THE OPEN UNIVERSITY OF TANZANIA

RED TEAM OPERATIONS AND ADVERSARY EMULATION TRAINING

START DATE: 1st July, 2024 DURATION: SIX WEEKS (3 hrs /day 3 days/week)

Course Overview

Penetration testing is good at finding weaknesses in systems, but it's not so great at dealing with the people and procedures that defend against attacks. Because of this, the teams defending against attacks (the Blue Teams) might not know exactly what they need to do better to stop future attacks. This can lead to a situation where organizations keep finding and fixing weaknesses in their systems, but they don't get better at catching and stopping attacks in the long run.

In this course, students will learn how to organize and carry out Red Teaming operations from start to finish. This involves mimicking the actions of real attackers to test a company's defenses. Students will learn how to set up a Red Team, use threat intelligence to understand how attackers operate, copy those methods in their tests, write reports about what they find, and analyze the results. The goal is to help the organization improve its overall security by identifying and fixing weaknesses. As part of the course, students will practice these skills by simulating an attack on a corporate or enterprise environment, including trying to breach systems like Active Directory, sending emails with fake intelligence, accessing file servers, and targeting both Windows and Linux computers.

This course is divided into six intensive sections. We will begin by using cyber threat intelligence to figure out which adversaries might have the intent, opportunity, and capability to attack the target organization. With this information, students will plan their attacks carefully, following a method called the Unified Kill Chain and using various tactics and techniques identified in the MITRE® ATT&CK™ framework. Over three sections, students will dive deep into technical skills used by Red Teams, from setting up advanced attack systems to exploiting weaknesses in Active Directory. Once they've gained access to the target systems, students will thoroughly explore each one, gathering technical information and valuable data, moving around within the network, and taking steps to maintain access and steal sensitive information. The course wraps up with an exercise where students analyze how the Blue Team (the defenders) respond to the attack, report their findings, and make plans to fix any vulnerabilities discovered before testing the defenses again.

In this course, you'll discover the significance of Red Teaming and adversary emulations for organizations. The primary goal of a Red Team is to enhance the capabilities of a (Defenders) Blue Team. It's a mutual learning process where offense teaches defense and vice versa. This course aims to cultivate skilled Red Team operators who can orchestrate systematic engagements. These engagements

prioritize training and evaluating the efficiency of the individuals, procedures, and technology employed to safeguard environments.

Course Objectives

— Understand how to use threat intelligence and plan a Red Team operation.
— Establish the necessary infrastructure with strong operational security for a successful operation.
— Develop methods to infiltrate an organization effectively.
— Use automated tools and manual techniques to gather important data needed to accomplish your goals.
— Navigate through a corporate network, moving from one system to another.
— Gain higher levels of access by exploiting various vulnerabilities and misconfigurations.
— Present your findings in a clear and valuable manner to provide maximum benefit to your client.

Learning Outcomes

How to analyze threat intelligence to understand how adversaries operate.
— Develop a plan to mimic adversary actions.
— Connect actions to the MITRE® ATT&CK™ framework to communicate effectively with the Blue Team.
— Set up strong and advanced communication and control (C2) infrastructure.
— Keep your operations secure throughout the engagement.
— Use your initial access to expand and move within a network.
— Identify and exploit vulnerabilities in Active Directory.
— Securely gather and remove sensitive data.
— Conclude an operation, provide value to your client, and prepare for future testing.

Course contents

Section 1: Planning Adversary Emulation and Threat Intelligence

— Adversary Emulation
— Ethical Hacking Maturity Model
— Frameworks and Methodologies
— Understanding Adversaries
— Unified Kill Chain
— MITRE® ATT&CK™
— Threat Intelligence
— Threat Report ATT&CK™ Mapping (TRAM)
— ATT&CK™ Navigator
— End-To-End Testing Model
— Assumed Breach
— Execution Phase

- Building a Red Team - Skill Development
- Reconnaissance
- Open-Source Intelligence (OSINT)
- Password Attacks
- Social Engineering
- Attacks Against MFA – evilnginx2

Section 2: Attack Infrastructure and Operational Security

- Red Team Tools
- Command and Control (C2)
- C2 Comparison
- Listeners and Communication Channels
- Advanced Infrastructure
- Redirectors
- Third-Party Hosting
- Comparison of Self-Hosted vs. Third-Party
- Operational Security
- Understand IoCs
- Introduction to VECTR Platform
- Covenant
- Cobalt Strike

Section 3: Initial Foothold and Persistence

- Weaponization
- Custom Executables
- Blending In
- Execution Guardrails
- Initial Access
- Network Propagation
- Discovery
- Operational Security
- Deception Technology
- Local Network Enumeration
- Local Privilege Escalation
- Password Cracking
- Persistence
- Defense Evasion - Static vs Dynamic Analysis
- AMSI Bypass internals

Section 4: Active Directory

- Introduction to Active Directory
- Trees and Forests
- Authentication, Authorization, Access Tokens
- AD Enumerate
- DNS Extraction
- Domain Privilege Escalation
- Access Token Manipulation
- Pass-The-Hash, Pass-The-Ticket
- Kerberoasting
- Silver Ticket, Golden Ticket, Skeleton Key
- AD Certificate Services
- Unconstrained and Constrained Delegation
- Coerced Authentication Using PrinterBug and PetitPotam
- Hopping the Trust
- Bloodhound/SharpHound
- AD Explorer
- SMB Pipes, Remote Desktop Protocol, PsExec, Windows Management Instrumentation, dcom
- SMB Relay
- Responder
- Setting Up Shadow Credentials
- Domain Privilege Abuse
- DC Sync
- Domain Lateral Movement, Domain Trust Attacks
- Pivoting Between Domains and Forests
- Forest Enumeration, Forest Attacks

Section 5: Actions on Objectives and Reporting

- Action on Objectives
- Database Attacks
- SQL Abuse
- Trust Abuse
- PowerupSQL
- Target Manipulation
- Collection
- Data Staging
- Exfiltration
- Impact
- Emulating Ransomware

— Engagement Closure
— Analysis and Response
— Red Team Reveal
— Measuring People and Processes
— Retesting
— Remediation and Action Plan
— Breach and Attack Simulation
— APTSimulator
— Network Flight Simulator
— Atomic Red Team
— MITRE® CALDERA

Section 6: Red Team Capture-the-Flag

— Adversary Emulation
— Reconnaissance
— Initial Access
— Persistence and Privilege Escalation
— Credential Access
— Discovery
— Lateral Movement
— Collection
— Command and Control
— Exfiltration
— Impact and Closure

Targeted group:
This course targets individuals who are interested in learning about red team operations and offensive security;

— Information Security Professionals.
— Penetration testers and Red Team members.
— Ethical Hackers and Cyber Security Professionals.
— Information Technology Professionals (System Administrators, Network Administrators).
— Auditors who need to build deeper technical skills.
— Network defenders, and forensic specialists
—

Training Mode
The course will be offered through F2F mode at HQ and online mode depending on course content and topic.

Teaching mode will include 40% theory and 60% practices using computer laboratories, you are also encouraged to bring your laptop.

Course fee: Tshs 800,000

To paid through
Bank name: NBC
Account no. 011103033713
Account name: OCB

Note: ONLY 30 Students Required for this class to start and all fees amount to be paid before class commences.

Register Here: https://forms.gle/rHY2fC6nH4zYZphWA

To register please contact us through the following details

Email: richlaizer.96@gmail.com, mwanuzi@gmail.com , george.oreku@gmail.com

Telephone: 0687063988/ 0753000102 /0719454547