NETWORK SECURITY PENETRATION TEST COURSE OVERVIEW

The aim of the course is to prepare students to perform a full local and wireless network penetration test. After enrolling in our course, participants will be given written materials that will provide a thorough description and explanation of every topic included in the course. At the end of each topic, students will be challenged to complete hands-on practical exercises that will encourage them to use the skills learned in the theoretical section. After completion of every topic in the course, a final lab will be open for completion for a student. To complete it, a student will need to combine some of the techniques learned through the course.

The course is divided into four main parts:

1. Network Security
2. Infrastructure Security
3. Privilege Escalation Techniques
4. Final Challenge

In the NETWORK SECURITY part, a student will learn the basics of computer networks as well as how to exploit common misconfigurations and launch Layer 2 and Layer 3 network attacks. Later in this section, the course includes the following exercise scenarios together with a theory part that will aid students in lab completion:

- **Networking Fundamentals** – introduction to computer networks with a good theoretical basic,
- **Wireshark and traffic analysis** – a chapter that will learn students how to analyze network traffic using Swiss army knife of traffic sniffers – Wireshark,
- **ARP Spoofing** – topic in which students will learn how to exploit Layer 2 ARP protocol in order to exploit other hosts in the network,
- **VLAN hopping** – by taking a misconfigured VLAN configuration on the workbench, a student will need to exploit the DTP protocol and gain access to other VLANs,
- **ICMP Redirects** – using scripting tools students will send malicious ICMP to redirect packets resulting in a MiTM attack against other hosts in the network,
- **Replay attacks** – by sniffing user's traffic, students will reuse other user hash in order to launch a replay attack against SMB network share,
- **IPv6 attacks** – in this scenario, we will demonstrate the security impact of a default Windows IPv6 configuration,
- **NAC bypass attacks** – this exercise will aim to teach a student how to bypass MAC address-based network access controls,
- **DHCP Security** – by exploiting a vulnerable DHCP server, students will launch a DHCP Spoofing attack to compromise other hosts in the network,
- **WiFi Security** – this topic will mainly focus on the practical aspect of wireless network penetration testing. In a virtualized environment students will try to exploit the following topics:

  Wireless network reconnaisance,
  Exploiting open Wi-Fi networks,
  WEP Authentication,
  PSK Authentication,
  Enterprise Authentication

The INFRASTRUCTURE SECURITY topic will mainly focus on the reconnaissance and exploitation of other hosts in the local network. Students will learn how to identify active hosts, look for exploitable services and gain remote code execution on vulnerable machines. Below we present the topics that are included in this course part:

Scanning networks for live hosts – introduction to Nmap and other tools that allow discovering active hosts in the network,

Scanning hosts for running services – using various scan types (SYN, TCP, UDP, etc.) to enumerate running services on the hosts,

Scanning services for known vulnerabilities – using NSE (Nmap Scripting Engine) to identify vulnerable services,

Scanning services for misconfigurations - using manual and automated tools to identify common misconfigurations,

Exploitation – using public exploit databases to find information allowing to compromise vulnerable hosts, using various payload types (reverse and bind shells), upgrading to interactive terminals and much more.

In PRIVILEGE ESCALATION TECHNIQUES students will learn what to do after the initial exploitation of a remote host. We will focus on the most common privilege escalation techniques found on Windows and Linux operating systems. After a short theoretical introduction, students will be encouraged to try to get their hands on the following lab topics:

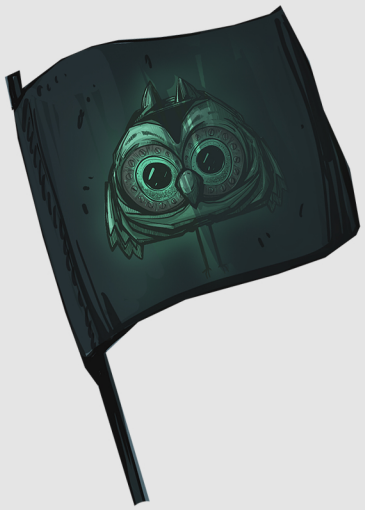
Escalation using SUID files – students will learn how to look for files with SUID bit enabled, what dangers this configuration may result in, and how to escalate privileges using the most common SUID misconfigurations,

Escalation using vulnerable cron scripts – a poorly configured cronjob may often result in privilege escalation. This scenario will be exploited in this topic.

Linux system pillaging – students will be taught how to find and identify secrets and passwords in plain text files to utilize them in the privilege escalation process,

DLL Injection – by exploiting a DLL Injection vulnerability students will try to execute code and escalate privileges on a Windows machine,

Escalation using task scheduler – with a misconfigured task scheduler job, the student's aim is to escalate on a Windows machine.



The FINAL CHALLENGE part will consist of multiple machines that students will need to compromise to finish the lab. Many of the techniques shown in previous chapters must be used to complete this challenge encouraging students to deepen their knowledge and push the boundaries of their network security skills.