

Verificación de la existencia de un elemento de protección perimetral.

Práctica 3 en equipo.

Miguel Marcos Pérez y Gonzalo Tudela Chavero

ÍNDICE DE CONTENIDOS

INTRODUCCION	1
EQUIPO	1
OBJETIVO	1
PRUEBAS.....	2
Ping a www.hackthissite.org	2
Nslookup a hackthissite.org	2
NMAP --top-ports 10 al rango 100-104.....	3
Pruebas realizadas en casa: Análisis del tráfico y anomalías.....	4
Pruebas realizadas en clase: Análisis del trafico y anomalías.....	5
NMAP --scan-delay	5
NMAP final	6
Pruebas HPING3 con flag SYN.....	7
Pruebas HPING3 con flag ACK.....	8
Comprobación de la existencia de un WAF (Web Application Firewall).....	9
CONCLUSIONES	10
De las pruebas:	10
Académicas:.....	10

ÍNDICE DE FIGURAS

Ilustración 1 - Ping a www.hackthissite.org	2
Ilustración 2 - Consulta nslookup.....	2
Ilustración 3 - NMAP de las 4 direcciones IPv4 en las que se aloja el sitio.....	3
Ilustración 4 - NMAP filtered puerto 21.....	4
Ilustración 5 - NMAP filtered puerto 21, RST, ACK 20 segundos más tarde.....	4
Ilustración 6 - Pruebas mediante hping3, telnet y ssh, siempre 20 segundos hasta el RST, ACK.....	4
Ilustración 7 - Trafico generado por NMAP solo indicando el puerto.....	5
Ilustración 8 - Tabla comparativa comunicación default de NMAP.....	5
Ilustración 9 - Resultado de NMAP con --scan-delay 3s	5
Ilustración 10 - Nmap final que muestra el verdadero estado del puerto 22.....	6
Ilustración 11 - HPING3 de los puertos explorados por nmap mediante flag SYN.....	7
Ilustración 12 - HPING3 envió de paquetes con flag ACK.....	8
Ilustración 13 - Uso de WAFW00F para la detección de WAF en una página de ejemplo con resultado positivo.....	9
Ilustración 14 - WAFW00F en uno de los hosts que albergan hackthissite.org	9

INTRODUCCION

Una de las primeras tareas durante una prueba de intrusión a un servidor es comprobar si este cuenta con un firewall como elemento de protección perimetral. Se realizan las pruebas necesarias que determinen la existencia o no de un firewall, si éste está en el mismo servidor o es una máquina intermedia entre el cliente o el servidor, etc....

La idea de este trabajo grupal es escoger un servidor en Internet, preferiblemente perteneciente a una organización, y realizar las pruebas técnicas con la calidad necesaria para determinar si se encuentra protegido con un firewall, e incluso poder inferir la posible topología de red.

Se realizará un documento donde se detallen las pruebas realizadas: herramientas utilizadas y parámetros empleados, análisis del tráfico de red (se aconseja el uso de filtros en la monitorización de paquetes con Wireshark).

Se realizará una presentación al resto de grupos de una duración máxima de 10 minutos donde se muestre el servidor elegido, pruebas realizadas, resultados obtenidos y conclusiones.

EQUIPO

Crear un equipo de trabajo y darle un nombre. Hay que especificar quiénes forman el grupo.

Nombre del equipo:

Integrantes: Miguel Marcos y Gonzalo Tudela

OBJETIVO

Localizar un servidor web en Internet para determinar si éste cuenta con protección, como por ejemplo un firewall. Envía el servidor web elegido para que otro grupo no pueda utilizarlo.

El host objetivo será:

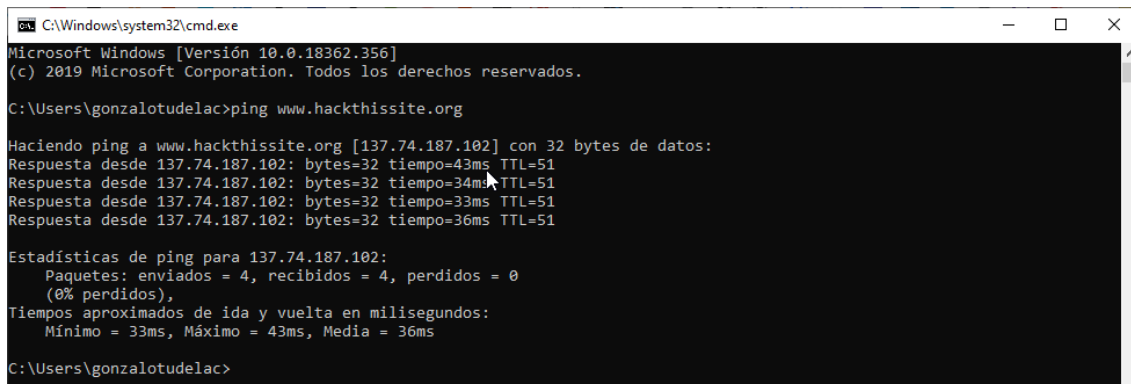
`http://hackthissite.org/`

PRUEBAS

Realiza las pruebas necesarias para determinar la existencia de un firewall o de un WAF (opcional). Para las pruebas, como mínimo, deberán utilizarse herramientas empleadas en test de intrusión o auditorías de red, como son nmap, hping3, telnet, wireshark, e interpretar los resultados que se obtienen. Es necesario realizar diversos escaneos de puertos relacionados con TCP para determinar la presencia o no de un firewall.

Ping a www.hackthissite.org

Queremos saber si tenemos conectividad con la IP de la página, para lo cual lanzamos un ping a la URL.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 10.0.18362.356]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\Users\gonzalotudela>ping www.hackthissite.org

Haciendo ping a www.hackthissite.org [137.74.187.102] con 32 bytes de datos:
Respuesta desde 137.74.187.102: bytes=32 tiempo=43ms TTL=51
Respuesta desde 137.74.187.102: bytes=32 tiempo=34ms TTL=51
Respuesta desde 137.74.187.102: bytes=32 tiempo=33ms TTL=51
Respuesta desde 137.74.187.102: bytes=32 tiempo=36ms TTL=51

Estadísticas de ping para 137.74.187.102:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 33ms, Máximo = 43ms, Media = 36ms

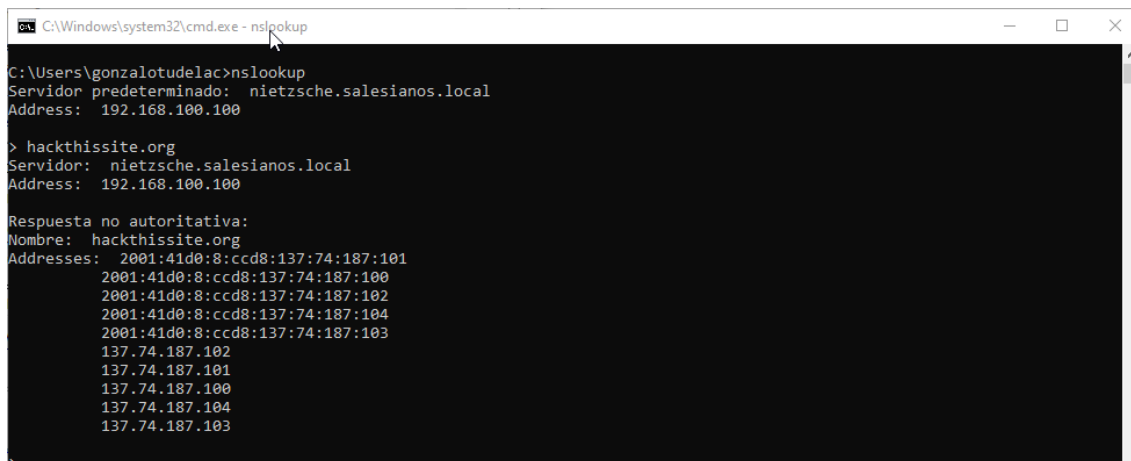
C:\Users\gonzalotudela>
```

Ilustración 1 - Ping a www.hackthissite.org

Nslookup a hackthissite.org

Nos damos cuenta de que la página responde con diferentes IP a los diferentes miembros del equipo, así que consultamos al servidor DNS para que nos diga cuantas IP hay tras ese dominio mediante el comando:

```
nslookup hackthissite.org
```



```
C:\Windows\system32\cmd.exe - nslookup
C:\Users\gonzalotudela>nslookup
Servidor predeterminado: nietsche.salesianos.local
Address: 192.168.100.100

> hackthissite.org
Servidor: nietsche.salesianos.local
Address: 192.168.100.100

Respuesta no autoritativa:
Nombre: hackthissite.org
Addresses: 2001:41d0:8:ccd8:137:74:187:101
          2001:41d0:8:ccd8:137:74:187:100
          2001:41d0:8:ccd8:137:74:187:102
          2001:41d0:8:ccd8:137:74:187:104
          2001:41d0:8:ccd8:137:74:187:103
          137.74.187.102
          137.74.187.101
          137.74.187.100
          137.74.187.104
          137.74.187.103
```

Ilustración 2 - Consulta nslookup.

NMAP --top-ports 10 al rango 100-104.

Una vez que tenemos resueltas las IP que hay tras www.hackthissite.org procedemos a realizar un escaneo de puertos tipo SYN(-sS) pero sin enviar paquetes ICMP(-Pn) utilizando los 10 puertos más utilizados según nmap.org a las IP acabadas en 100 hasta la 104 para ver si obtenemos variedad de estados en las diferentes maquinas.

```
nmap 137.74.187.100-104 --top-ports 10 -Pn -sS
```



```

root@GonKali: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@GonKali:~# nmap 137.74.187.100-104 --top-ports 10 -Pn -sS
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-04 22:48 CEST
Nmap scan report for hackthissite.org (137.74.187.100)
Host is up (0.046s latency).

PORT      STATE      SERVICE
21/tcp    filtered  ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
25/tcp    filtered  smtp
80/tcp    open      http
110/tcp   filtered  pop3
139/tcp   filtered  netbios-ssn
443/tcp   open      https
445/tcp   filtered  microsoft-ds
3389/tcp  filtered  ms-wbt-server

Nmap scan report for hackthissite.org (137.74.187.101)
Host is up (0.048s latency).

PORT      STATE      SERVICE
21/tcp    filtered  ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
25/tcp    filtered  smtp
80/tcp    open      http
110/tcp   filtered  pop3
139/tcp   filtered  netbios-ssn
443/tcp   open      https
445/tcp   filtered  microsoft-ds
3389/tcp  filtered  ms-wbt-server

Nmap scan report for hackthissite.org (137.74.187.102)
Host is up (0.048s latency).

PORT      STATE      SERVICE
21/tcp    filtered  ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
25/tcp    filtered  smtp
80/tcp    open      http
110/tcp   filtered  pop3
139/tcp   filtered  netbios-ssn
443/tcp   open      https
445/tcp   filtered  microsoft-ds
3389/tcp  filtered  ms-wbt-server

Nmap scan report for hackthissite.org (137.74.187.103)
Host is up (0.038s latency).

PORT      STATE      SERVICE
21/tcp    filtered  ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
25/tcp    filtered  smtp
80/tcp    open      http
110/tcp   filtered  pop3
139/tcp   filtered  netbios-ssn
443/tcp   open      https
445/tcp   filtered  microsoft-ds
3389/tcp  filtered  ms-wbt-server

Nmap scan report for hackthissite.org (137.74.187.104)
Host is up (0.047s latency).

PORT      STATE      SERVICE
21/tcp    filtered  ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
25/tcp    filtered  smtp
80/tcp    open      http
110/tcp   filtered  pop3
139/tcp   filtered  netbios-ssn
443/tcp   open      https
445/tcp   filtered  microsoft-ds
3389/tcp  filtered  ms-wbt-server

Nmap done: 5 IP addresses (5 hosts up) scanned in 3.55 seconds
root@GonKali:~#

```

Ilustración 3 - NMAP de las 4 direcciones IPv4 en las que se aloja el sitio.

En la ilustración 3 podemos ver que las 3 máquinas muestran el mismo comportamiento para los puertos explorados.

Pruebas realizadas en casa: Análisis del tráfico y anomalías.

Procedemos a comprobar el comportamiento de NMAP mediante la monitorización del tráfico usando Wireshark utilizando solo el host con la dirección IP acabada en 100, en este caso comprobamos solo el puerto 21, estas pruebas se realizaron desde la conexión de casa.

```
nmap 137.74.187.100 -p 21 -sS -Pn
```

Obtenemos el siguiente resultado:

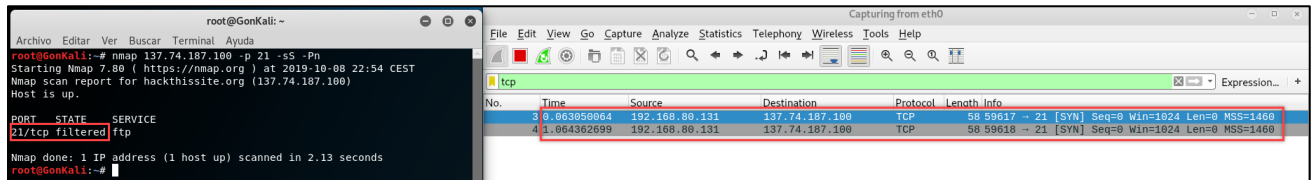


Ilustración 4 - NMAP filtered puerto 21.

Pero al cabo de 20 segundos se reciben 2 paquetes desde el puerto 21 del destino con los flag RST, ACK.

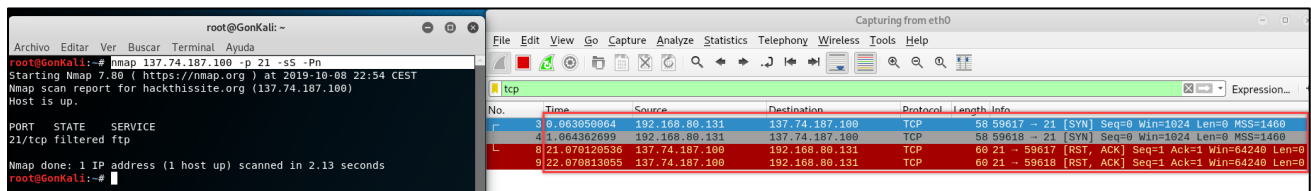


Ilustración 5 - NMAP filtered puerto 21, RST, ACK 20 segundos más tarde.

Realizamos otras pruebas intentando establecer conexión mediante telnet y ssh tanto en el puerto 21 como el 22, obteniendo conexión refused (rechazada) pero siempre con 20s de retardo.

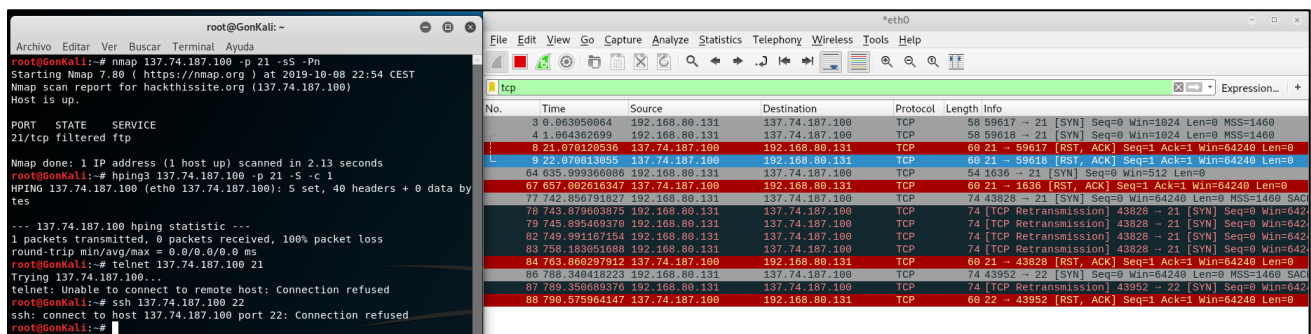


Ilustración 6 - Pruebas mediante hping3, telnet y ssh, siempre 20 segundos hasta el RST, ACK.

Pruebas realizadas en clase: Análisis del trafico y anomalías.

Esta vez nos aseguramos de ver todo excepto el tráfico que no nos interesa mediante el filtro siguiente:

```
!icmpv6 && !udp && !arp && !igmp
```

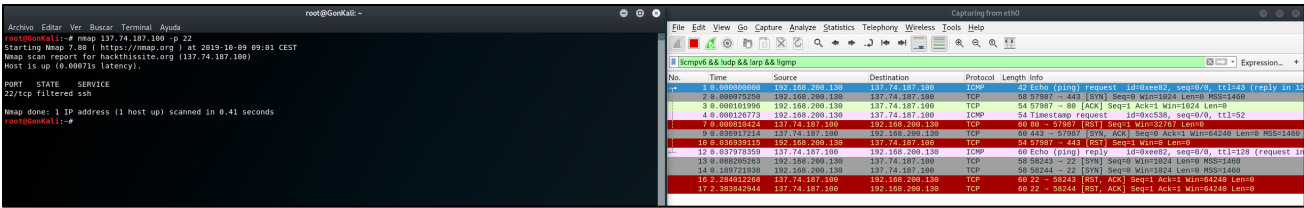


Ilustración 7 - Trafico generado por NMAP solo indicando el puerto.

Tabla explicativa de la comunicación realizada por NMAP.

Peticiones NMAP (default) a puerto 22	Respuestas de hackthissite.org
ICMP tipo ECHO	ICMP tipo REPLY
ICMP tipo TIMESTAMP	-
SYN a 443	SYN + ACK a puerto origen
ACK a 80	RST a puerto origen
SYN a 22 (2 envíos)	RST + ACK (2 respuestas con 2 segundos de delay)

Ilustración 8 - Tabla comparativa comunicación default de NMAP.

NMAP --scan-delay

Ahora indicamos a NMAP que espere unos segundos para que tenga en cuenta las respuestas con delay del objetivo y este cambia el estado para el puerto a CLOSED, lo que indica que hay una contramedida para intentar ocultar el estado del puerto 22 como filtered (sin respuesta) cuando en realidad se están denegando las conexiones (closed) de forma activa como se pudo ver mediante los comandos ssh y telnet en la Ilustración 6 - Pruebas mediante hping3, telnet y ssh, siempre 20 segundos hasta el RST, ACK.

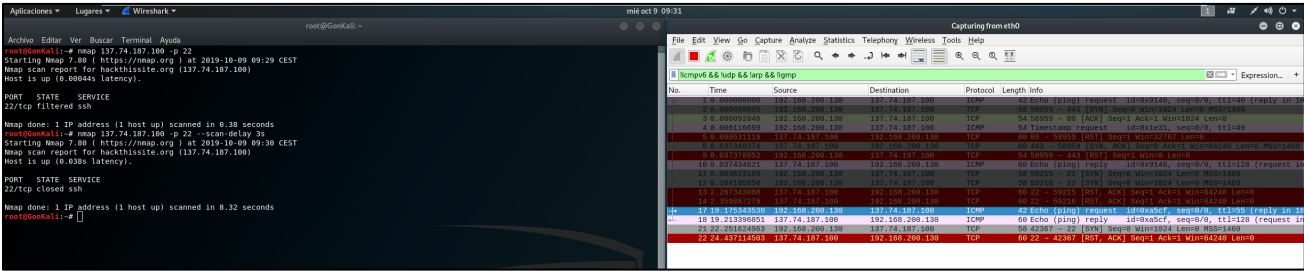


Ilustración 9 - Resultado de NMAP con --scan-delay 3s

Cuando se especifica que NMAP debe esperar 3 segundos podemos ver como el resultado de cada mensaje es más ordenado además de no producirse el envío de los SYN y ACK a los puertos 443 y 80 respectivamente.

NMAP final

Para finalizar las pruebas con nmap utilizaremos el siguiente comando:

```
Nmap 137.74.187.100 - -top-ports 10 - -scan-delay 3s -Pn -sS -r
```

Este comando analizara los 10 puertos mas escaneados con un retraso de 3 segundos sin utilizar paquetes ICMP (-Pn) y analizando los puertos en orden de menor a mayor (-r).

Podemos observar como ahora el puerto 22 aparece como closed lo que podría indicar que se ha tratado de ocultar un puerto activo a los escaneos con nmap.

The screenshot displays a terminal window on a Kali Linux system. The terminal shows the execution of the Nmap command: `nmap 137.74.187.100 --top-ports 10 --scan-delay 3s -Pn -sS -r`. The output indicates that the host is up and provides a list of scanned ports. The ports listed are: 21/tcp (filtered ftp), 22/tcp (closed ssh), 23/tcp (filtered telnet), 25/tcp (filtered smtp), 80/tcp (open http), 110/tcp (filtered pop3), 139/tcp (filtered netbios-ssn), 443/tcp (open https), and 3389/tcp (filtered ms-wbt-server). The scan took 65.94 seconds. To the right of the terminal, a Wireshark packet capture window is open, showing a list of captured packets. The packets include SYN, RST, and ACK packets, with the RST packet (No. 60) specifically showing a reset sequence, which is consistent with the 'closed' state of port 22.

Ilustración 10 - Nmap final que muestra el verdadero estado del puerto 22.

Pruebas HPING3 con flag SYN.

```
hping3 137.74.187.100 -c 1 -S -p n°puerto
```

```

root@GonKali: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@GonKali:~# hping3 137.74.187.100 -c 1 -S -p 21
HPING 137.74.187.100 (eth0 137.74.187.100): S set, 40 headers + 0 data bytes

--- 137.74.187.100 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@GonKali:~# hping3 137.74.187.100 -c 1 -S -p 22
HPING 137.74.187.100 (eth0 137.74.187.100): S set, 40 headers + 0 data bytes

--- 137.74.187.100 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@GonKali:~# hping3 137.74.187.100 -c 1 -S -p 23
HPING 137.74.187.100 (eth0 137.74.187.100): S set, 40 headers + 0 data bytes

--- 137.74.187.100 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@GonKali:~# hping3 137.74.187.100 -c 1 -S -p 25
HPING 137.74.187.100 (eth0 137.74.187.100): S set, 40 headers + 0 data bytes

--- 137.74.187.100 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@GonKali:~# hping3 137.74.187.100 -c 1 -S -p 80
HPING 137.74.187.100 (eth0 137.74.187.100): S set, 40 headers + 0 data bytes
len=46 ip=137.74.187.100 ttl=128 id=11894 sport=80 flags=SA seq=0 win=64240 rtt=47.9 ms

--- 137.74.187.100 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 47.9/47.9/47.9 ms
root@GonKali:~# hping3 137.74.187.100 -c 1 -S -p 110
HPING 137.74.187.100 (eth0 137.74.187.100): S set, 40 headers + 0 data bytes

--- 137.74.187.100 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@GonKali:~# hping3 137.74.187.100 -c 1 -S -p 139
HPING 137.74.187.100 (eth0 137.74.187.100): S set, 40 headers + 0 data bytes

--- 137.74.187.100 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@GonKali:~# hping3 137.74.187.100 -c 1 -S -p 443
HPING 137.74.187.100 (eth0 137.74.187.100): S set, 40 headers + 0 data bytes
len=46 ip=137.74.187.100 ttl=128 id=11898 sport=443 flags=SA seq=0 win=64240 rtt=39.9 ms

--- 137.74.187.100 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 39.9/39.9/39.9 ms
root@GonKali:~# hping3 137.74.187.100 -c 1 -S -p 445
HPING 137.74.187.100 (eth0 137.74.187.100): S set, 40 headers + 0 data bytes

--- 137.74.187.100 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@GonKali:~# hping3 137.74.187.100 -c 1 -S -p 3389
HPING 137.74.187.100 (eth0 137.74.187.100): S set, 40 headers + 0 data bytes

--- 137.74.187.100 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@GonKali:~#

```

Ilustración 11 - HPING3 de los puertos explorados por nmap mediante flag SYN.

Interpretamos de la ilustración 4 que solamente los puertos 80 y 443 responden al *handshake* por lo que se puede decir que están abiertos.

Pruebas HPING3 con flag ACK.



```
root@GonKali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@GonKali:~# hping3 137.74.187.100 -c 1 -A -p 21
HPING 137.74.187.100 (eth0 137.74.187.100): A set, 40 headers + 0 data bytes
len=46 ip=137.74.187.100 ttl=128 id=11909 sport=21 flags=R seq=0 win=32767 rtt=7.9 ms

--- 137.74.187.100 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 7.9/7.9/7.9 ms
root@GonKali:~# hping3 137.74.187.100 -c 1 -A -p 22
HPING 137.74.187.100 (eth0 137.74.187.100): A set, 40 headers + 0 data bytes
len=46 ip=137.74.187.100 ttl=128 id=11910 sport=22 flags=R seq=0 win=32767 rtt=3.9 ms

--- 137.74.187.100 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 3.9/3.9/3.9 ms
root@GonKali:~# hping3 137.74.187.100 -c 1 -A -p 23
HPING 137.74.187.100 (eth0 137.74.187.100): A set, 40 headers + 0 data bytes
len=46 ip=137.74.187.100 ttl=128 id=11911 sport=23 flags=R seq=0 win=32767 rtt=7.9 ms

--- 137.74.187.100 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 7.9/7.9/7.9 ms
root@GonKali:~# hping3 137.74.187.100 -c 1 -A -p 25
HPING 137.74.187.100 (eth0 137.74.187.100): A set, 40 headers + 0 data bytes
len=46 ip=137.74.187.100 ttl=128 id=11912 sport=25 flags=R seq=0 win=32767 rtt=7.9 ms

--- 137.74.187.100 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 7.9/7.9/7.9 ms
root@GonKali:~# hping3 137.74.187.100 -c 1 -A -p 110
HPING 137.74.187.100 (eth0 137.74.187.100): A set, 40 headers + 0 data bytes
len=46 ip=137.74.187.100 ttl=128 id=11913 sport=110 flags=R seq=0 win=32767 rtt=7.9 ms

--- 137.74.187.100 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 7.9/7.9/7.9 ms
root@GonKali:~# hping3 137.74.187.100 -c 1 -A -p 139
HPING 137.74.187.100 (eth0 137.74.187.100): A set, 40 headers + 0 data bytes
len=46 ip=137.74.187.100 ttl=128 id=11914 sport=139 flags=R seq=0 win=32767 rtt=7.9 ms

--- 137.74.187.100 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 7.9/7.9/7.9 ms
root@GonKali:~# hping3 137.74.187.100 -c 1 -A -p 445
HPING 137.74.187.100 (eth0 137.74.187.100): A set, 40 headers + 0 data bytes
len=46 ip=137.74.187.100 ttl=128 id=11915 sport=445 flags=R seq=0 win=32767 rtt=7.9 ms

--- 137.74.187.100 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 7.9/7.9/7.9 ms
root@GonKali:~# hping3 137.74.187.100 -c 1 -A -p 3389
HPING 137.74.187.100 (eth0 137.74.187.100): A set, 40 headers + 0 data bytes
len=46 ip=137.74.187.100 ttl=128 id=11916 sport=3389 flags=R seq=0 win=32767 rtt=3.9 ms

--- 137.74.187.100 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 3.9/3.9/3.9 ms
root@GonKali:~#
```

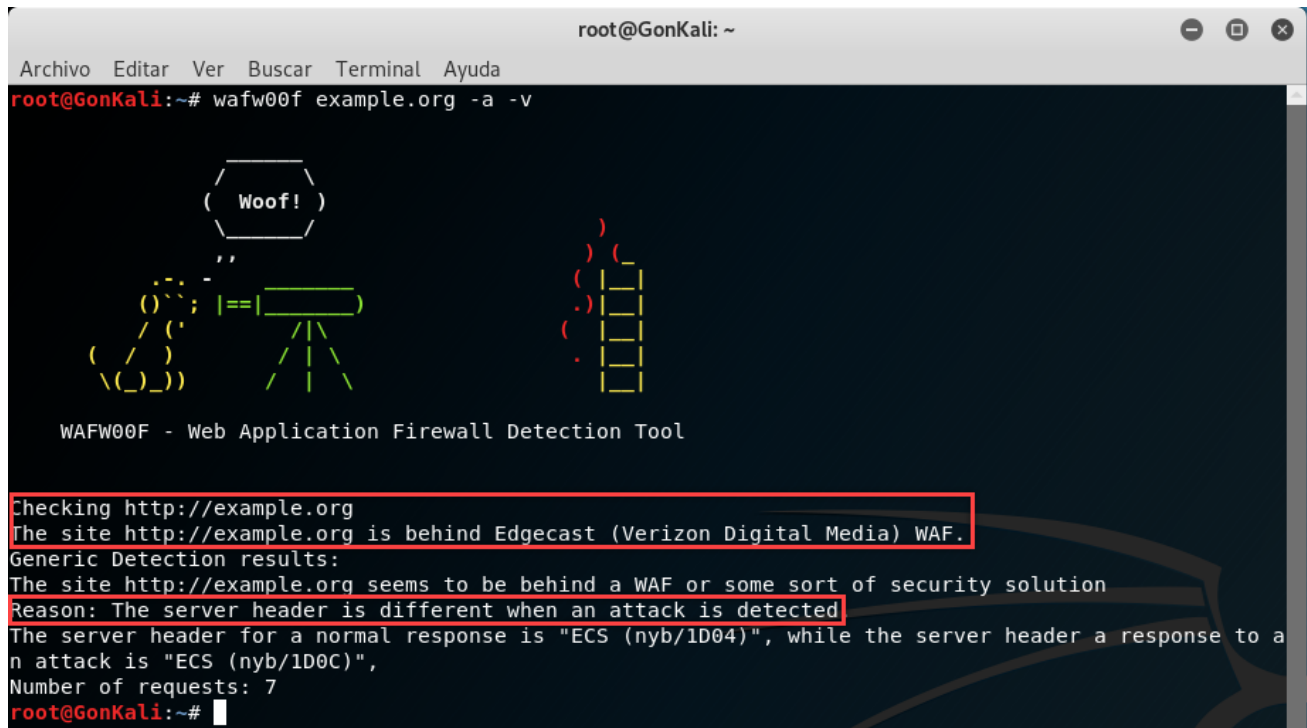
Ilustración 12 - HPING3 envió de paquetes con flag ACK.

En todos los casos se obtuvo una respuesta con el flag R(reset) por lo que se denegó la conexión.

Comprobación de la existencia de un WAF (Web Application Firewall)

Para esta comprobación hemos utilizado la herramienta wafw00f la cual es capaz de automatizar la detección de una gran variedad de WAF, mostramos primero un positivo.

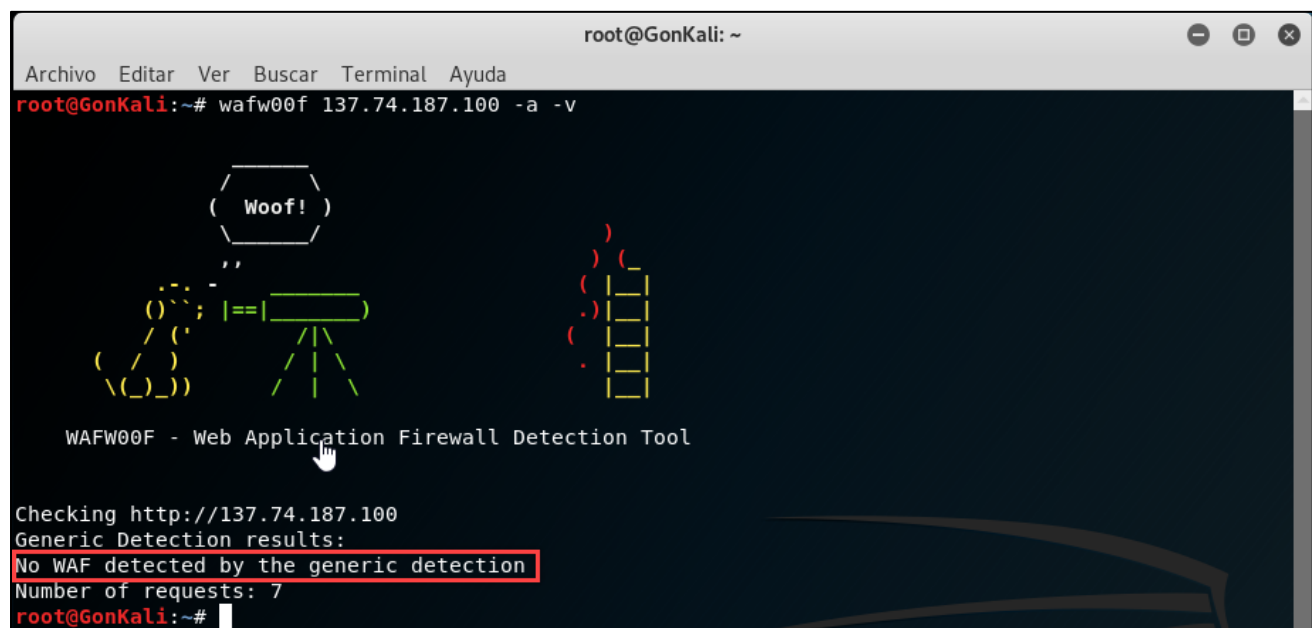
```
wafw00f example.org -a -v
```



```
root@GonKali: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@GonKali:~# wafw00f example.org -a -v  
  
      ( Woof! )  
      ''  
  ( ) ; |==| ( )  
  / \ / \ / \ / \  
 ( / ) / \ / \ / \  
 \ ( ) \ / \ / \ / \  
  \ ( ) \ / \ / \ / \  
  
WAFW00F - Web Application Firewall Detection Tool  
  
Checking http://example.org  
The site http://example.org is behind Edgecast (Verizon Digital Media) WAF.  
Generic Detection results:  
The site http://example.org seems to be behind a WAF or some sort of security solution  
Reason: The server header is different when an attack is detected  
The server header for a normal response is "ECS (nyb/1D04)", while the server header a response to a  
n attack is "ECS (nyb/1D0C)",  
Number of requests: 7  
root@GonKali:~#
```

Ilustración 13 - Uso de WAFW00F para la detección de WAF en una página de ejemplo con resultado positivo.

Ahora procedemos a mostrar el resultado en nuestro objetivo.



```
root@GonKali: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@GonKali:~# wafw00f 137.74.187.100 -a -v  
  
      ( Woof! )  
      ''  
  ( ) ; |==| ( )  
  / \ / \ / \ / \  
 ( / ) / \ / \ / \  
 \ ( ) \ / \ / \ / \  
  \ ( ) \ / \ / \ / \  
  
WAFW00F - Web Application Firewall Detection Tool  
  
Checking http://137.74.187.100  
Generic Detection results:  
No WAF detected by the generic detection  
Number of requests: 7  
root@GonKali:~#
```

Ilustración 14 - WAFW00F en uno de los hosts que albergan hackthissite.org.

CONCLUSIONES

De las pruebas:

De las pruebas realizadas mediante las herramientas nmap, hping3, wireshark, telnet, ssh y wafw00f hemos concluido que no existe un firewall a nivel de aplicación(WAF) pero sí existe un firewall que podría ser STATEFULL en la máquina por el aparente intento de evasión de resultados mediante nmap observado en los resultados y apoyado con ssh y telnet como los individuales con hping3.

La máquina remota tarda en enviar los paquetes de respuesta el tiempo suficiente para que nmap con una configuración básica determine que no existe respuesta cuando en realidad sí la hay.

Explicación sobre firewall statefull y stateless.

Fuente: web del conocido software seguridad y monitorización de Solarwinds.

<https://www.solarwindsmsp.com/blog/stateful-vs-stateless-firewall-differences>

Académicas:

Enviamos SYN y nos responden con SYN+ACK:

El puerto está abierto ya que quiere realizar el handshake.

Enviamos SYN y no obtenemos respuesta:

- a. El puerto no tiene ningún servicio escuchando o bien esta siendo filtrado por un firewall.
- b. Si tras este SYN mandamos un ACK y obtenemos RST entonces confirmamos firewall STATELESS.
- c. Si las respuestas varían de los casos anteriores entonces podríamos pensar en que existe algún tipo de tecnología que es sensible a estos flags y actúa en consecuencia como un firewall STATEFULL.

Enviamos SYN y obtenemos un RST:

El puerto está cerrado.