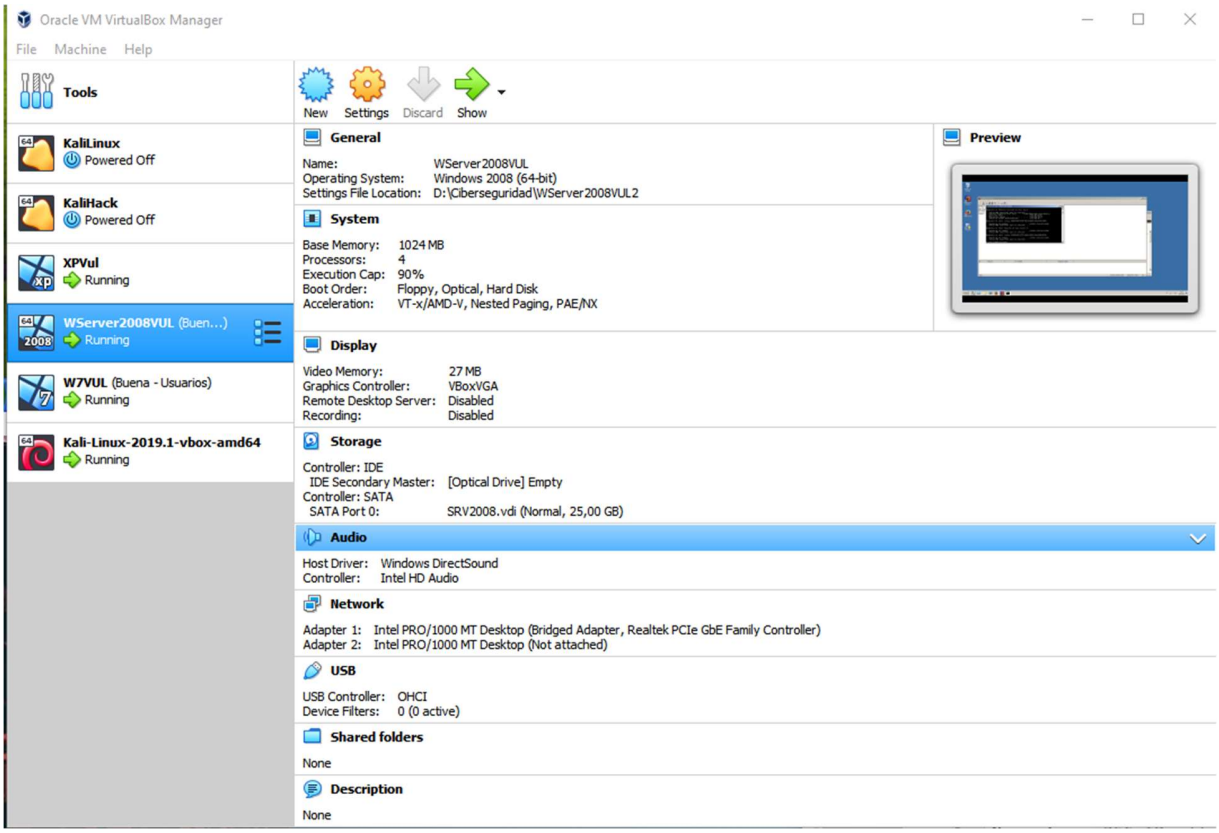
AUDITORIA TECNICA

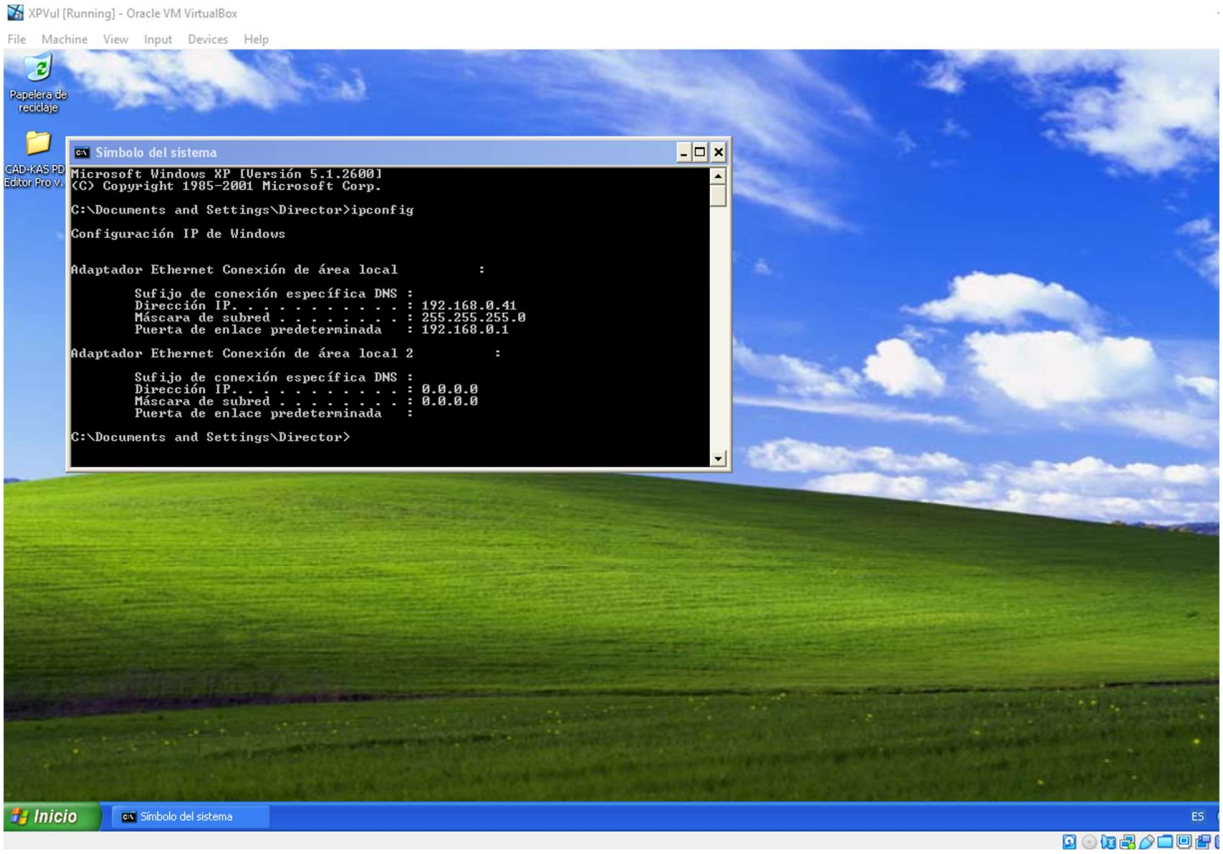
Oier Zalba Huarte

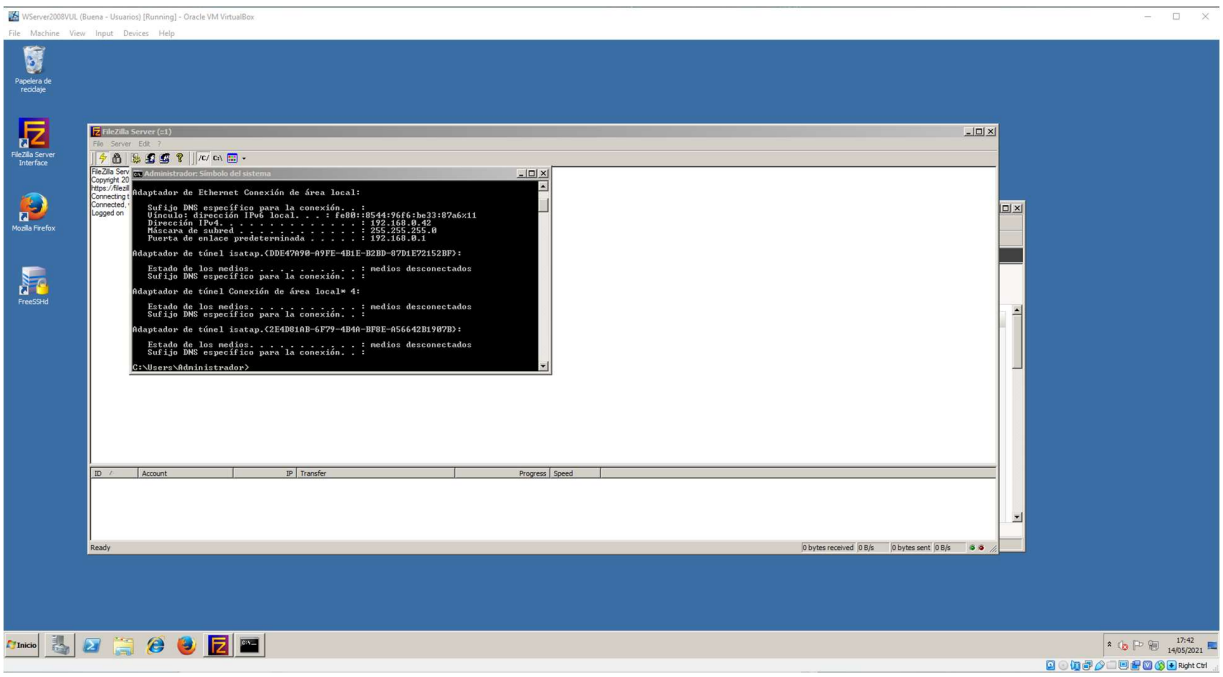
En primer lugar, he instalado todas las maquinas que tenemos a disposición.

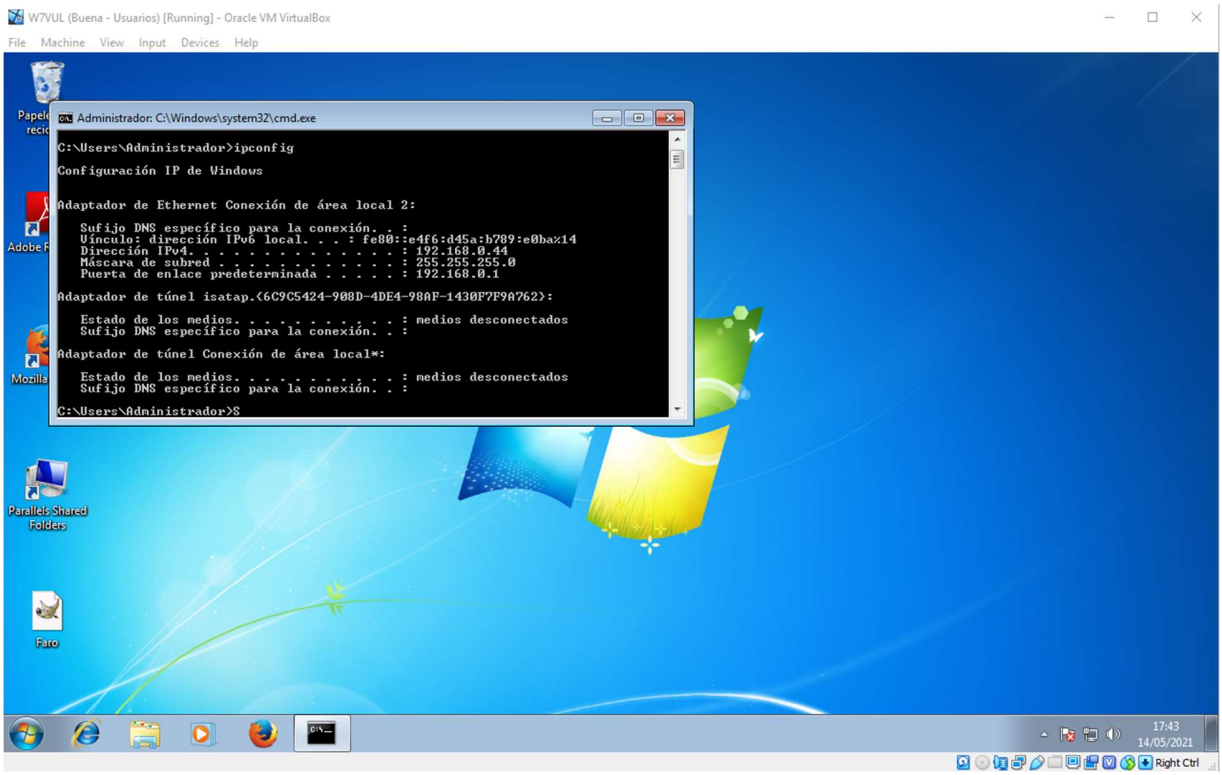
1. Windows XP vulnerable
2. Windows 7 vulnerable
3. Windows server vulnerable
4. Kali Linux 2019

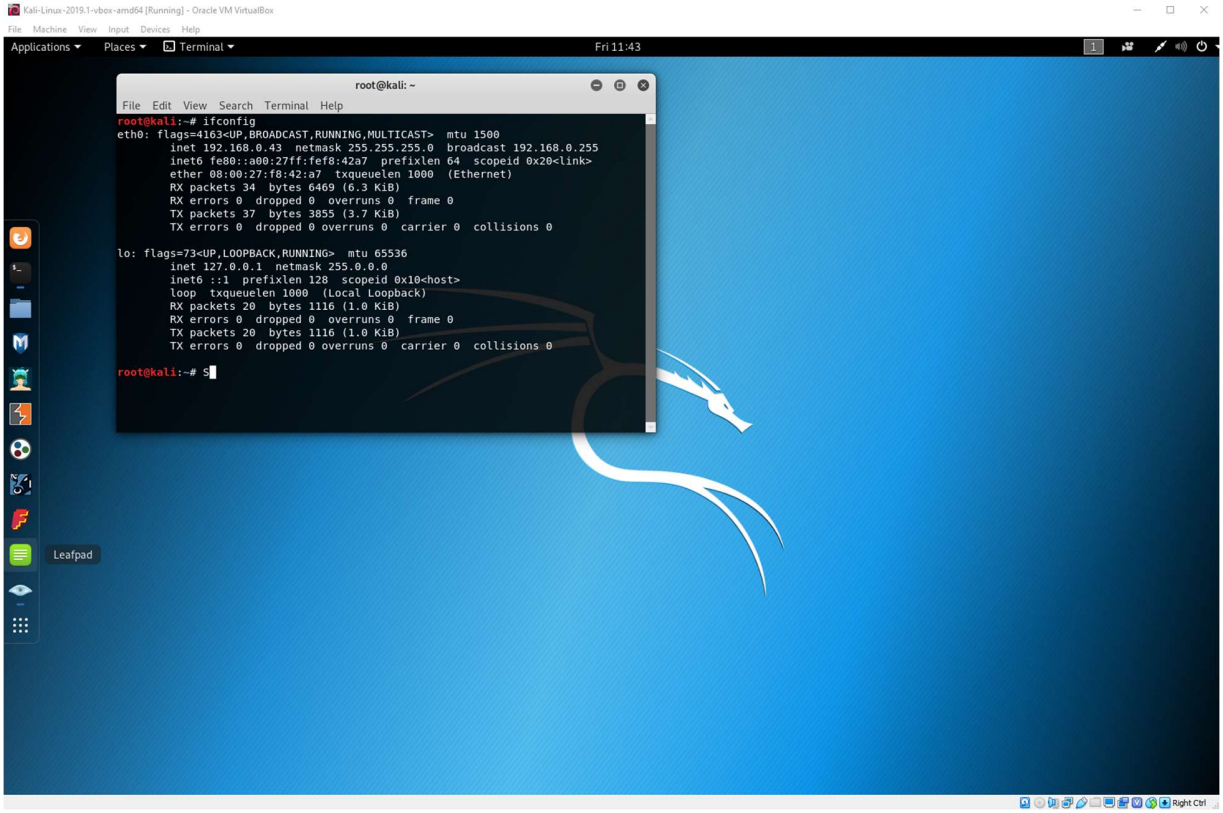


Comprobamos que funcionan bien ejecutándolas y viendo el ping interno de cada una de ellas


XPVul [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Papelera de reciclaje
CAD-KAS PDF Editor Pro v...
Símbolo del sistema
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Director>ipconfig
Configuración IP de Windows
Adaptador Ethernet Conexión de área local :
Sufijo de conexión específica DNS :
Dirección IP. . . . . : 192.168.0.41
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada : 192.168.0.1
Adaptador Ethernet Conexión de área local 2 :
Sufijo de conexión específica DNS :
Dirección IP. . . . . : 0.0.0.0
Máscara de subred . . . . . : 0.0.0.0
Puerta de enlace predeterminada :
C:\Documents and Settings\Director>
Inicio
Símbolo del sistema
ES

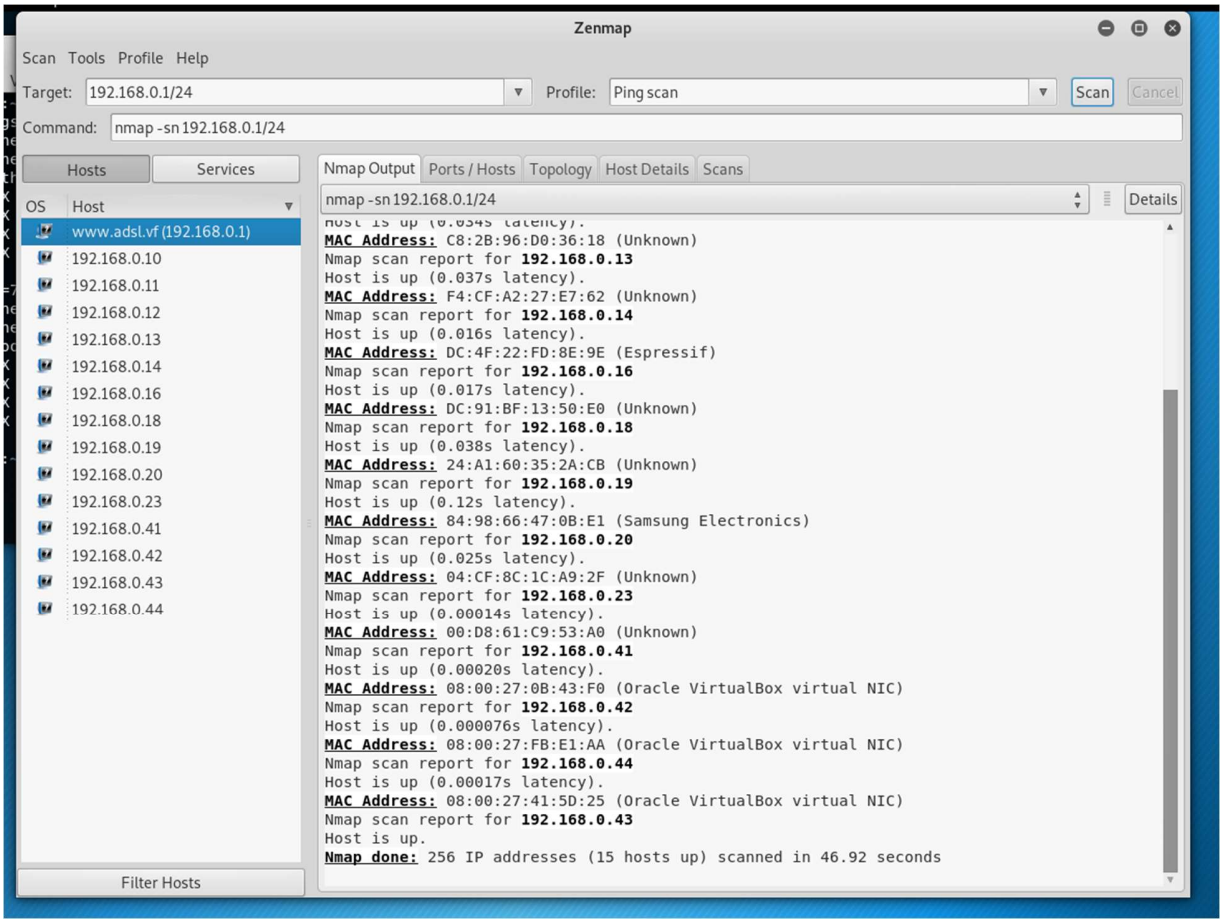

WServer2008VUL (Buena - Usuarios) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Papelera de reciclaje
FileZilla Server Interface
Mozilla Firefox
FreeSSHd
FileZilla Server (:1)
Administrador: Símbolo del sistema
Adaptador de Ethernet Conexión de área local:
Sufijo DNS específico para la conexión. . :
Vínculo: dirección IPv6 local. . . : fe80::8544:96f6:be33:87a6x11
Dirección IPv4. . . . . : 192.168.0.42
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 192.168.0.1
Adaptador de túnel isatap.{DDE47090-A9FE-4B1E-B2BD-87D1E72152BF}:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Adaptador de túnel Conexión de área local* 4:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Adaptador de túnel isatap.{2E4D81AB-6F79-4B4A-BF8E-A56642B1907B}:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
C:\Users\Administrador>
ID / Account IP Transfer Progress Speed
Ready
0 bytes received 0 B/s 0 bytes sent 0 B/s
Inicio
17:42
14/05/2021
Right Ctrl


W7VUL (Buena - Usuarios) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrador: C:\Windows\system32\cmd.exe
C:\Users\Administrador>ipconfig
Configuración IP de Windows
Adaptador de Ethernet Conexión de área local 2:
Sufijo DNS específico para la conexión. . :
Vínculo: dirección IPv6 local. . . : fe80::e4f6:d45a:b789:e0ba%14
Dirección IPv4. . . . . : 192.168.0.44
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 192.168.0.1
Adaptador de túnel isatap.{6C9C5424-908D-4DE4-98AF-1430F7F9A762}:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Adaptador de túnel Conexión de área local*:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
C:\Users\Administrador>S
Parallels Shared Folders
Faro
17:43
14/05/2021
Right Ctrl

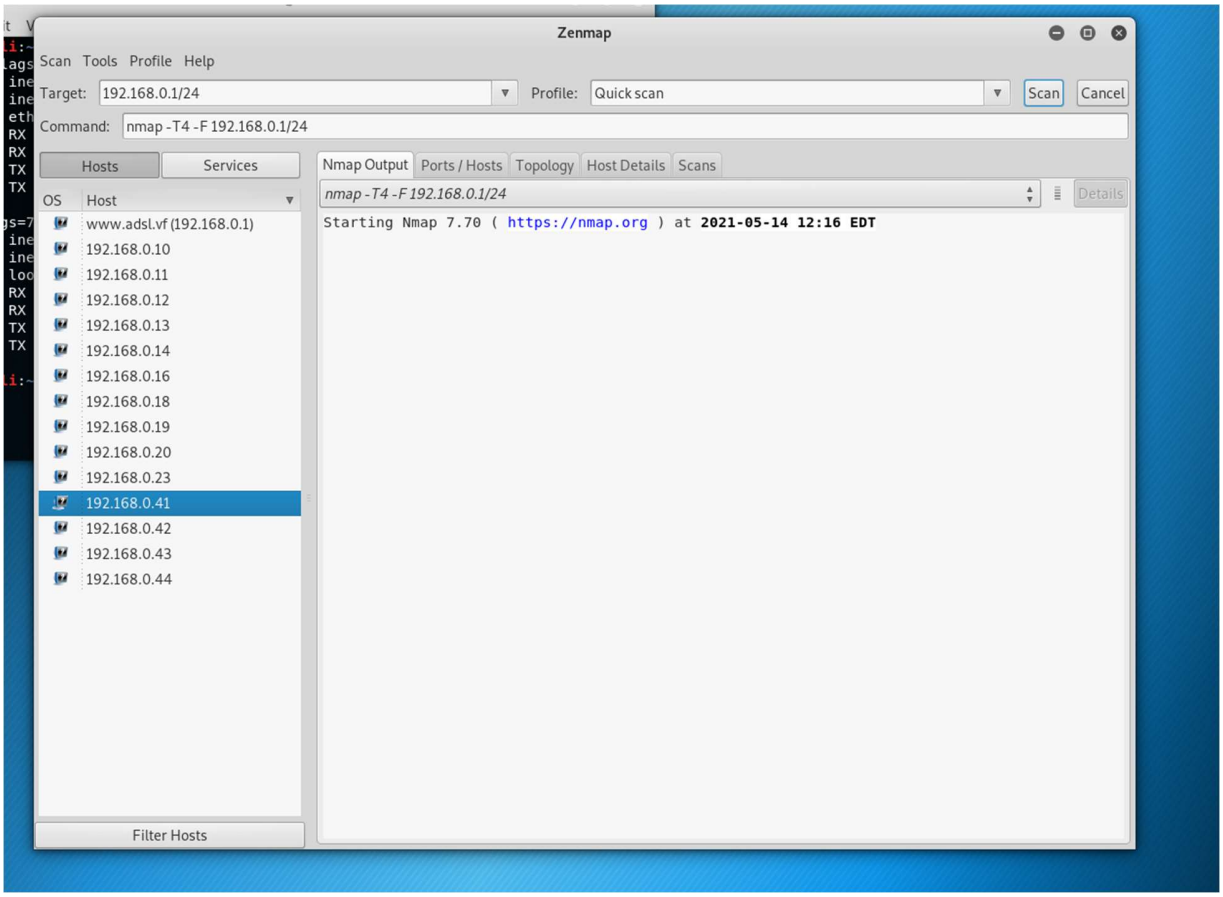

Kali-Linux-2019.1-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Fri 11:43
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.0.43 netmask 255.255.255.0 broadcast 192.168.0.255
inet6 fe80::a00:27ff:fef8:42a7 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:f8:42:a7 txqueuelen 1000 (Ethernet)
RX packets 34 bytes 6469 (6.3 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 37 bytes 3855 (3.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 20 bytes 1116 (1.0 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 20 bytes 1116 (1.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:~# S
Leafpad
Right Ctrl

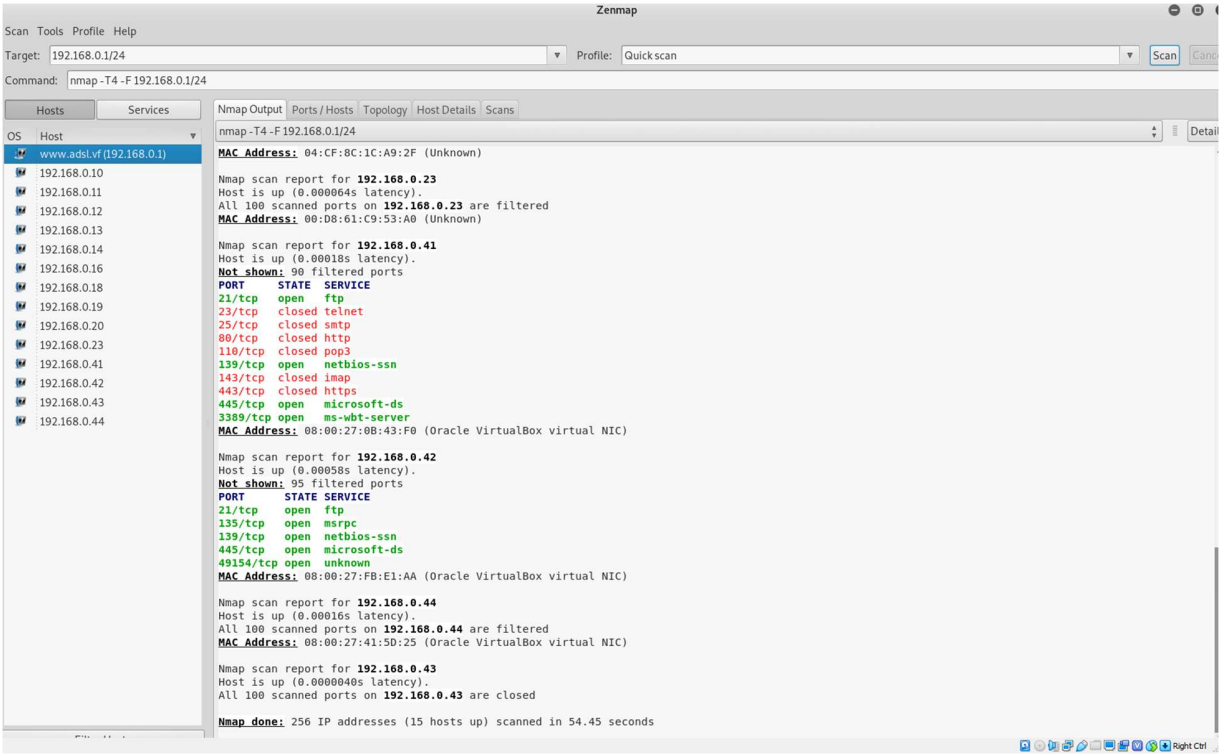
Procedemos a hacer un ping scan con zenmap para ver todas las maquinas que contestan al ping.

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



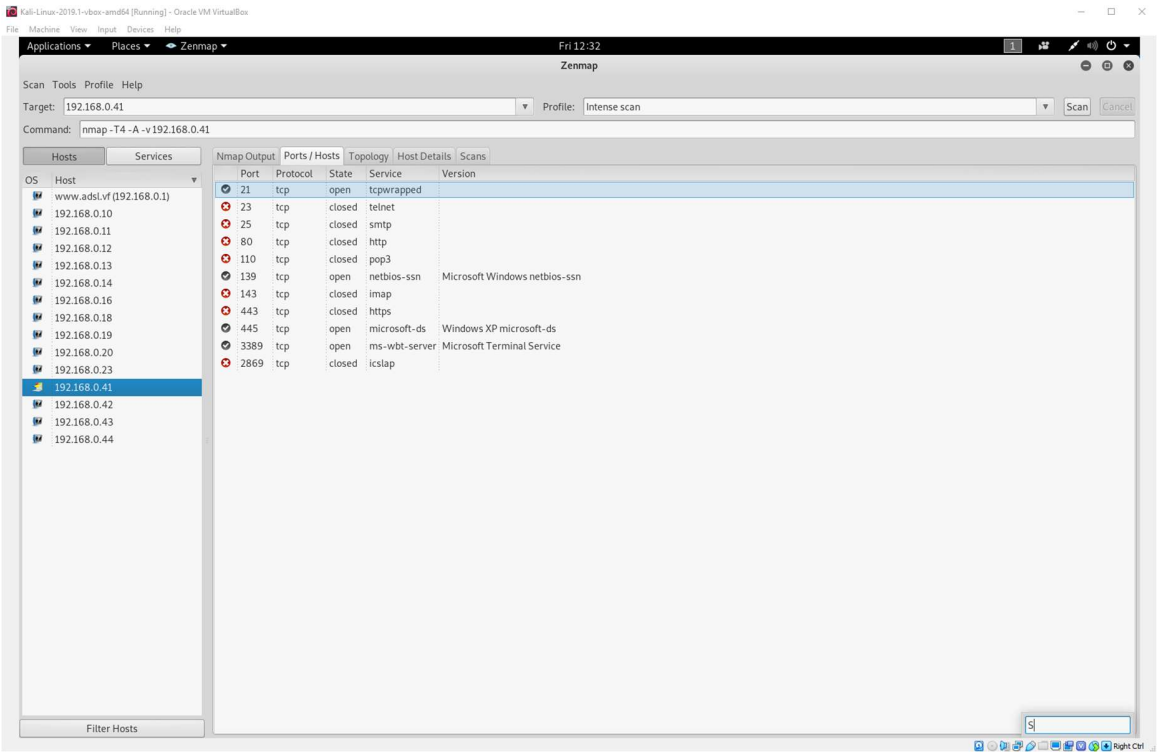
Luego hacemos un quick scan para escanear los 100 puertos mas comunes de todas las maquinas.

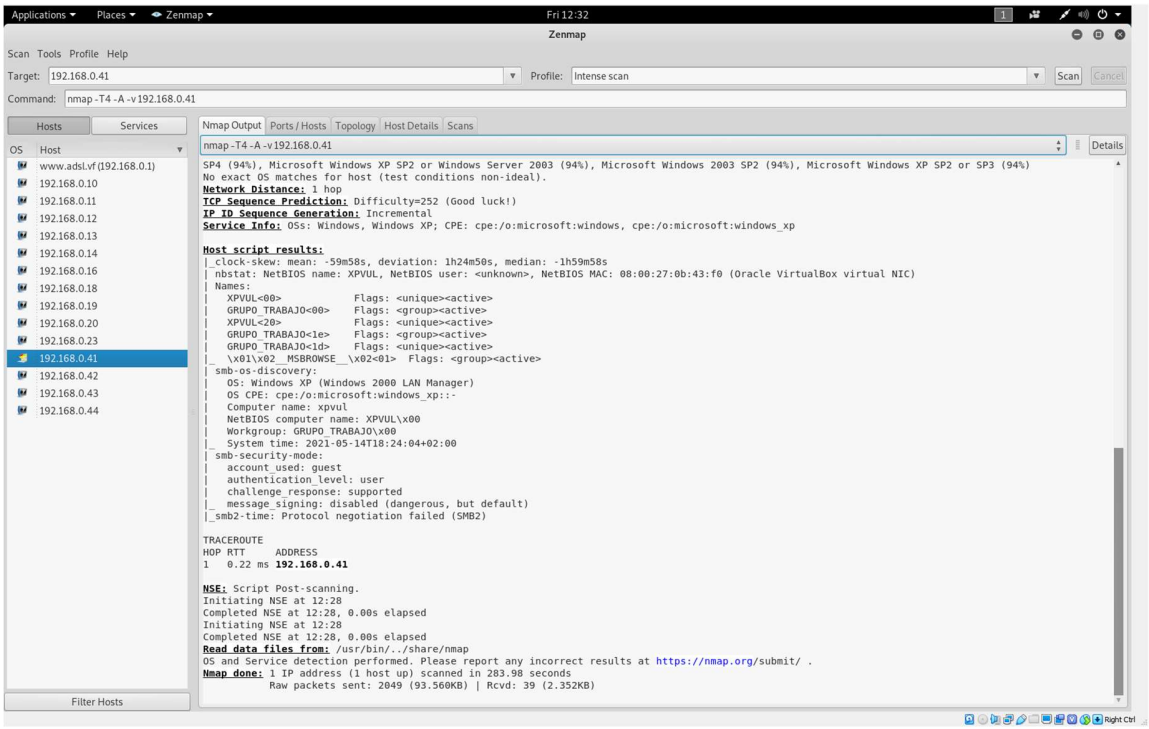

Zenmap
Scan Tools Profile Help
Target: 192.168.0.1/24
Profile: Quick scan
Scan
Cancel
Command: nmap -T4 -F 192.168.0.1/24
Hosts
Services
OS
Host
www.adsl.vf (192.168.0.1)
192.168.0.10
192.168.0.11
192.168.0.12
192.168.0.13
192.168.0.14
192.168.0.16
192.168.0.18
192.168.0.19
192.168.0.20
192.168.0.23
192.168.0.41
192.168.0.42
192.168.0.43
192.168.0.44
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -F 192.168.0.1/24
Details
Starting Nmap 7.70 (https://nmap.org) at 2021-05-14 12:16 EDT

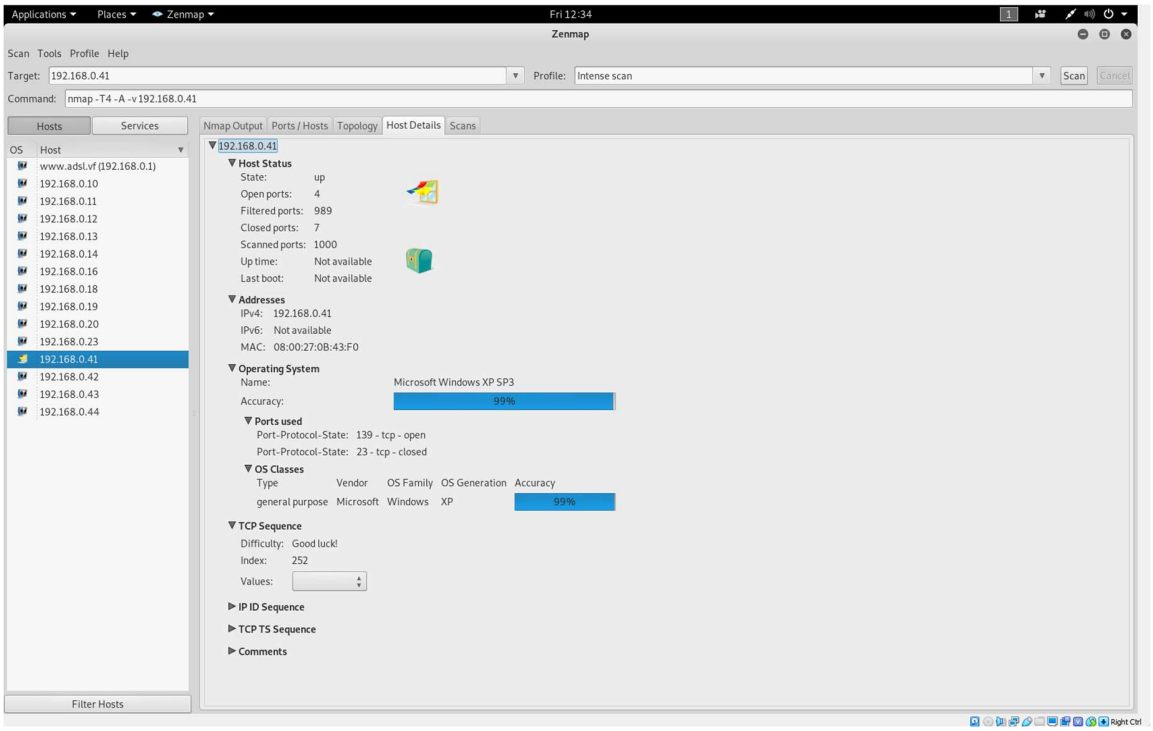

Zenmap
Scan Tools Profile Help
Target: 192.168.0.1/24
Profile: Quick scan
Scan
Command: nmap -T4 -F 192.168.0.1/24
Hosts
Services
OS
Host
www.adsl.vf (192.168.0.1)
192.168.0.10
192.168.0.11
192.168.0.12
192.168.0.13
192.168.0.14
192.168.0.16
192.168.0.18
192.168.0.19
192.168.0.20
192.168.0.23
192.168.0.41
192.168.0.42
192.168.0.43
192.168.0.44
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
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: 90 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 (0.00058s 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:FB:E1:AA (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 (0.0000040s 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.

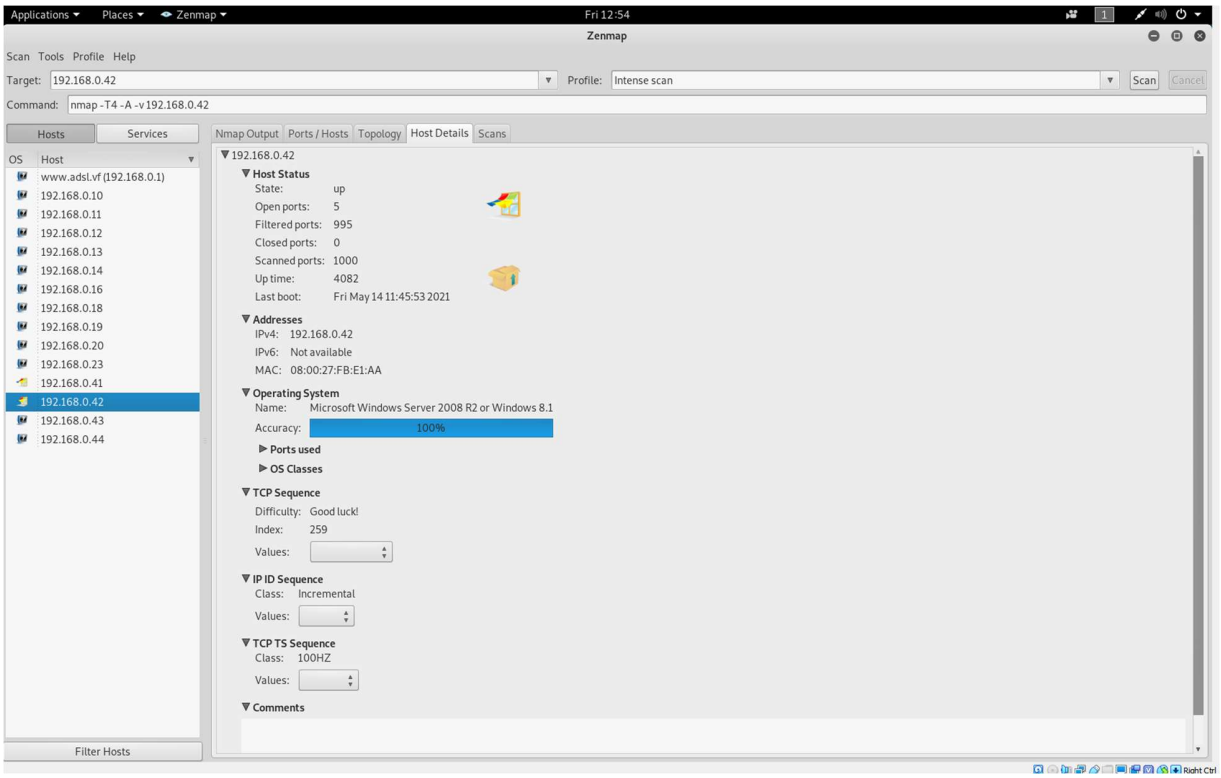
Windows xp:

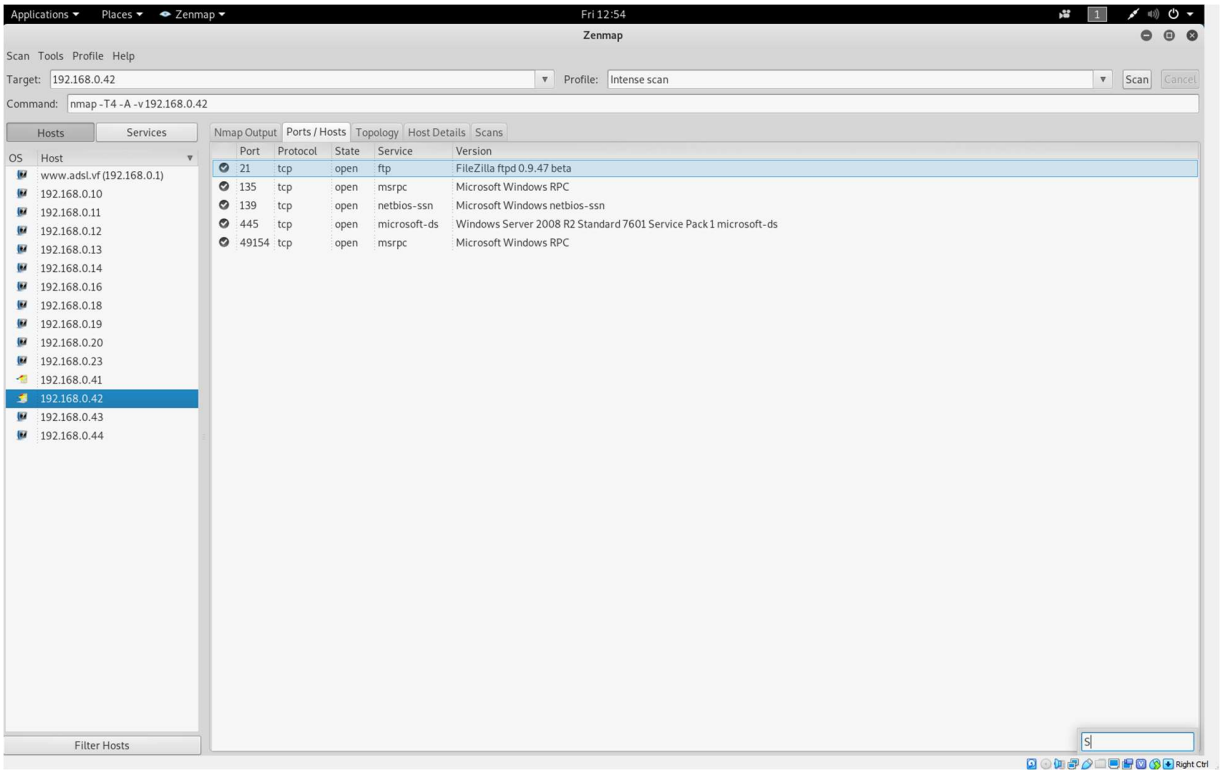


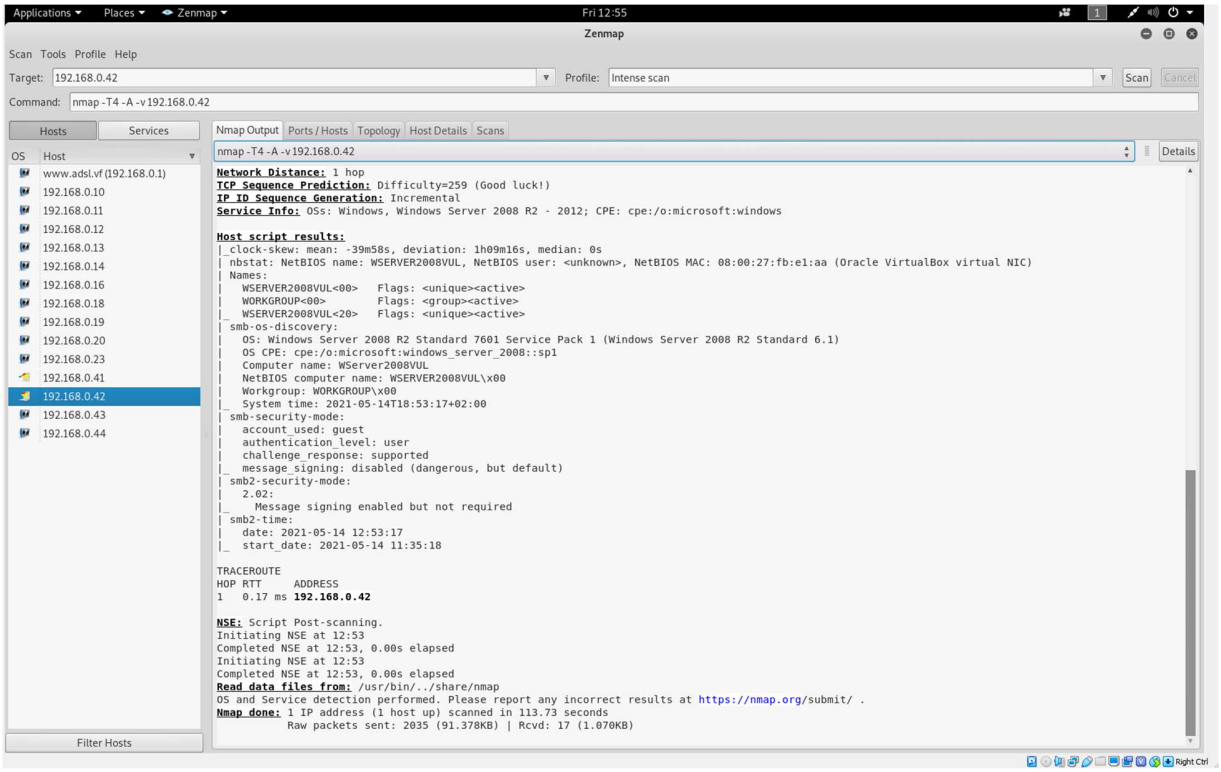




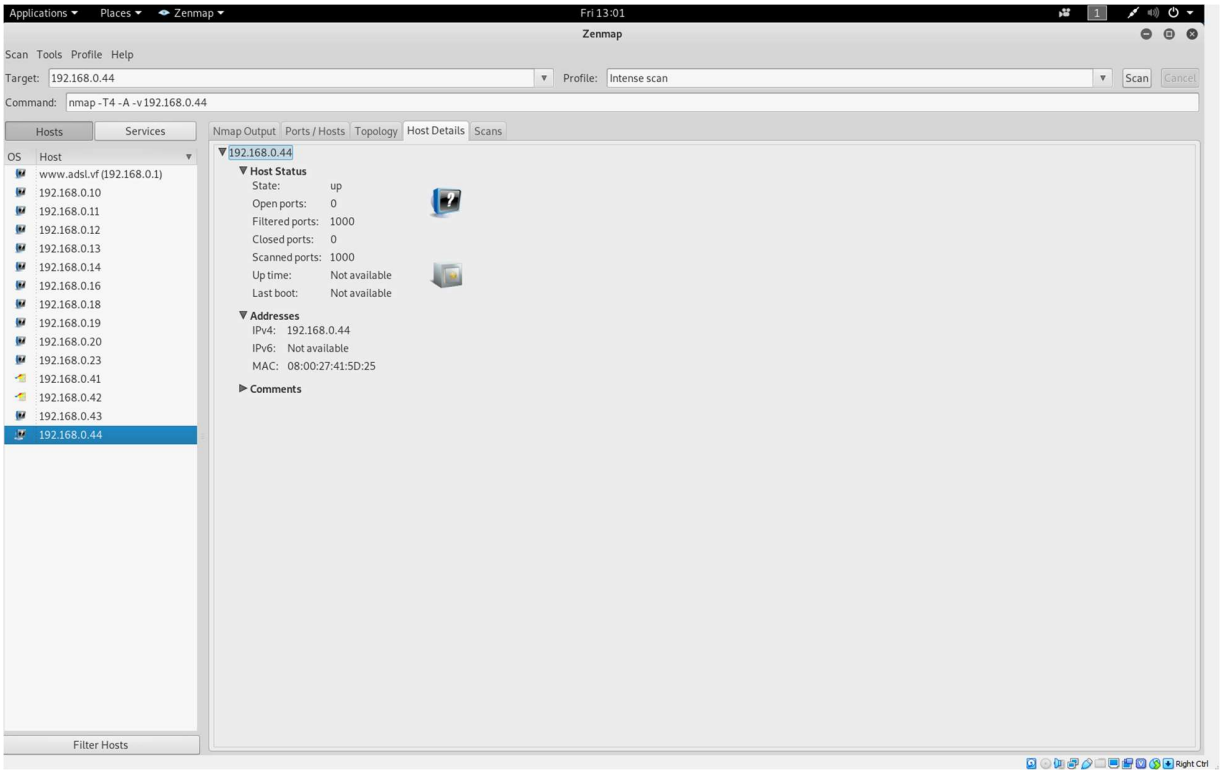
Windows server:

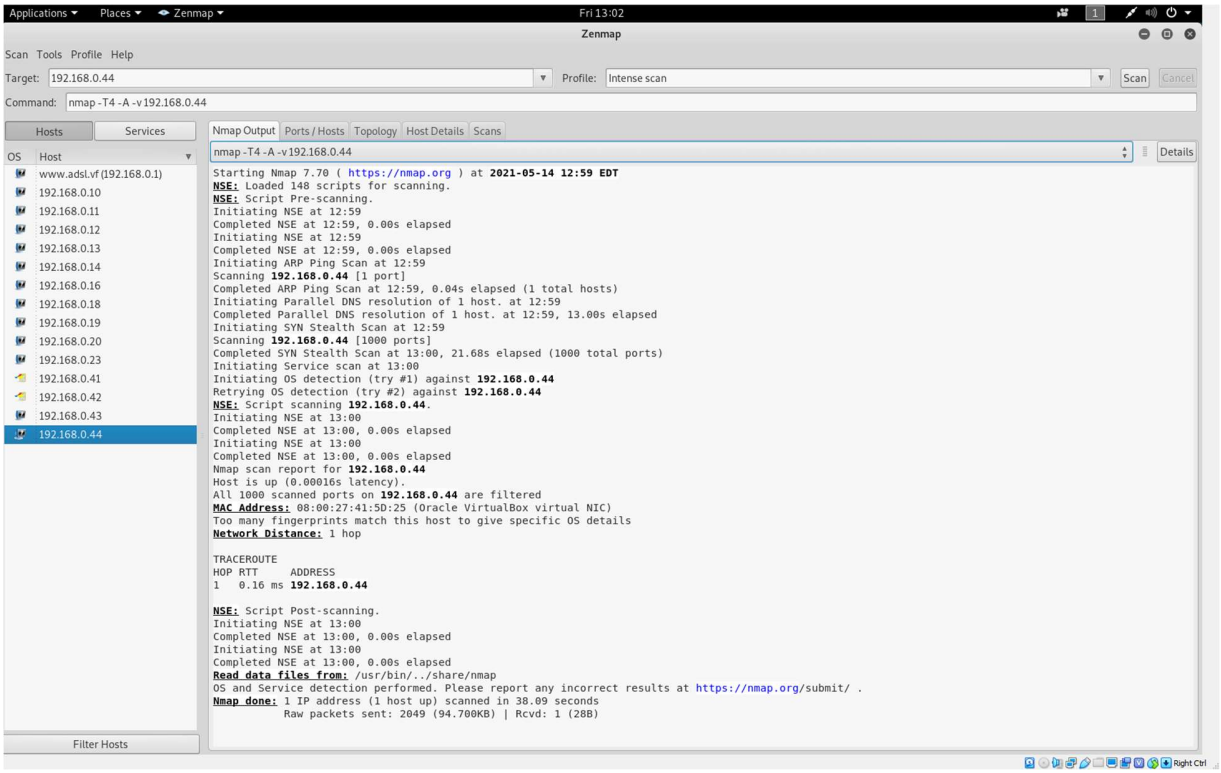


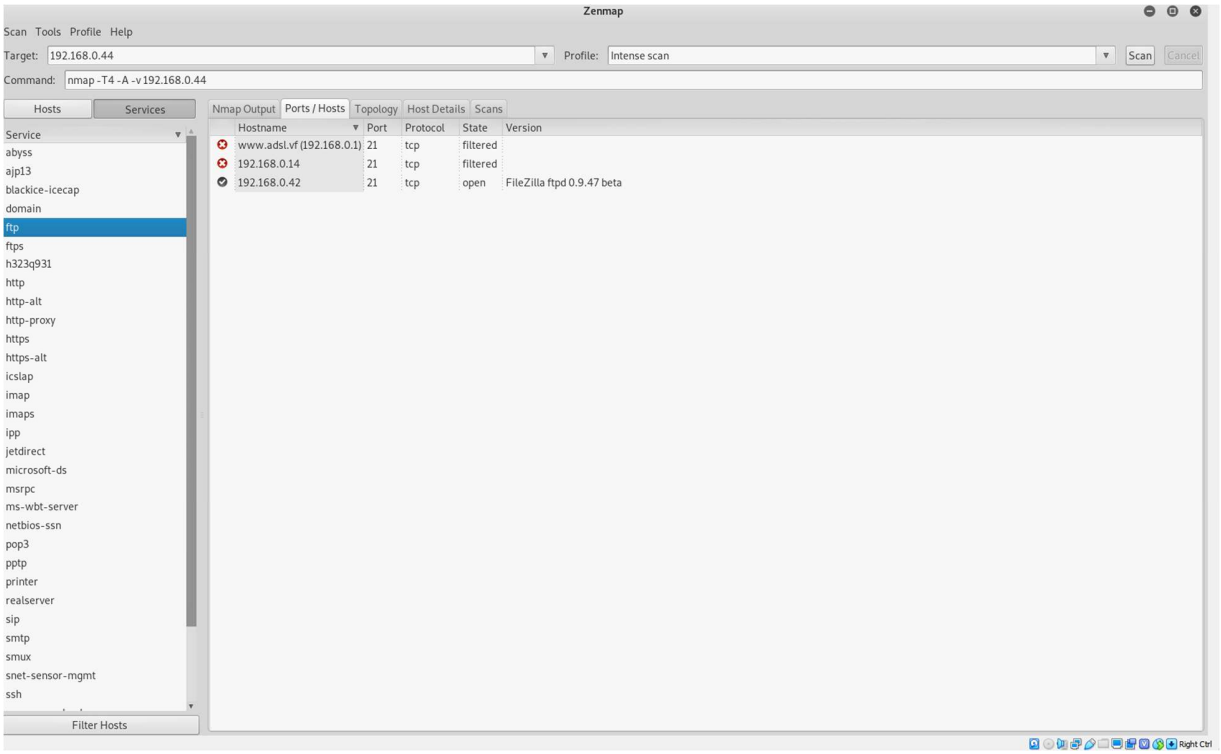

Applications
Places
Zenmap
Fri 12:54
Zenmap
Scan Tools Profile Help
Target: 192.168.0.42
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.0.42
Hosts
Services
OS
Host
www.adsl.vf (192.168.0.1)
192.168.0.10
192.168.0.11
192.168.0.12
192.168.0.13
192.168.0.14
192.168.0.16
192.168.0.18
192.168.0.19
192.168.0.20
192.168.0.23
192.168.0.41
192.168.0.42
192.168.0.43
192.168.0.44
Filter Hosts
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
Right Ctrl


Applications
Places
Zenmap
Fri 12:55
Zenmap
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
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 192.168.0.42
Details
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
Host 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:
| WSERVER2008VUL<00> Flags: <unique><active>
| WORKGROUP<00> Flags: <group><active>
|_ WSERVER2008VUL<20> Flags: <unique><active>
| smb-os-discovery:
| 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:
| 2.02:
|_ 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 (91.378KB) | Rcvd: 17 (1.070KB)
Right Ctrl

Windows 7:

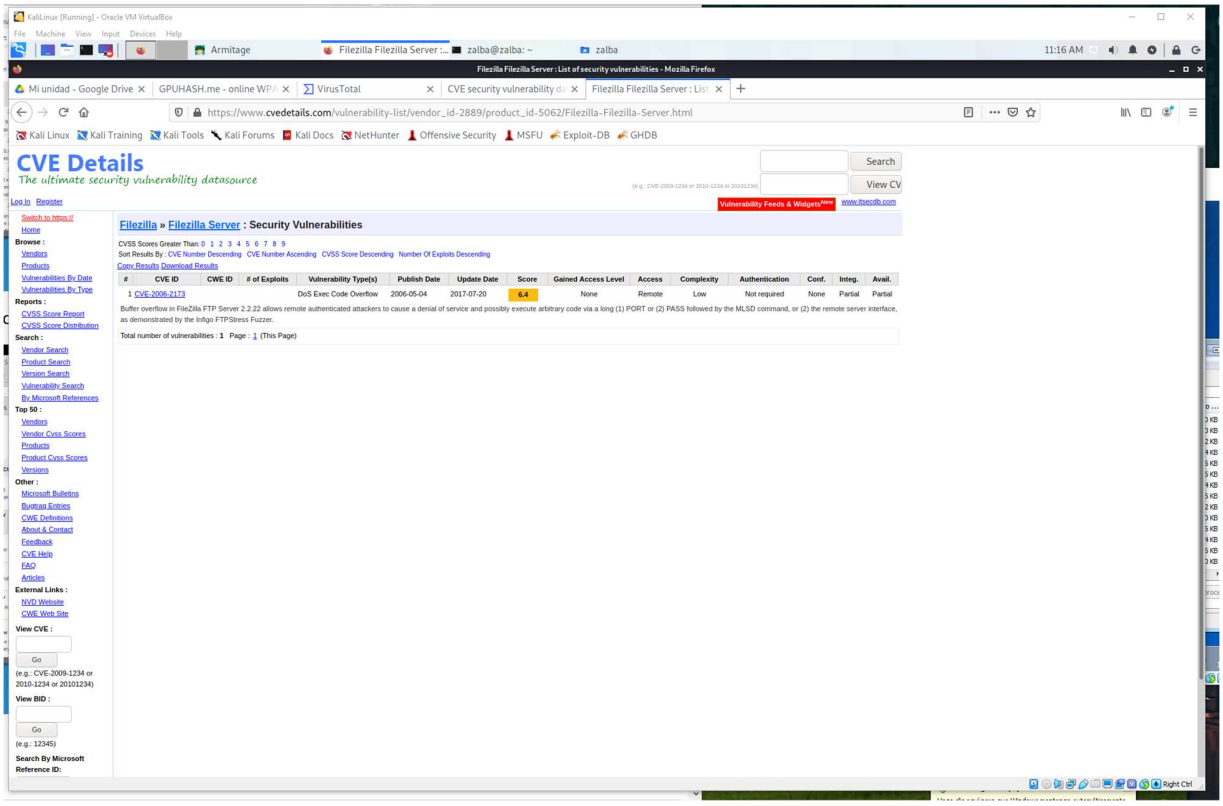

Applications
Places
Zenmap
Fri 13:01
Zenmap
Scan Tools Profile Help
Target: 192.168.0.44
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.0.44
Hosts
Services
OS
Host
www.adsl.vf (192.168.0.1)
192.168.0.10
192.168.0.11
192.168.0.12
192.168.0.13
192.168.0.14
192.168.0.16
192.168.0.18
192.168.0.19
192.168.0.20
192.168.0.23
192.168.0.41
192.168.0.42
192.168.0.43
192.168.0.44
Filter Hosts
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
Right Ctrl

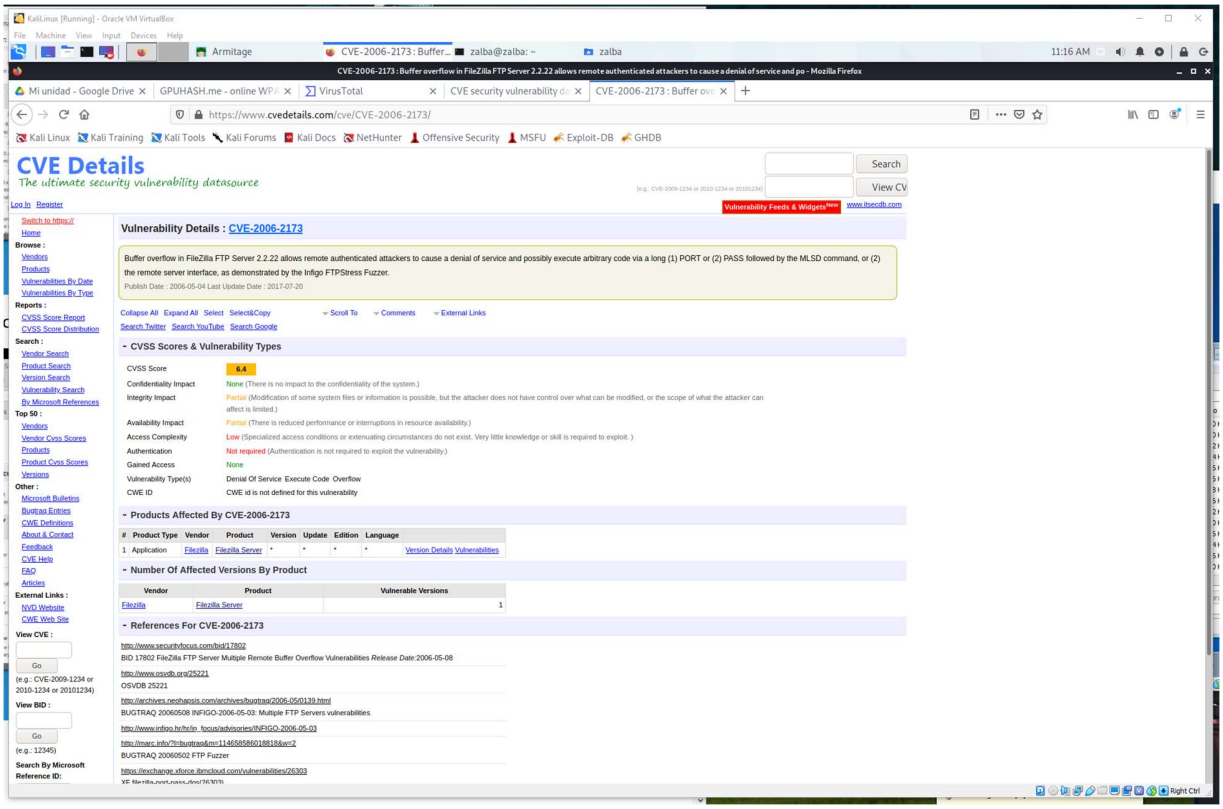

Applications
Places
Zenmap
Fri 13:02
Zenmap
Scan Tools Profile Help
Target: 192.168.0.44
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 192.168.0.44
Hosts
Services
OS
Host
www.adsl.vf (192.168.0.1)
192.168.0.10
192.168.0.11
192.168.0.12
192.168.0.13
192.168.0.14
192.168.0.16
192.168.0.18
192.168.0.19
192.168.0.20
192.168.0.23
192.168.0.41
192.168.0.42
192.168.0.43
192.168.0.44
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 192.168.0.44
Details
Starting Nmap 7.70 (https://nmap.org) at 2021-05-14 12:59 EDT
NSE: Loaded 148 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
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 (28B)
Right Ctrl



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

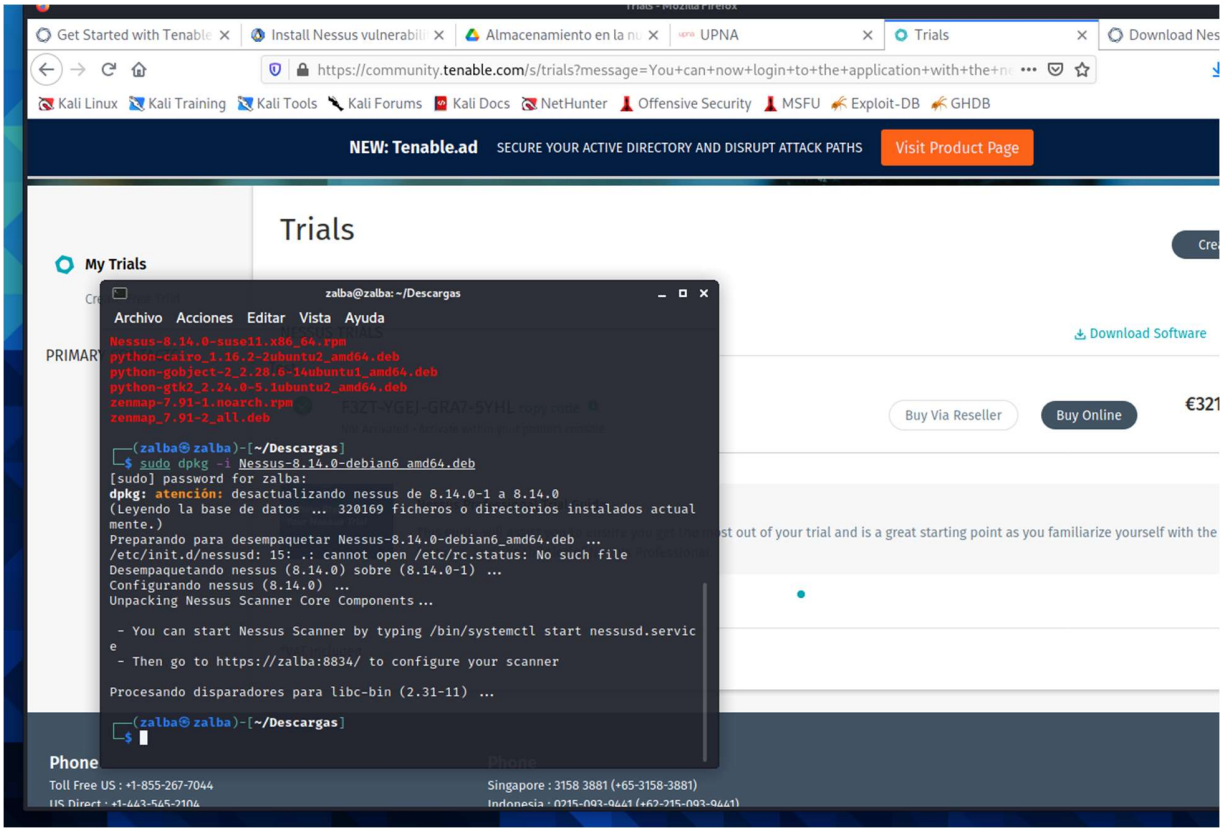
Para ver si existe alguna vulnerabilidad que poder explotar, podemos acudir a la web cve score

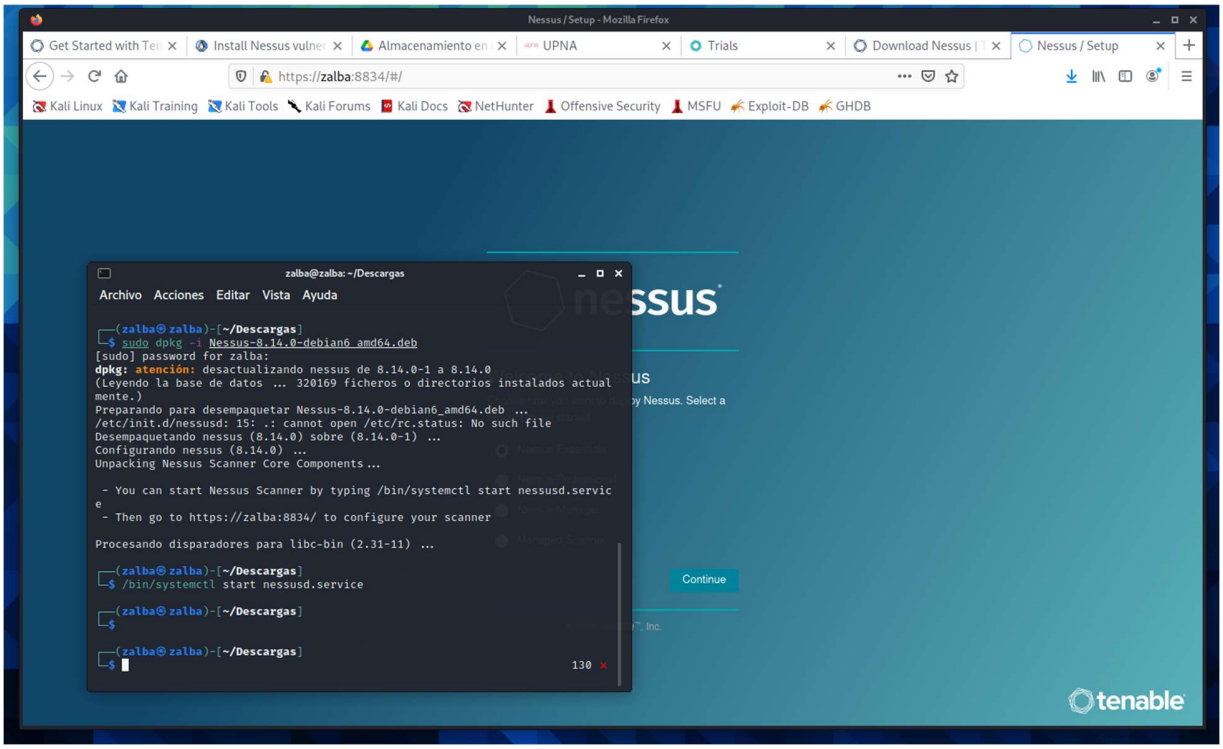


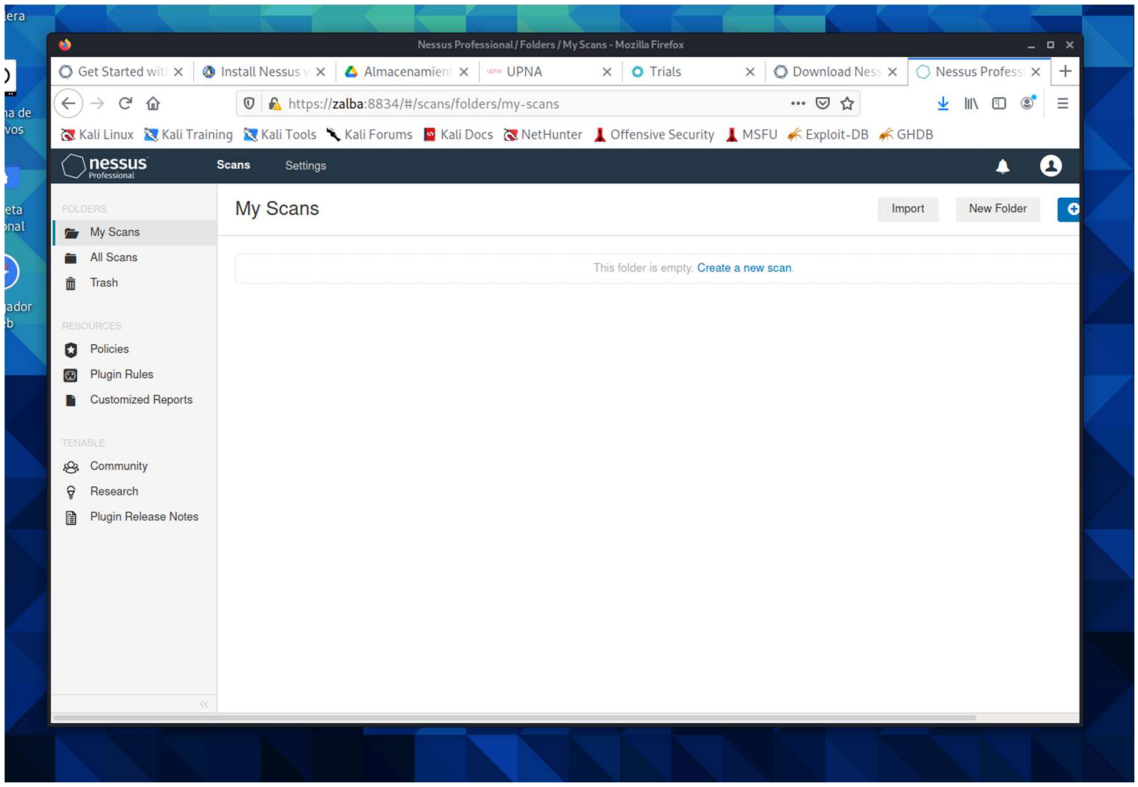


Otra base de datos de vulnerabilidades muy buena es Nessus. Nessus directamente hace el análisis y lista todas las vulnerabilidades posibles y las ordena según el cvss score.

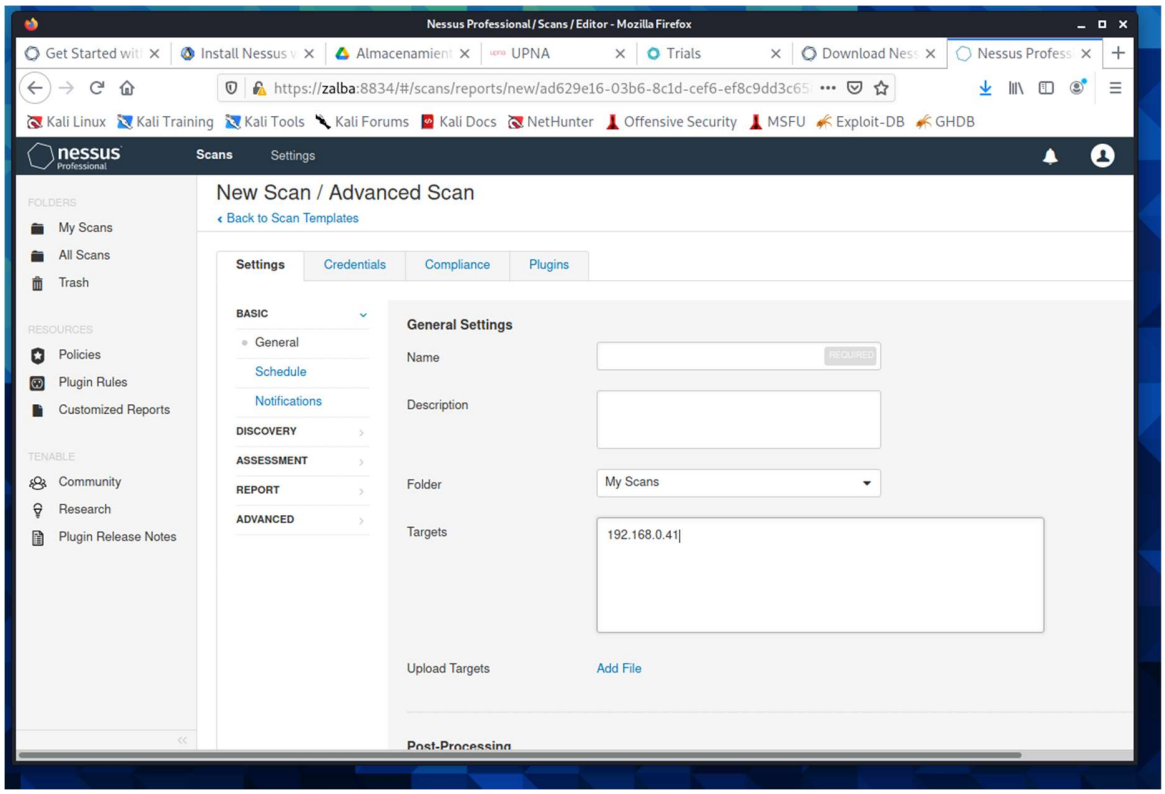
Descargamos Nessus


Get Started with Tenable
Install Nessus vulnerabili
Almacenamiento en la nu
UPNA
Trials
Download Nes
https://community.tenable.com/s/trials?message=You+can+now+login+to+the+application+with+the+ne
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
NEW: Tenable.ad
SECURE YOUR ACTIVE DIRECTORY AND DISRUPT ATTACK PATHS
Visit Product Page
Trials
My Trials
Download Software
Buy Via Reseller
Buy Online
€321
zalba@zalba: ~/Descargas
Archivo Acciones Editar Vista Ayuda
Nessus-8.14.0-suse11.x86_64.rpm
python-cairo_1.16.2-2ubuntu2_amd64.deb
python-gobject-2_2.28.6-14ubuntu1_amd64.deb
python-gtk2_2.24.0-5.1ubuntu2_amd64.deb
zenmap-7.91-1.noarch.rpm
zenmap_7.91-2_all.deb
(zalba㉿zalba)-[~/Descargas]
$ sudo dpkg -i Nessus-8.14.0-debian6_amd64.deb
[sudo] password for zalba:
dpkg: atención: desactualizando nessus de 8.14.0-1 a 8.14.0
(Leyendo la base de datos ... 320169 ficheros o directorios instalados actual
mente.)
Preparando para desempaquetar Nessus-8.14.0-debian6_amd64.deb ...
/etc/init.d/nessusd: 15: .: cannot open /etc/rc.status: No such file
Desempaquetando nessus (8.14.0) sobre (8.14.0-1) ...
Configurando nessus (8.14.0) ...
Unpacking Nessus Scanner Core Components ...
- You can start Nessus Scanner by typing /bin/systemctl start nessusd.servic
e
- Then go to https://zalba:8834/ to configure your scanner
Procesando disparadores para libc-bin (2.31-11) ...
(zalba㉿zalba)-[~/Descargas]
$
Phone
Toll Free US : +1-855-267-7044
Singapore : 3158 3881 (+65-3158-3881)

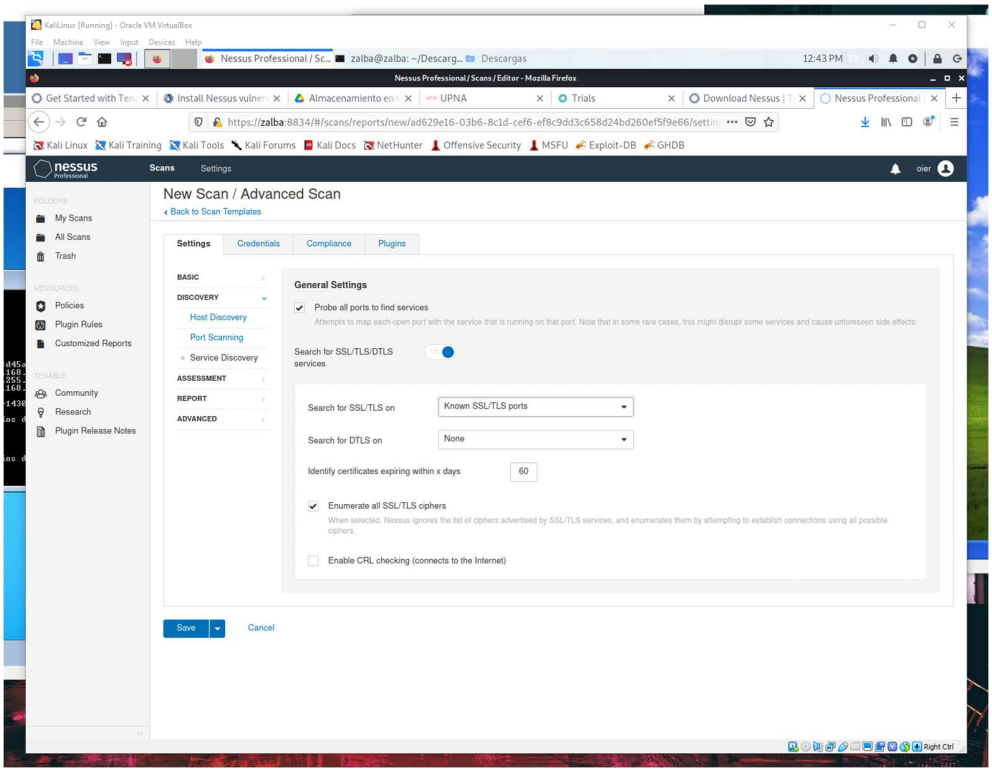

Nessus / Setup - Mozilla Firefox
Get Started with Ten
Install Nessus vulner
Almacenamiento en
UPNA
Trials
Download Nessus |
Nessus / Setup
https://zalba:8834/#/
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
zalba@zalba: ~/Descargas
Archivo Acciones Editar Vista Ayuda
(zalba㉿zalba)-[~/Descargas]
$ sudo dpkg -i Nessus-8.14.0-debian6_amd64.deb
[sudo] password for zalba:
dpkg: atención: desactualizando nessus de 8.14.0-1 a 8.14.0
(Leyendo la base de datos ... 320169 ficheros o directorios instalados actual
mente.)
Preparando para desempaquetar Nessus-8.14.0-debian6_amd64.deb ...
/etc/init.d/nessusd: 15: .: cannot open /etc/rc.status: No such file
Desempaquetando nessus (8.14.0) sobre (8.14.0-1) ...
Configurando nessus (8.14.0) ...
Unpacking Nessus Scanner Core Components ...
- You can start Nessus Scanner by typing /bin/systemctl start nessusd.servic
e
- Then go to https://zalba:8834/ to configure your scanner
Procesando disparadores para libc-bin (2.31-11) ...
(zalba㉿zalba)-[~/Descargas]
$ /bin/systemctl start nessusd.service
(zalba㉿zalba)-[~/Descargas]
$
(zalba㉿zalba)-[~/Descargas]
$
130
Continue
tenable

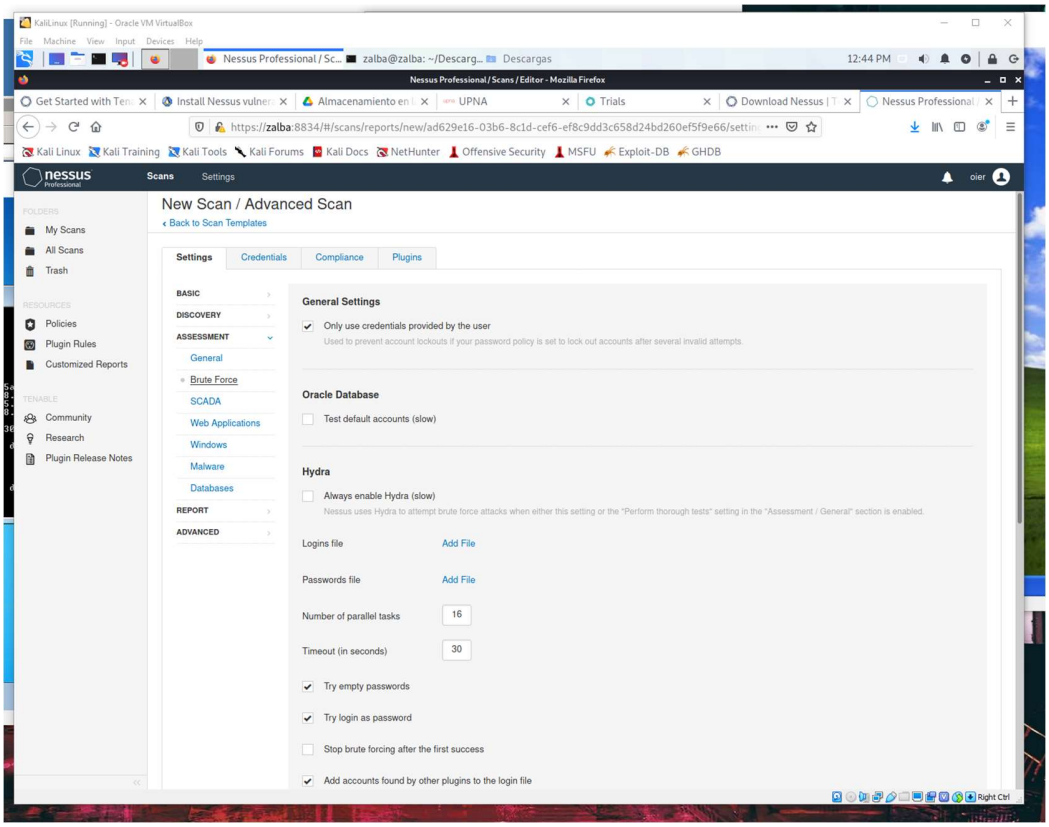


Iniciamos un escaneo avanzado

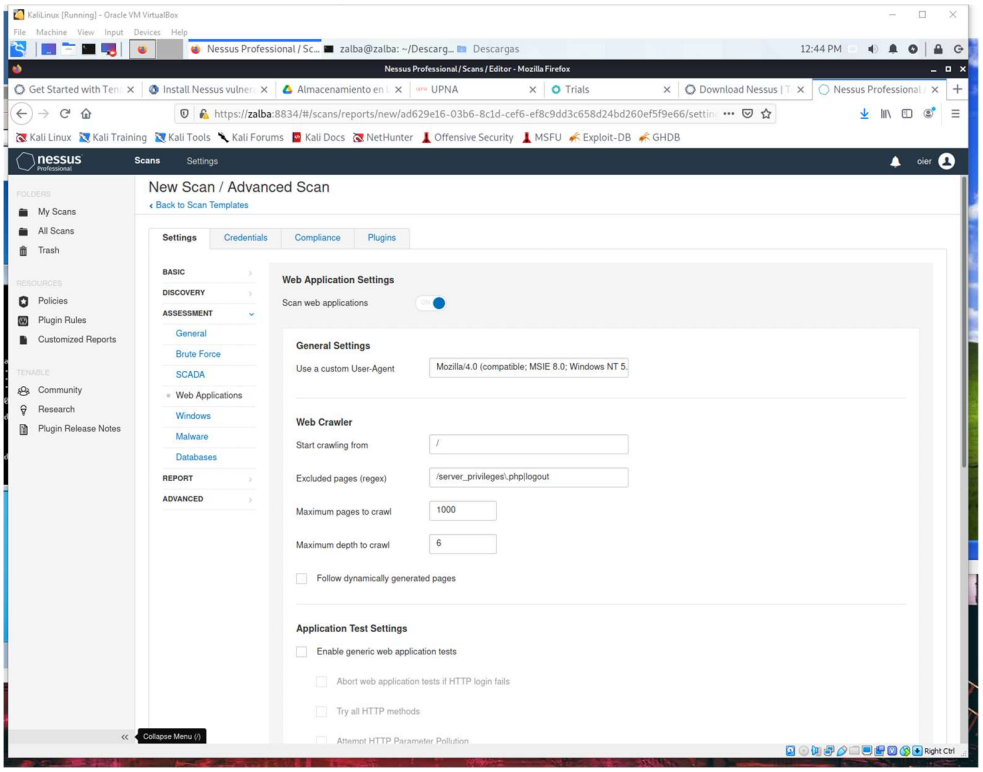


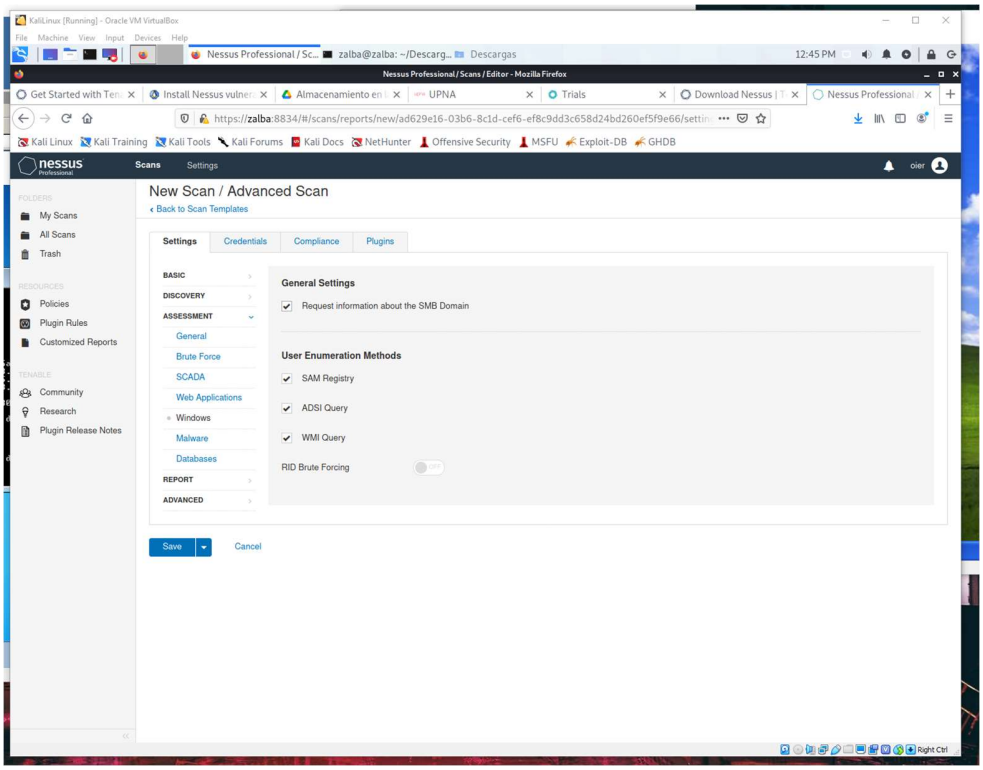
Metemos todos los parametros necesarios



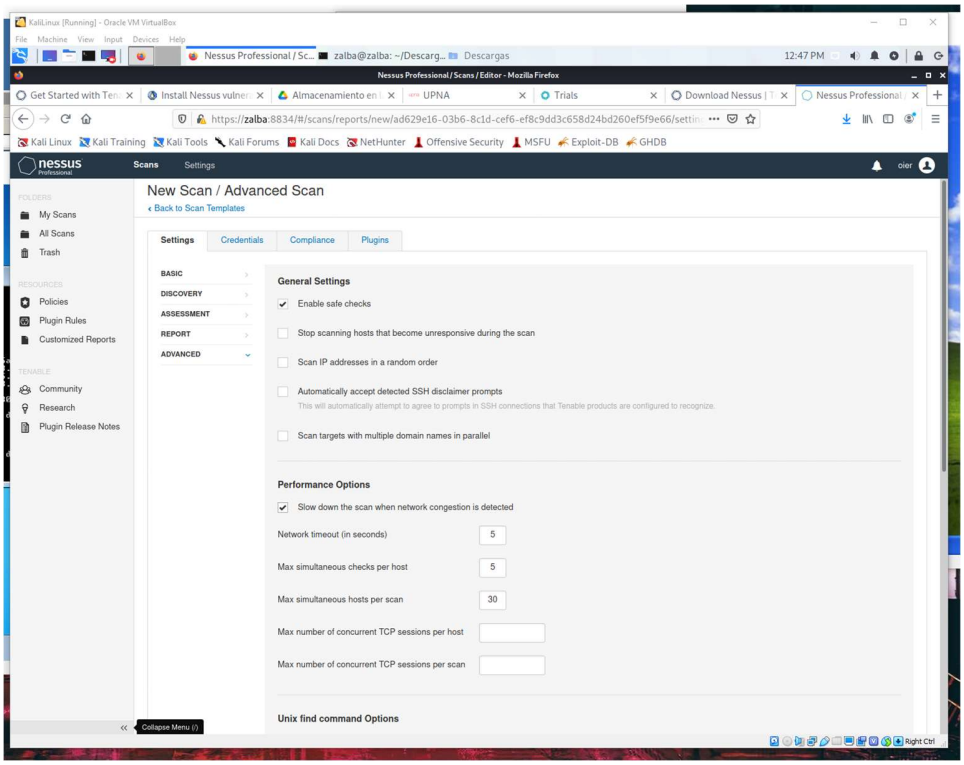


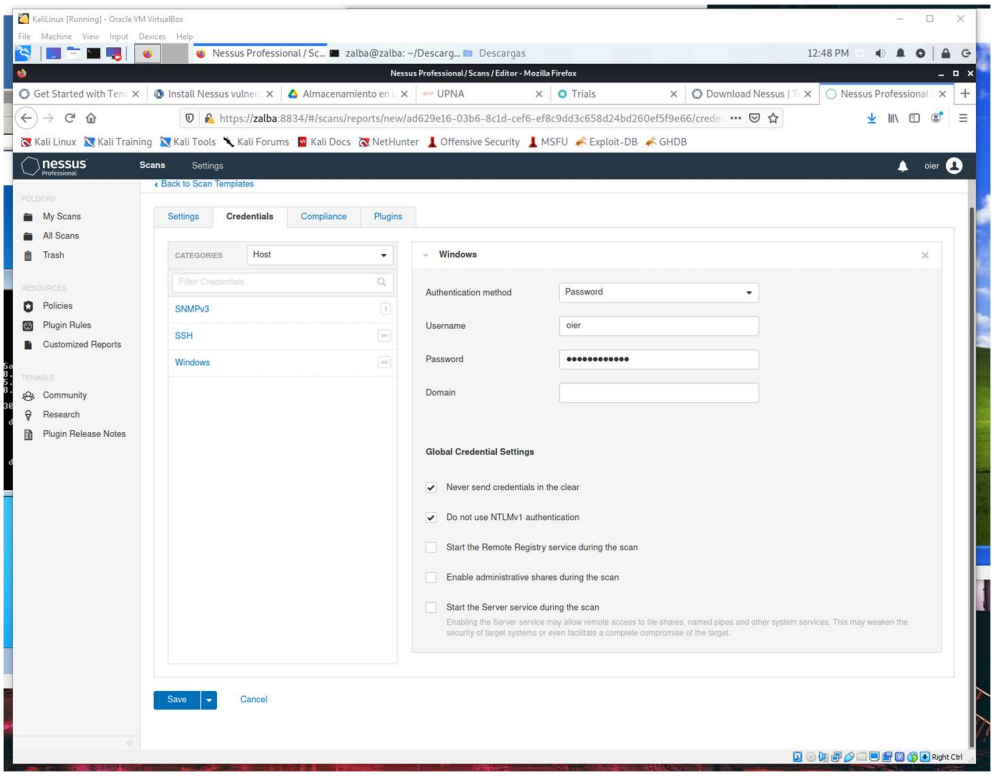
Para las aplicaciones web

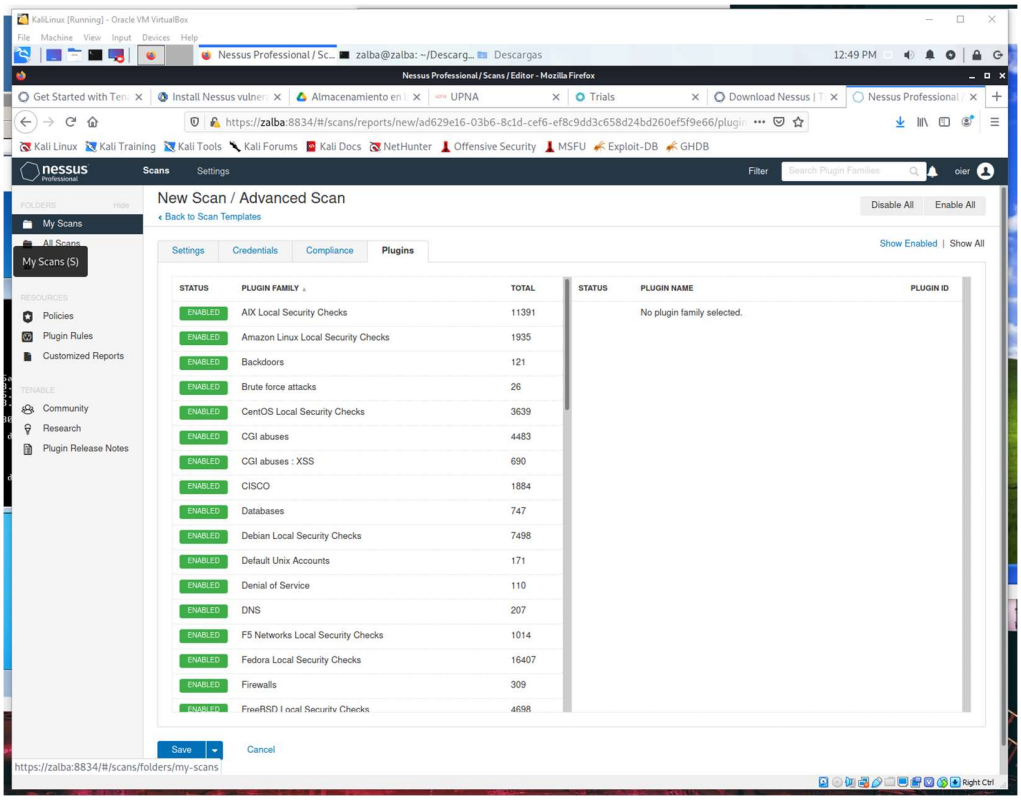




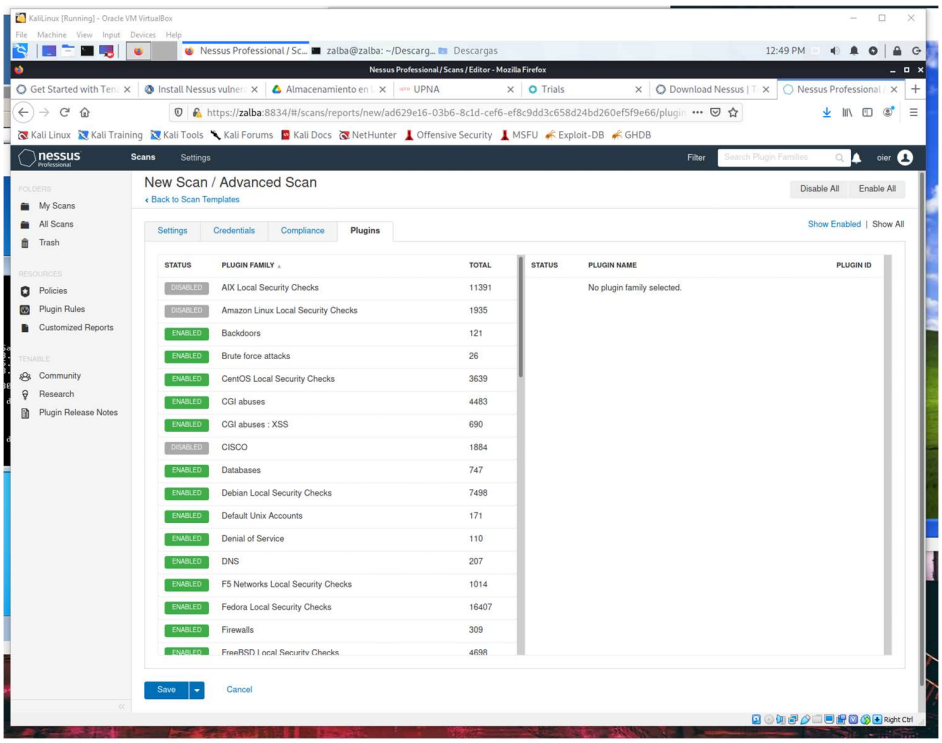
Marcamos la casilla de slow down para no congestionar la red y que no nos detecten entre otras cosas

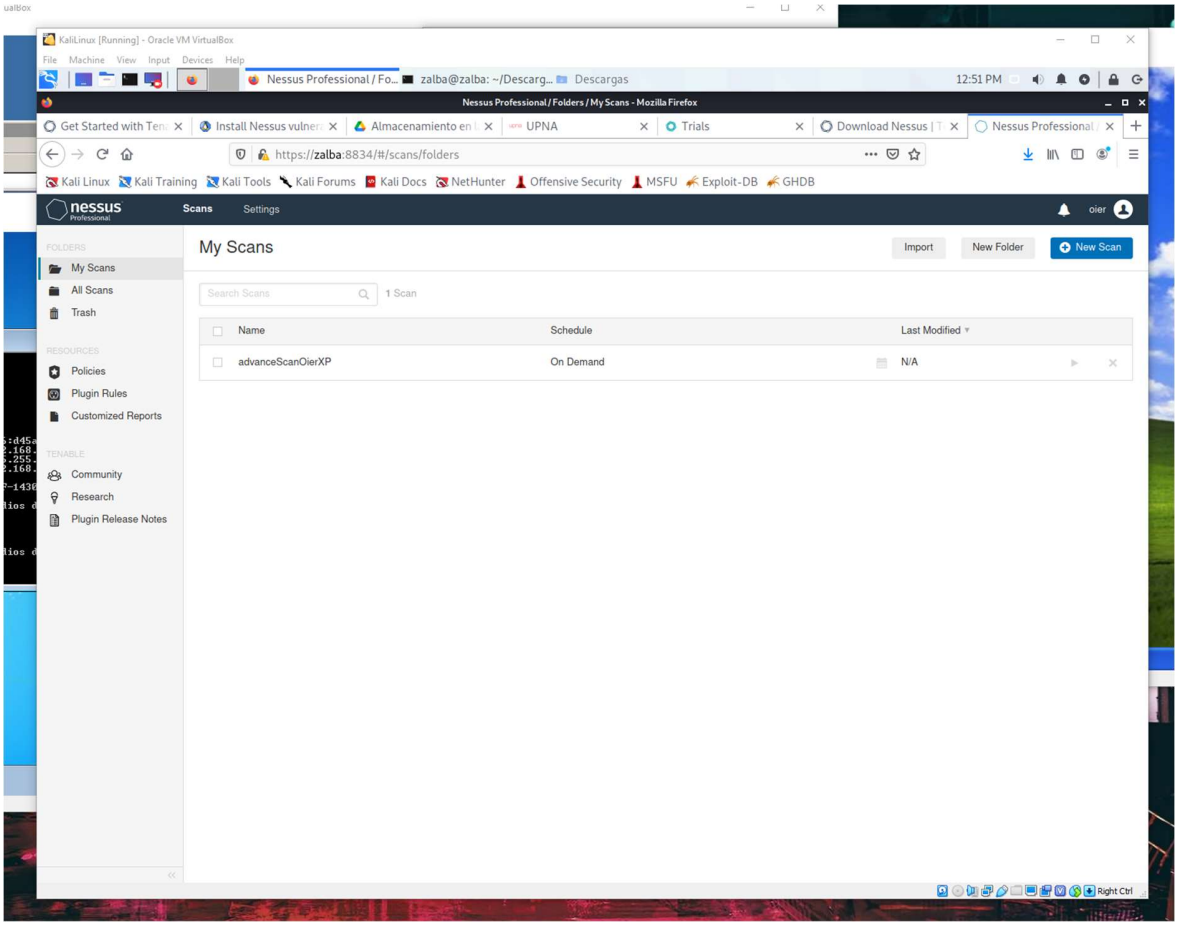


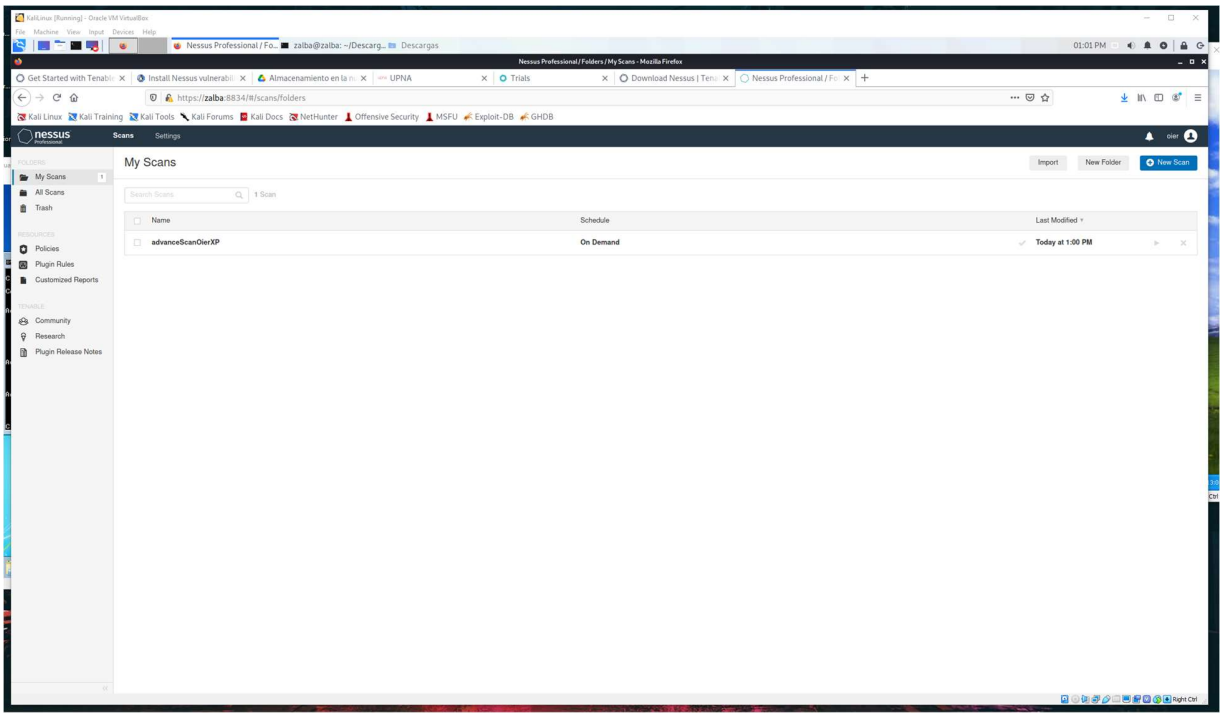




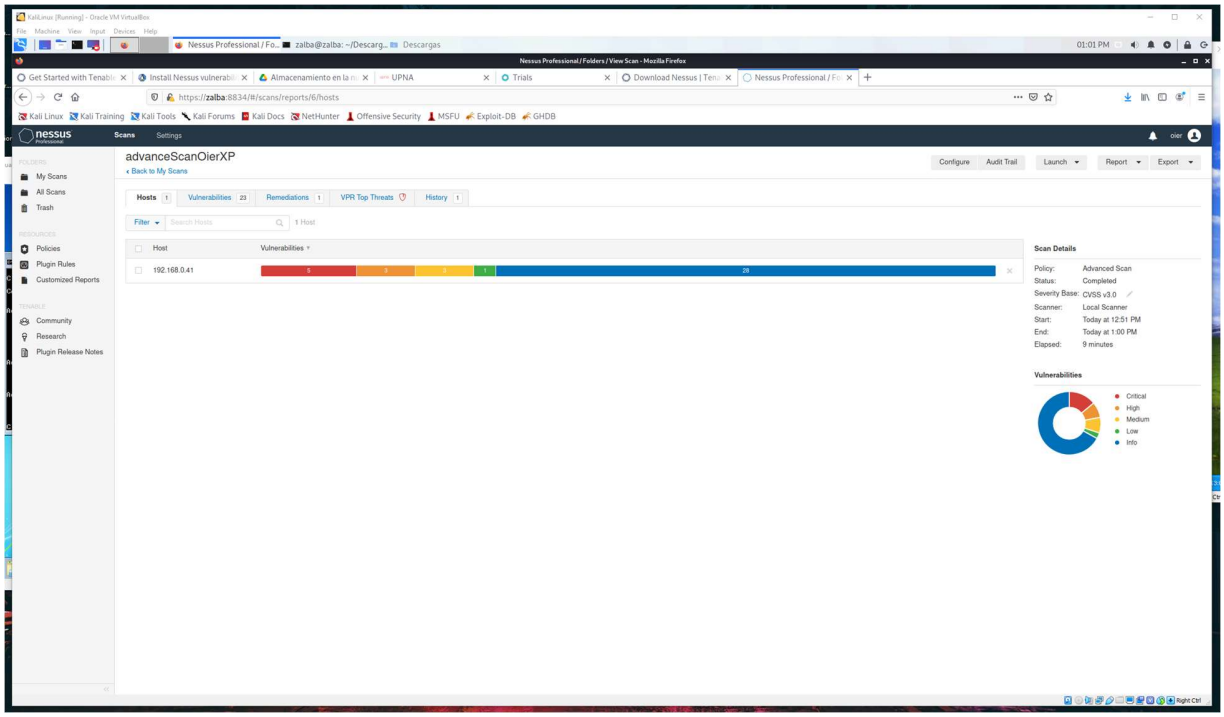
Desactivamos los plugins que no queramos

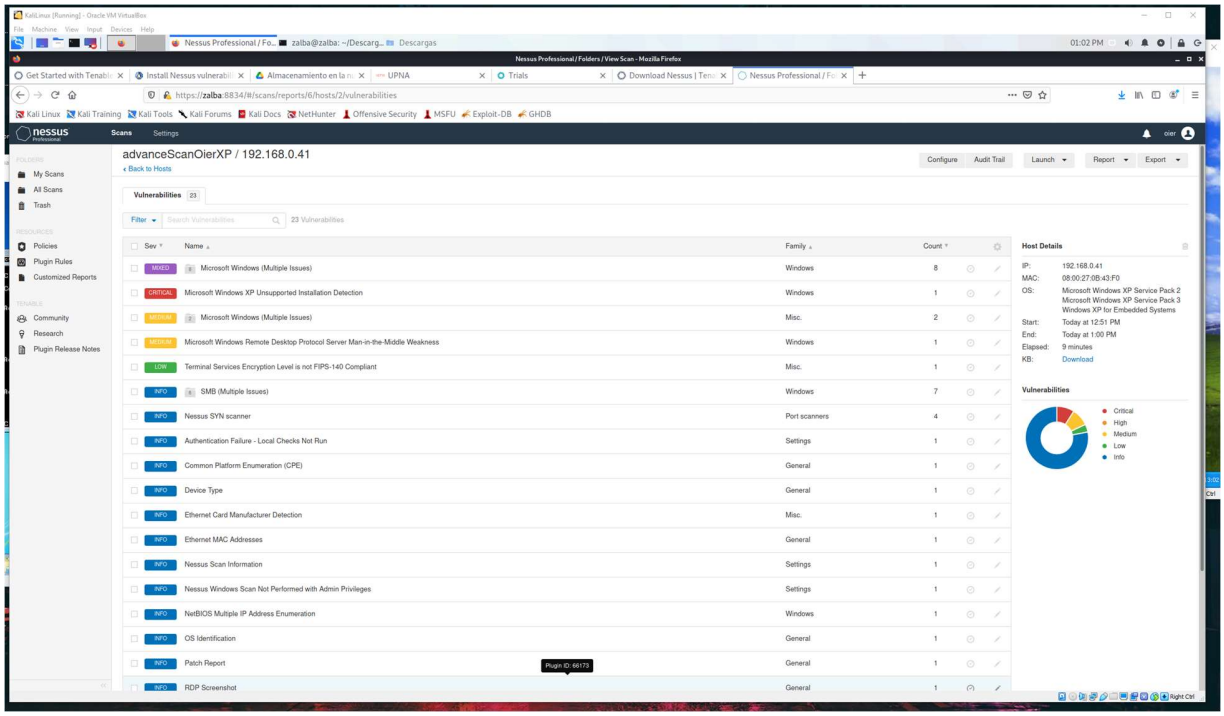



KaliLinux [Running] - Oracle VM VirtualBox
Nessus Professional / Folders / My Scans - Mozilla Firefox
https://zalba:8834/#/scans/folders
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
nessus Professional
Scans
Settings
oier
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
TENABLE
Community
Research
Plugin Release Notes
My Scans
Import
New Folder
New Scan
Search Scans
1 Scan
Name
Schedule
Last Modified
advanceScanOierXP
On Demand
N/A
Right Ctrl

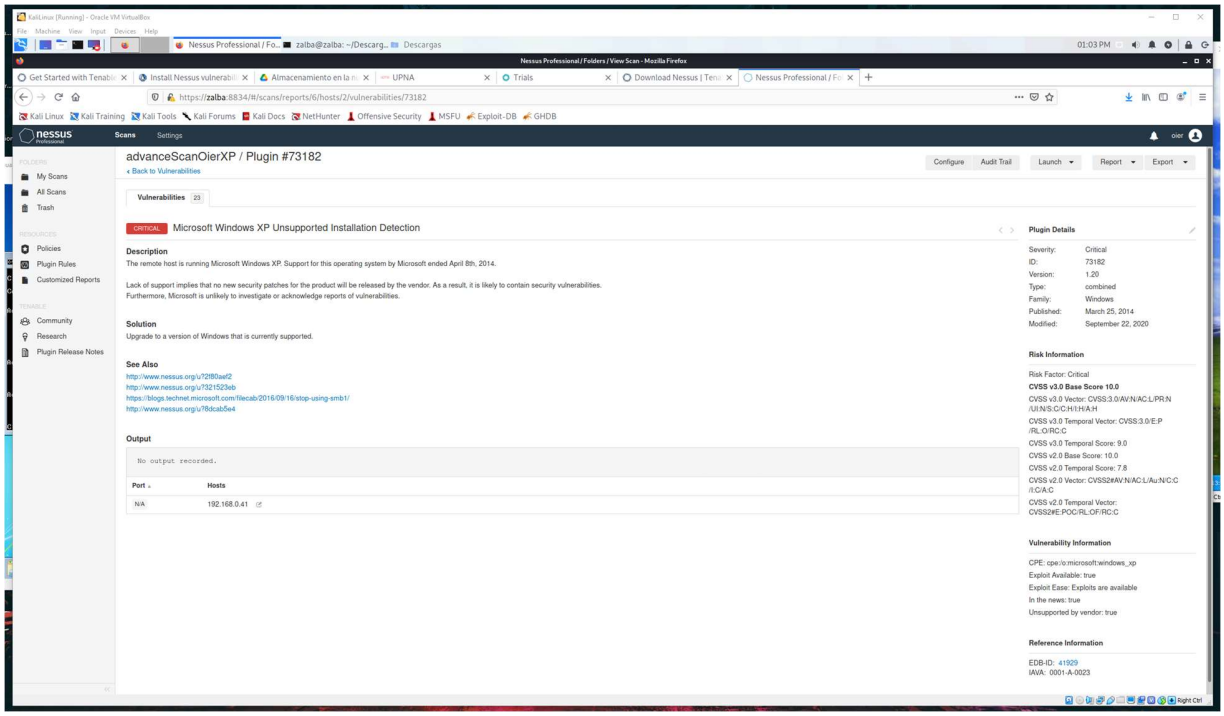

My Scans
Import
New Folder
New Scan
Name
Schedule
Last Modified
advanceScanOierXP
On Demand
Today at 1:00 PM

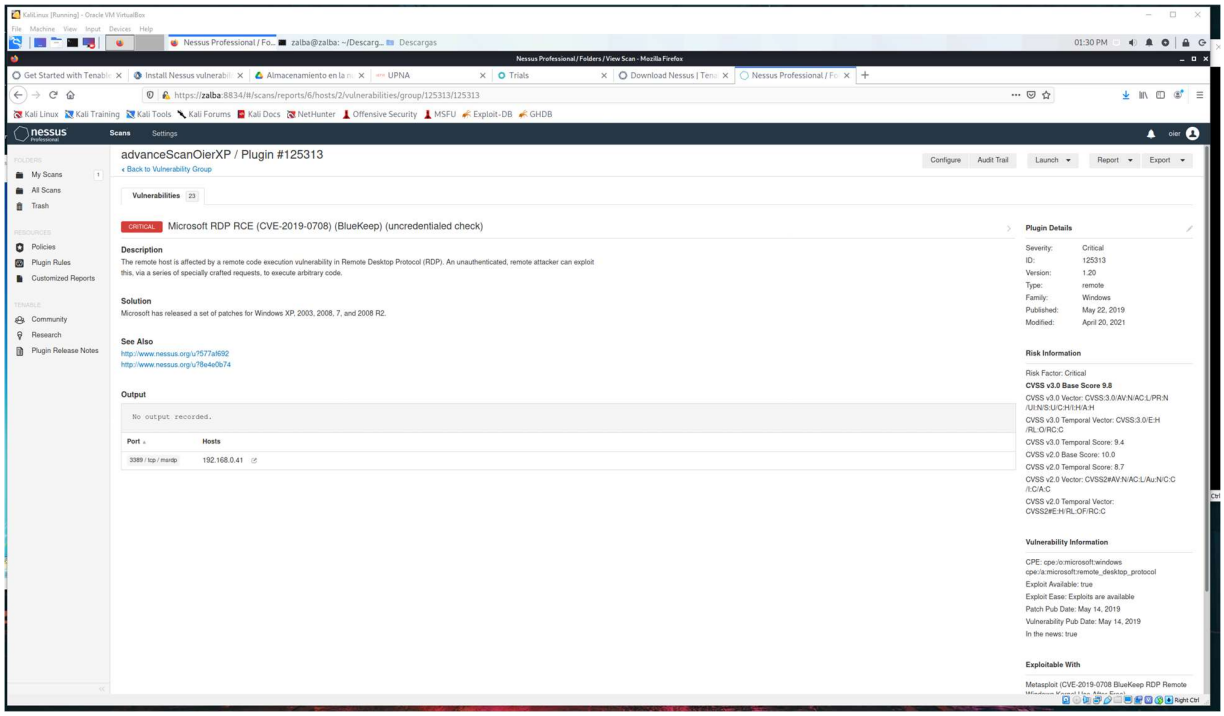
Podemos ver todas las vulnerabilidades, de mas criticas a menos



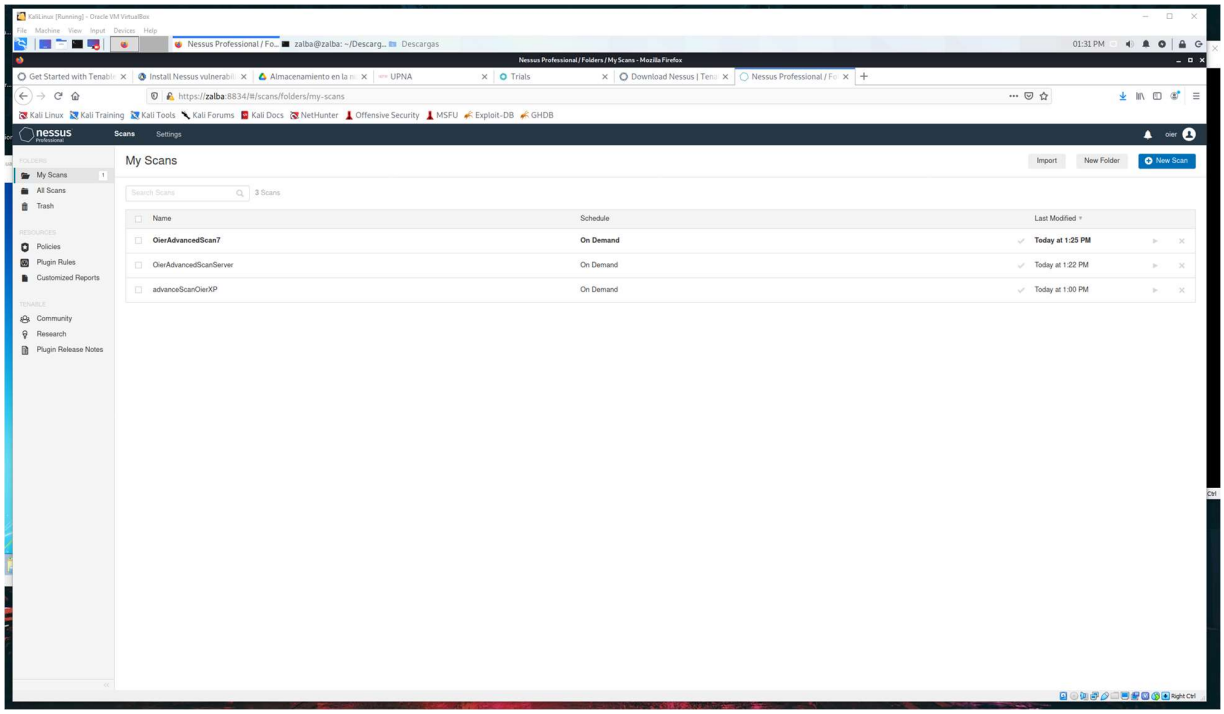


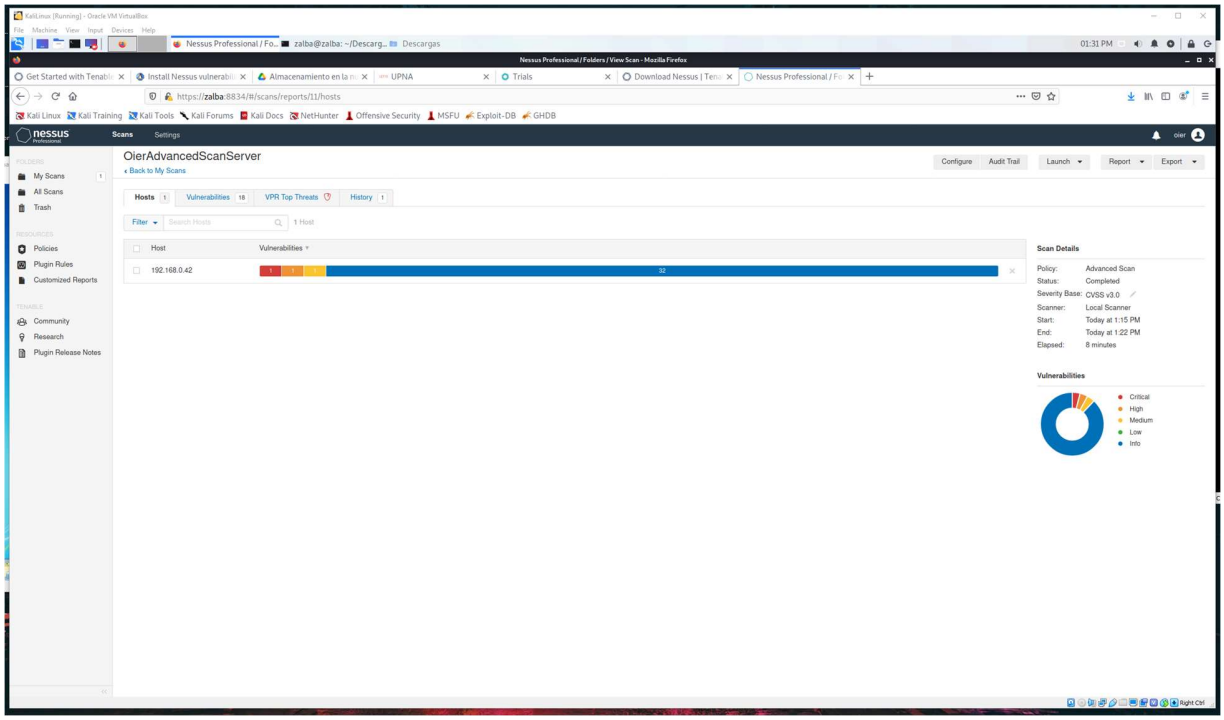
Las podemos ver con mas detalle

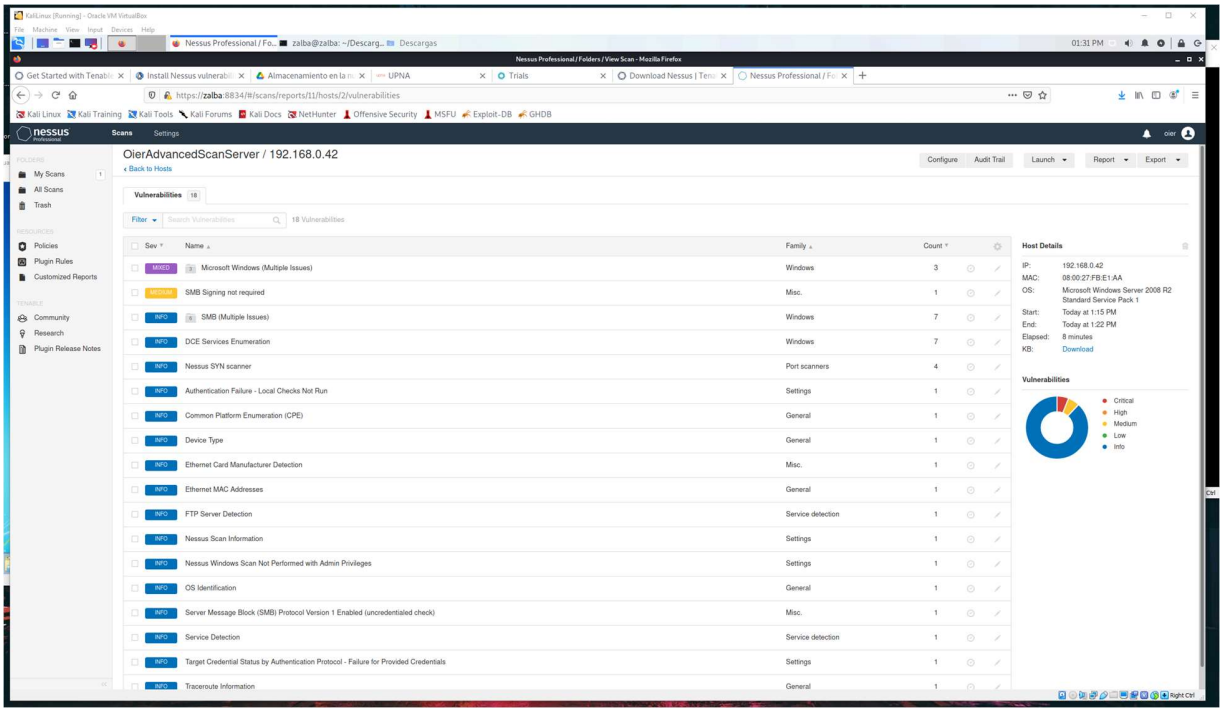


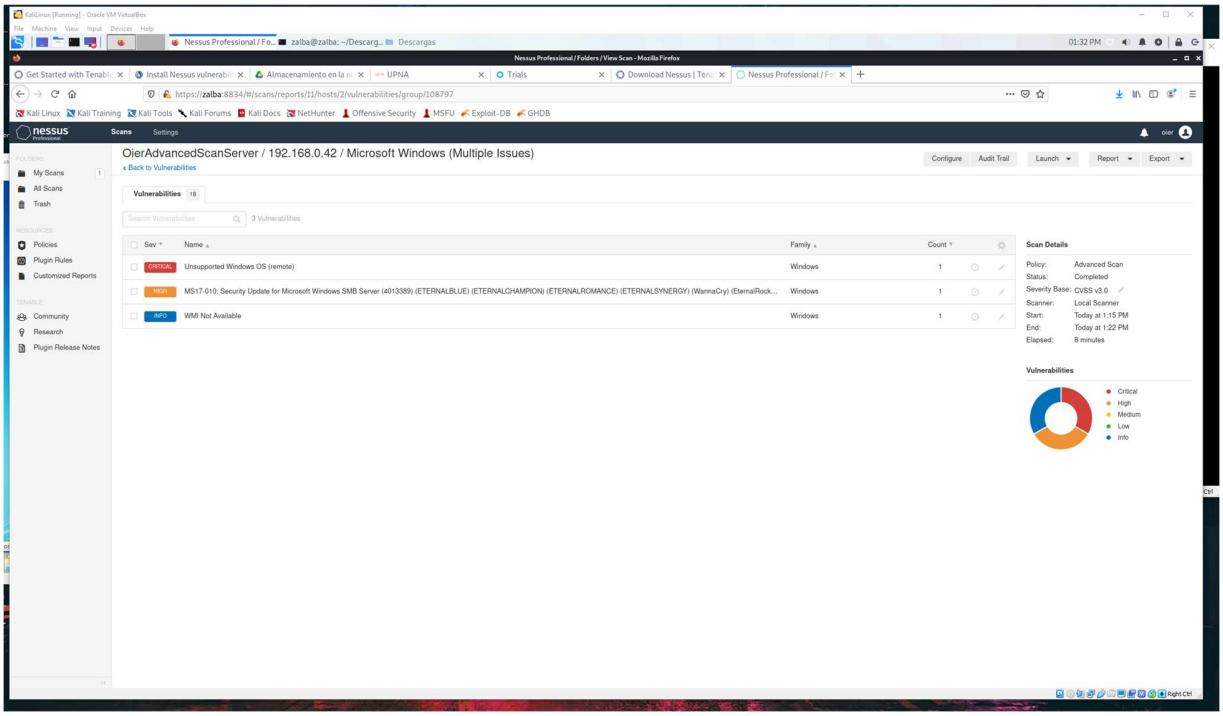


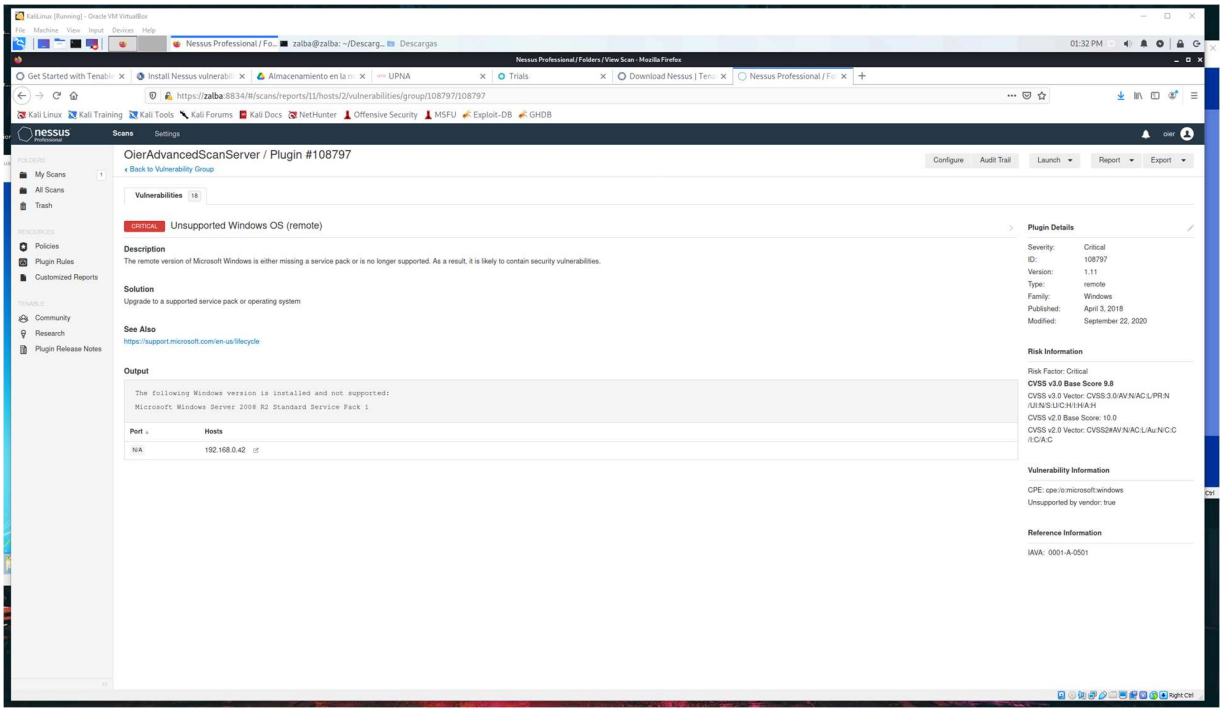
Obtenemos los escáneres de las 3 maquinas



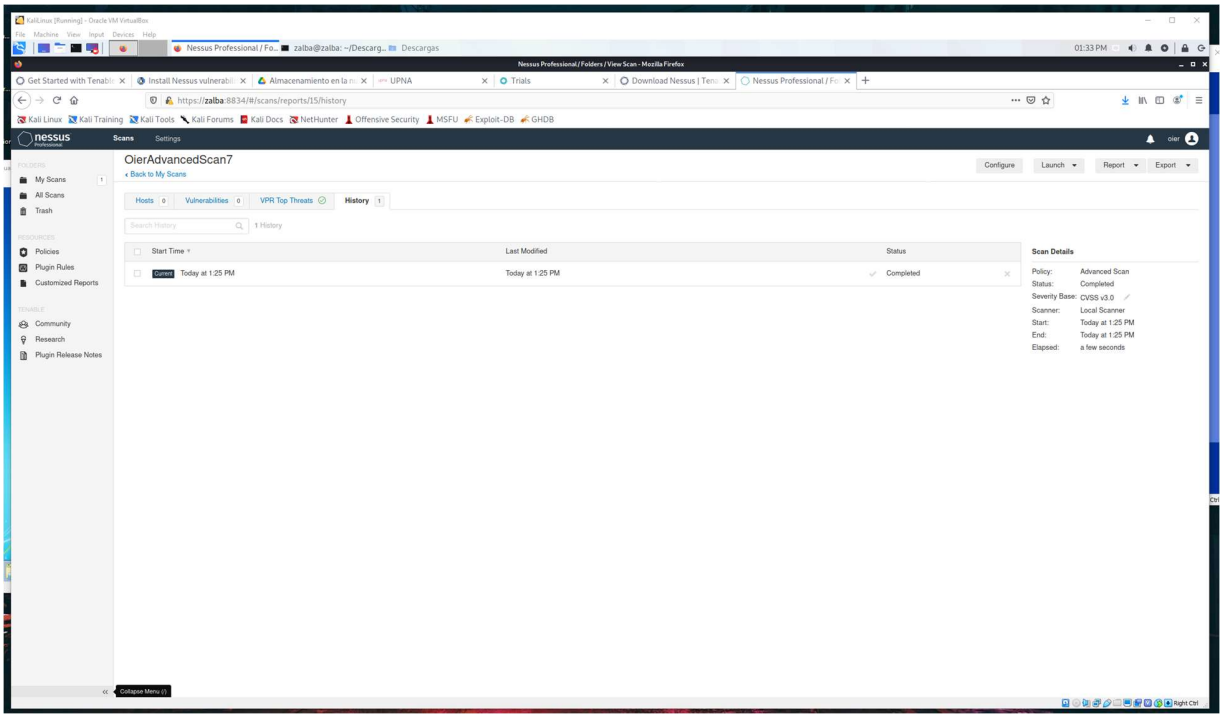



Nessus Professional / Folders / View Scan - Mozilla Firefox
https://zalba:8834/#/scans/reports/11/hosts/2/vulnerabilities
Scans
Settings
OierAdvancedScanServer / 192.168.0.42
Back to Hosts
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 18
Filter
Search Vulnerabilities
18 Vulnerabilities
Sev
Name
Family
Count
MIXED Microsoft Windows (Multiple Issues) Windows 3
MEDIUM 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 (uncredentialed 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
Critical
High
Medium
Low
Info

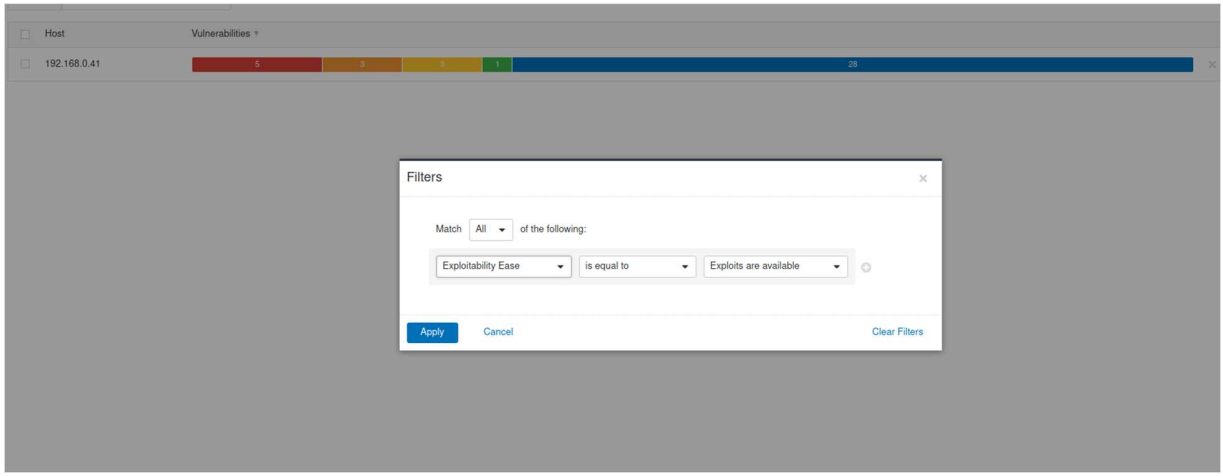

Nessus Professional / Folders / View Scan - Mozilla Firefox
https://zalba:8834/#/scans/reports/11/hosts/2/vulnerabilities/group/108797
Scans
Settings
OierAdvancedScanServer / 192.168.0.42 / Microsoft Windows (Multiple Issues)
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 18
Search Vulnerabilities
3 Vulnerabilities
Sev
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
Critical
High
Medium
Low
Info

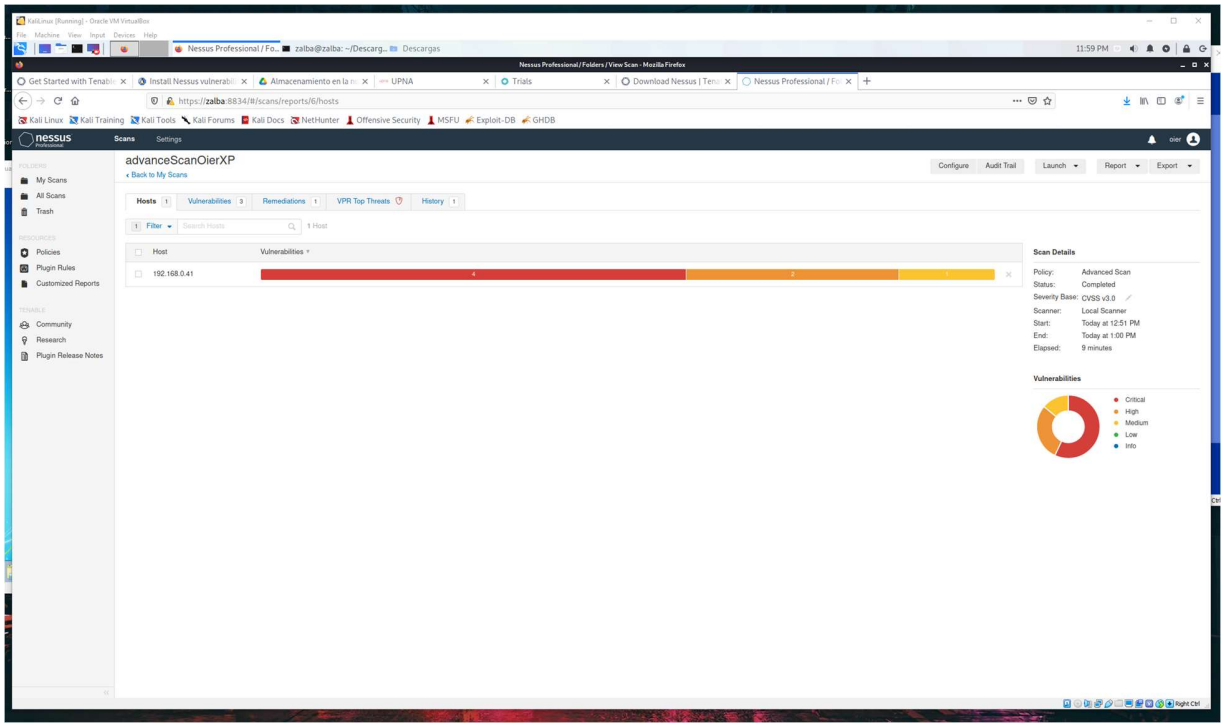


Para la de Windows 7 no conseguimos nada

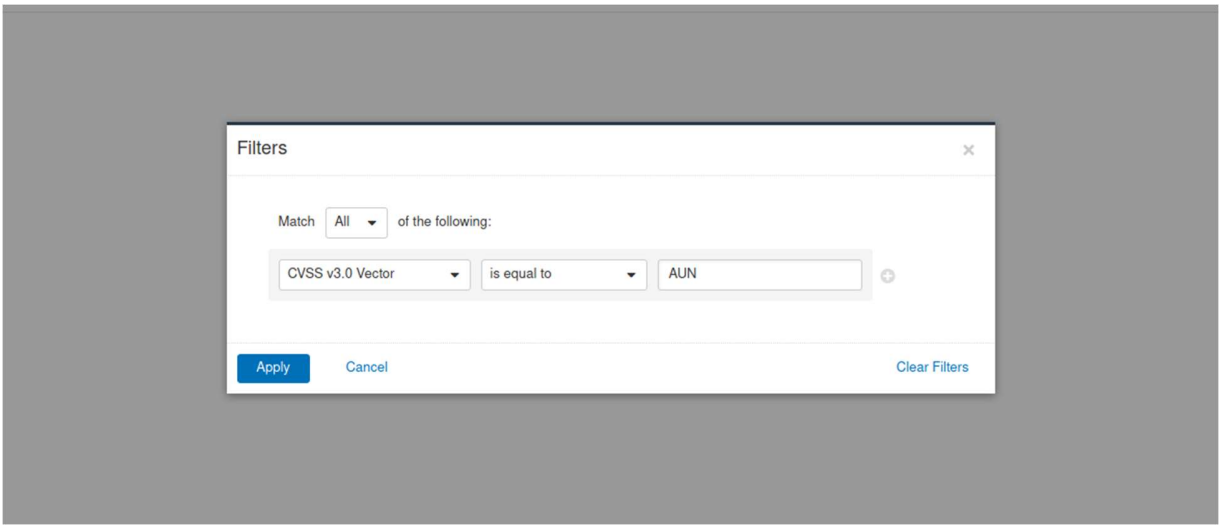


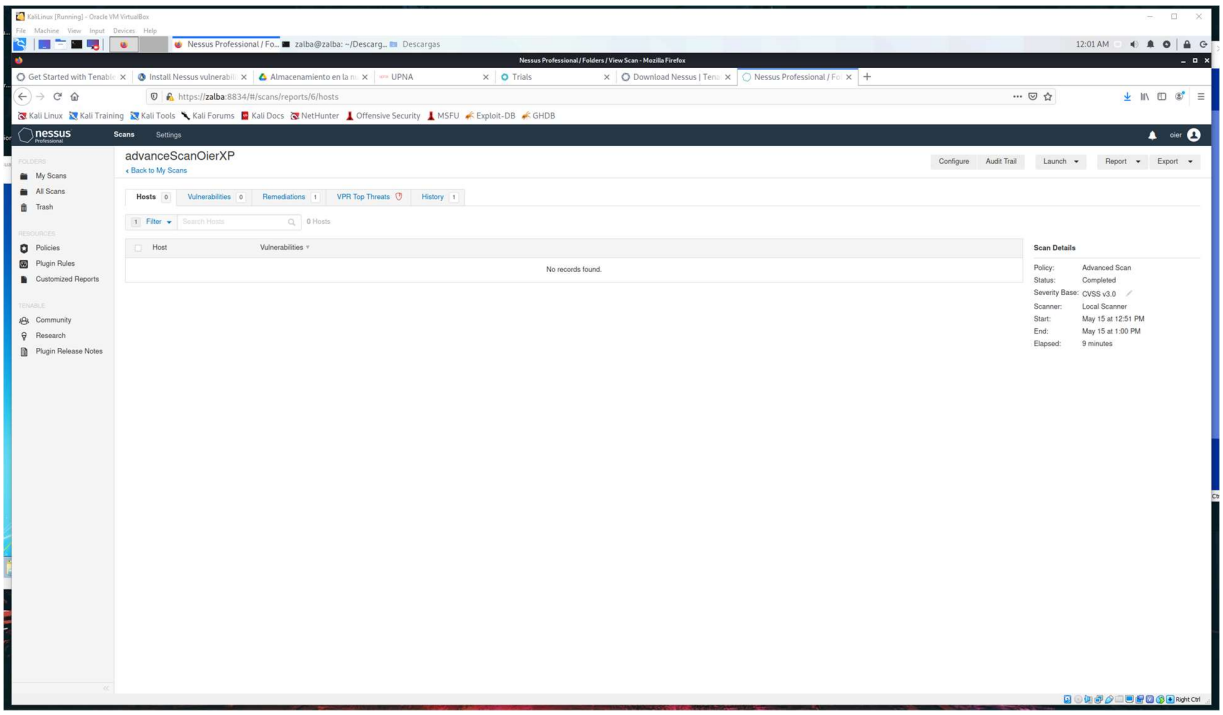
Ahora bien, podemos filtrar las vulnerabilidades que mas nos interesen, por ejemplo si son fáciles de explotar



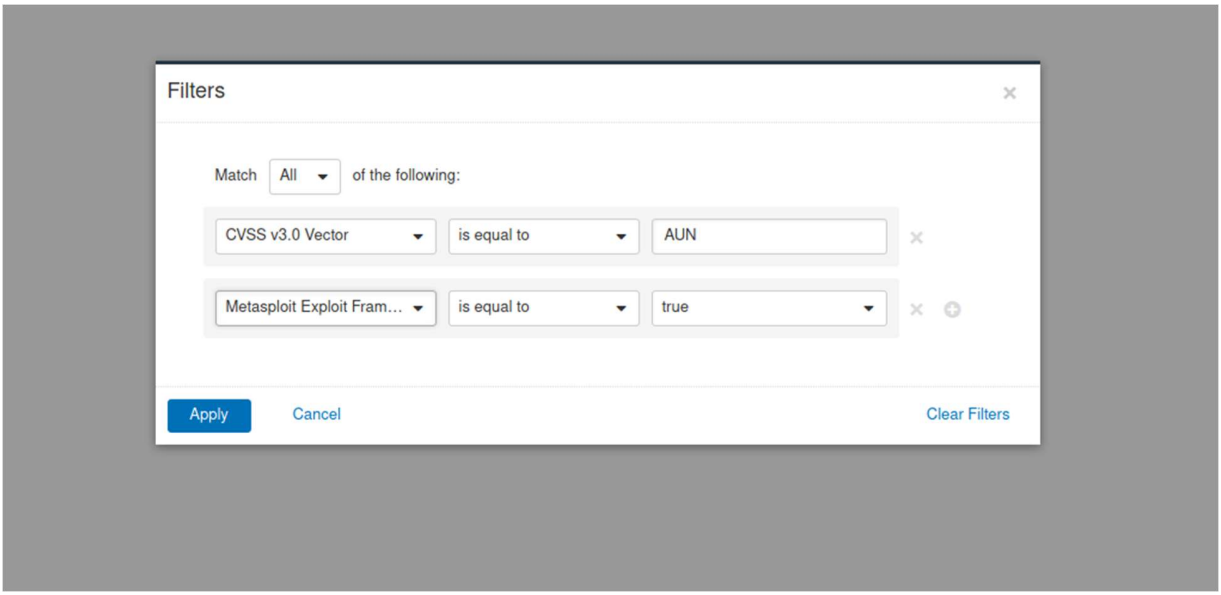


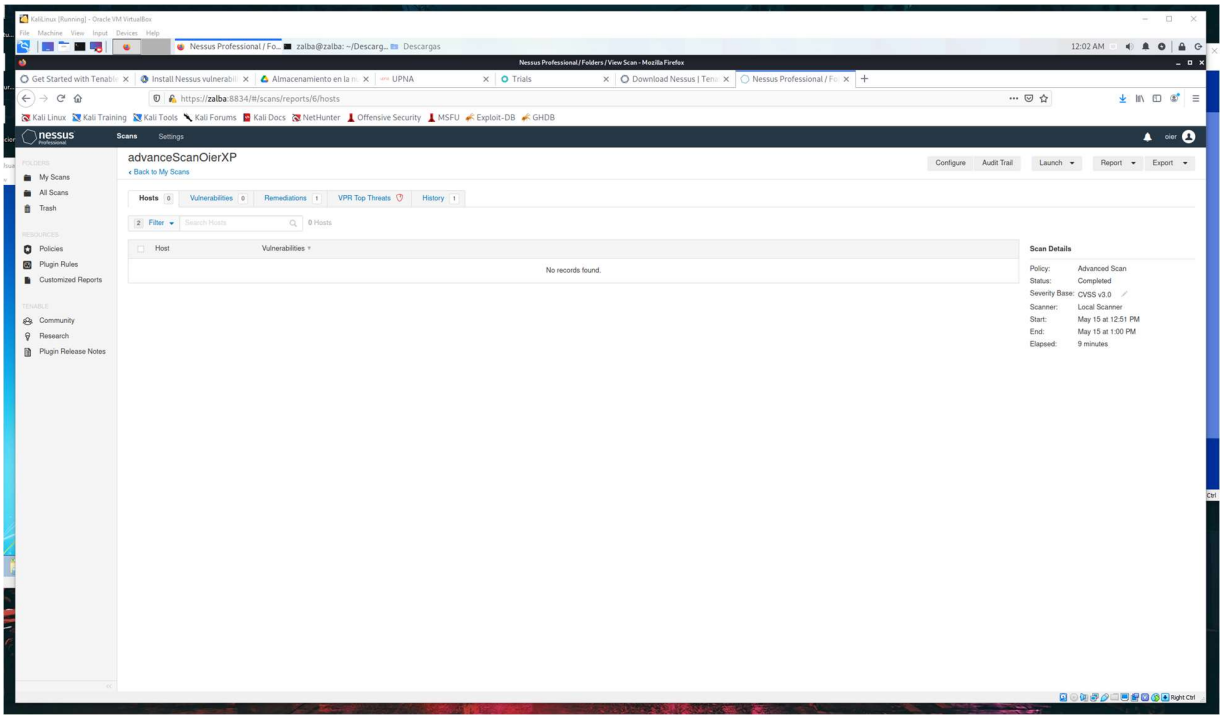
Con este filtro, filtramos las que se puedan explotar con un cvss vector



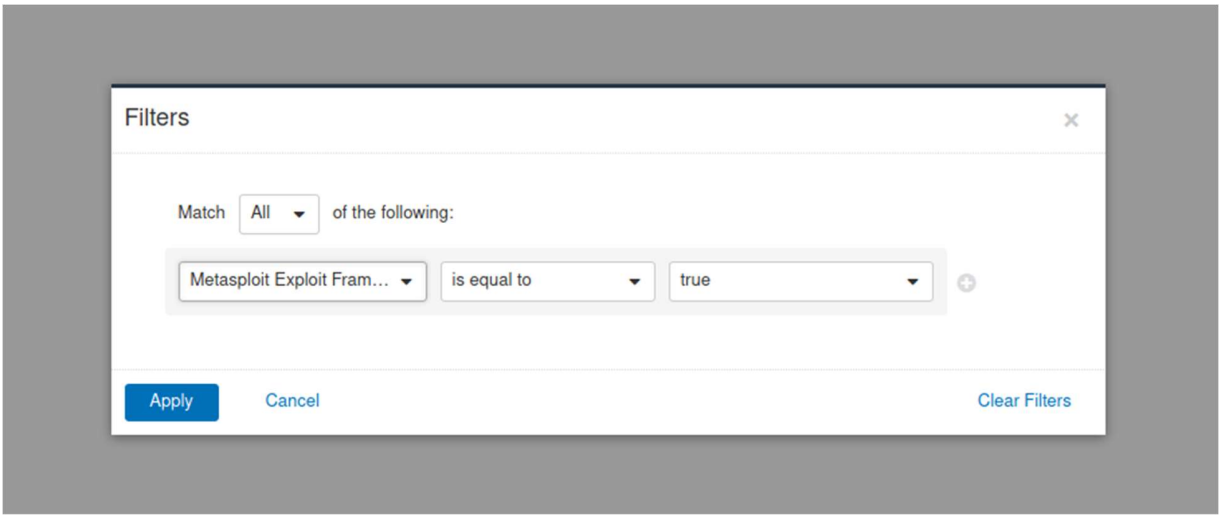


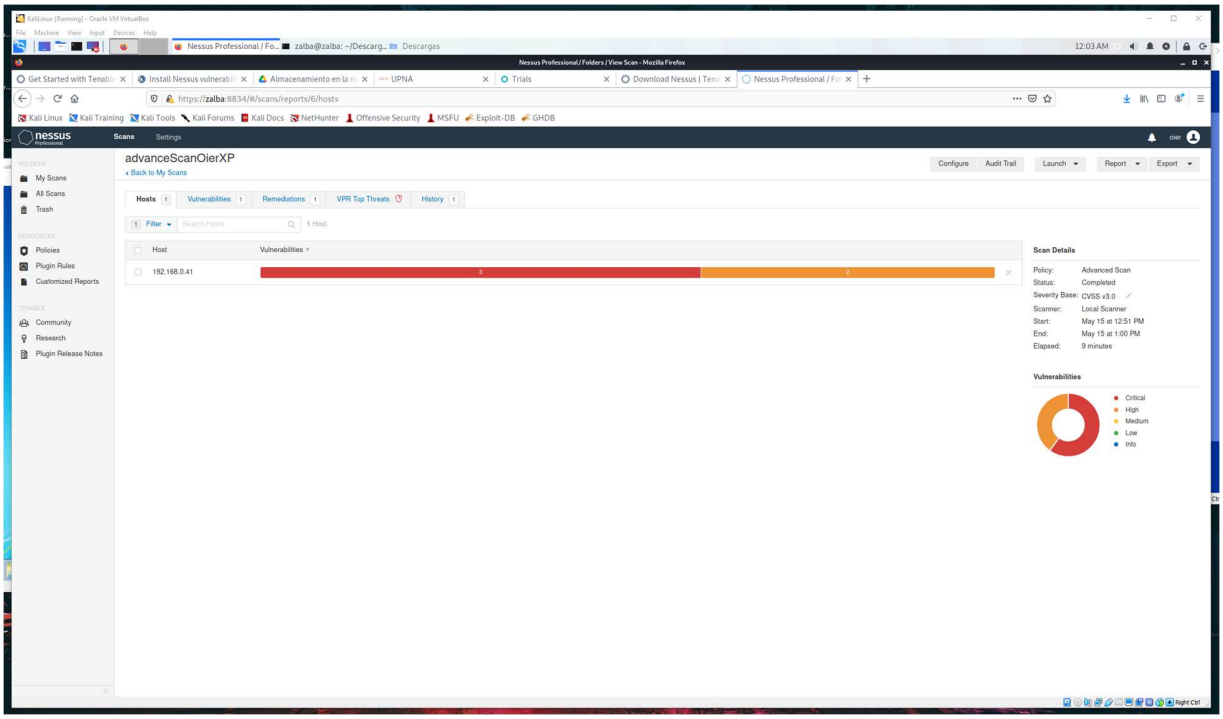
Incluso podemos aplicar varios filtros a la vez

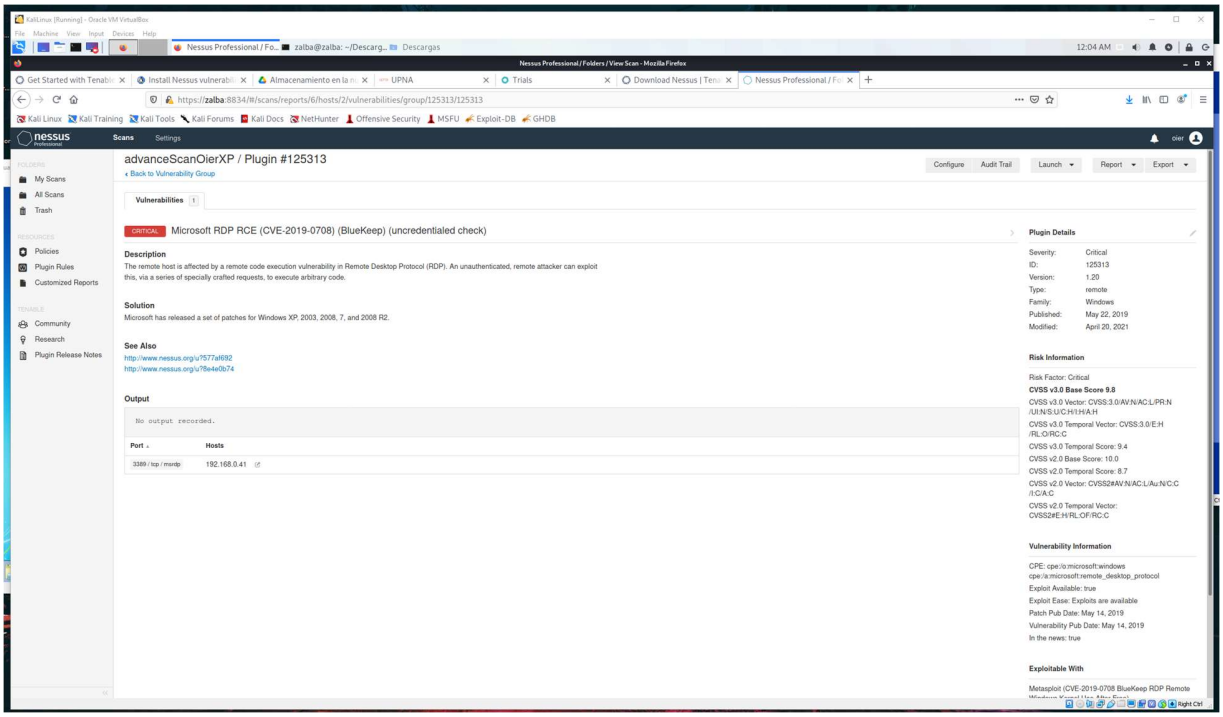


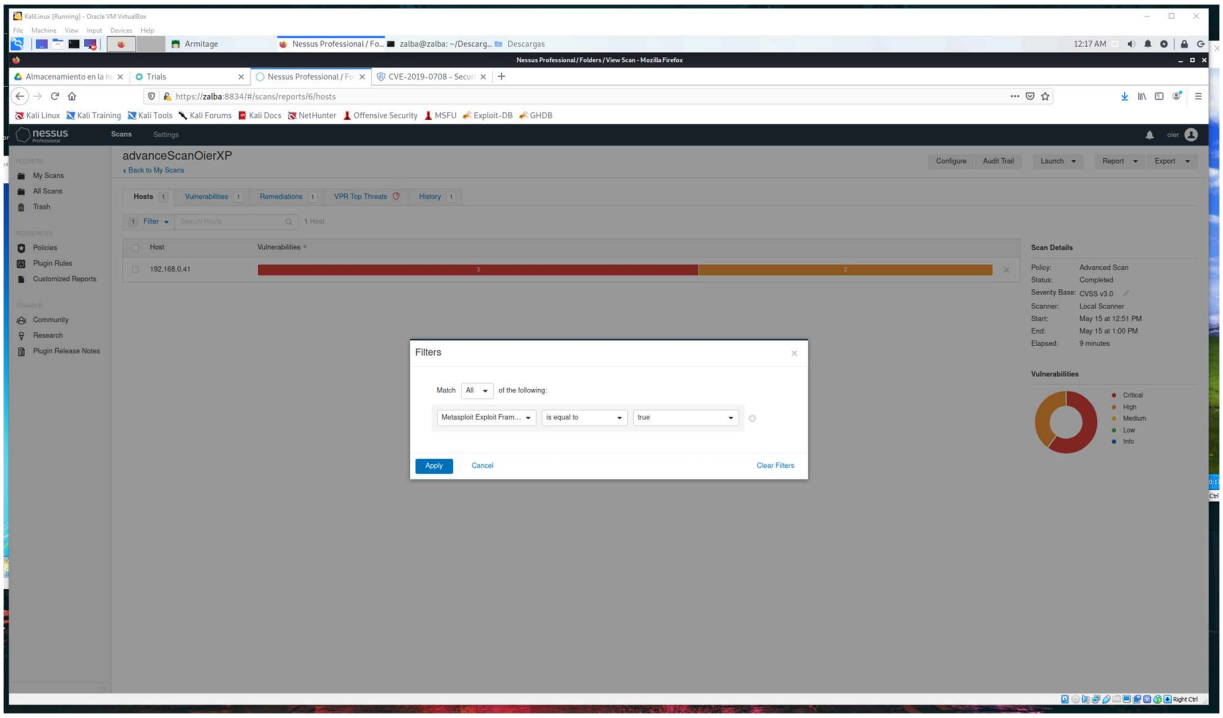


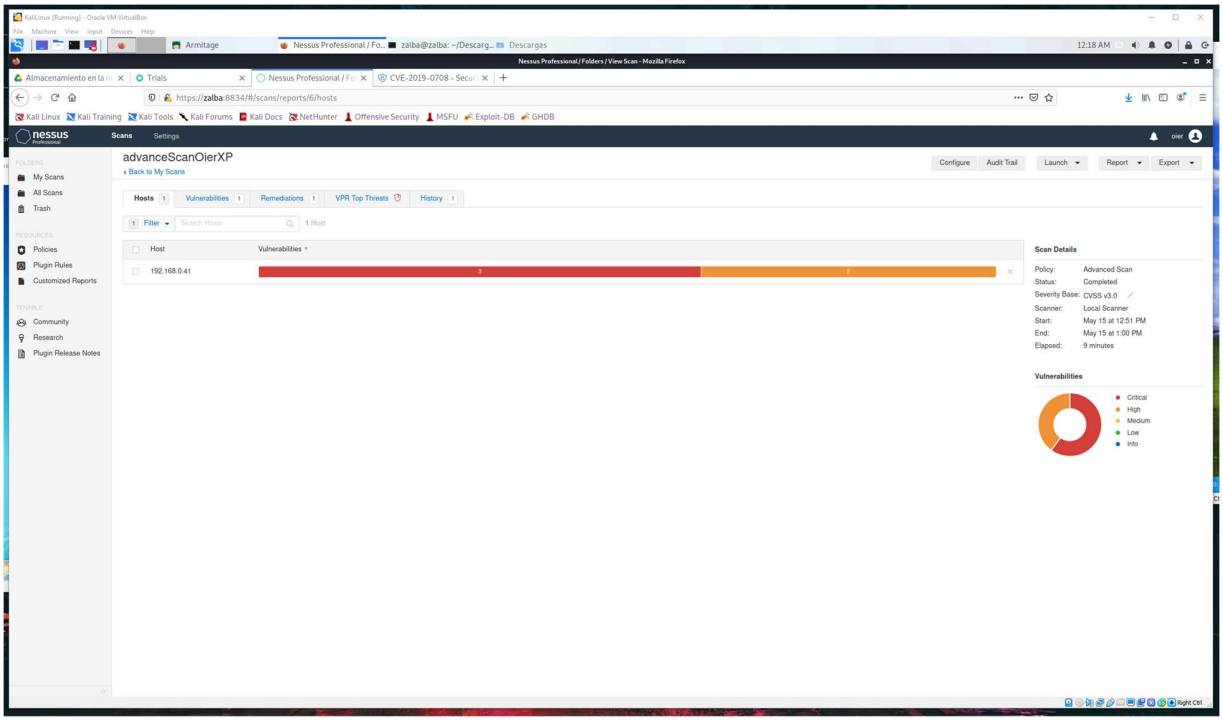
Este filtro es para vulnerabilidades con metaexploits

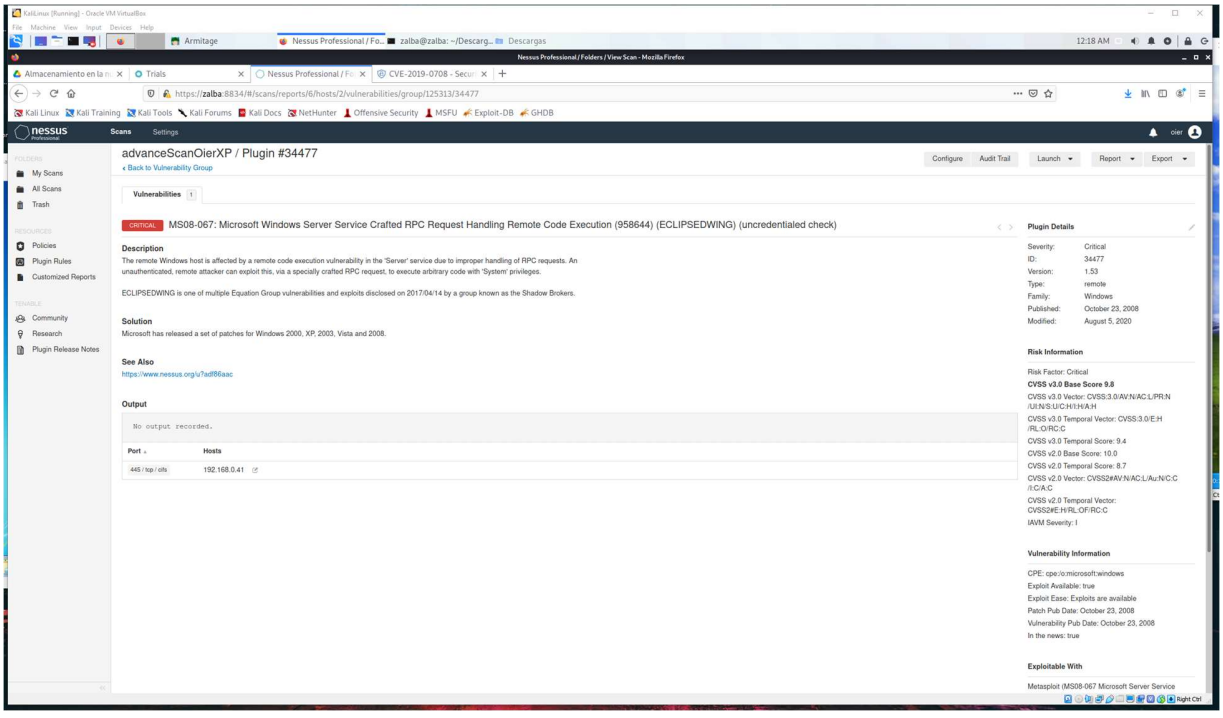

Filters
Match
All
of the following:
Metasploit Exploit Fram…
is equal to
true
Apply
Cancel
Clear Filters


nessus
Scans
Settings
advanceScanOierXP
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts
Vulnerabilities
Remediations
VPR Top Threats
History
Host
192.168.0.41
Scan Details
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
Vulnerabilities
Critical
High
Medium
Low
Info


advanceScanOierXP / Plugin #125313
Back to Vulnerability Group
Vulnerabilities 1
CRITICAL
Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed 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?577af692
http://www.nessus.org/u?8e4e0b74
Output
No output recorded.
Port
Hosts
3389 / tcp / msrdp
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 Base Score 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C
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/A:C
CVSS v2.0 Temporal Vector: CVSS2#E:H/RL:OF/RC:C
Vulnerability Information
CPE: cpe:/o:microsoft:windows
cpe:/a: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
Exploitable With
Metasploit (CVE-2019-0708 BlueKeep RDP Remote


advanceScanOierXP
Back to My Scans
Hosts 1
Vulnerabilities 1
Remediations 1
VPR Top Threats
History 1
Host
Vulnerabilities
192.168.0.41
Filters
Match All of the following:
Metasploit Exploit Fram...
is equal to
true
Apply
Cancel
Clear Filters
Scan Details
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
Vulnerabilities
Critical
High
Medium
Low
Info


advanceScanOierXP
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 1
Remediations 1
VPR Top Threats
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
192.168.0.41
3
2
Scan Details
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
Vulnerabilities
Critical
High
Medium
Low
Info


advanceScanOierXP / Plugin #34477
Back to Vulnerability Group
Vulnerabilities 1
CRITICAL
MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)
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.
ECLIPSEDWING 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
https://www.nessus.org/u?adf86aac
Output
No output recorded.
Port
Hosts
445 / tcp / cifs
192.168.0.41
Plugin Details
Severity: Critical
ID: 34477
Version: 1.53
Type: remote
Family: Windows
Published: October 23, 2008
Modified: August 5, 2020
Risk Information
Risk Factor: Critical
CVSS v3.0 Base Score 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C
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/A:C
CVSS v2.0 Temporal Vector: CVSS2#E:H/RL:OF/RC:C
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
Exploitable With
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

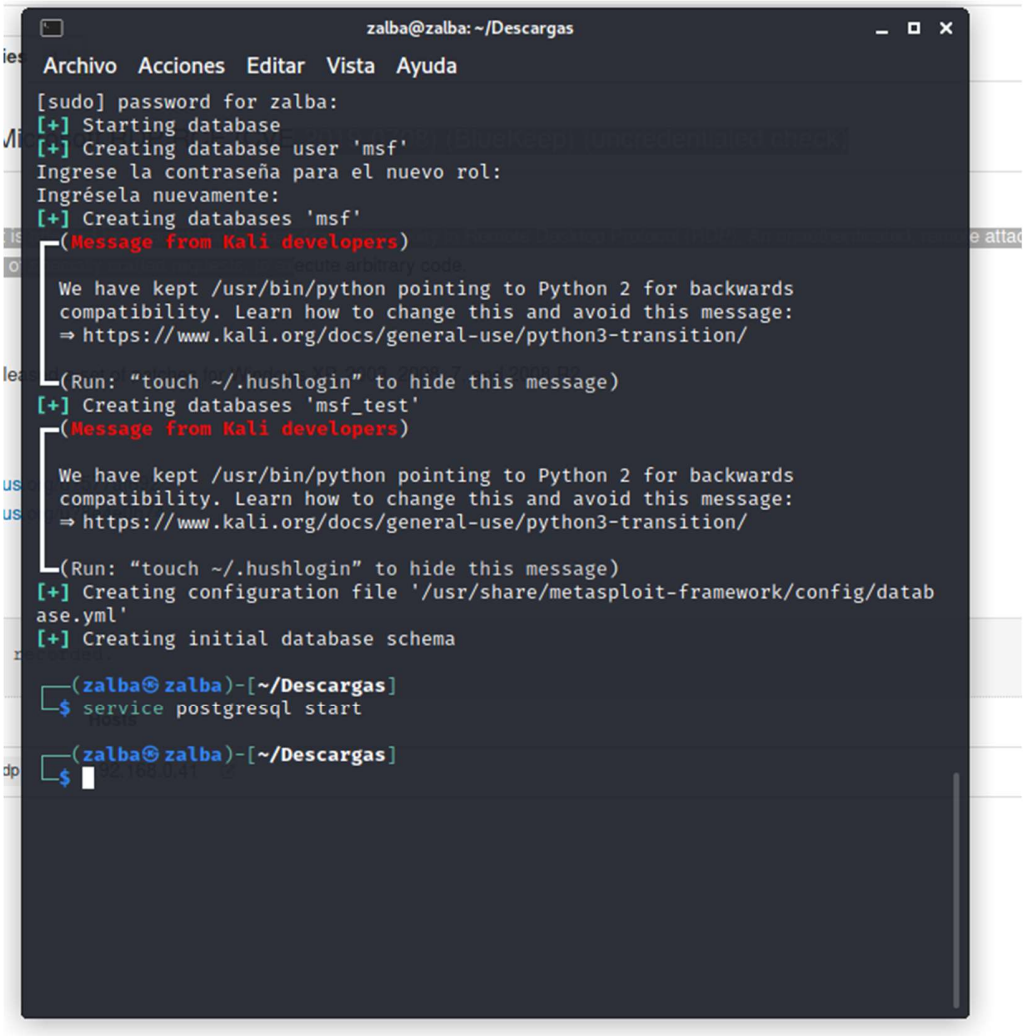
Metasploit (MS08-067 Microsoft Server Service Relative Path Stack Corruption)

CANVAS ()

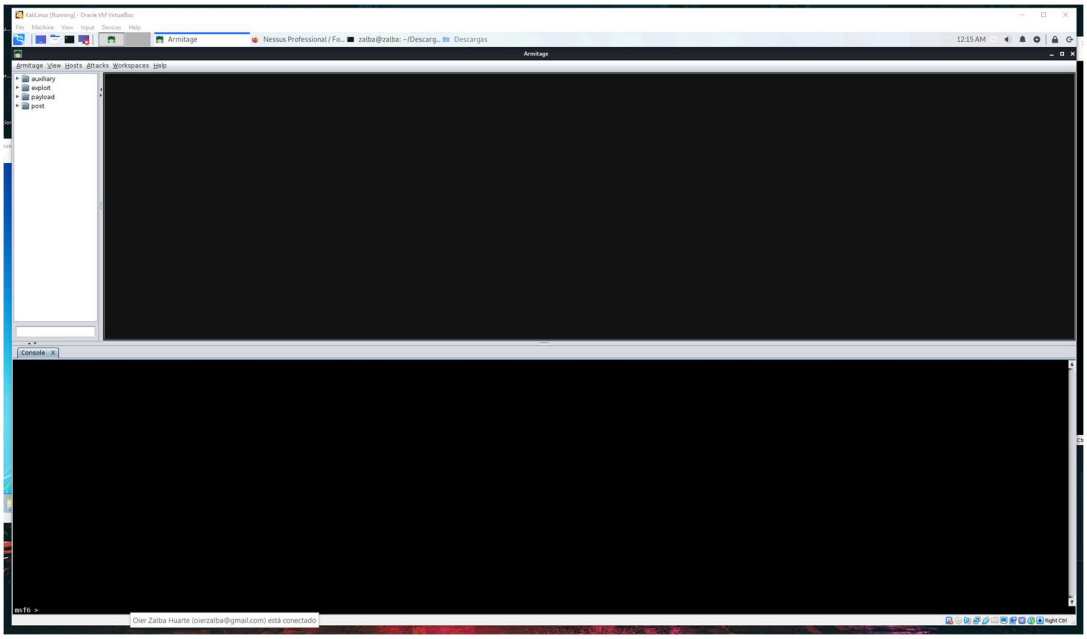
Core Impact

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

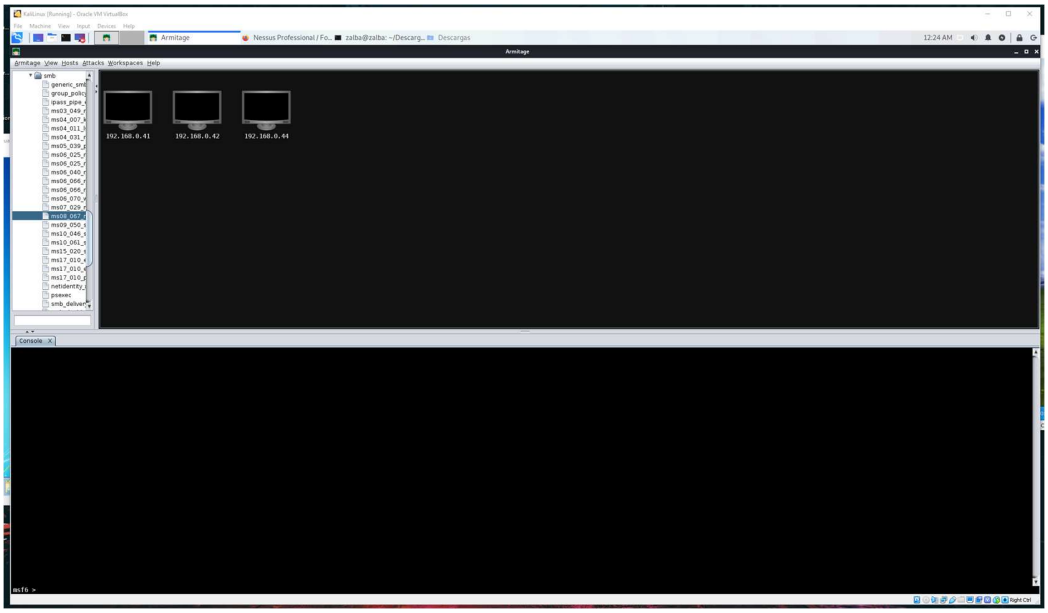
En primer lugar, tenemos que iniciar la base de datos y el servicio postgresql



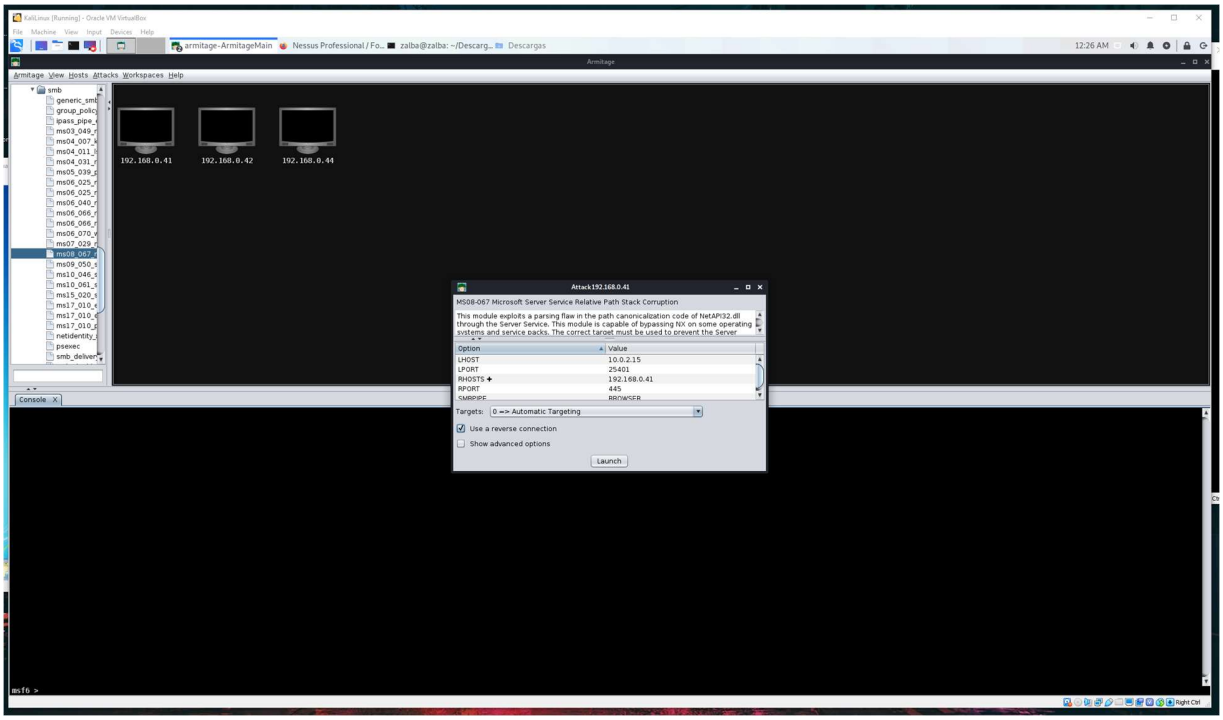
Ya podemos ejecutar armitage



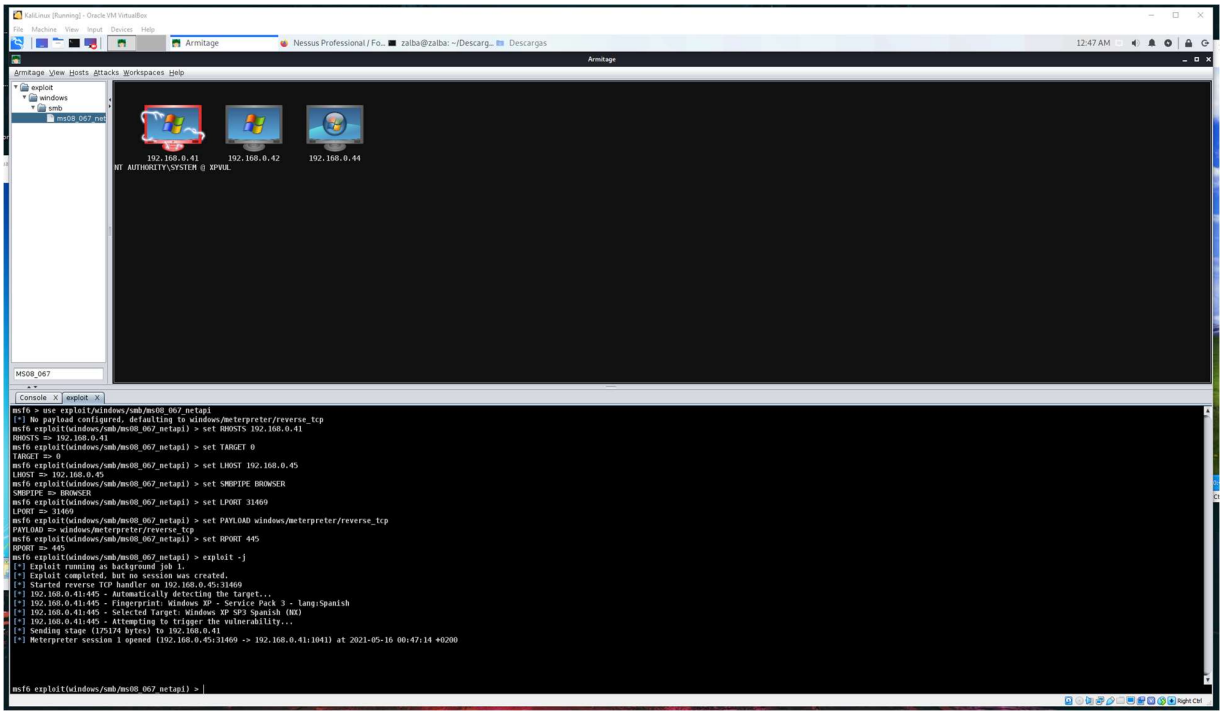
Añadimos los hosts de las maquinas que queremos atacar y les aplicamos un quick scan o un intense scan. Así podemos volver a ver los puertos abiertos (lo que hacíamos con nmap) y también podemos identificar el sistema operativo.



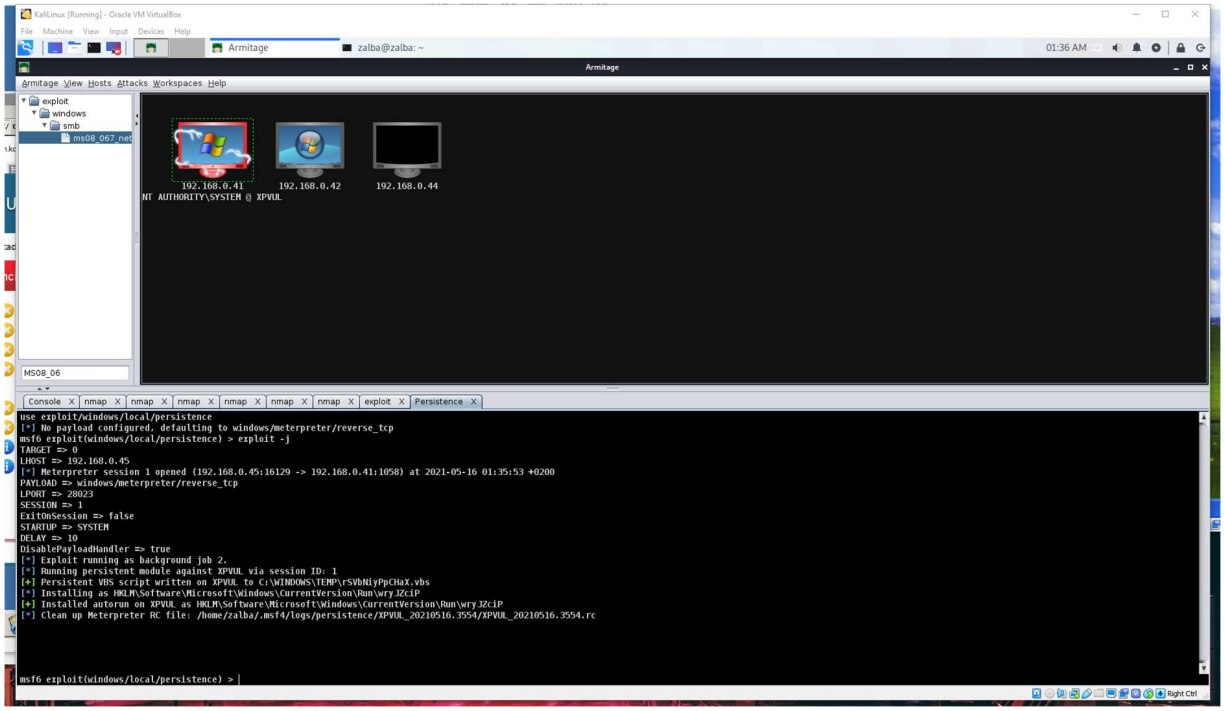
Buscamos el exploit que hemos encontrado en Nessus y lo aplicamos a la maquina correspondiente



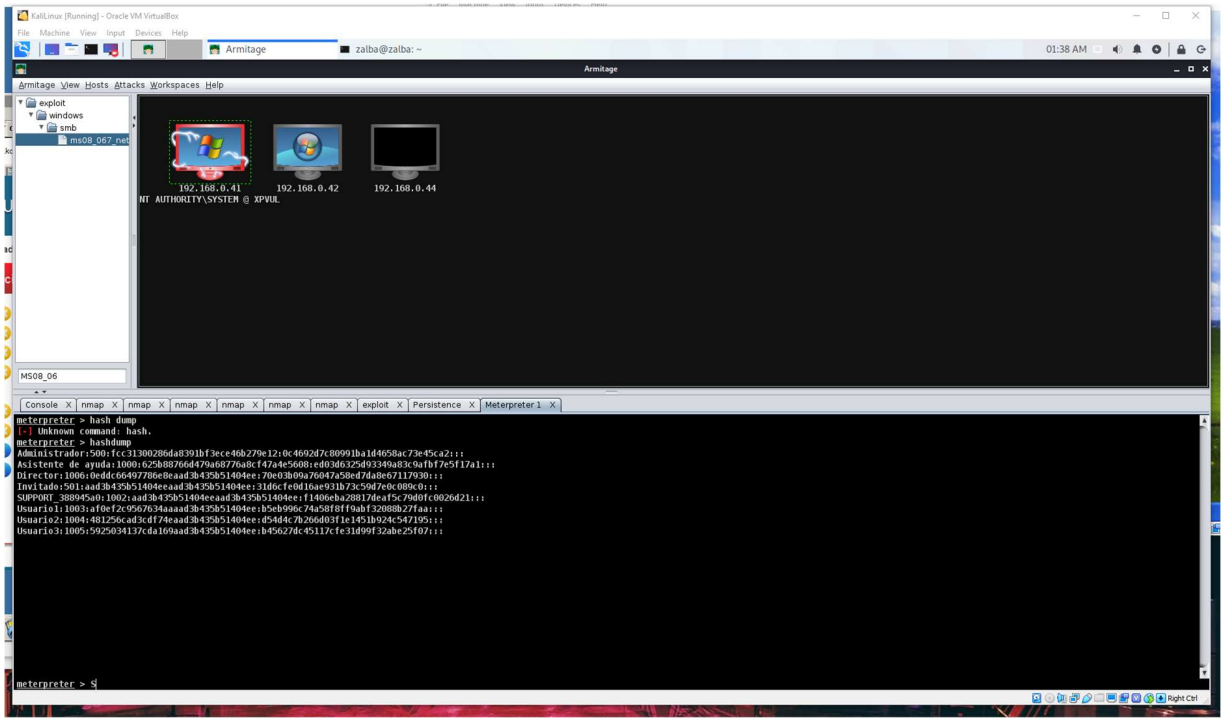
Cuando la maquina se pone en rojo, se ha vulnerado con éxito.



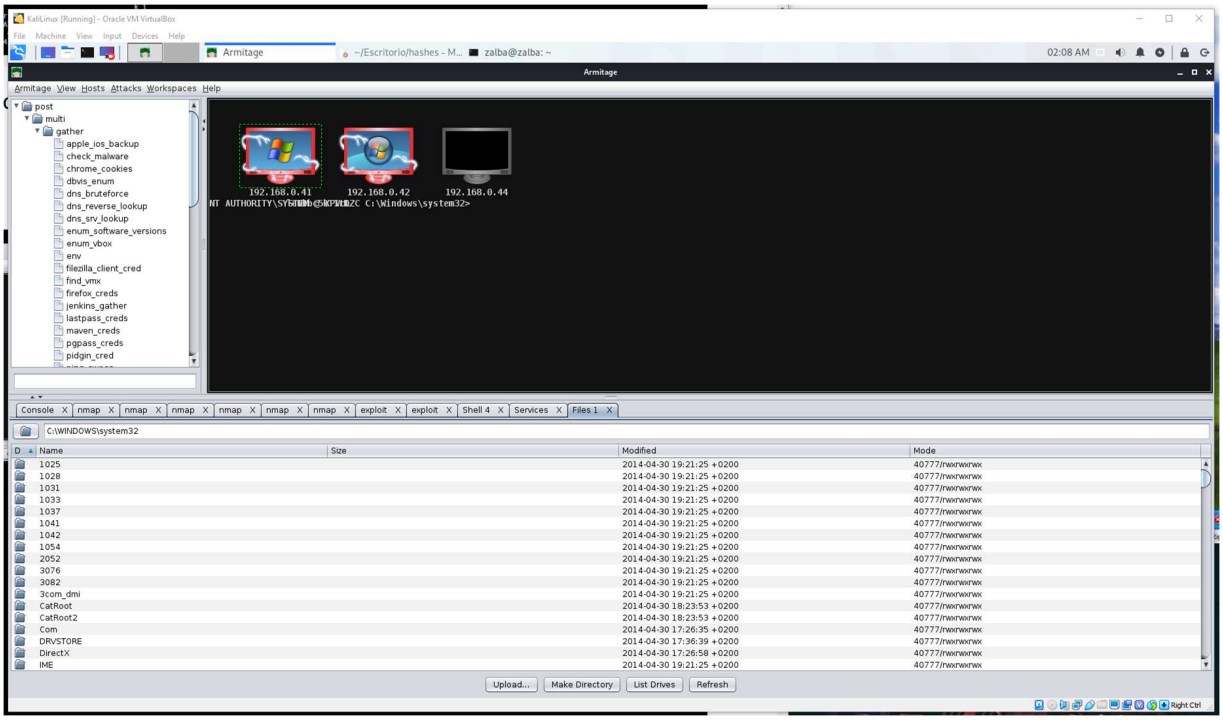
Lo primero que hay que hacer es ponerlo persistente para que aguante.



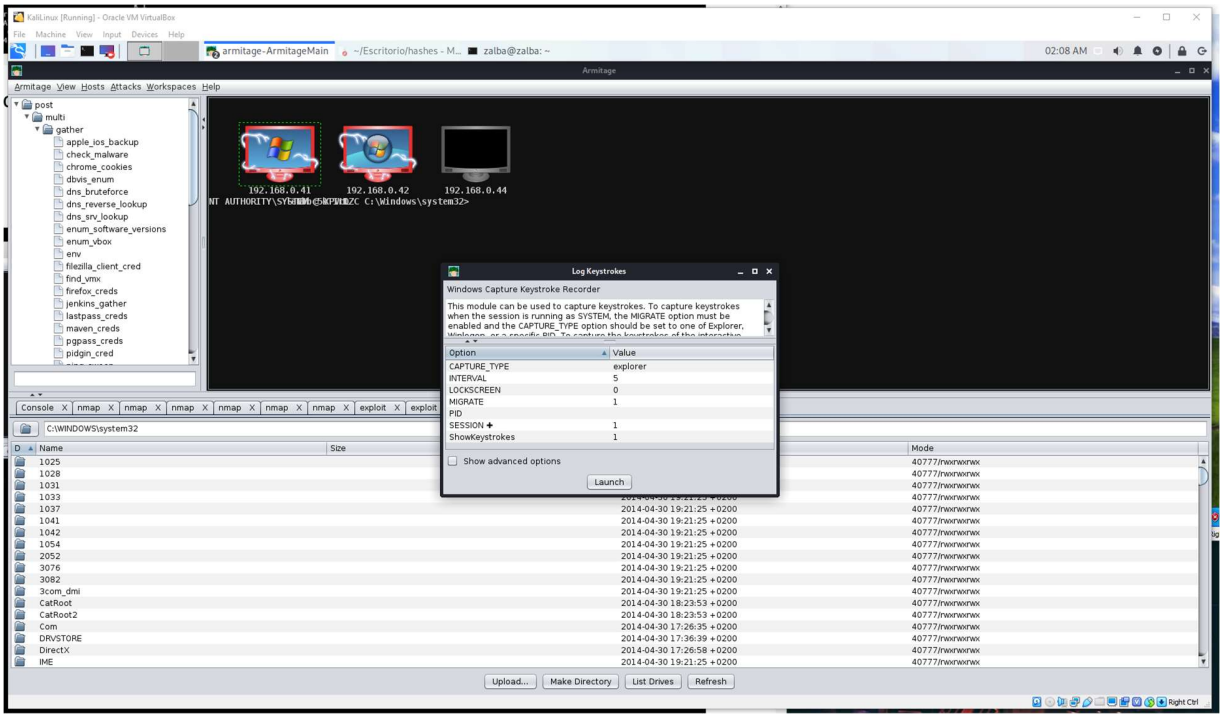
Abrimos una consola de meterpreter donde podemos ejecutar muchos comandos de interes. En este caso, hacemos un hashdump para obtener los hashes de las contraseñas del Windows.



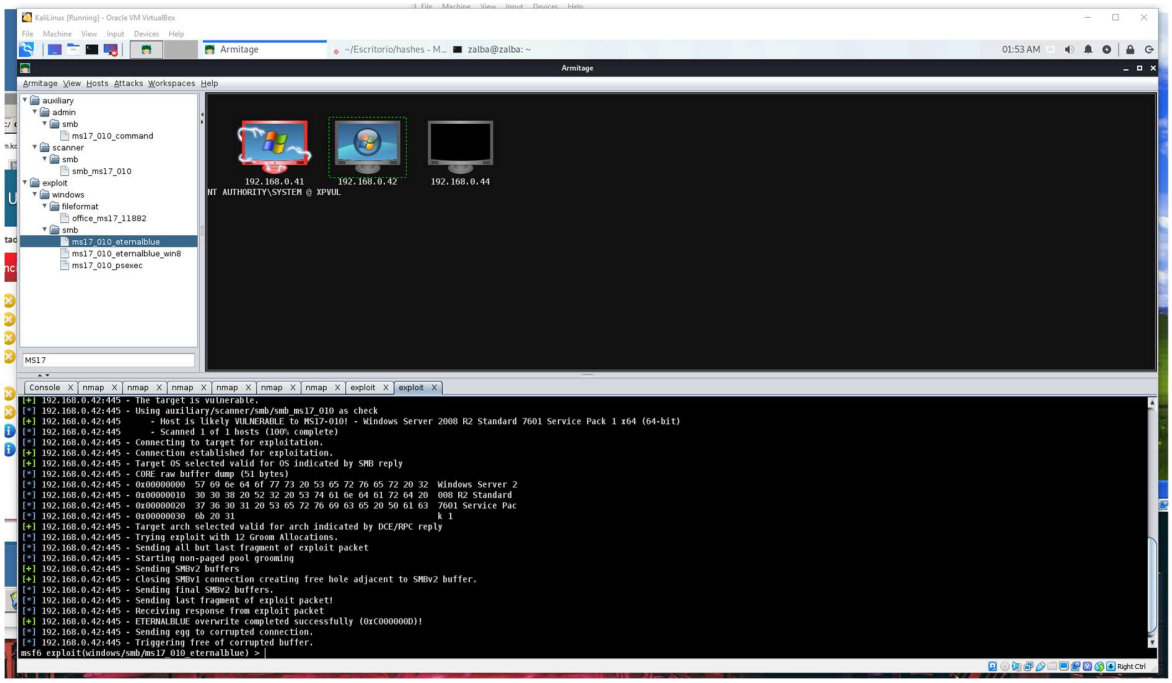
Una vez que la maquina esta vulnerada, podemos hacer muchas cosas, como por ejemplo ver los archivos del sistema.

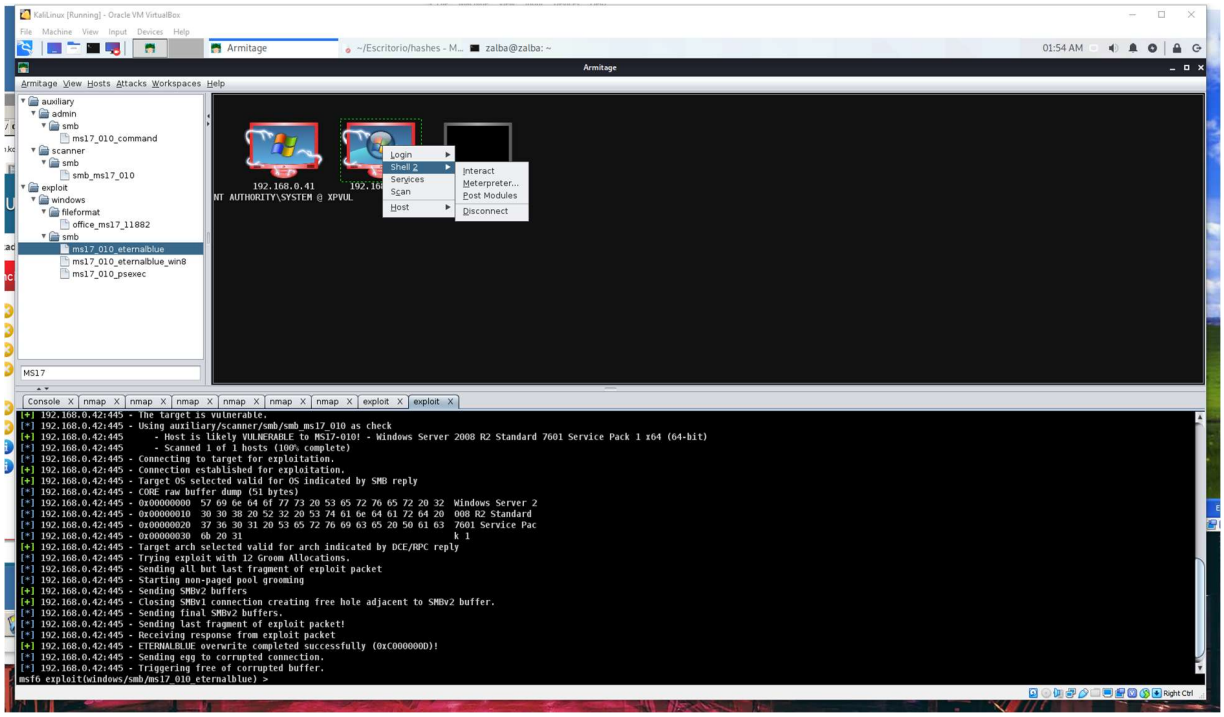


También podemos poner un keystroke para ver lo que teclea el sistema victima.

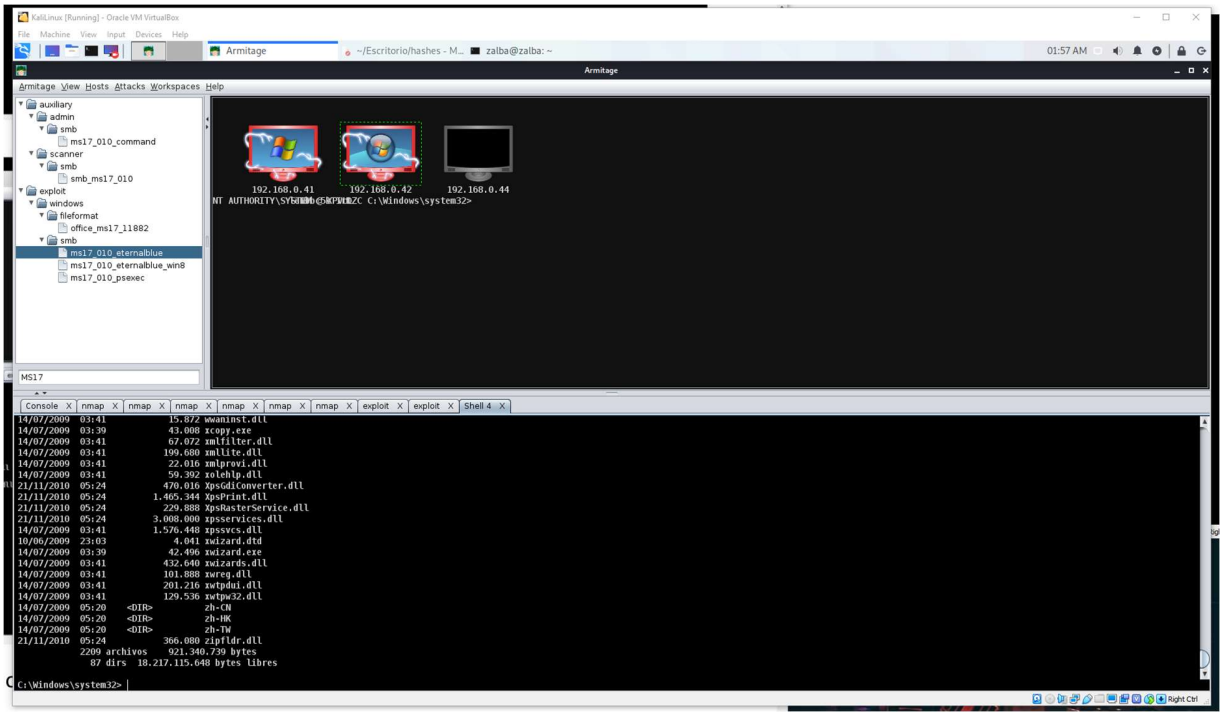


Ahora vamos a vulnerar la maquina con Windows server con el exploit ms17_010_eternalblue

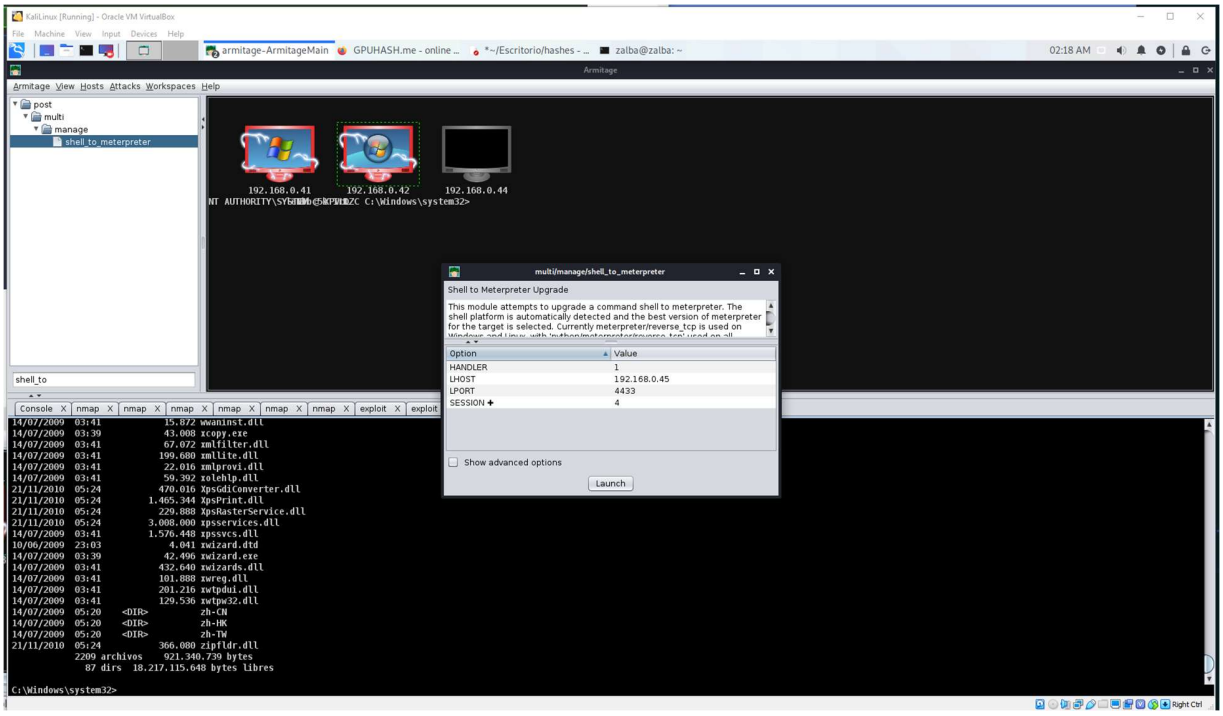




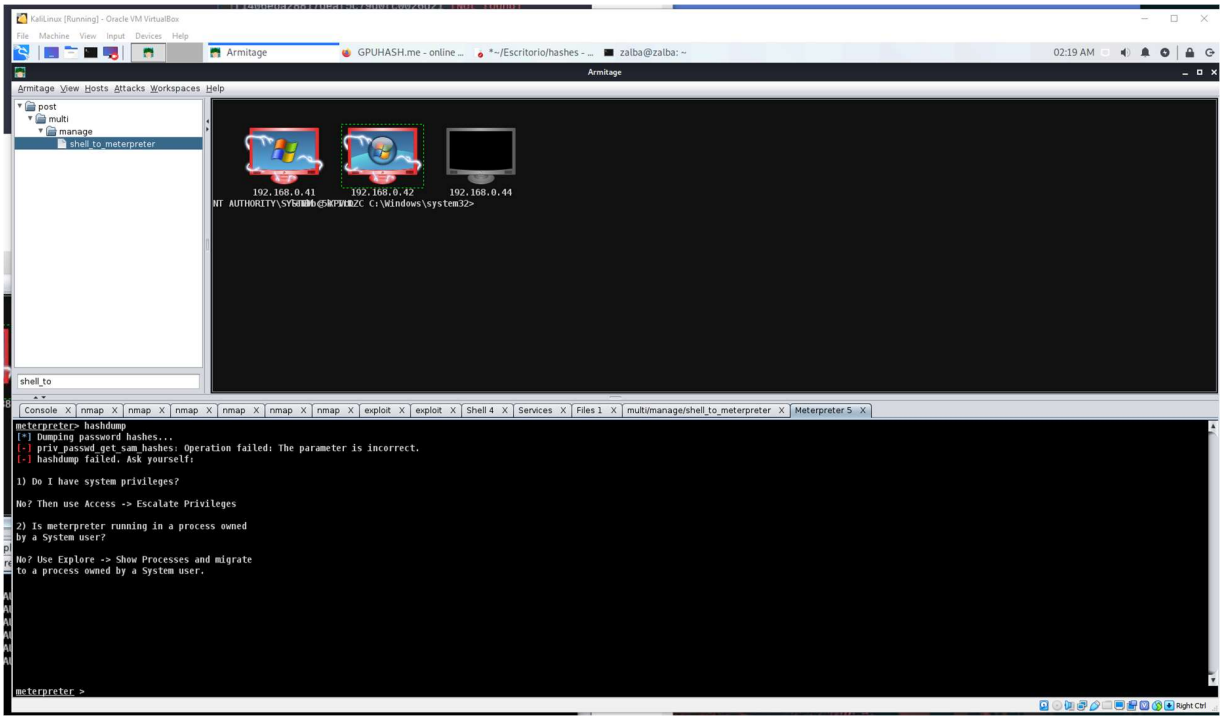
Abrimos una Shell del sistema de Windows server



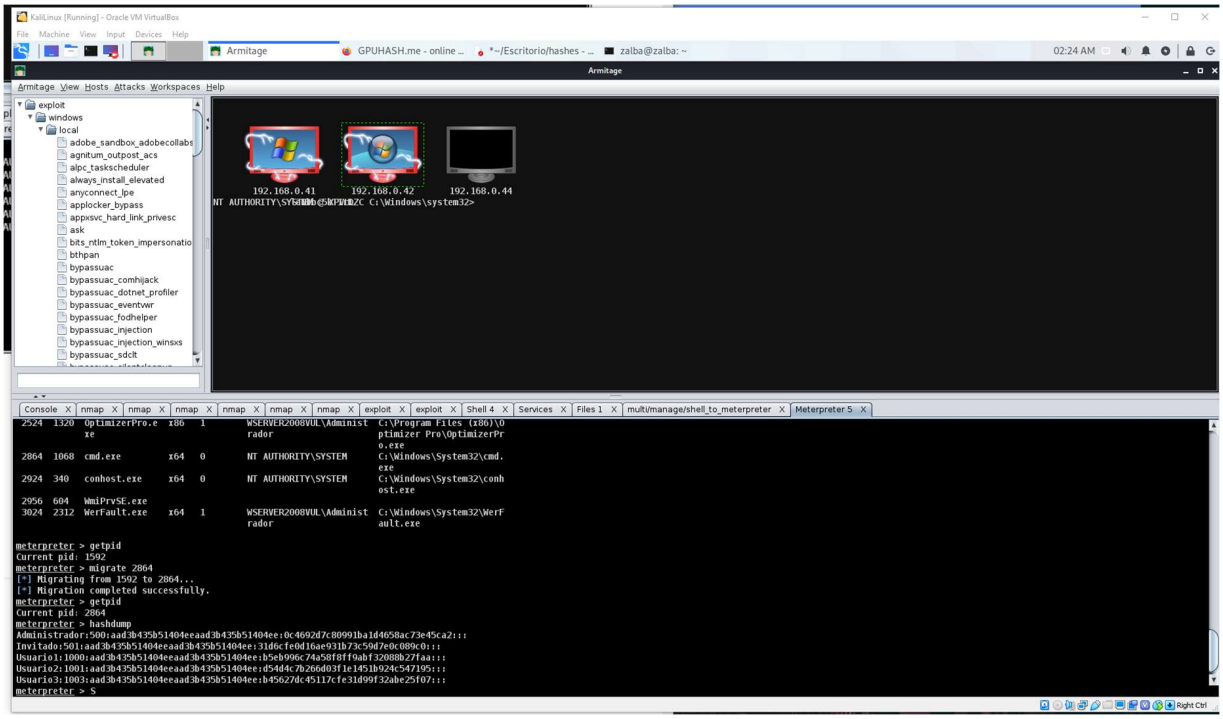
Podemos ejecutar otros scripts como Shell_to_meterpreter, para conseguir una consola meterpreter que es mas interesante.



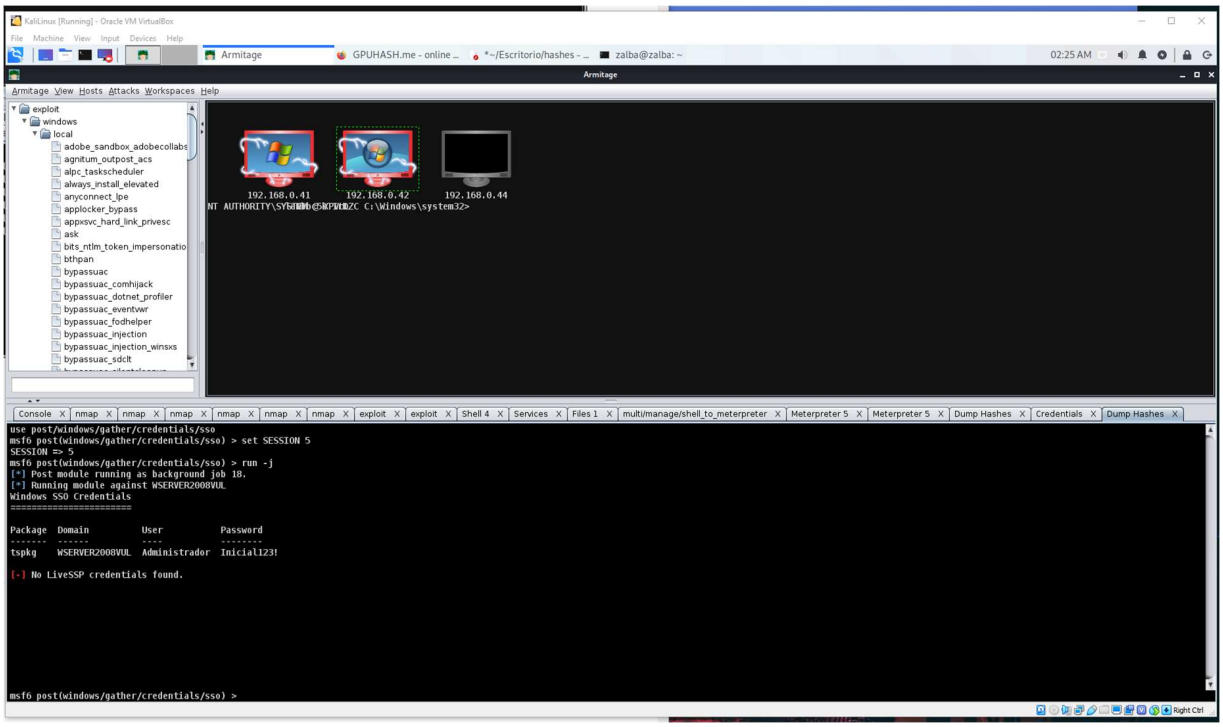
En este caso no tenemos los privilegios suficientes por lo que tendremos que escalar privilegios



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. Después de conseguir privilegios podemos ejecutar hashdump para obtener los hashes de esta segunda maquina.

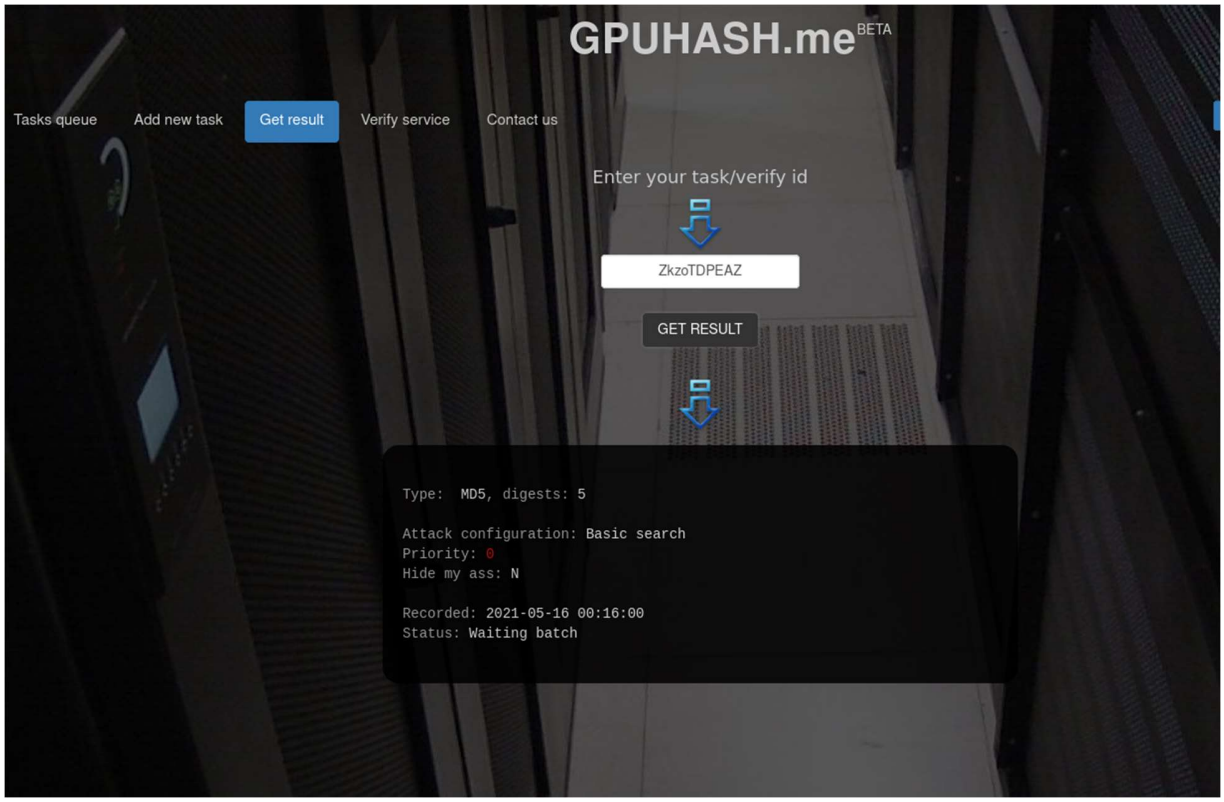


Utilizando una de las opciones de hash dump podemos intentar sacar en claro las propias contraseñás a partir de los hashes. NCon Windows xp no hemos tenido suerte pero con Windows server hemos conseguido las contraseñas Inicial123!

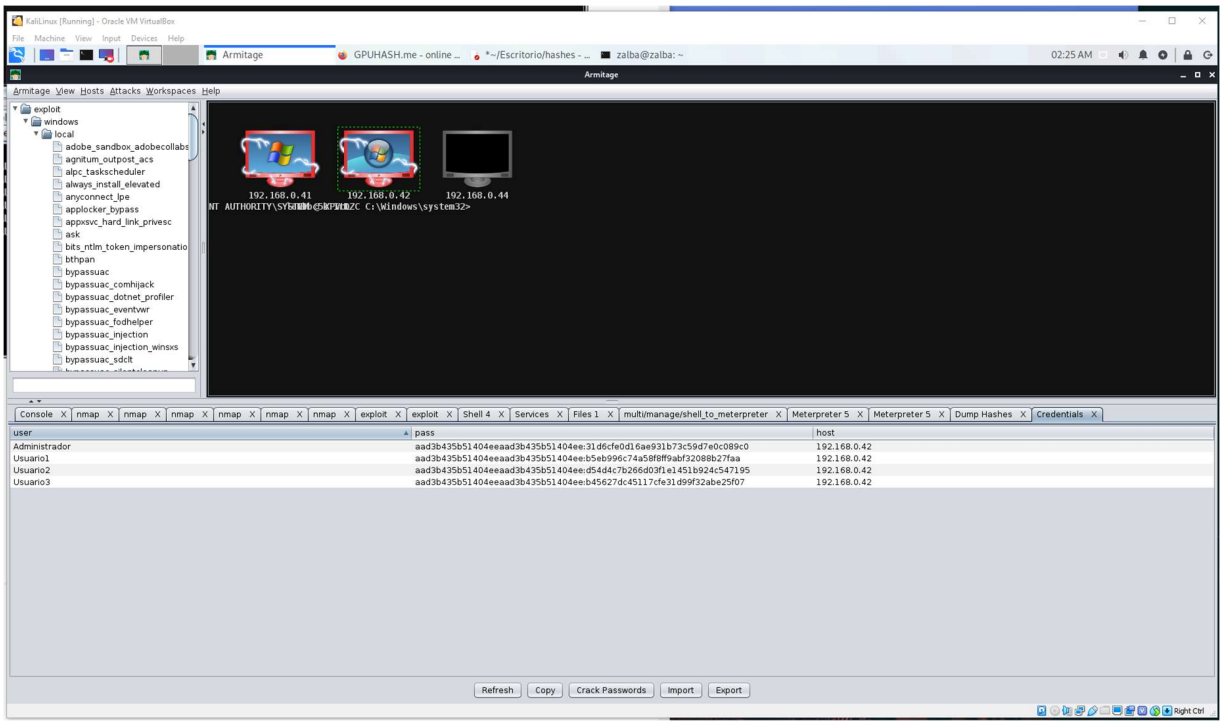


Con los hashes, luego podemos ir a web o librerías como cpuhash.me y especificando el método de encriptación utilizado podríamos sacar las contraseñas.

En mi caso no he conseguido que me lo ejecute.

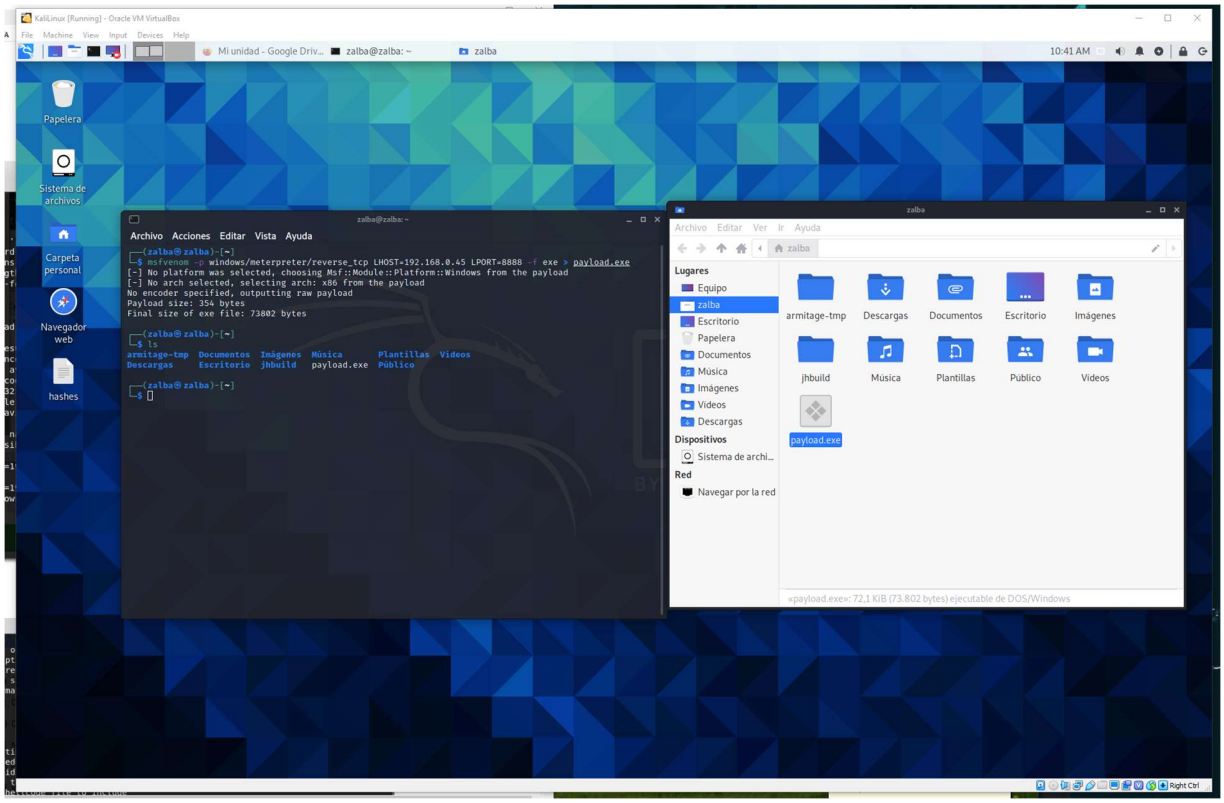


De todas formas, podes ir guardando todos los hashes en armitage para poder probarlos en las otras maquina de la red. Es posible que se hay usado la misma contraseña para los administradores por ejemplo, y obtenida una contraseña podemos acceder a varios dispositivos.

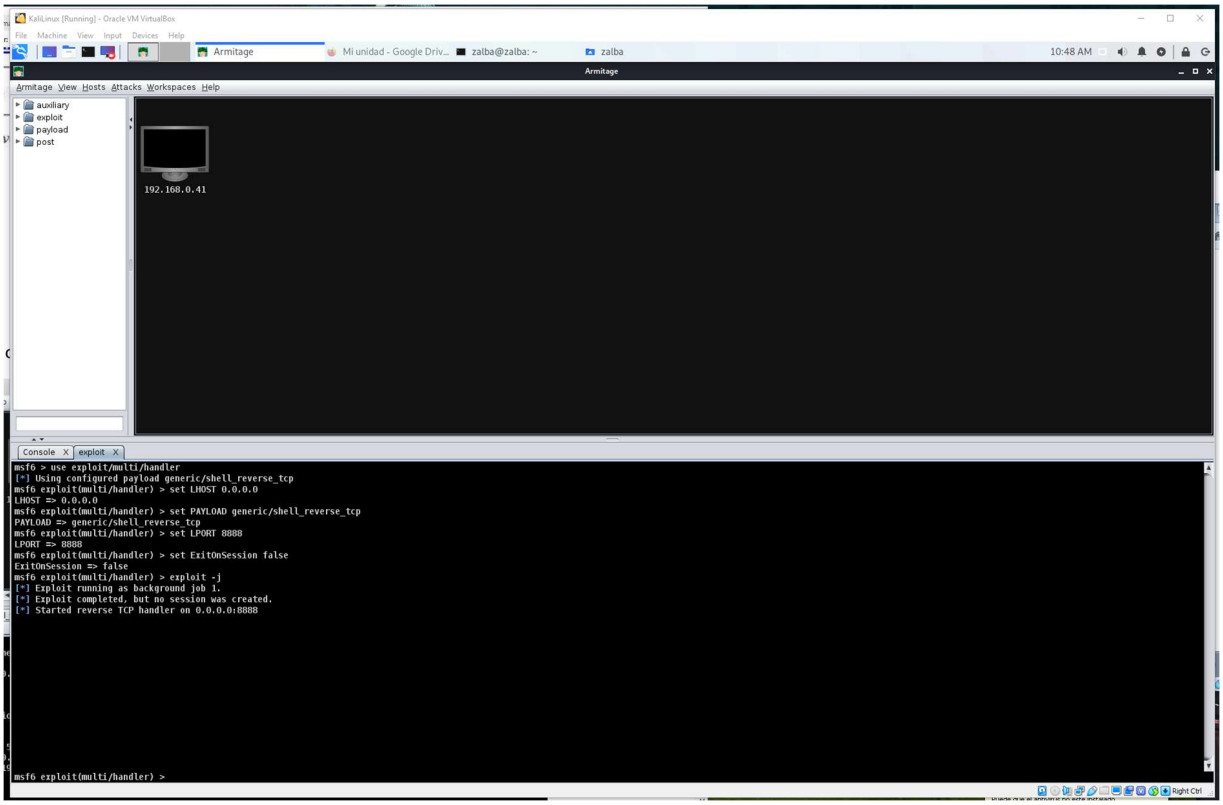


Ahora vamos a crear un payload para vulnerar maquinas manualmente. Se trata de un pequeño programa que se debe ejecutar en la maquina víctima, y abre una puerta trasera donde luego ermitage puede acceder.

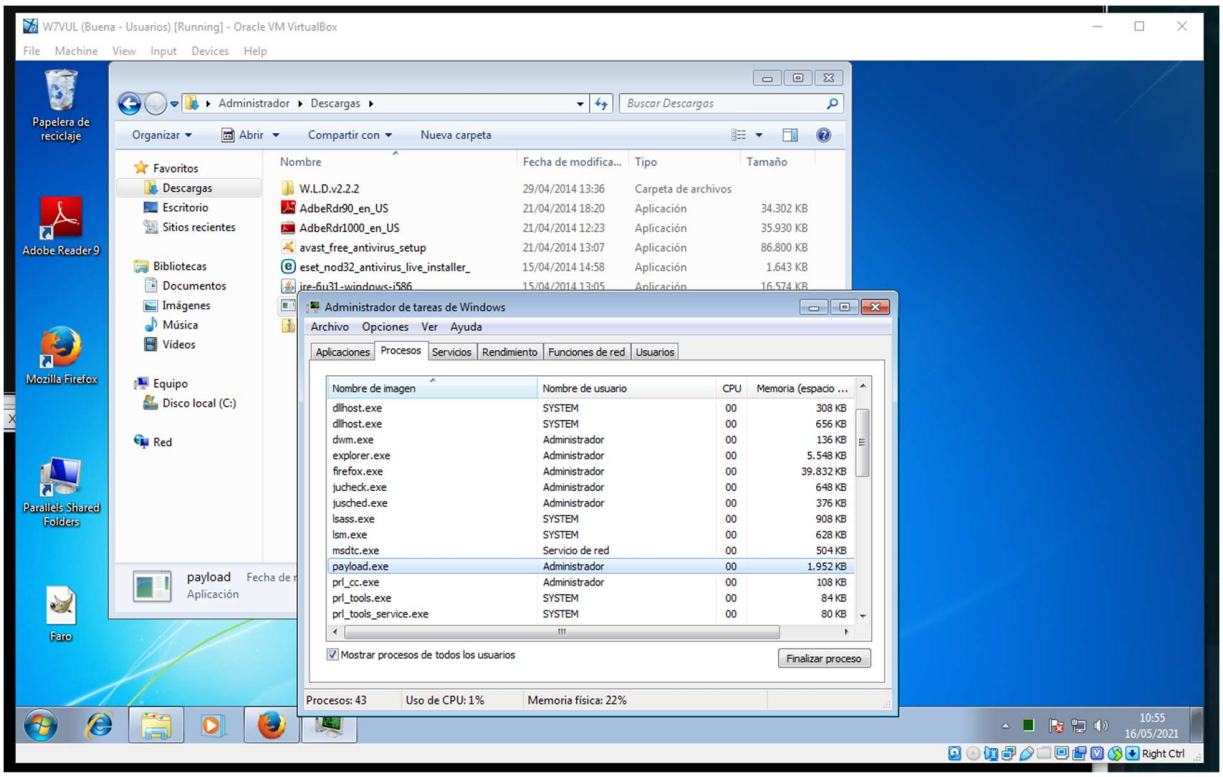
Se genera el payload con el siguiente comando: debemos especificar la ip del host donde queremos acceder y un puerto cualquiera.



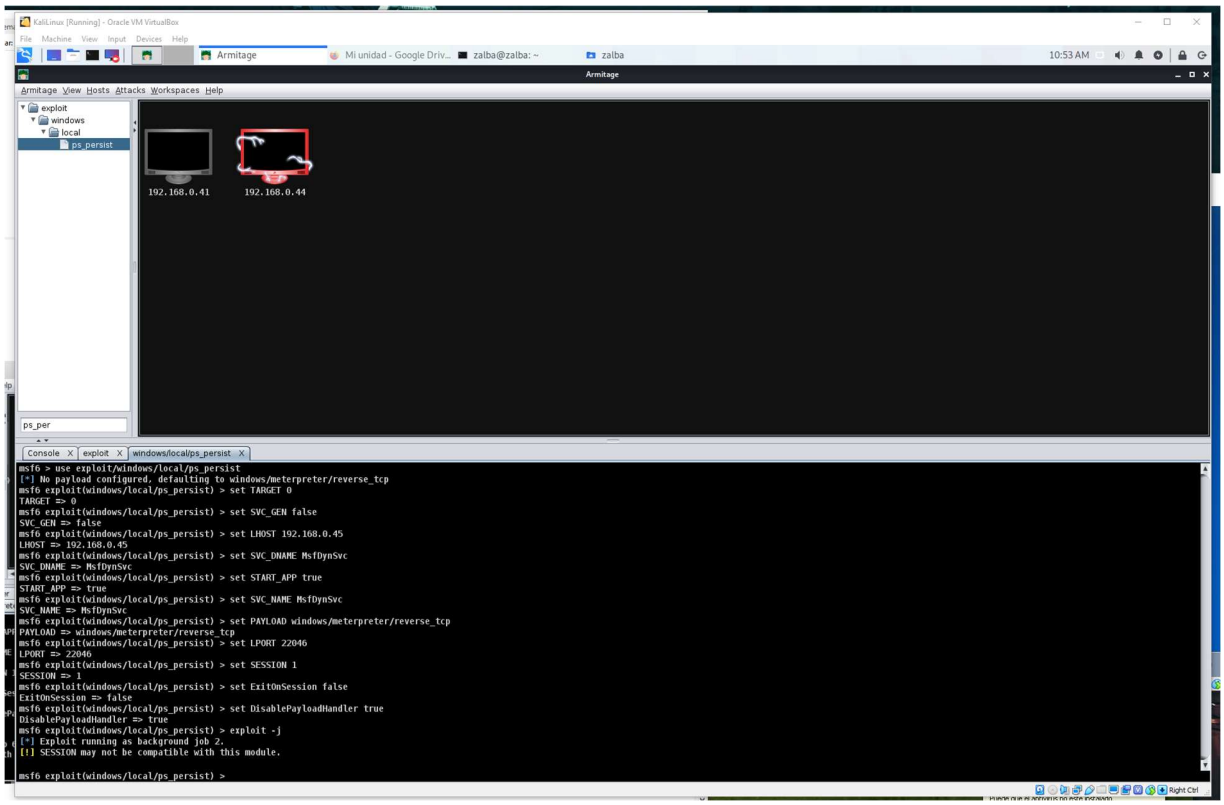
Ahora debemos aplicar un listener en armitage para esperar a que el payload se ejecute en la maquina victima.



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.



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 desapercivido.

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% (RDMK:cmRt...
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