- Dashboard
- Search
- Ongoing Labs 0
- Latest Additions
- Community Labs

EARN CREDENTIALS

- Verifiable Badges

WINDOWS SECURITY

- Reconnaissance
- Basic Exploitation
- Post Exploitation
- Service Exploitation
- Privilege Escalation
- Maintaining Access

CLOUD SECURITY

- AWS Cloud Security
- Bootcamp

LINUX SECURITY

- Linux Basics
  - Getting Started
  - Basics
- Reconnaissance
- Exploitation
- Post Exploitation
- Privilege Escalation
- Pivoting
- Maintaining Access
- MITRE ATTACK
- Exploit Research
- Bootcamp

WEBAPP PENTESTING BASICS

- Web Application Basics
- Tools of the Trade
- OWASP Top 10
- Webapp CVEs
- Bootcamp

ADVANCED PRIV-ESC

Dashboard

LINUX BASICS

Linux Basics

The objective of the Linux Basics section is to familiarize students with the Linux concepts and commands/tools required to interact with various services and applications.

What will you learn?

- Understanding the Linux filesystem and users
- Understanding the system and user crontabs
- Learning the important Linux commands and tools
- Fingerprinting web applications and network services such as FTP and SSH
- Creating bi-directional connections with socat

References:

- Linux (https://en.wikipedia.org/wiki/Linux)

Labs:

- Scheduling: Cron Basics
  - Objective: Analyse the scheduled cron jobs on the provided machine and answer questions.
- Scheduling: Cron Practice
  - Objective: Create a cron job to perform specific tasks.
- Switching users
  - Objective: Learn about how to switch between various users on the Linux system.
- Text File Analysis
  - Objective: Use various Linux commands and tools to analyze the content of a text file.
- Interaction: FTP Service
  - Objective: Use expect to interact with the FTP service.
- Interaction: Socat Listener
  - Objective: Use expect to interact with the socat listener.
- Interaction: SSH Service
  - Objective: Use expect to interact with the ssh service.
- Tool: Socat
  - Objective: Use socat to perform various operations.
- Tool: Netcat
  - Objective: Use netcat to perform various operations.
- Fingerprinting Webapp (CLI)
  - Objective: Fingerprint the web application using curl, Nmap, wget, lynx, browsh.
- Resource Monitoring
  - Objective: Use various Linux commands and tools such as top, htop and iotop to monitor system resources.
- Lesser-Known Hacks
  - Objective: Try out various lesser-known hacks that might be useful during pentesting.

- Dashboard
- Search
- Ongoing Labs 0
- Latest Additions
- Community Labs

EARN CREDENTIALS

- Verifiable Badges

WINDOWS SECURITY

- Reconnaissance
- Basic Exploitation
- Post Exploitation
- Service Exploitation
- Privilege Escalation
- Maintaining Access

CLOUD SECURITY

- AWS Cloud Security
- Bootcamp

LINUX SECURITY

- Linux Basics
  - Getting Started
  - Basics
- Reconnaissance
- Exploitation
- Post Exploitation
- Privilege Escalation
- Pivoting
- Maintaining Access
- MITRE ATTACK
- Exploit Research
- Bootcamp

WEBAPP PENTESTING BASICS

- Web Application Basics
- Tools of the Trade
- OWASP Top 10
- Webapp CVEs
- Bootcamp

ADVANCED PRIV-ESC

Scheduling: Cron Practice — Start

Switching users — Start

Text File Analysis — Start

Interaction: FTP Service — Start

Interaction: Socat Listener — Start

Interaction: SSH Service — Start

Tool: Socat — Start

Tool: Netcat — Start

Fingerprinting Webapp (CLI) — Start

Resource Monitoring — Start

Lesser Known Hacks — Start