



Lab Content 2022

Updated 21st June



Total labs: 1,669*

FUNDAMENTALS

208

Awareness

31

Staying Safe Online

16

Cyber Safety

15

Cyber Fundamentals

134

Networking

21

Linux Command Line

16

Modern Encryption

14

Cyber 101

12

Introduction to Cryptography

11

Historic Encryption

10

Interactive Regular Expressions

9

Windows Concepts

9

Encoding

8

Secure Fundamentals

7

Ethics & Laws

6

Introduction to Networking

6

Introduction to Digital Forensics

5

Management, Risk & Compliance

43

Compliance

15

Risk

11

Cyber for Executives

9

Cyber for Board Members

6

Rewards

2

MALWARE & REVERSE ENGINEERING

163

Exploitation Development

9

Exploitation Development

6

Introduction to Windows Exploitation

3

Malware

96

Malware - CTI

26

Ransomware

25

Malware Analysis

19

Introduction to Malware Analysis

11

Malicious Documents Analysis

10

Mobile Malware

5

Reverse Engineering

49

Computer Architecture

11

Introduction to Reverse Engineering

10

Assembly Language

8

RE - Interpreted Languages

7

Ghidra

5

WinDBG

5

Radare2

3

Source Code Analysis

9

Stack Overflow

9

**CHALLENGES & SCENARIOS 234**

Archive	49
Secure Code Competition	15
PowerShell Deobfuscation	12
DEFCON/Black Hat	11
Mini CTFs	11
Boot2Root	10
Pen Test CTFs	10
A Christmas Catastrophe	9
Blue Team Challenges	8
Defensive CTF - KWEEN Industries	8
Offensive CTF - KWEEN Industries	8
DFIR CTF	7
Ethereum - Smart Contracts (Solidity)	7
Immersive Labs: May 4th	7
SuperSonic	7
The Cyber Kill Chain	7
Omnipotent Productions	6
Halloween	5
Immersive Bank Mini-Series	5
Immersive Care Mini Series	5
Immersive Power Mini Series	5
Pharma Drama	5
Cyber Experts	4
Kate's Story	4
World Cup Special	4
BreathGen	3
BSides	2

APPLICATION SECURITY 305**Secure Coding 241**

PHP	20
Java - Beginner	14
Java - Intermediate	14
Python - Beginner	13
Real-world Playground	13
Ruby	13
C# .NET Core (MVC)	11
Node.js - Beginner	11
C# .NET Framework (MVC)	10
C++ - Beginner	10
C++ - Intermediate	10
Java Spring - Beginner	10
Node.js - Intermediate	10
Python - Advanced	10
Python - Intermediate	10
Rails - Beginner	10
Go - Beginner	9
C# .NET Framework (Web Forms)	8
Rails - Intermediate	8
Java API	7
Angular	5
Java - Advanced	5
React	5
Vue.js	5

Secure Engineering 20

Security Headers	10
Introduction to Content Security Policy (CSP)	6
Secure Engineering	4

Secure Fundamentals 37

Introduction to Cryptography	11
OWASP Top 10	11
TLS Fundamentals	8
Secure Fundamentals	7



Secure Operations	27
Apache	12
Apache Tomcat	7
NGINX	5
Secure Operations - Beginner	3
Secure Testing	11
Secure Testing - Beginner	11
Secure Tooling	26
OWASP ZAP - Basics	9
Browser Developer Tools	7
Burp Suite	5
Secure Tooling - Beginner	5

CLOUD SECURITY	159
Amazon Web Services	41
IAM (Identity and Access Management)	13
EC2 (Elastic Compute Cloud)	11
S3 (Simple Storage Service)	9
Amazon Web Services	8
Cloud Fundamentals	36
NCSC - Cloud Security Guidance	15
Cloud Fundamentals	11
NIST - Guidelines on Security and Privacy in Public Cloud Computing (800-144)	10
Cloud Tooling	51
Apache	12
Apache Tomcat	7
OAuth and OpenID Connect	6
Container Hardening - Docker	5
NGINX	5
Secure Terraform - AWS	5
Secure Terraform - Azure	4
Secure Terraform - Google Cloud Platform	4
AWS Community - Security Tooling	3
Kubernetes	31
Kubernetes - Fundamentals	8
Kubernetes - Pod Security	7
CISA and NSA Kubernetes Hardening Guidance	6
Kubernetes - Logging	5
Kubernetes - Offensive Security	5



DEFENSIVE CYBER

600

Defensive Fundamentals 38

NIST - Security and Privacy Controls for Information Systems and Organizations (800-53) 21

NIST - Guidelines on Security and Privacy in Public Cloud Computing (800-144) 10

Secure Fundamentals 7

Digital Forensics 42

Digital Forensics 18

Autopsy 10

Volatility 9

Introduction to Digital Forensics 5

Incident Response 150

Malware Analysis 19

Packet Analysis 17

Incident Response 14

CVEs (Threat Hunting) 13

Yara 12

Introduction to Malware Analysis 11

Snort 11

DFIR – Wizard Spider 10

Elastic Stack 10

Log Analysis 10

Malicious Documents Analysis 10

Introduction to Incident Response 7

Web Log Analysis 6

Malware (Defensive) 70

Ransomware 25

Malware Analysis 19

Introduction to Malware Analysis 11

Malicious Documents Analysis 10

Mobile Malware 5

Reverse Engineering (Defensive) 49

Computer Architecture 11

Introduction to Reverse Engineering 10

Assembly Language 8

RE - Interpreted Languages 7

Ghidra 5

WinDBG 5

Radare2Packet Analysis 3

Source Code Analysis (Defensive) 9

Stack Overflow 9

Threat Hunting 74

Threat Hunting - Theory 16

MITRE ATT&CK 15

Threat Hunting 13

Threat Hunting – APT29 (Elasticsearch) 10

Threat Hunting – APT29 (Splunk) 10

Threat Hunting – FIN7 (Splunk) 10

Tools (Defensive) 136

Packet Analysis 17

Powershell 12

Yara 12

Snort 11

Windows Sysinternals 11

Autopsy 10

Elastic Stack 10

Volatility 9

Zeek 9

Wireshark 8

Splunk 7

The OpenSCAP Project 7

Ghidra 5

WinDBG 5

Radare2 3

Vulnerability Management 32

Scanning 15

OWASP Top 10 11

Vulnerability Management 6



CYBER THREAT INTELLIGENCE		337	OFFENSIVE CYBER		530
CVEs	158	Adversary Simulation	32		
CVEs (Infrastructure Hacking)	33	Introducing the Cyber Kill Chain	9		
CVEs (2019)	26	Reconnaissance: DNS & Whois	7		
CVEs (2021)	24	Reconnaissance: User Enumeration	5		
CVEs (Web App Hacking)	20	Weaponization: Payloads	5		
CVEs (2020)	13	Exploitation	3		
CVEs (<2018)	13	Simulations	2		
CVEs (Threat Hunting)	13	Delivery	1		
CVEs (Privilege Escalation)	10	Exploit Development (Offensive)	9		
Hafnium	6	Exploitation Development	6		
Latest	42	Introduction to Windows Exploitation	3		
Latest CVE & Threats	34	Infrastructure Hacking	203		
Log4Shell (CVE-2021-44228 & CVE-2021-45046)	4	CVEs (Infrastructure Hacking)	33		
Spring4Shell (CVE-2022-22965)	4	Infrastructure Hacking	25		
Nation State: Russia	30	CANBus	16		
Threat Hunting - APT29 (Elasticsearch)	10	MITRE ATT&CK	15		
Threat Hunting - APT29 (Splunk)	10	Powershell	12		
Nobelium	5	Credential Access	11		
SUNBURST Supply Chain Compromise	5	CVEs (Privilege Escalation)	10		
Threats	107	Infrastructure Pen Testing	9		
Threat Actors	15	IoT & Embedded Devices	9		
Threat Research	15	Metasploit	9		
Threat Hunting	13	Persistence	9		
Events & Breaches	8	Privilege Escalation	9		
DFIR - Wizard Spider	10	Windows Exploitation	9		
Threat Hunting – APT29 (Elasticsearch)	10	Discovery	7		
Threat Hunting – APT29 (Splunk)	10	Hack Your First Computer	6		
Threat Hunting – FIN7 (Splunk)	10	Databases	5		
Hafnium	6	PoshC2	5		
Nobelium	5	Introduction to Penetration Testing	4		
SUNBURST Supply Chain Compromise	5	Malware (Offensive)	70		
		Ransomware	25		
		Malware Analysis	19		
		Introduction to Malware Analysis	11		



Malicious Documents Analysis	10
Mobile Malware	5
Reconnaissance	42
OSINT	15
Scanning	15
Reconnaissance: DNS & Whois	7
Reconnaissance	5
Secure Code Analysis (Offensive)	9
Stack Overflow	9
Tools (Offensive)	62
Powershell	12
Windows Sysinternals	11
Metasploit	9
Introduction to Cobalt Strike	7
Burp Suite	5
Ghidra	5
PoshC2	5
WinDBG	5
Radare2	3
Web App Hacking	103
CVEs (Web App Hacking)	20
Intro to Web App Hacking	12
OWASP Top 10	11
Authentication and Authorisation Flaws	10
Top 10 OWASP Java	9
Intermediate Web App Hacking	7
Hack Your First Web Application	6
SQL Injection Basics	6
Burp Suite	5
Databases	5
SQL Injection	5
Introduction to Penetration Testing	4
Cross-Site Scripting (XSS)	3

* Note that some labs appear under more than one category but are only counted once overall