



# Simulation-based Learning, Training & Practice Experiences

## THE CATALOGUE

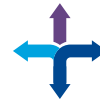
The Best-of-Breed Collection of



Security  
Labs



Simulation  
Playlists



Career  
Paths

POWERED BY  
the next-gen CYBER RANGES Workforce Development Platform

COMPLEMENTED WITH  
a growing library of Videos and Webinars



# The Catalogue

**Skills Development**

**Career Paths**

**MITRE ATT&CK® Simulations**

**Threat Emulation**

**Community**

**Single Scenarios**

Readily accessible via

- 🔗 our Enterprise Sales team
- 🔗 our Market Partners worldwide
- 🔗 directly in-App



CYBER RANGES contains hundreds of security deep-dive hands-on labs to address all organizational competency development needs across a wide range of topics and career paths. This catalogue contains only a selection of such content. For an updated status kindly refer to CYBER RANGES: [app.cyberranges.com](https://app.cyberranges.com)

# CYBER RANGES Skills Development Subscription



## Active Directory Fundamentals

### Description

This playlist will introduce you to the fundamentals of Active Directory and will teach you how to deploy, configure and manage a Windows Domain Controller in an Active Directory environment.

### Outcomes

After completing this playlist, student will be competent in the following areas:

-  Basics of deploying a Window Domain Controller and setting up an active directory.
-  Fundamentals of configuring and managing a Windows Domain Controller in an Active Directory environment



Nº of Scenarios  
**9 (nine)**



Difficulty  
**Easy**






## Active Directory Pen-testing

### Description

This playlist covers the essentials of Active Directory penetration testing and will teach you how to perform AD enumeration and reconnaissance with tools like BloodHound, lateral movement, privilege escalation, persistence, and Kerberoasting in an Active Directory environment.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Performing Active Directory enumeration and reconnaissance.
-  Exploitation of common Active Directory misconfigurations and vulnerabilities.
-  Performing lateral movement in an Active Directory environment.
-  Elevating privileges in an Active Directory environment.
-  Establishing persistence in an Active Directory environment



Nº of Scenarios  
**14 (fourteen)**



Difficulty  
**Intermediate**






## Web Server Administration

### Description

This playlist will teach you the fundamentals of configuring and managing an Apache web server for a production environment and also covers the process of securing and hardening Apache by leveraging tools like Modsecurity WAF (Web Application Firewall).

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Configuring and Managing an Apache Web Server.
-  Securing and Hardening Apache Web Server.
-  Securing an Apache Web Server with Modsecurity WAF



Nº of Scenarios  
**11 (eleven)**



Difficulty  
**Intermediate**



## Binary Exploitation

### Description

This playlist covers the fundamentals of binary exploitation and teaches you how to debug and disassemble binaries for the purpose of identifying and exploiting vulnerabilities like Buffer overflows in binaries..

### Outcomes

After completing this playlist, student will be competent in the following areas:

-  Performing binary analysis for possible attacks.
-  Debugging and Disassembly of binaries.
- Exploiting common vulnerabilities such Buffer Overflows and Stack overflows



Nº of Scenarios  
**16 (sixteen)**



Difficulty  
**Intermediate**




## Command Injection

### Description

This playlist contains tutorial scenarios that will teach you the process of identifying and exploiting command injection vulnerabilities in websites.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Understanding of command injection vulnerabilities.
-  How to identify command injection vulnerabilities in web applications.
-  How to exploit command injection vulnerabilities to perform remote code execution attacks on target systems



Nº of Scenarios  
**5 (five)**



Difficulty  
**Easy**




## Common Vulnerabilities and Exposures (CVE)

### Description

This playlist contains a series of scenarios that will teach you how to identify and exploit the latest CVEs affecting Windows, Linux and third-party solutions.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Identification and systems vulnerable to CVEs
-  Understanding of the latest CVEs and what causes them.
-  How to exploit CVEs manually and automatically with Metasploit



Nº of Scenarios  
**6 (six)**



Difficulty  
**Intermediate**





## CompTIA Security+ Assessment

### Description

This playlist contains challenge-based assessment scenarios that can be used to test and improve your knowledge of the CompTIA Security+ knowledge domains. This playlist is ideal for students looking to prepare for the CompTIA Security+ certification exam.

### Outcomes

After completing this playlist, student will be competent in the following areas:

-  CompTIA Security+ fundamentals.
-  Knowledge on Attacks, threats and vulnerabilities.
-  Understanding of secure architecture and design.
-  Operations and Incident Response



Nº of Scenarios  
**6 (six)**



Difficulty  
**Easy**




## Cross-Site Request Forgery (CSRF)

### Description

This playlist contains tutorial scenarios that will introduce you to CSRF vulnerabilities and will teach you the process of identifying and exploiting Cross Site Request Forgery (CSRF) vulnerabilities in websites.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Understanding of Cross Site Request Forgery vulnerabilities.
-  How to identify Cross Site Request Forgery vulnerabilities in web applications.
-  How to exploit Cross Site Request Forgery vulnerabilities in web applications



Nº of Scenarios  
**4 (four)**



Difficulty  
**Easy**




## Cross-Site Scripting (XSS)

### Description

This playlist contains tutorial scenarios that will teach you the process of identifying and exploiting Cross Site Scripting (XSS) vulnerabilities in websites.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Understanding of Cross Site Scripting (XSS) vulnerabilities.
-  How to identify Cross Site Scripting (XSS) vulnerabilities in web applications.
-  How to exploit Cross Site Scripting (XSS) vulnerabilities in web applications.



Nº of Scenarios  
**12 (twelve)**



Difficulty  
**Easy**






## CTF Competitions

### Description

This playlist contains challenge-based scenarios used in the international CyberStars CTF Competition programme by Silensec. These scenarios will teach you the fundamentals of incident response, digital forensics, log analysis and reverse engineering.

### Outcomes

After completing this playlist, student will be competent in the following areas:

-  Incident Response Fundamentals.
-  How to perform digital forensics.
-  How to analyse logs to find IOCs.
-  Perform network traffic analysis in order to identify malicious activity.
-  Reverse engineer and analyse malware samples



**Nº of Scenarios**  
**26 (twenty six)**



**Difficulty**  
**Intermediate**




## CTF Workshop

### Description

This playlist contains tutorial scenarios that will introduce you to CSRF vulnerabilities and will teach you the process of identifying and exploiting Cross Site Request Forgery (CSRF) vulnerabilities in websites.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Understanding of Cross Site Request Forgery vulnerabilities.
-  How to identify Cross Site Request Forgery vulnerabilities in web applications.
-  How to exploit Cross Site Request Forgery vulnerabilities in web applications.



**Nº of Scenarios**  
**4 (four)**



**Difficulty**  
**Easy**





## Stack Fundamentals

### Description

This playlist contains scenarios that will introduce students to the ELK Stack, teach students how to install and configure Elasticsearch, Logstash, Kibana and Beats and how to create users, authenticate them and assigning them roles.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Understanding of what the ELK stack is and what it can be used for.
-  How to install the different components of ELK Stack.
-  Knowledge of the different features of Kibana and how to use Kibana.
-  How to create standard users, authenticate them and assigning them roles.



**Nº of Scenarios**  
**6 (six)**



**Difficulty**  
**Easy**







## Ethical Ninja Hacking Series

### Description

This playlist is an introductory playlist designed for students looking to get started in penetration testing and covers the fundamentals of information gathering, vulnerability assessment, exploitation, and the basics of using the Metasploit Framework (MSF).

### Outcomes

After completing this playlist, student will be competent in the following areas:

-  Understanding of the different phases of a penetration test
-  How to perform information gathering and reconnaissance.
-  Using Nessus for vulnerability scanning and identification.
-  Using The Metasploit framework for exploitation.



N° of Scenarios  
**6 (six)**



Difficulty  
**Easy**


## Exploiting Linux Vulnerabilities

### Description

This playlist contains tutorial scenarios that cover the exploitation of common and high impact Linux vulnerabilities like SambaCry and Dirty Pipe.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Identification and exploitation of command and high impact Linux vulnerabilities like SambaCry, PwnKit, Dirty Pipe and Log4Shell



N° of Scenarios  
**4 (four)**



Difficulty  
**Intermediate**





## Exploiting Web Apps

### Description

This playlist contains tutorial scenarios that cover the fundamentals of web application security and introduces students to the process of identifying and exploiting vulnerabilities in web applications and content management systems with tools like Nikto and WPScan.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Understanding of the HTTP protocol and how it works.
-  The fundamentals of web application security.
-  How to perform vulnerability scans on web applications with tools like Nikto.
-  Exploiting common misconfigurations and vulnerabilities in web applications



N° of Scenarios  
**16 (sixteen)**



Difficulty  
**Easy**

## Exploiting Windows Vulnerabilities

### Description

This playlist contains tutorial scenarios that cover the exploitation of common and high impact Windows vulnerabilities In Microsoft Exchange, SMB and RDP.

### Outcomes

After completing this playlist, student will be competent in the following areas:

- 🔒 Identification and exploitation of Microsoft Exchange vulnerabilities (CVE-202-0688, CVE-2021-26855).
- 🔒 Exploitation of EternalBlue and BlueKeep vulnerability on Windows.



Nº of Scenarios  
**4 (four)**



Difficulty  
**Easy**

## File Upload Vulnerabilities

### Description

This playlist contains tutorial scenarios that will teach you the process of identifying and exploiting file upload vulnerabilities in websites.

### Outcomes

After completing this playlist, students will be competent in the following areas:

- 🔒 Understanding of file upload vulnerabilities and what causes them.
- 🔒 Identification and Exploitation of basic File Upload vulnerabilities to achieve Remote Code Execution



Nº of Scenarios  
**8 (eight)**



Difficulty  
**Easy**

## Introduction to Android Reverse Engineering

### Description

This playlist contains scenarios that are designed to teach students the fundamentals of reverse engineering modern Android applications (APKs).

### Outcomes

After completing this playlist, students will be competent in the following areas:

- 🔒 Understanding of the structure and organization of an Android application.
- 🔒 Android reverse engineering methodology.
- 🔒 Fundamentals of reverse engineering Android applications.
- 🔒 Handling obfuscation in Android applications.
- 🔒 How to reverse engineer native libraries.
- 🔒 Revere engineering DEX bytecode.



Nº of Scenarios  
**6 (six)**



Difficulty  
**Easy**






## Introduction To Cybersecurity

### Description

This playlist is designed for students looking to get started in Cybersecurity and covers the fundamentals of information security, the CIA triad and the various penetration testing frameworks and methodologies.

### Outcomes

After completing this playlist, student will be competent in the following areas:

-  The fundamentals of information security.
-  Familiarity with Infosec concepts and terminology.
-  Understanding of the various industry standard penetration testing methodologies



Nº of Scenarios  
**4 (four)**



Difficulty  
**Easy**







## Introduction to OSINT

### Description

This playlist contains scenarios that cover the fundamentals of OSINT from Google Dorking to reverse image searching and Social Media reconnaissance.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Familiarity with OSINT frameworks.
-  Conducting OSINT investigations.
-  Understanding of the data collection life cycle.
-  Leverage search engines for intelligence gathering.
-  Leverage Social Media platforms for conducting human reconnaissance.
-  Examine EXIF data and obtain geolocation information.



Nº of Scenarios  
**3 (three)**



Difficulty  
**Easy**





## Introduction To PowerShell

### Description

This is an introductory playlist that is designed to introduce students to the PowerShell scripting language and covers the fundamentals of using PowerShell for scripting and automation on Windows.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Fundamental knowledge of the PowerShell scripting language.
-  Knowledge of scripting and automation using PowerShell.



Nº of Scenarios  
**5 (five)**



Difficulty  
**Intermediate**




## Linux Essentials For Security Consultants

### Description

This playlist contains various scenarios designed to train security consultants, SOC analysts and penetration testers on how to effectively use and administer Linux.

### Outcomes

After completing this playlist, student will be competent in the following areas:

-  Fundamental knowledge of Linux system administration.
-  Knowledge of Linux text editors and usage of regular expressions.a
-  Fundamentals of shell scripting for automation.



Nº of Scenarios  
**28 (twenty eight)**



Difficulty  
**Easy**






## Linux Fundamentals

### Description

This is an introductory playlist designed to teach students the fundamentals of the Linux operating system.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Navigating the Linux filesystem.
-  Creating, Modifying, and deleting files and folders.
-  Managing File and Folder Permissions.
-  Installing and uninstalling packages.
-  Managing installed services.



Nº of Scenarios  
**12 (twelve)**



Difficulty  
**Easy**







## Linux System Administration

### Description

This playlist is designed for students looking to get started in Linux system administration and covers the fundamentals of Linux system administration from user management to shell scripting.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  User and password management.
-  Permission management.
-  Firewall and network management.
-  Package management.
-  Disk management.
-  Fundamentals of shell scripting for automation.



Nº of Scenarios  
**27 (twenty seven)**



Difficulty  
**Easy**




## Linux Privilege Escalation

### Description

This playlist contains tutorial scenarios that will teach students the process of identifying and exploiting privilege escalation vulnerabilities on Linux.

### Outcomes

After completing this playlist, student will be competent in the following areas:

-  Fundamental knowledge of Linux system administration.
-  Knowledge of Linux text editors and usage of regular expressions.
-  Fundamentals of shell scripting for automation.



Nº of Scenarios  
**13 (thirteen)**



Difficulty  
**Intermediate**




## Linux Text Editors

### Description

This playlist contains tutorial scenarios designed to introduce students to the various text editors available on Linux like Nano and VIM and covers various use cases to make students competent at viewing and modifying text on Linux.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Knowledge of how to use the Nano editor.
-  Familiarity with VIM and VIM key bindings.
-  Knowledge of how to use SED and regex



Nº of Scenarios  
**5 (five)**



Difficulty  
**Easy**



## Local File Inclusion (LFI)

### Description

This playlist contains tutorial scenarios that introduce students to Local File Inclusion vulnerabilities, how they can be identified and how they can be exploited.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Understanding of what Local File Inclusion vulnerabilities are and what causes them.
-  Identification and Exploitation of basic Local File Inclusion vulnerabilities.



Nº of Scenarios  
**4 (four)**



Difficulty  
**Easy**



## Malware Traffic Analysis

### Description

This playlist contains scenarios designed to teach students the process of identifying and analyzing malicious network traffic with Wireshark.

### Outcomes

After completing this playlist, student will be competent in the following areas:

-  Identifying malicious network traffic with Wireshark.
-  Analysing malicious network traffic with Wireshark in order to identify IOCs.



Nº of Scenarios  
**22 (twenty two)**



Difficulty  
**Intermediate**






## Memory Forensic Fundamentals

### Description

This playlist contains scenarios that introduce students to the fundamentals of memory forensics and covers the process of memory acquisition and analysis with tools like Volatility and teaches students how to perform malware memory analysis on a system infected with WannaCry ransomware.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Fundamentals of Memory Forensics.
-  Installing and configuring volatility.
-  Memory acquisition with volatility.
-  Volatility profile identification and creation.
-  Basics of malware memory forensics.



Nº of Scenarios  
**4 (four)**



Difficulty  
**Advanced**







## Network Lateral Movement

### Description

This playlist contains tutorial scenarios that cover the process of performing pivoting and lateral movement with SSH.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Understanding of what Local File Inclusion vulnerabilities are and what causes them.
-  Identification and Exploitation of basic Local File Inclusion vulnerabilities.
-  Perform local port forwarding.
-  Perform reverse port forwarding.
-  Perform dynamic port forwarding.
-  Lateral movement with SSH.



Nº of Scenarios  
**3 (three)**



Difficulty  
**Intermediate**






## Networking Fundamentals

### Description

This playlist is designed to introduce students to the fundamentals of networking and covers the OSI model, how TCP and UDP work, common services and ports and how to analyze PCAP files with Wireshark.

### Outcomes

After completing this playlist, student will be competent in the following areas:

-  Understanding of the OSI model and the layers that make up the model.
-  Familiarity with the network and transport layers of the OSI model.
-  Understanding of the different TCP header flags and why they are used.
-  Understanding of the TCP 3-Way handshake works.
-  Using Wireshark for packet capture and analysis.



Nº of Scenarios  
**11 (eleven)**



Difficulty  
**Easy**






## Nmap For Penetration Testing

### Description

This playlist contains scenarios that cover the fundamentals of Nmap and how it can be used in the context of a penetration test from performing host discovery to service detection and enumeration.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Understanding of how to perform host discovery with Nmap.
-  Performing TCP & UDP port scanning with Nmap.
-  Performing service enumeration with the Nmap Scripting Engine (NSE).
-  Detecting and evading firewalls with Nmap.
-  Speeding up or slowing down Nmap scans in order to evade detection.



Nº of Scenarios  
**6 (six)**



Difficulty  
**Easy**




## Password Attacks - Credential BruteForcing

### Description

This playlist contains tutorial scenarios that introduce students to credential brute force attacks and covers the process of performing brute force attacks with tools like Hydra against different network protocols like SSH.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Understanding of what a brute force attack is.
-  Knowledge of popular credential brute force tools like Hyrda.
-  Performing brute force attacks against network protocols like SSH.



Nº of Scenarios  
**9 (nine)**



Difficulty  
**Easy**


## Password Attacks - Hash Cracking

### Description

This playlist contains tutorial scenarios that introduce students to hash cracking and covers the process of cracking Windows and Linux password hashes with tools like John the Ripper and Hashcat.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Knowledge of popular hash cracking tools like John the Ripper and Hashcat.  
Cracking hashes in common formats to discover clear text credentials for Linux, Windows and several other applications



Nº of Scenarios  
**7 (seven)**



Difficulty  
**Easy**



## Reverse Engineering

### Description

This is a comprehensive playlist that covers advanced static and dynamic reverse engineering techniques with tools like IDA Pro & OllyDBG.

### Outcomes

After completing this playlist, student will be competent in the following areas:

-  Reverse engineering and malware analysis basics
-  Dynamic and static malware analysis



Nº of Scenarios  
**18 (eighteen)**



Difficulty  
**Advanced**




## System Administration on Windows

### Description

This playlist contains scenarios designed to introduce students to the fundamentals of system administration on Windows and covers the process of deploying, administering and securing Windows.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Understanding of the Windows operating system.
-  How to deploy and administer Windows systems.
-  Knowledge of how to secure and harden Windows.



Nº of Scenarios  
**11 (eleven)**



Difficulty  
**Easy**

## Vulnerable Web Applications

### Description

This playlist contains various intentionally vulnerable web applications with vulnerabilities that can be used as a playground for developing skills in web application exploitation.

### Outcomes

After completing this playlist, students will be competent in the following areas:

- 🔒 Identify and exploit web application vulnerabilities in popular vulnerable web apps.



Nº of Scenarios  
**7 (seven)**



Difficulty  
**Easy**

## Web Security with Burp Suite

### Description

This playlist contains scenarios that cover the fundamentals of how to use Burp Suite to analyze web requests, authentication vulnerabilities, session management vulnerabilities and authorization checks in web applications.

### Outcomes

After completing this playlist, student will be competent in the following areas:

- 🔒 Fundamentals of using Burp Suite in web security.
- 🔒 Discover, analyse and exploit web security vulnerabilities in web applications using Burp Suite.



Nº of Scenarios  
**5 (five)**



Difficulty  
**Easy**



## Windows Pen-testing

### Description

This playlist contains scenarios that encompass the process and methodology used when performing a penetration test on a Windows target. It covers the process of exploiting native Windows services and protocols like SMB, RDP and WinRM.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Performing enumeration on Windows services like SMB, RDP and WinRM.
-  Identifying and exploiting vulnerabilities in Windows services like SMB, RDP and WinRM.



Nº of Scenarios  
**18 (eighteen)**



Difficulty  
**Intermediate**





## Windows Privilege Escalation

### Description

This playlist contains tutorial scenarios that will teach students the process of identifying and exploiting privilege escalation vulnerabilities on Windows by leveraging techniques like Access Token Impersonation and insecure credential storage.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Identifying privilege escalation vectors on Windows.
-  Privilege escalation via Access Token Impersonation.
-  Exploiting kernel vulnerabilities.
-  Searching for and identifying locally stored credentials.



Nº of Scenarios  
**6 (six)**



Difficulty  
**Intermediate**











## CYBER RANGES Career Paths

### Junior Penetration Tester

#### Description

This learning path covers the fundamentals of cybersecurity, networking and penetration testing and provides students with the knowledge and skills required to become a Junior Penetration Tester.

#### Outcomes

-  Understand the fundamentals of cybersecurity.
-  Become familiar with the various industry standard penetration testing methodologies.
-  Understand the OSI model and the layers that make up the model.
-  Familiarity of the Windows operating system, how it works and how it can be exploited.
-  Perform Host discovery and port scanning with Nmap
-  Perform Credential Brute-Force Attacks against protocols like SSH.
-  Identify and exploit vulnerabilities in web applications.
-  Exploit Windows and Linux systems by leveraging various MITRE ATT&CK<sup>®</sup> exploitation techniques.



Nº of Playlists  
**11 (eleven)**



Difficulty  
**Easy**










### Senior Penetration Tester

#### Description

This learning path builds on the Junior Penetration Tester learning path and covers advanced exploitation, post-exploitation and privilege escalation techniques on both Windows and Linux.

This learning path will provide students with the knowledge and skills required to become a Senior Penetration Tester.

#### Outcomes

-  Perform Port scanning and enumeration with Nmap.
-  Crack Windows and Linux password hashes.
-  Identify and exploit Linux vulnerabilities
-  Identify and exploit vulnerabilities in web applications.
-  Develop PowerShell scripts for automation.
-  Identify and exploit privilege escalation vulnerabilities in Linux.
-  Identify and exploit privilege escalation vulnerabilities in Windows.
-  Understand how Active Directory environments are setup and configured.
-  Exploit Windows and Linux systems by leveraging various MITRE ATT&CK<sup>®</sup> exploitation techniques.



Nº of Playlists  
**11 (eleven)**












Difficulty  
**Intermediate**

## Web App Pen-Testing Professional

### Description

This learning path is designed to provide penetration testers with the knowledge and skills required to assess and exploit vulnerabilities in web applications.

### Outcomes

-  Assess the security of web applications.
-  Identify vulnerabilities in web applications.
-  Analyze and test the security of web applications with Burp Suite.
-  Identify and exploit vulnerabilities in content management systems like WordPress.
-  Identify and exploit SQL injection vulnerabilities.
-  Identify and exploit Cross Site Scripting (XSS) vulnerabilities.
-  Identify and exploit Cross Site Request Forgery vulnerabilities.
-  Identify and exploit Command Injection vulnerabilities.
-  Identify and exploit File Upload Vulnerabilities.



Nº of Playlists  
**8 (eight)**



Difficulty  
**Intermediate**








## Red Team Operator

### Description

This learning path is designed to make students influential Red Team experts, who can counter cyber threats and perform effective penetration testing to detect those threats.

This learning path combines all the tools and techniques needed to become an effective Red Team Cyber Security expert.

### Outcomes

-  Advanced MITRE® techniques.
-  Atomic Red Tests with MITRE®.
-  Windows penetration testing.
-  Exploiting Windows Vulnerabilities.
-  Exploiting Linux Vulnerabilities.
-  Linux Privilege Escalation.
-  Active Directory penetration testing.



Nº of Playlists  
**9 (nine)**



Difficulty  
**Intermediate**







## SOC Tier 1

### Description

This playlist is designed for students looking to become SOC Tier 1 analysts. It covers the fundamentals of networking, traffic analysis, incident response, threat intelligence and scripting.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  SOC Tier 1 Operations.
-  Networking concepts.
-  Windows and Linux Operating Systems.
-  Windows and Linux Logging.
-  Digital Forensics and Incident Response concepts.
-  Usage of MITRE ATT&CK Framework.



Nº of Scenarios  
**37 (thirty seven)**



Difficulty  
**Easy**









## SOC Tier 2

### Description

This playlist is designed for SOC analysts looking to improve their skills or to become SOC Tier 2 analysts. It covers knowledge domains like log management, Windows Registry, HIDS/NIDS solutions, Elastic Stack and malware analysis.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Log Management.
-  Interacting and querying the Windows Registry.
-  Implementing and configuring Host Intrusion Detection Systems.
-  Implementing and configuring Network Intrusion Detection Systems.
-  Host Monitoring System with Nagios.
-  Familiarity with OWASP Top 10.
-  Analysing malware.
-  Using Elastic Stack.



Nº of Scenarios  
**22 (twenty two)**



Difficulty  
**Intermediate**






## SOC Tier 3

### Description

This playlist is designed for advanced SOC analysts looking to improve their skills or to become SOC Tier 3 analysts. It covers knowledge domains like threat modelling, threat hunting, DFIR, memory forensics, malware identification with YARA and adversary emulation with Atomic Red Team tests.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Performing threat Modelling and Hunting.
-  Digital Forensic and Incident Response.
-  Using YARA for malware identification.
-  Adversary emulation with Atomic Red Team tests.
-  Memory Forensics.



Nº of Scenarios  
**18 (eighteen)**



Difficulty  
**Advanced**

# CYBER RANGES

## MITRE | ATT&CK®

SUBSCRIPTION 

**MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations, as developed and maintained by MITRE\*.**

The ATT&CK® knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge), MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK® is open and available to any person or organization for use at no charge. Moreover, the framework describes how attackers penetrate networks and then move laterally, escalate privileges, create a persistent state, or generally evade your defenses.

The ATT&CK® framework looks at the issue from an attacker's point of view and helps the cybersecurity professionals identify what is the goal of an attacker and what are the techniques and procedures the attacker will use to attain their goal.

ATT&CK® helps you understand how attackers might operate so that you can plan and build response playbooks to mitigate attacker incidents. Armed with this knowledge and “attack playbooks” you are now better prepared to understand how your adversaries prepare for, launch, and execute their attacks to achieve specific desired objectives.

Successful and comprehensive threat detection requires the understanding of common adversary TTPs, i.e. Tactics, Techniques and Procedures, especially those that pose a threat to your organization, and the appreciation of the ways to detect and mitigate these attacks.





## MITRE | ATT&CK® TRAINING

### Description

This playlist will introduce you to the fundamentals of using the MITRE ATT&CK® framework for threat intelligence and will teach you how to use the MITRE ATT&CK® framework in conjunction with Atomic Red Team tests to automate an adversary emulation campaign. This playlist also contains challenge-based hacking scenarios that are tied to specific MITRE ATT&CK® techniques and sub-techniques and are designed to improve your knowledge of the techniques used by adversaries and threat actors.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  The ability to use the MITRE ATT&CK® Framework and Navigator.
-  The ability to perform threat intelligence with the MITRE ATT&CK® Framework.
-  Knowledge on how to setup and automate an adversary emulation campaign with Atomic Red Team tests.
-  Comprehensive knowledge of the techniques and sub-techniques used by adversaries/threat actors during their campaigns.



Nº of Playlists  
**5 (five)**



Difficulty  
**Intermediate**

For more details please refer to the dedicated brochure from CYBER RANGES or contact: [mitre@cyberranges.com](mailto:mitre@cyberranges.com)

\*The MITRE Corporation is an American not-for-profit organization that manages federally funded research and development centers supporting various U.S. government agencies in the aviation, defense, healthcare, homeland security, and cybersecurity fields, among others. As a not-for-profit organization, MITRE works in the public interest across federal, state and local governments, as well as industry and academia. MITRE brings innovative ideas into existence in areas as varied as artificial intelligence, intuitive data science, quantum information science, health informatics, space security, policy and economic expertise, trustworthy autonomy, cyber threat sharing, and cyber resilience.

# CYBER RANGES Threat Emulation

SUBSCRIPTION 

## CYBER RANGES Incident Response Scenarios and MITRE ATT&CK®

CYBER RANGES include scenarios that are mapped to the techniques and methodologies used by attackers as set out by MITRE ATT&CK®.

Usage of the MITRE ATT&CK® framework aids in improving your team's ability to identified techniques and technologies used by attackers.

This will allow you to break down your training so that your team is exposed, in real time, to the different techniques and methodologies outlined by ATT&CK®, ensuring that your team will be prepared for the inevitable attack when it comes.

In order for you to fully grasp and take advantage of the CYBER RANGES content, we have broken down a scenario for you as shown below and showed the various tactics and techniques that have been simulated in this particular scenario





### Threat Emulation

#### Description

This playlist will teach you how to detect and hunt for common APTs (Advanced Persistent Threats), their IOCs (Indicators of Compromise) and exploitation techniques to improve your knowledge of threat actors and the techniques they employ during their campaigns. .

#### Outcomes

After completing this playlist, students will be competent in the following areas:

-  Detect APTs through incident Response.
-  Perform digital forensics on compromised hosts.
-  Analyse network traffic logs to identify malicious network activity.
-  Analyse and reverse engineer malware used by common APTs



Nº of Scenarios  
**24 (twenty four)**



Difficulty  
**Intermediate**

## Incident Response: Web and System Attack

### Scenario Description

You are part of the Official National Organization (ONO) Blue Team, tasked with defending and responding to outsider attacks.

A few days ago, your team received a threat intel report stating that an unknown hacker collective is demanding a ransom payment from your organization, otherwise they have threatened to carry out an imminent attack against your publicly-facing website and other IT assets.




You and your team are working under the assumption that the organization has been compromised. You have been tasked to identify, defend and respond against any such attacks.

### Attack Summary

It is suspected that the attacker followed the 7 steps for penetration testing and used information gained for the initial foothold access. Access is suspected to have been through SSH or a vulnerable web application. Additionally, it is suspected that the attacker TTPs included password spraying, wordlist based brute force attack to mention a few.

All the endpoints attacked are connected to a Log Management System and a Security Information and Event Management (SIEM) system. This system will have logs needed to investigate this incident guided by the assessment questions.

You and your team have been tasked with defending your website against an imminent attack by an unknown hacker collective that is blackmailing your organization for a ransom payment, to successfully define and finish the scenario:

-  Use ELK to detect, analyze and respond to any attacks.
-  Analyze the VulnWebsite for any potential vulnerabilities, and fix those appropriately.
-  If you get attacked, you can recover by replacing the website's home page with a backup one. You first need to find this file though.

### MITRE Techniques in Scenario

#### Initial Access

---

Exploit Public-Facing Application (T1190)

#### Defense Evasion

---

Valid Accounts (T1078)

#### Persistence

---

Create Account (T1136)

Account Manipulation (T1098)

#### Credential Access

---

Brute Force (T1110)

#### Privilege Escalation

---

Valid Accounts (T1078)

## The Hunt for APT40

### Scenario Description

APT40 is a cyber espionage threat group linked to the Chinese government, known for targeting critical technologies and traditional intelligence firms in North America, Europe, and East Asia.

In this scenario, an attack group leveraged spear-phishing emails that contained links to similar domains, created to mimic or resemble the domains of legitimate companies. In some cases, the threat actors leveraged hijacked credentials, to gain access to legitimate mail servers and then launch spear-phishing campaigns from within the victim entity or at other targeted entities. Once the threat actors gained a foothold in the victim environment, they proceeded to perform malicious activities on the victim's environment.

You are required to use the various SIEMs provided in this scenario to investigate the attacker's activities and any Indicators of Compromise.

### MITRE Techniques in Scenario

#### Initial Access

Phishing (T1566)  
Valid Account (T1078)  
Exploit Public-Facing Application (T1190)

#### Execution

Command and Scripting Interpreter (T1059)  
System Services (T1569)

#### Persistence

Server Software Component: Web Shell (T1505)  
Valid Account (T1078)  
Create Account (T1136)

#### Privilege Escalation

Valid Account (T1078)

#### Defense Evasion

Valid Account (T1078)

#### Exfiltration

Exfiltration Over C2 Channel

## XCallCenter Under Attack

### Scenario Description

Data theft is becoming an increasingly lucrative enterprise throughout the country. We don't know whether a single Advanced Persistent Threat (APT) group is behind this or numerous opportunists trying to bank on this unknown drive for purchasing personal information acquired through security breaches. One thing is for certain; organizations that weren't such attractive targets now shine like diamonds in a bag of coal.

### Attack Summary

XCallCenter, has been caught off guard by constant attacks on its infrastructure and its stakeholders are increasingly worried that they have been targeted by unknown assailants. The IT department has taken appropriate steps to ensure visibility throughout the network, but lack the knowledge to understand and respond to security incidents. Your team of experts has been called in to manage the monitoring and incident response of the organization until a suitable replacement can be found.

You are tasked with identifying and tracing the attacker actions on the network.

Ensure that you have thoroughly located the attack vectors and identified traffic being exfiltrated during these attacks.

### MITRE Techniques in Scenario

#### Reconnaissance

Active Scanning (T1595)

#### Initial Access

Exploit Public Facing Application (T1190)

Valid Accounts (T1078)

Exploit Public- Facing Application (T1190)

#### Execution

Command and Scripting Interpreter (T1059)

Exploitation For client Execution (T1203)

#### Persistence

Create Account (T1136)

Server Software Component (T1491)

Create Account (T1136)

#### Privilege Escalation

Abuse Elevation Control Mechanism (T1548)

#### Lateral Movement

SSH (T1021)

#### Impact

Internal Defacement (T1491)



# CYBER RANGES Community Playlists

## Non-Commercial










### Description

This playlist contains scenarios that introduce students to the fundamentals of adversary emulation with the MITRE ATT&CK® Framework and covers the process developing an adversary emulation plan, and how to plan, implement and automate adversary TTPs (Tactics, Techniques and Procedures).

### Outcomes

After completing this playlist, student will be competent in the following areas:

-  Identifying and analysing adversarial tactics and techniques.
-  Developing an adversary emulation plan.
-  Executing an adversary emulation plan.
-  Planning TTP implementations for adversary emulation.
-  Implementing adversary TTPs.
-  Automating adversary TTPs.
-  Identifying detections and mitigations.



Nº of Scenarios  
**7 (seven)**



Difficulty  
**Intermediate**

## Boot2Root Style Scenarios





### Description

This playlist contains challenge-based CTF scenarios that can be used to practice and improve your penetration testing skills and methodology.

This playlist is ideal for penetration testers and red teamers looking to practice and improve their knowledge of enumeration, exploitation and post-exploitation.

### Outcomes

After completing this playlist, students will be competent in the following areas:

-  The ability to identify open ports and services on target systems.
-  How to enumerate information from open ports.
-  Identify and exploit vulnerabilities on target systems.
-  How to perform privilege escalation on Linux.



Nº of Scenarios  
**72 (seventy two)**



Difficulty  
**Intermediate**



## About Us

CYBER RANGES is the ISO27001 certified next-generation military-grade full-content-lifecycle simulation platform for the validation of threat-informed defense capability and cyber resilience. Built on powerful cloud technology, CYBER RANGES is available as subscription-based, as managed service, as On-Premise and Portable rugged deployment options.

CYBER RANGES applies high automation, high orchestration and high scalability to the delivery of even complex large-audience deep-dive management tabletop and technical exercises based on high-fidelity IT/OT infrastructure replicas. CYBER RANGES fully supports MITRE (PRE-)ATT&CK across its entire cyber range architecture. Through its proprietary Injector Engine CYBER RANGES automatically emulates user traffic and the latest intel-based attacks, APTs and specific tactics and exploits from the MITRE ATT&CK Matrix™.

CYBER RANGES powers the CyberStars™ initiative ([www.cyberstars.pro](http://www.cyberstars.pro)) run in private-public collaboration with national focal points and regulatory authorities from around the world. CyberStars provides a turnkey project package for participating countries to organize national cybersecurity competitions and to participate in international ones, while at the same time meeting the objectives of national cybersecurity strategies in terms of talent growth.

CYBER RANGES actively participates as a key member organization in the European Cyber Security Organization (ECSO) WG5 on Cyber Ranges, Education and Training and Technical Exercises, advancing best practice in the domain of cybersecurity capability and resilience. CYBER RANGES also spearheads the “Top 10 Abilities” initiative, which helps CISOs to focus on pertinent, observable, measurable abilities for the development and assessment of job-specific capabilities in the workplace.

CYBER RANGES is also an active Partner of the Global Cyber Alliance – GCA (New York, Brussels, London) in its worldwide mission to sustain a trustworthy Internet by reducing cyber risk. CYBER RANGES is a founding member of the Canada-based Cyber Security Global Alliance (CSGA). CYBER RANGES is an ecosystem partner of the Quantico Cyber Hub in Virginia.



✉ [subscriptions@cyberranges.com](mailto:subscriptions@cyberranges.com)