IMMERSIVELABS

Ivan Righi

Completed 577 labs earning 82000 points.

Activity Report

Date	Lab	Description	Points Earned
2022-11-20	ALPC File Delete Zero-Day	Use Windows exploit code	100
2022-11-19	Nobelium: Network Analysis	Be able to detect Nobelium network traffic	100
2022-11-19	Nobelium: NativeZone and VaporRage	Be able to identify key elements of a DLL loader	300
2022-11-19	Power Query Embedded Payloads	Identify misuse of the Microsoft Excel Power Query feature	200
2022-11-12	PowerPoint as a Malware Dropper	Investigate indicators of compromise from malicious Microsoft Office documents	100
2022-11-12	Find the RAT	Identify indicators of malicious download sites	300
2022-11-12	Linux: Config Error I	Exposure to Linux security misconfigurations	200
2022-11-12	CVE-2021-32648 (October CMS) Offensive	Identify vulnerable versions of October CMS	200
2022-11-10	Ducky PCAP Analysis	Analyse network packet captures	300
2022-11-10	PA Toolkit	Familiarisation with PA Toolkit.	200

Activity Report Page 2 of 39

Date	Lab	Description	Points Earned
2022-11-10	CVE-2021-38647 (OMIGOD) Defensive	Identify OMI traffic in a PCAP file	200
2022-11-09	Copy & Paste Compromise: Malicious Documents Analysis	Demonstrate ability to analyse malicious visual basic commands	300
2022-11-09	CVE-2021-3156 (Baron Samedit) Defensive	Know how to filter Auditd and Linux Auth logs in Splunk	300
2022-11-09	PoshC2: Ep.3 Obtaining Credentials	How to use third-party PoshC2 modules	400
2022-11-08	Zerologon Live Logs	Identify logs related to Zerologon	200
2022-11-08	CVE-2021-1675 (PrintNightmare) Defensive	Understand how to search event logs for CVE-2021-1675 exploit attempts	200
2022-11-08	SDelete Analysis	Identify malicious behaviour on a network analysing Splunk logs	100
2022-11-08	Ghidra: Ep.5 Improving Decompilation	Use Ghidra to gain a bigger picture of a binary	300
2022-11-07	Social Engineering	Describe different social engineering attack techniques and their impacts	10
2022-11-06	Web Server Logs: Ep.1 What are Web Server Logs?	Recall the different types of web server logs	20
2022-11-06	FIN7: Threat Hunting Ep.5 Credential Access & Discovery Logs	Understand the techniques used by the FIN7 threat group during an attack	200
2022-11-06	CVE-2022-22965 (Spring4Shell) Offensive	Recall the software and versions affected by the Spring4Shell vulnerability	200
2022-11-06	Web Server Logs: Ep.5 Searching Web Server Logs using Linux CLI	Use cat, grep, cut, sort, uniq, and wc commands to search for information in web server logs	200
2022-11-06	Splunk: Malicious Account Creation	Identify and recognise malicious events in system logs	200
2022-11-06	Web Server Logs: Ep.6 The Tomcat's Out Of The Bag	Identify evidence of a compromise in web server logs	300

Activity Report Page 3 of 39

Date	Lab	Description	Points Earned
2022-11-06	FIN7: Threat Hunting Ep.6 Persistence and Exfiltrating Logs	Observe and recognize the techniques used by the FIN7 threat group during an attack	200
2022-11-06	Web Server Logs: Ep.2 Log Formats	Describe the different types of web server log formats	20
2022-11-06	Web Server Logs: Ep.3 Access Logs	Recognize web server access logs	100
2022-11-06	Web Server Logs: Ep.4 Error Logs	Recognize web server error logs	100
2022-11-06	Hafnium - DearCry Ransomware	Safely observe DearCry ransomware	100
2022-11-05	CVE-2018-11776 (Apache Struts 2)	Identify CVE's	300
2022-11-05	CVE-2019-16759 (vBulletin RCE)	Analyse the vBulletin vulnerability	100
2022-11-05	FIN7: Threat Hunting Ep.8 Data Loss Identification	Understand how to analyze multi-stage payloads	400
2022-11-05	CVE-2020-11738 (Duplicator Plugin for WordPress)	Identify the source of a compromise in web logs	200
2022-11-03	tcpdump	Analyse network packet captures	200
2022-11-03	Dharma Ransomware: Investigation	Use Splunk to identify Dharma ransomware infections	300
2022-11-03	ngrep	Analyse network packet captures	200
2022-11-03	Threat Hunting: Windows Odd One Out	Identify out of sort processes and artefacts	200
2022-11-03	Packet Capture Basics	Analyse network packet captures	100
2022-11-03	Wireshark Display Filters: Combining Filters	Analyse network packet captures using multiple operators	200

Date	Lab	Description	Points Earned
2022-11-03	BPF Syntax	Analyse network packet captures	100
2022-11-02	CVE-2018-11759 (mod_jk)	Identify methods to bypass web authentication processes	100
2022-11-02	Packet Capture: Key Extraction	Analyse network packet captures	300
2022-11-02	Traffic Analysis: Malware	Recognise useful starting points for analysts when viewing network traffic	200
2022-11-02	Demonstrate Your Skills: Packet Analysis	Demonstrate the skills acquired through the beginner Wireshark labs	400
2022-11-02	Wireshark: Stream/Object Extraction	Analyse network packet captures	200
2022-11-02	Traffic Analysis: Device Information	Recognise useful starting points for analysts when viewing network traffic	200
2022-11-01	Splunk: Threat Hunting Ep.2 Rapid Collection and Exfiltration	Identify various tactics from the MITRE ATT&CK framework	200
2022-11-01	Splunk: Threat Hunting Ep.1 Initial Compromise	Identify various tactics from the MITRE ATT&CK framework	200
2022-11-01	Hafnium - China Chopper	Demonstrate ability to use an exploit chain to gain persistence on a web server	200
2022-10-30	Splunk Basics: Ep.4 Advanced Searching (SPL & Transforming)	Use Splunk's Search Processing Language (SPL) to search for and transform specific information	200
2022-10-30	Splunk Basics: Ep.5 Dashboards and Visualization	Recognize dashboards and how they can be used	100
2022-10-30	Demonstrate Your Skills: Splunk Basics	Recall the Splunk features and how to use them	200
2022-10-30	CVE-2019-17387 (Aviatrix VPN Client Privilege Escalation)	Exploit CVE-2019-17387 to escalate privileges	200
2022-10-30	Tshark	Analyse network packet captures	200

Activity Report Page 5 of 39

Date	Lab	Description	Points Earned
2022-10-30	CVE-2019-0636 (Arbitrary File Read Zero Day)	Demonstrate ability to run basic exploits and assist in triaging	200
2022-10-30	Splunk Basics: Ep.3 Search	Identify the key structure of a basic Splunk search	100
2022-10-30	CVE-2019-11043 (PHP FPM)	Understand the scope and capabilities of the exploit	200
2022-10-30	CVE-2019-5021 (Alpine Linux Docker Image Credential Vulnerability)	Demonstrate practical ability to privilege escalate	200
2022-10-30	Splunk Basics: Ep.2 Data Sources	Be able to recall the various data sources supported by Splunk	40
2022-10-30	Analysing Sandbox Reports	Investigate malicious samples using sandbox reporting styles	100
2022-10-30	Snort Rules: Ep.10 Lord EK	Demonstrate usage of Snort rules against a malware packet capture file	400
2022-10-30	Snort Rules: Ep.9 Exploit Kits	Use Snort rules against a malware packet capture file	300
2022-10-30	Spelevo Exploit Kit	Analyse exploit traffic in a PCAP	200
2022-10-29	Snort Rules: Ep.7 Lokibot Infection Traffic	Use Snort rules against a malware packet capture file	300
2022-10-29	Snort Rules: Ep.8 Emotet with Trickbot Infection Traffic	Demonstrate usage of Snort rules against a malware packet capture file	300
2022-10-29	Snort Rules: Ep.5 Fake Tech Support Popup	Demonstrate usage of Snort rules against a malware packet capture file	300
2022-10-29	Snort Rules: Ep.3 HTTP	Demonstrate usage of Snort rules	300
2022-10-29	CVE-2019-0708 (BlueKeep - Exploitation)	Exploit BlueKeep	200
2022-10-29	Snort Rules: Ep.4 SMTP	Create Snort rules for SMTP events	300

Activity Report Page 6 of 39

Date	Lab	Description	Points Earned
2022-10-29	CVE-2019-1388 (Windows Priv Esc UAC Bypass)	Bypass User Account Controls	200
2022-10-29	CVE-2019-16097 (Harbor Privilege Escalation)	Apply an understanding of web application vulnerabilities to gain illegitimate access	200
2022-10-29	Snort Rules: Ep.2 DNS	Create Snort rules for DNS events	300
2022-10-29	Snort Rules: Ep.6 Credential Stealer via FTP Traffic	Demonstrate usage of Snort rules against a malware packet capture file	300
2022-10-26	Hack Your First Web App: Ep.6 Taking the Lead	Recognize the stages you need to follow when attempting to find and exploit vulnerable systems	300
2022-10-26	Hack Your First Web App: Ep.4 Medium-Risk Vulnerabilities	Recall how a vulnerability could be categorized as medium-risk	100
2022-10-26	Hack Your First Web App: Ep.5 High-Risk Vulnerabilities	Recall how a vulnerability could be categorized as high risk	200
2022-10-24	Hack Your First Web App: Ep.2 Enumeration	Identify the different web content scanning tools available to a penetration tester	200
2022-10-24	Hack Your First Web App: Ep.3 Low-Risk Vulnerabilities	Recall how a vulnerability could be categorized as low-risk	200
2022-10-24	Hack Your First Web App: Ep.1 Ozone Energy	Recognize the necessary steps for finding and exploiting vulnerable systems	200
2022-10-22	TeslaCrypt	Understanding of ways that modern malware evades debugging	300
2022-10-22	Ransomware: Sodinokibi	Identify signs of Sodinokibi ransomware infections on a Windows host	200
2022-10-22	Ransomware: WannaCry	Identify signs of WannaCry ransomware infections on a Windows host	300
2022-10-22	Conti: Source Code Leak	To be able to review malware source code to identify indicators of compromise	200
2022-10-22	StalinLocker/StalinScreamer	Analyse the StalinLocker malware source code	200

Activity Report Page 7 of 39

Date	Lab	Description	Points Earned
2022-10-22	Ransomware: Zeppelin	Identify signs of Zeppelin ransomware infections on a Windows host	300
2022-10-22	MegaCortex Ransomware	Demonstrate ability to analyse ransomware using Splunk and Sysmon	200
2022-10-22	BlackRouter Ransomware	Experience with basic malware analysis	200
2022-10-09	Cyber Kill Chain: Installation	Identify installation attempts in security event logs	200
2022-10-09	Cyber Kill Chain: Command & Control	Identify C2 traffic in security event logs	200
2022-10-09	Cyber Kill Chain: Weaponisation	Identify the weaponised payload used for successful attack	200
2022-10-09	Ransomware: AstraLocker	Identify signs of AstraLocker ransomware infections on a Windows host	300
2022-10-09	Cyber Kill Chain: Delivery	Identify delivery attempts in security event logs	200
2022-10-09	Cyber Kill Chain: Reconnaissance	Identify recon attempts in security event logs	200
2022-10-09	Cyber Kill Chain: Actions on Objectives	Identify attacker actions in security event logs	200
2022-10-09	Ransomware: Ryuk	Identify signs of Ryuk ransomware infections on a Windows host	100
2022-10-08	04. Reconnaissance: User Enumeration SMTP	Recall how to enumerate users on an SMTP server	200
2022-10-08	07. Reconnaissance: DNS Service Zone Transfers	Analyze DNS information revealed by a zone transfer	200
2022-10-08	06. Reconnaissance: DNS Service Brute Forcing	Enumerate a target's subdomains	100
2022-10-03	SuperSonic: Ep.7 LIFTON	Analyse imagery for codes and hidden files	200

Date	Lab	Description	Points Earned
2022-10-02	SuperSonic: Ep.5 TOWER	Analyse a post-attack packet capture file	100
2022-10-02	SuperSonic: Ep.2 BEVERLEY	Demonstrate Open Source Intelligence techniques	100
2022-10-02	SuperSonic: Ep.4 INSOMNIA	Analyse data in various formats	100
2022-10-02	SuperSonic: Ep.3 FLYING FISH	Demonstrate cracking passwords using John the Ripper	100
2022-10-02	SuperSonic: Ep.6 TEMPLE	Analyse an attack to identify an attacker's actions	200
2022-10-02	SuperSonic: Ep.1 FORUM	Use OSINT analysis techniques to identify details of a cyberattack	100
2022-07-18	Ransomware: Conti	Identify signs of Conti ransomware infections on a Windows host	300
2022-05-20	Hermetic Wiper: Ghidra Analysis	Identify log-based IoCs from a malware binary	300
2022-02-21	64-Bit Linux Reversing: Ep.1	Demonstrate the use of disassembly tools to perform static analysis on binaries	200
2022-02-21	32-Bit Linux Reversing: Ep.2	Demonstrate the use of disassembly tools to perform static analysis on binaries	200
2022-02-21	LightNeuron DLL	Investigate a malicious Trojan using static-code analysis and debugging	1000
2022-02-21	32-Bit Linux Reversing: Ep.1	Demonstrate the use of disassembly tools to perform static analysis on binaries	200
2022-02-21	64-Bit Linux Reversing: Ep.2	Be able to use disassembly tools to perform static analysis on binaries	200
2022-02-21	32-Bit Windows Reversing: Ep.1	Be able to use disassembly tools to perform static analysis on Windows binaries	200
2022-02-20	Process Explorer	Use Process Explorer effectively	100

Date	Lab	Description	Points Earned
2022-02-07	Windows: DLL Hijacking	Exploit the DLL search order to escalate Windows privileges	600
2022-02-07	CVE-2018-16858 (LibreOffice Remote Code Execution)	Identify commands in python script	200
2022-01-18	Web Server Brute Force Authentication: Ep.2	Write brute-force scripts	400
2022-01-18	Web Server Brute Force Authentication: Ep.1	Gain an understanding of basic web application brute force techniques	300
2022-01-17	Volatility: Ep.4 Memory Analysis (ARCHIVED)	Further understanding of memory analysis techniques with Volatility	400
2022-01-17	Volatility: Ep.5 Memory Analysis (ARCHIVED)	Further understanding of memory analysis techniques with Volatility	400
2022-01-17	Volatility: Ep.6 VolUtility (ARCHIVED)	Practise analysing memory using the VolUtility interface	200
2022-01-12	Volatility: Ep.3 Memory Analysis (ARCHIVED)	Use the Volatility tool to analyse a memory sample	400
2022-01-11	Volatility: Ep.2 Memory Analysis (ARCHIVED)	Practise memory analysis techniques with Volatility	300
2022-01-08	Incident Response Theory: Ep.6 Post-Incident Activity	Identify the post-incident activity stage of the NIST incident response process	40
2022-01-08	The Grotto	General knowledge and some fun!	40
2022-01-08	CANBus: Ep. 16 Real-World CAN Architectures	Be aware of the complex CAN networks used in real-world architectures	40
2022-01-08	Introduction to Kubernetes	Recognise the fundamental concepts of Kubernetes	40
2022-01-08	CANBus: Ep. 6 In The Rear-View Mirror	Identify areas of the theoretical knowledge that you may need to revisit	100
2022-01-08	CANBus: Ep. 2 Systems	Demonstrate an understanding of how CANBus systems are constructed and what they are connected to	40

Activity Report Page 10 of 39

Date	Lab	Description	Points Earned
2022-01-08	What Is the Heap?	Gain a high level understanding of heap memory	40
2022-01-08	What Is the Stack?	Gain a high level understanding of stack memory	40
2022-01-08	CANBus: Ep. 10 Physical Connection	Know the conditions required to interact with a CANBus	40
2022-01-08	CANBus: Ep. 5 SocketCAN	Be able to describe SocketCAN and how it enables intuitive interaction with CAN devices	40
2022-01-08	Incident Response Theory: Ep.4 Detection and Analysis	Identify the detection and analysis stage of the NIST incident response process	40
2022-01-08	DoS Primer Volumetric	Explain the different types of volumetric attacks	40
2022-01-08	What is Vulnerability Management?	Recall what vulnerability management is and its importance in defensive cybersecurity	20
2022-01-08	DoS Primer Vulnerabilities	Learn different types of denial of service vulnerabilities	40
2022-01-08	Spiderfoot	Scan and analyse data using speciality OSINT tools	40
2022-01-08	DoS Primer Resource Exhaustion	Explain the different types of resource exhaustion attacks	40
2022-01-08	Hashing	Recognise the importance of hashing	20
2022-01-08	Vigenre Ciphers	Describe what a Vigenre cipher is	40
2022-01-08	The History of Encryption	Recall the different methods of encryption used throughout history	40
2022-01-08	Introduction to 32-Bit Architectures	Gain a high-level understanding of 32-bit architectures	40
2022-01-08	Introduction to 64-Bit Architectures	Gain a high level understanding of 64-bit architectures	40

Date	Lab	Description	Points Earned
2022-01-08	Symmetric Key Encryption	Recognise symmetric encryption	40
2022-01-08	Unicode	Recall how Unicode functions	40
2022-01-08	NIST 800-53: Ep.4 Assessment, Authorization, and Monitoring	Recognize assessment, authorization, and monitoring controls and their purpose	20
2022-01-08	Introduction to SAML	Be able to recognise the advantages of Single Sign-On	40
2022-01-08	CANBus: Ep. 4 Messaging	Demonstrate an understanding of the CANBus message concepts and formats	100
2022-01-08	CANBus: Ep. 1 An Introduction	Demonstrate an understanding of CANBus concepts	20
2022-01-08	Demonstrate Your Knowledge: Networking	Demonstrate your networking knowledge	40
2022-01-07	DarkSide Overview	Be able to demonstrate a basic understanding of the DarkSide ransomware group	40
2022-01-07	NIST 800-53: Ep.6 Contingency Planning	Recognize contingency planning controls and their purpose	20
2022-01-07	OSI Model	Identify the different layers of the OSI model	40
2022-01-07	What is Splunk?	Recall what the Splunk tool is	40
2022-01-07	Splunk Basics: Ep.1 The Splunk Interface	Recognize the different components of the Splunk Interface	40
2022-01-07	Apache Symbolic Links	Recognize enabled symbolic links	40
2022-01-07	TLS Fundamentals: Ep.5 X.509 Introduction	Identify an X.509 certificate and its main purpose	40
2022-01-07	GDPR Aware - Practice (ARCHIVED)	Demonstrate GDPR awareness through practice	20

Activity Report Page 12 of 39

Date	Lab	Description	Points Earned
2022-01-07	NSA Kubernetes Hardening: Ep3. Network Separation & Hardening	Recall the NSAs guidance for hardening Kubernetes networks	40
2022-01-07	NIS Directive	Recognize what the NIS Directive is and how it protects the countries in the EU	20
2022-01-07	Threat Hunt Theory Pyramid of Pain	Recognize the pyramid of pain	20
2022-01-07	Incident Response Theory: Ep.5 Containment, Eradication, and Recovery	Identify the containment, eradication, and recovery stage of the NIST incident response process	40
2022-01-07	US Federal Cyber Law	Identify the main US federal laws that can be used to convict cyber criminals	10
2022-01-07	Threat Hunt Theory Types of Hunt	Recognize the different types of threat hunt	10
2022-01-07	Threat Hunt Theory Threat Intelligence Lifecycle	Recognize the intelligence lifecycle	40
2022-01-07	Threat Hunt Theory The Threat Hunting Loop	Recognize the threat hunting loop	40
2022-01-07	Threat Hunt Theory Documenting the Hunt	Recognize the importance of documentation and automation in threat hunting	40
2022-01-07	Threat Hunt Theory Maturity Model	Recognise the threat hunting maturity model	40
2022-01-07	Police Raid	Demonstrate an understanding of devices that would be confiscated in an investigation	40
2022-01-07	Burglary and Hacking	Demonstrate an understanding of how hacking can be similar to burglary	40
2022-01-07	Ethical and Unethical Hacking	Demonstrate the ability to determine the ethical choices of hackers	40
2022-01-07	Threat Hunt Theory Data Quality	Recognize "good" data and why data quality is important in threat hunting	40
2022-01-07	Threat Hunt Theory Threat Hunting Model	Recognise the threat hunting process	40

Activity Report Page 13 of 39

Date	Lab	Description	Points Earned
2022-01-07	Bugbusters	Demonstrate an understanding of bug bounties and the companies that offer them	40
2022-01-07	Threat Hunt Theory Understanding the Results	Recognize the importance of threat hunting results	40
2022-01-07	Threat Hunt Theory Diamond Model	Recognize the diamond model	40
2022-01-07	Introduction to Penetration Testing Infrastructure	Demonstrate an understanding of infrastructure pen testing concepts	40
2022-01-07	UK Cyber Law	Demonstrate an understanding of illegalities and breaches of law	40
2022-01-07	Introduction to Penetration Testing Mobile Applications	Demonstrate an understanding of iOS/Android pen testing concepts	40
2022-01-07	Threat Hunt Theory Management, Growth, Metrics, and Assessment	Recognize how the MaGMA model is used in threat hunting	40
2022-01-07	Introduction to Penetration Testing Web Applications	Be able to demonstrate an understanding of web application hacking concepts	40
2022-01-07	How Is Risk Measured?	Be able to describe risk, impact, and probability	40
2022-01-07	Threat Hunt Theory Introduction	Understand the fundamental concepts of threat hunting	40
2022-01-07	Process Monitor	Demonstrate an ability to use Process Monitor	200
2022-01-07	Threat Hunt Theory Hypothesis Creation	Recognise how to create a threat hunting hypothesis	40
2022-01-07	Node.js: Missing Authentication Logs	Have an awareness of the impact and consequences of missing authentication logging	40
2022-01-07	LockerGoga Ransomware	Practise analysing ransomware memory samples	200
2022-01-07	Introduction to OpenID Connect (OIDC)	Identify the differences between OAuth and OpenID Connect	40

Date	Lab	Description	Points Earned
2022-01-07	Introduction to Networking: Ep.2 Types of Networks	Recall multiple types of networks and how they differ	20
2022-01-07	Message Integrity	Be able to define the term message integrity	40
2022-01-07	Public Key Infrastructure	Define what public key infrastructure is	40
2022-01-07	Stream Ciphers	Define stream ciphers and recall their fundamental characteristics	40
2022-01-07	Threat Hunt Theory Targeted Hunting Integrating Threat Intelligence	Recognize how the Targeted Hunting integrating Threat Intelligence methodology is used in threat hunting	40
2022-01-07	Digital Signatures	Recall the importance of digital signatures	40
2022-01-07	Container Hardening	Recognise the importance of container hardening	40
2022-01-07	Incident Response Theory: Ep.3 Preparation	Identify the details of the preparation stage of NIST's incident response process	40
2022-01-07	Block Ciphers	Define a block cipher	40
2022-01-07	What is Encoding?	Recall how encoding functions	40
2022-01-07	Public and Private Key Management	Recognize the importance of managing public and private keys	40
2022-01-07	Asymmetric Encryption	Define asymmetric encryption	40
2022-01-07	Zeek: Ep.1 Log Types and Formats	Recognize what Zeek logs are	40
2022-01-07	Updates and Patches	Identify the differences between updates and patches	10
2022-01-07	NIST 800-53: Ep.19 System and Information Integrity	Recognize system and information integrity controls and their purpose	40

Activity Report Page 15 of 39

Date	Lab	Description	Points Earned
2022-01-07	What is Cryptography?	Recall the fundamentals of cryptography	40
2022-01-07	One-Time Pad	Define what a one-time pad cipher is	40
2022-01-06	Server Side Includes	Demonstrate SSI injection vulnerabilities	200
2022-01-06	DrupeScan	Practise automated scanning techniques using speciality tools	200
2022-01-06	Demonstrate Your Skills: Scanning	Scan and identify information about two targets	200
2022-01-06	Understanding Wireshark: TLS handshake	Revise information on the TLS Handshake	100
2022-01-06	CVE-2019-14287 (Sudo Exploit)	Demonstrate practical ability to escalate privileges	200
2022-01-06	Wireshark Display Filters: Filters In Depth	Analyse network packet captures using complex operators	200
2022-01-06	Wireshark Statistics	Analyse network packet captures using Wireshark statistics	100
2022-01-05	Mal Wars	Demonstrate critical thinking	200
2022-01-05	Accounting and Audit	Identify audit and accounting methodology	200
2022-01-05	HTTP Status Codes Expert	Develop your knowledge of HTTP status codes	200
2022-01-05	Rails: Brakeman	Identify vulnerable code in Ruby on Rails applications using Brakeman	200
2022-01-05	Git History	Analyse a Git repository to obtain user credentials	200
2022-01-05	Scanner: Progpilot	Identify insecure code using the progpilot tool	300

Date	Lab	Description	Points Earned
2022-01-05	Unpacking .pkgs	Extract files and content from Mac OSX PKG files	200
2022-01-03	WastedLocker Ransomware: Unpacking	Setting breakpoints	400
2022-01-02	Ransomware Decryption	Diagnose an infected system using ransomware decryption tools	100
2022-01-02	WannaCry Analysis (ARCHIVED)	Identify indicators of compromise	300
2022-01-02	Cr1pT0r ARM Ransomware	Investigate ARM ransomware using static-code analysis	300
2022-01-02	Petya or NotPetya	Safe ransomware observation	200
2022-01-02	Snake Ransomware: Execution	Observe Snake ransomware safely	100
2022-01-02	WannaCry (ARCHIVED)	Safely observe WannaCry ransomware	100
2022-01-02	Ransomware: Dharma	Identify signs of Dharma ransomware infections on a Windows host	300
2022-01-02	Port Bingo - Advanced Mode	Demonstration of critical thinking	400
2022-01-02	WastedLocker Ransomware: Execution	Observe WastedLocker ransomware safely	100
2022-01-02	Ranzy Ransomware: Execution	Recognize the effects of Ranzy Locker and identify elements to report	100
2022-01-02	MegaCortex Ransomware	Demonstrate ability to analyse ransomware using Splunk and Sysmon	200
2022-01-02	WastedLocker Ransomware: Decryption	Use custom ransomware decrypter	100
2021-10-24	FIN7: Threat Hunting Ep.1 What is FIN7?	Recall the most commonly targeted sectors	40

Activity Report Page 17 of 39

Date	Lab	Description	Points Earned
2021-10-24	North Korean Indictment: Ep.2	Analysis of Event Logs	400
2021-10-24	CVE-2019-0708 (BlueKeep: Snort Rule)	Apply principles of how security teams may update systems in preparation for known threats	100
2021-10-24	DarkSide Ransomware: Execution	Gain an understanding of DarkSide ransomware by viewing it safely	100
2021-10-24	Iranian Threat Groups	Recognise Iranian threat groups and their tools at a high level	20
2021-10-20	CVE-2019-6340 (Drupal)	Use the CVE-2019-6340 exploit to compromise a Drupal site	200
2021-10-18	CVE-2018-10933 (libssh)	Understand the libssh vulnerability	200
2021-10-18	CVE-2014-0160 (Heartbleed)	Demonstrate the Heartbleed vulnerability	100
2021-10-18	CVE-2019-10149 (Exim Server RCE) - Defensive	Identify the latest threat through network communication analysis	200
2021-10-18	CVE-2014-6271 (Shellshock)	Demonstrate the Shellshock vulnerability	200
2021-10-17	CVE-2018-9206 (jQuery-File-Uploader)	Knowledge of the jQuery-File-Upload Vulnerability	200
2021-10-17	Immersive Labs Threat Hunting	Summarise the 'threat research' skill line	20
2021-10-17	CVE-2017-5754 (Meltdown)	Demonstrate the Meltdown vulnerability	100
2021-10-16	Hack Your First PC: Ep.6 Privilege Escalation	Recall potential ways of discovering system vulnerabilities	200
2021-10-16	Hack Your First PC: Ep.3 Scanning for Targets	Recall how to use Nmap to scan computer systems	200
2021-10-16	Hack Your First PC: Ep.5 Gaining Access	Identify potential access vectors on a remote system	200

Activity Report Page 18 of 39

Date	Lab	Description	Points Earned
2021-10-16	Hack Your First PC: Ep.2 Kali Linux	Navigate the Kali Desktop environment	200
2021-10-16	Hack Your First PC: Ep.4 Brute Force	Recall the difference between a brute-force attack and a dictionary attack	200
2021-10-13	Hack Your First PC: Ep.1 Ozone Energy	Recognise the stages you need to follow when attempting to find and exploit vulnerable systems	200
2021-10-12	Burp Suite Basics: Repeater	Practise using the Repeater tool	200
2021-10-12	Burp Suite Basics: HTTPS	Configure and use Burp Suite with Firefox	100
2021-10-12	Burp Suite Basics: Target	Apply scope controls within Burp Suite	200
2021-10-12	Burp Suite Basics: Introduction	Set up and use Burp Suite with Firefox	100
2021-10-11	Burp Suite Basics: Intruder	Use the Burp Suite Intruder tool effectively	200
2021-10-11	SQL Injection: UNION	Employ advanced SQL injection techniques	300
2021-10-11	Credential Stuffing	Identify differences between multiple brute-forcing techniques	300
2021-10-10	Linux CLI: Ep.1 Introduction to the Linux Command Line Interface	Recall Linux command line fundamentals	40
2021-10-10	WPScan	Identify vulnerabilities in WordPress	200
2021-10-10	PKI (Public Key Infrastructure) Practical	Understand the different parts of PKI and their roles	200
2021-10-10	PKI (Public Key Infrastructure)	Understand the different parts of PKI and their roles	40
2021-10-10	WPA Wordlist Crack	Identify weaknesses in Wi-Fi protocols	100

Activity Report Page 19 of 39

Date	Lab	Description	Points Earned
2021-10-10	Demonstrate Your Skills: Historic Encryption	Demonstrate your knowledge of historic encryption techniques	200
2021-10-10	Encryption Tools: CyberChef Recipes	Recall how CyberChef recipes work	40
2021-10-10	Encryption Tools: CyberChef	Recall how CyberChef functions	40
2021-10-10	The Enigma Machine	Recall how the Enigma machine works	200
2021-10-09	Ghidra: Ep.4 Scripting	Be able to perform analysis with the reverse-engineering tool Ghidra	300
2021-10-08	What is Cyber Threat Intelligence?	A basic understanding of Cyber Threat Intelligences core areas	40
2021-10-08	Domain Intel	Understand the information associated with domain names	40
2021-10-08	Ghidra: Ep.1 Projects and Getting Started	Demonstrate the extensive use of disassembly with the Ghidra reverse engineering tool	300
2021-10-08	Ghidra: Ep.2 Using The Three Heads	Use Ghidra to gain a bigger picture of a binary	200
2021-10-08	Vulnerability Identification	Identify the different ways to conduct vulnerability identification	40
2021-10-08	Ghidra: Ep.3 Aiding Analysis	Use Ghidra to gain a bigger picture of a binary	300
2021-10-07	Python: XML External Entities (XXE)	Know what an XXE vulnerability is and how it works	100
2021-10-05	Python: Debug Console	Have an awareness of the impact and consequences of leaving a debug console enabled	100
2021-10-05	Python: Vulnerable Library	Have an awareness of the impact and consequences of using a vulnerable library within an application	40
2021-10-05	Python: Missing Authentication Logs	Have an awareness of the impact and consequences of missing authentication logging	40

Date	Lab	Description	Points Earned
2021-10-05	Python: Code Comments	Have an awareness of the impact and consequences of leaving sensitive details in code comments	40
2021-10-05	Python: Stored XSS	Know what a stored cross-site scripting (XSS) vulnerability is and how it works	100
2021-10-05	Python: SQL Injection	Know what an SQL injection vulnerability is and how it works	100
2021-10-05	Python: Reflected XSS	Know what a reflected XSS vulnerability is and how it works	100
2021-10-05	Python: Default Error Pages	Have an awareness of the impact and consequences of enabling default error pages in an application	40
2021-10-03	Reverse Engineering with Radare2: Ep.1	Identify the process of how x86_64 assembly disassembles	300
2021-10-03	Decompiling Python	Investigate various Python compiled executables	200
2021-10-03	WikiWorm.exe	Investigate malware through static-code analysis	400
2021-10-02	HOPLIGHT Analysis	Demonstrate runtime analysis of the latest malicious threats	200
2021-10-02	Banking APK	Identify static code analysis techniques for Android	300
2021-10-02	JBiFrost Analysis	Investigate the configuration of malicious Java based remote access trojans	200
2021-10-02	ELECTRICFISH	Apply memory analysis techniques to investigate the execution of malware	300
2021-10-02	AutoIt Malware	Analyse malware created with AutoIt	300
2021-10-02	Snort Rules: Ep.1	Demonstrate proficiency in basic Snort rules	200
2021-10-02	Steganographic Malvertising	Understand how malicious actors exploit adverts	40

Date	Lab	Description	Points Earned
2021-10-02	Tracking a LOLBins Campaign: Infection	Analyse malicious network connections	200
2021-10-02	Marap	Investigate the initial functionality of malicious software	200
2021-09-30	Ransomware: Maze	Identify signs of Maze ransomware infections on a Windows host	200
2021-09-30	Ryuk Ransomware: Execution (ARCHIVED)	Identify signs of Ryuk ransomware infections on a Windows host	100
2021-09-30	Ransomware: Bad Rabbit	Identify signs of Bad Rabbit ransomware infections on a Windows host	300
2021-09-30	INetSim	Practise installing, configuring and using INetSim	200
2021-09-30	Ransomware: Annabelle	Identify signs of Annabelle ransomware infections on a Windows host	300
2021-03-02	Parellus Power: Ep.3	Identify the attack surface of a given website	300
2021-03-02	Parellus Power: Ep.2	Identify flaws in a web application	200
2021-03-02	Parellus Power: Ep.4	Demonstrate performing a brute force attack	300
2021-03-02	SMTP User Enumeration	Enumerate an SMTP server	200
2021-03-01	Protocols SMTP	Describe the structure of SMTP messages	200
2021-03-01	Basic Browser Forensics: Firefox	Practise basic browser forensic techniques	100
2021-03-01	Protocols ARP	Identify packet structure of ARP requests and responses	100
2021-03-01	Nmap: Ep.3 Scripting Engine	Demonstrate more complex network scanning techniques	300

Date	Lab	Description	Points Earned
2021-03-01	Bulk Extractor	Practise using the Bulk Extractor tool to retrieve sensitive information	200
2021-03-01	Basic Browser Forensics: Chrome	Practise and understand basic browser forensic techniques	300
2021-03-01	Protocols FTP	Explain the core concepts of the File Transfer Protocol	100
2021-03-01	National Software Reference Library (NSRL)	Discover the national software reference library	100
2021-03-01	BusinessLayer.dll Analysis	Identify and extract relevant IoCs from a .NET DLL	400
2021-03-01	Zone Transfer	Analyse DNS information revealed by a zone transfer	200
2021-03-01	Nessus: Ep.1 The Basics	Demonstrate ability to analyse Nessus results	100
2021-03-01	Protocols LDAP	Analyse the LDAP protocol in an enterprise context	100
2021-03-01	DNS Enumeration	Knowledge of DNS enumeration techniques	200
2021-03-01	Port Knocking	Practise port knocking to enable services	200
2021-03-01	Introduction to Encryption	Identify different types of encryption algorithms	100
2021-03-01	Anatova Ransomware	Exposure to the Anatova ransomware	200
2021-03-01	Denial of Service	Describe how denial of service attacks appear	200
2021-03-01	Steganography	Analyze images and extract information using ExifTool and Steghide	200
2021-03-01	Nikto/DIRB	Identify vulnerabilities in web servers	100

Date	Lab	Description	Points Earned
2021-03-01	Wired Equivalent Privacy (WEP) Cracking	Identify weaknesses in Wi-Fi protocols	200
2021-03-01	Protocols Modbus	Reference the core concepts of the Modbus protocol	300
2021-03-01	Protocols DNS	Describe the structure of DNS requests and responses	200
2021-02-28	Sudo Caching	Identify exploit attempts that abuse the sudo caching technique	100
2021-02-28	Linux CLI: Ep. 9 Stream Redirection	Know how data can be manipulated via the terminal	100
2021-02-28	Linux CLI: Ep. 7 Using wc	Be able to count elements in a file using the wc tool	200
2021-02-28	Malicious Documents: VBA Analysis	Use oletools to extract and analyse malicious VBA	300
2021-02-28	Regex: Ep.3	Use regular expressions in Linux command line	200
2021-02-28	Nmap: Ep.2 OS Detection	Identify system information using network scanning techniques	200
2021-02-28	Introduction to Hashing	Identify the characteristics of a good hashing algorithm	100
2021-02-28	Regex: Ep.1	Create and use regular expressions	40
2021-02-28	Identifying IoCs	Be able to recognise IoCs and know how to search for them	100
2021-02-28	Regex: Ep.2	Use regular expressions in Linux command line	100
2021-02-28	The Inside of an ELF File	Be able to identify components of an ELF file	40
2021-02-28	An Introduction to Linux Internals	Gain a high level understanding of the Linux operating system's inner workings	40

Date	Lab	Description	Points Earned
2021-02-28	Introduction to Windows Internals	Gain a high-level understanding of the Windows operating system's inner workings	40
2021-02-28	The Inside of a PE File	Gain a high level understanding of Portable Executables	40
2021-02-05	Command History	Be able to identify the risk of passing credentials with the command line	100
2021-02-05	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
2021-02-05	Linux CLI: Ep. 14 Using Screen	Be able to explain screen's CLI usage	100
2021-02-05	Linux CLI: Ep. 15 Generating File Hashes	Be able to recognise file hashes	100
2021-02-05	Linux CLI: Ep. 12 Using Find	Recognise how the find command works and the filters and arguments that go with it	200
2021-02-05	Linux CLI: Ep. 8 Manipulating Text	Know how to modify text within files using basic command line tools	200
2021-01-26	Introduction to Malicious Documents	Identify different file structures used to create malicious documents	200
2020-11-27	SimpleHTTPServer	Basic understanding of SimpleHTTPServer	100
2020-11-27	SNMP	Perform network interrogation via SNMP	300
2020-11-27	Elliptic Curve Cryptography	Explain the basics of elliptic curve cryptography	40
2020-11-27	BloodHound Active Directory Enumeration	Ability to analyse and search BloodHound's output to discover paths to sensitive accounts	200
2020-11-27	Responder.py Network Poisoning	Be able to use network poisoning attacks successfully	200
2020-11-27	Pass The Hash	Perform a Pass-the-Hash attack on a vulnerable server	200

Activity Report Page 25 of 39

Date	Lab	Description	Points Earned
2020-11-25	Netcat: Ep.1	Use Netcat for various tasks	100
2020-11-25	FTP - Anonymous Login	Identify and exploit FTP servers that have anonymous login enabled	100
2020-11-25	Netcat: Ep.2	Experience using Netcat to communicate to other hosts	200
2020-11-25	FTP Backdoor Exploit	Experience exploiting well know vulnerabilities	200
2020-11-11	Brute-force Authentication	Practice brute forcing passwords for multiple services	200
2020-11-10	MobSTSPY Spyware	Investigate various APK files to extract useful data	200
2020-11-10	Passwords: Hashes	Practical experience in attacking password encryption methods	100
2020-11-10	CVE-2019-7304 (snapd)	Analyse the Ubuntu Snap vulnerability	100
2020-11-10	Password Hashes II	Understand the benefits of salting passwords	100
2020-11-10	Hydra: Brute Force	Perform password brute forcing of multiple protocols using hydra	200
2020-11-10	Volatility: Ep.1 Memory Analysis (ARCHIVED)	Practise techniques to analyse memory with Volatility	300
2020-11-10	LaZagne	Demonstrate an ability to steal user credentials using an open-source tool	200
2020-11-10	Password Spraying	Execute a password spraying attack against a web application	200
2020-11-10	Health Insurance Portability and Accountability Act (HIPAA)	Describe the five titles that form the structure of HIPAA	20
2020-11-09	Email Relay Abuse	Exploit and remediate misconfigured open relays	600

Activity Report Page 26 of 39

Date	Lab	Description	Points Earned
2020-11-08	Ragnar Locker - VDI	Identify malware in a VDI	300
2020-11-08	Halloween 2020: Ep.4 Autopsy Report	Recover deleted files	200
2020-11-08	Shadow Brokers' Victim	Demonstration of critical thinking	300
2020-11-03	Autopsy: Ep.9 Timeline	Identify forensics evidence using Autopsy timeline view	200
2020-11-03	Autopsy: Ep.10 Case Report	Demonstrate report generation in Autopsy	100
2020-11-02	Autopsy: Ep.7 Applications and Mobile	Demonstrate how to investigate installed programs and apps using Autopsy	200
2020-11-02	Autopsy: Ep.8 Media and Audio Visual	Demonstrate the ability to search media within a case using Autopsy	100
2020-10-28	Autopsy: Ep.5 Web and Browsers	Demonstrate the ability to analyse browser information and search history in Autopsy	100
2020-10-28	Autopsy: Ep.4 Files and Volumes	Demonstrate how to navigate files, volumes, and the information they hold using Autopsy	100
2020-10-28	Autopsy: Ep.3 Tags, Comments, and Reports	Demonstrate how to tag, comment, and generate reports in Autopsy	40
2020-10-28	Autopsy: Ep.2 Cases and Data	Demonstrate cases, data ingest modules, and correlation engines in Autopsy	40
2020-10-28	Autopsy: Ep.6 Email and Messages	Demonstrate how to recover emails with Autopsy	200
2020-10-24	Autopsy: Ep.1 Getting Started	Demonstrate the ability to navigate and identify components of Autopsy	100
2020-09-24	DirBuster: Ep.1	Use DirBuster	200
2020-09-21	Msfvenom	Use msfvenom to create a payload	300

Activity Report Page 27 of 39

Date	Lab	Description	Points Earned
2020-09-21	Scanner: Exakat	Identify insecure code using the Exakat tool	100
2020-09-20	Cached and Archived Websites	Interpret and analyse information collected from web archives	20
2020-09-20	Meterpreter	Experience navigating the basic functionality of Meterpreter payload	200
2020-09-20	Introduction to Computer Memory and Architecture	Gain a high level understanding of how memory works in a computer system	40
2020-09-20	Meterpreter Modules	Apply knowledge of Meterpreter's post-exploitation modules	200
2020-09-20	Online anonymity	Describe how to increase your online anonymity	40
2020-07-27	Linux CLI: Ep. 11 Using SSH and SCP	Recall what the SSH protocol is	100
2020-07-01	Port Bingo - Easy Mode	Demonstration of critical thinking	100
2020-07-01	Port Bingo - Intermediate Mode	Demonstration of critical thinking	300
2020-07-01	Basic x86 Assembly (ARCHIVED)	Analyse basic assembly concepts	200
2020-07-01	The Bombe Machine	Recognize how the Bombe machine works	200
2020-07-01	CVSS Calculator	Calculate CVSS scores for given vulnerabilities	300
2019-12-27	Merry Christmas 2019	Feel festive!	300
2019-08-31	Cyber Essentials	Identify the most common attacks outlined by the Cyber Essentials scheme	20
2019-08-31	Qualitative Risk Measurement	Summarize what qualitative risk is	20

Date	Lab	Description	Points Earned
2019-08-31	Payment Card Industry Data Security Standard (PCI-DSS)	Recall the different PCI-DSS control objectives	40
2019-08-31	How to Mitigate Risk	Explain how risk management can help mitigate risk	20
2019-08-31	CIA Triad	Identify how cyber attacks impact the confidentiality, integrity and availability of a system	20
2019-08-31	Inherent and Residual Risk (ARCHIVED)	Explain the difference between inherent and residual risk	20
2019-08-31	Investigator Operations Security (OPSEC)	Source online information relevant to an investigation	40
2019-08-31	Port Identification	Match common ports to services	100
2019-08-31	Web Applications: Page Source Review	Analyse the web application source code to recognise technologies being used	200
2019-08-31	STIX	Locate Cyber Threat Information from within STIX objects	40
2019-08-31	Intro to Malware Static Analysis	Demonstrate and understanding of basic malware concepts	40
2019-08-31	SQL Injection: An Introduction	A basic understanding of SQL injection attacks	200
2019-08-31	Information Technology Health Check (ITHC)	Recognize why an information technology health check is carried out	20
2019-08-31	ISO 27001	Describe the ISO 27001 frameworks and how the controls are structured	20
2019-08-31	Open Source Intelligence (OSINT): Deleted Tweet	Analyse information using open source intelligence techniques	40
2019-08-31	PowerShell: Getting Started	Practise using the PowerShell cmdlets	100
2019-08-31	GDPR Aware (ARCHIVED)	Explain the key details and impact of GDPR	10

Date	Lab	Description	Points Earned
2019-08-31	Pride 2019 [ARCHIVED]	Apply Pride knowledge	40
2019-08-31	Parellus Power: Ep.1	Identify OSINT techniques	100
2019-08-31	NIST Cybersecurity Framework	List the three main components of the NIST Cybersecurity Framework	40
2019-08-31	Shodan.io	Gain an understanding of the Shodan.io search engine and how to run queries	20
2019-08-31	Punycode/Homograph.	Identify threat of URI encoding techniques	40
2019-08-31	Intro to Malware Dynamic Analysis	Knowledge of dynamic analysis	40
2019-08-31	Containers	Describe containers and their advantages and disadvantages	20
2019-08-31	Fuzzy Hashing	Discover various methods of analysing files	300
2019-08-31	The NCSC's 10 Steps to Cybersecurity	Describe each of the 10 Steps to Cybersecurity	20
2019-08-31	What Is Risk?	Define the core concepts that formulate risk	20
2019-08-31	Virtualisation	Describe the uses and advantages of virtualisation	10
2019-08-31	Rainbow Tables	Describe what a rainbow table is	40
2019-08-31	Hexadecimal.	Practise converting various types of data to hexadecimal	40
2019-08-31	DevSecOps Introduction	Recall the evolution of software delivery methodologies	10
2019-08-31	Infrastructure as Code (IaC)	Explain what IaC is and how it is deployed	20

Activity Report Page 30 of 39

Date	Lab	Description	Points Earned
2019-08-31	ACPO Guidelines	Discover digital forensics legalities and standards	40
2019-08-31	Immersive Bank: Ep.1 Open Source and Credentials	Employ Open Source Intelligence to uncover the CEO's password	200
2019-08-31	Security Automation	Describe the advantages of security automation and orchestration	20
2019-08-31	The Typex Machine	Recognize how a Typex machine works	200
2019-08-31	Introduction to Command & Control Frameworks	An introduction to Command and Control Frameworks	40
2019-08-31	Cyber Kill Chain: Exploitation	Identify exploitation attempts in security event logs	200
2019-08-31	Incident Response Theory: Ep.1 Introduction	Identify incident response principles	40
2019-08-31	Kubernetes - Multi-Container Pods	Recognise how Kubernetes resources are grouped and accessed	200
2019-08-30	Incident Response Theory: Ep.2 Process	Recognize the stages of the incident response process	40
2019-08-30	Basic ARM Assembly	Knowledge of ARM assembly	200
2019-08-30	Open Source Intelligence (OSINT): Boarding Pass	Describe what type of information a boarding pass barcode contains	100
2019-08-30	VirusTotal	Discover automated malware analysis tools and communities	100
2019-08-30	ELF Execution Structure	Discover the internals of an ELF executable structure	200
2019-08-30	Quantitative Risk Measurement	Calculate quantitative risk as a function of impact and probability	40
2019-08-30	Bad Package (ARCHIVED)	Identify the risk posed by out-of-date and malicious packages	200

Activity Report Page 31 of 39

Date	Lab	Description	Points Earned
2019-08-30	Asset Inventory and Valuation	Define the asset identification and valuation processes	20
2019-08-30	Validating SIEM Results	Identify whether a SIEM's actions are accurate in any given scenario	40
2019-08-30	RSA	Gain an understanding of RSA encryption/decryption methods	400
2019-08-30	Intrusion Detection Systems	Describe intrusion detection and prevention principles	20
2019-08-30	C Code Audit (ARCHIVED)	Practise reviewing C code applications	200
2019-08-30	Risk Management Crossword [DRAFTED]	Test your risk management knowledge by completing this crossword	40
2019-08-30	Volatility: Memory Acquisition on Windows	Demonstrate ability to perform memory acquisition on a Windows system	200
2019-08-29	Msfconsole: Exploit (Archived)	Practise using Metasploit's exploit modules to attack services	200
2019-08-29	Wireshark TLS	Analyse network packet captures	300
2019-08-29	Webmin 1.900 RCE	Experience using Metasploit to execute public exploits	200
2019-08-29	ZWASP Phishing Vulnerability in Office 365	Assemble URLs containing ZWSPs to obfuscate a malicious link	100
2019-08-29	Intro to Wireshark	Analyse network packet captures	100
2019-08-29	Binary Analysis: Ep.2 (ARCHIVED)	Identify binary analysis techniques	300
2019-08-29	Fake Font Phishing	Practical experience of the fake font obfuscation technique	200
2019-08-29	Darknets	Recognize how darknets operate on the internet	10

Date	Lab	Description	Points Earned
2019-08-29	Intro to Cyber Security	Identify cyber security basics	10
2019-08-28	Symmetric vs Asymmetric Key Encryption	Apply symmetric key encryption and decryption techniques	100
2019-08-28	Binary	Recall how binary functions	40
2019-08-28	Hashing MD5	Apply the MD5 hashing algorithm to strings	100
2019-08-28	Base64 Encoding.	Practise encoding and decoding using Base64	40
2019-08-28	Hashing SHA-1	Apply the SHA1 hashing algorithm to strings	100
2019-08-28	ASCII.	Perform ASCII to plaintext conversions	40
2019-08-28	Binary Analysis: Ep.1 (ARCHIVED)	Binary analysis techniques	300
2019-08-28	Wireshark Display Filters: An Introduction	Analyse network packet captures	100
2019-08-28	Protocols DHCPv6	Discuss the use of DHCP in computer networks	200
2019-08-27	OpenLDAP - Plaintext Passwords	Analyse an LDAP post exploitation technique	100
2019-08-27	Cookies	Recognize how cookies are used by individuals and organizations	20
2019-08-27	Secure Passwords	An understanding of what makes a password secure	10
2019-08-27	Reverse Image Search	Identify image sources	40
2019-08-27	Phishing Fraud	Identify spoofed domains used in phishing emails	100

Activity Report Page 33 of 39

Date	Lab	Description	Points Earned
2019-08-27	AWS Security Groups	Analyse security configuration	40
2019-08-27	Java A7 - Insufficient Attack Protection	Identify insecure coding practices	200
2019-08-27	ASD Essential Eight	Practise securing a system against Microsoft Office macros	100
2019-08-27	Bank Discovers Customer Credit Card Numbers Traded Online	Practise using IRC and interact with bots	100
2019-08-27	North Korean Indictment: Ep.1	Analyse malicious documents	300
2019-08-27	Data Leaks: Exposing Your Credentials	Recognise the extent of this real-life data leak	300
2019-08-27	Protocols DHCPv4	Discuss the use of DHCP in computer networks	200
2019-08-27	Identity Theft	Recognize the ways to prevent identity theft and the warning signs to look out for	10
2019-08-27	Platform as a Service (PaaS)	Be able to explain the advantages and disadvantages of Platform as a Service	20
2019-08-27	Firewalls	A basic understanding of what a firewall is and how it protects a network	10
2019-08-27	Immersive Care: Ep.2	Develop critical thinking	200
2019-08-27	HTTP Status Codes	Develop knowledge of HTTP status codes	100
2019-08-27	Backups	Recognize the importance of backups	10
2019-08-27	Keylogging	Recognize what keyloggers are	10
2019-08-27	Tools Leak Who are APT34?	Familiarise yourself with APT34	40

Activity Report Page 34 of 39

Date	Lab	Description	Points Earned
2019-08-27	Immersive Care: Ep.1	Develop critical thinking	40
2019-08-27	Multi-Factor Authentication	Recall how multi-factor authentication works	10
2019-08-27	Patching	An understanding of the update and patch management	10
2019-08-27	Cryptocurrency & Blockchain	An introduction to cryptocurrency and blockchain concepts	10
2019-08-27	Infrastructure as a Service (IaaS)	Describe the advantages and disadvantages of Infrastructure as a Service (IaaS).	20
2019-08-27	Mobile Security Tips	Identify potential threats to mobile phone security	10
2019-08-27	Software as a Service (SaaS)	Be able to describe the advantages and disadvantages of SaaS	20
2019-08-27	Safer Browsing	Recall how to protect yourself and your privacy as you browse the web	10
2019-08-27	Password Managers	An understanding of the issues presented with passwords and how password managers can help	10
2019-08-27	Ports	Identify how ports are used in modern networks	40
2019-08-27	UDP (User Datagram Protocol)	Summarise the User Datagram Protocol	200
2019-08-27	Transport Protocols	Explain the core concepts of the the most common transport protocols	40
2019-08-27	Linux CLI: Ep. 16 Combining Commands	Identify the different ways of combining commands on the terminal	200
2019-08-27	Terminology	An understanding of key cyber terms and phrases	10
2019-08-27	It's a Game of Pong	Develop critical thinking	100

Date	Lab	Description	Points Earned
2019-08-27	Browser Bookmark Discovery	Identify enumeration techniques by analysing browser bookmark files	100
2019-08-27	Malware	Recognize the most common forms of malware and how they can affect you	10
2019-08-27	Java A2 - Broken Authentication and Session Management	Identify insecure coding practices	200
2019-08-27	Shoulder Surfing	Recognize how shoulder surfing works and the various ways it can be employed	10
2019-08-27	Wi-fi Hotspots	Learning how to look for obscure wireless networks	10
2019-08-27	Cyber Kill Chain	Recognize the purpose of the cyber kill chain	10
2019-08-27	Tactics Privilege Escalation	Recognise the purpose of the MITRE ATT&CK Privilege Escalation tactic	20
2019-08-27	Introduction to Networking: Ep.6 Domain Name System	Summarize the fundamentals of the Domain Name System	40
2019-08-27	Internet Protocol V4	Explain the core concepts of IPv4 addressing	100
2019-08-27	Protocols - HTTP	Describe the structure of HTTP GET and POST requests	200
2019-08-27	Mimikatz & Chrome Passwords	Describe the Cookies and Login Data files that Chrome stores in %LOCALAPPDATA%	200
2019-08-27	Cloud Security Alliance Cloud Controls Matrix	Describe the CSA CCM framework	20
2019-08-25	Linux CLI: Ep. 10 Using Sudo	Identify different user privileges in Linux	100
2019-08-25	Introduction to MITRE ATT&CK	Be familiar with the MITRE ATT&CK framework and know how it is used	20
2019-08-25	Mshta	Recognise .hta malware and how it is executed under mshta.exe	200

Date	Lab	Description	Points Earned
2019-08-25	Windows Service Investigation	Identify and investigate anomalous Windows services	200
2019-08-25	Linux CLI: Ep. 13 Searching and Sorting	Know how to employ searching techniques to find patterns in files	100
2019-08-25	Linux CLI: Ep. 6 Editing Files	Be able to recall some common Linux command line text editors	100
2019-08-25	Tor	Describe how Tor works	40
2019-08-24	Real World Examples of IoT/Embedded Security Issues	Identify security best practice for IoT devices	10
2019-08-24	Scheduled Tasks	Demonstrate how to navigate information in Windows Scheduled Tasks	100
2019-08-24	Kate's Story: Ep.1	Apply cyberstalking techniques to find information on Kate	200
2019-08-24	Binwalk	Extract data from firmware images with Binwalk	200
2019-08-24	Windows Sysinternals	An overview of the Sysinternals suite	100
2019-08-24	What Is IoT?	Recognise IoT devices and their associated risks	10
2019-08-24	Why Hackers Hack	Recognize some of the methods used by hackers	10
2019-08-24	Who are the Hackers?	Recognize the different types of hackers	10
2019-08-24	IoT Best Practice	Describe how to securely deploy IoT devices	10
2019-08-24	IoT/Embedded Hardware Reverse Engineering	Identify security best practices for IoT devices	10
2019-08-24	IoT/Embedded Network Protocols and Security	Express the importance of using encryption to secure communications	10

Activity Report Page 37 of 39

Date	Lab	Description	Points Earned
2019-08-23	Windows Registry	Evaluate registry values	100
2019-08-23	Policies	Exposure to Windows policy mechanisms	100
2019-08-23	Introduction to Threat Hunting	Exposure to threat hunting principles	40
2019-08-23	Windows File Permissions	Analyse Windows file permissions	100
2019-08-23	Alternate Data Streams	Exposure to ADS and data hiding	200
2019-08-22	John the Ripper	Exposure to John the Ripper tool chain	100
2019-08-22	Introduction to Mimikatz	Use Mimikatz to extract passwords in Windows	200
2019-08-22	SearchSploit	Locate information on exploits using SearchSploit	200
2019-08-22	SSL Scanning	Identify weak cryptographic ciphers	200
2019-08-22	SSL Cipher Suite Enum [ARCHIVED]	Identify weak cryptographic ciphers	200
2019-08-21	Timestomp	Autopsy usage	300
2019-08-21	Defence in Depth	Discover the principles of defence systems	20
2019-08-20	DDE Analysis	Investigate different ways malware achieves execution after initial access	200
2019-08-20	MagicBytes	Conduct file header analysis in a forensic context	200
2019-08-20	Lab Types	Summarise the labs and base knowledge of how they work	10

Date	Lab	Description	Points Earned
2019-08-20	File Command	Using file to identify true information about unusual looking files	100
2019-08-20	Windows Artefacts	Perform a forensic analysis on a compromised system	400
2019-08-20	Linux CLI: Ep. 5 File Permissions	Be able to read Linux file permissions	100
2019-08-20	Ubuntu Image Analysis	Investigate and analyse operating systems using common forensic techniques	400
2019-08-20	File Systems	Review and interpret the function of the Master Boot Record	300
2019-08-20	Caesar Ciphers	Recall how Caesar cipher encoding works	40
2019-08-20	Banner Grabbing	Identify and enumerate common services	100
2019-08-20	Network Scanning	Operate various network scanning tools to identify open ports	100
2019-08-20	Server Identification	Identify default honeypot configurations	200
2019-08-19	Collection: Protect and Acquire	Recognize how to protect evidence during collection	40
2019-08-18	Nmap: Ep.1 Basic Scanning	Demonstrate basic network scanning techniques	200
2019-08-17	Linux CLI: Ep. 2 Getting Started with the Terminal	Be able to recall fundamental concepts of the Linux terminal	100
2019-08-17	EXIF	Knowledge in the various sorts of data that is stored in images	40
2019-08-17	What is cyber?	A basic understanding of cyber terminology	10
2019-08-17	Linux CLI: Ep. 3 Moving Around	Have the ability to navigate through directories on the command line	100

Activity Report Page 39 of 39

Date	Lab	Description	Points Earned
2019-08-17	Robots.txt	Identify website information leakage	40
2019-08-16	Windows Forensics	Investigate and analyse operating systems using common forensic techniques	300
2019-08-16	Ethics	An understanding of the various ethical issues in cyber security	10
2019-08-16	Default Credentials	Knowledge of default credentials	20
2019-08-16	Introduction to Forensics (ARCHIVED)	Exposure to forensics principals	40
2019-08-14	Using the Clipboard	Knowledge of how to use the clipboard within the Immersive Labs platform	20
2019-08-14	Welcome to Immersive Labs	A base competency in how to use the platform	10
2019-08-13	Splunk: Event Analysis 2 (ARCHIVED)	Demonstrate and develop event log analysis techniques	200
2019-08-13	Log Finder	Perform web log analysis	100
2019-08-13	SMTP Log Analysis	Carry out a log analysis in order to identify particular information	100
2019-08-12	Intro to Splunk (ARCHIVED)	Use Splunk effectively	100
2019-08-12	Splunk: Event Analysis (ARCHIVED)	Demonstrate and develop basic event log analysis techniques	200

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.