

Wagih Saqqaw

Completed 140 labs earning 9000 points.



Activity Report

| Date | Lab | Description | Points Earned |
|------------|--|--|---------------|
| 2023-02-07 | Snort Rules: Ep.3 – HTTP | Demonstrate usage of Snort rules | 300 |
| 2023-02-07 | Snort Rules: Ep.2 – DNS | Create Snort rules for DNS events | 300 |
| 2023-02-07 | Snort Rules: Ep.1 | Demonstrate proficiency in basic Snort rules | 200 |
| 2023-02-06 | Parsing PST | Investigate email client files | 200 |
| 2023-02-06 | tcpdump | Analyse network packet captures | 200 |
| 2023-02-06 | Wireshark: Stream/Object Extraction | Analyse network packet captures | 200 |
| 2023-02-06 | Packet Capture Basics | Analyse network packet captures | 100 |
| 2023-01-28 | Exfiltration Over Alternative Protocol | Practise identifying instances where data has been exfiltrated | 100 |
| 2023-01-28 | Defence in Depth | Discover the principles of defence systems | 20 |
| 2023-01-26 | Windows Sysmon | Analyse and investigate system logs | 100 |

Activity Report Page 2 of 10

| Date | Lab | Description | Points Earned |
|------------|--|---|---------------|
| 2023-01-26 | Clipboard Data Theft | Analyse techniques used by adversaries to steal clipboard data | 100 |
| 2023-01-26 | Process Explorer | Use Process Explorer effectively | 100 |
| 2023-01-26 | Windows Sysinternals | An overview of the Sysinternals suite | 100 |
| 2023-01-26 | IR: Ep.3 – Compromised Host | Investigate host-based compromise and IOCs | 400 |
| 2023-01-25 | Domain Intel | Understand the information associated with domain names | 40 |
| 2023-01-24 | IR: Ep.1 – Suspicious Email | Investigate and gain information from suspected malicious documents | 200 |
| 2023-01-17 | MongoDB: An Introduction | A basic understanding of NoSQL Databases | 100 |
| 2023-01-17 | Stack Overflow | Demonstrate the risk of using code found online | 10 |
| 2023-01-17 | SQL: An Introduction | Gain an understanding of the SQL language and queries | 100 |
| 2023-01-17 | Wireshark Display Filters: An Introduction | Analyse network packet captures | 100 |
| 2023-01-17 | Intro to Wireshark | Analyse network packet captures | 100 |
| 2023-01-10 | PowerShell: Working with files | Practice reading from and writing to files in PowerShell | 100 |
| 2023-01-10 | PowerShell: Getting Started | Practise using the PowerShell cmdlets | 100 |
| 2022-12-16 | Intrusion Detection Systems | Describe intrusion detection and prevention principles | 20 |
| 2022-12-15 | The Bombe Machine | Recognize how the Bombe machine works | 200 |

Activity Report Page 3 of 10

| Date | Lab | Description | Points Earned |
|------------|--|--|---------------|
| 2022-12-15 | The Typex Machine | Recognize how a Typex machine works | 200 |
| 2022-12-15 | CertUtil | Analyse the function of CertUtil | 100 |
| 2022-12-15 | Protocols – LDAP | Analyse the LDAP protocol in an enterprise context | 100 |
| 2022-12-15 | Background Intelligent Transfer Service (BITS) | Gain an understanding of BITS and how it can be abused | 100 |
| 2022-12-15 | Protocols – ARP | Identify packet structure of ARP requests and responses | 100 |
| 2022-12-15 | Scheduled Tasks | Demonstrate how to navigate information in Windows Scheduled Tasks | 100 |
| 2022-12-15 | Windows Registry | Evaluate registry values | 100 |
| 2022-12-15 | Windows File Permissions | Analyse Windows file permissions | 100 |
| 2022-12-14 | The Enigma Machine | Recall how the Enigma machine works | 200 |
| 2022-12-14 | Spiderfoot | Scan and analyse data using speciality OSINT tools | 40 |
| 2022-12-14 | Encryption Tools: CyberChef — Recipes | Recall how CyberChef recipes work | 40 |
| 2022-12-14 | Encryption Tools: CyberChef | Recall how CyberChef functions | 40 |
| 2022-12-14 | Caesar Ciphers | Recall how Caesar cipher encoding works | 40 |
| 2022-12-14 | What Is IoT? | Recognise IoT devices and their associated risks | 10 |
| 2022-12-14 | Default Credentials | Knowledge of default credentials | 20 |

Activity Report Page 4 of 10

| Date | Lab | Description | Points Earned |
|------------|--|--|---------------|
| 2022-12-14 | Investigator Operations Security (OPSEC) | Source online information relevant to an investigation | 40 |
| 2022-12-09 | Protocols – FTP | Explain the core concepts of the File Transfer Protocol | 100 |
| 2022-12-09 | Linux CLI: Ep. 12 – Using Find | Recognise how the find command works and the filters and arguments that go with it | 200 |
| 2022-12-09 | Linux CLI: Ep. 10 – Using Sudo | Identify different user privileges in Linux | 100 |
| 2022-12-09 | Linux CLI: Ep. 14 – Using Screen | Be able to explain screen's CLI usage | 100 |
| 2022-12-09 | Linux CLI: Ep. 8 – Manipulating Text | Know how to modify text within files using basic command line tools | 200 |
| 2022-12-09 | Linux CLI: Ep. 13 – Searching and Sorting | Know how to employ searching techniques to find patterns in files | 100 |
| 2022-12-09 | Linux CLI: Ep. 16 – Combining Commands | Identify the different ways of combining commands on the terminal | 200 |
| 2022-12-09 | Linux CLI: Ep. 6 – Editing Files | Be able to recall some common Linux command line text editors | 100 |
| 2022-12-09 | Linux CLI: Ep. 7 – Using wc | Be able to count elements in a file using the wc tool | 200 |
| 2022-12-09 | Linux CLI: Ep. 9 – Stream Redirection | Know how data can be manipulated via the terminal | 100 |
| 2022-12-09 | Linux CLI: Ep. 15 – Generating File Hashes | Be able to recognise file hashes | 100 |
| 2022-12-09 | Linux CLI: Ep. 11 – Using SSH and SCP | Recall what the SSH protocol is | 100 |
| 2022-12-08 | Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface | Recall Linux command line fundamentals | 40 |
| 2022-12-08 | Introduction to Encryption | Identify different types of encryption algorithms | 100 |

Activity Report Page 5 of 10

| Date | Lab | Description | Points Earned |
|------------|--|--|---------------|
| 2022-12-08 | Introduction to Hashing | Identify the characteristics of a good hashing algorithm | 100 |
| 2022-12-08 | Introduction to Computer Memory and Architecture | Gain a high level understanding of how memory works in a computer system | 40 |
| 2022-12-08 | Linux CLI: Ep. 2 – Getting Started with the Terminal | Be able to recall fundamental concepts of the Linux terminal | 100 |
| 2022-12-08 | Rainbow Tables | Describe what a rainbow table is | 40 |
| 2022-12-08 | Linux CLI: Ep. 5 – File Permissions | Be able to read Linux file permissions | 100 |
| 2022-12-08 | Introduction to ELF Reverse Engineering | Exposure to ELF binary analysis | 100 |
| 2022-12-08 | Linux CLI: Ep. 4 – Changing Things | Know the five Linux CLI commands explored in the lab and be able to describe their basic usage | 100 |
| 2022-12-08 | Linux CLI: Ep. 3 – Moving Around | Have the ability to navigate through directories on the command line | 100 |
| 2022-12-08 | Symmetric vs Asymmetric Key Encryption | Apply symmetric key encryption and decryption techniques | 100 |
| 2022-12-08 | Hashing – MD5 | Apply the MD5 hashing algorithm to strings | 100 |
| 2022-12-08 | Hashing – SHA-1 | Apply the SHA1 hashing algorithm to strings | 100 |
| 2022-11-22 | NIST Cybersecurity Framework | List the three main components of the NIST Cybersecurity Framework | 40 |
| 2022-11-22 | Three Lines of Defense | Describe the Three Lines of Defense model | 10 |
| 2022-11-22 | Qualitative Risk Measurement | Summarize what qualitative risk is | 20 |
| 2022-11-22 | Risk and Control Self Assessment (RCSA) | Describe the purpose of an RCSA within the wider risk management framework | 20 |

Activity Report Page 6 of 10

| Date | Lab | Description | Points Earned |
|------------|---|---|---------------|
| 2022-11-22 | Quantitative Risk Measurement | Calculate quantitative risk as a function of impact and probability | 40 |
| 2022-11-22 | Vulnerability Identification | Identify the different ways to conduct vulnerability identification | 40 |
| 2022-11-22 | Asset Inventory and Valuation | Define the asset identification and valuation processes | 20 |
| 2022-11-22 | How to Mitigate Risk | Explain how risk management can help mitigate risk | 20 |
| 2022-11-21 | HTTP Status Codes | Develop knowledge of HTTP status codes | 100 |
| 2022-11-21 | OSI Model | Identify the different layers of the OSI model | 40 |
| 2022-11-21 | Ports | Identify how ports are used in modern networks | 40 |
| 2022-11-21 | Binary | Recall how binary functions | 40 |
| 2022-11-20 | The Internet | Explain the history of the internet | 20 |
| 2022-11-20 | Introduction to Networking: Ep.5 — IP Addresses | Recognize an IP address | 40 |
| 2022-11-20 | Payment Services Directive 2 (PSD2) | Describe how PSD2 works and affects the banking industry | 10 |
| 2022-11-20 | The NCSC's 10 Steps to Cybersecurity | Describe each of the 10 Steps to Cybersecurity | 20 |
| 2022-11-20 | Information Technology Health Check (ITHC) | Recognize why an information technology health check is carried out | 20 |
| 2022-11-20 | Health Insurance Portability and Accountability Act (HIPAA) | Describe the five titles that form the structure of HIPAA | 20 |
| 2022-11-20 | Compliance, Legislation, Regulation, and Standards | Describe the differences between compliance, legislation, regulation, and standards | 10 |

Activity Report Page 7 of 10

| Date | Lab | Description | Points Earned |
|------------|--|---|---------------|
| 2022-11-20 | Policies, Processes, and Procedures | Recall the differences between policies, processes, and procedures | 10 |
| 2022-11-20 | Payment Card Industry Data Security Standard (PCI-DSS) | Recall the different PCI-DSS control objectives | 40 |
| 2022-11-20 | NIS Directive | Recognize what the NIS Directive is and how it protects the countries in the EU | 20 |
| 2022-11-20 | Cyber Essentials | Identify the most common attacks outlined by the Cyber Essentials scheme | 20 |
| 2022-11-20 | How Is Risk Measured? | Be able to describe risk, impact, and probability | 40 |
| 2022-11-20 | What Is Risk? | Define the core concepts that formulate risk | 20 |
| 2022-11-20 | Accreditation | Describe the accreditation process | 10 |
| 2022-11-20 | Transport Protocols | Explain the core concepts of the the most common transport protocols | 40 |
| 2022-11-20 | Introduction to Networking: Ep.6 — Domain Name System | Summarize the fundamentals of the Domain Name System | 40 |
| 2022-11-20 | Internet Protocol V4 | Explain the core concepts of IPv4 addressing | 100 |
| 2022-11-19 | Accidental and Malicious Data Leaks | Recognize the differences between accidental leaks and malicious leaks | 10 |
| 2022-11-19 | Identifying Ransomware | Recognize the tell-tale signs of ransomware | 10 |
| 2022-11-19 | Rogue USB Devices | Recall how rogue USB devices can be used for malicious purposes | 10 |
| 2022-11-19 | Updates and Patches | Identify the differences between updates and patches | 10 |
| 2022-11-19 | Firewalls and VPNs | Recognize the benefits of firewalls and VPNs | 10 |

Activity Report Page 8 of 10

| Date | Lab | Description | Points Earned |
|------------|-----------------------------|--|---------------|
| 2022-11-19 | Information Security | Recognize the importance of information security for individuals and organizations | 10 |
| 2022-11-19 | Passwords | Recognize how to protect yourself and your devices with strong passwords | 10 |
| 2022-11-19 | Antivirus | Identify the purpose of antivirus software and its main features | 10 |
| 2022-11-19 | Why Hackers Hack | Recognize some of the methods used by hackers | 10 |
| 2022-11-19 | Virtual Card Numbers | Identify the different types of virtual card numbers | 10 |
| 2022-11-19 | Fake News | Recognize the characteristics of fake news | 10 |
| 2022-11-19 | Security Champions | Underline what a security champion is and their purpose | 10 |
| 2022-11-19 | Keylogging | Recognize what keyloggers are | 10 |
| 2022-11-19 | Geolocation | Recognize the differences between device-based and server-based geolocation tracking | 10 |
| 2022-11-19 | Mobile Security Tips | Identify potential threats to mobile phone security | 10 |
| 2022-11-19 | Darknets | Recognize how darknets operate on the internet | 10 |
| 2022-11-19 | Cookies | Recognize how cookies are used by individuals and organizations | 20 |
| 2022-11-19 | Identity Theft | Recognize the ways to prevent identity theft and the warning signs to look out for | 10 |
| 2022-11-19 | Backups | Recognize the importance of backups | 10 |
| 2022-11-19 | Multi-Factor Authentication | Recall how multi-factor authentication works | 10 |

Activity Report Page 9 of 10

| Date | Lab | Description | Points Earned |
|------------|--|--|---------------|
| 2022-11-19 | Malware | Recognize the most common forms of malware and how they can affect you | 10 |
| 2022-11-19 | Cyber Kill Chain | Recognize the purpose of the cyber kill chain | 10 |
| 2022-11-16 | Who are the Hackers? | Recognize the different types of hackers | 10 |
| 2022-11-16 | WannaCry (ARCHIVED) | Safely observe WannaCry ransomware | 100 |
| 2022-11-16 | GDPR Aware (ARCHIVED) | Explain the key details and impact of GDPR | 10 |
| 2022-11-12 | Case Study: Covid-19 Cybercriminals | Identify the characteristics of Covid-19 phishing scams | 10 |
| 2022-11-12 | Incident Response in the Workplace | Recall the advantages of an incident response plan | 10 |
| 2022-11-12 | Guidance on Remote Working | Identify the risks associated with remote working | 10 |
| 2022-11-12 | Security On The Go | Recognize the security risks of using devices when away from the office | 10 |
| 2022-11-12 | Personal Devices in the Workplace | Recognize the risks associated with using personal devices in the workplace | 10 |
| 2022-11-12 | The Importance of Information Security and Cybersecurity | Describe a simulated example of a breach and recall its emotional impact | 10 |
| 2022-11-12 | Privileged Access | Recall what privileged access is and why it's an attractive target for attackers | 10 |
| 2022-11-12 | Physical Security | Identify common physical security risks | 10 |
| 2022-11-12 | Privacy | Identify what privacy is and why it needs protecting | 10 |
| 2022-11-12 | Consequences and Impacts of Cyberattacks | Recognize the differences between the consequences and impacts of cyberattacks | 10 |

Activity Report Page 10 of 10

| Date | Lab | Description | Points Earned |
|------------|--|--|---------------|
| 2022-11-12 | Why Information Security Is Everyone's Business | Recognize the importance of information security | 10 |
| 2022-11-12 | What Is Information Security? | Identify the workplace and personal security challenges that good information security practices help to solve | 10 |
| 2022-11-12 | History of Information Security | Recall some of the key moments for information security throughout history | 10 |
| 2022-11-12 | Disposal of Device Information | Recognize why secure device disposal is core to an organization's information management process | 10 |
| 2022-11-12 | Information Security and Cybersecurity Terminology | Recall some key information security and cybersecurity terms and phrases | 10 |
| 2022-11-12 | Information Security – Starting at the Beginning | Recall the difference between information security and cybersecurity | 10 |
| 2022-11-12 | Social Engineering | Describe different social engineering attack techniques and their impacts | 10 |
| 2022-11-12 | Safer Browsing | Recall how to protect yourself and your privacy as you browse the web | 10 |
| 2022-11-12 | Phishing Emails | Recognize the main characteristics of phishing emails | 10 |
| 2022-11-12 | Shoulder Surfing | Recognize how shoulder surfing works and the various ways it can be employed | 10 |

About Immersive Labs

Immersive Labs is the world's first fully interactive, on-demand, and gamified cyber skills platform. Our technology delivers challenge-based assessments and upskilling exercises which are developed by cyber experts with access to the latest threat intelligence. Our unique approach engages users of every level, so all employees can be equipped with critical skills and practical experience in real time.