IMMERSIVELABS

Matthew Mcgovern

Completed 221 labs earning 19760 points.

Activity Report

Date	Lab	Description	Points Earned
2020-10-05	Tactics – Execution	Exposure to techniques that are contained in the Execution tactic	20
2020-09-23	Security Automation	Describe the advantages of security automation and orchestration	20
2020-09-23	Infrastructure as Code (IaC)	Describe the advantages of Infrastructure as Code (IaC)	20
2020-09-23	Infrastructure as a Service (IaaS)	Describe the advantages and disadvantages of Infrastructure as a Service (IaaS).	20
2020-09-23	AWS Security Groups	Analyse security configuration	40
2020-09-23	SecDevOps	Describe SecDevOps and its different component parts.	20
2020-09-23	Containers	Describe containers and their advantages and disadvantages.	20
2020-09-23	Mal Wars	Demonstrate critical thinking	40
2020-09-16	APT34 – Glimpse	Demonstrate an ability to identify Indicators of Compromise in malware with command line tools	200
2020-09-15	S3 Security Permissions	Discover Amazon S3 bucket functionality	200

Activity Report Page 2 of 16

Date	Lab	Description	Points Earned
2020-09-15	Tactics – Initial Access	Exposure to techniques contained in the Initial Access tactic	20
2020-09-15	CVE-2019-1388 (Windows Priv Esc UAC Bypass)	Bypass User Account Controls	200
2020-09-15	CVE-2019-0708 (BlueKeep: Snort Rule)	Apply principles of how security teams may update systems in preparation for known threats	100
2020-09-15	Tools Leak — Who are APT34?	Familiarise yourself with APT34	40
2020-09-15	CVE-2019-0708 (BlueKeep - Exploitation)	Exploit BlueKeep	200
2020-09-07	SQL Injection: UNION	Employ advanced SQL injection techniques	200
2020-09-05	sqlmap	Practise applying sqlmap to a database	200
2020-09-04	Container Security: Volumes	An understanding of how containers access files on the host	100
2020-09-04	JBiFrost Analysis	Investigate the configuration of malicious Java based remote access trojans	200
2020-09-04	Bad Rabbit	Safely observe Bad Rabbit ransomware	100
2020-09-04	Annabelle	Observe Annabelle ransomware safely	100
2020-09-04	Cross-Site Scripting (XSS) - Reflected	Perform reflected XSS attacks against a website	200
2020-09-03	CVE-2019-17387 (Aviatrix VPN Client Privilege Escalation)	Exploit CVE-2019-17387 to escalate privileges	200
2020-09-02	Analysing Sandbox Reports	Investigate malicious samples using sandbox reporting styles	40
2020-09-02	Intro to Malware – Static Analysis	Understanding of basic malware	40

Date	Lab	Description	Points Earned
2020-09-02	APT29 - Reverse Engineering an LNK file	Investigate various malware internal propagation techniques	400
2020-09-02	Server Identification	Identify default honeypot configurations	200
2020-09-02	STIX	Locate Cyber Threat Information from within STIX objects	40
2020-09-02	Introduction to Threat Hunting	Exposure to threat hunting principles	40
2020-09-02	Payment Card Industry Data Security Standard (PCI-DSS)	Classify the different PCI-DSS control objectives	20
2020-09-02	Intro to Malware – Dynamic Analysis	Knowledge of dynamic analysis	40
2020-09-02	Cloud Security Alliance – Cloud Controls Matrix	Describe the CSA CCM framework	20
2020-09-01	MongoDB: An Introduction	A basic understanding of NoSQL Databases	100
2020-09-01	Hydra: Brute Force	Perform password brute forcing of multiple protocols using hydra	200
2020-09-01	Introduction to MITRE ATT&CK™	Gain an understanding of the ATT&CK framework and how it is used	40
2020-09-01	Banner Grabbing	Identify and enumerate common services	100
2020-09-01	UK's NCSC 10 Steps to Cyber Security	Describe each of the 10 Steps to Cyber Security	20
2020-09-01	Web Applications: Directory Traversal	Conduct directory traversal attacks against a web server	200
2020-09-01	Decompiling .NET	Familiarisation with .NET	400
2020-09-01	VirusTotal	Discover automated malware analysis tools and communities	100

Activity Report Page 4 of 16

Date	Lab	Description	Points Earned
2020-09-01	WannaCry	Safely observe WannaCry ransomware	100
2020-09-01	SQL: An Introduction	Gain an understanding of the SQL language and queries	100
2020-09-01	Web Applications: HTTP Parameters and IP	Practise modifying HTTP parameters	200
2020-09-01	Zone Transfer	Analyse DNS information revealed by a zone transfer	200
2020-08-31	Mimikatz & Chrome Passwords	Use post-exploitation techniques	200
2020-08-31	Immersive Bank – Episode Two: Gaining Access	Apply critical thinking to gain access to the computer	100
2020-08-31	Immersive Bank – Episode One: Open Source and Credentials	Employ Open Source Intelligence to uncover the CEO's password	40
2020-08-30	Password Hashes II	Understand the benefits of salting passwords	100
2020-08-29	John the Ripper	Exposure to John the Ripper tool chain	100
2020-08-27	Windows: DLL Hijacking	A good understanding of DLL Hijacking and how it can be used to escalate privileges in Windows	600
2020-08-25	SimpleHTTPServer	Basic understanding of SimpleHTTPServer	100
2020-08-25	GDPR Aware	Explain the key details and impact of GDPR	10
2020-08-25	Accreditation	An understanding of accreditation within information systems	10
2020-08-25	Cyber Essentials	Identify the most common attacks outlined by the Cyber Essentials scheme	20
2020-08-25	Elf in a Shell(f)	Experience navigating the Linux file system	100

Activity Report Page 5 of 16

Date	Lab	Description	Points Earned
2020-08-25	Web Applications: Page Source Review	Analyse the web application source code to recognise technologies being used	200
2020-08-25	SSL Scanning	Identify weak cryptographic ciphers	200
2020-08-25	Python Coding – Introduction	Read Python code	100
2020-08-25	Pass The Hash	Perform a Pass-the-Hash attack on a vulnerable server	200
2020-08-25	OpenLDAP - Plaintext Passwords	Analyse an LDAP post exploitation technique	100
2020-08-24	Kringle Inc.	Protecting a global enterprise from malicious actors	100
2020-08-24	Compliance, Legislation, Regulation and Standards	Describe the differences between compliance, legislation, regulation and standards	10
2020-08-24	Policy, Process and Procedure	Describe the differences between policies, processes and procedures	10
2020-08-22	Exfiltration Over Alternative Protocol	Practise identifying instances where data has been exfiltrated	100
2020-08-22	National Software Reference Library (NSRL)	Discover the national software reference library	100
2020-08-22	Risk and Control Self Assessment (RCSA)	The role and purpose of an RCSA within the wider risk management framework	10
2020-08-22	Netcat	Use Netcat for various tasks	100
2020-08-22	Compromised Host	Investigate host-based compromise and IOCs	400
2020-08-22	Parsing PST	Investigate email client files	200
2020-08-22	Splunk - Event Analysis 2	Demonstrate and develop event log analysis techniques	200

Activity Report Page 6 of 16

Date	Lab	Description	Points Earned
2020-08-22	Suspicious Email	Investigate and gain information from suspected malicious documents	200
2020-08-22	How to Mitigate Risk	Explain how risk management can help in risk mitigation	20
2020-08-22	Log Finder	Perform web log analysis	100
2020-08-22	Space After Filename	Inspect suspicious files and analyse their function	100
2020-08-22	Introduction to Incident Response	Identify incident response principles	40
2020-08-22	Three Lines of Defence	Describe the Three Lines of Defence method for managing risk	10
2020-08-22	The Incident Response Process	Identify the details of each stage of the incident response process	40
2020-08-22	True or False	Identify the difference between false and true positives	100
2020-08-22	Inherent vs Residual Risk	Explain the difference between inherent and residual risk	20
2020-08-22	SMTP Log Analysis	Carry out a log analysis in order to identify particular information	100
2020-08-22	Clipboard Data Theft	Analyse techniques used by adversaries to steal clipboard data	100
2020-08-22	Stack Overflow	Demonstrate the risk of using code found online	10
2020-08-22	Introduction to ELF Reverse Engineering	Exposure to ELF binary analysis	100
2020-08-21	Introduction to Command & Control Frameworks	An introduction to Command and Control Frameworks	40
2020-08-21	Splunk - Event Analysis	Demonstrate and develop basic event log analysis techniques	200

Activity Report Page 7 of 16

Date	Lab	Description	Points Earned
2020-08-20	PowerShell: Episode 1	Practise using the PowerShell cmdlets	100
2020-08-20	Process Explorer	Use Process Explorer effectively	100
2020-08-20	Windows Sysmon	Analyse and investigate system logs	100
2020-08-20	Rainbow Tables	Explain why rainbow tables are useful for password cracking	100
2020-08-20	Punycode/Homograph	Identify threat of URI encoding techniques	40
2020-08-20	Windows Sysinternals	An overview of the Sysinternals suite	100
2020-08-20	PowerShell Empire	Demonstrate the ability to configure and run various PowerShell Empire functions	100
2020-08-20	PowerShell: Episode 2	Practice reading from and writing to files in PowerShell	100
2020-08-19	Investigator Operations Security (OPSEC)	Source online information relevant to an investigation	40
2020-08-19	IoT/Embedded Hardware Reverse Engineering	Identify security best practices for IoT devices	10
2020-08-19	Open Source Intelligence (OSINT): Deleted Tweet	Analyse information using open source intelligence techniques	40
2020-08-19	Qualitative Risk Measurement	Classify impacts and probabilities on a qualitative risk matrix	20
2020-08-19	NIST Cyber Security Framework	List the three main components of the NIST Cyber Security Framework	20
2020-08-19	Snort Rules: Episode 2 – DNS	Create Snort rules for DNS events	300
2020-08-19	Asset Inventory and Valuation	Define the asset identification and valuation processes	10

Activity Report Page 8 of 16

Date	Lab	Description	Points Earned
2020-08-19	IoT Best Practice	Describe how to securely deploy IoT devices	10
2020-08-19	Cached and Archived Websites	Interpret and analyse information collected from web archives	20
2020-08-19	Vulnerability Identification	Define the different ways to conduct vulnerability identification	10
2020-08-19	Supply Chain Hardware Tampering	Practise interacting with a Baseboard Management Controller	100
2020-08-19	Snort Rules: Episode 1	Demonstrate proficiency in basic Snort rules	200
2020-08-19	Snort Rules: Episode 3 – HTTP	Demonstrate usage of Snort rules	300
2020-08-19	Spiderfoot	Scan and analyse data using speciality OSINT tools	40
2020-08-19	IoT/Embedded Network Protocols and Security	Express the importance of using encryption to secure communications	10
2020-08-18	Virtualisation	Describe the uses and advantages of virtualisation	10
2020-08-18	Msfconsole: Auxiliaries	Use Metasploit auxiliary modules for scanning	100
2020-08-18	Burp Suite Basics: HTTPS	Configure and use Burp Suite with Firefox	100
2020-08-18	Burp Suite Basics: Introduction	Set up and use Burp Suite with Firefox	100
2020-08-18	Port Identification	Match common ports to services	100
2020-08-18	Msfconsole: Exploit	Practise using Metasploit's exploit modules to attack services	200
2020-08-18	Msfconsole: Using the Database	Apply Metasploit's database and project management features	100

Activity Report Page 9 of 16

Date	Lab	Description	Points Earned
2020-08-18	Port Bingo - Easy Mode	Demonstration of critical thinking	100
2020-08-17	CyberChef – Recipes	Basic encoding and encryption operations	40
2020-08-17	ASCII	Perform ASCII to plaintext conversions	40
2020-08-14	Symmetric vs Asymmetric Key Encryption	Apply symmetric key encryption and decryption techniques	100
2020-08-14	Typex	Practise using the CyberChef tool	100
2020-08-14	Hashing – SHA-1	Apply the SHA1 hashing algorithm to strings	100
2020-08-13	Hashing – MD5	Apply the MD5 hashing algorithm to strings	100
2020-08-11	Enigma	Discover the cipher methods used in the world wars	100
2020-08-11	The Bombe	Practise using the CyberChef tool	100
2020-08-10	Caesar Cipher	Solve Caesar Cipher	100
2020-08-10	CyberChef	Practise using CyberChef to encode and encrypt	100
2020-08-07	Software as a Service (SaaS)	Describe the advantages and disadvantages of Software as a Service (SaaS)	10
2020-08-07	Platform as a Service (PaaS)	Explain the advantages and disadvantages of Platform as a Service	10
2020-08-06	Open Source Intelligence (OSINT): Boarding Pass	Analyse information using open source intelligence techniques	100
2020-08-06	Msfvenom	Use msfvenom to create a payload	200

Activity Report Page 10 of 16

Date	Lab	Description	Points Earned
2020-08-06	tcpdump	Analyse network packet captures	200
2020-08-06	How Is Risk Measured?	Be able to define risk, impact, and probability	20
2020-08-06	Quantitative Risk Measurement	Calculate quantitative risk as a function of impact and probability	100
2020-08-06	Base64 Encoding	Practise encoding and decoding using Base64	40
2020-08-06	Tor	Describe how Tor works	40
2020-08-06	Shodan.io	Gain an understanding of the Shodan.io search engine and how to run queries	20
2020-08-06	Wireshark: Stream/Object Extraction	Analyse network packet captures	200
2020-08-05	Protocols – LDAP	Analyse the LDAP protocol in an enterprise context	100
2020-08-05	Wireshark Display Filters - An Introduction	Analyse network packet captures	100
2020-08-05	Going Places	Use SSH to connect to remote servers and SCP to copy files back to a local machine.	100
2020-08-05	Protocols – ARP	Identify packet structure of ARP requests and responses	100
2020-08-05	Intrusion Detection Systems	Discover IPS and IDS principles	20
2020-08-05	Updates and Patches	Recall what updates, backups, and patches are for and why they're important	10
2020-08-05	Domain Name System	Explain the roles of different name servers and the process of making a DNS request	100
2020-08-05	Identifying Ransomware	Identify the indicators of a ransomware infection	10

Activity Report Page 11 of 16

Date	Lab	Description	Points Earned
2020-08-05	Defence in Depth	Discover the principles of defence systems	20
2020-08-05	Accounting and Audit	Identify audit and accounting methodology	200
2020-08-05	Why Cybersecurity Is Everyone's Business	Recognise why cybersecurity is important for everyone	10
2020-08-05	Transport Protocols	Explain the core concepts of the the most common transport protocols	200
2020-08-05	Backups	Identify the different types of backups and their importance	10
2020-08-05	Getting hashed	Reproduce hashes on created files	100
2020-08-05	Protocols – FTP	Explain the core concepts of the File Transfer Protocol	100
2020-08-05	Binary	Perform text to binary conversions	40
2020-08-05	Firewalls and VPNs	Describe firewalls, VPNs, and their purpose	10
2020-08-05	HTTP Status Codes	Develop knowledge of HTTP status codes	100
2020-08-05	Windows Forensics	Investigate and analyse operating systems using common forensic techniques	300
2020-08-05	Screen	Practise creating and connecting to screens in Linux	100
2020-08-05	Sudo Caching	An understanding of the risks of sudo misconfiguration	100
2020-08-05	Regular Expressions	Practise creating and using regular expressions	200
2020-08-05	File Command	Using file to identify true information about unusual looking files	100

Activity Report Page 12 of 16

Date	Lab	Description	Points Earned
2020-08-05	Order of Volatility	Revision and analysis on the Order of Volatility	100
2020-08-05	Stream Redirection	Manipulate data streams using the terminal	100
2020-08-05	Passwords	Identify and demonstrate good password practices	10
2020-08-05	Command History	Identify the risk of using parsing credentials with the command line	100
2020-08-05	Mobile Security Tips	Understand best practices for mobile security	10
2020-08-05	Packet Capture Basics	Analyse network packet captures	100
2020-08-05	Safe Browsing	Recognise how to protect yourself and your privacy as you browse the web	10
2020-08-05	Timestomp	Autopsy usage	300
2020-08-05	Consequences and Impact of Cyberattacks	Define the consequences and impact of cyberattacks	10
2020-08-05	Internet Protocol V4	Explain the core concepts of IPv4 addressing	100
2020-08-05	CertUtil	Analyse the function of CertUtil	100
2020-08-05	Intro to Wireshark	Analyse network packet captures	100
2020-08-05	Identity Theft	Demonstrate an understanding of identity theft	10
2020-08-05	Manipulating Text	Experience manipulating file contents	200
2020-08-04	Nmap: Episode 1 – Basic Scanning	Demonstrate basic network scanning techniques	200

Activity Report Page 13 of 16

Date	Lab	Description	Points Earned
2020-08-04	Security Champions	Describe what a security champion is	10
2020-08-04	Keylogging	Recall how keyloggers are used to steal information	10
2020-08-04	Shoulder Surfing	Recognise how shoulder surfing is used as a form of social engineering	10
2020-08-04	Malware	Describe malware and its most common forms	10
2020-08-04	Moving Around	Demonstrate navigation of files and directories	100
2020-08-04	Cyber Kill Chain	Familiarisation with the kill chain	10
2020-08-04	Real World Examples of IoT/Embedded Security Issues	Identify security best practice for IoT devices	10
2020-08-04	Covid-19 Phishing Emails: How to Spot Them	Identify malicious emails	10
2020-08-04	Domain Intel	Knowledge of domain names	40
2020-08-04	Darknets	Gain knowledge of darknets and the technology that allows them to run	10
2020-08-04	History of Cybersecurity	Summarise the history of cybersecurity	10
2020-08-04	Cryptocurrency & Blockchain	An introduction to cryptocurrency and blockchain concepts	10
2020-08-04	Cybersecurity Basics	Understand the topics raised in the lab	10
2020-08-04	Linux File Permissions	Practise reading and setting file permissions in Linux	100
2020-08-04	Multi-Factor Authentication	Understand multi-factor authentication	10

Activity Report Page 14 of 16

Date	Lab	Description	Points Earned
2020-08-04	Cookies	Describe cookies, their uses, and how to remove them	10
2020-08-04	Physical Security	Describe the cybersecurity risks involved in physical security	10
2020-08-04	Physical Access Security	Recognise physical access security risks	10
2020-08-04	Geolocation	Recognise device-based and server-based geolocation tracking	10
2020-08-04	Scheduled Tasks	Demonstrate how to navigate information in Windows Scheduled Tasks	100
2020-08-04	Social Engineering	Gain a deeper understanding of social engineering	10
2020-08-04	EXIF	Knowledge in the various sorts of data that is stored in images	40
2020-08-04	Fake News	Describe and identify fake news	10
2020-08-04	Sudo	Use of the sudo command to elevate privileges in Linux	100
2020-08-04	Virtual Card Numbers	Recall the benefits of using virtual card numbers	10
2020-08-04	Hexadecimal	Practise converting various types of data to hexadecimal	40
2020-08-04	Background Intelligent Transfer Service (BITS)	Gain an understanding of BITS and how it can be abused	100
2020-08-04	Ports	Identify how ports are used in modern networks	40
2020-08-04	Privacy	Understand privacy and why it's important	10
2020-08-04	Windows File Permissions	Analyse Windows file permissions	100

Activity Report Page 15 of 16

Date	Lab	Description	Points Earned
2020-08-04	Who are the Hackers?	List and categorise different types of hacker	10
2020-08-04	Robots.txt	Identify website information leakage	40
2020-08-04	Antivirus	Understand antivirus software products and their features	10
2020-08-04	What Are IoT and Cyber?	Identify risks associated with IoT devices	10
2020-08-04	Text editors	Experience modifying files using Nano and Vi	100
2020-08-04	What Is Cybersecurity?	Summarise what cybersecurity means	10
2020-08-04	Changing Things	Identify Linux commands relating to files and folders	100
2020-08-04	Reverse Image Search	Identify image sources	40
2020-08-04	What Is Risk?	Be able to define the core concepts that formulate risk	20
2020-08-04	Disposing of Old Technology	Recognise which devices can hold information after incorrect disposal	10
2020-08-04	Windows Registry	Evaluate registry values	100
2020-08-04	Cyber Terminology	Recall key cyber terms and phrases	10
2020-08-04	Network Scanning	Operate various network scanning tools to identify open ports	100
2020-08-04	Introduction to Forensics	Exposure to forensics principals	40
2020-07-28	Default Credentials	Knowledge of default credentials	20

Date	Lab	Description	Points Earned
2020-07-28	Command Line Introduction	Identify relevant basic Linux commands	100

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.