

Escaneo de vulnerabilidades


KALI LINUX – NESSUS

Christian Ferdinand Mora Ramirez



Introducción

Este informe presenta el uso de Kali Linux junto con la herramienta Nessus para llevar a cabo un análisis avanzado de una máquina objetivo. A través de un escaneo detallado de puertos y la recolección de información sensible, se identifican posibles vulnerabilidades y datos comprometedores en una máquina evaluada.



Para iniciar el análisis de vulnerabilidades ejecutamos nuestro entorno de trabajo en este caso “Virtual Box” y encendemos nuestra máquina virtual “Kali Linux”.

Una vez iniciado el entorno de trabajo, accedemos al directorio donde previamente descargamos la herramienta Nessus desde su sitio web oficial e instalamos utilizando los comandos correspondientes. Tras completar la instalación, iniciaremos el servidor de Nessus con el comando “sudo systemctl start nessusd” Para verificar el estado del servidor podemos ejecutar “sudo systemctl status nessusd”

```
(kali@kali)-[~/Downloads]
└─$ sudo systemctl start nessusd
[sudo] password for kali:

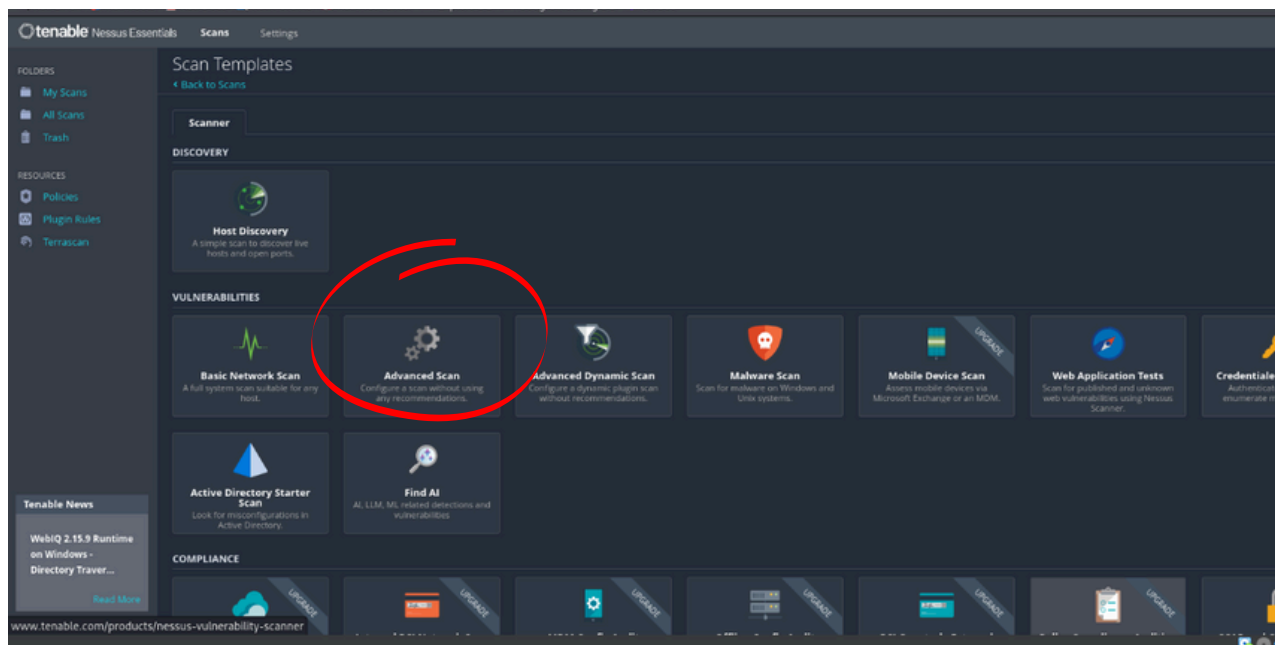
(kali@kali)-[~/Downloads]
└─$ sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)
   Active: active (running) since Mon 2024-10-07 21:09:34 EDT; 19s ago
     Invocation: f08ae9f711d542a7b24521ad0601d78c
    Main PID: 8130 (nessus-service)
      Tasks: 17 (limit: 2272)
     Memory: 609M (peak: 609M)
        CPU: 23.455s
    CGroup: /system.slice/nessusd.service
            └─8130 /opt/nessus/sbin/nessus-service -q
              └─8132 nessusd -q
```

Una vez confirmado que el servidor está funcionando correctamente, abrimos nuestro navegador preferido y accedemos a "https://localhost:8834" ya que el servicio de Nessus se ejecuta en el puerto 8834. Esta dirección nos llevará directamente a la interfaz de Nessus. Al ingresar, será necesario autenticarse con un usuario y contraseña, y realizar la configuración inicial de la herramienta.



Tras completar este proceso, podremos explorar los diferentes directorios y comenzar los escaneos de vulnerabilidades en la máquina objetivo.

Al acceder a la herramienta, podremos navegar por los diferentes apartados que ofrece. Para iniciar un nuevo escaneo, dirigimos el cursor a la opción 'New Scan'. Al seleccionarla, se desplegarán varias opciones; en nuestro caso, elegiremos la opción de escaneo avanzado.



Para este momento, debemos encender la máquina objetivo, que en este caso será Metasploitable y conseguir la IP de dicha máquina objetivo por medio del comando "ifconfig".

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:96:15:a6
          inet addr:192.168.3.113  Bcast:192.168.3.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe96:15a6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:26 errors:0 dropped:0 overruns:0 frame:0
          TX packets:55 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3078 (3.0 KB)  TX bytes:5850 (5.7 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)
msfadmin@metasploitable:~$
```

Una vez dentro de escáner avanzado proporcionaremos la IP de nuestra maquina objetivo así como la asignación de un nombre y una descripción breve, al finalizar moveremos el cursos a “Save” para guardar los datos.

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Name: Analysis-Prueba-2

Description: Analysis avanzado

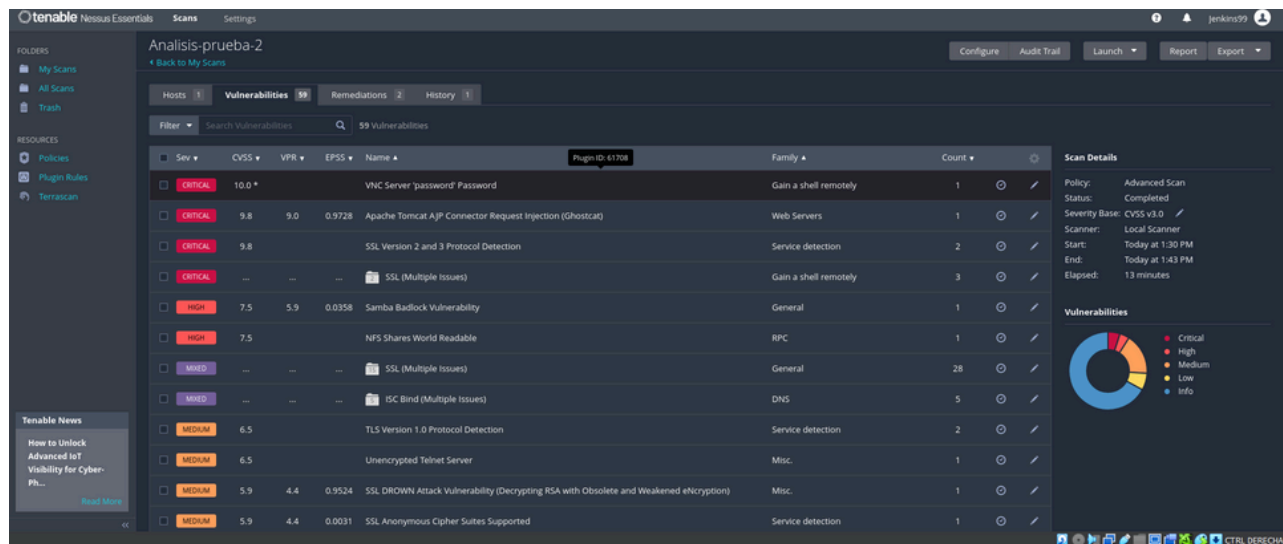
Folder: My Scans

Targets: 192.168.3.113

Upload Targets Add File

Save Cancel

En este punto solo queda ejecutar el escaneo y esperar a que finalice la detección de vulnerabilidades en la máquina objetivo, lo cual podría tomar algunos minutos. Al concluir accederemos con el nombre que le asignamos donde se listarán todas las vulnerabilidades encontradas que van desde vulnerabilidades críticas a bajas, así como información sensible.



The screenshot displays the Tenable Nessus Essentials interface. The main section shows a scan titled "Analisis-prueba-2" with 59 vulnerabilities. The interface includes a sidebar with navigation options like "My Scans", "All Scans", and "Trash". The main table lists vulnerabilities with columns for Severity, CVSS, VPR, EPSS, Name, Family, and Count. The right sidebar provides "Scan Details" including Policy, Status, Severity Base, Scanner, Start/End times, and Elapsed time. A "Vulnerabilities" pie chart is also present.

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0	-	-	VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8	9.0	0.9728	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	9.8	-	-	SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	-	-	-	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5	5.9	0.0358	Samba Badlock Vulnerability	General	1
HIGH	7.5	-	-	NFS Shares World Readable	RPC	1
MIXED	-	-	-	SSL (Multiple Issues)	General	28
MIXED	-	-	-	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5	-	-	TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	6.5	-	-	Unencrypted Telnet Server	Misc.	1
MEDIUM	5.9	4.4	0.9524	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened ebcryption)	Misc.	1
MEDIUM	5.9	4.4	0.0031	SSL Anonymous Cipher Suites Supported	Service detection	1



Conclusión

En conclusión, el uso combinado de Kali Linux y Nessus ha demostrado ser una estrategia eficaz para realizar análisis avanzados de seguridad en una máquina objetivo. Mediante el escaneo exhaustivo de puertos y la recolección de información sensible se logró identificar vulnerabilidades críticas y posibles puntos de compromiso. Este tipo de evaluación es fundamental para fortalecer la seguridad de los sistemas, anticiparse a amenazas potenciales y tomar medidas proactivas para mitigar riesgos.

