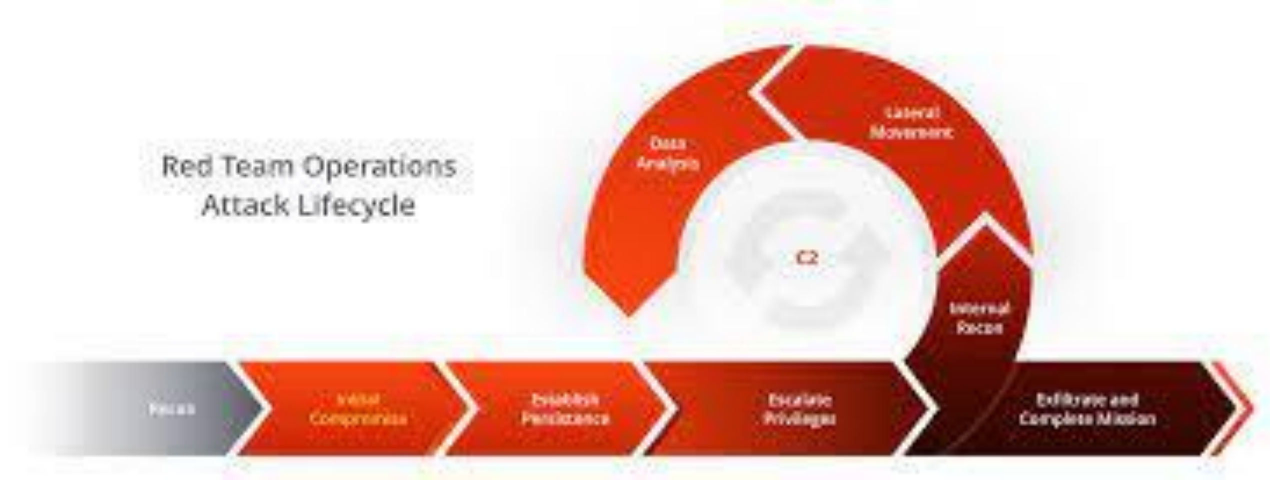
RED TEAM OPERATIONS – OVERVIEW PT.1

JOAS ANTONIO

Details

- This book is just an overview of Red Team techniques based on materials from books and courses

RED TEAM CONCEPTS



WHAT IS RED TEAM?

- O Red Team é formado com o objetivo de realizar testes de ciberataque na empresa. Estamos falando de profissionais com alto conhecimento sobre as principais ameaças e ataques existentes, sendo capazes de simular tentativas de penetrar na rede e ou sistemas. Com isso, eles se tornam capazes de identificar vulnerabilidades e, consequentemente, eliminá-las.

WHAT IS RED TEAM?

- The Red Team is formed with the objective of carrying out cyberattack tests in the company. We are talking about professionals with high knowledge about the main threats and attacks that exist, being able to simulate attempts to penetrate the network and / or systems. As a result, they are able to identify vulnerabilities and, consequently, eliminate them.

COMMAND AND CONTROL

- Os ataques maliciosos à rede aumentaram na última década. Um dos ataques mais prejudiciais, geralmente executado por DNS, é realizado por meio de comando e controle, também chamado de C2 ou C&C.

- O invasor começa infectando um computador, que pode estar atrás de um firewall. Isto pode ser feito de diversas maneiras:
  - Por meio de um e-mail de phishing que engana o usuário para seguir um link para um site malicioso ou abrir um anexo que executa um código malicioso.
  - Por meio de falhas de segurança nos plug-ins do navegador.
  - Por meio de outro software infectado.

- Uma vez que a comunicação é estabelecida, a máquina infectada envia um sinal ao servidor do invasor, procurando sua próxima instrução. O computador infectado executa os comandos do servidor C2 do invasor e pode instalar software adicional. O invasor agora tem controle total do computador da vítima e pode executar qualquer código. O código malicioso normalmente se espalha para mais computadores, criando um botnet - uma re

COMMAND AND CONTROL

- is accomplished through command and control, also called C2 or C&C.
- The attacker starts by infecting a computer, which may sit behind a firewall. This can be done in a variety of ways:
  - Via a phishing email that tricks the user into following a link to a malicious website or opening an attachment that executes malicious code.
  - Through security holes in browser plugins.
  - Via other infected software.
- Once communication is established, the infected machine sends a signal to the attacker's server looking for its next instruction. The infected computer will carry out the commands from the attacker's C2 server and may install additional software. The attacker now has complete control of the victim's computer and can execute any code. The malicious code will typically spread to more computers, creating a botnet – a network of infected machines. In this way, an attacker who is not authorized to access a company's network can obtain full control of that ne

C2 FRAMEWORK

- Uma estrutura C2 fornece aos operadores do Red Team um meio de interagir com os sistemas comprometidos alavancando ferramentas pós-exploração para avançar níveis maiores. O mais útil é o frameworks que não só têm recursos integrados, mas também permitem que os operadores tragam seus próprios ferramentas na estrutura.

C2 FRAMEWORK

- A C2 framework provides red team operators with a means of interacting with compromised systems and leveraging post-exploitation tools to further their engagements. The most useful frameworks not only have features built-in but also allow operators to bring their own custom tooling into the framework.

RED TEAM INFRAESTRUCTURE

- https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki
- Ao projetar uma infraestrutura de Red Team que precisa resistir a uma resposta ativa ou durar por um envolvimento de longo prazo (semanas, meses, anos), é importante segregar cada ativo com base na função. Isso fornece resiliência e agilidade contra o Blue Team quando os ativos da campanha começam a ser detectados. Por exemplo, se um e-mail de phishing de avaliação for identificado, o Red Team só precisará criar um novo servidor SMTP e servidor de hospedagem do payload, em vez de uma configuração de servidor de equipe inteira.

RED TEAM INFRAESTRUCTURE

- https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki
- When designing a red team infrastructure that needs to stand up to an active response or last for a long-term engagement (weeks, months, years), it’s important to segregate each asset based on function. This provides resilience and agility against the Blue Team when campaign assets start getting detected. For example, if an assessment’s phishing email is identified, the Red Team would only need to create a new SMTP server and payload hosting server, rather than a whole team se

RED TEAM PRACTICE

INITIAL COMPROMISSE - PHISHING

- https://github.com/ZeroPointSecurity/PhishingTemplates
- https://github.com/Arno0x/EmbedInHTML
- https://github.com/trustedsec/social-engineer-toolkit
- https://github.com/enigma0x3/Generate-Macro

INITIAL COMPROMISSE - PHISHING

- https://github.com/fireeye/ReelPhish/
- https://github.com/securestate/king-phisher
- https://github.com/gophish/gophish
- https://github.com/kgretzky/evilginx2

INITIAL COMPROMISSE – PASSWORD SPRAY

- https://github.com/Greenwolf/Spray
- https://github.com/dafthack/DomainPasswordSpray
- https://github.com/byt3bl33d3r/SprayingToolkit
- https://github.com/xFreed0m/RDPassSpray
- https://github.com/0xZDH/o365spray

INITIAL COMPROMISSE – RECONNAISSANCE

- https://github.com/GhostPack/Seatbelt
- https://github.com/darkoperator/dnsrecon
- https://github.com/maurosoria/dirsearch
- https://github.com/1N3/Sn1per
- https://github.com/helviojunior/turbosearch

INITIAL COMPROMISSE – RECONNAISSANCE

- https://github.com/SpiderLabs/social_mapper
- https://github.com/xillwillx/skiptracer
- https://github.com/ElevenPaths/FOCA
- https://github.com/laramies/metagoofil
- https://github.com/smicallef/spiderfoot

UACME Bypass

- https://github.com/hfiref0x/UACME
- https://attack.mitre.org/techniques/T1548/002/
- https://pentestlab.blog/2017/06/09/uac-bypass-sdclt/

Local Privilege Escalation

- https://github.com/SecWiki/windows-kernel-exploits
- https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1
- https://github.com/rsmudge/ElevateKit
- https://github.com/rasta-mouse/Sherlock
- https://github.com/rasta-mouse/Watson
- https://github.com/0xbadjuju/Tokenvator
- https://github.com/GhostPack/SharpUp
- https://github.com/gentilkiwi/mimikatz/wiki
- https://github.com/GhostPack/Rubeus
- https://github.com/TheWover/donut
- https://github.com/ZeroPointSecurity/ProcessInjection

LATERAL MOVEMENT

- https://www.ired.team/offensive-security/lateral-movement/t1047-wmi-for-lateral-movement
- https://posts.specterops.io/offensive-lateral-movement-1744ae62b14f
- https://redcanary.com/blog/lateral-movement-winrm-wmi/
- https://github.com/Mr-Un1k0d3r/PowerLessShell
- https://github.com/byt3bl33d3r/CrackMapExec
- https://github.com/vysec/ANGRYPUPPY
- https://github.com/BloodHoundAD/SharpHound
- https://github.com/PowerShellMafia/PowerSploit
- https://github.com/dafthack/MailSniper
- https://github.com/jaredhaight/PSAttack
- https://github.com/api0cradle/LOLBAS
- https://github.com/AlsidOfficial/WSUSpendu

C2 and C3

- https://www.thec2matrix.com/
- https://www.cobaltstrike.com/help-spear-phish
- https://blog.cobaltstrike.com/2014/12/17/whats-the-go-to-phishing-technique-or-exploit/
- https://www.youtube.com/watch?v=2QotQ3SCOcI&ab_channel=RedTeamVillage
- https://www.youtube.com/watch?v=KYCzakkmHqo&ab_channel=RedTeamVillage
- https://www.snaplabs.io/insights/covenant-c2-for-red-teaming
- https://docs.google.com/spreadsheets/d/1b4mUxa6cDQuTV2BPC6aA-GR4zGZi0ooPYtBe4IgPsSc/edit#gid=0
- https://github.com/FSecureLABS/C3
- https://attack.mitre.org/techniques/T1095/

REVERSE PORT

- https://blog.devolutions.net/2017/3/what-is-reverse-ssh-port-forwarding#:~:text=Reverse%20SSH%20Port%20Forwarding%20specifies,firewall%20from%20the%20outside%20world.
- https://medium.com/stolabs/reverse-port-forward-added-to-covenant-498f3c1836c4

KERBEROS

- https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Active%20Directory%20Attack.md#ms14-068-microsoft-kerberos-checksum-validation-vulnerability
- https://book.hacktricks.xyz/pentesting/pentesting-kerberos-88
- https://pentestlab.blog/tag/kerberos/
- https://adsecurity.org/?p=230
- https://github.com/blackc03r/OSCP-Cheatsheets/blob/master/offensive-security-experiments/active-directory-kerberos-abuse/kerberos-golden-tickets.md
- https://github.com/bryant-treacle/Kerberos_Golden_Ticket_Finder
- https://www.qomplx.com/qomplx-knowledge-golden-ticket-attacks-explained/
- https://adsecurity.org/?tag=goldenticket
- https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/kerberos-golden-tickets

KERBEROS

- https://adsecurity.org/?p=2011
- https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/kerberos-silver-tickets
- https://blog.varonis.com.br/kerberos-attack-silver-ticket-edition/
- https://medium.com/@mohnishdhage/how-to-get-a-reverse-shell-from-golden-silver-ticket-without-metasploit-52a9fc279e32
- https://www.youtube.com/watch?v=jVqKVdBYPp0&ab_channel=AnkitJoshi
- https://www.youtube.com/watch?v=f6SleGakcE0&ab_channel=StealthbitsnowpartofNe

DCSYNC

- https://attack.stealthbits.com/privilege-escalation-using-mimikatz-dcsync
- https://www.qomplx.com/kerberos_dcsync_attacks_explained/
- https://adsecurity.org/?p=1729
- https://attack.mitre.org/techniques/T1003/006/
- https://github.com/carlospolop/hacktricks/blob/master/windows/active-directory-methodology/dcsync.md
- https://github.com/shellster/DCSYNCMonitor

MSSQL

- https://www.darkoperator.com/blog/2009/11/27/attacking-mssql-with-metasploit.html
- https://www.tarlogic.com/en/blog/red-team-tales-0x01/
- https://book.hacktricks.xyz/pentesting/pentesting-mssql-microsoft-sql-server
- https://pentestlab.blog/2013/03/18/penetration-testing-sql-servers/

EXTRA

- https://www.paloaltonetworks.com/cyberpedia/command-and-control-explained.
- https://www.strongsecurity.com.br/blog/blue-team-e-red-team-entenda-o-que-sao-e-a-importancia-de-cada-um/
- https://github.com/S1ckB0y1337/Active-Directory-Exploitation-Cheat-Sheet
- https://github.com/dcsync
- https://github.com/balaasif6789/AD-Pentesting
- https://github.com/SofianeHamlaoui/Pentest-Notes
- https://github.com/swisskyrepo/PayloadsAllTheThings
- https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki
- https://github.com/yeyintminthuhtut/Awesome-Red-Teaming#-initial-access
- https://github.com/infosecn1nja/Red-Teaming-Toolkit
- https://drive.google.com/drive/u/0/folders/12Mvq6kE2HJDwN2CZhEGWizyWt87YunkU = Material Extras