IMMERSIVELABS

Zachary Wilson

Completed 611 labs earning 54470 points.

Activity Report

Date	Lab	Description	Points Earned
2022-12-15	Systems Manager – Patching and Compliance	Recognize SSM patch manager terminology	200
2022-12-15	Systems Manager – Demonstrate Your Skills	Demonstrate an understanding of AWS Systems Manager	300
2022-12-12	Introduction to OAuth 2.0 – Ep.2	Recall OAuth 2.0 tokens and scopes	100
2022-12-12	Introduction to OAuth 2.0 – Ep.1	Recall the key principles of OAuth 2.0	20
2022-12-12	Container Scanning – Dockle	Be able to scan Docker containers for vulnerabilities	100
2022-12-06	HashiCorp Vault – Secrets Engines	Recognize the different types of secrets engine available in Vault	100
2022-12-06	Container Scanning: Ep.2 – Trivy II	Gain knowledge on scanning container images for vulnerabilities	100
2022-12-06	Container Scanning: Ep.1 — Trivy	Gain knowledge on scanning container images for vulnerabilities	100
2022-11-28	Systems Manager – Automation	Produce SSM Automation runbooks to automate tasks	200
2022-11-28	HashiCorp Vault – Authentication	Recognize the use cases for vault authentication mechanisms	100

Activity Report Page 2 of 42

Date	Lab	Description	Points Earned
2022-11-28	HashiCorp Vault – Setup	Set up a Vault server	100
2022-11-21	HashiCorp Vault – Introduction	Recognize Vault's benefits and features	40
2022-11-21	Container Hardening	Recognise the importance of container hardening	40
2022-11-21	Containers	Describe containers and their advantages and disadvantages	20
2022-11-14	Configuring Secure Web Hosting with AWS CloudFront	Recall how to set up a CloudFront Distribution	200
2022-11-14	Securing Web Applications with AWS WAF and CloudFront	Create CloudFront distributions for web-serving origins	300
2022-11-14	AWS WAF and CloudFront – Demonstrate Your Skills	Manage web ACL resources and security rules	300
2022-11-08	ISO 27014: Ep.3 – Demonstrate Your Knowledge	Demonstrate your knowledge of ISO 27014	20
2022-11-08	ISO 27014: Ep.2 – Implementation Processes	Define the processes used to implement ISO 27014	10
2022-11-08	Introduction to AWS Web Application Firewall (WAF)	Recall how to define pattern-matching sets in AWS WAF	200
2022-11-01	ISO 27018: Ep.5 – Demonstrate Your Knowledge	Recall the information on ISO 27018	20
2022-11-01	ISO 27018: Ep.4 – Access Control, Asset Management, and Cryptography	Recognize the elements that govern access control, asset management, and cryptography	10
2022-11-01	ISO 27014: Ep.1 – Introduction	Recognize what the ISO 27014 standard is	10
2022-10-24	ISO 27018: Ep.3 – Operations and Communications Security	Recognize the elements that make operational security important for protecting the integrity of PII	20
2022-10-24	ISO 27018: Ep.2 – Human Resource and Physical Security	Define the human elements that can impact PII data integrity in the cloud	10

Activity Report Page 3 of 42

Date	Lab	Description	Points Earned
2022-10-24	ISO 27018: Ep.1 – Introduction	Recall the scope of ISO 27018 and why it's important	10
2022-10-21	IAM – Permissions Boundaries	Identify the use cases for permissions boundaries	300
2022-10-20	ISO 27001: Ep.5 – Conclusion and Knowledge Check	Recall the knowledge gained from previous labs on the ISO 27001 Annex A controls	20
2022-10-20	ISO 27001: Ep.4 – Systems, Suppliers, and Incidents	Recognize the purpose of ISO 27001 Annex A controls 14, 15, 16, 17, and 18	10
2022-10-20	IAM – Security Token Service (STS)	Recognize the offering of the security token service	100
2022-10-17	ISO 27001: Ep.2 – Policy, Process, Organization, People, Assets	Recognize the purpose of ISO 27001 Annex A controls 5, 6, 7, and 8	10
2022-10-17	ISO 27001: Ep.3 – Access, Cryptography, Security	Recognize the purpose of ISO 27001 Annex A controls 9, 10, 11, 12, and 13	10
2022-10-12	Systems Manager – Inventory	Recognize how SSM software inventory can provide insight into installed software on your managed-node	100
2022-10-10	Systems Manager – Session Manager	Recognize Session Manager's benefits and features	100
2022-10-10	Systems Manager – Introduction	Recognize the benefits of Systems Manager	100
2022-10-10	Systems Manager – Run Command	Recognize the benefits of System Manager Run Command	100
2022-10-04	IAM – Access Advisor	Recall how to interpret Access Advisor results	100
2022-10-04	IAM – Resource Policies	Demonstrate how to create resource policies	200
2022-10-04	IAM – Multi-Factor Authentication	Recall how to configure an MFA device as an AWS security credential	200
2022-10-03	IAM – Access Analyzer	Be able to construct Access Analyzer access archive rules	100

Activity Report Page 4 of 42

Date	Lab	Description	Points Earned
2022-10-03	IAM – Tagging	Tag resources for ease of management	100
2022-10-03	IAM – Users and Groups	Recognize different AWS IAM resources	100
2022-10-03	IAM – Roles	Recognize IAM role functionality	100
2022-10-03	IAM – Policy	Recall how to scope policies for least privilege security controls	100
2022-09-30	Secure Terraform – GCP Ep.3	Discover vulnerabilities in Terraform IaC	300
2022-09-30	Secure Terraform – GCP Ep.2	Discover vulnerabilities in Terraform IaC	200
2022-09-30	Secure Terraform – GCP Ep.1	Discover vulnerabilities in Terraform IaC	200
2022-09-28	AWS Logging and Monitoring – Demonstrate Your Skills	Demonstrate an understanding of logging fundamentals in AWS	300
2022-09-28	Secure Terraform – Azure Ep.3	Be familiar with security recommendations for Azure resources	300
2022-09-27	Secure Terraform – Azure Ep.2	Discover security recommendations for Azure resources	200
2022-09-27	Secure Terraform – Azure Ep.1	Discover security recommendations for Azure resources	200
2022-09-26	EC2 – Key Pairs	Recognize the use of key pairs in EC2	100
2022-09-26	Secure Terraform – AWS Ep.4	Discover vulnerabilities in Terraform IaC	200
2022-09-26	Secure Terraform – AWS Ep.3	Discover vulnerabilities in Terraform IaC	200
2022-09-26	Secure Terraform – AWS Ep.2	Discover vulnerabilities in Terraform IaC	200

Activity Report Page 5 of 42

Date	Lab	Description	Points Earned
2022-09-26	Secure Terraform – AWS Ep.1	Discover vulnerabilities in Terraform IaC	200
2022-09-22	AWS Logging and Monitoring – Automating Incident Response with EventBridge	Recall how to create and configure EventBridge rules and targets	200
2022-09-22	AWS Logging and Monitoring – CloudTrail SIEM Integration (Splunk)	Demonstrate how to integrate CloudTrail logs with Splunk	300
2022-09-21	AWS Logging and Monitoring – Configuring VPC Flow Logs	Recall how to create and configure VPC flow logs	200
2022-09-19	AWS Logging and Monitoring – Deploying CloudTrail	Navigate the CloudTrail console	100
2022-09-19	AWS Logging and Monitoring – CloudWatch Alarms and Metric Filters	Construct queries using basic metric filter syntax	200
2022-09-19	AWS Logging and Monitoring – Configuring EventBridge and Event Patterns	Navigate the AWS EventBridge Management Console	100
2022-09-19	AWS Logging and Monitoring – CloudWatch CIS Alarms	Construct queries using basic metric filter syntax	200
2022-09-19	AWS Logging and Monitoring – Introduction to EventBridge	Identify the core features of Amazon EventBridge	10
2022-09-19	AWS Logging and Monitoring – The CloudWatch Dashboard	Navigate the CloudWatch console	100
2022-09-19	AWS Logging and Monitoring – Introduction to CloudWatch	Identify the core features of AWS CloudWatch	20
2022-09-15	Python: Insecure Deserialisation	Know what an insecure deserialisation vulnerability is	100
2022-09-14	Kubernetes - Logging	Know how logs from containerised applications and Kubernetes resources can be accessed	200
2022-09-12	Python: Vulnerable Library	Have an awareness of the impact and consequences of using a vulnerable library within an application	40
2022-09-12	Python: Broken Session Management	Know what a broken session management vulnerability is	100

Activity Report Page 6 of 42

Date	Lab	Description	Points Earned
2022-09-12	Python: Missing Authentication Logs	Have an awareness of the impact and consequences of missing authentication logging	40
2022-09-12	Python: Debug Console	Have an awareness of the impact and consequences of leaving a debug console enabled	100
2022-09-12	What is Terraform?	Explain the benefits of Terraform for managing infrastructure	20
2022-09-09	Python: XML External Entities (XXE)	Know what an XXE vulnerability is and how it works	100
2022-09-09	Python: Forced Browsing	Know what a forced browsing vulnerability is and how it works	100
2022-09-08	Python: Reflected XSS	Know what a reflected XSS vulnerability is and how it works	100
2022-09-08	Python: Default Error Pages	Have an awareness of the impact and consequences of enabling default error pages in an application	40
2022-09-08	Python: Stored XSS	Know what a stored cross-site scripting (XSS) vulnerability is and how it works	100
2022-09-06	Python API: Hardcoded Secrets	Recognize the impact and consequences of using hardcoded secrets	40
2022-09-06	Introduction to API Vulnerabilities	Describe an application programming interface (API)	20
2022-09-06	Python API: Introduction	Use the Swagger GUI to send requests	20
2022-09-06	Python: Hardcoded Secrets	Recognize the impact and consequences of using hardcoded secrets	100
2022-09-06	Python: SQL Injection	Know what an SQL injection vulnerability is and how it works	100
2022-09-06	Python: Code Comments	Have an awareness of the impact and consequences of leaving sensitive details in code comments	40
2022-08-29	Search Engines	Recognise the difference between the surface web, deep web, and dark web	20

Activity Report Page 7 of 42

Date	Lab	Description	Points Earned
2022-08-29	Online anonymity	Describe how to increase your online anonymity	40
2022-08-29	Cached and Archived Websites	Interpret and analyse information collected from web archives	20
2022-08-29	Spiderfoot	Scan and analyse data using speciality OSINT tools	40
2022-08-29	Shodan.io	Gain an understanding of the Shodan.io search engine and how to run queries	20
2022-08-29	Open Source Intelligence (OSINT): Boarding Pass	Describe what type of information a boarding pass barcode contains	100
2022-08-29	Open Source Intelligence (OSINT): Deleted Tweet	Analyse information using open source intelligence techniques	40
2022-08-29	EXIF	Knowledge in the various sorts of data that is stored in images	40
2022-08-29	Reverse Image Search	Demonstrate the basics of reverse image searching	40
2022-08-29	Robots.txt	Identify website information leakage	40
2022-08-29	Domain Intel	Understand the information associated with domain names	40
2022-08-29	Tor	Describe how Tor works	40
2022-08-29	Investigator Operations Security (OPSEC)	Source online information relevant to an investigation	40
2022-08-29	Social Media and Privacy	Recognise the perils of having too much information on social media	10
2022-08-25	Yara: Ep.5	Investigate unique data related to malware samples	200
2022-08-25	Yara: Ep.4	Investigate unique data related to malware samples	200

Activity Report Page 8 of 42

Date	Lab	Description	Points Earned
2022-08-23	The Sarbanes-Oxley Act	Explain the purpose of the Sarbanes-Oxley Act	10
2022-08-23	EU-US Privacy Shield Ruled Invalid	Recall what the Privacy Shield is	10
2022-08-23	Payment Services Directive 2 (PSD2)	Describe how PSD2 works and affects the banking industry	10
2022-08-23	Information Technology Health Check (ITHC)	Recognize why an information technology health check is carried out	20
2022-08-23	Health Insurance Portability and Accountability Act (HIPAA)	Describe the five titles that form the structure of HIPAA	20
2022-08-23	Payment Card Industry Data Security Standard (PCI-DSS)	Recall the different PCI-DSS control objectives	40
2022-08-23	NIS Directive	Recognize what the NIS Directive is and how it protects the countries in the EU	20
2022-08-23	Cyber Essentials	Identify the most common attacks outlined by the Cyber Essentials scheme	20
2022-08-22	GDPR	Recognize the key details of the GDPR	10
2022-08-22	ISO 27001: Ep.1 – What Is ISO 27001?	Identify why the ISO 27001 standard is used	20
2022-08-22	The NCSC's 10 Steps to Cybersecurity	Describe each of the 10 Steps to Cybersecurity	20
2022-08-16	Kubernetes – Native Logging	Be able to implement Kubernetes native logging securely	100
2022-08-15	Cyber Insurance	Recognise the risks associated with cyberattacks and cyber insurance	10
2022-08-15	Policies, Processes, and Procedures	Recall the differences between policies, processes, and procedures	10
2022-08-15	Accreditation	Describe the accreditation process	10

Activity Report Page 9 of 42

Date	Lab	Description	Points Earned
2022-08-11	EC2 – Auto Scaling	Recognize the availability improvements offered by Auto Scaling	200
2022-08-11	EC2 – Load Balancers	Recognize the different types of AWS load balancers	200
2022-08-11	EC2 – Demonstrate Your Skills	Demonstrate an understanding of EC2 fundamentals	300
2022-08-11	Yara: Ep.3	Investigate unique data related to malware samples	200
2022-08-10	IAM and EC2 – Instance Profiles	Recognize the security benefits of using instance profiles	200
2022-08-09	EC2 – Launch Templates	Recognize the benefits of launch templates in EC2	100
2022-08-09	EC2 – Security Groups	Recall the difference between inbound and outbound rules	100
2022-08-09	EC2 – Amazon Machine Images (AMIs)	Recognize the characteristics that define different AMIs	100
2022-08-09	EC2 – Disk Encryption	Recognize characteristics of EC2 disk encryption	100
2022-08-09	EC2 – Practical Introduction	Recognize the components of an EC2 instance	100
2022-08-09	NSA Kubernetes Hardening: Ep6. – Log Auditing 2	Recall the NSA's guidance for logging and auditing within Kubernetes networks	20
2022-08-09	NSA Kubernetes Hardening: Ep5. – Log auditing 1	Recall the NSA's guidance for logging and auditing within Kubernetes networks	20
2022-08-09	NSA Kubernetes Hardening: Ep4. – Authentication & Authorization	Recall the NSA's guidance for adding authentication and authorization controls	20
2022-08-09	NSA Kubernetes Hardening: Ep3. – Network Separation & Hardening	Recall the NSA's guidance for hardening Kubernetes networks	40
2022-08-09	NSA Kubernetes Hardening: Ep2. – Pod Security	Recall the NSA's guidance for securing Kubernetes pods	40

Activity Report Page 10 of 42

Date	Lab	Description	Points Earned
2022-08-09	NSA Kubernetes Hardening: Ep1. – Introduction	Recognize the NSA's recommendations for Kubernetes hardening	10
2022-08-08	NCSC Cloud Security: Ep.14 – Secure Use of the Service	Describe the importance of securely using a cloud service as per NCSC guidelines	20
2022-08-08	NCSC Cloud Security: Ep.13 – Audit Information for Users	Recognise the role audit information plays in cloud security	20
2022-08-08	NCSC Cloud Security: Ep.12 – Secure Service Administration	Recall the recommendations for secure service administration from NCSC.	20
2022-08-08	NCSC Cloud Security: Ep.11 – External Interface Protection	Recognise how to protect external interfaces within cloud environments	20
2022-08-08	NCSC Cloud Security: Ep.9 – Secure User Management	Recognise the importance of secure user management as detailed by NCSC	20
2022-08-08	NCSC Cloud Security: Ep.8 – Supply Chain Security	Recognise the importance of supply chain security according to NCSC	20
2022-08-08	NCSC Cloud Security: Ep.7 – Secure Development	Recall the importance of secure development in cloud	20
2022-08-08	NCSC Cloud Security: Ep.6 – Personnel Security	Recognise why personnel security is important in cloud environments	20
2022-08-08	NCSC Cloud Security: Ep.5 – Operational Security	Recall the elements NCSC recommends understanding within a cloud provider's OPSEC	20
2022-08-08	NCSC Cloud Security: Ep.4 – Governance Framework	Identify how how governance fits in with implementation cloud solutions according to NCSC	20
2022-08-08	NCSC Cloud Security: Ep.3 – Separation Between Users	Recall why user separation is important in cloud environments	20
2022-08-08	NCSC Cloud Security: Ep.2 – Asset Protection and Resilience	Describe the concerns of asset protection and resilience for cloud environments as per the NCSC guidelines	20
2022-08-08	NCSC Cloud Security: Ep.10 – Identity and Authentication	Recognise identity and authentication management and its importance within cloud environments	20
2022-08-08	NCSC Cloud Security: Ep.1 – Data in Transit	Recall the ways in which data can be protected whilst it's in transit, according to NCSC	20

Activity Report Page 11 of 42

Date	Lab	Description	Points Earned
2022-08-08	NCSC Cloud Security Guidance	Recognise NCSC's Cloud Security Guidance at a high level	10
2022-08-05	Kubernetes – Image Security	Describe what admission controllers in Kubernetes are	200
2022-08-05	Kubernetes – Protecting Secrets	Know how information contained within secrets can be protected from compromise	200
2022-08-04	Kubernetes – Resource Policies	Recall the function of resource policies within clusters	100
2022-08-04	Kubernetes – Pod Security Policies	Recognize why you should use pod security policies and how they can protect your cluster	100
2022-08-04	Rewards - Bug Hunter	Earn points by helping to improve the platform	10
2022-08-03	Kubernetes – Immutable File Systems	Demonstrate how to deploy secure pods to a cluster	100
2022-08-02	Kubernetes – Log Forwarding	Investigate Kubernetes logs using a central log management system	100
2022-08-02	Kubernetes – Seccomp Auditing	Recall the importance of filtering dangerous syscalls	100
2022-08-02	Kubernetes – Network Policies	Describe the function of namespaces in defining scopes	100
2022-08-02	Kubernetes - Role Based Access Control	Discern authentication and authorisation concepts	100
2022-08-01	Presenting your Findings	Recall the different ways of presenting evidence	20
2022-08-01	Digital Forensics Tools	Recognize the most common digital forensics tools	20
2022-08-01	Digital Forensics Processes and Techniques	Recall digital forensics processes	40
2022-08-01	Digital Evidence	Define what digital evidence is	20

Activity Report Page 12 of 42

Date	Lab	Description	Points Earned
2022-08-01	Kubernetes - Auditing	Know the levels and rules of Kubernetes auditing policies	200
2022-08-01	John the Ripper	Exposure to John the Ripper tool chain	100
2022-07-29	Kubernetes – Attacking the Kubelet API: Ep.2	Develop a working knowledge of how to attack the Kubelet API	200
2022-07-28	Kube-hunter	Be able to recognise vulnerabilities in Kubernetes clusters	100
2022-07-28	Kubernetes - Attacking The Kubelet API: Ep.1	Develop a working knowledge of how to attack the Kubelet API	200
2022-07-26	Kubernetes – Logging	Identify different logging architectures used with Kubernetes	100
2022-07-25	OWASP API Security Top 10	Identify each of the vulnerabilities in OWASP's top 10 APIs	20
2022-07-25	What is Digital Forensics?	Define digital forensics	20
2022-07-25	OWASP 2021: Ep.10 – Server-Side Request Forgery	Summarize server-side request forgery and its relationship to the OWASP Top 10	20
2022-07-25	Kubernetes - Secrets	Know how secrets work within Kubernetes	200
2022-07-18	OWASP 2021: Ep.9 – Security Logging and Monitoring Failures	Summarize security logging and monitoring failures and their relationship to the OWASP Top 10	20
2022-07-18	OWASP 2021: Ep.8 – Software and Data Integrity Failures	Summarize software and data integrity failures and their relationship to the OWASP Top 10	20
2022-07-18	OWASP 2021: Ep.7 – Identification and Authentication Failures	Summarize identification and authentication failures and their relationship to the OWASP Top 10	20
2022-07-13	Kubernetes - Shell to a Container	Identify how shells enable the execution of commands within Kubernetes workloads	200
2022-07-12	Kubernetes - Workload Resources	Have a basic working knowledge of Deployments, ReplicaSets, and StatefulSets	300

Activity Report Page 13 of 42

Date	Lab	Description	Points Earned
2022-07-12	Kubernetes - Namespaces and Network Policies	Be able to use Kubernetes namespaces and network policies	200
2022-07-11	OWASP 2021: Ep.6 – Vulnerable and Outdated Components	Summarize the security misconfiguration and its relationship to the OWASP Top 10	20
2022-07-11	OWASP 2021: Ep.5 – Security Misconfiguration	Summarize security misconfiguration and its relationship to the OWASP Top 10	20
2022-07-11	OWASP 2021: Ep.4 – Insecure Design	Summarize insecure design and its relationship to the OWASP Top 10 list	20
2022-07-11	Kubernetes - Pods and Services	Know how to externally access Kubernetes pods	100
2022-07-11	Kubernetes - Volumes	Develop an understanding of volumes within Kubernetes	200
2022-07-11	Introduction to Kubernetes	Recognise the fundamental concepts of Kubernetes	40
2022-07-11	Kubernetes - Multi-Container Pods	Recognise how Kubernetes resources are grouped and accessed	200
2022-07-08	S3 – Backup and Recovery	Recall backup and recovery methods that can be used with S3	100
2022-07-08	S3 – Demonstrate Your Skills	Demonstrate an ability to fix vulnerabilities and security misconfigurations in S3 buckets	300
2022-07-08	S3 – Access Policies	Grant access to selected users	200
2022-07-07	S3 – Inventory Report	Recall the steps required for S3 inventory report configuration	100
2022-07-07	S3 – Protecting Objects	Recall S3 security enhancement methods	100
2022-07-07	S3 – Multi-Region Access Points (MRAPs)	Recognize the benefits of S3 object replication	100
2022-07-06	Secrets Management	Recognize the challenges involved with storing sensitive information	20

Activity Report Page 14 of 42

Date	Lab	Description	Points Earned
2022-07-06	Introduction to the AWS Console	Demonstrate service navigation using the AWS console	100
2022-07-06	S3 – Restricting Access	Recall access restriction mechanisms for S3 buckets and objects	100
2022-07-06	S3 – Practical Introduction	Navigate the AWS Management Console	100
2022-07-06	Prowler	Recall how to use Prowler to detect vulnerable configurations in AWS	100
2022-07-06	awspx: Ep.2 – Analysis	Develop an understanding of the awspx tool	200
2022-07-06	awspx: Ep.1 – Introduction	Learn how to interpret cloud access relationships	200
2022-07-05	OWASP 2021: Ep.3 – Injection	Advance your understanding of the OWASP Top 10	20
2022-07-05	OWASP 2021: Ep.2 – Cryptographic Failures	Summarize cryptographic failures and their relationship to the OWASP Top 10	20
2022-07-05	OWASP 2021: Ep.1 – Broken Access Control	Summarize broken access control and its relationship to the OWASP Top 10	20
2022-06-28	Introduction to the OWASP Top 10	Summarize the objectives of the OWASP	10
2022-06-28	FIN7: Threat Hunting Ep.1 – What is FIN7?	Recall the most commonly targeted sectors	40
2022-06-27	DevSecOps – Operate	Recall the security considerations of the DevSecOps operation stage	20
2022-06-27	DevSecOps – Monitor	Recall the security considerations of the DevSecOps monitoring phase	20
2022-06-27	DevSecOps – Deploy	Recall the security considerations of the DevSecOps deployment stage	20
2022-06-20	AWS Logging and Monitoring – Introduction to CloudTrail	Identify the core features of AWS CloudTrail	20

Activity Report Page 15 of 42

Date	Lab	Description	Points Earned
2022-06-20	Introduction to AWS Lambda	Establish how you can implement serverless computing across your AWS platform	20
2022-06-20	Introduction to EC2	Describe AWS EC2 and the features it offers	20
2022-06-20	Introduction to AWS Identity and Access Management (IAM)	Describe the features offered by IAM for access management	20
2022-06-20	Introduction to S3	Identify the features of S3 and how it provides secure storage services	20
2022-06-20	Introduction to Amazon Web Services	Describe what AWS is and the cloud services it offers	10
2022-06-20	Strings	Use the strings tool on a Windows system	200
2022-06-20	Sigcheck	Recognize how the Sysinternals tool Sigcheck works	200
2022-06-20	SDelete Analysis	Identify malicious behaviour on a network analysing Splunk logs	100
2022-06-20	Command History	Be able to identify the risk of passing credentials with the command line	100
2022-06-20	Compliance, Legislation, Regulation, and Standards	Describe the differences between compliance, legislation, regulation, and standards	10
2022-06-20	Stack Overflow	Demonstrate the risk of using code found online	10
2022-06-20	AWS Security Groups	Analyse security configuration	40
2022-06-20	S3 – Security Permissions	Discover Amazon S3 bucket functionality	200
2022-06-20	Web Applications: Page Source Review	Analyse the web application source code to recognise technologies being used	200
2022-06-20	Network Scanning	Operate various network scanning tools to identify open ports	100

Activity Report Page 16 of 42

Date	Lab	Description	Points Earned
2022-06-20	GDPR Aware (ARCHIVED)	Explain the key details and impact of GDPR	10
2022-06-20	Default Credentials	Knowledge of default credentials	20
2022-06-17	Mshta	Recognise .hta malware and how it is executed under mshta.exe	200
2022-06-17	Analysing Sandbox Reports	Investigate malicious samples using sandbox reporting styles	100
2022-06-15	Sysinternals Autoruns	Deduce what malicious file is executing at system start-up	100
2022-06-13	LOLBins	Be able to use LOLBins by spawning a child process via a specified binary	300
2022-06-13	Process Explorer	Use Process Explorer effectively	100
2022-06-13	AccessChk	Understand the Sysinternals tool AccessChk	200
2022-06-09	Netsh Persistence	Identify modern persistence methods used by malicious software	300
2022-06-07	Windows Sysmon	Analyse and investigate system logs	100
2022-06-07	Process Monitor	Demonstrate an ability to use Process Monitor	200
2022-06-07	Windows Sysinternals	An overview of the Sysinternals suite	100
2022-06-02	Mining Behaviour	Identify anomalous behaviour related to cryptocurrency	300
2022-05-31	DevSecOps – Release	Recall the security considerations of the DevSecOps release stage	20
2022-05-31	DevSecOps – Test	Recall the security considerations of the DevSecOps testing stage	20

Activity Report Page 17 of 42

Date	Lab	Description	Points Earned
2022-05-31	DevSecOps – Build	Recall the security considerations of the DevSecOps build stage	20
2022-05-31	Windows AppLocker: Bypassing Allowed Paths	Understand AppLocker and its configuration of path rules	300
2022-05-31	Windows AppLocker: Bypassing Hash Rules	Understand AppLocker hash rules and their configuration	200
2022-05-24	Windows AppLocker: Introduction to Bypassing Rules	Basic understanding of AppLocker and its configuration	100
2022-05-23	DevSecOps – Code	Recall the security considerations of the DevSecOps coding phase	20
2022-05-23	DevSecOps – Plan	Recall the security considerations of the DevSecOps planning stage	20
2022-05-23	NIST 800-144 Cloud Security: Ep.9 – Incident Response	Explain concerns and recommendations for incident response in cloud environments as detailed by NIST	10
2022-05-17	ProcDump	Use ProcDump to debug programs and dump process memory	200
2022-05-17	PsExec	Illustrate how the Sysinternals tool PsExec works	200
2022-05-16	NIST 800-144 Cloud Security: Ep.7 – Data Protection	Recall NIST 800-144 concerns and recommendations for data protection in cloud environments	10
2022-05-16	NIST 800-144 Cloud Security: Ep.8 – Availability	Describe the concerns and recommendations for cloud availability according to NIST 800-144	10
2022-05-16	NIST 800-144 Cloud Security: Ep.6 – Software Isolation	Recall what multi-tenancy architecture is	20
2022-05-09	NIST 800-144 Cloud Security: Ep.5 – Identity and Access Management	Recall the concerns and recommendations for identity and access management in cloud security as per NIST 800-144 guidelines	20
2022-05-09	NIST 800-144 Cloud Security: Ep.4 – Architecture	Explain NIST's recommendations and concerns about architecture with regards to cloud security	10
2022-05-09	NIST 800-144 Cloud Security: Ep.3 – Trust	Explain the concern for trust in cloud security	10

Activity Report Page 18 of 42

Date	Lab	Description	Points Earned
2022-05-02	NIST 800-144 Cloud Security: Ep.2 – Compliance	Recognise why compliance is important for cloud security	10
2022-05-02	NIST 800-144 Cloud Security: Ep.1 – Governance	Recall how governance is important to NIST cloud security guidelines	10
2022-05-02	NIST 800-144: Guidelines on Security and Privacy in Public Cloud Computing	Recall the NIST 800-144 guidelines at a high level	10
2022-05-02	DDE Analysis	Investigate different ways malware achieves execution after initial access	200
2022-04-25	NIST 800-53: Ep.20 – Supply Chain Risk Management	Recognize supply chain risk management controls	20
2022-04-25	NIST 800-53: Ep.19 – System and Information Integrity	Recognize system and information integrity controls and their purpose	40
2022-04-25	NIST 800-53: Ep.18 – System and Communications Protection	Recognize system and communications protection controls and their purpose	40
2022-04-25	NIST 800-53: Ep.17 – System and Services Acquisition	Recognize system and services acquisition controls	20
2022-04-18	NIST 800-53: Ep.16 – Risk Assessment	Recognize risk assessment controls	20
2022-04-18	NIST 800-53: Ep.15 – Personally Identifiable Information Processing and Transparency (PIIPT)	Recognize the PIIPT controls	40
2022-04-18	NIST 800-53: Ep.14 – Personnel Security	Recognize personnel security controls and their purpose	20
2022-04-11	NIST 800-53: Ep.13 – Program Management	Recognize program management controls and their purpose	20
2022-04-11	NIST 800-53: Ep.12 – Planning	Recognize planning controls and their purpose	20
2022-04-11	NIST 800-53: Ep.11 – Physical and Environmental Protection	Recognize physical and environmental protection controls and their purpose	20
2022-04-04	Inherent vs Residual Risk	Explain the difference between inherent and residual risk	20

Date	Lab	Description	Points Earned
2022-04-04	NIST 800-53: Ep.10 – Media Protection	Recognize media protection controls and their purpose	20
2022-04-04	NIST 800-53: Ep.9 – Maintenance	Recognize maintenance controls and their purpose	20
2022-03-28	NIST 800-53: Ep.8 – Incident Response	Recognize incident response controls and their purpose	20
2022-03-28	NIST 800-53: Ep.7 – Identification and Authentication	Recognize identification and authentication controls and their purpose	20
2022-03-28	NIST 800-53: Ep.6 – Contingency Planning	Recognize contingency planning controls and their purpose	20
2022-03-21	NIST 800-53: Ep.5 – Configuration Management	Recognize configuration management controls and their purpose	20
2022-03-21	NIST 800-53: Ep.4 – Assessment, Authorization, and Monitoring	Recognize assessment, authorization, and monitoring controls and their purpose	20
2022-03-21	NIST 800-53: Ep.3 – Audit and Accountability	Recognize audit and accountability controls and their purpose	20
2022-03-16	NIST 800-53: Ep.2 – Awareness and Training	Recognize the purpose of awareness and training controls	20
2022-03-16	NIST 800-53: Ep.1 – Access Control	Recognize the NIST 800-53 Access Control family and its purpose	20
2022-03-16	NIST 800-53: Security and Privacy Controls for Information Systems and Organizations	Familiarize yourself with NIST 800-53 and its purpose	20
2022-03-07	Tactics – Exfiltration	Recognise the purpose of the MITRE ATT&CK® Exfiltration tactic	20
2022-03-07	Tactics – Impact	Be able to explain the purpose of the MITRE ATT&CK® Impact tactic	20
2022-03-07	Tactics – Command and Control	Recognise the purpose of the MITRE ATT&CK® Command and Control tactic	20
2022-02-28	Tactics – Collection	Recognise the purpose of the MITRE ATT&CK® Collection tactic	20

Activity Report Page 20 of 42

Date	Lab	Description	Points Earned
2022-02-28	Tactics – Lateral Movement	Recognise the MITRE ATT&CK® Lateral Movement tactic and its purpose	20
2022-02-28	Tactics – Discovery	Recognise the purpose of the MITRE ATT&CK® Discovery tactic	20
2022-02-24	PowerPoint as a Malware Dropper	Investigate indicators of compromise from malicious Microsoft Office documents	100
2022-02-21	Tactics – Credential Access	Recognise the purpose of the MITRE ATT&CK® Credential Access tactic	20
2022-02-21	Tactics – Defence Evasion	Recognise the purpose of the MITRE ATT&CK® Defence Evasion tactic	20
2022-02-21	Tactics – Privilege Escalation	Recognise the purpose of the MITRE ATT&CK® Privilege Escalation tactic	20
2022-02-14	Tactics – Resource Development	Recognise the purpose of the MITRE ATT&CK® Resource Development tactic	20
2022-02-14	Tactics – Execution	Know the purpose of the MITRE ATT&CK® Execution tactic	20
2022-02-14	Tactics – Initial Access	Recognise the purpose of the MITRE ATT&CK® Initial Access tactic	20
2022-02-10	Zerologon – Live Logs	Identify logs related to Zerologon	200
2022-02-08	Tactics – Reconnaissance	Recognise the purpose of the MITRE ATT&CK® Reconnaissance tactic	20
2022-02-08	Introduction to MITRE ATT&CK®	Be familiar with the MITRE ATT&CK® framework and know how it is used	20
2022-02-07	Fuzzy Hashing	Discover various methods of analysing files	300
2022-02-02	STIX	Locate Cyber Threat Information from within STIX objects	40
2022-02-02	VirusTotal	Discover automated malware analysis tools and communities	100

Activity Report Page 21 of 42

Date	Lab	Description	Points Earned
2022-02-01	Splunk: Threat Hunting Ep.10 – Persistence Execution	Identify various tactics from the MITRE ATT&CK framework	200
2022-02-01	Splunk: Threat Hunting Ep.9 – Lateral Clean Up, Collection and Exfiltration	Identify various tactics from the MITRE ATT&CK framework	200
2022-02-01	Immersive Labs Threat Hunting	Summarise the 'threat research' skill line	20
2022-02-01	Introduction to Threat Hunting	Exposure to threat hunting principles	40
2022-02-01	Threat Hunting: Windows Odd One Out	Identify out of sort processes and artefacts	200
2022-02-01	Server Identification	Identify default honeypot configurations	200
2022-01-31	Splunk: Threat Hunting Ep.8 – Expand Access Laterally	Identify various tactics from the MITRE ATT&CK framework	200
2022-01-27	Splunk: Threat Hunting Ep.7 – Additional Collection & Exfiltration	Identify various tactics from the MITRE ATT&CK framework	200
2022-01-25	Splunk: Threat Hunting Ep.6 – Credential Access	Identify various tactics from the MITRE ATT&CK framework	200
2022-01-24	Splunk: Threat Hunting Ep.5 – Establish Persistence	Identify various tactics from the MITRE ATT&CK framework	200
2022-01-24	Splunk: Threat Hunting Ep.4 – Cleanup & Reconnaissance	Identify various tactics from the MITRE ATT&CK framework	200
2022-01-20	Splunk: Threat Hunting Ep.3 – Deploy Stealth Toolkit	Identify various tactics from the MITRE ATT&CK framework	200
2022-01-20	Splunk: Threat Hunting Ep.2 – Rapid Collection and Exfiltration	Identify various tactics from the MITRE ATT&CK framework	200
2022-01-17	Windows Service Investigation	Identify and investigate anomalous Windows services	200
2022-01-17	Image File Execution Options Injection (IFEO)	Practise the injection technique present in the IFEO registry key	200

Activity Report Page 22 of 42

Date	Lab	Description	Points Earned
2022-01-17	Persistence via Accessibility Features	Construct a method of persistent access on a Windows system	200
2022-01-13	Introduction to Zeek Logs (ARCHIVED)	Convert a PCAP then analyse logs using Zeek	200
2022-01-13	BPF Syntax	Analyse network packet captures	100
2022-01-13	bashrc Persistence	Experience identifying Linux persistence methods	200
2022-01-13	Trap	Apply trap commands that perform custom actions on receiving signals	100
2022-01-13	Component Object Model Hijacking	Apply knowledge of the Windows Registry to pick out IOCs	200
2022-01-13	Windows Logon Persistence	Recognize how attackers gain persistence on a system by abusing the Windows Registry	200
2022-01-13	Tactics – Persistence	Recognise the purpose of the MITRE ATT&CK® Persistence tactic	20
2022-01-13	ngrep	Analyse network packet captures	200
2022-01-13	tcpdump	Analyse network packet captures	200
2022-01-13	Packet Capture: Key Extraction	Analyse network packet captures	300
2022-01-11	What is Vulnerability Management?	Recall what vulnerability management is and its importance in defensive cybersecurity	20
2022-01-11	Vulnerability Management: Ep.3 — Evaluate and Prioritise	Explain the prioritising step within the Vulnerability Management process	20
2022-01-11	Vulnerability Management: Ep.4 — Remediate	Identify what it means to remediate discovered and known vulnerabilities	20
2022-01-11	Vulnerability Management: Ep.5 — Report	Understand the process of reporting vulnerabilities	20

Activity Report Page 23 of 42

Date	Lab	Description	Points Earned
2022-01-11	Vulnerability Management: Ep.2 — Monitoring and Identifying	Identify the process for monitoring and identifying vulnerabilities	20
2022-01-11	Vulnerability Management: Ep.1— Asset and System Inventory	Identify the hardware and software assets	20
2022-01-11	Splunk: Threat Hunting Ep.1 – Initial Compromise	Identify various tactics from the MITRE ATT&CK framework	200
2022-01-11	Introduction to Penetration Testing – Web Applications	Be able to demonstrate an understanding of web application hacking concepts	40
2022-01-11	Introduction to Penetration Testing – Mobile Applications	Demonstrate an understanding of iOS/Android pen testing concepts	40
2022-01-11	Introduction to Penetration Testing – Infrastructure	Demonstrate an understanding of infrastructure pen testing concepts	40
2022-01-11	Introduction to Penetration Testing – The Basics	Be able to describe basic pen testing concepts	20
2022-01-10	Password Filter DLL	Identify and investigate malicious password filters	200
2022-01-10	Parsing PST	Investigate email client files	200
2022-01-10	Malicious Documents: OLE tools	Investigate various malicious artefacts	300
2022-01-07	RAT Attacks	Identify encoded and encrypted C2 communications	400
2022-01-06	Application Shimming	Investigate signs of persistence on a Windows machine	200
2022-01-06	ZWASP Phishing Vulnerability in Office 365	Assemble URLs containing ZWSPs to obfuscate a malicious link	100
2022-01-06	Exfiltration Over Alternative Protocol	Practise identifying instances where data has been exfiltrated	100
2022-01-06	Persistence – Accessibility Features: Investigation	Exposure to the common vectors actors will use to gain persistence on a host	200

Activity Report Page 24 of 42

Date	Lab	Description	Points Earned
2022-01-05	Clipboard Data Theft	Analyse techniques used by adversaries to steal clipboard data	100
2022-01-04	IR: Ep.1 – Suspicious Email	Investigate and gain information from suspected malicious documents	200
2022-01-03	Windows Exploitation: Ep.3 – Tooling and Languages	List the tools used to perform Windows Exploitation	40
2022-01-03	Windows Exploitation: Ep. 2 – Types of Common Vulnerabilities	Recall the differences between common Windows vulnerabilities	40
2022-01-03	Windows Exploitation: Ep.1 – What is Windows Exploitation?	Define what Windows exploitation entails	40
2022-01-03	Introduction to 64-Bit Architectures	Gain a high level understanding of 64-bit architectures	40
2022-01-03	Introduction to 32-Bit Architectures	Gain a high-level understanding of 32-bit architectures	40
2022-01-03	The Inside of an ELF File	Be able to identify components of an ELF file	40
2022-01-03	The Inside of a PE File	Gain a high level understanding of Portable Executables	40
2022-01-03	What Is the Stack?	Gain a high level understanding of stack memory	40
2022-01-03	What Is the Heap?	Gain a high level understanding of heap memory	40
2022-01-03	Introduction to Windows Internals	Gain a high-level understanding of the Windows operating system's inner workings	40
2022-01-03	An Introduction to Linux Internals	Gain a high level understanding of the Linux operating system's inner workings	40
2022-01-03	Wireshark Display Filters: Combining Filters	Analyse network packet captures using multiple operators	200
2022-01-03	Introduction to Computer Memory and Architecture	Gain a high level understanding of how memory works in a computer system	40

Activity Report Page 25 of 42

Date	Lab	Description	Points Earned
2022-01-03	Tshark	Analyse network packet captures	200
2022-01-03	Wireshark TLS	Analyse network packet captures	300
2022-01-03	ELF Execution Structure	Discover the internals of an ELF executable structure	200
2022-01-03	Introduction to ELF Reverse Engineering	Exposure to ELF binary analysis	100
2021-12-28	Threat Hunt Theory – Emulating Adversaries	Recognize how emulating adversaries is beneficial in threat hunting	40
2021-12-28	Threat Hunt Theory – Targeted Hunting Integrating Threat Intelligence	Recognize how the Targeted Hunting integrating Threat Intelligence methodology is used in threat hunting	40
2021-12-28	Threat Hunt Theory – Management, Growth, Metrics, and Assessment	Recognize how the MaGMA model is used in threat hunting	40
2021-12-28	Threat Hunt Theory – Understanding the Results	Recognize the importance of threat hunting results	40
2021-12-28	Threat Hunt Theory – Data Quality	Recognize "good" data and why data quality is important in threat hunting	40
2021-12-28	Threat Hunt Theory – Documenting the Hunt	Recognize the importance of documentation and automation in threat hunting	40
2021-12-28	Threat Hunt Theory – Pyramid of Pain	Recognize the pyramid of pain	20
2021-12-28	Threat Hunt Theory – Types of Hunt	Recognize the different types of threat hunt	10
2021-12-28	Threat Hunt Theory – Threat Intelligence Lifecycle	Recognize the intelligence lifecycle	40
2021-12-28	Threat Hunt Theory – The Threat Hunting Loop	Recognize the threat hunting loop	40
2021-12-28	Threat Hunt Theory – Maturity Model	Recognise the threat hunting maturity model	40

Activity Report Page 26 of 42

Date	Lab	Description	Points Earned
2021-12-28	Threat Hunt Theory – Threat Hunting Model	Recognise the threat hunting process	40
2021-12-28	Threat Hunt Theory – Diamond Model	Recognize the diamond model	40
2021-12-28	Threat Hunt Theory – Mapping Adversaries	Understand how to map adversaries to the MITRE ATT&CK® framework	40
2021-12-28	Threat Hunt Theory – Introduction	Understand the fundamental concepts of threat hunting	40
2021-12-28	Threat Hunt Theory – Hypothesis Creation	Recognise how to create a threat hunting hypothesis	40
2021-12-28	Cloud Security: Frameworks, Standards and Guidelines	Be able to identify the different frameworks, standards and guidelines that relate to cloud security	10
2021-12-28	Cloud Security Alliance: Cloud Controls Matrix v4.0	Recall the domains within the CSA CCM v4.0	10
2021-12-28	Introduction to SAML	Be able to recognise the advantages of Single Sign-On	40
2021-12-28	Introduction to Cloud	Recognise key aspects of cloud computing and the benefits it can bring	10
2021-12-28	Virtualisation	Describe the uses and advantages of virtualisation	10
2021-12-28	Platform as a Service (PaaS)	Be able to explain the advantages and disadvantages of Platform as a Service	20
2021-12-28	Security Automation	Describe the advantages of security automation and orchestration	20
2021-12-28	Infrastructure as Code (IaC)	Explain what IaC is and how it is deployed	20
2021-12-28	DevSecOps – Introduction	Recall the evolution of software delivery methodologies	10
2021-12-28	Infrastructure as a Service (IaaS)	Describe the advantages and disadvantages of Infrastructure as a Service (IaaS).	20

Activity Report Page 27 of 42

Date	Lab	Description	Points Earned
2021-12-28	Software as a Service (SaaS)	Be able to describe the advantages and disadvantages of SaaS	20
2021-12-28	NIST Cybersecurity Framework	List the three main components of the NIST Cybersecurity Framework	40
2021-12-28	Three Lines of Defense	Describe the Three Lines of Defense model	10
2021-12-28	Qualitative Risk Measurement	Summarize what qualitative risk is	20
2021-12-28	Risk and Control Self Assessment (RCSA)	Describe the purpose of an RCSA within the wider risk management framework	20
2021-12-28	Quantitative Risk Measurement	Calculate quantitative risk as a function of impact and probability	40
2021-12-28	Inherent and Residual Risk (ARCHIVED)	Explain the difference between inherent and residual risk	20
2021-12-28	Vulnerability Identification	Identify the different ways to conduct vulnerability identification	40
2021-12-28	Asset Inventory and Valuation	Define the asset identification and valuation processes	20
2021-12-28	How Is Risk Measured?	Be able to describe risk, impact, and probability	40
2021-12-28	What Is Risk?	Define the core concepts that formulate risk	20
2021-12-28	How to Mitigate Risk	Explain how risk management can help mitigate risk	20
2021-12-27	Interactive RegEx: Ep. 9 — Demonstrate	Apply knowledge gained throughout the series to match specific data	200
2021-12-27	Interactive RegEx: Ep. 8 — Flags	Recall the different flags that can be applied to the regex engine	100
2021-12-27	Interactive RegEx: Ep. 7 — Groups	Recall how you previously used capture groups	200

Activity Report Page 28 of 42

Date	Lab	Description	Points Earned
2021-12-22	Interactive RegEx: Ep. 6 — Quantifiers	Recall how to use logical operators in regex	200
2021-12-22	Interactive RegEx: Ep. 5 — Logical Metacharacters	Recall how to match patterns with character sets	100
2021-12-22	Interactive RegEx: Ep. 4 — Character Sets	Recall how to match with the metacharacters dot, backslash, and line anchors	40
2021-12-22	Interactive RegEx: Ep. 3 — Simple Matching	Recall how to match alphanumeric characters in a string	40
2021-12-21	Interactive RegEx: Ep. 2 — The RegEx Interface	Be familiar with the interface that will be used throughout the series	20
2021-12-21	Interactive RegEx: Ep. 1 — An Introduction to RegEx	Recall what regular expressions are and the task they perform	10
2021-12-21	Introduction to Networking: Ep.4 – Network Topologies	Recognize network topologies	40
2021-12-21	Introduction to Networking: Ep.3 — Network Hardware	Recognize the different types of hardware used for networks	40
2021-12-21	Introduction to Networking: Ep.2 – Types of Networks	Recall multiple types of networks and how they differ	20
2021-12-21	Introduction to Networking: Ep.1 — What is a Network?	Recognize networks and their components	40
2021-12-21	Introduction to Networking: Ep.5 — IP Addresses	Recognize an IP address	40
2021-12-21	Introduction to Networking: Ep.6 — Domain Name System	Summarize the fundamentals of the Domain Name System	40
2021-12-20	Malicious Documents: Dropper Analysis	Analyse obfuscated VBA	300
2021-12-16	Applocker Bypass – SharpPick	Bypass AppLocker rules using .NET	300
2021-12-16	PowerShell: PS Remoting	Practice executing remote commands on Windows systems	300

Activity Report Page 29 of 42

Date	Lab	Description	Points Earned
2021-12-16	PowerShell: PowerUp	Practice using the Windows privilege escalation tool	300
2021-12-16	PowerShell: AMSI Bypass	Practise bypassing Windows Antimalware Scan Interface	300
2021-12-16	PowerShell: DownloadString-InvokeExpression	How to bypass Antivirus disk checks	300
2021-12-16	Introduction to Malicious Documents	Identify different file structures used to create malicious documents	200
2021-12-16	Malicious Documents: VBA Analysis	Use oletools to extract and analyse malicious VBA	300
2021-12-16	PowerShell Empire	Demonstrate the ability to configure and run various PowerShell Empire functions	100
2021-12-15	PowerShell: Bypassing Execution Policy	Bypassing restrictions when executing scripts	200
2021-12-15	CertUtil	Analyse the function of CertUtil	100
2021-12-15	Background Intelligent Transfer Service (BITS)	Gain an understanding of BITS and how it can be abused	100
2021-12-15	PowerShell: Reading Event Logs	Use the Get-EventLog cmdlet to analyse Windows event logs	200
2021-12-15	Linux CLI: Ep. 14 – Using Screen	Be able to explain screen's CLI usage	100
2021-12-15	PowerShell: Using Modules	Use PowerShell cmdlets to import and remove modules	200
2021-12-15	PowerShell: Working with cmdlets	Use PowerShell cmdlets to manipulate files	200
2021-12-15	Volume Shadow Copy Service	Exposure to VSS and its functionality	200
2021-12-15	PowerShell: Working with files	Practice reading from and writing to files in PowerShell	100

Activity Report Page 30 of 42

Date	Lab	Description	Points Earned
2021-12-15	PowerShell: Getting Started	Practise using the PowerShell cmdlets	100
2021-12-15	Linux CLI: Ep. 13 – Searching and Sorting	Know how to employ searching techniques to find patterns in files	100
2021-12-15	Linux CLI: Ep. 16 – Combining Commands	Identify the different ways of combining commands on the terminal	200
2021-12-15	Alternate Data Streams	Exposure to ADS and data hiding	200
2021-12-15	Scheduled Tasks	Demonstrate how to navigate information in Windows Scheduled Tasks	100
2021-12-15	Windows Registry	Evaluate registry values	100
2021-12-15	Policies	Exposure to Windows policy mechanisms	200
2021-12-15	Environment Variables	Exposure to Windows environment variables	200
2021-12-15	Windows File Permissions	Analyse Windows file permissions	100
2021-12-15	Linux CLI: Ep. 15 – Generating File Hashes	Be able to recognise file hashes	100
2021-12-14	Linux CLI: Ep.1 – Introduction to the Linux Command Line Interface	Recall Linux command line fundamentals	40
2021-12-14	Demonstrate Your Skills: Networking	Demonstrate your networking knowledge	100
2021-12-14	Protocols – LDAP	Analyse the LDAP protocol in an enterprise context	100
2021-12-14	Protocols – ARP	Identify packet structure of ARP requests and responses	100
2021-12-14	Protocols – FTP	Explain the core concepts of the File Transfer Protocol	100

Activity Report Page 31 of 42

Date	Lab	Description	Points Earned
2021-12-14	Protocols – DHCPv6	Discuss the use of DHCP in computer networks	200
2021-12-14	Protocols – Modbus	Reference the core concepts of the Modbus protocol	300
2021-12-14	Linux CLI: Ep. 12 – Using Find	Recognise how the find command works and the filters and arguments that go with it	200
2021-12-14	Linux CLI: Ep. 2 – Getting Started with the Terminal	Be able to recall fundamental concepts of the Linux terminal	100
2021-12-14	Protocols – DNS	Describe the structure of DNS requests and responses	200
2021-12-14	Protocols – SMTP	Describe the structure of SMTP messages	200
2021-12-14	Linux CLI: Ep. 10 – Using Sudo	Identify different user privileges in Linux	100
2021-12-14	Linux CLI: Ep. 5 – File Permissions	Be able to read Linux file permissions	100
2021-12-14	Linux CLI: Ep. 8 – Manipulating Text	Know how to modify text within files using basic command line tools	200
2021-12-14	Linux CLI: Ep. 6 – Editing Files	Be able to recall some common Linux command line text editors	100
2021-12-14	Linux CLI: Ep. 7 – Using wc	Be able to count elements in a file using the wc tool	200
2021-12-14	Linux CLI: Ep. 9 – Stream Redirection	Know how data can be manipulated via the terminal	100
2021-12-14	Linux CLI: Ep. 11 – Using SSH and SCP	Recall what the SSH protocol is	100
2021-12-14	Linux CLI: Ep. 4 – Changing Things	Know the five Linux CLI commands explored in the lab and be able to describe their basic usage	100
2021-12-14	Linux CLI: Ep. 3 – Moving Around	Have the ability to navigate through directories on the command line	100

Activity Report Page 32 of 42

Date	Lab	Description	Points Earned
2021-12-13	Demonstrate Your Knowledge: Networking	Demonstrate your networking knowledge	40
2021-12-13	DoS Primer – Resource Exhaustion	Explain the different types of resource exhaustion attacks	40
2021-12-13	DoS Primer – Vulnerabilities	Learn different types of denial of service vulnerabilities	40
2021-12-13	DoS Primer – Volumetric	Explain the different types of volumetric attacks	40
2021-12-13	Demonstrate Your Skills: Encryption	Demonstrate the skills acquired through the beginner Encryption labs	300
2021-12-13	The Internet	Explain the history of the internet	20
2021-12-13	HTTP Status Codes	Develop knowledge of HTTP status codes	100
2021-12-13	Protocols – DHCPv4	Discuss the use of DHCP in computer networks	200
2021-12-13	OSI Model	Identify the different layers of the OSI model	40
2021-12-13	Denial of Service	Describe how denial of service attacks appear	200
2021-12-13	Protocols - HTTP	Describe the structure of HTTP GET and POST requests	200
2021-12-13	Ports	Identify how ports are used in modern networks	40
2021-12-13	Transport Protocols	Explain the core concepts of the the most common transport protocols	40
2021-12-13	Internet Protocol V4	Explain the core concepts of IPv4 addressing	100
2021-12-10	Introduction to Hashing	Identify the characteristics of a good hashing algorithm	100

Activity Report Page 33 of 42

Date	Lab	Description	Points Earned
2021-12-10	Rainbow Tables	Describe what a rainbow table is	40
2021-12-10	Hashing – MD5	Apply the MD5 hashing algorithm to strings	100
2021-12-10	Hashing – SHA-1	Apply the SHA1 hashing algorithm to strings	100
2021-12-10	WPA Wordlist Crack	Identify weaknesses in Wi-Fi protocols	100
2021-12-10	Wired Equivalent Privacy (WEP) Cracking	Identify weaknesses in Wi-Fi protocols	200
2021-12-09	Demonstrate Your Skills: Encoding	Demonstrate your knowledge of encoding methods and techniques	200
2021-12-09	Punycode	Recall how Punycode functions	100
2021-12-09	Unicode	Recall how Unicode functions	40
2021-12-09	Base64 Encoding	Recall how Base64 encoding works	40
2021-12-09	ASCII	Recall how ASCII encoding functions	40
2021-12-09	Hexadecimal	Recall how hexadecimal functions	40
2021-12-09	What is Encoding?	Recall how encoding functions	40
2021-12-09	Vigenère Ciphers	Describe what a Vigenère cipher is	40
2021-12-09	The History of Encryption	Recall the different methods of encryption used throughout history	40
2021-12-09	Public and Private Key Management	Recognize the importance of managing public and private keys	40

Activity Report Page 34 of 42

Date	Lab	Description	Points Earned
2021-12-09	One-Time Pad	Define what a one-time pad cipher is	40
2021-12-09	Symmetric Key Encryption	Recognise symmetric encryption	40
2021-12-09	What is Cryptography?	Recall the fundamentals of cryptography	40
2021-12-09	Asymmetric Encryption	Define asymmetric encryption	40
2021-12-09	Block Ciphers	Define a block cipher	40
2021-12-09	Digital Signatures	Recall the importance of digital signatures	40
2021-12-09	Stream Ciphers	Define stream ciphers and recall their fundamental characteristics	40
2021-12-09	Hashing	Recognise the importance of hashing	20
2021-12-09	Public Key Infrastructure	Define what public key infrastructure is	40
2021-12-09	Message Integrity	Be able to define the term ‘message integrity’	40
2021-12-09	Demonstrate Your Skills: Historic Encryption	Demonstrate your knowledge of historic encryption techniques	200
2021-12-09	PKI (Public Key Infrastructure)	Understand the different parts of PKI and their roles	40
2021-12-09	PKI (Public Key Infrastructure) Practical	Understand the different parts of PKI and their roles	200
2021-12-09	Introduction to Encryption	Identify different types of encryption algorithms	100
2021-12-09	Elliptic Curve Cryptography	Explain the basics of elliptic curve cryptography	40

Activity Report Page 35 of 42

Date	Lab	Description	Points Earned
2021-12-09	The Bombe Machine	Recognize how the Bombe machine works	200
2021-12-09	The Typex Machine	Recognize how a Typex machine works	200
2021-12-09	The Enigma Machine	Recall how the Enigma machine works	200
2021-12-09	Encryption Tools: CyberChef — Recipes	Recall how CyberChef recipes work	40
2021-12-09	RSA	Gain an understanding of RSA encryption/decryption methods	400
2021-12-09	Encryption Tools: CyberChef	Recall how CyberChef functions	40
2021-12-09	Steganography	Analyze images and extract information using ExifTool and Steghide	200
2021-12-09	Symmetric vs Asymmetric Key Encryption	Apply symmetric key encryption and decryption techniques	100
2021-12-09	Binary	Recall how binary functions	40
2021-12-09	Caesar Ciphers	Recall how Caesar cipher encoding works	40
2021-12-08	Secure Fundamentals: The CIA Triad	Define confidentiality, integrity, and availability	20
2021-12-08	Secure Fundamentals: Attribution and Accountability	Recall the definitions of attribution and accountability	20
2021-12-08	Web Server Logs: Ep.6 — The Tomcat's Out Of The Bag	Identify evidence of a compromise in web server logs	300
2021-12-08	Web Server Logs: Ep.5 — Searching Web Server Logs using Linux CLI	Use cat, grep, cut, sort, uniq, and wc commands to search for information in web server logs	200
2021-12-08	Secure Fundamentals: Least Privileges	Be able to describe the principle of least privileges	10

Activity Report Page 36 of 42

Date	Lab	Description	Points Earned
2021-12-08	Secure Fundamentals: Defence in Depth	Describe the security concept of defence in depth	10
2021-12-08	Secure Fundamentals: Security Patching	Describe what a security patch is	10
2021-12-08	US Federal Cyber Law	Identify the main US federal laws that can be used to convict cyber criminals	10
2021-12-08	Secure Fundamentals: Authorisation	Describe the security concept of authorisation	10
2021-12-08	Secure Fundamentals: Authentication	Describe the security concept of authentication	10
2021-12-08	UK Cyber Law	Demonstrate an understanding of illegalities and breaches of law	40
2021-12-08	Incident Response in the Workplace	Recall the advantages of an incident response plan	10
2021-12-08	Guidance on Remote Working	Identify the risks associated with remote working	10
2021-12-08	Security On The Go	Recognize the security risks of using devices when away from the office	10
2021-12-08	Rogue USB Devices	Recall how rogue USB devices can be used for malicious purposes	10
2021-12-08	Personal Devices in the Workplace	Recognize the risks associated with using personal devices in the workplace	10
2021-12-08	The Importance of Information Security and Cybersecurity	Describe a simulated example of a breach and recall its emotional impact	10
2021-12-08	Privileged Access	Recall what privileged access is and why it's an attractive target for attackers	10
2021-12-08	Physical Security	Identify common physical security risks	10
2021-12-08	Privacy	Identify what privacy is and why it needs protecting	10

Activity Report Page 37 of 42

Date	Lab	Description	Points Earned
2021-12-08	Information Security	Recognize the importance of information security for individuals and organizations	10
2021-12-08	What Is Information Security?	Identify the workplace and personal security challenges that good information security practices help to solve	10
2021-12-08	History of Information Security	Recall some of the key moments for information security throughout history	10
2021-12-08	Disposal of Device Information	Recognize why secure device disposal is core to an organization's information management process	10
2021-12-08	Information Security and Cybersecurity Terminology	Recall some key information security and cybersecurity terms and phrases	10
2021-12-08	Information Security – Starting at the Beginning	Recall the difference between information security and cybersecurity	10
2021-12-08	Bugbusters	Demonstrate an understanding of bug bounties and the companies that offer them	40
2021-12-08	Ethical and Unethical Hacking	Demonstrate the ability to determine the ethical choices of hackers	40
2021-12-08	Burglary and Hacking	Demonstrate an understanding of how hacking can be similar to burglary	40
2021-12-08	Police Raid	Demonstrate an understanding of devices that would be confiscated in an investigation	40
2021-12-08	Who are the Hackers?	Recognize the different types of hackers	10
2021-12-08	Why Hackers Hack	Recognize some of the methods used by hackers	10
2021-12-08	Virtual Card Numbers	Identify the different types of virtual card numbers	10
2021-12-08	Fake News	Recognize the characteristics of fake news	10
2021-12-08	Security Champions	Underline what a security champion is and their purpose	10

Activity Report Page 38 of 42

Date	Lab	Description	Points Earned
2021-12-08	Keylogging	Recognize what keyloggers are	10
2021-12-08	Social Engineering	Describe different social engineering attack techniques and their impacts	10
2021-12-08	Geolocation	Recognize the differences between device-based and server-based geolocation tracking	10
2021-12-08	Darknets	Recognize how darknets operate on the internet	10
2021-12-08	Cookies	Recognize how cookies are used by individuals and organizations	20
2021-12-08	Cryptocurrency & Blockchain	An introduction to cryptocurrency and blockchain concepts	10
2021-12-08	Intrusion Detection Systems	Describe intrusion detection and prevention principles	20
2021-12-08	Shoulder Surfing	Recognize how shoulder surfing works and the various ways it can be employed	10
2021-12-08	Cyber Kill Chain	Recognize the purpose of the cyber kill chain	10
2021-12-07	Web Server Logs: Ep.4 — Error Logs	Recognize web server error logs	100
2021-12-07	Web Server Logs: Ep.3 — Access Logs	Recognize web server access logs	100
2021-12-07	Web Server Logs: Ep.2 — Log Formats	Describe the different types of web server log formats	20
2021-12-07	Web Server Logs: Ep.1 — What are Web Server Logs?	Recall the different types of web server logs	20
2021-12-07	Splunk: Malicious Account Creation	Identify and recognise malicious events in system logs	200
2021-12-07	Splunk: Event Analysis 2 (ARCHIVED)	Demonstrate and develop event log analysis techniques	200

Activity Report Page 39 of 42

Date	Lab	Description	Points Earned
2021-12-07	SMTP Log Analysis	Carry out a log analysis in order to identify particular information	100
2021-12-07	Accounting and Audit	Identify audit and accounting methodology	200
2021-12-07	Splunk: Event Analysis (ARCHIVED)	Demonstrate and develop basic event log analysis techniques	200
2021-12-07	Log Finder	Perform web log analysis	100
2021-12-02	Demonstrate Your Skills: Splunk Basics	Recall the Splunk features and how to use them	200
2021-12-02	Splunk Basics: Ep.5 – Dashboards and Visualization	Recognize dashboards and how they can be used	100
2021-12-02	Splunk Basics: Ep.4 – Advanced Searching (SPL & Transforming)	Use Splunk's Search Processing Language (SPL) to search for and transform specific information	200
2021-12-02	Splunk Basics: Ep.3 – Search	Identify the key structure of a basic Splunk search	100
2021-11-30	Splunk Basics: Ep.2 – Data Sources	Be able to recall the various data sources supported by Splunk	40
2021-11-30	Splunk Basics: Ep.1 – The Splunk Interface	Recognize the different components of the Splunk Interface	40
2021-11-30	What is Splunk?	Recall what the Splunk tool is	40
2021-11-30	Incident Response Theory: Ep.6 – Post-Incident Activity	Identify the post-incident activity stage of the NIST incident response process	40
2021-11-30	Incident Response Theory: Ep.4 – Detection and Analysis	Identify the detection and analysis stage of the NIST incident response process	40
2021-11-30	Incident Response Theory: Ep.5 – Containment, Eradication, and Recovery	Identify the containment, eradication, and recovery stage of the NIST incident response process	40
2021-11-30	Incident Response Theory: Ep.3 – Preparation	Identify the details of the preparation stage of NIST's incident response process	40

Activity Report Page 40 of 42

Date	Lab	Description	Points Earned
2021-11-30	Yara: Ep.2	Investigate unique data related to malware samples	200
2021-11-30	Yara: Ep.1	Investigate unique data related to malware samples	200
2021-11-30	Validating SIEM Results	Identify whether a SIEM's actions are accurate in any given scenario	40
2021-11-30	Incident Response Theory: Ep.2 – Process	Recognize the stages of the incident response process	40
2021-11-30	Incident Response Theory: Ep.1 – Introduction	Identify incident response principles	40
2021-11-29	Demonstrate Your Skills: Packet Analysis	Demonstrate the skills acquired through the beginner Wireshark labs	400
2021-11-29	Traffic Analysis: Malware	Recognise useful starting points for analysts when viewing network traffic	200
2021-11-29	Wireshark: Stream/Object Extraction	Analyse network packet captures	200
2021-11-23	Traffic Analysis: Device Information	Recognise useful starting points for analysts when viewing network traffic	200
2021-11-23	Understanding Wireshark: TLS handshake	Revise information on the TLS Handshake	100
2021-11-23	Wireshark Statistics	Analyse network packet captures using Wireshark statistics	100
2021-11-23	Wireshark Display Filters: Filters In Depth	Analyse network packet captures using complex operators	200
2021-11-23	Wireshark Display Filters: An Introduction	Analyse network packet captures	100
2021-11-23	Intro to Wireshark	Analyse network packet captures	100
2021-11-23	Packet Capture Basics	Analyse network packet captures	100

Activity Report Page 41 of 42

Date	Lab	Description	Points Earned
2021-11-22	Accidental and Malicious Data Leaks	Recognize the differences between accidental leaks and malicious leaks	10
2021-11-22	Case Study: Covid-19 Cybercriminals	Identify the characteristics of Covid-19 phishing scams	10
2021-11-22	Identifying Ransomware	Recognize the tell-tale signs of ransomware	10
2021-11-22	Updates and Patches	Identify the differences between updates and patches	10
2021-11-22	Firewalls and VPNs	Recognize the benefits of firewalls and VPNs	10
2021-11-22	Consequences and Impacts of Cyberattacks	Recognize the differences between the consequences and impacts of cyberattacks	10
2021-11-22	Why Information Security Is Everyone's Business	Recognize the importance of information security	10
2021-11-22	Passwords	Recognize how to protect yourself and your devices with strong passwords	10
2021-11-22	Antivirus	Identify the purpose of antivirus software and its main features	10
2021-11-22	Mobile Security Tips	Identify potential threats to mobile phone security	10
2021-11-22	Identity Theft	Recognize the ways to prevent identity theft and the warning signs to look out for	10
2021-11-22	Backups	Recognize the importance of backups	10
2021-11-22	Multi-Factor Authentication	Recall how multi-factor authentication works	10
2021-11-22	Safer Browsing	Recall how to protect yourself and your privacy as you browse the web	10
2021-11-22	Phishing Emails	Recognize the main characteristics of phishing emails	10

Date	Lab	Description	Points Earned
2021-11-22	Malware	Recognize the most common forms of malware and how they can affect you	10

About Immersive Labs

Immersive Labs is the world's first fully interactive, on-demand, and gamified cyber skills platform. Our technology delivers challenge-based assessments and upskilling exercises which are developed by cyber experts with access to the latest threat intelligence. Our unique approach engages users of every level, so all employees can be equipped with critical skills and practical experience in real time.