CRAW ACADEMY

CERTIFIED RED TEAM PROFESSIONAL

Training and Certification

Cyber Security Educational Courses Professional Sessions

ABOUT US

We offer Cyber Security and Information Security training and Certification in Delhi for Cyber Security and Information Technology aspirants. Since Decade, we have been in the Information Technology and Cybersecurity industry. You can learn more about cybersecurity, Techniques, and Tools to choose a better career path.

CERTIFIED RED TEAM PROFESSIONAL COURSE MODULE

1. Module 1: Active Directory – Introduction

1.1.1. Forest, Trust, Groups, Object, OUs, Structure etc.
1.1.2. Mapping Objects, Security Groups, Default computers, Default OUs.
1.1.3. Introduction to Tools (PowerView, AD Modules Rubeus, Mimikatz, Safetykatz BloodHound etc.)
1.1.4. Introduction to PowerShell and .NET
1.1.5. LDAP Functions and working.

2. Module 2: Enumeration – Active Directory

2.1.Active Directory - Manual Enumeration
2.1.1. Enumeration Using Legacy Windows Tools
2.1.1.1.1. Enumerate using net.exe
2.1.2. Enumerating Active Directory using PowerShell and .NET Classes
2.1.2.1.1. LDAP Path Prototype.
2.1.2.1.2. Basic PowerShell Script.
2.2.AD Enumeration with PowerView and AD Modules
2.2.1. Enumerate DC (Domain Controller)
2.2.2. Enumerate Users, groups, group memberships, computers, User properties, Trusts, ACLs etc.
2.2.3. Enumerate GPOs, Policy, Trusts, Forests.
2.2.4. Enumerate Domain Admins, Enterprise Admins, Domains Admins Groups.
2.2.5. User Hunting

3. Module 3: Local Privilege Escalation

3.1.Missing patches
3.2.Automated deployment and AutoLogon passwords in clear text
3.3.AlwaysInstallElevated (Any user can run MSI as SYSTEM) – Misconfigured Services
3.4.DLL Hijacking and more – NTLM Relaying a.k.a. Won't Fix
3.5.Local Privesc | PowerUp
3.6.Local Privesc | Privesc
3.7.Local Privesc | winPEAS
3.8.Feature Abuse | Jenkins Abuse

Module 4: Enumeration via Bloodhound

4.1.Introduction to Bloodhound
4.2.Sharphound.exe
4.3.Sharphound module Loading in PowerShell session.
4.4.Mapping objects in AD like Users, Computers, Rights, Groups etc
4.5.Shortest to Domain Admin

Module 5: Lateral Movement

5.1.PowerShell Remoting
5.1.1.Remoting via Psexec
5.1.2.Remoting via Winrm
5.1.3.Loading Sessions
5.1.4.Executing Command via PS Remoting (Invoke-Commands)
5.1.5.Session Variables Creation.
5.2.Invoke-MimiKatz
5.2.1.Extracting Credentials from LSASS
5.2.2.Over Pass the Hash (OPTH)
5.2.3.DCSync Attack Using MimiKatz

Module 6: Offensive .NET

6.1.1.AV Bypass
6.1.1.1.AV Bypass | DefenderCheck
6.1.1.2.AV Bypass | String Manipulation
6.1.1.3.AV Bypass | BetterSafetyKatz
6.1.1.4.AV Bypass | Obfuscation
6.1.2.Payload Delivery

Module 7: Authentication Mechanism in AD

7.1.Introduction to Kerberos.
7.2.Working of krbtgt hash.

Module 8: Persistence attacks

8.1.Golden Ticket (TGT)
8.2.Golden Ticket Generation
8.3.Request for Golden Ticket from DC using BetterSafetyKatz.exe.
8.4.Silver Ticket (TGS)
8.5.Difference in Silver and Golden Ticket.
8.6.Silver Ticket Generation
8.7.Command Execution Using Silver Ticket.
8.8.Diamond Ticket
8.9.Diamond Ticket Request Using Rebeus.exe
8.10.Skeleton Key
8.11.Skeleton key | lsass Process Abuse using MimiKatz.
8.12.Skeleton key | lsass protection bypass using mimidriv.sys
8.13.DSRM Attack Overview and working

Module 9: Domain Privilege Escalation

9.1.DSRM Attack Overview.
9.2.Kerberoast Overview.
9.3.Kerberoast Attacking Working.
9.4.Cracking Hash with John.
9.5.Kerberoasting| AS-REPs Attack.
9.6.Kerberoasting| Set SPN.

Module 10: Delegation Attacks
10.1.Kerberos Delegation
10.2.Unconstrained Delegation
10.3.Unconstrained Delegation | Printer bug
10.4.Constrained Delegation
10.5.Constrained Delegation with Protocol Transition.
10.6.Resource Based Constrained Delegation.
Module 11: Domain Trust Abuse
11.1.Across Trusts Overview
11.2.Child to parent
11.3.Child to Parent Trust Flow
11.4.Child to Parent Using Trust Keys
11.5.Trust Keys Attributes in BetterSafetyKatz.exe
11.6.Child to Parent using krbtgt hash
11.7.Trust Flow Across Forest
11.8.Across Forest using Trust keys attack
Module 12: MSSQL Links Abuse
12.1.MSSQL Server
12.2.Enumerate Database Links using PowerUpSQL
12.3.Exploit Database Links
Module 13: Detection and Defense
13.1.Protect and limit Domain Admins
13.2.Isolate administrative workstations
13.3.Secure local administrations
13.4.Time Bound Administration – JIT
13.5.Time Bound Administration – JEA
13.6.Detection and Defense - Tier Model
13.6.1.Tier Model: Control Restrictions
13.6.2.Tier Model: Logon Restrictions
13.7.Detection and Defense - ESAE
13.8.Detection and Defense - Credential Guard

Pre Requisites

1. Networking
2. Basic Pentesting

Duration : 24 Hours