Kashif mamda

Completed 116 labs earning 17880 points.

Activity Report

Date	Lab	Description	Points Earned
2021-05-15	Identifying Ransomware	Identify the indicators of a ransomware infection	10
2021-05-15	Background Intelligent Transfer Service (BITS)	Gain an understanding of BITS and how it can be abused	100
2021-05-15	Space After Filename	Inspect suspicious files and analyse their function	100
2021-05-15	Why Cybersecurity Is Everyone's Business	Recognise why cybersecurity is important for everyone	10
2021-05-15	Going Places	Use SSH to connect to remote servers	100
2021-05-15	Sudo Caching	An understanding of the risks of sudo misconfiguration	100
2021-05-15	Text editors	Experience modifying files using Nano and Vim	100
2021-05-15	File Command	Using file to identify true information about unusual looking files	100
2021-05-15	Manipulating Text	Demonstrating the use of basic linux commands to manipulate files	200
2021-05-15	Elf in a Shell(f)	Use and chain Linux builtin commands to navigate a file system	100

Activity Report Page 2 of 9

Date	Lab	Description	Points Earned
2021-05-15	XSL Script Processing	Demonstrate bypassing the restrictions set on PowerShell	100
2021-05-15	Order of Volatility	Revision and analysis on the Order of Volatility	100
2021-05-15	Windows Sysmon	Analyse and investigate system logs	100
2021-05-15	Backups	Identify the different types of backups and their importance	10
2021-05-15	Screen	Practise creating and connecting to screens in Linux	100
2021-05-15	Sudo	Use the sudo command to elevate privileges in Linux	100
2021-05-15	OpenLDAP - Plaintext Passwords	Analyse an LDAP post exploitation technique	100
2021-05-15	Linux File Permissions	Practise reading and setting file permissions in Linux	100
2021-05-14	S3 Security Permissions	Discover Amazon S3 bucket functionality	200
2021-05-14	SMTP Log Analysis	Carry out a log analysis in order to identify particular information	100
2021-05-14	Windows Registry	Evaluate registry values	100
2021-05-14	SimpleHTTPServer	Basic understanding of SimpleHTTPServer	100
2021-05-14	Protocols FTP	Explain the core concepts of the File Transfer Protocol	100
2021-05-14	Protocols ARP	Identify packet structure of ARP requests and responses	100
2021-05-14	Network Scanning	Operate various network scanning tools to identify open ports	100

Activity Report Page 3 of 9

Date	Lab	Description	Points Earned
2021-05-14	Log Finder	Perform web log analysis	100
2021-05-14	Protocols LDAP	Analyse the LDAP protocol in an enterprise context	100
2021-05-13	Container Security: Volumes	Learn how containers access files on the host	600
2021-05-13	APT29: Reverse Engineering an LNK file	Investigate various malware internal propagation techniques	400
2021-05-13	Accounting and Audit	Identify audit and accounting methodology	200
2021-05-13	Pass The Hash	Perform a Pass-the-Hash attack on a vulnerable server	200
2021-05-12	Bypassing HTTP Client-Side Controls	Recognise some common insecure user access controls that can be found in web applications	200
2021-05-12	JBiFrost Analysis	Investigate the configuration of malicious Java based remote access trojans	200
2021-05-11	Regular Expressions	Know how to create and use regular expressions	200
2021-05-09	Kringle Inc.	Decode common encoding and encryption schemes	300
2021-05-09	World Cup Trivia	Develop critical thinking	300
2021-05-09	It's a Game of Pong	Develop critical thinking	300
2021-05-09	Zone Transfer	Analyse DNS information revealed by a zone transfer	200
2021-05-09	Nmap: Ep.1 Basic Scanning	Demonstrate basic network scanning techniques	200
2021-05-08	CVE-2019-17387 (Aviatrix VPN Client Privilege Escalation)	Exploit CVE-2019-17387 to escalate privileges	400

Activity Report Page 4 of 9

Date	Lab	Description	Points Earned
2021-05-08	CVE-2019-0708 (BlueKeep - Exploitation)	Exploit BlueKeep	200
2021-05-07	Windows File Permissions	Analyse Windows file permissions	100
2021-05-07	Moving Around	Demonstrate navigation of files and directories	100
2021-05-07	Mal Wars	Demonstrate critical thinking	200
2021-05-07	Tactics Persistence	Recognise the techniques within the Execution tactic of the MITRE ATT&CK framework	40
2021-05-06	Snort Rules: Ep.2 DNS	Create Snort rules for DNS events	300
2021-05-06	Windows Forensics	Investigate and analyse operating systems using common forensic techniques	300
2021-05-06	Snort Rules: Ep.3 HTTP	Demonstrate usage of Snort rules	300
2021-05-06	Timestomp	Autopsy usage	300
2021-05-05	Msfvenom	Use msfvenom to create a payload	300
2021-05-05	Windows: DLL Hijacking	Exploit the DLL search order to escalate Windows privileges	600
2021-05-05	IR: Ep.3 Compromised Host	Investigate host-based compromise and IOCs	400
2021-05-04	Tracking a LOLBins Campaign: Acquisition	Identify infected hosts based on live traffic analysis	300
2021-05-04	Msfconsole: Using the Database	Apply Metasploit's database and project management features	100
2021-05-04	Msfconsole: Exploit	Practise using Metasploit's exploit modules to attack services	200

Activity Report Page 5 of 9

Date	Lab	Description	Points Earned
2021-05-04	Msfconsole: Auxiliaries	Use Metasploit auxiliary modules for scanning	100
2021-05-03	Immersive Bank: Ep. 2 Gaining Access	Apply critical thinking to gain access to the computer	100
2021-05-03	Symmetric vs Asymmetric Key Encryption	Apply symmetric key encryption and decryption techniques	100
2021-05-03	Snort Rules: Ep.1	Demonstrate proficiency in basic Snort rules	200
2021-05-03	Immersive Bank: Ep.1 Open Source and Credentials	Employ Open Source Intelligence to uncover the CEO's password	200
2021-05-03	Command Line Introduction	Identify relevant basic Linux commands	100
2021-04-30	Wireshark: Stream/Object Extraction	Analyse network packet captures	200
2021-04-30	Intro to Wireshark	Analyse network packet captures	100
2021-04-30	tcpdump	Analyse network packet captures	200
2021-04-30	Splunk: Event Analysis 2	Demonstrate and develop event log analysis techniques	200
2021-04-30	Splunk: Event Analysis	Demonstrate and develop basic event log analysis techniques	200
2021-04-30	Packet Capture Basics	Analyse network packet captures	100
2021-04-30	Wireshark Display Filters: An Introduction	Analyse network packet captures	100
2021-04-29	Unrestricted File Upload	Practise exploiting file-upload vulnerabilities in web applications	200
2021-04-29	Mimikatz & Chrome Passwords	Use post-exploitation techniques	200

Date	Lab	Description	Points Earned
2021-04-29	Domain Name System	Explain the roles of different name servers and the process of making a DNS request	100
2021-04-29	Cross-Site Request Forgery	Demonstrate the ability to bypass user input validation	200
2021-04-29	Password Hashes II	Understand the benefits of salting passwords	100
2021-04-29	APT34: PoisonFrog	Analyse the PoisonFrog malware	200
2021-04-29	Transport Protocols	Explain the core concepts of the the most common transport protocols	200
2021-04-29	APT34: Glimpse	Demonstrate an ability to identify Indicators of Compromise in malware with command line tools	200
2021-04-29	Hydra: Brute Force	Perform password brute forcing of multiple protocols using hydra	200
2021-04-28	Command History	Be able to identify the risk of passing credentials with the command line	100
2021-04-28	Data Compressed	Practise detecting data compressed prior to exfiltration	300
2021-04-28	CVE-2019-0708 (BlueKeep: Snort Rule)	Apply principles of how security teams may update systems in preparation for known threats	100
2021-04-28	Exfiltration Over Alternative Protocol	Practise identifying instances where data has been exfiltrated	100
2021-04-28	SQL Injection: UNION	Employ advanced SQL injection techniques	300
2021-04-28	Clipboard Data Theft	Analyse techniques used by adversaries to steal clipboard data	100
2021-04-28	CVE-2019-1388 (Windows Priv Esc UAC Bypass)	Bypass User Account Controls	200
2021-04-28	MongoDB: An Introduction	A basic understanding of NoSQL Databases	100

Activity Report Page 7 of 9

Date	Lab	Description	Points Earned
2021-04-28	Parsing PST	Investigate email client files	200
2021-04-28	Cross-Site Scripting (XSS) Stored	Be familiar with stored XSS attacks and how they arise	300
2021-04-28	Port Identification	Match common ports to services	100
2021-04-28	Port Bingo - Easy Mode	Demonstration of critical thinking	200
2021-04-28	Cross-Site Scripting (XSS) Reflected	Perform reflected XSS attacks against a website	200
2021-04-28	Tactics Defence Evasion	Exposure to techniques contained in the Execution tactic	20
2021-04-27	Hashing SHA-1	Apply the SHA1 hashing algorithm to strings	100
2021-04-27	Hashing MD5	Apply the MD5 hashing algorithm to strings	100
2021-04-27	Intrusion Detection Systems	Describe intrusion detection and prevention principles	20
2021-04-26	Server Identification	Identify default honeypot configurations	200
2021-04-26	IR: Ep.1 Suspicious Email	Investigate and gain information from suspected malicious documents	200
2021-04-26	Supply Chain Hardware Tampering	Practise interacting with a Baseboard Management Controller	100
2021-04-26	Introduction to Threat Hunting	Exposure to threat hunting principles	40
2021-04-26	The Incident Response Process	Identify the details of each stage of the incident response process	40
2021-04-26	sqlmap	Practise applying sqlmap to a database	200

Activity Report Page 8 of 9

Date	Lab	Description	Points Earned
2021-04-26	Introduction to Incident Response	Identify incident response principles	40
2021-04-26	Cyber Kill Chain	Familiarisation with the kill chain	10
2021-04-26	Python Coding Introduction	Read Python code	100
2021-04-26	Multi-Factor Authentication	Understand multi-factor authentication	10
2021-04-26	VirusTotal	Discover automated malware analysis tools and communities	100
2021-04-26	Analysing Sandbox Reports	Investigate malicious samples using sandbox reporting styles	100
2021-04-26	STIX	Locate Cyber Threat Information from within STIX objects	40
2021-04-26	Safe Browsing	Recognise how to protect yourself and your privacy as you browse the web	10
2021-04-26	Validating SIEM Results	Identify whether the activity or inactivity of a SIEM is accurate in any given scenario	40
2021-04-26	Defence in Depth	Discover the principles of defence systems	20
2020-08-12	Web Applications: Directory Traversal	Conduct directory traversal attacks against a web server	200
2020-08-12	Web Applications: Page Source Review	Analyse the web application source code to recognise technologies being used	200
2020-08-04	Netcat: Ep.1	Use Netcat for various tasks	100
2020-08-04	SQL: An Introduction	Gain an understanding of the SQL language and queries	100
2020-08-04	Internet Protocol V4	Explain the core concepts of IPv4 addressing	100

Activity Report Page 9 of 9

Date	Lab	Description	Points Earned
2020-08-04	Ports	Identify how ports are used in modern networks	40

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.