IMMERSIVELABS

Immersive Labs - Latest Labs Content

05-02-2024

Categories

Fundamentals (354 labs)

Awareness

These labs focus on educating users about cybersecurity best practices, common threats, and security awareness strategies. These labs aim to enhance users' understanding of social engineering techniques, phishing attacks, password security, and other critical aspects of cybersecurity awareness. By completing these labs, users can develop the knowledge and skills needed to recognize and mitigate security risks, ultimately contributing to a more security-conscious workforce.

Awareness	**86**
AI for Business	4
Authentication	5
Browsing Securely	5
Cyber 101	12
Cyber Safety	15
Data Handling	4

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Awareness	**86**
Device Security	4
Data Privacy	3
Digital Footprint	4
Physical Security	4
Security Reporting and Responsiveness	4
Social Engineering	5
Staying Safe Online	16

Crisis Management

These labs are designed to simulate cyber incidents and provide hands-on experience in responding to and managing security breaches. These labs offer practical scenarios where users can practice incident response, containment, and recovery strategies in a controlled environment. By engaging with these labs, users can develop critical skills in handling cybersecurity crises effectively, preparing them to respond swiftly and decisively to real-world security incidents.

Crisis Management	**10**
Business Continuity 101	5
Crisis Management 101	5

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Cyber Fundamentals

These labs offer a comprehensive introduction to essential cybersecurity concepts and principles. These labs cover topics such as networking basics, cryptography, security protocols, and common cyber threats. By completing these labs, users can build a solid foundation in cybersecurity knowledge and skills, making it an ideal starting point for beginners looking to enter the field or professionals seeking to reinforce their fundamental understanding of cybersecurity.

Cyber Fundamentals	**175**
Active Directory Basics	9
AI Fundamentals	9
Cyber 101	12
Encoding	8
Ethics & Laws	6
Historic Encryption	10
Human Factors in Cybersecurity	6
Interactive Regular Expressions	9
Introduction to Cryptography	12
Introduction to Digital Forensics	6
Introduction to Networking	7
Linux Command Line	17
Modern Encryption	15
Networking	23
Secure Fundamentals	8
Windows Basics	8

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Cyber Fundamentals	**175**
Windows Concepts	10

Management, Risk & Compliance

These labs focus on key aspects of cybersecurity governance, risk management, and compliance frameworks. These labs cover topics such as risk assessment, regulatory compliance, security policies, and security controls implementation. By completing these labs, users can gain a deeper understanding of how to effectively manage cybersecurity risks, ensure compliance with relevant regulations, and establish robust security practices within an organization.

Management, Risk & Compliance	**83**
AI for Business	4
Compliance	16
Cyber for Board Members	9
Cyber for Executives	8
Data Privacy	3
Introduction to Penetration Test Programs	11
ISO 22381 - Security and Resilience for Identification Systems	3
ISO 27001 - Information Security Management Systems	3
ISO 27014 - Governance of Information Security	3
ISO 27018 - Protecting Private Data in Public Clouds	5
ISO 28000 - Security Management Systems for Supply Chains	2
ISO 31000 - Risk Management	5
Risk	11

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Defensive Cyber (844 labs)

Defensive Fundamentals

These labs focus on practical exercises and simulations to enhance users' defensive cybersecurity skills. These labs cover topics such as threat detection, incident response, vulnerability management, and security monitoring. By engaging with these labs, users can develop the expertise needed to protect systems, detect and respond to threats effectively, and strengthen the overall security posture of an organization.

Defensive Fundamentals	**76**
AI Fundamentals	9
CTI First Principles	7
Introduction To Elastic	10
NIST - Guidelines on Security and Privacy in Public Cloud Computing (800-144)	10
NIST - Security and Privacy Controls for Information Systems and Organizations (800-53)	22
Secure Fundamentals	8
Windows Forensics Artifacts	10

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Digital Forensics

These labs are designed to provide hands-on experience in investigating and analyzing digital evidence related to cybersecurity incidents. These labs cover topics such as forensic tools, evidence collection, data analysis, and incident reconstruction. By completing these labs, users can develop the skills necessary to conduct thorough digital investigations, identify security breaches, and gather evidence for potential legal proceedings.

Digital Forensics	**81**
Autopsy	11
DDoS Analysis	5
Digital Forensics	19
Digital Forensics Process	9
Eric Zimmerman's Tools	11
Introduction to Digital Forensics	6
Volatility	10
Windows Forensics Artifacts	10

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Incident Response

These labs focus on preparing users to effectively respond to cybersecurity incidents in real-time. These labs simulate various cyber attack scenarios, requiring users to analyze, contain, eradicate, and recover from security breaches.

Incident Response	**168**
CVEs (Threat Hunting)	16
DFIR - Wizard Spider	10
Elastic Stack	10
Incident Response	14
Introduction to Detection Engineering	5
Introduction to Incident Response	8
Introduction to Malware Analysis	11
Introduction to Velociraptor	8
Log Analysis	10
Malicious Documents Analysis	10
Malware Analysis	19
Packet Analysis	18
Snort	11
Web Log Analysis	6
Yara	12

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Malware (Defensive)

These labs focus on equipping users with the knowledge and skills to detect, analyze, and mitigate malware threats. These labs cover topics such as malware types, behavior analysis, signature-based detection, and malware removal techniques.

Malware (Defensive)	**85**
Foundational Static Analysis	7
Introduction to Malware Analysis	11
Malicious Documents Analysis	10
Malware Analysis	19
Mobile Malware	5
Python Scripting for Malware Analysis	6
Ransomware	27

OT/ICS For Incident Responders

These labs focus on preparing incident responders to handle cybersecurity incidents in Operational Technology (OT) and Industrial Control Systems (ICS) environments. These labs cover topics such as OT/ICS architecture, protocols, vulnerabilities, and incident response strategies specific to critical infrastructure.

OT/ICS For Incident Responders	**17**
OT: Devices and Protocols	8
OT: Fundamentals	5
OT: Threats and Vulnerabilities	4

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Reverse Engineering (Defensive)

These labs focus on teaching users how to analyze and understand the behavior of malicious software through reverse engineering techniques. These labs cover topics such as disassembly, debugging, malware analysis, and identifying malware functionalities.

Reverse Engineering (Defensive)	**89**
Assembly Language	9
Computer Architecture	12
GDB	6
Ghidra	6
Heap Internals	6
Introduction to PowerShell Deobfuscation	6
Introduction to Reverse Engineering	11
PowerShell Deobfuscation	12
Radare2	3
RE - Interpreted Languages	7
WinDBG	6
x64dbg	5
Windows Source Code Analysis: Stack Overflow	9

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Source Code Analysis

These labs focus on teaching users how to review and analyze source code for security vulnerabilities and weaknesses. These labs cover topics such as static code analysis, code review techniques, identifying common coding errors, and secure coding practices.

Source Code Analysis	**9**
Windows Source Code Analysis: Stack Overflow	9

Threat Hunting

These labs are designed to train users in proactively seeking out and identifying potential security threats within an organization's network. These labs cover topics such as threat intelligence, log analysis, anomaly detection, and hunting for indicators of compromise. By engaging with these labs, users can develop the skills needed to detect and respond to advanced threats before they escalate, enhancing the overall cybersecurity defense capabilities of an organization.

Threat Hunting	**100**
Fundamental AI Algorithms	8
Introduction to Velociraptor	8
MITRE ATT&CK	17
Threat Hunting	18
Threat Hunting - Theory	17
Threat Hunting- APT29 (Elasticsearch)	11
Threat Hunting - APT29 (Splunk)	11
Threat Hunting - FIN7 (Splunk)	10

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Tools (Defensive)

These labs focus on familiarizing users with a variety of cybersecurity tools used for defensive purposes. These labs cover topics such as security tool installation, configuration, and utilization for tasks such as network monitoring, vulnerability scanning, and incident response. By completing these labs, users can gain hands-on experience with essential cybersecurity tools, enhancing their ability to protect systems and respond to security incidents effectively.

Tools (Defensive)	**190**
Autopsy	11
Elastic Data Ingest	8
Elastic Playground	4
Elastic Stack	10
Eric Zimmerman's Tools	11
Ghidra	6
Introduction to Sigma	4
Introduction to Velociraptor	8
Machine Learning	8
Packet Analysis	18
Powershell	12
Radare2	3
Snort	11
Splunk	7
The OpenSCAP Project	7
Volatility	10
WinDBG	6

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Tools (Defensive)	**190**
Windows Sysinternals	11
Wireshark	9
x64dbg	5
Yara	12
Zeek	9

Vulnerability Management

These labs focus on training users in identifying, assessing, prioritizing, and mitigating security vulnerabilities within an organization's systems and networks. These labs cover topics such as vulnerability scanning, risk assessment, patch management, and vulnerability remediation strategies. By engaging with these labs, users can develop the skills necessary to effectively manage vulnerabilities, reduce the attack surface, and strengthen the overall security posture of an organization.

Vulnerability Management	**29**
OWASP Top 10	13
Scanning	9
Vulnerability Management	7

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Offensive Cyber (705 labs)

Adversary Simulation

These labs simulate real-world cyber attacks to help users understand the tactics, techniques, and procedures used by threat actors. These labs cover topics such as penetration testing, red teaming, social engineering, and advanced persistent threats. By engaging with these labs, users can enhance their offensive cybersecurity skills, test the resilience of their defenses, and improve their ability to detect and respond to sophisticated cyber threats.

Adversary Simulation	**35**
Exploitation, Weaponization, and Delivery	10
Introducing the Cyber Kill Chain	10
Reconnaissance	13
Simulations	2

Exploit Development (Offensive)

These labs focus on teaching users how to identify, exploit, and mitigate software vulnerabilities. These labs cover topics such as buffer overflows, shellcoding, exploit writing, and reverse engineering. By completing these labs, users can enhance their skills in developing exploits, understanding the inner workings of vulnerabilities, and improving their overall offensive cybersecurity capabilities.

Exploit Development (Offensive)	**20**
Exploitation Development	7
Introduction to Heap Exploitation	5
Introduction to Linux Exploitation	4
Introduction to Windows Exploitation	4

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Infrastructure Hacking

These labs focus on training users in identifying and exploiting vulnerabilities in network infrastructure components. These labs cover topics such as network scanning, enumeration, privilege escalation, and lateral movement within a network. By engaging with these labs, users can develop the skills needed to assess and secure network infrastructure, simulate real-world attacks, and enhance their offensive cybersecurity capabilities.

Infrastructure Hacking	**244**
CANBus	16
Credential Access	11
CVEs (Infrastructure Hacking)	35
CVEs (Privilege Escalation)	12
Databases	5
Discovery	7
Hack Your First Computer	7
Infrastructure Hacking	25
Infrastructure Pen Testing	9
Introduction To Metasploit	9
Introduction to Penetration Testing	5
IoT & Embedded Devices	9
Kerberos	13
MITRE ATT&CK	17
Persistence	9
PoshC2	6
Post Exploitation With Metasploit	9

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Infrastructure Hacking	**244**
Powershell	12
Privilege Escalation: Linux	9
Privilege Escalation: Windows	9
Windows Exploitation	10

Malware (Offensive)

These labs focus on teaching users how to create, analyze, and deploy malware for offensive purposes. These labs cover topics such as malware development, obfuscation techniques, evasion tactics, and payload delivery methods. By completing these labs, users can enhance their skills in understanding malware behavior, developing countermeasures, and improving their offensive cybersecurity capabilities.

Malware (Offensive)	**72**
Introduction to Malware Analysis	11
Malicious Documents Analysis	10
Malware Analysis	19
Mobile Malware	5
Ransomware	27

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Reconnaissance

These labs focus on training users in gathering information about potential targets to identify vulnerabilities and plan cyber attacks effectively. These labs cover topics such as open-source intelligence (OSINT) gathering, foot printing, scanning, and enumeration techniques. By engaging with these labs, users can develop the skills needed to conduct thorough reconnaissance, assess the security posture of targets, and enhance their offensive cybersecurity capabilities.

Reconnaissance	**25**
OSINT	16
Scanning	9

Reverse Engineering (Offensive)

These labs focus on teaching users how to analyze and manipulate software and firmware to uncover vulnerabilities and develop exploits. These labs cover topics such as disassembly, debugging, code analysis, and exploit development techniques. By completing these labs, users can enhance their skills in reverse engineering, understand how malware operates, and improve their offensive cybersecurity capabilities.

Reverse Engineering (Offensive)	**90**
Assembly Language	9
Computer Architecture	12
GDB	6
Ghidra	6
Heap Internals	6
Introduction to Reverse Engineering	11
Radare2	3
RE - Interpreted Languages	7
WinDBG	6

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Source Code Analysis (Offensive)

These labs focus on training users in reviewing and analyzing source code to identify security vulnerabilities and weaknesses that can be exploited. These labs cover topics such as code auditing, identifying backdoors, analyzing authentication mechanisms, and understanding code logic flow. By engaging with these labs, users can enhance their skills in source code analysis, discover potential attack vectors, and improve their offensive cybersecurity capabilities.

Source Code Analysis (Offensive)	**24**
Linux Source Code Analysis: Stack Overflow	6
Windows Source Code Analysis: Heap Exploitation	9
Windows Source Code Analysis: Stack Overflow	9

Tools (Offensive)

These labs focus on familiarizing users with a variety of cybersecurity tools used for offensive purposes. These labs cover topics such as penetration testing tools, exploitation frameworks, network sniffers, and post-exploitation tools. By completing these labs, users can gain hands-on experience with essential offensive cybersecurity tools, enhancing their ability to simulate attacks, identify vulnerabilities, and improve overall offensive security capabilities.

Tools (Offensive)	**95**
Burp Suite	5
Ghidra	6
Introduction to Aircrack-ng	8
Introduction To Metasploit	9
Nessus	5
Nmap	9
PoshC2	6
Post Exploitation With Metasploit	9

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Tools (Offensive)	**95**
Powershell	12
Pwntools	6
Radare2	3
WinDBG	6
Windows Sysinternals	11

Web App Hacking

These labs focus on training users in identifying and exploiting vulnerabilities in web applications. These labs cover topics such as SQL injection, cross-site scripting (XSS), CSRF attacks, and web application firewall evasion techniques. By engaging with these labs, users can develop the skills needed to assess and secure web applications, understand common attack vectors, and enhance their offensive cybersecurity capabilities.

Web App Hacking	**124**
Authentication and Authorization Flaws	10
Burp Suite	5
Cross-Site Scripting (XSS)	7
CVEs (Web App Hacking)	26
Databases	5
Hack Your First Web Application	6
Intermediate Web App Hacking	7
Intro to Web App Hacking	12
Introduction to Penetration Testing	5
OWASP (2017) Java	10
OWASP Top 10	13

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Web App Hacking	124
Server-Side Template Injection	6
SQL Injection	5
SQL Injection Basics	7

Application Security (552 labs)

Please see the AppSec Lab Catalog

Cloud Security (266 labs)

Amazon Web Services

These labs focus on providing hands-on training for securing and managing AWS cloud environments. These labs cover topics such as identity and access management (IAM), network security, data encryption, and incident response in AWS. By engaging with these labs, users can enhance their skills in securing cloud infrastructure, understanding AWS security best practices, and improving their overall cloud security knowledge.

Amazon Web Services	124
Advanced Logging in AWS	5
Amazon Web Services	7
AWS Challenge: Jobs at Metrolio	3
AWS Config	6
AWS Security Hub	5
AWS Systems Manager	7
EC2 (Elastic Compute Cloud)	11
IAM (Identity and Access Management)	13

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Amazon Web Services	**124**
Incident Response and Forensics for EC2	3
Introduction to Incident Response & Forensics in AWS	5
Investigating IAM Incidents in AWS	4
Logging & Monitoring in AWS	12
S3 (Simple Storage Service)	9
Secrets and Encryption in AWS	4
Securing Serverless Workflows with AWS Lambda	5
Securing Web Applications with AWS WAF and CloudFront	4
Threat Detection with Amazon GuardDuty	4
Top 10 AWS Attacker Techniques 2023	10
VPC & Network Security	7

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Cloud Fundamentals

These labs focus on introducing users to the basic concepts and principles of cloud computing. These labs cover topics such as cloud service models, deployment models, shared responsibility model, and cloud security considerations. By completing these labs, users can gain a foundational understanding of cloud computing, learn about key cloud security concepts, and prepare for more advanced cloud security training within the IL Cyber Pro solution.

Cloud Fundamentals	**50**
Cloud Fundamentals	12
DevSecOps	9
NCSC - Cloud Security Guidance	15
NIST- Guidelines on Security and Privacy in Public Cloud Computing (800-144)	10
Zero Trust in the Cloud	4

Cloud Tooling

These labs focus on training users in utilizing various tools and technologies specific to cloud environments. These labs cover topics such as cloud monitoring tools, configuration management tools, cloud automation frameworks, and cloud security assessment tools. By engaging with these labs, users can gain hands-on experience with essential cloud tooling, enhance their cloud security skills, and improve their ability to manage and secure cloud infrastructures effectively.

Cloud Tooling	**61**
Apache	12
Apache Tomcat	7
AWS Community - Security Tooling	3
Container Hardening - Docker	5
NGINX	5

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Cloud Tooling	**61**
OAuth and OpenID Connect	6
Secrets Management with HashiCorp Vault	10
Secure Terraform - AWS	5
Secure Terraform - Azure	4
Secure Terraform - Google Cloud Platform	4

Kubernetes

These labs focus on training users in securing and managing Kubernetes container orchestration platforms. These labs cover topics such as Kubernetes architecture, pod security policies, network policies, and securing Kubernetes clusters. By engaging with these labs, users can develop the skills needed to secure containerized environments, implement best practices for Kubernetes security, and enhance their cloud security capabilities.

Kubernetes	**31**
CISA and NSA Kubernetes Hardening Guidance	6
Kubernetes - Fundamentals	8
Kubernetes - Logging	5
Kubernetes - Offensive Security	5
Kubernetes - Pod Security	7

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Cyber Threat Intelligence (471 labs)

Campaigns

These labs focus on simulating real-world cyber threat scenarios and attacks. These labs cover topics such as threat actor profiling, attack attribution, malware analysis, and incident response to sophisticated cyber campaigns. By engaging with these labs, users can enhance their skills in threat intelligence analysis, understand the tactics used by threat actors, and improve their ability to detect and respond to complex cyber threats effectively.

Campaigns	**32**
Events & Breaches	9
Hafnium	6
Log4Shell (CVE-2021-44228 & CVE-2021-45046)	4
MOVEit (CVE-2023-34362)	4
Spring4Shell (CVE-2022-22965)	4
SUNBURST Supply Chain Compromise	5

CTI Vendors & Tools

These labs focus on familiarizing users with various threat intelligence vendors and tools used in the cybersecurity industry. These labs cover topics such as threat intelligence platforms, open-source intelligence (OSINT) tools, threat feeds, and analysis tools. By completing these labs, users can gain hands-on experience with different CTI tools, understand how to leverage threat intelligence effectively, and enhance their skills in threat detection and analysis.

CTI Vendors & Tools	**4**
CTI Platforms	2
CTI Tools	2

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

CVEs

These labs focus on training users to analyze and respond to known vulnerabilities in software and systems. These labs cover topics such as CVE identification, vulnerability assessment, patch management, and vulnerability prioritization. By engaging with these labs, users can enhance their skills in vulnerability management, understand the impact of CVEs on cybersecurity, and improve their ability to mitigate risks associated with known vulnerabilities effectively.

CVEs	**229**
CISA KEV	10
CVEs (<2018)	14
CVEs (2019)	26
CVEs (2020)	14
CVEs (2021)	22
CVEs (2022)	25
CVEs (2023)	20
CVEs (2024)	3
CVEs (Infrastructure Hacking)	35
CVEs (Privilege Escalation)	12
CVEs (Threat Hunting)	16
CVEs (Web App Hacking)	26
Hafnium	6

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Latest

These labs focus on providing users with up-to-date scenarios and challenges based on the latest cyber threats and trends. These labs cover emerging threats, new attack techniques, recent data breaches, and evolving cybersecurity issues. By engaging with these labs, users can stay current with the rapidly changing cybersecurity landscape, enhance their threat intelligence skills, and prepare for real-world cyber threats effectively.

Latest	**36**
Emerging Threats	8
Latest CVEs	16
Trending Malware	12

Nation State: Russia

These labs focus on exploring the cyber threat landscape associated with Russian state-sponsored actors. These labs cover topics such as Russian cyber espionage tactics, malware campaigns linked to Russian threat actors, geopolitical motivations, and attribution challenges. By engaging with these labs, users can deepen their understanding of Russian cyber threats, enhance their threat intelligence analysis skills specific to this threat actor group, and improve their ability to detect and respond to cyber attacks originating from Russia.

Nation State: Russia	**32**
Nobelium	5
SUNBURST Supply Chain Compromise	5
Threat Hunting - APT29 (Elasticsearch)	11
Threat Hunting - APT29 (Splunk)	11

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Threat Actors and Threats

These labs focus on educating users about different threat actors, their tactics, techniques, and procedures (TTPs), as well as the various types of cyber threats organizations may face. These labs cover topics such as threat actor profiling, threat intelligence analysis, threat modeling, and understanding the motivations behind cyber attacks. By engaging with these labs, users can enhance their threat intelligence skills, improve their ability to identify and respond to specific threat actors and threats, and strengthen their overall cybersecurity posture.

Threat Actors and Threats	**138**
DFIR - Wizard Spider	10
Hafnium	6
Nobelium	5
Threat Actors	22
Threat Hunting - APT29 (Elasticsearch)	11
Threat Hunting - APT29 (Splunk)	11
Threat Hunting - FIN7 (Splunk)	10
Malware - CTI	25
Threat Hunting	18
Threat Research	20

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

Challenges and Scenarios (210 labs)

A Christmas Catastrophe	9
AI Challenges	3
Archive	52
AWS Challenge: Jobs at Metrolio	3
BSides	2
Cyber Experts	4
DEFCON 2023	8
DEFCON/Black Hat	11
DFIR CTF	7
Ethereum - Smart Contracts (Solidity)	7
Halloween: A Murder Mystery	5
Halloween: The Haunted Hollow	10
Immersive Bank Mini-Series	5
Immersive Care Mini Series	5
Immersive Labs: May 4th	7
Kate's Story	4
Mini CTFs	13
Omnipotent Productions	6
Parellus Power Mini Series	6
Pen Test CTFs	12

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved

PowerShell Deobfuscation	12
SuperSonic	7
The Cyber Kill Chain	8
World Cup Special	4

Sharing or forwarding this document is prohibited. Copyright 2024 Immersive Labs | All Rights Reserved