

Universidad Autónoma “Tomas Frías”
Carrera de ingeniería de sistemas

PRACTICA # 5



Nombres: Univ. Gonzalo Espinoza Chiri

Materia: Informática Forense SIS-939

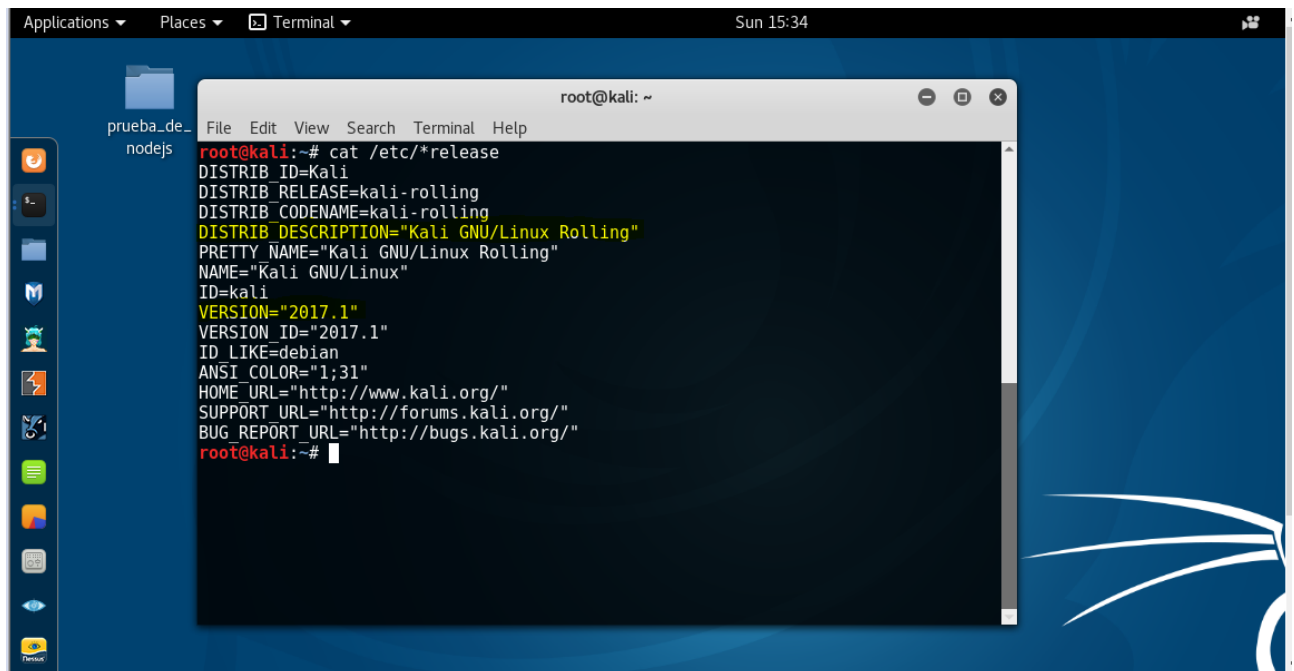
Docente: Ing. Ing. David Sossa L.

Auxiliar: Univ. Heber Zelaya C.

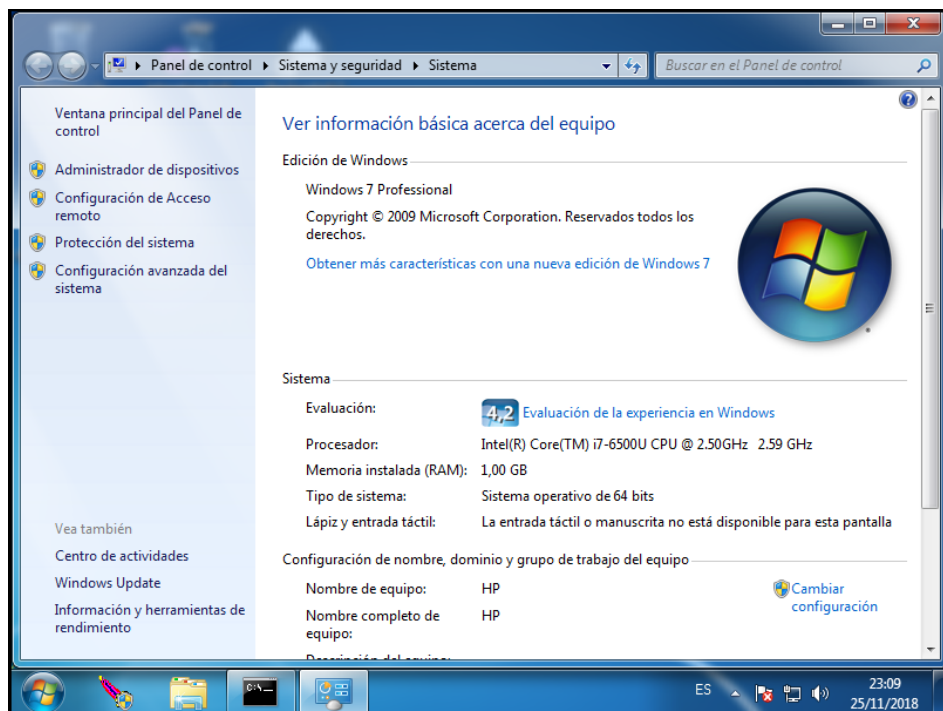
1. Monte una red con equipo virtual en vmware u otro (mínimamente debe estar instalado en la red: un KALI LINUX y un WINDOWS7).

Una vez que ya tengamos los archivos iso de los 2 sistemas operativos (kali Linux y Windows 7), procedemos a instalarlo en Vmware.

- Para ver la versión de kali

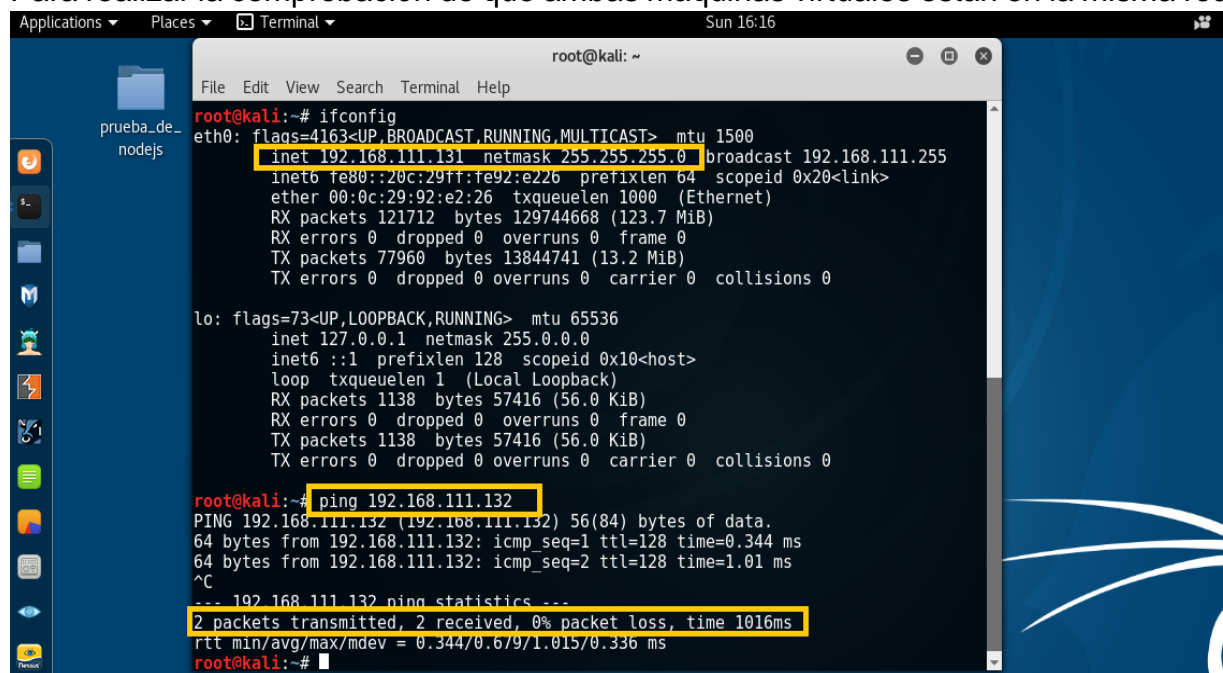


- Para ver la versión de Windows 7



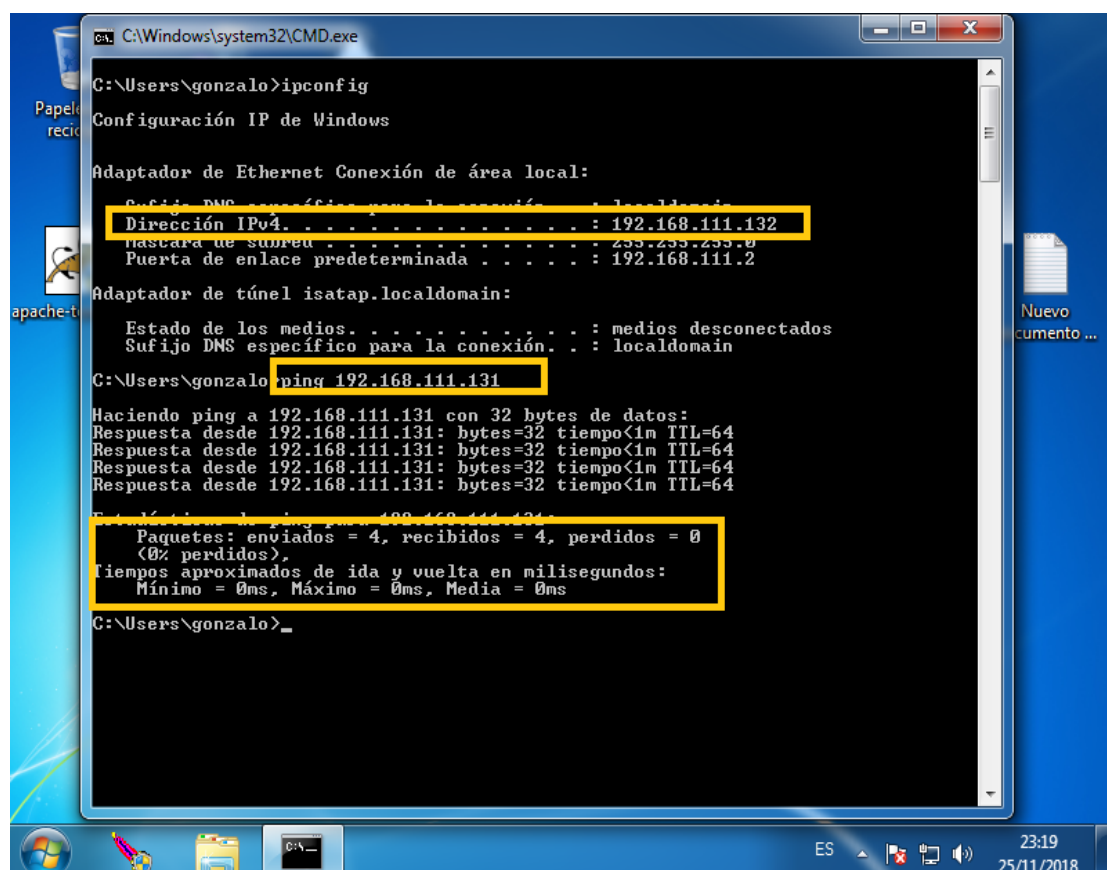
Después de la instalación configuramos ambos adaptadores de red, para que las dos maquina virtuales estén en red.

Para realizar la comprobación de que ambas máquinas virtuales están en la misma red:



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.111.131 netmask 255.255.255.0 broadcast 192.168.111.255  
    inet6 fe80::20c:29ff:fe92:e226 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:92:e2:26 txqueuelen 1000 (Ethernet)  
    RX packets 121712 bytes 129744668 (123.7 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 77960 bytes 13844741 (13.2 MiB)  
    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 1 (Local Loopback)  
    RX packets 1138 bytes 57416 (56.0 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 1138 bytes 57416 (56.0 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
root@kali:~# ping 192.168.111.132  
PING 192.168.111.132 (192.168.111.132) 56(84) bytes of data:  
64 bytes from 192.168.111.132: icmp_seq=1 ttl=128 time=0.344 ms  
64 bytes from 192.168.111.132: icmp_seq=2 ttl=128 time=1.01 ms  
^C  
--- 192.168.111.132 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1016ms  
rtt min/avg/max/mdev = 0.344/0.679/1.015/0.336 ms  
root@kali:~#
```

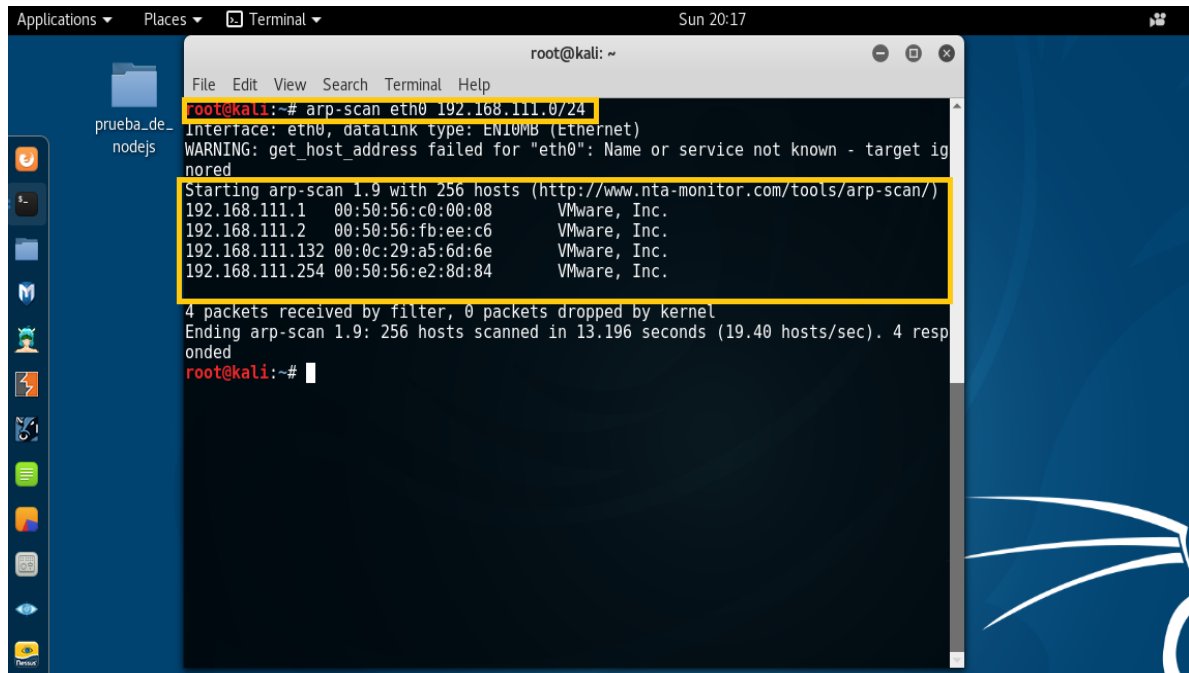
Comprobación en Windows 7, hacia la máquina virtual de kali linux



```
C:\Windows\system32\CMD.exe  
C:\Users\gonzalo>ipconfig  
Configuración IP de Windows  
  
Adaptador de Ethernet Conexión de área local:  
    Sufixo DNS específico para la conexión . . . : localdomain  
    Dirección IPv4. . . . . : 192.168.111.132  
    Máscara de subred . . . . . : 255.255.255.0  
    Puerta de enlace predeterminada . . . . . : 192.168.111.2  
  
Adaptador de túnel isatap.localdomain:  
    Estado de los medios. . . . . : medios desconectados  
    Sufijo DNS específico para la conexión. . . : localdomain  
  
C:\Users\gonzalo>ping 192.168.111.131  
  
Haciendo ping a 192.168.111.131 con 32 bytes de datos:  
Respuesta desde 192.168.111.131: bytes=32 tiempo<1m TTL=64  
Respuesta desde 192.168.111.131: bytes=32 tiempo<1m TTL=64  
Respuesta desde 192.168.111.131: bytes=32 tiempo<1m TTL=64  
Respuesta desde 192.168.111.131: bytes=32 tiempo<1m TTL=64  
Estadísticas de ping para 192.168.111.131:  
Paquetes: enviados = 4, recibidos = 4, perdidos = 0  
    (0% perdidos),  
Tiempos aproximados de ida y vuelta en milisegundos:  
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms  
  
C:\Users\gonzalo>
```

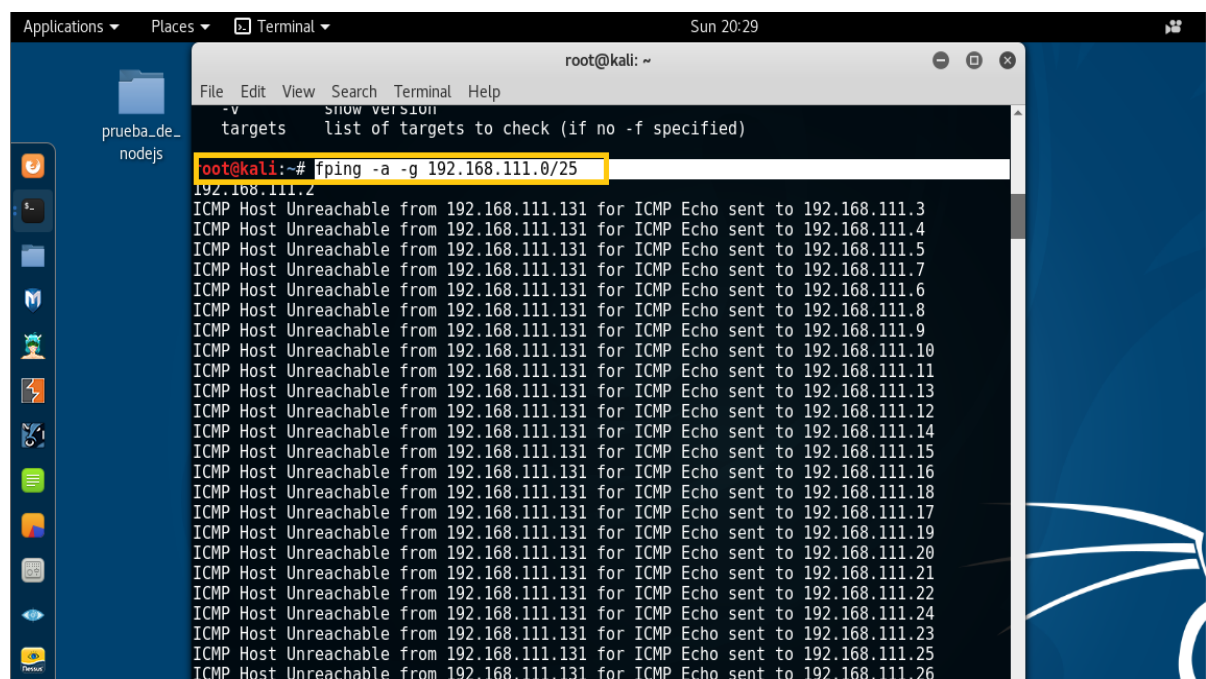
2. Con el KALI LINUX haga una exploración de la red interna (escaneo ARP, escaneo ICMP, escaneo SMB, escaneo TCP)

2.1. Escaneo ARP.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# arp-scan eth0 192.168.111.0/24  
Interface: eth0, dataLink type: ENIUMB (Ethernet)  
WARNING: get_host_address failed for "eth0": Name or service not known - target ignored  
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)  
192.168.111.1 00:50:56:c0:00:08 VMware, Inc.  
192.168.111.2 00:50:56:fb:ee:c6 VMware, Inc.  
192.168.111.132 00:0c:29:a5:6d:6e VMware, Inc.  
192.168.111.254 00:50:56:e2:8d:84 VMware, Inc.  
4 packets received by filter, 0 packets dropped by kernel  
Ending arp-scan 1.9: 256 hosts scanned in 13.196 seconds (19.40 hosts/sec). 4 responded  
root@kali:~#
```

2.2. escaneo ICMP.



```
root@kali: ~  
File Edit View Search Terminal Help  
-v show version  
targets list of targets to check (if no -f specified)  
root@kali:~# fping -a -g 192.168.111.0/25  
192.168.111.2  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.3  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.4  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.5  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.7  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.6  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.8  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.9  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.10  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.11  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.13  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.12  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.14  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.15  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.16  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.18  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.17  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.19  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.20  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.21  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.22  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.24  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.23  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.25  
ICMP Host Unreachable from 192.168.111.131 for ICMP Echo sent to 192.168.111.26
```

2.3. Escaneo SMB.

```
Applications ▾ Places ▾ Terminal ▾ Sun 20:33
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nbtscan 192.168.111.0/24
Doing NBT name scan for addresses from 192.168.111.0/24

IP address      NetBIOS Name    Server    User      MAC address
-----
192.168.111.0    Sendto failed:  Permission denied
192.168.111.1    DESKTOP-3R09M2U <server>  <unknown> 00:50:56:c0:00:08
192.168.111.132  HP              <server>  <unknown> 00:0c:29:a5:6d:6e
192.168.111.255 Sendto failed:  Permission denied
root@kali:~#
```

2.4. escaneo TCP.

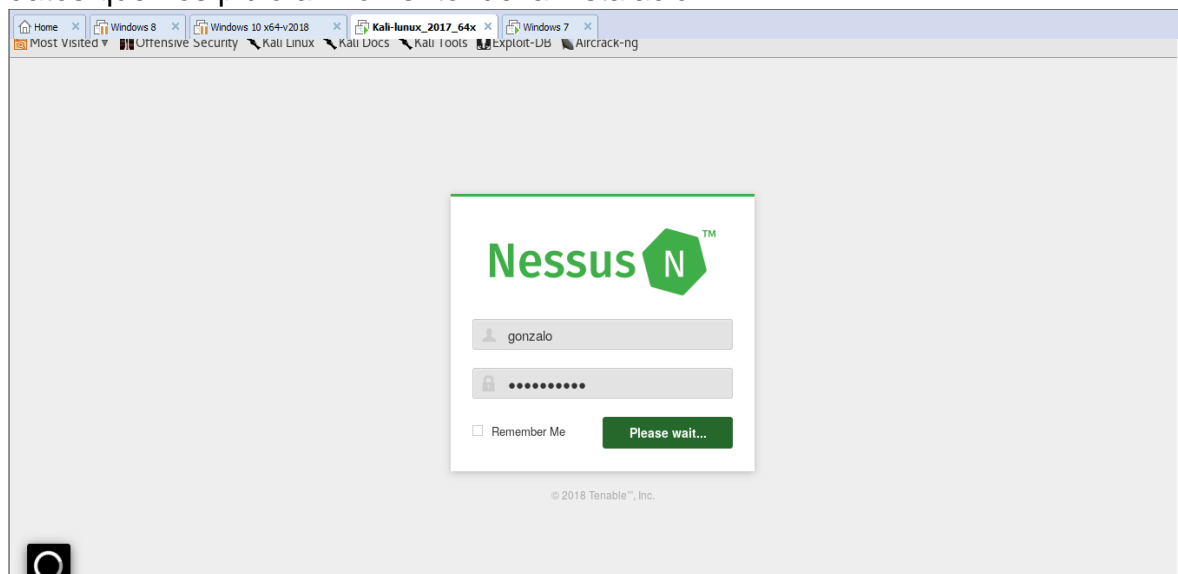
```
File Edit View Search Terminal Help
root@kali:~# masscan -p 22,23,80,443 192.168.111.0/24
Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2018-11-26 02:35:45 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 256 hosts [4 ports/host]
root@kali:~# masscan -p 22 192.168.111.0/24
Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2018-11-26 02:36:32 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 256 hosts [1 port/host]
root@kali:~# masscan -p 23 192.168.111.0/24
Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2018-11-26 02:38:44 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 256 hosts [1 port/host]
root@kali:~# masscan -p 80 192.168.111.0/24
Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2018-11-26 02:39:14 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 256 hosts [1 port/host]
root@kali:~# masscan -p 443 192.168.111.0/24
Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2018-11-26 02:40:47 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 256 hosts [1 port/host]
```

3. Con el programa **NESSUS** (desde kali linux) haga un escaneo de las vulnerabilidades de la máquina virtual con instalación **WINDOWS 7**

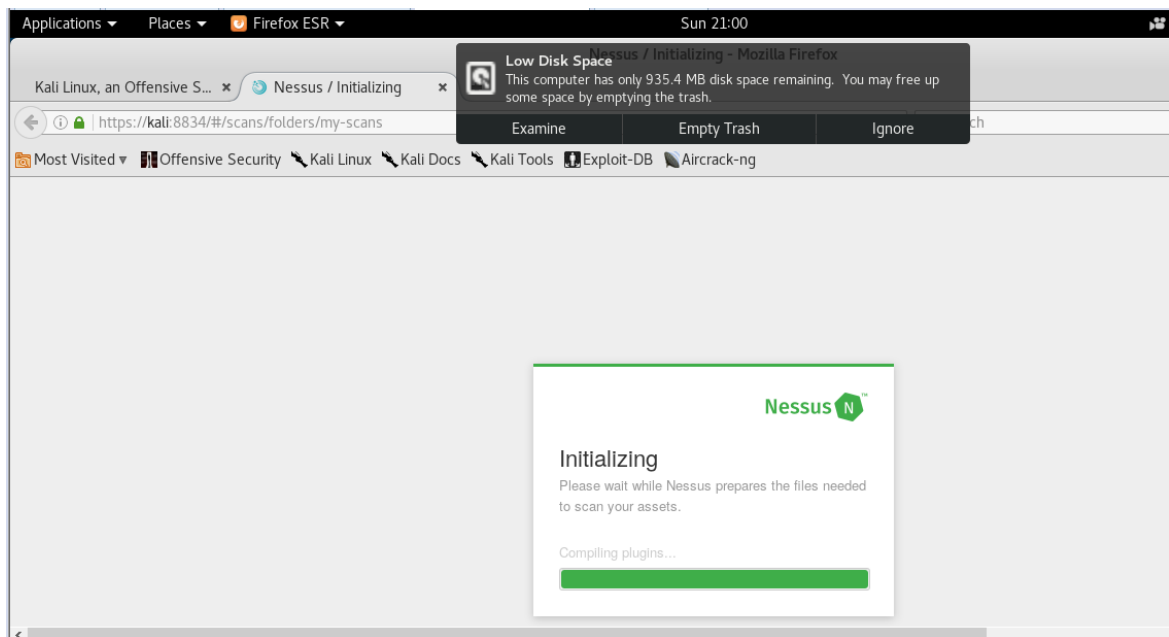
- una vez que terminamos la instalación de nessus, buscamos nessus y lo iniciamos



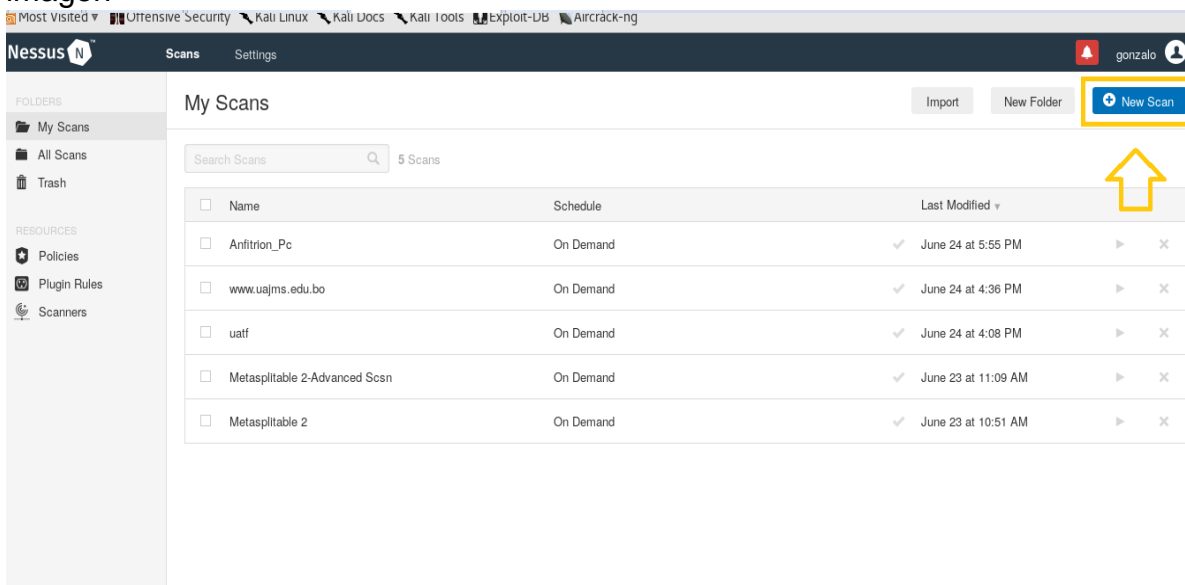
- Despues de iniciar Nessus, abrimos el navegador que tengamos instalado, una ves que estemos en el navegado nos aparecerá la ventana de login, colocamos los datos que nos pidió al momento de la instalación.



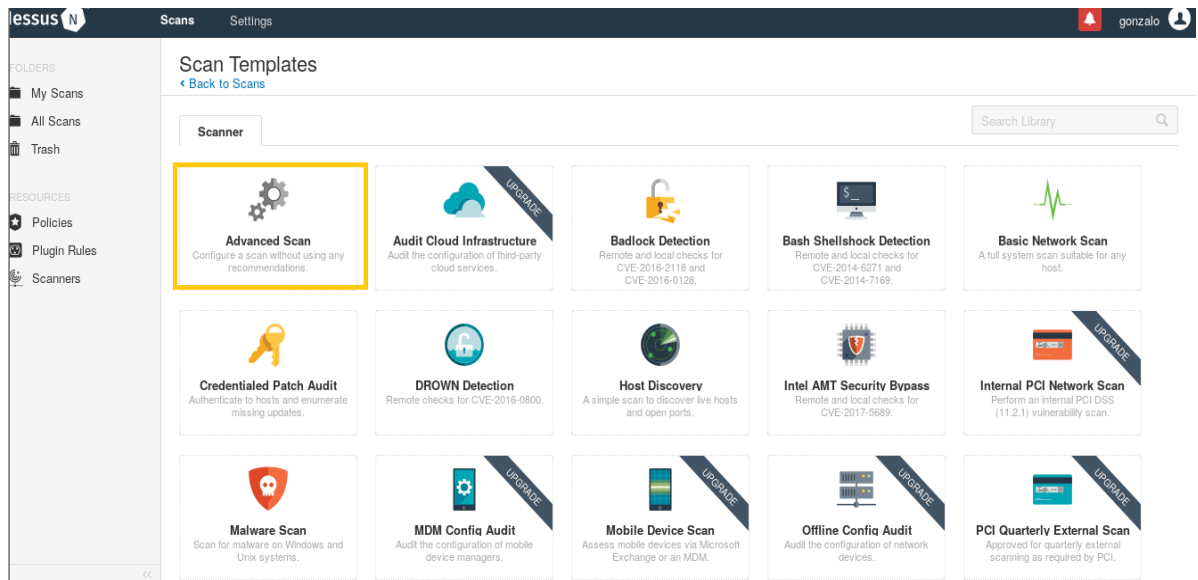
- la inicialización tardara unos montos.



- una vez que termine de inicializar, nos aparecerá una ventana en donde nos da la información de los escaneos que anteriormente realizamos. Para crear un nuevo escaneo debemos hacer clic el botón que dice **"New Scan"** como se muestra en la imagen

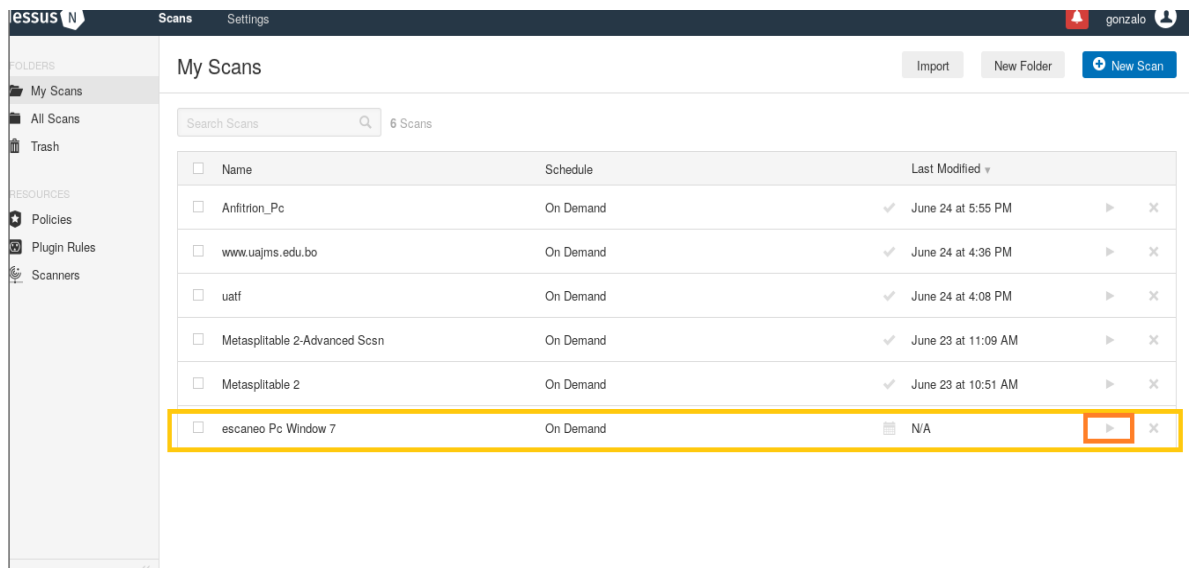


- Nos aparecerá la siguiente en la que seleccionamos la opción que dice **"Advanced Scan"** como se muestra.

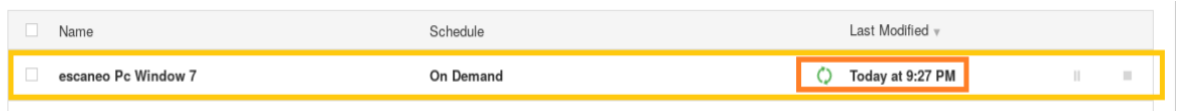


- Completamos el siguiente formulario, y guardamos los datos.

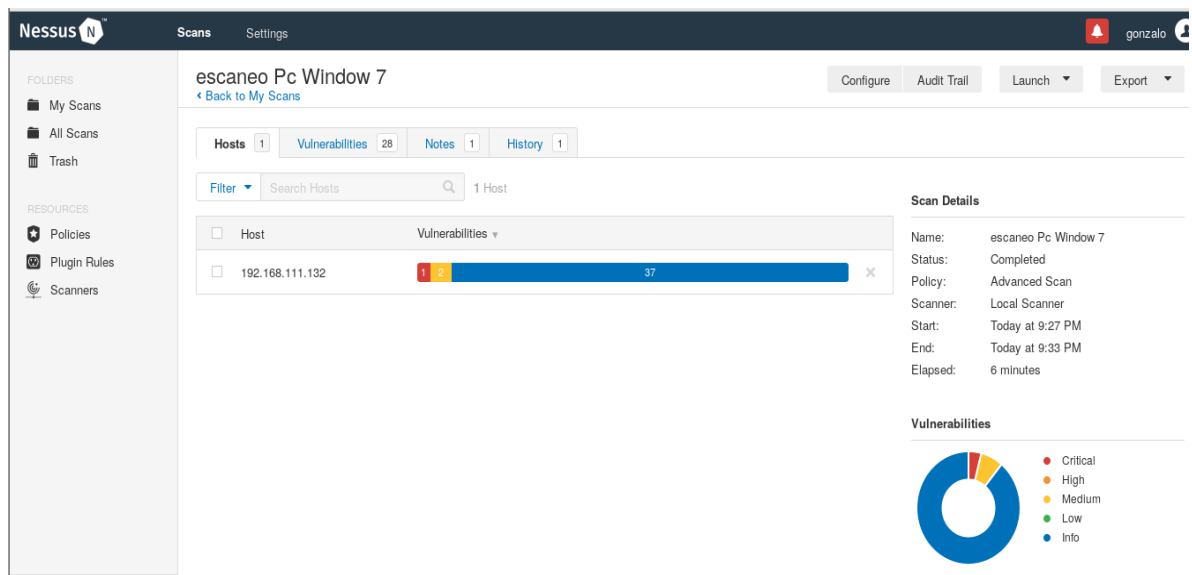
- Una vez que guardamos la configuración básica, presionamos la opción de iniciar, que se muestra en el pequeño recuadro de color naranja.



- Una vez iniciado nos mostrara un dialogo de iniciación como se muestra en la imagen.



- Una vez que concluya el análisis Nessus nos muestra los resultados, de la siguiente manera.



- Si haces clic sobre las vulnerabilidades encontradas, nos mostrara mas detalles de cada vulnerabilidades.

essus

Scans

Settings

gonzalo

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Scanners

escaneo Pc Window 7

Configure

Audit Trail

Launch

Export

Hosts 1

Vulnerabilities 28

Notes 1

History 1

Filter

Search Vulnerabilities

28 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	MS17-010: Security Update for Microsoft Windows SM...	Windows	1
MEDIUM	MS16-047: Security Update for SAM and LSAD Remot...	Windows	1
MEDIUM	SMB Signing not required	Misc.	1
INFO	DCE Services Enumeration	Windows	8
INFO	Nessus SYN scanner	Port scanners	5
INFO	Microsoft Windows SMB Service Detection	Windows	2
INFO	Additional DNS Hostnames	General	1
INFO	Common Platform Enumeration (CPE)	General	1

Scan Details

Name: escaneo Pc Window 7

Status: Completed

Policy: Advanced Scan

Scanner: Local Scanner

Start: Today at 9:27 PM

End: Today at 9:33 PM

Elapsed: 6 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

- Para ver concretamente el nombre de la clasificación de la vulnerabilidad en concreto.

essus

Scans

Settings

gonzalo

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Scanners

escaneo Pc Window 7 / Plugin #97833

Configure

Audit Trail

Launch

Export

Hosts 1

Vulnerabilities 28

Notes 1

History 1

CRITICAL

MS17-010: Security Update for Microsoft Windows SMB Server (40133...

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)
- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

Solution

Plugin Details

Severity: Critical

ID: 97833

Version: 1.16

Type: remote

Family: Windows

Published: March 20, 2017

Modified: May 21, 2018

Risk Information

Risk Factor: Critical

CVSS Base Score: 10.0

CVSS Temporal Score: 9.5

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Vector: CVSS2#E:F/RL:U/RC:ND