 – What About You? (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Guidance on Remote Working (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Public and Private Key Management (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Networking: Ep.6 — Domain Name System (Fundamentals)
* Introduction to Networking: Ep.7 — Demonstrate Your Knowledge (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Privacy (Fundamentals)
* Protocols: HTTP (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)

# Alex Read

Runshaw College

Total Labs Completed: **143** | Total Points: **8040** | Total Time: **12 hours 48 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* C++: Introduction (Application Security)
* Caesar Ciphers (Fundamentals)
* Cyber 101: Cookies (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Fake News (Fundamentals)
* Cyber 101: Geolocation (Fundamentals)
* Cyber 101: Information Security (Fundamentals)
* Cyber 101: Keylogging (Fundamentals)
* Cyber 101: Rogue USB Devices (Fundamentals)
* Cyber 101: Security Champions (Fundamentals)
* Cyber 101: Virtual Card Numbers (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Data Handling: Ep.2 – Gathering, Storing, and Processing Data (Fundamentals)
* Data Handling: Ep.3 – Data Privacy and Access (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Evidence (Defensive Cyber, Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Digital Forensics Process: Reporting (Defensive Cyber, Fundamentals)
* Digital Forensics Processes and Techniques (Defensive Cyber, Fundamentals)
* Digital Forensics Tools (Defensive Cyber, Fundamentals)
* Disposal of Device Information (Fundamentals)
* Encoding: What is Encoding? (Fundamentals)
* Encryption Tools: CyberChef (Fundamentals)
* Ethics & Laws: Bugbusters (Fundamentals)
* Ethics & Laws: Burglary and Hacking (Fundamentals)
* Ethics & Laws: Ethical and Unethical Hacking (Fundamentals)
* Ethics & Laws: Police Raid (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Ethics & Laws: US Federal Cyber Law (Fundamentals)
* Historic Encryption: Demonstrate Your Skills (Fundamentals)
* Human Factors in Cybersecurity: How People Make Security Mistakes (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Human Factors in Cybersecurity: Security Awareness and Behavior Change (Fundamentals)
* Human Factors in Cybersecurity: Security Culture (Fundamentals)
* Human Factors in Cybersecurity: Usable Security (Fundamentals)
* Introduction To Elastic: Ep.1 – What is Elastic? (Defensive Cyber)
* Introduction To Elastic: Ep.2 – Querying Data (Defensive Cyber)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Digital Forensics: Demonstrate Your Skills (Defensive Cyber, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Hashing (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Networking: Ep.6 — Domain Name System (Fundamentals)
* Introduction to Networking: Ep.7 — Demonstrate Your Knowledge (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Microsoft Azure Basics: Navigating the Web Portal (Cloud Security)
* Microsoft Azure Basics: Storage Accounts (Cloud Security)
* Modern Encryption: RSA (Fundamentals)
* Nessus: Ep.1 – Introduction to Nessus (Offensive Cyber)
* Nessus: Ep.2 – Network Scanning (Offensive Cyber)
* Nessus: Ep.3 – Authenticated Scanning (Offensive Cyber)
* Nessus: Ep.4 – Scan Results (Offensive Cyber)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* Nmap: Ep.2 – Using Nmap (Offensive Cyber)
* Nmap: Ep.3 – Host Discovery (Offensive Cyber)
* Nmap: Ep.4 – Port Scanning (Offensive Cyber)
* Nmap: Ep.5 – OS and Version Detection (Offensive Cyber)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* Packet Analysis: Packet Capture Basics (Defensive Cyber)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Protocols: ARP (Fundamentals)
* Protocols: DHCPv4 (Fundamentals)
* Protocols: DHCPv6 (Fundamentals)
* Protocols: DNS (Fundamentals)
* Protocols: FTP (Fundamentals)
* Protocols: HTTP (Fundamentals)
* Python: Code Comments (Application Security)
* Python: Hardcoded Secrets (Application Security)
* Scanning: Network Scanning (Defensive Cyber, Offensive Cyber)
* Secure Data Handling (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (US) (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Steganography (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Bombe Machine (Fundamentals)
* The Enigma Machine (Fundamentals)
* The History of Encryption (Fundamentals)
* The Internet (Fundamentals)
* The Typex Machine (Fundamentals)
* Transport Protocols (Fundamentals)
* Vigenère Ciphers (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Web Log Analysis: Ep.3 – Access Logs (Defensive Cyber)
* Web Log Analysis: Ep.4 — Error Logs (Defensive Cyber)
* What is Digital Forensics? (Defensive Cyber, Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Concepts: Environment Variables (Fundamentals)
* Windows Concepts: New Technology File System (NTFS) (Fundamentals)
* Windows Concepts: Scheduled Tasks (Fundamentals)
* Windows Concepts: Security Policies (Fundamentals)
* Windows Concepts: Windows Registry (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wireshark: Display Filters – Introduction to Filters (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)

# Alfie Grime

Runshaw College

Total Labs Completed: **70** | Total Points: **1820** | Total Time: **5 hours 29 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.2 – Case Studies (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Browsing Securely: Ep.5 – Demonstrate Your Knowledge (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Information Security (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.10 – Demonstrate Your Knowledge (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.2 – Case Studies (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Digital Footprint: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Elliptic Curve Cryptography (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Networking: Ep.6 — Domain Name System (Fundamentals)
* Introduction to Networking: Ep.7 — Demonstrate Your Knowledge (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Modern Encryption: RSA (Fundamentals)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* The Internet (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)

# Alisha Ghalib

Blackburn College

Total Labs Completed: **53** | Total Points: **1320** | Total Time: **3 hours 36 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)

# Andrew Baines

Blackpool and the Fylde College

Total Labs Completed: **148** | Total Points: **3960** | Total Time: **27 hours 35 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI for Business: Ep.1 – What is AI? (Fundamentals)
* AI for Business: Ep.2 – The Benefits of AI (Fundamentals)
* AI for Business: Ep.3 – The Risks of AI (Fundamentals)
* AI for Business: Ep.4 – Using AI at Work (Fundamentals)
* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Authentication: Ep.1 – What is Authentication? (Fundamentals)
* Authentication: Ep.2 – Why Are Passwords Important? (Fundamentals)
* Authentication: Ep.3 – Creating Secure Passwords (Fundamentals)
* Authentication: Ep.4 – Adding an Extra Layer of Security (Fundamentals)
* Authentication: Ep.5 – Demonstrate Your Knowledge (Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.2 – Case Studies (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Browsing Securely: Ep.5 – Demonstrate Your Knowledge (Fundamentals)
* C++: Hardcoded Secrets (Application Security)
* C++: Introduction (Application Security)
* Cyber 101: Cookies (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Fake News (Fundamentals)
* Cyber 101: Geolocation (Fundamentals)
* Cyber 101: Information Security (Fundamentals)
* Cyber 101: Keylogging (Fundamentals)
* Cyber 101: Rogue USB Devices (Fundamentals)
* Cyber 101: Security Champions (Fundamentals)
* Cyber 101: Virtual Card Numbers (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Data Handling: Ep.2 – Gathering, Storing, and Processing Data (Fundamentals)
* Data Handling: Ep.3 – Data Privacy and Access (Fundamentals)
* Data Handling: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Data Privacy: Ep.1 – Key Concepts (Fundamentals)
* Data Privacy: Ep.2 – Data Privacy Regulations (Fundamentals)
* Data Privacy: Ep.3 – What About You? (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Device Security: Ep.2 – Increasing Your Protection (Fundamentals)
* Device Security: Ep.3 – Case Studies (Fundamentals)
* Device Security: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.2 – Case Studies (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Digital Footprint: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Guidance on Remote Working (Fundamentals)
* History of Information Security (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* ISO 27001: Ep.1 – What Is ISO 27001? (Fundamentals)
* ISO 27001: Ep.2 – The Domains of ISO 27001 (Fundamentals)
* ISO 27001: Ep.3 – What About You? (Fundamentals)
* Incident Response in the Workplace (Fundamentals)
* Information Security and Cybersecurity Terminology (Fundamentals)
* Information Security: Starting at the Beginning (Fundamentals)
* Introduction To Elastic: Ep.1 – What is Elastic? (Defensive Cyber)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Message Integrity (Application Security, Fundamentals)
* Introduction to Cryptography: One-Time Pad (Application Security, Fundamentals)
* Introduction to Cryptography: Public Key Infrastructure (Application Security, Fundamentals)
* Introduction to Cryptography: Public and Private Key Management (Application Security, Fundamentals)
* Introduction to Cryptography: Stream Ciphers (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Networking: Ep.6 — Domain Name System (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Modern Encryption: RSA (Fundamentals)
* Nessus: Ep.1 – Introduction to Nessus (Offensive Cyber)
* Nessus: Ep.2 – Network Scanning (Offensive Cyber)
* Nessus: Ep.3 – Authenticated Scanning (Offensive Cyber)
* Nessus: Ep.4 – Scan Results (Offensive Cyber)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Deleted Tweet (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media and Privacy (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* Personal Devices in the Workplace (Fundamentals)
* Physical Security (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Physical Security: Ep.2 – Physical Security in Your Workplace (Fundamentals)
* Physical Security: Ep.3 – Physical Security When Working Remotely (Fundamentals)
* Physical Security: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Ports (Fundamentals)
* Privacy (Fundamentals)
* Privileged Access (Fundamentals)
* Python: Code Comments (Application Security)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Security On The Go (Fundamentals)
* Security Reporting and Responsiveness: Ep.1 – Reporting Incidents and Concerns (Fundamentals)
* Security Reporting and Responsiveness: Ep.2 – Case Studies (Fundamentals)
* Security Reporting and Responsiveness: Ep.3 – Responding Appropriately (Fundamentals)
* Security Reporting and Responsiveness: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Shoulder Surfing (Fundamentals)
* Social Engineering (Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Social Engineering: Ep.3 – How Is It Used? (Fundamentals)
* Social Engineering: Ep.4 – Protecting Yourself (Fundamentals)
* Social Engineering: Ep.5 – Demonstrate Your Skills (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (US) (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Importance of Information Security and Cybersecurity (Fundamentals)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* What Is Information Security? (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)

# Andrew S

STEM Bursary Management Direct Members

Total Labs Completed: **70** | Total Points: **2750** | Total Time: **7 hours 40 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI Challenges: Beat the Bot (Challenges & Scenarios)
* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction To Elastic: Ep.1 – What is Elastic? (Defensive Cyber)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* Nmap: Ep.2 – Using Nmap (Offensive Cyber)
* OSI Model (Fundamentals)
* PKI (Public Key Infrastructure) (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Python: Code Comments (Application Security)
* Python: Hardcoded Secrets (Application Security)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)

# Andy Alston

Runshaw College

Total Labs Completed: **16** | Total Points: **160** | Total Time: **26 minutes**

## Labs Completed:

* Disposal of Device Information (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)

# Asad Ali Butt

Runshaw College

Total Labs Completed: **179** | Total Points: **15020** | Total Time: **44 hours 11 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* 32-Bit Linux Assembly: Ep.1 – Structure and Registers (Defensive Cyber, Offensive Cyber)
* 32-Bit Windows Assembly: Ep.1 – Windows API and the Stack (Defensive Cyber, Offensive Cyber)
* 64-Bit Windows Assembly: Ep.1 – Windows APIs and Registers (Defensive Cyber, Offensive Cyber)
* A Christmas Catastrophe: Present Pandemonium (Challenges & Scenarios)
* A Christmas Catastrophe: Santa's Sleighdar (Challenges & Scenarios)
* A Christmas Catastrophe: The Grotto (Challenges & Scenarios)
* AI Challenges: Beat the Bot (Challenges & Scenarios)
* AI for Business: Ep.1 – What is AI? (Fundamentals)
* AI for Business: Ep.2 – The Benefits of AI (Fundamentals)
* AI for Business: Ep.3 – The Risks of AI (Fundamentals)
* AI for Business: Ep.4 – Using AI at Work (Fundamentals)
* AI: Artificial Intelligence for Incident Responders (Application Security, Defensive Cyber, Fundamentals)
* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Demonstrate Your Skills (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Function Calling (Challenges & Scenarios)
* AI: Generative AI Models (Application Security, Defensive Cyber, Fundamentals)
* AI: Image Classification (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* AI: Prompt Injection Attacks (Application Security, Defensive Cyber, Fundamentals)
* AI: TensorFlow for Machine Learning (Application Security, Defensive Cyber, Fundamentals)
* Authentication: Ep.1 – What is Authentication? (Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Burp Suite Basics: HTTPS (Application Security, Offensive Cyber)
* Burp Suite Basics: Introduction (Application Security, Offensive Cyber)
* C++: Hardcoded Secrets (Application Security)
* C++: Introduction (Application Security)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.3 – Weaponization Phase (Offensive Cyber)
* DDOS Analysis: Demonstrate Your Skills (Defensive Cyber)
* DDOS Analysis: Ping of Death (Defensive Cyber)
* DDOS Analysis: SYN Flood (Defensive Cyber)
* DDOS Analysis: UDP Flood (Defensive Cyber)
* DDOS Analysis: What are DDoS Attacks? (Defensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Data Privacy: Ep.1 – Key Concepts (Fundamentals)
* Data Privacy: Ep.2 – Data Privacy Regulations (Fundamentals)
* Data Privacy: Ep.3 – What About You? (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.2 – Case Studies (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Digital Footprint: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Elastic Playground: Accounting and Audit (Defensive Cyber)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Immersive Bank: Ep.1 – Open Source and Credentials (Challenges & Scenarios)
* Immersive Care: Ep.1 – Introduction (Challenges & Scenarios)
* Internet Protocol V4 (Fundamentals)
* Introduction To Elastic: Ep.1 – What is Elastic? (Defensive Cyber)
* Introduction To Elastic: Ep.2 – Querying Data (Defensive Cyber)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Hashing (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Metasploit: Ep.1 – What is Metasploit? (Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to Reverse Engineering: 32-Bit Linux – Part 1 (Defensive Cyber, Offensive Cyber)
* Introduction to Reverse Engineering: 32-Bit Windows – Part 1 (Defensive Cyber, Offensive Cyber)
* Introduction to Reverse Engineering: 64-Bit Windows – Part 1 (Defensive Cyber, Offensive Cyber)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Java: Command Injection III (Application Security)
* Kate's Story: Ep.2 – Exploitation (Challenges & Scenarios)
* Kerberos: Ep.2 – Enumeration (Offensive Cyber)
* Kusto Query Language: Ep.1 – Introduction to KQL (Cloud Security)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Log Finder (Defensive Cyber)
* Microsoft Azure Basics: Navigating the Web Portal (Cloud Security)
* Microsoft Azure Basics: Storage Accounts (Cloud Security)
* Modern Encryption: RSA (Fundamentals)
* Nessus: Ep.1 – Introduction to Nessus (Offensive Cyber)
* Nessus: Ep.2 – Network Scanning (Offensive Cyber)
* Nessus: Ep.3 – Authenticated Scanning (Offensive Cyber)
* Nessus: Ep.4 – Scan Results (Offensive Cyber)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* Nmap: Ep.2 – Using Nmap (Offensive Cyber)
* Nmap: Ep.3 – Host Discovery (Offensive Cyber)
* Nmap: Ep.4 – Port Scanning (Offensive Cyber)
* Nmap: Ep.5 – OS and Version Detection (Offensive Cyber)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* PKI (Public Key Infrastructure) Practical (Fundamentals)
* Packet Analysis: Packet Capture Basics (Defensive Cyber)
* Packet Analysis: TLS Handshake (Defensive Cyber)
* Parellus Power: Ep.1 – Gathering Information (Challenges & Scenarios)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Physical Security: Ep.2 – Physical Security in Your Workplace (Fundamentals)
* Physical Security: Ep.3 – Physical Security When Working Remotely (Fundamentals)
* Physical Security: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Ports (Fundamentals)
* PowerShell Deobfuscation: Ep.1 — Introduction (Defensive Cyber)
* Protocols: ARP (Fundamentals)
* Protocols: DHCPv4 (Fundamentals)
* Protocols: DHCPv6 (Fundamentals)
* Protocols: DNS (Fundamentals)
* Protocols: FTP (Fundamentals)
* Protocols: HTTP (Fundamentals)
* Protocols: HTTP – Status Codes (Fundamentals)
* Protocols: LDAP (Fundamentals)
* Protocols: SMTP (Fundamentals)
* Python: Code Comments (Application Security)
* Python: Debug Console (Application Security)
* Python: Default Error Pages (Application Security)
* Python: Forced Browsing (Application Security)
* Python: Hardcoded Secrets (Application Security)
* Python: Insecure Deserialization (Application Security)
* Python: Insecure Direct Object Reference (IDOR) (Application Security)
* Python: Reflected XSS (Application Security)
* Python: SQL Injection (Application Security)
* Python: Stored XSS (Application Security)
* Python: Unrestricted File Upload (Application Security)
* Python: XML External Entities (XXE) (Application Security)
* SMTP Log Analysis (Defensive Cyber)
* SQL Injection: File Download (Offensive Cyber)
* Scanning: Network Scanning (Defensive Cyber, Offensive Cyber)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (US) (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* TLS Fundamentals: Ep.1 – Introduction (Application Security)
* TLS Fundamentals: Ep.2 – Client Hello and Server Hello (Application Security)
* TLS Fundamentals: Ep.3 – Cipher Suites (Application Security)
* TLS Fundamentals: Ep.4 – Key Exchange and Session Resumes (Application Security)
* TLS Fundamentals: Ep.5 – X.509 Introduction (Application Security)
* TLS Fundamentals: Ep.6 – X.509 Analysis (Application Security)
* TLS Fundamentals: Ep.7 – TLS 1.3 (Application Security)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Web Log Analysis: Ep.3 – Access Logs (Defensive Cyber)
* Web Log Analysis: Ep.4 — Error Logs (Defensive Cyber)
* Web Log Analysis: Ep.5 – Searching Web Server Logs using Linux CLI (Defensive Cyber)
* Web Log Analysis: Ep.6 — The Tomcat's Out Of The Bag (Defensive Cyber)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wireshark: Display Filters – Introduction to Filters (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)
* World Cup Special: It's a Game of Pong (Challenges & Scenarios)

# Casey Mendell

Blackpool and the Fylde College

Total Labs Completed: **61** | Total Points: **2240** | Total Time: **10 hours 59 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI Challenges: Beat the Bot (Challenges & Scenarios)
* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Ethics & Laws: US Federal Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)

# Charlotte Torvell

Blackpool and the Fylde College

Total Labs Completed: **65** | Total Points: **3380** | Total Time: **3 hours 34 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* C++: Buffer Overflows (Application Security)
* C++: Command Injection (Application Security)
* C++: Format String (Application Security)
* C++: Hardcoded Secrets (Application Security)
* C++: Introduction (Application Security)
* C++: Relative Paths (Application Security)
* C++: SQL Injection (Application Security)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.10 – Using Sudo (Fundamentals)
* Linux CLI: Ep.11 – Using SSH and SCP (Fundamentals)
* Linux CLI: Ep.12 – Using Find (Fundamentals)
* Linux CLI: Ep.13 – Searching and Sorting (Fundamentals)
* Linux CLI: Ep.14 – Using Screen (Fundamentals)
* Linux CLI: Ep.15 – Generating File Hashes (Fundamentals)
* Linux CLI: Ep.16 – Combining Commands (Fundamentals)
* Linux CLI: Ep.17 – Demonstrate Your Skills (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Linux CLI: Ep.5 – File Permissions (Fundamentals)
* Linux CLI: Ep.6 – Editing Files (Fundamentals)
* Linux CLI: Ep.7 – Using wc (Fundamentals)
* Linux CLI: Ep.8 – Manipulating Text (Fundamentals)
* Linux CLI: Ep.9 – Stream Redirection (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)

# Christopher Olowonihi

Blackburn College

Total Labs Completed: **78** | Total Points: **2540** | Total Time: **14 hours 36 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Elliptic Curve Cryptography (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction To Elastic: Ep.1 – What is Elastic? (Defensive Cyber)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to Penetration Test Programs: Ep.2 – Cybersecurity Frameworks (Fundamentals)
* Introduction to Penetration Test Programs: Ep.3 – Defining your Testing Program (Fundamentals)
* Introduction to Penetration Test Programs: Ep.4 – Choosing a Supplier (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Modern Encryption: RSA (Fundamentals)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* OSI Model (Fundamentals)
* OWASP 2021: Ep.1 – Broken Access Control (Application Security, Defensive Cyber, Offensive Cyber)
* OWASP 2021: Ep.2 – Cryptographic Failures (Application Security, Defensive Cyber, Offensive Cyber)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)

# Daniel Queally

Cardinal Newman College

Total Labs Completed: **60** | Total Points: **1940** | Total Time: **5 hours 17 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)

# Daniel Regan

Runshaw College

Total Labs Completed: **200** | Total Points: **8920** | Total Time: **47 hours 12 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* An Introduction to Linux Internals (Defensive Cyber, Offensive Cyber)
* An Introduction to Linux Internals (Defensive Cyber, Offensive Cyber)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Computer Architecture: Demonstrate Your Knowledge (Defensive Cyber, Offensive Cyber)
* Computer Architecture: Demonstrate Your Knowledge (Defensive Cyber, Offensive Cyber)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Disposal of Device Information (Fundamentals)
* ELF Execution Structure (Defensive Cyber, Offensive Cyber)
* ELF Execution Structure (Defensive Cyber, Offensive Cyber)
* Ethics & Laws: Bugbusters (Fundamentals)
* Ethics & Laws: Bugbusters (Fundamentals)
* Ethics & Laws: Burglary and Hacking (Fundamentals)
* Ethics & Laws: Burglary and Hacking (Fundamentals)
* Ethics & Laws: Ethical and Unethical Hacking (Fundamentals)
* Ethics & Laws: Ethical and Unethical Hacking (Fundamentals)
* Ethics & Laws: Police Raid (Fundamentals)
* Ethics & Laws: Police Raid (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Ethics & Laws: US Federal Cyber Law (Fundamentals)
* Ethics & Laws: US Federal Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Internet Protocol V4 (Fundamentals)
* Internet Protocol V4 (Fundamentals)
* Introduction to 32-Bit Architectures (Defensive Cyber, Offensive Cyber)
* Introduction to 32-Bit Architectures (Defensive Cyber, Offensive Cyber)
* Introduction to 64-Bit Architectures (Defensive Cyber, Offensive Cyber)
* Introduction to 64-Bit Architectures (Defensive Cyber, Offensive Cyber)
* Introduction to Computer Memory and Architecture (Defensive Cyber, Offensive Cyber)
* Introduction to Computer Memory and Architecture (Defensive Cyber, Offensive Cyber)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Block Ciphers (Application Security, Fundamentals)
* Introduction to Cryptography: Block Ciphers (Application Security, Fundamentals)
* Introduction to Cryptography: Demonstrate Your Knowledge (Application Security, Fundamentals)
* Introduction to Cryptography: Demonstrate Your Knowledge (Application Security, Fundamentals)
* Introduction to Cryptography: Digital Signatures (Application Security, Fundamentals)
* Introduction to Cryptography: Digital Signatures (Application Security, Fundamentals)
* Introduction to Cryptography: Hashing (Application Security, Fundamentals)
* Introduction to Cryptography: Hashing (Application Security, Fundamentals)
* Introduction to Cryptography: Message Integrity (Application Security, Fundamentals)
* Introduction to Cryptography: Message Integrity (Application Security, Fundamentals)
* Introduction to Cryptography: One-Time Pad (Application Security, Fundamentals)
* Introduction to Cryptography: One-Time Pad (Application Security, Fundamentals)
* Introduction to Cryptography: Public Key Infrastructure (Application Security, Fundamentals)
* Introduction to Cryptography: Public Key Infrastructure (Application Security, Fundamentals)
* Introduction to Cryptography: Public and Private Key Management (Application Security, Fundamentals)
* Introduction to Cryptography: Public and Private Key Management (Application Security, Fundamentals)
* Introduction to Cryptography: Stream Ciphers (Application Security, Fundamentals)
* Introduction to Cryptography: Stream Ciphers (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to Windows Internals (Defensive Cyber, Offensive Cyber)
* Introduction to Windows Internals (Defensive Cyber, Offensive Cyber)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Modern Encryption: RSA (Fundamentals)
* Modern Encryption: RSA (Fundamentals)
* NIST 800-53: Ep.21 – Demonstrate your Knowledge (Defensive Cyber)
* NIST 800-53: Ep.21 – Demonstrate your Knowledge (Defensive Cyber)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* Nmap: Ep.2 – Using Nmap (Offensive Cyber)
* Nmap: Ep.2 – Using Nmap (Offensive Cyber)
* OSI Model (Fundamentals)
* OSI Model (Fundamentals)
* PKI (Public Key Infrastructure) (Fundamentals)
* PKI (Public Key Infrastructure) (Fundamentals)
* Packet Analysis: Packet Capture Basics (Defensive Cyber)
* Packet Analysis: Packet Capture Basics (Defensive Cyber)
* Packet Analysis: Using tcpdump (Defensive Cyber)
* Packet Analysis: Using tcpdump (Defensive Cyber)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Inside of a PE File (Defensive Cyber, Offensive Cyber)
* The Inside of a PE File (Defensive Cyber, Offensive Cyber)
* The Inside of an ELF File (Defensive Cyber, Offensive Cyber)
* The Inside of an ELF File (Defensive Cyber, Offensive Cyber)
* The Internet (Fundamentals)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Web Log Analysis: Ep.3 – Access Logs (Defensive Cyber)
* Web Log Analysis: Ep.3 – Access Logs (Defensive Cyber)
* Web Log Analysis: Ep.4 — Error Logs (Defensive Cyber)
* Web Log Analysis: Ep.4 — Error Logs (Defensive Cyber)
* What Is the Heap? (Defensive Cyber, Offensive Cyber)
* What Is the Heap? (Defensive Cyber, Offensive Cyber)
* What Is the Stack? (Defensive Cyber, Offensive Cyber)
* What Is the Stack? (Defensive Cyber, Offensive Cyber)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wireshark: Display Filters – Diving In (Defensive Cyber)
* Wireshark: Display Filters – Diving In (Defensive Cyber)
* Wireshark: Display Filters – Introduction to Filters (Defensive Cyber)
* Wireshark: Display Filters – Introduction to Filters (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)

# David Ajidagba

Cardinal Newman College

Total Labs Completed: **58** | Total Points: **1480** | Total Time: **2 hours 2 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.3 – Weaponization Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.4 – Delivery Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.5 – Exploitation Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.6 – Installation/Persistence Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.7 – What is the Command and Control (C2) Phase? (Offensive Cyber)
* Cyber Kill Chain: Ep.8 – Actions on Objectives Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.9 – Adversary Simulation (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to Penetration Test Programs: Ep.2 – Cybersecurity Frameworks (Fundamentals)
* Introduction to Penetration Test Programs: Ep.3 – Defining your Testing Program (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* The Internet (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)

# Dominic Hayward

Runshaw College

Total Labs Completed: **76** | Total Points: **2340** | Total Time: **14 hours 45 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: How People Make Security Mistakes (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Human Factors in Cybersecurity: Usable Security (Fundamentals)
* Information Security and Cybersecurity Terminology (Fundamentals)
* Information Security: Starting at the Beginning (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Linux CLI: Ep.5 – File Permissions (Fundamentals)
* Linux CLI: Ep.6 – Editing Files (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Social Engineering: Ep.3 – How Is It Used? (Fundamentals)
* Social Engineering: Ep.4 – Protecting Yourself (Fundamentals)
* Social Engineering: Ep.5 – Demonstrate Your Skills (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (US) (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Importance of Information Security and Cybersecurity (Fundamentals)
* The Internet (Fundamentals)
* What Is Information Security? (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)

# Ellis Evans

Runshaw College

Total Labs Completed: **79** | Total Points: **3400** | Total Time: **9 hours 7 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Hashing (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Modern Encryption: RSA (Fundamentals)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* PKI (Public Key Infrastructure) Practical (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Protocols: DHCPv4 (Fundamentals)
* Protocols: HTTP (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Web Log Analysis: Ep.3 – Access Logs (Defensive Cyber)
* Web Log Analysis: Ep.4 — Error Logs (Defensive Cyber)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wireshark: Display Filters – Introduction to Filters (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)

# Erin Rayworth

Blackpool and the Fylde College

Total Labs Completed: **105** | Total Points: **4670** | Total Time: **20 hours 11 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Authentication: Ep.1 – What is Authentication? (Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* C++: Hardcoded Secrets (Application Security)
* C++: Introduction (Application Security)
* Cyber 101: Cookies (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Data Privacy: Ep.1 – Key Concepts (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Guidance on Remote Working (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction To Elastic: Ep.1 – What is Elastic? (Defensive Cyber)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Hashing (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Metasploit: Ep.1 – What is Metasploit? (Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to Penetration Testing: Infrastructure (Offensive Cyber)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Kusto Query Language: Ep.1 – Introduction to KQL (Cloud Security)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Microsoft Azure Basics: Navigating the Web Portal (Cloud Security)
* Microsoft Azure Basics: Storage Accounts (Cloud Security)
* Modern Encryption: RSA (Fundamentals)
* Nessus: Ep.1 – Introduction to Nessus (Offensive Cyber)
* Nessus: Ep.2 – Network Scanning (Offensive Cyber)
* Nessus: Ep.3 – Authenticated Scanning (Offensive Cyber)
* Nessus: Ep.4 – Scan Results (Offensive Cyber)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* Nmap: Ep.2 – Using Nmap (Offensive Cyber)
* Nmap: Ep.3 – Host Discovery (Offensive Cyber)
* Nmap: Ep.4 – Port Scanning (Offensive Cyber)
* Nmap: Ep.5 – OS and Version Detection (Offensive Cyber)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Deleted Tweet (Offensive Cyber)
* Open Source Intelligence (OSINT): Online Anonymity (Offensive Cyber)
* Open Source Intelligence (OSINT): Search Engines (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media and Privacy (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* PKI (Public Key Infrastructure) Practical (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Privacy (Fundamentals)
* Protocols: HTTP (Fundamentals)
* Python: Code Comments (Application Security)
* Python: Hardcoded Secrets (Application Security)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Social Engineering: Ep.3 – How Is It Used? (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Tor (Offensive Cyber)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Web Log Analysis: Ep.3 – Access Logs (Defensive Cyber)
* Web Log Analysis: Ep.4 — Error Logs (Defensive Cyber)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)

# Eva O’connor

Cardinal Newman College

Total Labs Completed: **20** | Total Points: **270** | Total Time: **2 hours 54 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: How People Make Security Mistakes (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)

# Evan Billington

Cardinal Newman College

Total Labs Completed: **53** | Total Points: **1380** | Total Time: **3 hours 46 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: Burglary and Hacking (Fundamentals)
* Ethics & Laws: Ethical and Unethical Hacking (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Ethics & Laws: US Federal Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)

# Fabian Wnuk-Lipinski

Blackburn College

Total Labs Completed: **87** | Total Points: **3130** | Total Time: **8 hours 4 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* C++: Hardcoded Secrets (Application Security)
* C++: Introduction (Application Security)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Virtual Card Numbers (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.3 – Weaponization Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.4 – Delivery Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.5 – Exploitation Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.6 – Installation/Persistence Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.7 – What is the Command and Control (C2) Phase? (Offensive Cyber)
* Cyber Kill Chain: Ep.8 – Actions on Objectives Phase (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Hashing (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Modern Encryption: RSA (Fundamentals)
* Nessus: Ep.1 – Introduction to Nessus (Offensive Cyber)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Python: Code Comments (Application Security)
* Python: Hardcoded Secrets (Application Security)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)

# Faisal Hussain

Blackburn College

Total Labs Completed: **49** | Total Points: **1040** | Total Time: **2 hours 7 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* OSI Model (Fundamentals)
* PKI (Public Key Infrastructure) (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* The Internet (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)

# Farees Hussein

Cardinal Newman College

Total Labs Completed: **12** | Total Points: **130** | Total Time: **41 minutes**

## Labs Completed:

* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)

# Hamza Ahmed

Blackburn College

Total Labs Completed: **108** | Total Points: **3560** | Total Time: **19 hours 19 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)

# Hannah Bithell

Runshaw College

Total Labs Completed: **82** | Total Points: **3020** | Total Time: **20 hours 2 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.3 – Weaponization Phase (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Elliptic Curve Cryptography (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Linux CLI: Ep.5 – File Permissions (Fundamentals)
* Linux CLI: Ep.6 – Editing Files (Fundamentals)
* Linux CLI: Ep.7 – Using wc (Fundamentals)
* Modern Encryption: RSA (Fundamentals)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Deleted Tweet (Offensive Cyber)
* Open Source Intelligence (OSINT): Shodan.io (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (US) (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Tor (Offensive Cyber)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)

# Harry Chen

Cardinal Newman College

Total Labs Completed: **66** | Total Points: **1960** | Total Time: **10 hours 56 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cookies (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Rogue USB Devices (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* Tactics: Reconnaissance (Defensive Cyber, Offensive Cyber)
* Tactics: Resource Development (Defensive Cyber, Offensive Cyber)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)

# Holly Biddulph

Runshaw College

Total Labs Completed: **85** | Total Points: **3090** | Total Time: **9 hours 16 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.2 – Case Studies (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Browsing Securely: Ep.5 – Demonstrate Your Knowledge (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction To Elastic: Ep.1 – What is Elastic? (Defensive Cyber)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Microsoft Azure Basics: Navigating the Web Portal (Cloud Security)
* Modern Encryption: RSA (Fundamentals)
* Nessus: Ep.1 – Introduction to Nessus (Offensive Cyber)
* Nessus: Ep.2 – Network Scanning (Offensive Cyber)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Physical Security: Ep.2 – Physical Security in Your Workplace (Fundamentals)
* Physical Security: Ep.3 – Physical Security When Working Remotely (Fundamentals)
* Physical Security: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Ports (Fundamentals)
* Protocols: DHCPv4 (Fundamentals)
* Protocols: DNS (Fundamentals)
* Python: Code Comments (Application Security)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Social Engineering: Ep.3 – How Is It Used? (Fundamentals)
* Social Engineering: Ep.4 – Protecting Yourself (Fundamentals)
* Social Engineering: Ep.5 – Demonstrate Your Skills (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Threat Hunt Theory: Introduction (Defensive Cyber)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Web Log Analysis: Ep.3 – Access Logs (Defensive Cyber)
* Web Log Analysis: Ep.4 — Error Logs (Defensive Cyber)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wireshark: Display Filters – Introduction to Filters (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)

# Huzayfah Vorajee

Cardinal Newman College

Total Labs Completed: **54** | Total Points: **1330** | Total Time: **28 hours 56 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)

# Isaac Dickinson

Cardinal Newman College

Total Labs Completed: **17** | Total Points: **170** | Total Time: **1 hours 15 minutes**

## Labs Completed:

* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)

# Israa Khaled Baiza

Runshaw College

Total Labs Completed: **73** | Total Points: **2280** | Total Time: **29 hours 32 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Fake News (Fundamentals)
* Cyber 101: Geolocation (Fundamentals)
* Cyber 101: Virtual Card Numbers (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Modern Encryption: RSA (Fundamentals)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* Physical Security (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)

# Izma Malik

Cardinal Newman College

Total Labs Completed: **19** | Total Points: **190** | Total Time: **48 minutes**

## Labs Completed:

* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)

# Jack Fraser

Runshaw College

Total Labs Completed: **75** | Total Points: **2690** | Total Time: **15 hours 43 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* AI: Prompt Injection Attacks (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* CTI First Principles: Ep.1 – What is Cyber Threat Intelligence? (Cyber Threat Intelligence, Defensive Cyber)
* CTI First Principles: Ep.2 – Lifecycles (Cyber Threat Intelligence, Defensive Cyber)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.3 – Weaponization Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.4 – Delivery Phase (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Hashing (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Shodan.io (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)

# Jack Green

Blackpool and the Fylde College

Total Labs Completed: **154** | Total Points: **9510** | Total Time: **40 hours 36 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* 32-Bit Linux Assembly: Ep.1 – Structure and Registers (Defensive Cyber, Offensive Cyber)
* 32-Bit Windows Assembly: Ep.1 – Windows API and the Stack (Defensive Cyber, Offensive Cyber)
* 64-Bit Windows Assembly: Ep.1 – Windows APIs and Registers (Defensive Cyber, Offensive Cyber)
* AI for Business: Ep.1 – What is AI? (Fundamentals)
* AI for Business: Ep.2 – The Benefits of AI (Fundamentals)
* AI for Business: Ep.3 – The Risks of AI (Fundamentals)
* AI for Business: Ep.4 – Using AI at Work (Fundamentals)
* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Authentication: Ep.1 – What is Authentication? (Fundamentals)
* Authentication: Ep.2 – Why Are Passwords Important? (Fundamentals)
* Authentication: Ep.3 – Creating Secure Passwords (Fundamentals)
* Authentication: Ep.4 – Adding an Extra Layer of Security (Fundamentals)
* Authentication: Ep.5 – Demonstrate Your Knowledge (Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.2 – Case Studies (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Browsing Securely: Ep.5 – Demonstrate Your Knowledge (Fundamentals)
* Burp Suite Basics: HTTPS (Application Security, Offensive Cyber)
* Burp Suite Basics: Introduction (Application Security, Offensive Cyber)
* C++: Hardcoded Secrets (Application Security)
* C++: Introduction (Application Security)
* CVSS Calculator (Cyber Threat Intelligence, Offensive Cyber)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Data Handling: Ep.2 – Gathering, Storing, and Processing Data (Fundamentals)
* Data Handling: Ep.3 – Data Privacy and Access (Fundamentals)
* Data Handling: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Data Privacy: Ep.1 – Key Concepts (Fundamentals)
* Data Privacy: Ep.2 – Data Privacy Regulations (Fundamentals)
* Data Privacy: Ep.3 – What About You? (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Device Security: Ep.2 – Increasing Your Protection (Fundamentals)
* Device Security: Ep.3 – Case Studies (Fundamentals)
* Device Security: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.2 – Case Studies (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Digital Footprint: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* ISO 27001: Ep.1 – What Is ISO 27001? (Fundamentals)
* ISO 27001: Ep.2 – The Domains of ISO 27001 (Fundamentals)
* ISO 27001: Ep.3 – What About You? (Fundamentals)
* Introduction To Elastic: Ep.1 – What is Elastic? (Defensive Cyber)
* Introduction To Elastic: Ep.2 – Querying Data (Defensive Cyber)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Hashing (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to Reverse Engineering: 32-Bit Linux – Part 1 (Defensive Cyber, Offensive Cyber)
* Introduction to Reverse Engineering: 32-Bit Windows – Part 1 (Defensive Cyber, Offensive Cyber)
* Introduction to Reverse Engineering: 64-Bit Windows – Part 1 (Defensive Cyber, Offensive Cyber)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Kerberos: Ep.2 – Enumeration (Offensive Cyber)
* Kusto Query Language: Ep.1 – Introduction to KQL (Cloud Security)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Microsoft Azure Basics: Navigating the Web Portal (Cloud Security)
* Microsoft Azure Basics: Storage Accounts (Cloud Security)
* Modern Encryption: RSA (Fundamentals)
* Nessus: Ep.1 – Introduction to Nessus (Offensive Cyber)
* Nessus: Ep.2 – Network Scanning (Offensive Cyber)
* Nessus: Ep.3 – Authenticated Scanning (Offensive Cyber)
* Nessus: Ep.4 – Scan Results (Offensive Cyber)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* Nmap: Ep.2 – Using Nmap (Offensive Cyber)
* Nmap: Ep.3 – Host Discovery (Offensive Cyber)
* Nmap: Ep.4 – Port Scanning (Offensive Cyber)
* Nmap: Ep.5 – OS and Version Detection (Offensive Cyber)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* PKI (Public Key Infrastructure) Practical (Fundamentals)
* Packet Analysis: Packet Capture Basics (Defensive Cyber)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Physical Security: Ep.2 – Physical Security in Your Workplace (Fundamentals)
* Physical Security: Ep.3 – Physical Security When Working Remotely (Fundamentals)
* Physical Security: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Ports (Fundamentals)
* Protocols: ARP (Fundamentals)
* Protocols: DHCPv4 (Fundamentals)
* Protocols: DHCPv6 (Fundamentals)
* Protocols: DNS (Fundamentals)
* Protocols: FTP (Fundamentals)
* Protocols: HTTP (Fundamentals)
* Python: Code Comments (Application Security)
* Python: Hardcoded Secrets (Application Security)
* SQL Injection: File Download (Offensive Cyber)
* SQL Injection: UNION (Offensive Cyber)
* SQLi Basics: Basic SQL Injection (Offensive Cyber)
* SQLi Basics: Filter Evasion (Offensive Cyber)
* SQLi Basics: Hidden Data (Offensive Cyber)
* SQLi Basics: UNION Query (Offensive Cyber)
* Scanning: Network Scanning (Defensive Cyber, Offensive Cyber)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Security Reporting and Responsiveness: Ep.1 – Reporting Incidents and Concerns (Fundamentals)
* Security Reporting and Responsiveness: Ep.2 – Case Studies (Fundamentals)
* Security Reporting and Responsiveness: Ep.3 – Responding Appropriately (Fundamentals)
* Security Reporting and Responsiveness: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Social Engineering: Ep.3 – How Is It Used? (Fundamentals)
* Social Engineering: Ep.4 – Protecting Yourself (Fundamentals)
* Social Engineering: Ep.5 – Demonstrate Your Skills (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (US) (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Web Log Analysis: Ep.3 – Access Logs (Defensive Cyber)
* Web Log Analysis: Ep.4 — Error Logs (Defensive Cyber)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wireshark: Display Filters – Introduction to Filters (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)

# Jack Holloway

Blackpool and the Fylde College

Total Labs Completed: **135** | Total Points: **4030** | Total Time: **15 hours 38 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI Challenges: Beat the Bot (Challenges & Scenarios)
* AI for Business: Ep.1 – What is AI? (Fundamentals)
* AI for Business: Ep.2 – The Benefits of AI (Fundamentals)
* AI for Business: Ep.3 – The Risks of AI (Fundamentals)
* AI for Business: Ep.4 – Using AI at Work (Fundamentals)
* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Authentication: Ep.1 – What is Authentication? (Fundamentals)
* Authentication: Ep.2 – Why Are Passwords Important? (Fundamentals)
* Authentication: Ep.3 – Creating Secure Passwords (Fundamentals)
* Authentication: Ep.4 – Adding an Extra Layer of Security (Fundamentals)
* Authentication: Ep.5 – Demonstrate Your Knowledge (Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* CTI First Principles: Ep.1 – What is Cyber Threat Intelligence? (Cyber Threat Intelligence, Defensive Cyber)
* CTI First Principles: Ep.2 – Lifecycles (Cyber Threat Intelligence, Defensive Cyber)
* Cyber 101: Cookies (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Fake News (Fundamentals)
* Cyber 101: Geolocation (Fundamentals)
* Cyber 101: Information Security (Fundamentals)
* Cyber 101: Keylogging (Fundamentals)
* Cyber 101: Rogue USB Devices (Fundamentals)
* Cyber 101: Security Champions (Fundamentals)
* Cyber 101: Virtual Card Numbers (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.3 – Weaponization Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.4 – Delivery Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.5 – Exploitation Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.6 – Installation/Persistence Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.7 – What is the Command and Control (C2) Phase? (Offensive Cyber)
* Cyber Kill Chain: Ep.8 – Actions on Objectives Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.9 – Adversary Simulation (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Data Privacy: Ep.2 – Data Privacy Regulations (Fundamentals)
* Deepfakes (Cyber Threat Intelligence)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Elliptic Curve Cryptography (Fundamentals)
* Encoding: ASCII (Fundamentals)
* Encoding: Binary (Fundamentals)
* Encoding: Hexadecimal (Fundamentals)
* Encoding: What is Encoding? (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Guidance on Remote Working (Fundamentals)
* History of Information Security (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* ISO 27018: Ep.1 – Introduction (Fundamentals)
* ISO 27018: Ep.2 – Human Resource and Physical Security (Fundamentals)
* Incident Response in the Workplace (Fundamentals)
* Information Security and Cybersecurity Terminology (Fundamentals)
* Information Security: Starting at the Beginning (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Digital Signatures (Application Security, Fundamentals)
* Introduction to Cryptography: Message Integrity (Application Security, Fundamentals)
* Introduction to Cryptography: One-Time Pad (Application Security, Fundamentals)
* Introduction to Cryptography: Public Key Infrastructure (Application Security, Fundamentals)
* Introduction to Cryptography: Stream Ciphers (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Networking: Ep.6 — Domain Name System (Fundamentals)
* Introduction to Penetration Testing: Infrastructure (Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* NIST 800-53: Ep.1 – Access Control (Defensive Cyber)
* NIST 800-53: Security and Privacy Controls for Information Systems and Organizations (Defensive Cyber)
* OSI Model (Fundamentals)
* PKI (Public Key Infrastructure) (Fundamentals)
* Personal Devices in the Workplace (Fundamentals)
* Physical Security (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Privacy (Fundamentals)
* Privileged Access (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Security On The Go (Fundamentals)
* Security Reporting and Responsiveness: Ep.1 – Reporting Incidents and Concerns (Fundamentals)
* Security Reporting and Responsiveness: Ep.2 – Case Studies (Fundamentals)
* Security Reporting and Responsiveness: Ep.3 – Responding Appropriately (Fundamentals)
* Shoulder Surfing (Fundamentals)
* Social Engineering (Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Social Engineering: Ep.3 – How Is It Used? (Fundamentals)
* Social Engineering: Ep.4 – Protecting Yourself (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (US) (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* TLS Fundamentals: Ep.1 – Introduction (Application Security)
* The History of Encryption (Fundamentals)
* The Importance of Information Security and Cybersecurity (Fundamentals)
* The Internet (Fundamentals)
* Threat Hunting: Introduction (Cyber Threat Intelligence, Defensive Cyber)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* What Is Information Security? (Fundamentals)
* What Is Risk? (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)

# Jack Hughes

Blackpool and the Fylde College

Total Labs Completed: **32** | Total Points: **430** | Total Time: **3 hours 28 minutes**

## Labs Completed:

* Cyber 101: Cyber Kill Chain (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Ethics & Laws: US Federal Cyber Law (Fundamentals)
* Guidance on Remote Working (Fundamentals)
* Human Factors in Cybersecurity: How People Make Security Mistakes (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Human Factors in Cybersecurity: Usable Security (Fundamentals)
* Incident Response in the Workplace (Fundamentals)
* Physical Security (Fundamentals)
* Privileged Access (Fundamentals)
* Secure Data Handling (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Security On The Go (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (US) (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)

# Jack Ramsay

Blackpool and the Fylde College

Total Labs Completed: **68** | Total Points: **2090** | Total Time: **13 hours 21 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Geolocation (Fundamentals)
* Cyber 101: Virtual Card Numbers (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.3 – Weaponization Phase (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Find the Flaw: Node.js (JavaScript) – Injection (Application Security)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Node.js API: Introduction (Application Security)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)

# Jacob Hill

Blackpool and the Fylde College

Total Labs Completed: **35** | Total Points: **500** | Total Time: **4 hours 12 minutes**

## Labs Completed:

* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Physical Security (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (US) (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)

# Jacob Kenyon

Runshaw College

Total Labs Completed: **77** | Total Points: **2140** | Total Time: **4 hours 36 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.2 – Case Studies (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Browsing Securely: Ep.5 – Demonstrate Your Knowledge (Fundamentals)
* Cyber 101: Cookies (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Rogue USB Devices (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Device Security: Ep.2 – Increasing Your Protection (Fundamentals)
* Device Security: Ep.3 – Case Studies (Fundamentals)
* Device Security: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: Bugbusters (Fundamentals)
* Ethics & Laws: Burglary and Hacking (Fundamentals)
* Ethics & Laws: Ethical and Unethical Hacking (Fundamentals)
* Ethics & Laws: Police Raid (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Ethics & Laws: US Federal Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Physical Security: Ep.2 – Physical Security in Your Workplace (Fundamentals)
* Physical Security: Ep.3 – Physical Security When Working Remotely (Fundamentals)
* Physical Security: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Social Engineering: Ep.3 – How Is It Used? (Fundamentals)
* Social Engineering: Ep.4 – Protecting Yourself (Fundamentals)
* Social Engineering: Ep.5 – Demonstrate Your Skills (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)

# James Birch

Blackburn College

Total Labs Completed: **64** | Total Points: **1460** | Total Time: **2 hours 6 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.10 – Demonstrate Your Knowledge (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.3 – Weaponization Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.4 – Delivery Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.5 – Exploitation Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.6 – Installation/Persistence Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.7 – What is the Command and Control (C2) Phase? (Offensive Cyber)
* Cyber Kill Chain: Ep.8 – Actions on Objectives Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.9 – Adversary Simulation (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Guidance on Remote Working (Fundamentals)
* History of Information Security (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Incident Response in the Workplace (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* OSI Model (Fundamentals)
* Personal Devices in the Workplace (Fundamentals)
* Physical Security (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Privileged Access (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Security On The Go (Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)

# Jamie Rudge

Blackpool and the Fylde College

Total Labs Completed: **78** | Total Points: **2260** | Total Time: **9 hours 48 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cookies (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Geolocation (Fundamentals)
* Cyber 101: Rogue USB Devices (Fundamentals)
* Cyber 101: Virtual Card Numbers (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Guidance on Remote Working (Fundamentals)
* Hack Your First Web App: Ep.1 – Ozone Energy (Offensive Cyber)
* History of Information Security (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Incident Response in the Workplace (Fundamentals)
* Information Security and Cybersecurity Terminology (Fundamentals)
* Information Security: Starting at the Beginning (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* Personal Devices in the Workplace (Fundamentals)
* Physical Security (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Privileged Access (Fundamentals)
* Python: Code Comments (Application Security)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Security On The Go (Fundamentals)
* Shoulder Surfing (Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (US) (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Importance of Information Security and Cybersecurity (Fundamentals)
* The Internet (Fundamentals)
* What Is Information Security? (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)

# Jibran Shafi

Blackburn College

Total Labs Completed: **61** | Total Points: **1960** | Total Time: **18 hours 6 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)

# Joseph Thompson

Cardinal Newman College

Total Labs Completed: **3** | Total Points: **30** | Total Time: **30 minutes**

## Labs Completed:

* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)

# Josh Nolan

Runshaw College

Total Labs Completed: **104** | Total Points: **5990** | Total Time: **29 hours 17 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Burp Suite Basics: HTTPS (Application Security, Offensive Cyber)
* Burp Suite Basics: Introduction (Application Security, Offensive Cyber)
* C++: Hardcoded Secrets (Application Security)
* C++: Introduction (Application Security)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction To Elastic: Ep.1 – What is Elastic? (Defensive Cyber)
* Introduction To Elastic: Ep.2 – Querying Data (Defensive Cyber)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Hashing (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Kusto Query Language: Ep.1 – Introduction to KQL (Cloud Security)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Microsoft Azure Basics: Navigating the Web Portal (Cloud Security)
* Microsoft Azure Basics: Storage Accounts (Cloud Security)
* Modern Encryption: RSA (Fundamentals)
* Nessus: Ep.1 – Introduction to Nessus (Offensive Cyber)
* Nessus: Ep.2 – Network Scanning (Offensive Cyber)
* Nessus: Ep.3 – Authenticated Scanning (Offensive Cyber)
* Nessus: Ep.4 – Scan Results (Offensive Cyber)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* Nmap: Ep.2 – Using Nmap (Offensive Cyber)
* Nmap: Ep.3 – Host Discovery (Offensive Cyber)
* Nmap: Ep.4 – Port Scanning (Offensive Cyber)
* Nmap: Ep.5 – OS and Version Detection (Offensive Cyber)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* PKI (Public Key Infrastructure) Practical (Fundamentals)
* Packet Analysis: Packet Capture Basics (Defensive Cyber)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Protocols: ARP (Fundamentals)
* Protocols: DHCPv4 (Fundamentals)
* Protocols: DHCPv6 (Fundamentals)
* Protocols: DNS (Fundamentals)
* Protocols: FTP (Fundamentals)
* Protocols: HTTP (Fundamentals)
* Python: Code Comments (Application Security)
* Python: Hardcoded Secrets (Application Security)
* Scanning: Network Scanning (Defensive Cyber, Offensive Cyber)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Web Log Analysis: Ep.3 – Access Logs (Defensive Cyber)
* Web Log Analysis: Ep.4 — Error Logs (Defensive Cyber)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wireshark: Display Filters – Introduction to Filters (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)

# Joshua Kurian

Runshaw College

Total Labs Completed: **73** | Total Points: **2520** | Total Time: **6 hours 51 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.3 – Weaponization Phase (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* Nmap: Ep.2 – Using Nmap (Offensive Cyber)
* Nmap: Ep.3 – Host Discovery (Offensive Cyber)
* Nmap: Ep.4 – Port Scanning (Offensive Cyber)
* Nmap: Ep.5 – OS and Version Detection (Offensive Cyber)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wireshark: Display Filters – Introduction to Filters (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)

# Joshua Lamprecht

Runshaw College

Total Labs Completed: **90** | Total Points: **4200** | Total Time: **15 hours 56 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* 32-Bit Linux Assembly: Ep.1 – Structure and Registers (Defensive Cyber, Offensive Cyber)
* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Hashing (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Networking: Ep.6 — Domain Name System (Fundamentals)
* Introduction to Networking: Ep.7 — Demonstrate Your Knowledge (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Modern Encryption: RSA (Fundamentals)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* Packet Analysis: Packet Capture Basics (Defensive Cyber)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Protocols: DHCPv4 (Fundamentals)
* Protocols: DHCPv6 (Fundamentals)
* Protocols: DNS (Fundamentals)
* Protocols: HTTP (Fundamentals)
* Python: Code Comments (Application Security)
* Python: Hardcoded Secrets (Application Security)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Social Engineering: Ep.3 – How Is It Used? (Fundamentals)
* Social Engineering: Ep.4 – Protecting Yourself (Fundamentals)
* Social Engineering: Ep.5 – Demonstrate Your Skills (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Web Log Analysis: Ep.3 – Access Logs (Defensive Cyber)
* Web Log Analysis: Ep.4 — Error Logs (Defensive Cyber)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wireshark: Display Filters – Introduction to Filters (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)

# Jozef Royston

Runshaw College

Total Labs Completed: **79** | Total Points: **2950** | Total Time: **5 hours 52 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Virtual Card Numbers (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.3 – Weaponization Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.4 – Delivery Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.5 – Exploitation Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.6 – Installation/Persistence Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.7 – What is the Command and Control (C2) Phase? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Hashing (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Modern Encryption: RSA (Fundamentals)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* PKI (Public Key Infrastructure) Practical (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wireshark: Display Filters – Introduction to Filters (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)

# Junior Hardman

Blackpool and the Fylde College

Total Labs Completed: **61** | Total Points: **1860** | Total Time: **3 hours 34 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Virtual Card Numbers (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (US) (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)

# Kallel Marsden

Blackpool and the Fylde College

Total Labs Completed: **63** | Total Points: **1910** | Total Time: **12 hours 15 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Virtual Card Numbers (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.2 – Case Studies (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Data Handling (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (US) (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)

# Kausar Hussain

Runshaw College

Total Labs Completed: **62** | Total Points: **1870** | Total Time: **14 hours 55 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Authentication: Ep.1 – What is Authentication? (Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Data Privacy: Ep.1 – Key Concepts (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Privacy (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)

# Kellylee Illingworth-Turner

Cardinal Newman College

Total Labs Completed: **9** | Total Points: **90** | Total Time: **20 minutes**

## Labs Completed:

* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)

# Kerry Harrison

STEM Bursary Management Direct Members

Total Labs Completed: **58** | Total Points: **1180** | Total Time: **6 hours 56 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cookies (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Rogue USB Devices (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.2 – Case Studies (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Digital Footprint: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Physical Security: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Social Engineering: Ep.5 – Demonstrate Your Skills (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (US) (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)

# Korshan Singh-Dhillon

Blackpool and the Fylde College

Total Labs Completed: **99** | Total Points: **2620** | Total Time: **11 hours 19 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* CTI First Principles: Ep.1 – What is Cyber Threat Intelligence? (Cyber Threat Intelligence, Defensive Cyber)
* CTI First Principles: Ep.2 – Lifecycles (Cyber Threat Intelligence, Defensive Cyber)
* CTI First Principles: Ep.3 – Models and Methodologies (Cyber Threat Intelligence, Defensive Cyber)
* CTI First Principles: Ep.4 – Threat Actors and Attribution (Cyber Threat Intelligence, Defensive Cyber)
* CTI First Principles: Ep.5 – Threat Intelligence Sources (Cyber Threat Intelligence, Defensive Cyber)
* CTI First Principles: Ep.6 – Decomposition and Visualization (Cyber Threat Intelligence, Defensive Cyber)
* Cyber 101: Cookies (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Fake News (Fundamentals)
* Cyber 101: Geolocation (Fundamentals)
* Cyber 101: Information Security (Fundamentals)
* Cyber 101: Keylogging (Fundamentals)
* Cyber 101: Rogue USB Devices (Fundamentals)
* Cyber 101: Security Champions (Fundamentals)
* Cyber 101: Virtual Card Numbers (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Guidance on Remote Working (Fundamentals)
* History of Information Security (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Incident Response in the Workplace (Fundamentals)
* Information Security and Cybersecurity Terminology (Fundamentals)
* Information Security: Starting at the Beginning (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* NIST 800-53: Ep.1 – Access Control (Defensive Cyber)
* OSI Model (Fundamentals)
* Personal Devices in the Workplace (Fundamentals)
* Physical Security (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Privacy (Fundamentals)
* Privileged Access (Fundamentals)
* Secure Data Handling (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: Attribution and Accountability (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: Authentication (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: Authorization (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: Defense in Depth (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: Least Privileges (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: Security Patching (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Security On The Go (Fundamentals)
* Shoulder Surfing (Fundamentals)
* Social Engineering (Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (US) (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Importance of Information Security and Cybersecurity (Fundamentals)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* What Is Information Security? (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)

# Lewis Jackson

Blackpool and the Fylde College

Total Labs Completed: **53** | Total Points: **950** | Total Time: **2 hours 55 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.3 – Weaponization Phase (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Social Engineering: Ep.3 – How Is It Used? (Fundamentals)
* Social Engineering: Ep.4 – Protecting Yourself (Fundamentals)
* Social Engineering: Ep.5 – Demonstrate Your Skills (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* The Internet (Fundamentals)

# Luke Brown

Runshaw College

Total Labs Completed: **113** | Total Points: **7710** | Total Time: **22 hours 24 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* 32-Bit Linux Assembly: Ep.1 – Structure and Registers (Defensive Cyber, Offensive Cyber)
* 32-Bit Windows Assembly: Ep.1 – Windows API and the Stack (Defensive Cyber, Offensive Cyber)
* 64-Bit Windows Assembly: Ep.1 – Windows APIs and Registers (Defensive Cyber, Offensive Cyber)
* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Burp Suite Basics: HTTPS (Application Security, Offensive Cyber)
* Burp Suite Basics: Introduction (Application Security, Offensive Cyber)
* C++: Hardcoded Secrets (Application Security)
* C++: Introduction (Application Security)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.2 – Case Studies (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Digital Footprint: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction To Elastic: Ep.1 – What is Elastic? (Defensive Cyber)
* Introduction To Elastic: Ep.2 – Querying Data (Defensive Cyber)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Hashing (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to Reverse Engineering: 32-Bit Linux – Part 1 (Defensive Cyber, Offensive Cyber)
* Introduction to Reverse Engineering: 32-Bit Windows – Part 1 (Defensive Cyber, Offensive Cyber)
* Introduction to Reverse Engineering: 64-Bit Windows – Part 1 (Defensive Cyber, Offensive Cyber)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Kusto Query Language: Ep.1 – Introduction to KQL (Cloud Security)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Microsoft Azure Basics: Navigating the Web Portal (Cloud Security)
* Microsoft Azure Basics: Storage Accounts (Cloud Security)
* Modern Encryption: RSA (Fundamentals)
* Nessus: Ep.1 – Introduction to Nessus (Offensive Cyber)
* Nessus: Ep.2 – Network Scanning (Offensive Cyber)
* Nessus: Ep.3 – Authenticated Scanning (Offensive Cyber)
* Nessus: Ep.4 – Scan Results (Offensive Cyber)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* Nmap: Ep.2 – Using Nmap (Offensive Cyber)
* Nmap: Ep.3 – Host Discovery (Offensive Cyber)
* Nmap: Ep.4 – Port Scanning (Offensive Cyber)
* Nmap: Ep.5 – OS and Version Detection (Offensive Cyber)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* PKI (Public Key Infrastructure) Practical (Fundamentals)
* Packet Analysis: Packet Capture Basics (Defensive Cyber)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Protocols: ARP (Fundamentals)
* Protocols: DHCPv4 (Fundamentals)
* Protocols: DHCPv6 (Fundamentals)
* Protocols: DNS (Fundamentals)
* Protocols: FTP (Fundamentals)
* Protocols: HTTP (Fundamentals)
* Python: Code Comments (Application Security)
* Python: Hardcoded Secrets (Application Security)
* SQL Injection: File Download (Offensive Cyber)
* Scanning: Network Scanning (Defensive Cyber, Offensive Cyber)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Web Log Analysis: Ep.3 – Access Logs (Defensive Cyber)
* Web Log Analysis: Ep.4 — Error Logs (Defensive Cyber)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wireshark: Display Filters – Introduction to Filters (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)

# Luke R

STEM Bursary Management Direct Members

Total Labs Completed: **1** | Total Points: **200** | Total Time: **12 minutes**

## Labs Completed:

* Hack Your First PC: Ep.1 — Ozone Energy (Offensive Cyber)

# Lydia Wright

Cardinal Newman College

Total Labs Completed: **5** | Total Points: **50** | Total Time: **14 minutes**

## Labs Completed:

* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)

# Madiha Bux

Cardinal Newman College

Total Labs Completed: **3** | Total Points: **30** | Total Time: **8 minutes**

## Labs Completed:

* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)

# Mariana Berrill

Cardinal Newman College

Total Labs Completed: **22** | Total Points: **250** | Total Time: **1 hours 29 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)

# Markus Woods

Blackpool and the Fylde College

Total Labs Completed: **8** | Total Points: **570** | Total Time: **28 minutes**

## Labs Completed:

* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Linux CLI: Ep.7 – Using wc (Fundamentals)
* PKI (Public Key Infrastructure) (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)

# Mashhood Hussain

Blackburn College

Total Labs Completed: **67** | Total Points: **2270** | Total Time: **7 hours 16 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Hashing (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Modern Encryption: RSA (Fundamentals)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)

# Millie Farrington

Cardinal Newman College

Total Labs Completed: **69** | Total Points: **2120** | Total Time: **3 hours 9 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.3 – Weaponization Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.4 – Delivery Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.5 – Exploitation Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.6 – Installation/Persistence Phase (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.2 – Case Studies (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Digital Footprint: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Modern Encryption: RSA (Fundamentals)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Protocols: HTTP (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Web Log Analysis: Ep.3 – Access Logs (Defensive Cyber)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)

# Mohammed Awais Nadeem

Blackburn College

Total Labs Completed: **114** | Total Points: **7920** | Total Time: **27 hours 50 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* 32-Bit Linux Assembly: Ep.1 – Structure and Registers (Defensive Cyber, Offensive Cyber)
* 32-Bit Windows Assembly: Ep.1 – Windows API and the Stack (Defensive Cyber, Offensive Cyber)
* 64-Bit Windows Assembly: Ep.1 – Windows APIs and Registers (Defensive Cyber, Offensive Cyber)
* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Burp Suite Basics: HTTPS (Application Security, Offensive Cyber)
* Burp Suite Basics: Introduction (Application Security, Offensive Cyber)
* C++: Hardcoded Secrets (Application Security)
* C++: Introduction (Application Security)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction To Elastic: Ep.1 – What is Elastic? (Defensive Cyber)
* Introduction To Elastic: Ep.2 – Querying Data (Defensive Cyber)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Hashing (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to Reverse Engineering: 32-Bit Linux – Part 1 (Defensive Cyber, Offensive Cyber)
* Introduction to Reverse Engineering: 32-Bit Windows – Part 1 (Defensive Cyber, Offensive Cyber)
* Introduction to Reverse Engineering: 64-Bit Windows – Part 1 (Defensive Cyber, Offensive Cyber)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Kerberos: Ep.2 – Enumeration (Offensive Cyber)
* Kusto Query Language: Ep.1 – Introduction to KQL (Cloud Security)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Microsoft Azure Basics: Navigating the Web Portal (Cloud Security)
* Microsoft Azure Basics: Storage Accounts (Cloud Security)
* Modern Encryption: RSA (Fundamentals)
* Nessus: Ep.1 – Introduction to Nessus (Offensive Cyber)
* Nessus: Ep.2 – Network Scanning (Offensive Cyber)
* Nessus: Ep.3 – Authenticated Scanning (Offensive Cyber)
* Nessus: Ep.4 – Scan Results (Offensive Cyber)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* Nmap: Ep.2 – Using Nmap (Offensive Cyber)
* Nmap: Ep.3 – Host Discovery (Offensive Cyber)
* Nmap: Ep.4 – Port Scanning (Offensive Cyber)
* Nmap: Ep.5 – OS and Version Detection (Offensive Cyber)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* PKI (Public Key Infrastructure) Practical (Fundamentals)
* Packet Analysis: Packet Capture Basics (Defensive Cyber)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Protocols: ARP (Fundamentals)
* Protocols: DHCPv4 (Fundamentals)
* Protocols: DHCPv6 (Fundamentals)
* Protocols: DNS (Fundamentals)
* Protocols: FTP (Fundamentals)
* Protocols: HTTP (Fundamentals)
* Python: Code Comments (Application Security)
* Python: Hardcoded Secrets (Application Security)
* SQL Injection: File Download (Offensive Cyber)
* Scanning: Network Scanning (Defensive Cyber, Offensive Cyber)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (US) (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Web Log Analysis: Ep.3 – Access Logs (Defensive Cyber)
* Web Log Analysis: Ep.4 — Error Logs (Defensive Cyber)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wireshark: Display Filters – Introduction to Filters (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)

# Mohammed Hajat

Blackburn College

Total Labs Completed: **108** | Total Points: **3560** | Total Time: **19 hours 2 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)

# Mohammed Sidat

Blackburn College

Total Labs Completed: **61** | Total Points: **1900** | Total Time: **9 hours 58 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.10 – Demonstrate Your Knowledge (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.3 – Weaponization Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.4 – Delivery Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.5 – Exploitation Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.6 – Installation/Persistence Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.7 – What is the Command and Control (C2) Phase? (Offensive Cyber)
* Cyber Kill Chain: Ep.8 – Actions on Objectives Phase (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)

# Muhammad Bilal

Blackburn College

Total Labs Completed: **108** | Total Points: **7190** | Total Time: **31 hours 31 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* 32-Bit Linux Assembly: Ep.1 – Structure and Registers (Defensive Cyber, Offensive Cyber)
* 32-Bit Windows Assembly: Ep.1 – Windows API and the Stack (Defensive Cyber, Offensive Cyber)
* 64-Bit Windows Assembly: Ep.1 – Windows APIs and Registers (Defensive Cyber, Offensive Cyber)
* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* C++: Hardcoded Secrets (Application Security)
* C++: Introduction (Application Security)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction To Elastic: Ep.1 – What is Elastic? (Defensive Cyber)
* Introduction To Elastic: Ep.2 – Querying Data (Defensive Cyber)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Hashing (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to Reverse Engineering: 32-Bit Linux – Part 1 (Defensive Cyber, Offensive Cyber)
* Introduction to Reverse Engineering: 32-Bit Windows – Part 1 (Defensive Cyber, Offensive Cyber)
* Introduction to Reverse Engineering: 64-Bit Windows – Part 1 (Defensive Cyber, Offensive Cyber)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Kusto Query Language: Ep.1 – Introduction to KQL (Cloud Security)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Microsoft Azure Basics: Navigating the Web Portal (Cloud Security)
* Microsoft Azure Basics: Storage Accounts (Cloud Security)
* Modern Encryption: RSA (Fundamentals)
* Nessus: Ep.1 – Introduction to Nessus (Offensive Cyber)
* Nessus: Ep.2 – Network Scanning (Offensive Cyber)
* Nessus: Ep.3 – Authenticated Scanning (Offensive Cyber)
* Nessus: Ep.4 – Scan Results (Offensive Cyber)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* Nmap: Ep.2 – Using Nmap (Offensive Cyber)
* Nmap: Ep.3 – Host Discovery (Offensive Cyber)
* Nmap: Ep.4 – Port Scanning (Offensive Cyber)
* Nmap: Ep.5 – OS and Version Detection (Offensive Cyber)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* PKI (Public Key Infrastructure) Practical (Fundamentals)
* Packet Analysis: Packet Capture Basics (Defensive Cyber)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Protocols: ARP (Fundamentals)
* Protocols: DHCPv4 (Fundamentals)
* Protocols: DHCPv6 (Fundamentals)
* Protocols: DNS (Fundamentals)
* Protocols: FTP (Fundamentals)
* Protocols: HTTP (Fundamentals)
* Python: Code Comments (Application Security)
* Python: Hardcoded Secrets (Application Security)
* Scanning: Network Scanning (Defensive Cyber, Offensive Cyber)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Web Log Analysis: Ep.3 – Access Logs (Defensive Cyber)
* Web Log Analysis: Ep.4 — Error Logs (Defensive Cyber)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wireshark: Display Filters – Introduction to Filters (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)

# Muhammad Hammad

Blackburn College

Total Labs Completed: **60** | Total Points: **1070** | Total Time: **3 hours 31 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Guidance on Remote Working (Fundamentals)
* History of Information Security (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Incident Response in the Workplace (Fundamentals)
* Information Security and Cybersecurity Terminology (Fundamentals)
* Information Security: Starting at the Beginning (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* OSI Model (Fundamentals)
* Personal Devices in the Workplace (Fundamentals)
* Physical Security (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Privacy (Fundamentals)
* Privileged Access (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Security On The Go (Fundamentals)
* Shoulder Surfing (Fundamentals)
* Social Engineering (Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (US) (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* The Importance of Information Security and Cybersecurity (Fundamentals)
* The Internet (Fundamentals)
* What Is Information Security? (Fundamentals)

# Neng Yang

Blackpool and the Fylde College

Total Labs Completed: **56** | Total Points: **1300** | Total Time: **2 hours 46 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to Penetration Test Programs: Ep.2 – Cybersecurity Frameworks (Fundamentals)
* Introduction to Penetration Test Programs: Ep.3 – Defining your Testing Program (Fundamentals)
* Introduction to Penetration Test Programs: Ep.4 – Choosing a Supplier (Fundamentals)
* Introduction to Penetration Test Programs: Ep.5 – Testing Management (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* The Internet (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)

# Owais Akhtar

Blackburn College

Total Labs Completed: **45** | Total Points: **1000** | Total Time: **7 hours 43 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)

# Phoebe Skalik

Blackpool and the Fylde College

Total Labs Completed: **47** | Total Points: **1140** | Total Time: **1 hours 54 minutes**

## Labs Completed:

* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Social Engineering: Ep.3 – How Is It Used? (Fundamentals)
* Social Engineering: Ep.4 – Protecting Yourself (Fundamentals)
* Social Engineering: Ep.5 – Demonstrate Your Skills (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (US) (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)

# Pranesh Patel

Cardinal Newman College

Total Labs Completed: **80** | Total Points: **3190** | Total Time: **11 hours 12 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* C++: Introduction (Application Security)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Elliptic Curve Cryptography (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction To Elastic: Ep.1 – What is Elastic? (Defensive Cyber)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Hashing (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Microsoft Azure Basics: Navigating the Web Portal (Cloud Security)
* Microsoft Azure Basics: Storage Accounts (Cloud Security)
* Modern Encryption: RSA (Fundamentals)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Shodan.io (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Protocols: HTTP (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wireshark: Display Filters – Introduction to Filters (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)

# Ralph Pollard

Cardinal Newman College

Total Labs Completed: **42** | Total Points: **760** | Total Time: **3 hours 39 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* The Internet (Fundamentals)

# Rayyan Vally

Cardinal Newman College

Total Labs Completed: **58** | Total Points: **1820** | Total Time: **6 hours 33 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)

# Reece Munnings

Cardinal Newman College

Total Labs Completed: **58** | Total Points: **1820** | Total Time: **4 hours 22 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)

# Rehan Bhombal

Blackburn College

Total Labs Completed: **52** | Total Points: **1580** | Total Time: **10 hours 42 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)

# Rhys Webster

Runshaw College

Total Labs Completed: **50** | Total Points: **1130** | Total Time: **4 hours 30 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* OSI Model (Fundamentals)
* PKI (Public Key Infrastructure) (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)

# Ruqaiyah Muzzammil

Runshaw College

Total Labs Completed: **70** | Total Points: **2230** | Total Time: **16 hours 5 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Artificial Intelligence for Incident Responders (Application Security, Defensive Cyber, Fundamentals)
* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Generative AI Models (Application Security, Defensive Cyber, Fundamentals)
* AI: Image Classification (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* AI: TensorFlow for Machine Learning (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Public and Private Key Management (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Modern Encryption: RSA (Fundamentals)
* OSI Model (Fundamentals)
* PKI (Public Key Infrastructure) (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)

# Saad Rafi

Blackburn College

Total Labs Completed: **72** | Total Points: **2090** | Total Time: **5 hours 42 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cookies (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Fake News (Fundamentals)
* Cyber 101: Geolocation (Fundamentals)
* Cyber 101: Information Security (Fundamentals)
* Cyber 101: Keylogging (Fundamentals)
* Cyber 101: Rogue USB Devices (Fundamentals)
* Cyber 101: Security Champions (Fundamentals)
* Cyber 101: Virtual Card Numbers (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)

# Sufyan Ul Haq

Blackburn College

Total Labs Completed: **41** | Total Points: **610** | Total Time: **6 hours 0 minutes**

## Labs Completed:

* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: Demonstrate Your Understanding (Fundamentals)
* Human Factors in Cybersecurity: How People Make Security Mistakes (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Human Factors in Cybersecurity: Security Awareness and Behavior Change (Fundamentals)
* Human Factors in Cybersecurity: Security Culture (Fundamentals)
* Human Factors in Cybersecurity: Usable Security (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Physical Security (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Privileged Access (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* The Internet (Fundamentals)

# Szymon Bester

Runshaw College

Total Labs Completed: **73** | Total Points: **3010** | Total Time: **16 hours 31 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* 32-Bit Linux Assembly: Ep.1 – Structure and Registers (Defensive Cyber, Offensive Cyber)
* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Hashing (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Modern Encryption: RSA (Fundamentals)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* PKI (Public Key Infrastructure) Practical (Fundamentals)
* Packet Analysis: Packet Capture Basics (Defensive Cyber)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wireshark: Display Filters – Introduction to Filters (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)

# Thomas Beddes

Runshaw College

Total Labs Completed: **304** | Total Points: **20120** | Total Time: **103 hours 0 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* 32-Bit Linux Assembly: Ep.1 – Structure and Registers (Defensive Cyber, Offensive Cyber)
* 32-Bit Windows Assembly: Ep.1 – Windows API and the Stack (Defensive Cyber, Offensive Cyber)
* 64-Bit Windows Assembly: Ep.1 – Windows APIs and Registers (Defensive Cyber, Offensive Cyber)
* AI Challenges: Beat the Bot (Challenges & Scenarios)
* AI for Business: Ep.1 – What is AI? (Fundamentals)
* AI for Business: Ep.2 – The Benefits of AI (Fundamentals)
* AI for Business: Ep.3 – The Risks of AI (Fundamentals)
* AI for Business: Ep.4 – Using AI at Work (Fundamentals)
* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Demonstrate Your Skills (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Function Calling (Challenges & Scenarios)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* AI: Prompt Injection Attacks (Application Security, Defensive Cyber, Fundamentals)
* AI: TensorFlow for Machine Learning (Application Security, Defensive Cyber, Fundamentals)
* Active Directory Basics: Ep.1 – What is Active Directory? (Fundamentals)
* Active Directory Basics: Ep.2 – Console (Fundamentals)
* Active Directory Basics: Ep.3 – Objects (Fundamentals)
* Active Directory Basics: Ep.4 – Adding a Machine (Fundamentals)
* Active Directory Basics: Ep.5 – NTLM vs Kerberos (Fundamentals)
* Active Directory Basics: Ep.6 – Group Policy Management (Fundamentals)
* Active Directory Basics: Ep.7 – Replication (Fundamentals)
* Authentication: Ep.1 – What is Authentication? (Fundamentals)
* Authentication: Ep.2 – Why Are Passwords Important? (Fundamentals)
* Authentication: Ep.3 – Creating Secure Passwords (Fundamentals)
* Authentication: Ep.4 – Adding an Extra Layer of Security (Fundamentals)
* Authentication: Ep.5 – Demonstrate Your Knowledge (Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.2 – Case Studies (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Browsing Securely: Ep.5 – Demonstrate Your Knowledge (Fundamentals)
* Burp Suite Basics: HTTPS (Application Security, Offensive Cyber)
* Burp Suite Basics: Introduction (Application Security, Offensive Cyber)
* C++: Hardcoded Secrets (Application Security)
* C++: Introduction (Application Security)
* CVE-2020-0601 (Curveball) (Cyber Threat Intelligence)
* Caesar Ciphers (Fundamentals)
* Cyber 101: Cookies (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Fake News (Fundamentals)
* Cyber 101: Geolocation (Fundamentals)
* Cyber 101: Information Security (Fundamentals)
* Cyber 101: Keylogging (Fundamentals)
* Cyber 101: Rogue USB Devices (Fundamentals)
* Cyber 101: Security Champions (Fundamentals)
* Cyber 101: Virtual Card Numbers (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Data Handling: Ep.2 – Gathering, Storing, and Processing Data (Fundamentals)
* Data Handling: Ep.3 – Data Privacy and Access (Fundamentals)
* Data Handling: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Data Privacy: Ep.1 – Key Concepts (Fundamentals)
* Data Privacy: Ep.2 – Data Privacy Regulations (Fundamentals)
* Data Privacy: Ep.3 – What About You? (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Device Security: Ep.2 – Increasing Your Protection (Fundamentals)
* Device Security: Ep.3 – Case Studies (Fundamentals)
* Device Security: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Digital Evidence (Defensive Cyber, Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.2 – Case Studies (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Digital Footprint: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Digital Forensics Process: Reporting (Defensive Cyber, Fundamentals)
* Digital Forensics Processes and Techniques (Defensive Cyber, Fundamentals)
* Digital Forensics Tools (Defensive Cyber, Fundamentals)
* Disposal of Device Information (Fundamentals)
* DoS Primer: Practical (Fundamentals)
* DoS Primer: Resource Exhaustion (Fundamentals)
* DoS Primer: Volumetric (Fundamentals)
* DoS Primer: Vulnerabilities (Fundamentals)
* Elliptic Curve Cryptography (Fundamentals)
* Encoding: ASCII (Fundamentals)
* Encoding: Base64 (Fundamentals)
* Encoding: Binary (Fundamentals)
* Encoding: Demonstrate Your Skills (Fundamentals)
* Encoding: Hexadecimal (Fundamentals)
* Encoding: Punycode (Fundamentals)
* Encoding: Unicode (Fundamentals)
* Encoding: What is Encoding? (Fundamentals)
* Encryption Tools: CyberChef (Fundamentals)
* Encryption Tools: CyberChef — Recipes (Fundamentals)
* Ethics & Laws: Bugbusters (Fundamentals)
* Ethics & Laws: Burglary and Hacking (Fundamentals)
* Ethics & Laws: Ethical and Unethical Hacking (Fundamentals)
* Ethics & Laws: Police Raid (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Ethics & Laws: US Federal Cyber Law (Fundamentals)
* Guidance on Remote Working (Fundamentals)
* Historic Encryption: Demonstrate Your Skills (Fundamentals)
* History of Information Security (Fundamentals)
* Human Factors in Cybersecurity: How People Make Security Mistakes (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Human Factors in Cybersecurity: Usable Security (Fundamentals)
* ISO 27001: Ep.1 – What Is ISO 27001? (Fundamentals)
* ISO 27001: Ep.2 – The Domains of ISO 27001 (Fundamentals)
* ISO 27001: Ep.3 – What About You? (Fundamentals)
* Incident Response in the Workplace (Fundamentals)
* Information Security and Cybersecurity Terminology (Fundamentals)
* Information Security: Starting at the Beginning (Fundamentals)
* Interactive RegEx: Ep.1 — An Introduction to RegEx (Fundamentals)
* Interactive RegEx: Ep.2 — The RegEx Interface (Fundamentals)
* Internet Protocol V4 (Fundamentals)
* Introduction To Elastic: Ep.1 – What is Elastic? (Defensive Cyber)
* Introduction To Elastic: Ep.2 – Querying Data (Defensive Cyber)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Block Ciphers (Application Security, Fundamentals)
* Introduction to Cryptography: Demonstrate Your Knowledge (Application Security, Fundamentals)
* Introduction to Cryptography: Digital Signatures (Application Security, Fundamentals)
* Introduction to Cryptography: Hashing (Application Security, Fundamentals)
* Introduction to Cryptography: Message Integrity (Application Security, Fundamentals)
* Introduction to Cryptography: One-Time Pad (Application Security, Fundamentals)
* Introduction to Cryptography: Public Key Infrastructure (Application Security, Fundamentals)
* Introduction to Cryptography: Public and Private Key Management (Application Security, Fundamentals)
* Introduction to Cryptography: Stream Ciphers (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Digital Forensics: Demonstrate Your Skills (Defensive Cyber, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Hashing (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Networking: Ep.6 — Domain Name System (Fundamentals)
* Introduction to Networking: Ep.7 — Demonstrate Your Knowledge (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to Penetration Test Programs: Ep.10 – Improving your Program (Fundamentals)
* Introduction to Penetration Test Programs: Ep.11 – Demonstrate Your Knowledge (Fundamentals)
* Introduction to Penetration Test Programs: Ep.2 – Cybersecurity Frameworks (Fundamentals)
* Introduction to Penetration Test Programs: Ep.3 – Defining your Testing Program (Fundamentals)
* Introduction to Penetration Test Programs: Ep.4 – Choosing a Supplier (Fundamentals)
* Introduction to Penetration Test Programs: Ep.5 – Testing Management (Fundamentals)
* Introduction to Penetration Test Programs: Ep.6 – Pre-Engagement Activities (Fundamentals)
* Introduction to Penetration Test Programs: Ep.7 – Engagement Activities (Fundamentals)
* Introduction to Penetration Test Programs: Ep.8 – Penetration Test Reports (Fundamentals)
* Introduction to Penetration Test Programs: Ep.9 – Post-Engagement Activities (Fundamentals)
* Introduction to Python Scripting: Ep.1 – Setting up the Environment (Fundamentals)
* Introduction to Python Scripting: Ep.2 – Network Basics with Python (Fundamentals)
* Introduction to Python Scripting: Ep.3 – Network Reconnaissance with Python (Fundamentals)
* Introduction to Python Scripting: Ep.4 – Building an IDS with Python (Fundamentals)
* Introduction to Python Scripting: Ep.5 – Web Scraping (Fundamentals)
* Introduction to Python Scripting: Ep.6 – Log Analysis and Anomaly Detection with Python (Fundamentals)
* Introduction to Python Scripting: Ep.7 – Demonstrate Your Skills (Fundamentals)
* Introduction to Reverse Engineering: 32-Bit Linux – Part 1 (Defensive Cyber, Offensive Cyber)
* Introduction to Reverse Engineering: 32-Bit Windows – Part 1 (Defensive Cyber, Offensive Cyber)
* Introduction to Reverse Engineering: 64-Bit Windows – Part 1 (Defensive Cyber, Offensive Cyber)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Intrusion Detection Systems (Fundamentals)
* Java: Hardcoded Secrets (Application Security)
* Java: Stored XSS (Application Security)
* Kerberos: Ep.2 – Enumeration (Offensive Cyber)
* Kusto Query Language: Ep.1 – Introduction to KQL (Cloud Security)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.10 – Using Sudo (Fundamentals)
* Linux CLI: Ep.11 – Using SSH and SCP (Fundamentals)
* Linux CLI: Ep.12 – Using Find (Fundamentals)
* Linux CLI: Ep.13 – Searching and Sorting (Fundamentals)
* Linux CLI: Ep.15 – Generating File Hashes (Fundamentals)
* Linux CLI: Ep.16 – Combining Commands (Fundamentals)
* Linux CLI: Ep.17 – Demonstrate Your Skills (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Linux CLI: Ep.5 – File Permissions (Fundamentals)
* Linux CLI: Ep.6 – Editing Files (Fundamentals)
* Linux CLI: Ep.7 – Using wc (Fundamentals)
* Linux CLI: Ep.8 – Manipulating Text (Fundamentals)
* Microsoft Azure Basics: Fundamental Concepts (Cloud Security)
* Microsoft Azure Basics: Navigating the Web Portal (Cloud Security)
* Microsoft Azure Basics: Storage Accounts (Cloud Security)
* Modern Encryption: Demonstrate Your Skills (Fundamentals)
* Modern Encryption: MD5 Hashing (Fundamentals)
* Modern Encryption: RSA (Fundamentals)
* Modern Encryption: SHA-1 Hashes (Fundamentals)
* Nessus: Ep.1 – Introduction to Nessus (Offensive Cyber)
* Nessus: Ep.2 – Network Scanning (Offensive Cyber)
* Nessus: Ep.3 – Authenticated Scanning (Offensive Cyber)
* Nessus: Ep.4 – Scan Results (Offensive Cyber)
* Networking: Demonstrate Your Knowledge (Fundamentals)
* Networking: Demonstrate Your Skills (Fundamentals)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* Nmap: Ep.2 – Using Nmap (Offensive Cyber)
* Nmap: Ep.3 – Host Discovery (Offensive Cyber)
* Nmap: Ep.4 – Port Scanning (Offensive Cyber)
* Nmap: Ep.5 – OS and Version Detection (Offensive Cyber)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Cached and Archived Websites (Offensive Cyber)
* Open Source Intelligence (OSINT): Default Credentials (Offensive Cyber)
* Open Source Intelligence (OSINT): Deleted Tweet (Offensive Cyber)
* Open Source Intelligence (OSINT): Domain Intel (Offensive Cyber)
* Open Source Intelligence (OSINT): EXIF (Offensive Cyber)
* Open Source Intelligence (OSINT): Investigator Operations Security (OPSEC) (Offensive Cyber)
* Open Source Intelligence (OSINT): Online Anonymity (Offensive Cyber)
* Open Source Intelligence (OSINT): Robots.txt (Offensive Cyber)
* Open Source Intelligence (OSINT): Search Engines (Offensive Cyber)
* Open Source Intelligence (OSINT): Shodan.io (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media and Privacy (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* PKI (Public Key Infrastructure) Practical (Fundamentals)
* Packet Analysis: Packet Capture Basics (Defensive Cyber)
* Personal Devices in the Workplace (Fundamentals)
* Physical Security (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Physical Security: Ep.2 – Physical Security in Your Workplace (Fundamentals)
* Physical Security: Ep.3 – Physical Security When Working Remotely (Fundamentals)
* Physical Security: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Ports (Fundamentals)
* Privacy (Fundamentals)
* Privileged Access (Fundamentals)
* Protocols: ARP (Fundamentals)
* Protocols: DHCPv4 (Fundamentals)
* Protocols: DHCPv6 (Fundamentals)
* Protocols: DNS (Fundamentals)
* Protocols: FTP (Fundamentals)
* Protocols: HTTP (Fundamentals)
* Protocols: HTTP – Status Codes (Fundamentals)
* Protocols: LDAP (Fundamentals)
* Protocols: SMTP (Fundamentals)
* Python: Code Comments (Application Security)
* Python: Hardcoded Secrets (Application Security)
* Rainbow Tables (Fundamentals)
* SQL Injection: File Download (Offensive Cyber)
* SQL Injection: UNION (Offensive Cyber)
* Scanning: Network Scanning (Defensive Cyber, Offensive Cyber)
* Secure Data Handling (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: Attribution and Accountability (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: Authentication (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: Authorization (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: Defense in Depth (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: Least Privileges (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: Security Patching (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Security On The Go (Fundamentals)
* Security Reporting and Responsiveness: Ep.1 – Reporting Incidents and Concerns (Fundamentals)
* Security Reporting and Responsiveness: Ep.2 – Case Studies (Fundamentals)
* Security Reporting and Responsiveness: Ep.3 – Responding Appropriately (Fundamentals)
* Security Reporting and Responsiveness: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Shoulder Surfing (Fundamentals)
* Social Engineering (Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Social Engineering: Ep.3 – How Is It Used? (Fundamentals)
* Social Engineering: Ep.4 – Protecting Yourself (Fundamentals)
* Social Engineering: Ep.5 – Demonstrate Your Skills (Fundamentals)
* Spiderfoot (Offensive Cyber)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (US) (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Steganography (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Bombe Machine (Fundamentals)
* The Enigma Machine (Fundamentals)
* The Haunted Hollow: The Gatekeepers (Challenges & Scenarios)
* The History of Encryption (Fundamentals)
* The Importance of Information Security and Cybersecurity (Fundamentals)
* The Internet (Fundamentals)
* The Typex Machine (Fundamentals)
* Tor (Offensive Cyber)
* Transport Protocols (Fundamentals)
* Vigenère Ciphers (Fundamentals)
* WPA Wordlist Crack (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Web Log Analysis: Ep.3 – Access Logs (Defensive Cyber)
* Web Log Analysis: Ep.4 — Error Logs (Defensive Cyber)
* What Is Information Security? (Fundamentals)
* What is Digital Forensics? (Defensive Cyber, Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Basics: Ep.7 – Scheduled Tasks (Fundamentals)
* Windows Concepts: CertUtil (Fundamentals)
* Windows Concepts: New Technology File System (NTFS) (Fundamentals)
* Windows Concepts: Scheduled Tasks (Fundamentals)
* Windows Concepts: Windows Registry (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wired Equivalent Privacy (WEP) Cracking (Fundamentals)
* Wireshark: Display Filters – Introduction to Filters (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)

# Thomas Colby

Blackpool and the Fylde College

Total Labs Completed: **59** | Total Points: **1830** | Total Time: **8 hours 25 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)

# Thomas Long

Blackpool and the Fylde College

Total Labs Completed: **51** | Total Points: **970** | Total Time: **5 hours 24 minutes**

## Labs Completed:

* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.2 – Case Studies (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Digital Footprint: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Physical Security (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Privileged Access (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Social Engineering: Ep.3 – How Is It Used? (Fundamentals)
* Social Engineering: Ep.4 – Protecting Yourself (Fundamentals)
* Social Engineering: Ep.5 – Demonstrate Your Skills (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (US) (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)

# Tobias Lismanis

Runshaw College

Total Labs Completed: **103** | Total Points: **5440** | Total Time: **7 hours 35 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* C++: Hardcoded Secrets (Application Security)
* C++: Introduction (Application Security)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Hashing (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Kusto Query Language: Ep.1 – Introduction to KQL (Cloud Security)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Modern Encryption: RSA (Fundamentals)
* Nessus: Ep.1 – Introduction to Nessus (Offensive Cyber)
* Nessus: Ep.2 – Network Scanning (Offensive Cyber)
* Nessus: Ep.3 – Authenticated Scanning (Offensive Cyber)
* Nessus: Ep.4 – Scan Results (Offensive Cyber)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* Nmap: Ep.2 – Using Nmap (Offensive Cyber)
* Nmap: Ep.3 – Host Discovery (Offensive Cyber)
* Nmap: Ep.4 – Port Scanning (Offensive Cyber)
* Nmap: Ep.5 – OS and Version Detection (Offensive Cyber)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* PKI (Public Key Infrastructure) Practical (Fundamentals)
* Packet Analysis: Packet Capture Basics (Defensive Cyber)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Protocols: ARP (Fundamentals)
* Protocols: DHCPv4 (Fundamentals)
* Protocols: DHCPv6 (Fundamentals)
* Protocols: DNS (Fundamentals)
* Protocols: FTP (Fundamentals)
* Protocols: HTTP (Fundamentals)
* Python: Code Comments (Application Security)
* Python: Hardcoded Secrets (Application Security)
* Scanning: Network Scanning (Defensive Cyber, Offensive Cyber)
* Secure Data Handling (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Social Engineering: Ep.3 – How Is It Used? (Fundamentals)
* Social Engineering: Ep.4 – Protecting Yourself (Fundamentals)
* Social Engineering: Ep.5 – Demonstrate Your Skills (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (US) (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Web Log Analysis: Ep.3 – Access Logs (Defensive Cyber)
* Web Log Analysis: Ep.4 — Error Logs (Defensive Cyber)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wireshark: Display Filters – Introduction to Filters (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)

# Toby Rogers

Blackburn College

Total Labs Completed: **52** | Total Points: **1460** | Total Time: **4 hours 36 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Image Classification (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* AI: TensorFlow for Machine Learning (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)

# Tom Brooke

Blackpool and the Fylde College

Total Labs Completed: **98** | Total Points: **5150** | Total Time: **32 hours 49 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* C++: Hardcoded Secrets (Application Security)
* C++: Introduction (Application Security)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction To Elastic: Ep.1 – What is Elastic? (Defensive Cyber)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Hashing (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Microsoft Azure Basics: Navigating the Web Portal (Cloud Security)
* Modern Encryption: RSA (Fundamentals)
* Modern Encryption: SHA-1 Hashes (Fundamentals)
* Nessus: Ep.1 – Introduction to Nessus (Offensive Cyber)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* Nmap: Ep.2 – Using Nmap (Offensive Cyber)
* Nmap: Ep.3 – Host Discovery (Offensive Cyber)
* Nmap: Ep.4 – Port Scanning (Offensive Cyber)
* Nmap: Ep.5 – OS and Version Detection (Offensive Cyber)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* PKI (Public Key Infrastructure) Practical (Fundamentals)
* Packet Analysis: Packet Capture Basics (Defensive Cyber)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Protocols: ARP (Fundamentals)
* Protocols: DHCPv4 (Fundamentals)
* Protocols: DHCPv6 (Fundamentals)
* Protocols: DNS (Fundamentals)
* Protocols: FTP (Fundamentals)
* Protocols: HTTP (Fundamentals)
* Python: Code Comments (Application Security)
* Python: Hardcoded Secrets (Application Security)
* Scanning: Network Scanning (Defensive Cyber, Offensive Cyber)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Web Log Analysis: Ep.3 – Access Logs (Defensive Cyber)
* Web Log Analysis: Ep.4 — Error Logs (Defensive Cyber)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wireshark: Display Filters – Introduction to Filters (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)

# Tyler Lally

Blackpool and the Fylde College

Total Labs Completed: **259** | Total Points: **13530** | Total Time: **45 hours 22 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI for Business: Ep.1 – What is AI? (Fundamentals)
* AI for Business: Ep.2 – The Benefits of AI (Fundamentals)
* AI for Business: Ep.3 – The Risks of AI (Fundamentals)
* AI for Business: Ep.4 – Using AI at Work (Fundamentals)
* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Authentication: Ep.1 – What is Authentication? (Fundamentals)
* Authentication: Ep.2 – Why Are Passwords Important? (Fundamentals)
* Authentication: Ep.3 – Creating Secure Passwords (Fundamentals)
* Authentication: Ep.4 – Adding an Extra Layer of Security (Fundamentals)
* Authentication: Ep.5 – Demonstrate Your Knowledge (Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.2 – Case Studies (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Browsing Securely: Ep.5 – Demonstrate Your Knowledge (Fundamentals)
* C++: Hardcoded Secrets (Application Security)
* C++: Introduction (Application Security)
* Cloud Fundamentals: Introduction to SAML (Cloud Security)
* Cloud Security Alliance: Cloud Controls Matrix v4.0 (Cloud Security)
* Cloud Security: Frameworks, Standards, and Guidelines (Cloud Security)
* Cyber 101: Cookies (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Fake News (Fundamentals)
* Cyber 101: Geolocation (Fundamentals)
* Cyber 101: Information Security (Fundamentals)
* Cyber 101: Keylogging (Fundamentals)
* Cyber 101: Rogue USB Devices (Fundamentals)
* Cyber 101: Security Champions (Fundamentals)
* Cyber 101: Virtual Card Numbers (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.10 – Demonstrate Your Knowledge (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.3 – Weaponization Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.4 – Delivery Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.5 – Exploitation Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.6 – Installation/Persistence Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.7 – What is the Command and Control (C2) Phase? (Offensive Cyber)
* Cyber Kill Chain: Ep.8 – Actions on Objectives Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.9 – Adversary Simulation (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Data Handling: Ep.2 – Gathering, Storing, and Processing Data (Fundamentals)
* Data Handling: Ep.3 – Data Privacy and Access (Fundamentals)
* Data Handling: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Data Privacy: Ep.1 – Key Concepts (Fundamentals)
* Data Privacy: Ep.2 – Data Privacy Regulations (Fundamentals)
* Data Privacy: Ep.3 – What About You? (Fundamentals)
* DevSecOps: Introduction (Cloud Security)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Device Security: Ep.2 – Increasing Your Protection (Fundamentals)
* Device Security: Ep.3 – Case Studies (Fundamentals)
* Device Security: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Digital Evidence (Defensive Cyber, Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.2 – Case Studies (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Digital Footprint: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Digital Forensics Process: Reporting (Defensive Cyber, Fundamentals)
* Digital Forensics Processes and Techniques (Defensive Cyber, Fundamentals)
* Digital Forensics Tools (Defensive Cyber, Fundamentals)
* Disposal of Device Information (Fundamentals)
* DoS Primer: Practical (Fundamentals)
* DoS Primer: Resource Exhaustion (Fundamentals)
* DoS Primer: Volumetric (Fundamentals)
* DoS Primer: Vulnerabilities (Fundamentals)
* Elliptic Curve Cryptography (Fundamentals)
* Encoding: Binary (Fundamentals)
* Encoding: What is Encoding? (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Ethics & Laws: US Federal Cyber Law (Fundamentals)
* Guidance on Remote Working (Fundamentals)
* History of Information Security (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Incident Response in the Workplace (Fundamentals)
* Information Security and Cybersecurity Terminology (Fundamentals)
* Information Security: Starting at the Beginning (Fundamentals)
* Infrastructure as Code (IaC) (Cloud Security)
* Infrastructure as a Service (IaaS) (Cloud Security)
* Introduction To Elastic: Ep.1 – What is Elastic? (Defensive Cyber)
* Introduction To Elastic: Ep.2 – Querying Data (Defensive Cyber)
* Introduction To Elastic: Ep.3 – Triage (Defensive Cyber)
* Introduction To Elastic: Ep.4 – Focus (Alert Detailing) (Defensive Cyber)
* Introduction To Elastic: Ep.5 – Focus (Detection Rules) (Defensive Cyber)
* Introduction to Cloud (Cloud Security)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Block Ciphers (Application Security, Fundamentals)
* Introduction to Cryptography: Demonstrate Your Knowledge (Application Security, Fundamentals)
* Introduction to Cryptography: Digital Signatures (Application Security, Fundamentals)
* Introduction to Cryptography: Hashing (Application Security, Fundamentals)
* Introduction to Cryptography: Message Integrity (Application Security, Fundamentals)
* Introduction to Cryptography: One-Time Pad (Application Security, Fundamentals)
* Introduction to Cryptography: Public Key Infrastructure (Application Security, Fundamentals)
* Introduction to Cryptography: Public and Private Key Management (Application Security, Fundamentals)
* Introduction to Cryptography: Stream Ciphers (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Digital Forensics: Demonstrate Your Skills (Defensive Cyber, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Hashing (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Metasploit: Ep.1 – What is Metasploit? (Offensive Cyber)
* Introduction to Metasploit: Ep.2 – Modules (Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Networking: Ep.6 — Domain Name System (Fundamentals)
* Introduction to Networking: Ep.7 — Demonstrate Your Knowledge (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to Penetration Test Programs: Ep.2 – Cybersecurity Frameworks (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Intrusion Detection Systems (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.10 – Using Sudo (Fundamentals)
* Linux CLI: Ep.11 – Using SSH and SCP (Fundamentals)
* Linux CLI: Ep.12 – Using Find (Fundamentals)
* Linux CLI: Ep.13 – Searching and Sorting (Fundamentals)
* Linux CLI: Ep.14 – Using Screen (Fundamentals)
* Linux CLI: Ep.15 – Generating File Hashes (Fundamentals)
* Linux CLI: Ep.16 – Combining Commands (Fundamentals)
* Linux CLI: Ep.17 – Demonstrate Your Skills (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Linux CLI: Ep.5 – File Permissions (Fundamentals)
* Linux CLI: Ep.6 – Editing Files (Fundamentals)
* Linux CLI: Ep.7 – Using wc (Fundamentals)
* Linux CLI: Ep.8 – Manipulating Text (Fundamentals)
* Linux CLI: Ep.9 – Stream Redirection (Fundamentals)
* Microsoft Azure Basics: Fundamental Concepts (Cloud Security)
* Microsoft Azure Basics: Navigating the Web Portal (Cloud Security)
* Microsoft Azure Basics: Storage Accounts (Cloud Security)
* Microsoft Azure Basics: Virtual Networks (Cloud Security)
* Modern Encryption: MD5 Hashing (Fundamentals)
* Modern Encryption: RSA (Fundamentals)
* Modern Encryption: SHA-1 Hashes (Fundamentals)
* Nessus: Ep.1 – Introduction to Nessus (Offensive Cyber)
* Nessus: Ep.2 – Network Scanning (Offensive Cyber)
* Nessus: Ep.3 – Authenticated Scanning (Offensive Cyber)
* Nessus: Ep.4 – Scan Results (Offensive Cyber)
* Nessus: Ep.5 – Demonstrate your Skills (Offensive Cyber)
* Networking: Demonstrate Your Knowledge (Fundamentals)
* Networking: Demonstrate Your Skills (Fundamentals)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* Nmap: Ep.2 – Using Nmap (Offensive Cyber)
* Nmap: Ep.3 – Host Discovery (Offensive Cyber)
* Nmap: Ep.4 – Port Scanning (Offensive Cyber)
* Nmap: Ep.5 – OS and Version Detection (Offensive Cyber)
* OSI Model (Fundamentals)
* OWASP 2021: Ep.1 – Broken Access Control (Application Security, Defensive Cyber, Offensive Cyber)
* OWASP 2021: Ep.2 – Cryptographic Failures (Application Security, Defensive Cyber, Offensive Cyber)
* OWASP 2021: Ep.3 – Injection (Application Security, Defensive Cyber, Offensive Cyber)
* OWASP 2021: Ep.4 – Insecure Design (Application Security, Defensive Cyber, Offensive Cyber)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Deleted Tweet (Offensive Cyber)
* Open Source Intelligence (OSINT): Shodan.io (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* PKI (Public Key Infrastructure) Practical (Fundamentals)
* Packet Analysis: BPF Syntax (Defensive Cyber)
* Packet Analysis: Packet Capture Basics (Defensive Cyber)
* Packet Analysis: TLS Handshake (Defensive Cyber)
* Packet Analysis: Using tcpdump (Defensive Cyber)
* Personal Devices in the Workplace (Fundamentals)
* Physical Security (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Physical Security: Ep.2 – Physical Security in Your Workplace (Fundamentals)
* Physical Security: Ep.3 – Physical Security When Working Remotely (Fundamentals)
* Physical Security: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Platform as a Service (PaaS) (Cloud Security)
* Ports (Fundamentals)
* Privacy (Fundamentals)
* Privileged Access (Fundamentals)
* Protocols: ARP (Fundamentals)
* Protocols: DHCPv4 (Fundamentals)
* Protocols: DHCPv6 (Fundamentals)
* Protocols: DNS (Fundamentals)
* Protocols: FTP (Fundamentals)
* Protocols: HTTP (Fundamentals)
* Protocols: HTTP – Status Codes (Fundamentals)
* Protocols: LDAP (Fundamentals)
* Protocols: Modbus (Fundamentals)
* Protocols: SMTP (Fundamentals)
* Python: Code Comments (Application Security)
* Python: Hardcoded Secrets (Application Security)
* Rainbow Tables (Fundamentals)
* Scanning: Network Scanning (Defensive Cyber, Offensive Cyber)
* Secrets Management (Cloud Security)
* Secure Data Handling (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: Attribution and Accountability (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: Authentication (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: Authorization (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: Defense in Depth (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: Least Privileges (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: Security Patching (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Security Automation (Cloud Security)
* Security On The Go (Fundamentals)
* Security Reporting and Responsiveness: Ep.1 – Reporting Incidents and Concerns (Fundamentals)
* Security Reporting and Responsiveness: Ep.2 – Case Studies (Fundamentals)
* Security Reporting and Responsiveness: Ep.3 – Responding Appropriately (Fundamentals)
* Security Reporting and Responsiveness: Ep.4 – Demonstrate Your Knowledge (Fundamentals)
* Shoulder Surfing (Fundamentals)
* Social Engineering (Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Social Engineering: Ep.3 – How Is It Used? (Fundamentals)
* Social Engineering: Ep.4 – Protecting Yourself (Fundamentals)
* Social Engineering: Ep.5 – Demonstrate Your Skills (Fundamentals)
* Software as a Service (SaaS) (Cloud Security)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (US) (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Steganography (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Importance of Information Security and Cybersecurity (Fundamentals)
* The Internet (Fundamentals)
* Tor (Offensive Cyber)
* Transport Protocols (Fundamentals)
* Virtualization (Cloud Security)
* WPA Wordlist Crack (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Web Log Analysis: Ep.3 – Access Logs (Defensive Cyber)
* Web Log Analysis: Ep.4 — Error Logs (Defensive Cyber)
* What Is Information Security? (Fundamentals)
* What is Digital Forensics? (Defensive Cyber, Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Basics: Ep.6 – SMB and RDP (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wired Equivalent Privacy (WEP) Cracking (Fundamentals)
* Wireshark: Display Filters – Combining Filters (Defensive Cyber)
* Wireshark: Display Filters – Diving In (Defensive Cyber)
* Wireshark: Display Filters – Introduction to Filters (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)
* Wireshark: Metrics and Statistics (Defensive Cyber)

# Ujala Tassawar Muhammad

Blackburn College

Total Labs Completed: **63** | Total Points: **1780** | Total Time: **3 hours 47 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* An Introduction to Linux Internals (Defensive Cyber, Offensive Cyber)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.10 – Demonstrate Your Knowledge (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.3 – Weaponization Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.4 – Delivery Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.5 – Exploitation Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.6 – Installation/Persistence Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.7 – What is the Command and Control (C2) Phase? (Offensive Cyber)
* Cyber Kill Chain: Ep.8 – Actions on Objectives Phase (Offensive Cyber)
* Cyber Kill Chain: Ep.9 – Adversary Simulation (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to 32-Bit Architectures (Defensive Cyber, Offensive Cyber)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to Windows Internals (Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* The Inside of a PE File (Defensive Cyber, Offensive Cyber)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)

# Umar Akhtar

Cardinal Newman College

Total Labs Completed: **72** | Total Points: **2490** | Total Time: **5 hours 47 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Elliptic Curve Cryptography (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Modern Encryption: RSA (Fundamentals)
* Nessus: Ep.1 – Introduction to Nessus (Offensive Cyber)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)

# Umar Darsot

Runshaw College

Total Labs Completed: **108** | Total Points: **3560** | Total Time: **23 hours 30 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)

# Virtue Vincent-Hejirika

Cardinal Newman College

Total Labs Completed: **21** | Total Points: **250** | Total Time: **1 hours 17 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)

# Willow Richardson

Blackpool and the Fylde College

Total Labs Completed: **81** | Total Points: **2440** | Total Time: **10 hours 58 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.2 – Case Studies (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cookies (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Fake News (Fundamentals)
* Cyber 101: Geolocation (Fundamentals)
* Cyber 101: Information Security (Fundamentals)
* Cyber 101: Keylogging (Fundamentals)
* Cyber 101: Rogue USB Devices (Fundamentals)
* Cyber 101: Security Champions (Fundamentals)
* Cyber 101: Virtual Card Numbers (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Cyber Kill Chain: Ep.2 – Reconnaissance Phase (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: How People Make Security Mistakes (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Python: Code Comments (Application Security)
* Python: Hardcoded Secrets (Application Security)
* Secure Fundamentals: Attribution and Accountability (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: Least Privileges (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: Security Patching (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (US) (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Concepts: New Technology File System (NTFS) (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)

# Zack Hickson

Blackpool and the Fylde College

Total Labs Completed: **30** | Total Points: **370** | Total Time: **54 minutes**

## Labs Completed:

* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Secure Fundamentals: Defense in Depth (Application Security, Defensive Cyber, Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)

# Zahidullah Shinwari

Blackburn College

Total Labs Completed: **74** | Total Points: **1920** | Total Time: **9 hours 35 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Virtual Card Numbers (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Elliptic Curve Cryptography (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Internet Protocol V4 (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Linux CLI: Ep.5 – File Permissions (Fundamentals)
* Modern Encryption: RSA (Fundamentals)
* OSI Model (Fundamentals)
* OWASP 2021: Ep.1 – Broken Access Control (Application Security, Defensive Cyber, Offensive Cyber)
* OWASP 2021: Ep.2 – Cryptographic Failures (Application Security, Defensive Cyber, Offensive Cyber)
* OWASP 2021: Ep.3 – Injection (Application Security, Defensive Cyber, Offensive Cyber)
* OWASP 2021: Ep.4 – Insecure Design (Application Security, Defensive Cyber, Offensive Cyber)
* OWASP 2021: Ep.5 – Security Misconfiguration (Application Security, Defensive Cyber, Offensive Cyber)
* OWASP 2021: Ep.6 – Vulnerable and Outdated Components (Application Security, Defensive Cyber, Offensive Cyber)
* OWASP 2021: Ep.7 – Identification and Authentication Failures (Application Security, Defensive Cyber, Offensive Cyber)
* OWASP 2021: Ep.8 – Software and Data Integrity Failures (Application Security, Defensive Cyber, Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Tactics: Reconnaissance (Defensive Cyber, Offensive Cyber)
* Tactics: Resource Development (Defensive Cyber, Offensive Cyber)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)

# Zaid Laher

Blackburn College

Total Labs Completed: **77** | Total Points: **2940** | Total Time: **18 hours 12 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to Hashing (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Modern Encryption: RSA (Fundamentals)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media (Offensive Cyber)
* Open Source Intelligence (OSINT): Social Media and Privacy (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* PKI (Public Key Infrastructure) Practical (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Python: Code Comments (Application Security)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Web Log Analysis: Ep.3 – Access Logs (Defensive Cyber)
* Web Log Analysis: Ep.4 — Error Logs (Defensive Cyber)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)
* Wireshark: Introduction to Wireshark (Defensive Cyber)

# Zak Wood

Blackburn College

Total Labs Completed: **75** | Total Points: **2340** | Total Time: **15 hours 26 minutes**

Digital Skills 4 Defence: STEM and Digital Skills Bursary Cyber Fundamentals: **Successfully Completed**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Cyber 101: Cyber Kill Chain (Fundamentals)
* Cyber 101: Darknets (Fundamentals)
* Cyber 101: Who Are The Hackers? (Fundamentals)
* Cyber 101: Why Hackers Hack (Fundamentals)
* Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain? (Offensive Cyber)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Disposal of Device Information (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Encryption (Fundamentals)
* Introduction to MITRE ATT&CK® (Defensive Cyber, Offensive Cyber)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Introduction to Penetration Test Programs: Ep.1 – What is Pen Testing? (Fundamentals)
* Introduction to the OWASP Top 10 (Application Security, Defensive Cyber, Offensive Cyber)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* Modern Encryption: RSA (Fundamentals)
* Nmap: Ep.1 – Intro to Nmap (Offensive Cyber)
* OSI Model (Fundamentals)
* Open Source Intelligence (OSINT): Boarding Pass (Offensive Cyber)
* PKI (Public Key Infrastructure) (Fundamentals)
* Physical Security (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Privacy (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Shoulder Surfing (Fundamentals)
* Social Engineering (Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* Symmetric vs Asymmetric Key Encryption (Fundamentals)
* The Internet (Fundamentals)
* Transport Protocols (Fundamentals)
* Web Log Analysis: Ep.1 – What are Web Server Logs? (Defensive Cyber)
* Web Log Analysis: Ep.2 – Log Formats (Defensive Cyber)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)
* Windows Basics: Ep.5 – Services (Fundamentals)
* Windows Hardening: Ep.1 – Introduction (Defensive Cyber)

# Zymal Farhad

Blackburn College

Total Labs Completed: **55** | Total Points: **1560** | Total Time: **5 hours 30 minutes**

## Labs Completed:

* AI: Data Ethics and Responsible Use (Application Security, Defensive Cyber, Fundamentals)
* AI: Emerging Threats (Application Security, Defensive Cyber, Fundamentals)
* AI: Introduction to AI (Application Security, Defensive Cyber, Fundamentals)
* Browsing Securely: Ep.1 – What is Secure Browsing? (Fundamentals)
* Browsing Securely: Ep.3 – Browsers (Fundamentals)
* Browsing Securely: Ep.4 – Cookies and Pop-Ups (Fundamentals)
* Data Handling: Ep.1 – Data Fundamentals (Fundamentals)
* Device Security: Ep.1 – What is Device Security? (Fundamentals)
* Digital Footprint: Ep.1 – What is a Digital Footprint? (Fundamentals)
* Digital Footprint: Ep.3 – Protecting Yourself (Fundamentals)
* Ethics & Laws: UK Cyber Law (Fundamentals)
* Human Factors in Cybersecurity: How People Make Security Mistakes (Fundamentals)
* Human Factors in Cybersecurity: People Are The Strongest Link (Fundamentals)
* Human Factors in Cybersecurity: Security Awareness and Behavior Change (Fundamentals)
* Human Factors in Cybersecurity: Usable Security (Fundamentals)
* Introduction to Cryptography: Asymmetric Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: Symmetric Key Encryption (Application Security, Fundamentals)
* Introduction to Cryptography: What is Cryptography? (Application Security, Fundamentals)
* Introduction to Networking: Ep.1 — What is a Network? (Fundamentals)
* Introduction to Networking: Ep.2 – Types of Networks (Fundamentals)
* Introduction to Networking: Ep.3 — Network Hardware (Fundamentals)
* Introduction to Networking: Ep.4 – Network Topologies (Fundamentals)
* Introduction to Networking: Ep.5 — IP Addresses (Fundamentals)
* Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface (Fundamentals)
* Linux CLI: Ep.2 – Getting Started with the Terminal (Fundamentals)
* Linux CLI: Ep.3 – Moving Around (Fundamentals)
* Linux CLI: Ep.4 – Changing Things (Fundamentals)
* OSI Model (Fundamentals)
* Physical Security: Ep.1 – Introduction to Physical Security (Fundamentals)
* Ports (Fundamentals)
* Secure Fundamentals: The CIA Triad (Application Security, Defensive Cyber, Fundamentals)
* Social Engineering: Ep.1 – What is Social Engineering? (Fundamentals)
* Social Engineering: Ep.2 – Techniques (Fundamentals)
* Staying Safe Online: Accidental and Malicious Data Leaks (Fundamentals)
* Staying Safe Online: Antivirus Software (Fundamentals)
* Staying Safe Online: Backups (Fundamentals)
* Staying Safe Online: Consequences and Impacts of Cyberattacks (Fundamentals)
* Staying Safe Online: Covid-19 Cybercriminals (Fundamentals)
* Staying Safe Online: Firewalls and VPNs (Fundamentals)
* Staying Safe Online: Identifying Ransomware (Fundamentals)
* Staying Safe Online: Identity Theft (Fundamentals)
* Staying Safe Online: Malware (Fundamentals)
* Staying Safe Online: Mobile Security Tips (Fundamentals)
* Staying Safe Online: Multi-Factor Authentication (Fundamentals)
* Staying Safe Online: Passwords (Fundamentals)
* Staying Safe Online: Phishing Emails (Fundamentals)
* Staying Safe Online: Phishing Emails (US) (Fundamentals)
* Staying Safe Online: Safer Browsing (Fundamentals)
* Staying Safe Online: Updates and Patches (Fundamentals)
* Staying Safe Online: Why Information Security Is Everyone's Business (Fundamentals)
* The Internet (Fundamentals)
* Windows Basics: Ep.1 – Command Prompt (Fundamentals)
* Windows Basics: Ep.2 – Users and Groups (Fundamentals)
* Windows Basics: Ep.3 – Registry (Fundamentals)
* Windows Basics: Ep.4 – Managing Processes (Fundamentals)