Private Portable Pentest
and Network Information Framework

PENTEST REPORT

Name: CP-4

Description: Teste para Ambiente Doméstico - 4

Pentest date: 2019-05-02 22:40:31

Pentest elapsed time: 00:00:02.77

Report date: 2019-05-02 23:10:24

Created by: user

Result of the execution tools

Model: Model CP-4

Description: Modelo para Caso Prático Amb. Doméstico

Notes: Modelo para obter informações da rede, acessos ao exterior (Internet) e processos.

Tool: Netstat

```
Command 1/6 > netstat -an
```

#	Line command output
1	Active Connections
2	Proto Local Address Foreign Address State
3	TCP 0.0.0.0:80 0.0.0.0:0 LISTENING
4	TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
5	TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
6	TCP 0.0.0.0:5040 0.0.0.0:0 LISTENING
7	TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING
8	TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING
9	TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING
10	TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING
11	TCP 0.0.0.0:49668 0.0.0.0:0 LISTENING
12	TCP 0.0.0.0:49669 0.0.0.0:0 LISTENING
13	TCP 127.0.0.1:843 0.0.0.0:0 LISTENING
14	TCP 127.0.0.1:3306 0.0.0.0:0 LISTENING
15	TCP 127.0.0.1:3306 127.0.0.1:14475 TIME_WAIT
16	TCP 127.0.0.1:3306 127.0.0.1:14476 TIME_WAIT
17	TCP 127.0.0.1:3306 127.0.0.1:14478 TIME_WAIT
18	TCP 127.0.0.1:3306 127.0.0.1:14488 TIME_WAIT
19	TCP 127.0.0.1:3306 127.0.0.1:14502 TIME_WAIT
20	TCP 127.0.0.1:3306 127.0.0.1:14512 TIME_WAIT
21	TCP 127.0.0.1:3306 127.0.0.1:14527 TIME_WAIT
22	TCP 127.0.0.1:3306 127.0.0.1:14530 ESTABLISHED
23	TCP 127.0.0.1:3306 127.0.0.1:14533 ESTABLISHED
24	TCP 127.0.0.1:14475 127.0.0.1:3306 TIME_WAIT
25	TCP 127.0.0.1:14476 127.0.0.1:3306 TIME_WAIT

```
26 TCP 127.0.0.1:14477 127.0.0.1:3306 TIME_WAIT
27 TCP 127.0.0.1:14478 127.0.0.1:3306 TIME_WAIT
28 TCP 127.0.0.1:14487 127.0.0.1:3306 TIME_WAIT
29 TCP 127.0.0.1:14488 127.0.0.1:3306 TIME_WAIT
30 TCP 127.0.0.1:14496 127.0.0.1:3306 TIME_WAIT
31 TCP 127.0.0.1:14502 127.0.0.1:3306 TIME_WAIT
32 TCP 127.0.0.1:14508 127.0.0.1:3306 TIME_WAIT
33 TCP 127.0.0.1:14512 127.0.0.1:3306 TIME_WAIT
34 TCP 127.0.0.1:14527 127.0.0.1:3306 TIME_WAIT
35 TCP 127.0.0.1:14530 127.0.0.1:3306 ESTABLISHED
36 TCP 127.0.0.1:14533 127.0.0.1:3306 ESTABLISHED
37 TCP 127.0.0.1:17600 0.0.0.0:0 LISTENING
38 TCP 127.0.0.1:21703 127.0.0.1:21704 ESTABLISHED
39 TCP 127.0.0.1:21704 127.0.0.1:21703 ESTABLISHED
40 TCP 127.0.0.1:35153 0.0.0.0:0 LISTENING
41 TCP 169.254.89.216:139 0.0.0.0:0 LISTENING
42 TCP 192.168.1.132:139 0.0.0.0:0 LISTENING
43 TCP 192.168.1.132:9610 40.67.251.132:443 ESTABLISHED
44 TCP 192.168.1.132:9611 40.67.251.132:443 ESTABLISHED
45 TCP 192.168.1.132:10439 213.13.158.214:443 FIN_WAIT_2
46 TCP 192.168.1.132:11421 74.125.133.188:5228 ESTABLISHED
47 TCP 192.168.1.132:11489 216.58.201.165:443 ESTABLISHED
48 TCP 192.168.1.132:11744 162.125.68.7:443 CLOSE_WAIT
49 TCP 192.168.1.132:13371 18.213.183.225:443 CLOSE_WAIT
50 TCP 192.168.1.132:13432 162.125.68.10:443 ESTABLISHED
51 TCP 192.168.1.132:14041 151.101.133.140:443 ESTABLISHED
52 TCP 192.168.1.132:14072 151.101.65.69:443 ESTABLISHED
53 TCP 192.168.1.132:14076 104.16.25.34:443 ESTABLISHED
54 TCP 192.168.1.132:14226 162.125.68.3:443 ESTABLISHED
55 TCP 192.168.1.132:14242 162.125.68.3:443 ESTABLISHED
56 TCP 192.168.1.132:14356 162.125.34.137:443 CLOSE_WAIT
57 TCP 192.168.1.132:14376 13.107.6.254:443 ESTABLISHED
58 TCP 192.168.1.132:14378 13.107.136.254:443 ESTABLISHED
59 TCP 192.168.1.132:14379 51.140.40.24:443 ESTABLISHED
```

```
60  TCP 192.168.1.132:14380 204.79.197.222:443 ESTABLISHED
61  TCP 192.168.1.132:14449 104.90.145.230:443 ESTABLISHED
62  TCP 192.168.1.132:14500 216.58.211.36:80 TIME_WAIT
63  TCP 192.168.1.132:14509 216.58.211.36:80 TIME_WAIT
64  TCP 192.168.1.132:14515 162.125.18.133:443 ESTABLISHED
65  TCP 192.168.1.132:14528 216.58.211.36:80 TIME_WAIT
66  TCP [::]:80 [::]:0 LISTENING
67  TCP [::]:135 [::]:0 LISTENING
68  TCP [::]:445 [::]:0 LISTENING
69  TCP [::]:49664 [::]:0 LISTENING
70  TCP [::]:49665 [::]:0 LISTENING
71  TCP [::]:49666 [::]:0 LISTENING
72  TCP [::]:49667 [::]:0 LISTENING
73  TCP [::]:49668 [::]:0 LISTENING
74  TCP [::]:49669 [::]:0 LISTENING
75  TCP [::1]:80 [::1]:14437 TIME_WAIT
76  TCP [::1]:80 [::1]:14474 TIME_WAIT
77  TCP [::1]:80 [::1]:14523 ESTABLISHED
78  TCP [::1]:80 [::1]:14524 ESTABLISHED
79  TCP [::1]:14493 [::1]:80 TIME_WAIT
80  TCP [::1]:14523 [::1]:80 ESTABLISHED
81  TCP [::1]:14524 [::1]:80 ESTABLISHED
82  TCP [::1]:14532 [::1]:9229 SYN_SENT
83  UDP 0.0.0.0:5353 *:*
84  UDP 0.0.0.0:5353 *:*
85  UDP 0.0.0.0:5353 *:*
86  UDP 0.0.0.0:5353 *:*
87  UDP 0.0.0.0:5353 *:*
88  UDP 0.0.0.0:5353 *:*
89  UDP 0.0.0.0:5355 *:*
90  UDP 0.0.0.0:57179 *:*
91  UDP 0.0.0.0:62997 *:*
92  UDP 0.0.0.0:64972 *:*
93  UDP 127.0.0.1:1900 *:*
```

```
94    UDP 127.0.0.1:54092 *:*
95    UDP 127.0.0.1:59982 *:*
96    UDP 169.254.89.216:137 *:*
97    UDP 169.254.89.216:138 *:*
98    UDP 169.254.89.216:1900 *:*
99    UDP 169.254.89.216:2177 *:*
100    UDP 169.254.89.216:54090 *:*
101    UDP 192.168.1.132:137 *:*
102    UDP 192.168.1.132:138 *:*
103    UDP 192.168.1.132:1900 *:*
104    UDP 192.168.1.132:2177 *:*
105    UDP 192.168.1.132:54091 *:*
106    UDP [::]:5353 *:*
107    UDP [::]:5353 *:*
108    UDP [::]:5353 *:*
109    UDP [::]:5355 *:*
110    UDP [::1]:1900 *:*
111    UDP [::1]:54089 *:*
112    UDP [fe80::644c:d516:4a2a:24bd%20]:1900 *:*
113    UDP [fe80::644c:d516:4a2a:24bd%20]:2177 *:*
114    UDP [fe80::644c:d516:4a2a:24bd%20]:54088 *:*
115    UDP [fe80::f1ac:26c5:3f1c:59d8%2]:1900 *:*
116    UDP [fe80::f1ac:26c5:3f1c:59d8%2]:2177 *:*
117    UDP [fe80::f1ac:26c5:3f1c:59d8%2]:54087 *:*
```

Tool: Netstat

`Command 2/6 > 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     12...62 14 b3 c5 c9 d3 ......Microsoft Wi-Fi Direct Virtual Adapter
```

```
6...60 14 b3 c5 c9 d3 ......Microsoft Wi-Fi Direct Virtual Adapter #2
20...60 14 b3 c5 c9 d3 ......Realtek 8821AE Wireless LAN 802.11ac PCI-E NIC
16...60 14 b3 c5 c9 d4 ......Bluetooth Device (Personal Area Network)
1...........................Software Loopback Interface 1
=====================================================================
======
 IPv4 Route Table
=====================================================================
======
 Active Routes:
 Network Destination Netmask Gateway Interface Metric
  0.0.0.0 0.0.0.0 192.168.1.1 192.168.1.132 55
  127.0.0.0 255.0.0.0 On-link 127.0.0.1 331
  127.0.0.1 255.255.255.255 On-link 127.0.0.1 331
  127.255.255.255 255.255.255.255 On-link 127.0.0.1 331
  169.254.0.0 255.255.0.0 On-link 169.254.89.216 281
  169.254.89.216 255.255.255.255 On-link 169.254.89.216 281
  169.254.255.255 255.255.255.255 On-link 169.254.89.216 281
  192.168.1.0 255.255.255.0 On-link 192.168.1.132 311
  192.168.1.132 255.255.255.255 On-link 192.168.1.132 311
  192.168.1.255 255.255.255.255 On-link 192.168.1.132 311
  224.0.0.0 240.0.0.0 On-link 127.0.0.1 331
  224.0.0.0 240.0.0.0 On-link 192.168.1.132 311
  224.0.0.0 240.0.0.0 On-link 169.254.89.216 281
  255.255.255.255 255.255.255.255 On-link 127.0.0.1 331
  255.255.255.255 255.255.255.255 On-link 192.168.1.132 311
  255.255.255.255 255.255.255.255 On-link 169.254.89.216 281
=====================================================================
======
 Persistent Routes:
  None
 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:
50    None
```

Tool: Netstat

`Command 3/6 > netstat -s`

**Line command output**

```
1   IPv4 Statistics
2    Packets Received = 9886216
3    Received Header Errors = 0
4    Received Address Errors = 2269
5    Datagrams Forwarded = 0
6    Unknown Protocols Received = 77
7    Received Packets Discarded = 73090
8    Received Packets Delivered = 10458982
9    Output Requests = 8426639
10    Routing Discards = 0
11    Discarded Output Packets = 3894
```

```
 Output Packet No Route = 1127
 Reassembly Required = 26
 Reassembly Successful = 10
 Reassembly Failures = 0
 Datagrams Successfully Fragmented = 0
 Datagrams Failing Fragmentation = 0
 Fragments Created = 0
IPv6 Statistics
 Packets Received = 1565
 Received Header Errors = 0
 Received Address Errors = 240
 Datagrams Forwarded = 0
 Unknown Protocols Received = 0
 Received Packets Discarded = 6248
 Received Packets Delivered = 360269
 Output Requests = 373011
 Routing Discards = 0
 Discarded Output Packets = 0
 Output Packet No Route = 1
 Reassembly Required = 0
 Reassembly Successful = 0
 Reassembly Failures = 0
 Datagrams Successfully Fragmented = 0
 Datagrams Failing Fragmentation = 0
 Fragments Created = 0
ICMPv4 Statistics
 Received Sent
 Messages 1775 2436
 Errors 0 0
 Destination Unreachable 1774 2435
 Time Exceeded 0 0
 Parameter Problems 0 0
 Source Quenches 0 0
 Redirects 0 0
```

```
  Echo Replies 1 0
  Echos 0 1
  Timestamps 0 0
  Timestamp Replies 0 0
  Address Masks 0 0
  Address Mask Replies 0 0
  Router Solicitations 0 0
  Router Advertisements 0 0
ICMPv6 Statistics
  Received Sent
  Messages 15 322
  Errors 0 0
  Destination Unreachable 0 0
  Packet Too Big 0 0
  Time Exceeded 0 0
  Parameter Problems 0 0
  Echos 0 0
  Echo Replies 0 0
  MLD Queries 0 0
  MLD Reports 0 0
  MLD Dones 0 0
  Router Solicitations 0 181
  Router Advertisements 0 0
  Neighbor Solicitations 0 72
  Neighbor Advertisements 15 69
  Redirects 0 0
  Router Renumberings 0 0
TCP Statistics for IPv4
  Active Opens = 73994
  Passive Opens = 4207
  Failed Connection Attempts = 52074
  Reset Connections = 3176
  Current Connections = 25
  Segments Received = 4320472
```

80	Segments Sent = 7283023
81	Segments Retransmitted = 233221
82	TCP Statistics for IPv6
83	Active Opens = 52996
84	Passive Opens = 2093
85	Failed Connection Attempts = 50900
86	Reset Connections = 260
87	Current Connections = 4
88	Segments Received = 352682
89	Segments Sent = 249599
90	Segments Retransmitted = 101775
91	UDP Statistics for IPv4
92	Datagrams Received = 6100433
93	No Ports = 69599
94	Receive Errors = 8983
95	Datagrams Sent = 859025
96	UDP Statistics for IPv6
97	Datagrams Received = 13070
98	No Ports = 5759
99	Receive Errors = 489
100	Datagrams Sent = 16030

Tool: Netstat

```
Command 4/6 > netstat -bn
```

#	**Line command output**
1	A operau0087Æo pedida necessita de elevau0087Æo.

Tool: Autorunsc

```
Command 5/6 > tools\autorunsc.exe -nobanner
```

#	**Line command output**
1	HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms
2	rdpclip
3	rdpclip
4	Monitor de Área de Transferência de RDP

```
5    Microsoft Corporation
6    10.0.17763.1
7    c:\windows\system32\rdpclip.exe
8    16/03/1986 14:17
9   HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
10    C:\Windows\system32\userinit.exe
11    C:\Windows\system32\userinit.exe
12    Aplicação de início de sessão Userinit
13    Microsoft Corporation
14    10.0.17763.1
15    c:\windows\system32\userinit.exe
16    31/12/1958 12:49
17   HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\VmApplet
18    SystemPropertiesPerformance.exe
19    SystemPropertiesPerformance.exe
20    Alterar Definições de Desempenho do Computador
21    Microsoft Corporation
22    10.0.17763.1
23    c:\windows\system32\systempropertiesperformance.exe
24    27/12/1907 02:03
25   HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
26    explorer.exe
27    explorer.exe
28    Explorador do Windows
29    Microsoft Corporation
30    10.0.17763.348
31    c:\windows\explorer.exe
32    14/01/1972 16:17
33   HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell
34    cmd.exe
35    cmd.exe
36    Windows Command Processor
37    Microsoft Corporation
38    10.0.17763.1
```

```
 c:\windows\system32\cmd.exe
 20/11/1975 21:18
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 SecurityHealth
 %windir%\system32\SecurityHealthSystray.exe
 Windows Security notification icon
 Microsoft Corporation
 10.0.17763.1
 c:\windows\system32\securityhealthsystray.exe
 02/07/1906 03:12
 RTHDVCPL
 "C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe" -s
 Gestor de audio de alta definicao Realtek
 Realtek Semiconductor
 1.0.0.1105
 c:\program files\realtek\audio\hda\ravcpl64.exe
 26/07/2017 07:19
 RtHDVBg_LENOVO_DOLBYDRAGON
 "C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe" /LENOVO_DOLBYDRAGON
 HD Audio Background Process
 Realtek Semiconductor
 1.0.0.279
 c:\program files\realtek\audio\hda\ravbg64.exe
 07/08/2017 08:11
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
 Dropbox
 "C:\Program Files (x86)\Dropbox\Client\Dropbox.exe" /systemstartup
 Dropbox
 Dropbox, Inc.
 72.3.127.0
 c:\program files (x86)\dropbox\client\dropbox.exe
 30/04/2019 09:39
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components
 Microsoft Windows Media Player
```

```
73   %SystemRoot%\system32\unregmp2.exe /ShowWMP
74   Utilitário de Configuração do Microsoft Windows Media Player
75   Microsoft Corporation
76   12.0.17763.1
77   c:\windows\system32\unregmp2.exe
78   30/09/1990 08:30
79   Themes Setup
80   themeui.dll
81   API de tema do Windows
82   Microsoft Corporation
83   10.0.17763.55
84   c:\windows\system32\themeui.dll
85   25/12/1961 10:09
86   Microsoft Windows Media Player
87   %SystemRoot%\system32\unregmp2.exe /FirstLogon
88   Utilitário de Configuração do Microsoft Windows Media Player
89   Microsoft Corporation
90   12.0.17763.1
91   c:\windows\system32\unregmp2.exe
92   30/09/1990 08:30
93   Windows Desktop Update
94   shell32.dll
95   DLL comum da shell do Windows
96   Microsoft Corporation
97   10.0.17763.348
98   c:\windows\system32\shell32.dll
99   14/05/2026 07:18
100   Web Platform Customizations
101   C:\Windows\System32\ie4uinit.exe -UserConfig
102   Utilitário de Inicialização por utilizador do IE
103   Microsoft Corporation
104   11.0.17763.1
105   c:\windows\system32\ie4uinit.exe
106   23/12/1994 04:34
```

107 n/a

108 C:\Windows\System32\Rundll32.exe C:\Windows\System32\mscories.dll,Install

109 Microsoft .NET IE SECURITY REGISTRATION

110 Microsoft Corporation

111 2.0.50727.9031

112 c:\windows\system32\mscories.dll

113 08/08/2018 04:18

114 Google Chrome

115 "C:\Program Files (x86)\Google\Chrome\Application\74.0.3729.131\Installer\chrmstp.exe" --configure-user-settings --verbose-logging --system-level

116 Google Chrome Installer

117 Google Inc.

118 74.0.3729.131

119 c:\program files (x86)\google\chrome\application\74.0.3729.131\installer\chrmstp.exe

120 29/04/2019 06:00

121 HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components

122 Microsoft Windows Media Player

123 %SystemRoot%\system32\unregmp2.exe /ShowWMP

124 Utilitário de Configuração do Microsoft Windows Media Player

125 Microsoft Corporation

126 12.0.17763.1

127 c:\windows\syswow64\unregmp2.exe

128 03/01/2036 10:22

129 Microsoft Windows Media Player

130 %SystemRoot%\system32\unregmp2.exe /FirstLogon

131 Utilitário de Configuração do Microsoft Windows Media Player

132 Microsoft Corporation

133 12.0.17763.1

134 c:\windows\syswow64\unregmp2.exe

135 03/01/2036 10:22

136 n/a

137 C:\Windows\SysWOW64\Rundll32.exe C:\Windows\SysWOW64\mscories.dll,Install

138 Microsoft .NET IE SECURITY REGISTRATION

```
139  Microsoft Corporation
140  2.0.50727.9031
141  c:\windows\syswow64\mscories.dll
142  08/08/2018 04:28
143 HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\IconServiceLib
144  IconCodecService.dll
145  IconCodecService.dll
146  Converts a PNG part of the icon to a legacy bmp icon
147  Microsoft Corporation
148  10.0.17763.1
149  c:\windows\system32\iconcodecservice.dll
150  09/05/1956 01:37
151 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
152  OneDrive
153  "C:\Users\Lenovo\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
154  Microsoft OneDrive
155  Microsoft Corporation
156  19.43.304.7
157  c:\users\lenovo\appdata\local\microsoft\onedrive\onedrive.exe
158  06/04/2019 00:50
159  pteid
160  C:\Program Files\Portugal Identity Card\pteidguiV2.exe
161  Autenticacao.gov Application
162  Portuguese Government
163  3.0.17.6064
164  c:\program files\portugal identity card\pteidguiv2.exe
165  08/04/2019 15:54
166 C:\Users\Lenovo\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
167  Autenticacao.gov.pt.lnk
168  C:\Users\Lenovo\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Autenticacao.gov.pt.lnk
169  Autenticação.gov.pt
170  Agência para a Modernização Administrativa, IP
171  1.0.0.0
```

172 c:\program files (x86)\plugin autenticacao.gov\autenticacao.gov.pt.exe

173 17/01/2019 10:22

174 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

175 OneDrive

176 "C:\Users\Lenovo\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background

177 Microsoft OneDrive

178 Microsoft Corporation

179 19.43.304.7

180 c:\users\lenovo\appdata\local\microsoft\onedrive\onedrive.exe

181 06/04/2019 00:50

182 pteid

183 C:\Program Files\Portugal Identity Card\pteidguiV2.exe

184 Autenticacao.gov Application

185 Portuguese Government

186 3.0.17.6064

187 c:\program files\portugal identity card\pteidguiv2.exe

188 08/04/2019 15:54

189 C:\Users\Lenovo\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

190 Autenticacao.gov.pt.lnk

191 C:\Users\Lenovo\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Autenticacao.gov.pt.lnk

192 Autenticação.gov.pt

193 Agência para a Modernização Administrativa, IP

194 1.0.0.0

195 c:\program files (x86)\plugin autenticacao.gov\autenticacao.gov.pt.exe

196 17/01/2019 10:22

Tool: Tasklist

```
Command 6/6 > tasklist
```

# Line command output

1 Image Name PID Session Name Session# Mem Usage

2 ========================= ======== ================ =========== ============

3 System Idle Process 0 Services 0 8 K

4 System 4 Services 0 156 K

```
Registry 96 Services 0 53 168 K
smss.exe 324 Services 0 1 008 K
csrss.exe 572 Services 0 5 120 K
wininit.exe 656 Services 0 6 360 K
services.exe 800 Services 0 9 432 K
lsass.exe 816 Services 0 20 116 K
svchost.exe 928 Services 0 3 440 K
svchost.exe 952 Services 0 30 516 K
fontdrvhost.exe 968 Services 0 2 664 K
svchost.exe 8 Services 0 17 560 K
svchost.exe 948 Services 0 7 948 K
svchost.exe 1220 Services 0 9 024 K
svchost.exe 1272 Services 0 8 176 K
svchost.exe 1280 Services 0 6 472 K
svchost.exe 1288 Services 0 7 972 K
svchost.exe 1308 Services 0 13 068 K
svchost.exe 1356 Services 0 5 624 K
svchost.exe 1424 Services 0 9 940 K
svchost.exe 1488 Services 0 6 180 K
svchost.exe 1544 Services 0 5 340 K
svchost.exe 1672 Services 0 17 460 K
svchost.exe 1680 Services 0 8 840 K
svchost.exe 1812 Services 0 5 948 K
svchost.exe 1904 Services 0 5 084 K
svchost.exe 1944 Services 0 6 908 K
svchost.exe 1984 Services 0 9 256 K
svchost.exe 1992 Services 0 8 632 K
svchost.exe 2008 Services 0 5 024 K
svchost.exe 1444 Services 0 15 496 K
svchost.exe 2080 Services 0 7 060 K
Memory Compression 2152 Services 0 43 428 K
svchost.exe 2180 Services 0 7 632 K
svchost.exe 2264 Services 0 8 960 K
igfxCUIService.exe 2272 Services 0 6 392 K
```

```
svchost.exe 2348 Services 0 11 764 K
svchost.exe 2392 Services 0 6 960 K
svchost.exe 2400 Services 0 8 060 K
svchost.exe 2516 Services 0 8 480 K
svchost.exe 2612 Services 0 8 400 K
svchost.exe 2644 Services 0 11 924 K
svchost.exe 2700 Services 0 6 568 K
RtkAudioService64.exe 2840 Services 0 6 108 K
svchost.exe 2988 Services 0 5 756 K
svchost.exe 2996 Services 0 10 844 K
svchost.exe 2464 Services 0 15 716 K
svchost.exe 2924 Services 0 11 244 K
spoolsv.exe 3116 Services 0 11 100 K
svchost.exe 3180 Services 0 17 060 K
svchost.exe 3232 Services 0 6 620 K
svchost.exe 3440 Services 0 7 000 K
svchost.exe 3448 Services 0 12 016 K
svchost.exe 3468 Services 0 26 016 K
svchost.exe 3476 Services 0 32 788 K
ETDService.exe 3496 Services 0 4 556 K
svchost.exe 3536 Services 0 15 504 K
svchost.exe 3600 Services 0 5 424 K
RtkBtManServ.exe 3616 Services 0 6 832 K
svchost.exe 3640 Services 0 7 656 K
svchost.exe 3648 Services 0 7 564 K
svchost.exe 3660 Services 0 5 084 K
svchost.exe 3672 Services 0 18 436 K
svchost.exe 3856 Services 0 10 684 K
svchost.exe 3924 Services 0 6 324 K
svchost.exe 3936 Services 0 4 656 K
svchost.exe 3968 Services 0 10 732 K
PresentationFontCache.exe 5084 Services 0 16 148 K
DropboxUpdate.exe 5112 Services 0 1 120 K
svchost.exe 5128 Services 0 10 268 K
```

```
73  svchost.exe 5160 Services 0 6 688 K
74  svchost.exe 5324 Services 0 17 240 K
75  svchost.exe 5436 Services 0 5 540 K
76  svchost.exe 5744 Services 0 8 260 K
77  svchost.exe 812 Services 0 33 444 K
78  SearchIndexer.exe 6896 Services 0 50 440 K
79  svchost.exe 6612 Services 0 14 476 K
80  svchost.exe 3420 Services 0 20 096 K
81  svchost.exe 7396 Services 0 7 756 K
82  SecurityHealthService.exe 8824 Services 0 13 836 K
83  svchost.exe 10164 Services 0 7 192 K
84  SgrmBroker.exe 3556 Services 0 5 676 K
85  svchost.exe 10060 Services 0 8 440 K
86  MsMpEng.exe 1536 Services 0 304 984 K
87  svchost.exe 1964 Services 0 5 112 K
88  svchost.exe 2932 Services 0 8 240 K
89  OSPPSVC.EXE 2816 Services 0 11 652 K
90  svchost.exe 10040 Services 0 6 736 K
91  svchost.exe 9856 Services 0 8 676 K
92  csrss.exe 7956 Console 2 5 760 K
93  winlogon.exe 2232 Console 2 8 936 K
94  fontdrvhost.exe 200 Console 2 14 236 K
95  dwm.exe 9028 Console 2 80 976 K
96  ETDCtrl.exe 11468 Console 2 20 028 K
97  sihost.exe 6096 Console 2 36 512 K
98  svchost.exe 9596 Console 2 18 988 K
99  svchost.exe 5272 Console 2 33 916 K
100  taskhostw.exe 4956 Console 2 18 320 K
101  igfxEM.exe 7532 Console 2 11 092 K
102  RAVBg64.exe 2148 Console 2 11 676 K
103  explorer.exe 4868 Console 2 185 776 K
104  ETDCtrlHelper.exe 684 Console 2 9 572 K
105  svchost.exe 3768 Console 2 12 660 K
106  ETDIntelligent.exe 3108 Console 2 7 828 K
```

```
107 ctfmon.exe 7644 Console 2 40 516 K
108 ShellExperienceHost.exe 5520 Console 2 104 024 K
109 SearchUI.exe 10980 Console 2 125 644 K
110 RuntimeBroker.exe 9056 Console 2 30 536 K
111 RuntimeBroker.exe 4800 Console 2 27 400 K
112 SkypeApp.exe 3100 Console 2 17 644 K
113 SkypeBackgroundHost.exe 12120 Console 2 3 040 K
114 RuntimeBroker.exe 5832 Console 2 9 268 K
115 ApplicationFrameHost.exe 7148 Console 2 34 532 K
116 smartscreen.exe 6556 Console 2 31 072 K
117 SecurityHealthSystray.exe 5284 Console 2 8 032 K
118 RAVCpl64.exe 2964 Console 2 11 832 K
119 RAVBg64.exe 5984 Console 2 11 600 K
120 OneDrive.exe 9940 Console 2 60 044 K
121 RuntimeBroker.exe 7968 Console 2 20 660 K
122 RuntimeBroker.exe 2596 Console 2 20 472 K
123 WinStore.App.exe 4132 Console 2 996 K
124 svchost.exe 7812 Console 2 10 240 K
125 WindowsInternal.Composabl 296 Console 2 26 128 K
126 RuntimeBroker.exe 11496 Console 2 21 184 K
127 dllhost.exe 8968 Console 2 9 452 K
128 MicrosoftEdge.exe 5620 Console 2 43 728 K
129 browser_broker.exe 9136 Console 2 6 768 K
130 MicrosoftEdgeSH.exe 6012 Console 2 14 372 K
131 MicrosoftEdgeCP.exe 5552 Console 2 79 388 K
132 LockApp.exe 6120 Console 2 36 856 K
133 RuntimeBroker.exe 12240 Console 2 27 288 K
134 svchost.exe 4936 Console 2 6 364 K
135 NisSrv.exe 7872 Services 0 11 092 K
136 Video.UI.exe 10400 Console 2 10 692 K
137 RuntimeBroker.exe 6444 Console 2 8 328 K
138 svchost.exe 10160 Services 0 8 812 K
139 DbxSvc.exe 3876 Services 0 8 592 K
140 Dropbox.exe 4116 Console 2 244 100 K
```

```
Dropbox.exe 12324 Console 2 8 268 K
Dropbox.exe 11824 Console 2 8 032 K
Dropbox.exe 1656 Console 2 10 524 K
QtWebEngineProcess.exe 11556 Console 2 54 364 K
QtWebEngineProcess.exe 6924 Console 2 47 964 K
Calculator.exe 7576 Console 2 360 K
YourPhone.exe 2416 Console 2 5 112 K
RuntimeBroker.exe 8712 Console 2 7 248 K
Microsoft.Photos.exe 12780 Console 2 25 356 K
RuntimeBroker.exe 13308 Console 2 30 348 K
svchost.exe 13284 Services 0 11 532 K
svchost.exe 9824 Services 0 6 704 K
javaw.exe 5736 Console 2 39 972 K
UniController.exe 9184 Console 2 15 956 K
mysqld_z.exe 8072 Console 2 68 708 K
sublime_text.exe 8264 Console 2 79 160 K
plugin_host.exe 11848 Console 2 24 704 K
chrome.exe 7880 Console 2 224 772 K
chrome.exe 3504 Console 2 8 740 K
chrome.exe 12864 Console 2 9 416 K
chrome.exe 720 Console 2 195 096 K
chrome.exe 5180 Console 2 35 648 K
chrome.exe 1744 Console 2 46 320 K
chrome.exe 5468 Console 2 36 320 K
chrome.exe 10544 Console 2 164 464 K
chrome.exe 11828 Console 2 156 680 K
chrome.exe 6164 Console 2 90 636 K
chrome.exe 13168 Console 2 207 600 K
chrome.exe 12992 Console 2 108 244 K
SystemSettings.exe 10560 Console 2 340 K
chrome.exe 11744 Console 2 46 756 K
audiodg.exe 11272 Services 0 20 512 K
chrome.exe 6360 Console 2 342 252 K
cmd.exe 9092 Console 2 3 896 K
```

```
conhost.exe 11516 Console 2 16 264 K
SearchProtocolHost.exe 844 Services 0 13 356 K
Taskmgr.exe 6972 Console 2 51 868 K
httpd_z.exe 5924 Console 2 16 120 K
httpd_z.exe 6364 Console 2 28 756 K
chrome.exe 6512 Console 2 23 292 K
SearchFilterHost.exe 976 Services 0 8 456 K
cmd.exe 8328 Console 2 4 436 K
conhost.exe 2636 Console 2 10 920 K
tasklist.exe 9528 Console 2 7 696 K
WmiPrvSE.exe 12424 Services 0 8 480 K
```

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: Autorunsc

Description: Show what programs are configured to run during system bootup or login

Notes:

Tool #3: Tasklist

Description: List all windows processes

Notes: