immersive

Thonangi Mohan Krishna Reddy

Completed 583 labs earning 52530 points.

Activity Report

Date	Lab	Description	Points Earned
2025-06-09	AWS Community Security Tooling: Prowler	Recall how to use Prowler to detect vulnerable configurations in AWS	100
2025-06-05	APT29 Threat Hunting with Splunk: Ep.6 – Credential Access	Identify various tactics from the MITRE ATT&CK framework	200
2025-06-05	APT29 Threat Hunting with Splunk: Ep.5 – Establish Persistence	Identify various tactics from the MITRE ATT&CK framework	200
2025-06-04	IoCs and TTPs: Ep.3 – Extracting and Identifying	Outline how to identify adversarial tactics, techniques, and procedures	40
2025-06-04	Fundamental AI Algorithms: SVMs Introduction	Identify the core concepts of support vector machines	200
2025-06-04	Fundamental AI Algorithms: Decision Trees Introduction	Identify the core concepts of decision trees	200
2025-06-04	Introduction to Detection Engineering: Ep.4 – Advanced Skills	Recognize the uses and limitations of EQL	300
2025-06-04	APT29 Threat Hunting with Splunk: Ep.4 – Clean-up & Reconnaissance	Identify various tactics from the MITRE ATT&CK framework	200
2025-06-04	APT29 Threat Hunting with Splunk: Ep.3 – Deploy Stealth Toolkit	Identify various tactics from the MITRE ATT&CK framework	200
2025-06-04	Mimikatz and Chrome Passwords	Recall the cookies and login data files that Chrome stores in %LOCALAPPDATA%	200

Date	Lab	Description	Points Earned
2025-06-04	Introduction to Mimikatz	Describe how to extract passwords in Windows using Mimikatz	200
2025-06-04	John the Ripper	Exposure to John the Ripper tool chain	100
2025-06-01	Find the Flaw: Python – Injection	Recognize injection vulnerabilities in Python code	20
2025-06-01	Threat Research: Sliver C2 – Memory Forensics	Identify Sliver activity in memory	400
2025-06-01	Volatility Memory Analysis: Ep.7 – File Systems	Enumerate the Windows Master File Table	100
2025-06-01	Reconnaissance: WHOIS Service – Basics	Demonstrate an understanding of the WHOIS service by answering the questions	40
2025-06-01	Secure Testing: Path Traversal	Identify potential path traversal vulnerabilities in web applications, adding to your suite of QA tests	40
2025-06-01	Windows Sysinternals: Strings	Use the strings tool on a Windows system	200
2025-06-01	Tracking a LOLBins Campaign: Analysis	Demonstrate the ability to analyze malware infecting a machine	200
2025-06-01	Malware Analysis: Tracking a LOLBins Campaign – Acquisition	Identify infected hosts based on live traffic analysis	300
2025-05-31	GhostEngine: Analysis	Describe the unique execution flow used in the GhostEngine campaign	200
2025-05-31	Brute Ratel C4 (BRc4): Yara Detection	Create a Yara rule that detects Brute Ratel C4 malware	100
2025-05-31	Threat Hunting: Zerologon Live Logs	Identify logs related to Zerologon	200
2025-05-31	Persistence: Windows Logon	Recognize how attackers gain persistence on a system by abusing the Windows Registry	200
2025-05-31	OpenVAS	Identify vulnerabilities in network infrastructure with an open-source network scanner	200

Activity Report Page 3 of 40

Date	Lab	Description	Points Earned
2025-05-31	Threat Hunting: Fuzzy Hashing	Discover various methods of analysing files	300
2025-05-30	Offensive PowerShell: Ep.1 – What is Offensive PowerShell?	Explain the benefits of using PowerShell to perform offensive actions	40
2025-05-30	Brute Ratel: Extracting Indicators of Compromise	Demonstrate an ability to extract and decode configuration blocks from Brute Ratel Badgers	300
2025-05-30	Malware Analysis: Tracking a LOLBins Campaign – Infection	Analyze malicious network connections	200
2025-05-29	Volatility Memory Analysis: Ep.5 – Networking	Identify open connections in a memory capture	100
2025-05-29	Volatility Memory Analysis: Ep.2 – Processes and DLLs	Recognize system processes in memory	100
2025-05-29	Volatility Memory Analysis: Ep.1 – Getting Started	Demonstrate basic usage of the Volatility tool	100
2025-05-27	Systems Manager: Patching and Compliance	Recognize SSM patch manager terminology	200
2025-05-27	APT29 Threat Hunting with Splunk: Ep.2 – Rapid Collection and Exfiltration	Identify various tactics from the MITRE ATT&CK framework	200
2025-05-27	APT29 Threat Hunting with Splunk: Ep.1 – Initial Compromise	Identify various tactics from the MITRE ATT&CK framework	200
2025-05-26	Introduction to Python Scripting: Ep.7 – Demonstrate Your Skills	Demonstrate how to configure environments to write and execute Python scripts	300
2025-05-26	Introduction to Python Scripting: Ep.6 – Log Analysis and Anomaly Detection with Python	Be able to describe log analysis concepts	300
2025-05-26	Introduction to Python Scripting: Ep.5 – Web Scraping	Explain the fundamentals of web scraping, including its purpose and ethical considerations	100
2025-05-26	Introduction to Python Scripting: Ep.4 – Building an IDS with Python	Explain what an IDS is, including its purpose and significance in cybersecurity	300
2025-05-26	Introduction to Python Scripting: Ep.3 – Network Reconnaissance with Python	Describe networking concepts in Python	200

Activity Report Page 4 of 40

Date	Lab	Description	Points Earned
2025-05-26	Introduction to Python Scripting: Ep.2 – Network Basics with Python	Recall how servers manage incoming connections and how clients start requests on a network	200
2025-05-26	Incident Response: Suspicious Email – Part 1	Investigate and gain information from suspected malicious documents.	200
2025-05-22	Fundamental AI Algorithms: K-Means Beacon Detection	Recognize the potential applications of the k-means algorithm in cybersecurity	300
2025-05-22	SUNBURST: Identifying IoCs	Be able to recognize IoCs and know how to search for them	100
2025-05-22	Practical Malware Analysis: HOPLIGHT	Demonstrate runtime analysis of the latest malicious threats	200
2025-05-22	Snort Rules: Ep.1 – Introduction	Demonstrate proficiency in basic Snort rules	200
2025-05-20	Persistence: Windows Services	Identify and investigate anomalous Windows services	300
2025-05-18	Introduction to Python Scripting: Ep.1 – Setting up the Environment	Describe the basics of Python scripting and its applications in automation	100
2025-05-17	Introduction to Detection Engineering: Ep.3 – Parent Processes	Recognize the differences between ProcMon and Sysmon	200
2025-05-17	Introduction to Detection Engineering: Ep.2 – Foundational Concepts	Recognize applications of ProcMon process tree and filter features	200
2025-05-17	Open Source Intelligence (OSINT): Domain Intel	Understand the information associated with domain names	40
2025-05-14	Wizard Spider DFIR: Ep.3 – Risk Identification	Recognize the techniques used by Wizard Spider during an attack	200
2025-05-11	StrelaStealer Malware Campaign: Analysis	Outline the execution flow the threat actor uses to deploy their malware	300
2025-05-11	Fundamental AI Algorithms: K-Means Introduction	Identify the core concepts of the K-means algorithm	200
2025-05-11	Fundamental AI Algorithms: Introduction	Identify the core concepts of machine learning	40

Activity Report Page 5 of 40

Date	Lab	Description	Points Earned
2025-05-11	Investigating IAM Incidents in AWS: Detection and Analysis – Overly Permissive Policies	Identify overly permissive policies attached to IAM roles or users	200
2025-05-11	Investigating IAM Incidents in AWS: Detection and Analysis – Leaked Keys and Privilege Escalation	Recognize when AWS credentials have been compromised	200
2025-05-11	Introduction to Incident Response and Forensics in AWS: Post-incident Activity	Identify post-incident metrics for review	20
2025-05-10	Introduction to Detection Engineering: Ep.1 – Fundamentals	Recall how the Pyramid of Pain can be applied to defensive operations	40
2025-05-09	IoCs and TTPs: Ep.5 – Demonstrate Your Skills	Identify adversarial tactics, techniques, and procedures	100
2025-05-09	IoCs and TTPs: Ep.4 – Management	Describe how to manage IoCs and TTPs once they're obtained	40
2025-05-09	IoCs and TTPs: Ep.2 – What are TTPs?	Outline what tactics, techniques, and procedures are	40
2025-05-09	IoCs and TTPs: Ep.1 – What are IoCs?	Recall the aspects that make up an IoC	20
2025-05-09	AI for Business: Ep.4 – Using AI at Work	Identify how AI can be used in your day-to-day work	10
2025-05-09	AI for Business: Ep.3 – The Risks of AI	Define some of the risks associated with AI	10
2025-05-09	AI for Business: Ep.2 – The Benefits of AI	Define some of the benefits associated with the use of AI	10
2025-05-09	AI for Business: Ep.1 – What is AI?	Understand what AI is and what it can be used for	10
2025-05-09	Java: Broken Session Management	Know what a broken session management vulnerability is	200
2025-05-09	Java: SQL Injection	Know what an SQL injection vulnerability is and how it works	100
2025-05-09	Threat Hunting: Analyzing Sandbox Reports	Investigate malicious samples using sandbox reports	100

Activity Report Page 6 of 40

Date	Lab	Description	Points Earned
2025-05-09	Threat Hunting: VirusTotal	Demonstrate how to use malware analysis tools	100
2025-05-08	Microsoft Sentinel SOAR: Playbooks	Recall the key components and features of Microsoft Sentinel playbooks	200
2025-05-08	Investigating IAM Incidents in AWS: Containment and Eradication	Identify the steps required to contain a compromised IAM principal during an attack	100
2025-05-08	Introduction to Incident Response and Forensics in AWS: Detection	Know services and methods that can be used for detection	20
2025-05-08	Introduction to Incident Response and Forensics in AWS: Containment, Eradication, and Recovery	Recall AWS services available for incident containment, eradication, and recovery	20
2025-05-08	Introduction to Incident Response and Forensics in AWS: Analysis	Recall important log sources for analysis	20
2025-05-08	Interactive RegEx: Ep.9 — Demonstrate	Apply knowledge gained throughout the series to match specific data	200
2025-05-08	Incident Response in the Workplace	Recall the advantages of an incident response plan	10
2025-05-07	VPC & Network Security: Subnets, Route Tables, and Segmentation	Describe the use cases and functionality of public and private subnets	200
2025-05-07	Incident Response: Data Exfiltration	Practice identifying instances where data has been exfiltrated	100
2025-05-07	Qualitative Risk Measurement	Summarize what qualitative risk is	20
2025-05-07	Risk and Control Self Assessment (RCSA)	Describe the purpose of an RCSA within the wider risk management framework	20
2025-05-07	Vulnerability Identification	Identify the different ways to conduct vulnerability identification	40
2025-05-07	Risk: Asset Inventory and Valuation	Define the asset identification and valuation processes	20
2025-05-07	PHP: SQL Injection	Know what an SQL injection vulnerability is and how it works	100

Activity Report Page 7 of 40

Date	Lab	Description	Points Earned
2025-05-07	Immersive Care: Ep.4 – SQL Injection Mitigation	Be aware of the impact and consequences of an SQL injection attack	200
2025-05-07	Digital Forensics: File Systems	Review and interpret the function of the Master Boot Record	300
2025-05-07	How to Mitigate Risk	Explain how risk management can help mitigate risk	20
2025-05-06	Microsoft Sentinel Blue Team Ops: Incident Basics	Utilize Microsoft Sentinel for incident investigation and root cause analysis	200
2025-05-06	CVSS v4.0	Outline how CVSS v4 is used to score the severity of vulnerabilities	10
2025-05-06	Heap Exploitation: Ep.1 – Heap Overflow (Theory)	Identify which common C and C++ functions can be insecure	40
2025-05-06	Nmap: Ep.9 – Demonstrate Your Skills	Apply knowledge of Nmap to enumerate target systems	200
2025-05-06	Nmap: Ep.8 – Scan Output	Describe the different Nmap outputs available	100
2025-05-06	Mitre ATT&CK for ICS	Use MITRE ATT&CK to map ICS threats and attacks to a common framework	100
2025-05-06	Introduction to Metasploit: Ep.8 – Post-Exploitation	Recall how to select and launch post-exploitation modules against a target host	200
2025-05-06	CVSS Calculator	Calculate CVSS scores for given vulnerabilities	300
2025-05-06	Compliance: Payment Card Industry Data Security Standard (PCI-DSS)	Recall the different PCI-DSS control objectives	40
2025-05-06	Quantitative Risk Measurement	Calculate quantitative risk as a function of impact and probability	40
2025-05-05	Staying Safe Online: Phishing Emails (US)	Recognize the main characteristics of phishing emails	20
2025-05-05	Business Continuity 101: Ep.4 – Training and Exercising	Describe the different methods of training and exercising in business continuity	10

Activity Report Page 8 of 40

Date	Lab	Description	Points Earned
2025-05-05	Authentication: Ep.4 – Adding an Extra Layer of Security	Describe why adding more layers of authentication is important	10
2025-05-05	Interactive RegEx: Ep.8 — Flags	Recall the different flags that can be applied to the regex engine	100
2025-05-05	Interactive RegEx: Ep.7 — Groups	Recall how you previously used capture groups	200
2025-05-05	NCSC Cloud Security: Ep.10 – Secure User Management	Recognize the importance of secure user management as detailed by NCSC	20
2025-05-05	NCSC Cloud Security: Ep.5 – Governance Framework	Identify how governance fits in with implementation cloud solutions according to NCSC	20
2025-05-05	Introduction to 64-Bit Architectures	Gain a high level understanding of 64-bit architectures	40
2025-05-05	Introduction to 32-Bit Architectures	Gain a high-level understanding of 32-bit architectures	40
2025-05-05	Privileged Access	Recall what privileged access is and why it's an attractive target for attackers	10
2025-05-05	Container Hardening: Introduction to Containerization	Describe containers, their advantages, and disadvantages	20
2025-05-05	Scanning: DNS Zone Transfer	Analyze DNS information revealed by a zone transfer	200
2025-05-05	Scanning: Banner Grabbing	Identify and enumerate common services	100
2025-05-04	NIST Cybersecurity Framework	List the three main components of the NIST Cybersecurity Framework	40
2025-05-04	Three Lines of Defense	Describe the Three Lines of Defense model	10
2025-05-02	Nessus: Ep.5 – Demonstrate your Skills	Interact with Nessus using the web interface	200
2025-05-02	Nessus: Ep.4 – Scan Results	Demonstrate how to use Nessus to analyze exported scan results	100

Activity Report Page 9 of 40

Date	Lab	Description	Points Earned
2025-05-02	Interactive RegEx: Ep.6 — Quantifiers	Recall how to use logical operators in regex	200
2025-05-02	Nessus: Ep.3 – Authenticated Scanning	Demonstrate how to launch a Nessus scan from the basic network scan template	100
2025-05-02	Nessus: Ep.2 – Network Scanning	Demonstrate how to launch a Nessus scan from the Host Discovery template	100
2025-05-02	Nessus: Ep.1 – Introduction to Nessus	Describe typical uses of the Nessus Vulnerability Assessment tool	100
2025-05-02	How is Risk Measured?	Be able to describe risk, impact, and probability	40
2025-04-30	Inherent vs Residual Risk	Explain the difference between inherent and residual risk	20
2025-04-30	Introduction to Metasploit: Ep.7 – Meterpreter	Recognize common Meterpreter features	200
2025-04-30	Introduction to Metasploit: Ep.6 – Payloads	Recognize how to identify appropriate Metasploit payloads for a target system	100
2025-04-30	Introduction to Metasploit: Ep.5 – Exploits	Identify appropriate Metasploit exploit modules	100
2025-04-30	Introduction to Metasploit: Ep.4 – Enumeration	Recognize how enumeration modules can help gather information on a target	100
2025-04-30	Introduction to Metasploit: Ep.3 – Discovery	Recall how msfconsole modules can be used to scan and identify a target	100
2025-04-30	Introduction to Metasploit: Ep.2 – Modules	Demonstrate how to start msfconsole	100
2025-04-29	Introduction to Metasploit: Ep.1 – What is Metasploit?	Recall the fundamentals of Metasploit	20
2025-04-29	Interactive RegEx: Ep.5 — Logical Metacharacters	Recall how to match patterns with character sets	100
2025-04-29	Interactive RegEx: Ep.4 — Character Sets	Recall how to match with the metacharacters dot, backslash, and line anchors	40

Activity Report Page 10 of 40

Date	Lab	Description	Points Earned
2025-04-29	Interactive RegEx: Ep.3 — Simple Matching	Recall how to match alphanumeric characters in a string	40
2025-04-29	Interactive RegEx: Ep.2 — The RegEx Interface	Be familiar with the interface that will be used throughout the series	20
2025-04-28	ISO 27001: Ep.2 – The Domains of ISO 27001	Define risk-based security approaches	20
2025-04-28	ISO 27001: Ep.3 – What About You?	Compare how ISO 27001 applies across various areas of an organization	20
2025-04-28	Crisis Management 101: Ep.5 – Crisis Communications	Recognize principles of good crisis communication	10
2025-04-28	Crisis Management 101: Ep.4 – Cyber Crisis Decision Making	Recognize different types of decisions you'll experience in a crisis situation	10
2025-04-28	Crisis Management 101: Ep.3 – Tame and Wicked Problems	Identify key characteristics of tame and wicked problems	10
2025-04-28	Crisis Management 101: Ep.2 – Situational Awareness	Identify the steps involved in situational awareness	10
2025-04-28	Crisis Management 101: Ep.1 – Incidents Vs Crises	Describe the difference between cyber incidents and crises	10
2025-04-28	Interactive RegEx: Ep.1 — An Introduction to RegEx	Recall what regular expressions are and the task they perform	10
2025-04-28	ISO 27001: Ep.1 – What Is ISO 27001?	Identify why the ISO 27001 standard is used	20
2025-04-28	What Is Risk?	Define the core concepts that formulate risk	20
2025-04-28	Scanning: Network Scanning	Operate various network scanning tools to identify open ports	100
2025-04-25	SQLi Basics: Basic SQL Injection	Construct SQL injection payloads	100
2025-04-25	Scanning: Nikto and DIRB	Identify vulnerabilities in web servers	100

Activity Report Page 11 of 40

Date	Lab	Description	Points Earned
2025-04-24	Nmap: Ep.7 – Scan Optimization	Describe Nmap’s scan optimization techniques and options	100
2025-04-24	Scanning: Demonstrate Your Skills	Scan and identify information about two targets	200
2025-04-24	Scanning: DrupeScan	Practice automated scanning techniques using speciality tools	200
2025-04-24	Nmap: Ep.2 – Using Nmap	Recall how to run Nmap	100
2025-04-24	Scanning: WPScan	Identify vulnerabilities in WordPress	200
2025-04-24	Scanning: Port Knocking	Practice port knocking to enable services	200
2025-04-24	Scanning: DNS Enumeration	Knowledge of DNS enumeration techniques	200
2025-04-23	Nmap: Ep.4 – Port Scanning	Describe what port scanning is	100
2025-04-23	Nmap: Ep.3 – Host Discovery	Describe Nmap’s default host discovery options	100
2025-04-23	Nmap: Ep.6 – Scripting	Describe what NSE is	200
2025-04-23	Nmap: Ep.5 – OS and Version Detection	Describe what enumeration scans Nmap has available	100
2025-04-22	Nmap: Ep.1 – Intro to Nmap	Explain what nmap is	40
2025-04-09	APT29 Threat Hunting with Elasticsearch: Ep.10 – Persistence Execution	Identify various tactics from the MITRE ATT&CK framework	200
2025-04-09	APT29 Threat Hunting with Elasticsearch: Ep.9 – Image Steganography	Identify various tactics from the MITRE ATT&CK framework	400
2025-04-09	APT29 Threat Hunting with Elasticsearch: Ep.2 – Rapid Collection and Exfiltration	Identify various tactics from the MITRE ATT&CK framework	200

Activity Report Page 12 of 40

Date	Lab	Description	Points Earned
2025-03-24	AI Challenges: Beat the Bot	Identify potential risks, impacts, and examples of LLM prompt injection attacks	400
2025-03-24	Omnipotent Productions: Ep.2 – FTP Server Hardening	Use the CLI to reconfigure an FTP server	200
2025-03-22	Practical Malware Analysis: Static Analysis	Describe what static analysis is and how it's used for malware analysis	200
2025-03-22	Practical Malware Analysis: Dynamic Analysis	Describe what dynamic analysis is and how it's used for malware analysis	200
2025-03-21	Practical Malware Analysis: Splunk Log Analysis	Identify signs of Maze ransomware infections on a Windows host	100
2025-03-21	Omnipotent Productions: Ep.5 – Forensics	Demonstrate how to recover deleted files with Autopsy	200
2025-03-21	Practical Malware Analysis: Steganographic Malvertising	Describe how malicious actors exploit adverts	40
2025-03-20	Omnipotent Productions: Ep.6 – Theory	Understand how to identify and mitigate risk	10
2025-03-20	Autopsy: Ep.4 – Files and Volumes	Demonstrate how to navigate files, volumes, and the information they hold using Autopsy	100
2025-03-17	Omnipotent Productions: Ep.3 – OSINT	Employ open-source intelligence to investigate the hacking group and its related people	100
2025-03-17	Omnipotent Productions: Ep.4 – Packet Analysis	Be capable of analyzing malicious network traffic	40
2025-03-17	Autopsy: Ep.2 – Cases and Data	Demonstrate how to navigate around an Autopsy case	100
2025-03-17	Autopsy: Ep.1 – Getting Started	Demonstrate how to navigate and identify components of Autopsy	100
2025-03-15	Microsoft Azure Basics: Demonstrate Your Skills	Control networking access to Azure resources	300
2025-03-15	Omnipotent Productions: Ep.1 – Log Analysis	Examine Wireshark's analytics features	40

Activity Report Page 13 of 40

Date	Lab	Description	Points Earned
2025-03-14	Microsoft Sentinel Deployment & Log Ingestion: Demonstrate Your Skills	Demonstrate how to deploy a minimal Microsoft Sentinel deployment	300
2025-03-06	Threat Hunt Theory: Demonstrate Your Skills	Understand the fundamental concepts of threat hunting	100
2025-03-06	AI: Prompt Injection Attacks	Explain the concept of Large Language Models (LLMs) and prompts within the context of artificial intelligence	200
2025-03-06	AI: Demonstrate Your Skills	Demonstrate the skills acquired through the AI Fundamentals collection	100
2025-03-06	AI: TensorFlow for Machine Learning	Define machine learning	40
2025-03-06	AI: Introduction to AI	Define the key components of AI	20
2025-03-06	AI: Image Classification	Outline what image recognition is and how it's used in artificial intelligence	40
2025-03-06	AI: Generative AI Models	Understand the basic concepts and types of generative AI	20
2025-03-06	AI: Emerging Threats	Define some of the threats associated with AI	20
2025-03-06	AI: Data Ethics and Responsible Use	Define some of the risks associated with data that is collected and processed by AI	20
2025-03-06	AI: Artificial Intelligence for Incident Responders	Outline the risks and opportunities of AI in incident response, including what threats it poses	20
2025-03-06	Operational Technology Fundamentals: Common Threats and Vulnerabilities	Identify common threats and vulnerabilities relating to operational technology	40
2025-03-06	Operational Technology Fundamentals: SCADA and DCS	Differentiate between SCADA and DCS systems, including their primary purposes and architectures	40
2025-03-06	Operational Technology Fundamentals: Purdue Model for ICS – Enterprise Zone	Identify what devices sit in the Enterprise Zone of the Purdue Model	10
2025-03-06	Operational Technology Fundamentals: Purdue Model for ICS – Control Zone	Be able to identify what devices sit in the Control Zone of the Purdue Model	10

Activity Report Page 14 of 40

Date	Lab	Description	Points Earned
2025-03-06	Operational Technology Fundamentals: IT, OT, ICS, and Embedded Devices	Describe the differences in technologies used for IT and OT	20
2025-03-06	Threat Hunt Theory: Emulating Adversaries	Recognize how emulating adversaries is beneficial in threat hunting	40
2025-03-06	Threat Hunt Theory: Targeted Hunting Integrating Threat Intelligence	Recognize how the Targeted Hunting integrating Threat Intelligence methodology is used in threat hunting	40
2025-03-06	Threat Hunt Theory: Management, Growth, Metrics, and Assessment	Recognize how the MaGMA model is used in threat hunting	40
2025-03-06	Threat Hunt Theory: Understanding the Results	Recognize the importance of threat hunting results	40
2025-03-06	Threat Hunt Theory: Data Quality	Recognize "good" data and why data quality is important in threat hunting	40
2025-03-06	Threat Hunt Theory: Documenting the Hunt	Recognize the importance of documentation and automation in threat hunting	40
2025-03-06	Threat Hunt Theory: Pyramid of Pain	Recognize the pyramid of pain	20
2025-03-06	Threat Hunt Theory: Types of Hunt	Recognize the different types of threat hunt	10
2025-03-06	Threat Hunt Theory: Threat Intelligence Lifecycle	Recognize the intelligence lifecycle	40
2025-03-06	Threat Hunt Theory: The Threat Hunting Loop	Recognize the threat hunting loop	40
2025-03-06	Threat Hunt Theory: Maturity Model	Recognize the threat hunting maturity model	40
2025-03-06	Threat Hunt Theory: Threat Hunting Model	Recognize the threat hunting process	40
2025-03-06	Threat Hunt Theory: Diamond Model	Recognize the diamond model	40
2025-03-06	Threat Hunt Theory: Mapping Adversaries	Understand how to map adversaries to the MITRE ATT&CK® framework	40

Activity Report Page 15 of 40

Date	Lab	Description	Points Earned
2025-03-06	Cyber for Executives: Ep.4 – Common Threats	Identify the most common cyber threats facing organizations	10
2025-02-27	Microsoft Azure Basics: Virtual Machines	Manage virtual machines (VMs) in Azure	100
2025-02-27	Microsoft Azure Basics: Logic Apps	Build Azure Logic Apps	200
2025-02-27	Windows Forensics Artifacts: Demonstrate Your Skills	Recognize the different artifacts you can find in Windows	100
2025-02-27	Windows Forensics Artifacts: Link Files (LNK)	Recall what the Shell Link Binary File Format is	20
2025-02-27	Windows Forensics Artifacts: Master File Table	Recall what the Master File Table is	40
2025-02-27	Threat Hunt Theory: Introduction	Understand the fundamental concepts of threat hunting	40
2025-02-27	Threat Hunt Theory: Hypothesis Creation	Recognize how to create a threat hunting hypothesis	40
2025-02-27	Windows Sysinternals: ProcDump	Use ProcDump to debug programs and dump process memory	200
2025-02-27	Windows Sysinternals: Process Explorer	Use Process Explorer effectively	100
2025-02-27	Windows Sysinternals: Process Monitor	Demonstrate an ability to use Process Monitor	200
2025-02-26	Microsoft Azure Basics: Virtual Networks	Recall virtual networking concepts in Azure	100
2025-02-26	Microsoft Azure Basics: Fundamental Concepts	Know the differences between tenants, subscriptions, and resource groups	10
2025-02-26	Microsoft Azure Basics: Storage Accounts	Recall how to create and modify storage accounts	100
2025-02-26	Microsoft Azure Basics: Navigating the Web Portal	Access the Azure web portal	100

Activity Report Page 16 of 40

Date	Lab	Description	Points Earned
2025-02-26	Windows Sysinternals: Sysmon	Analyze and investigate system logs	100
2025-02-25	Microsoft Sentinel Deployment & Log Ingestion: Ingesting Virtual Machine Logs	Demonstrate how to configure a data connector in Microsoft Sentinel	200
2025-02-25	Microsoft Sentinel Deployment & Log Ingestion: Ingesting Platform Logs via Diagnostic Settings	Demonstrate how to configure a data connector in Microsoft Sentinel	200
2025-02-24	Microsoft Sentinel Deployment & Log Ingestion: Initial Setup	Recall the deployment process for Microsoft Sentinel	200
2025-02-24	Introduction to Microsoft Sentinel	Recall Microsoft Sentinel's features	100
2025-02-23	Elastic Data Ingest: Ep.7 – Elastic Agent	Analyze data collected with the Elastic Agent by using Kibana	100
2025-02-23	DDOS Analysis: Demonstrate Your Skills	Understand the mechanics of a DDoS attack and how they appear in logs	200
2025-02-23	DDOS Analysis: UDP Flood	Understand the mechanics of UDP Flood DDoS attacks	100
2025-02-23	DDOS Analysis: SYN Flood	Understand the mechanics of SYN Flood DDoS attacks	100
2025-02-23	DDOS Analysis: Ping of Death	Understand the mechanics of a Ping of Death attack	100
2025-02-23	DDOS Analysis: What are DDoS Attacks?	Understand the basic principles of DDoS attacks	20
2025-02-23	Windows Forensics Artifacts: Recycle Bin	Recall what Recycle Bin artifacts are	40
2025-02-23	Windows Forensics Artifacts: ShellBags	Recall what ShellBags are and where to find this artifact	40
2025-02-23	Windows Forensics Artifacts: UserAssist	Recall the location, use, and format of the UserAssist Key	40
2025-02-23	Vulnerability Management: Ep.6 — Demonstrate Your Knowledge	Recognize the fundamentals of vulnerability management	40

Activity Report Page 17 of 40

Date	Lab	Description	Points Earned
2025-02-23	Windows Forensics Artifacts: Event Logs	Recall what event logs are and where to find this artifact	40
2025-02-23	Windows Forensics Artifacts: Prefetch Files	Recall what prefetch files are and where to find them	40
2025-02-23	Windows Forensics Artifacts: AppCompatCache	Recall what the AppCompactCache is and where to find it	40
2025-02-23	Windows Forensics Artifacts: Amcache	Recall what the Amcache is and where to find this artifact	40
2025-02-23	What is Vulnerability Management?	Recall what vulnerability management is and its importance in defensive cybersecurity	20
2025-02-23	Vulnerability Management: Ep.3 — Evaluate and Prioritize	Explain the prioritizing step within the Vulnerability Management process	20
2025-02-23	Vulnerability Management: Ep.4 — Remediate	Identify what it means to remediate discovered and known vulnerabilities	20
2025-02-23	Vulnerability Management: Ep.5 — Report	Understand the process of reporting vulnerabilities	20
2025-02-23	Vulnerability Management: Ep.2 — Monitoring and Identifying	Identify the process for monitoring and identifying vulnerabilities	20
2025-02-23	Vulnerability Management: Ep.1 – Asset and System Inventory	Identify the hardware and software assets	20
2025-02-23	Elastic Data Ingest: Demonstrate Your Skills	Demonstrate log analysis techniques using the Elastic Stack to investigate suspicious activity	300
2025-02-23	Elastic Data Ingest: Ep.6 – Winlogbeat	Demonstrate log analysis techniques using Winlogbeat and the Elastic Stack	200
2025-02-23	Elastic Data Ingest: Ep.3 – Heartbeat	Demonstrate log analysis techniques using Heartbeat and the Elastic Stack	200
2025-02-23	Elastic Data Ingest: Ep.5 – Packetbeat	Demonstrate log analysis techniques using Packetbeat and the Elastic Stack	200
2025-02-23	Elastic Data Ingest: Ep.4 – Metricbeat	Demonstrate log analysis techniques using Metricbeat and the Elastic Stack	200

Date	Lab	Description	Points Earned
2025-02-23	Elastic Data Ingest: Ep.2 – Filebeat	Demonstrate log analysis techniques using Filebeat and the Elastic Stack	200
2025-02-23	Windows Sysinternals: Introduction to Sysinternals	Identify products in the Sysinternals Suite	40
2025-02-16	Malicious Document Analysis: Introduction to Malicious Documents	Identify different file structures used to create malicious documents	200
2025-02-15	Modern Encryption: Demonstrate Your Skills	Demonstrate the skills acquired through the beginner Encryption labs	300
2025-02-15	Wireshark: Metrics and Statistics	Analyze network packet captures using Wireshark statistics	100
2025-02-15	Wireshark: Display Filters – Combining Filters	Analyze network packet captures using multiple operators	200
2025-02-15	Wireshark: Demonstrate Your Skills	Identify relevant network traffic using Wireshark	300
2025-02-15	Wireshark: Using Tshark	Analyze network packet captures	200
2025-02-15	Wireshark: Stream/Object Extraction	Analyze network packet captures	200
2025-02-15	Wireshark: TLS Traffic	Analyze network packet captures	300
2025-02-14	PKI (Public Key Infrastructure) Practical	Understand the different parts of PKI and their roles	200
2025-02-14	Introduction to Hashing	Identify the characteristics of a good hashing algorithm	100
2025-02-14	Wireshark: Display Filters – Diving In	Analyze network packet captures using complex operators	200
2025-02-14	Rainbow Tables	Describe what a rainbow table is	40
2025-02-14	Steganography	Analyze images and extract information using ExifTool and Steghide	200

Activity Report Page 19 of 40

Date	Lab	Description	Points Earned
2025-02-14	Wireshark: Display Filters – Introduction to Filters	Analyze network packet captures	100
2025-02-14	Wireshark: Introduction to Wireshark	Analyze network packet captures	100
2025-02-14	Modern Encryption: MD5 Hashing	Recall what MD5 hashing is and how it works	40
2025-02-14	Modern Encryption: SHA-1 Hashes	Recall what SHA-1 hashing is and how it works	40
2025-02-14	WPA Wordlist Crack	Identify weaknesses in Wi-Fi protocols	100
2025-02-14	Wired Equivalent Privacy (WEP) Cracking	Identify weaknesses in Wi-Fi protocols	200
2025-02-13	Active Directory Basics: Demonstrate Your Skills	Interact with and modify objects in a directory database	300
2025-02-13	Active Directory Basics: Ep.8 – Managing Workstations	Explain how to find configuration details	100
2025-02-13	Active Directory Basics: Ep.7 – Replication	Describe what Active Directory replication is	40
2025-02-13	Active Directory Basics: Ep.6 – Group Policy Management	Explain what a Group Policy Object is	100
2025-02-13	Active Directory Basics: Ep.5 – NTLM vs Kerberos	Explain why authentication protocols are essential in an Active Directory environment	40
2025-02-13	Active Directory Basics: Ep.4 – Adding a Machine	Explain how to configure network settings for a DNS server	100
2025-02-13	Active Directory Basics: Ep.3 – Objects	Describe what AD objects are	100
2025-02-13	Active Directory Basics: Ep.2 – Console	Describe what the Active Directory Users and Computers console is	100
2025-02-13	PKI (Public Key Infrastructure)	Understand the different parts of PKI and their roles	40

Activity Report Page 20 of 40

Date	Lab	Description	Points Earned
2025-02-13	Introduction to Encryption	Identify different types of encryption algorithms	100
2025-02-13	Elliptic Curve Cryptography	Explain the basics of elliptic curve cryptography	100
2025-02-13	Modern Encryption: RSA	Describe what RSA encryption is, how it works, and why it's crucial in digital security	40
2025-02-13	Symmetric vs Asymmetric Key Encryption	Apply symmetric key encryption and decryption techniques	100
2025-02-12	Active Directory Basics: Ep.1 – What is Active Directory?	Describe what Active Directory is	40
2025-02-12	Cyber Kill Chain: Ep.10 – Demonstrate Your Knowledge	Recognize the fundamentals of the Cyber Kill Chain model	40
2025-02-12	Cyber Kill Chain: Ep.9 – Adversary Simulation	Recall the fundamentals of adversary simulation	100
2025-02-12	Cyber Kill Chain: Ep.8 – Actions on Objectives Phase	Recall the fundamentals of the 'actions on objectives' phase	40
2025-02-12	Cyber Kill Chain: Ep.7 – What is the Command and Control (C2) Phase?	Recall the fundamentals of the command and control phase	40
2025-02-12	Cyber Kill Chain: Ep.6 – Installation/Persistence Phase	Recall the fundamentals of the installation phase	40
2025-02-12	Cyber Kill Chain: Ep.5 – Exploitation Phase	Be able to recall the fundamentals of the exploitation phase	40
2025-02-12	Cyber Kill Chain: Ep.4 – Delivery Phase	Recall the fundamentals of the delivery phase	40
2025-02-12	Cyber Kill Chain: Ep.3 – Weaponization Phase	Recall the fundamentals of the weaponization phase	40
2025-02-12	Cyber Kill Chain: Ep.2 – Reconnaissance Phase	Recall the fundamentals of the reconnaissance phase	20
2025-02-12	Elastic Data Ingest: Ep.1 – Auditbeat	Demonstrate log analysis techniques using Auditbeat and the Elastic Stack	200

Date	Lab	Description	Points Earned
2025-02-11	Cyber Kill Chain: Demonstrate Your Skills	Describe all the stages from the Lockheed Martin Cyber Kill Chain®	400
2025-02-11	Introduction to Velociraptor: Ep.8 – Demonstrate Your Skills	Demonstrate how to use the Velociraptor tool	200
2025-02-10	Introduction to Velociraptor: Ep.4 – Searching	Recognize how and when to use Velociraptor	100
2025-02-10	Introduction to Velociraptor: Ep.3 – VQL	Identify VQL structure using Velociraptor	100
2025-02-10	Introduction to Velociraptor: Ep.2 – Getting Started	Identify event log structure using Velociraptor	100
2025-02-10	Introduction to Velociraptor: Ep.7 – Client Monitoring	Recognize how and when to use Velociraptor	100
2025-02-10	Introduction to Velociraptor: Ep.6 – Triage	Recognize how and when to use the Velociraptor tool	100
2025-02-10	Introduction to Velociraptor: Ep.5 – NTFS	Recognize how and when to use Velociraptor	100
2025-02-08	Elastic Playground: Web Logs	Demonstrate log analysis techniques using the Elastic Stack	100
2025-02-08	Elastic Playground: Flight Data	Demonstrate log analysis techniques using the Elastic Stack	100
2025-02-08	Elastic Playground: eCommerce Data	Demonstrate log analysis techniques using the Elastic Stack	100
2025-02-07	CTI First Principles: Ep.5 – Threat Intelligence Sources	Outline what sources are available for gathering and enriching threat intelligence	40
2025-02-07	Human Factors in Cybersecurity: Demonstrate Your Understanding	Demonstrate your understanding of human factors in cybersecurity	40
2025-02-07	Human Factors in Cybersecurity: Security Awareness and Behavior Change	Explain the role of security awareness and behavior change	20
2025-02-07	Human Factors in Cybersecurity: Security Culture	Explain the importance of security culture and how the principles apply to your organization	20

Activity Report Page 22 of 40

Date	Lab	Description	Points Earned
2025-02-07	Web Log Analysis: Ep.6 — The Tomcat's Out Of The Bag	Identify evidence of a compromise in web server logs	300
2025-02-07	Splunk Basics: Demonstrate Your Skills	Recall the Splunk features and how to use them	200
2025-02-07	Cyber Kill Chain: Actions on Objectives	Recognize the fundamentals of the actions on objectives phase in the Cyber Kill Chain	200
2025-02-07	Cyber Kill Chain: Command and Control	Recognize the fundamentals of the command and control phase in the Cyber Kill Chain	200
2025-02-07	Cyber Kill Chain: Installation	Recognize the fundamentals of the installation phase in the Cyber Kill Chain	200
2025-02-07	Cyber Kill Chain: Exploitation	Recognize the fundamentals of the exploitation phase in the Cyber Kill Chain	200
2025-02-07	Cyber Kill Chain: Delivery	Recognize the fundamentals of the delivery phase in the Cyber Kill Chain	200
2025-02-07	Cyber Kill Chain: Reconnaissance	Recognize the fundamentals of the reconnaissance phase	200
2025-02-07	Cyber Kill Chain: Weaponization	Recognize the fundamentals of the weaponization phase in the Cyber Kill Chain	200
2025-02-07	Elastic Playground: Accounting and Audit	Identify audit and accounting methodology	200
2025-02-06	CTI First Principles: Ep.7 – Demonstrate Your Knowledge	Describe cyber threat intelligence fundamentals	100
2025-02-06	CTI First Principles: Ep.3 – Models and Methodologies	Compare different models of CTI and their applications	40
2025-02-06	CTI First Principles: Ep.6 – Decomposition and Visualization	Recognize techniques for breaking down complex information	40
2025-02-06	CTI First Principles: Ep.4 – Threat Actors and Attribution	Outline what threat actors are and how they are attributed to incidents	100
2025-02-06	CTI First Principles: Ep.2 – Lifecycles	Outline the components of the intelligence cycle	20

Activity Report Page 23 of 40

Date	Lab	Description	Points Earned
2025-02-06	CTI First Principles: Ep.1 – What is Cyber Threat Intelligence?	Outline the relationship between data, information, and intelligence	10
2025-02-06	Human Factors in Cybersecurity: Usable Security	Explain usability and the causes of unusable security	20
2025-02-06	Introduction to Incident Response: Ep.7 – Demonstrate Your Knowledge	Recall the key steps of the NIST incident response process	40
2025-02-06	Introduction to Incident Response: Ep.6 – Post-Incident Activity	Recall the post-incident activity stage of the NIST incident response process	40
2025-02-06	Introduction to Incident Response: Ep.4 – Detection and Analysis	Discuss the detection and analysis stage of the NIST incident response process	40
2025-02-06	Introduction to Incident Response: Ep.5 – Containment, Eradication, and Recovery	Recall and discuss the containment, eradication, and recovery stage of the NIST incident response process	40
2025-02-06	Validating SIEM Results	Identify whether a SIEM's actions are accurate in any given scenario	40
2025-02-05	Human Factors in Cybersecurity: How People Make Security Mistakes	Explain the Swiss Cheese Model applied to cybersecurity	20
2025-02-05	Human Factors in Cybersecurity: People Are The Strongest Link	Explain what human factors are and why they're important	20
2025-02-05	Introduction to Velociraptor: Ep.1 – What is Velociraptor?	Recall what Velociraptor is and how it's used to aid DFIR investigations	20
2025-02-05	Introduction to Incident Response: Ep.3 – Preparation	Discuss the details of the preparation stage of NIST's incident response process	40
2025-02-05	Introduction to Incident Response: Ep.2 – Process	Recognize and outline the stages of the incident response process	40
2025-02-05	Introduction to Incident Response: Ep.1 – Introduction	Describe what an incident is	40
2025-02-04	Introduction To Elastic: Ep.9 – ES|QL	Understand the importance of using Elastic in investigating security incidents	300
2025-02-04	Security Reporting and Responsiveness: Ep.4 – Demonstrate Your Knowledge	Demonstrate an understanding of why security reporting and responsiveness is important	10

Activity Report Page 24 of 40

Date	Lab	Description	Points Earned
2025-02-04	Security Reporting and Responsiveness: Ep.3 – Responding Appropriately	Identify when you need to respond to potential incidents	10
2025-02-04	Security Reporting and Responsiveness: Ep.2 – Case Studies	Describe the potential impact of not reporting potential security incidents and concerns	10
2025-02-04	Security Reporting and Responsiveness: Ep.1 – Reporting Incidents and Concerns	Recognize the importance of reporting potential security incidents and concerns	10
2025-02-04	Introduction To Elastic: Ep.8 – Act	Demonstrate how to create a custom query rule in Elastic	200
2025-02-04	Introduction to Digital Forensics: Demonstrate Your Skills	Recognize the fundamentals of digital forensics	100
2025-02-04	OWASP 2021: Ep.11 – Demonstrate Your Knowledge	Recall different vulnerability categories in the 2021 OWASP Top 10	40
2025-02-04	OWASP API Security Top 10	Identify each of the vulnerabilities in OWASP's top 10 APIs	20
2025-02-04	Digital Forensics Process: Reporting	Recall the different ways of presenting evidence	20
2025-02-04	Digital Forensics Tools	Recognize the most common digital forensics tools	20
2025-02-04	Digital Forensics Processes and Techniques	Recall digital forensics processes	40
2025-02-04	Digital Evidence	Define what digital evidence is	20
2025-02-04	What is Digital Forensics?	Define digital forensics	20
2025-02-04	DevSecOps: Release	Recall the security considerations of the DevSecOps release stage	20
2025-02-04	DevSecOps: Operate	Recall the security considerations of the DevSecOps operation stage	20
2025-02-04	DevSecOps: Test	Recall the security considerations of the DevSecOps testing stage	20

Activity Report Page 25 of 40

Date	Lab	Description	Points Earned
2025-02-04	DevSecOps: Monitor	Recall the security considerations of the DevSecOps monitoring phase	20
2025-02-04	DevSecOps: Deploy	Recall the security considerations of the DevSecOps deployment stage	20
2025-02-04	OWASP 2021: Ep.10 – Server-Side Request Forgery	Summarize server-side request forgery and its relationship to the OWASP Top 10	20
2025-02-04	OWASP 2021: Ep.9 – Security Logging and Monitoring Failures	Summarize security logging and monitoring failures and their relationship to the OWASP Top 10	20
2025-02-04	OWASP 2021: Ep.8 – Software and Data Integrity Failures	Summarize software and data integrity failures and their relationship to the OWASP Top 10	20
2025-02-04	OWASP 2021: Ep.7 – Identification and Authentication Failures	Summarize identification and authentication failures and their relationship to the OWASP Top 10	20
2025-02-04	OWASP 2021: Ep.6 – Vulnerable and Outdated Components	Summarize the security misconfiguration and its relationship to the OWASP Top 10	20
2025-02-04	OWASP 2021: Ep.5 – Security Misconfiguration	Summarize security misconfiguration and its relationship to the OWASP Top 10	20
2025-02-04	OWASP 2021: Ep.4 – Insecure Design	Summarize insecure design and its relationship to the OWASP Top 10 list	20
2025-02-04	OWASP 2021: Ep.3 – Injection	Advance your understanding of the OWASP Top 10	20
2025-02-04	OWASP 2021: Ep.2 – Cryptographic Failures	Summarize cryptographic failures and their relationship to the OWASP Top 10	20
2025-02-04	OWASP 2021: Ep.1 – Broken Access Control	Summarize broken access control and its relationship to the OWASP Top 10	20
2025-02-04	Introduction to the OWASP Top 10	Summarize the objectives of the OWASP	10
2025-02-04	NIST 800-144 Cloud Security: Ep.9 – Incident Response	Explain concerns and recommendations for incident response in cloud environments as detailed by NIST	10
2025-02-04	NIST 800-144 Cloud Security: Ep.7 – Data Protection	Recall NIST 800-144 concerns and recommendations for data protection in cloud environments	10

Activity Report Page 26 of 40

Date	Lab	Description	Points Earned
2025-02-04	NIST 800-144 Cloud Security: Ep.8 – Availability	Describe the concerns and recommendations for cloud availability according to NIST 800-144	10
2025-02-04	NIST 800-144 Cloud Security: Ep.6 – Software Isolation	Recall what multi-tenancy architecture is	20
2025-02-04	NIST 800-144 Cloud Security: Ep.5 – Identity and Access Management	Recall the concerns and recommendations for identity and access management in cloud security as per NIST 800-144 guidelines	20
2025-02-04	NIST 800-144 Cloud Security: Ep.4 – Architecture	Explain NIST's recommendations and concerns about architecture with regards to cloud security	10
2025-02-04	NIST 800-144 Cloud Security: Ep.3 – Trust	Explain the concern for trust in cloud security	10
2025-02-04	NIST 800-144 Cloud Security: Ep.2 – Compliance	Recognize why compliance is important for cloud security	10
2025-02-04	NIST 800-144 Cloud Security: Ep.1 – Governance	Recall how governance is important to NIST cloud security guidelines	10
2025-02-04	NIST 800-144: Guidelines on Security and Privacy in Public Cloud Computing	Recall the NIST 800-144 guidelines at a high level	10
2025-02-03	Windows Basics: Ep.6 – SMB and RDP	Demonstrate how to use SMB and RDP to manage the target system remotely	100
2025-02-03	Introduction To Elastic: Ep.7 – Escalate	Understand the importance of using Elastic in escalating security incidents	100
2025-02-03	Introduction To Elastic: Ep.6 – Investigate	Recall the importance of using Elastic in investigating security incidents	100
2025-02-03	Introduction To Elastic: Ep.5 – Focus (Detection Rules)	Demonstrate how to gather further information on a pre-defined rule in Kibana	200
2025-02-03	Introduction To Elastic: Ep.4 – Focus (Alert Detailing)	Demonstrate how to gather further information on alerts in Kibana	200
2025-02-03	Introduction To Elastic: Ep.3 – Triage	Understand the importance of using Elastic in triaging security incidents	100
2025-02-03	Introduction To Elastic: Ep.2 – Querying Data	Understand the importance of using Elastic when investigating security incidents	200

Activity Report Page 27 of 40

Date	Lab	Description	Points Earned
2025-02-02	Splunk: Malicious Account Creation	Identify and recognize malicious events in system logs	200
2025-01-30	Windows Basics: Ep.7 – Scheduled Tasks	Demonstrate the ability to create and modify tasks	100
2025-01-30	Web Log Analysis: 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
2025-01-30	Splunk Basics: Ep.5 – Dashboards and Visualization	Recognize dashboards and how they can be used	100
2025-01-30	Splunk Basics: Ep.4 – Advanced Searching (SPL & Transforming)	Use Splunk's Search Processing Language (SPL) to search for and transform specific information	200
2025-01-30	Splunk Basics: Ep.3 – Search	Identify the key structure of a basic Splunk search	100
2025-01-30	Splunk Basics: Ep.1 – The Splunk Interface	Recognize the different components of the Splunk Interface	40
2025-01-30	SMTP Log Analysis	Carry out a log analysis to identify particular information	100
2025-01-29	Introduction To Elastic: Ep.1 – What is Elastic?	Recall what the Elastic stack is	40
2025-01-29	Web Log Analysis: Ep.4 — Error Logs	Recognize web server error logs	100
2025-01-29	Web Log Analysis: Ep.3 – Access Logs	Recognize web server access logs	100
2025-01-29	Web Log Analysis: Ep.2 – Log Formats	Describe the different types of web server log formats	20
2025-01-28	Windows Basics: Ep.5 – Services	Demonstrate how to set up and modify Windows services	100
2025-01-28	Windows Basics: Ep.4 – Managing Processes	Explain how to view processes on the Windows system	100
2025-01-28	Windows Basics: Ep.3 – Registry	Recall how to view the Windows registry	100

Activity Report Page 28 of 40

Date	Lab	Description	Points Earned
2025-01-28	Windows Basics: Ep.2 – Users and Groups	Recall how to find users and groups on a Windows system	100
2025-01-28	Web Log Analysis: Ep.1 – What are Web Server Logs?	Recall the different types of web server logs	20
2025-01-28	Networking: Demonstrate Your Skills	Demonstrate how to analyze PCAP files	100
2025-01-28	DoS Primer: Resource Exhaustion	Explain the different types of resource exhaustion attacks	40
2025-01-28	DoS Primer: Vulnerabilities	Learn different types of denial of service vulnerabilities	40
2025-01-28	DoS Primer: Volumetric	Explain the different types of volumetric attacks	40
2025-01-28	Protocols: LDAP	Analyze the LDAP protocol in an enterprise context	100
2025-01-28	Protocols: ARP	Identify packet structure of ARP requests and responses	100
2025-01-28	Protocols: FTP	Explain the core concepts of the File Transfer Protocol	100
2025-01-28	Protocols: DHCPv6	Discuss the use of DHCP in computer networks	200
2025-01-28	Protocols: DHCPv4	Discuss the use of DHCP in computer networks	200
2025-01-28	Protocols: Modbus	Reference the core concepts of the Modbus protocol	300
2025-01-28	DoS Primer: Tools	Describe several denial of service tools	200
2025-01-28	Protocols: DNS	Describe the structure of DNS requests and responses	200
2025-01-28	Protocols: SMTP	Describe the structure of SMTP messages	200

Activity Report Page 29 of 40

Date	Lab	Description	Points Earned
2025-01-28	Protocols: HTTP	Describe the structure of HTTP GET and POST requests	200
2025-01-28	Intrusion Detection Systems	Recognize what an IDS is and how they’re used	20
2025-01-27	DevSecOps: Build	Recall the security considerations of the DevSecOps build stage	20
2025-01-27	The Internet	Explain the history of the internet	20
2025-01-27	Protocols: HTTP – Status Codes	Develop knowledge of HTTP status codes	100
2025-01-27	OSI Model	Identify the different layers of the OSI model	40
2025-01-27	Ports	Identify how ports are used in modern networks	40
2025-01-27	Transport Protocols	Explain the core concepts of the the most common transport protocols	40
2025-01-27	Internet Protocol V4	Explain the core concepts of IPv4 addressing	100
2025-01-26	Linux CLI: Ep.17 – Demonstrate Your Skills	Demonstrate your understanding of the Linux CLI	100
2025-01-26	Zero Trust in the Cloud: Endpoint Security	Recognize the core concepts of zero trust endpoint security	10
2025-01-26	Zero Trust in the Cloud: Identity and Access Management	Recognize the core concepts of zero trust identity management	10
2025-01-26	Zero Trust in the Cloud: Networking	Identify tools for implementing zero trust networking in the cloud	10
2025-01-26	Secrets Management	Recognize the challenges involved with storing sensitive information	20
2025-01-26	DevSecOps: Code	Recall the security considerations of the DevSecOps coding phase	20

Date	Lab	Description	Points Earned
2025-01-26	DevSecOps: Plan	Recall the security considerations of the DevSecOps planning stage	20
2025-01-26	Cloud Security: Frameworks, Standards, and Guidelines	Be able to identify the different frameworks, standards, and guidelines that relate to cloud security	10
2025-01-26	Cloud Security Alliance: Cloud Controls Matrix v4.0	Recall the domains within the CSA CCM v4.0	10
2025-01-26	Cloud Fundamentals: Introduction to SAML	Be able to recognize the advantages of Single Sign-On	40
2025-01-26	Virtualization	Describe the uses and advantages of virtualization	10
2025-01-26	Platform as a Service (PaaS)	Be able to explain the advantages and disadvantages of Platform as a Service	20
2025-01-26	Security Automation	Describe the advantages of security automation and orchestration	20
2025-01-26	Infrastructure as Code (IaC)	Explain what IaC is and how it is deployed	20
2025-01-26	DevSecOps: Introduction	Recall the evolution of software delivery methodologies	10
2025-01-26	Infrastructure as a Service (IaaS)	Describe the advantages and disadvantages of Infrastructure as a Service (IaaS)	20
2025-01-26	Software as a Service (SaaS)	Be able to describe the advantages and disadvantages of SaaS	20
2025-01-26	Linux CLI: Ep.12 – Using Find	Recognize how the find command work	200
2025-01-26	Linux CLI: Ep.14 – Using Screen	Describe how `screen` works in the CLI	100
2025-01-26	Linux CLI: Ep.13 – Searching and Sorting	Employ searching techniques to find patterns in files	100
2025-01-26	Linux CLI: Ep.16 – Combining Commands	Identify the different ways of combining commands on the terminal	200

Activity Report Page 31 of 40

Date	Lab	Description	Points Earned
2025-01-26	Linux CLI: Ep.15 – Generating File Hashes	Recognize file hashes	100
2025-01-26	Linux CLI: Ep.11 – Using SSH and SCP	Recall what the SSH protocol is	100
2025-01-24	PowerShell Basics: Demonstrate Your Skills	Creating and editing PowerShell scripts	200
2025-01-24	Linux CLI: Ep.10 – Using Sudo	Identify different user privileges in Linux	100
2025-01-24	Linux CLI: Ep.5 – File Permissions	Be able to read Linux file permissions	100
2025-01-24	Linux CLI: Ep.8 – Manipulating Text	Modify text within files using basic command line tools	200
2025-01-24	Linux CLI: Ep.6 – Editing Files	Be able to recall some common Linux command line text editors	100
2025-01-24	Linux CLI: Ep.7 – Using wc	Count elements in a file using the wc tool	200
2025-01-24	Linux CLI: Ep.9 – Stream Redirection	Describe how data can be manipulated via the terminal	100
2025-01-23	PowerShell Basics: Ep.9 – Error Handling	Describe the different types of PowerShell errors	100
2025-01-23	PowerShell Basics: Ep.8 – ISE and Scripting	Recall how to open PowerShell ISE	100
2025-01-23	PowerShell Basics: Ep.6 – Processes and Services	Explain how to find processes and services with PowerShell	100
2025-01-23	PowerShell Basics: Ep.4 – Operators and Expressions	Explain what PowerShell operators are	100
2025-01-23	PowerShell Basics: Ep.3 – Variables	Describe what PowerShell variables are	100
2025-01-23	NIST 800-53: Ep.21 – Demonstrate your Knowledge	Demonstrate your understanding of NIST 800-53 and its purpose	40

Activity Report Page 32 of 40

Date	Lab	Description	Points Earned
2025-01-23	Tactics: Demonstrate your Knowledge	Demonstrate your understanding of tactics in the MITRE ATT&CK® framework	40
2025-01-23	Zero Trust in the Cloud: Introduction	Recognize elements of a zero trust security strategy	10
2025-01-23	NIST 800-53: Ep.20 – Supply Chain Risk Management	Recognize supply chain risk management controls	20
2025-01-23	NIST 800-53: Ep.19 – System and Information Integrity	Recognize system and information integrity controls and their purpose	40
2025-01-23	NIST 800-53: Ep.18 – System and Communications Protection	Recognize system and communications protection controls and their purpose	40
2025-01-23	NIST 800-53: Ep.17 – System and Services Acquisition	Recognize system and services acquisition controls	20
2025-01-23	NIST 800-53: Ep.16 – Risk Assessment	Recognize risk assessment controls	20
2025-01-23	NIST 800-53: Ep.15 – Personally Identifiable Information Processing and Transparency (PIIPT)	Recognize the PIIPT controls	40
2025-01-23	NIST 800-53: Ep.14 – Personnel Security	Recognize personnel security controls and their purpose	20
2025-01-23	NIST 800-53: Ep.13 – Program Management	Recognize program management controls and their purpose	20
2025-01-23	NIST 800-53: Ep.12 – Planning	Recognize planning controls and their purpose	20
2025-01-23	NIST 800-53: Ep.11 – Physical and Environmental Protection	Recognize physical and environmental protection controls and their purpose	20
2025-01-23	NIST 800-53: Ep.10 – Media Protection	Recognize media protection controls and their purpose	20
2025-01-23	NIST 800-53: Ep.9 – Maintenance	Recognize maintenance controls and their purpose	20
2025-01-23	NIST 800-53: Ep.8 – Incident Response	Recognize incident response controls and their purpose	20

Date	Lab	Description	Points Earned
2025-01-23	NIST 800-53: Ep.7 – Identification and Authentication	Recognize identification and authentication controls and their purpose	20
2025-01-23	NIST 800-53: Ep.6 – Contingency Planning	Recognize contingency planning controls and their purpose	20
2025-01-23	NIST 800-53: Ep.5 – Configuration Management	Recognize configuration management controls and their purpose	20
2025-01-23	NIST 800-53: Ep.4 – Assessment, Authorization, and Monitoring	Recognize assessment, authorization, and monitoring controls and their purpose	20
2025-01-23	NIST 800-53: Ep.3 – Audit and Accountability	Recognize audit and accountability controls and their purpose	20
2025-01-23	NIST 800-53: Ep.2 – Awareness and Training	Recognize the purpose of awareness and training controls	20
2025-01-23	NIST 800-53: Ep.1 – Access Control	Recognize the NIST 800-53 Access Control family and its purpose	20
2025-01-23	NIST 800-53: Security and Privacy Controls for Information Systems and Organizations	Familiarize yourself with NIST 800-53 and its purpose	20
2025-01-23	Splunk Basics: Ep.2 – Data Sources	Be able to recall the various data sources supported by Splunk	40
2025-01-23	What is Splunk?	Recall what the Splunk tool is	40
2025-01-23	Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface	Recall Linux command line fundamentals	40
2025-01-23	Tactics: Exfiltration	Recognize the purpose of the MITRE ATT&CK® Exfiltration tactic	20
2025-01-23	Tactics: Impact	Be able to explain the purpose of the MITRE ATT&CK® Impact tactic	20
2025-01-23	Tactics: Collection	Recognize the purpose of the MITRE ATT&CK® Collection tactic	20
2025-01-23	Tactics: Command and Control	Recognize the purpose of the MITRE ATT&CK® Command and Control tactic	20

Date	Lab	Description	Points Earned
2025-01-23	Tactics: Lateral Movement	Recognize the MITRE ATT&CK® Lateral Movement tactic and its purpose	20
2025-01-23	Tactics: Discovery	Recognize the purpose of the MITRE ATT&CK® Discovery tactic	20
2025-01-23	Introduction to Cloud	Recognize key aspects of cloud computing and the benefits it can bring	10
2025-01-23	PowerShell Basics: Ep.11 – Remoting	Recall how to create, manage, and remove remote sessions with PowerShell	200
2025-01-23	Linux CLI: Ep.2 – Getting Started with the Terminal	Recall fundamental concepts of the Linux terminal	100
2025-01-23	PowerShell Basics: Ep.10 – Event Logs	Recall how to view, filter, and analyze event logs using PowerShell	100
2025-01-23	PowerShell Basics: Ep.7 – Functions and Modules	Describe what PowerShell functions and modules are	100
2025-01-23	PowerShell Basics: Ep.2 – Cmdlets	Explain what PowerShell cmdlets are	100
2025-01-23	PowerShell Basics: Ep.5 – Files and Folders	Explain how to navigate around a system with PowerShell	100
2025-01-23	Linux CLI: Ep.4 – Changing Things	Recall the Linux CLI commands explored in the lab	100
2025-01-23	Linux CLI: Ep.3 – Moving Around	Navigate through directories on the command line	100
2025-01-22	Secure Data Handling	Recall fundamental concepts of input validation and output encoding	40
2025-01-22	Windows Basics: Demonstrate Your Skills	Demonstrate how to interact with and modify a Windows system with the Windows Command Prompt	400
2025-01-22	Windows Concepts: Demonstrate Your Skills	Demonstrate proficiency in navigating and manipulating the Windows registry to achieve specific configurations or extract information.	200
2025-01-22	Introduction to Cryptography: Demonstrate Your Knowledge	Demonstrate an understanding of cryptography	40

Activity Report Page 35 of 40

Date	Lab	Description	Points Earned
2025-01-22	Introduction to Networking: Ep.7 — Demonstrate Your Knowledge	Demonstrate an understanding of networking technology fundamentals	40
2025-01-22	Cyber Kill Chain: Ep.1 – What is the Cyber Kill Chain?	Recognize the fundamentals of the Cyber Kill Chain model	20
2025-01-22	Encoding: Demonstrate Your Skills	Recall encoding methods and techniques	200
2025-01-22	Encoding: Punycode	Recall how Punycode functions	100
2025-01-22	Encoding: Unicode	Recall how Unicode functions	40
2025-01-22	Encoding: Base64	Recall how Base64 encoding works	40
2025-01-22	Encoding: ASCII	Recall how ASCII encoding functions	40
2025-01-22	Encoding: Hexadecimal	Recall how hexadecimal functions	40
2025-01-22	Encoding: What is Encoding?	Recall how encoding functions	40
2025-01-22	Secure Fundamentals: The CIA Triad	Define confidentiality, integrity, and availability	20
2025-01-22	Secure Fundamentals: Attribution and Accountability	Recall the definitions of attribution and accountability	20
2025-01-22	Introduction to Networking: Ep.4 – Network Topologies	Recognize network topologies	40
2025-01-22	Introduction to Networking: Ep.3 — Network Hardware	Recognize the different types of hardware used for networks	40
2025-01-22	Introduction to Networking: Ep.2 – Types of Networks	Recall multiple types of networks and how they differ	20
2025-01-22	Introduction to Networking: Ep.1 — What is a Network?	Recognize networks and their components	40

Date	Lab	Description	Points Earned
2025-01-22	Introduction to Cryptography: Public and Private Key Management	Recognize the importance of managing public and private keys	40
2025-01-22	Introduction to Cryptography: One-Time Pad	Define what a one-time pad cipher is	40
2025-01-22	Introduction to Cryptography: Symmetric Key Encryption	Recognize symmetric encryption	40
2025-01-22	Introduction to Cryptography: What is Cryptography?	Recall the fundamentals of cryptography	40
2025-01-22	Introduction to Cryptography: Asymmetric Encryption	Define asymmetric encryption	40
2025-01-22	Introduction to Cryptography: Block Ciphers	Define a block cipher	40
2025-01-22	Introduction to Cryptography: Digital Signatures	Recall the importance of digital signatures	40
2025-01-22	Introduction to Cryptography: Stream Ciphers	Define stream ciphers and recall their fundamental characteristics	40
2025-01-22	Introduction to Cryptography: Hashing	Recognize the importance of hashing	20
2025-01-22	Introduction to Cryptography: Public Key Infrastructure	Define what public key infrastructure is	40
2025-01-22	Introduction to Cryptography: Message Integrity	Be able to define the term ‘message integrity’	40
2025-01-22	Tactics: Reconnaissance	Recognize the purpose of the MITRE ATT&CK® Reconnaissance tactic	20
2025-01-22	Tactics: Credential Access	Recognize the purpose of the MITRE ATT&CK® Credential Access tactic	20
2025-01-22	Tactics: Resource Development	Recognize the purpose of the MITRE ATT&CK® Resource Development tactic	20
2025-01-22	Secure Fundamentals: Principle of Least Privilege	Describe the principle of least privilege	10

Activity Report Page 37 of 40

Date	Lab	Description	Points Earned
2025-01-22	Secure Fundamentals: Security Patching	Describe what a security patch is	10
2025-01-22	Ethics & Laws: US Federal Cyber Law	Identify the main US federal laws that can be used to convict cyber criminals	10
2025-01-22	Secure Fundamentals: Authorization	Describe the security concept of authorization	10
2025-01-22	Ethics & Laws: UK Cyber Law	Demonstrate an understanding of illegalities and breaches of law	40
2025-01-22	Compliance: General Data Protection Regulation (GDPR)	Recognize the key details of the GDPR	10
2025-01-22	Introduction to Networking: Ep.5 — IP Addresses	Recognize an IP address	40
2025-01-22	Cyber 101: Rogue USB Devices	Recall how rogue USB devices can be used for malicious purposes	10
2025-01-22	Staying Safe Online: Updates and Patches	Identify the differences between updates and patches	10
2025-01-22	Cyber 101: Information Security	Recognize the importance of information security for individuals and organizations	10
2025-01-22	Ethics & Laws: Bugbusters	Demonstrate an understanding of bug bounties and the companies that offer them	40
2025-01-22	Ethics & Laws: Ethical and Unethical Hacking	Demonstrate the ability to determine the ethical choices of hackers	40
2025-01-22	Ethics & Laws: Burglary and Hacking	Demonstrate an understanding of how hacking can be similar to burglary	40
2025-01-22	Ethics & Laws: Police Raid	Demonstrate an understanding of devices that would be confiscated in an investigation	40
2025-01-22	Cyber 101: Who Are The Hackers?	Recognize the different types of hackers	10
2025-01-22	Cyber 101: Why Hackers Hack	Recognize some of the methods used by hackers	10

Date	Lab	Description	Points Earned
2025-01-22	Tactics: Defense Evasion	Recognize the purpose of the MITRE ATT&CK® Defense Evasion tactic	20
2025-01-22	Tactics: Privilege Escalation	Recognize the purpose of the MITRE ATT&CK® Privilege Escalation tactic	20
2025-01-22	Tactics: Persistence	Recognize the purpose of the MITRE ATT&CK® Persistence tactic	20
2025-01-22	Tactics: Execution	Know the purpose of the MITRE ATT&CK® Execution tactic	20
2025-01-22	Tactics: Initial Access	Recognize the purpose of the MITRE ATT&CK® Initial Access tactic	20
2025-01-22	Cyber 101: Virtual Card Numbers	Identify the different types of virtual card numbers	10
2025-01-22	Cyber 101: Fake News	Recognize the characteristics of fake news	10
2025-01-22	Windows Concepts: CertUtil	Analyze the function of CertUtil	100
2025-01-22	Cyber 101: Security Champions	Underline what a security champion is and their purpose	10
2025-01-22	Windows Concepts: Background Intelligent Transfer Service (BITS)	Gain an understanding of BITS and how it can be abused	100
2025-01-22	Cyber 101: Keylogging	Recognize what keyloggers are	10
2025-01-22	Cyber 101: Geolocation	Recognize the differences between device-based and server-based geolocation tracking	10
2025-01-22	Introduction to MITRE ATT&CK®	Be familiar with the MITRE ATT&CK® framework and know how it's used	20
2025-01-22	Cyber 101: Darknets	Recognize how darknets operate on the internet	10
2025-01-22	Cyber 101: Cookies	Recognize how cookies are used by individuals and organizations	20

Activity Report Page 39 of 40

Date	Lab	Description	Points Earned
2025-01-22	Staying Safe Online: Multi-Factor Authentication	Recall how multi-factor authentication works	10
2025-01-22	Windows Concepts: Volume Shadow Copy Service	Exposure to VSS and its functionality	200
2025-01-22	PowerShell Basics: Ep.1 – What is PowerShell?	Describe what PowerShell is	40
2025-01-22	Windows Concepts: Alternate Data Streams	Exposure to ADS and data hiding	200
2025-01-22	Windows Concepts: Scheduled Tasks	Demonstrate how to navigate information in Windows Scheduled Tasks	100
2025-01-22	Windows Concepts: Windows Registry	Evaluate registry values	100
2025-01-22	Windows Concepts: Security Policies	Exposure to Windows policy mechanisms	200
2025-01-22	Windows Concepts: Environment Variables	Understand the function of environment variables in Windows	200
2025-01-22	Windows Concepts: New Technology File System (NTFS)	Analyze Windows file permissions	100
2025-01-22	Introduction to Networking: Ep.6 — Domain Name System	Summarize the fundamentals of the Domain Name System	40
2025-01-22	Encoding: Binary	Recall how binary functions	40
2025-01-22	Log Finder	Perform web log analysis	100
2025-01-22	Cyber 101: Cyber Kill Chain	Recognize the purpose of the cyber kill chain	10
2025-01-13	Windows Basics: Ep.1 – Command Prompt	Recall how to open the Windows Command Prompt	40
2025-01-12	Introduction To Elastic: Demonstrate Your Skills	Demonstrate how to use the various apps in Kibana to identify the tactics, techniques, and procedures of an advanced persistent threat group	300

Activity Report Page 40 of 40

Date	Lab	Description	Points Earned
2025-01-12	Secure Fundamentals: Defense In Depth	Describe the security concept of defense in depth	10
2025-01-12	Secure Fundamentals: Authentication	Describe the security concept of authentication	10
2025-01-10	Networking: Demonstrate Your Knowledge	Demonstrate your networking knowledge	100

About Immersive

Immersive 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.