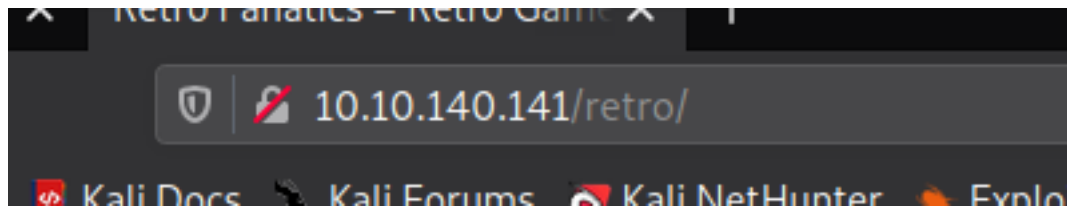


Retro

Enumeration

Webserver has a directory named retro



Only http and rdp is running

we see that retro is running wordpress

CMS



[WordPress](#) 5.2.1

Programming languages



[PHP](#) 7.1.29

Blogs



[WordPress](#) 5.2.1

Operating systems



[Windows Server](#)

Font scripts




[Font Awesome](#)

Databases



[MySQL](#)

 [Google Font API](#)

JavaScript libraries



[jQuery](#)

Web servers



[IIS](#) 10.0



[jQuery Migrate](#) 1.4.1

we ran wpscan and found a possible user

```
[i] User(s) Identified:

[+] wade
  | Found By: Author Posts - Author Pattern (Passive Detection)
  | Confirmed By:
  |   Wp Json Api (Aggressive Detection)
  |     - http://10.10.140.141/retro/index.php/wp-json/wp/v2/users/?per_page=100&page=1
  |   Author Id Brute Forcing - Author Pattern (Aggressive Detection)
  |   Login Error Messages (Aggressive Detection)

[+] Wade
  | Found By: Rss Generator (Passive Detection)
  | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/
```

ON viewing users posts ,saw a comment which could be a potential password

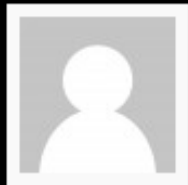
One Comment on "Ready Player One"

Wade

December 9, 2019

Leaving myself a note here just in case I forget how to spell it: [parzival](#)

REPLY

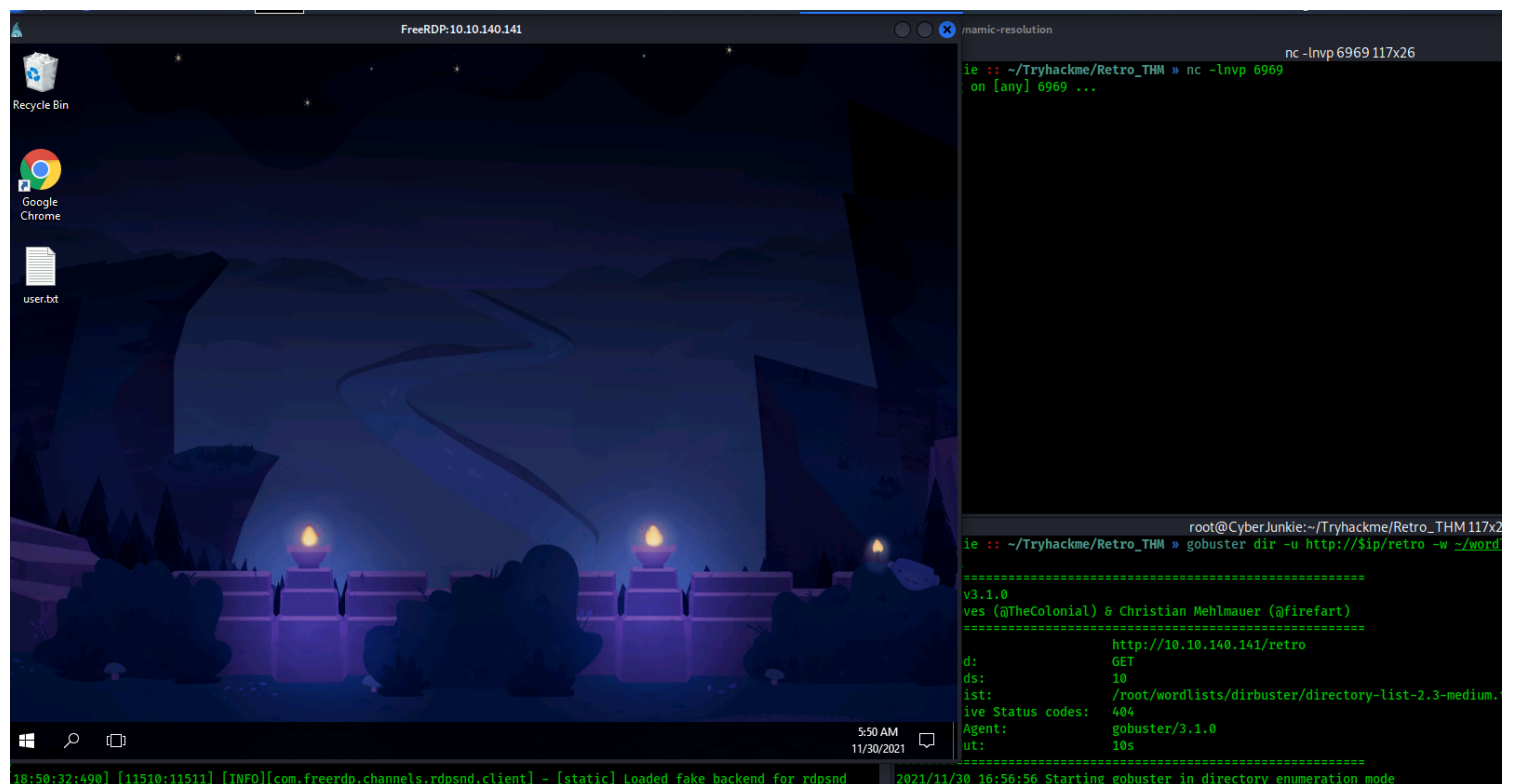


We logged in wp dashboard

Running (JUST GUESSING): Microsoft Windows 2016 (89%), FreeBSD 6.X (85%)
 OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:freebsd:freebsd:6.2
 OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
 Aggressive OS guesses: Microsoft Windows Server 2016 (89%), FreeBSD 6.2-RELEASE (85%)
 No exact OS matches for host (test conditions non-ideal).
 TCP/IP fingerprint:
 SCAN(V=7.92%E=4%D=11/30%OT=80%CT=%CU=%PV=Y%G=N%TM=61A69D1F%P=x86_64-pc-linux-gnu)
 SEQ(SP=101%GCD=1%ISR=10B%TS=A)
 SEQ(SP=101%GCD=1%ISR=10B%TI=I%TS=A)
 OPS(O1=M505NW8ST11%O2=M505NW8ST11%O3=M505NW8NNT11%O4=M505NW8ST11%O5=M505NW8ST11%O6=M505ST11)
 WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)
 ECN(R=Y%DF=Y%TG=80%W=2000%O=M505NW8NNS%CC=Y%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=N)
 Uptime guess: 0.014 days (since Tue Nov 30 16:33:03 2021)
 TCP Sequence Prediction: Difficulty=257 (Good luck!)
 IP ID Sequence Generation: Incremental
 Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Exploitation

Eventually i couldnt get the wordpress rce to get a shell back but using same wade credentials on rdp gave us a session



LOLzzzz

PostExploitation

we had a UAC shell elevated bug butit wasnt working because of a problem with the box

running exploit suggerter got us some potential exploits

```

<0x1b>[1;34m*]<0x1b>[0;0m attempting to read from the systeminfo input file
<0x1b>[1;32m+]<0x1b>[0;0m systeminfo input file read successfully (ascii)
<0x1b>[1;34m*]<0x1b>[0;0m querying database file for potential vulnerabilities
<0x1b>[1;34m*]<0x1b>[0;0m comparing the 0 hotfix(es) against the 160 potential bulletins(s) with a database of 137 known exploits
<0x1b>[1;34m*]<0x1b>[0;0m there are now 160 remaining vulns
<0x1b>[1;34m*]<0x1b>[0;0m searching for local exploits only
<0x1b>[1;32m+]<0x1b>[0;0m [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
<0x1b>[1;32m+]<0x1b>[0;0m windows version identified as 'Windows 10 64-bit'
<0x1b>[1;34m*]<0x1b>[0;0m
<0x1b>[1;32mM]<0x1b>[0;0m MS16-075: Security Update for Windows SMB Server (3164038) - Important
<0x1b>[1;34m*]<0x1b>[0;0m https://github.com/foxglovesec/RottenPotato
<0x1b>[1;34m*]<0x1b>[0;0m https://github.com/Kevin-Robertson/Tater
<0x1b>[1;34m*]<0x1b>[0;0m https://bugs.chromium.org/p/project-zero/issues/detail?id=222 -- Windows: Local WebDAV NTLM Reflection Elevation of Privilege
<0x1b>[1;34m*]<0x1b>[0;0m https://foxglovesecurity.com/2016/01/16/hot-potato/ -- Hot Potato - Windows Privilege Escalation
<0x1b>[1;34m*]<0x1b>[0;0m
<0x1b>[1;32mE]<0x1b>[0;0m MS16-032: Security Update for Secondary Logon to Address Elevation of Privile (3143141) - Important
<0x1b>[1;34m*]<0x1b>[0;0m https://www.exploit-db.com/exploits/40107/ -- MS16-032 Secondary Logon Handle Privilege Escalation, MSF
<0x1b>[1;34m*]<0x1b>[0;0m https://www.exploit-db.com/exploits/39574/ -- Microsoft Windows 8.1/10 - Secondary Logon Standard Handles Missing Sanitization Priv
<0x1b>[1;34m*]<0x1b>[0;0m https://www.exploit-db.com/exploits/39719/ -- Microsoft Windows 7-10 & Server 2008-2012 (x32/x64) - Local Privilege Escalation (MS1
<0x1b>[1;34m*]<0x1b>[0;0m https://www.exploit-db.com/exploits/39809/ -- Microsoft Windows 7-10 & Server 2008-2012 (x32/x64) - Local Privilege Escalation (MS1
<0x1b>[1;34m*]<0x1b>[0;0m
<0x1b>[1;32mM]<0x1b>[0;0m MS16-016: Security Update for WebDAV to Address Elevation of Privilege (3136041) - Important
<0x1b>[1;34m*]<0x1b>[0;0m https://www.exploit-db.com/exploits/40085/ -- MS16-016 mrxdav.sys WebDav Local Privilege Escalation, MSF
<0x1b>[1;34m*]<0x1b>[0;0m https://www.exploit-db.com/exploits/39788/ -- Microsoft Windows 7 - WebDAV Privilege Escalation Exploit (MS16-016) (2), PoC
<0x1b>[1;34m*]<0x1b>[0;0m https://www.exploit-db.com/exploits/39432/ -- Microsoft Windows 7 SP1 x86 - WebDAV Privilege Escalation (MS16-016) (1), PoC
<0x1b>[1;34m*]<0x1b>[0;0m

```

we were able to eleavte to system via ms16_075 exploit and transfered a exploit binary which spawned a system shell for us

```

C:\> Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>cd c
The system cannot find the path specified.

C:\Windows\system32>cd c/
The system cannot find the path specified.

C:\Windows\system32>cd ../../

C:\>cd users

C:\Users>cd Administrator

C:\Users\Administrator>cd Desktop

C:\Users\Administrator\Desktop>type root.txt.txt
7958b569565d7bd88d10c6f22d1c4063
C:\Users\Administrator\Desktop>_

```

7958b569565d7bd88d10c6f22d1c4063

Loot

Credentials

wordpress

wade : parzival

RDP

wade : parzival

Flags

User Flag

3b99fbd6d430bfb51c72c651a261927

system flag

7958b569565d7bd88d10c6f22d1c4063