MASTERCLASS: RED TEAM - BLUE TEAM OPERATIONS

DURATION: 5 DAYS

COURSE OVERVIEW

This is a deep dive course on Red Team – Blue Team Operations: The cyber kill chain

Security is a business enabler, and it is only when it is viewed from a business perspective that we can truly make the right decisions. Identifying, protecting and restricting data that can be monetized by adversaries is essential and should be reviewed and defined on a regular basis as only then can you identify potential gaps in your security posture.

Every organization should expect to be hacked at some point so it is vital that all members of your blue and red teams are up to speed on the latest hacking techniques.

The term Cyber Kill Chain defines the steps used by cyber attackers in today's cyber based attacks and this course reviews all of those steps from both a red and blue team perspective.

Reconnaissance is the first phase, during which the attacker gathers information on the target before the actual attack starts. The data gathering is essential skill of every red teamer. From blue teamer perspective, it is crucial to understand what kind of information is publicly available and to learn how to protect that information.

Without remote code execution vulnerability even the most sophisticated payload needs to be delivered to the victim. There are plenty of ways to achieve that so blue team needs to ensure that payloads are detected and blocked at early stage.

After successful delivery, malicious code exploits a vulnerability to execute code on victim's system. There are many mechanisms that, if properly configured, significantly reduce attack scope.

The successful exploitation attack often results in code execution with limited privileges. Both, red teamers and blue teamers should be familiar with common techniques and misconfigurations allowing for privilege escalation.

The next after gaining admin privileges on single host is lateral movement that gives access to additional resources within the company. Before red teamer can reach Domain Controller or other critical servers, blue team can implement numerous protections against that threat

Even after attack is stopped and contained, the attacker will want to ensure persistency and possibility of returning to a compromised host.

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

Module 1: Identifying Areas of Vulnerability

1. Defining the assets which your company needs to protect
2. Defining the other sensitive information that needs to be protected

Module 2: Modern Attack Techniques

1. OS platform threats and attacks
2. Web based threats and attacks
3. E-mail threats and attacks
4. Physical access threats and attacks
5. Social threats and attacks
6. Wireless threats and attacks

Module 3: Reconnaissance

1. Open Source Intelligence (OSINT)
2. Google hacking
3. Social Media presence
4. DNS 5. Shodan
5. Physical reconnaissance
6. Port scanning
7. Service discovery

8. SIEM
9. Intrusion Prevention Systems

Module 4: Weaponization

1. Generating malicious payload
2. Hiding malicious content in Office Suite documents
3. Reverse shells
4. Meta sploit
5. Empire
6. AV evasion techniques

Module 5: Delivery

1. Building phishing campaign
2. Planting malicious device
3. Attacks on 3rd parties
4. Enabling phishing protection
5. O365 / Safe links
6. Smart Screen
7. Secure proxy
8. Sinkholing
9. APT campaigns

Module 6: Exploitation and Installation

1. Types of vulnerabilities
2. Establishing foothold
3. Stage-less and staged payloads / C&C
4. Anti-Virus
5. Firewall
6. Application Whitelisting
7. WDAC
8. Living Off the Land Binaries
9. Exploit Guard
10. AMSI

Module 7: Privilege escalation

1. Privileged accounts
2. System services security

3. Common misconfigurations
4. Security tokens
5. Just Enough Administration
6. Patch maintenance

Module 8: Lateral movement

1. Credential harvesting
2. Mimikatz
3. Network reconnaissance
4. Building network map
5. Responder
6. Pass-the-hash
7. Pass-the-ticket
8. Credential Guard
9. LAPS
10. GPO policies
11. Windows ATA
12. Defender ATP

Module 9: Persistency

1. Sleeping agents
2. Piggybacking on network packets
3. Rootkits
4. Sysinternals
5. Searching for rogue servers
6. Looking for network anomalies

COURSE PREREQUISITES

Attendees should meet the following prerequisites:

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

TEST CERTIFICATION

Recommended preparation for exams:

There are no exams aligned to this course