INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 07 ISSUE: 12 | DECEMBER - 2023 SJIF RATING: 8.176 ISSN: 2582-3930

Red Teaming vs. Blue Teaming: A Comparative Analysis of Cyber Security Strategies in the Digital Battlefield

(Bharat Kotwani, Department of Information Technology,
Vivekanand Education Society, Institute of Technology.)

Miss Rohini Sawant
Assistant Professor
Department of Information Technology
Vivekanand Education Society, Institute
of Technology.
Mumbai 400 074, India
rohini.sawant@ves.ac.in

Dr Shalu Chopra
Head of Department,
Information Technology,
Institute of Technology.
Mumbai 400 074, India
shalu.chopra@ves.ac.in

***Abstract*— In the ever-evolving landscape of cybersecurity, organizations face continuous threats and attacks that can potentially compromise their systems and data. To enhance security measures, two primary methodologies have emerged: red teaming and blue teaming. Red teaming involves simulating adversarial attacks to identify vulnerabilities and weaknesses, while blue teaming focuses on defending systems and mitigating risks. This research paper aims to provide an in-depth comparative analysis of red teaming and blue teaming, exploring their objectives, methodologies, benefits, and challenges. By understanding the strengths and limitations of both approaches, organizations can effectively employ these strategies to fortify their cybersecurity defenses.**

***Keywords*—** *Cyber Security, Blue Teaming, Red Teaming, Defensive, Offensive.*

I. INTRODUCTION

The sudden surge of user engagement over the internet resulting in the demand of miscellaneous services have undoubtedly attracted several adversaries in attempting to push beyond the security reinforcements set up by Cyber Security Engineers on the front-line. From sensitive and other confidential information getting leaked to falling in the laps of ransomware traps, organizations and multinational conglomerates have been left pondering, "What would it take to strengthen our defence?"

The entirety of Cyber Space [9] has proven to be a critical realm for the Conglomerates who bank upon the latter to safe-keep their records, company optics and several other configurations which help them steer in the uncharted waters of trades and businesses. This has indeed led to the rise of opportunities and in fact opened up several sectors to be held down while the rest negotiate with the others across the globe and aim for the metrics.

II. NETWORK INFRASTRUCTURE SECURITY

Network Infrastructure Security [2] [3] is just a front to countless hours being dedicated by your organization or enterprise followed by troubleshooting every vulnerable aspect in the network which may have crippled the whole backbone. Backed by intricate architecture and strategies, all the hardware and the services which follow are made sure to run as optimal they could and on a reliable, trusted digital signature.

Your network infrastructure is built around several high-tech parts and components. From routers and switches to cables, LAN cards, and more, it all boils down to how efficiently they will tether and contribute towards a highly secure infrastructure. This is followed by heavy duty devices like Firewalls, IDS and other protocols which helps in setting up the reinforcements. The final primary component of a network infrastructure relates to its services.

From different types of hardware like LAN Cards, cables, routers to server machines, every physical part plays a key role and contributes towards the security alongside essential software including Operating Systems, Intrusion Detection Systems, Firewalls and other demanding items on the agenda.

Every unintentional and unexpected traffic needs to be monitored and that is where the above infrastructure comes into the play as everything boils down to a flexible budget which will in turn set the tone for you and your company. A holistic approach is expected to be adapted by the organization if they were to build a secure wall around their assets and highly confidential records.

Penetration testers are often regarded as the core members of the Network Infrastructure Team where they are often asked to find and exploit vulnerabilities within this newly set up Infrastructure to assure quality testing and endurance. This indeed helps to keep several adversaries on the bay and reinforcing or making concrete changes to even a minor leak in the system.

The whole idea behind Network Infrastructure Security is the break-down of the overall network into smaller segments or pieces. These fragments could be everything including firewalls, intrusion detection systems or other similar security protocols. This is done to add layering to the security aspect so that any intruder who tends to compromise the network would dent with a lesser impact. Just like an

Onion, the network security should be multiple layered so as to make it harder to be peeled off.

A typical Network Infrastructure Security can't be managed single-handedly and this requires a group of individuals who are spread out in maybe two or three groups. They are the Red, Blue and the Purple Teamers.

III. DEFENSIVE SECURITY (BLUE TEAM)

Defensive Security is as important as the other teams in the realm of Cyber Security. The name says it all, "defense". Personnels working with Defensive Security are responsible for defending an organization's information systems and the overall network infrastructure from cyber threats.

The Blue team or Defensive Security personnels work in unison with the Red (responsible for simulating attacks) and the purple teams (responsible for assessing defensive measures and clubbing the blue and red teams). Technically the Blue team proactively defend the network infrastructure against and respond to security incidents

To fulfil their objectives, blue team members engage in various activities. These include risk assessment, vulnerability management, security monitoring, incident response, and continuous improvement of security measures.

The above activities contribute towards every task performed by the blue team. It involves identifying and evaluating potential vulnerabilities, threats, and risks specific to an organization's infrastructure, applications, and data. By conducting thorough risk assessments, the team can develop a comprehensive understanding of the organization's security posture and establish priorities for mitigating vulnerabilities.

Network monitoring is a crucial activity done by the blue team that involves the continuous monitoring and analysis of network traffic, system logs, and other relevant data sources to detect signs of suspicious or malicious activities. They make use of security information and event management (SIEM) systems, intrusion detection systems (IDS), and other tools to identify potential security incidents promptly. This helps them to minimize the overall impact.

When an individual is signed to task and perform within a blue team, they always start as a Junior Security Analyst under the Security Operations Center (SOC). They might also be called a "Triage Specialist" since their goal would be to figure out an approach to identifying and prioritizing a cyber incident / attack on the basis of their severity.

The Blue team would also employ least-privilege access, which means that the organization grants the lowest level of access possible to each user or device to help limit lateral movement across the network in the event of a breach.

Overall, there are three tiers under the Security Operations Center.

1. Triage Specialist
2. Tier 2: Security Operations Analyst - Incident Responder
3. Tier 3: Security Operations Analyst - Threat Hunter

Incident Responders and Threat Hunters basically come under the Security Operations Analyst roles, who mitigate and lessen the impact of the cyberattack at a higher level with access to much deeper investigations, adversary research and might also participate in malware reversing.

As a part of the Security Operations Team, you will be entitled to perform these following activities:

1. Ticketing
2. Gathering Knowledge and Data related to the incident occurred
3. Performing Research and Development.
4. Performing Threat Intelligence
5. Making use of Security Information & Event Management (SIEM) [13] and Endpoint Detection and Response (EDR) to monitor the network and perform analysis
6. Reporting the incident along with a report

IV. OFFENSIVE SECURITY (RED TEAM)

Red team or the Offensive Security [4] [5] unlike the blue team personnels are known to plan their approaches in a simulated environment where they pose as real-world attackers. They would perform penetration testing if and only authorized by the enterprise or an organization and may end up facing legal consequences if not done.

We can relate Red Teaming [10] to those of Military exercises. In Military exercises, a particular group takes up the roles of a red team and mimics as adversaries. This is done to test the proactiveness of the blue team. This in turn helps to come up with new security strategies which translate further into the world of Cybersecurity as "Tactics, Techniques and Procedures (TTPs)." This indeed allows the Blue Team to improve their security protocols and revamp the same if needed.

Red teams are often known as adversaries, attempting to penetrate an enterprise' security controls to escalate privileges, steal sensitive information, or disrupt operations. By mimicking these attacks, organizations can determine the potentiality of their security measures and identify any vulnerabilities that need to be addressed.

Before getting into Red Teaming, your machine or system should be whitelisted by your organization or the Enterprise in order to proceed with the vulnerability discovery process. This allows you to evaluate every host on the network and revert back with the best available remediation effort.

Penetration Testers adopt a comprehensive approach, with a blend of technical expertise and social engineering, and other methodologies to bust vulnerabilities from different points of view. Their activities are typically conducted with a defined goal-list, procedures, and a set of guidelines. The objectives establish the particular goals and outcomes the red team hopes to achieve, while the scope lays out the assets, systems, or networks that are part of the evaluation. To ensure the involvement meets the organization's goals, the rules of engagement set boundaries and constraints.

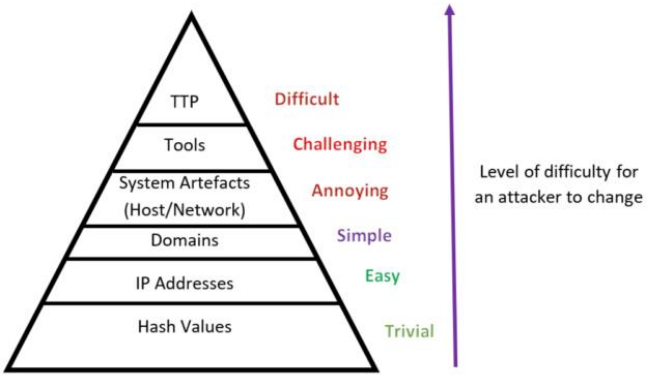
Red teams give organizations detailed reports on their findings, methods, vulnerabilities exploited, and potential impact. The paper contains specific solutions to address risks and weaknesses. Stakeholders can debate the assessment results and understand the ramifications of potential real-world assaults during the debriefing session.

V. ARTIFACTS, FRAMEWORK AND METHODOLOGIES

1. PYRAMID OF PAIN

Artifacts in the Cyber Security landscape allow us to improve the effectiveness of Cyber Threat Intelligence, threat hunting and incident response. The Pyramid of Pain is one among the most famous visual representations that categorizes different types of Indicators that are often left behind by an adversary or an attacker post a cyberattack.

The Pyramid of Pain deals in several layers, typically arranged in a pyramid shape as the name goes, with the most easily changed or replaced indicators / artifacts at the bottom and the most difficult to alter at the top.



(Fig. The Pyramid of Pain)

Image Courtesy: Google Images

The concept of the Pyramid of Pain helps both the red and lue teams in prioritizing their defensive efforts. By focusing on higher layers of the pyramid, engineers can yield more sustainable and robust results in countering threats, as attackers are often made to invest a massive amount of time and resources to bypass the new barriers and penetrate the same.

2. MITRE ATT&CK Framework: ATT&CK

MITRE is a non-profit organization, developed by MITRE Corporation. They work with private industries and the Government of the United States of America in a bid to make their proceedings reside in a safer place on the internet. MITRE [6] have done tons of work around Counterterrorism, bank fraud and certainly cybersecurity.

The MITRE ATT&CK framework consists of three matrices,

i. pre-ATT&CK : Initial Reconnaissance
ii. ATT&CK : Delivery
iii. Mobile : Privilege Escalation, Lateral Movement, Command and Control.

Together they comprise an end-to-end attack chain filled with all of those successful techniques that adversaries use if they were to breach an enterprise or a network.

MITRE really provides crucial information to Blue Teams that was previously only reserved for Elite Incident Responders. Just like the periodic table in Chemistry, the MITRE matrix has its own column headers outlining every phase in the Attack Chain. The MITRE ATT&CK framework is further organized into matrices, which are specific to different platforms or environments such as enterprise, mobile, and cloud.

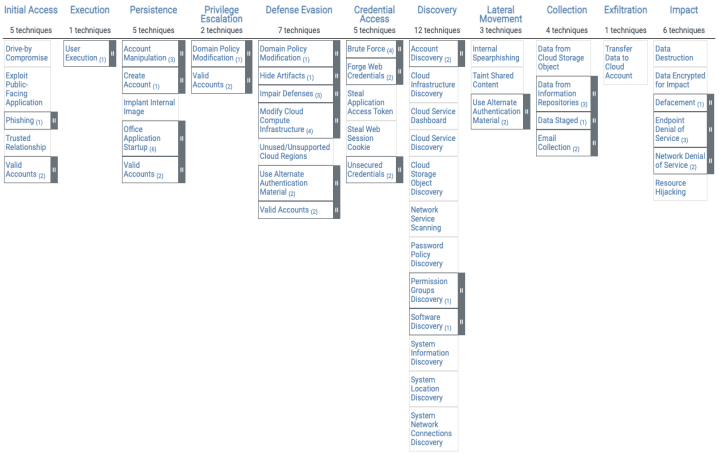


Image Courtesy: attack.mitre.org

This is how the MITRE ATT&CK framework for Cloud looks like.

The framework covers the entire attack lifecycle, including initial access, execution, persistence, privilege escalation, defense evasion, credential theft, lateral movement, collection, exfiltration, and impact.

Tactics within the ATT&CK framework represent aforementioned high-level adversary objectives, such as initial access, execution, or exfiltration. Techniques, on the other hand, are specific methods employed by adversaries to achieve these objectives. For example, a technique under the "Execution" tactic might be "Command-Line Interface" (CLI) execution, which refers to adversaries running commands directly on a compromised system.

3. OSINT (Open Source Intelligence)

OSINT, also known as Open-Source Intelligence, is the most profitable approach [1] [7] to collecting information from open sources available publicly. OSINT allows us to gain insights and valuable intelligence about certain individuals, organizations or any other particular subject of interest. Websites, Social Media Platforms, News Articles and Public Records can contribute towards the OSINT methodology.

With that being discussed, OSINT plays a crucial role in a plethora of fields including Cyber Security, Law Enforcement and Private Corporate Investigations.

The primary goal of OSINT is to leverage publicly accessible information to gather intelligence [7] and support decision-making processes. Unlike classified or restricted data, open sources are freely available and do not require specialized access or clearance.

Image Courtesy: Google Images

OSINT provides a means to collect information ethically and legally, respecting privacy and legal boundaries. However, it's essential to note that while open sources can provide valuable insights, the information gathered should always be verified and analyzed critically to ensure accuracy and reliability.

Data Collection is one of the key aspects of OSINT. It basically involves identifying relevant sources and the systematical extraction of data from the gathered data sources. By analyzing web pages online and through others such as Data Mining or web scraping, OSINT can be achieved with much at one's ease of access.

Social media platforms have emerged as a rich source of OSINT. Individuals and organizations often share personal and professional details on platforms like Facebook, Twitter, LinkedIn, and Instagram.

OSINT practitioners utilize advanced search techniques and analysis tools to monitor public posts, profiles, and connections. By analyzing patterns, relationships, and interactions, they can gain insights into social dynamics, affiliations, and potential vulnerabilities. Press Releases, news articles and blogs can also prove to be valuable sources to put OSINT into practice.

VII. CAREERS IN CYBER SECURITY

If someone were to choose Cybersecurity as the primary line of their careers, they might be just instantly exposed to the vast ocean of Network and Infrastructure Security openings. Where does one actually start from or what exactly would it look like at the very beginning have been the most common questions that have been wanting to be answered.

Careers in Cybersecurity indeed demand certain prerequisites to be fulfilled before one nose dives into the world of Digital Certainty. Scripting languages and several other computing basics involving knowledge across Operating Systems like Linux and Windows come handy while planning out your moves on the defence.

The whole idea about choosing the correct roadmap in the realm of Cybersecurity depends upon how the concerned person wants to kick start their journey. In hindsight, every event triggered while working as a Network Engineer needs to be handled according to a standard operating procedure.

The personnels who take up Cyber Security as their core expertise may need to set boundaries before taking up roles that of an Ethical Hacker or within the Security Managerial Areas. Ethical Hacking is basically posing as an attacker and contemplating their moves as if they were that same person.

In Layman's terms, you would take up the role of a penetration tester if you were to pose as an attacker. Finding vulnerabilities, tying up loose ends and deploying security patches within the network will be your primary goals but that doesn't answer everything.

Penetration testing highlights the procedures which are listed under Red Teaming, also coined as Offensive Security. Now if we contrast the aforementioned security technique, we are bound to be exposed to Defensive Security which also serves the same purpose as that of Red Teaming but mainly focuses on identifying the nature of the attacks and putting in an effort in mitigating the same.

Before we actually focus on how these two goes head-to-head in terms of proactively securing the systems, let us take a look at how the security protocols for a network infrastructure are designed and put into a use case.

VIII. ACKNOWLEDGMENT

I would like to express my sincere gratitude and appreciation to Miss. Rohini Sawant for her invaluable support and guidance throughout the process of writing my research paper. Her profound knowledge, insightful feedback, and unwavering encouragement have been instrumental in shaping the success of this work. I am truly fortunate to have had her as my mentor and grateful for her dedication and commitment to my academic growth. Her contributions have been immeasurable, and I am profoundly grateful for her unwavering support.

REFERENCES

[1] Ludo Block (2023) The long history of OSINT, Journal of Intelligence History, DOI: 10.1080/16161262.2023.2224091

[2] Kumar, s & T J, Jaya. (2021). Analysis of Security Parameters and Network Infrastructure on Cloud. IOP Conference Series: Materials Science and Engineering. 1085. 012036. 10.1088/1757-899X/1085/1/012036.

[3] G. Manimaran and B. Al-Duwairi, "Internet infrastructure security," *13th Symposium on High Performance Interconnects (HOTI'05)*, Stanford, CA, USA, 2005, pp. 6-7, doi: 10.1109/CONECT.2005.25.

[4] Ajmal, Abdul Basit & Shah, Munam & Maple, Carsten & Asghar, Muhammad & Islam, Saif. (2021). Offensive Security: Towards Proactive Threat Hunting via Adversary Emulation. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3104260.

[5] M. U. Rana, O. Ellahi, M. Alam, J. L. Webber, A. Mehbodniya and S. Khan, "Offensive Security: Cyber Threat Intelligence Enrichment With Counterintelligence and Counterattack," in *IEEE*

Access, vol. 10, pp. 108760-108774, 2022, doi: 10.1109/ACCESS.2022.3213644.

[6] Georgiadou, Anna & Mouzakitis, Spiros & Askounis, Dimitris. (2021). Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. Sensors. 21. 3267. 10.3390/s21093267.

[7] J. Pastor-Galindo, P. Nespoli, F. Gómez Mármol and G. Martínez Pérez, "The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends," in *IEEE Access*, vol. 8, pp. 10282-10304, 2020, doi: 10.1109/ACCESS.2020.2965257.

[8] Al-Mohannadi, Hamad & Awan, Irfan & Hamar, Jassim & Cullen, Andrea & Disso, Jules & Armitage, Lorna. (2018). Cyber Threat Intelligence from Honeypot Data Using Elasticsearch. 900-906. 10.1109/AINA.2018.00132.

[9] Sheth, Mrs & Bhosale, Sachin & Kurupkar, Mr & Prof, Asst. (2021). Research Paper on Cyber Security. 2021.

[10] Kraemer, Sara & Carayon, Pascale & Duggan, Ruth. (2004). Red Team Performance for Improved Computer Security. Human Factors and Ergonomics Society Annual Meeting Proceedings. 48. 10.1177/154193120404801410.

[11] Kokkonen, Tero & Puuska, Samir. (2018). Blue Team Communication and Reporting for Enhancing Situational Awareness from White Team Perspective in Cyber Security Exercises: 18th International Conference, NEW2AN 2018, and 11th Conference, ruSMART 2018, St. Petersburg, Russia, August 27–29, 2018, Proceedings. 10.1007/978-3-030-01168-0_26.

[12] You, Y., Jiang, J., Jiang, Z. *et al.* TIM: threat context-enhanced TTP intelligence mining on unstructured threat data. *Cybersecurity* 5, 3 (2022). https://doi.org/10.1186/s42400-021-00106-5

[13] González-Granadillo G, González-Zarzosa S, Diaz R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors (Basel). 2021 Jul 12;21(14):4759. doi: 10.3390/s21144759. PMID: 34300500; PMCID: PMC8309804.

[14] Danquah, P. (2020) Security Operations Center: A Framework for Automated Triage, Containment and Escalation. *Journal of Information Security*, **11**, 225-240. doi: 10.4236/jis.2020.114015.