

ACTIVIDAD DE APRENDIZAJE 2 UNIDAD 3:

Buscando vulnerabilidades

Fase Transversal - Interpretación, aprehensión y transferencia conceptual / temática.

En esta actividad se pondrá en práctica la ejecución de análisis y escaneo de vulnerabilidades en una máquina de Windows 7 por medio de las herramientas de Nmap y Nessus, de modo tal se requerirá el manejo de conceptos previos de comandos para consolas en Linux que permitirán la manipulación de las herramientas de escaneo desde una máquina con Kali Linux. También se debe prever la adecuación del entorno, tanto de la máquina atacante como de la máquina objetivo, la configuración de aspectos de red y la instalación de las herramientas requeridas para el ejercicio.

Por otro lado, se realizará un análisis de los resultados generados por los escaneos de vulnerabilidades con base al script **vulners**, de modo tal se deberá recabar información desde las fuentes entregadas por los análisis, revisando datos como el vector de ataque, puntaje, descripción y exploit existentes para dicha vulnerabilidad. En este caso, y por la naturaleza del ejercicio, se buscará volver lo más vulnerable la máquina objetivo para poder obtener la mayor cantidad de información que para analizar.

Finalmente, se profundizará en los conceptos de Exploit y Payload, explicando su relación entre sí y con conceptos previamente manejados como el de vulnerabilidad, esto permitiendo entender a que se refieren en el momento de la identificación de las vulnerabilidades y sus exploits previamente extraídos del escaneo de vulnerabilidades.

Fase Uno – Planteamiento de estudio de casos o actividad

1. Ejecutar Nmap para escaneo de la red y escaneo de vulnerabilidades (tomar evidencia)

```
nmap -sV --script vulners <target ip>  
nmap -sV --script vulners --script-args mincvss=5.0 <target ip>
```

2. Completar la siguiente tabla:

CVE	SCORT 3x	Vector	Descripción (url)	Exploit

- Indagar como se ejecuta el scan de vulnerabilidades con **NESSUS** o **OPENVASS** (según la que tenga instalada) aplique un scan a la maquina objetivo, contraste los resultados no **nmap**; e Indague las vulnerabilidades de nivel crítico alto y medio que de como resultado el scan
- A partir de lo indicado en clase y con apoyo en fuentes externas indique que es un **Payload**, y un **exploit**.

Fase Dos – Planteamiento de la respuesta y solución de la actividad

1. Escaneo de vulnerabilidades con NMAP

Para conocer la IP de la maquina objetivo, en este escenario en el cual podemos tener acceso a la maquina objetivo, se va a realizar una verificación desde la maquina atacante en la cual se realice un escaneo a la red local en la que se encuentra también la maquina objetivo:

```
(root@kali)-[/home/tao/Escritorio]
# nmap -sP 192.168.0.*
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-21 22:36 -05
Nmap scan report for 192.168.0.1
Host is up (0.0013s latency).
MAC Address: 50:39:55:53:04:9B (Cisco Spvtg)
Nmap scan report for 192.168.0.10
Host is up (0.12s latency).
MAC Address: D0:9C:7A:DD:83:62 (Xiaomi Communications)
Nmap scan report for 192.168.0.11
Host is up (0.00067s latency).
MAC Address: 08:00:27:EC:9F:6D (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.0.14
Host is up (0.00045s latency).
MAC Address: 2C:F0:5D:10:13:8B (Micro-star Intl)
Nmap scan report for 192.168.0.25
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.49 seconds
```

Ilustración 1 Identificación del objetivo con NMAP

Dentro del recuadro rojo se puede ver que, desde la maquina atacante, se puede reconocer la IP de la maquina objetivo, la cual se valida por medio de la ejecución del comando IPCONFIG en la maquina objetivo:

```
C:\Users\tao>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::29b2:3877:5ee8:45ca%11
    Dirección IPv4. . . . . : 192.168.0.11
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.0.1

Adaptador de túnel isatap.{F01ED4C8-073B-4C83-A015-A1FB1963EAE5}:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :
```

Ilustración 2 identificación de dirección IP de la maquina objetivo

Con la IP del objetivo definida, se ejecuta la siguiente instrucción para el escaneo de vulnerabilidades:

```
nmap -sV --script vulners 192.168.0.11
```

Con esta instrucción se obtuvo la siguiente respuesta:

```
└─(root@kali)-[/home/tao/Escritorio]
└─# nmap -sV --script vulners 192.168.0.11
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-22 23:10 -05
Nmap scan report for 192.168.0.11
Host is up (0.00054s latency).
Not shown: 979 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd 0.9.41 beta
| vulners:
| cpe:/a:filezilla-project:filezilla_server:0.9.41_beta:
|   VMSA-2008-0014.3    10.0    https://vulners.com/vmware/VMSA-2008-0014.3
|   SSV:3950            10.0    https://vulners.com/seebug/SSV:3950      *EXPLOIT*
|   VMSA-2008-0018      9.3     https://vulners.com/vmware/VMSA-2008-0018
|   SSV:4423            9.3     https://vulners.com/seebug/SSV:4423      *EXPLOIT*
|   VMSA-2009-0007      7.5     https://vulners.com/vmware/VMSA-2009-0007
|   SSV:3423            7.5     https://vulners.com/seebug/SSV:3423      *EXPLOIT*
```



```

|      SSV:3166      7.5      https://vulners.com/seebug/SSV:3166      *EXPLOIT*
|
|      MSF:ILITIES/SUSE-CVE-2008-1808/      7.5
|      https://vulners.com/metasploit/MSF:ILITIES/SUSE-CVE-2008-1808/      *EXPLOIT*
|
|      MSF:ILITIES/SUSE-CVE-2008-1807/      7.5
|      https://vulners.com/metasploit/MSF:ILITIES/SUSE-CVE-2008-1807/      *EXPLOIT*
|
|      MSF:ILITIES/SUSE-CVE-2008-1806/      7.5
|      https://vulners.com/metasploit/MSF:ILITIES/SUSE-CVE-2008-1806/      *EXPLOIT*
|
|      MSF:ILITIES/LINUXRPM-RHSA-2008-0558/      7.5
|      https://vulners.com/metasploit/MSF:ILITIES/LINUXRPM-RHSA-2008-0558/      *EXPLOIT*
|
|      MSF:ILITIES/GENTOO-LINUX-CVE-2008-1806/      7.5
|      https://vulners.com/metasploit/MSF:ILITIES/GENTOO-LINUX-CVE-2008-1806/      *EXPLOIT*
|
|      VMSA-2008-0019.1      7.2      https://vulners.com/vmware/VMSA-2008-0019.1
|
|      SSV:4528      7.2      https://vulners.com/seebug/SSV:4528      *EXPLOIT*
|
|      SSV:4422      6.9      https://vulners.com/seebug/SSV:4422      *EXPLOIT*
|
|      SSV:3949      5.0      https://vulners.com/seebug/SSV:3949      *EXPLOIT*
|
|      SSV:11498      4.0      https://vulners.com/seebug/SSV:11498      *EXPLOIT*
|_
|      SSV:3947      2.1      https://vulners.com/seebug/SSV:3947      *EXPLOIT*
22/tcp      open      ssh      OpenSSH for_Windows_8.6 (protocol 2.0)
25/tcp      open      smtp      Mercury/32 smtpd (Mail server account Maiser)
79/tcp      open      finger      Mercury/32 fingerd
80/tcp      open      http      Apache httpd 2.4.48 ((Win64) OpenSSL/1.1.1l PHP/7.4.23)
|_http-server-header: Apache/2.4.48 (Win64) OpenSSL/1.1.1l PHP/7.4.23
| vulners:
|   cpe:/a:apache:http_server:2.4.48:
|_
|_      CVE-2021-33193      5.0      https://vulners.com/cve/CVE-2021-33193
106/tcp      open      pop3pw      Mercury/32 poppass service
110/tcp      open      pop3      Mercury/32 pop3d
135/tcp      open      msrpc      Microsoft Windows RPC
139/tcp      open      netbios-ssn      Microsoft Windows netbios-ssn
143/tcp      open      imap      Mercury/32 imapd 4.62
443/tcp      open      ssl/http      Apache httpd 2.4.48 ((Win64) OpenSSL/1.1.1l PHP/7.4.23)

|_http-server-header: Apache/2.4.48 (Win64) OpenSSL/1.1.1l PHP/7.4.23
| vulners:
|   cpe:/a:apache:http_server:2.4.48:

```



```
|_ CVE-2021-33193 5.0 https://vulners.com/cve/CVE-2021-33193
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup:
WORKGROUP)
2869/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
3306/tcp open mysql?
| fingerprint-strings:
| DNSVersionBindReqTCP, FourOhFourRequest, LDAPSearchReq, NULL, RPCCheck, X11Probe:
|_ Host '192.168.0.25' is not allowed to connect to this MariaDB server
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
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
49157/tcp open msrpc Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please
submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service
:
SF-Port3306-TCP:V=7.91%I=7%D=9/22%Time=614BFE34%P=x86_64-pc-linux-gnu%r(NU
SF:LL,4B,"G\0\0\x01\xffj\x04Host\x20'192\.168\.0\.25'\x20is\x20not\x20allo
SF:wed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(RPCCheck,4B
SF:,"G\0\0\x01\xffj\x04Host\x20'192\.168\.0\.25'\x20is\x20not\x20allowed\x
SF:20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(DNSVersionBindRe
SF:qTCP,4B,"G\0\0\x01\xffj\x04Host\x20'192\.168\.0\.25'\x20is\x20not\x20al
SF:lowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(X11Probe,
SF:4B,"G\0\0\x01\xffj\x04Host\x20'192\.168\.0\.25'\x20is\x20not\x20allowed
SF:\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(FourOhFourRequ
SF:est,4B,"G\0\0\x01\xffj\x04Host\x20'192\.168\.0\.25'\x20is\x20not\x20all
SF:owed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(LDAPSearch
SF:Req,4B,"G\0\0\x01\xffj\x04Host\x20'192\.168\.0\.25'\x20is\x20not\x20all
SF:owed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server");
MAC Address: 08:00:27:EC:9F:6D (Oracle VirtualBox virtual NIC)
```



```
Service Info: Hosts: localhost, TAO-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 61.81 seconds
```

Luego se ejecutó la siguiente instrucción la cual es la misma que la anterior, operando con el script vulners pero definiéndole como argumentos por medio de la cláusula --script-args la versión mínima para CVSS, en este caso se define la versión 5.0:

```
nmap -sV --script vulners --script-args mincvss=5.0 192.168.0.11
```

Esta instrucción retorna los siguientes resultados:

```
(root@kali)-[/home/tao/Escritorio]
# nmap -sV --script vulners --script-args mincvss=5.0 192.168.0.11
130 x
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-22 23:17 -05
Nmap scan report for 192.168.0.11
Host is up (0.00072s latency).
Not shown: 979 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd 0.9.41 beta
| vulners:
|   cpe:/a:filezilla-project:filezilla_server:0.9.41_beta:
|       VMSA-2008-0014.3      10.0      https://vulners.com/vmware/VMSA-2008-0014.3
|       SSV:3950              10.0      https://vulners.com/seebug/SSV:3950      *EXPLOIT*
|       VMSA-2008-0018      9.3      https://vulners.com/vmware/VMSA-2008-0018
|       SSV:4423              9.3      https://vulners.com/seebug/SSV:4423      *EXPLOIT*
|       VMSA-2009-0007      7.5      https://vulners.com/vmware/VMSA-2009-0007
|       SSV:3423              7.5      https://vulners.com/seebug/SSV:3423      *EXPLOIT*
|       SSV:3166              7.5      https://vulners.com/seebug/SSV:3166      *EXPLOIT*
|
|       MSF:ILITIES/SUSE-CVE-2008-1808/      7.5
|       https://vulners.com/metasploit/MSF:ILITIES/SUSE-CVE-2008-1808/      *EXPLOIT*
|
|       MSF:ILITIES/SUSE-CVE-2008-1807/      7.5
|       https://vulners.com/metasploit/MSF:ILITIES/SUSE-CVE-2008-1807/      *EXPLOIT*
```



```

| MSF:ILITIES/SUSE-CVE-2008-1806/ 7.5
| https://vulners.com/metasploit/MSF:ILITIES/SUSE-CVE-2008-1806/ *EXPLOIT*
| MSF:ILITIES/LINUXRPM-RHSA-2008-0558/ 7.5
| https://vulners.com/metasploit/MSF:ILITIES/LINUXRPM-RHSA-2008-0558/ *EXPLOIT*
| MSF:ILITIES/GENTOO-LINUX-CVE-2008-1806/ 7.5
| https://vulners.com/metasploit/MSF:ILITIES/GENTOO-LINUX-CVE-2008-1806/ *EXPLOIT*
| VMSA-2008-0019.1 7.2 https://vulners.com/vmware/VMSA-2008-0019.1
| SSV:4528 7.2 https://vulners.com/seebug/SSV:4528 *EXPLOIT*
| SSV:4422 6.9 https://vulners.com/seebug/SSV:4422 *EXPLOIT*
| SSV:3949 5.0 https://vulners.com/seebug/SSV:3949 *EXPLOIT*
| SSV:11498 4.0 https://vulners.com/seebug/SSV:11498 *EXPLOIT*
|_ SSV:3947 2.1 https://vulners.com/seebug/SSV:3947 *EXPLOIT*
22/tcp open ssh OpenSSH for_Windows_8.6 (protocol 2.0)
25/tcp open smtp Mercury/32 smtpd (Mail server account Maiser)
79/tcp open finger Mercury/32 fingerd
80/tcp open http Apache httpd 2.4.48 ((Win64) OpenSSL/1.1.1l PHP/7.4.23)
|_http-server-header: Apache/2.4.48 (Win64) OpenSSL/1.1.1l PHP/7.4.23
| vulners:
| cpe:/a:apache:http_server:2.4.48:
|_ CVE-2021-33193 5.0 https://vulners.com/cve/CVE-2021-33193
106/tcp open pop3pw Mercury/32 poppass service
110/tcp open pop3 Mercury/32 pop3d
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
143/tcp open imap Mercury/32 imapd 4.62
443/tcp open ssl/http Apache httpd 2.4.48 ((Win64) OpenSSL/1.1.1l PHP/7.4.23)
|_http-server-header: Apache/2.4.48 (Win64) OpenSSL/1.1.1l PHP/7.4.23
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup:
WORKGROUP)
2869/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
3306/tcp open mysql?
| fingerprint-strings:
| Help, LANDesk-RC, LDAPSearchReq, LPDString, NULL, RPCCheck, RTSPRequest:
|_ Host '192.168.0.25' is not allowed to connect to this MariaDB server

```




```
5357/tcp open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
```

```
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
49157/tcp open  msrpc           Microsoft Windows RPC
```

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

```
SF-Port3306-TCP:V=7.91%I=7%D=9/22%Time=614BFFD0%P=x86_64-pc-linux-gnu%r(NU
SF:LL,4B,"G\0\0\x01\xffj\x04Host\x20'192\0.168\0.25'\x20is\x20not\x20allo
SF:wed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(RTSPRequest
SF:,4B,"G\0\0\x01\xffj\x04Host\x20'192\0.168\0.25'\x20is\x20not\x20allowe
SF:d\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(RPCCheck,4B,"
SF:G\0\0\x01\xffj\x04Host\x20'192\0.168\0.25'\x20is\x20not\x20allowed\x20
SF:to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(Help,4B,"G\0\0\x01
SF:\xffj\x04Host\x20'192\0.168\0.25'\x20is\x20not\x20allowed\x20to\x20con
SF:nect\x20to\x20this\x20MariaDB\x20server")%r(LPDString,4B,"G\0\0\x01\xff
SF:j\x04Host\x20'192\0.168\0.25'\x20is\x20not\x20allowed\x20to\x20connect
SF:\x20to\x20this\x20MariaDB\x20server")%r(LDAPSearchReq,4B,"G\0\0\x01\xff
SF:j\x04Host\x20'192\0.168\0.25'\x20is\x20not\x20allowed\x20to\x20connect
SF:\x20to\x20this\x20MariaDB\x20server")%r(LANDesk-RC,4B,"G\0\0\x01\xffj\x
SF:04Host\x20'192\0.168\0.25'\x20is\x20not\x20allowed\x20to\x20connect\x2
SF:0to\x20this\x20MariaDB\x20server");
```

MAC Address: 08:00:27:EC:9F:6D (Oracle VirtualBox virtual NIC)

Service Info: Hosts: localhost, TAO-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 79.16 seconds

En conclusión y en base a ambos escaneos, uno definiendo la versión de CVSS y otro no, se pudieron detectar las siguientes vulnerabilidades, las cuales se especificarán a mayor profundidad en el siguiente punto:

Servicio	FileZilla ftpd 0.9.41 beta		
Puerto	21		
Vulnerabilidades detectadas			
cpe:/a:filezilla-project:filezilla_server:0.9.41_beta:			
	VMSA-2008-0014.3	10.0	https://vulners.com/vmware/VMSA-2008-0014.3
	SSV:3950	10.0	https://vulners.com/seebug/SSV:3950 *EXPLOIT*
	VMSA-2008-0018	9.3	https://vulners.com/vmware/VMSA-2008-0018
	SSV:4423	9.3	https://vulners.com/seebug/SSV:4423 *EXPLOIT*
	VMSA-2009-0007	7.5	https://vulners.com/vmware/VMSA-2009-0007
	SSV:3423	7.5	https://vulners.com/seebug/SSV:3423 *EXPLOIT*
	SSV:3166	7.5	https://vulners.com/seebug/SSV:3166 *EXPLOIT*
	MSF:ILITIES/SUSE-CVE-2008-1808/		7.5
	https://vulners.com/metasploit/MSF:ILITIES/SUSE-CVE-2008-1808/		*EXPLOIT*
	MSF:ILITIES/SUSE-CVE-2008-1807/		7.5
	https://vulners.com/metasploit/MSF:ILITIES/SUSE-CVE-2008-1807/		*EXPLOIT*
	MSF:ILITIES/SUSE-CVE-2008-1806/		7.5
	https://vulners.com/metasploit/MSF:ILITIES/SUSE-CVE-2008-1806/		*EXPLOIT*
	MSF:ILITIES/LINUXRPM-RHSA-2008-0558/		7.5
	https://vulners.com/metasploit/MSF:ILITIES/LINUXRPM-RHSA-2008-0558/		*EXPLOIT*
	MSF:ILITIES/GENTOO-LINUX-CVE-2008-1806/		7.5
	https://vulners.com/metasploit/MSF:ILITIES/GENTOO-LINUX-CVE-2008-1806/		
EXPLOIT			
	VMSA-2008-0019.1	7.2	https://vulners.com/vmware/VMSA-2008-0019.1
	SSV:4528	7.2	https://vulners.com/seebug/SSV:4528 *EXPLOIT*
	SSV:4422	6.9	https://vulners.com/seebug/SSV:4422 *EXPLOIT*
	SSV:3949	5.0	https://vulners.com/seebug/SSV:3949 *EXPLOIT*
	SSV:11498	4.0	https://vulners.com/seebug/SSV:11498 *EXPLOIT*

_	SSV:3947	2.1	https://vulners.com/seebug/SSV:3947	*EXPLOIT*
---	----------	-----	---	-----------

Ilustración 3 Vulnerabilidades detectadas en FileZilla

Servicio	Apache httpd 2.4.48
Puerto	80
Vulnerabilidades detectadas	
<pre> vulners: cpe:/a:apache:http_server:2.4.48: _ CVE-2021-33193 5.0 https://vulners.com/cve/CVE-2021-33193</pre>	

Ilustración 4 Vulnerabilidades detectadas en Apache

2. Resultado de vulnerabilidades

A continuación se expondrán las vulnerabilidades las cuales estén asociadas a la información rescatada en ambos escaneos, cabe resaltar que, aunque las vulnerabilidades se encuentren asociadas a algún registro dentro de NVD, muchas de estas no cuentan con una descripción, puntaje actualizado en la versión CVSS 3.x, vector o información que sirva para conocer de que trata la vulnerabilidad, esta situación se repitió a lo largo de las vulnerabilidades asociadas a los enlaces retornados por los escaneos, por lo que solo se presentara información de las dos vulnerabilidades que presentaron toda la información para llenar la tabla adecuadamente

Notas

- Como se puede evidenciar en el punto anterior, se retornaron enlaces a distintos tipos de vulnerabilidades dentro de la pagina <https://vulners.com/> y cada uno de estos se reviso con el fin de rescatar la mayor cantidad de información, pero lastimosamente no se pudo recatar mucha información.
- Las vulnerabilidades detectadas se generaron mediante la instalación de un servidor apache y demás componentes como FileZilla, debido a que, al momento de escanear la maquina en su estado inicial, no se pudo detectar ninguna vulnerabilidad que sirviera para el análisis y la naturaleza del ejercicio.
- La única vulnerabilidad detectada directamente fue CVE-2021-33193, en cambio la vulnerabilidad CVE-2008-1447 se obtuvo mediante el análisis de la información asociada a la vulnerabilidad VMSA-2008-0014.3 presentada en el siguiente enlace <https://vulners.com/vmware/VMSA-2008-0014.3>

CVE	SCORT 3x	Vector	Descripción (url)	Exploit
2008-1447	6.8 (Medio)	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:H/A:N	El protocolo DNS, implementado en (1) BIND 8 y 9 antes de 9.5.0-P1, 9.4.2-P1 y 9.3.5-P1; (2) DNS de Microsoft en Windows 2000 SP4, XP SP2 y SP3, y Server 2003 SP1 y SP2; y otras implementaciones permiten a los atacantes remotos falsificar el tráfico de DNS a través de un ataque... (Enlace)	Exploit 1 Exploit 2 Exploit 3
2021-33193	7.5 (alto)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N	Un método elaborado enviado a través de HTTP / 2 omitirá la validación y será reenviado por mod_proxy, lo que puede llevar a la división de solicitudes o al envenenamiento de la caché. Este problema afecta a Apache HTTP Server 2.4.17 a 2.4.48. (Enlace)	

Ilustración 5 Vulnerabilidades identificadas

En el siguiente punto se contrarrestarán los resultados del análisis realizado con Nmap mediante el uso de la herramienta para el análisis y gestión de vulnerabilidades Nessus, por lo que se vera como, de forma gráfica, se podrá rescatar información de la maquina objetivo y como esta es enriquecida por parte de la herramienta a emplear.

3. Escaneo de vulnerabilidades con Nessus

Para realizar el escaneo de vulnerabilidades se eligió la herramienta Nessus, esto debido a que, previamente ya se había instalado OpenVAS y se tuvieron muchos problemas con su puesta en marcha, definición de puertos, declaración de objetivos y la manipulación en general de la herramienta. En el caso de Nessus, el proceso de instalación fue muy demorado, esto se deduce que puede ser por la configuración de la máquina. A continuación, se mostrará en marcha la herramienta para el escaneo y la maquina objetivo, la cual tienen en marcha a los servicios de Apache, MySQL, FileZilla y Mercury, mismos servicios empleado en el escaneo de vulnerabilidades desarrollado con NMAP en los puntos anteriores:

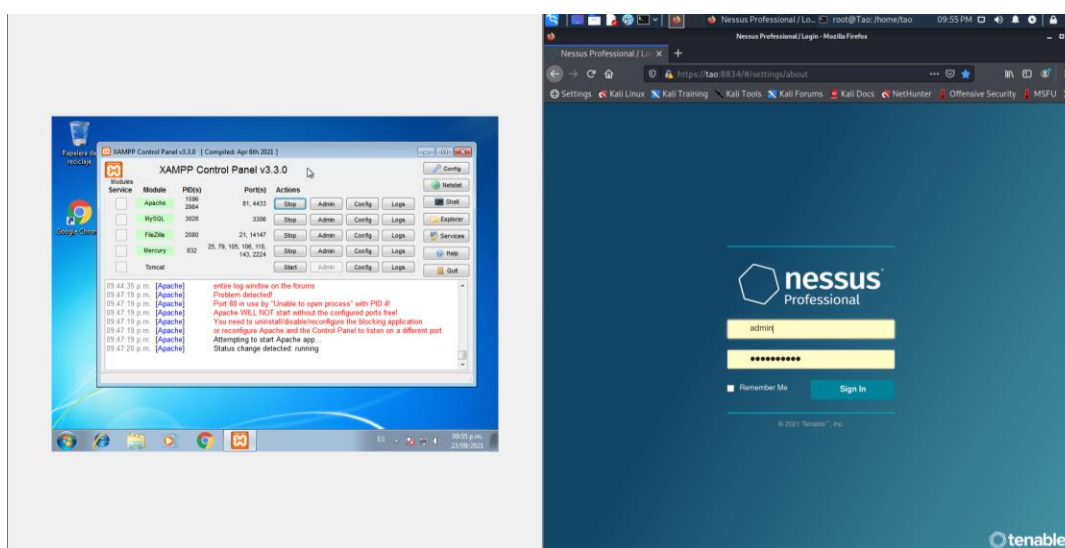


Ilustración 6 Maquina objetivo (izquierda) y maquina atacante (derecha) con Nessus

A continuación, se definirá toda la información y parámetros requeridos para el escaneo de vulnerabilidades, en este caso realizando un escaneo básico de vulnerabilidades. Cabe destacar que, en la siguiente imagen se vera la definición de la IP de la maquina objetivo, pero, en la parte izquierda se puede apreciar como se muestran otros apartados en los cuales se puede definir horarios para realizar el escaneo de vulnerabilidades de los objetivos definidos (Schedule), los puertos a analizar de las maquinas objetivos, el tipo de escaneo que se va a realizar, la forma en que se reportan las vulnerabilidades detectadas y la definición de alteras, entre otros elementos que precisamente ayudan a diferenciar el concepto de escáner y gestor de vulnerabilidades. También se debe observar en la primera imagen como se permite por medio de la opción **Live_result** la cual permitirá obtener en tiempo real información sobre las vulnerabilidades que se generen en la maquina objetivo.

New Scan / Basic Network Scan

[Back to Scan Templates](#)

Settings

Credentials

Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

General Settings

Name

Escaneo basico 1

Description

Escaneo basico de la maquina objetivo

Folder

My Scans

Targets

192.168.0.11

Upload Targets

Add File

Post-Processing

☐ Live Results

Enabling this option will identify potential issues discovered by plugins added during updates without actively scanning targets. Note that this requires the KB to be included in the scan result.

Ilustración 7 Definición de datos del objetivo

Settings

Credentials

Plugins

BASIC

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Scan Type

Default

Default

Scan for known web vulnerabilities

Scan for all web vulnerabilities (quick)

Scan for all web vulnerabilities (complex)

Custom

Ilustración 8 Definición del tipo de escaneo

Settings

Credentials

Plugins

BASIC

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Scan Type

Port scan (all ports)

Port scan (common ports)

Port scan (all ports)

Custom

Use fast network discovery

Port Scanner Settings:

Scan all ports (1-65535)

Ilustración 9 Definición de los puertos a escanear

Después de definir toda la información del escaneo y la máquina objetivo, se nos redirige a la página donde se encuentran los escaneos definidos, para iniciar el escaneo se debe dar clic en el botón de play en la parte derecha del escaneo:

My Scans

Import

New Folder

New Scan

Search Scans 1 Scan

<input type="checkbox"/>	Name	Schedule	Last Modified
<input type="checkbox"/>	Escaneo basico 1	On Demand	N/A

Ilustración 10 Escaneo creado

A continuación, se muestra el escaneo en ejecución:

<input type="checkbox"/>	Name	Schedule	Last Modified
<input type="checkbox"/>	Escaneo basico 1	On Demand	Today at 10:17 PM

Ilustración 11 Escaneo en operación

Al ingresar al escaneo, nos podemos encontrar con la información que el escaneo va recuperando, en el cual se clasifica la vulnerabilidad, se grafica en un grafico de torta el resultado de las vulnerabilidades y se agrupan con relación a familias definidas por Nessus con relación a los componentes y las actividades que estos desempeñan.

Escaneo basico 1

Configure

Back to My Scans

Hosts 1

Vulnerabilities 3

History 1

Filter

Search Vulnerabilities

3 Vulnerabilities

Sev	Name	Family	Count
INFO	Nessus SYN scanner	Port scanners	26
INFO	DCE Services Enumeration	Windows	8
INFO	SMB (Multiple Issues)	Windows	4

Scan Details

Policy:

Basic Network Scan

Status:

Running

Severity Base:

CVSS v3.0


Scanner:

Local Scanner

Start:

Today at 10:17 PM

Vulnerabilities



- Critical
- High
- Medium
- Low
- Info

Ilustración 12 Inicio del escaneo y análisis de vulnerabilidades

El proceso de escaneo y análisis puede variar con relación a los puertos que se definan y el tipo de escaneo definido, en este caso, el escaneo y análisis de vulnerabilidades se demora 9 minutos, al finalizar se obtuvieron 46 vulnerabilidades las cuales fueron un 76% de tipo informativo, es decir, que obtuvieron información que le sirva al atacante o al responsable de la seguridad de la máquina objetivo. Por otro lado, el 24% restante presentan vulnerabilidades desde leves hasta críticas, relacionadas con componentes como el servidor Telnet, Apache y actualizaciones requeridas por parte del sistema.

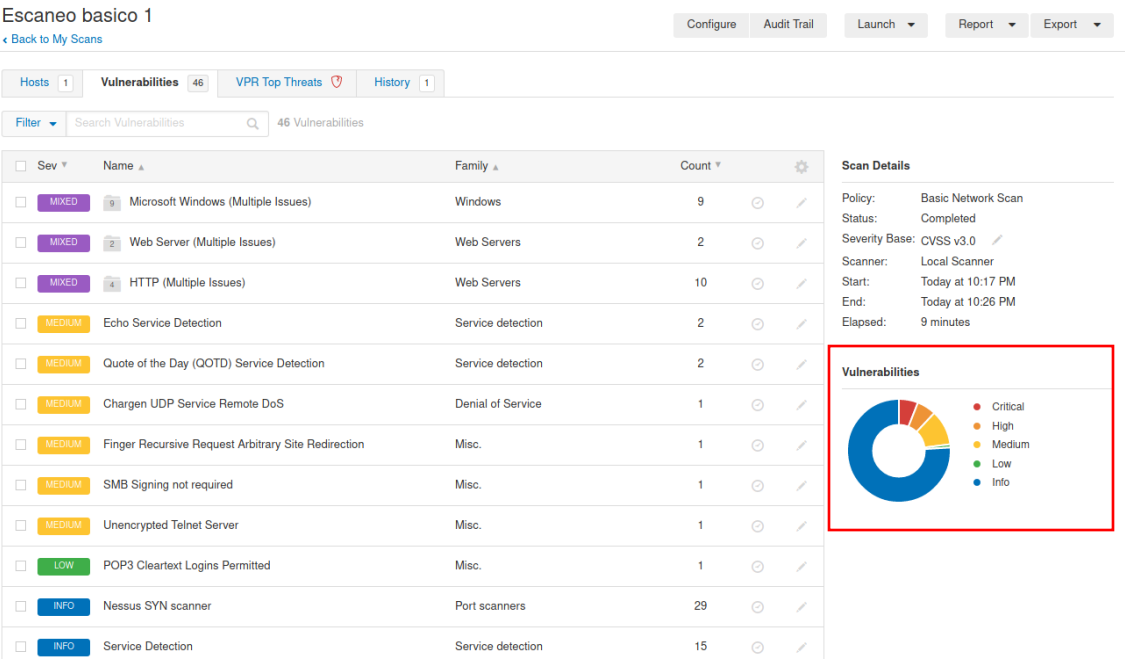


Ilustración 13 Listado de las vulnerabilidades detectadas

Por otro lado, Tenable también nos entrega un listado en el cual se clasifican las vulnerabilidades detectadas de nivel crítico a bajo:

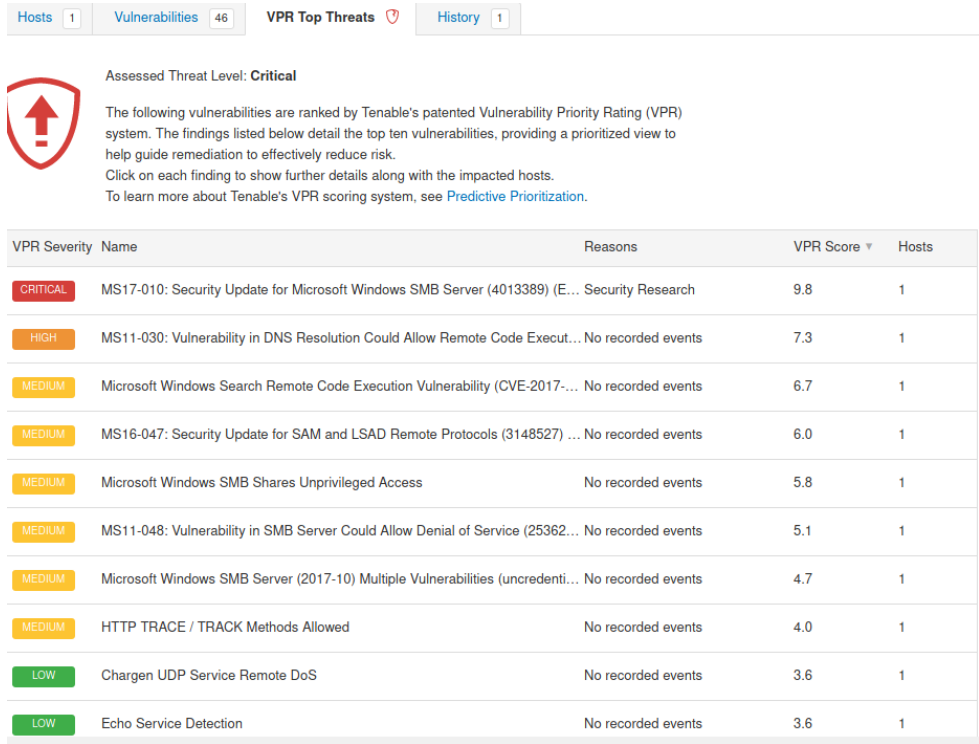


Ilustración 14 Listado de vulnerabilidades de Tenable

Para profundizar en cada una de las vulnerabilidades, solo requeriremos acceder a cada una de estas, y podremos ver una descripción de la vulnerabilidad y enlaces que nos ayuden a analizar y recatar más información:

HIGH Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (unauthenticated check)

Description
The remote Windows host is affected by the following vulnerabilities :

- A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server. (CVE-2017-11780)
- A denial of service vulnerability exists in the Microsoft Server Block Message (SMB) when an attacker sends specially crafted requests to the server. An attacker who exploited this vulnerability could cause the affected system to crash. To attempt to exploit this issue, an attacker would need to send specially crafted SMB requests to the target system. Note that the denial of service vulnerability would not allow an attacker to execute code or to elevate their user rights, but it could cause the affected system to stop accepting requests. The security update addresses the vulnerability by correcting the manner in which SMB handles specially crafted client requests. (CVE-2017-11781)

Note that Microsoft uses AC:H for these two vulnerabilities. This could mean that an exploitable target is configured in a certain way that may include that a publicly accessible file share is available and share enumeration is allowed for anonymous users.

Solution
Microsoft has released a set of patches for Windows 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016.

See Also
<http://www.nessus.org/u?72a4ce73>
<http://www.nessus.org/u?742adf289>

Output
No output recorded.

Plugin Details

Severity:	High
ID:	103876
Version:	1.5
Type:	remote
Family:	Windows
Published:	October 17, 2017
Modified:	November 12, 2019

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score: 7.0
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C
CVSS v3.0 Temporal Score: 6.1
CVSS v2.0 Base Score: 6.8
CVSS v2.0 Temporal Score: 5.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P
CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:O/RC:C

Vulnerability Information
CPE: cpe:/o:microsoft:windows

Ilustración 15 Muestra de una vulnerabilidad

En la anterior imagen se expone un conjunto de vulnerabilidades asociados con mucha información que ayuda a describir de mejor manera el resultado, además de que se asocia directamente con la descripción de vulnerabilidades en NVD, tal cual como se muestra a continuación:

CVE-2017-11780 Detail

Current Description

The Server Message Block 1.0 (SMBv1) on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, allows a remote code execution vulnerability when it fails to properly handle certain requests, aka "Windows SMB Remote Code Execution Vulnerability".

[+View Analysis Description](#)

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score: 7.0 HIGH** **Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L**

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

Ilustración 16 Ejemplo de una vulnerabilidad en NDA

Curiosidad: con base a los dos escaneos realizados, uno con NMAP y otro con Nessus, y los resultados de estos se puede evidenciar como el proceso de documentación de las vulnerabilidades ha mejorado al paso del tiempo, ya que, vulnerabilidades detectadas hace más de 10 años, no cuentan con mucha información en cambio, vulnerabilidades detectadas en los últimos 5 años cuentan con más información y recursos.

Con base a las vulnerabilidades detectadas, se revisó cada una de las vulnerabilidades detectadas de nivel crítico, alto y medio, encontrando la siguiente información bajo los criterios empleados en el punto anterior:

CVE	SCORT 3x	Vector	Descripción (url)	Exploit
2017-8543	9.8 (Critico)	CVSS:3.0/AV:N/AC: L/PR:N/UI:N/S:U/C: H/I:H/A:H	Una gran cantidad de versiones de Windows permiten al atacante tomar el control del sistema por medio de un fallo en Windows Search. (Enlace)	
2017-11780	7.0 (Alto)	CVSS:3.0/AV:N/AC: H/PR:N/UI:N/S:U/C: H/I:L/A:L	El servidor Message Block 1.0 presente en varias versiones de Windows permite la ejecución remota de código al momento de fallar en la recepción de ciertas peticiones(Enlace)	
2017-11781	7.5 (Alto)	CVSS:3.0/AV:N/AC: L/PR:N/UI:N/S:U/C: N/I:N/A:H	El servidor Message Block 1.0 presente en varias versiones de Windows permite la negación de servicios en el sistema al momento de que se envíen peticiones diseñadas para este proposito (Enlace)	
2017-0143	8.1 (Alto)	CVSS:3.0/AV:N/AC: H/PR:N/UI:N/S:U/C: H/I:H/A:H	El servidor SMBv1 que se encuentra presente en varias versiones de Windows permite la ejecución remota	Exploit 1 Exploit 2 Exploit 3

			de código por medio de paquetes diseñados para este propósito (Enlace)	
2017-0144	8.1 (Alto)	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	El servidor SMBv1 que se encuentra presente en varias versiones de Windows permite la ejecución remota de código por medio de paquetes diseñados para este propósito (Enlace)	Exploit 1 Exploit 2 Exploit 3 Exploit 4
2017-0145	8.1 (Alto)	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	El servidor SMBv1 que se encuentra presente en varias versiones de Windows permite la ejecución remota de código por medio de paquetes diseñados para este propósito (Enlace)	Exploit 1 Exploit 2
2017-0146	8.1 (Alto)	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	El servidor SMBv1 que se encuentra presente en varias versiones de Windows permite la ejecución remota de código por medio de paquetes diseñados para este propósito (Enlace)	Exploit 1 Exploit 2 Exploit 3
2016-0128	6.8 (Medio)	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N	Los protocolos SAM y LSAD implementados en varias versiones de Windows no establece un canal RPC, de modo tal se permite al atacante realizar ataques de hombre en el medio (Enlace)	

Conclusiones del uso de Nessus y Nmap

- El uso de Nmap entrega muy poca información con relación a las vulnerabilidades de un objetivo, por lo que se aconseja usar esta herramienta solo para un reconocimiento del objetivo y la red.
- Con el uso de Nmap se requiere de un proceso de análisis mucho más profundo de la información que entrega esta herramienta.
- El uso de Nessus facilita mucho el proceso de escaneo y análisis de vulnerabilidades, ya que retorna mucha más información que Nmap, recalcando la diferencia entre un gestor de vulnerabilidades y un escáner de vulnerabilidades.
- Nessus, al ser un gestor de vulnerabilidades, se encuentra dotado de una multitud de características que son de gran utilidad en el proceso de detectar vulnerabilidades, no solo de una máquina, sino de un conjunto de máquinas y todo por medio de una interfaz gráfica que facilita toda la administración de vulnerabilidades.

4. Payload y Exploit

Continuando con el manejo de conceptos relacionados con los ataques de ciberseguridad, se debe tener presente la existencia de los conceptos de Payload y Exploit, los cuales están relacionados entre sí y con el concepto de vulnerabilidad. Recordemos que, una vulnerabilidad es cualquier falla en el diseño, implementación o manipulación de un sistema, es decir, es cualquier elemento o actividad dentro de un sistema resultado de su uso o despliegue que pone en riesgo al sistema. De modo tal, al existir una vulnerabilidad en un sistema, se genera una brecha que puede ser explotada y/o aprovechada por alguien con malas intenciones, en este punto es donde entra el concepto de Exploit, el cual se describirá a continuación y se recabará con información que ayude a describirlo lo mejor posible.

Exploit

Para poder aprovechar una vulnerabilidad primero que todo debemos saber que vulnerabilidades existen, que agujeros de seguridad son los que nos posibilitarán realizar las acciones que requiramos en el objetivo, por lo que, al momento de abordar la definición de exploit se debe tener en cuenta que será una secuencia de instrucciones o un programa que permitirá el aprovechamiento de una vulnerabilidad detectada en un sistema. Por ende, la creación de cualquier exploit se basará en el previo análisis de las vulnerabilidades existentes, sin conocer el componente que posee dicha vulnerabilidad no se podrá desplegar un exploit que la explote apropiadamente. Un ejemplo práctico es el de un ladrón: para entrar a una casa, este ladrón requiere estudiar los puntos débiles de la casa, por ejemplo, ver si hay cámaras de seguridad, el comportamiento y las actividades de quienes viven en la casa y lugares que le permitan acceder a la casa, precisamente, al terminar su análisis, detecta que, a cierta hora de la noche, alguien dentro de la casa deja abierta una ventana del segundo piso de la casa, por lo que usará una escalera para entrar al lugar. Este ejemplo, convirtiéndolo en una analogía con relación a un ataque a un sistema informático, se entiende que la casa es el sistema al cual el

atacante quiere entrar, el estudio que realiza el ladrón es el análisis de vulnerabilidades que podemos realizar con herramientas como NMAP, y la escalera será el exploit, por lo que se puede determinar que un exploit como tal será el medio que permita aprovechar una vulnerabilidad, será el canal que abra esa brecha de seguridad para que sea usada como el ciberdelincuente la requiera (Fernández, 2015; Nica Latto & Avast, 2020).

Con base a lo explicado anteriormente, se puede reforzar el hecho de como los exploits como secuencias de código o software malicioso, puede permitir el acceso de los ciber atacantes de distintas formas, desde los ataques dirigidos a un objetivo en específico, ejemplo muy conocido y mencionado en la primera actividad de este curso es el caso de Stuxnet, el cual se enfocó en la vulnerabilidad de las maquinas empleadas en los procesos nucleares usando un exploit especificado para este entorno de ataque, también existen los exploits incrustados en paginas web y archivos, en este caso la maquina victima es testeada por medio de los exploits incrustados a modo tal, al detectar los exploits que hayan podido explotar una vulnerabilidad, se continúe con el ataque, apegado a este tipo de ataques, existen exploits que pueden circular en la red y los cuales no requieren de un vector o actividad que le permita acceder a la maquina víctima, estos exploits se pueden ver en redes de organizaciones en los cuales, el exploit va como un ratón a través de la red detectando y atacando las maquinas en donde haya podido encontrar las vulnerabilidades a las cuales está destinado explotar (Castaneda, 2015).

Por último, antes de hablar sobre el concepto de payload, se van a definir los dos tipos de exploits existentes, debido a la importancia que tienen reconocer las amenazas existentes en el ámbito de la seguridad de los sistemas (ESET, 2014; Nica Latto & Avast, 2020):

- **Exploits conocidos:** a medida que se detectan y evidencian vulnerabilidades, a la par de puede ver como existe constancia de los exploits relacionados con dichas vulnerabilidades, este tipo de exploits son quizá los menos peligrosos ya que, al existir evidencia de su existencia y conocer la o las vulnerabilidades que permite explotar a los responsables de la seguridad de los sistemas se le facilita el prevenir sufrir algún ataque que emplee las vulnerabilidades del sistema.
- **Exploits desconocidos:** a contracara del tipo anterior de exploits, este tipo de exploits son todos aquellos que son desarrollados y ejecutados justo el mismo día en que se detecta la vulnerabilidad de un sistema que se haya puesto en operación en ese mismo día, o que simplemente explotan vulnerabilidades de un sistema las cuales solo han sido detectadas por el atacante, de modo tal, se deja al os usuarios y responsables del sistema atacado en una desventaja frente al atacante ya que este tiene conocimiento de una brecha de seguridad y tiene la herramienta que le permita aprovecharla.

Payload

Con el concepto de exploit definido se puede abordar finalmente el concepto de payload o carga útil, el cual se define como la secuencia de código la cual se ejecuta o activa al momento de que se aprovecha la vulnerabilidad por medio de un exploit, de modo tal, aquí un payload será

el encargado del aprovechamiento de la vulnerabilidad que previamente ya había sido explotada (Catoira, 2013; Rizaldos, 2018). Continuando con el ejemplo del ladrón, se puede decir que el mismo ladrón es la representación del payload ya que será el encargado de ejecutar las tareas, como el robo de dinero o objetos, que se encuentran en el objetivo, la casa. Los payloads a su vez puede ser usados por varios exploits, al igual que cada exploit puede usar uno o varios payloads los cuales se apoyarán en la vulnerabilidad para realizar el ataque que requiera el ciberdelincuente. A continuación, se expondrán algunos de los payloads más conocidos (Offensive Security, 2019):

- **Meterpreter:** es uno de los payloads más conocidos debido a su capacidad de adaptarse a distintos entornos y poder ejecutarse sin ser percibido por parte del sistema (DragonJAR, 2010).
- **PassiveX:** dentro de Windows existe un plugin llamado ActiveX el cual permite la creación de programas y el despliegue de estos en aplicaciones distribuidas, debido a su estructura es que este payload aprovecha este plugin permitiéndole evadir el firewall dentro del sistema de la maquina objetivo.
- **Inline:** se considera como uno de los payloads más completos al tener código de consola o Shell enfocado en una tarea, de modo tal no se requiere realizar ninguna carga o combinación con otros payloads.

Relación entre los conceptos

Para resumir la información previamente expuesta, se debe definir que al existir una vulnerabilidad se desarrollan herramientas que permitan su explotación, en dichas herramientas se incluye código que será el encargado del aprovechamiento y la ejecución de las tareas destinadas para el ataque, por lo tanto, los exploits por si solos son capaces de permitir la posterior ejecución de las instrucciones definidas en el payload. A continuación, se va a ejemplificar el ejemplo del ladrón de modo tal se pueda representar de forma grafica la relación entre los conceptos expuestos (Rizaldos, 2018).



Ilustración 17 Ejemplo de payload y exploit



En la anterior imagen se expone como el exploit, siendo la escalera, posibilitara al delincuente ejecutar o realizar las actividades definidas en el ataque apoyándose en la previa explotación y definición de la vulnerabilidad, por lo que, como se muestra en la primera imagen a la derecha, de nada sirve tener un exploit si este no posee el payload que le permita generar el daño o si el exploit desarrollado trata de explotar una vulnerabilidad (la ventana) que ya fue parcheada, o como en la ultima imagen a la derecha en donde se ejemplifica el hecho de que los exploit deben estar hechos acorde a la vulnerabilidad para posibilitar su explotación y uso en el ataque.

Bibliografía

- Castaneda, A. (2015). *IDENTIFICACION Y EXPLOTACION DE VULNERABILIDADES EN APLICACIONES WEB DE UN ENTORNO ACADEMICO*.
<https://repository.unimilitar.edu.co/bitstream/handle/10654/16513/CastanedaSuarezAndresFernando2017.pdf?sequence=2&isAllowed=y>
- Catoira. (2013). Pruebas de penetración para principiantes: explotando una vulnerabilidad con Metasploit Framework | . *Revista .Seguridad*, 1(19).
<https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetración-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra>
- DragonJAR. (2010, June 14). *Manual en español de Meterpreter* . DragonJAR.
<https://www.dragonjar.org/manual-en-espanol-de-meterpreter.xhtml>
- ESET. (2014, October 9). *¿Sabes qué es un exploit y cómo funciona?* WeLiveSecurity.
<https://www.welivesecurity.com/la-es/2014/10/09/exploits-que-son-como-funcionan/>
- Fernández, C. (2015). *Definición de metodología para el descubrimiento del Zero Days* [UNIVERSIDAD DE ALCALÁ].
https://ebuah.uah.es/dspace/bitstream/handle/10017/22752/TFG_Fernández_Rivas_2015.pdf?sequence=1&isAllowed=y#:~:text=Exploit es un fragmento de,comportamiento no deseado del mismo.
- Nica Latto, & Avast. (2020, September 29). *¿Qué es un exploit de ordenador? Definición de exploit* . Avast. <https://www.avast.com/es-es/c-exploits>
- Offensive Security. (2019, August 16). *Payload Types - Metasploit Unleashed*. Offensive Security. <https://www.offensive-security.com/metasploit-unleashed/payload-types/>
- Rizaldos, H. (2018, October 24). *Qué es un Payload*. OpenWebinars.

<https://openwebinars.net/blog/que-es-payload/>

Tabla de ilustraciones

Ilustración 1 Identificación del objetivo con NMAP	2
Ilustración 2 identificación de dirección IP de la maquina objetivo	3
Ilustración 3 Vulnerabilidades detectadas en FileZilla	10
Ilustración 4 Vulnerabilidades detectadas en Apache	10
Ilustración 5 Vulnerabilidades identificadas	11
Ilustración 6 Maquina objetivo (izquierda) y maquina atacante (derecha) con Nessus	12
Ilustración 7 Definicion de datos del objetivo	13
Ilustración 8 Definición del tipo de escaneo.....	13
Ilustración 9 Definición de los puertos a escanear	13
Ilustración 10 Escaneo creado	14
Ilustración 11 Escaneo en operación.....	14
Ilustración 12 Inicio del escaneo y análisis de vulnerabilidades	14
Ilustración 13 Listado de las vulnerabilidades detectadas	15
Ilustración 14 Listado de vulnerabilidades de Tenable	15
Ilustración 15 Muestra de una vulnerabilidad	16
Ilustración 16 Ejemplo de una vulnerabilidad en NDA	16
Ilustración 17 Ejemplo de payload y exploit.....	21