IMMERSIVELABS

DATA SHEET

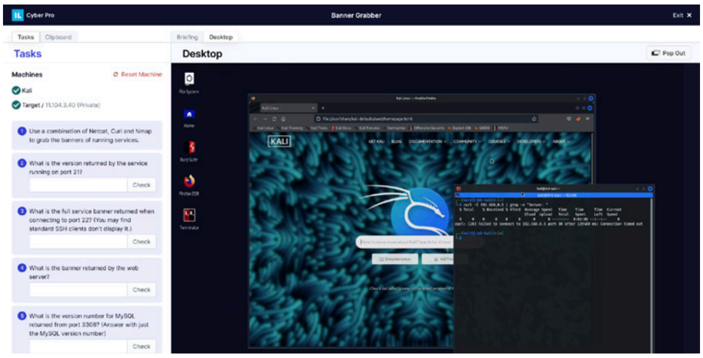
Hands-on Labs: Continuously master the latest cyber threats

When the unexpected happens, resilience is essential. The entire organization must be prepared with the knowledge, skills, and judgment to respond to cyber threats.

Unfortunately, legacy cybersecurity training is ineffective because it is focused on activities, not outcomes and individuals instead of teams. It's time for a new approach.

Assess, build, and prove your people-centric resilience with highly-technical labs that cover all aspects of cybersecurity, including offensive, defensive, cloud, and application security.

Use the latest gamified techniques and live environments to learn topics from security fundamentals to malware reverse engineering and advanced threat hunting.



Tasks

Machines

Reset Machine

✓ Kali

✓ Target / 11.104.3.40 (Private)

1. Use a combination of Netcat, Curl and Nmap to grab the banners of running services.
2. What is the version returned by the service running on port 21? Check
3. What is the full service banner returned when connecting to port 22? (You may find standard SSH clients don't display it.) Check
4. What is the banner returned by the web server? Check
5. What is the version number for MySQL returned from port 3306? (Answer with just the MySQL version number) Check

Desktop

Labs use live environments to ensure learning is engaging and memorable

Benefits

- Improve individual and team cybersecurity capabilities across a comprehensive range of subjects
- Benchmark and prove current levels of cyber capabilities across the organization
- Demonstrate team ability aligned to security frameworks (e.g., MITRE ATT&CK)
- Improve speed of response to emerging threats
- Increase efficacy in recruitment, retention, and promotion
- Reduce vulnerabilities early and across the SDLC
- Securely configure cloud workloads

Audiences

- Defensive Cybersecurity Professionals
- Penetration Testers
- Developers
- Application Security Experts
- Cloud & Infrastructure Security
- Entire Workforce

Broad & Deep Content
Over 1,700 hands-on challenges for beginner, intermediate, and the most advanced audiences.

Always Up-To-Date
The latest Cyber Threat Intelligence labs enable teams to understand and defend against new threats in as little as 24 hours.

Evidence-Based
Performance data for both individual and teams can help organizations understand, baseline, benchmark, and prove their cyber capabilities.

Always-On
On-demand content enables teams to learn anywhere and at any time, enabling continuous skill development.

Trusted by the world's largest companies, governments, and defense organizations

HSBC Pfizer citi DAIMLER McLaren nationalgrid

Cybersecurity Labs

Immersive Labs provides an extensive coverage of topics for cybersecurity professionals, developers and infrastructure engineers, with over 1,700 labs across multiple categories. Below is a non-comprehensive set of examples of the coverage provided.

FUNDAMENTALS

Staying Safe Online
Networking
Risk & Compliance

DEFENSIVE CYBER

Packet Analysis
Incident Response
Threat Hunting

APPLICATION SECURITY

OWASP Top 10
Secure Testing
Secure Coding

MALWARE AND REVERSE ENGINEERING

Exploit Development
Assembly Language
Source Code Analysis

CYBER THREAT INTELLIGENCE

Spring4Shell
Threat Hunting
Latest Threats

CLOUD SECURITY

Amazon Web Services
Kubernetes Security
DevSecOps

CHALLENGES AND SCENARIOS

Secure Code Competition
Powershell Deobfuscation
Incident Response Scenarios

OFFENSIVE CYBER

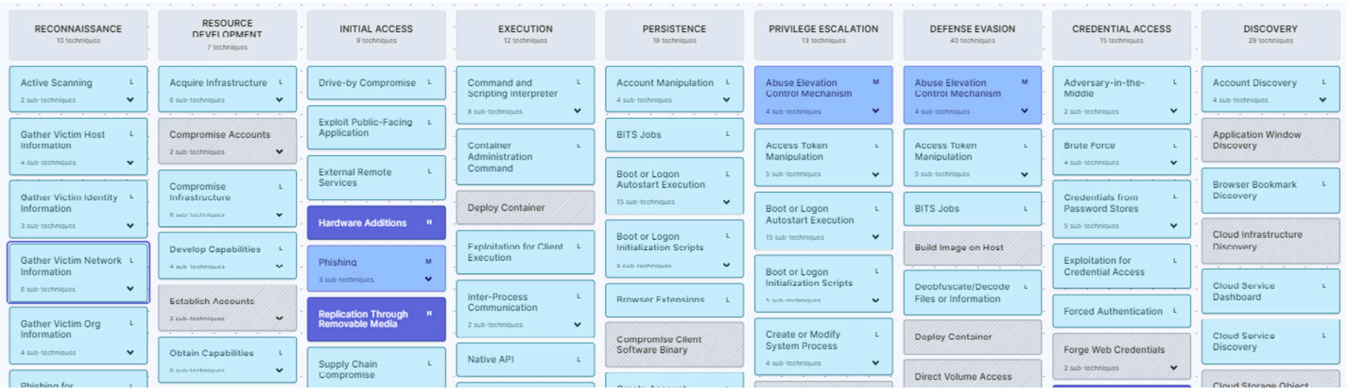
Reconnaissance
Infra/web app pen testing
Privilege Escalation

TOOLS

Burp Suite
Wireshark
Snort

Understand MITRE ATT&CK Coverage and Close Gaps

Identify individual and organizational capabilities according to the MITRE ATT&CK Framework and fill gaps with specifically-tailored labs.



RECONNAISSANCE 10 techniques	RESOURCE DEVELOPMENT 7 techniques	INITIAL ACCESS 9 techniques	EXECUTION 12 techniques	PERSISTENCE 19 techniques	PRIVILEGE ESCALATION 13 techniques	DEFENSE EVASION 40 techniques	CREDENTIAL ACCESS 15 techniques	DISCOVERY 29 techniques
Active Scanning L 2 sub-techniques	Acquire Infrastructure L 6 sub-techniques	Drive-by Compromise L	Command and Scripting Interpreter L 8 sub-techniques	Account Manipulation L 4 sub-techniques	Abuse Elevation Control Mechanism M 4 sub-techniques	Abuse Elevation Control Mechanism M 4 sub-techniques	Adversary-in-the-Middle L 2 sub-techniques	Account Discovery L 4 sub-techniques
Gather Victim Host Information L 4 sub-techniques	Compromise Accounts 2 sub-techniques	Exploit Public-Facing Application L	Container Administration Command L	BITS Jobs L	Access Token Manipulation L 5 sub-techniques	Access Token Manipulation L 5 sub-techniques	Brute Force L 4 sub-techniques	Application Window Discovery
Gather Victim Identity Information L 3 sub-techniques	Compromise Infrastructure L 6 sub-techniques	External Remote Services L	Deploy Container	Boot or Logon Autostart Execution L 15 sub-techniques	Boot or Logon Autostart Execution L 15 sub-techniques	BITS Jobs L	Credentials from Password Stores L 5 sub-techniques	Browser Bookmark Discovery L
Gather Victim Network Information L 6 sub-techniques	Develop Capabilities L 4 sub-techniques	Hardware Additions H	Exploitation for Client Execution L	Boot or Logon Initialization Scripts L 5 sub-techniques	Boot or Logon Initialization Scripts L 5 sub-techniques	Build Image on Host	Exploitation for Credential Access L	Cloud Infrastructure Discovery
Gather Victim Org Information L 4 sub-techniques	Establish Accounts 2 sub-techniques	Phishing M 3 sub-techniques	Inter-Process Communication L 2 sub-techniques	Browser Extensions L	Create or Modify System Process L 4 sub-techniques	Deobfuscate/Decode Files or Information L	Forced Authentication L	Cloud Service Dashboard L
Phishing for L	Obtain Capabilities L 6 sub-techniques	Replication Through Removable Media H	Native API L	Compromise Client Software Binary		Deploy Container	Forge Web Credentials 2 sub-techniques	Cloud Service Discovery L
		Supply Chain Compromise L		Create Account		Direct Volume Access		Cloud Storage Object

Certification & Compliance

Information Security Management ISO 27001 Certified

CYBER ESSENTIALS CERTIFIED PLUS

GDPR

Trusted by the world's largest organizations

Over **400** customers	**>3.5M** total labs completed	**>100,000** unique users	**>1,700** hands-on challenges

Let's get started! Ready to accelerate your Cyber Workforce Resilience journey with Hands-on Labs? Contact your Immersive Labs Account Manager to learn more.

IMMERSIVELABS

immersivelabs.com | sales@immersivelabs.com |