Certamen II

1.- Realizar un análisis de vulnerabilidades del servidor denominado itmon-uni.uv.cl específicamente en los puertos 22,80,443,53,135,137,139. **20 puntos**
El análisis debe hacerlo utilizando nmap y sus opciones, considerando el tipo de servidor debe interpretar las salidas y de acuerdo con los resultados entregar las sugerencias en materia de ciberseguridad.
Lo anterior, debe complementarlo (de acuerdo con el análisis realizado con nmap) con la regla o las reglas que serían necesarias en el FW para que los resultados de nmap sean equivalentes en todos los puertos que UD determine que son necesarios.
Además, debe analizar los resultados en general y en base a estos últimos entregar al menos 4 medidas de mitigación que según UD. deben ser tomadas en cuenta para disminuir el riesgo de algún activo.

Respuesta:

```
# Nmap 7.92 scan initiated Wed May 24 12:08:19 2023 as: nmap -sS -sV -O -p22,80,443,53,135,137,139 -oN Pregunta1 itmon-uni.uv.cl
# Nmap done at Wed May 24 12:08:23 2023 -- 1 IP address (0 hosts up) scanned in 4.19 seconds
# Nmap 7.92 scan initiated Wed May 24 12:08:45 2023 as: nmap -sA -sV -O -p22,80,443,53,135,137,139 -oN Pregunta1 --append-output itmon-uni.uv.cl
# Nmap done at Wed May 24 12:08:49 2023 -- 1 IP address (0 hosts up) scanned in 4.19 seconds
# Nmap 7.92 scan initiated Wed May 24 12:09:04 2023 as: nmap -sX -sV -O -p22,80,443,53,135,137,139 -oN Pregunta1 --append-output itmon-uni.uv.cl
# Nmap done at Wed May 24 12:09:07 2023 -- 1 IP address (0 hosts up) scanned in 4.18 seconds
# Nmap 7.92 scan initiated Wed May 24 12:09:22 2023 as: nmap -Pn -sV -O -p22,80,443,53,135,137,139 -oN Pregunta1 --append-output itmon-uni.uv.cl
Nmap scan report for itmon-uni.uv.cl (10.60.1.4)
Host is up.

PORT    STATE    SERVICE     VERSION
22/tcp  filtered ssh
53/tcp  filtered domain
80/tcp  filtered http
135/tcp filtered msrpc
137/tcp filtered netbios-ns
139/tcp filtered netbios-ssn
443/tcp filtered https
Too many fingerprints match this host to give specific OS details

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed May 24 12:09:35 2023 -- 1 IP address (1 host up) scanned in 13.83 seconds
```

- Se evidencia el puerto 80 y 443 abiertos, al ser un servidor web no debería figurar en un análisis los puertos adicionales que se muestran, tales como los son DNS, los puertos para compartir archivos de Windows y el 22.
- Dado que esta información se obtuvo utilizando la opción -Pn, se debe bloquear los accesos syn a los puertos 22,53,135,137,139 con una regla en el FW o cerrar los puertos en el servidor, la regla sería la siguiente:
    - INPUT * – tcp -syn -dport 53, 135, 137,139, 443 DROP
- Claramente, al no obtener información con -sS, -sA y -sX el servidor está siendo filtrado por un Firewall, por lo que se debe ampliar su contención al tráfico que genera la opción -Pn: Drop general a los paquetes que vayan al 22, 53, 135, 137, 139, 443
- Medidas de mitigación:
    - Proteger los puertos que no usemos: El resto de los puertos deberán estar cerrados, sobre todo aquellos puertos que se asocian a servicios internos o propios de una LAN, tales como el 135, 137 y 139
    - Proteger el acceso a los servicios que deban ser restringidos: Si debemos ofrecer un servicio pero no de forma pública, éste debe ser protegido mediante sistemas de autentificación adecuados.
    - Proteger las conexiones: Siempre que sea posible, usar conexiones cifradas: SSL se debe tener siempre presente.
    - Los usuarios de la escuela en particular y de la universidad en general, deben estar concientizados respecto de la seguridad y también deben estar al tanto de las políticas de seguridad que deben respetar y seguir al pie de la letra.

2.- Realizar un análisis de vulnerabilidades del servidor denominado ahg.uv.cl específicamente en los puertos 22,80,443,444,445,53. **20 puntos**
El análisis debe hacerlo utilizando nmap y sus opciones, considerando el tipo de servidor debe interpretar las salidas y de acuerdo con los resultados entregar las sugerencias en materia de ciberseguridad.
Lo anterior, debe complementarlo (de acuerdo con el análisis realizado con nmap) con la regla o las reglas que serían necesarias en el firewall para que los resultados de nmap solo muestre los puertos asociados al servicio de un portal web.
Además, debe analizar los resultados en general y en base a estos últimos entregar al menos 4 medidas de mitigación que según UD. deben ser tomadas en cuenta para disminuir el riesgo de algún activo.

```
# Nmap 7.92 scan initiated Wed May 24 18:26:17 2023 as: nmap -sS -sV -O -p22,80,443,444,445,53 -oN Pregunta2 ahg.uv.cl
Nmap scan report for ahg.uv.cl (10.50.200.100)
Host is up (0.12s latency).

PORT    STATE    SERVICE      VERSION
22/tcp  open     ssh          OpenSSH 7.5 (FreeBSD 20170903; protocol 2.0)
53/tcp  filtered domain
80/tcp  open     http         Apache httpd
443/tcp open     ssl/http     Apache httpd
444/tcp filtered snpp
445/tcp filtered microsoft-ds
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (89%)
OS CPE: cpe:/o:freebsd:freebsd:11.0
Aggressive OS guesses: FreeBSD 11.0-RELEASE (89%), FreeBSD 11.2-STABLE (89%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed May 24 18:26:40 2023 -- 1 IP address (1 host up) scanned in 23.60 seconds
# Nmap 7.92 scan initiated Wed May 24 18:27:29 2023 as: nmap -sA -sV -O -p22,80,443,444,445,53 -oN Pregunta2 -append-output ahg.uv.cl
Nmap scan report for ahg.uv.cl (10.50.200.100)
Host is up (0.13s latency).

PORT    STATE    SERVICE      VERSION
22/tcp  filtered ssh
53/tcp  filtered domain
80/tcp  filtered http
443/tcp filtered https
444/tcp filtered snpp
445/tcp filtered microsoft-ds
Too many fingerprints match this host to give specific OS details

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed May 24 18:27:38 2023 -- 1 IP address (1 host up) scanned in 9.22 seconds
# Nmap 7.92 scan initiated Wed May 24 18:28:15 2023 as: nmap -sX -sV -O -p22,80,443,444,445,53 -oN Pregunta2 -append-output ahg.uv.cl
Nmap scan report for ahg.uv.cl (10.50.200.100)
Host is up (0.12s latency).

PORT    STATE         SERVICE    VERSION
22/tcp  open          ssh        OpenSSH 7.5 (FreeBSD 20170903; protocol 2.0)
53/tcp  open          domain?
80/tcp  open          http       Apache httpd
443/tcp open          ssl/http   Apache httpd
444/tcp open|filtered tcpwrapped
445/tcp open|filtered tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (89%)
OS CPE: cpe:/o:freebsd:freebsd:11.0
Aggressive OS guesses: FreeBSD 11.0-RELEASE (89%), FreeBSD 11.2-STABLE (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed May 24 18:28:38 2023 -- 1 IP address (1 host up) scanned in 24.09 seconds
```

- Al tratarse de un servidor web y estar expuesto a la red pública debe tener abierto solo los puertos atingentes a este último servidor y no otros.

- Claramente no esta siendo filtrado debidamente a nivel de Firewall ni a nivel del servidor, en este último solo hace falta cerrar los puertos o desinstalar las aplicaciones
- Debe ocultar las versiones de los servicios que se encuentren activos
- iptables −A INPUT −p tcp −−dport 80 −j ACCEPT
- iptables −A INPUT −p tcp −−dport 443 −j ACCEPT
- iptables −A INPUT −p tcp −−dport 1:1024 −j DROP

- Tener el software actualizado: De nada le sirve a un atacante saber la versión de nuestro Apache si no hay fallos conocidos. Conviene así mismo estar al tanto de estos fallos para reaccionar un paso por delante del atacante.
- •. Proteger los puertos que no usemos: El resto de los puertos deberán estar cerrados, o mejor aún, silenciosos.
- Proteger el acceso a los servicios que deban ser restringidos: Si debemos ofrecer un servicio pero no de forma pública, éste debe ser protegido mediante sistemas de autentificación adecuados.
- Proteger las conexiones: Siempre que sea posible, usar conexiones cifradas: SSL se debe tener siempre presente.
- •. Los usuarios de la escuela en particular y de la universidad en general, deben estar concientizados respecto de la seguridad y también deben estar al tanto de las políticas de seguridad que deben respetar y seguir al pie de la letra.

3.- Utilizar Nmap y realizar un análisis de vulnerabilidades del servidor denominado ingenieriaoceanica.uv.cl, revise los problemas y de acuerdo con estos últimos y a la función que cumple el servidor, proponga mitigaciones a nivel de servidor y de firewall con reglas que Ud considere adecuadas. **20 puntos**

```
sh-3.2# nmap -sS -sV -O ingenieriaoceanica.uv.cl
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-25 18:36 -04
sendto in send_ip_packet_sd: sendto(7, packet, 44, 0, 10.50.200.100, 16) => Protocol wrong type for socket
Offending packet: TCP 10.100.250.235:47904 > 10.50.200.100:53 S ttl=59 id=28110 iplen=11264  seq=4249224154 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(7, packet, 44, 0, 10.50.200.100, 16) => Protocol wrong type for socket
Offending packet: TCP 10.100.250.235:47906 > 10.50.200.100:53 S ttl=42 id=37965 iplen=11264  seq=4248830940 win=1024 <mss 1460>
Nmap scan report for ingenieriaoceanica.uv.cl (10.50.200.100)
Host is up (0.12s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE  SERVICE  VERSION
22/tcp   open   ssh      OpenSSH 7.5 (FreeBSD 20170903; protocol 2.0)
80/tcp   open   http     Apache httpd
443/tcp  open   ssl/http Apache httpd
1433/tcp closed ms-sql-s
3306/tcp open   mysql    MySQL (unauthorized)
Device type: general purpose|phone
Running (JUST GUESSING): FreeBSD 11.X (86%), Google Android 5.X (86%)
OS CPE: cpe:/o:freebsd:freebsd:11.0 cpe:/o:google:android:5.0.1
Aggressive OS guesses: FreeBSD 11.0-STABLE or 11.0-RELEASE (86%), Android 5.0.1 (86%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd

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 43.31 seconds
```

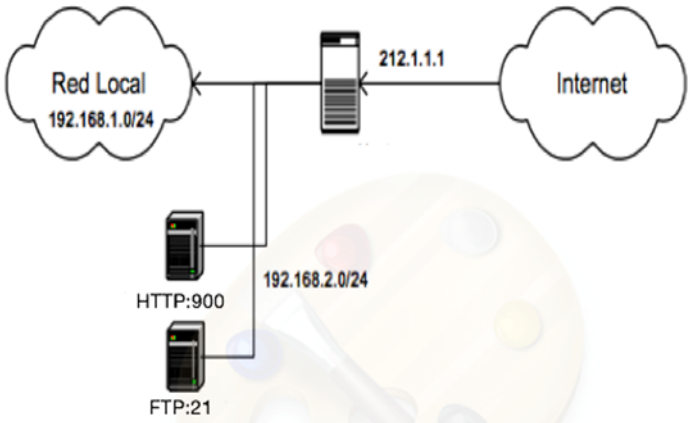
- Se puede evidenciar que es un servidor que cumple la función de un portal web, por lo tanto, de preferncia solo debe estar expuesto los servicios asociados a los puertos 80 (http) y 443 (https).
- Se debe ocultar las versiones o nombres de los servicios que estarán habilitados.
- Al poseer un servicio asociado a un motor de base de datos (MySQL) lo hace especialmente sensible a posibles ataques. No es recomendable tener este tipo de servicios en servidores expuestos a la red pública.
- iptables −A INPUT −p tcp −−dport 80 −j ACCEPT
- iptables −A INPUT −p tcp −−dport 443 −j ACCEPT
- iptables −A INPUT −p tcp −−dport 1:1024 −j DROP
- iptables −A INPUT −p tcp −−dport 1433 −j DROP
- iptables −A INPUT −p tcp −−dport 3306 −j DROP

4.- Determine el significado de las siguientes reglas y defina las que figuran como requerimientos **40 puntos**

a. iptables -t nat -A PREROUTING -d 200.14.67.201 -p tcp --dport 22 -j DNAT --to-destination 192.168.22.1:22
b. iptables -t nat -A PREROUTING -d 200.14.67.201 -p tcp --dport 25 -j DNAT --to-destination 192.168.22.2:25
c. iptables -t nat -A PREROUTING -d 200.14.67.201 -p tcp --dport 80 -j DNAT--to-destination 192.168.22.3:80

Respuesta: se específica que si un paquete va destinado a la dirección 200.32.106.148, puerto 22, éste se vaya dirigido al IP 192.168.22.1, puerto 22 (podríamos hasta cambiar el puerto destino si quisiéramos). Se aplica lo mismo con los puertos 25 y 80.

d. La figura (1) muestra una arquitectura en la que el servidor WEB está recibiendo peticiones externas por la IP 212.1.1.1 y puerto 80, aunque en realidad este tiene la IP 192.168.2.5 y su servicio está habilitado por el puerto 900. Por otro lado, muestra un servidor FTP con la IP 192.168.2.10 escuchando por el puerto standard 21 y por seguridad se necesita que se defina un puerto no reservado, por ejemplo 3690.



Se requiere que defina las reglas en el FW, para que tanto las consultas al servicio http como FTP se mantengan en la red pública y sean enmascaradas a los servicios internos. Utilice las direcciones y puertos ya definidos en el resumen y figura (1).

iptables -t nat -A PREROUTING -d 212.1.1.1 -p tcp --dport 80 -j DNAT --to 192.168.2.5:900 # http
iptables -t nat -A PREROUTING -d 212.1.1.1 -p tcp --dport 3690 -j DNAT --to 192.168.2.10:21 # FTP

e. A modo de evitar el spoofing, eliminar direcciones de red privada en la interfaz pública (Suponiendo eth1 como interfaz pública).

   iptables -A INPUT -i eth1 -s 192.168.0.0/24 -j DROP
   iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j DROP
   iptables -A INPUT -i eth1 -s 172.168.0.0/16 -j DROP

f. Se tiene una red LAN con 2 segmentos, el 192.168.0..1/24 y el 172.16.0.1/16 y se requiere que ambos segmentos se enmascaren por la interfaz pública del firewall

   iptables -t nat -A POSTROUTING -s 192.168.0.1/24 -o eth1 -j MASQUERADE
   iptables -t nat -A POSTROUTING -s 172.160.0.1/16 -o eth1 -j MASQUERADE

g. Por otro lado, se require que todas los equipos conectados al segmento 192.168.0.1/24 puedan navegar por Internet.

   iptables -A FORWARD -s 192.168.0.0/24 -i eth0 -p tcp --dport 80 -j ACCEPT
   iptables -A FORWARD -s 192.168.0.0/24 -i eth0 -p tcp --dport 443 -j ACCEPT

h. Tomando en cuenta lo anterior, se debe habilitar en el firewall el servicio SSH al ip del administrador de sistemas

   iptables -A INPUT -p tcp -s 200.14.67.90 -m tcp --dport 22 -j ACCEPT