RED TEAM OPERATIONS – OVERVIEW PT.2

JOAS ANTONIO

Details

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

- My LinkedIn: https://www.linkedin.com/in/joas-antonio-dos-santos/

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.

WHAT IS RED TEAM?

Red Teaming is the process of using tactics, techniques, and procedures (TTPs) to emulate real-world threats to train and measure the effectiveness of the people, processes, and technology used to defend environments. Built on the fundamentals of penetration testing, Red Teaming uses a comprehensive approach to gain insight into an organization's overall security to test its ability to detect, respond to, and recover from an attack. When properly conducted, Red Team activities significantly improve an organization's security controls, help hone defensive capabilities, and measure the effectiveness of security operations.

The Red Team concept requires a different approach from a typical security testing and relies heavily on well-defined TTPs, which are critical to successfully emulating a realistic threat or adversary. Red Team results exceed a typical list of penetration test vulnerabilities, provide a deeper understanding of how an organization would perform against an actual threat, and identify where security strengths and weaknesses exist. Whether you support a defensive or offensive role in security, understanding how Red Teams can be used to improve security is extremely valuable. Organizations spend a great deal of time and money on the security of their systems, and it is critical to have professionals who can effectively and efficiently operate them. This book will provide you with the skills to manage and operate a Red Team, conduct Red Team engagements, and understand the role of a Red Team and its importance in security testing.

RED TEAM CHALLENGE

Red Teaming provides a means to challenge and test conventional wisdom and thought. A few standard methods to apply Red Teaming scenarios are:

Tabletop exercises – An activity where key individuals walk through a simulated situation to answer "what if" questions. Actual technical testing does not occur. Discussions of potential outcomes are explored and examined in an open discussion format.
Physical attacks – An attack on a physical resource, such as a facility or building, to test scenarios based on attack paths involving physical assets.
Human attacks – An attack that involves social engineering and the manipulation of people to achieve Red Team goals.
Cyber exercises – A Red vs. Blue exercise designed to train or evaluate staff and security operation defenses. Exercises can range from a focuses offensive threat scenario to a full Red vs. Blue war game.
Full-scale cyber operation – The most realistic attack an organization can endure outside of an attack from a real threat. The elements of the operation collectively assess all aspects of a specific scenario. The scenario drives the need and may leverage physical, human, and cyber weaknesses to accomplish desired objectives.

RED TEAM SPECIFIC GOALS

These goals may include compromising an application or network, stealing data, emulating a specific target, measuring the effectiveness of technical defenses, measuring the effectiveness of a security team, etc. The vulnerabilities and weaknesses identified during an assessment may need to be addressed and mitigated, but this is not the focus of Red Teaming. Red Teaming focuses on the bigger picture by providing insight into a target's detection and response capabilities. It gives understanding Mean-Time to Detect (MTTD) and Mean-Time to Recover (MTTR) from individual breaches. It exercises the relationship between its incident response and threat hunting teams by testing network defenders and their tools in ways that cannot be achieved through traditional threat intelligence, literature, or structured testing.

Measuring the effectiveness of the people, processes, and technology used to defend a network
When a Red Team uses real-world attack techniques against a target’s production network, the extent of the organization’s defenses are challenged. For example, an engagement has the goal of stealing critical data from a target. A targeted phishing attack tests the end user’s willingness to participate in an attack. The payload of the attack tests the network and host defenses against the delivery of malware and ultimately against code execution. If the attack does trigger a defensive control, the response measures the defender’s actions in identifying, responding, or stopping the attack. Red teaming provides a means to measure security operations as a whole and not only focus on technical controls.

Testing and understanding specific threats or threat scenarios

A Red Team can execute and emulate a current, new, or custom threat as part of an engagement to test or validate the effectiveness of security controls. Threat emulation scenarios distinguish red teaming from other types of security assessments and can be used to understand an organization's posture against various threats. This approach provides the means to test scenarios based on new undiscovered threats or zero-day exploits. A great example is the EternalBlue exploit.
This exploit involved remote code execution using the SMB protocol, a key protocol used in Microsoft environments. Before the exploit was known, a Red Team could have easily designed a scenario where an attacker was able to propagate over the SMB protocol to measure the impact of this type of dangerous attack. Red teams don’t need (or shouldn’t) wait for a threat to develop and attack paths. Custom scenarios are a great way to understand current and future threats. More information can be found on ExternalBlue in CVE-2017-0144.

We’ve described what Red Teams do, but let’s give them a definition to add to our common lexicon. A Red Team is an independent group that, from the perspective of a threat or adversary, explores alternative plans and operations to challenge an organization to improve its effectiveness.

Red Teams perform actions during a Red Teaming engagement outlined by the Rules of Engagement (ROE). We will discuss these rules in detail later. For now, think of them as a guide used by a Red Team as to how they should conduct actions. Red Teams are independent groups that are technically skilled and capable of executing a threat based-plan safely and professionally.

Comparison Summary

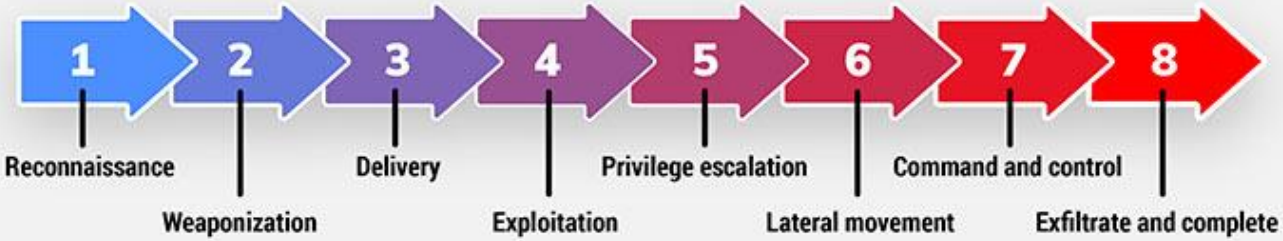
Method	Description	Goal in Terms of Risk
Penetration Test	An attack against a system, network, or application designed to identify and measure risks associated with the exploitation of a target's attack surface. **Think: Attack path validation**	Attack surface reduction
Vulnerability Assessment	An assessment used to identify the adequacy of security measures, identify security deficiencies, and confirm the mitigations are in place with the goal of reducing a target's attack surface **Think: Flaw identification**	Attack surface reduction
Red Team Engagement	The process of using Tactics, Techniques, and Procedures (TTPs) to emulate a real-world threat with the goals of training or measuring the effectiveness of the people, processes, and technology used to defend an environment. **Think: Measure security operation's capabilities as a whole**	Training and measuring the effectiveness of the people, processes, and technology (security operations)

The NIST has provided general guidance in the form of the Cybersecurity Framework for improving critical infrastructure cybersecurity. This framework provides a common taxonomy and mechanism for organizations to:

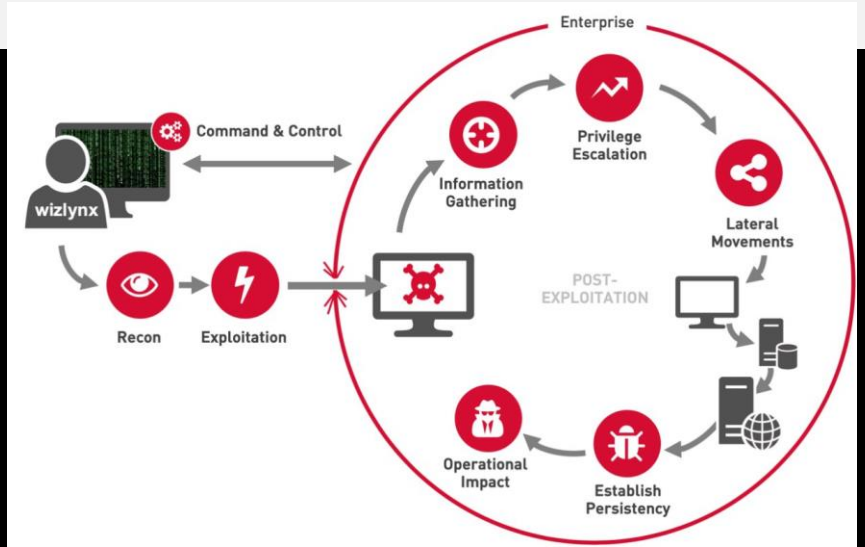
1. Describe their current cybersecurity posture
2. Describe their target state for cybersecurity
3. Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
4. Assess progress toward the target state
5. Communicate among internal and external stakeholders about cybersecurity risk

https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-components

Red Team Operations Attack Approach



SecurityTrails



Three Red Team Focus Areas

Goal: Improve Decision Making

Tasks

- Improve decisions affecting plans, operations, concepts, organizations and capabilities.
  - Identify gaps, vulnerabilities, opportunities and faulty and unstated assumptions.
  - Ensure the OE is accounted for in concepts, experiments, war games.
  - Improve planning estimates and staff synchronization of functions .

Goal: Improve Problem Solving

Tasks

- Improve problem identification, end state definition and assessment measures.
  - Think from the perspectives of partner stakeholders and others.
  - Think with a perspective on the OE.
  - Improve independent critical reviews and analysis of plans, operations, concepts, organizational designs and capabilities.

Goal: Improve Adversarial Understanding

Tasks

- Improve synchronization of intelligence with other stakeholders.
  - Think from the perspectives of adversaries and others and account for cultures and other OE variables.
  - Conduct alternative (or competitive) analyses.
  - Ensure enemy is appropriately war-gamed.

Commonality: Critical Thinking and Analysis to Challenge and Provide Alternatives

Unannounced Red Team Engagement

- The organization (especially the security operations team) does not know that an engagement is underway.

This can impact an engagement in the following ways.

- An organization will act and respond as it would on any given day. This provides very realistic results by measuring the actual posture of security operations.
- Fear of the unknown causes some organizations to react with the “sky is falling” mentality. This fear may cause unintended self-inflicted damages if policies and procedures are not followed.
- Goals and targets may not be included in the planning. When only a small number of an organization's team is part of planning, critical assets may be missed and not included in the scope. This oversight can cause an engagement to lose focus on areas that may expose an organization to considerable risk

RED TEAM TIP

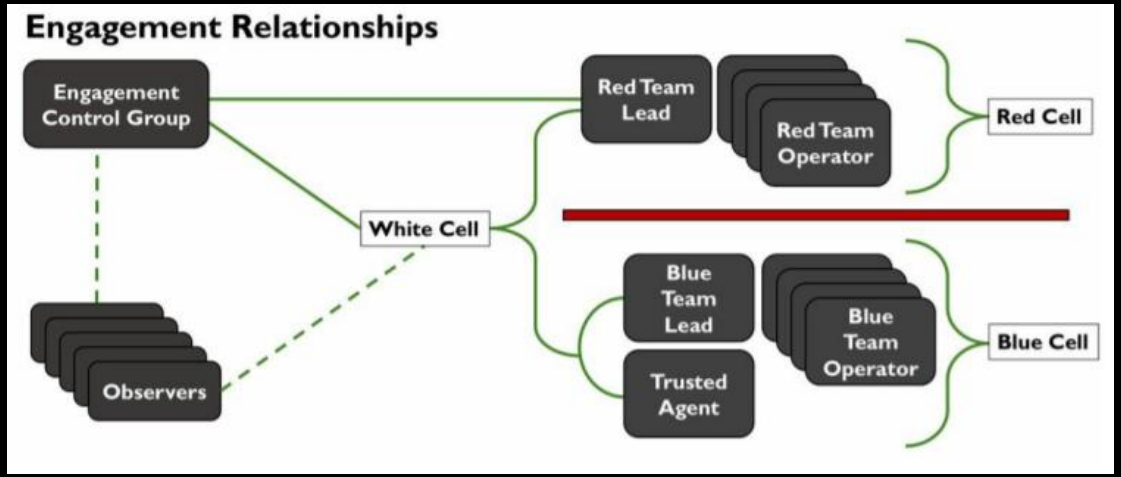
- 1) If the overall goal is to measure the effectiveness of an organization’s security operations, start the planning with an unannounced engagement. Even with the limitations, the results will be the most accurate and realistic in terms of understanding a threat’s impact
- 2) If the overall goal is to measure the effectiveness of a specific capability, tool, process, or technology, start the planning with an announced engagement. When goals are specific or targeted, including the defenders can ensure the scope and rules are adequately designed to achieve the desired results.

RED TEAM LEAD

- A Red Team should have a lead for each engagement. The lead may perform the role of the action officer, the engagement lead, an operator, the customer interface, and, often, an analyst. In general, the Red Team lead:
- Provides overall direction and guidance for the team Provides information and research data for all laws, regulations, policies, programs, and operations Provides oversight for operational planning and execution Coordinates with each of the roles within the Red Team engagement Plans and manages the budget, personnel, and equipment Provides oversight for the team calendar Provides information related to engagements, capabilities, technology, and trends Provisions training and personnel development requirements Performs a budget analysis, including equipment and travel Identifies technical research and development directions
- When planning or executing an engagement, the Red Team Lead:
- Oversees coordination with all stakeholders for the purpose of engagement execution Oversees training activities Is responsible for maintaining and coordinating logistics and the scheduling of the engagement space, time, and equipment Oversees compliance with all laws, regulations, policies, programs, and operations Is responsible for ensuring the accurate and timely completion of a final engagement report

RED TEAM OPERATOR

- Red Team operators are the individuals who execute the actions required for an engagement to meet the goals. Each Red Team operator complies with all Red Team policies and regulations under the direction of the Red Team Lead. In general, the operator:
- Executes engagement requirements as directed Complies with all laws, regulations, policies, programs, and Rules of Engagement Implements the team's operational methodology and TTPs Identifies and has input to target environment deficiencies Researches and develops new exploit and tests tools for functionality Performs Open Source Intelligence as required for the engagement Identifies and assesses actions that reveal system vulnerabilities and capabilities Assists the Red Team Lead in the development of the final engagement report Performs physical assessment support under the direction of Red Team Lead Executes operational impacts as approved by the ECG



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.

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

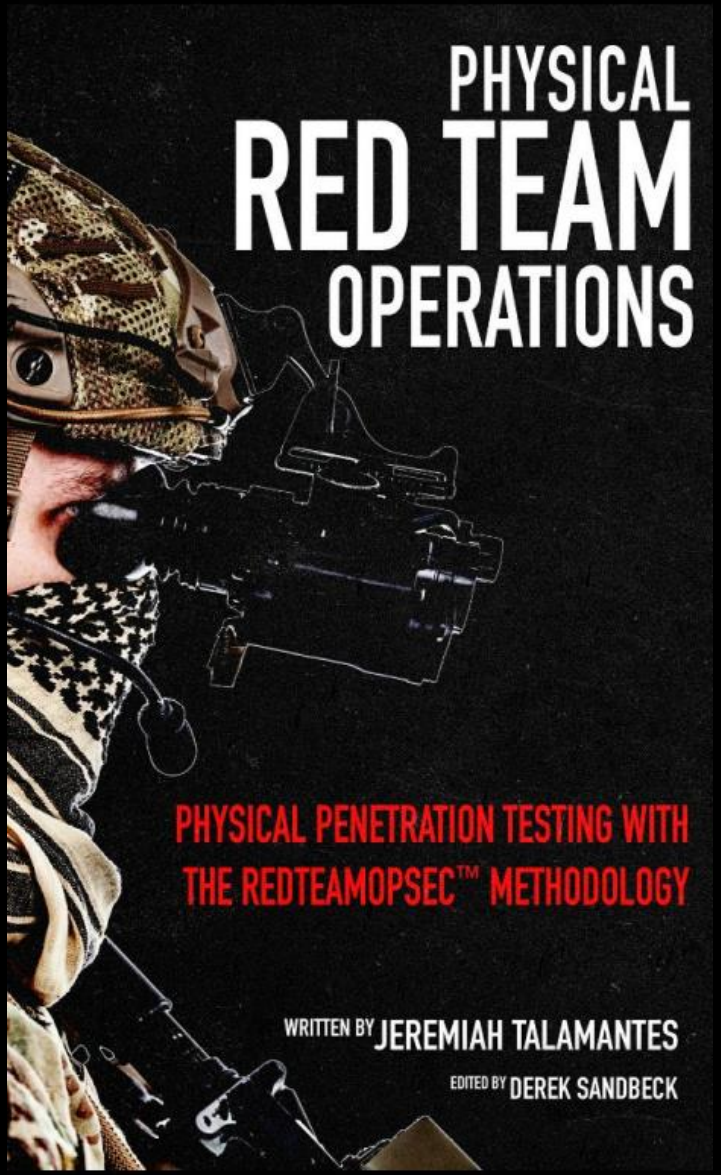
DCSYNC

- 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/

BOOKS


PHYSICAL
RED TEAM
OPERATIONS
PHYSICAL PENETRATION TESTING WITH
THE REDTEAMOPSEC™ METHODOLOGY
WRITTEN BY JEREMIAH TALAMANTES
EDITED BY DEREK SANDBECK


RED TEAM
DEVELOPMENT AND OPERATIONS
ZERO-DAY EDITION
JOE VEST & JAMES TUBBERVILLE
RED TEAM
DEVELOPMENT AND OPERATIONS
ZERO-DAY EDITION
JOE VEST & JAMES TUBBERVILLE

Red Team Operations

https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/pf/ms/ds-red-team-operations.pdf
https://www.fireeye.com/content/dam/fireeye-www/regional/pt_BR/services/pdfs/ds-red-team-operations.pdf
https://redteamvillage.org/slides/Abhijith-b-r-Diana-Initiative-Red-Team-Village-Aug2020-Tactical-Adversary-building-internal-red-team.pdf
https://www.cyberbutler.eu/cache/mandiant-red-team-operations_2211/mandiant-red-team-operations.pdf
https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/risk/ch-en-risk-red-teaming-operations.pdf
https://www2.deloitte.com/content/dam/Deloitte/jp/Documents/risk/cr/jp-cr-red-team-operations-attackers%20report%202020-2.pdf

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://github.com/yeyintminthuhtut/Awesome-Red-Teaming
- https://github.com/winterwolf32/Red-teaming
- https://github.com/mantvydasb/RedTeam-Tactics-and-Techniques
- https://github.com/akbarq/Red-Team-Operations
- https://github.com/an4kein/awesome-red-teaming
- https://github.com/sectool/redteam-hardware-toolkit
- https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki

https://drive.google.com/drive/u/0/folders/12Mvq6kE2HJDwN2CZhEGWizyWt87YunkU = Material Extras