



*Private Portable Pentest  
and Network Information Framework*

## **PENTEST REPORT**

**Name:** CP-5

**Description:** Teste para Ambiente Doméstico - 5

**Pentest date:** 2019-05-04 23:19:39

**Pentest elapsed time:** 00:01:24.09

**Report date:** 2019-05-04 23:45:27

**Created by:** user

## ***Result of the execution tools***

**Model:** Model CP-5

**Description:** Modelo para Caso Prático Amb. Doméstico

**Notes:**

---

**Tool:** Netstat

Command 1/4 > netstat -r

**# Line command output**

**1**

=====

**2** Interface List

**3** 15...54 ee 75 e6 97 27 .....Realtek PCIe GBE Family Controller

**4** 2...02 00 4c 4f 4f 50 .....Npcap Loopback Adapter

**5** 6...60 14 b3 c5 c9 d3 .....Microsoft Wi-Fi Direct Virtual Adapter #2

**6** 57...00 09 0f fe 00 01 .....Fortinet Virtual Ethernet Adapter (NDIS 6.30)

**7** 20...60 14 b3 c5 c9 d3 .....Realtek 8821AE Wireless LAN 802.11ac PCI-E NIC

**8** 16...60 14 b3 c5 c9 d4 .....Bluetooth Device (Personal Area Network)

**9** 1.....Software Loopback Interface 1

**10**

=====

**11** IPv4 Route Table

**12**

=====

**13** Active Routes:

**14** Network Destination Netmask Gateway Interface Metric

**15** 0.0.0.0 0.0.0.0 192.168.1.1 192.168.1.132 55

**16** 127.0.0.0 255.0.0.0 On-link 127.0.0.1 331

**17** 127.0.0.1 255.255.255.255 On-link 127.0.0.1 331

**18** 127.255.255.255 255.255.255.255 On-link 127.0.0.1 331

**19** 169.254.0.0 255.255.0.0 On-link 169.254.89.216 281

**20** 169.254.89.216 255.255.255.255 On-link 169.254.89.216 281

**21** 169.254.255.255 255.255.255.255 On-link 169.254.89.216 281  
**22** 192.168.1.0 255.255.255.0 On-link 192.168.1.132 311  
**23** 192.168.1.132 255.255.255.255 On-link 192.168.1.132 311  
**24** 192.168.1.255 255.255.255.255 On-link 192.168.1.132 311  
**25** 224.0.0.0 240.0.0.0 On-link 127.0.0.1 331  
**26** 224.0.0.0 240.0.0.0 On-link 192.168.1.132 311  
**27** 224.0.0.0 240.0.0.0 On-link 169.254.89.216 281  
**28** 255.255.255.255 255.255.255.255 On-link 127.0.0.1 331  
**29** 255.255.255.255 255.255.255.255 On-link 192.168.1.132 311  
**30** 255.255.255.255 255.255.255.255 On-link 169.254.89.216 281

**31**

=====

=====

**32** Persistent Routes:

**33** None

**34** IPv6 Route Table

**35**

=====

=====

**36** Active Routes:

**37** If Metric Network Destination Gateway

**38** 1 331 ::1/128 On-link

**39** 20 311 fe80::/64 On-link

**40** 2 281 fe80::/64 On-link

**41** 20 311 fe80::644c:d516:4a2a:24bd/128

**42** On-link

**43** 2 281 fe80::f1ac:26c5:3f1c:59d8/128

**44** On-link

**45** 1 331 ff00::/8 On-link

**46** 20 311 ff00::/8 On-link

**47** 2 281 ff00::/8 On-link

**48**

=====

=====

**49** Persistent Routes:

**Tool: Netstat**

Command 2/4 > netstat -s

**# Line command output**

- 1 IPv4 Statistics
- 2 Packets Received = 13215482
- 3 Received Header Errors = 0
- 4 Received Address Errors = 3291
- 5 Datagrams Forwarded = 0
- 6 Unknown Protocols Received = 77
- 7 Received Packets Discarded = 97969
- 8 Received Packets Delivered = 13961693
- 9 Output Requests = 14100843
- 10 Routing Discards = 0
- 11 Discarded Output Packets = 4170
- 12 Output Packet No Route = 1510
- 13 Reassembly Required = 46
- 14 Reassembly Successful = 18
- 15 Reassembly Failures = 0
- 16 Datagrams Successfully Fragmented = 0
- 17 Datagrams Failing Fragmentation = 0
- 18 Fragments Created = 0
- 19 IPv6 Statistics
- 20 Packets Received = 2527
- 21 Received Header Errors = 0
- 22 Received Address Errors = 478
- 23 Datagrams Forwarded = 0
- 24 Unknown Protocols Received = 0
- 25 Received Packets Discarded = 7669
- 26 Received Packets Delivered = 498559
- 27 Output Requests = 515035
- 28 Routing Discards = 0
- 29 Discarded Output Packets = 0

30 Output Packet No Route = 2  
31 Reassembly Required = 0  
32 Reassembly Successful = 0  
33 Reassembly Failures = 0  
34 Datagrams Successfully Fragmented = 0  
35 Datagrams Failing Fragmentation = 0  
36 Fragments Created = 0  
37 ICMPv4 Statistics  
38 Received Sent  
39 Messages 1897 2863  
40 Errors 0 0  
41 Destination Unreachable 1896 2862  
42 Time Exceeded 0 0  
43 Parameter Problems 0 0  
44 Source Quenches 0 0  
45 Redirects 0 0  
46 Echo Replies 1 0  
47 Echos 0 1  
48 Timestamps 0 0  
49 Timestamp Replies 0 0  
50 Address Masks 0 0  
51 Address Mask Replies 0 0  
52 Router Solicitations 0 0  
53 Router Advertisements 0 0  
54 ICMPv6 Statistics  
55 Received Sent  
56 Messages 18 435  
57 Errors 0 0  
58 Destination Unreachable 0 0  
59 Packet Too Big 0 0  
60 Time Exceeded 0 0  
61 Parameter Problems 0 0  
62 Echos 0 0  
63 Echo Replies 0 0

64 MLD Queries 0 0  
65 MLD Reports 0 0  
66 MLD Dones 0 0  
67 Router Solicitations 0 246  
68 Router Advertisements 0 0  
69 Neighbor Solicitations 0 97  
70 Neighbor Advertisements 18 92  
71 Redirects 0 0  
72 Router Renumberings 0 0  
73 TCP Statistics for IPv4  
74 Active Opens = 107160  
75 Passive Opens = 6007  
76 Failed Connection Attempts = 76696  
77 Reset Connections = 4303  
78 Current Connections = 30  
79 Segments Received = 6611070  
80 Segments Sent = 12568606  
81 Segments Retransmitted = 286226  
82 TCP Statistics for IPv6  
83 Active Opens = 73771  
84 Passive Opens = 2977  
85 Failed Connection Attempts = 70792  
86 Reset Connections = 314  
87 Current Connections = 4  
88 Segments Received = 486851  
89 Segments Sent = 343619  
90 Segments Retransmitted = 141553  
91 UDP Statistics for IPv4  
92 Datagrams Received = 7299380  
93 No Ports = 92994  
94 Receive Errors = 12508  
95 Datagrams Sent = 1176116  
96 UDP Statistics for IPv6  
97 Datagrams Received = 20441

98 No Ports = 7106  
99 Receive Errors = 577  
100 Datagrams Sent = 22095

---

**Tool: Netstat**

Command 3/4 > netstat -fa

**# Line command output**

1 Active Connections  
2 Proto Local Address Foreign Address State  
3 TCP 0.0.0.0:80 DESKTOP-EAK7JTF:0 LISTENING  
4 TCP 0.0.0.0:135 DESKTOP-EAK7JTF:0 LISTENING  
5 TCP 0.0.0.0:445 DESKTOP-EAK7JTF:0 LISTENING  
6 TCP 0.0.0.0:5040 DESKTOP-EAK7JTF:0 LISTENING  
7 TCP 0.0.0.0:49664 DESKTOP-EAK7JTF:0 LISTENING  
8 TCP 0.0.0.0:49665 DESKTOP-EAK7JTF:0 LISTENING  
9 TCP 0.0.0.0:49666 DESKTOP-EAK7JTF:0 LISTENING  
10 TCP 0.0.0.0:49667 DESKTOP-EAK7JTF:0 LISTENING  
11 TCP 0.0.0.0:49668 DESKTOP-EAK7JTF:0 LISTENING  
12 TCP 0.0.0.0:49669 DESKTOP-EAK7JTF:0 LISTENING  
13 TCP 127.0.0.1:843 DESKTOP-EAK7JTF:0 LISTENING  
14 TCP 127.0.0.1:3306 DESKTOP-EAK7JTF:0 LISTENING  
15 TCP 127.0.0.1:3306 DESKTOP-EAK7JTF:29808 TIME\_WAIT  
16 TCP 127.0.0.1:3306 DESKTOP-EAK7JTF:29811 TIME\_WAIT  
17 TCP 127.0.0.1:3306 DESKTOP-EAK7JTF:29817 TIME\_WAIT  
18 TCP 127.0.0.1:3306 DESKTOP-EAK7JTF:29820 ESTABLISHED  
19 TCP 127.0.0.1:3306 DESKTOP-EAK7JTF:29822 ESTABLISHED  
20 TCP 127.0.0.1:17600 DESKTOP-EAK7JTF:0 LISTENING  
21 TCP 127.0.0.1:27493 DESKTOP-EAK7JTF:27494 ESTABLISHED  
22 TCP 127.0.0.1:27494 DESKTOP-EAK7JTF:27493 ESTABLISHED  
23 TCP 127.0.0.1:29808 DESKTOP-EAK7JTF:3306 TIME\_WAIT  
24 TCP 127.0.0.1:29811 DESKTOP-EAK7JTF:3306 TIME\_WAIT  
25 TCP 127.0.0.1:29817 DESKTOP-EAK7JTF:3306 TIME\_WAIT  
26 TCP 127.0.0.1:29820 DESKTOP-EAK7JTF:3306 ESTABLISHED  
27 TCP 127.0.0.1:29822 DESKTOP-EAK7JTF:3306 ESTABLISHED

28 TCP 127.0.0.1:35153 DESKTOP-EAK7JTF:0 LISTENING  
29 TCP 169.254.89.216:139 DESKTOP-EAK7JTF:0 LISTENING  
30 TCP 192.168.1.132:139 DESKTOP-EAK7JTF:0 LISTENING  
31 TCP 192.168.1.132:27409 40.67.254.36:https ESTABLISHED  
32 TCP 192.168.1.132:27422 wr-in-f188.1e100.net:5228 ESTABLISHED  
33 TCP 192.168.1.132:27497 162.125.68.3:https CLOSE\_WAIT  
34 TCP 192.168.1.132:27528 ec2-34-192-22-186.compute-1.amazonaws.com:https  
CLOSE\_WAIT  
35 TCP 192.168.1.132:27529 a95-101-25-129.deploy.static.akamaitechnologies.com:https  
CLOSE\_WAIT  
36 TCP 192.168.1.132:27530 a95-101-25-129.deploy.static.akamaitechnologies.com:https  
CLOSE\_WAIT  
37 TCP 192.168.1.132:27531 a95-101-25-129.deploy.static.akamaitechnologies.com:https  
CLOSE\_WAIT  
38 TCP 192.168.1.132:27532 a2-21-170-216.deploy.static.akamaitechnologies.com:http  
CLOSE\_WAIT  
39 TCP 192.168.1.132:27533 a2-21-170-216.deploy.static.akamaitechnologies.com:http  
CLOSE\_WAIT  
40 TCP 192.168.1.132:27535 a2-21-170-216.deploy.static.akamaitechnologies.com:http  
CLOSE\_WAIT  
41 TCP 192.168.1.132:27536 a2-21-170-216.deploy.static.akamaitechnologies.com:http  
CLOSE\_WAIT  
42 TCP 192.168.1.132:27537 a2-21-170-216.deploy.static.akamaitechnologies.com:http  
CLOSE\_WAIT  
43 TCP 192.168.1.132:27538 a2-21-170-216.deploy.static.akamaitechnologies.com:http  
CLOSE\_WAIT  
44 TCP 192.168.1.132:28704 162.125.68.7:https CLOSE\_WAIT  
45 TCP 192.168.1.132:28768 muc03s14-in-f5.1e100.net:https ESTABLISHED  
46 TCP 192.168.1.132:28972 ec2-34-237-73-95.compute-1.amazonaws.com:https  
ESTABLISHED  
47 TCP 192.168.1.132:29390 162.125.68.10:https ESTABLISHED  
48 TCP 192.168.1.132:29569 162.125.33.7:https CLOSE\_WAIT  
49 TCP 192.168.1.132:29576 getclicky.com:https ESTABLISHED  
50 TCP 192.168.1.132:29592 162.125.34.129:https ESTABLISHED  
51 TCP 192.168.1.132:29599 162.125.68.3:https CLOSE\_WAIT  
52 TCP 192.168.1.132:29753 162.125.68.3:https ESTABLISHED  
53 TCP 192.168.1.132:29780 162.125.18.133:https ESTABLISHED



54 TCP 192.168.1.132:29783 mad07s10-in-f7.1e100.net:https ESTABLISHED  
55 TCP 192.168.1.132:29809 mad06s25-in-f4.1e100.net:http TIME\_WAIT  
56 TCP 192.168.1.132:29818 mad06s25-in-f4.1e100.net:http TIME\_WAIT  
57 TCP [::]:80 DESKTOP-EAK7JTF:0 LISTENING  
58 TCP [::]:135 DESKTOP-EAK7JTF:0 LISTENING  
59 TCP [::]:445 DESKTOP-EAK7JTF:0 LISTENING  
60 TCP [::]:49664 DESKTOP-EAK7JTF:0 LISTENING  
61 TCP [::]:49665 DESKTOP-EAK7JTF:0 LISTENING  
62 TCP [::]:49666 DESKTOP-EAK7JTF:0 LISTENING  
63 TCP [::]:49667 DESKTOP-EAK7JTF:0 LISTENING  
64 TCP [::]:49668 DESKTOP-EAK7JTF:0 LISTENING  
65 TCP [::]:49669 DESKTOP-EAK7JTF:0 LISTENING  
66 TCP [::1]:80 DESKTOP-EAK7JTF:29813 ESTABLISHED  
67 TCP [::1]:29813 DESKTOP-EAK7JTF:http ESTABLISHED  
68 UDP 0.0.0.0:5353 \*:.\*  
69 UDP 0.0.0.0:5353 \*:.\*  
70 UDP 0.0.0.0:5353 \*:.\*  
71 UDP 0.0.0.0:5353 \*:.\*  
72 UDP 0.0.0.0:5353 \*:.\*  
73 UDP 0.0.0.0:5353 \*:.\*  
74 UDP 0.0.0.0:5355 \*:.\*  
75 UDP 0.0.0.0:55092 \*:.\*  
76 UDP 0.0.0.0:56062 \*:.\*  
77 UDP 0.0.0.0:62209 \*:.\*  
78 UDP 127.0.0.1:1900 \*:.\*  
79 UDP 127.0.0.1:50987 \*:.\*  
80 UDP 127.0.0.1:59982 \*:.\*  
81 UDP 169.254.89.216:137 \*:.\*  
82 UDP 169.254.89.216:138 \*:.\*  
83 UDP 169.254.89.216:1900 \*:.\*  
84 UDP 169.254.89.216:2177 \*:.\*  
85 UDP 169.254.89.216:50985 \*:.\*  
86 UDP 192.168.1.132:137 \*:.\*  
87 UDP 192.168.1.132:138 \*:.\*

88 UDP 192.168.1.132:1900 \*:\*  
89 UDP 192.168.1.132:2177 \*:\*  
90 UDP 192.168.1.132:50986 \*:\*  
91 UDP [::]:5353 \*:\*  
92 UDP [::]:5353 \*:\*  
93 UDP [::]:5353 \*:\*  
94 UDP [::]:5355 \*:\*  
95 UDP [::1]:1900 \*:\*  
96 UDP [::1]:50984 \*:\*  
97 UDP [fe80::644c:d516:4a2a:24bd%20]:1900 \*:\*  
98 UDP [fe80::644c:d516:4a2a:24bd%20]:2177 \*:\*  
99 UDP [fe80::644c:d516:4a2a:24bd%20]:50983 \*:\*  
100 UDP [fe80::f1ac:26c5:3f1c:59d8%2]:546 \*:\*  
101 UDP [fe80::f1ac:26c5:3f1c:59d8%2]:1900 \*:\*  
102 UDP [fe80::f1ac:26c5:3f1c:59d8%2]:2177 \*:\*  
103 UDP [fe80::f1ac:26c5:3f1c:59d8%2]:50982 \*:\*

---

#### **Tool: PsLoggedOn**

Command 4/4 > tools\PsLoggedon.exe -nobanner

#### **# Line command output**

- 1 Users logged on locally:
- 2 04/05/2019 21:31:40 - DESKTOP-EAK7JTF\Lenovo
- 3 No one is logged on via resource shares.

### ***Tools used in pentest***

#### **Tool #1: Netstat**

**Description:** Netstat is a useful tool for checking network and Internet connections. Some useful applications for the average PC user are considered, including checking for malware connections.

#### **Notes:**

---

#### **Tool #2: PsLoggedOn**

**Description:** Display active logon sessions locally and via resources shares

**Notes:**

---