3PNiF

Private Portable Pentest
and Network Information Framework

PENTEST REPORT

Name: CP-1

Description: Teste para Ambiente Doméstico - 1

Pentest date: 2019-05-04 18:03:00

Pentest elapsed time: 00:00:50.43

Report date: 2019-05-04 18:08:56

Created by: user

Result of the execution tools

Model: Model CP-1

Description: Modelo para Caso Prático Amb. Doméstico

Notes: Modelo para deteção de equipamentos na rede, estados portos locais e systeminfo.

Tool: _Tool nmap

```
Command 1/3 > tools\nmap\\nmap.exe -sP 192.168.1.0/24
```

**Line command output**

1 Starting Nmap 7.70 (https://nmap.org) at 2019-05-04 18:02 Hora de Veru00e3o de GMT

2 Nmap scan report for vodafonegw (192.168.1.1)

3 Host is up (0.0064s latency).

4 MAC Address: C8:8D:83:64:49:B9 (Huawei Technologies)

5 Nmap scan report for unknown48f7c0ed31eb.lan (192.168.1.66)

6 Host is up (0.094s latency).

7 MAC Address: 48:F7:C0:ED:31:EB (Technicolor CH USA)

8 Nmap scan report for XboxOne.lan (192.168.1.235)

9 Host is up (0.015s latency).

10 MAC Address: F0:1D:BC:16:DE:32 (Microsoft)

11 Nmap scan report for DESKTOP-EAK7JTF.lan (192.168.1.132)

12 Host is up.

13 Nmap done: 256 IP addresses (4 hosts up) scanned in 10.73 seconds

---

Tool: _Tool nmap

```
Command 2/3 > tools\nmap\\nmap.exe -p 21,22,23,25,53,80,110,143 192.168.1.132
```

**Line command output**

1 Starting Nmap 7.70 (https://nmap.org) at 2019-05-04 18:02 Hora de Veru00e3o de GMT

2 Nmap scan report for DESKTOP-EAK7JTF.lan (192.168.1.132)

3 Host is up (0.00088s latency).

4 PORT STATE SERVICE

5 21/tcp closed ftp

6 22/tcp closed ssh

7 23/tcp closed telnet

8 25/tcp closed smtp

9   53/tcp closed domain

10   80/tcp open http

11   110/tcp closed pop3

12   143/tcp closed imap

13   Nmap done: 1 IP address (1 host up) scanned in 10.61 seconds

---

Tool: systeminfo

```
Command 3/3 > systeminfo
```

#	Line command output
1	Host Name: DESKTOP-EAK7JTF
2	OS Name: Microsoft Windows 10 Home
3	OS Version: 10.0.17763 N/A Build 17763
4	OS Manufacturer: Microsoft Corporation
5	OS Configuration: Standalone Workstation
6	OS Build Type: Multiprocessor Free
7	Registered Owner: Lenovo
8	Registered Organization:
9	Product ID: 00326-10000-00000-AA675
10	Original Install Date: 16/03/2019, 10:28:51
11	System Boot Time: 23/04/2019, 19:11:10
12	System Manufacturer: LENOVO
13	System Model: 80TL
14	System Type: x64-based PC
15	Processor(s): 1 Processor(s) Installed.
16	[01]: Intel64 Family 6 Model 78 Stepping 3 GenuineIntel ~1992 Mhz
17	BIOS Version: LENOVO 1KCN45WW, 19/06/2018
18	Windows Directory: C:\Windows
19	System Directory: C:\Windows\system32
20	Boot Device: \Device\HarddiskVolume2
21	System Locale: pt;Portuguu0088s (Portugal)
22	Input Locale: pt;Portuguu0088s (Portugal)
23	Time Zone: (UTC+00:00) Dublin, Edimburgo, Lisboa, Londres
24	Total Physical Memory: 12 085 MB
25	Available Physical Memory: 6 938 MB

26   Virtual Memory: Max Size: 13 941 MB

27   Virtual Memory: Available: 7 545 MB

28   Virtual Memory: In Use: 6 396 MB

29   Page File Location(s): C:\pagefile.sys

30   Domain: WORKGROUP

31   Logon Server: \DESKTOP-EAK7JTF

32   Hotfix(s): 9 Hotfix(s) Installed.

33   [01]: KB4486553

34   [02]: KB4470502

35   [03]: KB4470788

36   [04]: KB4480056

37   [05]: KB4480979

38   [06]: KB4489907

39   [07]: KB4493478

40   [08]: KB4493510

41   [09]: KB4493509

42   Network Card(s): 5 NIC(s) Installed.

43   [01]: Realtek PCIe GBE Family Controller

44   Connection Name: Ethernet

45   Status: Media disconnected

46   [02]: Realtek 8821AE Wireless LAN 802.11ac PCI-E NIC

47   Connection Name: Wi-Fi

48   DHCP Enabled: Yes

49   DHCP Server: 192.168.1.1

50   IP address(es)

51   [01]: 192.168.1.132

52   [02]: fe80::644c:d516:4a2a:24bd

53   [03]: Bluetooth Device (Personal Area Network)

54   Connection Name: Ligau0087u00c6o de Rede Bluetooth

55   Status: Media disconnected

56   [04]: Microsoft KM-TEST Loopback Adapter

57   Connection Name: Npcap Loopback Adapter

58   DHCP Enabled: Yes

59   DHCP Server: 255.255.255.255

60 IP address(es)

61 [01]: 169.254.89.216

62 [02]: fe80::f1ac:26c5:3f1c:59d8

63 [05]: Fortinet Virtual Ethernet Adapter (NDIS 6.30)

64 Connection Name: Ethernet 4

65 Status: Media disconnected

66 Hyper-V Requirements: VM Monitor Mode Extensions: Yes

67 Virtualization Enabled In Firmware: Yes

68 Second Level Address Translation: Yes

69 Data Execution Prevention Available: Yes

Tools used in pentest

Tool #1: _Tool nmap

Description: O Nmap("Network Mapper") é uma ferramenta de segurança usada para detectar computadores e serviços numa rede.

Notes: Testes com ferramenta nmap - nmap

Tool #2: systeminfo

Description: info about local system windows

Notes: