Alexander Ahmann

Completed 164 labs earning 10920 points.

Activity Report

Date	Lab	Description	Points Earned
2021-12-21	Msfvenom	Use msfvenom to create a payload	300
2021-12-21	Snort Rules: Ep.1	Demonstrate proficiency in basic Snort rules	200
2021-12-11	SecDevOps	Describe SecDevOps and its different components	20
2021-12-11	Real World Examples of IoT/Embedded Security Issues	Identify security best practice for IoT devices	10
2021-12-11	Hydra: Brute Force	Perform password brute forcing of multiple protocols using hydra	200
2021-12-11	IoT/Embedded Network Protocols and Security	Express the importance of using encryption to secure communications	10
2021-12-11	Introduction to Incident Response	Identify incident response principles	40
2021-09-14	Pass The Hash	Perform a Pass-the-Hash attack on a vulnerable server	200
2021-09-07	Intro to Malware Static Analysis	Demonstrate and understanding of basic malware concepts	40
2021-09-07	JBiFrost Analysis	Investigate the configuration of malicious Java based remote access trojans	200

Activity Report Page 2 of 12

Date	Lab	Description	Points Earned
2021-09-05	OpenLDAP - Plaintext Passwords	Analyse an LDAP post exploitation technique	100
2021-08-22	Windows Sysmon	Analyse and investigate system logs	100
2021-08-22	Process Explorer	Use Process Explorer effectively	100
2021-08-22	Bad Rabbit	Safely observe Bad Rabbit ransomware	100
2021-08-21	Data Compressed	Practise detecting data compressed prior to exfiltration	100
2021-08-21	File Command	Using file to identify true information about unusual looking files	100
2021-08-21	Cross-Site Scripting (XSS) Reflected	Perform reflected XSS attacks against a website	200
2021-08-21	Windows Sysinternals	An overview of the Sysinternals suite	100
2021-08-21	PowerShell: Ep.2	Practice reading from and writing to files in PowerShell	100
2021-08-21	PowerShell: Ep.1	Practise using the PowerShell cmdlets	100
2021-08-21	Annabelle	Observe Annabelle ransomware safely	100
2021-08-21	Sudo Caching	Identify exploit attempts that abuse the sudo caching technique	100
2021-08-20	XSL Script Processing	Demonstrate bypassing the restrictions set on PowerShell	100
2021-08-20	MongoDB: An Introduction	A basic understanding of NoSQL Databases	100
2021-08-20	Intro to Wireshark	Analyse network packet captures	100

Date	Lab	Description	Points Earned
2021-08-19	SSL Scanning	Identify weak cryptographic ciphers	200
2021-08-19	Space After Filename	Inspect suspicious files and analyse their function	100
2021-08-18	Introduction to MITRE ATT&CK	Be familiar with the MITRE ATT&CK framework and know how it is used	20
2021-08-18	Tactics Defence Evasion	Recognise the purpose of the MITRE ATT&CK Defence Evasion tactic	20
2021-08-18	Tactics Privilege Escalation	Recognise the purpose of the MITRE ATT&CK Privilege Escalation tactic	20
2021-08-18	Tactics Persistence	Recognise the purpose of the MITRE ATT&CK Persistence tactic	20
2021-08-18	Tactics Execution	Know the purpose of the MITRE ATT&CK Execution tactic	20
2021-08-18	Tactics Initial Access	Recognise the purpose of the MITRE ATT&CK Initial Access tactic	20
2021-08-18	Command History	Be able to identify the risk of passing credentials with the command line	100
2021-08-18	Network Scanning	Operate various network scanning tools to identify open ports	100
2021-08-18	Zone Transfer	Analyse DNS information revealed by a zone transfer	200
2021-08-18	Msfconsole: Exploit	Practise using Metasploit's exploit modules to attack services	200
2021-08-18	Banner Grabbing	Identify and enumerate common services	100
2021-08-18	Web Applications: Page Source Review	Analyse the web application source code to recognise technologies being used	200
2021-08-18	Msfconsole: Auxiliaries	Use Metasploit auxiliary modules for scanning	100

Activity Report Page 4 of 12

Date	Lab	Description	Points Earned
2021-08-18	SimpleHTTPServer	Basic understanding of SimpleHTTPServer	100
2021-08-18	Intro to Malware Dynamic Analysis	Knowledge of dynamic analysis	40
2021-08-18	Decompiling .NET	Familiarisation with .NET	400
2021-08-18	SQL: An Introduction	Gain an understanding of the SQL language and queries	100
2021-08-17	Nmap: Ep.1 Basic Scanning	Demonstrate basic network scanning techniques	200
2021-08-16	Spiderfoot	Scan and analyse data using speciality OSINT tools	40
2021-08-16	Domain Intel	Understand the information associated with domain names	40
2021-08-16	Msfconsole: Using the Database	Apply Metasploit's database and project management features	100
2021-08-16	Default Credentials	Knowledge of default credentials	20
2021-08-16	Open Source Intelligence (OSINT): Deleted Tweet	Analyse information using open source intelligence techniques	40
2021-08-16	Tor	Describe how Tor works	40
2021-08-16	Shodan.io	Gain an understanding of the Shodan.io search engine and how to run queries	20
2021-08-16	Open Source Intelligence (OSINT): Boarding Pass	Analyse information using open source intelligence techniques	100
2021-08-16	EXIF	Knowledge in the various sorts of data that is stored in images	40
2021-08-16	Reverse Image Search	Identify image sources	40

Date	Lab	Description	Points Earned
2021-08-16	Robots.txt	Identify website information leakage	40
2021-08-16	Investigator Operations Security (OPSEC)	Source online information relevant to an investigation	40
2021-08-16	Social Media and Privacy	Recognise the perils of having too much information on social media	10
2021-08-16	Cached and Archived Websites	Interpret and analyse information collected from web archives	20
2021-08-16	Online anonymity	Describe how to increase your online anonymity	40
2021-08-16	Search Engines	Recognise the difference between the surface web, deep web, and dark web	20
2021-08-16	Accreditation	An understanding of accreditation within information systems	10
2021-08-16	Policy, Process and Procedure	Describe the differences between policies, processes and procedures	10
2021-08-16	Compliance, Legislation, Regulation and Standards	Describe the differences between compliance, legislation, regulation and standards	10
2021-08-16	NIST Cyber Security Framework	List the three main components of the NIST Cyber Security Framework	40
2021-08-16	Three Lines of Defence	Describe the Three Lines of Defence method for managing risk	10
2021-08-16	Risk and Control Self Assessment (RCSA)	The role and purpose of an RCSA within the wider risk management framework	20
2021-08-16	How to Mitigate Risk	Explain how risk management can help in risk mitigation	20
2021-08-13	Linux CLI: Ep. 14 Using Screen	Be able to explain screen's CLI usage	100
2021-08-13	Vulnerability Identification	Define the different ways to conduct vulnerability identification	20

Activity Report Page 6 of 12

Date	Lab	Description	Points Earned
2021-08-13	Asset Inventory and Valuation	Define the asset identification and valuation processes	20
2021-08-13	Qualitative Risk Measurement	Classify impacts and probabilities on a qualitative risk matrix	20
2021-08-13	Quantitative Risk Measurement	Calculate quantitative risk as a function of impact and probability	100
2021-08-13	How Is Risk Measured?	Be able to describe risk, impact, and probability	40
2021-08-13	What Is Risk?	Define the core concepts that formulate risk	20
2021-08-13	Protocols ARP	Identify packet structure of ARP requests and responses	100
2021-08-13	CertUtil	Analyse the function of CertUtil	100
2021-08-13	Background Intelligent Transfer Service (BITS)	Gain an understanding of BITS and how it can be abused	100
2021-08-13	Scheduled Tasks	Demonstrate how to navigate information in Windows Scheduled Tasks	100
2021-08-13	Linux CLI: Ep. 16 Combining Commands	Identify the different ways of combining commands on the terminal	200
2021-08-13	Linux CLI: Ep. 15 Generating File Hashes	Be able to recognise file hashes	100
2021-08-13	Inherent vs Residual Risk	Explain the difference between inherent and residual risk	20
2021-08-13	Linux CLI: Ep. 13 Searching and Sorting	Know how to employ searching techniques to find patterns in files	100
2021-08-13	Linux CLI: Ep. 12 Using Find	Recognise how the find command works and the filters and arguments that go with it	200
2021-08-13	Linux CLI: Ep. 11 Using SSH and SCP	Recall what the SSH protocol is	100

Activity Report Page 7 of 12

Date	Lab	Description	Points Earned
2021-08-13	Linux CLI: Ep. 10 Using Sudo	Identify different user privileges in Linux	100
2021-08-13	Linux CLI: Ep. 9 Stream Redirection	Know how data can be manipulated via the terminal	100
2021-08-13	Linux CLI: Ep. 8 Manipulating Text	Know how to modify text within files using basic command line tools	200
2021-08-13	Linux CLI: Ep. 7 Using wc	Be able to count elements in a file using the wc tool	200
2021-08-13	Linux CLI: Ep. 6 Editing Files	Be able to recall some common Linux command line text editors	100
2021-08-13	Linux CLI: Ep. 5 File Permissions	Be able to read Linux file permissions	100
2021-08-13	Protocols FTP	Explain the core concepts of the File Transfer Protocol	100
2021-08-13	Linux CLI: Ep. 3 Moving Around	Have the ability to navigate through directories on the command line	100
2021-08-13	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
2021-08-12	Encryption Tools: CyberChef Recipes	Recall how CyberChef recipes work	40
2021-08-12	Encryption Tools: CyberChef	Recall how CyberChef functions	40
2021-08-12	ASCII.	Perform ASCII to plaintext conversions	40
2021-08-12	Base64 Encoding.	Practise encoding and decoding using Base64	40
2021-08-12	Hexadecimal.	Practise converting various types of data to hexadecimal	40
2021-08-12	Binary	Recall how binary functions	40

Activity Report Page 8 of 12

Date	Lab	Description	Points Earned
2021-08-12	Virtual Card Numbers	Recall the benefits of using virtual card numbers	10
2021-08-12	Rogue USB Devices	Identify malicious USB devices	10
2021-08-12	Cryptocurrency & Blockchain	An introduction to cryptocurrency and blockchain concepts	10
2021-08-12	Darknets	Gain knowledge of darknets and the technology that allows them to run	10
2021-08-12	Keylogging	Recall how keyloggers are used to steal information	10
2021-08-12	Fake News	Describe and identify fake news	10
2021-08-12	Geolocation	Recognise device-based and server-based geolocation tracking	10
2021-08-12	Cookies	Describe cookies, their uses, and how to remove them	10
2021-08-12	Intrusion Detection Systems	Describe intrusion detection and prevention principles	20
2021-08-12	Why Hackers Hack	List and categorise different motivations of hackers	10
2021-08-12	Who are the Hackers?	List and categorise different types of hacker	10
2021-08-12	Cyber Kill Chain	Familiarisation with the kill chain	10
2021-08-12	Security Champions	Describe what a security champion is	10
2021-08-12	Caesar Ciphers	Recall how Caesar cipher encoding works	40
2021-08-12	Information Security	Describe the CIA triad and other information security principals	10

Activity Report Page 9 of 12

Date	Lab	Description	Points Earned
2021-08-11	Updates and Patches	Recall what updates, backups, and patches are for and why they're important	10
2021-08-11	Accidental Data Leaks	Identify accidental data leaks	10
2021-08-11	Backups	Identify the different types of backups and their importance	10
2021-08-11	Identity Theft	Demonstrate an understanding of identity theft	10
2021-08-11	Firewalls and VPNs	Describe firewalls, VPNs, and their purpose	10
2021-08-11	Identifying Ransomware	Identify the indicators of a ransomware infection	10
2021-08-11	Malware	Describe malware and its most common forms	10
2021-08-11	Antivirus	Understand antivirus software products and their features	10
2021-08-11	Multi-Factor Authentication	Understand multi-factor authentication	10
2021-08-11	Mobile Security Tips	Understand best practices for mobile security	10
2021-08-11	Safe Browsing	Recognise how to protect yourself and your privacy as you browse the web	10
2021-08-11	Covid-19 Phishing Emails: How to Spot Them	Identify malicious emails	10
2021-08-11	Phishing Emails	Be able to distinguish between phishing emails and legitimate emails	10
2021-08-11	Consequences and Impact of Cyberattacks	Define the consequences and impact of cyberattacks	10
2021-08-11	Why Cybersecurity Is Everyone's Business	Recognise why cybersecurity is important for everyone	10

Activity Report Page 10 of 12

Date	Lab	Description	Points Earned
2021-08-11	Passwords	Identify and demonstrate good password practices	10
2021-08-10	History of Cybersecurity	Summarise the history of cybersecurity	10
2021-08-10	Personal Devices in the Workplace	Recognize the risks associated with using personal devices in the workplace	10
2021-08-10	Incident Response in the Workplace	Recall general workplace incident response processes	10
2021-08-09	Privacy	Identify what privacy is and why it needs protecting	10
2021-08-09	Privileged Access	Recall what privileged access is and why it's an attractive target for attackers	10
2021-08-09	Physical Security	Identify common physical security risks	10
2021-08-09	Shoulder Surfing	Recognize how shoulder surfing works and the various ways it can be employed	10
2021-08-09	Information Security and Cybersecurity Terminology	Recall some key information security and cybersecurity terms and phrases	10
2021-08-09	Security On The Go	Recognize the security risks of using devices when away from the office	10
2021-08-09	Social Engineering	Describe different social engineering attack techniques and their impacts	10
2021-08-09	Disposal of Device Information	Recognize why secure device disposal is core to an organizations information management process	10
2021-08-09	The Importance of Information Security and Cybersecurity	Describe a simulated example of a breach and recall its emotional impact	10
2021-08-09	Information Security Starting at the Beginning	Recall the difference between information security and cybersecurity	10
2021-08-09	Linux CLI: Ep. 2 Getting Started with the Terminal	Be able to recall fundamental concepts of the Linux terminal	100

Activity Report Page 11 of 12

Date	Lab	Description	Points Earned
2021-08-09	Linux CLI: Ep.1 Introduction to the Linux Command Line Interface	Recall Linux command line fundamentals	40
2021-08-09	Windows Registry	Evaluate registry values	100
2021-08-09	Introduction to Command & Control Frameworks	An introduction to Command and Control Frameworks	40
2021-08-09	sqlmap	Practise applying sqlmap to a database	200
2021-08-09	Guidance on Remote Working	Identify the risks associated with remote working	10
2021-08-09	Introduction to Computer Memory and Architecture	Gain a high level understanding of how memory works in a computer system	40
2021-08-09	Windows File Permissions	Analyse Windows file permissions	100
2021-08-09	Introduction to ELF Reverse Engineering	Exposure to ELF binary analysis	100
2021-08-07	Protocols LDAP	Analyse the LDAP protocol in an enterprise context	100
2021-08-07	HTTP Status Codes	Develop knowledge of HTTP status codes	100
2021-08-07	Transport Protocols	Explain the core concepts of the the most common transport protocols	40
2021-08-07	What Is Information Security?	Identify the workplace and personal security challenges that good information security practices help to solve	10
2021-08-07	Stack Overflow	Demonstrate the risk of using code found online	10
2021-08-07	Introduction to Networking: Ep.6 Domain Name System	Summarize the fundamentals of the Domain Name System	40
2021-08-07	Internet Protocol V4	Explain the core concepts of IPv4 addressing	100

Activity Report Page 12 of 12

Date	Lab	Description	Points Earned
2021-08-07	Ports	Identify how ports are used in modern networks	40
2021-08-07	Introduction to Networking: Ep.5 IP Addresses	Recognize an IP address	40
2021-08-07	OSI Model	Identify the different layers of the OSI model	40
2021-08-07	The Internet	Explain the history of the internet	20

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.