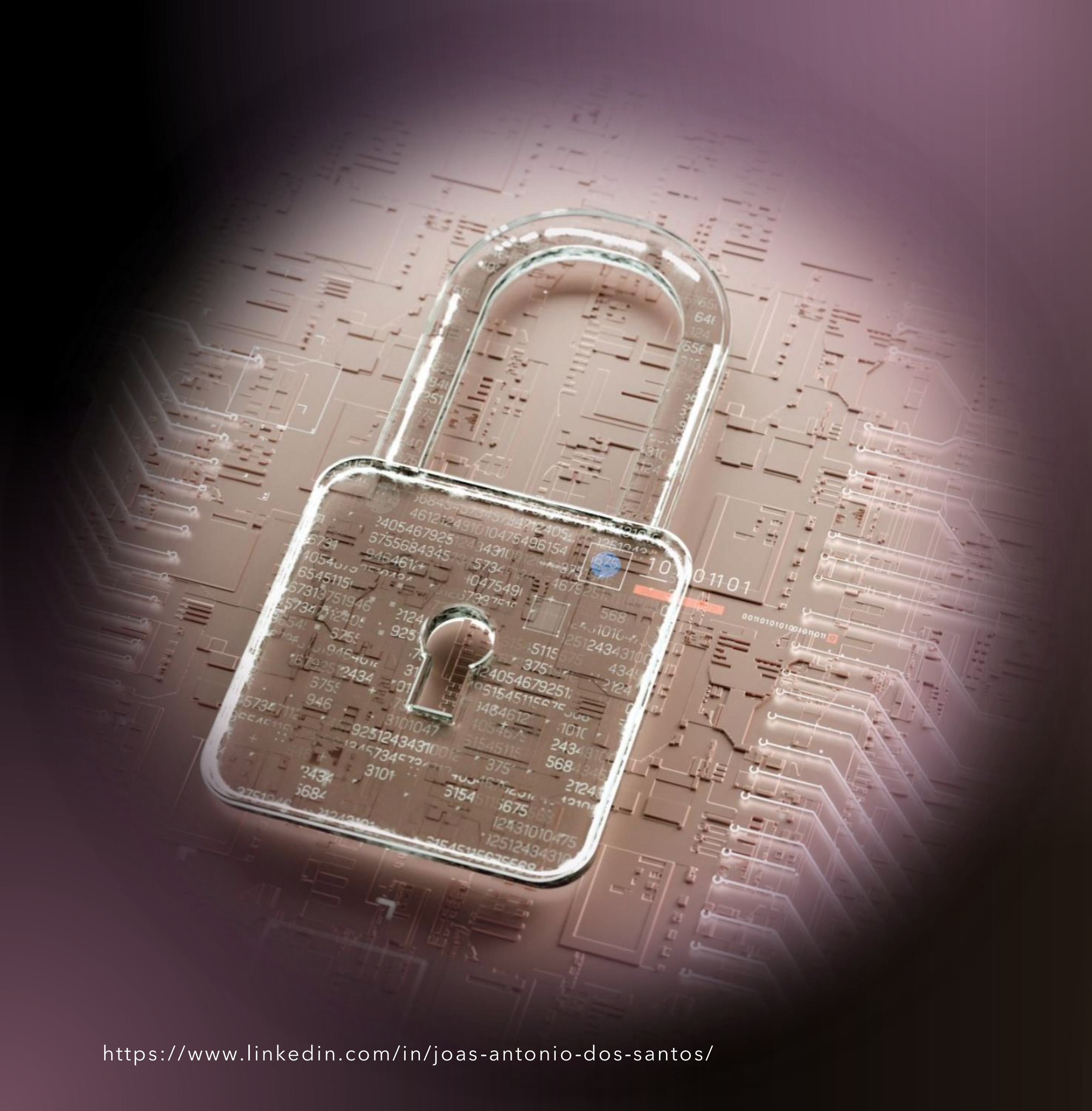


Cyber Security Complete Journey – Red Team #1

JOAS A SANTOS

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

Red Team Concept

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

What is Red Teaming

- Red teaming is the process of using Tactics, Techniques, and Procedures (TTPs) to emulate real-world threats with the goal of training and measuring the effectiveness of the people, processes, and technology used to defend an environment.
- In terms of business risk, a red team engagement focuses on understanding how well security operations deal with a threat through training or measurement. Technical findings are often revealed during an engagement but are not the focus. Red teaming engagements are designed to challenge security operation's defensive strategies and assumptions and to identify gaps or flaws in the defensive strategies. Improving security operations through training or measurement is the goal of a red teaming engagement.
- Reference: https://redteam.guide/docs/definitions#red-team

Mitre Att&ck

- MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a knowledge base that is used to describe the actions and behaviors of cyber adversaries. It provides a comprehensive and detailed mapping of the tactics, techniques, and procedures (TTPs) that attackers use to achieve their objectives throughout the cyber kill chain.
- The MITRE ATT&CK framework is organized into matrices, each representing a different platform or environment. Common matrices include ATT&CK for Enterprise, ATT&CK for Mobile, and ATT&CK for Cloud. The Enterprise matrix, for example, covers tactics and techniques relevant to traditional IT environments.
- Security professionals use MITRE ATT&CK to enhance threat intelligence, improve threat detection and response capabilities, and develop a better understanding of the behaviors and TTPs of cyber adversaries. It serves as a valuable resource for organizations aiming to improve their cybersecurity posture by aligning defenses with real-world threats.

What is TTPs

- TTPs stands for Tactics, Techniques, and Procedures. This term is commonly used in the context of cybersecurity, military operations, and intelligence to describe the behavior and methods employed by adversaries. Here's a breakdown of what each component means:
- **Tactics:** High-level plans or strategies to achieve a specific objective. In the context of cybersecurity, tactics might include goals like gaining unauthorized access, stealing data, or disrupting services.
- **Techniques:** The specific methods or ways in which tactics are executed. Techniques are more detailed than tactics and describe the actual steps or actions taken to achieve a goal. For example, a technique in cybersecurity might involve using a specific type of malware or exploiting a particular vulnerability.
- **Procedures:** The step-by-step processes or sequences followed to implement a technique. Procedures are the most granular level of TTPs and provide detailed instructions on how to carry out specific actions. In cybersecurity, this might include the specific commands used to deploy malware or exploit a system.

What is Red Team Lead

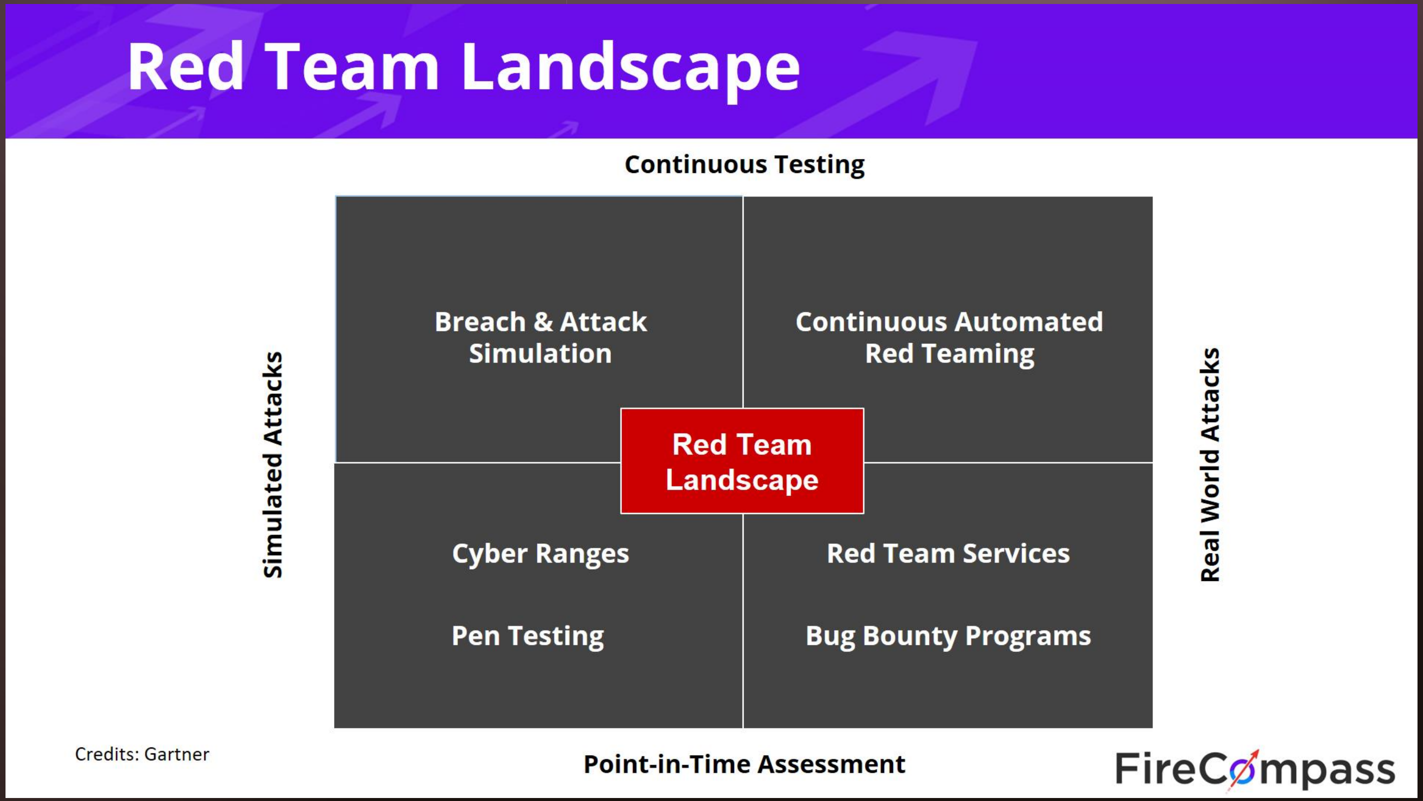
- Serves as the operational and administrative lead for the Red Team. Conducts engagement, budget, and resource management for the Red Team, Provides oversight and guidance for engagements, capabilities, and technologies. Ensures adherence to all laws, regulations, policies, and Rules of Engagement.
- Reference: https://redteam.guide/docs/definitions#red-team

What is Threat Scenario

- Scenarios provide insight into how a defensive solution will perform and conform to the processes, procedures, policies, activities, personnel, organizations, environment, threats, constraints, assumptions, and support involved in the security mission. Scenarios generally describe the role of the threat, how it will interact with the systems and networks within the target environment, and elicits real-world truth of how essential internal practices are employed. In short, it answers how the target's security operations would dynamically perform an action to deliver results, outputs, or prove capability.
- Reference: https://redteam.guide/docs/definitions#red-team

Red Team Landscape

Reference: https://www.cisoplatform.com/profiles/blogs/red-team-landscape-amp-why-red-teaming-is-crucial-for-businesses



Red Team Landscape

Continuous Testing

Simulated Attacks

Breach & Attack Simulation

Continuous Automated Red Teaming

Red Team Landscape

Cyber Ranges

Pen Testing

Red Team Services

Bug Bounty Programs

Real World Attacks

Point-in-Time Assessment

Credits: Gartner

FireCompass

Red Team Overview

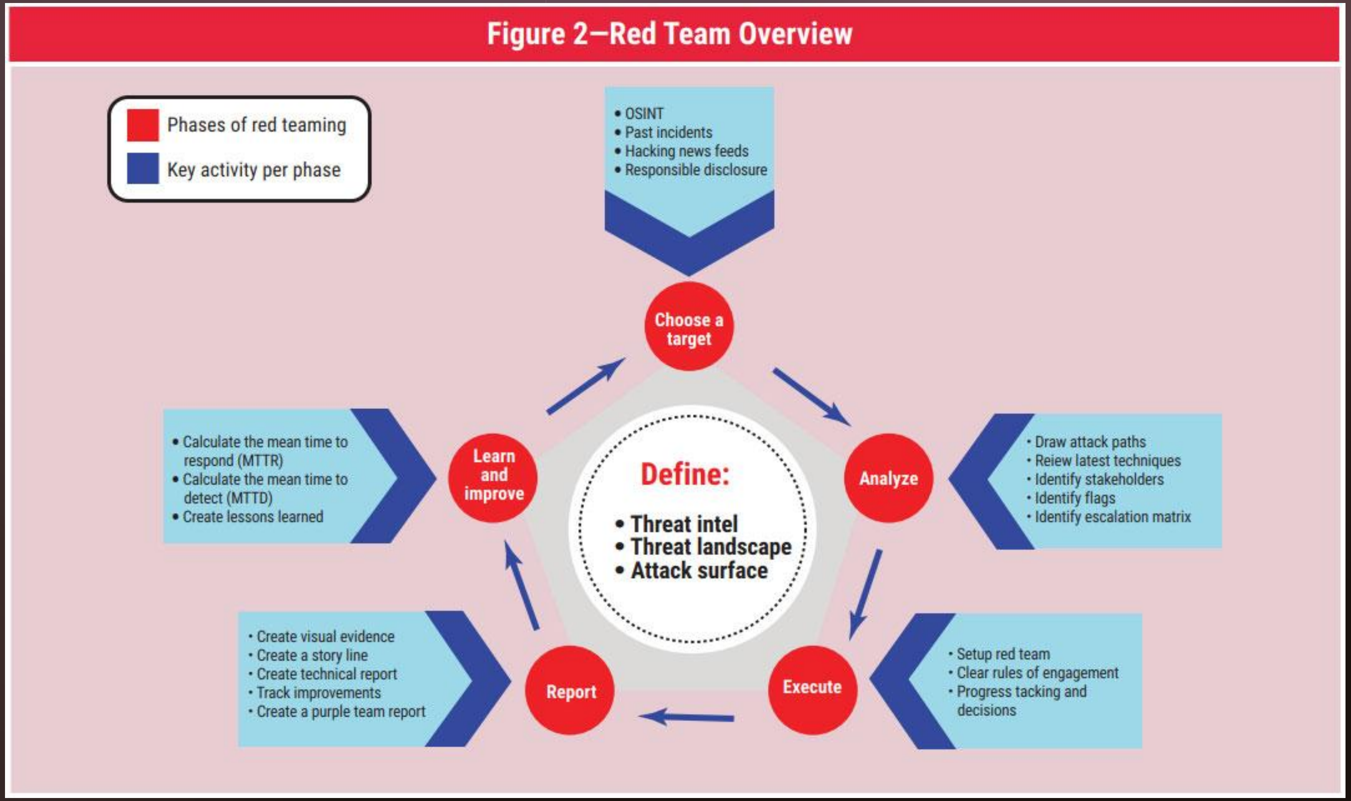
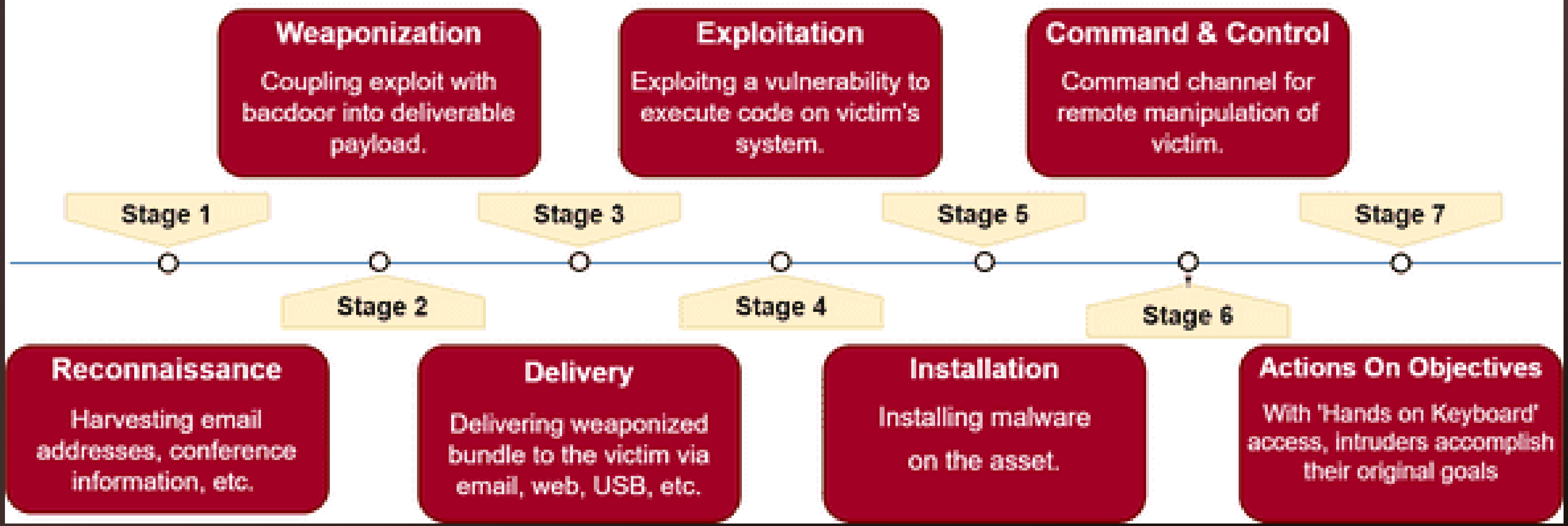


Figure 2—Red Team Overview

Reference: https://www.isaca.org/resources/isaca-journal/issues/2018/volume-5/red-teaming-for-cybersecurity

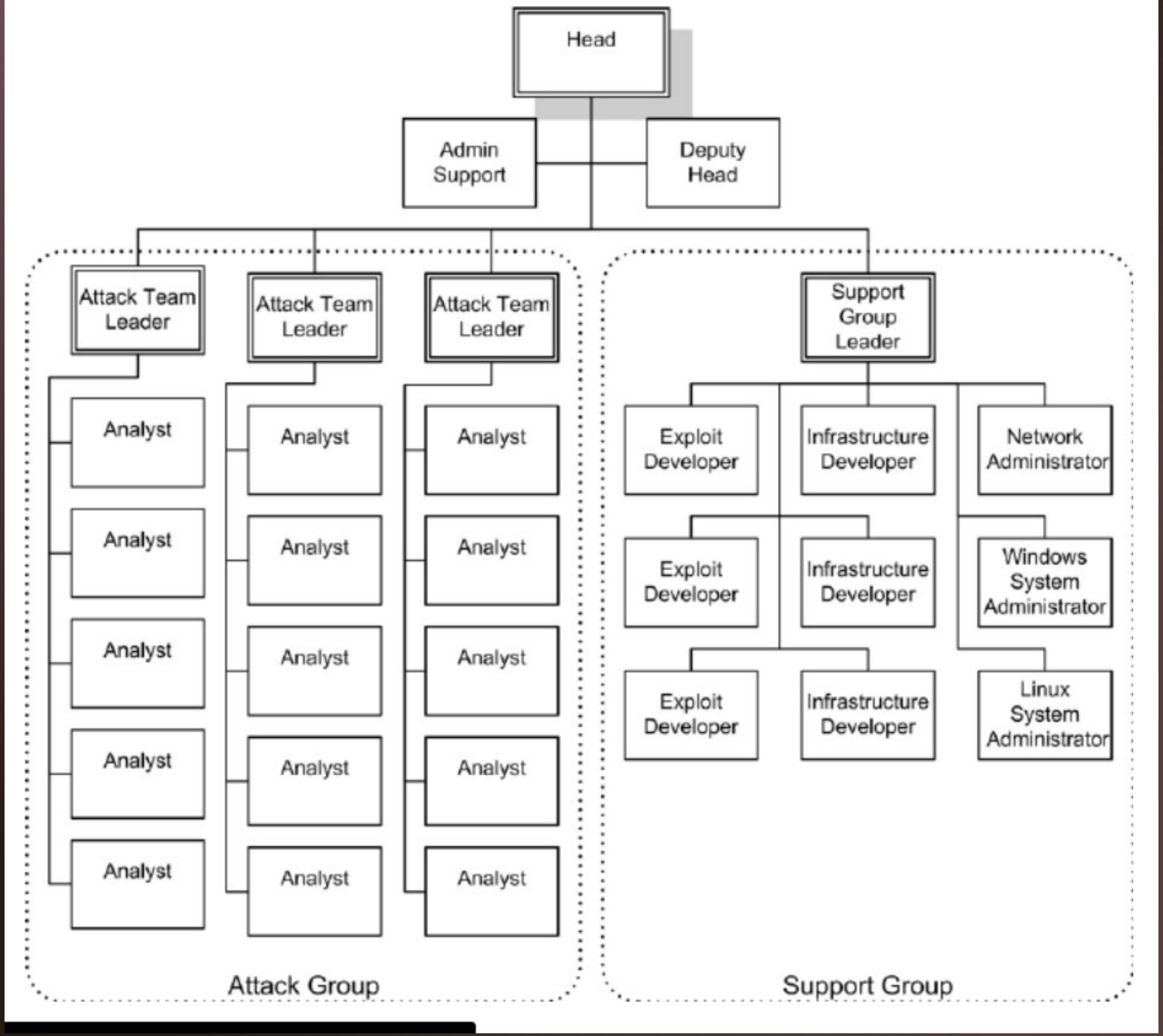
Cyber Kill Chain



Stage 1
Reconnaissance
Harvesting email addresses, conference information, etc.
Stage 2
Weaponization
Coupling exploit with bacdoor into deliverable payload.
Stage 3
Delivery
Delivering weaponized bundle to the victim via email, web, USB, etc.
Stage 4
Exploitation
Exploitng a vulnerability to execute code on victim's system.
Stage 5
Installation
Installing malware on the asset.
Stage 6
Command & Control
Command channel for remote manipulation of victim.
Stage 7
Actions On Objectives
With 'Hands on Keyboard' access, intruders accomplish their original goals

Reference: https://www.prplbx.com/resources/blog/what-is-red-teaming/

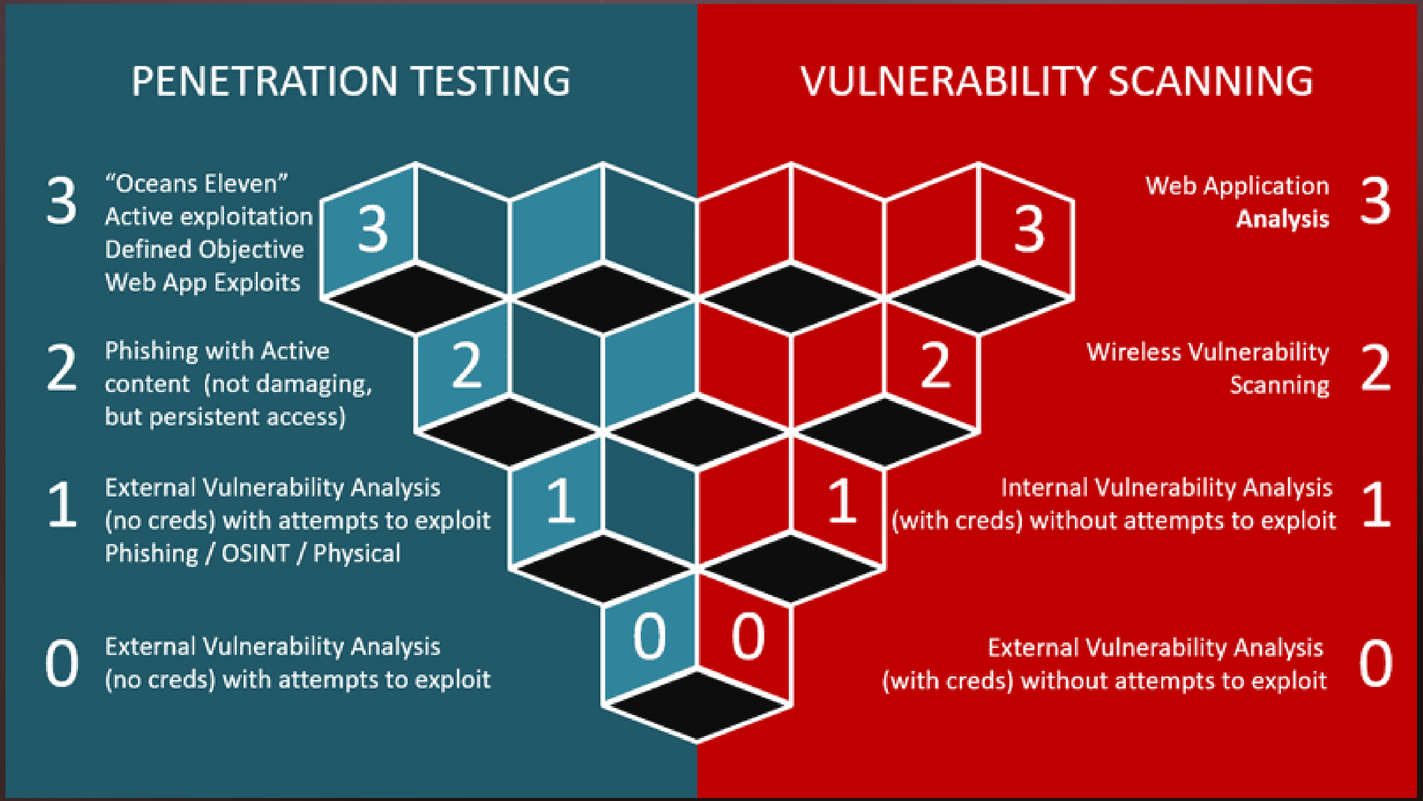
Red Team Structure Example



Reference: https://www.researchgate.net/figure/fig1_252019409

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

PenTest x Vulnerability Scanning



PENETRATION TESTING

3 “Oceans Eleven” Active exploitation Defined Objective Web App Exploits

2 Phishing with Active content (not damaging, but persistent access)

1 External Vulnerability Analysis (no creds) with attempts to exploit Phishing / OSINT / Physical

0 External Vulnerability Analysis (no creds) with attempts to exploit

VULNERABILITY SCANNING

Web Application Analysis 3

Wireless Vulnerability Scanning 2

Internal Vulnerability Analysis (with creds) without attempts to exploit 1

External Vulnerability Analysis (with creds) without attempts to exploit 0

Reference: https://privasec.com/blog/red-teaming-penetration-testing/

PenTest Methodology

- There are several penetration testing methodologies that cybersecurity professionals can follow when assessing the security of systems and networks. Some of the main methodologies in English include:
- OWASP Testing Guide: Published by the Open Web Application Security Project (OWASP), this guide provides comprehensive guidelines for web application security testing. It covers a wide range of topics, from information gathering to vulnerability exploitation.
- PTES (Penetration Testing Execution Standard): PTES is an initiative aimed at creating a standard for the execution of penetration tests. It covers all phases of testing, from initiation to the delivery of the final report.
- OSSTMM (Open Source Security Testing Methodology Manual): This methodology focuses on network and system security testing. It is maintained by the Institute for Security and Open Methodologies (ISECOM) and aims to be an open and collaborative approach to security testing.
- NIST SP 800-115: Published by the National Institute of Standards and Technology (NIST), this document provides guidance on conducting penetration testing on information technology systems.
- ISSAF (Information Systems Security Assessment Framework): ISSAF is a set of tools and methodologies for system security assessment. It covers various areas, from information gathering to exploitation and reporting.

Adversary Emulation

- Adversary emulation is a cybersecurity practice that involves simulating the tactics, techniques, and procedures (TTPs) of real-world adversaries to assess the effectiveness of an organization's security defenses. The goal of adversary emulation is to replicate the behaviors and actions of threat actors, such as advanced persistent threats (APTs) or other malicious actors, in order to identify and remediate vulnerabilities and weaknesses in the security infrastructure.

Key aspects of adversary emulation include:

- Realism: Emulating real-world adversaries involves replicating their behaviors as closely as possible. This includes using known TTPs and leveraging the latest threat intelligence to ensure authenticity.
- Scenario-based Testing: Adversary emulation often takes the form of scenario-based testing, where security teams simulate specific cyber threats to assess how well the organization's defenses, detection, and response capabilities perform under such conditions.
- Purple Teaming: Adversary emulation often involves collaboration between the "Red Team" (the team simulating the adversary) and the "Blue Team" (the organization's defenders). This collaborative approach, known as "Purple Teaming," aims to enhance communication and cooperation between offensive and defensive security teams.
- Continuous Improvement: Adversary emulation is not a one-time event but rather a continuous process. Organizations may regularly conduct these simulations to adapt to evolving threats and ensure that their security posture remains robust.
- Learning and Improvement: The primary purpose of adversary emulation is to identify areas for improvement in an organization's security controls, incident response procedures, and overall cybersecurity posture. It helps organizations learn more about their strengths and weaknesses and provides actionable insights for enhancing security.
- Adversary emulation goes beyond traditional penetration testing by focusing on emulating the holistic approach of real-world adversaries, including their tactics for infiltration, lateral movement, data exfiltration, and evasion techniques.

Rules of Engagement

- The Rules of Engagement establish the responsibilities, relationships, and guidelines among the Red Team, the customer, the system owner, and any stakeholders required for engagement execution.
- Reference: https://redteam.guide/docs/definitions#rules-of-engagement-roe

Command and Control

- Command and Control (C2) is the influence an attacker has over a compromised computer system that they control.
- Designing a robust C2 infrastructure involves creating multiple layers of Command and Control. These can be described as tiers. Each tier offers a level of capability and covertness. The idea of using multiple tiers is the same as not putting all your eggs in one basket. If C2 is detected and blocked, having a backup will allow operations to continue.
- C2 tiers generally fall into three categories: Interactive, Short Haul, and Long Haul. These are sometimes labeled as Tier 1, 2, or 3. There is nothing unique to each tier other than how they are to be used.

Interactive

- Used for general commands, enumeration, scanning, data exfiltration, etc.
- This tier has the most interaction and is at the greatest risk of exposure.
- Plan to lose access from communication failure, agent failure, or Blue Team actions.
- Run enough interactive sessions to maintain access. Although interactive, this doesn't mean blasting the client with packets. Use good judgment to minimize interaction just enough to perform an action.

Short haul

- Used as a backup to reestablish interactive sessions.
- Use covert communications that blend in with the target.
- Slow callback times. Callback times in the 1–24 hr. range are common.

Long haul

- The same as Short Haul but even lower and slower.
- Slow callback times. Callback times of 24+ hours are common

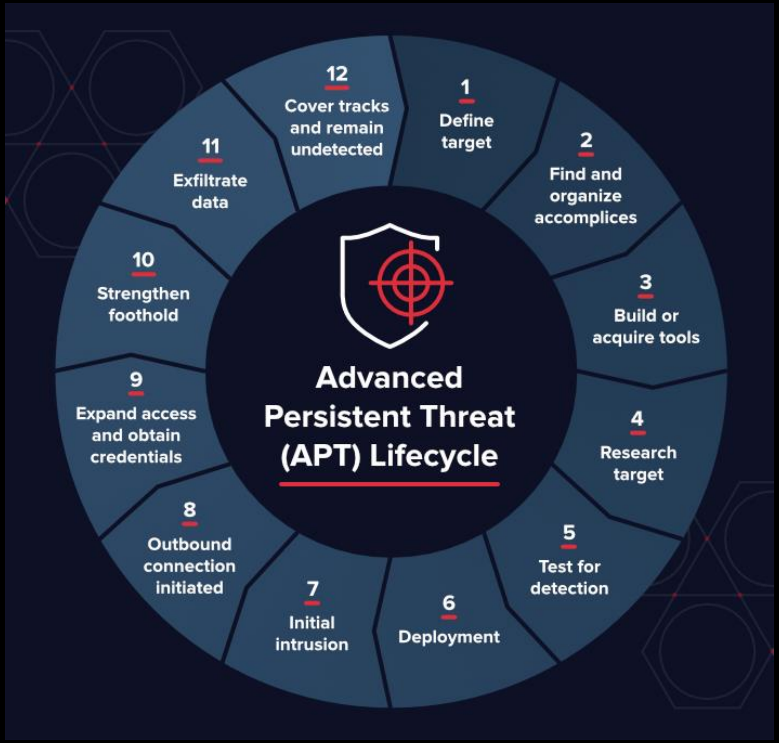
Reference: https://redteam.guide/docs/definitions#command-and-control-c2

Advanced Persistent Threat

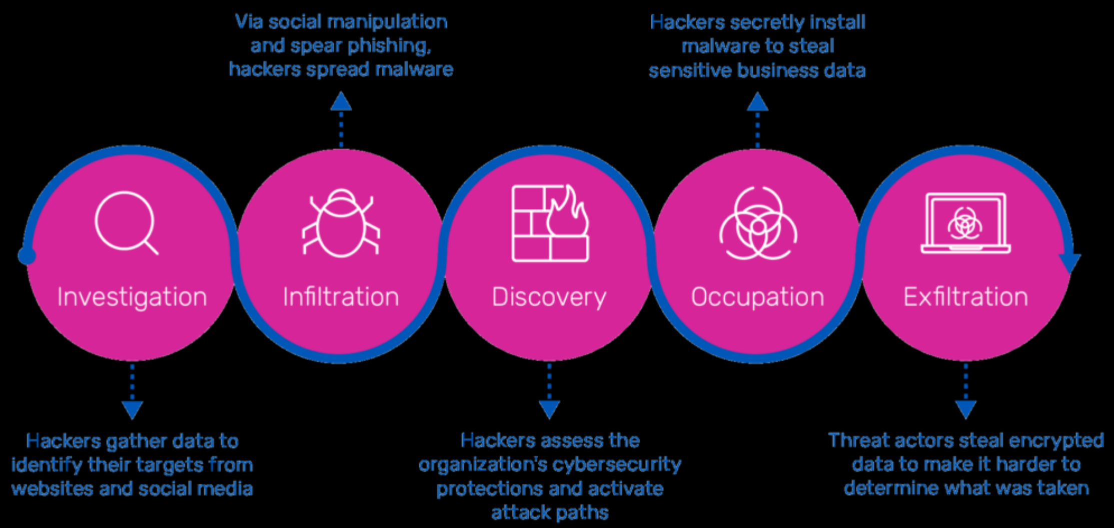
- An Advanced Persistent Threat (APT) is a sophisticated and targeted cyberattack in which an unauthorized user gains access to a network and remains undetected for an extended period. APTs are characterized by their advanced tactics, techniques, and procedures (TTPs), often employed by well-funded and organized threat actors, such as nation-states or highly skilled hacking groups.
- Key characteristics of Advanced Persistent Threats include:

1. **Persistence:** APTs are designed to remain undetected within a targeted network for an extended duration. Attackers aim to establish a long-term presence to conduct espionage, steal sensitive information, or achieve other malicious objectives.
2. **Advanced Tactics:** APTs typically involve sophisticated and advanced methods to infiltrate and navigate through a network. This can include the use of zero-day vulnerabilities, custom malware, and evasion techniques to bypass security measures.
3. **Targeted Approach:** APTs are highly focused on specific organizations, industries, or even individuals. The attackers often conduct thorough reconnaissance to understand the target's infrastructure, personnel, and security controls.
4. **Coordinated and Persistent Attacks:** APTs involve a series of coordinated and persistent attacks rather than a one-time event. Attackers may use a variety of tactics, such as social engineering, spear-phishing, and watering hole attacks, to gain initial access.
5. **Data Exfiltration:** The primary goal of many APTs is to steal sensitive information. Attackers may conduct extensive data exfiltration to obtain intellectual property, financial data, or other valuable information.
6. **Nation-State Involvement:** A significant number of APTs are attributed to nation-states or state-sponsored actors. These entities may conduct cyber espionage, cyber warfare, or economic espionage to gain a strategic advantage.

Advanced Persistent Threat



Advanced Persistent Threat (APT) Lifecycle
1 Define target
2 Find and organize accomplices
3 Build or acquire tools
4 Research target
5 Test for detection
6 Deployment
7 Initial intrusion
8 Outbound connection initiated
9 Expand access and obtain credentials
10 Strengthen foothold
11 Exfiltrate data
12 Cover tracks and remain undetected



Via social manipulation and spear phishing, hackers spread malware
Hackers secretly install malware to steal sensitive business data
Investigation
Infiltration
Discovery
Occupation
Exfiltration
Hackers gather data to identify their targets from websites and social media
Hackers assess the organization's cybersecurity protections and activate attack paths
Threat actors steal encrypted data to make it harder to determine what was taken

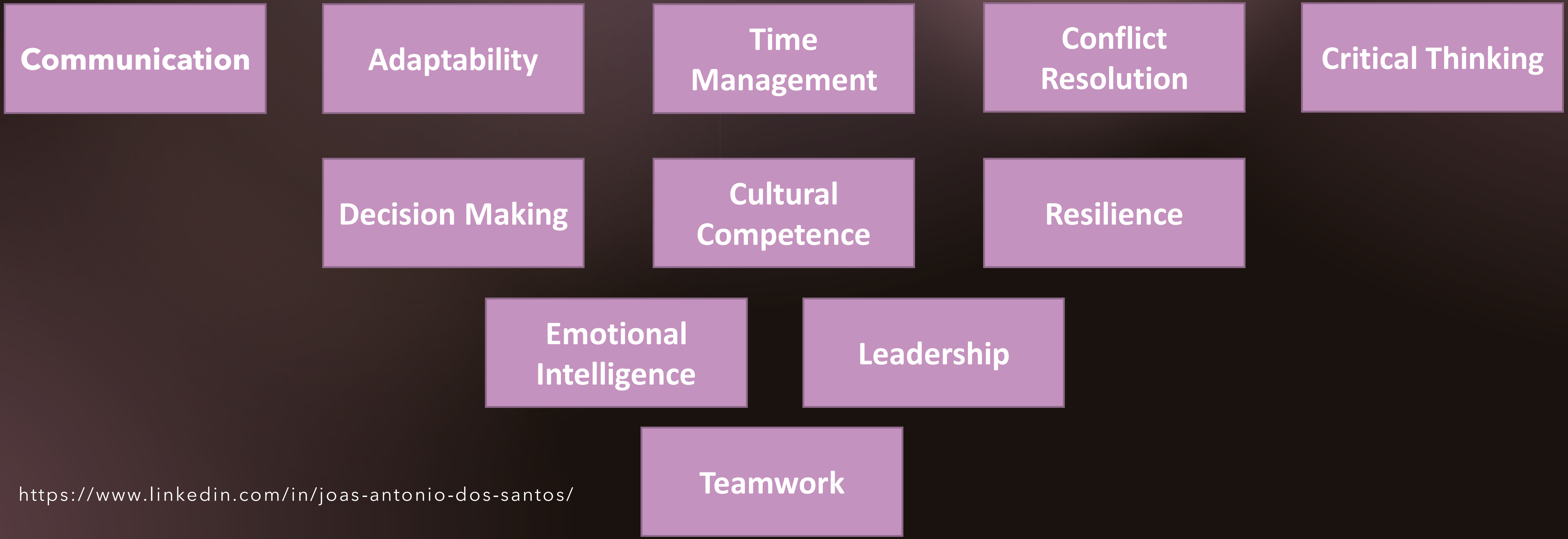
Reference: https://www.varonis.com/blog/advanced-persistent-threat

Reference: https://www.a10networks.com/glossary/what-is-an-advanced-persistent-threat/

Red Team Journey

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

Soft Skills #1



- Communication
- Adaptability
- Time Management
- Conflict Resolution
- Critical Thinking
- Decision Making
- Cultural Competence
- Resilience
- Emotional Intelligence
- Leadership
- Teamwork

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

Soft Skills #2

- In a Red Team environment, where critical assessment and simulation of adversities are essential, the importance of interpersonal skills, also known as soft skills, becomes even more evident. Effective communication is the foundation, enabling a clear exchange of information and fluid collaboration between team members. Adaptability and problem solving are crucial to facing unforeseen challenges and developing counterattack strategies.
- Managing time properly is essential for meeting deadlines and responding promptly to threats. Leadership not only guides the team, but also promotes a proactive cybersecurity culture. Empathy and conflict resolution are vital to maintaining a cohesive work environment, while critical thinking informs strategic safety decisions.
- Networking skills and cultural competence broaden the Red Team's vision, enriching the understanding of potential threats in different contexts. Creativity drives innovation in the approach to security testing, while resilience allows the team to overcome setbacks and persist in searching for vulnerabilities.
- Skilled negotiation is crucial when collaborating with other security teams and seeking effective solutions. Stress management and self-motivation ensure that Red Team members remain focused and efficient, even in extreme pressure situations. Attention to detail is essential to identify and thoroughly exploit security holes.
- Finally, emotional intelligence contributes to the subtle understanding of human and behavioral dynamics, expanding the ability to anticipate opponent movements.

Hard Skills

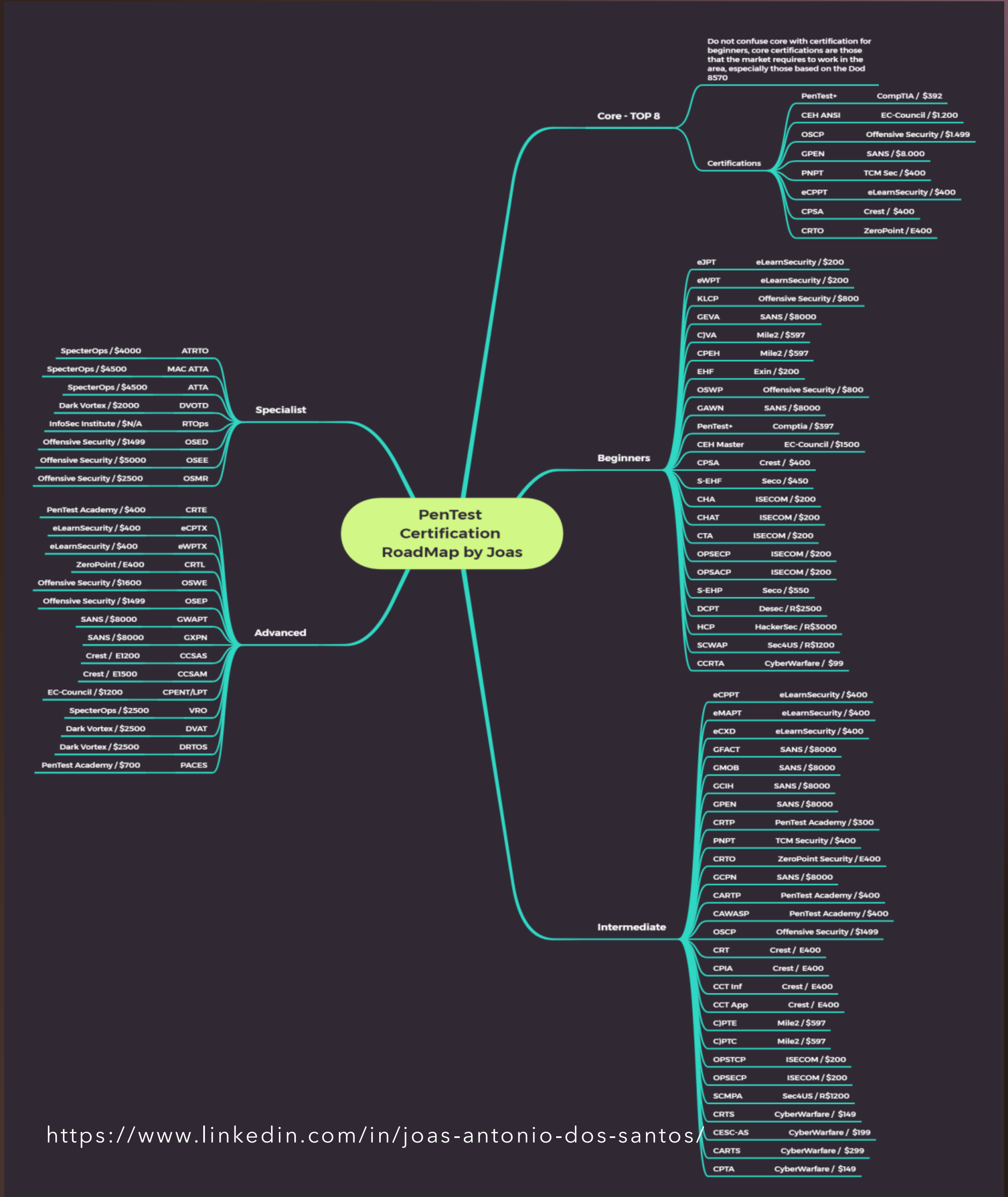
- PenTest
- Social Engineering
- Mitre Attack
- Physical PenTest
- Adversary Emulation
- Exploit Development
- Cyber Kill Chain
- Threat Hunting
- Cloud Attack
- Defense Evasion
- Cyber Threat Intelligence
- Programming Expertise (Python, Go or C#)
- Threat Modeling
- Command and Control
- Risk Identified
- Hardware Hacking

Some fundamental Hard skills for your career, based on vacancies found on Indeed

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

Detailed: https://github.com/CyberSecurityUP/PenTest-Certifications-Roadmap

Certifications MAP



PenTest Certification RoadMap by Joas

Core - TOP 8

Do not confuse core with certification for beginners, core certifications are those that the market requires to work in the area, especially those based on the Dod 8570

Certifications

PenTest+	CompTIA / $392
CEH ANSI	EC-Council / $1.200
OSCP	Offensive Security / $1.499
GPEN	SANS / $8.000
PNPT	TCM Sec / $400
eCPPT	eLearnSecurity / $400
CPSA	Crest / $400
CRTO	ZeroPoint / E400

Beginners

eJPT	eLearnSecurity / $200
eWPT	eLearnSecurity / $200
KLCP	Offensive Security / $800
GEVA	SANS / $8000
C)VA	Mile2 / $597
CPEH	Mile2 / $597
EHF	Exin / $200
OSWP	Offensive Security / $800
GAWN	SANS / $8000
PenTest+	Comptia / $397
CEH Master	EC-Council / $1500
CPSA	Crest / $400
S-EHF	Seco / $450
CHA	ISECOM / $200
CHAT	ISECOM / $200
CTA	ISECOM / $200
OPSECP	ISECOM / $200
OPSACP	ISECOM / $200
S-EHP	Seco / $550
DCPT	Desec / R$2500
HCP	HackerSec / R$3000
SCWAP	Sec4US / R$1200
CCRTA	CyberWarfare / $99

Intermediate

eCPPT	eLearnSecurity / $400
eMAPT	eLearnSecurity / $400
eCXD	eLearnSecurity / $400
GFACT	SANS / $8000
GMOB	SANS / $8000
GCIH	SANS / $8000
GPEN	SANS / $8000
CRTP	PenTest Academy / $300
PNPT	TCM Security / $400
CRTO	ZeroPoint Security / E400
GCPN	SANS / $8000
CARTP	PenTest Academy / $400
CAWASP	PenTest Academy / $400
OSCP	Offensive Security / $1499
CRT	Crest / E400
CPIA	Crest / E400
CCT Inf	Crest / E400
CCT App	Crest / E400
C)PTE	Mile2 / $597
C)PTC	Mile2 / $597
OPSTCP	ISECOM / $200
OPSECP	ISECOM / $200
SCMPA	Sec4US / R$1200
CRTS	CyberWarfare / $149
CESC-AS	CyberWarfare / $199
CARTS	CyberWarfare / $299
CPTA	CyberWarfare / $149

Specialist

SpecterOps / $4000	ATRTO
SpecterOps / $4500	MAC ATTA
SpecterOps / $4500	ATTA
Dark Vortex / $2000	DVOTD
InfoSec Institute / $N/A	RTOps
Offensive Security / $1499	OSED
Offensive Security / $5000	OSEE
Offensive Security / $2500	OSMR

Advanced

PenTest Academy / $400	CRTE
eLearnSecurity / $400	eCPTX
eLearnSecurity / $400	eWPTX
ZeroPoint / E400	CRTL
Offensive Security / $1600	OSWE
Offensive Security / $1499	OSEP
SANS / $8000	GWAPT
SANS / $8000	GXPN
Crest / E1200	CCSAS
Crest / E1500	CCSAM
EC-Council / $1200	CPENT/LPT
SpecterOps / $2500	VRO
Dark Vortex / $2500	DVAT
Dark Vortex / $2500	DRTOS
PenTest Academy / $700	PACES

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

Certifications in Job Offers

Information taken based on vacancies found on LinkedIn and Indeed. These are the certifications that you often find in Red Team vacancies, apart from the SANS certifications of which I only added 2 because they are the most requested.

START	BEGINNING CAREER	NEXT STEP CAREER	SPECIALIZATION	SOLID CAREER
Security+ (CompTIA)	PenTest+	OSCP	CRTO II	OSED/OSCE^3
eJPT (INE)	CEH ANSI	CRTO	OSWE	GPEN / GXPN
BCSP (Portswigger)	eWPTX	PNPT	OSEP	CISSP
$750	$1600	$2900	$4600	$20000

Development Skills

- Ways for you to develop your skills is to practice in laboratories, there are numerous websites and projects on github that can help on this journey.
- If you are learning cloud attacks, consider setting up an infrastructure to put your skills into practice.
- It is essential that you can execute it, however understanding how it works is very important, so in addition to laboratories, additional courses for your career are necessary, especially to learn a new market technology.

Red Team Career Tips

1. **Continuous Education:**
   1. Stay updated on the latest trends in cybersecurity.
   2. Pursue recognized certifications in the field, such as Certified Ethical Hacker (CEH) or Offensive Security Certified Professional (OSCP).
2. **Technical Development:**
   1. Deepen technical skills, including penetration testing, malware analysis, and vulnerability exploitation.
   2. Familiarize yourself with common security tools and know how to apply them effectively.
3. **Practical Experience:**
   1. Engage in hands-on projects, including Capture The Flag (CTF) challenges and open-source security projects.
   2. Consider internships, freelance work, or volunteer contributions to gain practical experience.
4. **Portfolio Building:**
   1. Develop a portfolio that highlights your projects, achievements, and skills.
   2. Document your processes and security testing results.
5. **Networking:**
   1. Attend conferences, workshops, and events related to cybersecurity.
   2. Build a professional network by connecting with other industry professionals.

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

Red Team Career Tips #2

1. **Compliance Knowledge:**
    1. Familiarize yourself with relevant security regulations such as GDPR, HIPAA, and PCI DSS.
    2. Understand the legal and ethical implications of Red Team work.
2. **Behavioral Skills:**
    1. Develop interpersonal skills for effective communication.
    2. Hone public relations skills, as interaction with other teams is crucial.
3. **Ethical Stance:**
    1. Strictly adhere to ethical guidelines when conducting security testing.
    2. Clearly communicate with stakeholders and respect the privacy and integrity of systems.
4. **Learn from Experiences:**
    1. Analyze previous security incidents and vulnerabilities to enhance your strategies.
    2. Always be willing to learn from challenges and successes.
5. **Stay Curious:**
    1. Cultivate a curious and inquisitive mindset to explore new approaches and techniques.
    2. Always be willing to adapt to changes in the cybersecurity landscape.

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

Red Team Career Tips #3

- A good Red Team professional is one who understands business and organization, as it is essential for you to be able to put into practice and develop a good Red Team strategy in your company.
- Selling the Red Team area is a little difficult, especially explaining the work to senior management, which is why having metrics such as KPIs and other indicators that measure the success of the red team's existence in the company and the impact it generated on the organization becomes important. even to justify budget.
- Therefore, before starting, define strategies to collect KPIs and define processes that the Red Team will use as a basis for executing tasks.

Job Interview Tips

1. **Understand the Role:**
    1. Ensure you have a clear understanding of the Red Team position and its responsibilities.
    2. Familiarize yourself with the specific skills and knowledge required for the role.
2. **Highlight Relevant Experience:**
    1. Showcase your relevant experience in penetration testing, vulnerability assessments, and other cybersecurity practices.
    2. Provide specific examples of successful Red Team engagements or projects you have worked on.
3. **Demonstrate Technical Proficiency:**
    1. Be prepared to discuss your technical skills in detail. This may include knowledge of penetration testing tools, network security, and incident response.
    2. Discuss any programming or scripting languages you are proficient in.
4. **Problem-Solving Scenarios:**
    1. Expect scenarios or hypothetical situations related to Red Team activities. Be ready to demonstrate how you would approach and solve these challenges.

Job Interview Tips #2

1. **Communication Skills:**
   1. Effective communication is crucial in a Red Team role. Be articulate in explaining complex technical concepts to non-technical stakeholders.
   2. Discuss how you document and report findings in a clear and understandable manner.
2. **Team Collaboration:**
   1. Red Team engagements often require collaboration with other security professionals. Highlight your ability to work well in a team, communicate findings, and contribute to collaborative efforts.
3. **Stay Updated on Industry Trends:**
   1. Be aware of current trends and developments in cybersecurity and Red Team practices.
   2. Discuss how you stay informed about the latest threats and security technologies.
4. **Ethical Considerations:**
   1. Emphasize your commitment to ethical hacking practices and respect for legal and compliance considerations.
   2. Discuss any experiences where you had to make ethical decisions during security assessments.

Tips for Studying with Efficient

- Some ways for you to study efficiently:
- 1) Set a study schedule based on your weekly routine
- 2) Use techniques such as Pomodoro and William Glasser's pyramid to achieve greater success in absorbing knowledge and learning
- 3) Create study groups and share knowledge with your colleagues and friends
- 4) Create flashcards of the subjects that you have the most difficulty with and always review constantly until you feel the confidence necessary to explain the content to your study group or even record a video for a YouTube channel, this way you even practice your communication skills.

Starting from Scratch in Red Team

- If you are completely new to the area, consider looking for the fundamentals before taking any step to study Red Team content, today the current scenario requires a professional to know

- Computer network
- Programming language
- Cloud computing
- Container and applications
- Operating systems (Windows, Linux and MAC) and their internals
- Information Security Fundamentals

- Once you have the foundation to be able to study the main cybersecurity content, especially the fundamentals, it is time for you to move up another level towards developing your skills as a Red Team. But never stop learning the fundamentals first so you can develop later, try to absorb this knowledge through an undergraduate degree, a postgraduate degree in a specific area or even through complementary courses and the possibility of obtaining a certification to put you one step ahead. from the market.

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