Project Report: Honeypot and Attack Simulation

1. Introduction

Overview

The rise in cyber threats necessitates innovative methods to enhance security measures and understand the behavior of attackers. This project focused on deploying a honeypot to simulate an attack environment, allowing us to study various attack techniques while gaining insights into common vulnerabilities. We utilized several tools, including Cowrie, Nmap, Hydra, and Metasploit, to create a robust framework for this analysis.

Objectives

* To deploy a honeypot (Cowrie) that emulates vulnerable systems.
* To conduct network reconnaissance using Nmap.
* To perform password attacks with Hydra.
* To simulate and analyze attacks using Metasploit.

2. Tools Used

2.1 Cowrie

Cowrie is a popular SSH and Telnet honeypot designed to log brute-force attacks and the entire shell interaction. It captures shell commands entered by attackers and records the session, providing valuable data for analysis.

2.2 Nmap

Nmap (Network Mapper) is an open-source tool used for network discovery and security auditing. It allows us to scan our honeypot to identify open ports and services, facilitating the selection of potential targets for attack simulations.

2.3 Hydra

Hydra is a fast and flexible password-cracking tool that supports various protocols. It is useful for executing brute-force attacks on the services running on the honeypot.

2.4 Metasploit

Metasploit is a penetration testing framework that provides the infrastructure, content, and tools to conduct penetration tests and security assessments. It includes various exploits and payloads that help simulate real-world attacks.

3. Methodology

3.1 Honeypot Deployment

* **Installation of Cowrie**: We installed Cowrie on a virtual machine, configuring it to listen on standard SSH and Telnet ports.
* **Logging Configuration**: Cowrie was configured to log all interactive sessions and attacks, allowing for analysis of attacker behavior.

3.2 Network Scanning with Nmap

We conducted regular Nmap scans against our honeypot to detect any insecure configurations or vulnerabilities.

**Command Used**: `nmap -sS -p 22,23 {Honeypot\_IP}` to scan for open services.

3.3 Password Cracking with Hydra

Using Hydra, we targeted the SSH service to conduct a brute-force attack.

**Command Used**: `hydra -l admin -P password\_list.txt ssh://{Honeypot\_IP}`

This identified weak or common passwords, demonstrating how attackers often exploit poor password hygiene.

3.4 Exploit Simulation with Metasploit

We used Metasploit to perform a simulated attack on the services running on our honeypot.

**Commands & Techniques**: Utilized existing exploits specific to the services identified during the Nmap scan to compromise the honeypot and see what information could be gathered.

4. Results

4.1 Data Analysis

Cowrie logged a significant number of attack attempts, with most being SSH brute-force attempts using common usernames and passwords.

Nmap results showed various open ports beyond SSH and Telnet that we did not initially configure, indicating potential misconfigurations.

Hydra successfully cracked a few weak passwords, highlighting the importance of strong password policies.

Metasploit revealed possible vulnerabilities that could be exploited if similar systems were deployed in production without adequate security controls.

5. Discussion

The project underscored the effectiveness of honeypots as a proactive security measure. By simulating attacks and observing how they unfold, we gained crucial insights into the tactics, techniques, and procedures (TTPs) employed by malicious actors. Moreover, the project emphasized the need for organizations to continuously monitor their systems, employ effective security measures, and educate users about strong password practices to mitigate the risk of unauthorized access.

6. Conclusion

The honeypot project was a valuable learning experience, enhancing our understanding of cybersecurity threats and the tools available to analyze them. The deployment of Cowrie facilitated the monitoring of real-world attacks, while Nmap, Hydra, and Metasploit provided practical exercises in network security and vulnerability assessment.