Microtel
Training institute

TESTS D'INSTRUSION

CODE DE LA FORMATION:
MTI-SC-TI

DURÉE:
5 JOURS

Cette formation prépare à mener avec succès des tests d'intrusion sur des infrastructures et applications informatiques. La formation aura pour but de vous apprendre la méthodologie et les techniques utilisées par les auditeurs (Pentesters) professionnels pour identifier et exploiter les vulnérabilités à grande échelle et montrer le risque business réel pour l'organisation ou l'entreprise auditée. Le contenu du cours est composé d'une partie théorique et d'une grande partie pratique sous forme d'exercices pratiques (Labs)..

PRÉREQUIS:

Tous les apprenants doivent avoir :

- Une solide compréhension des réseaux TCP/IP
- Une expérience raisonnable de l'administration de Windows et de Linux
- Familiarité avec les bases de scripts Bash et/ou Python

Prérequis matériels :

Une station de travail ou Laptop pour chaque apprenant avec la configuration suivante :

- 16 Go de RAM
- 500 GB
- Processeur i5 8ème génération ou plus

PUBLIC:

- Professionnels de l'informatique voulant se convertir vers les tests d'intrusion
- Pentesters voulant préparer une certification reconnue
- Professionnels de la sécurité voulant approfondir leurs connaissances des techniques de cyber-attaques.

OBJECTIFS:

- Savoir organiser une mission d'audit de sécurité de type test d'intrusion
- Se mettre en situation réelle d'Audit
- Mettre en application les compétences techniques acquises dans le cadre d'une intervention professionnelle
- Être en mesure de rédiger un rapport d'audit professionnel
- Savoir présenter et transmettre un rapport d'audit

CONTENU:

Introduction to penetration test:

- Pentest definition

Methodology

Objectives

Bash scripting:

- Bash introduction

Basic commands and redirections

Language structure
Variables, conditions, and loops
Passive information gathering:
- Open web information gathering

Search engines
Google dorks
- Other resources

Email harvesting
Netcraft
Whois enumeration
- Recon-ng

Networking tools:
- Netcat p

Connecting to TCP/UDP ports
Listening to TCP/UDP ports
File transfer
Remote administration
- Ncat
- Wireshark

Introduction to wireshark
Traffic capturing and filters
Follow TCP stream
- Tcpdum

Traffic filtering
Advanced header filtering
Active information gathering:
- DNS Enumeration
- DNS lookups

Forward lookup brute force
Reverse lookup brute force
DNS zone transfer
- Port scanning

TCP ports scanning
UDP ports scanning
Port scanning with NMAP
Service enumeration
OS fingerprinting
Nmap scripting Engine (NSE)
- Additional enumeration

SMB enumeration
SMTP enumeration
SNMP enumeration
Vulnerability scanning:
- NMAP Vulnerability scanning
- Nessus vulnerability scanning

Web application attacks:
- Introduction to Web Proxy (Burp)
- Cross site scripting (XSS)

Cross site scripting types
Browser redirection and IFRAME injection

Cookies stealing and Session information
- File inclusion

Local file inclusion
Remote file inclusion
- MySQL injection

Authentication bypass
Enumerating the database
Column number enumeration
Data extraction
Code execution
Win32 buffer overflow exploitation:
- Introduction to debugger
- Types of buffer overflow
- Fuzzing
- Replicating the crash
- Exploiting the vulnerability

Controlling EIP
Locating space for shellcode
Checking for bad characters
Redirecting the execution flow
Generating the shellcode
Getting a shell
Linux buffer overflow exploitation:
- Introduction to GDB Generating the shellcode
- Replicating the crash
- Exploiting the vulnerability

Controlling EIP
Locating space for shellcode
Checking for bad characters
Redirecting the execution flow
Getting a shell
Working with exploits:
- Searching for exploits

Finding exploits in Kali
Finding exploits on the web
- Customizing and fixing exploits

Customizing exploit
- Fixing exploit

Password attacks:
- Offline password attacks

Dictionary files
Key space brute force
pwdump and fg dump
Windows credential editor
Password profiling
Password mutating
- Online password attacks

Hydra, Medusa and Ncrack
Choosing the right protocol: Speed vs Reward
- Password cracking

Password hashes
John the ripper
Rainbow tables
Passing the hash in windows
Data exfiltration:
- File transfer methods

Non interactive shell
Uploading files
Metasploit framework:
- Introduction to user interfaces
- Installation and updates
- Metasploit framework structure

Auxiliary modules
Exploit modules
- Metasploit payloads

Staged and non-staged payloads
Executable payloads
- Meterpreter

Meterpreter payloads
Multi handler
Meterpreter post exploitation
Post exploitation modules
Reporting:
- Vulnerabilities risk rating

CVSS and CWE concepts
CVSS calculation tools
OWASP risk rating
- Vulnerability definition and details
- Recommendations and fix priority
- Writing your report