Cyber Warfare

Index: **RT420**

Duration: 40 hours- 5 Days

Description

This training is an advanced course that covers topics in the Red-Team Cyber Warfare methodologies. The participants will get an in-depth look into the mind of a Black-Hat hacker. The training includes defense and offense and takes a deep dive into its practical world using the CYBERIUM ARENA simulator. Students will learn the different information-gathering tools and security bypassing products that can be leveraged to attack against every layer of defense.

Target Audience

- IT Professionals and Organizations that would like to embrace Red-Team's capabilities

Pre-requisites

- ThinkCyber Level-2 Courses

Objectives

- Acquiring the knowledge and tools to become better Red-Team member
- Becoming familiar with a variety of available tools for performing security-related tasks
- Becoming familiar with a variety of attack scenarios
- Understanding different attack possibilities
- Using automation as a Red-Team member

Day 1

Module 1: Red-Team Target Discovery

In this module, students will learn to act as Red-Team while attempting to gain information about the target using brute-force, craft discovery tools, fingerprinting websites. Furthermore, students will learn to use social engineering skills to trick the target into revealing information and their location.

- **Advanced Web-Discovery**
  - DNS Bruting
    - Amass
    - Sublist3r
    - aiodnsbrute
  - Passive Discovery
    - awesome-osint
    - ShodanHat
    - LinkedInt
  - Crafting Discovery Tools in Bash
  - Using recursebuster
  - Cloud AWS S3 Buckets using inSp3ctor
  - Fingerprinting Web Applications
    - BlindElephant
    - Red-Team Banner Grabbing
    - Firewall Detection using wafw00f
- **Gaining Information about the Target**
  - Advanced Social Engineering Techniques
  - The Browser Exploitation Framework (BeEF)
  - Tracking user Locations using Google API
  - Enumerating Services
    - Extracting Users from SAMBA
    - NetBIOS
    - RPCClent
  - Vulnerability Detection and CVE identifying
  - Shodan CLI
  - Maltego Teeth

Day 2

Module 2: Exploiting and Attacking

This module is all about gaining access at any cost. Students will learn to build a password list for brute-force wordlist attacks, preform advanced fuzzing, and finally automate the attacks. Also, students will practice advanced Red-Team attacks over the network using various specialized tools.

- **Gaining Access**
  - Creating Password Lists
    - Wordhound
    - Brutescrape
    - Gitrob
    - CUPP
    - Crunch
  - Online Brute-Force to Gain Access
    - SSH Bruting using Hydra
    - Burpsuite Intruder
    - RDP Cracking using Crowbar
  - Fuzzing
    - Application Fuzzing
    - Protocol Fuzzing
    - File Format Fuzzing
    - Fuzzers Advantages and Limitations
  - Crafting Malware from Source using The-ZOO
  - Automating the Attack
    - Advanced Features of Metasploit
    - Crafting Scapy Tools
    - Forging RC Scripts
    - Automating Empire's API using DeathStar
- **Network Attacks**
  - Exposed Printers Abuse
  - Advanced MiTM Techniques for Red-Teams
    - Using the DHCP Protocol to Gain MiTM Status
    - DNS Proxy Crafting using DNSChef and MiTMProxy
  - Catching LLMNR and NBT-NS Credentials using Responder
  - DHCP Starvation Usages and Advantages
  - Flooding SIP and SOP Invite Protocol using inviteflood
  - Advanced DDoS using UFONET-Framework
  - Paralyzing Windows Hosts using Default Services

Day 3

Module 3: Escalating Privileges and Maintaining Access

During this module, students will learn a variety of methods to gain higher access to the exposed target, such as offline brute-forcing, disabling the SSL function, spying over VoIP and WSL, and more.

- **Escalating Privileges**
    - Using Meterpreter for Privilege Escalation
    - Gaining Passwords Using Offline Brute-Force
        - John The Ripper
        - Cain and Abel
        - L0phtCrack
        - DaveGrohl
    - Privilege Escalation using Vulnerable Services
    - Uncovering Hidden Credentials on Windows Server using BloodHound
    - Seemless SSL-Striping
    - Intercepting and Abusing WSL Service
    - Spying on IP-Phones using VoIP-Hopper and ohrwurm
    - Red-Team NSE User Enumeration
    - Windows and Linux Exploit-Suggesters
- **Maintaining Persistence**
    - Crafting Backdoors
        - Msfvenom
        - Nishang
    - Firewall, IDS and Honeypot Evasion Techniques
        - Recompiling the Backdoors
        - Forging Tunnels using the HTTPTunnel Tool
        - Using SSH to Hide Backdoor Traffic
        - Using Automater to Identify Honeypots
    - Linux Rootkits for Red Teams
        - Linux Boot Process
        - Browsing the Kernel Code
        - Accessing User Space Process Memory
        - Understanding the Kernel Network Stack

Days 4-5

Module 4: Surfing the Exposed Network

This module will demonstrate to the new Red-Team, the usage of advanced techniques to map the exposed network from the inside, and finally, gain control of the main components of the network.

- **Mapping the Exposed Network**
  - Advanced Nmap Reports
  - Abusing SQL Server Trust
  - Trusted Features of PowerShell
  - Finding Exposed Targets using CrackMapExec
  - Querying Active Directory
    - Advanced ACL/ACE Bloodhound
    - DNS Beacon
    - Empire - Info Module
- **Taking Over the Network**
  - Pass-the-Hash
  - Harvesting Kerberos Tickets
  - Abusing the DCOM application
  - Empire - PSInject
  - Building a Keylogger
  - THP Red-Team Droppers
  - Domain-Control Dump
  - Advanced Linux Pivoting using mimipenguin