

Jamie Cowan

Completed 202 labs earning 12490 points.



Activity Report

Date	Lab	Description	Points Earned
2021-02-02	Introduction to ELF Reverse Engineering	Exposure to ELF binary analysis	100
2021-01-31	Msfconsole: Auxiliaries	Use Metasploit auxiliary modules for scanning	100
2021-01-31	Banner Grabbing	Identify and enumerate common services	100
2021-01-25	It's a Game of Pong	Develop critical thinking	300
2021-01-25	Stream Redirection	Manipulate data streams using the terminal	100
2021-01-25	Kringle Inc.	Decode common encoding and encryption schemes	100
2021-01-25	CertUtil	Analyse the function of CertUtil	100
2021-01-25	Tactics Initial Access	Be able to recognise the techniques within the Initial Access tactic of the MITRE ATT&CK framework	40
2021-01-24	Netcat: Ep.1	Use Netcat for various tasks	100
2021-01-24	Windows Forensics	Investigate and analyse operating systems using common forensic techniques	300

Activity Report Page 2 of 14

Date	Lab	Description	Points Earned
2021-01-24	Msfconsole: Using the Database	Apply Metasploit's database and project management features	100
2021-01-24	MongoDB: An Introduction	A basic understanding of NoSQL Databases	100
2021-01-24	Packet Capture Basics	Analyse network packet captures	100
2021-01-24	Burp Suite Basics: Introduction	Set up and use Burp Suite with Firefox	200
2021-01-24	SimpleHTTPServer	Basic understanding of SimpleHTTPServer	100
2021-01-24	Process Explorer	Use Process Explorer effectively	100
2021-01-24	CVE-2019-1388 (Windows Priv Esc UAC Bypass)	Bypass User Account Controls	200
2021-01-24	Network Scanning	Operate various network scanning tools to identify open ports	100
2021-01-24	Intro to Wireshark	Analyse network packet captures	100
2021-01-24	Introduction to Encryption	Identify different types of encryption algorithms	200
2021-01-24	Supply Chain Hardware Tampering	Practise interacting with a Baseboard Management Controller	100
2021-01-24	SMTP Log Analysis	Carry out a log analysis in order to identify particular information	100
2021-01-24	Scheduled Tasks	Demonstrate how to navigate information in Windows Scheduled Tasks	100
2021-01-24	Windows Registry	Evaluate registry values	100
2021-01-24	Protocols LDAP	Analyse the LDAP protocol in an enterprise context	100

Activity Report Page 3 of 14

Date	Lab	Description	Points Earned
2021-01-24	World Cup Trivia	Develop critical thinking	300
2021-01-24	Getting Hashed	Reproduce hashes on created files	100
2021-01-24	Clipboard Data Theft	Analyse techniques used by adversaries to steal clipboard data	100
2021-01-24	Sudo	Use the sudo command to elevate privileges in Linux	100
2021-01-24	Exfiltration Over Alternative Protocol	Practise identifying instances where data has been exfiltrated	100
2021-01-24	OpenLDAP - Plaintext Passwords	Analyse an LDAP post exploitation technique	100
2021-01-24	Parsing PST	Investigate email client files	200
2021-01-24	CVE-2019-0708 (BlueKeep: Snort Rule)	Apply principles of how security teams may update systems in preparation for known threats	100
2021-01-24	Symmetric vs Asymmetric Key Encryption	Apply symmetric key encryption and decryption techniques	100
2021-01-24	Wireshark Display Filters: An Introduction	Analyse network packet captures	100
2021-01-24	Tactics Execution	Exposure to techniques that are contained in the Execution tactic	20
2021-01-24	Tactics Privilege Escalation	Recognise MITRE ATT&CK Privilege Escalation techniques	20
2021-01-24	XSL Script Processing	Demonstrate bypassing the restrictions set on PowerShell	100
2021-01-24	Windows Sysmon	Analyse and investigate system logs	100
2021-01-23	Virtualisation	Describe the uses and advantages of virtualisation	10

Activity Report Page 4 of 14

Date	Lab	Description	Points Earned
2021-01-23	Who are the Hackers?	List and categorise different types of hacker	10
2021-01-23	Why Hackers Hack	List and categorise different motivations of hackers	10
2021-01-23	Tactics Defence Evasion	Exposure to techniques contained in the Execution tactic	20
2021-01-23	Typex	Practise using the CyberChef tool	100
2021-01-23	Tactics Persistence	Recognise the techniques within the Execution tactic of the MITRE ATT&CK framework	40
2021-01-23	The Bombe	Practise using the CyberChef tool	300
2021-01-23	Data Compressed	Practise detecting data compressed prior to exfiltration	300
2021-01-23	Virtual Card Numbers	Recall the benefits of using virtual card numbers	10
2021-01-23	Port Identification	Match common ports to services	100
2021-01-23	Tools Leak Who are APT34?	Familiarise yourself with APT34	40
2021-01-23	Introduction to Computer Memory and Architecture	Gain a high level understanding of how memory works in a computer system	40
2021-01-23	Platform as a Service (PaaS)	Be able to explain the advantages and disadvantages of Platform as a Service	20
2021-01-23	HTTP Status Codes	Develop knowledge of HTTP status codes	100
2021-01-23	Binary	Perform text to binary conversions	40
2021-01-23	Base64 Encoding	Practise encoding and decoding using Base64	40

Activity Report Page 5 of 14

Date	Lab	Description	Points Earned
2021-01-23	Hashing SHA-1	Apply the SHA1 hashing algorithm to strings	40
2021-01-23	Security Automation	Describe the advantages of security automation and orchestration	20
2021-01-23	Infrastructure as Code (IaC)	Explain what IaC is and how it is deployed	20
2021-01-23	SecDevOps	Describe SecDevOps and its different components	20
2021-01-23	Infrastructure as a Service (IaaS)	Describe the advantages and disadvantages of Infrastructure as a Service (IaaS).	20
2021-01-23	Intrusion Detection Systems	Describe intrusion detection and prevention principles	20
2021-01-23	Security Champions	Describe what a security champion is	10
2021-01-23	How to Mitigate Risk	Explain how risk management can help in risk mitigation	20
2021-01-23	Software as a Service (SaaS)	Be able to describe the advantages and disadvantages of SaaS	20
2021-01-23	Accounting and Audit	Identify audit and accounting methodology	100
2021-01-23	Containers	Describe containers and their advantages and disadvantages	20
2021-01-23	Command History	Be able to identify the risk of passing credentials with the command line	100
2021-01-23	NIST Cyber Security Framework	List the three main components of the NIST Cyber Security Framework	40
2021-01-23	Going Places	Use SSH to connect to remote servers	100
2021-01-23	WannaCry	Safely observe WannaCry ransomware	100

Activity Report Page 6 of 14

Date	Lab	Description	Points Earned
2021-01-23	IoT Best Practice	Describe how to securely deploy IoT devices	10
2021-01-23	Space After Filename	Inspect suspicious files and analyse their function	100
2021-01-23	STIX	Locate Cyber Threat Information from within STIX objects	40
2021-01-23	Internet Protocol V4	Explain the core concepts of IPv4 addressing	100
2021-01-23	Three Lines of Defence	Describe the Three Lines of Defence method for managing risk	10
2021-01-23	Domain Name System	Explain the roles of different name servers and the process of making a DNS request	100
2021-01-23	IoT/Embedded Hardware Reverse Engineering	Identify security best practices for IoT devices	10
2021-01-23	Qualitative Risk Measurement	Classify impacts and probabilities on a qualitative risk matrix	20
2021-01-23	IoT/Embedded Network Protocols and Security	Express the importance of using encryption to secure communications	10
2021-01-23	Risk and Control Self Assessment (RCSA)	The role and purpose of an RCSA within the wider risk management framework	20
2021-01-23	Quantitative Risk Measurement	Calculate quantitative risk as a function of impact and probability	100
2021-01-23	Inherent vs Residual Risk	Explain the difference between inherent and residual risk	20
2021-01-23	Information Security	Describe the CIA triad and other information security principals	10
2021-01-23	Vulnerability Identification	Define the different ways to conduct vulnerability identification	20
2021-01-23	Asset Inventory and Valuation	Define the asset identification and valuation processes	20

Activity Report Page 7 of 14

Date	Lab	Description	Points Earned
2021-01-23	Enigma	Discover the cipher methods used in the world wars	300
2021-01-23	Real World Examples of IoT/Embedded Security Issues	Identify security best practice for IoT devices	10
2021-01-23	Protocols ARP	Identify packet structure of ARP requests and responses	100
2021-01-23	Protocols FTP	Explain the core concepts of the File Transfer Protocol	100
2021-01-23	How Is Risk Measured?	Be able to define risk, impact, and probability	40
2021-01-23	What Is Risk?	Be able to define the core concepts that formulate risk	20
2021-01-23	Keylogging	Recall how keyloggers are used to steal information	10
2021-01-23	Web Applications: Page Source Review	Analyse the web application source code to recognise technologies being used	200
2021-01-23	Transport Protocols	Explain the core concepts of the the most common transport protocols	200
2021-01-23	OSI Model	Identify the different layers of the OSI model	40
2021-01-23	Log Finder	Perform web log analysis	100
2021-01-23	Ports	Identify how ports are used in modern networks	40
2021-01-23	ASCII	Perform ASCII to plaintext conversions	40
2021-01-23	Introduction to MITRE ATT&CK	Be familiar with the MITRE ATT&CK framework and know how it is used	40
2021-01-23	Hexadecimal	Practise converting various types of data to hexadecimal	40

Activity Report Page 8 of 14

Date	Lab	Description	Points Earned
2021-01-23	The Importance of Cybersecurity	Recognise the importance of cybersecurity	10
2021-01-23	Server Identification	Identify default honeypot configurations	200
2021-01-23	Intro to Malware Static Analysis	Understanding of basic malware	40
2021-01-23	Intro to Malware Dynamic Analysis	Knowledge of dynamic analysis	40
2021-01-23	Introduction to Command & Control Frameworks	An introduction to Command and Control Frameworks	40
2021-01-23	Punycode/Homograph	Identify threat of URI encoding techniques	40
2021-01-23	Spiderfoot	Scan and analyse data using speciality OSINT tools	40
2021-01-23	Introduction to Hashing	Identify the characteristics of a good hashing algorithm	100
2021-01-23	IP Addresses	Explain the core concepts behind IP addressing	40
2021-01-23	File Command	Using file to identify true information about unusual looking files	100
2021-01-23	Introduction to Incident Response	Identify incident response principles	40
2021-01-23	CyberChef Recipes	Basic encoding and encryption operations	40
2021-01-23	Stack Overflow	Demonstrate the risk of using code found online	10
2021-01-23	The Incident Response Process	Identify the details of each stage of the incident response process	40
2021-01-23	Introduction to Forensics	Exposure to forensics principals	40

Activity Report Page 9 of 14

Date	Lab	Description	Points Earned
2021-01-23	SQL: An Introduction	Gain an understanding of the SQL language and queries	100
2021-01-23	Cybersecurity On The Go	Recognise the risks of using company and personal devices while travelling	10
2021-01-23	Tor	Describe how Tor works	40
2021-01-23	Introduction to Threat Hunting	Exposure to threat hunting principles	40
2021-01-23	AWS Security Groups	Analyse security configuration	40
2021-01-23	Windows Sysinternals	An overview of the Sysinternals suite	100
2021-01-23	Incident Response in the Workplace	Recall general workplace incident response processes	10
2021-01-23	Covid-19 Phishing Emails: How to Spot Them	Identify malicious emails	10
2021-01-23	Accidental Data Leaks	Identify accidental data leaks	10
2021-01-23	Port Bingo - Easy Mode	Demonstration of critical thinking	200
2021-01-23	Online anonymity	Describe how to increase your online anonymity	40
2021-01-23	Rainbow Tables	Explain why rainbow tables are useful for password cracking	40
2021-01-23	The Internet	Explain the history of the internet	40
2021-01-23	Validating SIEM Results	Identify whether the activity or inactivity of a SIEM is accurate in any given scenario	40
2021-01-23	VirusTotal	Discover automated malware analysis tools and communities	100

Activity Report Page 10 of 14

Date	Lab	Description	Points Earned
2021-01-23	Search Engines	Recognise the difference between the surface web, deep web, and dark web	20
2021-01-23	Defence in Depth	Discover the principles of defence systems	20
2021-01-23	CyberChef	Practise using CyberChef to encode and encrypt	100
2021-01-23	Immersive Bank: Ep.1 Open Source and Credentials	Employ Open Source Intelligence to uncover the CEO's password	200
2021-01-23	PowerShell: Ep.2	Practice reading from and writing to files in PowerShell	100
2021-01-23	Order of Volatility	Revision and analysis on the Order of Volatility	100
2021-01-23	PowerShell: Ep.1	Practise using the PowerShell cmdlets	100
2021-01-23	Immersive Bank: Ep.2 Gaining Access	Apply critical thinking to gain access to the computer	200
2021-01-23	Caesar Cipher	Solve Caesar Cipher	40
2021-01-22	Accreditation	An understanding of accreditation within information systems	10
2021-01-22	Open Source Intelligence (OSINT): Deleted Tweet	Analyse information using open source intelligence techniques	40
2021-01-22	Linux File Permissions	Practise reading and setting file permissions in Linux	100
2021-01-22	Open Source Intelligence (OSINT): Boarding Pass	Analyse information using open source intelligence techniques	100
2021-01-22	Command Line Introduction	Identify relevant basic Linux commands	100
2021-01-22	Safe Browsing	Recognise how to protect yourself and your privacy as you browse the web	10

Activity Report Page 11 of 14

Date	Lab	Description	Points Earned
2021-01-22	Cryptocurrency & Blockchain	An introduction to cryptocurrency and blockchain concepts	10
2021-01-22	Multi-Factor Authentication	Understand multi-factor authentication	10
2021-01-22	Backups	Identify the different types of backups and their importance	10
2021-01-22	Identity Theft	Demonstrate an understanding of identity theft	10
2021-01-22	Shodan.io	Gain an understanding of the Shodan.io search engine and how to run queries	20
2021-01-22	Cookies	Describe cookies, their uses, and how to remove them	10
2021-01-22	Darknets	Gain knowledge of darknets and the technology that allows them to run	10
2021-01-22	Cached and Archived Websites	Interpret and analyse information collected from web archives	20
2021-01-22	Mobile Security Tips	Understand best practices for mobile security	10
2021-01-22	EXIF	Knowledge in the various sorts of data that is stored in images	40
2021-01-22	Geolocation	Recognise device-based and server-based geolocation tracking	10
2021-01-22	Social Engineering	Gain a deeper understanding of social engineering	10
2021-01-22	Cyber Essentials	Identify the most common attacks outlined by the Cyber Essentials scheme	20
2021-01-22	Text editors	Experience modifying files using Nano and Vim	100
2021-01-22	NIS Directive	Explain the NIS Directive and compare to the NIST Cyber Security Framework	20

Activity Report Page 12 of 14

Date	Lab	Description	Points Earned
2021-01-22	Payment Card Industry Data Security Standard (PCI-DSS)	Classify the different PCI-DSS control objectives	20
2021-01-22	Windows File Permissions	Analyse Windows file permissions	100
2021-01-22	Policy, Process and Procedure	Describe the differences between policies, processes and procedures	10
2021-01-22	Compliance, Legislation, Regulation and Standards	Describe the differences between compliance, legislation, regulation and standards	10
2021-01-22	Health Insurance Portability and Accountability Act (HIPAA)	Describe the five titles that form the structure of HIPAA	20
2021-01-22	Information Technology Health Check (ITHC)	Identify the part of internal and external testing required by the ITHC	20
2021-01-22	Cloud Security Alliance Cloud Controls Matrix	Describe the CSA CCM framework	20
2021-01-22	Changing Things	Identify Linux commands relating to files and folders	100
2021-01-22	Moving Around	Demonstrate navigation of files and directories	100
2021-01-22	UK's NCSC 10 Steps to Cyber Security	Describe each of the 10 Steps to Cyber Security	20
2021-01-22	Payment Services Directive 2 (PSD2)	Describe how PSD2 works and affects the banking industry	10
2021-01-22	Fake News	Describe and identify fake news	10
2021-01-22	Antivirus	Understand antivirus software products and their features	10
2021-01-22	Hashing MD5	Apply the MD5 hashing algorithm to strings	100
2021-01-22	Cybersecurity Basics	Understand the topics raised in the lab	10

Activity Report Page 13 of 14

Date	Lab	Description	Points Earned
2021-01-22	Cyber Terminology	Recall key cyber terms and phrases	10
2021-01-22	Disposing of Old Technology	Recognise which devices can hold information after incorrect disposal	10
2021-01-22	Passwords	Identify and demonstrate good password practices	10
2021-01-22	History of Cybersecurity	Summarise the history of cybersecurity	10
2021-01-22	What Is Cybersecurity?	Summarise what cybersecurity means	10
2021-01-22	Why Cybersecurity Is Everyone's Business	Recognise why cybersecurity is important for everyone	10
2021-01-22	Consequences and Impact of Cyberattacks	Define the consequences and impact of cyberattacks	10
2021-01-22	What Is IoT?	Recognise IoT devices and their associated risks	10
2021-01-22	Firewalls and VPNs	Describe firewalls, VPNs, and their purpose	10
2021-01-22	Updates and Patches	Recall what updates, backups, and patches are for and why they're important	10
2021-01-22	Privacy	Understand privacy and why it's important	10
2021-01-22	Physical Security	Describe the cybersecurity risks involved in physical security	10
2021-01-22	Physical Access Security	Recognise physical access security risks	10
2021-01-22	Using Your Own Tech At Work	Recognise risks associated with using your own tech for work	10
2021-01-22	Rogue USB Devices	Identify malicious USB devices	10

Activity Report Page 14 of 14

Date	Lab	Description	Points Earned
2021-01-22	Identifying Ransomware	Identify the indicators of a ransomware infection	10
2021-01-22	GDPR Aware	Explain the key details and impact of GDPR	10
2021-01-22	Reverse Image Search	Identify image sources	40
2021-01-22	Robots.txt	Identify website information leakage	40
2021-01-22	Default Credentials	Knowledge of default credentials	20
2021-01-22	Domain Intel	Understand the information associated with domain names	40
2021-01-22	NIST Guidance on Remote Working	Identify the risks associated with remote working	10
2021-01-22	Investigator Operations Security (OPSEC)	Source online information relevant to an investigation	40
2021-01-22	Malware	Describe malware and its most common forms	10
2021-01-22	Social Media and Privacy	Recognise the perils of having too much information on social media	10
2021-01-22	Shoulder Surfing	Recognise how shoulder surfing is used as a form of social engineering	10
2021-01-22	Cyber Kill Chain	Familiarisation with the kill chain	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.