

```

Rules Engine: SF_SHORT_DETECTION_ENGINE Version 2.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_PIPELNEI Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Commencing packet processing (pid=2164)
03/29-23:53:16.033913 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] (TCP) 192.168.1.1:80 -> 192.168.1.20:56506
03/29-23:53:16.035372 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] (TCP) 192.168.1.1:80 -> 192.168.1.20:56507
03/29-23:53:16.036479 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] (TCP) 192.168.1.1:80 -> 192.168.1.20:56508
03/29-23:53:16.037093 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] (TCP) 192.168.1.1:80 -> 192.168.1.20:56509
03/29-23:53:16.142921 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] (TCP) 192.168.1.1:80 -> 192.168.1.20:302
03/29-23:53:16.194409 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] (TCP) 192.168.1.1:80 -> 192.168.1.20:56510
03/29-23:53:16.677078 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] (TCP) 192.168.1.1:80 -> 192.168.1.20:56512
03/29-23:53:16.808301 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] (TCP) 192.168.1.1:80 -> 192.168.1.20:56513
03/29-23:53:16.944237 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] (TCP) 192.168.1.1:80 -> 192.168.1.20:56514
03/29-23:53:16.948012 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] (TCP) 192.168.1.1:80 -> 192.168.1.20:56515
03/29-23:53:16.953992 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] (TCP) 192.168.1.1:80 -> 192.168.1.20:56516
03/29-23:53:16.967744 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] (TCP) 192.168.1.1:80 -> 192.168.1.20:56517
03/29-23:53:16.982649 [**] [120:3:1] <http_inspect> NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] (TCP) 192.168.1.1:80 -> 192.168.1.20:56518

```



```
Administrator: C:\Windows\system32\cmd.exe
Total Memory Allocated: 0
Snort exiting
C:\Snort\bin>snort -W

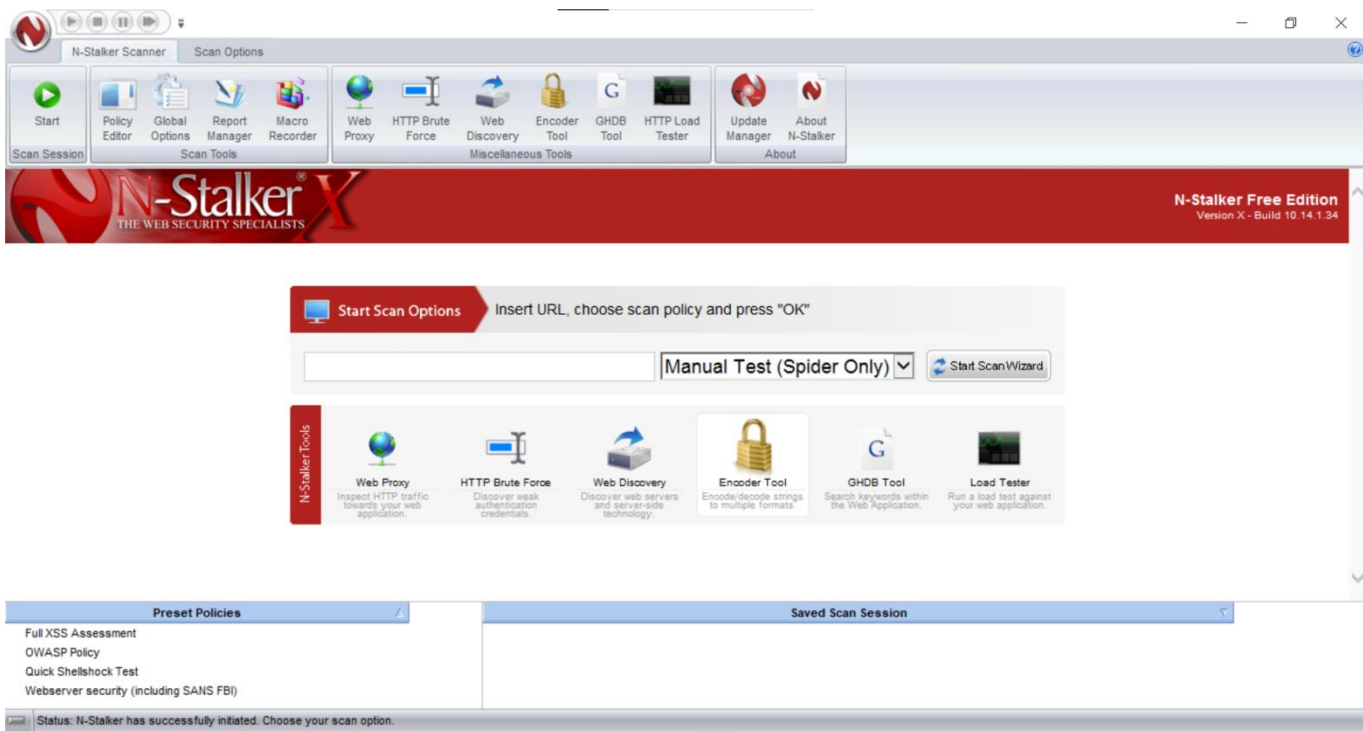
-*> Snort! <*-
Version 2.9.6.0-WIN32 GRE (Build 47)
By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-team

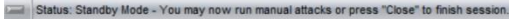
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.3

Index  Physical Address      IP Address      Device Name      Description
-----
1      00:00:00:00:00:00      0000:0000:fe80:0000:0000:0000:78d2:6299 \Device\
NPF_{45DAC1EF-70A2-4C33-B712-AE311620EB7A} VMware Virtual Ethernet Adapter
2      00:00:00:00:00:00      0000:0000:fe80:0000:0000:0000:bca3:2f66 \Device\
NPF_{C355D233-3D77-484F-A344-65626159980E} VMware Virtual Ethernet Adapter
3      00:00:00:00:00:00      0000:0000:fe80:0000:0000:0000:ada3:46c9 \Device\
NPF_{3264BC0F-4BF2-49C5-B5D9-A12EFE40F17C} Microsoft

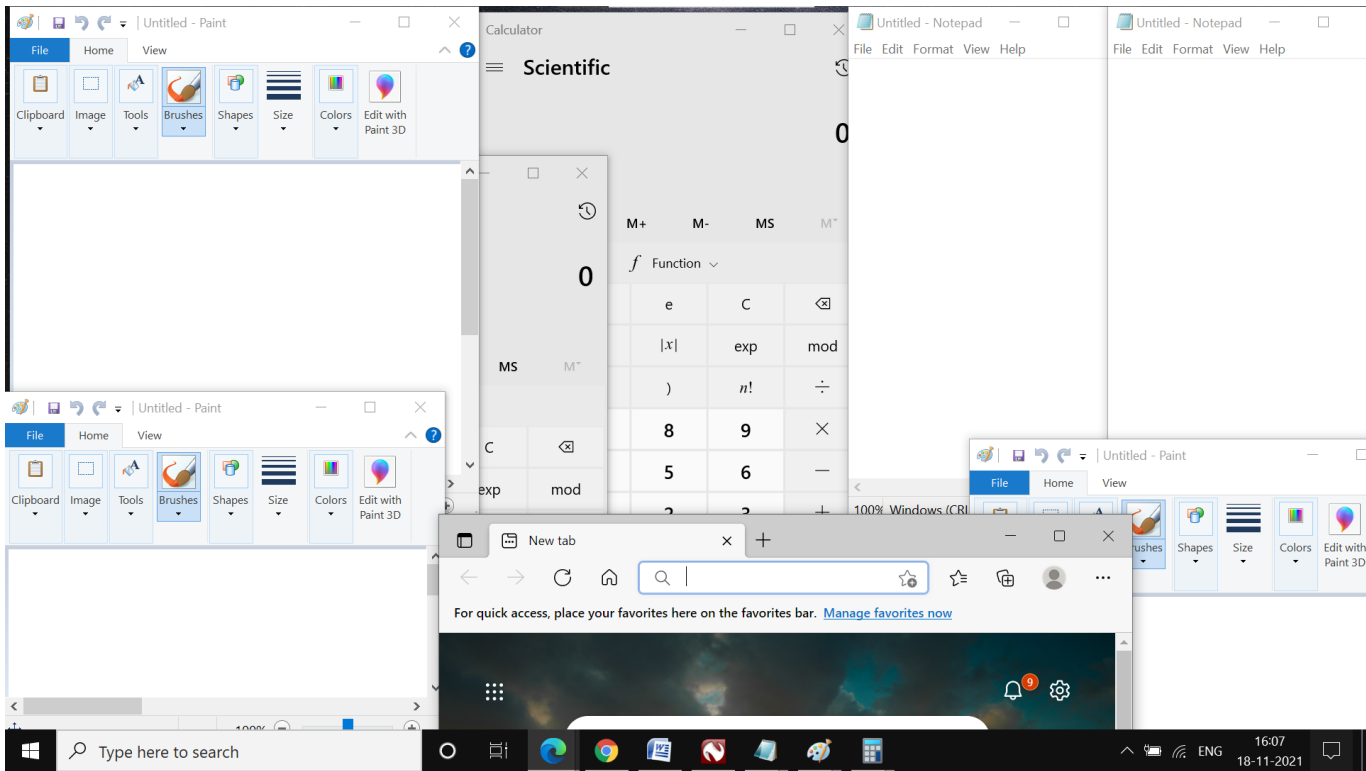
C:\Snort\bin>
```

EX NO 10





EX NO 11 A



EX NO 11 B

Type	Name	Value
.text	C:\WINDOWS\system32\vd.dllKdSetHiberRange + 29	ffff80244c910bd 2 bytes [4C, 8B]
.text	C:\WINDOWS\system32\vd.dllKdSetHiberRange + 36	ffff80244c910c4 4 bytes [E8, B7, 45, CF]
.text	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsLnBlockOffset + 118	ffff80244cd4bd6 2 bytes [4C, 8B]
.text	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsLnBlockOffset + 125	ffff80244cd4bdd 4 bytes [E8, 9E, F0, F1]
.text	...	* 27
.text	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsLnLess + 56	ffff80244cd6a28 2 bytes [4C, 8B]
.text	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsLnLess + 63	ffff80244cd6a2f 4 bytes [E8, 3C, BF, C4]
.text	...	* 11
.text	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsLnCreate + 204	ffff80244cd705c 2 bytes [4C, 8B]
.text	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsLnCreate + 211	ffff80244cd7063 4 bytes [E8, 48, 20, B3]
.text	...	* 15
.text	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsLnRecordSequence + 320	ffff80244cd7d90 2 bytes [4C, 8B]
.text	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsLnRecordSequence + 327	ffff80244cd7d97 4 bytes [E8, 14, 13, B3]
.text	...	* 3
.text	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsLnDiffernce + 447	ffff80244cd851f 2 bytes [4C, 8B]
.text	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsLnDiffernce + 454	ffff80244cd8526 4 bytes [E8, 75, F3, C4]
.text	...	* 7
.text	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsLnInvalid + 483	ffff80244cd8a4d3 2 bytes [4C, 8B]
.text	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsLnInvalid + 490	ffff80244cd8a4da 5 bytes [CALL 0x12d6c66]
.text	...	* 13
.text	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsLnContainer + 436	ffff80244cdad54 2 bytes [4C, 8B]
.text	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsLnContainer + 443	ffff80244cdad5b 4 bytes [E8, 70, D5, C4]
PAGE	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsMgmtQueryPolicy + 56	ffff80244cf7198 2 bytes [4C, 8B]
PAGE	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsMgmtQueryPolicy + 63	ffff80244cf719f 4 bytes [E8, 9C, EC, B0]
PAGE	...	* 15
PAGE	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsAdvanceLogBase + 134	ffff80244cf78b6 2 bytes [4C, 8B]
PAGE	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsAdvanceLogBase + 141	ffff80244cf78bd 4 bytes [E8, 7E, E5, B0]
PAGE	...	* 9
PAGE	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsDeleteLogByPointer + 69	ffff80244cf7e25 2 bytes [4C, 8B]
PAGE	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsDeleteLogByPointer + 76	ffff80244cf7e2c 4 bytes [E8, 0F, E0, B0]
PAGE	...	* 7
PAGE	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsFreeReservedLog + 105	ffff80244cf8109 2 bytes [4C, 8B]
PAGE	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsFreeReservedLog + 112	ffff80244cf8110 4 bytes [E8, 2B, DD, B0]
PAGE	...	* 7
PAGE	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsFlushBuffers + 295	ffff80244cf8547 2 bytes [4C, 8B]
PAGE	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsFlushBuffers + 302	ffff80244cf854e 4 bytes [E8, 9D, 07, B1]
PAGE	...	* 15
PAGE	C:\WINDOWS\system32\drivers\CLFS.SYSIClfsFlushToLn + 139	ffff80244cf8bbcb 2 bytes [4C, 8B]

Sections: C:\WINDOWS\system32\lsass.exe [908] @ C:\WINDOWS\system32\rsaenh.dll

GMER 2.2.19882 WINDOWS 6.2.9200 x64 AntiVirus: http://www.avast.com

Rootkit/Malware > > >

Type	Name	Value
Thread	C:\WINDOWS\system32\csrss.exe [732:772]	ffff8f0fea536c20
Thread	C:\WINDOWS\system32\backgroundTaskHost.exe ...	00007ffaa9da48e0
Thread	C:\WINDOWS\system32\backgroundTaskHost.exe ...	00007ffab16025a0
Service	C:\WINDOWS\system32\svchost.exe (*** hidden ***)	[AUTO] CDPUserSvc_554df
Service	C:\WINDOWS\system32\svchost.exe (*** hidden ***)	[MANUAL] MessagingService_554df
Service	C:\WINDOWS\system32\svchost.exe (*** hidden ***)	[AUTO] OneSyncSvc_554df
Service	C:\WINDOWS\system32\svchost.exe (*** hidden ***)	[MANUAL] PimIndexMaintenanceSvc_554df
Service	C:\WINDOWS\system32\svchost.exe (*** hidden ***)	[MANUAL] UnistoreSvc_554df
Service	C:\WINDOWS\system32\svchost.exe (*** hidden ***)	[MANUAL] UserDataSvc_554df
Service	C:\WINDOWS\system32\svchost.exe (*** hidden ***)	[MANUAL] WpnUserService_554df


☒ System
☒ Sections
☒ IAT/EAT
☒ Devices
☒ Trace I/O
☒ Modules
☒ Processes
☒ Threads
☒ Libraries
☒ Services
☒ Registry
☒ Files
☒ Quick scan
☐ C:\

☒ ADS
☐ Show all
☐ 3rd party

Scan

Copy

Save ...



WARNING !!!

GMER has found system modification, which might have been caused by ROOTKIT activity.

Do you want to fully scan your system ?

Oui Non

GMER 2.2.19882 WINDOWS 6.2.9200 x64 AntiVirus: <http://www.avast.com>

Exit