RED TEAM ≠ PENTEST

JOAS ANTONIO

ABOUT ME

- Joas Antonio dos Santos;
- Offensive Security Research Synack Red Team;
- OWASP Project Leader;
- Red Team Leader;
- Hacking is Not a Crime Advocate;

Red Team x PenTest

two different concepts

What is PenTest

- A PenTest (Penetration Testing) or Penetration Test is a vulnerability assessment with the aim of testing a company or organization's security holes to simulate a cyber attack. Penetration testing professionals look for holes in systems to try to compromise them and try to go as far as possible, exploiting known vulnerabilities or even creating a security hole to break into a certain system.

- The need to carry out a PenTest today is very great, as with the increase of Cyberattacks all over the world, it has resulted in a race in search of the best means to protect a company's information assets* against any type of threat that may arise. , whether digitally or physically.

- The scope of a PenTest must be well designed, especially when we talk about risks that can occur in a penetration test, whether due to environment configuration errors or the use of tools that cause a lot of stress, since our main objective is to ensure the CID (Confidentiality, Integrity and Availability)

What is Red Team

- A Red Team consists of security professionals who act as adversaries to overcome cybersecurity controls.
- They use all available techniques to find weaknesses in people, processes and technology to gain unauthorized access to assets. As a result of these simulated attacks, the red team makes recommendations and plans how to strengthen an organization's security posture. Generally, a methodology widely followed by the Red Team is the Cyber Kill Chain, as it is used even within the military or in large companies that have a solid Red Team process.

Process of a PenTest

- Determine the scope of tests;
- Collect target information both passively and actively;
- Plan methods to collect and analyze the information obtained passively or actively;

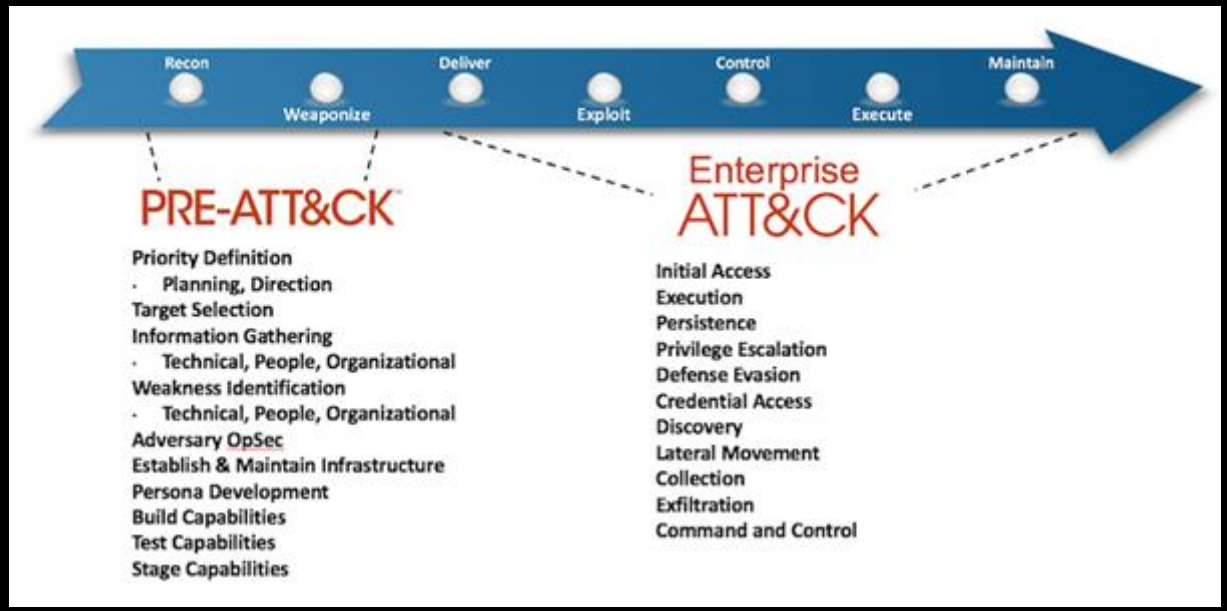
- Detect potential security breaches, either by enumerating information, collecting target port, version and service details;
- Carry out the tests by performing the exploration and post-exploitation;
- Analyze the results and generate a report;
- Test the effectiveness of remedies;

Att&ck Miter

- MITER introduced ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) in 2013 as a way to describe and classify enemy behaviors based on real-world observations. The ATT&CK is a structured list of known aggressor behaviors, which have been compiled into tactics and techniques and expressed in various matrices as well as via STIX/TAXII. Because this list is a comprehensive representation of attackers' behaviors when compromising networks, it is useful for various offensive and defensive analyses, representations, and other mechanisms.

- In addition to being very useful for the Red Team when validating a threat or even simulating an attack on your organization. Especially if in that period there are attacks linked to APT groups that are specifically targeting a specific system or technology. So Miter Att&ck brings details of how the attackers are acting and so the Red Team validates the techniques used to assist in the implementation of security controls with the Blue Team.

Miter Att&ck – PRE and ENTERPRISE



Red Team Operator

Red Team Operators are the individuals who take the actions necessary to accomplish engagement goals. Each Red Team operator complies with all Red Team policies and regulations under the direction of the Red Team Leader.

In general, the operator:

- Executes contracting requirements as indicated
- Complies with all laws, regulations, policies, programs and Rules of Engagement
- Implements team operational methodology and TTPs
- Identifies and has information to address deficiencies in the environment
- Research and develop new explore and test tools for functionality
- Performs open source intelligence as needed for engagement
- Identifies and evaluates actions that reveal system vulnerabilities and capabilities
- Assists the Red Team Lead in the development of the final report of the work
- Conducts physical assessment support under the direction of the Red Team Leader
- Executes operational impacts as approved by the ECG

Red Team Lead

A Red Team Lead must have a lead for each engagement. The lead can play the role of the action official, the job leader, an operator, the customer interface, and oftentimes, an analyst. In general the Red Team Lead:

- Provides overall direction and guidance to the team
- Provides research information and data for all laws, regulations, policies, programs and operations
- Provides oversight for operational planning and execution
- Coordinates with each of the roles within Red Team involvement
- Plans and manages budget, personnel and equipment
- Provides oversight for the team calendar
- Provides information related to appointments, resources, technology and trends
- Provides staff training and development requirements
- Conducts budget analysis, including equipment and travel Identifies technical research and development directions

TTPS

TTPs help establish the attribution of an adversary group, aiding in the maturing of what they are after. For example, the objective could be to gather policies and, based on classified information, be used for cyber warfare. Potential targets are also identified based on past targets seen in the campaign, as well as potential future targets (eg policy personnel responsible for areas in Asia). TTPs also help identify a common attack vector – email with an Office attachment containing a first stage and payload, such as a downloader. This helps position you for ongoing campaign attacks such as revising and changing policy related to Windows Data Execution Prevention (DEP); using Sandboxies as a virtualized application layer for the endpoint to open suspicious files; a review of potential endpoint protection solutions, and so on. This hyper-focus on known and potential campaign targets helps IT and security proactively protect against attacks and minimize damage (should an incident occur) through threat hunting exercises and additional forensic investigation.

PenTest vs Red Teams

Penetration Tests	Red Teams
Methodical Security Assessments: • Pre-engagement Interactions • Intelligence Gathering • Vulnerability Analysis • Exploitation • Post Exploitation • Reporting	Flexible Security Assessments: • Intelligence Gathering • Initial Foothold • Persistence/Local Privilege Escalation • Local/Network Enumeration • Lateral Movement • Data Identification/Exfiltration • Domain Privilege Escalation/Dumping Hashes • Reporting
Scope: • Restrictive Scope • 1-2 Week Engagement • Generally Announced • Identify vulnerabilities	Scope: • No Rules* • 1 Week – 6 Month Engagement • No announcement • Test Blue teams on program, policies, tools, and skills *Can't be illegal…

Vulnerability Analysis vs PenTest

Characteristic	Vulnerability Assessments	Penetration Testing
Goal	Uncover known vulnerabilities across the environment	Uncover and exploit vulnerabilities to show how criminals would use them to move laterally or deeper into the environment
Scope	Wide, broad, scanning the surface	Focused, deep
Performed by	Automated tool(s) (with human oversight)	Experienced hackers
Outcome	List of vulnerabilities	Prioritized list of vulnerabilities, methodologies to exploit them, narrative walkthrough of attack scenario, remediation recommendations
Next step	Prioritize for remediation and apply patches	Apply patches and other fixes that reduce the most risk
Best for	Understanding basic level of security posture	Understanding all facets of security posture

PenTest vs Red Team

- **The PenTests**take vulnerability assessments to the next level by exploring and proving attack paths. PenTests can often look like Red Team involvement and even use some of the same tools or techniques. The main difference is in the goals and intention. The purpose of a penetration test is to execute an attack against a target system to identify and measure the risks associated with exploiting a target's attack surface. Organizational risks can be measured indirectly and are usually extrapolated from some technical attack. What about people and processes? This is where the red team comes in.

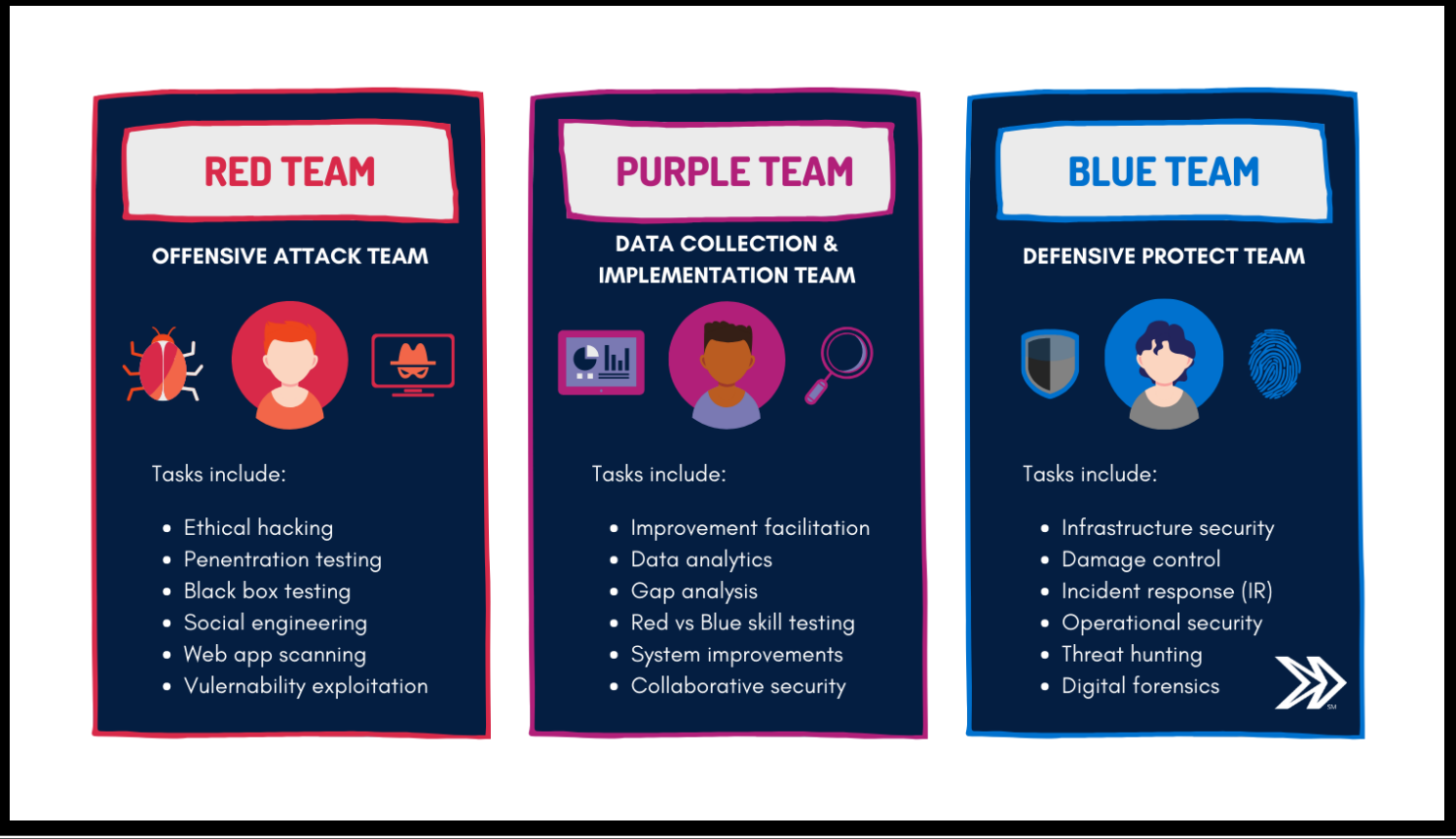
PenTest vs Red Team

- **Red Team Engagements**are scenario-based engagements driven by specific threat targets. The Red Team focuses on security operations as a whole and includes people, processes and technology. Red Team specifically focuses on goals related to training Blue Team or measuring how security operations can affect a threat's ability to operate. Technical failures are secondary to understanding how the threat was able to impact an organization's operations or how security operations were able to impact a threat's ability to operate.

Red Team

Developing an operation in practice

Red Team vs Purple Team vs Blue Team



Developing your Red Team - Home

- Pursuing budget;
- Set goals and objectives;
- Develop ROE (Rules of Engagement) model;
- Determine required knowledge and skills;
- Hiring talent in Red Team;

ROE

- The Rules of Engagement (ROE) document the approvals, authorizations, and critical implementation issues required to execute the commitment. The signature of the ROE constitutes acknowledgment and approval by the customer, system owner and Red Team from the Red Team authorities in the execution of the commitment.
- The ROE must be updated when the target space, authorized actions, objectives or scope change. For example, the original scope may be limited to computer network attacks. If physical attacks are planned, the ROE must be updated to reflect additional activities and controls. The Red Team Leader will address suggestions or adjustments to the
  ROE Each review result must be provided to the author. The final ROE must be approved by a Trusted Agent in the top management of the target environment.

Developing your Red Team - Planning

- Develop a Red Team methodology;
- Develop technical briefing model;
- Develop report template;
- Operational Impact Planning;

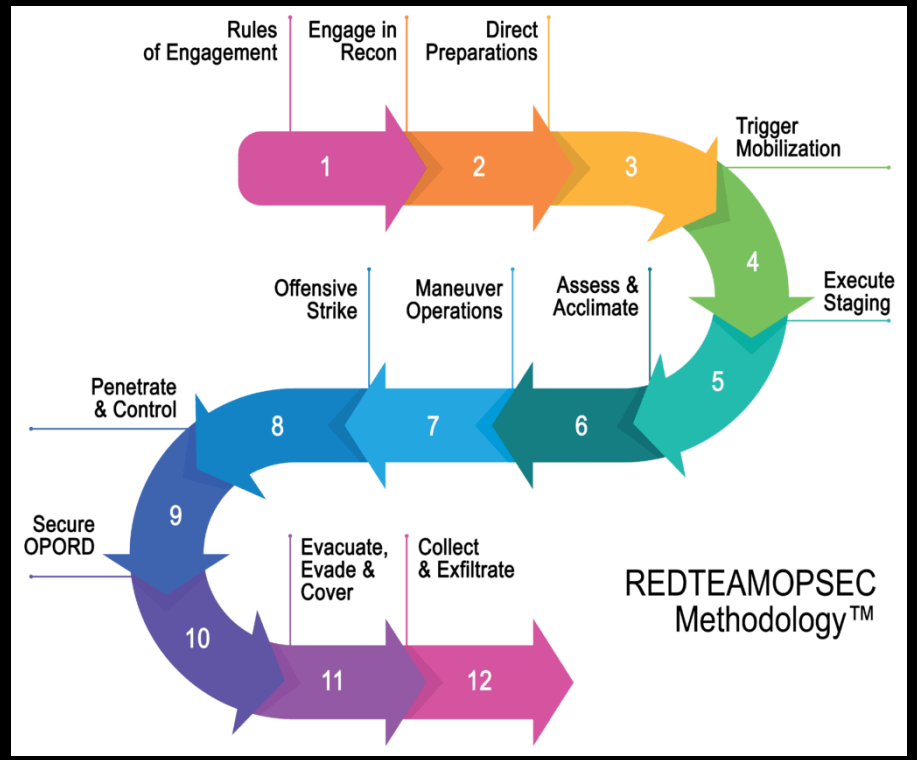
Developing Your Red Team - Execution

- Capture records;
- Capture system changes;
- Update attack diagram in real time;

Developing Your Red Team - Completion

- Engagement Closure;
- Accumulate data;
- Revert system changes;
- Executive Summary;
- Observation draft and findings;
- Finalize the attack diagram;
- Finalize report;

Red Team Methodology



TTPs and Tradecraft

- This template should be used to define general guidance on Red Team Tradecraft and TTPs. Each Red Team must have a guidance document. Keep this document updated and distributed to all Red Team members. This document is to be used to guide the Red Team actions of all Red Team operators on all engagements. Exceptions to these rules can (and will be) made based on specific Rules of Engagement (ROE) or decisions made by Red Team leaders during an engagement. Exceptions must be documented as part of the job log. It is important to use and follow this document to maintain a high quality professional Red Team.

- Add custom or specific TTP and Tradecraft Guidance to this document as needed. This includes specific or customs tools that must be used for various tasks, C2, enumeration, etc.

Do vs Don't

Fazer	Não
Registre todos os eventos significativos	Use ferramentas não testadas em um sistema de destino
Consulte os colegas	Use canais não criptografados para C2
Entenda as ferramentas e a tecnologia utilizada	Tentativa de explorar ou atacar sites não criptografados
Realize a consciência situacional	Executar a partir de locais não executáveis
Minimizar o volume de retorno de chamada (C2)	Baixar conjuntos de dados restritos
	Use binários para acesso inicial

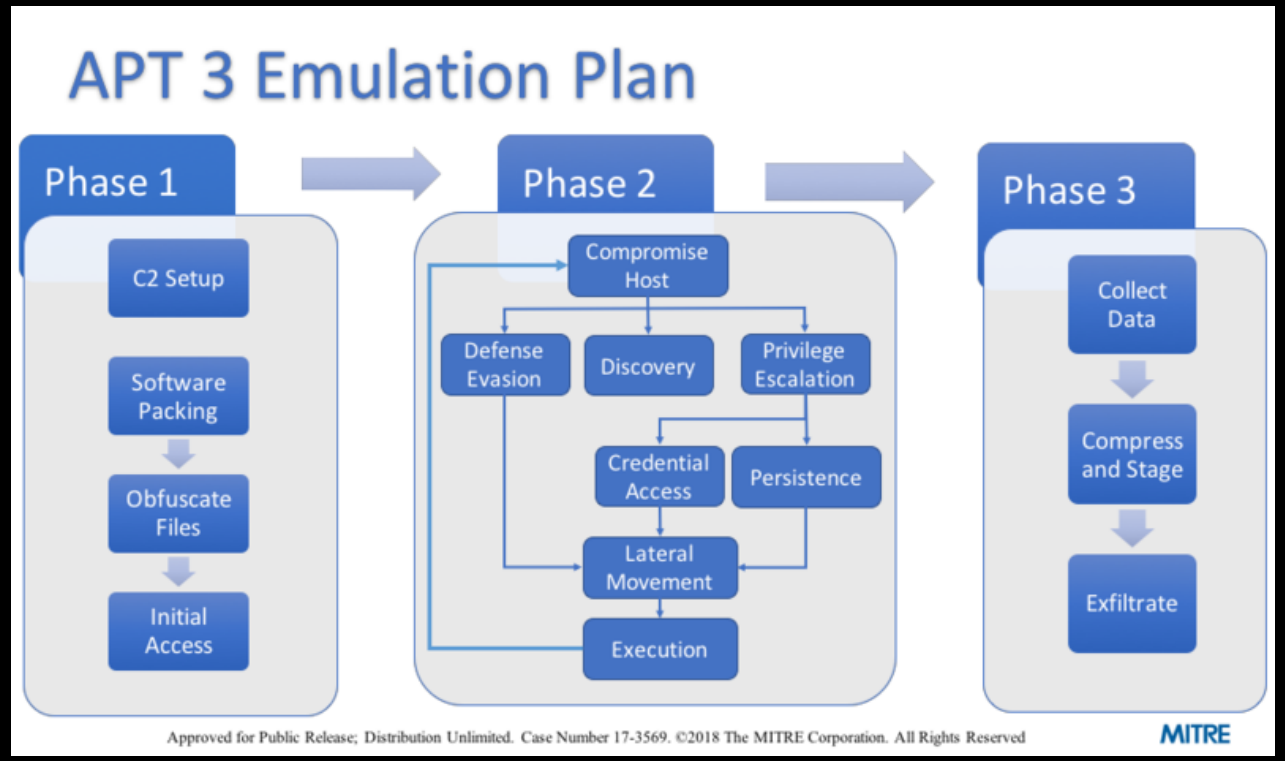
Creating a Report

- Executive Summary;
- Methodology and Objectives;
- Scenario and Scope;
- Attack Narrative;
- Critical details;
- Observations and Recommendations;

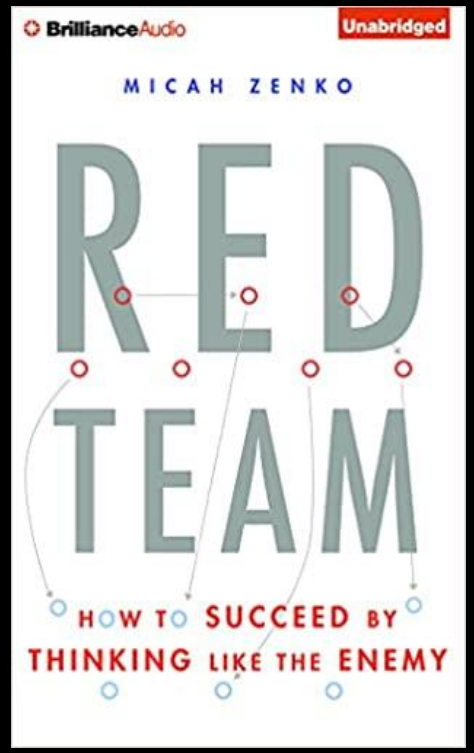
Adversary Emulation

- Adversary Emulation helps organizations focus their security testing to prioritize the threats the blue team may face every day.
- Adversary Emulation is a collaborative effort across multiple domains of cybersecurity expertise, primarily Red Team and Cyber Threat Intelligence (CTI) professionals. CTI professionals work with the security operations center (SOC) and senior leadership to determine what types of threats can hit the organization, while red teams work to test and investigate defenses. Red Teams have the craft and skill set to take malicious actions to subvert defenses, but this experience is far more valuable for organizations trying to understand the implications of Red Team's findings on their security posture when data-bound. of real-world threats.

APT 3 Emulation Plan



bedside books



CONCLUSION

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

links

- https://redteam.guide/docs/references_templates_talks/
- https://threatexpress.com/redteaming/redteamplanning/roeguide/
- https://redteam.guide/docs/Templates/roe_template/
- https://about.gitlab.com/handbook/engineering/security/security-operations/red-team/red-team-roe.html
- https://attack.mitre.org/resources/adversary-emulation-plans/
- https://www.youtube.com/watch?v=sRaLleKghrE
- https://www.youtube.com/watch?v=CXpHaY-2Fvw
- https://vulners.com/pentestit/PENTESTIT:F65D9F8AED2541BFB9D6A54086003A31
- https://hackerculture.com.br/?p=1047