Red Team References

Red Team References

External references that contain Red Team related information.

Description	Link
Red Team: How to think like the enemy - Micha Zenko	https://www.cfr.org/book/red-team
Strategic Cyber Blog	http://blog.cobaltstrike.com
SpecterOps Blog	https://posts.specterops.io
ThreatExpress Blog	http://threatexpress.com
Cobalt Strike Aggressor Scripts @harleyQu1nn	https://github.com/harleyQu1nn/AggressorScripts
Cobalt Strike Aggressor Scripts @bluescreenofjeff	https://github.com/bluscreenofjeff/AggressorScripts
Awesome-Red-Teaming	https://github.com/yeyintminthuhtut/Awesome-Red-Teaming
Red Team Journal	http://redteamjournal.com

Red Team Infrastructure

Tips and tricks on building a Red Team infrastructure.

Description	Link
Red Team Infrastructure Wiki	https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki
Designing Covert Red Team Infrastructure	https://bluescreenofjeff.com/2017-12-05-designing-effective-covert-red-team-attack-infrastructure/
Mod_Rewrite Redirectors	https://bluescreenofjeff.com/2016-06-28-cobalt-strike-http-c2-redirectors-with-apache-mod_rewrite/
CobaltStrike Profiles to Mod_Rewrite	http://threatexpress.com/2018/02/automating-cobalt-strike-profiles-apache-mod_rewrite-htaccess-files-intelligent-c2-redirection/
SSL Certificate installation/transparency reports	https://cryptoreport.websecurity.symantec.com
SSL Certificate installation/transparency reports	https://transparencyreport.google.com/https/certificates?hl=en

Red Team Tools

Highlighted Red Team tools based on the Get In, Stay In, and Act concept and the Cyber Kill Chain

Get In

Reconnaissance

Tools for information gathering

Description	Link
BloodHound	https://github.com/BloodHoundAD/BloodHound
DomainHunter	https://github.com/threatexpress/domainhunter
EyeWitness	https://github.com/ChrisTruncer/EyeWitness
MailSniper	https://github.com/dafthack/MailSniper
Nmap	https://nmap.org
Recon-NG	https://bitbucket.org/LaNMaSteR53/recon-ng
Shodan	https://www.shodan.io/
OPSEC Considerations for Beacon Commands	https://blog.cobaltstrike.com/2017/06/23/opsec-considerations-for-beacon-commands/

Weaponization

Tools for creating payloads

Description	Link
CACTUSTORCH	https://github.com/mdsecactivebreach/CACTUSTORCH
Backdoor Factory	https://github.com/secretsquirrel/the-backdoor-factory
Unicorn	https://github.com/trustedsec/unicorn
Veil	https://github.com/Veil-Framework
10 Process Injection techniques	https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

Delivery

Tools for initial access and payload delivery

Description	Link
Social Engineering Toolkit	https://github.com/trustedsec/social-engineer-toolkit
GoPhish	https://getgophish.com/

Description	Link
FiercePhish	https://github.com/Raikia/FiercePhish

Exploitation

Tools for exploitation

Description	Link
Burp Suite	https://portswigger.net/burp
Exploit-DB	https://www.exploit-db.com
Metasploit	https://www.metasploit.com
Zed Attack Proxy	https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Stay In

Installation

Tools for persistence and payload installation

Description	Link
Windows Privilege Escalation Checklist	https://github.com/netbiosX/Checklists/blob/master/Windows-Privilege-Escalation.md
Persistence	https://rastamouse.me/2018/03/a-view-of-persistence/
PowerSploit	https://github.com/PowerShellMafia/PowerSploit

Command and Control

Command and Control tools and frameworks

Description	Link
Empire	http://www.powershellempire.com/
CobaltStrike	https://cobaltstrike.com/
Kodiac	https://github.com/zerosum0x0/koadic
PoshC2	https://github.com/nettitude/PoshC2
Pupy	https://github.com/n1nj4sec/pupy
Merlin	https://github.com/Ne0nd0g/merlin

Description	Link
Metasploit	https://www.metasploit.com/
TinyShell	https://github.com/threatexpress/tinyshell
Throwback	https://github.com/silentbreaksec/Throwback
WMImplant	https://github.com/ChrisTruncer/WMImplant

Act

Action on Objectives

Tools that perform actions on a target

Description	Link
Misc PowerShell Post Exploitation Scripts	https://github.com/rvrsh3ll/Misc-Powershell-Scripts
Hashcat	https://hashcat.net/hashcat/
GhostPack	https://github.com/GhostPack
DCOM objects for lateral movement	https://www.cybereason.com/blog/dcom-lateral-movement-techniques
Mimikatz	https://github.com/gentilkiwi/mimikatz
PowerUp	https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1
PowerView	https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1
WMIOps	https://github.com/ChrisTruncer/WMIOps/