International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

Red Team Analysis of Information Security Measures and Response

Khushboo Amin[1], Dr. Priyanka Sharma[2]

[1] Student, School of Information Technology & Cyber Security, Raksha Shakti University, Gujarat, India
[2]Dean, Research & Development, Raksha Shakti University, Gujarat, India

---

Abstract - *This research attempts to develop a factor understanding of Red Team assessment strategies in computer and data security. The Red Team is a 'cultured form' of assessment that identifies weaknesses during a quite information and security system. This research aims to identify and define the form of dimensions of the Red Team's effectiveness from the customer, management, individual, and team member to strengthen the knowledge system's security and performance. The Red Team generally addresses the protection risks present within the knowledge systems by Vulnerability Assessment and Penetration Testing (VAPT). VAPT consisting of two separate terms i.e. Vulnerability Assessment (VA) and Penetration Testing (PT) is an offensive technique where the cyber assets of any organization are exploited in a controlled environment to simulate a real-time attack on the information system. Vulnerability assessment includes the employment of assorted automated tools and manual testing techniques to work out the protection posture of the target system. During this step, all the breach points and loopholes are found. These breach points/loopholes if found by an attacker may end in heavy data loss and fraudulent intrusion activities. During Penetration Testing, the pen-tester simulates the activities carried out by a malicious actor trying to use the vulnerabilities present in the targeted system. This process of VAPT helps in assessing the effectiveness of the protection measures that are present on the target system. While authoring this paper, I've described the entire process of VAPT, the methodologies, models and global standards used to assess information security infrastructure.*

Key Words: Ethical hacking, Information Security, Penetration Testing, Red Team, Security Testing, Vulnerability Assessment.

1.INTRODUCTION

This research paper is a part of my project for partial fulfilment to achieve the Master of Technology degree. The topics and concepts mentioned in this paper are discussed thoroughly within the project report along with the vulnerabilities uncovered and their recommendations.

As we all know today, the cybersecurity threat landscape may be a dynamic one and is continually changing. The cyber attacker of today uses a combination of both traditional and advanced hacking techniques. On top of this, new variants of the existing malicious threat actors are seen daily. Red Teaming may be a full-scope, multi-layered attack simulation designed to live how well a company's people and networks, applications and physical security controls can withstand an attack from the real-life adversary.

2. DIFFERENT SORTS OF TEAM

2.1 Red Team

They work dedicated as part of the internal infrastructure or an external entity to test the effectiveness of a security mechanism by mirroring the tools and techniques of attackers as close to a real-world attack on the infrastructure.

2.2 Blue Team

It refers to the internal security team that works as the defenders against both the real-world internal/external attackers and the Red Team attacks. Blue Teams differs from a traditional security team in most organizations, as most personnel in a 'security-operations' team don't have a mentality of constant vigilance against attack, which is the true and only mission and perspective of a true-Blue Team that makes it stand out from the traditional security operations and monitoring teams.

2.3 Purple Team

Purple Team exists to confirm and maximize the effectiveness of the Red and Blue teams. They are the integration of the defensive tactics and controls from the Blue Team and the attack skills from the Red Team into one single team maximizing the security throughput. Ideally, the Purple Team should not be a team the least bit, rather a permanent dynamic between Red and Blue.

3. SECURITY ASSESSMENT: VAPT

Vulnerability Assessment and Penetration Testing is beyond the audit in which the loopholes of the system or infrastructure are found externally.

3.1 Vulnerability Assessment

Vulnerability assessment is the working to identify, classify and prioritize the vulnerability uncovered in computer systems during a security assessment of the applications, and network infrastructures; providing the organization with a comprehensive report that addresses the risk status and the business impact of each vulnerability. The comprehensive report helps in proper assessment of the available knowledge, awareness and risk background to understand the threats to the information system from the respective vulnerability and react accordingly.

3.2 Penetration Testing

A penetration test, also known as a pen test, defines a cyber-attack that is simulated against the organization's information system to check the exploitability of the vulnerabilities. Speaking from a web application security perspective, penetration testing is commonly used to harden the web application firewall (WAF) defending the web application infrastructure of the organization.

Pen testing attempts to breach any number of application systems, endpoints and other assets to uncover vulnerabilities hidden within the information system, such as providing corrupt inputs inducing a code injection attack.

4. METHODOLOGY

A system of methods used in the vulnerability assessment and penetration testing. The Red Team is highly dependent upon the security needs of the client. For example, the entire IT and network infrastructure might be evaluated, or a certain part of the infrastructure may be tested. The specific functionalities of what will be tested are critically examined based on the results from the security evaluation.

4.1 Reconnaissance

Reconnaissance is the preliminary phase; during which an attacker gathers as much possible information about the target and its infrastructure before launching the attack this helps the attacker to maximize the impact of the attack

4.2 Scanning

This phase is the logical extension of the active reconnaissance where the attacker uses the details gathered to actively probe the target to identify the existing entry points and vulnerabilities in the information system.

4.3 Gaining Access

This is the third and most important phase of an attack in terms of potential damage. Direct access to the information system may not always be required to cause damage. For instance, denial- of service attacks eliminate the systems resources or stop the critical services from running on the target system. A process (es) on the target can be killed in order to stop a service, using a logic/time bomb, or even knowingly misconfiguring and crashing the system. A network outage on the local network can exhaust the resources.

The targeted setup can be exploited locally in the network, offline via direct contact, or the Internet as a means of deception to cause theft. Many factors contribute to an attacker successfully gaining access into a target system like the architecture and configuration, the skill set of the attacker, and the initial level of access obtained. The most damaging type of denial-of-service attacks can be distributed denial-of-service attacks, where an attacker uses zombie software distributed over several machines on the Internet to trigger an orchestrated large-scale denial of services.

4.4 Maintaining Access

Access Once an attacker gains access to the target system, the attacker can choose to use both the system and its resources, and further use the system as a pivot to penetrate deeper into the network via scanning and exploiting other systems or keep a low profile staying hidden to continue exploiting the system as and when needed; both these actions can equally damage the organization and impact the business in unpredictable ways. For instance, the attacker can employ a sniffer to collect the traffic flowing in the network, including the unencrypted telnet and FTP sessions.

4.5 Clearing Tracks

In order to stay anonymous and maintain access of the system, the attacker would destroy evidence of his/her presence and activities. Erasing evidence of a compromise is a requirement for an attacker who would like to remain obscure. This is one of the best methods to evade trace back.

This usually starts with erasing the failed login attempts and any error messages encountered during the gaining access phase, e.g., the messages left in the system logs and event viewer in Windows systems. Next, the action is to reconfigure the logging mechanism to evade logging future login attempts. The system administrator can be convinced about the credibility of the output of the system logs is correct and that there is no intrusion or system compromise by manipulating and tweaking the event logs.

Risk = Threat * Vulnerability * Impact

As per the SOP, the first thing a system administrator does to monitor unusual activity is to check the system log files, the intruders commonly use utilities to modify the system logs to evade the administrator. A rootkit can be deployed to disable logging altogether and discard all existing logs as the best measure by the intruder. This happens if the intruders intend to use the system for a longer period as a launch base for future intrusions. Only those portions of logs that can reveal the intruder's presence are then removed to stay hidden. The system must look and function as it did before the attack and the backdoor deployment. Any modifications to critical/non-critical files should be changed back to its original attributes. The information listed, such as file size and date, just attributes information contained within the file.

5. RED TEAM

When used in a computer security context, a Red Team is a group of white-hat hackers that attack an organization's digital infrastructure as a malicious attacker would test the organization's defenses (also known as "pen testing"). A red team from a cybersecurity prospective is the "Core of the Cyber Opposition Force" ethically exploiting the information system is a controlled environment and without malicious intent. A red team assessment does not look for multiple vulnerabilities but for those vulnerabilities that will achieve their goal. The goal is often the same as the penetration test. Red Teamers implement multiple OSINT methods to achieve their goals like Social Engineering i.e. interviewing the employees to uncover critical information, wireless attacks to test the APs security, external attacks to test the perimeter devices, and more.

Red team deployment is mostly suited for organizations with a mature security program. Organizations that often have routine pentests, patched most vulnerabilities, and generally have a positive pentest result. An intensive red team test will expose risk factors residing in technology, people, and physical infrastructure.

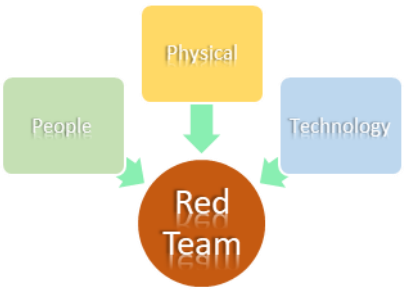

Fig -1: Red Team test

During a red team engagement, highly-trained security veterans personate attack scenarios to reveal the potential flaws in the physical, hardware, software and human components of the information system. Red team engagements also uncover opportunities for insider attacks compromising the systems and networks or enable data breaches.

6. RED TEAM VERSUS TRADITIONAL VAPT

To determine the risk to the network infrastructure of an organization, it is the primary responsibility of Red Team operators to recognize potential threats or vulnerability. Assorted of open-source tools or commercial tools can be used by the Red Team to recognize vulnerabilities and to exploit them to their preference. The red team approach is more in-depth than what most malicious threat actors follow as they are attempting to find a single vulnerability, whereas security professionals need to find all possible vulnerabilities for a given information system to assess the business impact of the risk. Red Team members test all feasible attacks to provide a complete security assessment of the information system. The complete awareness of security infrastructure is the result of a detailed Red Team research of the information system. However, a Red Team will not be sufficient in identifying every risk present in the infrastructure; the organization should always maintain targeted security measures from their end to appropriately manage risk and provide security protection.

Pen testing is used to monitor, control and identify the vulnerabilities to secure them along with testing the efficiency of the vulnerability management procedures set in place. It further helps to secular for the foundation in the information security policies. Pen testing is testing the security environment of infrastructure to find and patch vulnerabilities in a limited period so that we can eliminate

the false positive scenarios. In comparison to Red Team, Pen testing is the most rigorous and methodical testing of a network, hardware or application. During Pen testing, the pen testers search for vulnerabilities, analysis them and exploit them. Penetration tests are well defined and usually take up to one to two weeks for the whole process. Red Team includes tactics, techniques, and procedures (TTP) by adversaries. Red -Team is just like Pen testing in many ways but it is more targeted. The Red Team comprehensive accesses and evaluate different areas of information security over a multi-layered path. The aim is to attempt to improve the company's response which is to present real-world scenarios. Each and every area of information security defines how the target will respond or how it is accessed. It follows the concept of defense in depth; therefore, the target must be tested on each layer.

The objective of the Red Team is to not find many vulnerabilities as potential but to test the detection and the response capabilities of the framework along with their security status. Vulnerability assessment is the process of analyzing a system that focuses on finding the vulnerability and prioritizing them by risk. Exploitation or endorsement of a vulnerability is not performed while vulnerability assessment. When vulnerability assessment compared to Red Team engagement doesn't take preference. A Red Team may not use any vulnerabilities. Red Team may achieve an operational impact that any insider can implement to test the feedback of an insider attack. The Red Teams rarely if ever compile common vulnerability assessment tools as they are loud and execute more traffic than a typical Red Team engagement is willing to accept.

7. RED TEAM WORKING

7.1 Threat Emulation

The process mimics the TTP's of a specific threat. The measure can be carried out for different attacks i.e. zero-day, script kiddie to a progressive attacker or an addressed threat like botnets, ransom ware, DDOS, etc. The main hurdle in the threat emulation is simulating the threat to a level where the analyst believes that it is real. It can be achieved from using real malware to developing custom payloads, using tools to generate the IOC (indicators of compromise).

7.2 Operational Impacts

The actions or effects performed against a target that is designed to demonstrate the physical, informational or operational weaknesses in security infrastructure are observed in the Operational Impacts section. These effects can be as general as performing a denial of service attack on a service or more specific such as using high jacked SWIFT Token to control the International SWIFT Transactions. Operational Impacts are adequate in demonstrating sensible impacts against a target. The level of depth and the impact can be as awful as management is active to explore. These impacts are typically performed against live production systems to have the highest level of fidelity but can be executed on User Acceptance Testing environments if they are representative systems.

8. RED TEAM: RULES OF ENGAGEMENT

- Execute engagement requirements as directed.
- Comply with all laws, regulations, policies, programs, and Rules of Engagement.
- Implement the Team's operational methodology and TTP.
- Identify and has input to target environment deficiencies.
- Research and develop new exploit tools and test tools for functionality.
- Perform OSINT as and when required for the engagement.
- Identify and assess actions that reveal system vulnerabilities.
- Assist the Red Team Lead in the development of the final engagement report.
- Perform Physical Assessment support under the direction of Red Team Lead.

9. K.A CYBER LLP: THE VIRTUAL VAPT

- Broken Walls Inc. engaged to conduct a Penetration Test on the network systems of K.A. Cyber LLP from January 2020 to April 2020. Broken Walls Inc.'s objective is to discover significant vulnerabilities within the K.A. Cyber LLP network infrastructure. The findings are to be utilized with a risk analysis to assist in developing security architecture for K.A. Cyber LLP.
- The most significant findings related to the overall design philosophy behind the K.A. Cyber LLP trust model, the lack of a consistent Identification and Authentication (I&A) scheme, the inconsistent and uneven implementation of and compliance with existing policies and procedures, a lack of sufficient audit controls and procedures, and a significant number of vulnerabilities that result in the network and systems being susceptible to compromise from the internal network.
- The detailed penetration testing findings are ordered according to their severity and discussed in detail in the executive report.

- The culture and philosophy of the company dictate the trust model. The trust model of management is the logical basis upon which security architecture is built. The security architecture provides a common framework for all other security tools, policies, and procedures. K.A. Cyber LLP has a trust model that assumes the internal users of the network are to be trusted. This model is designed to meet the business needs of K.A. Cyber LLP in which people routinely change locations within the building and resources need to be allocated dynamically. The model is designed to have a fluid business environment.
- The fluid environment at K.A. Cyber LLP creates a situation in which control measures cannot be easily added to the network infrastructure. Due to insufficient access control mechanisms, violations of current policies and procedures that are not necessarily prevented or detected in the environment frequently. Additionally, there is no mechanism to verify and non-repudiate the identity of individuals. Also, some user IDs are locally administered and do not exist in the Active Directory and therefore inconsistent across systems. The existing security policies and procedures are unevenly administered, and the audit logs and information collected from various systems are not reviewed regularly.
- Following is the virtual diagram of Cyber LLP.

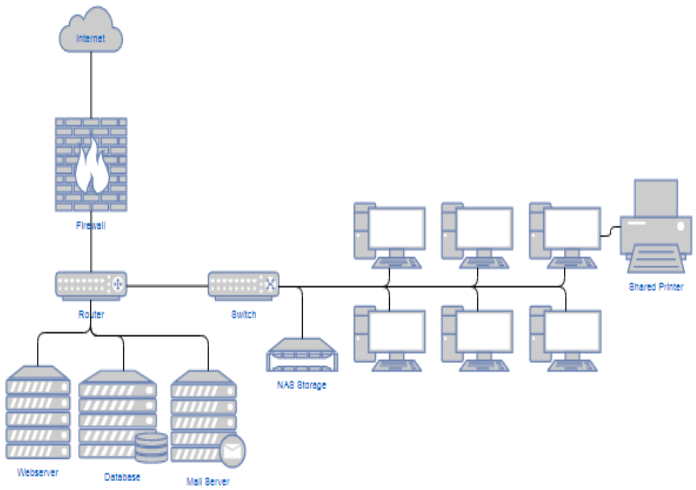

Fig -2: K.A Cyber LLP Sample Environment

9. RESULTS AND DISCUSSION

Regardless of the frequency of vulnerability testing, no critical system is often considered well protected unless both the network segments and therefore the critical hosts/servers are monitored steadily for signs of exploitation and intrusion attempts. As results of new exploits and vulnerabilities within devices and network operating systems are detected regularly, it's inconceivable to check a network completely, giving 100 per cent security of being invulnerable to penetration either from inside or from outside. Additionally, K.A. Cyber LLP has chosen a trust model within which the appliance of stronger internal controls is harder than during a more restrictive trust model. Therefore, the best method of detecting exploitation would be some variety of intrusion detection system that's both networks based and may do user profiling. Without apportion of identification and authentication of users, ascribe misuse to specific individuals becomes unreliable. Without appropriate audit controls to make sure compliance with policies, the policies and procedures themselves become untenable.

Broken walls Security Solutions believes the corrective actions and proposals during this report will improve K.A Cyber LLP Services' ability to avoid breaches of knowledge security. However, Broken Walls Security Solutions strongly recommends that an Intrusion Detection and Identification and Authentication capability be added to the network to detect misuse and intrusions and supply the data necessary to support forensic investigations. It is also endorsed that audit controls for broken walls like compliance testing, independent log review, or configuration audits are implemented, with the results of those incorporated controls with the conclusion of the Intrusion detection capability. A policy and procedure review, combined with a risk analysis, would even be very beneficial at this time to streamline and reiterate those policies that are critical to the functioning of the enterprise.

10. CONCLUSION

KA Cyber LLP encountered subsequent failures of the security controls, which led to a complete compromise of the company's sample assets. These minor looking failures could hit the business operations hard if they were exploited in the wild. Current password reuse policies, the company's trust-model and a lack of an access control mechanism are the main causes of failure to mitigate the impact of the vulnerabilities discovered during the testing.

A targeted attack against KA Cyber LLP can result in a complete compromise of organizational assets leaving the company completely defenseless. Multiple issues, typically considered as minor were leveraged in concert, resulting in the compromise of the KA Cyber LLP's sampled assets. It is important to note that this collapse of the KA Cyber LLP security infrastructure can be greatly attributed to insufficient access controls at both the network boundary and host levels.

ACKNOWLEDGMENT

I am highly indebted to Raksha Shakti University and Sequretek IT Pvt. Ltd. for their guidance and constant supervision as well as for providing necessary information regarding this research and also for their support in completing this endeavor.

I would like to express my special gratitude and thanks to my internal and external guide Prof. Dr. Priyanka Sharma for imparting her knowledge and expertise in this study. I would heartily thank Dean of School of Information Technology and Cyber Security Prof. Chandresh Parekh to allow me to work over this research paper and their endless and great support.

REFERENCES

[1]. Bradley J. Wood, Ruth A. Duggan, " Red Teaming of Advanced Information Assurance Concept", Lesson Learned,http://cs.uccs.edu/~cchow/pub/master/sjelinek/doc/research/red, [Accessed: 17 April 2020].

[2]. "Red Teaming Overview , Assessment & Methodology", Introduction, [online].available: https://resources.infosecinstitute.com/red-teaming-overview-assessment-methodology/#gref, [Accessed: 17 April 2020].

[3]. "The Different between Vulnerability Assessment and Penetration Testing"[online].available: https://www.acunetix.com/blog/articles/difference-vulnerability-assessment-penetration-testing/, [Accessed: 20 April 2020].

[4]. Christopher Peake, "Red Teaming: The art of Ethical Hacking", Red Team Methodology, Journal of SANS Institute,2003, p. 9-14

[5]. "Red Team Penetration Testing"[online].available: https://www.coresecurity.com/what-red-team-security, [Accessed: 20 April 2020].

[6]. "Penetration Test Red Team Assessment: The Age Old Debate of Pirates vs. Ninjas Continues",[online].available: https://blog.rapid7.com/2016/06/23/penetration-testing-vs-red-teaming-the-age-old-debate-of-pirates-vs-ninja-continues/, [Accessed: 20 April 2020]

[7]. " Guide to red team Operations", What are the aspects of the Red team ?, https://www.hackingarticles.in/guide-to-red-team-operations/, [Accessed: 20 April 2020].

[8]. "Red team Guide", Second edition, Successful of Red team, Role of end user, Journal of Joint Force Commander and Chief of Staff, January 2013, p. 2:1 - 3:11.

[9]. MegaCorp One, "Penetration Test Report", Escalation to Local Administrator, Journal of Offensive Security Service, August 2013, p. 6-12.

BIOGRAPHIES

Khushboo Amin, Master of Technology, School of Information Technology and Cyber Security, Raksha Shakti University, Lavad, Gandhinagar, Gujarat, India.
Email: khushbooamin@outlook.com

Dr. Priyanka Sharma, Dean, Research & Development School of Information Technology & Cyber Security, Raksha Shakti University, Lavad, Gandhinagar, Gujarat, India.
Email: ps.it@rsu.ac.in