|  |  |
| --- | --- |
| **Vulnerability 17** | **Findings** |
| **Title** | Shellshock (CVE-2014-6271) |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | critical |
| **Description** | A Shellshock vulnerability was discovered on host 192.168.13.11, allowing an attacker to exploit services that allow unauthorized remote users to assign Bash environment variables using Metasploit. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.11 |
| **Remediation** | To remediate the issue of a Shellshock vulnerability being discovered on host 192.168.13.11, you should verify the existence of the vulnerability by performing testing and enabling a Web Application Firewall (WAF) to detect and block malicious traffic that may be attempting to exploit the vulnerability. Additional measures, such as input validation and regular security assessments, may also be necessary to fully secure the host against Shellshock attacks. |

|  |  |
| --- | --- |
| **Vulnerability 18** | **Findings** |
| **Title** | Apache Struts Jakarta Multipart Parser OGNL Injection (Metasploit) (CVE-2017-5638) |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | critical |
| **Description** | An Apache Struts vulnerability was discovered through a Nessus scan of the host. The vulnerability was successfully exploited using Metasploit, allowing for remote code execution on the host. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.12 |
| **Remediation** | To remediate the issue of an Apache Struts vulnerability being discovered on the host, you should upgrade to the most recent version of Apache Struts after performing appropriate testing. This will help to ensure that any known vulnerabilities, including the one that was exploited in the previous statement, have been fixed and that the risk of successful exploitation of the vulnerability is reduced. Additional measures, such as input validation and regular security assessments, may also be necessary to fully secure the host against exploitation of the Apache Struts vulnerability. |

|  |  |
| --- | --- |
| **Vulnerability 19** | **Findings** |
| **Title** | Drupal Core RCE (CVE-2019-6340) |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | High |
| **Description** | A Drupal RESTful Web Services unserialize() Remote Code Execution (RCE) vulnerability was discovered due to the lack of field sanitization from non-form sources. This vulnerability allows for arbitrary remote code execution on the host server. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.13 |
| **Remediation** | To remediate the issue of a Drupal RESTful Web Services unserialize() Remote Code Execution (RCE) vulnerability being discovered on the host, you should upgrade to the most recent version of Drupal. This will help to ensure that any known vulnerabilities, including the one described in the previous statement, have been fixed and that the risk of successful exploitation of the vulnerability is reduced. Additional measures, such as input validation and regular security assessments, may also be necessary to fully secure the host against exploitation of the Drupal RESTful Web Services un-serialize() RCE vulnerability. It is recommended to follow best practices when using Drupal and its RESTful Web Services, including ensuring that only trusted users have access to these features. |

|  |  |
| --- | --- |
| **Vulnerability 20** | **Findings** |
| **Title** | Sudo 1.8.27 – Security Bypass (CVE-2019-14287) |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | High |
| **Description** | A security policy bypass vulnerability was discovered that allows users to execute commands as root in the terminal, despite the user's permissions being explicitly restricted from running these commands as root in the sudoers file. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.14 |
| **Remediation** | To remediate the issue of a security policy bypass vulnerability that allows users to execute commands as root in the terminal despite being restricted in the sudoers file, you should upgrade to a version of sudo that is released after version 1.8.28. This can be done using the command **sudo apt-get upgrade**, which will update all packages on the system, including sudo, to their latest available versions. It is recommended to carefully review the list of packages that will be updated before running this command to ensure that you do not inadvertently update any critical packages that may be incompatible with your system. Additionally, it is recommended to implement additional security measures such as input validation or sanitization, as well as performing regular security assessments to ensure the continued security of the system. |

|  |  |
| --- | --- |
| **Vulnerability 21** | **Findings** |
| **Title** | Sensitive Data Exposure |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Medium |
| **Description** | Using open-source intelligence (OSINT) searches, exposed data was discovered on totalrekall's GitHub repositories, including IP information, open ports, and credentials to access totalrekall servers. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.0/24 |
| **Remediation** | To remediate the issue of exposed data being discovered on totalrekall's GitHub repositories, efforts should focus on minimizing the amount and sensitivity of data available to external parties. This can be achieved through implementing measures such as input validation or sanitization, as well as performing regular security assessments to ensure the continued security of the system. By reducing the amount of data that is available to external parties and minimizing the sensitivity of the data that is available, you can limit the information that is available to potential attackers and reduce the risk of successful exploitation of the data. It is recommended to follow best practices when using GitHub and other online platforms, including ensuring that only trusted users have access to sensitive data. |

|  |  |
| --- | --- |
| **Vulnerability 22** | **Findings** |
| **Title** | Anonymous FTP Vulnerability (CVE-1999-0497) |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Information |
| **Description** | An anonymous FTP vulnerability was discovered on an open port of the host, allowing for remote access to the server through an unsecure FTP open port using anonymous login. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20, Port 21 |
| **Remediation** | To remediate the issue of an anonymous FTP vulnerability discovered on an open port of the host, it is recommended to disable anonymous FTP login and use firewall rules to limit access. By disabling anonymous FTP login, you can ensure that only authenticated users are able to access the server via FTP. By using firewall rules to limit access, you can further restrict access to the server and reduce the risk of successful exploitation of the vulnerability. Additionally, it is recommended to implement additional security measures such as input validation or sanitization, as well as performing regular security assessments to ensure the continued security of the system. It is also recommended to follow best practices when using FTP and other protocols, including ensuring that only trusted users have access to the server. |

|  |  |
| --- | --- |
| **Vulnerability 23** | **Findings** |
| **Title** | Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (CVE-2003-0264) |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | critical |
| **Description** | An open port 110 on the host was found to be vulnerable to SLMail attacks. Using the windows/pop3/seattlelab\_pass exploit in Metasploit, we were able to successfully exploit this vulnerability and gain a Meterpreter session on the host. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20, Port 110 |
| **Remediation** | To remediate the issue of a vulnerability in SLMail due to an open port 110 on the host, it is recommended to upgrade SLMail or restrict access to the service. Upgrading SLMail will ensure that the latest security updates and patches are applied to the system, which can help to reduce the risk of successful exploitation of the vulnerability. Alternatively, if upgrading is not feasible or practical, restricting access to the service can also help to reduce the risk of successful exploitation by limiting the number of potential attackers who are able to reach the vulnerable service. It is also recommended to implement additional security measures such as input validation or sanitization, as well as performing regular security assessments to ensure the continued security of the system. It is also recommended to follow best practices when using mail servers and other services, including ensuring that only trusted users have access to the system. |

Add any additional vulnerabilities below.