RED TEAM VS BLUE TEAM CYBERWAR CHALLENGE

DURATION: 5 DAYS

COURSE OVERVIEW

Two Teams, two different approaches, Red Team vs Blue Team Cyberwar Challenge! The cyber kill chain - reconnaissance, attack planning and delivery, system exploitation, privilege escalation and lateral movement, anomalies detection, discovery of industry attacks and threats, understanding how compromised system or solution looks like, defining the indicators of the attack, and incident handling.

Is your security program effective?
Are you able to stop simulated attacks?
Are you ready for this cyberwar challenge, who will win?

This is an ultimate aim to test organization's' security as well as ability to detect and respond to an attack.

Challenge yourself and join the Red Team vs Blue Team Cyberwar Challenge!

- Red Team Training (Cyber-Attack)
- Blue Team Training (Cyber-Defense)
- Cyber-Competition Red Team vs Blue Team (Capture the Flag!)

TARGET AUDIENCE

Red team and blue team members, enterprise administrators, infrastructure architects, security professionals, systems engineers, network administrators, IT professionals, security consultants and other people responsible for implementing network and perimeter security.

COURSE OBJECTIVES

After completing this course you should be able to:

1. Analyze emerging trends in attacks
2. Identify areas of vulnerability within your organization
3. Prepare a risk assessment for your organization
4. Report and recommend countermeasures
5. Develop a threat management plan for your organization
6. Organize Red Team – Blue Team exercises

COURSE CONTENT

Red Team Training (Cyber-Attack)

Module 1: Modern Attack Techniques

- OS platform threats and attacks
- Web based threats and attacks
- E-mail threats and attacks
- Physical access threats and attacks
- Social threats and attacks
- Wireless threats and attacks

Module 2: Reconnaissance

- Open Source Intelligence (OSINT)
- Google hacking
- Shodan
- DNS
- Port scanning
- Service discovery

Module 3: Weaponisation and Delivery

- Generating malicious payload
- Hiding malicious content in Office Suite documents
- Reverse shells
- Meta sploit
- Empire
- AV evasion techniques.
- Building phishing campaign
- Planting malicious device
- Attacks on 3rd parties
- Stage-less and staged payloads / C&C

Module 4: Exploitation and Installation

- Types of vulnerabilities
- Establishing foothold
- Stage-less and staged payloads
- Command and Control (C2)

Module 5: Privilege escalation

- Privileged accounts
- System services security
- Common misconfigurations
- Security tokens

Module 6: Lateral movement and Persistency

- Credential harvesting
- Mimikatz
- Network reconnaissance
- Building network map
- Responder
- Pass-the-hash
- Pass-the-ticket
- Sleeping agents
- Piggybacking on network packets
- Rootkits

Blue Team Training (Cyber-Defense)

Module 1: Identifying Areas of Vulnerability

- Defining the assets which your company needs to protect
- Defining the other sensitive information that needs to be protected

Module 2: Protecting entry points

- Setting up firewall
- DNS hardening
- Log collectors and SIEM
- Intrusion Prevention Systems
- Security awareness
- O365 / Safe links
- Smart Screen
- Secure proxy
- Sandboxing
- Sinkholing
- APT campaigns

Module 3: Deploying guards

- Anti-Virus
- Firewall
- Application Whitelisting
- WDAC
- Living Off the Land Binaries
- Exploit Guard
- AMSI

Module 4: Least privilege principle

- Patch management
- Group Managed Service Accounts

- Just Enough Administration
- Vulnerability Management

Module 5: Inspecting own backyard

- Logging
- GPO policies
- LAPS
- Credential Guard
- Windows ATA
- Defender ATP

Module 6: Clean-up

- Searching for rogue servers
- Looking for network anomalies
- Looking for backdoors

Cyber-Competition Red Team vs Blue Team (Capture the Flag!)

Students will be divided into two groups – both will have a mix of Red Team and Blue Team people. Both groups will get their own small set of machines to configure and protect. The machines will serve various purposes – some of them will have services configured, such as WWW, DNS or SMB.

System hardening

The first two hours will be used to understand the architecture, find out what services are running, what is the configuration, and so on. Cooperating as a group, their job would be to harden the configuration, find and fix misconfigurations and plan future services – such as logging the events!

Cyberwar

After two hours, the big firewall between two groups is disabled, and groups can see each other's networks. The fun starts here. Red Team members will try to find vulnerabilities in target systems and recover some sort of secret (the flag). At the sametime Blue Team members will try hard to prevent that - by deploying a set of protections, monitoring the network and actively stopping the attacks.

To make things even more exciting, automated clients will also interact with the services. Each group has to make sure, that the services are not interrupted, and regular clients can still use them.
Each flag will be unique. After it is obtained, it should be sent to our scoring systems, where groups can see the description of all challenges, as well as, current scoreboard! Each flag is scored differently; the harder it is to get it, the more points at the end! Points can also be used to buy additional hints if group cannot move forward with one of other challenges.

Wrap-up Discussion
The last hour would be used to summarize what worked and what did not – groups would describe what they did to retrieve the flag or what they did to prevent the other team from recovering it. The Instructor would also answer all the questions and show what the intended solution is to beat some of the challenges.

COURSE PREREQUISITES

Good hands-on experience in administering a Windows infrastructure. At least 8 years in the field is recommended.

TEST CERTIFICATION

Recommended as preparation for the following exams:

There is no specific exam aligned to this course, however all attendees will receive an online Certificate of Attendance