CyberArk Red Team TTP Training

Course Outline

Code execution

Opsec / non opsec safe code execution

AV/EDR evasion

Application whitelisting bypass

Memory injection

Custom implants

Covert Channels

Staged vs stateless payloads

Http / https based c2 communication

SMB DNS Application layer

C2 Domain fronting Persistence

Windows native persistence

On disk persistence

Fileless malware

Dll hijack Privilege escalation

Understanding Windows privileges

Common privilege escalation

3rd party escalation

Fuzzing for windows privesc vulnerabilities

Lateral movement

Situational awareness

Abusing credentials for lateral movement

Understanding protocols usage during lateral movement

Pivoting segmented networks