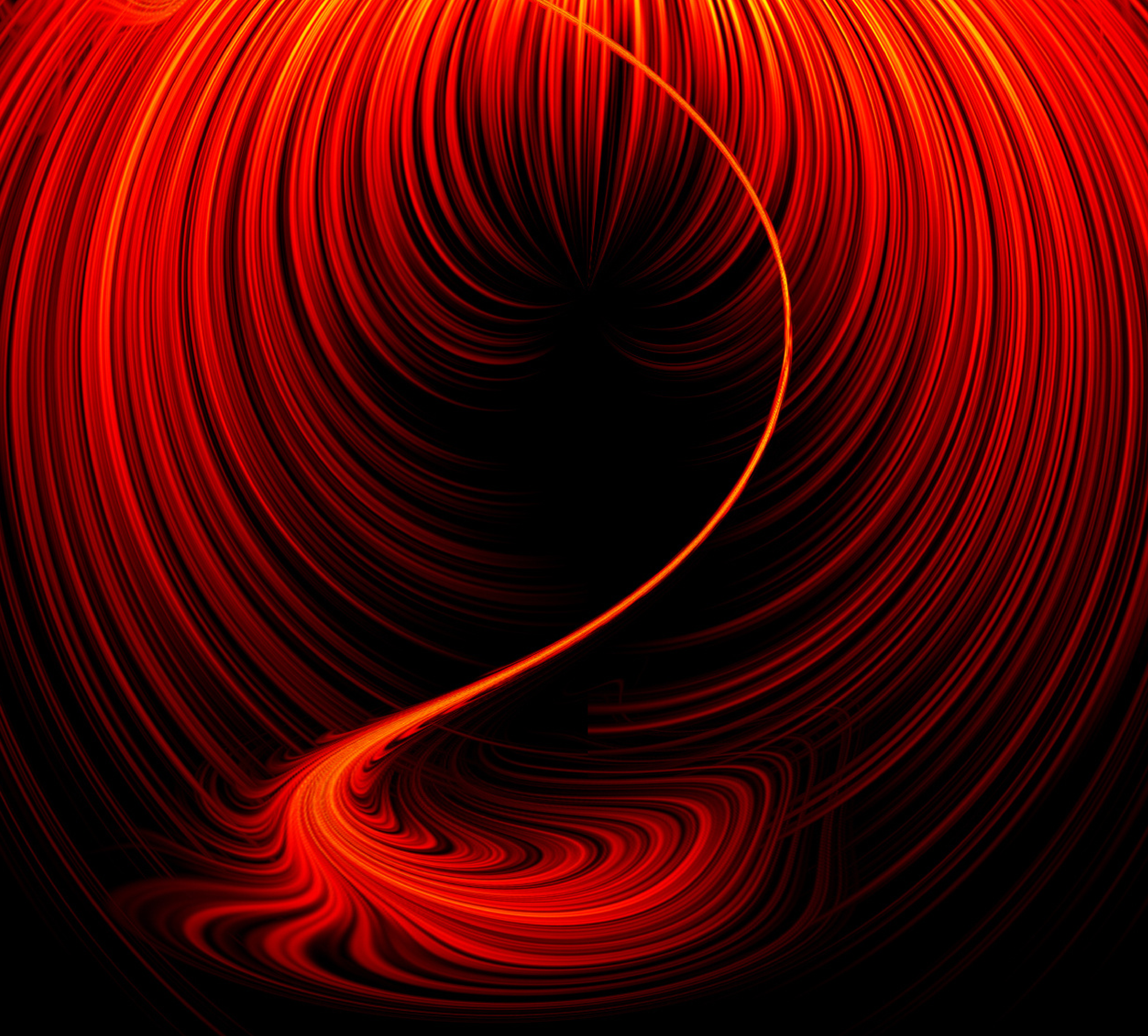

ACTIVE DIRECTORY PENETRATION TESTING

TRAINING PROGRAM

Why you should choose this course ?

Learn about Active Directory Pentest Courseware and the vulnerabilities to an organization's infrastructure through online training for security experts.

Professionals who want to learn about the most common risks can benefit from this course. To begin, you'll do a sneak reconnaissance and enumeration of hosts, servers, services, and privileged users to identify them.

To wrap things up, you will learn how to conduct red team attacks on Active Directory by targeting common misconfigurations and leveraging genuine Windows/Active Directory features.

Who should Join this course ?

- Ethical hackers
- System Administrators
- Network Administrators
- Security Professionals
- Pentester
- Blue Teamer
- Red Teamer

COURSE DURATION: 25 to 35 HOURS

AD

COURSE CONTENT

Initial AD Exploitation

- Introduction to AD
- Lab Setup
- Discovering Hosts with SMB Signing and SMBv1
- SMB DLL Delivery
- LLMNR Poisoning Attack
- Capturing NTLMv2 Hashes

Active Directory Post Enumeration

- RPCClient
- Bloodhound
- PowerView

Abusing Kerberos

- Kerberos Authentication
- AS-REP Roasting
- Kerberoasting Attack
- Kerberos Brute Force Attack

Credential Dumping

- Domain Cache Credential
- LAPS
- DCSync Attack
- NTDS.dit

Privilege Escalation

- HiveNightmare (CVE-2021-36934)
- sAMAccountName Spoofing (CVE-2021-42287)
- SeBackupPrivilege
- Token Impersonation
- PrintNightmare (CVE-2021-34527)

Persistence

- Golden Certificate Attack
- DSRM
- DC Shadow Attack
- Golden Ticket Attack
- Skeleton Key

Lateral Movement

- Pass the Ticket
- Pass the Cache
- Over Pass the Hash
- Pass the Hash

Bonus

- Covenant for Pentester Basics
- CrackMapExec
- Impacket