TALLER SI – PRÁCTICA 21

NÚMERO DE GRUPO	FUNCIÓNS	Apelidos, Nome
	Coordinador/a:	
	Responsable Limpeza:	
	Responsable Documentación:	

ESCENARIO:

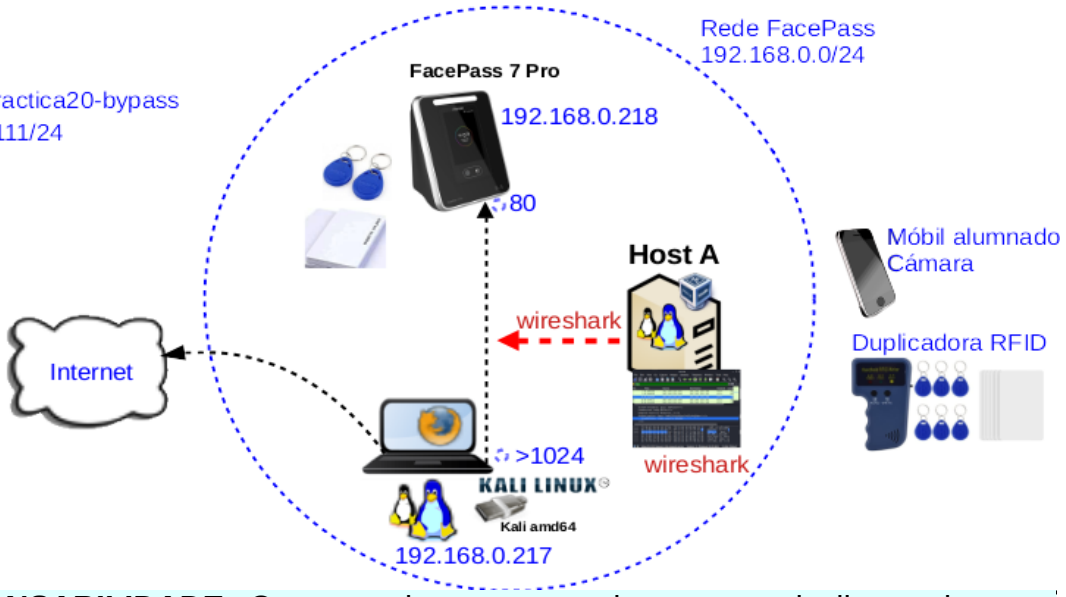
Portátil
Firefox

HostA alumnado
Máquina virtual Practica20-bypass
192.168.0.111/24
Wireshark

FacePass 7 Pro
Web Server: 192.168.0.218

Móbil alumnado Android
Cámara

Duplicadora RFID



Material necesario	Práctica: Bypass Biometría
■ Host alumnado ■ Portátil ■ USB Live amd64 Kali ■ Regleta e Switch 5-Port Gigabit ■ Cableado rede ■ [1] Anviz FacePass 7 Pro ■ [2] FacePass 7 Pro Flyer ES ■ [3] FacePass 7 Pro Quick Guide ■ [4] RFID Etiqueta Chaveiro ■ [5] RFID Tarxetas identificación ■ [6] [USER GUIDE] How to enroll face on Facepass 7 device?-ANVIZ Malaysia ■ [7] FacePass 7 Pro User Manual ■ [8] Protección IP ■ [9] Práctica Wireshark ■ [10] Práctica 20 ■ [11] RFID chaveiros, tarxetas identificadoras sen configurar e configuradas en [10]	(1) Prerrequisito: Ter realizada a Práctica 20 [10] (2) Conectar portátil, FacePass 7 Pro e host do alumnado ao switch. (3) Bypass: ■ Autenticación administrador por defecto ■ http ■ RFID ■ Identificación facial

Procedemento:

(1) Ter realizada a Práctica 20.

(2) Conectar no mesmo segmento de rede o portátil, o host A do alumnado e o dispositivo FacePass 7 Pro.

(a) Conectar a regleta á corrente eléctrica na vosa zona de traballo.

(b) Conectar o switch á regleta.

(c) Conectar o portátil ao switch.

(d) Conectar co cableado de rede o HostA (un equipo de alumnado) ao switch.

(e) Conectar o dispositivo FacePass 7 Pro á regleta e ao switch.

(f) Non conectar o switch á roseta da aula.

(g) Accender o dispositivo e esperar a que esté activo para poder proceder co apartado seguinte.

Bypass autenticación administrador por defecto

(3) Buscar nas ligazóns indicadas na sección **Material Necesario**, ou ben, a través de Internet cal é o usuario administrador e o contrasinal por defecto deste usuario para acceder como tal ao dispositivo FacePass 7 Pro. Cubrir a seguinte táboa:

	Credencias por defecto	
Administrador	**ID**	**Contrasinal**

(4) Verificar no dispositivo (pantalla táctil) o acceso co usuario administrador preconfigurado por defecto, coas credenciais indicadas no apartado anterior.

(5) Avisar ao docente para revisión. [1]

Bypass http

(6) HostA alumnado:

(a) Crear unha máquina virtual coas seguintes características (ver escenario):

i. RAM ≥ 2048MB
ii. CPU ≥ 2
iii. PAE/NX habilitado
iv. Rede: Soamente unha tarxeta activada en modo bridge (ponte)
v. ISO: Kali Live amd64
vi. Nome: Practica21-bypass

(b) Arrancar a máquina virtual.

(c) Configurar a rede para a NIC eth0. Executar nunha consola:

```
$ setxkbmap es #Configurar teclado en español

$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)

  # /etc/init.d/avahi-daemon stop #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflicto con este demo.

  # /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo network-manager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar doutro xeito (co comando ip(ifconfig) de forma manual ou mediante networking (ficheiros /etc/init.d/networking, /etc/init.d/networking.d) a configuración de rede e non ter conflicto con este xestor.

  # ip addr show eth0 #Amosar información sobre a NIC eth0.

  # ip addr add 192.168.0.111/24 dev eth0 #Configurar a tarxeta de rede eth0, coa IP: 192.168.0.111 e máscara de subrede: 255.255.255.0

  # ip addr show eth0 #Amosar información sobre a NIC eth0.
```

(d) Lanzar o analizador de tráfico wireshark [9]:

```
# exit #Saír da shell
$ sudo wireshark & #Lanzar o programa wireshark (sniffer) para poder visualizar o que acontece na rede (protocolos,paquetes). O comando sudo permite executar o programa wireshark con permisos de root(administrador) e o caracter & serve para executar en segundo plano o programa e así devolver o prompt da consola para poder seguir traballando nela.
```

(e) Avisar ao docente para revisión. ☐ 2

(7) Portátil. Acceso e configuración mediante o Web Server embedido no dispositivo:

(a) Arrancar cun USB Live amd64 Kali GNU/Linux

(b) Configurar a rede para a NIC eth0. Executar nunha consola:

```
$ setxkbmap es #Configurar teclado en español
$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
# /etc/init.d/avahi-daemon stop #Parar o demo avahi-daemon(control resolución de nomes) para poder configurar de forma manual a configuración de rede e non ter conflicto con este demo.
# /etc/init.d/network-manager stop || pkill NetworkManager #Parar o demo network-manager(xestor de rede) ou o script NetworkManager (executado sen ser demo) para poder configurar doutro xeito (co comando ip(ifconfig) de forma manual ou mediante networking (ficheiros /etc/init.d/networking, /etc/init.d/networking.d) a configuración de rede e non ter conflicto con este xestor.
# ip addr show eth0 #Amosar información sobre a NIC eth0.
# ip addr add 192.168.0.217/24 dev eth0 #Configurar a tarxeta de rede eth0, coa IP: 192.168.0.217 e máscara de subrede: 255.255.255.0
# ip addr show eth0 #Amosar información sobre a NIC eth0.
```

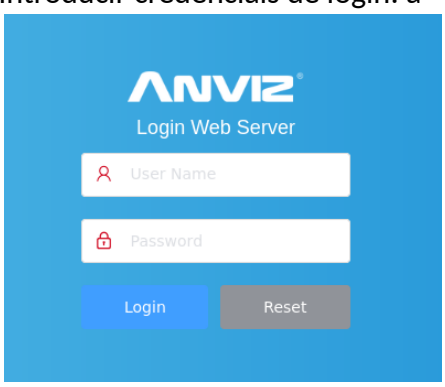
(c) Acceder mediante un navegador ao servidor web embedido do dispositivo:

```
# exit #Saír da shell
$ firefox http://192.168.0.218
```

(8) Máquina virtual Practica21-bypass (HostA alumnado): Play (icono azul aleta tiburón) en wireshark, é dicir, arrancamos o wireshark.

(9) Portátil:

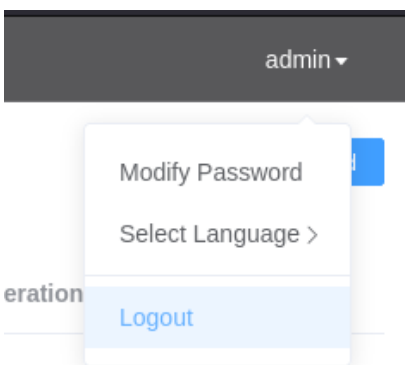
(a) Introducir credenciais de login: a

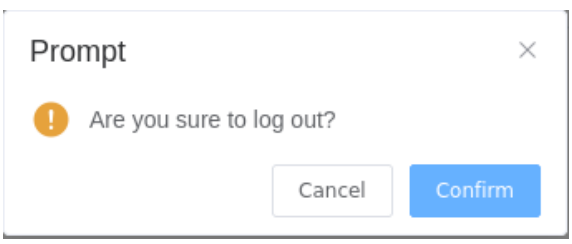


username=admin

password=12345

(b) Pechar sesión e confirmar:





(10) Máquina virtual Practica21-bypass (HostA alumnado):

(a) Stop (icono vermello cadrado) en wireshark, é dicir, paramos o wireshark.

(b) Gardar o tráfico capturado ao ficheiro `practica21.pcap`

(c) Identificar os paquetes de login/logout. É posible ver as credenciais do usuario `admin` en texto claro? En caso afirmativo explica o proceso realizado para chegar a conseguir as credenciais en texto claro e captura unha imaxe do wireshark onde se amosen esas credenciais.

IMAXE A CAPTURAR

(d) Executar nunha consola:

```
$ setxkbmap es #Configurar teclado en español
$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
  # apt update #Actualizar o listado de paquetes dos repositorios (/etc/apt/sources.list, /etc/apt/sources.list.d/)
  # apt -y install tcpflow #Instalar o paquete tcpflow. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete.
  # tcpflow practica21.pcap #Executar tcpflow sobre o ficheiro capturado practica21.pcap para obter as posibles conversacións establecidas na captura realizada.
  # ls -l #Listar de forma extendida o contido do directorio actual.
```

(e) Ver o contido dos ficheiros xerados a través do comanto `tcpflow`. É posible ver as credenciais en texto claro?

(11) Avisar ao docente para revisión. ☐$_3$

Bypass RFID

(12) Verificar identificación RFID – Tarxeta identificación:

Comprobar que segue sendo posible a fichaxe mediante as tarxetas de identificación RFID configuradas polo grupo na práctica 20 [10]. Así:

(a) Proceder a fichaxe de entrada de cada compoñente do grupo:

i. *Achegar a Tarxeta identificativa durante uns segundos na zona inferior dereita do dispositivo, icona ((...)) , para proceder ao escaneo RFID.*

ii. *Se o escaneo RFID é efectivo, premer na sección **IN***

iii. *Escolle o estado **IN** para realizar a fichaxe de entrada.*

iv. *Premer na icona inferior dereita (Check) para acceder a verificar a zona de fichaxe.*

v. *Verificar a fichaxe: ID, Name e Check Time.*

(b) Proceder a fichaxe de saída de cada compoñente do grupo:

i. *Achegar a Tarxeta identificativa durante uns segundos na zona inferior dereita do dispositivo, icona ((...)) , para proceder ao escaneo RFID.*

ii. *Se o escaneo RFID é efectivo, premer na sección **IN***

iii. *Escolle o estado **OUT** para realizar a fichaxe de saída.*

iv. *Premer na icona inferior dereita (Check) para acceder a verificar a zona de fichaxe.*

v. *Verificar a fichaxe: ID, Name e Check Time.*

(c) Avisar ao docente para revisión.

(13) Duplicadora RFID. Seguindo o manual da clonadora copia cada tarxeta identificadora[11] empregada no apartado anterior.

(14) Voltar a realizar o apartado (14) pero agora coas tarxetas identificadoras RFID clonadas no apartado (15).

(15) Avisar ao docente para revisión. ☐4

Bypass Identificación facial

(16) Coller o móbil de alumnado e sacar foto en primeira plana dos compoñentes do grupo.

(17) É posible a fichaxe mediante a foto sacada co móbil de todos os compoñentes do grupo? Indicar que acontece e por que.

(18) Avisar ao docente para revisión. ☐5

(19) Coller o móbil de alumnado e sacar un vídeo en primeira plana por cada compoñente do grupo.

(20) É posible a fichaxe de cada compoñente do grupo empregando cadanseu vídeo grabado?

(21) Avisar ao docente para revisión. ☐6

(22) Contesta brevemente e razoa as respostas:

(a) Que habería que facer co contrasinal por defecto do usuario `admin`?

(b) Sería posible capturar as credenciais texto en claro do usuario `admin` se o protocolo web de acceso ao dispositivo FacePass 7 Pro fose `https` e non `http`?

(c) A clonación RFID é "invasiva", é dicir, pódese facer sen obter a tarxeta identificativa RFID orixinal? Cando tempo leva a clonación dunha tarxeta?

(d) Unha persoa podería fichar por outra no caso de dispoñer dunha imaxe con boa resolución da persoa a fichar? Ten algo que ver con iso o algoritmo de recoñecemento facial do dispositivo?

(e) Unha persoa podería fichar por outra no caso de dispoñer dun vídeo con boa resolución da persoa a fichar? Ten algo que ver con iso o algoritmo de recoñecemento facial do dispositivo?

(f) Indica outros 2 métodos de biometría posibles para unha posible fichaxe aínda que este dispositivo non os permita. Poderíase facer bypass deses métodos indicados? Cómo (explicación, ligazóns)?

(23) Avisar ao docente para revisión e entrega da práctica. ☐7

Revisión:

☐1 ☐2 ☐3 ☐4 ☐5 ☐6 ☐7