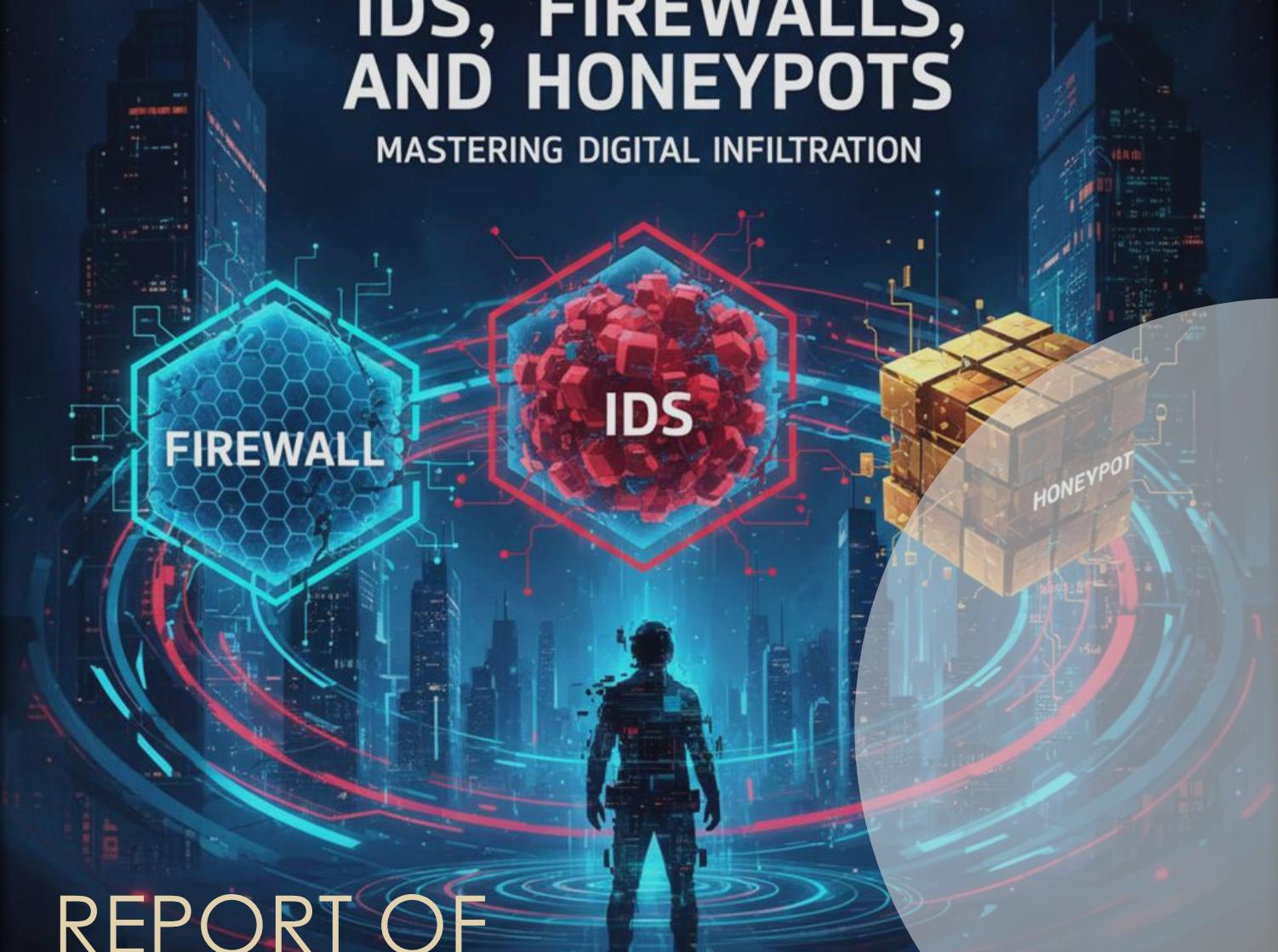


EVADING IDS, FIREWALLS, AND HONEYPOTS

MASTERING DIGITAL INFILTRATION



FIREWALL

IDS

HONEYPOT

REPORT OF EVADING IDS, FIREWALLS, AND HONEYPOTS

BY SACHCHITANAND YADAV

EVADING IDS, FIREWALLS, AND HONEYPOTS

MODULE - 12

Learning Objectives -

- Explain Evading IDS, Firewalls, and Honeypots Concepts
- Perform Intrusion Detection using Various Tools
- Explain Evading IDS, Firewalls, and Honeypots Countermeasures

Table of Contents

1. Evading IDS, Firewalls, and Honeypots Concepts

1.1 IDS, IPS, and Firewall Concepts

1.2 Firewall

- 1.2.1 Firewall: The Network Control Barrier
- 1.2.2 Classification of Firewalls
- 1.2.3 Importance of Firewalls
- 1.2.4 Firewall Operational Overview

1.3 Intrusion Detection System (IDS)

- 1.3.1 Introduction to Intrusion Detection System
- 1.3.2 Objectives of IDS
- 1.3.3 Types of Intrusion Detection Systems
- 1.3.4 Intrusion Detection Techniques
- 1.3.5 IDS Alert Categories

1.4 Intrusion Prevention System (IPS)

- 1.4.1 Introduction to Intrusion Prevention System
- 1.4.2 IPS Response Actions
- 1.4.3 IPS Functional Workflow
- 1.4.4 Types of Intrusion Prevention Systems

1.5 Honeypot

- 1.5.1 Honeypot: Deception-Based Security
- 1.5.2 Objectives of Honeypots
- 1.5.3 Honeypot Operation
- 1.5.4 Types of Honeypots
- 1.5.5 Honeynet

2. Performing Intrusion Detection Using Tools

- 2.1 Introduction to Snort
- 2.2 Objectives and Uses of Snort
- 2.3 Key Features of Snort
- 2.4 Snort Architecture
- 2.5 Modes of Operation of Snort

- 2.6 Snort Installation and Basic Setup
 - 2.7 Advantages of Snort
 - 2.8 Limitations of Snort
-

3. Snort Configuration and Implementation

- 3.1 Download and Installation
 - 3.2 Configuration File Setup
 - 3.3 Rule Configuration
 - 3.4 Command-Line Execution
 - 3.5 Validation and Testing of Configuration
 - 3.6 Starting Snort in IDS Mode
-

4. Evading IDS, Firewalls, and Honeypots – Countermeasures

- 4.1 Countermeasures Against IDS Evasion
 - 4.2 Countermeasures Against Firewall Evasion
 - 4.3 Countermeasures Against Honeypot Evasion
 - 4.4 Conclusion
-

5. Module Summary

- 5.1 Evading IDS
- 5.2 Evading Firewalls
- 5.3 Evading Honeypots

Evading IDS, Firewalls, and Honeypots

Concepts: -

IDS, IPS, and Firewall Concepts

Ethical hackers should understand the function, role, placement, and design of firewalls, IDS, and IPS, as well as how attackers evade these security measures. This section provides an overview of these concepts.

Firewall: The Network Control Barrier

A firewall is a security mechanism—hardware or software—that regulates network traffic using predefined security policies. Its primary role is to create a controlled boundary between trusted internal networks and untrusted external networks, such as the internet.

Rather than trusting everything, a firewall assumes traffic must prove itself first.

Classification of Firewalls

1. Packet Filtering Firewall

Operates at the network layer by examining packet headers such as source/destination IP, port numbers, and protocols.

It is fast and resource-efficient but lacks deep inspection capabilities.

2. Stateful Inspection Firewall

Tracks the state of active connections and evaluates traffic based on session context.

This method offers better protection by understanding whether packets belong to legitimate sessions.

3. Application-Level Gateway (Proxy Firewall)

Functions at the application layer and acts as an intermediary between users and services.

It inspects application data directly, offering enhanced security against application-layer attacks.

4. Next-Generation Firewall (NGFW)

An advanced firewall that integrates traditional filtering with modern security features such as:

- Deep packet inspection
- Intrusion prevention
- Application identification
- Malware and threat intelligence integration

5. Software Firewall

Installed on individual endpoints to protect a single system from unauthorized access.

6. Hardware Firewall

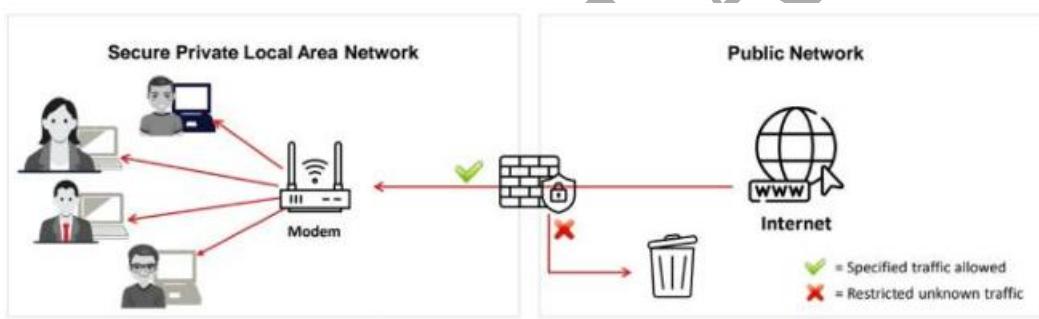
A dedicated physical device that secures an entire network, commonly used in enterprise environments.

Importance of Firewalls

Firewalls play a crucial role in network security by:

- Preventing unauthorized access
- Reducing exposure to cyber threats
- Enforcing organizational security rules
- Monitoring and logging network activity

Despite newer technologies, firewalls remain a foundational security control.



Firewall Operational Overview

When traffic attempts to enter or leave a network, the firewall evaluates it against predefined rules. If the traffic complies, it is allowed; otherwise, it is blocked and logged for analysis.

Simple logic. Zero tolerance.

Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is a monitoring solution that analyzes network or system activity to identify suspicious behavior, security violations, or attempted attacks. Unlike firewalls, IDS does not block traffic—it detects and alerts.

Think of it as the network's surveillance system.

Objectives of IDS

IDS is designed to:

- Monitor traffic and system behavior
- Detect intrusion attempts
- Generate alerts for security teams
- Identify malware and exploit patterns
- Enable early incident detection
- Support forensic investigations
- Detect insider threats
- Maintain logs for compliance and audits

IDS enhances visibility where firewalls stop short.

Types of Intrusion Detection Systems

Network-Based IDS (NIDS)

Monitors traffic across network segments to detect malicious patterns.
It is deployed at strategic locations such as gateways or DMZs.

Advantages:

- Broad network visibility
- Effective against external attacks

Examples: Snort, Suricata

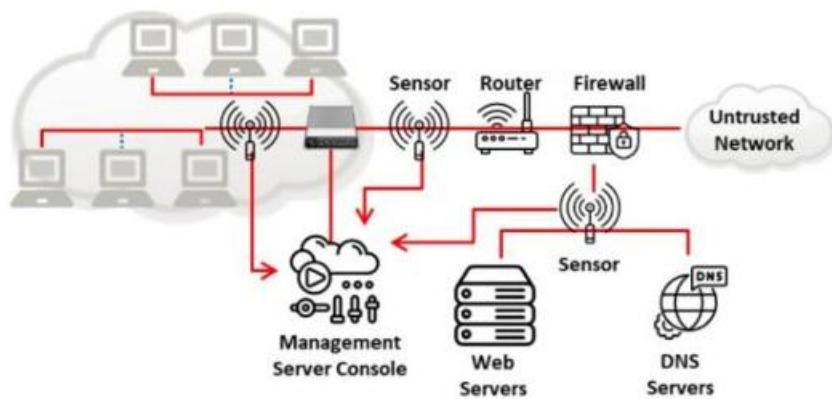


Fig:-Network-Based IDS

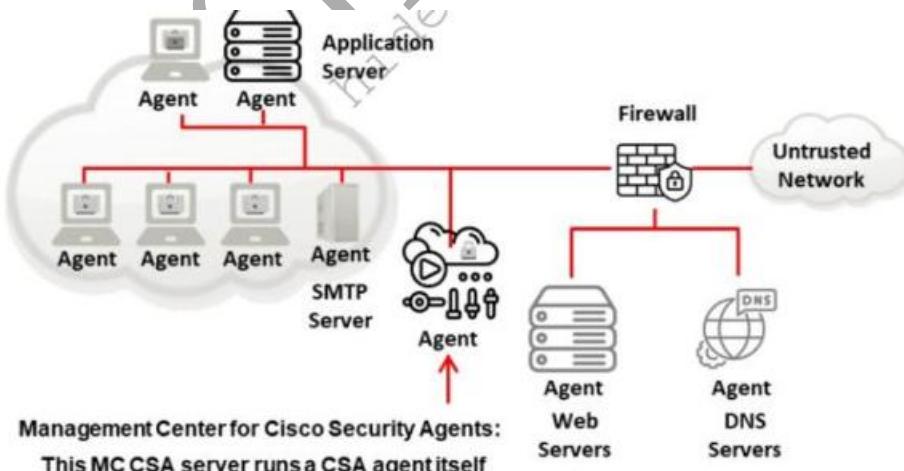
Host-Based IDS (HIDS)

Installed on individual systems to monitor internal activity such as file changes, logs, and user actions.

Advantages:

- Detects insider threats
- Protects critical servers

Examples: OSSEC, Tripwire



Intrusion Detection Techniques

Signature-Based Detection

Matches activity against known attack signatures.

Highly accurate for known threats but ineffective against new attacks.

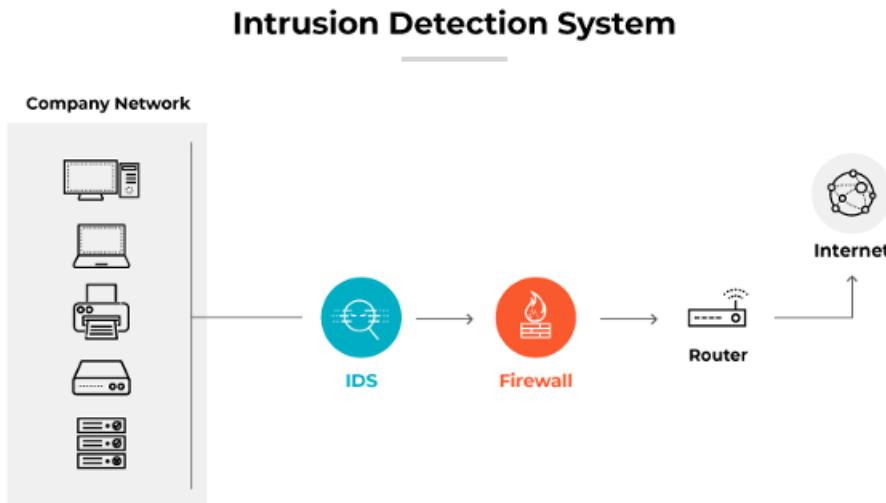
Anomaly-Based Detection

Establishes a baseline of normal behavior and flags deviations.

Capable of detecting zero-day attacks but may generate false alerts.

Protocol Anomaly Detection

Identifies violations of protocol standards, indicating possible exploitation attempts.



IDS Alert Categories

- **True Positive:** Correct detection of an attack
- **True Negative:** Correct identification of normal behavior
- **False Positive:** Benign activity flagged as malicious
- **False Negative:** Attack not detected (most dangerous scenario)

Security success depends on minimizing false negatives without drowning in false positives.

Intrusion Prevention System (IPS)

An Intrusion Prevention System (IPS) is an inline security device that actively monitors and blocks malicious traffic in real time. Unlike IDS, IPS can take immediate corrective action.

It doesn't warn—it intervenes.

IPS Response Actions

- Dropping malicious packets
- Blocking IP addresses
- Resetting connections
- Generating alerts

IPS Functional Workflow

1. Continuous traffic inspection
2. Signature and behavior analysis
3. Threat identification
4. Automatic prevention before damage occurs

Speed is everything here.

Types of IPS

Network-Based IPS (NIPS):

Protects entire networks and monitors traffic between hosts.

Host-Based IPS (HIPS):

Secures individual systems by monitoring system calls and application behavior.

Wireless IPS (WIPS):

Protects wireless networks from rogue devices and wireless attacks.

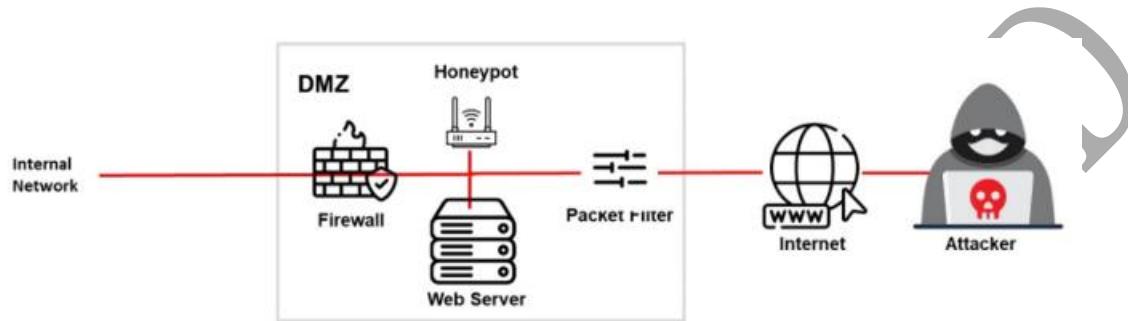
Network Behavior Analysis IPS (NBA):

Uses traffic behavior modeling to detect anomalies, insider threats, and large-scale attacks.

Honeypot: Deception-Based Security

A honeypot is a deliberately vulnerable system designed to attract attackers. It serves no legitimate purpose other than to observe, record, and analyze malicious behavior.

The attacker thinks they're winning. They're actually being studied.



Objectives of Honeypots

- Detect unauthorized activity
- Divert attackers from real assets
- Collect threat intelligence
- Improve defensive strategies

Honeypot Operation

Honeypots simulate real systems in isolated environments. Any interaction with them is treated as suspicious and logged for analysis.

Zero noise. Pure signal.

Types of Honeypots

- Low, medium, and high interaction honeypots
- Research and production honeypots
- Internal and external honeypots
- Specialized honeypots (malware, web, database, ICS)

Honeynet:

A group of interconnected honeypots that simulate an entire network for large-scale attack analysis.

Conclusion

Firewalls establish control.

IDS provides visibility.

IPS delivers immediate defense.

Honeypots offer intelligence through deception.

SACHCHITANAND

Perform Intrusion Detection using Various Tools

Snort

Snort is an open-source **Network Intrusion Detection System (NIDS)** and **Intrusion Prevention System (IPS)** originally developed by Martin Roesch and currently maintained by **Cisco Systems**. It is widely used for real-time traffic analysis, packet inspection, and logging on IP-based networks.

Snort operates by analyzing network packets and comparing them against a set of predefined rules to detect malicious activity. When configured in IPS mode, it can actively block threats, making it both a detection and prevention tool.

Objectives and Uses of Snort

Snort is used in network security environments to:

- Detect network intrusions in real time
- Perform deep packet inspection (DPI)
- Monitor network traffic for suspicious patterns
- Capture and log packets for later analysis
- Prevent attacks when deployed in IPS mode
- Detect port scanning and reconnaissance activities
- Identify malware, exploits, and suspicious payloads
- Enforce organizational security policies
- Support custom rule creation for advanced threat detection
- Assist in forensic analysis and incident response

Key Features of Snort

- **Open-source and customizable**
- **Signature-based detection engine**
- **Flexible deployment (IDS or IPS)**
- **Real-time alerting and logging**
- **Cross-platform support (Linux, Windows)**
- **Large community and rule database**

Snort Architecture

Snort follows a modular architecture consisting of:

1. **Packet Decoder**
Captures packets from the network interface.
2. **Preprocessors**
Normalize traffic, reassemble fragments, and detect protocol anomalies.
3. **Detection Engine**
Compares traffic against Snort rules to identify attacks.
4. **Logging and Alerting System**
Generates alerts and logs suspicious activity.
5. **Output Modules**
Stores logs in files, databases, or sends alerts to consoles or SIEM tools.

Modes of Operation of Snort

Snort can operate in three main modes:

1. Sniffer Mode

Displays packets on the console in real time.
Used mainly for learning and traffic observation.

2. Packet Logger Mode

Logs packets to disk for offline analysis.
Helpful during investigations.

3. Network Intrusion Detection / Prevention Mode

Analyzes traffic against rules and generates alerts or blocks traffic.
This is where Snort earns its reputation.

How to Use Snort (Basic Setup)

1. Download and install Snort from the official website.
2. Navigate to the Snort installation directory.
3. Open the `etc` folder, which contains:
 - o `snort.conf` (main configuration file)
 - o Rule files

- Preprocessor settings
 - 4. Configure the following in `snort.conf`:
 - Network variables (HOME_NET, EXTERNAL_NET)
 - Rule paths
 - Preprocessor settings
 - 5. Update or add custom rules in the **rules** directory.
 - 6. Run Snort using command-line options based on the desired mode (IDS or IPS).
 - 7. Monitor alerts and logs generated by Snort for suspicious activity.
-

Advantages of Snort

- Free and open-source
 - Highly customizable rule-based detection
 - Strong community and documentation
 - Suitable for small networks and enterprises
 - Integrates well with SIEM tools
-

Limitations of Snort

- Requires manual tuning to reduce false positives
 - Performance depends on hardware and rule complexity
 - Signature-based detection may miss zero-day attacks
 - Command-line interface has a learning curve
-

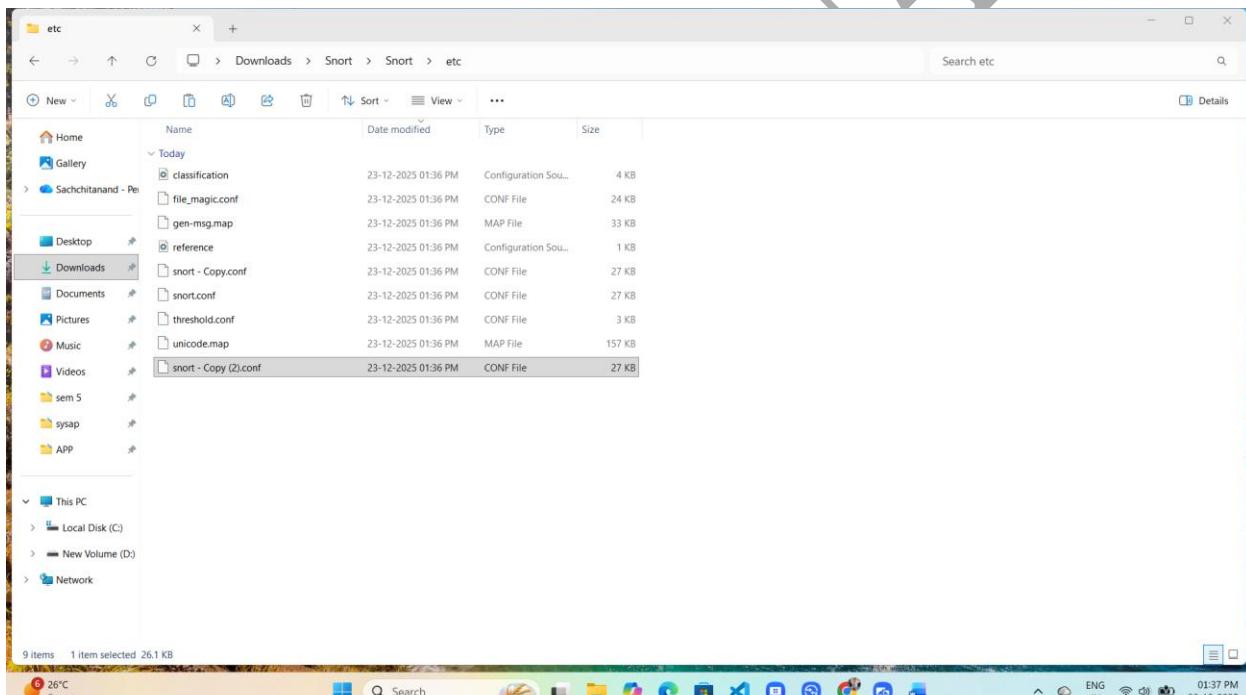
Snort Configuration

Download Link

<https://www.snort.org/downloads>

How to use it :-

- After installation snort, go to the snort location and open etc folder
- Copy snort file and paste it
- Now , open copied file in Notepad++



MODULE – 12 EVADING IDS, FIREWALLS, AND HONEYPOTS



C:\Users\Sachchitanand Yadav\Downloads\Snort\Snort\etc\snort - Copy (2).conf - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

change.log snort - Copy (2).conf

```
1 #-----  
2 # VRT Rule Packages Snort.conf  
3 #  
4 # For more information visit us at:  
5 # http://www.snort.org Snort Website  
6 # http://vti-blog.snort.org/ Sourcefire VRT Blog  
7 #  
8 # Mailing list Contact: snort-users@lists.snort.org  
9 # False Positive reports: fp@sourcefire.com  
10 # Snort bugs: bugs@snort.org  
11 #  
12 # Compatible with Snort Versions:  
13 # VERSIONS : 2.9.20  
14 #  
15 # Snort build options:  
16 # OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm --enable-perfprofiling --enable-zlib --enable-active-response --enable-normalizer --enable-reload --ena  
17 #  
18 # Additional information:  
19 # This configuration file enables active response, to run snort in  
20 # test mode -> you are required to supply an interface -i <interface>  
21 # or test mode will fail to fully validate the configuration and  
22 # exit with a FATAL error  
23 #-----  
24 #####  
25 # This file contains a sample snort configuration.  
26 # You should take the following steps to create your own custom configuration:  
27 #  
28 # 1) Set the network variables.  
29 # 2) Configure the decoder  
30 # 3) Configure the base detection engine  
31 # 4) Configure the needed libraries  
32 # 5) Configure preprocessors  
33 # 6) Configure output plugins  
34 # 7) Customize your rule set  
35 # 8) Customize preprocessor and decoder rule set  
36 # 9) Customize shared object rule set  
37 #####  
38 #####  
39 #####  
40 #####  
41 # Step #1: Set the network variables. For more information, see README.variables  
42 #####  
43
```

Properties file length: 26,798 lines: 690 Lx: 1 Col: 1 Pos: 1 Unix (LF) UTF-8 INS

26°C Sunny 01:37 PM 23-12-2025

- Go to the line number 45

And replace Any word to the ip range

- Go to the line number 48

Replace Any to the !\$HOME_NET



C:\Users\Sachchitanand Yadav\Downloads\Snort\Snort\etc\snort - Copy (2).conf - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

change.log snort - Copy (2).conf snort - Copy (3).conf

```
43 # Setup the network addresses you are protecting  
44 ipvar HOME_NET 192.168.1.0/24  
45 # Set up the external network addresses. Leave as "any" in most situations  
46 ipvar EXTERNAL_NET !$HOME_NET  
47 # List of DNS servers on your network  
48 ipvar DNS_SERVERS $HOME_NET  
49 # List of SMTP servers on your network  
50 ipvar SMTP_SERVERS $HOME_NET  
51 # List of web servers on your network  
52 ipvar HTTP_SERVERS $HOME_NET  
53 # List of sql servers on your network  
54 ipvar SQL_SERVERS $HOME_NET  
55 # List of telnet servers on your network  
56 ipvar TELNET_SERVERS $HOME_NET  
57 # List of ssh servers on your network  
58 ipvar SSH_SERVERS $HOME_NET  
59 # List of ftp servers on your network  
60 ipvar FTP_SERVERS $HOME_NET  
61 # List of sip servers on your network  
62 ipvar SIP_SERVERS $HOME_NET  
63 # List of ports you run web servers on  
64 portvar HTTP_PORTS {80,81,311,383,591,593,901,1220,1414,1741,1830,2301,2381,2809,3037,3128,3702,4343,4848,5250,6988,7000,7001,7144,7145,7510,7777,7779,8000,8008,8014,8028,8080,8085.  
65 # List of ports you want to look for SHELLCODE on.  
66 portvar SHELLCODE_PORTS {80  
67 # List of ports you might see oracle attacks on  
68 portvar ORACLE_PORTS 1024:  
69 # List of ports you want to look for SSH connections on:  
70 portvar SSH_PORTS 22  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
999  
1000  
1001  
1002  
1003  
1004  
1005  
1006  
1007  
1008  
1009  
1009  
1010  
1011  
1012  
1013  
1014  
1015  
1016  
1017  
1018  
1019  
1019  
1020  
1021  
1022  
1023  
1024  
1025  
1026  
1027  
1028  
1029  
1029  
1030  
1031  
1032  
1033  
1034  
1035  
1036  
1037  
1038  
1039  
1039  
1040  
1041  
1042  
1043  
1044  
1045  
1046  
1047  
1048  
1049  
1049  
1050  
1051  
1052  
1053  
1054  
1055  
1056  
1057  
1058  
1059  
1059  
1060  
1061  
1062  
1063  
1064  
1065  
1066  
1067  
1068  
1069  
1069  
1070  
1071  
1072  
1073  
1074  
1075  
1076  
1077  
1078  
1079  
1079  
1080  
1081  
1082  
1083  
1084  
1085  
1086  
1087  
1088  
1089  
1089  
1090  
1091  
1092  
1093  
1094  
1095  
1096  
1097  
1098  
1099  
1099  
1100  
1101  
1102  
1103  
1104  
1105  
1106  
1107  
1108  
1109  
1109  
1110  
1111  
1112  
1113  
1114  
1115  
1116  
1117  
1118  
1119  
1119  
1120  
1121  
1122  
1123  
1124  
1125  
1126  
1127  
1128  
1129  
1129  
1130  
1131  
1132  
1133  
1134  
1135  
1136  
1137  
1138  
1139  
1139  
1140  
1141  
1142  
1143  
1144  
1145  
1146  
1147  
1148  
1149  
1149  
1150  
1151  
1152  
1153  
1154  
1155  
1156  
1157  
1158  
1159  
1159  
1160  
1161  
1162  
1163  
1164  
1165  
1166  
1167  
1168  
1169  
1169  
1170  
1171  
1172  
1173  
1174  
1175  
1176  
1177  
1178  
1179  
1179  
1180  
1181  
1182  
1183  
1184  
1185  
1186  
1187  
1188  
1189  
1189  
1190  
1191  
1192  
1193  
1194  
1195  
1196  
1197  
1198  
1199  
1199  
1200  
1201  
1202  
1203  
1204  
1205  
1206  
1207  
1208  
1209  
1209  
1210  
1211  
1212  
1213  
1214  
1215  
1216  
1217  
1218  
1219  
1219  
1220  
1221  
1222  
1223  
1224  
1225  
1226  
1227  
1228  
1229  
1229  
1230  
1231  
1232  
1233  
1234  
1235  
1236  
1237  
1238  
1239  
1239  
1240  
1241  
1242  
1243  
1244  
1245  
1246  
1247  
1248  
1249  
1249  
1250  
1251  
1252  
1253  
1254  
1255  
1256  
1257  
1258  
1259  
1259  
1260  
1261  
1262  
1263  
1264  
1265  
1266  
1267  
1268  
1269  
1269  
1270  
1271  
1272  
1273  
1274  
1275  
1276  
1277  
1278  
1279  
1279  
1280  
1281  
1282  
1283  
1284  
1285  
1286  
1287  
1288  
1289  
1289  
1290  
1291  
1292  
1293  
1294  
1295  
1296  
1297  
1298  
1299  
1299  
1300  
1301  
1302  
1303  
1304  
1305  
1306  
1307  
1308  
1309  
1309  
1310  
1311  
1312  
1313  
1314  
1315  
1316  
1317  
1318  
1319  
1319  
1320  
1321  
1322  
1323  
1324  
1325  
1326  
1327  
1328  
1329  
1329  
1330  
1331  
1332  
1333  
1334  
1335  
1336  
1337  
1338  
1339  
1339  
1340  
1341  
1342  
1343  
1344  
1345  
1346  
1347  
1348  
1349  
1349  
1350  
1351  
1352  
1353  
1354  
1355  
1356  
1357  
1358  
1359  
1359  
1360  
1361  
1362  
1363  
1364  
1365  
1366  
1367  
1368  
1369  
1369  
1370  
1371  
1372  
1373  
1374  
1375  
1376  
1377  
1378  
1379  
1379  
1380  
1381  
1382  
1383  
1384  
1385  
1386  
1387  
1388  
1389  
1389  
1390  
1391  
1392  
1393  
1394  
1395  
1396  
1397  
1398  
1399  
1399  
1400  
1401  
1402  
1403  
1404  
1405  
1406  
1407  
1408  
1409  
1409  
1410  
1411  
1412  
1413  
1414  
1415  
1416  
1417  
1418  
1419  
1419  
1420  
1421  
1422  
1423  
1424  
1425  
1426  
1427  
1428  
1429  
1429  
1430  
1431  
1432  
1433  
1434  
1435  
1436  
1437  
1438  
1439  
1439  
1440  
1441  
1442  
1443  
1444  
1445  
1446  
1447  
1448  
1449  
1449  
1450  
1451  
1452  
1453  
1454  
1455  
1456  
1457  
1458  
1459  
1459  
1460  
1461  
1462  
1463  
1464  
1465  
1466  
1467  
1468  
1469  
1469  
1470  
1471  
1472  
1473  
1474  
1475  
1476  
1477  
1478  
1479  
1479  
1480  
1481  
1482  
1483  
1484  
1485  
1486  
1487  
1488  
1489  
1489  
1490  
1491  
1492  
1493  
1494  
1495  
1496  
1497  
1498  
1499  
1499  
1500  
1501  
1502  
1503  
1504  
1505  
1506  
1507  
1508  
1509  
1509  
1510  
1511  
1512  
1513  
1514  
1515  
1516  
1517  
1518  
1519  
1519  
1520  
1521  
1522  
1523  
1524  
1525  
1526  
1527  
1528  
1529  
1529  
1530  
1531  
1532  
1533  
1534  
1535  
1536  
1537  
1538  
1539  
1539  
1540  
1541  
1542  
1543  
1544  
1545  
1546  
1547  
1548  
1549  
1549  
1550  
1551  
1552  
1553  
1554  
1555  
1556  
1557  
1558  
1559  
1559  
1560  
1561  
1562  
1563  
1564  
1565  
1566  
1567  
1568  
1569  
1569  
1570  
1571  
1572  
1573  
1574  
1575  
1576  
1577  
1578  
1579  
1579  
1580  
1581  
1582  
1583  
1584  
1585  
1586  
1587  
1588  
1589  
1589  
1590  
1591  
1592  
1593  
1594  
1595  
1596  
1597  
1598  
1599  
1599  
1600  
1601  
1602  
1603  
1604  
1605  
1606  
1607  
1608  
1609  
1609  
1610  
1611  
1612  
1613  
1614  
1615  
1616  
1617  
1618  
1619  
1619  
1620  
1621  
1622  
1623  
1624  
1625  
1626  
1627  
1628  
1629  
1629  
1630  
1631  
1632  
1633  
1634  
1635  
1636  
1637  
1638  
1639  
1639  
1640  
1641  
1642  
1643  
1644  
1645  
1646  
1647  
1648  
1649  
1649  
1650  
1651  
1652  
1653  
1654  
1655  
1656  
1657  
1658  
1659  
1659  
1660  
1661  
1662  
1663  
1664  
1665  
1666  
1667  
1668  
1669  
1669  
1670  
1671  
1672  
1673  
1674  
1675  
1676  
1677  
1678  
1679  
1679  
1680  
1681  
1682  
1683  
1684  
1685  
1686  
1687  
1688  
1689  
1689  
1690  
1691  
1692  
1693  
1694  
1695  
1696  
1697  
1698  
1699  
1699  
1700  
1701  
1702  
1703  
1704  
1705  
1706  
1707  
1708  
1709  
1709  
1710  
1711  
1712  
1713  
1714  
1715  
1716  
1717  
1718  
1719  
1719  
1720  
1721  
1722  
1723  
1724  
1725  
1726  
1727  
1728  
1729  
1729  
1730  
1731  
1732  
1733  
1734  
1735  
1736  
1737  
1738  
1739  
1739  
1740  
1741  
1742  
1743  
1744  
1745  
1746  
1747  
1748  
1749  
1749  
1750  
1751  
1752  
1753  
1754  
1755  
1756  
1757  
1758  
1759  
1759  
1760
```

MODULE – 12 EVADING IDS, FIREWALLS, AND HONEYPOTS

- Go to the line number 104
 - Set rules folder location

C:\\Snort\\rules

- Go to the line number 106 and set preproc_rules

C:\Snort\preproc_rules

- go to the line number 113 and 114
 - and add rules file path/location

*C:\Users\Sachchitanand Yadav\Downloads\Snort\Snort\etc\snort - Copy (2).conf - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

change.log snort - Copy (2).conf snort - Copy (3).conf

```
94
95 # List of GTP ports for GTP preprocessor
96 portvar GTP_PORTS [2123,2152,3386]
97
98 # other variables, these should not be modified
99 ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9.0/24,205.188.153.0/24,205.188.179
100
101 # Path to your rules files (this can be a relative path)
102 # Note for Windows users: You are advised to make this an absolute path,
103 # such as: c:\snort\rules
104 var RULE_PATH C:\Snort\rules
105 var SO_RULE_PATH .../so_rules
106 var PREPROC_RULE_PATH C:\Snort\preproc_rules
107
108 # If you are using reputation preprocessor set these
109 # Currently there is a bug with relative paths, they are relative to where snort is
110 # not relative to snort.conf like the above variables
111 # This is completely inconsistent with how other vars work, BUG 89986
112 # Set the absolute path appropriately
113 var WHITELIST_PATH C:\Snort\rules
114 var BLACKLIST_PATH C:\Snort\rules
115
116 ##### Step #1: Configure the snort decoder
117 # Step #2: Configure the decoder. For more information, see README.decode
118 #####
119
120 # Stop generic decode events:
121 config disable_decode_alerts
122
123 # Stop Alerts on experimental TCP options
124 config disable_tcpopt_experimental_alerts
125
126 # Stop Alerts on obsolete TCP options
127 config disable_tcpopt_obsolete_alerts
128
129 # Stop Alerts on T/TCP alerts
130 config disable_tcpopt_ttcp_alerts
131
132 # Stop Alerts on all other TCPOption type events:
133 config disable_tcpopt_alerts
134
135 # Stop Alerts on invalid ip options
136 config disable_inetd_alerts
```

- Step 2
 - go to the line number 186
 - remove hash
 - Step 3
 - Don't do anything , no need to change

MODULE – 12 EVADING IDS, FIREWALLS, AND HONEYPOTS

```
#C:\Users\Sachchitanand.Yadav\Downloads\Snort\Snort\etc\snort - Copy (2).conf - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log snort - Copy (2).conf > snort - Copy (3).conf

172 # config set_uid:
173
174 # Configure default snaplen. Snort defaults to MTU of in use interface. For more information see README
175 #
176 #config snaplen:
177 #
178
179 # Configure default bpf_file to use for filtering what traffic reaches snort. For more information see snort -h command line options (-F)
180 #
181 #config bpf_file:
182 #
183
184 # Configure default log directory for snort to log to. For more information see snort -h command line options (-l)
185 #
186 config logdir:C:\Snort\log
187
188
189 #####
190 # Step #3: Configure the base detection engine. For more information, see README.decode
191 #####
192
193 # Configure PCRE match limitations
194 config pore_match_limit: 3500
195 config pore_match_limit_recursion: 1500
196
197 # Configure the detection engine See the Snort Manual, Configuring Snort - Includes - Config
198 config detection: search-method ac-split search-optimize max-pattern-len 20
199
200 # Configure the event queue. For more information, see README.event_queue
201 config event_queue: max_queue 8 log 5 order_events content_length
202
203 #####
204 ## Configure GTP if it is to be used.
205 ## For more information, see README.GTP
206 #####
207
208 # config enable_gtp
209
210 #####
211 # Per packet and rule latency enforcement
212 # For more information see README.ppm
213 #####
214

Properties file
length: 26,839  lines: 690  Lx: 661  Col: 1  Pos: 25,734  Unix (LF)  UTF-8  INS
26°C Sunny
Search 23-12-2025 02:12 PM
```

• Step 4

- Go to the line number 247

Set snort_dynamicpreprocessor file path/location :-
c:\Snort\lib\snort_preprocessor

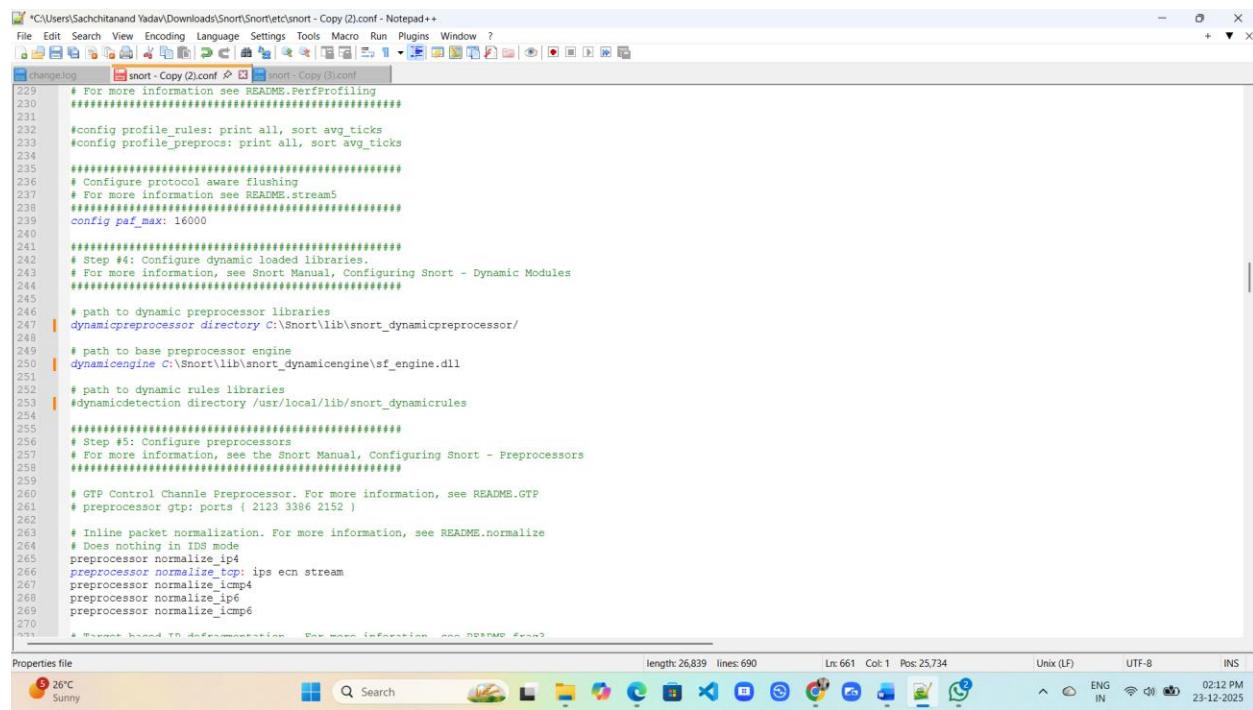
- Go to the line number number 250

Set sf_engine.dll file location :-
c:\Snort\lib\snort_dynamicengine/sf_engine.dll

- Go to the line number 253

Add # on front of the line number 253

MODULE – 12 EVADING IDS, FIREWALLS, AND HONEYPOTS



The screenshot shows a Notepad++ window with two tabs open: "snort - Copy (2).conf" and "snort - Copy (3).conf". The code in both tabs is identical, representing Snort configuration rules. The code includes sections for performance profiling, dynamic modules, dynamic preprocessors, and preprocessors like GTP and normalization. The Notepad++ interface shows line numbers from 229 to 270, and the status bar indicates the file has 26,839 length, 690 lines, and is in UTF-8 encoding.

```
229 # For more information see README.Perfprofiling
230 ######
231
232 #config profile_rules: print all, sort avg_ticks
233 #config profile_procs: print all, sort avg_ticks
234
235 ######
236 # Configure protocol aware flushing
237 # For more information see README.stream5
238 ######
239 config paf_max: 16000
240
241 ######
242 # Step #4: Configure dynamic loaded libraries.
243 # For more information, see Snort Manual, Configuring Snort - Dynamic Modules
244 ######
245
246 # path to dynamic preprocessor libraries
247 dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor/
248
249 # path to base preprocessor engine
250 dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
251
252 # path to dynamic rules libraries
253 #dynamicrule directory /usr/local/lib/snort_dynamicrules
254
255 ######
256 # Step #5: Configure preprocessors
257 # For more information, see the Snort Manual, Configuring Snort - Preprocessors
258 ######
259
260 # GTP Control Channel Preprocessor. For more information, see README.GTP
261 # preprocessor gtp: ports { 2123 3386 2152 }
262
263 # Inline packet normalization. For more information, see README.normalize
264 # Does nothing in IDS mode
265 preprocessor normalize_ip4
266 preprocessor normalize_tcp: ips ecn stream
267 preprocessor normalize_icmp4
268 preprocessor normalize_ip6
269 preprocessor normalize_icmp6
270
```

• Step 5

- Go to the line number 511 and 512

Note:- before changing on the line number 511 and 512 , firstly go to the snort >>rules folder and there is file in folder i.e blacklist.rules copy file and paste in same folder and rename copy file to the whitelist.rules

Replace white_list.rules to whitelist.rules on 511

Replace black_list.rules to blacklist.rules on 512

• Step 6

- Don't do anything , no need to change

MODULE – 12 EVADING IDS, FIREWALLS, AND HONEYPOTS

*C:\Users\Sachchitanand Yadav\Downloads\Snort\Snort\etc\snort - Copy (2).conf - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

change.log snort - Copy (2).conf snort - Copy (3).conf

```
499 # preprocessor modbus: ports { 502 }
500
501     # BNP3 preprocessor. For more information see README.dnp3
502     preprocessor dnp3: ports { 20000 } \
503         memcap 262144 \
504         check_crc
505
506     # Reputation preprocessor. For more information see README.reputation
507     preprocessor reputation: \
508         memcap 500, \
509         priority whitelist, \
510         nested_in_inner, \
511         whitelist $WHITE_LIST_PATH/whitelist.rules, \
512         blacklist $BLACK_LIST_PATH/blacklist.rules
513
514 ##### Step #6: Configuration output plugins #####
515 # Step #6: Configuration output plugins
516 # For more information, see Snort Manual, Configuring Snort - Output Modules
517 #####
518
519 # unified2
520 # Recommended for most installs
521 # output unified2: filename merged.log, limit 128, nostamp, mpls_event_types, vlan_event_types
522
523 # Additional configuration for specific types of installs
524 # output alert_unified2: filename snort.alert, limit 128, nostamp
525 # output log_unified2: filename snort.log, limit 128, nostamp
526
527 # syslog
528 # output alert_syslog: LOG_AUTH LOG_ALERT
529
530 # pcap
531 # output log_tcpdump: tcpdump.log
532
533 # metadata reference data. do not modify these lines
534 include classification.config
535 include reference.config
536
537 #####
538 # Step #7: Customize your rule set
539 # For more information, see Snort Manual, Writing Snort Rules
540 #####
541
```

- step 7

- go to the line number 546
 - replace “/” to “\” 546 upto 651

MODULE – 12 EVADING IDS, FIREWALLS, AND HONEYPOTS



*C:\Users\Sachchitanand.Yadav\Downloads\Snort\Snort\etc\snort - Copy (2).conf - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

change-log snort - Copy (2).conf snort - Copy (3).conf

```
583 include $RULE_PATH\indicator-shellcode.rules
584 include $RULE_PATH\info.rules
585 include $RULE_PATH\malware-backdoor.rules
586 include $RULE_PATH\malware-cnc.rules
587 include $RULE_PATH\malware-other.rules
588 include $RULE_PATH\malware-trojan.rules
589 include $RULE_PATH\misc.rules
590 include $RULE_PATH\multimedia.rules
591 include $RULE_PATH\mysql.rules
592 include $RULE_PATH\netbios.rules
593 include $RULE_PATH\nntp.rules
594 include $RULE_PATH\oracle.rules
595 include $RULE_PATH\os-linux.rules
596 include $RULE_PATH\os-other.rules
597 include $RULE_PATH\os-solaris.rules
598 include $RULE_PATH\os-windows.rules
599 include $RULE_PATH\os-windows-2k.rules
600 include $RULE_PATH\p2p.rules
601 include $RULE_PATH\phishing-spam.rules
602 include $RULE_PATH\policy-multimedia.rules
603 include $RULE_PATH\policy-other.rules
604 include $RULE_PATH\policy.rules
605 include $RULE_PATH\policy-social.rules
606 include $RULE_PATH\policy-spam.rules
607 include $RULE_PATH\pop2.rules
608 include $RULE_PATH\pop3.rules
609 include $RULE_PATH\protocol-finger.rules
610 include $RULE_PATH\protocol-ftp.rules
611 include $RULE_PATH\protocol-icmp.rules
612 include $RULE_PATH\protocol-imap.rules
613 include $RULE_PATH\protocol-pop.rules
614 include $RULE_PATH\protocol-voip.rules
615 include $RULE_PATH\pua-adware.rules
616 include $RULE_PATH\pua-other.rules
617 include $RULE_PATH\pua-p2p.rules
618 include $RULE_PATH\pua-toolbars.rules
619 include $RULE_PATH\rpc.rules
620 include $RULE_PATH\services.rules
621 include $RULE_PATH\scada.rules
622 include $RULE_PATH\scan.rules
623 include $RULE_PATH\server-apache.rules
624 include $RULE_PATH\server-iis.rules
625 include $RULE_PATH\server-mail.rules
626 include $RULE_PATH\server-mssql.rules
627 include $RULE_PATH\server-mysql.rules
628 include $RULE_PATH\server-oracle.rules
629 include $RULE_PATH\server-other.rules
630 include $RULE_PATH\server-webapp.rules
631 include $RULE_PATH\server-x11.rules
632 include $RULE_PATH\smmp.rules
633 include $RULE_PATH\snmp.rules
634 include $RULE_PATH\specific-threats.rules
635 include $RULE_PATH\spyware-put.rules
636 include $RULE_PATH\sql.rules
637 include $RULE_PATH\telnet.rules
638 include $RULE_PATH\tftp.rules
639 include $RULE_PATH\virus.rules
640 include $RULE_PATH\voip.rules
641 include $RULE_PATH\web-active.rules
642 include $RULE_PATH\web-attacks.rules
643 include $RULE_PATH\web-client.rules
644 include $RULE_PATH\web-coldfusion.rules
645 include $RULE_PATH\web-frontpage.rules
646 include $RULE_PATH\web-iis.rules
647 include $RULE_PATH\web-misc.rules
648 include $RULE_PATH\web-php.rules
649 include $RULE_PATH\x11.rules
650
651 #####
652 # Step #8: Customize your preprocessor and decoder alerts
653 # For more information, see README.decoder_preproc_rules
654 #####
655
656 #####
657 # decoder and preprocessor event rules
658 include $PREPROC_RULE_PATH\preprocessor.rules
659 include $PREPROC_RULE_PATH\decoder.rules
660 include $PREPROC_RULE_PATH\sensitive-data.rules
661
662 #####
663 #####
664 # Clean up. Don't leave any Shared Objects, Shared Rules
```

Properties file

length: 26,839 lines: 690 Lx: 661 Col: 1 Pos: 25,734 Unix (LF) UTF-8 INS

26°C Sunny 02:13 PM 23-12-2025

• step 8

- go to the line number 659

remove hash line number 659 to 661

- replace “/” to “\” 659 upto 661



*C:\Users\Sachchitanand.Yadav\Downloads\Snort\Snort\etc\snort - Copy (2).conf - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

change-log snort - Copy (2).conf snort - Copy (3).conf

```
622 include $RULE_PATH\scada.rules
623 include $RULE_PATH\scan.rules
624 include $RULE_PATH\server-apache.rules
625 include $RULE_PATH\server-iis.rules
626 include $RULE_PATH\server-mail.rules
627 include $RULE_PATH\server-mssql.rules
628 include $RULE_PATH\server-mysql.rules
629 include $RULE_PATH\server-oracle.rules
630 include $RULE_PATH\server-other.rules
631 include $RULE_PATH\server-webapp.rules
632 include $RULE_PATH\smmp.rules
633 include $RULE_PATH\snmp.rules
634 include $RULE_PATH\specific-threats.rules
635 include $RULE_PATH\spyware-put.rules
636 include $RULE_PATH\sql.rules
637 include $RULE_PATH\telnet.rules
638 include $RULE_PATH\tftp.rules
639 include $RULE_PATH\virus.rules
640 include $RULE_PATH\voip.rules
641 include $RULE_PATH\web-active.rules
642 include $RULE_PATH\web-attacks.rules
643 include $RULE_PATH\web-client.rules
644 include $RULE_PATH\web-coldfusion.rules
645 include $RULE_PATH\web-frontpage.rules
646 include $RULE_PATH\web-iis.rules
647 include $RULE_PATH\web-misc.rules
648 include $RULE_PATH\web-php.rules
649 include $RULE_PATH\x11.rules
650
651 #####
652 # Step #8: Customize your preprocessor and decoder alerts
653 # For more information, see README.decoder_preproc_rules
654 #####
655
656 #####
657 # decoder and preprocessor event rules
658 include $PREPROC_RULE_PATH\preprocessor.rules
659 include $PREPROC_RULE_PATH\decoder.rules
660 include $PREPROC_RULE_PATH\sensitive-data.rules
661
662 #####
663 #####
664 # Clean up. Don't leave any Shared Objects, Shared Rules
```

Properties file

length: 26,839 lines: 690 Lx: 661 Col: 1 Pos: 25,734 Unix (LF) UTF-8 INS

26°C Sunny 02:13 PM 23-12-2025

• Configuration done

MODULE – 12 EVADING IDS, FIREWALLS, AND HONEYPOTS

Now open command line interface as a administrator

- Go to the Snort\bin Folder



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.26200.7462]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd ..

C:\Windows>cd\Snort

C:\Snort>cd\Snort

C:\Snort>cd bin

C:\Snort\bin>snort.exe -v
C:\Snort\bin>snort.exe -V
C:\Snort\bin>
```

- There is file in snort bin folder >> snort.exe
- Run file snort.exe -v (v for version)



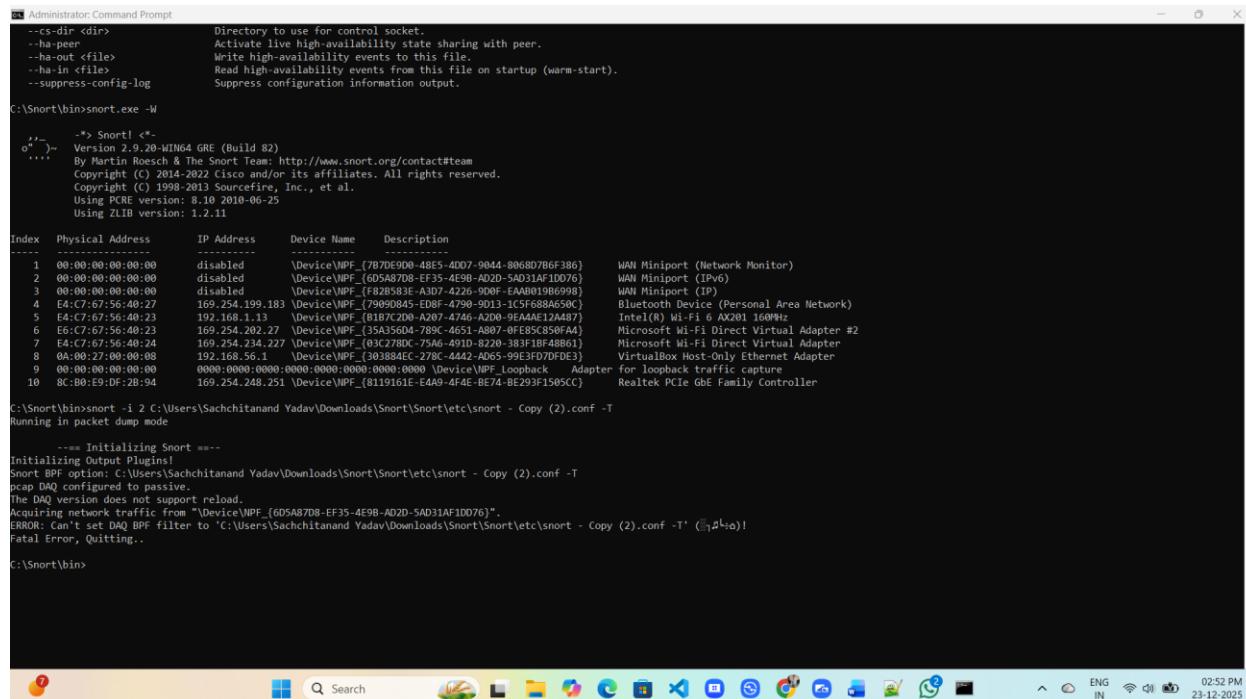
```
Select Administrator: Command Prompt
55 G 2:      0 ( 0.000%
Total:      0
=====
Memory Statistics for File at:Tue Dec 23 14:48:28 2025
Total buffers allocated:      0
Total buffers freed:         0
Total buffers released:       0
Total file mempool:          0
Total allocated file mempool: 0
Total freed file mempool:     0
Total released file mempool:  0
=====
Heap Statistics of file:
Total Statistics:
  Memory in use:      0 bytes
  No of allocs:       0
  No of frees:        0
=====
Snort exiting
=====
C:\Snort\bin>snort.exe -V

'--> Snort! <-
o" '--> Version 2.9.20-WIN64 GRE (Build 82)
... By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 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: 1.2.11

C:\Snort\bin>
C:\Snort\bin>
C:\Snort\bin>
C:\Snort\bin>
C:\Snort\bin>
C:\Snort\bin>
C:\Snort\bin>
C:\Snort\bin>snort.exe -w
snort.exe: option requires an argument -- w
'--> Snort! <-
o" '--> Version 2.9.20-WIN64 GRE (Build 82)
... By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
```

MODULE – 12 EVADING IDS, FIREWALLS, AND HONEYPOTS

- use next command for finding network interface
- snort.exe -W



```
Administrator: Command Prompt
--es-dir <dir>          Directory to use for control socket.
--ha-peer                 Activate live high-availability state sharing with peer.
--ha-out <file>           Write high-availability events to this file.
--ha-in <file>            Read high-availability events from this file on startup (warm-start).
--suppress-config-log     Suppress configuration information output.

C:\Snort\bin>snort.exe -W
'--> Snort| <--'
`--> Version 2.9.20-WIN64 GRE (Build 82)
    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
    Copyright (C) 2014-2022 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: 1.2.11

Index Physical Address      IP Address       Device Name        Description
---- -----------
1   00:00:00:00:00:00      disabled         \Device\NPF_{7D97C090-ABE5-4D07-0A44-8068D796F306}  WAM Miniport (Network Monitor)
2   00:00:00:00:00:00      disabled         \Device\NPF_{605A87D8-EF35-AE9B-AD2D-5A021AF1D076}  WAM Miniport (IPv6)
3   00:00:00:00:00:00      disabled         \Device\NPF_{F82B583E-A307-4226-9006-EAA0B19B6998}  WAM Miniport (IP)
4   E4:C7:67:56:40:27      169.254.199.183 \Device\NPF_{799090845-E08F-4790-9013-1CF5F688A650C}  Bluetooth Device (Personal Area Network)
5   E4:C7:67:56:40:23      192.168.1.13   \Device\NPF_{8187C2D4-A207-4746-A200-9EAAA1E2A87}  Intel(R) Wi-Fi 6 AX201 160MHz
6   E6:C7:67:56:40:23      169.254.202.27 \Device\NPF_{35A35604-789C-4651-A807-0FE85C850FA4}  Microsoft Wi-Fi Direct Virtual Adapter #2
7   E4:C7:67:56:40:24      169.254.234.227 \Device\NPF_{03C278D0-75A6-491D-B200-383F1BF48B61}  Microsoft Wi-Fi Direct Virtual Adapter
8   0A:00:27:00:00:08      192.168.56.1   \Device\NPF_{30388AE4-278C-4442-A065-99E3FD7DFDE3}  VirtualBox Host-Only Ethernet Adapter
9   00:00:00:00:00:00      0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback Adapter for loopback traffic capture
10  BC:B0:E9:D8:2B:94      169.254.248.251 \Device\NPF_{8119161-E4A9-4F4E-BE74-BE293F1505CC}  Realtek PCIe GbE Family Controller

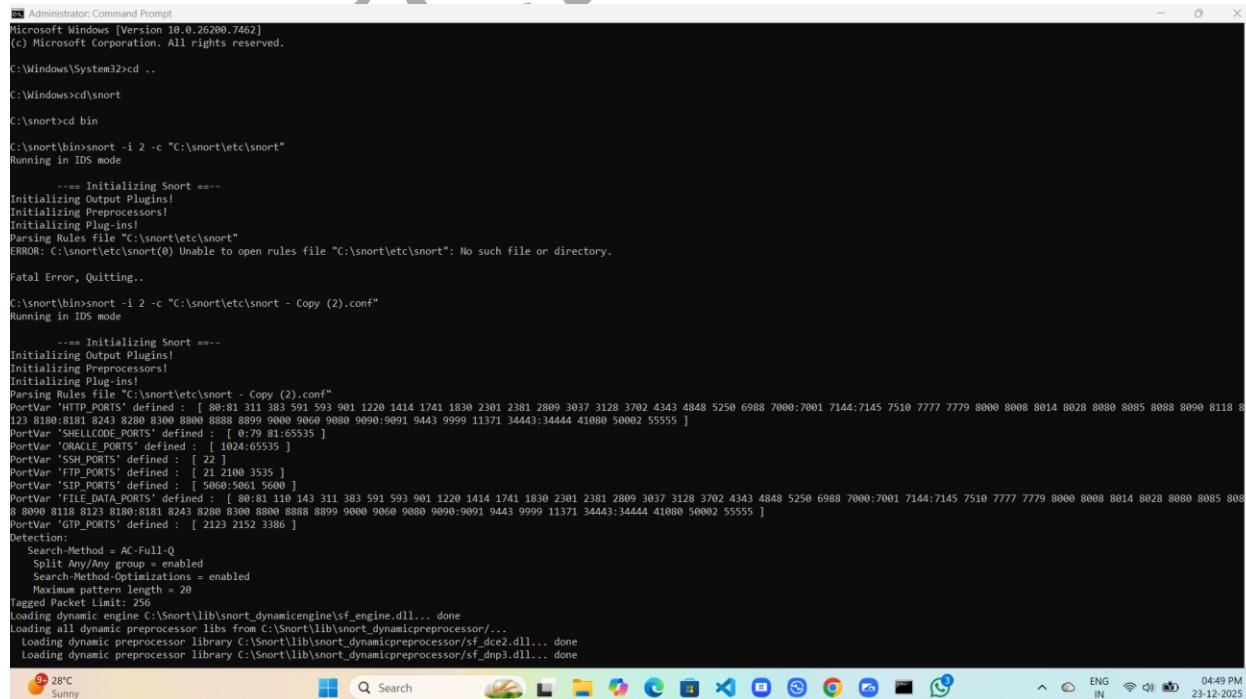
C:\Snort\bin>snort -i 2 C:\Users\Sachchitanand Yadav\Downloads\Snort\Snort\etc\snort - Copy (2).conf -T
Running in packet dump mode

    === Initializing Snort ===
Initializing Output Plugins!
Snort BPF option: C:\Users\Sachchitanand Yadav\Downloads\Snort\Snort\etc\snort - Copy (2).conf -T
ncap DAO configured to passive.
The DAO version does not support reload.
Acquiring network traffic from "\Device\NPF_{605A87D8-EF35-AE9B-AD2D-5A021AF1D076}".
ERROR: Can't set DAO BPF filter to 'C:\Users\Sachchitanand Yadav\Downloads\Snort\Snort\etc\snort - Copy (2).conf -T' (gammaic)
Fatal Error, Quitting..

C:\Snort\bin>
```

- use command for configuration testing

command :-: snort.exe -i 2 -c "c:\snort\etc\file name "



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.26200.7462]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd ..
C:\Windows>cd snort
C:\snort>cd bin
C:\snort\bin>snort -i 2 -c "C:\snort\etc\snort"
Running in IDS mode

    === Initializing Snort ===
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "C:\snort\etc\snort"
ERROR: C:\snort\etc\snort(0) Unable to open rules file "C:\snort\etc\snort": No such file or directory.
Fatal Error, Quitting..

C:\snort\bin>snort -i 2 -c "C:\snort\etc\snort - Copy (2).conf"
Running in IDS mode

    === Initializing Snort ===
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "C:\snort\etc\snort - Copy (2).conf"
PortVar 'HTTP_PORTS' defined : [ 80:81 311 381 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined : [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined : [ 1024:65535 ]
PortVar 'SSH_PORTS' defined : [ 22 ]
PortVar 'FTP_PORTS' defined : [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined : [ 5060:5061 5060 ]
PortVar 'DATA_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined : [ 2123 2152 3386 ]
PortVar 'Detection':
    Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine C:\Snort\lib\snort_dynamicengine\sf_engine.dll... done
Loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor...
    Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_de2.dll... done
    Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dmp3.dll... done
28°C
Sunny
04:49 PM
23-12-2025
```

MODULE – 12 EVADING IDS, FIREWALLS, AND HONEYPOTS

```
Administrator: Command Prompt
WARNING: ip6 normalizations disabled because not inline.
WARNING: icmp6 normalizations disabled because not inline.
Frag3 global config:
    Max frags: 65536
    Fragment memory cap: 4194304 bytes
Fragment cache config:
    Bound Address: default
    Target-based policy: WINDOWS
    Fragment timeout: 180 seconds
    Fragment min_ttl: 1
    Fragment Anomalies: Alert
    Overlap Limit: 10
    Min fragment Length: 100
    Max Expected Streams: 768
Stream global config:
    Track TCP sessions: ACTIVE
    Max TCP sessions: 262144
    TCP cache pruning timeout: 30 seconds
    TCP cache nominal timeout: 3600 seconds
    Memory (for reassembly packet storage): 8388608
    Track UDP sessions: ACTIVE
    Max UDP sessions: 131072
    UDP cache pruning timeout: 30 seconds
    UDP cache nominal timeout: 180 seconds
    Track ICMP sessions: INACTIVE
    Track IP sessions: INACTIVE
    Log info if session memory consumption exceeds 1048576
    Send up to 2 active responses
    Wait at least 5 seconds between responses
    Protocol Aware Flushing: ACTIVE
    Maximum Flush Point: 16000
Stream TCP config:
    Bound Address: default
    Reassembly Policy: WINDOWS
    Timeout: 180 seconds
    Limit on TCP Overlaps: 10
    Maximum number of bytes to queue per session: 1048576
    Maximum number of segs to queue per session: 2621
    Options:
        Require 3-Way Handshake: YES
        3-way Handshake Timeout: 180
        Detect Anomalies: YES
    Reassembly Ports:
        21 client (Footprint)
        22 client (Footprint)
        23 client (Footprint)
        25 client (Footprint)
        42 client (Footprint)
        53 client (Footprint)
28°C
Sunny
04:51 PM
23-12-2025
```

```
Select Administrator: Command Prompt
10644 detection rules
193 decoder rules
291 preprocessor rules
11088 Option Chains linked into 331 Chain Headers
*****-----[Rule Port Counts]-----*****
src      tcp   udp   icmp  ip
3831    23    0     0     0
dst      6442   77    0     0
any     712    4     3     0
nc      452    0     0     0
sd      4     2     0     0

-----[detection-filter-config]-----
memory-cap : 1048576 bytes
-----[detection-filter-rules]-----


-----[rate-filter-config]-----
memory-cap : 1048576 bytes
-----[rate-filter-rules]-----
none

-----[event-filter-config]-----
memory-cap : 1048576 bytes
-----[event-filter-global]-----
-----[event-filter-local]-----
none
-----[suppression]-----
none

Rule application order: pass->drop->drop->reject->alert->log
Verifying Preprocessor Configurations!
WARNING: flowbits key 'skype' is set but not ever checked.
WARNING: flowbits key 'file210_Connectionthroughword' is set but not ever checked.
WARNING: flowbits key 'winsnpy.upload.client-to-server' is set but not ever checked.
WARNING: flowbits key 'AccessRemotePC detection' is set but not ever checked.
WARNING: flowbits key 'file.mx4' is set but not ever checked.
WARNING: flowbits key 'smb.trans2.get.dfs.referral' is set but not ever checked.
WARNING: flowbits key 'yg.download' is set but not ever checked.
WARNING: flowbits key 'blackhole.jar' is set but not ever checked.
WARNING: flowbits key 'file.qt' is set but not ever checked.
WARNING: flowbits key 'AccessRemotePC_RPCdetection' is set but not ever checked.
WARNING: flowbits key 'foscam.ua' is set but not ever checked.
WARNING: flowbits key 'file.drm.FAV' is set but not ever checked.
WARNING: flowbits key 'file.pmd' is set but not ever checked.
28°C
Sunny
04:51 PM
23-12-2025
```

MODULE – 12 EVADING IDS, FIREWALLS, AND HONEYPOTS

```
Select Administrator: Command Prompt
WARNING: flowbits key 'RemoteKeyLog.b.Info_detection' is set but not ever checked.
WARNING: flowbits key 'file.dir' is set but not ever checked.
WARNING: flowbits key 'netwire_ping' is set but not ever checked.
WARNING: flowbits key 'ABSystemPy.LogRetrieve' is set but not ever checked.
WARNING: flowbits key 'file.rdp' is set but not ever checked.
WARNING: flowbits key 'file.ftp' is set but not ever checked.
WARNING: flowbits key 'file.r' is set but not ever checked.
WARNING: flowbits key 'file.123' is set but not ever checked.
WARNING: flowbits key 'file.rss' is set but not ever checked.
WARNING: flowbits key 'file.bz2' is set but not ever checked.
WARNING: flowbits key 'file.cab' is set but not ever checked.
WARNING: flowbits key 'want.session' is set but not ever checked.
WARNING: flowbits key 'file.onenote.embedded' is checked but not ever set.
WARNING: flowbits key 'lp.controlfile' is set but not ever checked.
WARNING: flowbits key 'smb.null_session' is set but not ever checked.
WARNING: flowbits key 'Bugs_InitConnection' is set but not ever checked.
WARNING: flowbits key 'cobraloader1.0_detection' is set but not ever checked.
WARNING: flowbits key 'file.fl1' is set but not ever checked.
WARNING: flowbits key 'file.123' is set but not ever checked.
WARNING: flowbits key 'file.apk' is set but not ever checked.
WARNING: flowbits key 'PerfectKeylogger2' is set but not ever checked.
WARNING: flowbits key 'Sohoanywhere_Init' is set but not ever checked.
WARNING: flowbits key 'backdoor_bloodox' is set but not ever checked.
WARNING: flowbits key 'file.ses' is set but not ever checked.
WARNING: flowbits key 'file.screensaver' is set but not ever checked.
WARNING: flowbits key 'file.maki' is set but not ever checked.
WARNING: flowbits key 'file.rat' is set but not ever checked.
WARNING: flowbits key 'file.hpj' is set but not ever checked.
WARNING: flowbits key 'file.wmf' is set but not ever checked.
WARNING: flowbits key 'file.alif' is set but not ever checked.
WARNING: flowbits key 'file.mif' is set but not ever checked.
WARNING: flowbits key 'file.smil' is set but not ever checked.
WARNING: flowbits key 'file.3dm' is set but not ever checked.
WARNING: flowbits key 'safari.dll' is set but not ever checked.
WARNING: flowbits key 'file.usk' is set but not ever checked.
WARNING: flowbits key 'systemsecurity2009' is set but not ever checked.
WARNING: flowbits key 'file.symantec' is set but not ever checked.
WARNING: flowbits key 'file.rpt' is set but not ever checked.
WARNING: flowbits key 'file.plf' is set but not ever checked.
WARNING: flowbits key 'file.works' is set but not ever checked.
WARNING: flowbits key 'file.pac' is set but not ever checked.
WARNING: flowbits key 'file.realplayer' is set but not ever checked.
WARNING: flowbits key 'file.jar.agent_helper' is set but not ever checked.
WARNING: flowbits key 'file.vtx' is set but not ever checked.
WARNING: flowbits key 'file.rtx' is set but not ever checked.
WARNING: flowbits key 'file.cell' is set but not ever checked.
WARNING: flowbits key 'file.torrent' is set but not ever checked.
WARNING: flowbits key 'file.sr3' is set but not ever checked.

04:52 PM
23-12-2025

Gold +3.38%
```

ATA

```
Select Administrator: Command Prompt
IMAP Config
Used Memory : 1379
No of Allocs : 3
No of Frees : 48
Total memory used : 1379

Heap Statistics of imap:
Total Statistics:
Memory in use: 1379 bytes
No of Allocs: 3
No of frees: 48
Config Statistics:
Memory in use: 1379 bytes
No of allocs: 3
No of frees: 48
=====
Memory Statistics for File at:Tue Dec 23 16:49:03 2025
Total buffers allocated: 0
Total buffers freed: 0
Total buffers released: 0
total file mempool: 0
Total allocated file mempool: 0
Total freed file mempool: 0
Total released file mempool: 0

Heap Statistics of file:
Total Statistics:
Memory in use: 288 bytes
No of allocs: 6
No of frees: 1
Session Statistics:
Memory in use: 0 bytes
No of allocs: 1
No of frees: 1
Mempool Statistics:
Memory in use: 288 bytes
No of allocs: 5
No of frees: 0
=====
Snort exiting
C:\snort\bin>snort -i 2 -c "C:\snort\etc\snort - Copy (2).conf" -T
Running in Test mode
==== Initializing Snort ====
Initializing Output Plugins!
Initializing Preprocessors!
```

ATA

```
04:53 PM
23-12-2025

Gold +3.38%
```

MODULE – 12 EVADING IDS, FIREWALLS, AND HONEYPOTS

- use command for configuration testing

command :- snort.exe -i 2 -c "c:\Snort\etc\file name" -T

```
cmd Select Administrator: Command Prompt
=====
Snort exiting
C:\snort\bin>snort -i 2 -c "C:\Snort\etc\snort - Copy (2).conf" -T
Running in Test mode

    === Initializing Snort ===
Initializing Output Plugins
Initializing Preprocessors
Initializing Plugins
Parsing Rules file 'C:\snort\etc\snort - Copy (2).conf'
PortVar 'HTTP_PORTS' defined : [ 80:81 311 383 591 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHLLCODE_PORTS' defined : [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined : [ 1024:65535 ]
PortVar 'SSH_PORTS' defined : [ 22 ]
PortVar 'FTP_PORTS' defined : [ 21 2100 3535 ]
PortVar 'DCCP_PORTS' defined : [ 5060:5061 5060 ]
PortVar 'FILE_DATA_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined : [ 2123 2152 3306 ]
Tagged Packet Limit: 256
Loading dynamic engine C:\Snort\lib\snort_dynamicengine\sf_engine.dll... done
Loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor\...
    Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dce2.dll... done
    Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dnp3.dll... done
    Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dnpnet.dll... done
    Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ftpm.dll... done
    Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ftppn.dll... done
    Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_imap.dll... done
    Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_modbus.dll... done
    Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_pop.dll... done
    Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_reputation.dll... done
    Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_sdf.dll... done
    Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_sip.dll... done
    Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_smtp.dll... done
    Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ssh.dll... done
    Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ssl.dll... done
Finished loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor\
Log directory: C:\Snort\log
WARNING: dns normalization disabled because not inline.
WARNING: tcp normalization disabled because not inline.
WARNING: icmp4 normalization disabled because not inline.
WARNING: ip6 normalization disabled because not inline.
04:54 PM
23-12-2025
```

```
cmd Select Administrator: Command Prompt
=====
MaxRss at the end of dynamic preproc config:1693204208

=====
Initializing rule chains...
11088 Snort rules read
10644 detection rules
153 decoder rules
291 preprocessor rules
11088 Option Chains linked into 331 Chain Headers
=====

-----[Rule Port Counts]-----
src      tcp   udp   icmp   ip
src  3831   23     0     0
dst  6442   77     0     0
any    712    4     3     0
nc    452    0     0     0
s+d     4     2     0     0

-----[detection-filter-config]-----
memory-cap : 1048576 bytes
-----[detection-filter-rules]-----

-----[rate-filter-config]-----
memory-cap : 1048576 bytes
-----[rate-filter-rules]-----
| none

-----[event-filter-config]-----
memory-cap : 1048576 bytes
-----[event-filter-global]-----
-----[event-filter-local]-----
| none
-----[suppression]-----
| none

Rule application order: pass->drop->drop->reject->alert->log
Verifying Preprocessor Configurations!
WARNING: flowbits key 'file.sis' is set but not ever checked.
WARNING: flowbits key 'file.search-ms' is set but not ever checked.
WARNING: flowbits key 'netwir_ping' is set but not ever checked.
WARNING: flowbits key 'smtp.contenttype.attachment' is set but not ever checked.
WARNING: flowbits key 'file.bzip' is set but not ever checked.
WARNING: flowbits key 'file.drm.F4V' is set but not ever checked.
WARNING: flowbits key 'file.4xm' is set but not ever checked.
04:54 PM
23-12-2025
```

MODULE – 12 EVADING IDS, FIREWALLS, AND HONEYPOTS

```
cmd Select Administrator: Command Prompt.
WARNING: flowbits key 'file.gzip' is set but not ever checked.
WARNING: flowbits key 'file.vap' is set but not ever checked.
WARNING: flowbits key 'file.jar.agent_helper' is set but not ever checked.
499 out of 1024 flowbits in use.

MaxRSS at the end of rules:1693204208

[ Port Based Pattern Matching Memory ]
-- [ Aho-Corasick Summary ] -----
| Storage Format : Full-Q
| Finite Automaton : DFA
| Alphabet Size : 256 Chars
| Siz eof State : Variable (1,2,4 bytes)
| Instances : 227
| 1 byte states : 214
| 2 byte states : 11
| 4 byte states : 2
| Characters : 220293
| States : 101676
| Transitions : 3175877
| State Density : 68.3%
| Patterns : 10772
| Match States : 11866
| Memory (MB) : 162.28
| Patterns : 1.26
| Match Lists : 2.85
| DFA
| 1 byte states : 1.25
| 2 byte states : 19.06
| 4 byte states : 137.47

[ Number of patterns truncated to 20 bytes: 651 ]

MaxRSS at the end of detection rules:1693204208
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "DeviceNPF_{6D5A8708-EF35-4E9B-AD2D-5A031A1D0076}".

---- Initialization Complete ----

-> Snort! <-
o--> Snort 2.9.20-WIN64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 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: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>

Gold +3.38% 04:54 PM 23-12-2025
```

```
cmd Select Administrator: Command Prompt.
WARNING: flowbits key 'lizmoon.get_ur' is set but not ever checked.
WARNING: flowbits key 'ibmdb2.acscce' is set but not ever checked.
WARNING: flowbits key 'file.mcl' is set but not ever checked.
WARNING: flowbits key 'file.cur' is set but not ever checked.
WARNING: flowbits key 'file.pecompact' is set but not ever checked.
WARNING: flowbits key 'file.rdp' is set but not ever checked.
WARNING: flowbits key 'file.nab' is set but not ever checked.
WARNING: flowbits key 'afreload' is set but not ever checked.
WARNING: flowbits key 'websocket' is set but not ever checked.
WARNING: flowbits key 'fvolli.backup' is set but not ever checked.
WARNING: flowbits key 'file.liv' is set but not ever checked.
WARNING: flowbits key 'file.csd' is set but not ever checked.
WARNING: flowbits key 'ldap.bindsuccess' is set but not ever checked.
WARNING: flowbits key 'file.ong' is set but not ever checked.
WARNING: flowbits key 'file.cell' is set but not ever checked.
WARNING: flowbits key 'file.exploit_kit_jar' is set but not ever checked.
WARNING: flowbits key 'file.cd' is set but not ever checked.
WARNING: flowbits key 'file.onenote.embedded' is checked but not ever set.
WARNING: flowbits key 'file.apk' is set but not ever checked.
WARNING: flowbits key 'file.pip' is set but not ever checked.
WARNING: flowbits key 'vnc.server.auth.types' is set but not ever checked.
WARNING: flowbits key 'clandestine.C1S1' is set but not ever checked.
WARNING: flowbits key 'file.vbscript' is set but not ever checked.
WARNING: flowbits key 'trojanmail' is set but not ever checked.
WARNING: flowbits key 'file.fon' is set but not ever checked.
WARNING: flowbits key 'file.xpf' is set but not ever checked.
WARNING: flowbits key 'RemoteKeyLog.h.Info_detection' is set but not ever checked.
WARNING: flowbits key 'FindNotGuardDog_detection' is set but not ever checked.
WARNING: flowbits key 'hawklgr' is set but not ever checked.
WARNING: flowbits key 'file.wmf' is set but not ever checked.
WARNING: flowbits key 'file.maki' is set but not ever checked.
WARNING: flowbits key 'file.xlsb' is set but not ever checked.
WARNING: flowbits key 'file.psd' is set but not ever checked.
WARNING: flowbits key 'CA_response' is set but not ever checked.
WARNING: flowbits key 'OnlyIRAT_Control' is set but not ever checked.
WARNING: flowbits key 'file.xls' is set but not ever checked.
WARNING: flowbits key 'trojan-dan-torologer' is set but not ever checked.
WARNING: flowbits key 'file.lakerb' is set but not ever checked.
WARNING: flowbits key 'file.wk' is set but not ever checked.
WARNING: flowbits key 'file.xcf' is set but not ever checked.
WARNING: flowbits key 'file.eps' is set but not ever checked.
WARNING: flowbits key 'file.gzip' is set but not ever checked.
WARNING: flowbits key 'file.jar.agent_helper' is set but not ever checked.
499 out of 1024 flowbits in use.

MaxRSS at the end of rules:1693204208

Watchlist Ideas 04:55 PM 23-12-2025
```

MODULE – 12 EVADING IDS, FIREWALLS, AND HONEYPOTS

```
MaxRSS at the end of rules:1693204208
[ Port Based Pattern Matching Memory ]
  [ Aho-Corasick Summary ] -----
  States Format : Full-Q
  Finite Automaton : DFA
  Alphabet Size : 256 Chars
  Sizeof State : Variable (1,2,4 bytes)
  Instances : 227
    1 byte states : 214
    2 byte states : 11
    4 byte states : 2
  Characters : 229293
  States : 181676
  Transitions : 3155877
  State Density : 68.3%
  Patterns : 39772
  Matched Patterns : 11066
  Memory (MB) : 162.28
  Patterns : 1.26
  Match Lists : 2.85
  DFA
    1 byte states : 1.25
    2 byte states : 19.06
    4 byte states : 137.47
[ Number of patterns truncated to 20 bytes: 651 ]

MaxRSS at the end of detection rules:1693204208
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "DeviceWPF_{6D5A87D8-EF35-4E9B-AD20-5AD31AF1D076}".

==== Initialization Complete ====
o'^-'--> Snort! <-
Version 2.9.20-WIN64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 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: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 9>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>

0 Watchlist
Ideas
Search
04:56 PM
23-12-2025
```

• Configuration successful validate

```
MaxRSS at the end of detection rules:1693204208
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "DeviceWPF_{6D5A87D8-EF35-4E9B-AD20-5AD31AF1D076}".

==== Initialization Complete ====
o'^-'--> Snort! <-
Version 2.9.20-WIN64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 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: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 9>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDP 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_DCERP2 Version 1.0 <Build 3>

Total snort Fixed Memory Cost - MaxRSS:214905504
Snort successfully validated the configuration!
Snort exiting

C:\snort\bin>
```

MODULE – 12 EVADING IDS, FIREWALLS, AND HONEYPOTS

- Type command to start snort

Command :-: snort.exe -i 2 -c "c:\snort\etc\file name “ -A console

- Here snort started

The image contains two screenshots of a Windows Command Prompt window. The top screenshot shows the output of the command 'snort -i 2 -c "c:\snort\etc\file name “ -A console'. It displays the Snort configuration validation message, the Snort version (2.9.20-WIN64 GRE (Build 82)), copyright information, and usage instructions. The bottom screenshot shows the long options and their single-character equivalents for Snort, which is a detailed list of command-line parameters and their descriptions.

```
Administrator: Command Prompt
Snort successfully validated the configuration!
snort exiting

C:\snort\bin>snort -i 2 -c "C:\snort\etc\snort - Copy (2).conf" -A
snort: option requires an argument -- A

... --> Snort! <-
o" ... Version 2.9.20-WIN64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.18 2018-06-25
Using ZLIB version: 1.2.11

USAGE: snort [-options] <filter options>
snort /SERVICE {INSTALL |UNINSTALL} <filter options>
snort /SERVICE {UNINSTALL}
snort /SERVICE {SHOW}

Options:
-A      Set alert mode: fast, full, console, test or none (alert file alerts only)
-B      Log packets in tcpdump format (much faster)
-B <mask> Obfuscate IP addresses in alerts and packet dumps using CIDR mask
-c <rules> Use Rules File <rules>
-C      Print out payloads with character data only (no hex)
-d      Dump the Application Layer
-e      Display the second layer header info
-E      Log alert messages to NtEventLog. (Win32 only)
-f      Turn on Win32 file system calls after binary log writes
-f <bpf> Read BPF filter from file <bpf>
-G <oxid> Log Identifier (to uniquely id events for multiple snorts)
-h <hn> Set home network = <hn>
        (for use with -l or -B, does NOT change $HOME_NET in IDS mode)
-H      Make hash tables deterministic.
-i <if> Listen on interface <if>
-I      Add Interface name to alert output
-k <mode> Logging mode (tcpdump,pcap,notcp,noudp,noicmp,none)
-K <mode> Logging mode (pcap[default],ascii,none)
-l <ld> Log to directory <ld>
-L <file> Log to this tcpdump file
-n <cnt> Exit after receiving <cnt> packets
-N      Turn off logging (alerts still work)
-O      Obfuscate the logged IP addresses
-p      Disable promiscuous mode sniffing
-P <snap> Set snapshot length of packet (default: 1514)
-q      Quiet. Don't show banner and status report
-r <tf> Read and process tcpdump file <tf>
-R <id> Include 'id' in snort_intfcids.pid file name
-s      Log alert messages to syslog
-S <n> Set rules file variable n equal to value v

28°C
Sunny
Search
ENG IN 04:58 PM
23-12-2025

Administrator: Command Prompt
Longname Options and their corresponding single char version
--logid <oxid> Same as -G
--perfmom-file <file> Same as -Z
--pid-path <dir> Specify the directory for the Snort PID file
--snapslen <snap> Same as -P
--spool <spool> Same as -S
--version Same as -V
--alert-before-pass Process alert, drop, sdrop, or reject before pass, default is pass before alert, drop,...
--treat-drop-as-alert Converts drop, sdrop, and reject rules into alert rules during startup
--treat-drop-as-ignore Use drop, sdrop, and reject rules to ignore session traffic when not inline.
--preprocess-dir <path> Preprocess rules in directory (dynamic, alert,...), default stops after 1st action group
--enable-inline-test Enable Inline-Test Mode Operation
--dynamic-engine-lib <file> Load a dynamic detection engine
--dynamic-engine-lib-dir <path> Load all dynamic engines from directory
--dynamic-detection-lib <file> Load a dynamic rules library
--dynamic-detection-lib-dir <path> Load all dynamic rules libraries from directory
--dynamic-preprocessor-lib <file> Create stub rule files of all loaded rules libraries
--dynamic-preprocessor-lib-dir <path> Load all dynamic preprocessor libraries from directory
--dynamic-output-lib <file> Load a dynamic output library
--dynamic-output-lib-dir <path> Load all dynamic output libraries from directory
--pcap-single <ctr> ...
--pcap-file <file> file that contains a list of pcaps to read - read mode is implied.
--pcap-list <list> a space separated list of pcaps to read - read mode is implied.
--pcap-loop <count> this option will read the pcaps specified on command line continuously.
        for example: snort -i eth0 -r 1:10 if reading multiple pcaps, reset snort to post-configuration state before reading next pcap.
--pcap-reset If reading multiple pcaps, reset snort to post-configuration state before reading next pcap.
--pcap-show Signal termination after <count> callbacks from DAQ_Acquire(), showing the time it
        takes from signaling until DAQ_Stop() is called.
--exit-check <count> ...
--conf-error-out Same as -E
--enable-mpls-multicast Allow multicast MPLS
--enable-mpls-overlapping-ip Handle overlapping IPs within MPLS (clouds
--max-mpls-labelchain-len Specify the max MPLS label chain
--mpls-payload-type Specify the protocol (ip4v, ipv6, ethernet) that is encapsulated by MPLS
--mpls-include-sid Require that all labels have SID specified.
--daq <type> Select the socket acquisition module (default is pcap).
--daq-mode <mode> Select the DAQ operating mode.
--daq-var <name=value> Specify extra DAQ configuration variable.
--daq-dir <dir> Tell snort where to find desired DAQ.
--daq-list [<dir>] List packet acquisition modules available in dir. Default is static modules only.
--daq-sock <sock> Don't attach sockets and allow snort on shutdown.
--cs-dir <dir> Directory to use for control socket.
--ha-peer Activate live high-availability state sharing with peer.
--ha-out <file> Write high-availability events to this file.
--ha-in <file> Read high-availability events from this file on startup (warm-start).
--suppress-config-log Suppress configuration information output.

28°C
Sunny
Search
ENG IN 04:58 PM
23-12-2025
```

Conclusion

Snort remains one of the most trusted and widely deployed intrusion detection and prevention tools in cybersecurity. Its flexibility, open-source nature, and real-time detection capabilities make it an essential component of network defense strategies.

Evading IDS, Firewalls, and Honeypots – Countermeasures

Evading techniques are used by attackers to bypass security mechanisms like IDS, firewalls, and honeypots. To stop this sneaky business, defenders deploy **countermeasures**—basically smarter locks, sharper eyes, and better bait. Old-school principles, modern execution.

1. Countermeasures Against IDS Evasion

IDS watches the road. Attackers try to drive slow, sideways, or in pieces.

Intrusion Detection Systems can be evaded using packet fragmentation, obfuscation, or encryption. To counter these evasion techniques:

- **Traffic normalization** is used to reassemble fragmented packets before analysis, eliminating ambiguity.
- **Signature-based detection updates** ensure the IDS recognizes new attack patterns.
- **Anomaly-based detection** identifies unusual traffic behavior rather than relying only on known signatures.
- **Encrypted traffic inspection** helps analyze malicious activity hidden inside SSL/TLS traffic.
- **Log correlation and centralized monitoring** combine multiple alerts to detect stealthy attacks.

Reality check: IDS that isn't updated is just a very expensive diary.

2. Countermeasures Against Firewall Evasion

Firewalls are gatekeepers. Attackers wear disguises.

Attackers often tunnel traffic through allowed ports or spoof protocols to bypass firewalls. Effective countermeasures include:

- **Stateful inspection firewalls** track session states, not just individual packets.
- **Deep Packet Inspection (DPI)** examines packet payloads, not only headers.
- **Application-layer firewalls** identify traffic based on application behavior rather than port numbers.
- **Strict rule-set management** reduces misconfigurations that attackers exploit.
- **Egress filtering** monitors outgoing traffic to prevent malware from communicating externally.

Classic rule still wins: *deny by default, allow by necessity.*

3. Countermeasures Against Honeypot Evasion

Honeypots are traps. Attackers try to smell the trap.

Skilled attackers attempt to detect honeypots by analyzing system behavior. Defenders counter this by making honeypots more realistic:

- **High-interaction honeypots** simulate real operating systems and services.
- **Randomized system responses** prevent fingerprinting.
- **Delayed and human-like responses** mimic real network latency.
- **Blending honeypots into production environments** avoids standing out.
- **Regular updates and patching** make honeypots appear legitimate.

A bad honeypot screams “trap.” A good one whispers “home.”

Conclusion

Security is not about one tool—it’s about layers working together. IDS detects, firewalls block, honeypots deceive, and administrators decide. Attackers evolve, so defenses must evolve faster.

Module Summary: Evading IDS, Firewalls, and Honeypots

This module explores how attackers attempt to bypass security mechanisms and how defenders counter these evasion techniques using layered, intelligent defenses. The focus is not on breaking systems, but on **strengthening them against stealthy attacks**.

Intrusion Detection Systems can be evaded through packet fragmentation, traffic obfuscation, encryption, and low-and-slow attack techniques. To counter this, organizations deploy traffic normalization, session reassembly, anomaly-based detection, frequent signature updates, and centralized log correlation. Modern IDS solutions increasingly rely on behavioral analysis and machine learning to detect unknown threats.

Firewalls are commonly bypassed using port manipulation, protocol tunneling, spoofing, and crafted packets. Countermeasures include stateful inspection, deep packet inspection, application-aware filtering, strict rule management, anti-spoofing techniques, and the use of next-generation firewalls. The Zero Trust model further strengthens firewall defenses by verifying every access request regardless of network location.

Honeypots are targeted by attackers who attempt to identify and avoid them through fingerprinting and behavioral analysis. To prevent honeypot evasion, defenders use high-interaction and hybrid honeypots, realistic system behavior, dynamic configurations, delayed responses, and seamless integration with production networks. Honeynets extend this concept by simulating entire network environments.

Overall, the module emphasizes **defense in depth**, where IDS, firewalls, honeypots, SIEM systems, and human analysis work together. Security is shown as a continuous process that requires constant monitoring, updating, and adaptation to evolving threats.

THANK YOU

SACHCHITANAND