Competition 1 – Report

Mihir Katre

University at Albany, SUNY

BCYB 650 - Cyber Vulnerability Exploitation

Prof. Yuksel Celik

April 03, 2024

Contents

Executive Summary

This report provides a summary of the working environment, network, systems, and changes that were performed to defend the company systems from any possible attacks from adversaries, cyber attackers, or red team in this scenario.

This simulation was aimed towards strengthening of company assets, the blue team consisted of 6 people, working on 6 different UNIX machines to identify vulnerabilities, weaknesses and remediating any possible system flaws and overcoming any attack led by the red team.

The major objective of blue team as cyber defenders is to protect stealing or tampering of data, which was achieved by protecting the flag files, stopping unauthorized access towards the systems, breaking the persistence achieved by the red team and protecting the system from any attack that might lead towards compromising of confidentiality, integrity, and authorization.

Elaborating more towards the technical setup, it was assumed and configured in such a way that attackers are present inside the same network as of the victim machines (company assets), all the machines for this simulation were UNIX based and being in the same network, they were easily accessible to any attacker machine unless configured otherwise.

The blue team had to spend ample time understanding the network setup, having provided a /24 subnet range, there were lot of unidentified IP addresses that could have been attacking or accessing the victim machines. The team spent a lot of time towards identifying the installed packages, services, analyzing authorized users, groups, and their level of access, SSH keys any pre-configured scripts, automatic schedulers, firewall rules, open ports on the system and remediate them as per industry standards as well as company requirements.

There is only so much you can do to stop infiltrating, but we also need to have plan to deal with any scenarios of unauthorized access, the blue team continuously monitored the network traffic, list of active users, list of running services, CRON jobs, SSH connections, etc. on all the 6 machines intended to defend.

The summary can be concluded by stating that the blue team did a pretty good job in maintaining effective communication across the team, hardening the systems, protecting the network and would like to provide suggestions such as implementation of adept monthly patching cycles for remediating vulnerabilities on outdated packages, implementing bi-weekly security audits on critical files, monitoring users, groups and services running/installed on these systems.

Introduction

To continuously enhance the security of the systems it becomes ideal to run simulations such as red and blue teaming over the company assets to identify weaknesses, flaws and use these findings towards strengthening the systems and avoid exposure towards attacks.

Technical Environment

Virtualization Environment: Xen Orchestra.

Network Ranges: /24 subnet ranges consisting of the attacking and defending machines.

Operating Systems: The attacking and defending machines were having Ubuntu flavored 6 red team and 6 blue team machines.

Technical Ask

The blue team machines are configured with some weaknesses, outdated packages, lots of open services, ports, no security mechanisms, firewall rules, and no access restrictions of any kind.

One of the blue team machines also consists of FLAGS which the red team is supposed to get hold, these FLAGS can be referred to highly sensitive and private company data.

The task of blue teamers is to secure all the machines, implement adept security mechanisms, protect the FLAGS by moving them into secure places, and stop unauthorized access and persistence of any attackers to these systems.

Report Body – Steps Performed

As soon as the blue team gets access to the systems the blue team starts assigning assets to everyone that would work on securing and performing actions on. It is crucial to maintain effective communication and distribute tasks accordingly.

The blue team then follows a 5-minute plan which acts as a starting point to start securing the systems, as there are a lot of things to be done, this plan provides a good direction to start

executing the steps, the 5-minute plan can be found attached towards the end of the document with references.

The below are the steps followed by blue team to protect and harden the company assets:

1. **Change of Default Passwords:**

   The first step always performed by the blue team is to change all the default passwords assigned to all the users and replace them with strong alphanumeric passwords. The passwords of local admins as well as root user are changed to strong passwords so that attackers cannot utilize these weak passwords or users to gain access to the systems.

2. **Updating all the packages to their latest versions:**

   There were several outdated packages with many known vulnerabilities found present inside the system, this is why blue team ran an upgrade of all these default packages and updated them to their latest version which has almost no known vulnerabilities for exploiting. There were various packages we upgraded which could be exploited by red team using Metasploit to gain access to the servers.

3. **Start the wireshark capture:**

   As we carry on with further steps to harden our systems, we start capturing network traffic in the background using wireshark tool to continuously check for any unauthorized activity that might be happening over the network.

4. **Audit the passwd and shadow file:**

   The passwd file and shadow file stores the critical information about the users and groups present on the system with their access, encrypted passwords, and shell access. We check for this for any malicious users with terminal access or any process users with shell access and remediated and blocked access for unknown users.

5. **Check users and groups with sudo access:**

   We checked for all the users present in the SUDO group as they have escalated privileges to harm the systems, we could not find any malicious users with sudo access although we kept an eye that only our designated user has the sudo access.

6. **Encrypt and hide the flags:**

   The flags were present in the Downloads folder which could be easily viewed by anyone with system access. We created hidden folders inside the system directories recursively and moved the Flags inside them. Additionally, we also encrypted all the FLAG files with Open SSL tool using AES-256-CBC encryption by providing 2048-bit encryption key only known to the blue team. This ensures that even if some unauthorized user gets access to these FLAG files, they won't be able to view their contents without the key. The red team were unable to find the FLAG file location at all.

7. **Identify any active users on the system:**

   We continuously monitored our systems to check any SSH connections or any other users logged inside the system by monitoring the system processes and logs. At one instance we did find a logged in users and we executed a command to kill their process ID, changed the password and revoked terminal access of the user.

8. **Identify any existing SSH Keys on the system:**

   The pair of public and private SSH keys allows users to login inside the system without any password. We located all the files inside the user's directory and scan the entire system to locate these key pairs and deleted the occurrences. We did find some public and private keys created by the red team for their access inside the system and we erased them to stop their access.

9. **Disable SSH Root Login into the system:**

   We modified the sshd.config file which is responsible for providing configuration for SSH service and disabled the option of ROOT login to the system. This ensured that no user outside the system can SSH inside with root login.

10. **Check for any active CRON jobs running on the system:**

    CRON service in UNIX systems is used to schedule recurring tasks in specific intervals. We dig inside the CRON job files and ensured that there are no active tasks which are scheduled to run in specific intervals, we also deleted all active CRON jobs on the system.

11. **Identify Open Ports and Running Services:**

    The system has open ports to exploit by attackers as there might be some services running on them which are not necessarily used. We ran various commands to find out these unnecessary services and the ports they were running on, this ensures to reduce the attack surface.

12. **Monitor System Logs:**

    We kept monitoring system logs inside the /var/log directory for any errors inside the running services, any failed logins, unauthorized access. These logs provide great insights on what might be happening on the system.

Conclusion

The blue team would like to conclude the report stating that there are various requirements identified to implement continuous improvement plans for the company assets. As mentioned inside the report body, there are various instances such as outdated packages, malicious users and weak security mechanisms configured on the system which can act as an entry point for various threat actors which would in-turn compromise the systems.

This simulation acted as a brilliant opportunity to work more on system security and identifying weaknesses which can be missed out on during the day-to-day activities. As mentioned above, regular patching cycles, security audits, network scanning tools can be continuously implemented as part of security practices.

Performing such regular simulations provides enhanced way of security by regularly identifying weaklings and missed configurations. The blue and red team working in their best capacity to attack and defend a system in-turn contributes towards improving the overall security posture of the company.

References

https://github.com/MihirK21/CyberDefenceRepo/blob/main/Mihir%20Katre%20-%20Blue%20Team%20Plan%20HW%20Assignment.pdf

https://github.com/C0nd4/CCDC-Blueteam-Manual

https://systemoverlord.com/2015/08/15/blue-team-players-guide-for-pros-vs-joes-ctf/