Private Portable Pentest
and Network Information Framework

PENTEST REPORT

Name: CP-4
Description: Teste para Ambiente Doméstico - 4

Pentest date: 2019-05-03 23:44:22
Pentest elapsed time: 00:00:02.51
Report date: 2019-05-04 00:02:29

Created by: user

Result of the execution tools

Model: Model CP-4

Description: Modelo para Caso Prático Amb. Doméstico

Notes: Modelo para obter informações de processos em execução.

Tool: Registry

```
Command 1/7 > reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run
```

# Line command output

1 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

2 Dropbox REG_SZ "C:\Program Files (x86)\Dropbox\Client\Dropbox.exe" /systemstartup

Tool: Registry

```
Command 2/7 > reg query
HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
```

No results for this tool.

Tool: Registry

```
Command 3/7 > reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run
```

# Line command output

1 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

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

3 pteid REG_SZ C:\Program Files\Portugal Identity Card\pteidguiV2.exe

Tool: Registry

```
Command 4/7 > reg query
HKCU\Software\Microsoft\Windows\CurrentVersion\Runonce
```

# Line command output

1 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce

2 Delete Cached Update Binary REG_SZ C:\Windows\system32\cmd.exe /q /c del /q "C:\Users\Lenovo\AppData\Local\Microsoft\OneDrive\Update\OneDriveSetup.exe"

3 Delete Cached Standalone Update Binary REG_SZ C:\Windows\system32\cmd.exe /q /c del /q "C:\Users\Lenovo\AppData\Local\Microsoft\OneDrive\StandaloneUpdater\OneDriveSetup.exe"

4 Uninstall 19.043.0304.0007\amd64 REG_SZ C:\Windows\system32\cmd.exe /q /c rmdir /s

	/q "C:\Users\Lenovo\AppData\Local\Microsoft\OneDrive\19.043.0304.0007\amd64"
5	Uninstall 19.043.0304.0007 REG_SZ C:\Windows\system32\cmd.exe /q /c rmdir /s /q "C:\Users\Lenovo\AppData\Local\Microsoft\OneDrive\19.043.0304.0007"

Tool: PsList

```
Command 5/7 > tools\pslist.exe -nobanner
```

#	Line command output
1	Process information for DESKTOP-EAK7JTF:
2	Name Pid Pri Thd Hnd Priv CPU Time Elapsed Time
3	Idle 0 0 4 0 56 159:35:52.656 244:33:11.226
4	System 4 8 147 7121 192 1:43:30.265 244:33:11.226
5	Registry 96 8 4 0 1096 0:00:12.578 244:33:13.692
6	smss 324 11 2 53 508 0:00:00.250 244:33:11.219
7	csrss 572 13 11 734 1884 0:00:05.281 244:33:04.404
8	wininit 656 13 1 172 1492 0:00:00.046 244:33:04.001
9	services 800 9 9 693 5536 0:01:08.000 244:33:03.885
10	lsass 816 9 9 1746 9360 0:01:16.593 244:33:03.843
11	svchost 928 8 2 85 984 0:00:00.031 244:33:03.582
12	svchost 952 8 20 1246 17780 0:02:32.531 244:33:03.564
13	fontdrvhost 968 8 5 48 1796 0:00:00.171 244:33:03.562
14	svchost 8 8 12 1396 10064 0:05:11.859 244:33:02.910
15	svchost 948 8 7 327 3012 0:00:10.062 244:33:02.861
16	svchost 1220 8 5 235 2580 0:00:02.687 244:33:02.595
17	svchost 1272 8 7 250 2568 0:00:00.890 244:33:02.577
18	svchost 1280 8 4 159 1768 0:00:00.156 244:33:02.577
19	svchost 1288 8 2 155 2076 0:00:02.125 244:33:02.577
20	svchost 1308 8 6 392 5964 0:00:14.250 244:33:02.571
21	svchost 1356 8 3 193 1900 0:00:02.781 244:33:02.555
22	svchost 1424 8 3 241 2824 0:00:00.921 244:33:02.538
23	svchost 1488 8 3 233 1972 0:00:00.109 244:33:02.507
24	svchost 1544 8 6 133 1656 0:00:00.156 244:33:02.490
25	svchost 1672 8 7 435 15644 0:00:16.250 244:33:02.426
26	svchost 1680 8 8 1219 3188 0:00:15.218 244:33:02.421
27	svchost 1812 8 3 158 1828 0:00:00.984 244:33:02.367

```
svchost 1904 8 2 124 1364 0:00:00.093 244:33:02.289
svchost 1944 8 5 177 2032 0:00:00.718 244:33:02.270
svchost 1984 8 4 217 2608 0:01:51.156 244:33:02.257
svchost 1992 8 3 153 5304 0:00:25.375 244:33:02.254
svchost 2008 8 3 240 1320 0:00:01.562 244:33:02.249
svchost 1444 8 5 305 7048 0:10:37.562 244:33:02.206
svchost 2080 8 8 235 2600 0:02:07.125 244:33:02.187
Memory Compression 2152 8 86 0 340 0:00:33.203 244:33:02.156
svchost 2180 8 2 223 2304 0:00:01.359 244:33:02.145
svchost 2264 8 3 228 2380 0:00:00.500 244:33:02.111
igfxCUIService 2272 8 2 170 1724 0:00:00.093 244:33:02.110
svchost 2348 8 12 384 5772 0:01:11.750 244:33:02.058
svchost 2392 8 4 189 1896 0:00:00.953 244:33:02.025
svchost 2400 8 6 181 2120 0:00:07.671 244:33:02.023
svchost 2516 8 10 374 3384 0:00:33.718 244:33:01.864
svchost 2612 8 13 247 3756 0:10:45.281 244:33:01.690
svchost 2644 8 9 376 3636 0:00:13.125 244:33:01.615
svchost 2700 8 4 186 2120 0:00:18.531 244:33:01.564
RtkAudioService64 2840 8 2 175 1788 0:00:00.281 244:33:01.471
svchost 2988 8 4 143 1728 0:00:03.015 244:33:00.973
svchost 2996 8 8 454 3520 0:00:08.125 244:33:00.973
svchost 2464 8 9 514 6048 0:00:14.359 244:33:00.854
svchost 2924 8 6 265 3400 0:00:01.328 244:33:00.809
spoolsv 3116 8 8 460 5780 0:00:05.296 244:33:00.741
svchost 3180 8 14 424 10324 0:01:23.343 244:33:00.691
svchost 3232 8 6 191 2104 0:00:03.953 244:33:00.646
svchost 3440 8 5 225 1948 0:00:00.406 244:33:00.386
svchost 3448 8 7 296 4636 0:00:05.671 244:33:00.385
svchost 3468 8 12 561 15988 0:00:17.359 244:33:00.382
svchost 3476 8 17 384 36232 0:03:49.406 244:33:00.381
ETDService 3496 8 2 120 1164 0:00:00.437 244:33:00.366
svchost 3536 8 14 380 7924 0:00:48.000 244:33:00.350
svchost 3600 8 2 134 1644 0:00:00.078 244:33:00.321
RtkBtManServ 3616 8 2 151 2368 0:00:02.968 244:33:00.315
```

```
62 svchost 3640 8 5 188 2172 0:00:05.359 244:33:00.304
63 svchost 3648 8 6 211 2384 0:00:01.953 244:33:00.302
64 svchost 3660 8 3 127 1328 0:00:00.062 244:33:00.300
65 svchost 3672 8 7 403 5276 0:00:07.296 244:33:00.297
66 svchost 3856 8 5 473 3624 0:00:24.250 244:33:00.251
67 svchost 3924 8 10 207 2196 0:00:00.218 244:33:00.209
68 svchost 3936 8 3 108 1320 0:00:00.359 244:33:00.192
69 svchost 3968 8 13 436 3872 0:00:00.515 244:33:00.082
70 PresentationFontCache 5084 8 4 233 25272 0:00:00.218 244:32:58.111
71 DropboxUpdate 5112 8 3 221 2012 0:00:01.015 244:32:58.097
72 svchost 5128 8 9 240 3356 0:00:04.218 244:32:57.859
73 svchost 5160 8 4 176 1824 0:00:00.187 244:32:57.833
74 svchost 5324 8 13 371 5080 0:00:09.718 244:32:57.524
75 svchost 5436 8 2 145 1372 0:00:00.453 244:32:57.333
76 svchost 5744 8 7 224 3992 0:00:12.687 244:32:56.879
77 svchost 812 8 8 1014 20360 0:00:11.812 244:32:55.141
78 SearchIndexer 6896 8 19 892 39108 0:01:40.718 244:32:53.123
79 svchost 6612 8 8 295 4252 0:00:03.890 244:32:52.071
80 svchost 3420 8 15 546 11208 0:00:08.312 244:32:47.491
81 svchost 7396 8 9 273 2784 0:00:09.156 244:32:47.357
82 SecurityHealthService 8824 8 11 476 5228 0:00:03.156 244:32:42.390
83 svchost 10164 8 1 180 2012 0:00:00.671 244:32:29.215
84 SgrmBroker 3556 8 3 85 3720 0:00:06.250 244:30:59.628
85 svchost 10060 8 6 220 2440 0:00:01.000 244:30:59.213
86 MsMpEng 1536 8 38 2472 544848 0:49:37.828 244:28:58.016
87 svchost 1964 8 1 117 1276 0:00:00.109 244:22:19.901
88 svchost 2932 8 4 195 6228 0:00:00.187 244:06:45.285
89 OSPPSVC 2816 8 1 197 2856 0:00:05.625 241:52:44.291
90 svchost 10040 8 5 179 2464 0:00:03.703 194:15:23.571
91 svchost 9856 8 2 168 2252 0:00:04.750 170:24:45.884
92 csrss 7956 13 13 806 2340 0:04:20.250 141:29:34.141
93 winlogon 2232 13 7 280 2784 0:00:01.062 141:29:34.113
94 fontdrvhost 200 8 5 48 9000 0:00:22.921 141:29:34.046
95 dwm 9028 13 13 1054 80924 0:40:50.468 141:29:33.909
```

96 ETDCtrl 11468 10 13 549 11024 0:00:11.328 133:07:20.718

97 sihost 6096 8 11 825 13316 0:00:48.109 133:07:20.611

98 svchost 9596 8 13 329 8344 0:00:38.500 133:07:20.595

99 svchost 5272 8 7 543 8752 0:00:23.578 133:07:20.535

100 taskhostw 4956 8 9 357 8156 0:00:06.703 133:07:20.474

101 igfxEM 7532 8 3 210 3512 0:00:00.828 133:07:19.847

102 RAVBg64 2148 8 4 314 5992 0:00:00.187 133:07:19.795

103 explorer 4868 8 112 3247 124796 0:26:19.078 133:07:19.727

104 ETDCtrlHelper 684 10 1 155 3032 0:00:00.187 133:07:18.824

105 svchost 3768 8 6 256 2984 0:00:05.578 133:07:18.687

106 ETDIntelligent 3108 8 2 166 2332 0:00:01.468 133:07:18.401

107 ctfmon 7644 13 9 480 43364 0:01:14.437 133:07:17.446

108 ShellExperienceHost 5520 8 27 1213 47888 0:00:43.968 133:07:17.331

109 SearchUI 10980 8 34 1267 101900 0:00:39.468 133:07:16.964

110 RuntimeBroker 9056 8 12 672 26384 0:00:14.390 133:07:16.684

111 RuntimeBroker 4800 8 5 473 7292 0:00:12.093 133:07:16.286

112 SkypeApp 3100 8 17 489 14800 0:00:01.031 133:07:14.848

113 SkypeBackgroundHost 12120 8 4 152 1960 0:00:00.109 133:07:14.519

114 RuntimeBroker 5832 8 1 200 2264 0:00:00.109 133:07:11.222

115 ApplicationFrameHost 7148 8 5 559 22600 0:00:07.718 133:07:11.039

116 smartscreen 6556 8 10 482 18064 0:00:06.312 133:07:09.758

117 SecurityHealthSystray 5284 8 1 151 1804 0:00:00.343 133:07:05.120

118 RAVCpl64 2964 8 6 358 4140 0:00:00.859 133:07:04.427

119 RAVBg64 5984 8 4 313 5920 0:00:00.578 133:07:03.363

120 RuntimeBroker 7968 8 10 363 5416 0:00:04.171 133:05:56.142

121 RuntimeBroker 2596 8 3 387 6492 0:00:25.250 133:05:53.426

122 WinStore.App 4132 8 21 927 42840 0:00:02.046 133:05:29.567

123 svchost 7812 8 1 255 2868 0:00:00.171 133:05:20.498

124 WindowsInternal.ComposableShell.Experiences.TextInput.InputApp 296 8 33 829 16164 0:00:00.562 132:57:51.362

125 RuntimeBroker 11496 8 3 448 8628 0:00:01.312 132:53:15.867

126 dllhost 8968 8 5 225 3720 0:00:00.343 132:52:49.196

127 MicrosoftEdge 5620 8 36 1054 24292 0:00:01.218 132:52:14.433

128 browser_broker 9136 8 2 139 1680 0:00:00.062 132:52:14.188

```
129 MicrosoftEdgeSH 6012 8 12 416 5032 0:00:00.421 132:52:13.863
130 MicrosoftEdgeCP 5552 8 31 1007 58124 0:00:02.125 132:52:13.849
131 LockApp 6120 8 12 515 12972 0:00:02.828 132:43:20.928
132 RuntimeBroker 12240 8 6 384 8124 0:00:13.656 132:43:20.535
133 svchost 4936 8 2 139 1644 0:00:00.062 97:37:37.784
134 NisSrv 7872 8 7 206 7788 0:00:08.593 96:59:55.773
135 Video.UI 10400 8 20 709 21048 0:00:01.203 96:57:25.266
136 RuntimeBroker 6444 8 1 170 1936 0:00:00.203 96:57:24.790
137 svchost 10160 8 7 221 2524 0:00:00.250 95:52:52.533
138 Calculator 7576 8 20 511 15036 0:00:00.484 50:24:50.559
139 YourPhone 2416 8 14 647 12756 0:00:01.000 48:59:46.583
140 RuntimeBroker 8712 8 4 368 3848 0:00:00.343 48:59:46.145
141 svchost 13284 8 2 255 2608 0:00:00.750 47:14:06.126
142 mysqld_z 8072 8 26 667 125752 0:00:06.953 26:00:33.981
143 chrome 7880 8 34 2690 289700 0:16:19.218 25:49:18.739
144 chrome 3504 8 6 336 2216 0:00:00.187 25:49:18.665
145 chrome 12864 8 2 150 2076 0:00:00.156 25:49:18.420
146 chrome 720 8 12 681 292952 0:19:25.468 25:49:18.287
147 chrome 5180 8 14 521 24552 0:03:21.500 25:49:18.281
148 chrome 5468 8 11 286 26616 0:00:02.312 25:49:17.949
149 chrome 10544 8 12 300 206624 0:01:25.375 25:49:17.917
150 chrome 13168 4 15 707 256656 0:03:57.921 25:48:48.160
151 chrome 11744 4 11 317 74028 0:00:05.187 25:31:26.365
152 httpd_z 5924 8 1 180 7844 0:00:01.265 25:05:07.414
153 httpd_z 6364 8 154 550 46920 0:05:40.203 25:05:06.073
154 chrome 3356 4 11 297 41028 0:00:01.140 23:37:20.712
155 chrome 764 4 12 373 55228 0:00:03.312 23:36:28.836
156 scheduler 7032 8 5 548 5572 0:00:07.375 5:56:38.703
157 FCDBLog 4084 8 25 677 11748 0:00:11.046 5:56:38.275
158 FortiTray 2256 8 50 906 9568 0:00:05.250 5:56:37.229
159 FortiESNAC 11348 8 10 321 4808 0:00:28.031 5:56:36.831
160 FortiSSLVPNdaemon 1192 10 7 297 14956 0:00:52.109 5:56:36.749
161 FortiSettings 11828 8 2 190 2372 0:00:00.078 5:56:36.647
162 sublime_text 9784 8 11 806 71416 0:00:39.921 5:55:59.608
```

```
plugin_host 10640 8 4 221 17880 0:00:01.203 5:55:58.286
chrome 7908 4 14 380 60016 0:00:02.640 5:55:38.554
WINWORD 12536 8 13 949 134000 0:00:49.546 5:51:36.650
splwow64 12452 8 5 242 4724 0:00:00.750 5:51:26.421
OneDrive 8496 8 16 682 24140 0:00:02.765 2:18:32.284
chrome 9048 8 14 406 81812 0:03:35.703 2:08:27.829
SystemSettings 6296 8 21 763 17520 0:00:00.937 2:07:05.220
chrome 10820 4 14 373 101364 0:00:13.750 2:06:51.696
chrome 5800 4 11 291 28872 0:00:00.421 2:06:45.829
chrome 1028 4 11 291 29416 0:00:00.437 2:06:42.131
chrome 10364 4 11 295 29420 0:00:00.484 2:06:41.267
chrome 6680 4 11 299 29024 0:00:00.593 2:06:40.895
cmd 12844 8 1 75 2576 0:00:00.109 2:04:33.874
conhost 688 8 3 201 3516 0:00:07.296 2:04:33.850
chrome 7728 4 12 331 60528 0:00:03.890 2:01:23.535
chrome 6396 4 12 354 123508 0:01:26.046 2:01:20.701
chrome 4816 4 12 305 20284 0:00:02.375 1:56:07.059
chrome 8084 8 11 341 45168 0:00:20.015 1:28:03.930
chrome 13908 8 6 240 20784 0:00:08.078 1:28:02.987
chrome 8184 4 12 329 51748 0:00:03.281 1:14:05.676
chrome 2592 4 12 359 56164 0:00:04.062 1:03:38.928
chrome 4356 4 12 388 70548 0:00:13.546 1:03:29.034
Microsoft.Photos 12712 8 22 1000 29380 0:00:01.046 1:02:08.168
RuntimeBroker 4208 8 4 293 3644 0:00:00.453 1:02:06.959
javaw 8052 8 17 408 36972 0:00:02.921 1:01:19.384
DbxSvc 15104 8 25 188 3312 0:00:00.171 0:59:52.563
Dropbox 14080 8 119 2654 204308 0:05:23.953 0:59:43.718
Dropbox 10112 8 6 185 2020 0:00:00.078 0:59:43.632
Dropbox 10524 8 5 171 1856 0:00:00.046 0:59:43.596
Dropbox 8328 8 4 302 2408 0:00:00.078 0:59:43.533
QtWebEngineProcess 13404 8 16 336 32120 0:00:04.140 0:59:33.526
QtWebEngineProcess 4984 8 14 289 34732 0:00:01.234 0:59:24.271
svchost 13972 8 3 166 1648 0:00:00.062 0:55:28.788
mspaint 664 8 7 311 47116 0:00:17.281 0:37:05.916
```

197 chrome 752 4 11 277 13936 0:00:00.187 0:14:20.704

198 SearchProtocolHost 13456 4 3 259 1732 0:00:00.093 0:03:32.519

199 SearchProtocolHost 7624 4 6 380 2740 0:00:00.218 0:03:18.748

200 SearchFilterHost 5732 4 3 124 1312 0:00:00.031 0:01:07.619

201 backgroundTaskHost 4344 8 23 734 28632 0:00:01.203 0:00:25.485

202 backgroundTaskHost 464 8 13 325 11580 0:00:00.343 0:00:25.477

203 svchost 5724 8 6 119 2652 0:00:00.109 0:00:25.457

204 RuntimeBroker 6984 8 12 332 6000 0:00:00.421 0:00:25.304

205 svchost 14544 8 15 344 10816 0:00:00.921 0:00:25.239

206 WmiPrvSE 5080 8 11 214 4184 0:00:00.187 0:00:25.076

207 cmd 7432 8 4 100 5772 0:00:00.015 0:00:00.343

208 conhost 12788 8 5 120 6588 0:00:00.031 0:00:00.331

209 pslist 14936 13 4 249 3468 0:00:00.453 0:00:00.282

Tool: Tasklist

```
Command 6/7 > tasklist /svc
```

# Line command output

1 Image Name PID Services

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

3 System Idle Process 0 N/A

4 System 4 N/A

5 Registry 96 N/A

6 smss.exe 324 N/A

7 csrss.exe 572 N/A

8 wininit.exe 656 N/A

9 services.exe 800 N/A

10 lsass.exe 816 EFS, KeyIso, SamSs, VaultSvc

11 svchost.exe 928 PlugPlay

12 svchost.exe 952 BrokerInfrastructure, DcomLaunch, Power,

13 SystemEventsBroker

14 fontdrvhost.exe 968 N/A

15 svchost.exe 8 RpcEptMapper, RpcSs

16 svchost.exe 948 LSM

```
17  svchost.exe 1220 NcbService
18  svchost.exe 1272 bthserv
19  svchost.exe 1280 BthAvctpSvc
20  svchost.exe 1288 TimeBrokerSvc
21  svchost.exe 1308 Schedule
22  svchost.exe 1356 CoreMessagingRegistrar
23  svchost.exe 1424 ProfSvc
24  svchost.exe 1488 DisplayEnhancementService
25  svchost.exe 1544 hidserv
26  svchost.exe 1672 EventLog
27  svchost.exe 1680 UserManager
28  svchost.exe 1812 BTAGService
29  svchost.exe 1904 DeviceAssociationService
30  svchost.exe 1944 EventSystem
31  svchost.exe 1984 SysMain
32  svchost.exe 1992 nsi
33  svchost.exe 2008 Themes
34  svchost.exe 1444 StateRepository
35  svchost.exe 2080 Dhcp
36  Memory Compression 2152 N/A
37  svchost.exe 2180 SENS
38  svchost.exe 2264 SEMgrSvc
39  igfxCUIService.exe 2272 igfxCUIService2.0.0.0
40  svchost.exe 2348 NlaSvc
41  svchost.exe 2392 AudioEndpointBuilder
42  svchost.exe 2400 FontCache
43  svchost.exe 2516 netprofm
44  svchost.exe 2612 Dnscache
45  svchost.exe 2644 Audiosrv
46  svchost.exe 2700 WinHttpAutoProxySvc
47  RtkAudioService64.exe 2840 RtkAudioService
48  svchost.exe 2988 DusmSvc
49  svchost.exe 2996 Wcmsvc
50  svchost.exe 2464 WlanSvc
```

51 svchost.exe 2924 ShellHWDetection

52 spoolsv.exe 3116 Spooler

53 svchost.exe 3180 BFE, mpssvc

54 svchost.exe 3232 LanmanWorkstation

55 svchost.exe 3440 CertPropSvc

56 svchost.exe 3448 CryptSvc

57 svchost.exe 3468 DiagTrack

58 svchost.exe 3476 DPS

59 ETDService.exe 3496 ETDService

60 svchost.exe 3536 Winmgmt

61 svchost.exe 3600 SstpSvc

62 RtkBtManServ.exe 3616 RtkBtManServ

63 svchost.exe 3640 stisvc

64 svchost.exe 3648 LanmanServer

65 svchost.exe 3660 TrkWks

66 svchost.exe 3672 WpnService

67 svchost.exe 3856 iphlpsvc

68 svchost.exe 3924 TapiSrv

69 svchost.exe 3936 WdiServiceHost

70 svchost.exe 3968 RasMan

71 PresentationFontCache.exe 5084 FontCache3.0.0.0

72 DropboxUpdate.exe 5112 N/A

73 svchost.exe 5128 TokenBroker

74 svchost.exe 5160 TabletInputService

75 svchost.exe 5324 CDPSvc

76 svchost.exe 5436 Appinfo

77 svchost.exe 5744 PcaSvc

78 svchost.exe 812 UsoSvc

79 SearchIndexer.exe 6896 WSearch

80 svchost.exe 6612 LicenseManager

81 svchost.exe 3420 BITS

82 svchost.exe 7396 SSDPSRV

83 SecurityHealthService.exe 8824 SecurityHealthService

84 svchost.exe 10164 StorSvc

85 SgrmBroker.exe 3556 SgrmBroker

86 svchost.exe 10060 wscsvc

87 MsMpEng.exe 1536 WinDefend

88 svchost.exe 1964 seclogon

89 svchost.exe 2932 DsSvc

90 OSPPSVC.EXE 2816 osppsvc

91 svchost.exe 10040 QWAVE

92 svchost.exe 9856 camsvc

93 csrss.exe 7956 N/A

94 winlogon.exe 2232 N/A

95 fontdrvhost.exe 200 N/A

96 dwm.exe 9028 N/A

97 ETDCtrl.exe 11468 N/A

98 sihost.exe 6096 N/A

99 svchost.exe 9596 CDPUserSvc_5e63c75

100 svchost.exe 5272 WpnUserService_5e63c75

101 taskhostw.exe 4956 N/A

102 igfxEM.exe 7532 N/A

103 RAVBg64.exe 2148 N/A

104 explorer.exe 4868 N/A

105 ETDCtrlHelper.exe 684 N/A

106 svchost.exe 3768 cbdhsvc_5e63c75

107 ETDIntelligent.exe 3108 N/A

108 ctfmon.exe 7644 N/A

109 ShellExperienceHost.exe 5520 N/A

110 SearchUI.exe 10980 N/A

111 RuntimeBroker.exe 9056 N/A

112 RuntimeBroker.exe 4800 N/A

113 SkypeApp.exe 3100 N/A

114 SkypeBackgroundHost.exe 12120 N/A

115 RuntimeBroker.exe 5832 N/A

116 ApplicationFrameHost.exe 7148 N/A

117 smartscreen.exe 6556 N/A

118 SecurityHealthSystray.exe 5284 N/A

```
119 RAVCpl64.exe 2964 N/A
120 RAVBg64.exe 5984 N/A
121 RuntimeBroker.exe 7968 N/A
122 RuntimeBroker.exe 2596 N/A
123 WinStore.App.exe 4132 N/A
124 svchost.exe 7812 OneSyncSvc_5e63c75
125 WindowsInternal.Composabl 296 N/A
126 RuntimeBroker.exe 11496 N/A
127 dllhost.exe 8968 N/A
128 MicrosoftEdge.exe 5620 N/A
129 browser_broker.exe 9136 N/A
130 MicrosoftEdgeSH.exe 6012 N/A
131 MicrosoftEdgeCP.exe 5552 N/A
132 LockApp.exe 6120 N/A
133 RuntimeBroker.exe 12240 N/A
134 svchost.exe 4936 PrintWorkflowUserSvc_5e63c75
135 NisSrv.exe 7872 WdNisSvc
136 Video.UI.exe 10400 N/A
137 RuntimeBroker.exe 6444 N/A
138 svchost.exe 10160 RmSvc
139 Calculator.exe 7576 N/A
140 YourPhone.exe 2416 N/A
141 RuntimeBroker.exe 8712 N/A
142 svchost.exe 13284 Netman
143 mysqld_z.exe 8072 N/A
144 chrome.exe 7880 N/A
145 chrome.exe 3504 N/A
146 chrome.exe 12864 N/A
147 chrome.exe 720 N/A
148 chrome.exe 5180 N/A
149 chrome.exe 5468 N/A
150 chrome.exe 10544 N/A
151 chrome.exe 13168 N/A
152 chrome.exe 11744 N/A
```

```
153 httpd_z.exe 5924 N/A
154 httpd_z.exe 6364 N/A
155 chrome.exe 3356 N/A
156 chrome.exe 764 N/A
157 scheduler.exe 7032 FA_Scheduler
158 FCDBLog.exe 4084 N/A
159 FortiTray.exe 2256 N/A
160 FortiESNAC.exe 11348 N/A
161 FortiSSLVPNdaemon.exe 1192 N/A
162 FortiSettings.exe 11828 N/A
163 sublime_text.exe 9784 N/A
164 plugin_host.exe 10640 N/A
165 chrome.exe 7908 N/A
166 WINWORD.EXE 12536 N/A
167 splwow64.exe 12452 N/A
168 OneDrive.exe 8496 N/A
169 chrome.exe 9048 N/A
170 SystemSettings.exe 6296 N/A
171 chrome.exe 10820 N/A
172 chrome.exe 5800 N/A
173 chrome.exe 1028 N/A
174 chrome.exe 10364 N/A
175 chrome.exe 6680 N/A
176 cmd.exe 12844 N/A
177 conhost.exe 688 N/A
178 chrome.exe 7728 N/A
179 chrome.exe 6396 N/A
180 chrome.exe 4816 N/A
181 chrome.exe 8084 N/A
182 chrome.exe 13908 N/A
183 chrome.exe 8184 N/A
184 chrome.exe 2592 N/A
185 chrome.exe 4356 N/A
186 Microsoft.Photos.exe 12712 N/A
```

```
187   RuntimeBroker.exe 4208 N/A
188   javaw.exe 8052 N/A
189   DbxSvc.exe 15104 DbxSvc
190   Dropbox.exe 14080 N/A
191   Dropbox.exe 10112 N/A
192   Dropbox.exe 10524 N/A
193   Dropbox.exe 8328 N/A
194   QtWebEngineProcess.exe 13404 N/A
195   QtWebEngineProcess.exe 4984 N/A
196   svchost.exe 13972 lmhosts
197   mspaint.exe 664 N/A
198   chrome.exe 752 N/A
199   SearchProtocolHost.exe 13456 N/A
200   SearchProtocolHost.exe 7624 N/A
201   SearchFilterHost.exe 5732 N/A
202   backgroundTaskHost.exe 4344 N/A
203   backgroundTaskHost.exe 464 N/A
204   svchost.exe 5724 ClipSVC
205   RuntimeBroker.exe 6984 N/A
206   svchost.exe 14544 wuauserv
207   WmiPrvSE.exe 5080 N/A
208   cmd.exe 12076 N/A
209   conhost.exe 7408 N/A
210   tasklist.exe 10796 N/A
```

Tool: Netstat

`Command 7/7 > netstat -ano`

# Line command output

```
1  Active Connections
2   Proto Local Address Foreign Address State PID
3   TCP 0.0.0.0:80 0.0.0.0:0 LISTENING 5924
4   TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 8
5   TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
6   TCP 0.0.0.0:5040 0.0.0.0:0 LISTENING 5324
```

```
7    TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING 656
8    TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING 1308
9    TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING 1672
10    TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING 3116
11    TCP 0.0.0.0:49668 0.0.0.0:0 LISTENING 800
12    TCP 0.0.0.0:49669 0.0.0.0:0 LISTENING 816
13    TCP 127.0.0.1:843 0.0.0.0:0 LISTENING 14080
14    TCP 127.0.0.1:1840 127.0.0.1:3306 TIME_WAIT 0
15    TCP 127.0.0.1:1846 127.0.0.1:3306 TIME_WAIT 0
16    TCP 127.0.0.1:1863 127.0.0.1:3306 TIME_WAIT 0
17    TCP 127.0.0.1:1867 127.0.0.1:3306 TIME_WAIT 0
18    TCP 127.0.0.1:1871 127.0.0.1:3306 TIME_WAIT 0
19    TCP 127.0.0.1:1892 127.0.0.1:3306 TIME_WAIT 0
20    TCP 127.0.0.1:1896 127.0.0.1:3306 ESTABLISHED 6364
21    TCP 127.0.0.1:1899 127.0.0.1:3306 ESTABLISHED 6364
22    TCP 127.0.0.1:3306 0.0.0.0:0 LISTENING 8072
23    TCP 127.0.0.1:3306 127.0.0.1:1840 TIME_WAIT 0
24    TCP 127.0.0.1:3306 127.0.0.1:1846 TIME_WAIT 0
25    TCP 127.0.0.1:3306 127.0.0.1:1859 TIME_WAIT 0
26    TCP 127.0.0.1:3306 127.0.0.1:1863 TIME_WAIT 0
27    TCP 127.0.0.1:3306 127.0.0.1:1867 TIME_WAIT 0
28    TCP 127.0.0.1:3306 127.0.0.1:1871 TIME_WAIT 0
29    TCP 127.0.0.1:3306 127.0.0.1:1896 ESTABLISHED 8072
30    TCP 127.0.0.1:3306 127.0.0.1:1899 ESTABLISHED 8072
31    TCP 127.0.0.1:16572 127.0.0.1:16573 ESTABLISHED 14080
32    TCP 127.0.0.1:16573 127.0.0.1:16572 ESTABLISHED 14080
33    TCP 127.0.0.1:17600 0.0.0.0:0 LISTENING 14080
34    TCP 127.0.0.1:35153 0.0.0.0:0 LISTENING 8052
35    TCP 169.254.89.216:139 0.0.0.0:0 LISTENING 4
36    TCP 192.168.1.132:139 0.0.0.0:0 LISTENING 4
37    TCP 192.168.1.132:1078 162.125.34.6:443 CLOSE_WAIT 14080
38    TCP 192.168.1.132:1155 74.125.133.188:5228 ESTABLISHED 5180
39    TCP 192.168.1.132:1158 62.28.158.210:4443 CLOSE_WAIT 2256
40    TCP 192.168.1.132:1240 172.217.168.165:443 ESTABLISHED 5180
```

```
41 TCP 192.168.1.132:1630 162.125.68.3:443 ESTABLISHED 14080
42 TCP 192.168.1.132:1633 162.125.68.10:443 ESTABLISHED 14080
43 TCP 192.168.1.132:1760 162.125.68.3:443 ESTABLISHED 14080
44 TCP 192.168.1.132:1767 162.125.68.3:443 ESTABLISHED 14080
45 TCP 192.168.1.132:1826 172.217.17.7:443 ESTABLISHED 5180
46 TCP 192.168.1.132:1841 172.217.168.164:80 TIME_WAIT 0
47 TCP 192.168.1.132:1849 95.101.25.129:443 ESTABLISHED 4344
48 TCP 192.168.1.132:1850 95.101.25.129:443 ESTABLISHED 4344
49 TCP 192.168.1.132:1860 172.217.168.164:80 TIME_WAIT 0
50 TCP 192.168.1.132:1868 172.217.168.164:80 TIME_WAIT 0
51 TCP 192.168.1.132:1886 162.125.18.133:443 ESTABLISHED 14080
52 TCP 192.168.1.132:1893 172.217.168.164:80 TIME_WAIT 0
53 TCP 192.168.1.132:16431 40.67.251.132:443 ESTABLISHED 3672
54 TCP 192.168.1.132:16445 93.184.220.29:80 CLOSE_WAIT 2416
55 TCP 192.168.1.132:16576 162.125.68.3:443 CLOSE_WAIT 14080
56 TCP 192.168.1.132:16634 34.202.246.86:443 CLOSE_WAIT 14080
57 TCP 192.168.1.132:18205 162.125.68.7:443 CLOSE_WAIT 14080
58 TCP 192.168.1.132:18206 162.125.34.129:443 ESTABLISHED 14080
59 TCP 192.168.1.132:18207 162.125.34.129:443 ESTABLISHED 14080
60 TCP [::]:80 [::]:0 LISTENING 5924
61 TCP [::]:135 [::]:0 LISTENING 8
62 TCP [::]:445 [::]:0 LISTENING 4
63 TCP [::]:49664 [::]:0 LISTENING 656
64 TCP [::]:49665 [::]:0 LISTENING 1308
65 TCP [::]:49666 [::]:0 LISTENING 1672
66 TCP [::]:49667 [::]:0 LISTENING 3116
67 TCP [::]:49668 [::]:0 LISTENING 800
68 TCP [::]:49669 [::]:0 LISTENING 816
69 TCP [::1]:80 [::1]:1833 TIME_WAIT 0
70 TCP [::1]:80 [::1]:1855 TIME_WAIT 0
71 TCP [::1]:80 [::1]:1888 ESTABLISHED 5924
72 TCP [::1]:80 [::1]:1889 ESTABLISHED 5924
73 TCP [::1]:1834 [::1]:80 TIME_WAIT 0
74 TCP [::1]:1856 [::1]:80 TIME_WAIT 0
```

```
75   TCP [::1]:1888 [::1]:80 ESTABLISHED 5180
76   TCP [::1]:1889 [::1]:80 ESTABLISHED 5180
77   UDP 0.0.0.0:5353 *:* 7880
78   UDP 0.0.0.0:5353 *:* 7880
79   UDP 0.0.0.0:5353 *:* 7880
80   UDP 0.0.0.0:5353 *:* 7880
81   UDP 0.0.0.0:5353 *:* 5180
82   UDP 0.0.0.0:5353 *:* 2612
83   UDP 0.0.0.0:5355 *:* 2612
84   UDP 0.0.0.0:63047 *:* 5180
85   UDP 127.0.0.1:1900 *:* 7396
86   UDP 127.0.0.1:59982 *:* 3856
87   UDP 127.0.0.1:63089 *:* 7396
88   UDP 169.254.89.216:137 *:* 4
89   UDP 169.254.89.216:138 *:* 4
90   UDP 169.254.89.216:1900 *:* 7396
91   UDP 169.254.89.216:2177 *:* 10040
92   UDP 169.254.89.216:63087 *:* 7396
93   UDP 169.254.89.216:64245 *:* 7880
94   UDP 192.168.1.132:137 *:* 4
95   UDP 192.168.1.132:138 *:* 4
96   UDP 192.168.1.132:1900 *:* 7396
97   UDP 192.168.1.132:2177 *:* 10040
98   UDP 192.168.1.132:63088 *:* 7396
99   UDP 192.168.1.132:64246 *:* 7880
100   UDP [::]:5353 *:* 2612
101   UDP [::]:5353 *:* 7880
102   UDP [::]:5353 *:* 7880
103   UDP [::]:5355 *:* 2612
104   UDP [::1]:1900 *:* 7396
105   UDP [::1]:63086 *:* 7396
106   UDP [fe80::644c:d516:4a2a:24bd%20]:1900 *:* 7396
107   UDP [fe80::644c:d516:4a2a:24bd%20]:2177 *:* 10040
108   UDP [fe80::644c:d516:4a2a:24bd%20]:63085 *:* 7396
```

```
109   UDP [fe80::f1ac:26c5:3f1c:59d8%2]:1900 *:* 7396
110   UDP [fe80::f1ac:26c5:3f1c:59d8%2]:2177 *:* 10040
111   UDP [fe80::f1ac:26c5:3f1c:59d8%2]:63084 *:* 7396
```

Tools used in pentest

Tool #1: Registry

Description: Tool that allows access to the registry using command prompt

Notes:

Tool #2: PsList

Description: Show statistics for active processes

Notes:

Tool #3: Tasklist

Description: Displays a list of currently running processes

Notes:

Tool #4: 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: