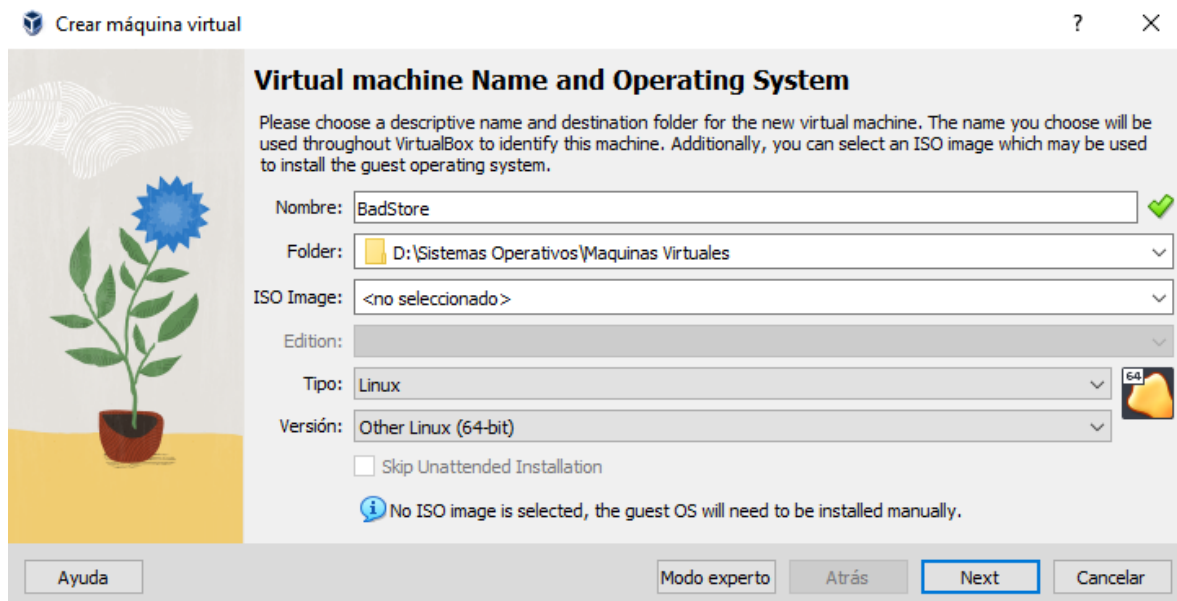


BADSTORE

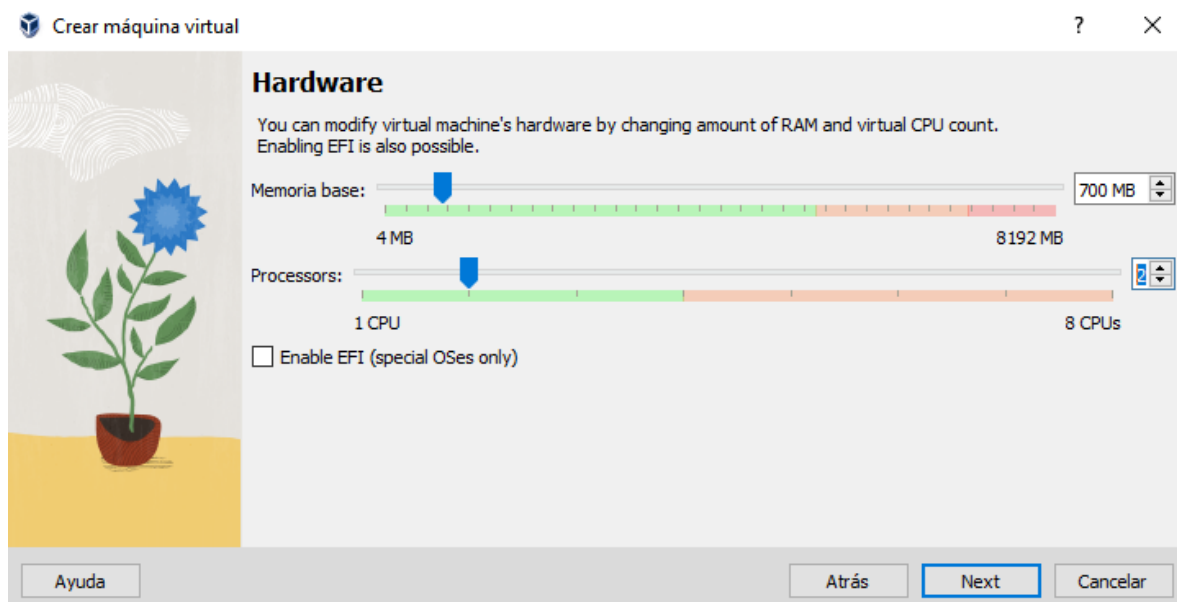
A. Descripción del proceso desarrollado para la instalación y el escaneo de BadStore

Para poder escanear las vulnerabilidades de BadStore con Nessus, el primer paso es instalar una máquina virtual, usando la imagen de BadStore.

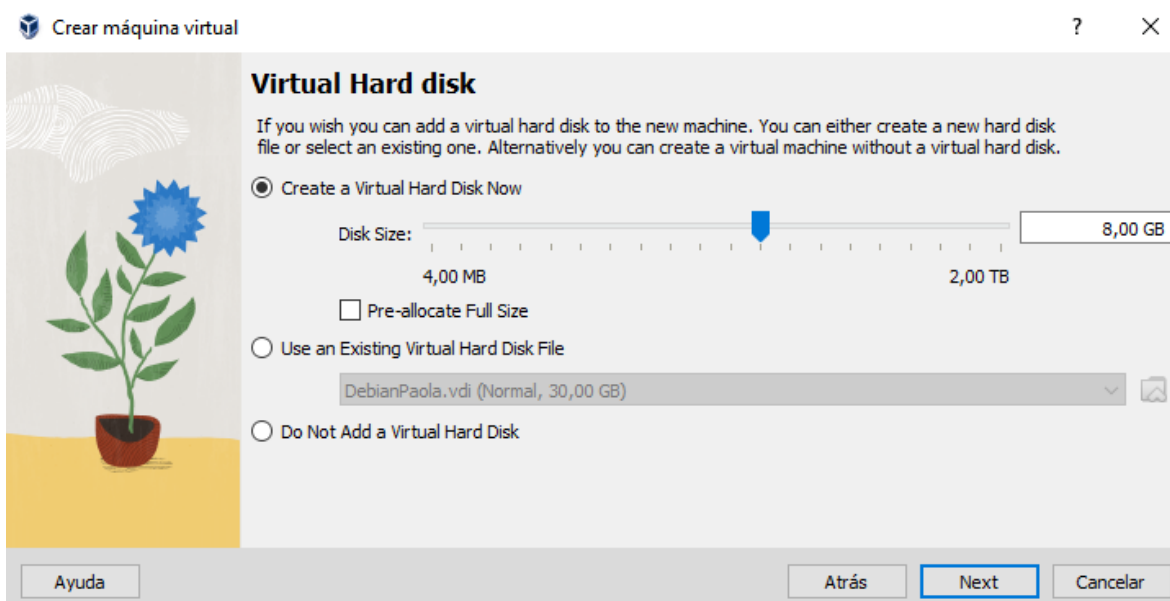
Por lo que primero se crea una nueva máquina virtual con el nombre de BadStore de tipo Linux



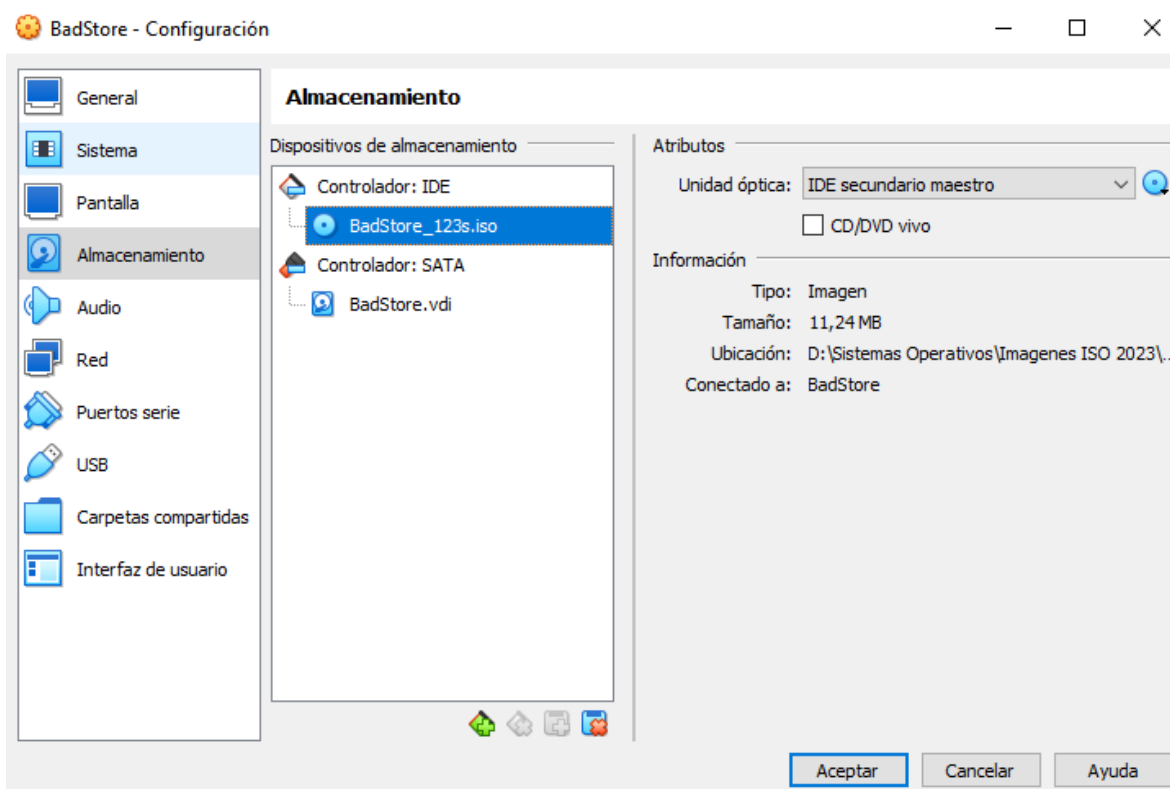
Luego se deja la memoria base con el valor predeterminado y se aumentan los procesadores



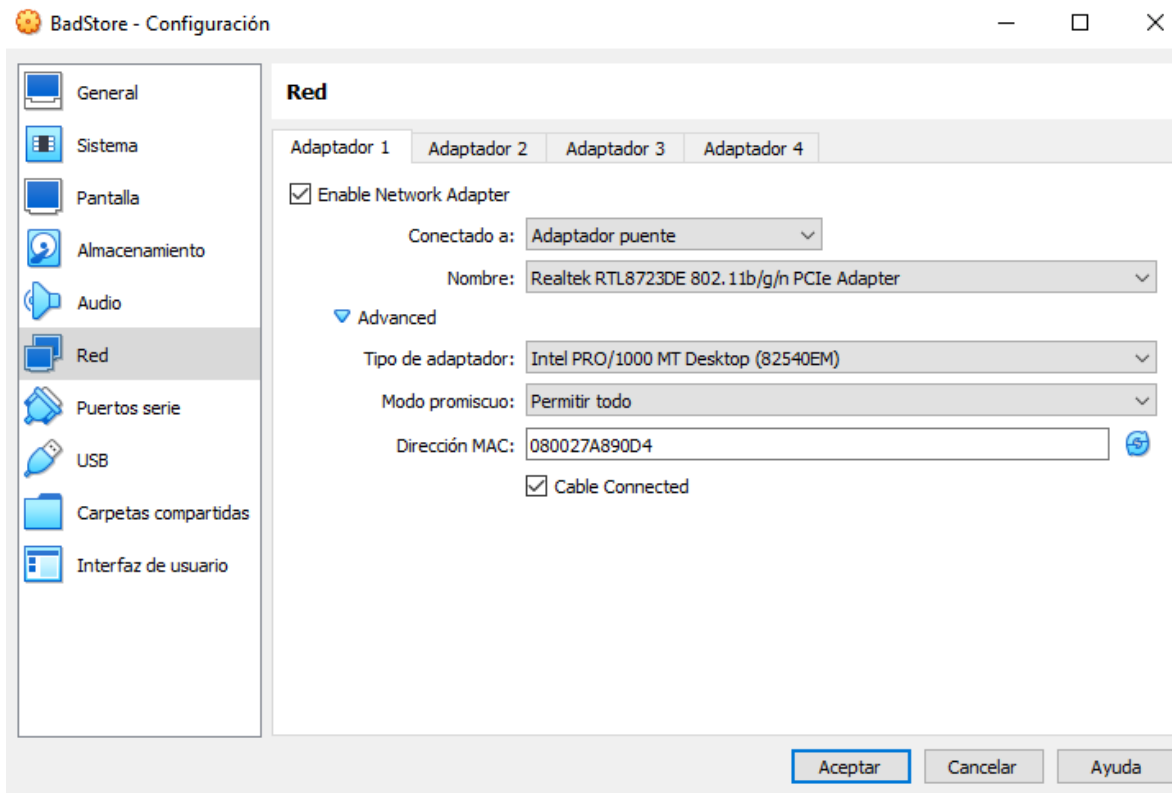
Se deja una memoria de disco de 8 gigas y se continua con el proceso



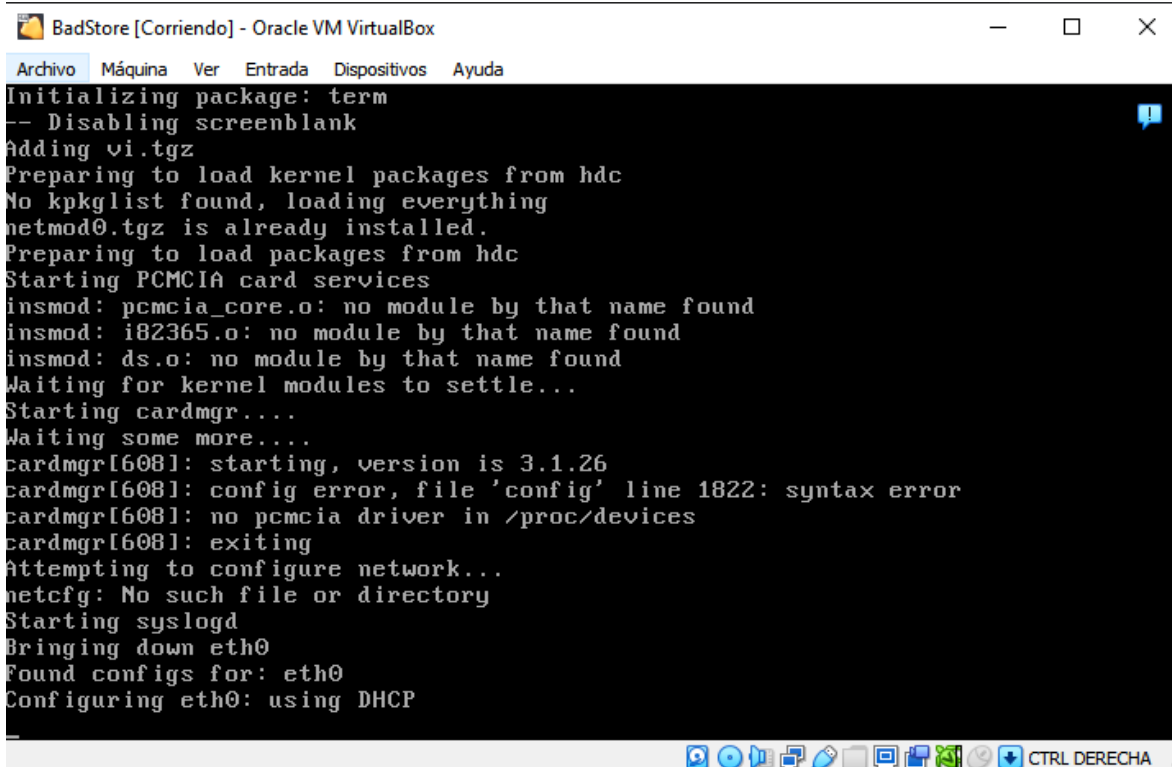
Después de realizar los anteriores pasos, vamos a las configuraciones de la maquina virtual y agregamos la ISO de BadStore en la opción de almacenamiento



En las configuraciones de red seleccionamos la opción de conexión al **Adaptador puente** y en el modo promiscuo a **Permitir todo**, con el propósito de que nos coja la red de wifi

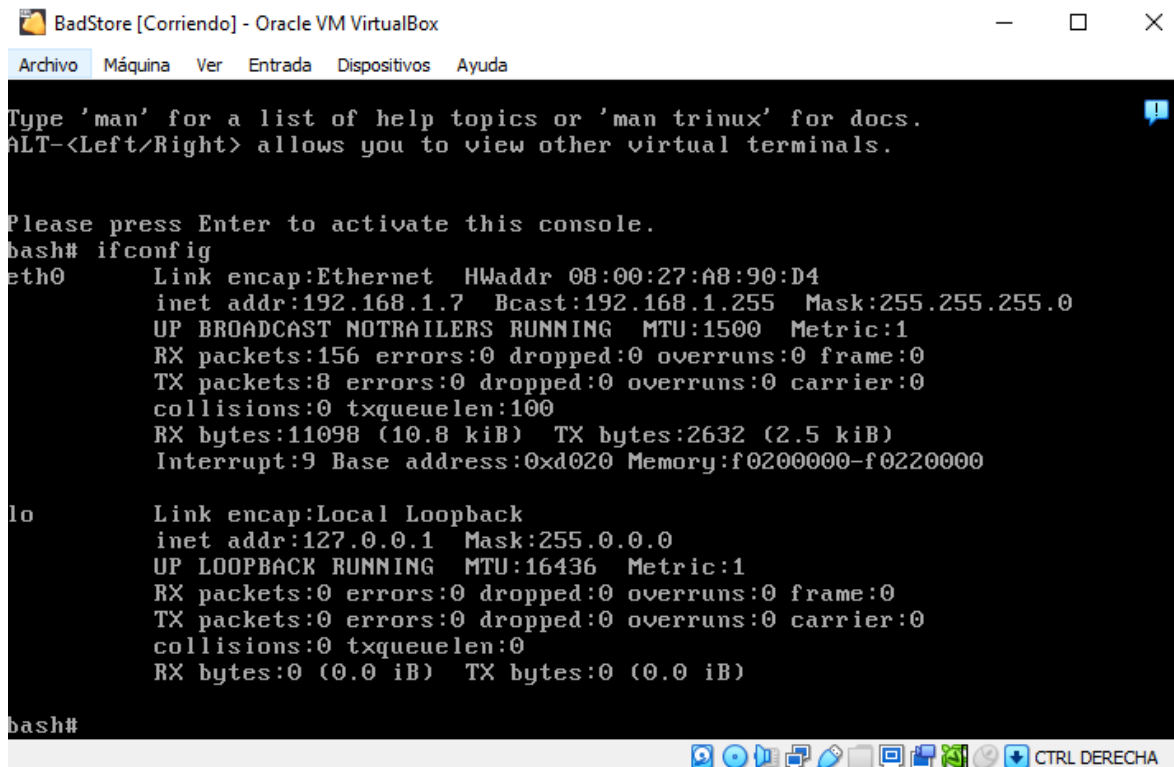


Comenzamos a inicializar la máquina virtual y esperamos un tiempo para que arranque



Para comprobar que está funcionando tenemos que investigar la dirección IP en donde está el BadStore, por lo que escribimos el comando **ifconfig** para mostrar la información detallada sobre las interfaces de red.

Cómo podemos observar en la siguiente imagen la IP donde esta es **192.168.1.7**



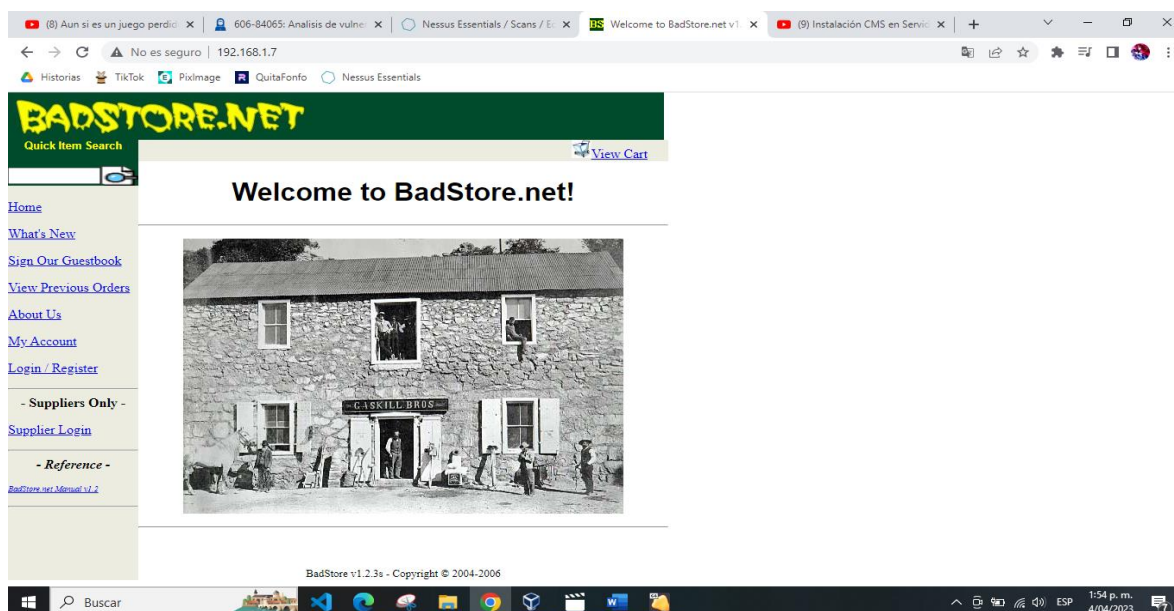
```
Type 'man' for a list of help topics or 'man trinux' for docs.
ALT-Left/Right allows you to view other virtual terminals.

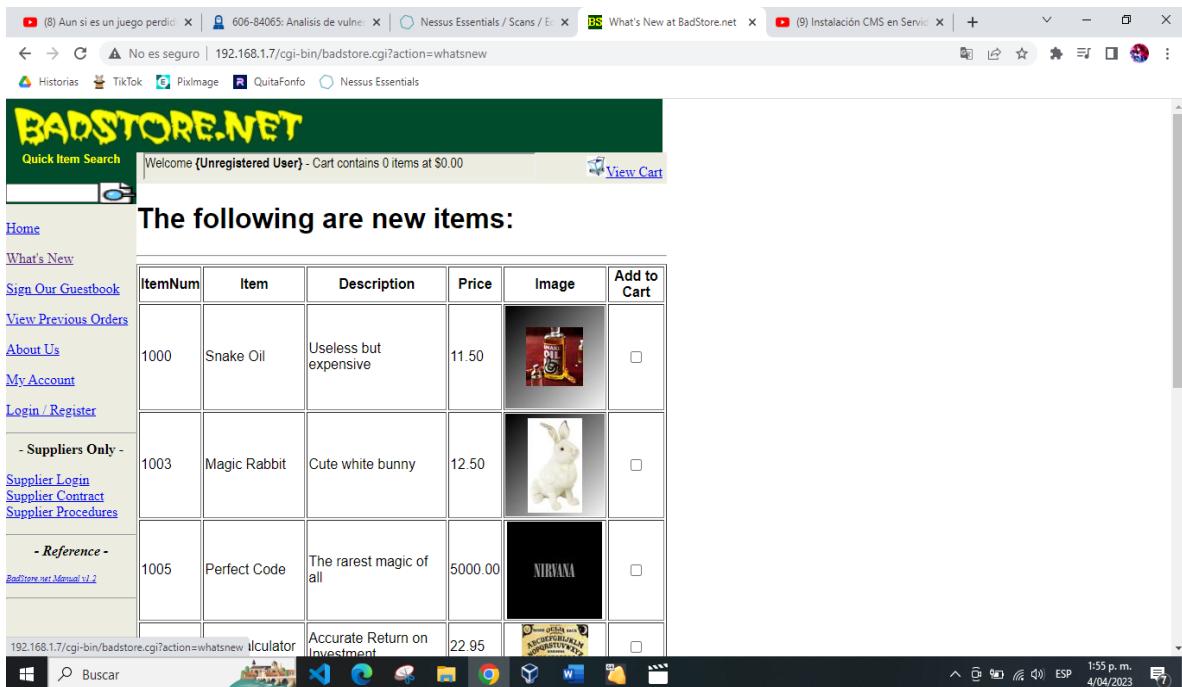
Please press Enter to activate this console.
bash# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:A8:90:D4
          inet addr:192.168.1.7  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MTU:1500 Metric:1
          RX packets:156 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:11098 (10.8 kiB)  TX bytes:2632 (2.5 kiB)
          Interrupt:9 Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 iB)  TX bytes:0 (0.0 iB)

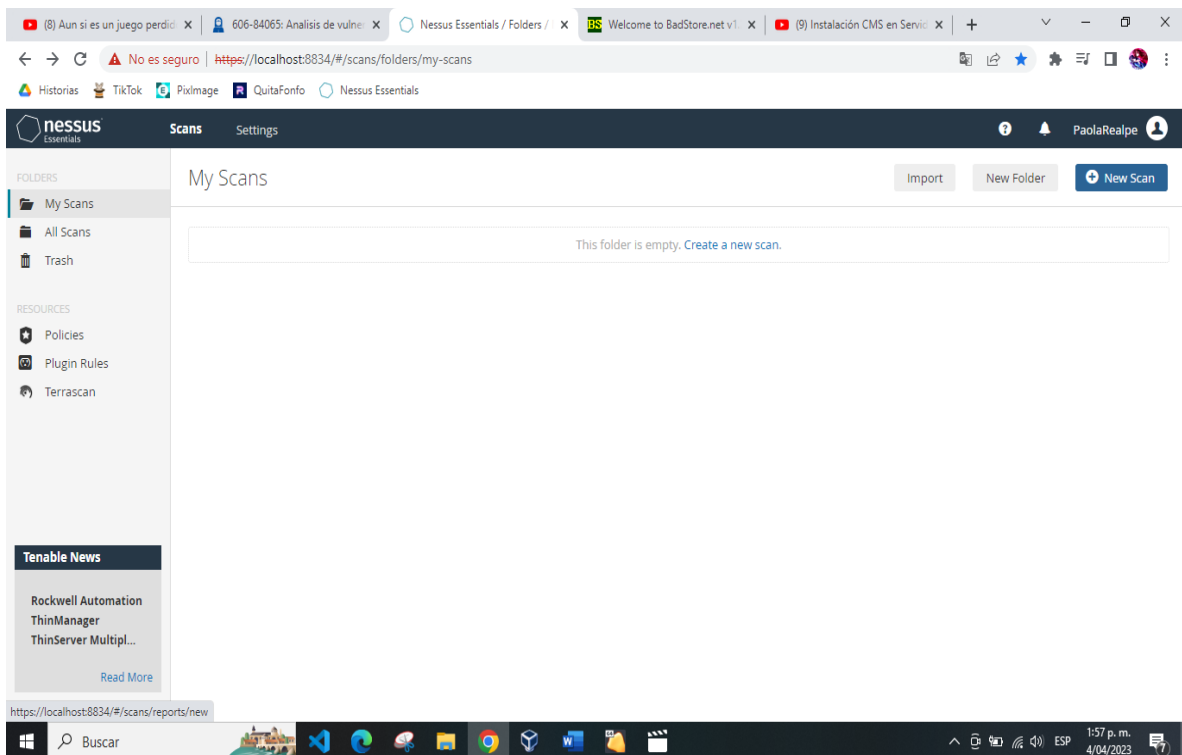
bash#
```

Ahora nos ubicamos en el navegador de Google y escribimos la dirección IP para poder navegar en la BadStore

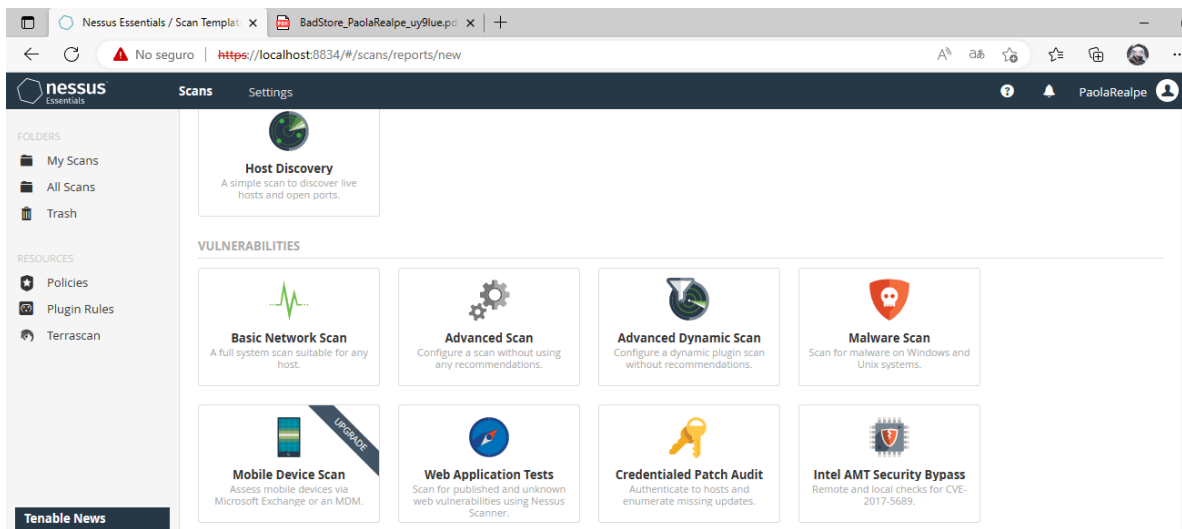




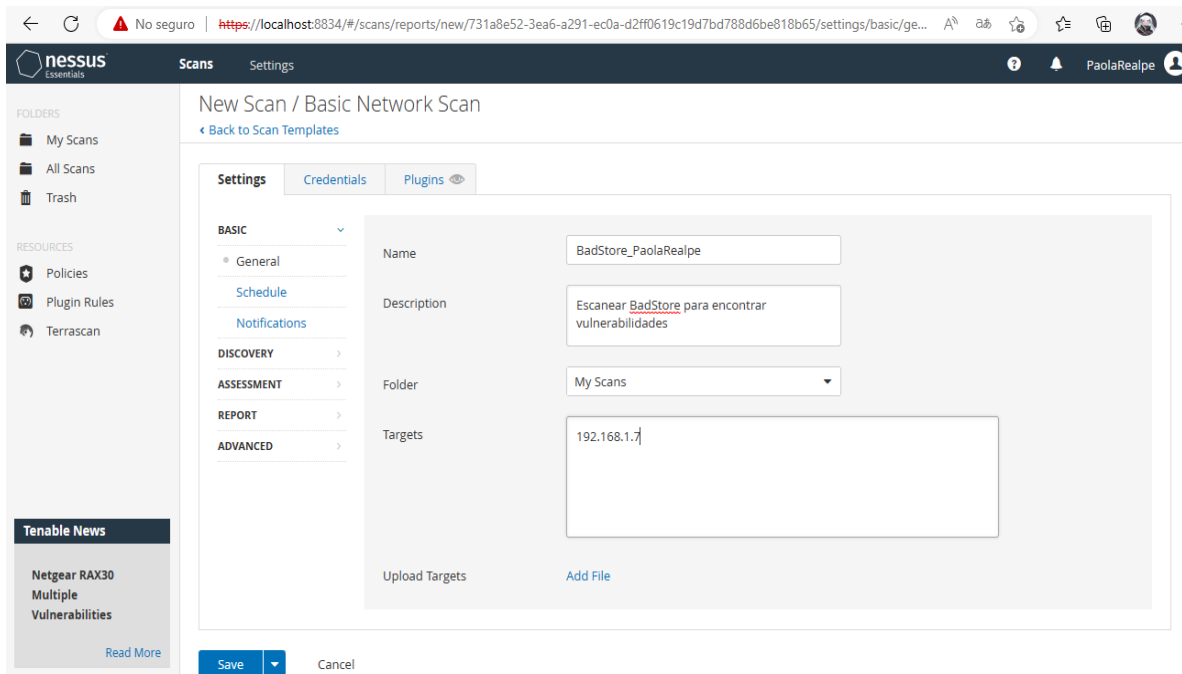
Ahora se abre la aplicación de Nessus en el navegador Exploret y se crea un **New Scan** con el botón de la esquina superior izquierda



Se selecciona Basic Network Scan o un escaneo de red básico, que se utiliza para analizar la seguridad de los sistemas activos en una red como es el caso de BadStore

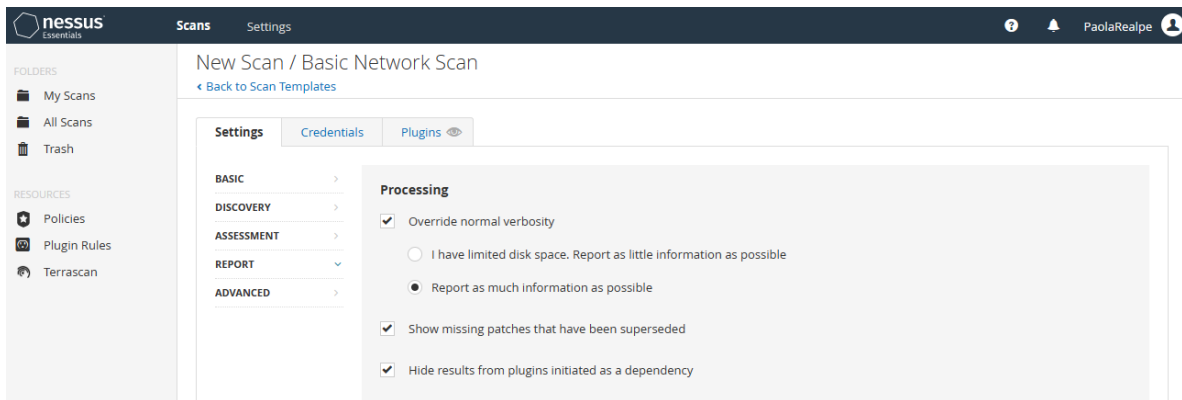


Se agrega el nombre **BadStore_PaolaRealpe**, una descripción donde especifique lo que se va a realizar y en la Target se escribe la dirección IP en la que se encuentra el BadStore que en este caso es **192.168.1.7**

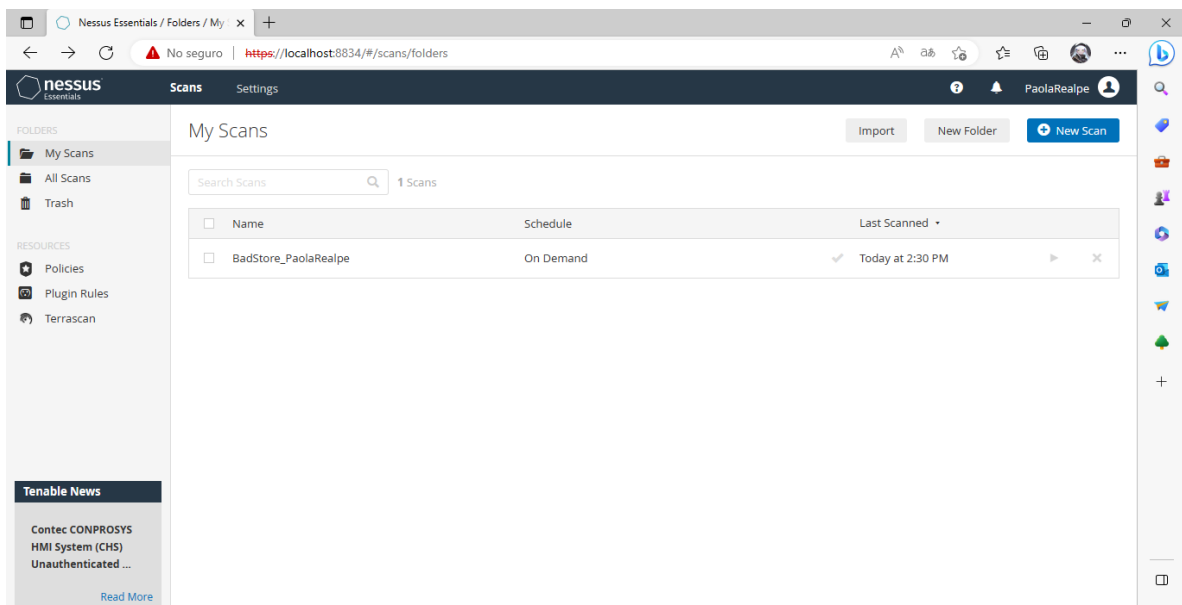


En la parte de opciones de Reporte, se agregó en el proceso la opción para proporcionar la mayor información posible en todas las vulnerabilidades que se encuentren, después del escaneo.

Por último, se da clic a la opción **Save**



Iniciamos el escaneo de BadStore dando clic a el icono de Start y esperamos unos minutos para que termine de realizar el proceso



Ahora podemos comprobar las vulnerabilidades que tiene y nos damos cuenta que son 2 de tipo Medio y 5 de tipo de información

The screenshot shows the Nessus Scans page for a scan named 'BadStore_PaolaRealpe'. The left sidebar contains 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main content area has tabs for 'Hosts' (1), 'Vulnerabilities' (4), and 'History' (1). Below the tabs is a search bar and a table with one host: 192.168.1.7, showing 2 vulnerabilities. To the right, 'Scan Details' are listed: Policy: Basic Network Scan, Status: Completed, Severity Base: CVSS v2.0, Scanner: Local Scanner, Start: Today at 2:24 PM, End: Today at 2:30 PM, Elapsed: 6 minutes. Below this is a 'Vulnerabilities' donut chart showing a distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (dark blue).

Para poder observarlas mejor le damos clic a la pestaña de vulnerabilidades y nos las enlista de la siguiente manera

The screenshot shows the Nessus Scans page for the same scan, but with the 'Vulnerabilities' tab selected. The main content area displays a table of 4 vulnerabilities. The first row is highlighted with a purple 'MIXED' label. The other three rows are labeled 'INFO'.

Sev	CVSS	VPR	Name	Family	Count
MIXED	4 D...	DNS	4
INFO			Eth...	Misc.	1
INFO			Eth...	General	1
INFO			Nes...	Settings	1

The 'Scan Details' and 'Vulnerabilities' donut chart are also visible on the right side of the page.

En la casilla morada de Mixed podemos ver que es como una carpeta que contiene mas vulnerabilidades encontradas, las podemos ver al dar clic sobre ella

Nessus Essentials / Folders / View x +

No seguro | <https://localhost:8834/#/scans/reports/20/vulnerabilities/group/15753>

nessus Essentials Scans Settings ? PaolaRealpe

BadStore_PaolaRealpe / DNS (Multiple Issues)

[Back to Vulnerabilities](#) [Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

Hosts 1 Vulnerabilities 4 History 1

Search Vulnerabilities 4 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
MEDIUM	5.0	2.7	Mul...	DNS	1	
MEDIUM	5.0		DN...	DNS	1	
INFO			DN...	DNS	1	
INFO			DN...	DNS	1	

Scan Details

Policy: Basic Network Scan
 Status: Completed
 Severity Base: CVSS v2.0
 Scanner: Local Scanner
 Start: Today at 2:24 PM
 End: Today at 2:30 PM
 Elapsed: 6 minutes

Vulnerabilities

Unauthenticated Command Injection in TP-Link Arche... [Read More](#)

Nessus también tiene la función de describir las características de las vulnerabilidades encontradas y las posibles soluciones que se pueden aplicar para mejorar la seguridad

Nessus Essentials / Folders / View x +

No seguro | <https://localhost:8834/#/scans/reports/20/vulnerabilities/group/15753/15753>

nessus Essentials Scans Settings ? PaolaRealpe

Hosts 1 Vulnerabilities 4 History 1

MEDIUM Multiple Vendor DNS Response Flooding Denial Of Service

Description

The remote DNS server is vulnerable to a denial of service attack because it replies to DNS responses.

An attacker could exploit this vulnerability by spoofing a DNS packet so that it appears to come from 127.0.0.1 and make the remote DNS server enter into an infinite loop, therefore denying service to legitimate users.

Solution

Contact the vendor for an appropriate upgrade.

See Also

<http://www.nessus.org/u7a04dcb96>

Output

```
Nessus sent the following response data :
0x00: 76 82 81 80 00 01 00 00 01 00 00 03 77 77 77 v.....www
0x10: 06 67 6F 67 6C 65 03 63 6F 6D 00 00 10 00 01 .google.com....
0x20: C0 10 00 06 00 01 00 00 00 3C 00 26 03 6E 73 31 .....<.f.nsl
0x30: C0 10 09 64 6E 73 2D 61 64 6D 69 6E C0 10 1F 14 ...dns-admin....
0x40: 14 23 00 00 03 84 00 00 03 84 00 00 07 08 00 00 .#.
0x50: 00 3C .<
```

[more...](#)

Plugin Details

Severity: Medium
 ID: 15753
 Version: 1.22
 Type: remote
 Family: DNS
 Published: November 18, 2004
 Modified: July 10, 2018

VPR Key Drivers

Threat Recency: No recorded events
 Threat Intensity: Very Low
 Exploit Code Maturity: Unproven
 Age of Vuln: 730 days +
 Product Coverage: Very High
 CVSSv3 Impact Score: 2.7
 Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 2.7

Authentication Bypass in Netgear RAX30 (AX2400) <... [Read More](#)

Nessus Essentials / Folders / View x +

No seguro | <https://localhost:8834/#/scans/reports/20/vulnerabilities/group/15753/12217>

nessus Essentials Scans Settings PaolaRealpe

BadStore_PaolaRealpe / Plugin #12217

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 4 History 1

MEDIUM DNS Server Cache Snooping Remote Information Disclosure

Description
The remote DNS server responds to queries for third-party domains that do not have the recursion bit set.

This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited.

For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more.

Note: If this is an internal DNS server not accessible to outside networks, attacks would be limited to the internal network. This may include employees, consultants and potentially users on a guest network or WiFi connection if supported.

Solution
Contact the vendor of the DNS software for a fix.

Plugin Details

Severity: Medium
ID: 12217
Version: 1.26
Type: remote
Family: DNS
Published: April 27, 2004
Modified: April 7, 2020

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score: 5.3
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/E:N/A/N
CVSS v2.0 Base Score: 5.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Tenable News

Tenable Cyber Watch:
Help for MITRE
ATT&CK Mapping...
[Read More](#)

Generar Informe PDF

Nessus permite generar un informe de las vulnerabilidades encontradas. En este caso se realizará dos reportes, para ello seleccionamos la opción Report de la parte superior y luego, le decimos que queremos el formato en pdf de **Detailed Vulnerabilities By Host** y seleccionamos **Generate Report**

Nessus Essentials / Folders / View x +

No seguro | <https://localhost:8834/#/scans/reports/20/vulnerabilities>

nessus Essentials Scans Settings PaolaRealpe

BadStore_PaolaRealpe

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 4 History 1

Filter Search Vulnerabilities 4 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
MIXED	D...	DNS	4	
INFO			Eth...	Misc.	1	
INFO			Eth...	General	1	
INFO			Nes...	Settings	1	

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v2.0
Scanner: Local Scanner
Start: Today at 2:24 PM
End: Today at 2:30 PM
Elapsed: 6 minutes

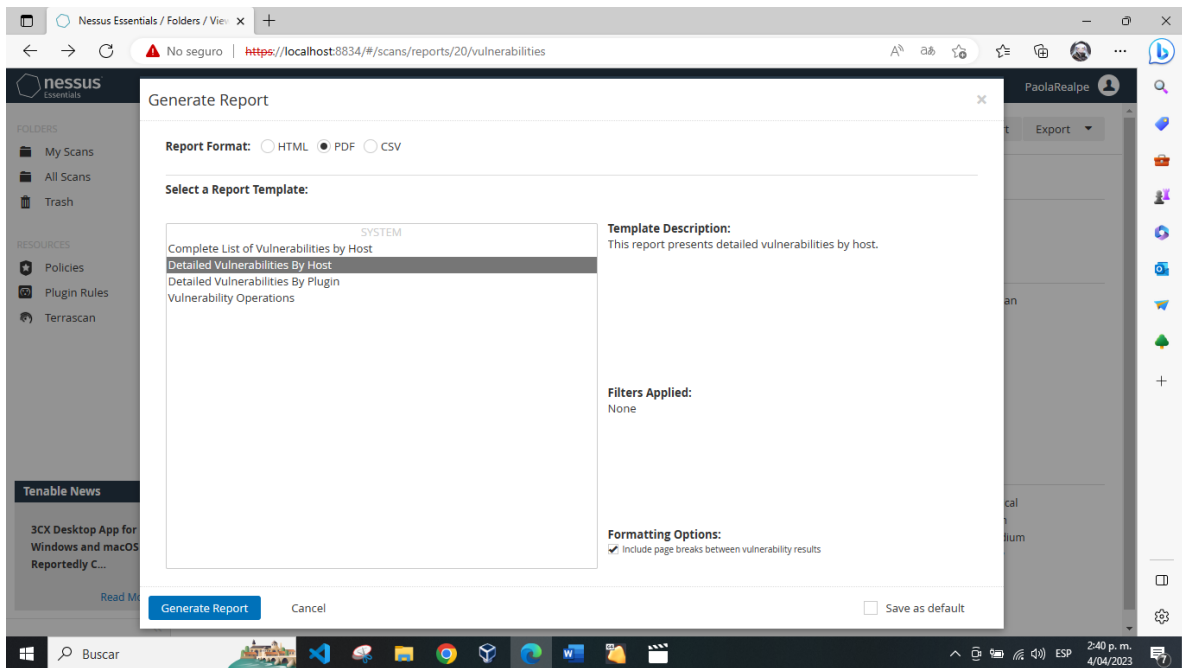
Vulnerabilities

● Critical
● High
● Medium
● Low
● Info

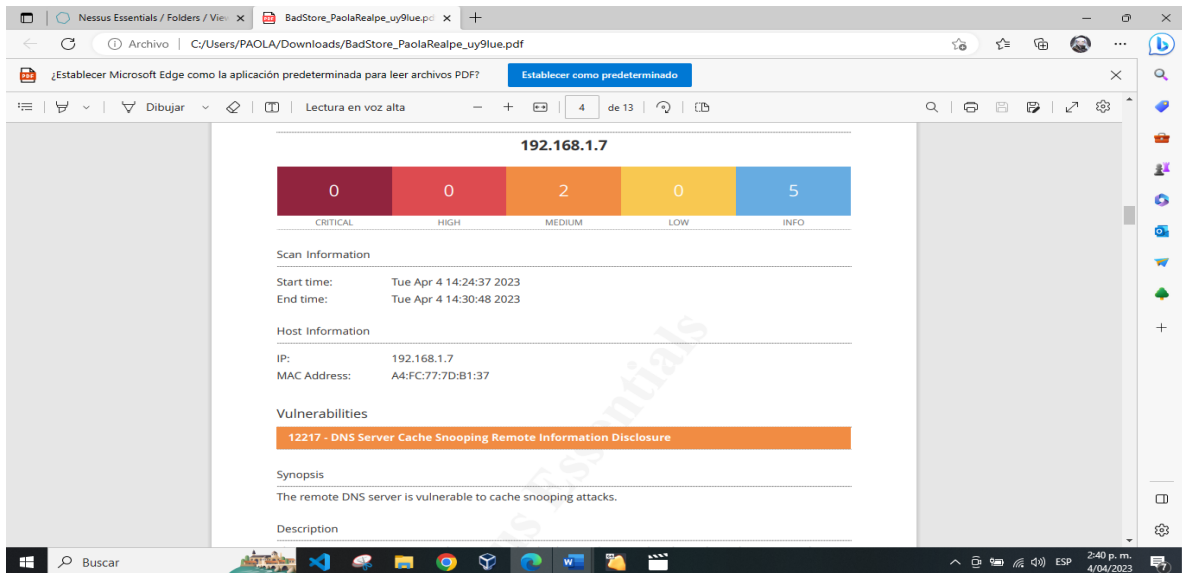
<https://localhost:8834/#>

Buscar

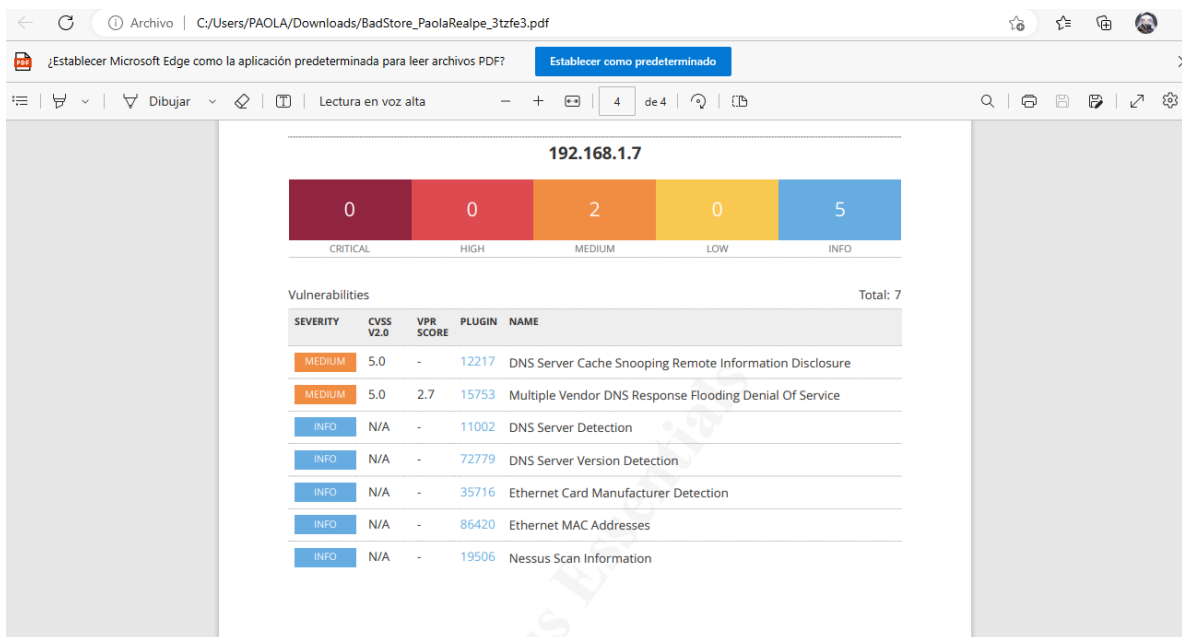
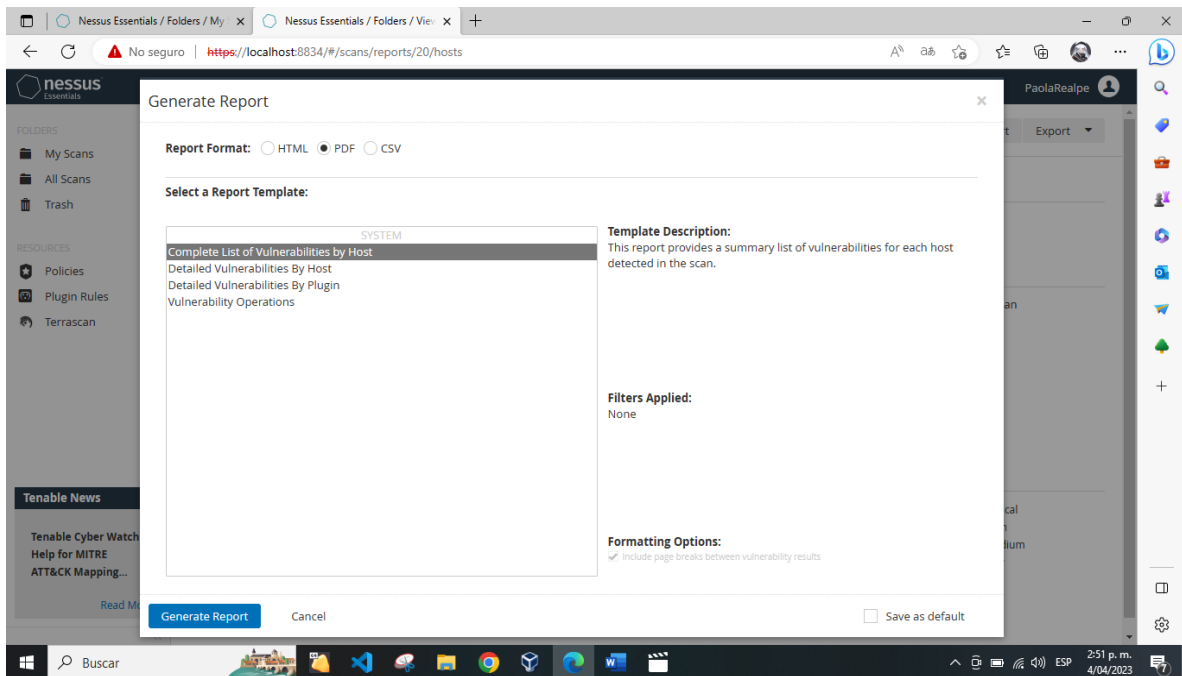
2:40 p. m.
4/04/2023



Luego se descarga automáticamente el archivo con los detalles de las vulnerabilidades encontradas



Se debe generar otro reporte de entrega por lo que se realiza los mismos pasos excepto que esta vez en la selección de reporte se escoge **Complete List of Vulnerabilities**



B. Describa con sus propias palabras las vulnerabilidades encontradas en cada caso y describa con sus palabras teniendo en cuenta la documentación que sugiere nessus, como se debería solucionar o qué medidas se deben tomar para resolver la vulnerabilidad

MEDIUM - Multiple Vendor DNS Response Flooding Denial Of Service (Respuesta DNS de múltiples proveedores Inundación)

Esta Vulnerabilidad de nivel medio que se encontró en BadStore afirma que el servidor DNS puede ser perjudicado por un ataque de denegación de servicio. Esto se debe a que se recibe una gran cantidad de solicitudes de consulta por DNS lo que puede agotar los recursos y no ser capaz de manejarlos. En otras palabras, un ciberdelincuente puede aprovechar esto suplantando un paquete DNS que puede provenir de la dirección 127.0.0.1 (IP falsa), para hacer que entre en un bucle infinito para que de esta manera se deniegue el servicio que ofrece BadStore y se vuelve inaccesible para los usuarios.

SOLUCION NESSUS

La solución que aconseja Nessus es ponerse en contacto con el proveedor para obtener una actualización, esto quiere decir que la vulnerabilidad puede estar relacionada con el software del servidor DNS que proporciona un proveedor, o también existe el caso de que se haya lanzado una actualización para solucionar este tipo de vulnerabilidad.

Entre otras posibles soluciones que se pueden encontrar es la limitación de la cantidad de tráfico que se acepta, aplicando las reglas de un firewall y otros programas de seguridad.

SOLUCION INTEGRANTES DEL GRUPO

También se puede realizar una configuración del DNS para autenticar a los usuarios que ingresan, o implementar los servicios de protección de DNS que detectan y mitigan los ataques de DDos para proteger los servidores.

Otras medidas de prevención que se deben seguir para proteger el DNS es ubicar el servidor web en una zona desmilitarizada, con el propósito de que el ciberdelincuente no pueda acceder a la red interna que usa BadStore, la implementación de un sistema de detección como IDS o IPS para monitorizar las conexiones que se realizan.

MEDIUM - DNS Server Cache Snooping Remote Information Disclosure (Divulgación remota de información de espionaje de caché)

El servidor DNS es vulnerable porque responde a las solicitudes de diversos dominios que no poseen el bit de recursión, así que un ciberdelincuente puede determinar fácilmente el dominio del servidor y los hosts que se han visitado.

Esto puede ser una gran vulnerabilidad ya que, si una empresa utiliza los servicios en línea, en base a asuntos financieros, le da capacidad de construir un modelo estadísticos de los recursos que se manejan.

Cabe aclarar que si es interno solo se limitara a esa red, lo que puede incluir invitados, empleados y consultores.

SOLUCION NESSUS

La solución que aconseja Nessus es ponerse en contacto con el proveedor DNS para obtener una corrección, esto sugiere que la vulnerabilidad puede estar ligada al servidor DNS que proporciona un proveedor, y que puede ser solucionada con una corrección.

SOLUCION DE INTEGRANTES DEL GRUPO

Otras soluciones para esta vulnerabilidad son la actualización del software del servidor DNS, deshabilitar la memoria cache del servidor o la implementación de medidas de seguridad adicionales como la detección y prevención de intrusiones.

INFO - DNS Server Detection (Detección de servidor DNS)

Se presenta una detección de servidor en otras palabras, el servicio remoto es un servidor DNS que traduce los hosts de internet en dirección IP, organizándola en una jerarquía

SOLUCION NESSUS

La solución que aconseja Nessus es deshabilitar el servicio o restringir el acceso a los hosts internos si es que está disponible de forma externa, lo cual significa que se necesitan tomar medidas con el propósito de mitigar los posibles riesgos de seguridad en el sistema para que este no esté abierto a terceros.

SOLUCION DE GRUPO

Las soluciones que se pueden sugerir según la información dada, es la configuración de un túnel VPN de red privada para la encriptación de DNS, también se puede utilizar un sistema de nombres de dominio no convencional, usar un DNS privado para evitar que el tráfico de DNS sea detectado, entre otros métodos