Microtel
Training institute

TESTS D'INTRUSION AVANCÉS

CODE DE LA FORMATION:
MTI-SC-TIA

DURÉE:
5 JOURS

Cette formation de tests d'intrusions avancés enseigne le cycle de vie d'une cyberattaque du point de vue d'un adversaire. Vous allez vous familiariser avec les outils de tests d'intrusions les plus utilisés, manipuler le trafic réseau et réaliser des attaques d'applications Web avancées, l'élévation des privilèges sous Windows et Linux, ainsi que les attaques sur Active Directory. 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 :

- Avoir suivi une formation technique sur les Tests d'intrusions ou avoir les
- connaissances équivalentes
- Une solide compréhension des réseaux TCP/IP
- Une maitrise des systèmes Windows et de Linux
- Maitrise de langages de Scripting Bash et/ou Python.
- Une expérience avec l'exploitation des vulnérabilités Web et Buffer Overflow

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:

- Découvrir facilement et rapidement le réseau cible
- Exploiter en toute sécurité les vulnérabilités identifiées
- Élever ses privilèges pour accéder et manipuler les ressources critiques
- Rebondir sur le réseau compromis

CONTENU:

Passive information gathering:

- Taking Notes
- Website Recon
- Open-Source Code
- Shodan
- Security Headers Scanner

- SSL Server Test
- Pastebin
- User Information Gathering
- Social Media Tools
- Stack Overflow
- Information Gathering Frameworks

OSINT Framework

Maltego

Networking tools:

- Socat

Netcat vs Socat

Socat File Transfers

Socat Reverse Shells

Socat Encrypted Bind Shells

- PowerShell and Powercat

PowerShell File Transfers

PowerShell Reverse Shells

PowerShell Bind Shells

Powercat

Powercat File Transfers

Powercat Reverse Shells

Powercat Bind Shells Powercat Stand-Alone Payloads

Active Information Gathering

- Port scanning

Masscan

Web application attacks:

- Introduction to OWASP Top 10
- File inclusion

Local File Inclusion

Remote File Inclusion

- Automated SQL Injection tools

SQL Map

Writing SQL Injection Exploit

- Advances XSS

Privilege escalation:

- Information Gathering

Manual Enumeration

Automated Enumeration

- Windows Privilege Escalation Examples

Understanding Windows Privileges and Integrity Levels

Introduction to User Account Control (UAC)

Insecure File Permissions

Leveraging Unquoted Service Paths

- Linux Privilege Escalation Examples

Understanding Linux Privileges

Insecure File Permissions

Insecure File Permissions: /etc/passwd

Kernel Vulnerabilities

Client side attacks:

- Collecting client information

Passive client information gathering
Active client information gathering
Social engineering and client side attacks
- Client side exploits

Browser based exploits
Browser based exploit tools
Network tunneling and port redirection:
- Port forwarding and redirection
- SSH Tunneling

Local port forwarding
Remote port forwarding
Dynamic port forwarding
- Proxy chains
- HTTP Tunneling
- Traffic encapsulation

File Transfers:
- Considerations and Preparation

Danger of Transferring Attack Tools
Installing Pure-FTPd
The Non-Interactive Shell
- Transferring Files with Windows Hosts

Non Interactive FTP Download
Windows Downloads Using Scripting Languages
Windows Downloads with exec2hex and PowerShel
Windows Uploads Using Windows Scripting Languages
Uploading Files with TFTP
- Building an MSF module

Metasploit framework:
- Post Exploitation with Metasploit

Core Post-Exploitation Features
Migrating Processes
Post-Exploitation Modules
Pivoting with the Metasploit Framework
Metasploit Automation
Antivirus Evasion:
- What is Antivirus Software
- Methods of Detecting Malicious Code

Signature Based Detection
Heuristic and Behavioral Based Detection
- Bypassing Antivirus Detection

On-Disk Evasion
In-Memory Evasion
Practical Example
Active Directory Attacks:
- Active Directory Theory
- Active Directory Enumeration

Traditional Approach
A Modern Approach
Resolving Nested Groups
Currently Logged on Users

Enumeration Through Service Principal Names

- Active Directory Authentication

NTLM Authentication

Kerberos Authentication

Cached Credential Storage and Retrieval

Service Account Attacks Low and Slow Password Guessing

- Active Directory Lateral Movement

Pass the Hash

Overpass the Hash

Pass the Ticket

Distributed Component Object Model

- Active Directory Persistence

Golden Tickets

Domain Controller Synchronization

PowerShell Empire:

- Installation, Setup, and Usage

PowerShell Empire Syntax

Listeners and Stagers

The Empire Agent

- PowerShell Modules

Situational Awareness

Credentials and Privilege Escalation

Lateral Movement

- Switching Between Empire and Metasploit