

```
>>> Software for security tests
```

```
Name: Sofía Almeida Bruno  
      Fernando de la Hoz Moreno
```

1. Introduction

Kali Linux

2. John the Ripper

3. Aircrack-ng

4. Wireshark

5. Nmap

6. Metasploit

7. Pros and Cons

8. Bibliography

>>> Introduction



>>> Kali Linux

- * Pentesting and security auditing
- * Safe development environment
- * More than 300 tools



>>> Kali Linux



>>> John the Ripper



```
>>> John the Ripper
```

How does it work?

- * Dictionary attack

```
>>> John the Ripper
```

How does it work?

- * Password file
- * Wordlist
- * Compare encryptions


```
>>> John the Ripper
```

How does it work?

- * Dictionary attack
- * Brute force attack

```
>>> Aircrack-ng
```



>>> Aircrack-ng

Nets 802.11 WEP and WPA/WPA2-PSK

Aircrack-ng 0.5

```
1      2      3      4      500:00:151 Tested 451275 keys (got 566683 IVs)
KB      depth  byte(vote)
0      0/ 1    AE< 50> 11< 20> 71< 20> 10< 12> 84< 12> 68< 12>
1      1/ 2    5B< 31> BD< 18> F8< 17> E6< 16> 35< 15> CF< 13>
2      0/ 3    7F< 31> 74< 24> 54< 17> 1C< 13> 73< 13> 86< 12>
3      0/ 1    3A< 148> EC< 20> EB< 16> FB< 13> F9< 12> 81< 12>
4      0/ 1    03< 140> 90< 31> 4A< 15> 8F< 14> E9< 13> AD< 12>
5      0/ 1    D0< 69> 04< 27> C8< 24> 60< 24> A1< 20> 26< 20>
6      0/ 1    AF< 124> D4< 29> C8< 20> EE< 18> 54< 12> 3F< 12>
7      0/ 1    9B< 168> 90< 24> 72< 22> F5< 21> 11< 20> F1< 20>
8      0/ 1    F6< 157> EE< 24> 66< 20> EA< 18> DA< 18> E0< 18>
9      0/ 2    8D< 82> 7B< 44> E2< 30> 11< 27> DE< 23> A4< 20>
10     0/ 1    A5< 176> 44< 30> 95< 22> 4E< 21> 94< 21> 4D< 19>
```

KEY FOUND! [AE:5B:7F:3A:03:D0:AF:9B:F6:8D:A5:E2:C7]

>>> Wireshark

- * Network protocol analyzer
- * Dynamic analysis of malware
- * Intruder detection



```
>>> Nmap
```

- * Host discovery
- * Port analysis
- * Other functionalities



>>> Nmap

Host discovery

- * IP from active hosts
- * Send packets

```
root@kali:~# nmap -PS -p 21 10.0.2.8
Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-27 05:00 EST
Nmap scan report for 10.0.2.8
Host is up (0.00038s latency).
DSCP: CS0, ECN: Not-ECT)

PORT      STATE SERVICE
21/tcp    closed ftp
MAC Address: 08:00:27:AC:5E:F0 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.64 seconds
```

>>> Nmap

Host discovery

Aplicaciones ▾ Lugares ▾ Wireshark ▾ lun 05:02 1

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_81:b1:df	Broadcast	ARP	42	Who has 10.0.2.8? Tell 10.0.2.15
2	0.000294455	PcsCompu_ac:5e:f0	PcsCompu_81:b1:df	ARP	60	10.0.2.8 is at 08:00:27:ac:5e:f0
3	0.210199537	10.0.2.15	10.0.2.1	DNS	81	Standard query 0x8660 PTR 8.2.0.10.in-addr.arpa
4	0.227144002	10.0.2.1	10.0.2.15	DNS	131	Standard query response 0x8660 No such name PTR 8.2.0.10
5	0.258840102	10.0.2.15	10.0.2.8	TCP	58	43587 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	0.259524132	10.0.2.8	10.0.2.15	TCP	60	21 → 43587 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	0.358912099	10.0.2.15	10.0.2.8	TCP	58	43588 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	0.359342729	10.0.2.8	10.0.2.15	TCP	60	21 → 43588 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

▶ Frame 5: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0

▶ Ethernet II, Src: PcsCompu_81:b1:df (08:00:27:81:b1:df), Dst: PcsCompu_ac:5e:f0 (08:00:27:ac:5e:f0)

▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.8

100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 44

0000	08 00 27 ac 5e f0 08 00 27 81 b1 df 08 00 45 00	..^.....E.
0010	00 2c d9 56 00 00 2a 06 9f 5f 0a 00 02 0f 0a 00	..V...*.....
0020	02 08 aa 43 00 15 a2 72 a6 7c 00 00 00 00 60 02	...C...r.
0030	04 00 88 c8 00 00 02 04 05 b4

Ethernet (eth), 14 bytes

Packets: 8 · Displayed: 8 (100.0%)

>>> Nmap

Host discovery

Aplicaciones ▾ Lugares ▾ Terminal ▾ lun 05:13 1

root@kali: ~

Archivo Editar Ver Buscar Terminal Ayuda

root@kali:~# nmap -PS -p 21 10.0.2.0/24

Starting Nmap 7.60 (<https://nmap.org>) at 2017-11-27 05:10 EST
Nmap scan report for 10.0.2.1
Host is up (0.00033s latency).

PORT STATE SERVICE
21/tcp closed ftp
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Wellcome to Wireshark

Nmap scan report for 10.0.2.2
Host is up (0.00049s latency).

...using this filter: All interfaces shown ▾

PORT STATE SERVICE
21/tcp closed ftp
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
Host is up (0.00033s latency).

PORT STATE SERVICE
21/tcp filtered ftp
MAC Address: 08:00:27:E4:8D:49 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.4
Host is up (0.00030s latency).

PORT STATE SERVICE
21/tcp closed ftp
MAC Address: 08:00:27:AC:5E:F0 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.15
Host is up (0.000066s latency).

PORT STATE SERVICE
21/tcp closed ftp

Nmap done: 256 IP addresses (5 hosts up) scanned in 2.80 seconds

root@kali:~#

No Packets

[5. Nmap]\$ _

Learn More · Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 2.4.1 (Git Rev Unknown from unknown).

>>> Nmap

Host discovery

Aplicaciones ▾ Lugares ▾ Wireshark ▾ lun 05:15 1

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
519	5.628503861	10.0.2.15	10.0.2.1	DNS	81	Standard query 0x8efd PTR 1.2.0.10.in-addr.arpa
520	5.628634748	10.0.2.15	10.0.2.1	DNS	81	Standard query 0x8efe PTR 2.2.0.10.in-addr.arpa
521	5.628685494	10.0.2.15	10.0.2.1	DNS	81	Standard query 0x8eff PTR 3.2.0.10.in-addr.arpa
522	5.628750137	10.0.2.15	10.0.2.1	DNS	81	Standard query 0x8f00 PTR 8.2.0.10.in-addr.arpa
523	5.631763113	10.0.2.1	10.0.2.15	DNS	131	Standard query response 0x8efd No such name PTR 1.2.0.10.in-addr.arpa
524	5.631819453	10.0.2.1	10.0.2.15	DNS	131	Standard query response 0x8efe No such name PTR 2.2.0.10.in-addr.arpa
525	5.631826012	10.0.2.1	10.0.2.15	DNS	131	Standard query response 0x8eff No such name PTR 3.2.0.10.in-addr.arpa
526	5.632470994	10.0.2.1	10.0.2.15	DNS	131	Standard query response 0x8f00 No such name PTR 8.2.0.10.in-addr.arpa
527	5.632997505	10.0.2.15	10.0.2.1	DNS	82	Standard query 0x8f01 PTR 15.2.0.10.in-addr.arpa
528	5.637937456	10.0.2.1	10.0.2.15	DNS	132	Standard query response 0x8f01 No such name PTR 15.2.0.10.in-addr.arpa
529	5.674572882	10.0.2.15	10.0.2.2	TCP	58	50495 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
530	5.674674555	10.0.2.15	10.0.2.3	TCP	58	50495 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
531	5.674721647	10.0.2.15	10.0.2.8	TCP	58	50495 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
532	5.674769375	10.0.2.15	10.0.2.1	TCP	58	50495 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
533	5.675242500	10.0.2.1	10.0.2.15	TCP	60	21 → 50495 [RST, ACK] Seq=1 Ack=1 Win=32768 Len=0
534	5.675267457	10.0.2.2	10.0.2.15	TCP	60	21 → 50495 [RST, ACK] Seq=1 Ack=1 Win=32768 Len=0
535	5.675285611	10.0.2.8	10.0.2.15	TCP	60	21 → 50495 [RST, ACK] Seq=1 Ack=1 Win=32768 Len=0
536	5.774657714	10.0.2.15	10.0.2.2	TCP	58	50496 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
537	5.775063931	10.0.2.2	10.0.2.15	TCP	60	21 → 50496 [RST, ACK] Seq=1 Ack=1 Win=32768 Len=0
538	5.780109228	10.0.2.15	10.0.2.1	TCP	58	50496 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
539	5.780154984	10.0.2.15	10.0.2.3	TCP	58	50496 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
540	5.780193565	10.0.2.15	10.0.2.8	TCP	58	50496 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
541	5.780260002	10.0.2.1	10.0.2.15	TCP	60	21 → 50496 [RST, ACK] Seq=1 Ack=1 Win=32768 Len=0
542	5.780536327	10.0.2.8	10.0.2.15	TCP	60	21 → 50496 [RST, ACK] Seq=1 Ack=1 Win=32768 Len=0

0000 ff ff ff ff ff ff 08 00 27 81 b1 df 08 06 00 01 '.....
0010 08 00 06 04 00 01 08 00 27 81 b1 df 0a 00 02 0f '.....

Ethernet (eth), 14 bytes Packets: 542 · Displayed: 542 (100.0%)

[5. Nmap]\$ _

[15/20]

>>> Nmap

Port analysis

- * Attack vector
- * Send different types of packets
- * Analyse the answer

```
root@kali:~# nmap -sU 10.0.2.8
Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-27 05:19 EST
Nmap scan report for 10.0.2.8
Host is up (0.00037s latency).
Not shown: 992 closed ports
PORT      STATE      SERVICE
123/udp    open       ntp
137/udp    open       netbios-ns
138/udp    open|filtered netbios-dgm
445/udp    open|filtered microsoft-ds
500/udp    open|filtered isakmp
1025/udp   open|filtered blackjack
1900/udp   open|filtered upnp
4500/udp   open|filtered nat-t-ike
MAC Address: 08:00:27:AC:5E:F0 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 3.49 seconds
```

>>> Nmap

Port analysis

Aplicaciones ▾ Lugares ▾ Wireshark ▾ lun 05:28 1

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1308	1.424769068	10.0.2.15	10.0.2.8	UDP	42	36028 → 1051 Len=0
1309	1.424802579	10.0.2.15	10.0.2.8	UDP	42	36028 → 45928 Len=0
1310	1.424834793	10.0.2.15	10.0.2.8	UDP	42	36028 → 47808 Len=0
1311	1.424884352	10.0.2.8	10.0.2.15	ICMP	70	Destination unreachable (Port unreachable)
1312	1.424890595	10.0.2.8	10.0.2.15	ICMP	70	Destination unreachable (Port unreachable)
1313	1.424893659	10.0.2.8	10.0.2.15	ICMP	70	Destination unreachable (Port unreachable)
1314	1.424896774	10.0.2.8	10.0.2.15	ICMP	70	Destination unreachable (Port unreachable)
1315	1.425091458	10.0.2.8	10.0.2.15	NTP	90	NTP Version 3, server
1316	1.425110567	10.0.2.15	10.0.2.8	ICMP	118	Destination unreachable (Port unreachable)
1317	1.425128946	10.0.2.8	10.0.2.15	ICMP	110	Destination unreachable (Port unreachable)
1318	1.425132172	10.0.2.8	10.0.2.15	ICMP	70	Destination unreachable (Port unreachable)
1319	1.425133948	10.0.2.8	10.0.2.15	ICMP	70	Destination unreachable (Port unreachable)
1320	1.425200619	10.0.2.8	10.0.2.15	ICMP	70	Destination unreachable (Port unreachable)
1321	1.425204118	10.0.2.8	10.0.2.15	ICMP	70	Destination unreachable (Port unreachable)
1322	1.427151919	10.0.2.15	10.0.2.8	UDP	42	36028 → 45685 Len=0
1323	1.427240730	10.0.2.15	10.0.2.8	UDP	42	36028 → 16779 Len=0
1324	1.427299056	10.0.2.15	10.0.2.8	UDP	42	36028 → 42431 Len=0
1325	1.427341221	10.0.2.15	10.0.2.8	UDP	42	36028 → 19605 Len=0
1326	1.427367300	10.0.2.8	10.0.2.15	ICMP	70	Destination unreachable (Port unreachable)
1327	1.427376671	10.0.2.15	10.0.2.8	UDP	42	36028 → 1067 Len=0
1328	1.427446317	10.0.2.15	10.0.2.8	UDP	42	36028 → 51255 Len=0
1329	1.427480513	10.0.2.15	10.0.2.8	UDP	42	36028 → 49172 Len=0
1330	1.427510338	10.0.2.15	10.0.2.8	UDP	42	36028 → 1024 Len=0
1331	1.427510502	10.0.2.8	10.0.2.15	ICMP	70	Destination unreachable (Port unreachable)
1332	1.427516820	10.0.2.8	10.0.2.15	ICMP	70	Destination unreachable (Port unreachable)
1333	1.427520182	10.0.2.8	10.0.2.15	ICMP	70	Destination unreachable (Port unreachable)
1334	1.427522205	10.0.2.8	10.0.2.15	ICMP	70	Destination unreachable (Port unreachable)

Ethernet (eth), 14 bytes

Packets: 2018 · Displayed: 2018 (100.0%)

```
>>> Metasploit
```

- * Vulnerabilities
- * Exploits
- * Payloads



```
>>> Pros and cons
```

Pros:

- * Security evaluation of system
- * Unplanned functionalities
- * Administration

Cons:

- * Evil intentions
- * Never completely safe

>>> Bibliography

- * <http://www.openwall.com/john/doc/>
- * https://en.wikipedia.org/wiki/John_the_Ripper
- * <https://nmap.org/man/es>
- * <https://www.aircrack-ng.org/doku.php?id=aircrack-ng>
- * https://en.wikipedia.org/wiki/Metasploit_Project