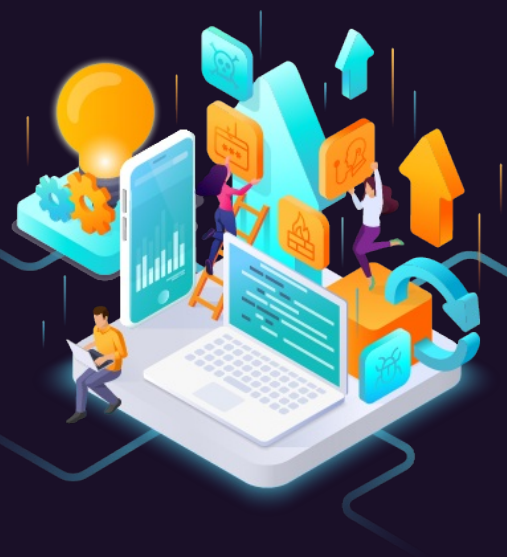
immersive



Andrew Ingram

Completed 1461 labs earning 157100 points.

Activity Report

Date	Lab	Description	Points Earned
2026-02-25	Offensive PowerShell: What is Offensive PowerShell?	Explain the benefits of using PowerShell to perform offensive actions	40
2026-02-23	CrowdStrike: Scenario	Discuss the capabilities of CrowdStrike Falcon	200
2026-02-20	Threat Actors: Turla	Analyze and identify specific TTPs used by Turla	100
2026-02-20	Threat Actors: Fancy Bear	Analyze and identify specific TTPs used by Fancy Bear	100
2026-02-20	Threat Actors: Chimera	Analyze and identify specific TTPs used by Chimera	100
2026-02-20	Threat Actors: APT32	Analyze and identify specific TTPs used by APT32	100
2026-02-12	CrowdStrike: NG-SIEM	Navigate the log management and search pages in Falcon	200
2026-02-12	CrowdStrike: Endpoint Security Configuration	Describe the difference between policies and rules in Falcon	200
2026-02-12	CrowdStrike: Endpoint detections	Describe techniques to manage detections in the Falcon console	200
2026-02-11	Lotus Blossom: Notepad++ Campaign Analysis	Outline the TTPs for Lotus Blossom	300

Activity Report Page 2 of 98

Date	Lab	Description	Points Earned
2026-02-11	CrowdStrike: Host setup and management	Explain the difference between roles and permissions in Falcon	100
2026-02-04	CrowdStrike: Introduction	Identify the core features of CrowdStrike Falcon	20
2026-01-27	Introduction to Business Logic Flaws	Summarize what business logic flaws are	40
2026-01-15	CVE-2019-11043 (PHP FPM)	Understand the scope and capabilities of the exploit	200
2026-01-14	Detecting RMM Tools: Atera	Outline how to bypass existing detections for Atera	300
2026-01-14	Windows LPE (InstallerFileTakeOver) – Defensive	Identify the exploit from the logs	400
2026-01-14	CVE-2020-16898 (Bad Neighbor) – Defensive	Analyze IPv6 Traffic	300
2026-01-14	CVE-2019-10149 (Exim Server RCE) — Defensive	Identify the latest threat through network communication analysis	200
2026-01-08	Meterpreter	Experience navigating the basic functionality of Meterpreter payload	200
2026-01-06	MalTerminal: Malware Analysis	Outline the key features of LLM-enabled malware	200
2026-01-02	Heap Internals: Introduction to the NT Heap	Recognize how the NT Heap is managed	40
2026-01-02	Heap Internals: Introduction to the Heap	Identify how the heap manager in Windows manages memory allocations	40
2025-12-30	Chrome Alone: Transforming a Browser Into a C2 Platform	Outline how Chrome extension sideloading can bypass normal extension store controls	200
2025-12-23	Detecting RMM Tools: MeshCentral	Outline how to bypass existing detections for MeshCentral	300
2025-12-12	Building with AI: Claude Code – Subagents	Explain how subagents work with the main agent	100

Activity Report Page 3 of 98

Date	Lab	Description	Points Earned
2025-12-11	Building with AI: Claude Code – Claude Skills	Explain how to use Claude Skills to perform actions	100
2025-12-09	Building with AI: Claude Code – Tools and MCP	Recall the baseline tools available in Claude Code	100
2025-12-09	Building with AI: Claude Code – Spec-Driven Development	Describe the benefits of using specification-driven development	100
2025-12-09	Building with AI: Claude Code – Slash Commands	Recall the benefits of the default slash commands	100
2025-12-02	Building with AI: Claude Code – Manual Prompting	Recall the benefits of using manual prompts and human-in-the-loop design	40
2025-11-26	Building with AI: Claude Code – Introduction	Explain how to use Claude Code for basic operations	40
2025-11-26	DevSecOps: Release	Recall the security considerations of the DevSecOps release stage	20
2025-11-26	DevSecOps: Operate	Recall the security considerations of the DevSecOps operation stage	20
2025-11-26	DevSecOps: Test	Recall the security considerations of the DevSecOps testing stage	20
2025-11-26	DevSecOps: Build	Recall the security considerations of the DevSecOps build stage	20
2025-11-26	DevSecOps: Code	Recall the security considerations of the DevSecOps coding phase	20
2025-11-26	DevSecOps: Monitor	Recall the security considerations of the DevSecOps monitoring phase	20
2025-11-26	DevSecOps: Deploy	Recall the security considerations of the DevSecOps deployment stage	20
2025-11-26	DevSecOps: Plan	Recall the security considerations of the DevSecOps planning stage	20
2025-11-21	Malicious Document Analysis: OLE tools	Investigate various malicious artifacts	300

Activity Report Page 4 of 98

Date	Lab	Description	Points Earned
2025-11-17	OWASP Top 10 (2025): A07 – Authentication Failures	Summarize authentication failures and their relationship to the OWASP Top 10	20
2025-11-17	OWASP Top 10 (2025): A04 – Cryptographic Failures	Summarize cryptographic failures and their relationship to the OWASP Top 10	20
2025-11-17	OWASP Top 10 (2025): A10 – Mishandling of Exceptional Conditions	Summarize the mishandling of exceptional conditions and its relationship to the OWASP Top 10	20
2025-11-17	OWASP Top 10 (2025): A09 – Logging and Alerting Failures	Summarize logging and alerting failures and their relationship to the OWASP Top 10	20
2025-11-17	OWASP Top 10 (2025): A08 – Software or Data Integrity Failures	Summarize software or data integrity failures and their relationship to the OWASP Top 10	20
2025-11-17	OWASP Top 10 (2025): A06 – Insecure Design	Summarize insecure design and its relationship to the OWASP Top 10 list	20
2025-11-17	OWASP Top 10 (2025): A05 – Injection	Explain injection in the context of the OWASP Top 10	20
2025-11-17	OWASP Top 10 for LLMs and GenAI: Misinformation	Summarize misinformation and its relationship to the Top 10 list	20
2025-11-17	OWASP Top 10 for LLMs and GenAI: Vector and Embedding Weaknesses	Summarize vector and embedding weaknesses and their relationship to the Top 10 list	20
2025-11-17	OWASP Top 10 for LLMs and GenAI: System Prompt Leakage	Summarize system prompt leakage and its relationship to the Top 10 list	20
2025-11-17	OWASP Top 10 for LLMs and GenAI: Excessive Agency	Summarize excessive agency and its relationship to the Top 10 list	20
2025-11-17	OWASP Top 10 for LLMs and GenAI: Improper Output Handling	Summarize improper output handling and its relationship to the Top 10 list	20
2025-11-17	OWASP Top 10 for LLMs and GenAI: Data and Model Poisoning	Summarize data and model poisoning and its relationship to the Top 10 list	20
2025-11-17	OWASP Top 10 for LLMs and GenAI: Supply Chain	Summarize supply chain vulnerabilities and their relationship to the Top 10 list	20
2025-11-17	OWASP Top 10 for LLMs and GenAI: Unbounded Consumption	Summarize unbounded consumption and its relationship to the Top 10 list	20

Activity Report Page 5 of 98

Date	Lab	Description	Points Earned
2025-11-17	OWASP Top 10 for LLMs and GenAI: Sensitive Information Disclosure	Summarize sensitive information disclosure and its relationship to the Top 10 list	20
2025-11-13	OWASP Top 10 (2025): A03 – Software Supply Chain Failures	Summarize software supply chain failures and their relationship to the OWASP Top 10	20
2025-11-13	OWASP Top 10 (2025): A02 – Security Misconfiguration	Summarize security misconfiguration and its relationship to the OWASP Top 10	20
2025-11-13	OWASP Top 10 (2025): Introduction	Recall the OWASP organization's objectives	10
2025-11-13	OWASP Top 10 (2025): A01 – Broken Access Control	Summarize broken access control and its relationship to the OWASP Top 10	20
2025-11-13	OWASP Top 10 for LLMs and GenAI: Prompt Injection	Summarize prompt injection and its relationship to the Top 10 list	20
2025-11-13	TerraPoint: Global Synthesis	Improve your location accuracy with careful observation and pattern recognition	100
2025-11-13	TerraPoint: Equatorial Scenes	Improve your location accuracy with careful observation and pattern recognition	100
2025-11-13	Secrets Management	Recognize the challenges involved with storing sensitive information	20
2025-11-13	Cloud Security: Frameworks, Standards, and Guidelines	Be able to identify the different frameworks, standards, and guidelines that relate to cloud security	10
2025-11-13	Cloud Security Alliance: Cloud Controls Matrix v4.0	Recall the domains within the CSA CCM v4.0	10
2025-11-13	Cloud Fundamentals: Introduction to SAML	Be able to recognize the advantages of Single Sign-On	40
2025-11-13	Introduction to Cloud	Recognize key aspects of cloud computing and the benefits it can bring	10
2025-11-10	TerraPoint: Northern Frontiers	Improve your location accuracy with careful observation and pattern recognition	100
2025-11-07	TerraPoint: City Forms and Flow	Improve your location accuracy with careful observation and pattern recognition	100

Activity Report Page 6 of 98

Date	Lab	Description	Points Earned
2025-11-07	TerraPoint: Rural Patterns	Improve your location accuracy with careful observation and pattern recognition	100
2025-11-07	TerraPoint: Continental Interiors	Improve your location accuracy with careful observation and pattern recognition	100
2025-11-05	TerraPoint: Cultural Networks	Improve your location accuracy with careful observation and pattern recognition	100
2025-11-05	TerraPoint: Coastal and Urban Mix	Improve your location accuracy with careful observation and pattern recognition	100
2025-11-05	TerraPoint: Heritage and Structure	Improve your location accuracy with careful observation and pattern recognition	100
2025-11-05	TerraPoint: Landmarks and Symbols	Improve your location accuracy with careful observation and pattern recognition	100
2025-10-29	Event Tracing for Windows: Introduction to ETW Internals	Identify the different components that make up ETW	10
2025-10-27	Trick or Treat on Specter Street: Wizard's Wicked Wish	Identify potentially vulnerable systems	300
2025-10-24	Trick or Treat on Specter Street: S.I.L.V.E.R.	Outline how the dark web is used by cybercriminals to plan operations	100
2025-10-24	Trick or Treat on Specter Street: Cursed Canvas	Analyze images, text, and audio	300
2025-10-24	Trick or Treat on Specter Street: Ripper's Riddle	Demonstrate your ability to use password cracking tools	200
2025-10-24	Trick or Treat on Specter Street: Trick or Trace	Demonstrate your Wireshark skills	100
2025-10-16	Business Impact Analysis: Mapping BIA Outputs to Continuity Strategy	Translate BIA outputs into continuity strategies	10
2025-10-16	Business Impact Analysis: Identifying Minimum Staffing and Key Skills	Assess minimum staffing requirements for critical processes	10
2025-10-16	Business Impact Analysis: Tracing Internal and External Dependencies	Identify internal and external dependencies during BIA interviews	10

Activity Report Page 7 of 98

Date	Lab	Description	Points Earned
2025-10-16	Business Impact Analysis: Uncovering Technical Dependencies	Identify the IT systems and technical dependencies linked to critical processes	10
2025-10-16	Business Impact Analysis: Impact Interviews	Structure effective BIA interviews with business units	10
2025-10-16	Business Impact Analysis: RTOs, RPOs, and MAOs	Define and explain the difference between RTOs, RPOs, and MAOs	10
2025-10-16	Hack Your First HMI: Exploitation	Explain why an attacker would target a human-machine interface (HMI)	200
2025-10-16	Hack Your First HMI: Discovering HMIs Using Wireshark	Analyze Modbus TCP/IP communications in a packet capture using Wireshark	200
2025-10-15	Business Impact Analysis: Identifying Critical Processes and Dependencies	Identify what makes a business process “critical”	10
2025-10-15	Hack Your First HMI: Discovering Internet Accessible HMIs with Shodan	Explain the purpose and capabilities of the Shodan search engine for industrial control system reconnaissance	20
2025-10-15	Hack Your First HMI: Introduction	Describe why an attacker would target a human-machine interface (HMI)	20
2025-10-15	Business Impact Analysis: What's a BIA and Why Does It Matter?	Explain the role and purpose of a BIA	10
2025-10-02	Packet Analysis: BPF Syntax	Analyze network packet captures	100
2025-10-02	Wireshark: Display Filters – Diving In	Analyze network packet captures using complex operators	200
2025-10-02	Malware Analysis: Scranos Rootkit	Investigate a malicious Windows driver using various malware analysis techniques	300
2025-10-02	Wireshark: Using Tshark	Analyze network packet captures	200
2025-10-02	Packet Capture: Key Extraction	Analyze network packet captures	300
2025-09-25	Fundamental AI Algorithms: Introduction	Identify the core concepts of machine learning	40

Activity Report Page 8 of 98

Date	Lab	Description	Points Earned
2025-09-24	Introduction to Detection Engineering: Foundational Concepts	Recognize applications of ProcMon process tree and filter features	200
2025-09-22	Snort Rules: Demonstrate Your Skills	Demonstrate usage of Snort rules against a malware packet capture file	400
2025-09-22	Snort Rules: Lokibot Infection Traffic	Use Snort rules against a malware packet capture file	300
2025-09-22	Snort Rules: Credential Stealer via FTP Traffic	Demonstrate usage of Snort rules against a malware packet capture file	300
2025-09-22	Snort Rules: Fake Tech Support Popup	Demonstrate usage of Snort rules against a malware packet capture file	300
2025-09-22	Snort Rules: SMTP	Create Snort rules for SMTP events	300
2025-09-19	Pharma Drama: LlaMalware	Identify the IOCs related to this malware	200
2025-09-19	Pharma Drama: Patch the App	Be able to identify when directory listing is enabled on a web server	40
2025-09-15	Pharma Drama: Back to the Start	Identify suspicious activity using Splunk	200
2025-09-15	Pharma Drama: Spot the Logs	Be able to identify the attack methods used by examining the suspicious activity	200
2025-09-10	Browser Extensions: Chrome	Extract IOCs from extensions	200
2025-08-29	Malware Analysis: Kovter Trojan	Perform dynamic malware analysis	200
2025-08-28	CVE-2025-9074 (Docker Container Escape): Defensive	Outline how Docker's isolation technology works	300
2025-08-28	AI Foundations: Model Context Protocol (MCP)	Describe how the MCP is used within AI systems	20
2025-08-28	AI Foundations: Demonstrate Your Knowledge	Demonstrate the knowledge gained throughout the AI Foundations collection	10

Activity Report Page 9 of 98

Date	Lab	Description	Points Earned
2025-08-28	AI Foundations: Agentic AI	Identify use cases for AI agents	20
2025-08-28	AI Foundations: Retrieval Augmented Generation (RAG)	Recognize the different types of RAG	20
2025-08-28	AI Foundations: Large Language Models (LLMs)	Describe the benefits of fine-tuning models	10
2025-08-28	AI Foundations: Core Components	Identify the popular types of machine learning models	10
2025-08-28	AI Foundations: Artificial Intelligence	Identify the differences between AI, generative AI, and AGI	10
2025-08-28	CVE-2024-3094 (xz) – Supply Chain Compromise	Understand the mechanism used by the vulnerable library to deliver the backdoor binary file	300
2025-08-28	Malware: Analyzing Temporary .NET Assemblies	Identify malicious temporary .NET assemblies	300
2025-08-28	Windows Sysinternals: PsExec	Illustrate how the Sysinternals tool PsExec works	200
2025-08-27	Eric Zimmerman's Tools: SBECmd and ShellBags Explorer	Recognize the value of shellbags artifacts during a forensic investigation	100
2025-08-27	Eric Zimmerman's Tools: RECmd and Registry Explorer	Recognize the value of Registry artifacts during a forensic investigation	100
2025-08-27	Eric Zimmerman's Tools: RBCmd	Recognize the value of Recycle Bin artifacts	100
2025-08-27	Eric Zimmerman's Tools: MFTECmd and MFTExplorer	Recognize the value of the Master File Table artifacts during a forensic investigation	100
2025-08-27	Eric Zimmerman's Tools: LECmd	Recognize the value of LNK file artifacts during a forensic investigation	100
2025-08-27	Eric Zimmerman's Tools: PECmd	Recognize the value of prefetch file artifacts during a forensic investigation	100
2025-08-27	Digital Forensics: Using analyzeMFT	Recall what the $MFT is and its importance in forensic investigations	200

Activity Report Page 10 of 98

Date	Lab	Description	Points Earned
2025-08-25	Digital Forensics: Windows Artifacts	Perform a forensic analysis on a compromised system	400
2025-08-22	Scattered Spider and DragonForce: Campaign Analysis	Outline Scattered Spider's tactics, techniques, and procedures	300
2025-08-22	32-Bit Linux Assembly: Structure and Registers	Demonstrate use of assembly language to utilize system calls	200
2025-08-21	PoshC2: Obtaining NTLM hashes	Describe what an NTLM hash is and why they're a target for attackers	400
2025-08-21	PoshC2: An Introduction to PoshC2	Discuss the notable features of the PoshC2 framework	200
2025-08-18	Infrastructure Pen Testing: Your First Pen Test	Demonstrate pen testing skills	400
2025-08-18	Persistence: Netsh	Identify modern persistence methods used by malicious software	300
2025-08-18	Persistence: Accessibility Features	Construct a method of persistent access on a Windows system	200
2025-08-11	Introduction to PowerShell Deobfuscation: Demonstrate Your Skills	Demonstrate knowledge of various PowerShell deobfuscation techniques	300
2025-08-11	PowerShell Deobfuscation: System and Environment Interaction	List common system interaction functionality used by malware	100
2025-08-11	PowerShell Deobfuscation: Logical and Structural Obfuscation	Identify common logical and structural obfuscation techniques	100
2025-08-11	PowerShell Deobfuscation: String Manipulation and Command Obfuscation	Recite common techniques used to manipulate strings	100
2025-08-11	Introduction to PowerShell Deobfuscation: Encoding and Encryption	Describe what encoding and encryption are and how they differ	100
2025-08-11	Mini CTFs: Vulnerable Web App – The Final Feature	Demonstrate you can capture the flag with minimal guidance	300
2025-08-11	Mini CTFs: Fault Finding	Demonstrate how to identify vulnerable and misconfigured services	300

Activity Report Page 11 of 98

Date	Lab	Description	Points Earned
2025-08-06	Windows Sysinternals: ProcDump	Use ProcDump to debug programs and dump process memory	200
2025-08-04	Incident Response: RAT Attacks	Identify encoded and encrypted C2 communications	400
2025-08-01	Assessment: Infrastructure Security Testing	["Demonstrate knowledge of the methodologies, tools, and techniques used to perform penetration tests against internal and external network infrastructure."]	0
2025-07-30	Assessment: Application Security	["Demonstrate knowledge of common application vulnerabilities and secure development practices."]	0
2025-07-30	Assessment: IT Operations	["[\"Demonstrate your knowledge of common systems administrator and infrastructure engineer tasks\"]"]	0
2025-07-30	Assessment: Security Operations	["Demonstrate knowledge of the processes, tools, and functions of a modern Security Operations Center (SOC)."]	0
2025-07-29	Assessment: Offensive Security	["Demonstrate an understanding of the methodologies, tools, and ethical considerations of offensive security."]	0
2025-07-29	Assessment: Cybersecurity	["Demonstrate a foundational knowledge of cybersecurity principles, risk management, and core domains"]	0
2025-07-29	Assessment: Web Application Security Testing	["Demonstrate knowledge of the practical methodologies and manual techniques required to conduct a web application penetration test."]	0
2025-07-28	Server-Side Template Injection: SSTI in Embedded Ruby (ERB) Templates	Demonstrate how to use template expressions to exploit a server-side template injection vulnerability in the ERB template engine	300
2025-07-28	Server-Side Template Injection: SSTI in Jinja2 Templates	Use template expressions to exploit a server-side template injection vulnerability in the Jinja2 template engine	300
2025-07-28	Server-Side Template Injection: Identifying SSTI Vulnerabilities	Demonstrate how to identify a potential server-side template injection vulnerability	200
2025-07-28	Server-Side Template Injection: What is Server-Side Template Injection?	Describe what server-side template injection is	20
2025-07-28	Windows Sysinternals: Strings	Use the strings tool on a Windows system	200
2025-07-28	Windows Sysinternals: Autoruns	Deduce what malicious file is executing at system start-up	100

Activity Report Page 12 of 98

Date	Lab	Description	Points Earned
2025-07-25	CVE-2025-53770 (ToolShell SharePoint RCE): Defensive	Outline how attackers can bypass authentication using SignOut.aspx	300
2025-07-25	CVE-2025-53770 (ToolShell SharePoint RCE): Offensive	Outline how to exploit CVE-2025-53770 by performing an unauthorized deserialization attack	300
2025-07-21	Google Cloud Basics: VPC Networks	Recall core virtual networking concepts in Google Cloud	200
2025-07-21	Google Cloud Basics: Cloud Storage	Explain how to create and modify Cloud Storage buckets	200
2025-07-21	Google Cloud Basics: Identity and Access Management (IAM)	Describe the difference between user and workload identities	200
2025-07-21	Google Cloud Basics: Fundamental Concepts	Describe the differences between organizations, projects, and folders	10
2025-07-21	Google Cloud Basics: Introduction to the Console	Confidently use the Google Cloud console	100
2025-07-16	Tomcat: User Management – Theory	Describe the relationship between users, roles, and realms	40
2025-07-14	Diving Into SonarQube: What is SonarQube?	Describe what SonarQube is and what it's used for	10
2025-07-14	Diving Into SonarQube: Issues and Security Hotspots	Recognize how issues and security hotspots are raised in SonarQube	10
2025-07-14	Diving into SonarQube: What is SAST?	Describe what SAST is	10
2025-07-14	Real-World Playground: PHP – Broken Password Reset	Identify the vulnerability in the password reset functionality	100
2025-07-14	CVE-2022-30190 (Follina) ms-msdt Scheme Abuse – Offensive	Demonstrate how to compromise a vulnerable server with a PoC script	300
2025-07-14	Content Security Policy: Hashes	Be aware of the benefits of utilizing hashes within a Content Security Policy	100
2025-07-14	Content Security Policy: Introduction to CSP	Know the dangers of cross-site scripting vulnerabilities	10

Activity Report Page 13 of 98

Date	Lab	Description	Points Earned
2025-07-14	Content Security Policy: Reporting	Be aware of the benefits of reporting within a content security policy	40
2025-07-14	Content Security Policy: Inline JavaScript	Know what a content security policy is	40
2025-07-14	Content Security Policy: Directives and Values	Know the key directives and values that can be used in a content security policy	20
2025-07-14	CVE-2021-41773 (Apache) – Defensive	Detect exploitation attempts against an Apache server	200
2025-07-14	Secure Testing: Logic Flaws	Be able to describe a logic flaw vulnerability	40
2025-07-14	Secure Testing: Code Comments	Be able to describe what a code comment is	100
2025-07-14	Secure Testing: File and Directory Enumeration	Describe file and directory enumeration	100
2025-07-14	Secure Testing: Open Redirect	Be able to identify potential open redirect vulnerabilities in web applications, adding to your suite of QA tests	100
2025-07-14	Secure Testing: URL Parameters	Identify any potentially sensitive details being leaked in URL parameters, adding to your suite of QA tests	40
2025-07-14	Secure Testing: Insecure Direct Object Reference (IDOR)	Describe what an IDOR vulnerability is	100
2025-07-14	CVE-2018-11759 (mod_jk)	Identify methods to bypass web authentication processes	100
2025-07-14	CVE-2014-0160 (Heartbleed)	Demonstrate the Heartbleed vulnerability	100
2025-07-14	CVE-2014-6271 (Shellshock)	Demonstrate the Shellshock vulnerability	200
2025-07-10	CVE-2025-33073 (SMB Elevation of Privilege): Defensive	Outline the conditions required to achieve privilege elevation on the compromised machine	300
2025-07-09	CVE-2025-32463 (Sudo Chroot Elevation of Privilege): Offensive	Outline how sudo works to manage privileges in Linux	300

Activity Report Page 14 of 98

Date	Lab	Description	Points Earned
2025-07-09	Norwegian Dam Compromise: Campaign Analysis	Describe how a dam works to generate electricity	300
2025-06-26	Embedded Application Security: Introduction	Recall the risks and challenges of embedded application security	40
2025-06-26	Embedded Application Security: Working With ESP32	Describe the ESP32 series	40
2025-06-26	Embedded Application Security: Debug Code and Interfaces	Recognize debug code	100
2025-06-26	Embedded Application Security: Transport Layer Security	Recognize how Transport Layer Security (TLS) helps protect data	100
2025-06-26	Embedded Application Security: Firmware Updates and Cryptographic Signatures	Describe how firmware updates and cryptographic signatures help protect devices	20
2025-06-26	Threat Research: Cobalt Strike C2 – Host Forensics	Analyze packet captures to observe traffic between the Cobalt Strike team server and the beacon	200
2025-06-12	Stealth Falcon (CVE-2025-33053) – WebDAV Server Remote Code Execution	Outline how Stealth Falcon used CVE-2025-33053 to achieve code execution on victim machines and deploy malware	300
2025-06-12	Interactive RegEx: Demonstrate	Apply knowledge gained throughout the series to match specific data	200
2025-05-29	CVE-2023-43770 (Roundcube Stored XSS)	Outline how the Roundcube XSS vulnerability is exploited	200
2025-05-29	Storm-0978: Malware Analysis	Outline the Cuba malware's TTPs	300
2025-05-29	Plex Exploit: Vulnerability Chain	Exploit a vulnerable Plex server using existing exploit modules	200
2025-05-29	CVE-2019-7304 (snapd)	Analyze the Ubuntu Snap vulnerability	100
2025-05-28	BadSuccessor: Offensive	Recall the function and characteristics of dMSAs in Active Directory	200
2025-05-28	BadSuccessor: Defensive	Describe the function and characteristics of dMSAs in Active Directory	200

Activity Report Page 15 of 98

Date	Lab	Description	Points Earned
2025-05-28	APT29 Threat Hunting with Splunk: Initial Compromise	Identify various tactics from the MITRE ATT&CK framework	200
2025-05-27	Interactive RegEx: Flags	Recall the different flags that can be applied to the regex engine	100
2025-05-27	Interactive RegEx: Groups	Recall how you previously used capture groups	200
2025-05-22	Sandworm Campaign: ZEROLOT Wiper	Describe Sandworm Team's latest TTPs	200
2025-05-22	Threat Actors: APT35	Analyze and identify specific TTPs used by APT35	100
2025-05-21	CVE-2024-5910 (Palo Alto Expedition) – Defensive	Understand how defenders can use details from publicly disclosed details to identify signs of exploitation on a Palo Alto Expedition server	300
2025-05-19	Wizard Spider DFIR: Demonstrate Your Skills	Demonstrate your understanding of the techniques used by Wizard Spider during an attack	300
2025-05-19	Wizard Spider DFIR: Dropper Analysis	Identify indicators of compromise in malicious Microsoft Office documents	300
2025-05-19	Wizard Spider DFIR: Initial Access	Recognize the techniques used by the Wizard Spider threat group during an attack	200
2025-05-16	SQL Injection: UNION	Employ advanced SQL injection techniques	300
2025-05-12	StrelaStealer Malware Campaign: Analysis	Outline the execution flow the threat actor uses to deploy their malware	300
2025-05-12	Brute Ratel: Extracting Indicators of Compromise	Demonstrate an ability to extract and decode configuration blocks from Brute Ratel Badgers	300
2025-05-09	Ransomware Groups: DragonForce	Outline how DragonForce has evolved from RaaS to a cartel structure	100
2025-05-09	Threat Actors: Akira	Outline Akira's TTPs	100
2025-05-09	Threat Actors: Salt Typhoon – SNAPPYBEE Campaign Analysis	Outline Salt Typhoon's tactics, techniques, and procedures	300

Activity Report Page 16 of 98

Date	Lab	Description	Points Earned
2025-05-09	Threat Modeling: Case Study	Recognize the key elements and principles of threat modeling	300
2025-05-09	Threat Modeling: OWASP Threat Dragon	Identify the features and functionality of the Threat Dragon application	100
2025-05-09	Threat Modeling: Tools	Recognize common tools for threat modeling	40
2025-05-09	Threat Actors: Sandworm Team	Analyze and identify specific TTPs used by Sandworm Team	100
2025-05-09	Threat Actors: OilRig	Analyze and identify specific tactics, techniques, and procedures (TTPs) used by OilRig	100
2025-05-09	Threat Actors: FIN7	Analyze and identify specific TTPs used by FIN7	100
2025-05-09	Threat Actors: APT29	Analyze and identify specific tactics, techniques, and procedures (TTPs) used by APT29	100
2025-05-06	Threat Modeling: Attack Trees	Recognize the basic structure of an attack tree	40
2025-04-29	Threat Modeling: STRIDE	Identify the STRIDE threat categories	40
2025-04-29	Threat Modeling: Methodologies	Recognize threat modelling methodologies	20
2025-04-29	Threat Modeling: Introduction	Recall the benefits and challenges of threat modeling	10
2025-04-23	Find the Flaw: PHP – Software and Data Integrity Failures	Recognize software and data integrity failures in PHP code	20
2025-04-23	Find the Flaw: PHP – Security Misconfigurations	Recognize security misconfiguration vulnerabilities in PHP code	20
2025-04-23	Find the Flaw: PHP – Insecure Design	Recognize insecure design flaws in PHP code	20
2025-04-23	Find the Flaw: Python – Vulnerable and Outdated Components	Recognize the use of vulnerable and outdated components in Python code	20

Activity Report Page 17 of 98

Date	Lab	Description	Points Earned
2025-04-23	Find the Flaw: Python – Software and Data Integrity Failures	Recognize software and data integrity failures in Python code	20
2025-04-23	Find the Flaw: Python – Security Misconfiguration	Recognize security misconfiguration vulnerabilities in Python code	20
2025-04-23	Find the Flaw: Python – Cryptographic Failures	Recognize cryptographic failures in Python code	20
2025-04-23	Find the Flaw: Python – Insecure Design	Recognize insecure design flaws in Python code	20
2025-04-22	Find the Flaw: PHP – Injection	Recognize injection vulnerabilities in PHP code	20
2025-04-22	Find the Flaw: PHP – Identification and Authentication Failures	Recognize identity and authentication failures in PHP code	20
2025-04-21	Find the Flaw: PHP – Cryptographic Failures	Recognize cryptographic failures in PHP code	20
2025-04-21	Find the Flaw: PHP – Broken Access Control	Recognize broken access control vulnerabilities in PHP code	20
2025-04-21	Stack Overflow: Advanced (Theory)	Identify when to use an SEH overflow	100
2025-04-21	Stack Overflow: Intermediate Plus (Theory)	Identify how data is passed into a program	100
2025-04-21	Stack Overflow: Intermediate (Theory)	Identify which common C and C++ functions can be insecure	40
2025-04-21	Infrastructure Hacking: Responder Network Poisoning	Be able to use network poisoning attacks successfully	200
2025-04-16	Introduction to Active Directory Attacks: Overview	Describe the techniques used for active directory attacks	40
2025-04-16	Introduction to Active Directory Attacks: Local Passwords	Retrieve passwords from various sources on standalone Windows systems	100
2025-04-16	Introduction to Active Directory Attacks: Domain Passwords	Retrieve domain passwords from various sources on domain-connected Windows systems	100

Activity Report Page 18 of 98

Date	Lab	Description	Points Earned
2025-04-10	CVE-2025-31161 (CrushFTP): Defensive	Outline how CVE-2025-31161 is used by attackers to achieve code execution	300
2025-04-09	Digital Forensics: LSASS Driver	Use volatility to analyze memory dumps	300
2025-04-09	Digital Forensics: File Carving	Recover deleted files from a disk image using Foremost and Scalpel	200
2025-04-03	Water Gamayun: (CVE-2025-26633) Campaign Analysis	Outline how Water Gamayun used the MSC EvilTwin vulnerability to hide malicious code and deploy malware	300
2025-04-03	Threat Actors: Salt Typhoon	Analyze and identify specific TTPs used by Salt Typhoon	100
2025-04-03	Threat Actors: APT43	Analyze and identify specific TTPs used by APT43	100
2025-04-03	Threat Actors: Lapsus$	Analyze and identify specific TTPs used by Lapsus$	10
2025-04-03	Iranian Threat Groups	Recognize Iranian threat groups and their tools at a high level	20
2025-03-28	CVE-2023-22527: Confluence OGNL RCE – Defensive	Outline how attackers can abuse legitimate processes for malicious means	200
2025-03-28	CVE-2023-23397 (Outlook NTLM relay)	Extract information and indicators of compromise from the malicious EML file	100
2025-03-28	CVE-2022-30190 (Follina) ms-msdt Scheme Abuse – Defensive	Summarize indicators of compromise	200
2025-03-28	CVE-2022-1388 (F5 BIG-IP) – Offensive	Recognize how the CVE-2022-1388 works	200
2025-03-27	Persistence: Component Object Model Hijacking	Apply knowledge of the Windows Registry to pick out IOCs	200
2025-03-24	Creating Quantum Circuits: Random Number Generator	Generate a simple random number using a quantum computer	200
2025-03-24	Creating Quantum Circuits: Grover's Algorithm	Describe what Grover's algorithm is used for	300

Activity Report Page 19 of 98

Date	Lab	Description	Points Earned
2025-03-24	Creating Quantum Circuits: Deutsch-Jozsa Algorithm	Describe what the Deutsch-Jozsa algorithm shows	200
2025-03-24	Creating Quantum Circuits: Bell States	Describe what a bell state is	200
2025-03-24	Quantum Computing Fundamentals: Cryptography	Explain how the fundamental principles of quantum mechanics relate to cryptography	100
2025-03-24	Quantum Computing Fundamentals: Quantum Circuits	Apply quantum gates inside a quantum circuit	200
2025-03-24	Quantum Computing Fundamentals: Quantum Gates	Identify the effects of basic quantum gates	100
2025-03-24	Quantum Computing Fundamentals: What is Quantum Computing?	Explain the basic differences between classical and quantum computing	40
2025-03-24	TypeForge: Code (Intermediate)	Recognize that timed practice and real-time feedback boost typing speed and accuracy	40
2025-03-24	TypeForge: Facts (Intermediate)	Recognize that timed practice and real-time feedback boost typing speed and accuracy	40
2025-03-24	TypeForge: Words (Intermediate)	Recognize that timed practice and real-time feedback boost typing speed and accuracy	40
2025-03-24	TypeForge: Code (Novice)	Recognize that timed practice and real-time feedback boost typing speed and accuracy	20
2025-03-24	TypeForge: Facts (Novice)	Recognize that timed practice and real-time feedback boost typing speed and accuracy	20
2025-03-24	TypeForge: Words (Novice)	Recognize that timed practice and real-time feedback boost typing speed and accuracy	20
2025-03-21	CVE-2024-38112 and CVE-2024-43461 (Windows MSHTML Platform Spoofing): Defensive	Outline how Microsoft HTML is abused to deploy malware	300
2025-03-21	CVE-2024-21413 (MonikerLink) – Defensive	Outline the outlook RCE vulnerability	100
2025-03-21	CVE-2023-7028 (GitLab Account Takeover) – Defensive	Identify the account takeover vulnerability in the GitLab v.16.2.4 server	200

Activity Report Page 20 of 98

Date	Lab	Description	Points Earned
2025-03-21	CVE-2022-26134 (Confluence) – OGNL Injection	Recognize the exploitation of CVE-2022-26134	200
2025-03-21	Real-World Playground: Apache Log4j RCE (CVE-2021-44228)	Recognize the CVE-2021-44228 vulnerability in Apache Log4j allowing RCE on affected systems	100
2025-03-19	GDB: Understanding Debuggers	Gain a fundamental understanding of debuggers	40
2025-03-18	CVE-2021-1675 (PrintNightmare) – Defensive	Understand how to search event logs for CVE-2021-1675 exploit attempts	200
2025-03-18	Infrastructure Hacking: Kerberoasting	Identify and exploit service accounts	200
2025-03-17	Threat Hunting: Investigating a Fake PoC	Identify suspicious code	200
2025-03-17	Threat Hunting: Windows Odd One Out	Identify out of sort processes and artifacts	200
2025-03-12	Threat Research: Power Query Embedded Payloads	Identify misuse of the Microsoft Excel Power Query feature	200
2025-03-12	Threat Research: Webmin 1.900 RCE	Experience using Metasploit to execute public exploits	200
2025-03-10	CVE-2023-22515 (Confluence Server) – Defensive	Outline how attackers can abuse legitimate processes for malicious means	200
2025-03-10	Kerberos: AS-REP Roasting	Demonstrate how to discover accounts that are AS-REP roastable using Rubeus	40
2025-03-10	Kerberos: Kerberoasting	Use Rubeus to discover service principal names (SPNs)	100
2025-03-10	Kerberos: Pass-the-Ticket	Impersonate domain users with a Kerberos ticket	40
2025-03-10	CVE-2022-1388 (F5 BIG-IP) – Defensive	Identify indicators of compromise in F5 BIG-IP logs	200
2025-03-10	CVE-2021-40444 (MSHTML) – Defensive	Identify network traffic related to CVE-2021-40444	100

Activity Report Page 21 of 98

Date	Lab	Description	Points Earned
2025-03-10	Malware Analysis: AutoIt	Analyze malware created with AutoIt	300
2025-03-07	Threat Actors: Mint Sandstorm – Campaign Analysis	Outline the details of Mint Sandstorm's latest campaign	300
2025-03-07	Events & Breaches: Monero Wallet Supply Chain Compromise	Handle PGP and GPG keys to validate software legitimacy	200
2025-03-07	Events & Breaches: Magecart Skimmer	Demonstrate ability to analyze web traffic to identify threats	300
2025-03-07	CVE-2017-5754 (Meltdown)	Demonstrate the Meltdown vulnerability	100
2025-03-06	Events & Breaches: Data Leaks	Recognize the extent of this real-life data leak	300
2025-03-05	Exploitation: Vulnerable WebApps – WordPress	Weaponize access to WordPress	200
2025-03-04	CUPS Remote Code Execution Vulnerability – Defensive	Outline how CUPS servers can be used to achieve remote code execution	200
2025-03-04	Ransomware: Annabelle	Identify signs of Annabelle ransomware infections on a Windows host	300
2025-02-27	UAC-0063 Intrusion: SIEM Analysis	Describe the technical elements of the UAC-0063 intrusion set	300
2025-02-27	The Haunted Hollow: The Cursed Crypt	Recognize encoding techniques used in ciphers	100
2025-02-27	Brute Ratel C4 (BRc4): Yara Detection	Create a Yara rule that detects Brute Ratel C4 malware	100
2025-02-26	APT29 Threat Hunting with Elasticsearch: Additional Collection and Exfiltration	Identify various tactics from the MITRE ATT&CK framework	200
2025-02-26	A Christmas Catastrophe: The Grotto	General knowledge and some fun!	40
2025-02-19	Halloween 2020: Death by Ink	Gain access to an internal network to retrieve the flag	300

Activity Report Page 22 of 98

Date	Lab	Description	Points Earned
2025-02-14	Threat Actors: Peach Sandstorm	Analyze and identify specific TTPs used by Peach Sandstorm	100
2025-02-14	Threat Actors: Wizard Spider	Analyze and identify specific tactics, techniques, and procedures (TTPs) used by Wizard Spider	100
2025-02-11	CVE-2025-0411 (7-ZIP MoTW Bypass): Defensive	Outline how Mark of the Web (MoTW) identifies malicious downloads	300
2025-02-11	Marap	Investigate the initial functionality of malicious software	200
2025-02-10	Human Connection Challenge: Season 1 – Web Exploitation	Demonstrate how to identify and exploit web application vulnerabilities	400
2025-02-06	Python API: Introduction	Explain how to use the Swagger GUI to send requests	20
2025-02-05	Introduction to API Vulnerabilities	Describe an application programming interface (API)	20
2025-02-04	Security Headers: Introduction to Cache-Control	Be aware of the benefits of cache-control	20
2025-02-04	Security Headers: Introduction to Cookies	Recognize the benefits of cookies in relation to security headers	20
2025-02-04	Introduction to Security Headers	Recognize the benefits of enabling security headers	20
2025-01-30	Zero-Day Behavior: PDF Samples	Analyze a PDF that contains abnormal data streams	200
2025-01-29	PowerShell Basics: Demonstrate Your Skills	Creating and editing PowerShell scripts	200
2025-01-29	DDOS Analysis: Demonstrate Your Skills	Understand the mechanics of a DDoS attack and how they appear in logs	200
2025-01-29	DDOS Analysis: UDP Flood	Understand the mechanics of UDP Flood DDoS attacks	100
2025-01-29	Incident Response: Application Shimming	Investigate signs of persistence on a Windows machine	200

Activity Report Page 23 of 98

Date	Lab	Description	Points Earned
2025-01-29	Incident Response: ZWSP Phishing Vulnerability in Office 365	Assemble URLs containing ZWSPs to obfuscate a malicious link	100
2025-01-29	Incident Response: Persistence via Accessibility Features	Exposure to the common vectors actors will use to gain persistence on a host	200
2025-01-28	FIN7 Threat Hunting with Splunk: Demonstrate Your Skills	Understand the techniques used by the FIN7 threat group during an attack	300
2025-01-27	Practical Malware Analysis: Demonstrate Your Skills	Demonstrate a robust methodology for conducting malware analysis	300
2025-01-27	Yara: Demonstrate Your Skills	Create Yara rules to tackle emerging threats	300
2025-01-24	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
2025-01-24	Yara: Modules	Investigate unique data related to malware samples	200
2025-01-23	Introduction To Elastic: Act	Demonstrate how to create a custom query rule in Elastic	200
2025-01-23	Introduction To Elastic: Escalate	Understand the importance of using Elastic in escalating security incidents	100
2025-01-23	Introduction To Elastic: Investigate	Recall the importance of using Elastic in investigating security incidents	100
2025-01-23	Introduction To Elastic: Focus (Detection Rules)	Demonstrate how to gather further information on a pre-defined rule in Kibana	200
2025-01-23	Introduction To Elastic: Focus (Alert Detailing)	Demonstrate how to gather further information on alerts in Kibana	200
2025-01-23	Introduction to Sigma: Custom Field Mapping	Construct a query using a custom field mapping configuration	200
2025-01-23	Introduction to Sigma: Demonstrate Your Skills	Demonstrate how to modify a configuration file	300
2025-01-23	Introduction to Sigma: Sigma Tools	Recall the function of each Sigma tool	200

Activity Report Page 24 of 98

Date	Lab	Description	Points Earned
2025-01-23	Introduction to Sigma: Syntax and Structure	Inspect the contents of Sigma rules written in YAML	40
2025-01-23	Introduction to Sigma: What is Sigma?	Recognize what Sigma is, how it's used, and who it helps	20
2025-01-23	Python: Hardcoded Secrets	Recognize the impact and consequences of using hardcoded secrets	100
2025-01-23	Python: SQL Injection	Explain what an SQL injection vulnerability is and how it works	100
2025-01-23	Yara: Rule Building with Matching Strings	Investigate unique data related to malware samples	200
2025-01-23	Yara: Detecting Evasive Malware	Investigate unique data related to malware samples	200
2025-01-23	Yara: Strings for Rule Creation	Investigate unique data related to malware samples	200
2025-01-23	Yara: Scanning Malicious Files	Investigate unique data related to malware samples	200
2025-01-23	Yara: Regular Expressions	Investigate unique data related to malware samples	200
2025-01-23	Yara: Detecting Cryptographic Strings	Investigate unique data related to malware samples	200
2025-01-22	TLS Fundamentals: TLS 1.3	Identify key differences between TLS 1.3 and prior versions	40
2025-01-22	TLS Fundamentals: X.509 Analysis	Describe how certificates are exchanged during a TLS handshake	100
2025-01-21	S3: Multi-Region Access Points (MRAPs)	Recognize the benefits of S3 object replication	100
2025-01-21	Digital Forensics: MagicBytes	Conduct file header analysis in a forensic context	200
2025-01-17	Threat Hunting: Cowrie Honeypot	Identify techniques used by attackers during SSH sessions	200

Activity Report Page 25 of 98

Date	Lab	Description	Points Earned
2025-01-17	Threat Hunting: Fuzzy Hashing	Discover various methods of analysing files	300
2025-01-15	Introduction to Aircrack-ng: Demonstrate Your Skills	Demonstrate your knowledge of how to use aircrack-ng to investigate and attack wireless networks	300
2025-01-15	Intro to Web App Hacking: Stack Trace	Identify sensitive information in verbose error messages	100
2025-01-14	NSA Kubernetes Hardening: Introduction	Recognize the NSA's recommendations for Kubernetes hardening	10
2025-01-13	ICS Malware: Triton	Be able to reverse engineer py2exe files	200
2025-01-13	IEC 61131-3: PLC Programming	Be able to recognize PLC programs written in IEC-61131-3 languages	100
2025-01-13	Human Machine Interfaces	Understand HMIs and their role in OT and ICS	100
2025-01-13	Programmable Logic Controllers	Configure OpenPLC	200
2025-01-13	PKI (Public Key Infrastructure) Practical	Understand the different parts of PKI and their roles	200
2025-01-13	IoT & Embedded Devices: Binwalk	Extract data from firmware images with Binwalk	200
2025-01-10	Interactive RegEx: Quantifiers	Recall how to use logical operators in regex	200
2025-01-10	Interactive RegEx: Logical Metacharacters	Recall how to match patterns with character sets	100
2025-01-09	Digital Forensics: Mozilla Firefox Artifacts	Practice basic browser forensic techniques	100
2025-01-09	Digital Forensics: Google Chrome Artifacts	Practice and understand basic browser forensic techniques	100
2025-01-08	Introduction to Python Scripting: Demonstrate Your Skills	Demonstrate how to configure environments to write and execute Python scripts	300

Activity Report Page 26 of 98

Date	Lab	Description	Points Earned
2025-01-03	Interactive RegEx: Character Sets	Recall how to match with the metacharacters dot, backslash, and line anchors	40
2025-01-02	Interactive RegEx: Simple Matching	Recall how to match alphanumeric characters in a string	40
2024-12-31	S3: Restricting Access	Recall access restriction mechanisms for S3 buckets and objects	100
2024-12-31	NGINX: Directory Listing	Be able to identify that directory listing is enabled on a web server	40
2024-12-31	Hafnium: China Chopper	Demonstrate ability to use an exploit chain to gain persistence on a web server	200
2024-12-30	Human Connection Challenge: Season 1 – Scanning	Demonstrate how to use scanning tools and techniques to enumerate and connect to targets	400
2024-12-30	PowerShell Basics: Error Handling	Describe the different types of PowerShell errors	100
2024-12-30	PowerShell Basics: ISE and Scripting	Recall how to open PowerShell ISE	100
2024-12-30	PowerShell Basics: Processes and Services	Explain how to find processes and services with PowerShell	100
2024-12-30	Introduction to the AWS Console	Demonstrate service navigation using the AWS console	100
2024-12-30	S3: Practical Introduction	Navigate the AWS Management Console	100
2024-12-30	PowerShell Basics: Remoting	Recall how to create, manage, and remove remote sessions with PowerShell	200
2024-12-30	PowerShell Basics: Event Logs	Recall how to view, filter, and analyze event logs using PowerShell	100
2024-12-30	PowerShell Basics: Functions and Modules	Describe what PowerShell functions and modules are	100
2024-12-24	Kerberos: Enumeration	Recall various techniques to enumerate an Active Directory domain	200

Activity Report Page 27 of 98

Date	Lab	Description	Points Earned
2024-12-24	Infrastructure Pen Testing: Network Enumeration	Recognize how the Nmap tool and its associated arguments work	400
2024-12-24	Infrastructure Hacking: FTP Anonymous Login	Identify and exploit FTP servers that have anonymous login enabled	100
2024-12-24	Persistence: Trap	Apply trap commands that perform custom actions on receiving signals	100
2024-12-24	PoshC2: Enumerating the System	Knowledge of how to utilize the PoshC2 implant	300
2024-12-24	Modern Encryption: RSA	Describe what RSA encryption is, how it works, and why it's crucial in digital security	40
2024-12-24	Infrastructure Hacking: Using SearchSploit	Locate information on exploits using SearchSploit	200
2024-12-23	Stack Overflow: Beginner (Theory)	Identify which common C and C++ functions can be insecure	40
2024-12-23	Offensive PowerShell: Defense Evasion	Recall the cmdlets used to learn information about a Windows firewall configuration	200
2024-12-23	Discovery: Browser Bookmarks	Identify enumeration techniques by analyzing browser bookmark files	100
2024-12-23	Discovery: Enumeration Scripts – Networks and Software	Identify information of interest to an attacker	200
2024-12-23	Discovery: Enumeration Scripts – Introduction	Identify information of interest to an attacker	200
2024-12-23	Netcat: Advanced Features	Experience using Netcat to communicate to other hosts	200
2024-12-23	Intro to Web App Hacking: Command Injection	Practice leveraging web applications to execute arbitrary commands	200
2024-12-20	Reconnaissance: User Enumeration – Scraping Obfuscated Emails	Extract obfuscated emails from websites	200
2024-12-20	Discovery: Active Directory Enumeration	Describe how to obtain info about objects and shares using Veil-PowerView	300

Activity Report Page 28 of 98

Date	Lab	Description	Points Earned
2024-12-20	Scanning: DrupeScan	Practice automated scanning techniques using speciality tools	200
2024-12-19	Microsoft Sentinel Deployment & Log Ingestion: Initial Setup	Recall the deployment process for Microsoft Sentinel	200
2024-12-19	Microsoft Azure Basics: Fundamental Concepts	Know the differences between tenants, subscriptions, and resource groups	10
2024-12-19	Introduction to Microsoft Sentinel	Recall Microsoft Sentinel's features	100
2024-12-19	Microsoft Azure Basics: Storage Accounts	Recall how to create and modify storage accounts	100
2024-12-19	Microsoft Azure Basics: Navigating the Web Portal	Access the Azure web portal	100
2024-12-18	Find the Flaw: C – Cryptographic Failures	Recognize cryptographic failures in C code	20
2024-12-18	Practical Malware Analysis: Ransomware Static Analysis	Identify signs of Maze ransomware infections on a Windows host	200
2024-12-18	Computer Architecture: Demonstrate Your Knowledge	Demonstrate knowledge of computer architecture	100
2024-12-18	Computer Architecture: Introduction to 64-Bit Architectures	Gain a high level understanding of 64-bit architectures	40
2024-12-18	Computer Architecture: Introduction to 32-Bit Architectures	Gain a high-level understanding of 32-bit architectures	40
2024-12-18	Computer Architecture: The Inside of an ELF File	Be able to identify components of an ELF file	40
2024-12-18	Computer Architecture: The Inside of a PE File	Gain a high level understanding of Portable Executables	40
2024-12-18	Computer Architecture: What Is the Stack?	Gain a high level understanding of stack memory	40
2024-12-18	Computer Architecture: What Is the Heap?	Gain a high level understanding of heap memory	40

Activity Report Page 29 of 98

Date	Lab	Description	Points Earned
2024-12-18	Computer Architecture: Introduction to Windows Internals	Gain a high-level understanding of the Windows operating system's inner workings	40
2024-12-18	Computer Architecture: An Introduction to Linux Internals	Gain a high level understanding of the Linux operating system's inner workings	40
2024-12-18	Computer Architecture: ELF Execution Structure	Discover the internals of an ELF executable structure	200
2024-12-17	PowerShell Basics: Operators and Expressions	Explain what PowerShell operators are	100
2024-12-17	PowerShell Basics: Variables	Describe what PowerShell variables are	100
2024-12-17	AWS Logging and Monitoring: Introduction to CloudTrail	Identify the core features of AWS CloudTrail	20
2024-12-17	AWS Lambda: Introduction to Serverless Functions on AWS	Describe how Lambda provides Function as a Service	20
2024-12-17	AWS: Introduction to Elastic Cloud Compute (EC2)	Describe AWS EC2 and the features it offers	20
2024-12-17	AWS: Introduction to AWS Identity and Access Management (IAM)	Describe the features offered by IAM for access management	20
2024-12-17	AWS: Introduction to Simple Storage Service (S3)	Identify the features of S3 and how it provides secure storage services	20
2024-12-17	AWS: Introduction to Amazon Web Services (AWS)	Describe what AWS is and the cloud services it offers	10
2024-12-17	Splunk: Malicious Account Creation	Identify and recognize malicious events in system logs	200
2024-12-17	PowerShell Basics: Cmdlets	Explain what PowerShell cmdlets are	100
2024-12-16	Secrets Management: Secret Lifecycle	Identify the stages of a secret's lifecycle	20
2024-12-16	Secrets Management: Implementation	Describe key secrets management concepts	20

Activity Report Page 30 of 98

Date	Lab	Description	Points Earned
2024-12-16	Secrets Management: Introduction	Identify what a secret is	20
2024-12-16	Secrets Management: How Secrets Leak	Identify the causes of secret leakage	20
2024-12-16	Git Security: What are Version Control Systems?	Recall what version control is	20
2024-12-16	Git Security: SSH Keys	Recall why SSH keys are used	40
2024-12-16	Git Security: Public and Private Repositories	Recall when to create a public or private Git repository	100
2024-12-16	Git Security: Introduction to Git	Identify the correct commands to create and commit to Git repositories	100
2024-12-16	Web Log Analysis: The Tomcat's Out Of The Bag	Identify evidence of a compromise in web server logs	300
2024-12-16	Web Log Analysis: 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
2024-12-06	Immersive Care: Reverse Engineering	Develop critical thinking	300
2024-12-06	DFIR CTF: Malware Memory	Demonstrate your ability to capture the flag with no guidance	300
2024-12-05	TypeLib: COM Persistence	Outline malicious use cases for COM objects and monikers to abuse the Windows registry	200
2024-12-04	DEEP GOSU Campaign: Analysis	Outline the ingress vectors used by Kimusky to deliver malware during the GOSU campaign	300
2024-12-04	BlackCat WinSCP ISO Trojan: Analysis	Analyze the BlackCat Trojan	200
2024-12-04	GOOTLOADER Downloader: Analysis	Extract indicators of compromise from a GOOTLOADER infection chain	300
2024-11-25	Tuoni 101: Payloads	Describe what a Tuoni payload is	100

Activity Report Page 31 of 98

Date	Lab	Description	Points Earned
2024-11-25	Tuoni 101: Listeners	Describe what a Tuoni listener is	100
2024-11-25	Tuoni 101: What is Tuoni?	Identify the core features of Tuoni	20
2024-11-25	Secure Testing: Sitemaps & Robots.txt	Identify potential sitemap and robots.txt risks in web applications, adding to your suite of QA tests	40
2024-11-25	SQLite3: An Introduction	Practice querying an SQLite database file from the command line	100
2024-11-22	CVE-2024-0012 and CVE-2024-9474 (Palo Alto PAN-OS) – Defensive	Describe how attackers and offensive teams can use public PoC code to exploit a vulnerable Palo Alto PAN-OS server	200
2024-11-18	Introduction to Kubernetes	Recognize the fundamental concepts of Kubernetes	40
2024-11-18	Kubernetes: Multi-Container Pods	Recognize how Kubernetes resources are grouped and accessed	200
2024-11-15	Threat Hunting: Analyzing Malicious Python Packages	Interact with a Python Package Index server	200
2024-11-13	Human Connection Challenge: Season 1 – Basic OS Skills	Demonstrate how to use various Linux and Windows command line tools	300
2024-11-13	NCSC Cloud Security: Secure Use of the Service	Describe the importance of securely using a cloud service as per NCSC guidelines	20
2024-11-13	NCSC Cloud Security: Audit Information for Users	Recognize the role audit information plays in cloud security	20
2024-11-13	NCSC Cloud Security: Secure Service Administration	Recall the recommendations for secure service administration from NCSC	20
2024-11-13	NCSC Cloud Security: External Interface Protection	Recognize how to protect external interfaces within cloud environments	20
2024-11-13	NCSC Cloud Security: Secure User Management	Recognize the importance of secure user management as detailed by NCSC	20
2024-11-13	NCSC Cloud Security: Supply Chain Security	Recognize the importance of supply chain security according to NCSC	20

Activity Report Page 32 of 98

Date	Lab	Description	Points Earned
2024-11-13	NCSC Cloud Security: Secure Development	Recall the importance of secure development in cloud	20
2024-11-13	NCSC Cloud Security: Personnel Security	Recognize why personnel security is important in cloud environments	20
2024-11-13	NCSC Cloud Security: Operational Security	Recall the elements NCSC recommends understanding within a cloud provider's OPSEC	20
2024-11-13	NCSC Cloud Security: Governance Framework	Identify how governance fits in with implementation cloud solutions according to NCSC	20
2024-11-13	NCSC Cloud Security: Separation Between Users	Recall why user separation is important in cloud environments	20
2024-11-13	NCSC Cloud Security: Asset Protection and Resilience	Describe the concerns of asset protection and resilience for cloud environments as per the NCSC guidelines	20
2024-11-13	NCSC Cloud Security: Identity and Authentication	Recognize identity and authentication management and its importance within cloud environments	20
2024-11-13	NCSC Cloud Security: Data in Transit	Recall the ways in which data can be protected while it's in transit, according to NCSC	20
2024-11-13	NCSC Cloud Security: Introduction	Recognize NCSC's Cloud Security Guidance at a high level	10
2024-11-13	Threat Research: What is Cyber Threat Intelligence?	A basic understanding of Cyber Threat Intelligence’s core areas	40
2024-11-13	Threat Research: ASD Essential Eight	Practice securing a system against Microsoft Office macros	100
2024-11-01	Return to Haunted Hollow: Encryption Enigma	Demonstrate encryption and decryption basics	200
2024-11-01	OpenSCAP: Workbench	Recall the function of SCAP Workbench and its applications	100
2024-11-01	What is OpenSCAP?	Describe what OpenSCAP is and how it works	20
2024-11-01	What is SCAP?	Describe the SCAP standard and its applications	20

Activity Report Page 33 of 98

Date	Lab	Description	Points Earned
2024-11-01	SQLi Basics: Basic SQL Injection	Construct SQL injection payloads	100
2024-10-31	Practical Malware Analysis: Splunk Log Analysis	Identify signs of Maze ransomware infections on a Windows host	100
2024-10-31	Tickler Malware: Analysis	Demonstrate runtime analysis of the latest malicious threats	200
2024-10-31	Practical Malware Analysis: HOPLIGHT	Demonstrate runtime analysis of the latest malicious threats	200
2024-10-30	Windows Exploitation: LOLBins	Be able to use LOLBins by spawning a child process via a specified binary	300
2024-10-30	Practical Malware Analysis: Network Simulation	Demonstrate an understanding of the INetSim application for malware analysis	200
2024-10-29	Fortinet's Next-Generation Firewall: Intro to Fortigate	Recall Fortinet's firewall products	40
2024-10-28	Return to Haunted Hollow: PCAP Pandemonium	Demonstrate Wireshark skills	100
2024-10-22	Return to Haunted Hollow: Phishing for Treats	Identify how to spot the eerie signs that reveal a phishing email	20
2024-10-17	IoCs and TTPs: Demonstrate Your Skills	Identify adversarial tactics, techniques, and procedures	100
2024-10-17	IoCs and TTPs: Management	Describe how to manage IoCs and TTPs once they're obtained	40
2024-10-17	IoCs and TTPs: Extracting and Identifying	Outline how to identify adversarial tactics, techniques, and procedures	40
2024-10-17	IoCs and TTPs: What are TTPs?	Outline what tactics, techniques, and procedures are	40
2024-10-17	IoCs and TTPs: What are IoCs?	Recall the aspects that make up an IoC	20
2024-10-09	Privilege Escalation: Linux – Identifying Privilege Escalation Vulnerabilities	Recall where to look for privilege escalation vulnerabilities on a Linux system	100

Activity Report Page 34 of 98

Date	Lab	Description	Points Earned
2024-10-09	Privilege Escalation: Linux – Automated Enumeration	Describe what tools can be used to enumerate a Linux system for privilege escalation vulnerabilities	200
2024-10-09	Privilege Escalation: Linux – Introduction	Describe what privilege escalation is	100
2024-10-08	GhostEngine: Analysis	Describe the unique execution flow used in the GhostEngine campaign	200
2024-10-08	CVE-2018-16858 (LibreOffice Remote Code Execution)	Identify commands in python script	200
2024-10-08	What is a CVE?	Basic understanding of what CVEs are and why you should care	10
2024-10-07	Post Exploitation With Metasploit: Working With Workspaces	Describe what workspaces are	100
2024-10-03	Post Exploitation With Metasploit: Database Configuration	Explain how to configure a PostgreSQL database	100
2024-10-02	Mobile Application Security Fundamentals: OWASP Mobile Application Security Verification Standard	Recall the concepts of the OWASP Mobile Application Security Verification Standard	40
2024-10-02	Mobile Application Security Fundamentals: OWASP Mobile Application Security Testing Guide	Recall the concepts of the OWASP Mobile Application Security Testing Guide	40
2024-10-02	Mobile Application Security Fundamentals: Insufficient Binary Protections	Recall the fundamental concepts of insufficient binary protections	20
2024-10-02	Mobile Application Security Fundamentals: Insecure Data Storage	Recall the fundamental concepts of insecure data storage	20
2024-10-02	Mobile Application Security Fundamentals: Insecure Communication	Recall the fundamental concepts of insecure communication	20
2024-09-30	CVSS v4.0	Outline how CVSS v4 is used to score the severity of vulnerabilities	10
2024-09-30	APT29 Threat Hunting with Splunk: Rapid Collection and Exfiltration	Identify various tactics from the MITRE ATT&CK framework	200
2024-09-30	CVSS Calculator	Calculate CVSS scores for given vulnerabilities	300

Activity Report Page 35 of 98

Date	Lab	Description	Points Earned
2024-09-26	Introduction to Python Scripting: Log Analysis and Anomaly Detection with Python	Be able to describe log analysis concepts	300
2024-09-26	Introduction to Python Scripting: Web Scraping	Explain the fundamentals of web scraping, including its purpose and ethical considerations	100
2024-09-26	Introduction to PowerShell Deobfuscation: Introduction	Recall what PowerShell is and what it's used for	20
2024-09-26	Windows Sysinternals: Process Monitor	Demonstrate an ability to use Process Monitor	200
2024-09-25	Hack Your First Web App: Demonstrate Your Skills	Recognize the stages you need to follow when attempting to find and exploit vulnerable systems	300
2024-09-25	Hack Your First Web App: High-Risk Vulnerabilities	Recall how a vulnerability could be categorized as high risk	200
2024-09-25	Hack Your First Web App: Medium-Risk Vulnerabilities	Recall how a vulnerability could be categorized as medium-risk	100
2024-09-25	Hack Your First Web App: Low-Risk Vulnerabilities	Recall how a vulnerability could be categorized as low-risk	200
2024-09-23	Discovery: Windows System Enumeration	Experience enumerating users, patch levels, and password policy on Windows OS	200
2024-09-20	Foundational Static Analysis: Calling Conventions and Register Flow	Gain familiarity with the internals of malware from an assembly perspective	200
2024-09-20	Foundational Static Analysis: API Analysis	Perform analysis to identify potential API calls within malware samples	200
2024-09-19	CVE-2024-1086 (Linux nf_tables Privilege Escalation) Elastic Analysis – Defensive	Outline a use-after-free vulnerability in the Linux kernel	300
2024-09-19	CVE-2024-1086 (Linux nf_tables Privilege Escalation) – Offensive	Outline a use-after-free vulnerability in the Linux kernel	300
2024-09-19	CVE-2024-1086 (Linux nf_tables Privilege Escalation) Splunk Analysis – Defensive	Outline a use-after-free vulnerability in the Linux kernel	300
2024-09-19	CVE-2024-24576 (Rust RCE)	Outline the components that allow the vulnerability to be exploited	200

Activity Report Page 36 of 98

Date	Lab	Description	Points Earned
2024-09-18	CVE-2024-30051 (Windows DWM Core Library Elevation of Privilege): Defensive	Outline how complex heap-based buffer overflows work against the Windows DWM Core Library	300
2024-09-18	CVE-2024-23692 (Rejetto HFS Template Injection) – Defensive	Outline how CVE-2024-23692 is exploited	100
2024-09-18	CANBus: In The Rear-View Mirror	Identify areas of the theoretical knowledge that you may need to revisit	100
2024-09-18	CANBus: SocketCAN	Be able to describe SocketCAN and how it enables intuitive interaction with CAN devices	40
2024-09-18	CANBus: Messaging	Demonstrate an understanding of the CANBus message concepts and formats	100
2024-09-17	Linux Exploitation: Demonstrate Your Knowledge	Demonstrate an understanding of Linux exploitation processes and tools	40
2024-09-17	Mitre ATT&CK for ICS	Use MITRE ATT&CK to map ICS threats and attacks to a common framework	100
2024-09-17	Operational Technology Fundamentals: Common Threats and Vulnerabilities	Identify common threats and vulnerabilities relating to operational technology	40
2024-09-17	Operational Technology Fundamentals: SCADA and DCS	Differentiate between SCADA and DCS systems, including their primary purposes and architectures	40
2024-09-17	Linux Exploitation: Tooling	Understand what types of tools are commonly used within exploit development	40
2024-09-17	Linux Exploitation: The Exploit Development Process	Understand how the exploit development process generally functions	40
2024-09-17	Linux Exploitation: What is Linux Exploitation?	Outline what software exploitation is and why it can be a powerful tool	40
2024-09-17	Kerberos: What is Kerberos?	Recognize the fundamentals of the Kerberos protocol	40
2024-09-16	CANBus: Threat Models	Recognize how threat models aid in analyzing CANBus security	20
2024-09-16	CANBus: Systems	Demonstrate an understanding of how CANBus systems are constructed and what they are connected to	40

Activity Report Page 37 of 98

Date	Lab	Description	Points Earned
2024-09-16	CANBus: An Introduction	Demonstrate an understanding of CANBus concepts	20
2024-09-10	Introduction to Aircrack-ng: Cracking Network Encryption Keys	Recall the different methods of cracking network encryption keys with Aircrack-ng	100
2024-09-10	Introduction to Aircrack-ng: ARP Request Replay Attacks with Aireplay	Recall how an ARP request replay attack works	200
2024-09-10	Introduction to Aircrack-ng: Deauthentication Attacks with Aireplay	Recall how to connect to a target access point	100
2024-09-10	Introduction to Aircrack-ng: Sniffing for Wireless Networks with Airodump	Recall how to use airodump-ng to discover networks and connect to them	100
2024-09-10	Introduction to Aircrack-ng: Configuring Network Interfaces with Airmon	Recall what monitor mode is	100
2024-09-10	Introduction to Aircrack-ng: Packet Injection with Aireplay	Recall what packet injection is	40
2024-09-09	Introduction to Aircrack-ng: What is Aircrack-ng?	Summarize what Aircrack-ng is	40
2024-09-06	Linux Stack Overflow: Introduction	Describe the history of stack overflow vulnerabilities	40
2024-09-06	Discovery: SMTP User Enumeration	Enumerate an SMTP server	200
2024-09-03	Introduction to Python Scripting: Building an IDS with Python	Explain what an IDS is, including its purpose and significance in cybersecurity	300
2024-09-03	Introduction to Python Scripting: Network Basics with Python	Recall how servers manage incoming connections and how clients start requests on a network	200
2024-08-30	Introduction to Velociraptor: Demonstrate Your Skills	Demonstrate how to use the Velociraptor tool	200
2024-08-29	LaZagne	Recall how LaZagne interacts with different types of applications	200
2024-08-29	Credential Access: Password Hashing Algorithms	Recall several common hashing algorithms used for securing passwords	100

Activity Report Page 38 of 98

Date	Lab	Description	Points Earned
2024-08-26	Black Hat 2019: Binee	Identify API calls using binee	100
2024-08-23	Nmap: Demonstrate Your Skills	Apply knowledge of Nmap to enumerate target systems	200
2024-08-23	Packet Analysis: Demonstrate Your Skills	Demonstrate the skills acquired through the beginner Wireshark labs	400
2024-08-23	Infrastructure Hacking: Demonstrate Your Skills – Attacking Network Protocols	Identify and exploit misconfigured services	200
2024-08-22	PA Toolkit	Familiarization with PA Toolkit	200
2024-08-21	Zeek: Scripting	Identify the fundamental components of the Zeek scripting engine	100
2024-08-21	Mobile Malware: Apktool	Describe how Apktool can be used	300
2024-08-20	Threat Actors: Onyx Sleet	Analyze and identify specific TTPs used by Onyx Sleet	100
2024-08-20	Threat Actors: Water Sigbin	Analyze and identify specific TTPs used by Water Sigbin	100
2024-08-20	Threat Actors: LightBasin	Analyze and identify specific TTPs used by LightBasin	100
2024-08-20	Threat Actors: Earth Krahang	Analyze and identify specific TTPs used by Earth Krahang	100
2024-08-20	Threat Actors: Volt Typhoon	Analyze and identify specific TTPs used by Volt Typhoon	100
2024-08-20	Threat Actors: Scattered Spider	Analyze and identify specific TTPs used by Scattered Spider	100
2024-08-20	Threat Actors: Lazarus	Analyze and identify specific tactics, techniques, and procedures (TTPs) used by Lazarus	100
2024-08-20	DarkSide: Overview	Be able to demonstrate a basic understanding of the DarkSide ransomware group	40

Activity Report Page 39 of 98

Date	Lab	Description	Points Earned
2024-08-19	WinDbg: Getting Started and the Workspace	Use WinDbg to analyze a Windows binary	200
2024-08-16	Python Scripting for Malware Analysis: Introduction	Introduce the role and significance of Python in malware analysis and reverse engineering	40
2024-08-16	C++: Introduction	Gain an understanding of how to use C++ beginner labs	40
2024-08-16	Introduction to Active Directory Attacks: Basic Hunting with BloodHound	Find the shortest path to high value targets	200
2024-08-16	Password Spraying	Execute a password spraying attack against a web application	200
2024-08-16	Mobile Malware: MobSTSPY	Explain what MobSTSPY is	200
2024-08-15	Events & Breaches: Data Exposure	Practice using IRC and interact with bots	100
2024-08-14	Ransomware: AstraLocker	Identify signs of AstraLocker ransomware infections on a Windows host	300
2024-08-14	Ransomware: BlackRouter	Experience with basic malware analysis	200
2024-08-14	Digital Forensics: Bulk Extractor	Practice using the Bulk Extractor tool to retrieve sensitive information	200
2024-08-13	Ransomware: LockerGoga	Practice analyzing ransomware memory samples	200
2024-08-12	Ransomware: Maze	Identify signs of Maze ransomware infections on a Windows host	200
2024-08-12	Ransomware: Anatova	Exposure to the Anatova ransomware	200
2024-08-09	Ransomware: Zeppelin	Identify signs of Zeppelin ransomware infections on a Windows host	300
2024-08-09	Ransomware: Ranzy Locker	Recognize the effects of Ranzy Locker and identify elements to report	100

Activity Report Page 40 of 98

Date	Lab	Description	Points Earned
2024-08-09	Ransomware: Cr1pT0r ARM	Investigate ARM ransomware using static-code analysis	300
2024-08-09	Ransomware: TeslaCrypt	Practice analyzing malware and extracting key information	300
2024-08-08	Windows Hardening: Initial Access	Recognize the importance of hardening public-facing applications	400
2024-08-08	Windows Hardening: Reconnaissance	Analyze penetration testing reports	300
2024-08-08	Windows Hardening: Introduction	Recall the different sections of a pen test report, what they include, and why they're important	200
2024-08-08	Ransomware: Ryuk	Identify signs of Ryuk ransomware infections on a Windows host	100
2024-08-08	Ransomware: WannaCry	Identify signs of WannaCry ransomware infections on a Windows host	300
2024-08-08	Ransomware: Dharma	Identify signs of Dharma ransomware infections on a Windows host	300
2024-08-08	Ransomware: StalinLocker/StalinScreamer	Analyze the StalinLocker malware source code	200
2024-08-07	Ransomware: Darkside	Identify signs of DarkSide ransomware infections on a Windows machine	300
2024-08-07	Ransomware: Snake	Observe Snake ransomware safely	100
2024-08-07	Ransomware: Ragnar Locker	Identify malware in a VDI	200
2024-08-07	Ransomware: Sodinokibi	Identify signs of Sodinokibi ransomware infections on a Windows host	200
2024-08-06	Practical Malware Analysis: Steganographic Malvertising	Describe how malicious actors exploit adverts	40
2024-08-05	Introduction to Velociraptor: Client Monitoring	Recognize how and when to use Velociraptor	100

Activity Report Page 41 of 98

Date	Lab	Description	Points Earned
2024-08-02	Ransomware: Conti	Identify signs of Conti ransomware infections on a Windows host	300
2024-07-30	Introduction to Python Scripting: Network Reconnaissance with Python	Describe networking concepts in Python	200
2024-07-30	DEFCON 2023: RDP Tradecraft	Analyze captured RDP sessions using RDP Player to identify potential indicators of compromise and understand threat actor techniques	100
2024-07-30	Protocols: HL7	Analyze and interpret HL7 data within a PCAP file, demonstrating an understanding of the structure and function of HL7 messages transmitted over MLLP	200
2024-07-29	Introduction to Python Scripting: Setting up the Environment	Describe the basics of Python scripting and its applications in automation	100
2024-07-29	The Haunted Hollow: The Gatekeepers	Demonstrate how to recover data from barcodes	20
2024-07-29	Digital Forensics: DDE Analysis	Investigate different ways malware achieves execution after initial access	200
2024-07-26	Privilege Escalation: Windows – Finding Passwords	Describe how to use the Windows command line to find files containing credentials for privilege escalation	200
2024-07-26	Vulnerable Components: Ghostscript (CVE-2018-16509)	Know the fundamentals of the Ghostscript image-processing vulnerability	200
2024-07-25	Wizard Spider DFIR: Enumeration	Recognize techniques used by Wizard Spider during an attack	200
2024-07-25	Wizard Spider DFIR: Network Traversal	Recognize the techniques used by the Wizard Spider threat group during an attack	200
2024-07-25	Wizard Spider DFIR: Compromise Assessment	Recognize the techniques used by the Wizard Spider threat group during an attack	200
2024-07-25	What is the Zed Attack Proxy (ZAP)?	Identify the key features of an intercepting proxy and how it's used in security testing	20
2024-07-25	Secure Tooling: Nikto	Be able to run a Nikto scan to perform a security scan of a web application	40
2024-07-24	Deepfakes	Discuss the impact deepfakes can have on businesses	40

Activity Report Page 42 of 98

Date	Lab	Description	Points Earned
2024-07-24	Find the Flaw: Python – Injection	Recognize injection vulnerabilities in Python code	20
2024-07-24	Find the Flaw: Python – Identity and Authentication Failures	Recognize identity and authentication failures in Python code	20
2024-07-24	Find the Flaw: Python – Broken Access Control	Recognize broken access control vulnerabilities in Python code	20
2024-07-24	Threat Actors: Storm-0978	Analyze and identify specific TTPs used by Storm-0978	100
2024-07-24	Exploitation: Vulnerable WebApps – XSS	Recall how cross-site scripting vulnerabilities can affect web applications	200
2024-07-24	Weaponization: Payloads – Basics	Recall what a payload is and where it is used	20
2024-07-24	Digital Forensics: Ubuntu Image Analysis	Investigate and analyze operating systems using common forensic techniques	400
2024-07-18	CVE-2022-41049 (ZippyReads) – Offensive	Identify vulnerable versions of Windows	100
2024-07-18	Ransomware: MegaCortex	Demonstrate ability to analyze ransomware using Splunk and Sysmon	200
2024-07-15	Reconnaissance: WHOIS Service – Basics	Demonstrate an understanding of the WHOIS service by answering the questions	40
2024-07-12	CTI First Principles: Demonstrate Your Knowledge	Describe cyber threat intelligence fundamentals	100
2024-07-12	CTI First Principles: Models and Methodologies	Compare different models of CTI and their applications	40
2024-07-12	CTI First Principles: Decomposition and Visualization	Recognize techniques for breaking down complex information	40
2024-07-12	CTI First Principles: Threat Intelligence Sources	Outline what sources are available for gathering and enriching threat intelligence	40
2024-07-12	CTI First Principles: Threat Actors and Attribution	Outline what threat actors are and how they are attributed to incidents	100

Activity Report Page 43 of 98

Date	Lab	Description	Points Earned
2024-07-12	CTI First Principles: Lifecycles	Outline the components of the intelligence cycle	20
2024-07-12	CTI First Principles: What is Cyber Threat Intelligence?	Outline the relationship between data, information, and intelligence	10
2024-07-12	Introduction To Elastic: Triage	Understand the importance of using Elastic in triaging security incidents	100
2024-07-12	Introduction To Elastic: Querying Data	Understand the importance of using Elastic when investigating security incidents	200
2024-07-12	Introduction To Elastic: What is Elastic?	Recall what the Elastic stack is	40
2024-07-11	Nmap: Scan Optimization	Describe Nmap's scan optimization techniques and options	100
2024-07-11	Nmap: Port Scanning	Describe what port scanning is	100
2024-07-11	Nmap: Host Discovery	Describe Nmap's default host discovery options	100
2024-07-11	Nmap: Intro to Nmap	Explain what nmap is	40
2024-07-11	Operational Technology Fundamentals: Purdue Model for ICS – Enterprise Zone	Identify what devices sit in the Enterprise Zone of the Purdue Model	10
2024-07-11	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
2024-07-11	Operational Technology Fundamentals: IT, OT, ICS, and Embedded Devices	Describe the differences in technologies used for IT and OT	20
2024-07-11	Digital Forensics: File Systems	Review and interpret the function of the Master Boot Record	300
2024-07-11	Nmap: Scripting	Describe what NSE is	200
2024-07-11	Nmap: OS and Version Detection	Describe what enumeration scans Nmap has available	100

Activity Report Page 44 of 98

Date	Lab	Description	Points Earned
2024-07-10	Autopsy: Demonstrate Your Skills	Demonstrate the skills you've gained in the Autopsy collection	300
2024-07-10	Browser Developer Tools: Inspect Element	Recognize the benefits of using Inspect Element	20
2024-07-10	Browser Developer Tools: Storage Inspector and Cookies (Firefox)	Recognize the benefits of using the Storage Inspector in Firefox	20
2024-07-10	Browser Developer Tools: Application and Cookies (Chrome)	Recognize the benefits of using the Application tab in Chrome	20
2024-07-10	Introduction to Browser Developer Tools	Recognize the benefits of using browser developer tools	10
2024-07-10	Browser Developer Tools: Network (Firefox)	Recognize the benefits of using the Network panel in Firefox	20
2024-07-10	Browser Developer Tools: Network (Chrome)	Recognize the benefits of using the Network panel in Chrome	40
2024-07-10	Browser Developer Tools: Console and JavaScript Execution	Identify the console panel within the browser developer tools	20
2024-07-09	Intro to Web App Hacking: Introduction to OWASP ZAP	Employ OWASP ZAP to analyze the web app	300
2024-07-08	Introduction to Metasploit: Post-Exploitation	Recall how to select and launch post-exploitation modules against a target host	200
2024-07-08	Introduction to Metasploit: Meterpreter	Recognize common Meterpreter features	200
2024-07-08	Introduction to Metasploit: Payloads	Recognize how to identify appropriate Metasploit payloads for a target system	100
2024-07-08	Introduction to Metasploit: Exploits	Identify appropriate Metasploit exploit modules	100
2024-07-08	Introduction to Metasploit: Enumeration	Recognize how enumeration modules can help gather information on a target	100
2024-06-28	Hack Your First PC: Demonstrate Your Skills	Demonstrate the ability to scan a Linux host with Nmap	300

Activity Report Page 45 of 98

Date	Lab	Description	Points Earned
2024-06-28	Introduction to Metasploit: Discovery	Recall how msfconsole modules can be used to scan and identify a target	100
2024-06-28	Introduction to Metasploit: Modules	Demonstrate how to start msfconsole	100
2024-06-28	Introduction to Metasploit: What is Metasploit?	Recognize the fundamentals of Metasploit	20
2024-06-28	Introduction to Mimikatz	Describe how to extract passwords in Windows using Mimikatz	200
2024-06-26	Packet Analysis: Malware Traffic	Recognize useful starting points for analysts when viewing network traffic	200
2024-06-26	Wireshark: Demonstrate Your Skills	Identify relevant network traffic using Wireshark	300
2024-05-09	Hack Your First PC: Privilege Escalation	Recall potential ways of discovering system vulnerabilities	200
2024-05-09	Hack Your First PC: Gaining Access	Identify potential access vectors on a remote system	200
2024-05-09	Hack Your First PC: Brute Force	Recall the difference between a brute-force attack and a dictionary attack	200
2024-05-09	Hack Your First PC: Scanning for Targets	Recall how to use Nmap to scan computer systems	200
2024-05-09	Hack Your First PC: Kali Linux	Navigate the Kali Desktop environment	200
2024-05-09	Hack Your First PC: Ozone Energy	Recognize the stages you need to follow when attempting to find and exploit vulnerable systems	200
2024-04-30	Staying Safe Online: Phishing Emails (US)	Recognize the main characteristics of phishing emails	20
2024-04-16	Introduction to Velociraptor: Searching	Recognize how and when to use Velociraptor	100
2024-04-16	Introduction to Velociraptor: VQL	Identify VQL structure using Velociraptor	100

Activity Report Page 46 of 98

Date	Lab	Description	Points Earned
2024-04-16	Introduction to Velociraptor: Getting Started	Identify event log structure using Velociraptor	100
2024-04-16	Introduction to Velociraptor: Triage	Recognize how and when to use the Velociraptor tool	100
2024-04-16	Introduction to Velociraptor: NTFS	Recognize how and when to use Velociraptor	100
2024-04-11	Autopsy: Media and Audio-Visual Data	Demonstrate how to search media in an Autopsy case	200
2024-04-11	Autopsy: Applications and Mobile	Demonstrate how to investigate installed programs and apps using Autopsy	200
2024-04-11	Autopsy: Email and Messages	Demonstrate how to recover emails with Autopsy	200
2024-04-11	Autopsy: Case Report	Demonstrate verbose tagging in Autopsy	100
2024-04-11	Autopsy: Timeline	Identify forensics evidence using Autopsy's timeline view	200
2024-04-11	Malware Analysis: Tracking a LOLBins Campaign – Infection	Analyze malicious network connections	200
2024-04-09	Autopsy: Web and Browsers	Demonstrate the ability to analyze browser information and search history in Autopsy	100
2024-04-09	Autopsy: Files and Volumes	Demonstrate how to navigate files, volumes, and the information they hold using Autopsy	100
2024-04-09	Python: Code Comments	Have an awareness of the impact and consequences of leaving sensitive details in code comments	40
2024-04-05	Introduction to Velociraptor: What is Velociraptor?	Recall what Velociraptor is and how it's used to aid DFIR investigations	20
2024-04-03	ISO 28000: Application and Compliance	Outline what the PDCA model is	10
2024-04-03	APT29 Threat Hunting with Elasticsearch: Clean-up and Reconnaissance	Identify various tactics from the MITRE ATT&CK framework	200

Activity Report Page 47 of 98

Date	Lab	Description	Points Earned
2024-04-02	Hack Your First Web App: Enumeration	Identify the different web content scanning tools available to a penetration tester	200
2024-04-02	Hack Your First Web App: Ozone Energy	Recognize the necessary steps for finding and exploiting vulnerable systems	200
2024-03-29	Packet Analysis: Device Information	Recognize useful starting points for analysts when viewing network traffic	200
2024-03-28	Active Directory Basics: Demonstrate Your Skills	Interact with and modify objects in a directory database	300
2024-03-28	Active Directory Basics: Managing Workstations	Explain how to find configuration details	100
2024-03-28	Active Directory Basics: Replication	Describe what Active Directory replication is	40
2024-03-28	Active Directory Basics: Group Policy Management	Explain what a Group Policy Object is	100
2024-03-28	Active Directory Basics: NTLM vs Kerberos	Explain why authentication protocols are essential in an Active Directory environment	40
2024-03-28	Active Directory Basics: Adding a Machine	Explain how to configure network settings for a DNS server	100
2024-03-28	Active Directory Basics: Objects	Describe what AD objects are	100
2024-03-27	Device Security: Demonstrate Your Knowledge	Demonstrate an understanding of what device security is	10
2024-03-27	Windows Exploitation: Demonstrate Your Knowledge	Demonstrate an understanding of Windows exploitation processes and tools	40
2024-03-27	Tactics: Demonstrate your Knowledge	Demonstrate your understanding of tactics in the MITRE ATT&CK® framework	40
2024-03-27	Windows Exploitation: Tooling and Languages	List the tools used to perform Windows Exploitation	40
2024-03-27	Windows Exploitation: Types of Common Vulnerabilities	Recall the differences between common Windows vulnerabilities	40

Activity Report Page 48 of 98

Date	Lab	Description	Points Earned
2024-03-27	Windows Exploitation: What is Windows Exploitation?	Define what Windows exploitation entails	40
2024-03-27	Tactics: Exfiltration	Recognize the purpose of the MITRE ATT&CK® Exfiltration tactic	20
2024-03-27	Tactics: Impact	Be able to explain the purpose of the MITRE ATT&CK® Impact tactic	20
2024-03-27	Tactics: Collection	Recognize the purpose of the MITRE ATT&CK® Collection tactic	20
2024-03-27	Tactics: Command and Control	Recognize the purpose of the MITRE ATT&CK® Command and Control tactic	20
2024-03-27	Tactics: Lateral Movement	Recognize the MITRE ATT&CK® Lateral Movement tactic and its purpose	20
2024-03-27	Malicious Document Analysis: Introduction to Malicious Documents	Identify different file structures used to create malicious documents	200
2024-03-27	Malicious Document Analysis: Visual Basic for Applications (VBA)	Use oletools to extract and analyze malicious VBA	300
2024-03-26	Device Security: Case Studies	Understand the concept of device security and its importance	10
2024-03-26	Device Security: Increasing Your Protection	Understand the steps you should take to protect your devices in the office and when working in public places	10
2024-03-26	Device Security: What is Device Security?	Understand the concept of device security and its importance	10
2024-03-26	Threat Hunt Theory: Demonstrate Your Skills	Understand the fundamental concepts of threat hunting	100
2024-03-26	Threat Hunt Theory: Emulating Adversaries	Recognize how emulating adversaries is beneficial in threat hunting	40
2024-03-26	Threat Hunt Theory: Targeted Hunting Integrating Threat Intelligence	Recognize how the Targeted Hunting integrating Threat Intelligence methodology is used in threat hunting	40
2024-03-26	Threat Hunt Theory: Management, Growth, Metrics, and Assessment	Recognize how the MaGMA model is used in threat hunting	40

Activity Report Page 49 of 98

Date	Lab	Description	Points Earned
2024-03-26	Threat Hunt Theory: Understanding the Results	Recognize the importance of threat hunting results	40
2024-03-26	Threat Hunt Theory: Data Quality	Recognize "good" data and why data quality is important in threat hunting	40
2024-03-26	Threat Hunt Theory: Documenting the Hunt	Recognize the importance of documentation and automation in threat hunting	40
2024-03-26	Threat Hunt Theory: Pyramid of Pain	Recognize the pyramid of pain	20
2024-03-26	Threat Hunt Theory: Types of Hunt	Recognize the different types of threat hunt	10
2024-03-26	Threat Hunt Theory: Threat Intelligence Lifecycle	Recognize the intelligence lifecycle	40
2024-03-26	Threat Hunt Theory: The Threat Hunting Loop	Recognize the threat hunting loop	40
2024-03-26	Threat Hunt Theory: Maturity Model	Recognize the threat hunting maturity model	40
2024-03-26	Threat Hunt Theory: Threat Hunting Model	Recognize the threat hunting process	40
2024-03-26	Threat Hunt Theory: Diamond Model	Recognize the diamond model	40
2024-03-26	Tactics: Credential Access	Recognize the purpose of the MITRE ATT&CK® Credential Access tactic	20
2024-03-26	Tactics: Discovery	Recognize the purpose of the MITRE ATT&CK® Discovery tactic	20
2024-03-26	Exploitation Development: Compiled HTML	Describe the structure and contents of a CHM file	200
2024-03-07	Active Directory Basics: Console	Describe what the Active Directory Users and Computers console is	100
2024-03-06	Modern Encryption: Demonstrate Your Skills	Demonstrate the skills acquired through the beginner Encryption labs	300

Activity Report Page 50 of 98

Date	Lab	Description	Points Earned
2024-03-04	DDOS Analysis: SYN Flood	Understand the mechanics of SYN Flood DDoS attacks	100
2024-03-04	DDOS Analysis: Ping of Death	Understand the mechanics of a Ping of Death attack	100
2024-03-04	DDOS Analysis: What are DDoS Attacks?	Understand the basic principles of DDoS attacks	20
2024-03-04	ISO 22381: Demonstrate Your Knowledge	Demonstrate your knowledge of ISO 22381	20
2024-03-04	ISO 27018: Demonstrate Your Knowledge	Recall the information on ISO 27018	20
2024-03-04	ISO 27018: Access Control, Asset Management, and Cryptography	Recognize the elements that govern access control, asset management, and cryptography	10
2024-03-04	ISO 27018: Operations and Communications Security	Recognize the elements that make operational security important for protecting the integrity of PII	20
2024-03-04	ISO 27018: Human Resource and Physical Security	Define the human elements that can impact PII data integrity in the cloud	10
2024-03-04	ISO 27018: Introduction	Recall the scope of ISO 27018 and why it's important	10
2024-03-04	ISO 22381: Interoperability Process	Define the components that facilitate the interoperability process	10
2024-03-04	ISO 22381: Introduction	Define what policies are set out within the ISO 22381 standard	10
2024-03-04	ISO 27014: Demonstrate Your Knowledge	Demonstrate your knowledge of ISO 27014	20
2024-03-04	ISO 27014: Implementation Processes	Define the processes used to implement ISO 27014	10
2024-03-04	ISO 27014: Introduction	Recognize what the ISO 27014 standard is	10
2024-03-04	ISO 31000: Demonstrate Your Knowledge	Recall the information provided throughout the lab series	40

Activity Report Page 51 of 98

Date	Lab	Description	Points Earned
2024-03-04	ISO 31000: Process	Recall the process components illustrated within the ISO 31000 standard	10
2024-03-04	ISO 31000: Principles	Recall how ISO 31000 addresses policy and governance within its framework	10
2024-03-04	ISO 31000: Framework	Recall how ISO 31000 uses a framework to apply principles and processes to a risk management program	10
2024-03-04	ISO 31000: Introduction	Define what policies are set out within the ISO 31000 standard	10
2024-03-01	Business Continuity 101: Demonstrate Your Knowledge	Demonstrate your understanding of business continuity fundamentals	10
2024-03-01	Business Continuity 101: Training and Exercising	Describe the different methods of training and exercising in business continuity	10
2024-03-01	Business Continuity 101: Strategies	Identify the different types of business continuity strategies	10
2024-03-01	Business Continuity 101: Understanding Risks and Impacts	Identify the various risks and threats that can disrupt business operations	10
2024-03-01	Business Continuity 101: What is Business Continuity?	Explain the definition and scope of business continuity	10
2024-03-01	Active Directory Basics: What is Active Directory?	Describe what Active Directory is	40
2024-03-01	Data Handling: Demonstrate Your Knowledge	Demonstrate your understanding of data handling	10
2024-03-01	Data Handling: Data Privacy and Access	Understand the concepts surrounding data privacy	10
2024-03-01	Data Handling: Gathering, Storing, and Processing Data	Understand how to gather and store data securely	10
2024-03-01	Data Handling: Data Fundamentals	Understand the concept of data handling	10
2024-03-01	Security Reporting and Responsiveness: Demonstrate Your Knowledge	Demonstrate an understanding of why security reporting and responsiveness is important	10

Activity Report Page 52 of 98

Date	Lab	Description	Points Earned
2024-03-01	Security Reporting and Responsiveness: Responding Appropriately	Identify when you need to respond to potential incidents	10
2024-03-01	Security Reporting and Responsiveness: Case Studies	Describe the potential impact of not reporting potential security incidents and concerns	10
2024-03-01	Security Reporting and Responsiveness: Reporting Incidents and Concerns	Recognize the importance of reporting potential security incidents and concerns	10
2024-03-01	Introduction to Penetration Testing: Demonstrate Your Knowledge	Demonstrate an understanding of different penetration testing forms and concepts	40
2024-03-01	Interactive RegEx: The RegEx Interface	Be familiar with the interface that will be used throughout the series	20
2024-03-01	Interactive RegEx: An Introduction to RegEx	Recall what regular expressions are and the task they perform	10
2024-03-01	Introduction to Penetration Testing: Web Applications	Be able to demonstrate an understanding of web application hacking concepts	40
2024-03-01	Introduction to Penetration Testing: Mobile Applications	Demonstrate an understanding of iOS/Android pen testing concepts	40
2024-03-01	Introduction to Penetration Testing: Infrastructure	Demonstrate an understanding of infrastructure penetration testing concepts	40
2024-03-01	Introduction to Penetration Testing: The Basics	Be able to describe basic pen testing concepts	20
2024-02-29	LockBit Builder: Analysis	Outline how the LockBit ransomware builder operates	200
2024-02-29	Ransomware: LockBit	Identify signs of LockBit ransomware infections on a Windows host	300
2024-02-28	Secure Data Handling	Recognize poor data handling practices	40
2024-02-23	Intro to Web App Hacking: Authentication Design Flaws	Know how to identify design flaws in a login authentication mechanism	200
2024-02-23	Intro to Web App Hacking: Dirbuster – Custom Headers	Practice using DirBuster with some of its more advanced options	200

Activity Report Page 53 of 98

Date	Lab	Description	Points Earned
2024-02-23	Intro to Web App Hacking: Dirbuster – Introduction	Use DirBuster	200
2024-02-23	Intro to Web App Hacking: Mapping Web Applications	Enumerate a website's content and functionality	200
2024-02-23	Intro to Web App Hacking: Server Side Includes	Demonstrate SSI injection vulnerabilities	200
2024-02-22	Reconnaissance: User Enumeration – WordPress	Enumerate usernames from WordPress websites	100
2024-02-22	Reconnaissance: User Enumeration – SMTP	Recall how to enumerate users on an SMTP server	200
2024-02-22	Reconnaissance: User Enumeration – Building Web Scrapers	Demonstrate extracting emails from websites	40
2024-02-22	Reconnaissance: User Enumeration – Basics	Recall how user enumeration is performed	20
2024-02-22	Reconnaissance: DNS Service – Zone Transfers	Analyze DNS information revealed by a zone transfer	200
2024-02-22	Reconnaissance: DNS Service – Brute Forcing	Enumerate a target's subdomains	100
2024-02-13	Wizard Spider DFIR: Risk Identification	Recognize the techniques used by Wizard Spider during an attack	200
2024-02-08	CVE-2019-0636 (Arbitrary File Read Zero Day)	Demonstrate ability to run basic exploits and assist in triaging	200
2024-02-07	CVE-2023-24934 – Defender Pretender	Outline the Windows Defender feature bypass vulnerability	100
2024-02-02	CVE-2021-34473 (ProxyShell)	Outline how the ProxyShell vulnerability is exploited	100
2024-02-02	CVE-2021-26084 (Confluence) – RCE	Outline how the CVE-2021-26084 vulnerability leads to an RCE	40
2024-02-01	Windows Basics: SMB and RDP	Demonstrate how to use SMB and RDP to manage the target system remotely	100

Activity Report Page 54 of 98

Date	Lab	Description	Points Earned
2024-01-31	Windows Basics: Demonstrate Your Skills	Demonstrate how to interact with and modify a Windows system with the Windows Command Prompt	400
2024-01-30	Windows Basics: Scheduled Tasks	Demonstrate the ability to create and modify tasks	100
2024-01-30	Windows Basics: Services	Demonstrate how to set up and modify Windows services	100
2024-01-30	Windows Basics: Managing Processes	Explain how to view processes on the Windows system	100
2024-01-30	Nessus: Demonstrate your Skills	Interact with Nessus using the web interface	200
2024-01-30	Nessus: Scan Results	Demonstrate how to use Nessus to analyze exported scan results	100
2024-01-30	Pwntools: What is Pwntools?	Recall what Pwntools is and how it functions	40
2024-01-30	Nessus: Authenticated Scanning	Demonstrate how to launch a Nessus scan from the basic network scan template	100
2024-01-26	Cyber Kill Chain: Demonstrate Your Skills	Describe all the stages from the Lockheed Martin Cyber Kill Chain®	400
2024-01-26	Wizard Spider DFIR: Ransomware Analysis	Recognize the techniques used by the Wizard Spider threat group during an attack	200
2024-01-25	Privilege Escalation: Windows – Automated Enumeration	Describe what tools can be used to enumerate a Windows system for privilege escalation vulnerabilities	200
2024-01-25	Privilege Escalation: Windows – Identifying Privilege Escalation Vulnerabilities	Describe where to look for privilege escalation vulnerabilities on a Windows system	200
2024-01-25	Privilege Escalation: Windows – Introduction	Describe what privilege escalation is	100
2024-01-25	Wireshark: Metrics and Statistics	Analyze network packet captures using Wireshark statistics	100
2024-01-24	Cyber Kill Chain: Actions on Objectives	Recognize the fundamentals of the actions on objectives phase in the Cyber Kill Chain	200

Activity Report Page 55 of 98

Date	Lab	Description	Points Earned
2024-01-24	Cyber Kill Chain: Command and Control	Recognize the fundamentals of the command and control phase in the Cyber Kill Chain	200
2024-01-24	Cyber Kill Chain: Installation	Recognize the fundamentals of the installation phase in the Cyber Kill Chain	200
2024-01-24	Cyber Kill Chain: Exploitation	Recognize the fundamentals of the exploitation phase in the Cyber Kill Chain	200
2024-01-19	Windows Basics: Registry	Recall how to view the Windows registry	100
2024-01-19	Windows Basics: Users and Groups	Recall how to find users and groups on a Windows system	100
2024-01-19	Windows Basics: Command Prompt	Recall how to open the Windows Command Prompt	40
2024-01-19	Browsing Securely: Demonstrate Your Knowledge	Demonstrate your understanding of browsing securely	10
2024-01-19	Browsing Securely: Cookies and Pop-Ups	Identify how to protect yourself with cookies, warnings, and pop-ups	10
2024-01-19	Browsing Securely: Browsers	Identify the different ways that you can protect yourself when browsing online	10
2024-01-19	Browsing Securely: Case Studies	Recall key facts about notable insecure browsing incidents	10
2024-01-19	Browsing Securely: What is Secure Browsing?	Identify what secure browsing is	10
2024-01-18	Authentication: Demonstrate Your Knowledge	Demonstrate your knowledge of authentication	10
2024-01-18	Authentication: Adding an Extra Layer of Security	Describe why adding more layers of authentication is important	10
2024-01-18	Authentication: Creating Secure Passwords	Describe why passwords are important	10
2024-01-18	Authentication: Why Are Passwords Important?	Describe why passwords are important	10

Activity Report Page 56 of 98

Date	Lab	Description	Points Earned
2024-01-18	Authentication: What is Authentication?	Identify what authentication is	10
2024-01-15	ISO 28000: What is ISO 28000?	Outline the ISO 28000 standard	10
2024-01-14	Omnipotent Productions: Theory	Understand how to identify and mitigate risk	10
2024-01-14	Omnipotent Productions: Forensics	Demonstrate how to recover deleted files with Autopsy	200
2024-01-12	Omnipotent Productions: OSINT	Employ open-source intelligence to investigate the hacking group and its related people	100
2024-01-12	Omnipotent Productions: Packet Analysis	Be capable of analyzing malicious network traffic	40
2024-01-12	Omnipotent Productions: FTP Server Hardening	Use the CLI to reconfigure an FTP server	200
2024-01-12	Cyber Kill Chain: Delivery	Recognize the fundamentals of the delivery phase in the Cyber Kill Chain	200
2024-01-12	Cyber Kill Chain: Weaponization	Recognize the fundamentals of the weaponization phase in the Cyber Kill Chain	200
2024-01-11	Scanning: Demonstrate Your Skills	Scan and identify information about two targets	200
2024-01-09	Vulnerability Management: Demonstrate Your Knowledge	Recognize the fundamentals of vulnerability management	40
2024-01-09	What is Vulnerability Management?	Recall what vulnerability management is and its importance in defensive cybersecurity	20
2024-01-09	Vulnerability Management: Evaluate and Prioritize	Explain the prioritizing step within the Vulnerability Management process	20
2024-01-09	Vulnerability Management: Remediate	Identify what it means to remediate discovered and known vulnerabilities	20
2024-01-09	Vulnerability Management: Report	Understand the process of reporting vulnerabilities	20

Activity Report Page 57 of 98

Date	Lab	Description	Points Earned
2024-01-09	Vulnerability Management: Monitoring and Identifying	Identify the process for monitoring and identifying vulnerabilities	20
2024-01-09	Vulnerability Management: Asset and System Inventory	Identify the hardware and software assets	20
2024-01-09	Packet Analysis: TLS Handshake	Revise information on the TLS Handshake	100
2024-01-09	Nessus: Network Scanning	Demonstrate how to launch a Nessus scan from the Host Discovery template	100
2024-01-09	Nessus: Introduction to Nessus	Describe typical uses of the Nessus Vulnerability Assessment tool	100
2024-01-05	Cyber for Board Members: Planning and Response	Outline how your organization can detect and respond to cyber incidents	10
2024-01-05	Cyber for Board Members: Supply Chains	Define supply chains	10
2024-01-05	Cyber for Board Members: Cybersecurity Implementation	Recognize why an effective cybersecurity strategy is important	10
2024-01-05	ISO 27001: The Domains of ISO 27001	Define risk-based security approaches	20
2024-01-05	ISO 27001: What About You?	Compare how ISO 27001 applies across various areas of an organization	20
2024-01-05	Web Log Analysis: Error Logs	Recognize web server error logs	100
2024-01-05	NIST 800-144 Cloud Security: Incident Response	Describe key considerations in cloud incident response	10
2024-01-05	NIST 800-144 Cloud Security: Data Protection	Recall NIST 800-144 concerns and recommendations for data protection in cloud environments	10
2024-01-05	NIST 800-144 Cloud Security: Availability	Describe the concerns and recommendations for cloud availability according to NIST 800-144	10
2024-01-05	NIST 800-144 Cloud Security: Software Isolation	Describe what multi-tenancy architecture is	20

Activity Report Page 58 of 98

Date	Lab	Description	Points Earned
2024-01-05	NIST 800-144 Cloud Security: Identity and Access Management	Describe the concerns and recommendations for identity and access management in cloud security as per NIST 800-144 guidelines	20
2024-01-05	NIST 800-144 Cloud Security: Architecture	Explain NIST's recommendations and concerns about architecture with regards to cloud security	10
2024-01-05	NIST 800-144 Cloud Security: Trust	Explain the concern for trust in cloud security	10
2024-01-05	NIST 800-144 Cloud Security: Compliance	Recognize why compliance is important for cloud security	10
2024-01-05	NIST 800-144 Cloud Security: Governance	Recall how governance is important to NIST cloud security guidelines	10
2024-01-05	NIST 800-144: Guidelines on Security and Privacy in Public Cloud Computing	Recall the NIST 800-144 guidelines at a high level	10
2024-01-05	Cyber for Board Members: Risk Management	Outline why risk management is more than just compliance	10
2024-01-05	Cyber for Board Members: Cyber Threats	Define common cyber threats	10
2024-01-05	Cyber for Board Members: Culture and Cybersecurity	Discuss why a positive culture is needed	10
2024-01-05	Cyber for Board Members: Security Posture	Define security posture	10
2024-01-05	Cyber for Board Members: Cyber Expertise	Demonstrate your knowledge of what makes a qualified cyber professional	10
2024-01-05	Cyber for Board Members: Cybersecurity and Business Objectives	Define cybersecurity and business objectives	10
2024-01-04	NIST 800-53: Demonstrate Your Knowledge	Demonstrate your understanding of NIST 800-53 and its purpose	40
2024-01-04	NIST 800-53: Supply Chain Risk Management	Recognize supply chain risk management controls	20
2024-01-04	NIST 800-53: System and Information Integrity	Recognize system and information integrity controls and their purpose	40

Activity Report Page 59 of 98

Date	Lab	Description	Points Earned
2024-01-04	NIST 800-53: System and Communications Protection	Recognize system and communications protection controls and their purpose	40
2024-01-04	NIST 800-53: System and Services Acquisition	Recognize system and services acquisition controls	20
2024-01-04	NIST 800-53: Risk Assessment	Recognize risk assessment controls	20
2024-01-04	NIST 800-53: Personally Identifiable Information Processing and Transparency (PIIPT)	Recognize the PIIPT controls	40
2024-01-04	NIST 800-53: Personnel Security	Recognize personnel security controls and their purpose	20
2024-01-04	NIST 800-53: Program Management	Recognize program management controls and their purpose	20
2024-01-04	NIST 800-53: Planning	Recognize planning controls and their purpose	20
2024-01-04	NIST 800-53: Physical and Environmental Protection	Recognize physical and environmental protection controls and their purpose	20
2024-01-04	NIST 800-53: Media Protection	Recognize media protection controls and their purpose	20
2024-01-04	NIST 800-53: Maintenance	Recognize maintenance controls and their purpose	20
2024-01-04	NIST 800-53: Incident Response	Recognize incident response controls and their purpose	20
2024-01-04	NIST 800-53: Identification and Authentication	Recognize identification and authentication controls and their purpose	20
2024-01-04	NIST 800-53: Contingency Planning	Recognize contingency planning controls and their purpose	20
2024-01-04	NIST 800-53: Configuration Management	Recognize configuration management controls and their purpose	20
2024-01-04	NIST 800-53: Assessment, Authorization, and Monitoring	Recognize assessment, authorization, and monitoring controls and their purpose	20

Activity Report Page 60 of 98

Date	Lab	Description	Points Earned
2024-01-04	NIST 800-53: Audit and Accountability	Recognize audit and accountability controls and their purpose	20
2024-01-04	Splunk Basics: Demonstrate Your Skills	Recall the Splunk features and how to use them	200
2024-01-04	Splunk Basics: Dashboards and Visualization	Recognize dashboards and how they can be used	100
2024-01-04	Splunk Basics: Advanced Searching (SPL & Transforming)	Use Splunk's Search Processing Language (SPL) to search for and transform specific information	200
2024-01-03	Splunk Basics: Search	Identify the key structure of a basic Splunk search	100
2024-01-03	Elastic Data Ingest: Demonstrate Your Skills	Demonstrate log analysis techniques using the Elastic Stack to investigate suspicious activity	300
2024-01-03	Elastic Data Ingest: Winlogbeat	Demonstrate log analysis techniques using Winlogbeat and the Elastic Stack	200
2024-01-03	Elastic Data Ingest: Heartbeat	Demonstrate log analysis techniques using Heartbeat and the Elastic Stack	200
2024-01-03	Elastic Data Ingest: Packetbeat	Demonstrate log analysis techniques using Packetbeat and the Elastic Stack	200
2024-01-03	Elastic Data Ingest: Metricbeat	Demonstrate log analysis techniques using Metricbeat and the Elastic Stack	200
2024-01-03	Elastic Data Ingest: Auditbeat	Demonstrate log analysis techniques using Auditbeat and the Elastic Stack	200
2024-01-03	Elastic Data Ingest: Filebeat	Demonstrate log analysis techniques using Filebeat and the Elastic Stack	200
2024-01-03	Elastic Playground: Flight Data	Demonstrate log analysis techniques using the Elastic Stack	100
2024-01-02	Splunk Basics: Data Sources	Be able to recall the various data sources supported by Splunk	40
2024-01-02	Splunk Basics: The Splunk Interface	Recognize the different components of the Splunk Interface	40

Activity Report Page 61 of 98

Date	Lab	Description	Points Earned
2024-01-02	What is Splunk?	Recall what the Splunk tool is	40
2024-01-02	Elastic Playground: Web Logs	Demonstrate log analysis techniques using the Elastic Stack	100
2024-01-02	Elastic Playground: eCommerce Data	Demonstrate log analysis techniques using the Elastic Stack	100
2024-01-02	WPA Wordlist Crack	Identify weaknesses in Wi-Fi protocols	100
2024-01-02	Wired Equivalent Privacy (WEP) Cracking	Identify weaknesses in Wi-Fi protocols	200
2024-01-02	Pen Test CTFs: Shadow Brokers' Victim	Exploiting a victim	300
2024-01-01	Linux CLI: Demonstrate Your Skills	Demonstrate your understanding of the Linux CLI	100
2024-01-01	PKI (Public Key Infrastructure)	Understand the different parts of PKI and their roles	40
2023-12-30	Windows Forensics Artifacts: Demonstrate Your Skills	Recognize the different artifacts you can find in Windows	100
2023-12-30	Windows Forensics Artifacts: Link Files (LNK)	Recall what the Shell Link Binary File Format is	20
2023-12-30	Windows Forensics Artifacts: Master File Table	Recall what the Master File Table is	40
2023-12-30	Windows Forensics Artifacts: Recycle Bin	Recall what Recycle Bin artifacts are	40
2023-12-30	Windows Forensics Artifacts: ShellBags	Recall what ShellBags are and where to find this artifact	40
2023-12-30	Windows Forensics Artifacts: UserAssist	Recall the location, use, and format of the UserAssist Key	40
2023-12-30	Digital Forensics Process: Demonstrate Your Skills	Recognize the fundamentals of the forensic process	40

Activity Report Page 62 of 98

Date	Lab	Description	Points Earned
2023-12-30	Windows Forensics Artifacts: Event Logs	Recall what event logs are and where to find this artifact	40
2023-12-30	Windows Forensics Artifacts: Prefetch Files	Recall what prefetch files are and where to find them	40
2023-12-30	Windows Forensics Artifacts: AppCompatCache	Recall what the AppCompactCache is and where to find it	40
2023-12-30	Windows Forensics Artifacts: Amcache	Recall what the Amcache is and where to find this artifact	40
2023-12-30	Digital Forensics Process: Collection – Ensure Integrity	Identify how the integrity of digital evidence is verified	20
2023-12-30	Digital Forensics Process: Anti-Forensics Techniques	Identify what anti-forensics techniques are	40
2023-12-30	Digital Forensics Process: Interpretation – Analyzing Findings	Recall the process of analyzing forensic evidence	40
2023-12-30	Digital Forensics Process: Interpretation – Identify and Extract	Recall how to navigate through data and find forensic artifacts	40
2023-12-30	Digital Forensics Process: Collection – Types of Acquisition	Identify the different types of acquisition	40
2023-12-30	Digital Forensics Process: Introduction	Recall the steps of the digital forensics process	20
2023-12-30	Elliptic Curve Cryptography	Explain the basics of elliptic curve cryptography	100
2023-12-30	Cyber for Executives: Supply Chain Security	Define 'supply chain security'	10
2023-12-30	Cyber for Executives: Whaling	Define 'whaling'	10
2023-12-30	Cyber for Executives: Common Threats	Identify the most common cyber threats facing organizations	10
2023-12-30	Cyber for Executives: Incidents	Outline what executives can do to contribute to the protection of their organization during an incident	10

Activity Report Page 63 of 98

Date	Lab	Description	Points Earned
2023-12-30	Cyber for Executives: Compliance	Be able to define 'compliance'	10
2023-12-30	Cyber for Executives: Skills Shortage	Define skills shortages and how they can impact organizations	10
2023-12-30	Cyber for Executives: Risk	Define 'risk'	10
2023-12-30	Cyber for Executives: What is InfoSec?	Define the scope of information security	10
2023-12-29	Introduction to Incident Response: Demonstrate Your Knowledge	Recall the key steps of the NIST incident response process	40
2023-12-29	Volatility Memory Analysis: File Systems	Enumerate the Windows Master File Table	100
2023-12-29	Volatility Memory Analysis: Registry	Enumerate registry hive information	100
2023-12-29	Volatility Memory Analysis: Networking	Identify open connections in a memory capture	100
2023-12-29	Crisis Management 101: Crisis Communications	Recognize principles of good crisis communication	10
2023-12-29	Crisis Management 101: Cyber Crisis Decision Making	Recognize different types of decisions you'll experience in a crisis situation	10
2023-12-29	Crisis Management 101: Tame and Wicked Problems	Identify key characteristics of tame and wicked problems	10
2023-12-29	Crisis Management 101: Situational Awareness	Identify the steps involved in situational awareness	10
2023-12-29	NIST 800-53: Awareness and Training	Recognize the purpose of awareness and training controls	20
2023-12-29	NIST 800-53: Access Control	Recognize the NIST 800-53 Access Control family and its purpose	20
2023-12-29	NIST 800-53: Security and Privacy Controls for Information Systems and Organizations	Familiarize yourself with NIST 800-53 and its purpose	20

Activity Report Page 64 of 98

Date	Lab	Description	Points Earned
2023-12-29	Crisis Management 101: Incidents Vs Crises	Describe the difference between cyber incidents and crises	10
2023-12-29	Introduction to Incident Response: Post-Incident Activity	Recall the post-incident activity stage of the NIST incident response process	40
2023-12-29	Introduction to Incident Response: Detection and Analysis	Discuss the detection and analysis stage of the NIST incident response process	40
2023-12-29	Introduction to Incident Response: Containment, Eradication, and Recovery	Recall and discuss the containment, eradication, and recovery stages of the NIST incident response process	40
2023-12-29	Introduction to Incident Response: Preparation	Discuss the details of the preparation stage of NIST's incident response process	40
2023-12-28	Volatility Memory Analysis: Kernel Memory and Objects	Recall the fundamentals of kernel modules and drivers	100
2023-12-28	Volatility Memory Analysis: Process Memory	Recall fundamental memory structures and operations	100
2023-12-28	Volatility Memory Analysis: Processes and DLLs	Recognize system processes in memory	100
2023-12-28	Volatility Memory Analysis: Getting Started	Demonstrate basic usage of the Volatility tool	100
2023-12-28	Volatility: What is the Volatility Framework?	Recall what the Volatility framework is	20
2023-12-27	Introduction to Penetration Test Programs: Demonstrate Your Knowledge	Demonstrate your understanding of penetration test programs	40
2023-12-27	Cyber Kill Chain: Demonstrate Your Knowledge	Recognize the fundamentals of the Cyber Kill Chain model	40
2023-12-27	Introduction to Networking: Demonstrate Your Knowledge	Demonstrate an understanding of networking technology fundamentals	40
2023-12-27	Introduction to Penetration Test Programs: Improving your Program	Describe how a penetration testing program could be improved	20
2023-12-27	Introduction to Penetration Test Programs: Post-Engagement Activities	Describe what post-engagement activities are	20

Activity Report Page 65 of 98

Date	Lab	Description	Points Earned
2023-12-27	Introduction to Penetration Test Programs: Penetration Test Reports	Describe what is typically contained in a penetration report and how findings should be presented to an organization.	20
2023-12-27	Introduction to Penetration Test Programs: Engagement Activities	Identify some of the activities an organization can expect to happen during a penetration test	20
2023-12-27	Introduction to Penetration Test Programs: Pre-Engagement Activities	Identify some of the activities an organization might perform before each penetration test	20
2023-12-27	Introduction to Penetration Test Programs: Testing Management	Identify management processes required when performing penetration tests	20
2023-12-27	Introduction to Penetration Test Programs: Choosing a Supplier	Identify criteria for a penetration test supplier	20
2023-12-27	Introduction to Penetration Test Programs: Defining your Testing Program	Identify which areas of a pen testing program need to be defined	20
2023-12-27	Introduction to Penetration Test Programs: Cybersecurity Frameworks	Describe how technical assurance frameworks can include penetration testing	20
2023-12-27	Introduction to Penetration Test Programs: What is Pen Testing?	Define what a penetration test is	20
2023-12-27	Inherent vs Residual Risk	Explain the difference between inherent and residual risk	20
2023-12-27	Reconnaissance: DNS Enumeration – TXT	Summarize the fundamentals of TXT records	40
2023-12-27	Reconnaissance: DNS Service – MX Record	Demonstrate finding a domain's mail server	40
2023-12-27	Reconnaissance: DNS Enumeration – NS	Summarize the fundamentals of the name server	40
2023-12-27	Reconnaissance: DNS Service – Basics	Summarize how the DNS service operates	40
2023-12-27	Cyber Kill Chain: Adversary Simulation	Recall the fundamentals of adversary simulation	100
2023-12-27	Cyber Kill Chain: Actions on Objectives Phase	Recall the fundamentals of the 'actions on objectives' phase	40

Activity Report Page 66 of 98

Date	Lab	Description	Points Earned
2023-12-27	Cyber Kill Chain: What is the Command and Control (C2) Phase?	Recall the fundamentals of the command and control phase	40
2023-12-27	Cyber Kill Chain: Installation/Persistence Phase	Recall the fundamentals of the installation phase	40
2023-12-27	Cyber Kill Chain: Exploitation Phase	Be able to recall the fundamentals of the exploitation phase	40
2023-12-27	Cyber Kill Chain: Delivery Phase	Recall the fundamentals of the delivery phase	40
2023-12-27	Cyber Kill Chain: Weaponization Phase	Recall the fundamentals of the weaponization phase	40
2023-12-27	Cyber Kill Chain: Reconnaissance Phase	Recall the fundamentals of the reconnaissance phase	20
2023-12-27	Cyber Kill Chain: What is the Cyber Kill Chain?	Recognize the fundamentals of the Cyber Kill Chain model	20
2023-12-27	Secure Fundamentals: The CIA Triad	Define confidentiality, integrity, and availability	20
2023-12-27	Secure Fundamentals: Attribution and Accountability	Explain attribution and accountability	20
2023-12-27	TLS Fundamentals: X.509 Introduction	Identify an X.509 certificate and its main purpose	40
2023-12-27	TLS Fundamentals: Key Exchange and Session Resumes	Describe the role of the key exchange in a TLS handshake	40
2023-12-27	TLS Fundamentals: Cipher Suites	Describe the different sections of a TLS cipher suite	100
2023-12-27	TLS Fundamentals: Client Hello and Server Hello	Recall the different features in the client and server hello	40
2023-12-27	TLS Fundamentals: Introduction	Describe the function and purpose of TLS	40
2023-12-27	Introduction to Networking: Network Topologies	Recognize network topologies	40

Activity Report Page 67 of 98

Date	Lab	Description	Points Earned
2023-12-27	Introduction to Networking: Network Hardware	Recognize the different types of hardware used for networks	40
2023-12-27	Introduction to Networking: Types of Networks	Recall multiple types of networks and how they differ	20
2023-12-27	Introduction to Networking: What is a Network?	Recognize networks and their components	40
2023-12-27	Secure Fundamentals: Principle of Least Privilege	Describe the principle of least privilege	10
2023-12-27	Secure Fundamentals: Defense In Depth	Describe the security concept of defense in depth	10
2023-12-27	Secure Fundamentals: Security Patching	Describe what a security patch is	10
2023-12-27	Ethics & Laws: US Federal Cyber Law	Identify the main US federal laws that can be used to convict cyber criminals	10
2023-12-27	Compliance: The Sarbanes-Oxley Act	Explain the purpose of the Sarbanes-Oxley Act	10
2023-12-27	Secure Fundamentals: Authorization	Describe the concept of authorization	10
2023-12-27	Secure Fundamentals: Authentication	Describe the concept of authentication	10
2023-12-27	Compliance: EU-US Privacy Shield	Recall what the Privacy Shield is	10
2023-12-27	Ethics & Laws: UK Cyber Law	Demonstrate an understanding of illegalities and breaches of law	40
2023-12-27	Compliance: General Data Protection Regulation (GDPR)	Recognize the key details of the GDPR	10
2023-12-27	Compliance: Cyber Insurance	Identify what cyber insurance is and what it can cover	10
2023-12-27	ISO 27001: What Is ISO 27001?	Identify why the ISO 27001 standard is used	20

Activity Report Page 68 of 98

Date	Lab	Description	Points Earned
2023-12-27	Ethics & Laws: Bugbusters	Describe bug bounty programs	40
2023-12-27	Ethics & Laws: Ethical and Unethical Hacking	Demonstrate the ability to determine the ethical choices of hackers	40
2023-12-27	Ethics & Laws: Burglary and Hacking	Demonstrate an understanding of how hacking can be similar to burglary	40
2023-12-27	Ethics & Laws: Police Raid	Demonstrate an understanding of devices that would be confiscated in an investigation	40
2023-12-26	AI: Prompt Injection Attacks	Explain the concept of Large Language Models (LLMs) and prompts within the context of artificial intelligence	200
2023-12-26	AI: Demonstrate Your Skills	Demonstrate the skills acquired through the AI Fundamentals collection	100
2023-12-26	AI: Image Classification	Outline what image recognition is and how it's used in artificial intelligence	40
2023-12-26	AI: Generative AI Models	Understand the basic concepts and types of generative AI	20
2023-12-26	AI: Artificial Intelligence for Incident Responders	Outline the risks and opportunities of AI in incident response, including what threats it poses	20
2023-12-26	Events & Breaches: Phishing Fraud	Identify spoofed domains used in phishing emails	100
2023-12-22	Human Factors in Cybersecurity: Demonstrate Your Understanding	Demonstrate your understanding of human factors in cybersecurity	40
2023-12-22	Human Factors in Cybersecurity: Security Awareness and Behavior Change	Explain the role of security awareness and behavior change	20
2023-12-22	Human Factors in Cybersecurity: Security Culture	Explain the importance of security culture and how the principles apply to your organization	20
2023-12-22	Human Factors in Cybersecurity: Usable Security	Explain usability and the causes of unusable security	20
2023-12-22	Human Factors in Cybersecurity: How People Make Security Mistakes	Explain the Swiss Cheese Model applied to cybersecurity	20

Activity Report Page 69 of 98

Date	Lab	Description	Points Earned
2023-12-22	Human Factors in Cybersecurity: People Are The Strongest Link	Explain what human factors are and why they're important	20
2023-12-22	Digital Footprint: Demonstrate Your Knowledge	Demonstrate an understanding of what digital footprints are	10
2023-12-22	Digital Footprint: Protecting Yourself	Recognize the different methods that can be used to uncover your digital footprint	10
2023-12-22	Digital Footprint: Case Studies	Recall key facts about case studies involving digital footprints	10
2023-12-22	Digital Footprint: What is a Digital Footprint?	Recognize the concept of digital footprints and their significance	10
2023-12-22	Physical Security: Demonstrate Your Knowledge	Demonstrate your knowledge on physical security	10
2023-12-22	Physical Security: Physical Security When Working Remotely	Recognize physical security risks when working remotely	10
2023-12-22	Physical Security: Physical Security in Your Workplace	Recognize physical security risks in the office	10
2023-12-22	Physical Security: Introduction to Physical Security	Describe what physical security is	10
2023-12-22	Windows Concepts: Demonstrate Your Skills	Demonstrate proficiency in navigating and manipulating the Windows registry to achieve specific configurations or extract information.	200
2023-12-22	Social Engineering: Demonstrate Your Skills	Demonstrate your understanding of social engineering	10
2023-12-22	Social Engineering: Protecting Yourself	Understand the different ways that you can protect yourself from social engineering	10
2023-12-22	Social Engineering: How Is It Used?	Recall key facts about notable social engineering attacks	10
2023-12-22	Social Engineering: Techniques	Understand the common techniques used in social engineering	10
2023-12-22	Social Engineering: What is Social Engineering?	Understand what social engineering is	10

Activity Report Page 70 of 98

Date	Lab	Description	Points Earned
2023-12-22	AI for Business: Using AI at Work	Identify how AI can be used in your day-to-day work	10
2023-12-22	AI for Business: The Risks of AI	Define some of the risks associated with AI	10
2023-12-22	AI for Business: The Benefits of AI	Define some of the benefits of using AI	10
2023-12-22	AI for Business: What is AI?	Explain what AI is and how you can use it	10
2023-12-22	AI: TensorFlow for Machine Learning	Define machine learning	40
2023-12-22	AI: Introduction to AI	Define the key components of AI	20
2023-12-22	AI: Emerging Threats	Define some of the threats associated with AI	20
2023-12-22	AI: Data Ethics and Responsible Use	Define some of the risks associated with data that is collected and processed by AI	20
2023-12-22	Data Privacy: What About You?	Outline why data privacy is important	20
2023-12-22	Data Privacy: Data Privacy Regulations	Summarize what data privacy regulations are	20
2023-12-22	Data Privacy: Key Concepts	Explain the key concepts of data privacy	10
2023-12-22	Windows Concepts: Volume Shadow Copy Service	Exposure to VSS and its functionality	200
2023-12-22	Windows Concepts: Alternate Data Streams	Exposure to ADS and data hiding	200
2023-12-22	Windows Concepts: Security Policies	Exposure to Windows policy mechanisms	200
2023-12-22	Windows Concepts: Environment Variables	Understand the function of environment variables in Windows	200

Activity Report Page 71 of 98

Date	Lab	Description	Points Earned
2023-12-21	Introduction to Digital Forensics: Demonstrate Your Skills	Recognize the fundamentals of digital forensics	100
2023-12-21	Introduction to Cryptography: Demonstrate Your Knowledge	Demonstrate an understanding of cryptography	40
2023-12-21	Digital Forensics Process: Reporting	Recall the different ways of presenting evidence	20
2023-12-21	Digital Forensics Tools	Recognize the most common digital forensics tools	20
2023-12-21	Digital Forensics Processes and Techniques	Recall digital forensics processes	40
2023-12-21	Digital Evidence	Define what digital evidence is	20
2023-12-21	What is Digital Forensics?	Define digital forensics	20
2023-12-21	Encoding: Demonstrate Your Skills	Recall encoding methods and techniques	200
2023-12-21	Encoding: Punycode	Recall how Punycode functions	100
2023-12-21	Encoding: Unicode	Recall how Unicode functions	40
2023-12-21	Encoding: Base64	Recall how Base64 encoding works	40
2023-12-21	Encoding: ASCII	Recall how ASCII encoding functions	40
2023-12-21	Encoding: Hexadecimal	Recall how hexadecimal functions	40
2023-12-21	Encoding: What is Encoding?	Recall how encoding functions	40
2023-12-21	Vigenère Ciphers	Describe what a Vigenère cipher is	40

Activity Report Page 72 of 98

Date	Lab	Description	Points Earned
2023-12-21	The History of Encryption	Recall the different methods of encryption used throughout history	40
2023-12-21	Introduction to Cryptography: Block Ciphers	Define a block cipher	40
2023-12-21	Introduction to Cryptography: Digital Signatures	Recall the importance of digital signatures	40
2023-12-21	Introduction to Cryptography: Hashing	Recognize the importance of hashing	20
2023-12-21	Introduction to Cryptography: Public Key Infrastructure	Define what public key infrastructure is	40
2023-12-21	Networking: Demonstrate Your Skills	Demonstrate how to analyze PCAP files	100
2023-12-21	Networking: Demonstrate Your Knowledge	Demonstrate your networking knowledge	100
2023-12-21	DoS Primer: Resource Exhaustion	Explain the different types of resource exhaustion attacks	40
2023-12-21	DoS Primer: Vulnerabilities	Learn different types of denial of service vulnerabilities	40
2023-12-21	DoS Primer: Volumetric	Explain the different types of volumetric attacks	40
2023-12-21	Historic Encryption: Demonstrate Your Skills	Demonstrate your knowledge of historic encryption techniques	200
2023-12-21	Protocols: DHCPv6	Discuss the use of DHCP in computer networks	200
2023-12-21	Protocols: DHCPv4	Discuss the use of DHCP in computer networks	200
2023-12-21	Protocols: Modbus	Reference the core concepts of the Modbus protocol	300
2023-12-21	DoS Primer: Tools	Describe several denial of service tools	200

Activity Report Page 73 of 98

Date	Lab	Description	Points Earned
2023-12-21	Protocols: DNS	Describe the structure of DNS requests and responses	200
2023-12-21	Protocols: SMTP	Describe the structure of SMTP messages	200
2023-12-21	Protocols: HTTP	Describe the structure of HTTP GET and POST requests	200
2023-12-21	Steganography	Analyze images and extract information using ExifTool and Steghide	200
2023-12-20	OWASP 2021: Demonstrate Your Knowledge	Recall different vulnerability categories in the 2021 OWASP Top 10	40
2023-12-20	Eric Zimmerman's Tools: Introduction	Recall what Eric Zimmerman’s tools are and where to download them	40
2023-12-20	OWASP API Security Top 10	Identify each of the vulnerabilities in OWASP's API list	20
2023-12-20	OWASP 2021: Server-Side Request Forgery	Summarize server-side request forgery and its relationship to the OWASP Top 10	20
2023-12-20	Introduction to Cryptography: Public and Private Key Management	Recognize the importance of managing public and private keys	40
2023-12-20	Introduction to Cryptography: One-Time Pad	Define what a one-time pad cipher is	40
2023-12-20	Introduction to Cryptography: Symmetric Key Encryption	Recognize symmetric encryption	40
2023-12-20	Introduction to Cryptography: What is Cryptography?	Recall the fundamentals of cryptography	40
2023-12-20	Introduction to Cryptography: Asymmetric Encryption	Define asymmetric encryption	40
2023-12-20	Introduction to Cryptography: Stream Ciphers	Define stream ciphers and recall their fundamental characteristics	40
2023-12-20	Introduction to Cryptography: Message Integrity	Be able to define the term ‘message integrity’	40

Activity Report Page 74 of 98

Date	Lab	Description	Points Earned
2023-12-19	OWASP 2021: Security Logging and Monitoring Failures	Summarize security logging and monitoring failures and their relationship to the OWASP Top 10	20
2023-12-19	OWASP 2021: Software and Data Integrity Failures	Summarize software and data integrity failures and their relationship to the OWASP Top 10	20
2023-12-19	OWASP 2021: Identification and Authentication Failures	Summarize identification and authentication failures and their relationship to the OWASP Top 10	20
2023-12-19	OWASP 2021: Vulnerable and Outdated Components	Summarize the security misconfiguration and its relationship to the OWASP Top 10	20
2023-12-19	OWASP 2021: Security Misconfiguration	Summarize security misconfiguration and its relationship to the OWASP Top 10	20
2023-12-19	OWASP 2021: Insecure Design	Summarize insecure design and its relationship to the OWASP Top 10 list	20
2023-12-19	OWASP 2021: Cryptographic Failures	Summarize cryptographic failures and their relationship to the OWASP Top 10	20
2023-12-19	OWASP 2021: Broken Access Control	Summarize broken access control and its relationship to the OWASP Top 10	20
2023-12-19	Omnipotent Productions: Log Analysis	Examine Wireshark's analytics features	40
2023-12-19	Cyber Kill Chain: Reconnaissance	Recognize the fundamentals of the reconnaissance phase	200
2023-12-18	Kate's Story: Exploitation	Demonstrate how to analyze a malicious payload	300
2023-12-18	Immersive Care: Binary File Analysis	Develop critical thinking	200
2023-12-18	Immersive Care: Packet Capture Analysis	Develop critical thinking	200
2023-12-18	Immersive Care: Introduction	Develop critical thinking	40
2023-12-15	CVE-2019-16759 (vBulletin RCE)	Analyze the vBulletin vulnerability	100

Activity Report Page 75 of 98

Date	Lab	Description	Points Earned
2023-12-13	Wizard Spider DFIR: What is Wizard Spider?	Describe the most common TTPs used by Wizard Spider	40
2023-12-13	Parellus Power: Room Reconnaissance	Identify the attack surface of a given website	300
2023-12-08	Parellus Power: Interception	Identify flaws in a web application	200
2023-12-08	Parellus Power: Gathering Information	Identify OSINT techniques	100
2023-12-08	Scanning: WPScan	Identify vulnerabilities in WordPress	200
2023-12-08	Scanning: Nikto and DIRB	Identify vulnerabilities in web servers	100
2023-12-08	Scanning: Port Knocking	Use port knocking techniques to open a port on a server	200
2023-12-08	Scanning: DNS Enumeration	Knowledge of DNS enumeration techniques	200
2023-12-07	Ghidra: Projects and Getting Started	Demonstrate the extensive use of disassembly with the Ghidra reverse engineering tool	300
2023-12-05	Introduction to Detection Engineering: Fundamentals	Recall how the Pyramid of Pain can be applied to defensive operations	40
2023-12-05	Autopsy: Tags, Comments, and Reports	Outline how Autopsy can be used to tag, comment, and report on evidence and artifacts	40
2023-12-05	Autopsy: Cases and Data	Demonstrate how to navigate around an Autopsy case	40
2023-12-05	Autopsy: Getting Started	Demonstrate how to navigate and identify components of Autopsy	100
2023-12-04	Hafnium: Detection of IoCs	Be able to use scripts to detect IoCs	100
2023-12-04	HTTP Status Codes: Challenge	Develop your knowledge of HTTP status codes	200

Activity Report Page 76 of 98

Date	Lab	Description	Points Earned
2023-12-02	Cross-Site Scripting: What is Cross-Site Scripting?	Describe what cross-site scripting is	20
2023-12-02	Cross-Site Scripting: Stored XSS	Identify stored cross-site scripting vulnerabilities in a web application	200
2023-12-01	CVE-2023-34362 (MOVEit SQL Injection) – Defensive	Outline how attackers are able to exploit a SQL injection vulnerability in MOVEit Transfer to exfiltrate data	200
2023-07-10	Port Identification	Recognize common default port numbers and their associated services	100
2023-06-14	A Christmas Catastrophe: Kringle Inc.	Decode common encoding and encryption schemes	300
2023-05-12	Threat Research: iOS Implant	Identify command and control functions used by the implant	300
2023-05-12	Packet Analysis: Using tcpdump	Analyze network packet captures	200
2023-05-10	Decompiling .NET	Familiarisation with .NET	400
2023-05-09	Introduction to Computer Memory and Architecture	Gain a high level understanding of how memory works in a computer system	40
2023-04-21	Burp Suite Basics: HTTPS	Configure and use Burp Suite with Firefox	100
2023-04-20	Hunting for Public S3 Buckets	Explain why public S3 buckets are often compromised	200
2023-04-17	AWS: Introduction to Security Groups	Analyze security configuration	40
2023-04-11	Python Coding – Introduction	Read Python code	100
2023-04-11	Msfvenom	Use msfvenom to create a payload	300
2023-04-11	Intro to Web App Hacking: Directory Traversal	Conduct directory traversal attacks against a web server	200

Activity Report Page 77 of 98

Date	Lab	Description	Points Earned
2023-04-07	Offensive PowerShell: Empire	Demonstrate how to configure and run various PowerShell Empire functions	100
2023-04-06	Incident Response: Suspicious Email – Evidence of Compromise	Investigate host-based compromise and IOCs	400
2023-03-31	Compliance: Payment Card Industry Data Security Standard (PCI-DSS)	Recall the different PCI-DSS control objectives	40
2023-03-09	Container Hardening: Introduction to Containerization	Describe containers, their advantages, and disadvantages	20
2023-03-09	Msfconsole: Exploit	Practice using Metasploit's exploit modules to attack services	200
2023-03-08	IoT & Embedded Devices: Supply Chain Hardware Tampering	Practice interacting with a Baseboard Management Controller	100
2023-02-24	World Cup Special: World Cup Trivia	Complete the trivia challenge with minimal guidance	300
2023-02-24	Splunk: Event Analysis 2	Demonstrate and develop event log analysis techniques	200
2023-02-24	WannaCry	Safely observe WannaCry ransomware	100
2023-02-24	Splunk: Event Analysis	Demonstrate and develop basic event log analysis techniques	200
2023-02-22	Windows Sysinternals: Sysmon	Analyze and investigate system logs	100
2023-02-17	The Bombe Machine	Recognize how the Bombe machine works	200
2023-02-17	Immersive Bank: Gaining Access	Apply critical thinking to gain access to the computer	100
2023-02-14	Infrastructure Hacking: OpenLDAP Plaintext Passwords	Analyze an LDAP post exploitation technique	100
2023-02-14	Infrastructure Hacking: Space After Filename	Inspect suspicious files and analyze their function	100

Activity Report Page 78 of 98

Date	Lab	Description	Points Earned
2023-02-14	Infrastructure Hacking: SimpleHTTPServer	Use Python's SimpleHTTPServer to spawn web servers	100
2023-02-14	Infrastructure Hacking: SSL Scanning	Identify weak cryptographic ciphers	200
2023-02-14	Introduction to Active Directory Attacks: Pass-the-Hash	Gain access to a system using pass-the-hash	200
2023-02-14	Netcat: Connecting with Netcat	Use Netcat for various tasks	100
2023-02-10	Compliance: Payment Services Directive 2 (PSD2)	Describe how PSD2 works and affects the banking industry	10
2023-02-10	NIST Cybersecurity Framework	List the three main components of the NIST Cybersecurity Framework	40
2023-02-10	Compliance: Information Technology Health Check (ITHC)	Recognize why an information technology health check is carried out	20
2023-02-10	Compliance: Health Insurance Portability and Accountability Act (HIPAA)	Describe the five titles that form the structure of HIPAA	20
2023-02-10	Three Lines of Defense	Describe the Three Lines of Defense model	10
2023-02-10	Qualitative Risk Measurement	Summarize what qualitative risk is	20
2023-02-10	Risk and Control Self Assessment (RCSA)	Describe the purpose of an RCSA within the wider risk management framework	20
2023-02-10	Quantitative Risk Measurement	Calculate quantitative risk as a function of impact and probability	40
2023-02-10	Inherent and Residual Risk	Explain the difference between inherent and residual risk	20
2023-02-10	Compliance: Networks and Information Systems (NIS) Directive	Recognize what the NIS Directive is and how it protects the countries in the EU	20
2023-02-10	Vulnerability Identification	Identify the different ways to conduct vulnerability identification	40

Activity Report Page 79 of 98

Date	Lab	Description	Points Earned
2023-02-10	Risk: Asset Inventory and Valuation	Define the asset identification and valuation processes	20
2023-02-10	Compliance: The Cyber Essentials Scheme	Identify the most common attacks outlined by the Cyber Essentials scheme	20
2023-02-10	How to Mitigate Risk	Explain how risk management can help mitigate risk	20
2023-02-10	GDPR Aware	Explain the key details and impact of GDPR	10
2023-02-09	Intro to Web App Hacking: Bypassing HTTP Client-Side Controls	Recognize some common insecure user access controls that can be found in web applications	200
2023-02-09	Intro to Web App Hacking: Page Source Review	Analyze the web application source code to recognize technologies being used	200
2023-02-08	PoshC2: Introduction to Command and Control Frameworks	Describe command and control frameworks, their uses, and benefits	40
2023-02-08	Elastic Playground: Accounting and Audit	Identify audit and accounting methodology	200
2023-02-08	IoT & Embedded Devices: Best Practice	Describe how to securely deploy IoT devices	10
2023-02-08	IoT & Embedded Devices: Hardware Reverse Engineering	Identify security best practices for IoT devices	10
2023-02-08	IoT and Embedded Devices: Network Protocols and Security	Express the importance of using encryption to secure communications	10
2023-02-08	IoT & Embedded Devices: Security Issues	Identify security best practice for IoT devices	10
2023-02-03	Ransomware: Bad Rabbit	Identify signs of Bad Rabbit ransomware infections on a Windows host	300
2023-02-02	Incident Response: Data Exfiltration	Practice identifying instances where data has been exfiltrated	100
2023-02-02	Incident Response: Clipboard Data Theft	Analyze techniques used by adversaries to steal clipboard data	100

Activity Report Page 80 of 98

Date	Lab	Description	Points Earned
2023-01-31	Infrastructure Hacking: Sudo Caching	Identify exploit attempts that abuse the sudo caching technique	100
2023-01-31	Practical Malware Analysis: Java RATs	Identify the file structure for a JAR application	200
2023-01-31	Infrastructure Hacking: Bash History	Be able to identify the risk of passing credentials with the command line	100
2023-01-31	How is Risk Measured?	Be able to describe risk, impact, and probability	40
2023-01-31	Digital Forensics: Using file	Using file to identify true information about unusual looking files	100
2023-01-31	Digital Forensics: Timestomping	Gain an understanding of the MFT	300
2023-01-31	Digital Forensics: National Software Reference Library (NSRL)	Use the national software reference library	100
2023-01-31	SMTP Log Analysis	Carry out a log analysis to identify particular information	100
2023-01-31	Log Finder	Perform web log analysis	100
2023-01-31	Packet Analysis: Packet Capture Basics	Analyze network packet captures	100
2023-01-30	PowerShell Basics: Files and Folders	Explain how to navigate around a system with PowerShell	100
2023-01-30	Introduction to Forensics	Exposure to forensics principals	40
2023-01-27	Practical Malware Analysis: Static Analysis	Describe what static analysis is and how it's used for malware analysis	40
2023-01-26	Windows Sysinternals: Process Explorer	Use Process Explorer effectively	100
2023-01-25	Windows Sysinternals: Introduction to Sysinternals	Identify products in the Sysinternals Suite	100

Activity Report Page 81 of 98

Date	Lab	Description	Points Earned
2023-01-25	PowerShell Basics: What is PowerShell?	Describe what PowerShell is	100
2023-01-23	Mimikatz and Chrome Passwords	Recall the cookies and login data files that Chrome stores in %LOCALAPPDATA%	200
2023-01-23	Cross-Site Scripting: Reflected XSS	Identify reflected cross-site scripting vulnerabilities in a web application	200
2023-01-23	SQL Injection: sqlmap	Practice applying sqlmap to a database	200
2023-01-23	Credential Access: Using Hydra	Perform attacks on different network protocols	200
2023-01-23	Open Source Intelligence (OSINT): Social Media	Demonstrate the use of OSINT techniques to identify useful information from social media platforms	40
2023-01-23	John the Ripper	Exposure to John the Ripper tool chain	100
2023-01-23	Computer Architecture: Introduction to ELF Reverse Engineering	Exposure to ELF binary analysis	100
2023-01-23	Credential Access: Password Hashing and Salting Techniques	Describe the benefits of salting passwords	100
2023-01-20	SQL: An Introduction	Gain an understanding of the SQL language and queries	100
2023-01-13	Virtualization	Describe the uses and advantages of virtualization	10
2023-01-13	Platform as a Service (PaaS)	Be able to explain the advantages and disadvantages of Platform as a Service	20
2023-01-13	Security Automation	Describe the advantages of security automation and orchestration	20
2023-01-13	Infrastructure as Code (IaC)	Explain what IaC is and how it is deployed	20
2023-01-13	DevSecOps: Introduction	Recall the evolution of software delivery methodologies	10

Activity Report Page 82 of 98

Date	Lab	Description	Points Earned
2023-01-13	Infrastructure as a Service (IaaS)	Describe the advantages and disadvantages of Infrastructure as a Service (IaaS)	20
2023-01-13	Software as a Service (SaaS)	Be able to describe the advantages and disadvantages of SaaS	20
2023-01-13	MongoDB: An Introduction	A basic understanding of NoSQL Databases	100
2023-01-13	Linux CLI: Using Screen	Describe how `screen` works in the CLI	100
2023-01-13	Linux CLI: Combining Commands	Identify the different ways of combining commands on the terminal	200
2023-01-13	Linux CLI: Generating File Hashes	Recognize file hashes	100
2023-01-12	Linux CLI: Using Find	Recognize how the find command work	200
2023-01-12	Linux CLI: Searching and Sorting	Employ searching techniques to find patterns in files	100
2023-01-12	Linux CLI: Using SSH and SCP	Recall what the SSH protocol is	100
2023-01-04	World Cup Special: It's a Game of Pong	Develop critical thinking	100
2022-12-30	Compliance: The NCSC's 10 Steps to Cybersecurity	Describe each of the 10 Steps to Cybersecurity	20
2022-12-30	Compliance: Legislation, Regulation, and Standards	Describe the differences between compliance, legislation, regulation, and standards	10
2022-12-30	Compliance: Policies, Processes, and Procedures	Recall the differences between policies, processes, and procedures	10
2022-12-30	Compliance: Accreditation	Describe the accreditation process	10
2022-12-29	Digital Forensics Process: Collection – Evidence Acquisition and Protection	Recognize how to protect evidence during collection	40

Activity Report Page 83 of 98

Date	Lab	Description	Points Earned
2022-12-29	Digital Forensics: Windows Image Analysis	Investigate and analyze operating systems using common forensic techniques	300
2022-12-28	What Is Risk?	Define the core concepts that formulate risk	20
2022-12-27	Protocols: LDAP	Analyze the LDAP protocol in an enterprise context	100
2022-12-27	Protocols: ARP	Identify packet structure of ARP requests and responses	100
2022-12-27	Stack Overflow	Recall the risks of using code found online	10
2022-12-27	Cryptocurrency and Blockchain	An introduction to cryptocurrency and blockchain concepts	10
2022-12-27	Linux CLI: Using Sudo	Identify different user privileges in Linux	100
2022-12-27	Defense in Depth	Discover the principles of defense systems	20
2022-12-27	Linux CLI: Manipulating Text	Modify text within files using basic command line tools	200
2022-12-27	Linux CLI: Stream Redirection	Describe how data can be manipulated via the terminal	100
2022-12-27	Intrusion Detection Systems	Recognize what an IDS is and how they're used	20
2022-12-27	IoT & Embedded Devices: What Is IoT?	Recognize IoT devices and their associated risks	10
2022-12-16	The Typex Machine	Recognize how a Typex machine works	200
2022-12-16	Infrastructure Hacking: XSL Script Processing	Recognize how XSL files can obscure malicious code with embedded scripts	200
2022-12-16	Exploitation Development: Data Compression	Recognize how data compression can be used to exfiltrate data	100

Activity Report Page 84 of 98

Date	Lab	Description	Points Earned
2022-12-16	Protocols: HTTP – Status Codes	Develop knowledge of HTTP status codes	100
2022-12-16	Protocols: FTP	Explain the core concepts of the File Transfer Protocol	100
2022-12-16	Encryption Tools: CyberChef — Recipes	Recall how CyberChef recipes work	40
2022-12-16	Incident Response: Parsing PST	Investigate email client files	200
2022-11-22	Tactics: Defense Evasion	Recognize the purpose of the MITRE ATT&CK® Defense Evasion tactic	20
2022-11-22	Tactics: Privilege Escalation	Recognize the purpose of the MITRE ATT&CK® Privilege Escalation tactic	20
2022-11-22	Tactics: Persistence	Recognize the purpose of the MITRE ATT&CK® Persistence tactic	20
2022-11-22	Tactics: Execution	Know the purpose of the MITRE ATT&CK® Execution tactic	20
2022-11-22	Threat Hunting: Analyzing Sandbox Reports	Investigate malicious samples using sandbox reports	100
2022-11-21	Threat Hunting: STIX	Locate Cyber Threat Information from within STIX objects	40
2022-11-21	Threat Hunting: VirusTotal	Demonstrate how to use malware analysis tools	100
2022-11-21	Threat Hunting: Introduction	Describe threat hunting concepts	40
2022-11-21	Threat Hunting: Honeypots	Describe what a honeypot is	200
2022-11-18	Tools Leak — Who is APT34?	Familiarize yourself with APT34	40
2022-11-10	Linux CLI: Introduction to the Linux Command Line Interface	Recall Linux command line fundamentals	40

Activity Report Page 85 of 98

Date	Lab	Description	Points Earned
2022-11-10	Linux CLI: Getting Started with the Terminal	Recall fundamental concepts of the Linux terminal	100
2022-11-10	Linux CLI: File Permissions	Read Linux file permissions	100
2022-11-10	Linux CLI: Editing Files	Be able to recall some common Linux command line text editors	100
2022-11-10	Linux CLI: Using wc	Count elements in a file using the wc tool	200
2022-11-10	Linux CLI: Changing Things	Recall the Linux CLI commands explored in the lab	100
2022-11-10	Linux CLI: Moving Around	Navigate through directories on the command line	100
2022-11-08	The Internet	Explain the history of the internet	20
2022-11-08	Introduction to Encryption	Identify different types of encryption algorithms	100
2022-11-08	Introduction to Hashing	Identify the characteristics of a good hashing algorithm	100
2022-11-08	OSI Model	Identify the different layers of the OSI model	40
2022-11-08	Rainbow Tables	Describe what a rainbow table is	40
2022-11-08	Ports	Identify how ports are used in modern networks	40
2022-11-08	Transport Protocols	Explain the core concepts of the the most common transport protocols	40
2022-11-08	Internet Protocol V4	Explain the core concepts of IPv4 addressing	100
2022-11-08	Symmetric vs Asymmetric Key Encryption	Apply symmetric key encryption and decryption techniques	100

Activity Report Page 86 of 98

Date	Lab	Description	Points Earned
2022-11-08	Modern Encryption: MD5 Hashing	Recall what MD5 hashing is and how it works	100
2022-11-08	Modern Encryption: SHA-1 Hashes	Recall what SHA-1 hashing is and how it works	100
2022-10-27	Validating SIEM Results	Identify whether an SIEM's actions are accurate in any given scenario	40
2022-10-27	Burp Suite Basics: Introduction	Set up and use Burp Suite with Firefox	100
2022-10-27	Introduction to Incident Response: Process	Recognize and outline the stages of the incident response process	40
2022-10-27	Introduction to Incident Response: Introduction	Describe what an incident is	40
2022-10-25	CVE-2019-0708 (BlueKeep) – Offensive	Exploit BlueKeep	200
2022-10-25	CVE-2019-0708 (BlueKeep: Snort Rule)	Apply principles of how security teams may update systems in preparation for known threats	100
2022-10-25	The Enigma Machine	Recall how the Enigma machine works	200
2022-10-25	Encryption Tools: CyberChef	Recall how CyberChef functions	40
2022-10-25	Caesar Ciphers	Recall how Caesar cipher encoding works	40
2022-10-21	CVE-2019-17387 (Aviatrix VPN Client Privilege Escalation)	Exploit CVE-2019-17387 to escalate privileges	200
2022-10-20	CVE-2019-1388 (Windows Priv Esc UAC Bypass)	Bypass User Account Controls	200
2022-10-17	Cyber 101: Rogue USB Devices	Recall how rogue USB devices can be used for malicious purposes	10
2022-10-17	Cyber 101: Who Are The Hackers?	Recognize the different types of hackers	10

Activity Report Page 87 of 98

Date	Lab	Description	Points Earned
2022-10-17	Cyber 101: Why Hackers Hack	Recognize some of the methods used by hackers	10
2022-10-17	Cyber 101: Virtual Card Numbers	Identify the different types of virtual card numbers	10
2022-10-17	Cyber 101: Fake News	Recognize the characteristics of fake news	10
2022-10-17	Cyber 101: Keylogging	Recognize what keyloggers are	10
2022-10-17	Cyber 101: Geolocation	Recognize the differences between device-based and server-based geolocation tracking	10
2022-10-17	Cyber 101: Darknets	Recognize how darknets operate on the internet	10
2022-10-17	Cyber 101: Cookies	Recognize how cookies are used by organizations	20
2022-10-14	Cyber 101: Information Security	Recognize the importance of information security for individuals and organizations	10
2022-10-14	Cyber 101: Security Champions	Explain what a security champion is and their purpose	10
2022-10-14	Cyber 101: Cyber Kill Chain	Recognize the purpose of the cyber kill chain	10
2022-09-29	Windows Concepts: CertUtil	Analyze the function of CertUtil	100
2022-09-29	Windows Concepts: Background Intelligent Transfer Service (BITS)	Gain an understanding of BITS and how it can be abused	100
2022-09-29	Windows Concepts: Scheduled Tasks	Demonstrate how to navigate information in Windows Scheduled Tasks	100
2022-09-29	Windows Concepts: Windows Registry	Evaluate registry values	100
2022-09-29	Windows Concepts: New Technology File System (NTFS)	Analyze Windows file permissions	100

Activity Report Page 88 of 98

Date	Lab	Description	Points Earned
2022-09-28	Incident Response in the Workplace	Recall the advantages of an incident response plan	10
2022-09-28	Introduction to Networking: IP Addresses	Recognize an IP address	40
2022-09-28	Personal Devices in the Workplace	Recognize the risks associated with using personal devices in the workplace	10
2022-09-28	History of Information Security	Recall some of the key moments for information security throughout history	10
2022-09-28	Introduction to Networking: Domain Name System	Summarize the fundamentals of the Domain Name System	40
2022-09-27	Guidance on Remote Working	Identify the risks associated with remote working	10
2022-09-27	Security On The Go	Recognize the security risks of using devices when away from the office	10
2022-09-27	The Importance of Information Security and Cybersecurity	Describe a simulated example of a breach and recall its emotional impact	10
2022-09-27	Privileged Access	Recall what privileged access is and why it's an attractive target for attackers	10
2022-09-27	Physical Security	Identify common physical security risks	10
2022-09-27	Privacy	Identify what privacy is and why it needs protecting	10
2022-09-27	What Is Information Security?	Identify the workplace and personal security challenges that good information security practices help to solve	10
2022-09-27	Disposal of Device Information	Recognize why secure device disposal is core to an organization’s information management process	10
2022-09-27	Information Security and Cybersecurity Terminology	Recall some key information security and cybersecurity terms and phrases	10
2022-09-27	Information Security: Starting at the Beginning	Recall the difference between information security and cybersecurity	10

Activity Report Page 89 of 98

Date	Lab	Description	Points Earned
2022-09-27	Social Engineering	Describe different social engineering attack techniques and their impacts	10
2022-09-27	Spiderfoot	Scan and analyze data using specialty OSINT tools	40
2022-09-27	Open Source Intelligence (OSINT): Shodan.io	Gain an understanding of the Shodan.io search engine and how to run queries	20
2022-09-27	Nmap: Using Nmap	Recall how to run Nmap	200
2022-09-27	Scanning: DNS Zone Transfer	Analyze DNS information revealed by a zone transfer	200
2022-09-27	Open Source Intelligence (OSINT): Deleted Tweet	Analyze information using open source intelligence techniques	40
2022-09-27	Scanning: Banner Grabbing	Identify and enumerate common services	100
2022-09-27	Scanning: Network Scanning	Operate various network scanning tools to identify open ports	100
2022-09-27	Open Source Intelligence (OSINT): Default Credentials	Knowledge of default credentials	20
2022-09-27	Open Source Intelligence (OSINT): Domain Intel	Understand the information associated with domain names	40
2022-09-27	Tor	Describe how Tor works	40
2022-09-27	Shoulder Surfing	Recognize how shoulder surfing works and the various ways it can be employed	10
2022-09-26	Open Source Intelligence (OSINT): Search Engines	Recognize the difference between the surface web, deep web, and dark web	20
2022-09-26	Open Source Intelligence (OSINT): Online Anonymity	Describe how to increase your online anonymity	40
2022-09-26	Open Source Intelligence (OSINT): Cached and Archived Websites	Interpret and analyze information collected from web archives	20

Activity Report Page 90 of 98

Date	Lab	Description	Points Earned
2022-09-26	Open Source Intelligence (OSINT): EXIF	Identify types of data stored in images	40
2022-09-26	Reverse Image Search	Demonstrate the basics of reverse image searching	40
2022-09-26	Open Source Intelligence (OSINT): Robots.txt	Identify resources in robots.txt files	40
2022-09-26	Open Source Intelligence (OSINT): Investigator Operations Security (OPSEC)	Use OSINT techniques to gather information	40
2022-09-26	Open Source Intelligence (OSINT): Social Media and Privacy	Recognize the perils of having too much information on social media	10
2022-09-23	Staying Safe Online: Accidental and Malicious Data Leaks	Recognize the differences between accidental leaks and malicious leaks	10
2022-09-23	Staying Safe Online: Covid-19 Cybercriminals	Identify the characteristics of Covid-19 phishing scams	10
2022-09-23	Staying Safe Online: Identifying Ransomware	Recognize the tell-tale signs of ransomware	10
2022-09-23	Staying Safe Online: Updates and Patches	Identify the differences between updates and patches	10
2022-09-23	Staying Safe Online: Firewalls and VPNs	Recognize the benefits of firewalls and VPNs	10
2022-09-23	Staying Safe Online: Consequences and Impacts of Cyberattacks	Define what a cyberattack is	10
2022-09-23	Staying Safe Online: Why Information Security is Everyone's Business	Recognize the importance of information security	10
2022-09-23	Staying Safe Online: Passwords	Recognize how to protect yourself and your devices with strong passwords	10
2022-09-23	Staying Safe Online: Antivirus Software	Identify the purpose of antivirus software and its main features	10
2022-09-23	Staying Safe Online: Mobile Security Tips	Identify potential threats to mobile phone security	10

Activity Report Page 91 of 98

Date	Lab	Description	Points Earned
2022-09-23	Staying Safe Online: Identity Theft	Recognize the ways to prevent identity theft and the warning signs to look out for	10
2022-09-23	Staying Safe Online: Backups	Recognize the importance of backups	10
2022-09-23	Staying Safe Online: Multi-Factor Authentication	Recall how multi-factor authentication works	10
2022-09-23	Staying Safe Online: Safer Browsing	Recall how to protect yourself and your privacy as you browse the web	10
2022-09-23	Staying Safe Online: Phishing Emails	Recognize the main characteristics of phishing emails	10
2022-09-23	Staying Safe Online: Malware	Recognize the most common forms of malware and how they can affect you	10
2022-09-22	Incident Response: Suspicious Email – Initial Inspection	Investigate and gain information from suspected malicious documents.	200
2022-09-21	Encoding: Binary	Recall how binary functions	40
2022-09-16	Immersive Bank: Open Source and Credentials	Employ open-source intelligence to uncover the CEO's password	200
2022-09-15	Port Bingo: Easy Mode	Develop your knowledge of port numbers and their services	100
2022-04-25	APT29 Threat Hunting with Elasticsearch: Deploy Stealth Toolkit	Identify various tactics from the MITRE ATT&CK framework	200
2022-04-19	Zeek: Log Analysis	Identify information in Zeek logs	200
2022-04-19	FIN7 Threat Hunting with Splunk: Execution Logs	Observe and recognize the techniques used by the FIN7 threat group during an attack	200
2022-04-15	APT29 Threat Hunting with Elasticsearch: Rapid Collection and Exfiltration	Identify various tactics from the MITRE ATT&CK framework	200
2022-04-14	Malicious Documents Analysis: Copy and Paste Compromise	Demonstrate the ability to analyze malicious visual basic commands	300

Activity Report Page 92 of 98

Date	Lab	Description	Points Earned
2022-04-14	PowerPoint as a Malware Dropper	Investigate indicators of compromise from malicious Microsoft Office documents	200
2022-04-08	FIN7 Threat Hunting with Splunk: Initial Access	Demonstrate how to parse and extract elements from an RTF document	200
2022-03-31	APT29 Threat Hunting with Elasticsearch: Initial Compromise	Identify various tactics from the MITRE ATT&CK framework	200
2022-03-30	Ransomware: Petya/NotPetya	Safe ransomware observation	200
2022-03-29	Malware Analysis: HTTPotato.dll	Demonstrate ability to analyze C# DLLs and associated exploits	300
2022-03-29	Yara: Boolean Operators	Investigate unique data related to malware samples	200
2022-03-29	Yara: Creating Rules	Investigate unique data related to malware samples	200
2022-03-29	Wireshark: Stream/Object Extraction	Analyze network packet captures	200
2022-03-28	Wireshark: Display Filters – Combining Filters	Analyze network packet captures using multiple operators	200
2022-03-25	APT34: PoisonFrog	Analyze the PoisonFrog malware	200
2022-03-24	Snort Rules: HTTP	Demonstrate usage of Snort rules	300
2022-03-24	Snort Rules: DNS	Create Snort rules for DNS events	300
2022-03-23	Snort Rules: Introduction	Demonstrate proficiency in basic Snort rules	200
2022-03-22	APT34: HighShell PCAP	Identify methods of compromise used by threat actors	200
2022-03-21	Ransomware: Conti – Source Code Analysis	To be able to review malware source code to identify indicators of compromise	200

Activity Report Page 93 of 98

Date	Lab	Description	Points Earned
2022-03-21	Hermetic Wiper: Ghidra Analysis	Identify log-based IoCs from a malware binary	300
2022-03-21	CVE-2021-44228 (Log4j) – Defensive	Identify server components vulnerable to Log4Shell	100
2022-03-14	Hafnium: DearCry Ransomware	Safely observe DearCry ransomware	100
2022-03-11	Zeek: Working with PCAPs	Recall the different formats Zeek outputs logs into	100
2022-03-11	Threat Hunt Theory: Mapping Adversaries	Understand how to map adversaries to the MITRE ATT&CK® framework	40
2022-03-11	Threat Hunt Theory: Hypothesis Creation	Recognize how to create a threat hunting hypothesis	40
2022-03-09	Zeek: Log Types and Formats	Recognize what Zeek logs are	40
2022-03-09	Threat Hunt Theory: Introduction	Understand the fundamental concepts of threat hunting	40
2022-03-08	What is Zeek?	Recognize the key features of Zeek	20
2022-03-08	Web Log Analysis: Access Logs	Recognize web server access logs	100
2022-03-08	Web Log Analysis: Log Formats	Describe the different types of web server log formats	20
2022-03-08	Web Log Analysis: What are Web Server Logs?	Recall the different types of web server logs	20
2022-03-08	Tactics: Reconnaissance	Recognize the purpose of the MITRE ATT&CK® Reconnaissance tactic	20
2022-03-08	Tactics: Resource Development	Recognize the purpose of the MITRE ATT&CK® Resource Development tactic	20
2022-03-08	FIN7 Threat Hunting with Splunk: What is FIN7?	Recall the most commonly targeted sectors	40

Activity Report Page 94 of 98

Date	Lab	Description	Points Earned
2022-03-08	Tactics: Initial Access	Recognize the purpose of the MITRE ATT&CK® Initial Access tactic	20
2022-03-08	Introduction to MITRE ATT&CK®	Be familiar with the MITRE ATT&CK® framework and know how it's used	20
2022-03-08	Practical Malware Analysis: Dynamic Analysis	Describe what dynamic analysis is and how it's used for malware analysis	40
2022-03-08	Wireshark: Display Filters – Introduction to Filters	Analyze network packet captures	100
2022-03-08	Wireshark: Introduction to Wireshark	Analyze network packet captures	100
2022-01-31	Java: XSS Everywhere	Demonstrate remediation techniques for vulnerabilities in code caused by unsanitised parameters	400
2022-01-13	Cross-Site Request Forgery	Explain what cross-site request forgery (CSRF) attacks are	200
2021-12-27	Python: Forced Browsing	Know what a forced browsing vulnerability is and how it works	100
2021-12-22	PowerShell Deobfuscation – Challenge 11	Analyze multi-stage payloads	400
2021-12-20	PowerShell Deobfuscation – Challenge 4	Analyze multi-stage payloads	200
2021-12-17	PowerShell Deobfuscation – Challenge 6	Analyze multi-stage payloads	200
2021-12-17	PowerShell Deobfuscation – Challenge 5	Analyze multi-stage payloads	200
2021-12-17	PowerShell Deobfuscation – Challenge 3	Analyze multi-stage payloads	100
2021-12-13	PowerShell Deobfuscation – Challenge 2	Analyze multi-stage payloads	100
2021-12-13	PowerShell Deobfuscation – Challenge 1	Analyze multi-stage payloads	100

Activity Report Page 95 of 98

Date	Lab	Description	Points Earned
2021-12-03	Trash Talk	Demonstration of critical thinking	400
2021-12-02	Ransomware: WastedLocker – Unpacking	Setting breakpoints	400
2021-11-21	Halloween 2020: JinjaBread Man	Employ server-side template injection (SSTI) techniques to achieve command execution on this server	400
2021-11-03	CVE-2021-3156 (Baron Samedit) – Offensive	Demonstrate your practical ability to escalate privileges using proof of concept code	200
2021-11-01	CVE-2021-3156 (Baron Samedit) – Defensive	Know how to filter Auditd and Linux Auth logs in Splunk	300
2021-10-27	Ransomware: WastedLocker – Decryption	Use custom ransomware decrypter	100
2021-10-26	Ransomware: WastedLocker – Execution	Observe WastedLocker ransomware safely	40
2021-10-15	Nobelium: EnvyScout	Analyze a Nobelium implant	200
2021-10-14	ASP.NET MVC: Broken Session Management	Know what a broken session management vulnerability is	200
2021-10-14	SuperSonic: LIFTON	Analyze imagery for codes and hidden files	200
2021-10-12	Open Source Intelligence (OSINT): Boarding Pass	Describe what type of information a boarding pass barcode contains	100
2021-10-10	SUNBURST: BusinessLayer.dll Analysis	Identify and extract relevant IoCs from a .NET DLL	400
2021-10-08	Malware Analysis: Quasar RAT	Investigate encryption methods related to popular RATs	600
2021-10-05	OWASP 2021: Injection	Explain injection's position in the OWASP Top 10	20
2021-10-05	Introduction to the OWASP Top 10	Summarize the objectives of the OWASP	10

Activity Report Page 96 of 98

Date	Lab	Description	Points Earned
2021-10-05	CVE-2021-25281 (SaltStack) – Defensive	Be able to identify forensic evidence left behind after a SaltStack compromise	200
2021-09-30	CVE-2020-11651 (SaltStack RCE) – Defensive	Identify forensic evidence left behind after a SaltStack compromise	300
2021-09-30	CVE-2019-19781 (Citrix RCE) – Defensive	Create Snort rule for malicious traffic	200
2021-09-29	CVE-2021-25281 (SaltStack) – Offensive	Be able to identify and exploit vulnerable SaltStack instances	200
2021-09-29	CVE-2020-11651 (SaltStack RCE) – Offensive	Exploit the server	200
2021-09-23	Nobelium: BoomBox	Be able to reverse engineer a Nobelium downloader	200
2021-09-16	Hafnium: Event Log Analysis	Be able to use Windows Event Viewer to identify threats	200
2021-09-06	SUNBURST: Build Server Investigation	Identify and investigate a breach in a compromised build server	400
2021-09-03	Threat Research: Signalling System No.7 (SS7) Interception	Investigate two-factor authentication vulnerabilities linked to the SS7 protocol	300
2021-09-02	CVE-2020-1472 (Zerologon) – Offensive	Use public PoCs to exploit domain controllers	300
2021-09-01	Halloween 2020: The SeQueL	Employ SQLi techniques to extract hidden database tables	200
2021-08-30	Threat Hunting: Zerologon Live Logs	Identify logs related to Zerologon	200
2021-08-30	APT34: Glimpse	Demonstrate an ability to identify Indicators of Compromise in malware with command line tools	200
2021-08-28	CVE-2020-28243 (SaltStack Local Priv Esc) – Offensive	Know how to use the POC in order to escalate privileges on a SaltStack minion	100
2021-08-28	SuperSonic: TEMPLE	Analyze an attack to identify an attacker's actions	200

Activity Report Page 97 of 98

Date	Lab	Description	Points Earned
2021-08-26	Nobelium: Network Analysis	Be able to detect Nobelium network traffic	100
2021-08-20	CVE-2020-5902 (F5 BIG-IP) – Offensive	Exploit CVE-2020-5902 to gain root access to a BIG-IP server	200
2021-08-19	Halloween 2020: Autopsy Report	Recover deleted files	200
2021-08-18	Halloween 2020: Decomposing	Solving nested archives	200
2021-08-18	Events & Breaches: Unauthenticated Elasticsearch	Identify weaknesses in unauthenticated Elasticsearch instances	200
2021-08-17	Hafnium: Yara Scanning	Be able to use YARA to identify malware	100
2021-08-16	Nobelium: NativeZone and VaporRage	Be able to identify key elements of a DLL loader	300
2021-08-13	CVE-2020-5902 (F5 BIG-IP) – Defensive	Identify evidence on a compromised F5 BIG-IP appliance	200
2021-08-11	Kate's Story: Forensic Investigation	Identify actions taken by an attacker and the exploit they employed	100
2021-08-11	Kate's Story: Clicking the Link	Awareness of the potential risk posed by seemingly harmless documents	300
2021-08-06	SuperSonic: INSOMNIA	Analyze data in various formats	100
2021-08-06	Rebel Intercept	Demonstration of critical thinking	200
2021-08-05	It's a Trap!	Demonstrate critical thinking	400
2021-08-05	Mal Wars	Analyze multiple payloads	200
2021-08-03	ASP.NET MVC: XXE Read Files	Know what an XXE vulnerability is and how it works	100

Activity Report Page 98 of 98

Date	Lab	Description	Points Earned
2021-08-02	SuperSonic: TOWER	Analyze a post-attack packet capture file	100
2021-07-27	SuperSonic: FLYING FISH	Demonstrate cracking passwords using John the Ripper	100
2021-07-26	Python: Debug Console	Have an awareness of the impact and consequences of leaving a debug console enabled	100
2021-07-26	SuperSonic: BEVERLEY	Demonstrate Open Source Intelligence techniques	100
2021-07-23	SUNBURST: Identifying IoCs	Be able to recognize IoCs and know how to search for them	100
2021-07-23	Master Code Breaker	Develop critical thinking	200
2021-07-22	Kate's Story: Gathering Intelligence	Apply cyberstalking techniques to find information on Kate	200
2021-07-16	Nobelium: Introduction	Be able to explain what Nobelium is and recognize the tools and tactics used by the group	40
2021-02-09	SuperSonic: FORUM	Use OSINT analysis techniques to identify details of a cyberattack	100
2020-12-22	SUNBURST: Who are UNC2452?	Be able to explain who UNC2452 are and recognize the tools and tactics used by the group	20
2020-12-22	SUNBURST: Compromising SolarWinds Orion	Become familiar with the timeline of the SolarWinds compromise	40

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.