

Practica 3

Illia nechesa | Pablo ospino

Seguridad en Sistemas Informáticos | 4º Curso | 06-11-2019

# Certificados SSL y ataques de contraseña

**Configuración**

Primero procedemos a descargar la maquina virtual, y seguido abrimos VirtualBox, aplicando todas las configuraciones necesarias, indicadas en las instrucciones de las practicas.

En cuanto a la configuración de red, vamos a utilizar NAT cuando sea necesario conectarse a internet, y Host-Only cuando sea necesario tener conectividad entre varias máquinas virtuales.

Para conectar con ssh, ponemos las dos maquinas en host only, y escribimos

* ssh usuario@<ip> 🡪 En donde pone <ip> escribimos la IP donde esta corriendo el servidor (no poner <>) 🡪 Seguidamente nos pide una contraseña, que seria la del servidor al cual nos estamos conectando.

**Añadir usuarios**

Ahora vamos a hacer usuarios en una distribución de Unix, en concreto añadiremos el usuario en nuestra maquina que actuará como host.

* sudo useradd ssi29
  + password será ssi29

**Conexión**

Para conectarnos entre las dos máquinas, lo primero es obtener la dirección IP del host. Así podremos conectarnos desde la otra máquina (Cliente).

HOST:

* ifconfig 🡪 192.168.56.102

Cliente:

* ssh [ssi29@192.168.56.102](mailto:ssi29@192.168.56.102) 🡪 Seguidamente nos pide la contraseña
* ssi29 🡪Esta es la contraseña que habíamos definido.

Una vez hecho esto, ya hemos establecido conexión.

**Permisos de usuarios para el acceso ssh**

Ahora, configuramos los permisos para unos usuarios, y para otros no.

Primero, modificamos el archivo /etc/ssh/sshd\_config

Port 1234

PermitRootLogin no

AllowUsers ssi29

Reiniciamos el servicio de ssh para que obtenga la nueva configuración.

* sudo service ssh reload

Comprobamos que todo funcione correctamente como esperado.

ssh ssi29@192.168.56.102

> ssi29

Connection

exit

ssh tlm@192.168.56.102

> tlm

Permission denied, please try again Connection

exit

Podemos ver que funciona correctamente, ya que nos deja conectarnos con el usuario que le hemos indicado en la configuración (ssi29), pero no con otro usuario.

**Autentificación de usuario con clave pública**

Desde cliente creamos un par de claves. (Publica privada). Y utilizamos la IP del host que previamente hemos obtenido para copiar la clave publica en el HOST. Nos pide la contraseña para poder acceder y finalmente la copiamos.

ssh-keygen *# Generate the key-pair.*

ssh-copy-id ssi29@192.168.56.102

**>** ssi29 *# Use the password*

Ahora se conecta directamente sin pedir la contraseña

ssh ssi29@192.168.56.102

**Ataques de login**

Vamos a realizar los ataques de login con la utilidad de hydra. Creamos una nueva máquina virtual e instalamos hydra en ella.

* NAT network configuration, para tener acceso a internet.
* sudo apt-get update
* sudo apt-get install hydra

Para poder realizar ahora los ataques de login es necesario cambiar la configuración de red a host-only para poder acceder al HOST de ssh. Después nos encontramos con un problema en el que es necesario realizar un cambio de ip para la máquina de hydra.

Hasta ahora tenemos dos máquinas virtuales corriendo, una de ellas tiene la ip terminada en 101 y la otra 102. Al lanzar otra tercera máquina esta obtiene la 101, por lo que la tenemos que cambiar manualmente.

*> sudo ifconfig eth0 192.168.56.103 # los otros tienen la 101 y 102.*

Ahora podemos realizar ataques utilizando hydra:

hydra -l root -p admin 192.168.1.105 -t 4 ssh

hydra -l user\_name -p single\_password ip -t n\_threads server\_type\_it\_will\_attack

Documentación:

# El usuario que vamos a atacar

- -l

# Listado de usuarios

- -L

# Contraseña con la que vamos a probar

- -p

# Lista de posibles contraseñas word list en vez de una sola contraseña

- -P

# Numero de hilos

- -t

Ataques:

hydra -l ssi29 -p dict.txt 192.168.56.102 -t 4 ssh

*# Diccionario con todas las palabras para probar*

*# Fuerza bruta de todas conbinaciones de 3 caracteres*

crunch 3 3 **>** dict.txt

Al utilizar un diccionario si hemos dado con una clave correcta nos saldrá en el output, tras finalizar hydra.

**Defensas**

- [x] Configure que solo algunos usuarios puedan entrar

- [x] Pruebe a cambiar el puerto del servidor de ssh

  - Search for port in nano -w /etc/ssh/ssh\_config

  - Port 889, different

- [x] Deshabilitar root login

- [x] Passwordless login - with ssh-keygen

  - Disable empty password

- [x] Pruebe a cambiar los parámetros de ssh que afectan a la velocidad con que un atacante puede intentar contraseñas

Probamos a cambiar los parámetros de segundos que afectan a la velocidad con la que un atacante puede intentar contraseñas.

> sudo nano -w /etc/ssh/sshd\_config

...

LoginGraceTime 120 # Bajado a 10 y da error

...

120 indica el número de segundos en que la pantalla de login estará disponible.

Bajamos el número de segundos para que no pueda estar una pantalla abierta.

Ahora vamos a instalar y configurar monitores de login que corten el acceso a quien haga varios intentos de acceso fallidos.

> sudo nano -w /etc/ssh/sshd\_config

...

MaxAuthTries 2

...

Por último, vamos a investigar sobre el port-knocking.

* Se trata de un mecanismo para abrir puertos externamente en un firewall mediante una secuencia preestablecida de intentos de conexión a puertos que se encuentran cerrados. Una vez que el firewall recibe la secuencia de conexiones correcta, permite al host que realizó los intentos conectarse al puerto especifico.
* Instrucciones
  + apt-get update -y
  + apt-get upgrade -y
* Instalar y configurar tablas
  + ufw disable 🡪 hay que deshabilitar ufw antes de instalar las tablas
  + apt-get install iptables iptables-persistent 🡪 instalamos iptables
  + iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT 🡪 permitir todas las conexiones por iptables
  + iptables -A INPUT -p tcp --dport 22 -j REJECT 🡪 bloquear ssh de entrada por el puerto 22
  + netfilter-persistent sabe 🡪 guardar las reglas del firewall
  + netfilter-persisten reload
* Ahora podemos testear que puertos ssh están bloqueados
  + nmap 192.168.0.190
* Ahora instalamos y configuramos Knockd
  + apt-get install knockd -y
  + nano /etc/default/knockd
    - Dentro, cambiamos el valor de START\_KNOCKD de cero a uno.
  + nano /etc/knockd.conf 🡪 Aquí cambiamos la secuencia tanto de openSSH como de close SSH por la que queramos

[options]

logfile = /var/log/knockd.log

[openSSH]

sequence = 10001,10002,10003

seq\_timeout = 20

tcpflags = syn

command = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCEPT

[closeSSH]

sequence = 10003,10002,10001

seq\_timeout = 20

command = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT

tcpflags = syn

* systemctl start knockd 🡪 lanzamos el servicio knock para aplicar los cambios
* Ahora vamos a testea Knockd desde el cliente
  + apt-get install telnet -y
* Lanzamos los siguientes comandos en orden

telnet 192.168.0.190 10001

telnet 192.168.0.190 10002

telnet 192.168.0.190 10003

Para ver el log introducimos el siguiente comando:

* tail -f /var/log/syslog

[2017-09-25 09:11] 192.168.0.191: openSSH: Stage 1

[2017-09-25 09:12] 192.168.0.191: openSSH: Stage 2

[2017-09-25 09:13] 192.168.0.191: openSSH: Stage 3

[2017-09-25 09:13] 192.168.0.191: openSSH: OPEN SESAME

[2017-09-25 09:13] openSSH: running command: /sbin/iptables -I INPUT -s 192.168.0.191 -p tcp --dport 22 -j ACCEPT

* nmap 192.168.0.190 🡪 Ahora ya somos capaces de conectar nuestro servidor ssh desde el cliente.

Starting Nmap 6.40 ( http://nmap.org ) at 2017-09-25 9:20 IST

Nmap scan report **for** 192.168.0.190

Host **is** up (0.00037s latency).

Not shown: 996 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

443/tcp open https

3306/tcp open mysql

MAC Address: 08:00:27:7C:5B:40 (Cadmus Computer Systems)

Nmap **done**: 1 IP address (1 host up) scanned **in** 1.69 seconds

Por último, para cerrar la conexión, introducimos los siguientes comandos en orden secuencial.

telnet 192.168.0.190 10003

telnet 192.168.0.190 10002

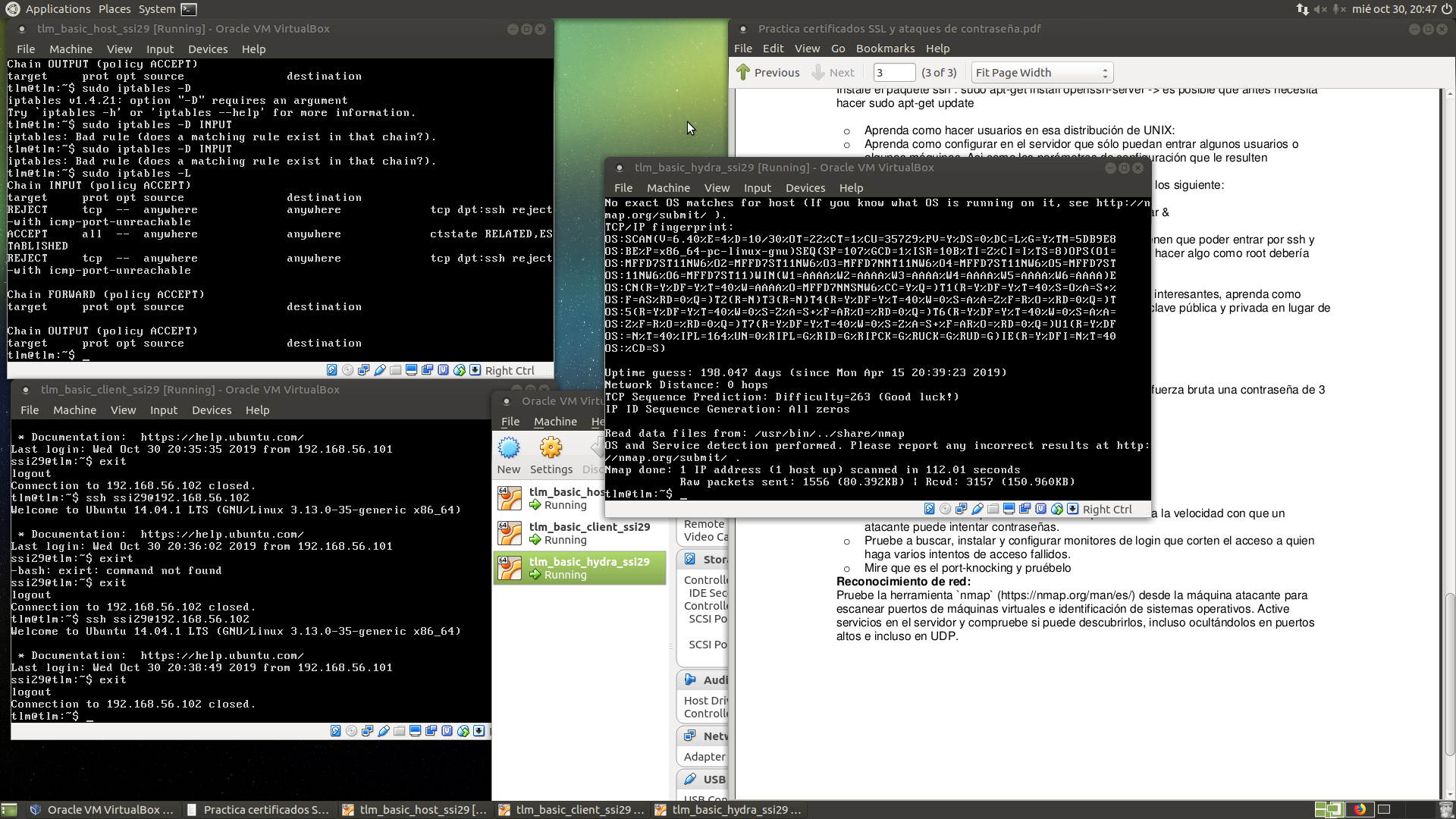
telnet 192.168.0.190 10001

**\*\***

**Todas estas pruebas son suponiendo que la IP del servidor es** 192.168.0.190 **y la del cliente** 192.168.0.191

**\*\***

**Aquí dejo los screenshots con nuestras pruebas**

****

