Snort Sniffing Tool

Theory:

Snort is an open-source security software product that looks at network traffic in real time and logs packets to perform detailed analysis used to facilitate security and authentication efforts.

Snort was released by Martin Roesch in 1998.

Snort is useful for developers or others working on different types of system troubleshooting.

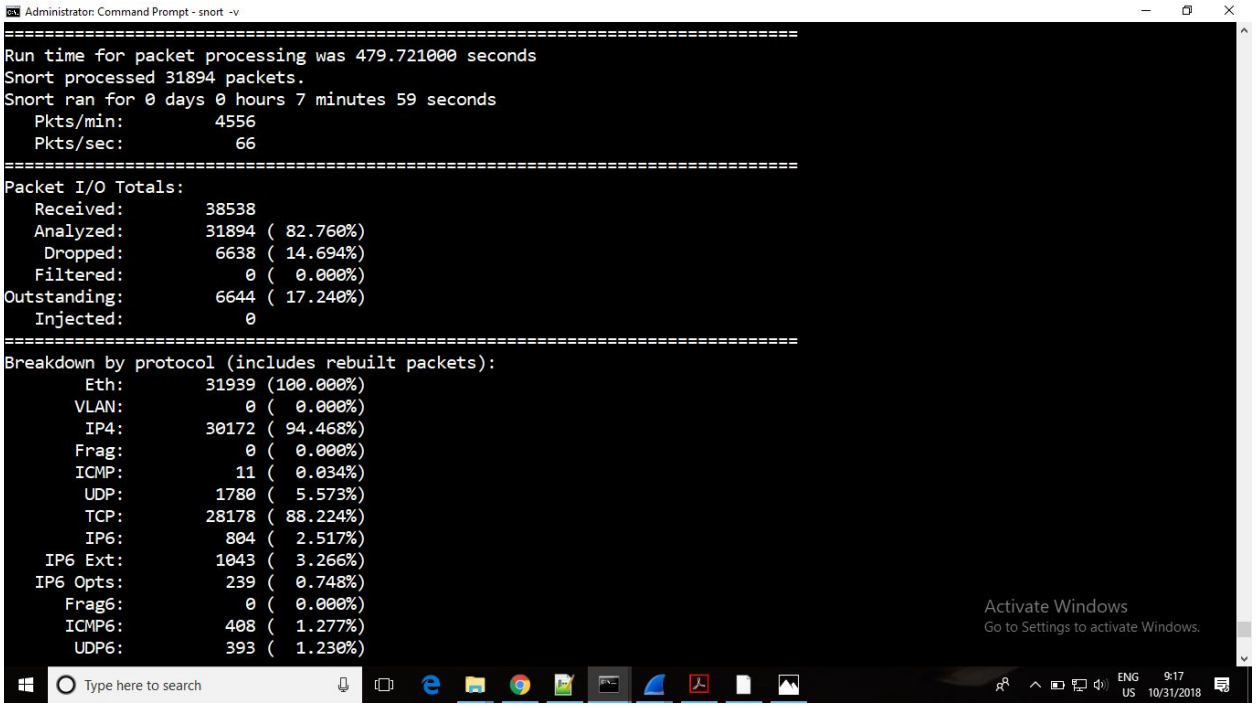
The security tool has three different modes, as follows:

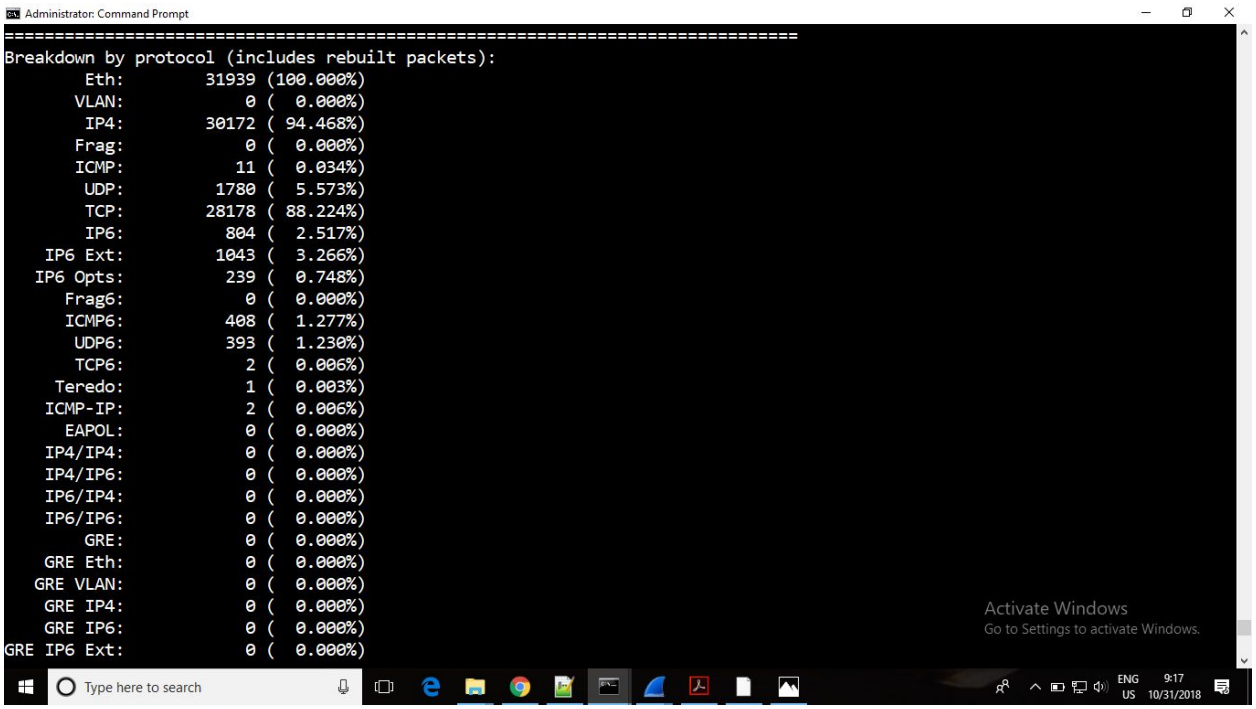
- Packet sniffer
- Consistent logging of network traffic to facilitate debugging
- Active network intrusion handling system

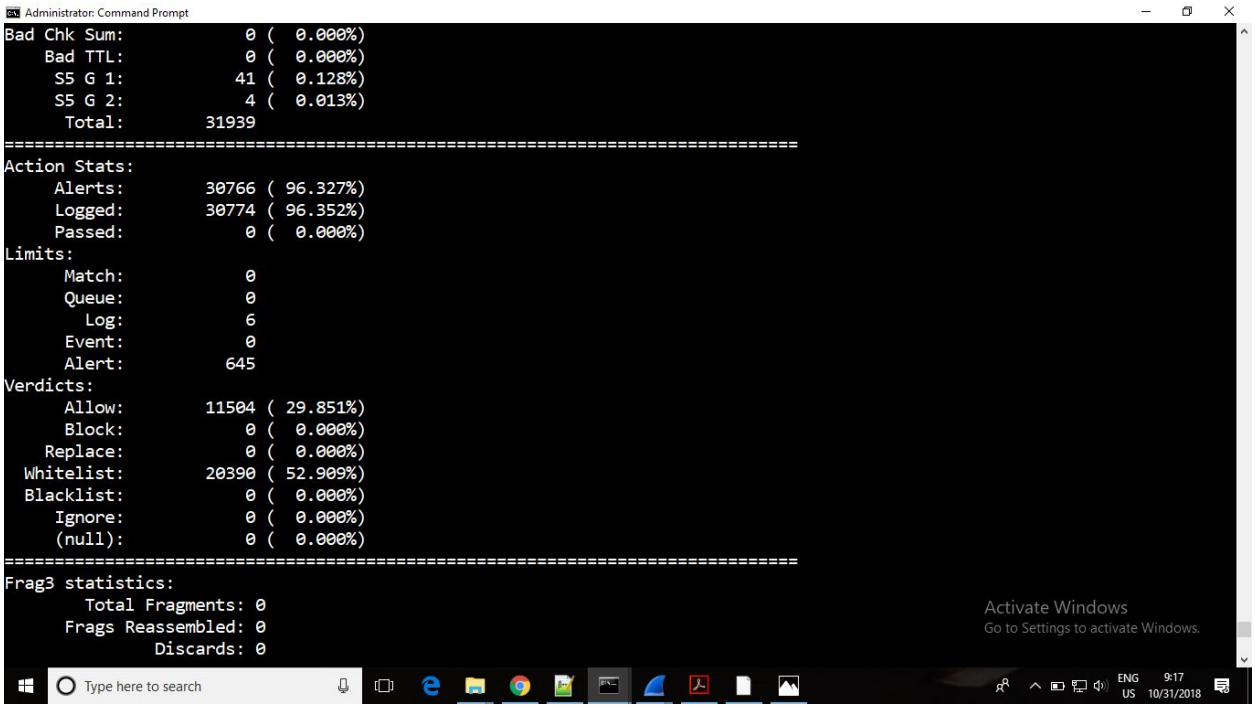
Snort is built to detect various types of hacking and uses a flexible rules language to determine the types of network traffic that should be collected.

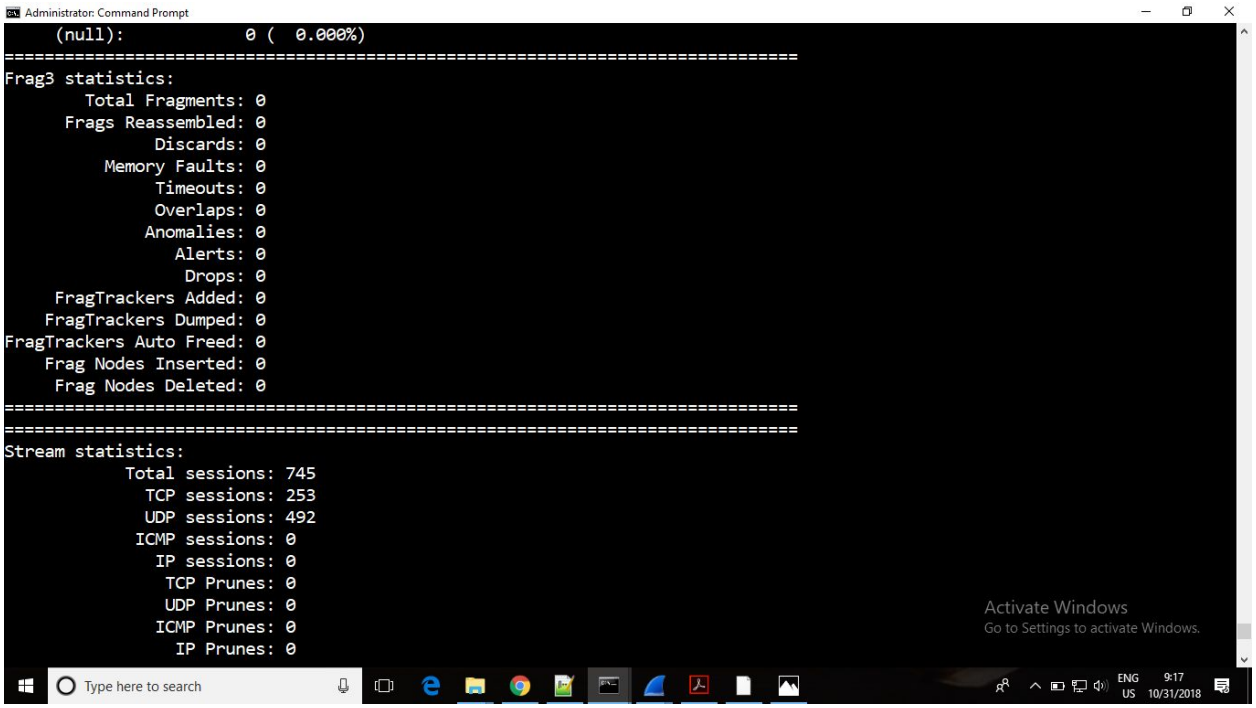
For Snort to work correctly, users must identify directories for use and perform calibrations to specify how the program should work in any of its three basic modes.

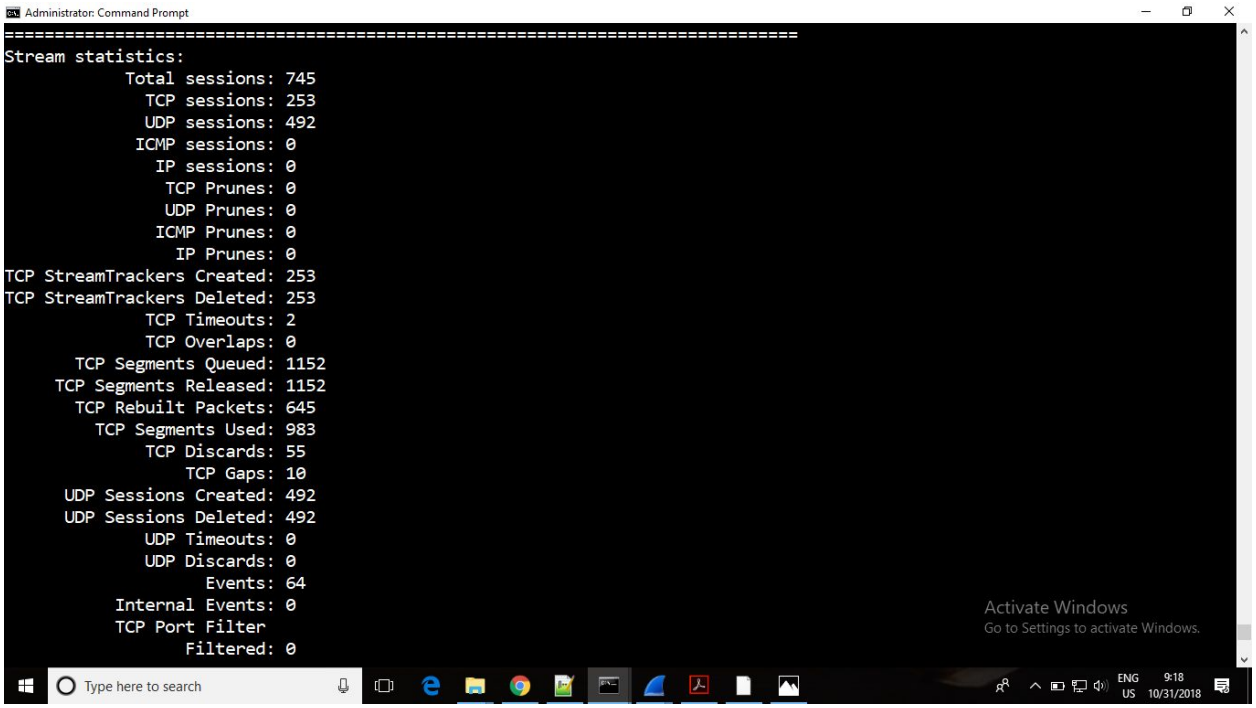
Implementation:

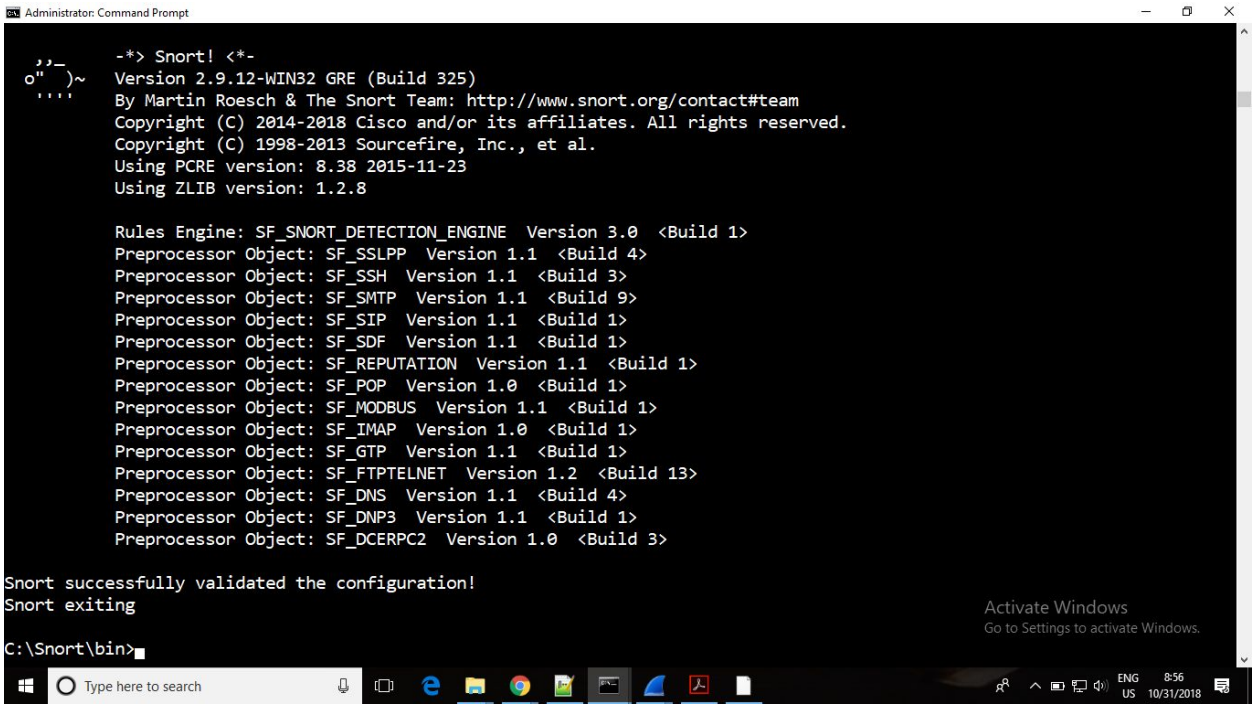


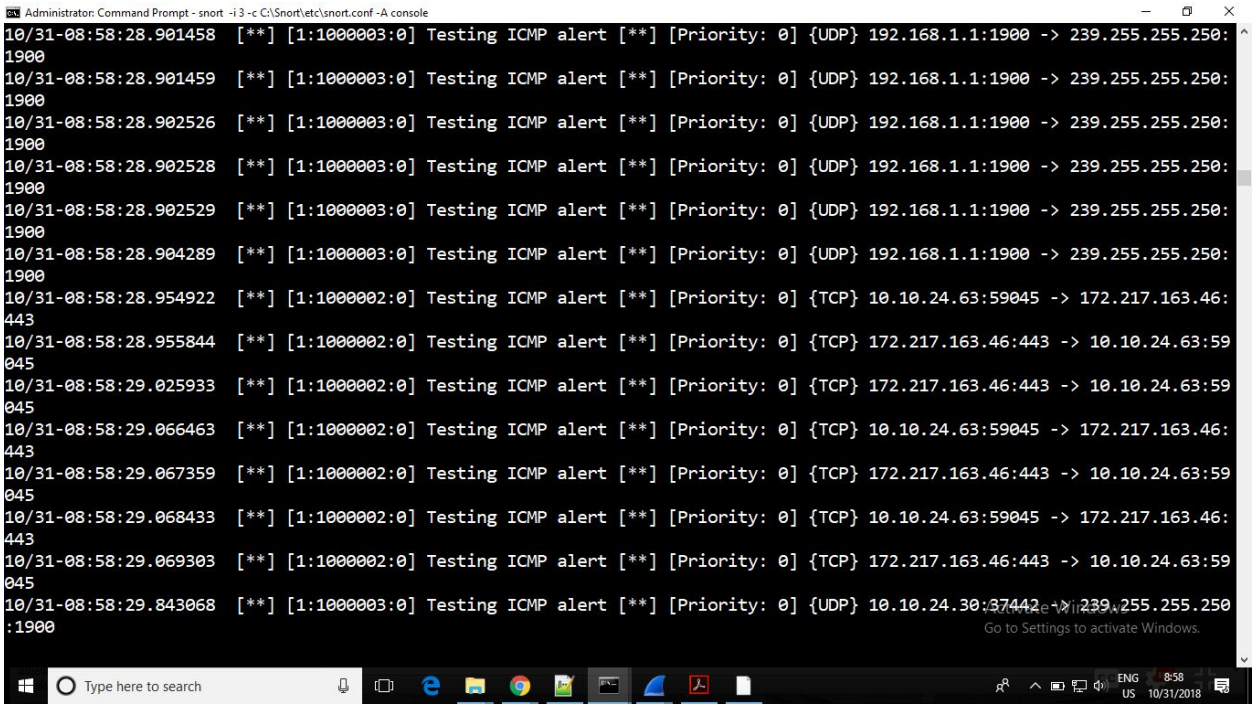


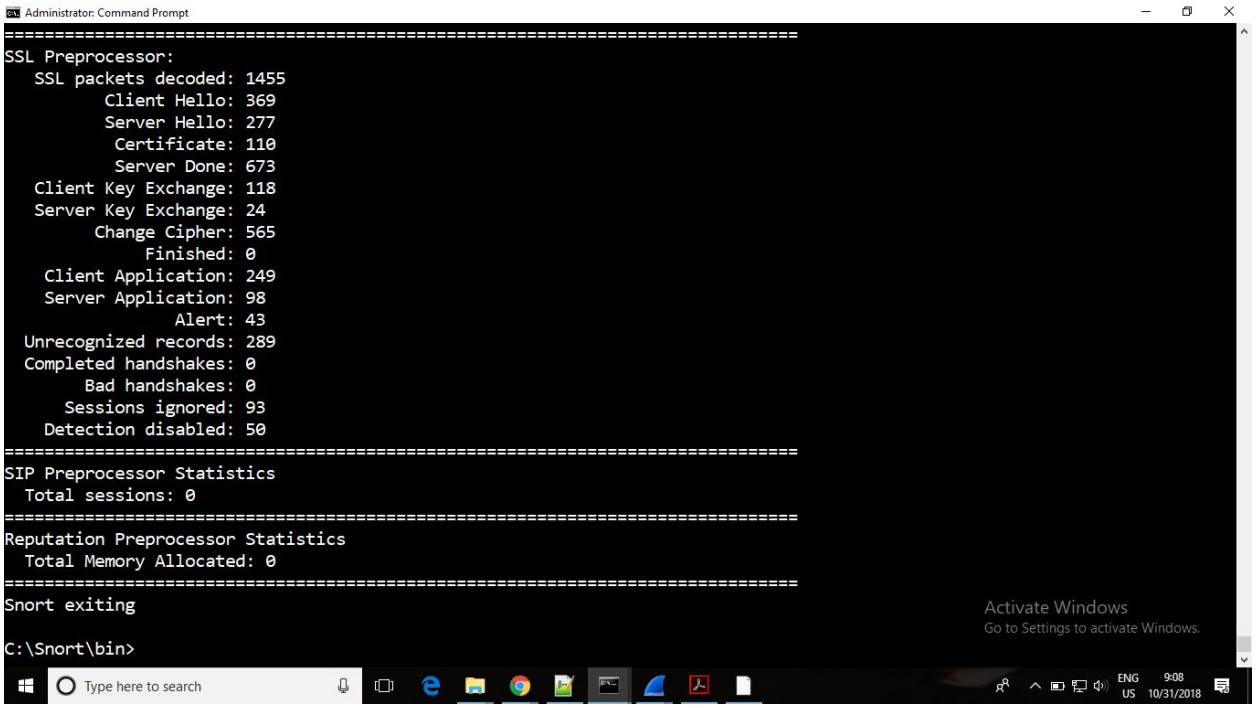

Administrator: Command Prompt
Bad Chk Sum: 0 (0.000%)
Bad TTL: 0 (0.000%)
S5 G 1: 41 (0.128%)
S5 G 2: 4 (0.013%)
Total: 31939
Action Stats:
Alerts: 30766 (96.327%)
Logged: 30774 (96.352%)
Passed: 0 (0.000%)
Limits:
Match: 0
Queue: 0
Log: 6
Event: 0
Alert: 645
Verdicts:
Allow: 11504 (29.851%)
Block: 0 (0.000%)
Replace: 0 (0.000%)
Whitelist: 20390 (52.909%)
Blacklist: 0 (0.000%)
Ignore: 0 (0.000%)
(null): 0 (0.000%)
Frag3 statistics:
Total Fragments: 0
Frags Reassembled: 0
Discards: 0
Activate Windows
Go to Settings to activate Windows.
Type here to search
ENG
US
9:17
10/31/2018


Administrator: Command Prompt
(null): 0 (0.000%)
Frag3 statistics:
Total Fragments: 0
Frags Reassembled: 0
Discards: 0
Memory Faults: 0
Timeouts: 0
Overlaps: 0
Anomalies: 0
Alerts: 0
Drops: 0
FragTrackers Added: 0
FragTrackers Dumped: 0
FragTrackers Auto Freed: 0
Frag Nodes Inserted: 0
Frag Nodes Deleted: 0
Stream statistics:
Total sessions: 745
TCP sessions: 253
UDP sessions: 492
ICMP sessions: 0
IP sessions: 0
TCP Prunes: 0
UDP Prunes: 0
ICMP Prunes: 0
IP Prunes: 0
Activate Windows
Go to Settings to activate Windows.
Type here to search
ENG US 9:17 10/31/2018


Administrator: Command Prompt
Stream statistics:
Total sessions: 745
TCP sessions: 253
UDP sessions: 492
ICMP sessions: 0
IP sessions: 0
TCP Prunes: 0
UDP Prunes: 0
ICMP Prunes: 0
IP Prunes: 0
TCP StreamTrackers Created: 253
TCP StreamTrackers Deleted: 253
TCP Timeouts: 2
TCP Overlaps: 0
TCP Segments Queued: 1152
TCP Segments Released: 1152
TCP Rebuilt Packets: 645
TCP Segments Used: 983
TCP Discards: 55
TCP Gaps: 10
UDP Sessions Created: 492
UDP Sessions Deleted: 492
UDP Timeouts: 0
UDP Discards: 0
Events: 64
Internal Events: 0
TCP Port Filter
Filtered: 0
Activate Windows
Go to Settings to activate Windows.
Type here to search
ENG US 9:18 10/31/2018


Administrator: Command Prompt
-*> Snort! <*-
Version 2.9.12-WIN32 GRE (Build 325)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2018 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.38 2015-11-23
Using ZLIB version: 1.2.8
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.0 <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_FTPTELNET 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>
Snort successfully validated the configuration!
Snort exiting
C:\Snort\bin>
Activate Windows
Go to Settings to activate Windows.
Type here to search
ENG US 8:56 10/31/2018


Administrator: Command Prompt - snort -i 3 -c C:\Snort\etc\snort.conf -A console
10/31-08:58:28.901458 [**] [1:1000003:0] Testing ICMP alert [**] [Priority: 0] {UDP} 192.168.1.1:1900 -> 239.255.255.250:1900
10/31-08:58:28.901459 [**] [1:1000003:0] Testing ICMP alert [**] [Priority: 0] {UDP} 192.168.1.1:1900 -> 239.255.255.250:1900
10/31-08:58:28.902526 [**] [1:1000003:0] Testing ICMP alert [**] [Priority: 0] {UDP} 192.168.1.1:1900 -> 239.255.255.250:1900
10/31-08:58:28.902528 [**] [1:1000003:0] Testing ICMP alert [**] [Priority: 0] {UDP} 192.168.1.1:1900 -> 239.255.255.250:1900
10/31-08:58:28.902529 [**] [1:1000003:0] Testing ICMP alert [**] [Priority: 0] {UDP} 192.168.1.1:1900 -> 239.255.255.250:1900
10/31-08:58:28.904289 [**] [1:1000003:0] Testing ICMP alert [**] [Priority: 0] {UDP} 192.168.1.1:1900 -> 239.255.255.250:1900
10/31-08:58:28.954922 [**] [1:1000002:0] Testing ICMP alert [**] [Priority: 0] {TCP} 10.10.24.63:59045 -> 172.217.163.46:443
10/31-08:58:28.955844 [**] [1:1000002:0] Testing ICMP alert [**] [Priority: 0] {TCP} 172.217.163.46:443 -> 10.10.24.63:59045
10/31-08:58:29.025933 [**] [1:1000002:0] Testing ICMP alert [**] [Priority: 0] {TCP} 172.217.163.46:443 -> 10.10.24.63:59045
10/31-08:58:29.066463 [**] [1:1000002:0] Testing ICMP alert [**] [Priority: 0] {TCP} 10.10.24.63:59045 -> 172.217.163.46:443
10/31-08:58:29.067359 [**] [1:1000002:0] Testing ICMP alert [**] [Priority: 0] {TCP} 172.217.163.46:443 -> 10.10.24.63:59045
10/31-08:58:29.068433 [**] [1:1000002:0] Testing ICMP alert [**] [Priority: 0] {TCP} 10.10.24.63:59045 -> 172.217.163.46:443
10/31-08:58:29.069303 [**] [1:1000002:0] Testing ICMP alert [**] [Priority: 0] {TCP} 172.217.163.46:443 -> 10.10.24.63:59045
10/31-08:58:29.843068 [**] [1:1000003:0] Testing ICMP alert [**] [Priority: 0] {UDP} 10.10.24.30:37442 -> 239.255.255.250:1900
Activate Windows
Go to Settings to activate Windows.
Type here to search
ENG US 8:58 10/31/2018



What is zero day attack?

A zero-day (also known as 0-day) vulnerability is a computer-software vulnerability that is unknown to those who would be interested in mitigating the vulnerability (including the vendor of the target software). Until the vulnerability is mitigated, hackers can exploit it to adversely affect computer programs, data, additional computers or a network. An exploit directed at a zero-day is called a zero-day exploit, or zero-day attack

In the jargon of computer security, "Day Zero" is the day on which the interested party (presumably the vendor of the targeted system) learns of the vulnerability. Up until that day, the vulnerability is known as a zero-day vulnerability. Similarly, an exploitable bug that has been known for thirty days would be called a 30-day vulnerability. Once the vendor learns of the vulnerability, the vendor will usually create patches or advise workarounds to mitigate it.[2]

The fewer the days since Day Zero, the higher the chance no fix or mitigation has been developed. Even after a fix is developed, the fewer the days since Day Zero, the higher is the probability that an attack against the afflicted software will be successful, because not every user of that software will have applied the fix. For zero-day exploits, the probability that a user has patched their bugs is zero, so the exploit should always succeed.[3] Zero-day attacks are a severe threat.[4]

.

Can Snort catch zero day attacks? why?

A frequent claim that has not been validated is that signature based network intrusion detection systems (SNIDS) cannot detect zero-day attacks. This paper studies this property by testing 356 severe attacks on the SNIDS Snort, configured with an old official rule set. Of these attacks, 183 attacks are zero-days' to the rule set and 173 attacks are theoretically known to it. The results from the study show that Snort clearly is able to detect zero-days' (a mean of 17% detection). The detection rate is however on overall greater for theoretically known attacks (a mean of 54% detection). The paper then investigates how the zero-days' are detected, how prone the corresponding signatures are to false alarms, and how easily they can be evaded. Analyses of these aspects suggest that a conservative estimate on zero-day detection by Snort is 8.2%

Conclusion: How to use sniffing tool to capturing attack is studied