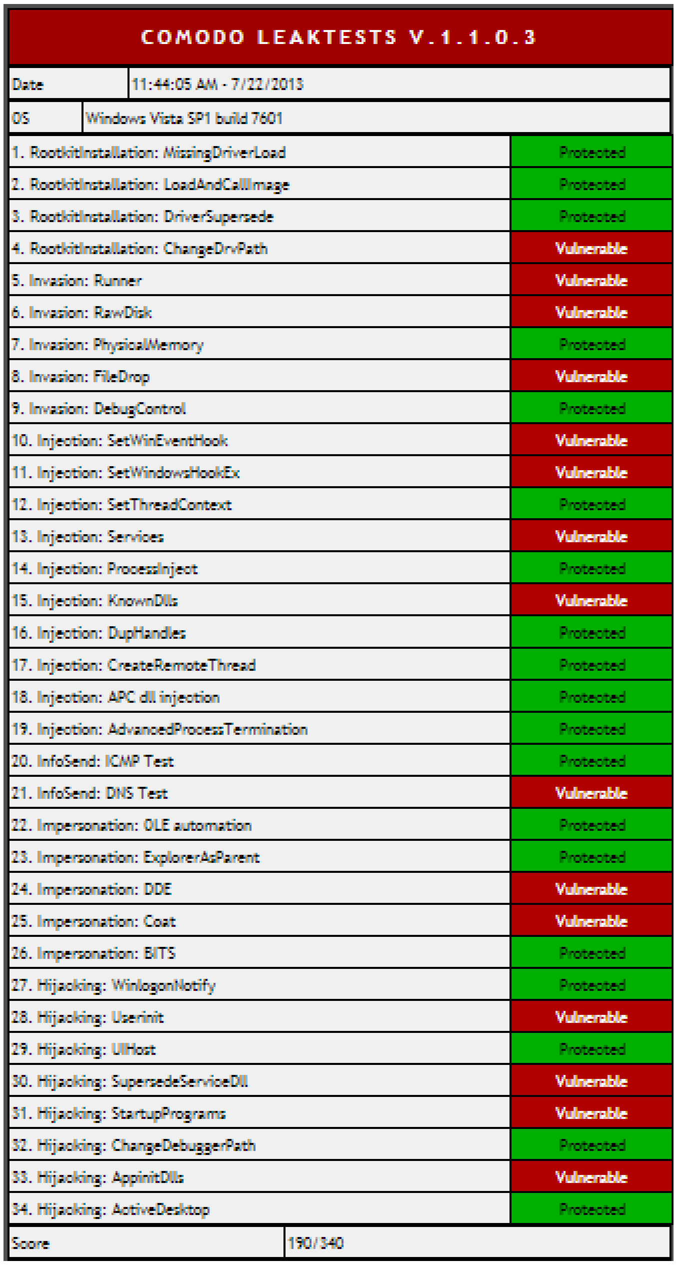
6 Firewallls Tested by Comodo LeakTests (Updated and Default Settings)

Malware Security

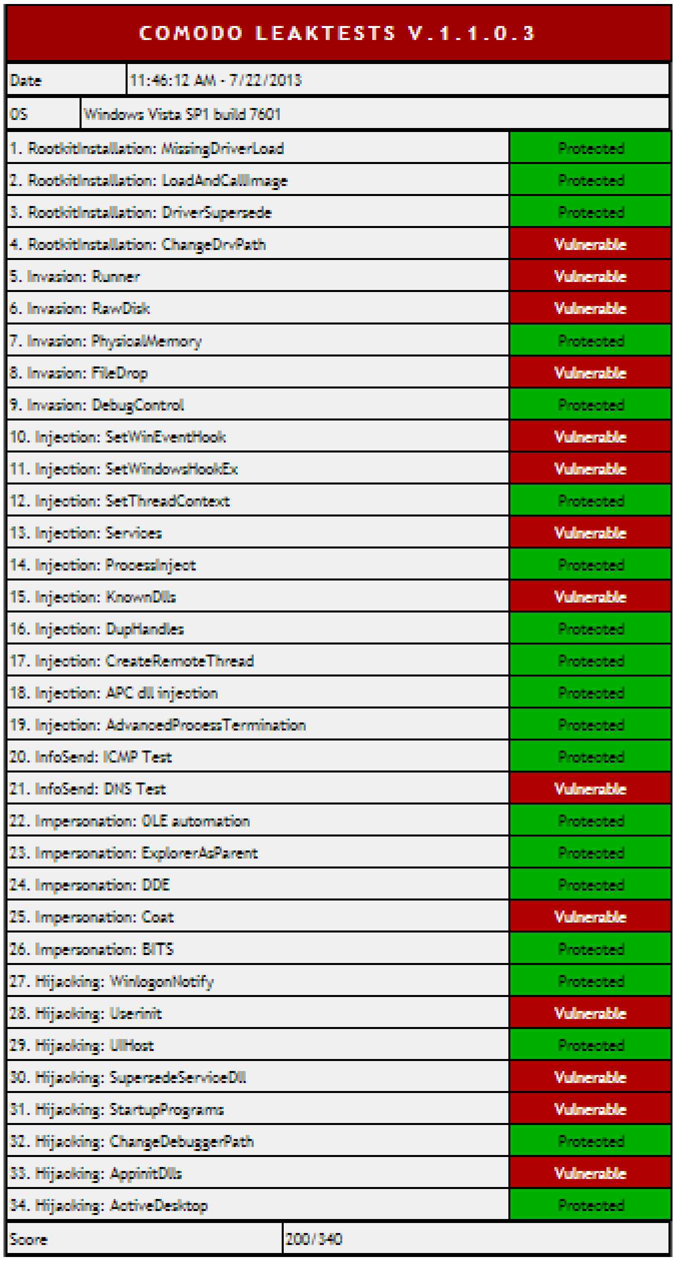
1. **Comodo Free Firewall:**
   - **190/340**



COMODO LEAKTESTS V.1.1.0.3

Date	11:44:05 AM - 7/22/2013
OS	Windows Vista SP1 build 7601
1. RootkitInstallation: MissingDriverLoad	Protected
2. RootkitInstallation: LoadAndCallImage	Protected
3. RootkitInstallation: DriverSupersede	Protected
4. RootkitInstallation: ChangeDrvPath	Vulnerable
5. Invasion: Runner	Vulnerable
6. Invasion: RawDisk	Vulnerable
7. Invasion: PhysicalMemory	Protected
8. Invasion: FileDrop	Vulnerable
9. Invasion: DebugControl	Protected
10. Injection: SetWinEventHook	Vulnerable
11. Injection: SetWindowsHookEx	Vulnerable
12. Injection: SetThreadContext	Protected
13. Injection: Services	Vulnerable
14. Injection: ProcessInject	Protected
15. Injection: KnownDlls	Vulnerable
16. Injection: DupHandles	Protected
17. Injection: CreateRemoteThread	Protected
18. Injection: APC dll injection	Protected
19. Injection: AdvancedProcessTermination	Protected
20. InfoSend: ICMP Test	Protected
21. InfoSend: DNS Test	Vulnerable
22. Impersonation: OLE automation	Protected
23. Impersonation: ExplorerAsParent	Protected
24. Impersonation: DDE	Vulnerable
25. Impersonation: Coat	Vulnerable
26. Impersonation: BITS	Protected
27. Hijacking: WinlogonNotify	Protected
28. Hijacking: Userinit	Vulnerable
29. Hijacking: UIHost	Protected
30. Hijacking: SupersedeServiceDll	Vulnerable
31. Hijacking: StartupPrograms	Vulnerable
32. Hijacking: ChangeDebuggerPath	Protected
33. Hijacking: AppinitDlls	Vulnerable
34. Hijacking: ActiveDesktop	Protected
Score	190/340

2. **Eset Firewall (From Smart Security 6)**
   - **200/340**

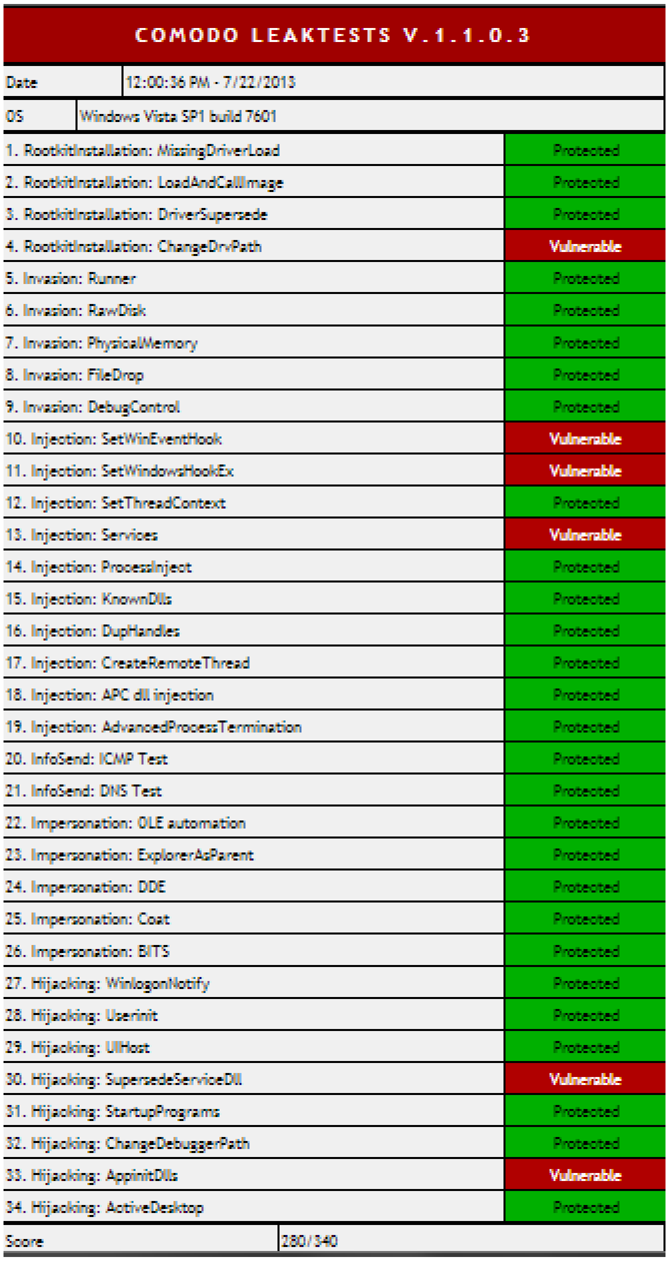


COMODO LEAKTESTS V.1.1.0.3

Date	11:46:12 AM - 7/22/2013
OS	Windows Vista SP1 build 7601
1. RootkitInstallation: MissingDriverLoad	Protected
2. RootkitInstallation: LoadAndCallImage	Protected
3. RootkitInstallation: DriverSupersede	Protected
4. RootkitInstallation: ChangeDrvPath	Vulnerable
5. Invasion: Runner	Vulnerable
6. Invasion: RawDisk	Vulnerable
7. Invasion: PhysicalMemory	Protected
8. Invasion: FileDrop	Vulnerable
9. Invasion: DebugControl	Protected
10. Injection: SetWinEventHook	Vulnerable
11. Injection: SetWindowsHookEx	Vulnerable
12. Injection: SetThreadContext	Protected
13. Injection: Services	Vulnerable
14. Injection: ProcessInject	Protected
15. Injection: KnownDlls	Vulnerable
16. Injection: DupHandles	Protected
17. Injection: CreateRemoteThread	Protected
18. Injection: APC dll injection	Protected
19. Injection: AdvancedProcessTermination	Protected
20. InfoSend: ICMP Test	Protected
21. InfoSend: DNS Test	Vulnerable
22. Impersonation: OLE automation	Protected
23. Impersonation: ExplorerAsParent	Protected
24. Impersonation: DDE	Protected
25. Impersonation: Coat	Vulnerable
26. Impersonation: BITS	Protected
27. Hijacking: WinlogonNotify	Protected
28. Hijacking: Userinit	Vulnerable
29. Hijacking: UIHost	Protected
30. Hijacking: SupersedeServiceDll	Vulnerable
31. Hijacking: StartupPrograms	Vulnerable
32. Hijacking: ChangeDebuggerPath	Protected
33. Hijacking: AppinitDlls	Vulnerable
34. Hijacking: ActiveDesktop	Protected
Score	200/340

3. Online Armor Free Firewall (When clicking “allow” on few pop ups)

- 280/340

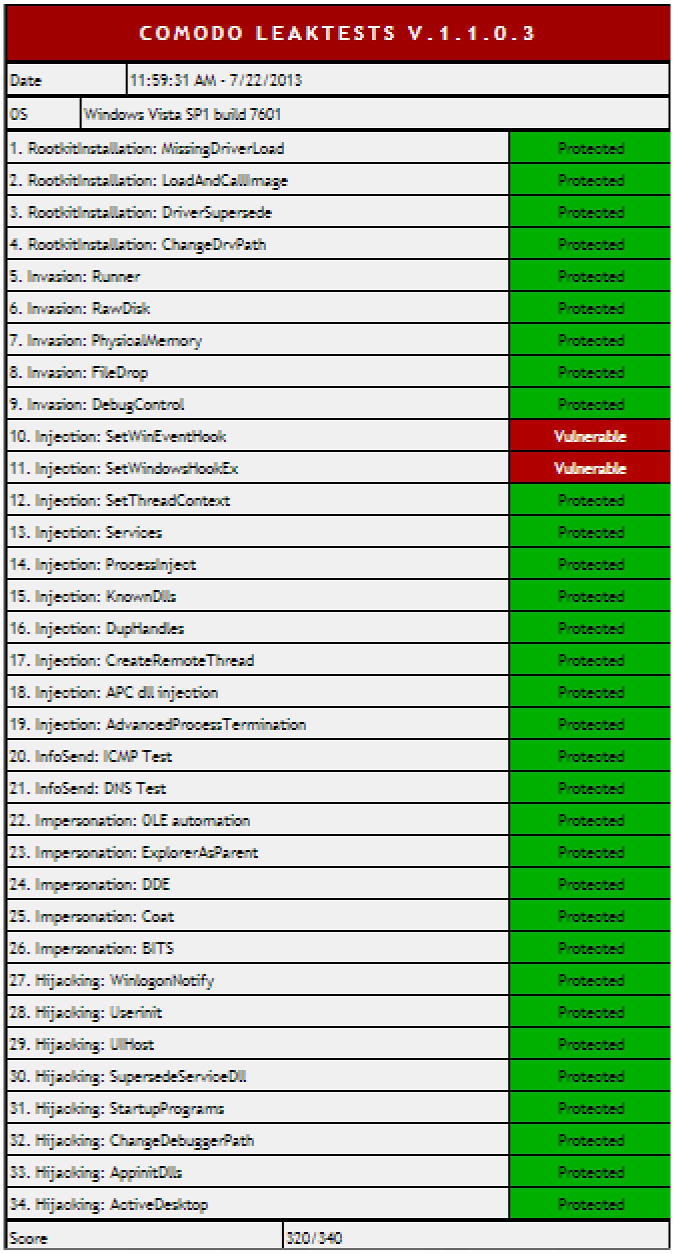


COMODO LEAKTESTS V.1.1.0.3

Date	12:00:36 PM - 7/22/2013
OS	Windows Vista SP1 build 7601
1. RootkitInstallation: MissingDriverLoad	Protected
2. RootkitInstallation: LoadAndCallImage	Protected
3. RootkitInstallation: DriverSupersede	Protected
4. RootkitInstallation: ChangeDrvPath	Vulnerable
5. Invasion: Runner	Protected
6. Invasion: RawDisk	Protected
7. Invasion: PhysicalMemory	Protected
8. Invasion: FileDrop	Protected
9. Invasion: DebugControl	Protected
10. Injection: SetWinEventHook	Vulnerable
11. Injection: SetWindowsHookEx	Vulnerable
12. Injection: SetThreadContext	Protected
13. Injection: Services	Vulnerable
14. Injection: ProcessInject	Protected
15. Injection: KnownDlls	Protected
16. Injection: DupHandles	Protected
17. Injection: CreateRemoteThread	Protected
18. Injection: APC dll injection	Protected
19. Injection: AdvancedProcessTermination	Protected
20. InfoSend: ICMP Test	Protected
21. InfoSend: DNS Test	Protected
22. Impersonation: OLE automation	Protected
23. Impersonation: ExplorerAsParent	Protected
24. Impersonation: DDE	Protected
25. Impersonation: Coat	Protected
26. Impersonation: BITS	Protected
27. Hijacking: WinlogonNotify	Protected
28. Hijacking: Userinit	Protected
29. Hijacking: UIHost	Protected
30. Hijacking: SupersedeServiceDll	Vulnerable
31. Hijacking: StartupPrograms	Protected
32. Hijacking: ChangeDebuggerPath	Protected
33. Hijacking: AppinitDlls	Vulnerable
34. Hijacking: ActiveDesktop	Protected
Score	280/340

Online Armor Free Firewall (When clicking "Block" on few pop ups)

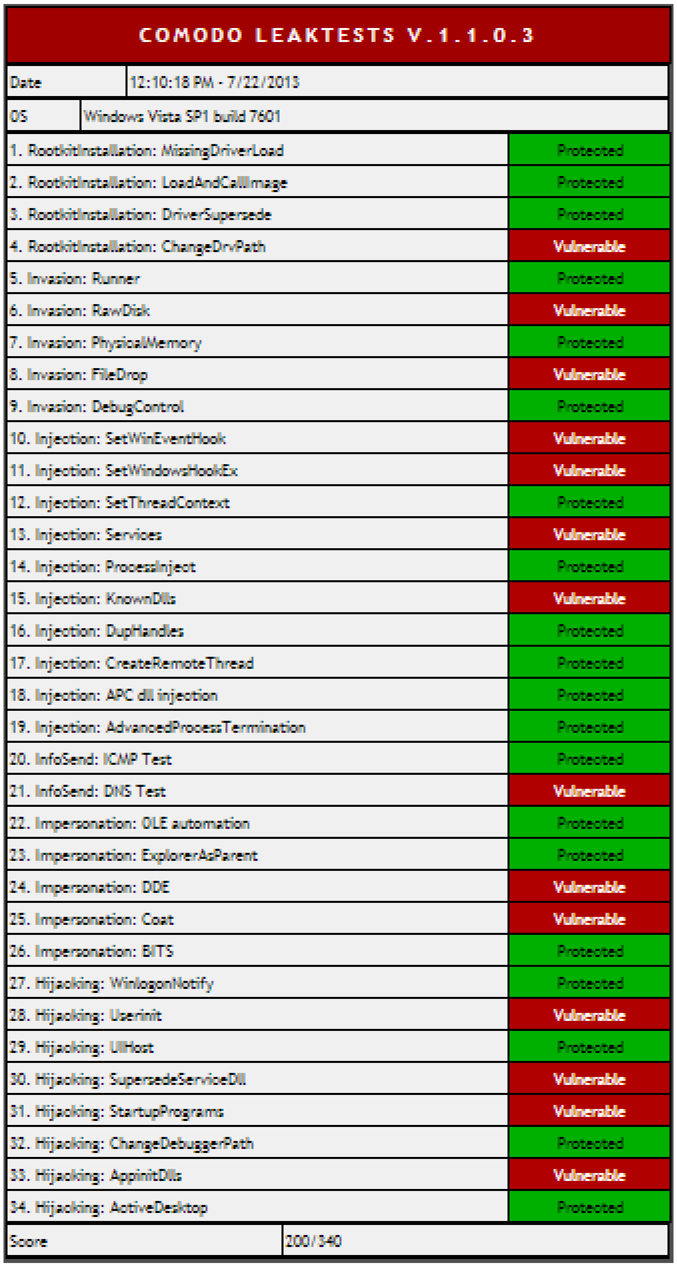
- **320/340**



COMODO LEAKTESTS V.1.1.0.3

Date	11:59:31 AM - 7/22/2013
OS	Windows Vista SP1 build 7601
1. RootkitInstallation: MissingDriverLoad	Protected
2. RootkitInstallation: LoadAndCallImage	Protected
3. RootkitInstallation: DriverSupersede	Protected
4. RootkitInstallation: ChangeDrvPath	Protected
5. Invasion: Runner	Protected
6. Invasion: RawDisk	Protected
7. Invasion: PhysicalMemory	Protected
8. Invasion: FileDrop	Protected
9. Invasion: DebugControl	Protected
10. Injection: SetWinEventHook	Vulnerable
11. Injection: SetWindowsHookEx	Vulnerable
12. Injection: SetThreadContext	Protected
13. Injection: Services	Protected
14. Injection: ProcessInject	Protected
15. Injection: KnownDlls	Protected
16. Injection: DupHandles	Protected
17. Injection: CreateRemoteThread	Protected
18. Injection: APC dll injection	Protected
19. Injection: AdvancedProcessTermination	Protected
20. InfoSend: ICMP Test	Protected
21. InfoSend: DNS Test	Protected
22. Impersonation: OLE automation	Protected
23. Impersonation: ExplorerAsParent	Protected
24. Impersonation: DDE	Protected
25. Impersonation: Coat	Protected
26. Impersonation: BITS	Protected
27. Hijacking: WinlogonNotify	Protected
28. Hijacking: Userinit	Protected
29. Hijacking: UIHost	Protected
30. Hijacking: SupersedeServiceDll	Protected
31. Hijacking: StartupPrograms	Protected
32. Hijacking: ChangeDebuggerPath	Protected
33. Hijacking: AppinitDlls	Protected
34. Hijacking: ActiveDesktop	Protected
Score	320/340

4. **Zone Alarm Free Firewall (<u>When clicking “allow” on few pop ups)</u>**
   - ○ **200/340**

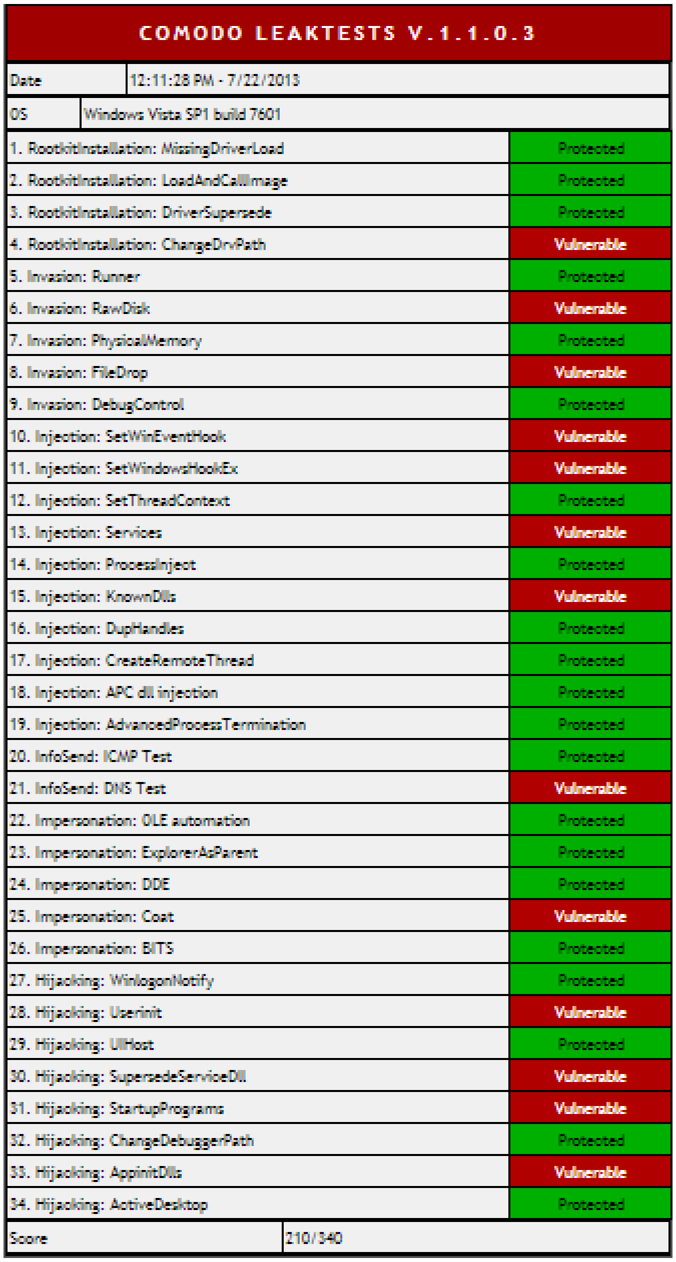


COMODO LEAKTESTS V.1.1.0.3

Date	12:10:18 PM - 7/22/2013
OS	Windows Vista SP1 build 7601
1. RootkitInstallation: MissingDriverLoad	Protected
2. RootkitInstallation: LoadAndCallImage	Protected
3. RootkitInstallation: DriverSupersede	Protected
4. RootkitInstallation: ChangeDrvPath	Vulnerable
5. Invasion: Runner	Protected
6. Invasion: RawDisk	Vulnerable
7. Invasion: PhysicalMemory	Protected
8. Invasion: FileDrop	Vulnerable
9. Invasion: DebugControl	Protected
10. Injection: SetWinEventHook	Vulnerable
11. Injection: SetWindowsHookEx	Vulnerable
12. Injection: SetThreadContext	Protected
13. Injection: Services	Vulnerable
14. Injection: ProcessInject	Protected
15. Injection: KnownDlls	Vulnerable
16. Injection: DupHandles	Protected
17. Injection: CreateRemoteThread	Protected
18. Injection: APC dll injection	Protected
19. Injection: AdvancedProcessTermination	Protected
20. InfoSend: ICMP Test	Protected
21. InfoSend: DNS Test	Vulnerable
22. Impersonation: OLE automation	Protected
23. Impersonation: ExplorerAsParent	Protected
24. Impersonation: DDE	Vulnerable
25. Impersonation: Coat	Vulnerable
26. Impersonation: BITS	Protected
27. Hijacking: WinlogonNotify	Protected
28. Hijacking: Userinit	Vulnerable
29. Hijacking: UIHost	Protected
30. Hijacking: SupersedeServiceDll	Vulnerable
31. Hijacking: StartupPrograms	Vulnerable
32. Hijacking: ChangeDebuggerPath	Protected
33. Hijacking: AppinitDlls	Vulnerable
34. Hijacking: ActiveDesktop	Protected
Score	200/340

Zone Alarm Free Firewall (<u>When clicking "Deny" on few pop ups)</u>

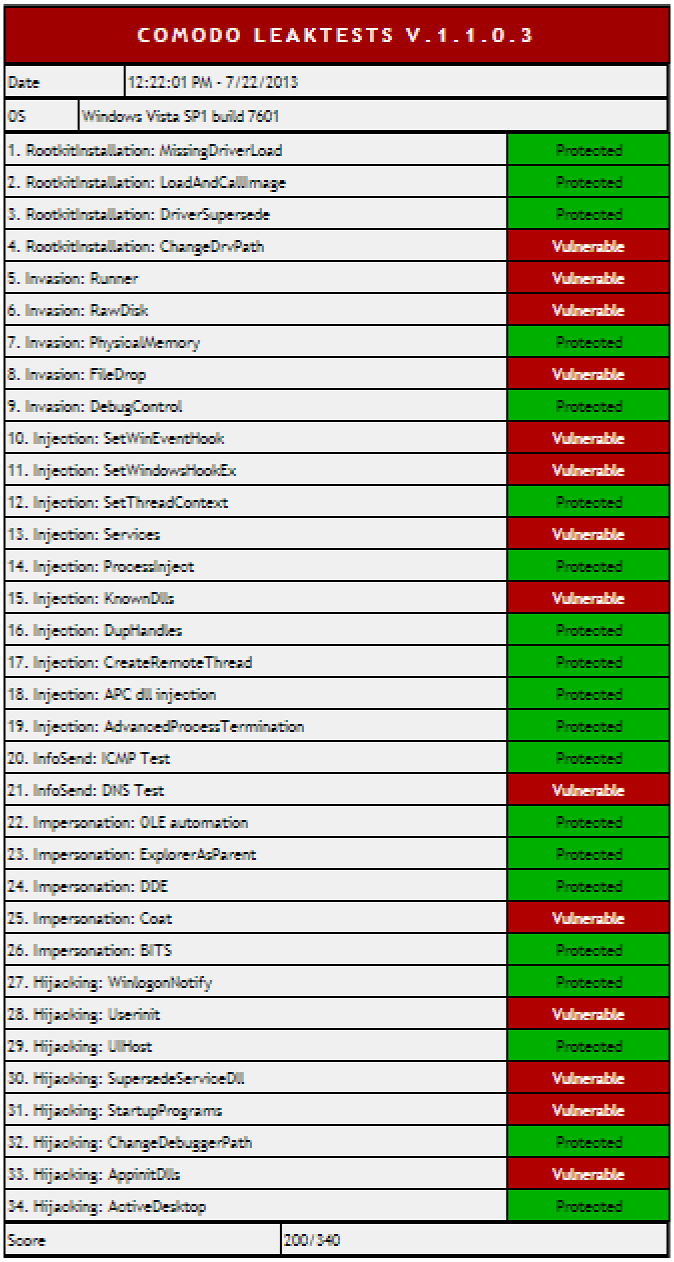
- **210/340**



COMODO LEAKTESTS V.1.1.0.3

Date	12:11:28 PM - 7/22/2013
OS	Windows Vista SP1 build 7601
1. RootkitInstallation: MissingDriverLoad	Protected
2. RootkitInstallation: LoadAndCallImage	Protected
3. RootkitInstallation: DriverSupersede	Protected
4. RootkitInstallation: ChangeDrvPath	Vulnerable
5. Invasion: Runner	Protected
6. Invasion: RawDisk	Vulnerable
7. Invasion: PhysicalMemory	Protected
8. Invasion: FileDrop	Vulnerable
9. Invasion: DebugControl	Protected
10. Injection: SetWinEventHook	Vulnerable
11. Injection: SetWindowsHookEx	Vulnerable
12. Injection: SetThreadContext	Protected
13. Injection: Services	Vulnerable
14. Injection: ProcessInject	Protected
15. Injection: KnownDlls	Vulnerable
16. Injection: DupHandles	Protected
17. Injection: CreateRemoteThread	Protected
18. Injection: APC dll injection	Protected
19. Injection: AdvancedProcessTermination	Protected
20. InfoSend: ICMP Test	Protected
21. InfoSend: DNS Test	Vulnerable
22. Impersonation: OLE automation	Protected
23. Impersonation: ExplorerAsParent	Protected
24. Impersonation: DDE	Protected
25. Impersonation: Coat	Vulnerable
26. Impersonation: BITS	Protected
27. Hijacking: WinlogonNotify	Protected
28. Hijacking: Userinit	Vulnerable
29. Hijacking: UIHost	Protected
30. Hijacking: SupersedeServiceDll	Vulnerable
31. Hijacking: StartupPrograms	Vulnerable
32. Hijacking: ChangeDebuggerPath	Protected
33. Hijacking: AppinitDlls	Vulnerable
34. Hijacking: ActiveDesktop	Protected
Score	210/340

5. **Private Firewall Free:**
    - **200/340**

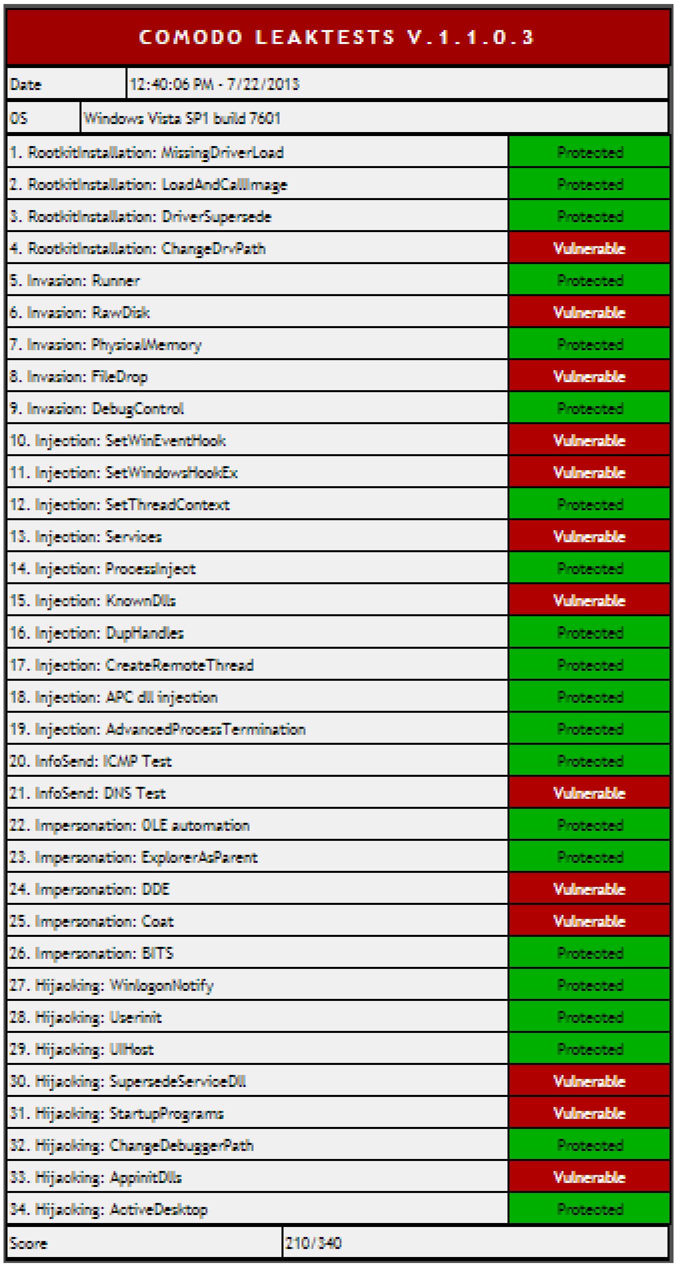


COMODO LEAKTESTS V.1.1.0.3

Date	12:22:01 PM - 7/22/2013
OS	Windows Vista SP1 build 7601
1. RootkitInstallation: MissingDriverLoad	Protected
2. RootkitInstallation: LoadAndCallImage	Protected
3. RootkitInstallation: DriverSupersede	Protected
4. RootkitInstallation: ChangeDrvPath	Vulnerable
5. Invasion: Runner	Vulnerable
6. Invasion: RawDisk	Vulnerable
7. Invasion: PhysicalMemory	Protected
8. Invasion: FileDrop	Vulnerable
9. Invasion: DebugControl	Protected
10. Injection: SetWinEventHook	Vulnerable
11. Injection: SetWindowsHookEx	Vulnerable
12. Injection: SetThreadContext	Protected
13. Injection: Services	Vulnerable
14. Injection: ProcessInject	Protected
15. Injection: KnownDlls	Vulnerable
16. Injection: DupHandles	Protected
17. Injection: CreateRemoteThread	Protected
18. Injection: APC dll injection	Protected
19. Injection: AdvancedProcessTermination	Protected
20. InfoSend: ICMP Test	Protected
21. InfoSend: DNS Test	Vulnerable
22. Impersonation: OLE automation	Protected
23. Impersonation: ExplorerAsParent	Protected
24. Impersonation: DDE	Protected
25. Impersonation: Coat	Vulnerable
26. Impersonation: BITS	Protected
27. Hijacking: WinlogonNotify	Protected
28. Hijacking: Userinit	Vulnerable
29. Hijacking: UIHost	Protected
30. Hijacking: SupersedeServiceDll	Vulnerable
31. Hijacking: StartupPrograms	Vulnerable
32. Hijacking: ChangeDebuggerPath	Protected
33. Hijacking: AppinitDlls	Vulnerable
34. Hijacking: ActiveDesktop	Protected
Score	200/340

6. Outpost Firewall Pro:

- **210/340**



COMODO LEAKTESTS V.1.1.0.3

Date	12:40:06 PM - 7/22/2013
OS	Windows Vista SP1 build 7601
1. RootkitInstallation: MissingDriverLoad	Protected
2. RootkitInstallation: LoadAndCallImage	Protected
3. RootkitInstallation: DriverSupersede	Protected
4. RootkitInstallation: ChangeDrvPath	Vulnerable
5. Invasion: Runner	Protected
6. Invasion: RawDisk	Vulnerable
7. Invasion: PhysicalMemory	Protected
8. Invasion: FileDrop	Vulnerable
9. Invasion: DebugControl	Protected
10. Injection: SetWinEventHook	Vulnerable
11. Injection: SetWindowsHookEx	Vulnerable
12. Injection: SetThreadContext	Protected
13. Injection: Services	Vulnerable
14. Injection: ProcessInject	Protected
15. Injection: KnownDlls	Vulnerable
16. Injection: DupHandles	Protected
17. Injection: CreateRemoteThread	Protected
18. Injection: APC dll injection	Protected
19. Injection: AdvancedProcessTermination	Protected
20. InfoSend: ICMP Test	Protected
21. InfoSend: DNS Test	Vulnerable
22. Impersonation: OLE automation	Protected
23. Impersonation: ExplorerAsParent	Protected
24. Impersonation: DDE	Vulnerable
25. Impersonation: Coat	Vulnerable
26. Impersonation: BITS	Protected
27. Hijacking: WinlogonNotify	Protected
28. Hijacking: Userinit	Protected
29. Hijacking: UIHost	Protected
30. Hijacking: SupersedeServiceDll	Vulnerable
31. Hijacking: StartupPrograms	Vulnerable
32. Hijacking: ChangeDebuggerPath	Protected
33. Hijacking: AppinitDlls	Vulnerable
34. Hijacking: ActiveDesktop	Protected
Score	210/340