|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Vulnerability Scanning 1 (Core)  Otis Smith / Cybersecurity Professional / 11.1.23 |  |
|  |  |  |  |
| Pipette dropping liquid in a petri dish | | | |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | |
|  |  | TABLE OF CONTENTS |  |
|  |  | Summary …………………………..  Discovery……………………………  Vulnerability……………………….  Exploitation………………………..  References.………………………..  Mitigation………………………….. |  |



|  |  |  |
| --- | --- | --- |
| Summary |  | |
| This Vulnerability Scanning exercise aimed to scan, enumerate, and exploit a target using the Metasploit framework. The process involved downloading a password file, scanning Metasploitable 3 for open ports, specifically 4848, 8080, and 8181, and conducting a successful brute force attack on the GlassFish server. The subsequent exploitation phase utilized Metasploit to gain unauthorized access and establish a reverse shell on the target machine, achieving the exercise's learning objectives.  A hand holding a glowing city  Description automatically generated | |  |
| Discovery   1. Resource Acquisition:    * Successfully downloaded the password file (passwd\_list2023.txt) for use in the lab. 2. Metasploitable 3 Initialization:    * Launched the Metasploitable 3 Windows virtual machine.    * Logged in as the administrator to Metasploitable 3.    * A screenshot of a computer       Description automatically generated 3. Port Scanning and Enumeration:    * Conducted an advanced nmap scan to identify open ports and vulnerabilities on the Metasploitable3 machine.    * Uncovered information on ports 4848, 8080, and 8181 associated with Oracle GlassFish 4.0.   A screenshot of a computer  Description automatically generated | |  |
|  | |  |

|  |  |  |
| --- | --- | --- |
| Vulnerability |  | |
| 1. Brute Force Attack:    * Utilized Metasploit to perform a brute force attack on the GlassFish server.   A screenshot of a computer program  Description automatically generated   * + Configured Metasploit settings, including RHOST, THREADS, STOP\_ON\_SUCCESS, VERBOSE, SSL, and RPORT.   A screenshot of a computer  Description automatically generated   * + Successfully identified the password 'admin:sploit' after 35 minutes of brute force.   A screen shot of a computer  Description automatically generated | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Exploitation |  | |  | |  |
| 1. Metasploit Exploitation:    * Explored Metasploit modules related to GlassFish using commands such as 'search glassfish.'      * + Selected the appropriate module "exploit/multi/http/glassfish\_deployer" for Authenticated Code Execution.   A screenshot of a computer  Description automatically generated   * + Configured module options, including PASSWORD, RHOSTS, and SSL settings.   A screenshot of a computer program  Description automatically generated   * + Loaded Metasploit with the selected payload "payload/java/meterpreter/reverse\_tcp."   A screenshot of a computer  Description automatically generated   1. Payload Setup:    * Configured payload settings using the Java Meterpreter reverse TCP stager.   A screenshot of a computer  Description automatically generated   * + Set the target as Metasploitable3 and initiated the exploit.   + Gained access to the target machine through a reverse shell.      |  |  |  |  | | --- | --- | --- | --- | | References |  |  |  |   No external references were utilized for this exercise. | |  | |  | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | |  |  | | |  | |  |   Mitigation:   1. **Password Management:**    * Enforce strong password policies to mitigate the risk of successful brute force attacks. 2. Patch Management:    * Regularly apply security patches to address vulnerabilities in services like GlassFish. 3. Network Segmentation:    * Implement network segmentation to limit the impact of successful intrusions. 4. Intrusion Detection System (IDS):    * Employ an IDS to detect and respond to suspicious activities in real-time. 5. User Training:    * Provide security awareness training to users to recognize and report phishing attempts. 6. Service Hardening:    * Disable unnecessary services and harden configurations to reduce the attack surface.   Conclusion:  This Vulnerability Scanning exercise provided hands-on experience in scanning, enumerating, and exploiting a target using Metasploit. The comprehensive report outlines the steps taken, from resource acquisition to the successful exploitation of the GlassFish server on Metasploitable 3. The mitigation strategies underscore the importance of proactive security measures, including robust password management, timely patching, network segmentation, intrusion detection, user training, and service hardening. |  | |
|  | |  |