Risk Assessment

This is a report of all the existing risks in your systems.

|  |  |
| --- | --- |
| Risk Statement | The Linux Exploit Suggester identified several potential vulnerabilities (CVEs) in the system's kernel and sudo configuration. While the likelihood of successful exploitation depends on various factors, the presence of these vulnerabilities poses a significant risk. |
| Risk Likelihood | High |
| Risk Impact | Very High |
| Impact of Risk on system | Attackers could potentially exploit vulnerabilities in the system's kernel or sudo configuration to gain root privileges. |
| What to do | Update your system's kernel and sudo to the latest versions. Ensure that all security patches are applied. Contact your IT administrator or security professional for guidance on addressing these vulnerabilities. |

|  |  |
| --- | --- |
| Risk Statement | The Linpeas output revealed the presence of network discovery and port scanning tools (fping, bash, nc, nmap). An attacker could use these tools to map the system's network, identify open ports, and potentially exploit vulnerabilities. |
| Risk Likelihood | Medium |
| Risk Impact | High |
| Impact of Risk on system | Attackers could use these tools to map the system's network, identify open ports, and potentially exploit vulnerabilities. |
| What to do | Review the network discovery and port scanning tools listed in the Linpeas output. If any are not needed, remove them immediately. Consult your IT administrator for assistance if needed. Regularly update these tools to ensure they have the latest security patches. |

|  |  |
| --- | --- |
| Risk Statement | The Linpeas output shows several writable configuration files, including systemd service files. An attacker could modify these files to compromise the system. |
| Risk Likelihood | High |
| Risk Impact | High |
| Impact of Risk on system | Attackers could modify these files to compromise the system. |
| What to do | Review the writable configuration files listed in the Linpeas output. If any are not expected to be writable, change their permissions to restrict write access to only authorized users. Consult your IT administrator for assistance if needed. |

|  |  |
| --- | --- |
| Risk Statement | Multiple vulnerabilities were identified in the system, including the presence of writable files in critical directories (/etc/passwd), SUID/SGID binaries with potential for privilege escalation, and the availability of network discovery and port scanning tools. These vulnerabilities, combined with the lack of several security protections, create a high likelihood of successful exploitation. |
| Risk Likelihood | Very High |
| Risk Impact | Very High |
| Impact of Risk on system | These vulnerabilities, combined with the lack of several security protections, create a high likelihood of successful exploitation. |
| What to do | Because you are already root and you have identified several risks, you should immediately contact your IT administrator or security professional. They can help you secure your system and prevent unauthorized access. Do not attempt to fix these issues yourself unless you are an experienced IT professional. |

|  |  |
| --- | --- |
| Risk Statement | The Linpeas output shows environment variables containing sensitive information such as SSH\_AGENT\_PID and XAUTHORITY. While not directly exploitable, this information could aid an attacker in further compromising the system. |
| Risk Likelihood | Medium |
| Risk Impact | Medium |
| Impact of Risk on system | An attacker could use this information to further compromise the system. |
| What to do | Review the environment variables listed in the Linpeas output. If any contain sensitive information, remove or change them immediately. Consult your IT administrator for assistance if needed. |

|  |  |
| --- | --- |
| Risk Statement | The Linpeas output identified several SUID/SGID binaries. These files have elevated privileges and could be exploited by attackers to gain root access if vulnerabilities exist within them. |
| Risk Likelihood | High |
| Risk Impact | Very High |
| Impact of Risk on system | Attackers could potentially exploit vulnerabilities in the system's kernel or sudo configuration to gain root privileges. |
| What to do | Review the SUID/SGID binaries listed in the Linpeas output. If any are not required, remove them or change their ownership and permissions to reduce the risk of exploitation. Consult your IT administrator for assistance if needed. |

|  |  |
| --- | --- |
| Risk Statement | The Linpeas output indicates that several security protections (AppArmor, grsecurity, PaX, Execshield, SELinux, Seccomp) are not enabled or are disabled. This significantly weakens the system's defenses against attacks. |
| Risk Likelihood | High |
| Risk Impact | High |
| Impact of Risk on system | This significantly weakens the system's defenses against attacks. |
| What to do | Enable and configure appropriate security protections, such as AppArmor, SELinux, or Seccomp, to enhance the system's security posture. Consult your IT administrator or security professional for guidance on configuring these protections. |

|  |  |
| --- | --- |
| Risk Statement | The Linpeas output shows several software packages that have known vulnerabilities or are outdated. These vulnerabilities could be exploited by attackers. |
| Risk Likelihood | Medium |
| Risk Impact | High |
| Impact of Risk on system | These vulnerabilities could be exploited by attackers. |
| What to do | Update all software packages to their latest versions. Ensure that all security patches are applied. Regularly check for and install updates to minimize the risk of exploitation. |

|  |  |
| --- | --- |
| Risk Statement | The Linpeas output shows that several ports are open. These open ports could be exploited by attackers to gain unauthorized access to the system. |
| Risk Likelihood | Medium |
| Risk Impact | High |
| Impact of Risk on system | These open ports could be exploited by attackers to gain unauthorized access to the system. |
| What to do | Review the open ports listed in the Linpeas output. If any ports are not needed, close them immediately. Consult your IT administrator for assistance if needed. Regularly review and update firewall rules to ensure only necessary ports are open. |

|  |  |
| --- | --- |
| Risk Statement | The Linpeas scan revealed the presence of sensitive data in various files, such as password hashes and API keys (if the '-r' parameter had been used). This data could be exploited by attackers. |
| Risk Likelihood | Medium |
| Risk Impact | High |
| Impact of Risk on system | This data could be exploited by attackers. |
| What to do | Review the sensitive data listed in the Linpeas output. If any sensitive data is found, remove or change it immediately. Consult your IT administrator for assistance if needed. Implement secure storage mechanisms for sensitive information. |