SECURITY ESSENTIALS

The aim of the course is to introduce students to penetration testing fundamentals. It includes command line basics, network security basics, common web application attacks, privilege escalation techniques, and introduction to local exploitation.

There are five modules:

1. Fundamentals
2. Pentest introduction
3. Web applications security
4. Privilege escalation
5. Local exploitation

THE FUNDAMENTAL MODULE covers all elementary knowledge and techniques necessary to know to understand the next modules. Participants will learn how to efficiently use the terminal and the most useful commands.

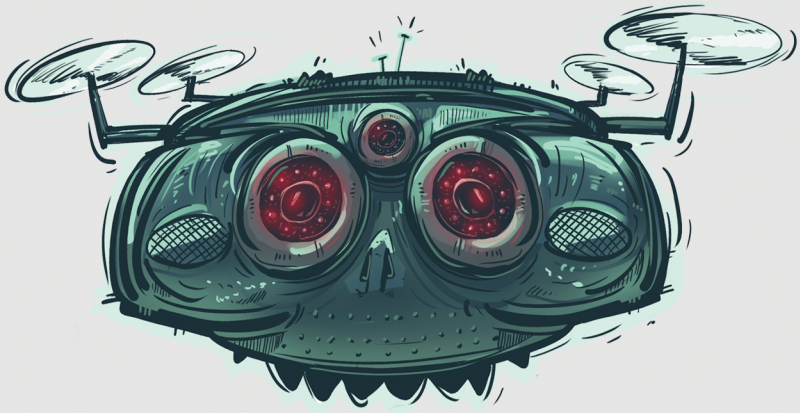
- Command line basics
- Bash basics
- Client-Server model
- Data transfer techniques
- Reverse shells
- Bind shells
- Interactive shells

THE PENTEST INTRODUCTION module allows participants to perform their first infrastructure and web application pentest. They will learn common methodologies, tactics, and common mistakes. The module will be concluded by writing a technical report.

- Network scanning
- HTTP basics
- Remote command execution
- Automatic privilege escalation
- Network pivoting
- Backdoor detection
- Reporting

THE WEB APPLICATIONS security module will provide an overview of the most common vulnerabilities that can be found in web applications. Participants will enumerate and exploit ten vulnerable web applications.

- Enumeration
- Password security
- Command injection
- Client-side security
- File upload security
- SQL Injection
- Template Injection
- XML external entity injection
- Cross-site scripting
- Cross-Site Request Forgery
- Local file inclusion
- Remote file inclusion



THE PRIVILEGE ESCALATION module provides additional steps to perform after taking control over web applications. Students will continue enumeration on compromised servers to find more vulnerabilities and gain administrative privileges

- File permissions
- Sudo permissions
- Cron jobs misconfiguration
- Privileged containers
- Local services
- OS exploits

THE LOCAL EXPLOITATION module is an extension of privilege escalation techniques. It will cover the most common programming mistakes that can be made in applications written in C. It avoids low-level knowledge and assembly/machine code.

- SUID and capabilities
- Hardcoded data
- Buffer overflows
- Environment variables
- Side channel attacks
- Handling signals
- Symlinks
- Inherited file descriptors