Private Portable Pentest
and Network Information Framework

PENTEST REPORT

Name: CP-3
Description: Teste para ambiente Doméstico - 3

Pentest date: 2019-05-06 22:18:25
Pentest elapsed time: 00:00:06.25
Report date: 2019-05-06 22:44:56

Created by: user

Result of the execution tools

Model: Model CP-3

Description: Modelo para Caso Prático Amb. Doméstico

Notes: Modelo para obter informação das redes sem fios e interfaces num ambiente doméstico

---

Tool: Netsh

`Command 1/5 > Netsh wlan show networks`

#	Line command output
1	Interface name : Wi-Fi
2	There are 13 networks currently visible.
3	SSID 1 : ShinChan
4	Network type : Infrastructure
5	Authentication : WPA2-Personal
6	Encryption : CCMP
7	SSID 2 : MEO-WiFi
8	Network type : Infrastructure
9	Authentication : Open
10	Encryption : None
11	SSID 3 : delsinhocorreria
12	Network type : Infrastructure
13	Authentication : WPA2-Personal
14	Encryption : CCMP
15	SSID 4 : MEO-9BA1D0
16	Network type : Infrastructure
17	Authentication : WPA2-Personal
18	Encryption : CCMP
19	SSID 5 : Vodafone-3ABEE2
20	Network type : Infrastructure
21	Authentication : WPA2-Personal
22	Encryption : CCMP
23	SSID 6 : Vodafone-F75FA5_2
24	Network type : Infrastructure
25	Authentication : WPA2-Personal

26 Encryption : CCMP
27 SSID 7 : MEO_SOUSA
28 Network type : Infrastructure
29 Authentication : WPA2-Personal
30 Encryption : CCMP
31 SSID 8 : NOS-2526
32 Network type : Infrastructure
33 Authentication : WPA2-Personal
34 Encryption : CCMP
35 SSID 9 : Parceiros
36 Network type : Infrastructure
37 Authentication : WPA2-Personal
38 Encryption : CCMP
39 SSID 10 : Bro:s House
40 Network type : Infrastructure
41 Authentication : WPA2-Personal
42 Encryption : CCMP
43 SSID 11 : MEO-8A1D91
44 Network type : Infrastructure
45 Authentication : WPA2-Personal
46 Encryption : CCMP
47 SSID 12 : XIX
48 Network type : Infrastructure
49 Authentication : WPA2-Personal
50 Encryption : CCMP
51 SSID 13 :
52 Network type : Infrastructure
53 Authentication : Open
54 Encryption : WEP

Tool: Netsh

`Command 2/5 > Netsh wlan show profiles`

 # Line command output

1 Profiles on interface Wi-Fi:

2 Group policy profiles (read only)

3 ---------------------------------

4

5 User profiles

6 -------------

7 All User Profile : eduroam

8 All User Profile : ShinChan

Tool: Netsh

`Command 3/5 > Netsh wlan show drivers`

#	**Line command output**
1	Interface name: Wi-Fi
2	Driver : Realtek 8821AE LAN sem fios 802.11ac PCI-E NIC
3	Vendor : Realtek Semiconductor Corp.
4	Provider : Microsoft
5	Date : 09/01/2018
6	Version : 2023.70.109.2018
7	INF file : netrtwlane.inf
8	Type : Native Wi-Fi Driver
9	Radio types supported : 802.11n 802.11g 802.11b 802.11ac 802.11n 802.11a
10	FIPS 140-2 mode supported : Yes
11	802.11w Management Frame Protection supported : Yes
12	Hosted network supported : No
13	Authentication and cipher supported in infrastructure mode:
14	Open None
15	WPA2-Personal CCMP
16	Open WEP-40bit
17	Open WEP-104bit
18	Open WEP
19	WPA-Enterprise TKIP
20	WPA-Personal TKIP
21	WPA2-Enterprise TKIP
22	WPA2-Personal TKIP
23	WPA-Enterprise CCMP

24 WPA-Personal CCMP
25 WPA2-Enterprise CCMP
26 Vendor defined TKIP
27 Vendor defined CCMP
28 Vendor defined Vendor defined
29 Vendor defined Vendor defined
30 WPA2-Enterprise Vendor defined
31 WPA2-Enterprise Vendor defined
32 Vendor defined Vendor defined
33 Vendor defined Vendor defined
34 Wireless Display Supported: Yes (Graphics Driver: Yes, Wi-Fi Driver: Yes)

Tool: Netsh

```
Command 4/5 > Netsh wlan show interfaces
```

#	Line command output
1	There is 1 interface on the system:
2	Name : Wi-Fi
3	Description : Realtek 8821AE Wireless LAN 802.11ac PCI-E NIC
4	GUID : ec6e4695-8f21-4be8-95d2-25b5172e6f0d
5	Physical address : 60:14:b3:c5:c9:d3
6	State : connected
7	SSID : ShinChan
8	BSSID : c8:8d:83:64:49:c0
9	Network type : Infrastructure
10	Radio type : 802.11n
11	Authentication : WPA2-Personal
12	Cipher : CCMP
13	Connection mode : Auto Connect
14	Channel : 8
15	Receive rate (Mbps) : 72.2
16	Transmit rate (Mbps) : 72.2
17	Signal : 100%
18	Profile : ShinChan
19	Hosted network status : Not available

Tool: WifiInfoView

```
Command 5/5 > tools\WifiInfoView.exe /stab
```

 # Line command output

1 SSID - MAC Address - PHY Type - RSSI - Signal Quality - Average Signal Quality - Frequency - Channel - Information Size - Elements Count - Company - Router Model - Router Name - Security - Cipher - Maximum Speed - Channel Width - Channels Range - BSS Type - WPS Support - First Detection - Last Detection - Detection Count - Start Time - Minimum Signal Quality - Maximum Signal Quality - 802.11 Standards - Connected - Stations Count - Channel Utilization - Country Code - Description -

2 - 62-45-B6-05-B7-DE - 802.11a - -51 - 100 - 100.0 - 5,220 - 44 - 20 - 2 - - - - WEP - WEP - 0 Mbps - 20 MHz - 42 - 46 - Infrastructure - No - 06/05/2019 22:18:24 - 06/05/2019 22:18:24 - 1 - 19/04/2019 08:41:32 - 100 - 100 - - No - - - - -

3 Bro:s House - 70-4F-57-81-BE-FF - 802.11g/n - -82 - 15 - 15.0 - 2,417 - 2 - 224 - 14 - TP-LINK TECHNOLOGIES CO.,LTD. - - - WPA2-PSK - CCMP - 300 Mbps - 40 MHz - 1 - 8 - Infrastructure - Configured - 06/05/2019 22:18:24 - 06/05/2019 22:18:24 - 1 - 22/04/2019 16:08:25 - 15 - 15 - 802.11e/i - No - 0 - 0.0% - - -

4 delsinhocorreria - 00-06-91-7E-E5-B0 - 802.11g/n - -84 - 6 - 6.0 - 2,462 - 11 - 261 - 16 - PT Inovacao - - - WPA-PSK + WPA2-PSK - TKIP+CCMP - 216 Mbps - 20 MHz - 9 - 13 - Infrastructure - Configured - 06/05/2019 22:18:24 - 06/05/2019 22:18:24 - 1 - 04/05/2019 15:19:59 - 6 - 6 - 802.11e/i - No - 1 - 7.5% - - -

5 MEO-8A1D91 - 9C-97-26-8A-1D-91 - 802.11g/n - -78 - 35 - 35.0 - 2,437 - 6 - 214 - 15 - Technicolor - - - WPA-PSK + WPA2-PSK - TKIP+CCMP - 130 Mbps - 20 MHz - 4 - 8 - Infrastructure - Configured - 06/05/2019 22:18:24 - 06/05/2019 22:18:24 - 1 - 21/01/2019 00:10:17 - 35 - 35 - 802.11i - No - - - - -

6 MEO-9BA1D0 - 00-06-91-9B-A1-D0 - 802.11g/n - -88 - 12 - 12.0 - 2,437 - 6 - 255 - 16 - PT Inovacao - - - WPA-PSK + WPA2-PSK - TKIP+CCMP - 216 Mbps - 20 MHz - 4 - 8 - Infrastructure - Configured - 06/05/2019 22:18:24 - 06/05/2019 22:18:24 - 1 - 20/04/2019 15:34:50 - 12 - 12 - 802.11e/i - No - 5 - 15.3% - - -

7 MEO-WiFi - 9E-97-26-8A-1D-92 - 802.11g/n - -78 - 35 - 35.0 - 2,437 - 6 - 140 - 12 - - - - None - None - 130 Mbps - 20 MHz - 4 - 8 - Infrastructure - No - 06/05/2019 22:18:24 - 06/05/2019 22:18:24 - 1 - 21/01/2019 00:10:17 - 35 - 35 - - No - - - - -

8 MEO-WiFi - 0A-76-FF-06-DE-C8 - 802.11g/n - -83 - 15 - 15.0 - 2,412 - 1 - 130 - 11 - - - - None - None - 130 Mbps - 20 MHz - 1 - 3 - Infrastructure - No - 06/05/2019 22:18:24 - 06/05/2019 22:18:24 - 1 - 02/04/2019 15:17:25 - 15 - 15 - - No - - - - -

9 MEO-WiFi - 00-06-91-9B-A1-D2 - 802.11g/n - -84 - 5 - 5.0 - 2,437 - 6 - 148 - 13 - PT Inovacao - - - None - None - 216 Mbps - 20 MHz - 4 - 8 - Infrastructure - No - 06/05/2019 22:18:24 - 06/05/2019 22:18:24 - 1 - 20/04/2019 15:34:50 - 5 - 5 - 802.11e - No - 0 - 15.3% - - -

10 MEO_SOUSA - 08-76-FF-06-DE-C7 - 802.11g/n - -84 - 14 - 14.0 - 2,412 - 1 - 203 - 14 - Thomson Telecom Belgium - - - WPA-PSK + WPA2-PSK - TKIP+CCMP - 130 Mbps - 20 MHz - 1 - 3 - Infrastructure - Configured - 06/05/2019 22:18:24 - 06/05/2019 22:18:24 - 1 -

02/04/2019 15:17:25 - 14 - 14 - 802.11i - No - - - - -

11 NOS-2526 - 44-34-A7-2C-25-26 - 802.11g/n - -82 - 15 - 15.0 - 2,462 - 11 - 249 - 15 - ARRIS Group, Inc. - - - WPA2-PSK - CCMP - 216 Mbps - 20 MHz - 9 - 13 - Infrastructure - Configured - 06/05/2019 22:18:24 - 06/05/2019 22:18:24 - 1 - 21/04/2019 19:17:23 - 15 - 15 - 802.11d/e/i - No - 0 - 20.0% - PT - -

12 Parceiros - 04-B0-E7-52-ED-68 - 802.11g/n - -82 - 15 - 15.0 - 2,432 - 5 - 268 - 18 - HUAWEI TECHNOLOGIES CO.,LTD - - - WPA-PSK + WPA2-PSK - TKIP+CCMP - 216 Mbps - 20 MHz - 3 - 7 - Infrastructure - Configured - 06/05/2019 22:18:24 - 06/05/2019 22:18:24 - 1 - 06/05/2019 17:04:56 - 15 - 15 - 802.11d/e/i - No - 2 - 3.1% - PT - -

13 ShinChan - C8-8D-83-64-49-C4 - 802.11n/ac - -49 - 100 - 100.0 - 5,220 - 44 - 437 - 20 - HUAWEI TECHNOLOGIES CO.,LTD - Huawei - HG8245Q - WPA-PSK + WPA2-PSK - TKIP+CCMP - 1300 Mbps - 80 MHz - 42 - 58 - Infrastructure - Configured - 06/05/2019 22:18:24 - 06/05/2019 22:18:24 - 1 - 07/04/2019 01:27:39 - 100 - 100 - 802.11d/e/h/i - No - 1 - 1.6% - PT - -

14 ShinChan - C8-8D-83-64-49-C0 - 802.11g/n - -54 - 100 - 100.0 - 2,447 - 8 - 226 - 17 - HUAWEI TECHNOLOGIES CO.,LTD - - - WPA-PSK + WPA2-PSK - TKIP+CCMP - 216 Mbps - 20 MHz - 6 - 10 - Infrastructure - No - 06/05/2019 22:18:24 - 06/05/2019 22:18:24 - 1 - 07/04/2019 01:27:01 - 100 - 100 - 802.11d/e/i - Yes - 3 - 6.7% - PT - -

15 Vodafone-3ABEE2 - C4-B8-B4-3A-BE-E8 - 802.11g/n - -71 - 55 - 55.0 - 2,447 - 8 - 296 - 18 - HUAWEI TECHNOLOGIES CO.,LTD - - - WPA-PSK + WPA2-PSK - TKIP+CCMP - 216 Mbps - 20 MHz - 6 - 10 - Infrastructure - Configured - 06/05/2019 22:18:24 - 06/05/2019 22:18:24 - 1 - 06/05/2019 17:43:23 - 55 - 55 - 802.11d/i - No - - - PT - -

16 Vodafone-3ABEE2 - C4-B8-B4-3A-BE-EC - 802.11n/ac - -82 - 14 - 14.0 - 5,220 - 44 - 377 - 20 - HUAWEI TECHNOLOGIES CO.,LTD - - - WPA-PSK + WPA2-PSK - TKIP+CCMP - 1733 Mbps - 80 MHz - 42 - 58 - Infrastructure - Configured - 06/05/2019 22:18:24 - 06/05/2019 22:18:24 - 1 - 07/04/2019 01:24:29 - 14 - 14 - 802.11d/i - No - - - PT - -

17 Vodafone-F75FA5_2 - 02-11-6B-74-05-D5 - 802.11g/n - -86 - 14 - 14.0 - 2,412 - 1 - 208 - 14 - - - - WPA-PSK + WPA2-PSK - TKIP+CCMP - 144 Mbps - 20 MHz - 1 - 3 - Infrastructure - No - 06/05/2019 22:18:24 - 06/05/2019 22:18:24 - 1 - 06/05/2019 20:25:30 - 14 - 14 - 802.11d/i - No - - - IT - -

18 XIX - 28-F0-76-14-49-FA - 802.11g/n - -71 - 65 - 65.0 - 2,462 - 11 - 166 - 12 - Apple, Inc. - - - WPA2-PSK - CCMP - 216 Mbps - 20 MHz - 9 - 13 - Infrastructure - No - 06/05/2019 22:18:24 - 06/05/2019 22:18:24 - 1 - 06/05/2019 10:05:22 - 65 - 65 - 802.11i - No - - - - -

Tools used in pentest

Tool #1: Netsh

Description: Network shell (netsh) is a command-line utility that allows you to configure and display the status of various network communications

Notes:

Tool #2: WifiInfoView

Description: Scans the wireless networks and displays extensive information.

Notes: Save the list of wireless networks into a tab-delimited text file.
