ENTERPRISE TECHNIQUES FOR RED TEAM ASSESSMENT

WHOAMI #

BLAY ABU SAFIAN

FOUNDER OF INVETECK GLOBAL

CTF TEAM LEAD BLACK CYBERSECURITY ASSOCIATION

IG: K1NGBLAY

ASSESSMENT IN CYBERSECURITY

INVETECK GLOBAL

WHO IS A RED TEAMER?

INVETECK GLOBAL

Ninja form of a Penetration Tester

ENTERPRISE RED TACTICS

INVETECK GLOBAL

ENTERPRISE RED TACTICS

- Recon – Red teamer gathering info about the organization.
- Initial Compromise – Trying to execute malicious codes without detection.
- Establish Persistence – Maintaining of access.
- Escalate Privilege – Gaining higher access
- Internal Recon& Lateral Movement& Data Analysis&C2 – Red teamer gathers credentials, draws map of environment and communicates with systems to control them
- Exfiltration& Mission completion - Stealing of data for the given task

INVETECK
GLOBAL

ENTERPRISE RED TOOLS

- Recon : eyewitness, social mapper, sub-z.
- Initial Compromise :demiguise, don’t kill my cat, credsniper
- C2 : cobalt strike, empire, koadic, covenant
- Lateral movement : CrackMapExec, SharpHound, Responder, Impacket
- Exfiltration : PyExfil, DNSExfiltrator

ENTERPRISE RED TECHNIQUES (CREDENTIAL STUFFING)

Red Teamers may use dumped credentials into gaining access to a network.

Using the same credentials across personal and business platforms.

ENTERPRISE RED TECHNIQUES (COMMON PORTS)

FTP (21)
SSH (22)
TELNET (23)
SMB (139,445)
KERBEROS (88)
MYSQL (3306)
VNC (5900)
RDP (3389)

ENTERPRISE RED TECHNIQUES (OTHER SERVICES)

OFFICE 365

GMAIL

ZOOM

ACCOUNT MANIPULATION MITIGATION

SETTING MFA

SETTING PASSWORD POLICIES

ACCOUNT MANIPULATION DETECTION

Monitor authentication logs

ENTERPRISE RED TECHNIQUES (POWERSHELL)

Red teamers utilize PowerShell command and scripts for information disclosure, download and execution purpose.

ACCOUNT MANIPULATION MITIGATION

INVETECK GLOBAL

Disable/Restrict WinRM services to prevent remote connection with PowerShell

Anti malware/Anti virus can be used to detect and delete malicious programs or executable files

ACCOUNT MANIPULATION DETECTION

Monitor for powershell assembles like System.Management.Automation.dll etc

When proper execution policy is set, the change in policy of the system can be detected .

Q&A

WWW.INVETECKGLOBAL.COM

THANK YOU