A red background with white text

Description automatically generated

***Red Team Report:***

Ethical Penetration and Analysis of a Metasploitable3-Windows Server

By,

Mounika Lakamsani

Sravani Bokka

Nikhil Babu Jakkam

**Executive Summary:**

In this controlled cybersecurity exercise, our red team was tasked with ethically penetrating and analyzing a Metasploitable3-Windows server. We began with comprehensive planning and reconnaissance using tools like Nmap, Metasploit, Hydra, Ncrack, and Burp Suite. Our efforts focused on identifying and exploiting vulnerabilities, notably targeting ports 8022 and 4848, which hosted Apache Tomcat and GlassFish Server, respectively. Although we initially fell for a decoy dummy port, our persistence led to successful username cracking on the GlassFish server using Burp Suite. Despite challenges, our systematic approach enabled us to learn valuable lessons in cybersecurity attack strategies and defense mechanisms.

**Introduction:**

In this cybersecurity exercise, our team assumed the role of the red team, tasked with ethically penetrating and evaluating the security of a Metasploitable3-Windows server, mirroring the server of our opponents. Our approach involved detailed planning and execution of various cyber attack strategies. The primary objectives were to identify system vulnerabilities, gain unauthorized access, and maintain ethical standards throughout the exercise. Key phases included reconnaissance, vulnerability scanning, exploitation, and thorough documentation. Our initial action was an Nmap scan of the target server to identify open ports and potential vulnerabilities, setting the stage for subsequent penetration attempts and learning experiences.

**Team Composition and Roles:**

In this controlled cybersecurity exercise, our red team was composed of diverse roles and expertise, each contributing uniquely to our goal of ethically penetrating and analyzing the security of a Metasploitable3-Windows server. The team included network analysts responsible for reconnaissance and scanning, utilizing tools like Nmap to identify open ports and services. Ethical hackers, skilled in exploitation techniques, focused on targeting specific vulnerabilities, notably on Apache Tomcat and the GlassFish Server, employing tools like Metasploit, Hydra, and Ncrack. Our security testers, using Burp Suite, played a crucial role in cracking login credentials. Additionally, our documentation specialists meticulously recorded each step, ensuring a comprehensive and educational report of our findings and methodologies. This collaborative approach underlined the importance of varied skill sets in cybersecurity operations.

**Planning and Strategy:**

As the red team in this cybersecurity exercise, our primary strategy involved meticulously planning our approach to ethically penetrate and analyze the security of a Metasploitable3-Windows server. Our goals included identifying system vulnerabilities, gaining unauthorized access, and ensuring our actions remained within ethical boundaries. We employed a multi-faceted approach that started with reconnaissance to gather information about the target system. This was followed by scanning and vulnerability assessment using various tools to detect open ports and vulnerable services. We then moved to exploitation, where we attempted to exploit the identified vulnerabilities to gain access. Throughout the exercise, we meticulously documented our actions and findings for thorough analysis and reporting, using tools like Burp Suite and Nmap for effective execution. Our strategy was not only focused on breaching the system but also on learning and adapting our methods based on the responses and defenses of the target server.

**Planning the Attack:**

As the red team in a controlled cybersecurity exercise, we strategically planned and executed an ethical cyber attack on a Metasploitable3-Windows server. Our primary goals were to identify system vulnerabilities and gain unauthorized access while adhering to ethical guidelines. We began with comprehensive reconnaissance, utilizing an Nmap scan to identify open ports and potential vulnerabilities. Intrigued by an open port, 8022, we targeted Apache Tomcat using the Metasploit framework, successfully cracking the login credentials. However, we discovered this port was a decoy. Shifting focus to another open port, 4848, hosting a Glassfish Server, we deployed tools like Hydra and Ncrack for brute-forcing credentials. Ultimately, our perseverance in password cracking was rewarded when we used Burp Suite to infiltrate the server, demonstrating our ability to mimic cyber attackers while gaining invaluable insights into cybersecurity defense mechanisms.

**Attack Simulation:**

As the red team in a cybersecurity exercise, we focused on ethically breaching a Metasploitable3-Windows server. Our strategy involved comprehensive reconnaissance, using tools like Nmap for scanning and identifying vulnerabilities, and exploiting these using frameworks like Metasploit. Notably, we targeted Apache Tomcat on port 8022, successfully cracking credentials only to discover it was a decoy. We then shifted our efforts to a GlassFish Server on port 4848, where we employed tools like Hydra, Ncrack, and especially Burp Suite for password cracking. Although we faced challenges, our persistent and methodical approach led to significant learning experiences in cybersecurity practices.

**Our strategy included:**

* **Reconnaissance:** Gathering as much information about the target system as possible.
* **Scanning and Vulnerability Assessment:** Using tools to detect open ports and vulnerable services.
* **Exploitation:** Attempting to exploit identified vulnerabilities to gain access.
* **Documentation:** Recording our actions and findings for analysis and reporting.
* **Execution:** Cyber Offense in Action

A computer screen shot of a program

Description automatically generated**Conducting an Nmap Scan:**

**Initial Reconnaissance**

Our first step in this exercise was to conduct a comprehensive Nmap scan of the IP address 172.31.17.157. This initial reconnaissance aimed to identify open ports and running services that could potentially be exploited. The scan results were illuminating, revealing several open ports which are detailed in the attached document. It shows that a total of 12 TCP ports are open on the targeted machine. The open ports listed include 80/tcp (HTTP), 135/tcp (MSRPC), 139/tcp (netbios-ssn), 443/tcp (HTTPS), 445/tcp (microsoft-ds), 1433/tcp (ms-sql-s), 4848/tcp (appserv-http), 7676/tcp (iJMS), 8080/tcp (HTTP-alt), 8181/tcp (unknown), 4848/tcp (appserv-https), and 49152/tcp (unknown). These open ports suggest that various services, such as web servers (HTTP and HTTPS), Microsoft network services (MSRPC, netbios-ssn, microsoft-ds), SQL server, and application servers, are running and accessible on the machine.

**Exploiting Port 8022**

**Attempted Breach on Apache Tomcat:**

Among the various open ports, port 8022 particularly piqued our interest. Attempting to access 172.31.17.157:8022, we were redirected to a web service, which we identified as Apache Tomcat. Sensing an opportunity, we launched an attack using the Metasploit framework, aiming to exploit known vulnerabilities in Apache Tomcat.

A screenshot of a computer

Description automatically generated

**Cracking Credentials:**

Our strategy involved employing a variety of hacking techniques to retrieve the username and password. After several attempts and methodical use of different Metasploit modules, we successfully deciphered the login credentials. Triumphantly, we used these credentials to gain access to the service.

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

**The Discovery of a Dummy Port:**

Upon gaining access, we conducted a thorough examination of the system. To our surprise, we discovered that the port was a decoy—a dummy port designed to mislead potential attackers. It was a dead end, but this realization was a valuable part of our learning journey.

**Targeting Port 4848: GlassFish Server**

**Initial Discovery and Access Attempts:**

Upon further investigation, we identified an open port, 4848, which led us to a service identified as "Glassfish Server open-source edition." The service was protected with a username and password authentication mechanism. Eager to gain access, we deployed multiple tools in an attempt to crack these credentials.

A screenshot of a computer

Description automatically generated

**Utilizing Hydra and Ncrack:**

We first used the Hydra tool, renowned for its efficiency in brute-forcing login credentials. Alongside Hydra, we employed Ncrack, a high-speed network authentication cracking tool. Despite our concerted efforts with these tools, and keeping the Metasploitable console open for real-time monitoring, we did not achieve the breakthrough we anticipated.

**Breakthrough with Burp Suite**

**Successful Username Cracking**

Undeterred, we turned our attention to Burp Suite, an integrated platform for performing security testing of web applications. Our persistence paid off when we successfully cracked the username after an extensive session of trial and error, using default user and password files.

A screenshot of a computer

Description automatically generated

**Password Cracking Endeavor**

**Setting Up Burp Suite for the Attack:**

With the username in hand, our next objective was to crack the password. We set up Burp Suite, ensuring the intercept feature was turned off in the Proxy tab. We then accessed the login page of the GlassFish server in our browser.

A close-up of a computer screen

Description automatically generated

**Capturing the Login Request:**

Upon visiting the login page, we turned on the intercept feature in Burp Suite's Proxy tab. This allowed us to capture the login request, which we could then manipulate. We right-clicked on the request in the Intercept tab and sent it to Burp Suite's Intruder module.

**Configuring the Intruder for Password Cracking:**

In the Intruder's "Payloads" tab, we configured our attack. We set the "Payload set" to "1" and chose "Simple list" as the "Payload type." In the "Payload settings" field, we entered several potential passwords, some manually and others from a custom payload list.

A screenshot of a computer

Description automatically generated

**Planning the Attack Vulnerability Assessment:**

In our role as the red team in a controlled cybersecurity exercise, our initial strategy focused on comprehensive planning and vulnerability assessment of a Metasploitable3-Windows server. We set clear objectives to identify system vulnerabilities, gain unauthorized access, and adhere to the ethical boundaries of the exercise. Our approach involved detailed reconnaissance to gather as much information as possible about the target system, followed by scanning and vulnerability assessment using various tools to detect open ports and vulnerable services. This meticulous planning was crucial in preparing for the exploitation phase, where we aimed to leverage identified vulnerabilities to gain access, all while meticulously documenting our actions and findings for thorough analysis and reporting.

**Challenges and Mitigation:**

We faced significant challenges in penetrating the Metasploitable3-Windows server. Our initial Nmap scans and exploitation attempts on ports like 8022 (Apache Tomcat) and 4848 (GlassFish Server) were met with hurdles, including decoy ports and robust security measures. However, we overcame these obstacles through persistence and adapting our strategies. Tools like Metasploit, Hydra, Ncrack, and particularly Burp Suite proved instrumental in our success, allowing us to crack credentials and gain unauthorized access. Throughout, we ensured our actions remained within ethical boundaries, focusing on learning and improving our cyber offense skills.

**Learning Outcome:**

Our primary learning outcomes included mastering various hacking techniques and tools, such as Nmap, Metasploit, Hydra, Ncrack, and Burp Suite. We gained hands-on experience in conducting reconnaissance, scanning for vulnerabilities, and exploiting them, especially with the intriguing challenge presented by Apache Tomcat and the GlassFish server. Importantly, we learned the significance of adaptability and persistence in cybersecurity, as evidenced by our strategic shift to Burp Suite for successful credential cracking. Additionally, the discovery of a dummy port underscored the importance of expecting and identifying potential traps or decoys in real-world cybersecurity scenarios. This exercise not only enhanced our technical skills but also deepened our understanding of ethical hacking practices within the bounds of a controlled environment.

**Conclusion**

We successfully executed a series of strategic cyberattacks on a Metasploitable3-Windows server. Our approach involved detailed reconnaissance, employing tools like Nmap, Metasploit, Hydra, Ncrack, and Burp Suite to identify vulnerabilities and attempt breaches. We discovered open ports and services, cracked login credentials, and learned from deceptive elements like a dummy port. Our efforts in exploiting the Apache Tomcat and GlassFish Server demonstrated our adaptability and persistence. This exercise was not only a testament to our team's technical skills but also highlighted the importance of ethical hacking in strengthening cybersecurity defenses.

**Appendices**

Key documentation includes our successful breach of Apache Tomcat via Metasploit, revealing it as a decoy, and our attempts to infiltrate the GlassFish Server on port 4848 using tools like Hydra, Ncrack, and Burp Suite. We successfully cracked the username with Burp Suite and meticulously documented the setup and configuration process for this attack, capturing login requests and configuring payload settings for effective password cracking.

**References:**

* Rapid7 Blog - "Metasploitable3: An Intentionally Vulnerable Machine for Exploit Testing":https://www.rapid7.com/blog/post/2016/11/15/test-your-might-with-the-shiny-new-metasploitable3/
* HackerSploit Blog - "Metasploitable 3 Installation Guide": https://hackersploit.org/metasploitable-3-installation-guide/
* Kali Linux Tutorials - "How to Install Metasploitable3 on Windows": <https://kalilinuxtutorials.com/install-metasploitable3-windows/>
* SecurityOnline - "Learn Penetration Testing with Metasploitable3": https://securityonline.info/learn-penetration-testing-metasploitable3/
* Metasploit Documentation - "Setting Up a Vulnerable Target": https://docs.rapid7.com/metasploit/setting-up-a-vulnerable-target/