M.Kumarasamy
College of Engineering
NAAC Accredited Autonomous Institution
Approved by AICTE & Affiliated to Anna University
ISO 9001:2015 Certified Institution
Thalavapalayam, Karur, Tamilnadu.

DEPARTMENT OF ARTIFICIAL INTELLIGENCE & DATA SCIENCE

EXPERENTIAL LEARNING - 2

NAME	VINOHARSITHA A S
REGISTER NUMBER	927621BAD060
SUBJECT	CRYPTOGRAPHY & NETWORK SECURITY
SUBJECT CODE	18AIC307T
SUBMITTED TO	Ms. A. NITHYASRI (AP/AI)
DATE	25.05. 2024

INTRUSION DETECTION SYSTEM USING SNORT

INTRODUCTION TO SNORT

Snort is an open source tool for Intrusion Detection and Prevention System. It uses a series of rules that help define malicious network activities and uses those rules to find packets that match against them and generates alerts for users.

Snort has three primary uses :

- As a packet sniffer like tcpdump
- As a packet logger — which is useful for network traffic debugging
- As a full-blown network intrusion prevention system.

AIM

To detect the intrusion using the snort software.

PROCEDURE

- To download the Snort Software :
    a. Download Snort tool for 32-bit or 64-bit Windows Operating system.
    b. After downloading the Snort tool, double click on it for installation. It will show a license agreement on the users' screen.
    c. Select the Snort, Dynamic Modules, and Documentation components and click on Next button.
    d. The default path is "C:/Snort" to install the Snort tool. After successful installation, a message with "snort has successfully been installed" will display on the screen
    e. Open a command prompt and type the path where Snort has been installed (i.e., cd \snort) and press Enter and Type "cd bin" to go to bin folder.Type "snort –V" in command prompt to check the version of Snort tool.
- To download the rules :
    a. Download the rules. Click on "Sign in" button to create an account or login
    b. The rules can be downloaded after successful sign in. A compressed folder "snortrules-snapshot29161.tar.gz" will be downloaded in the personal computer. Unzip the compressed folder

c. Open the “snortrules-snapshot-29161.tar” folder and find “rules” folder. Open the “rules” folder and copy all the rules present inside it

d. Go to “C:\Snort\rules” and paste all the rules files.

- To edit the snort.conf file :

  a. Go to “C:\Snort\etc” to open the snort.conf file.

  b. Open the command prompt and type “ipconfig”. The IP address of the personal computer or laptop will be displayed on the command prompt

  c. Set the network variables of snort.conf file by typing the IP address (192.168.43.160). Set up the external network address as home network ($HOME_NET).

  d. Set the path of the rules files as “C:\Snort\rules” and “C:\Snort\preproc_rules” . Set the white list and black list path as to “C:\Snort\rules”.

  e. Configure the decoder of snort.conf file by setting the path of the log directory as “C:\Snort\log”.

  f. Configure preprocessors in snort.conf file by removing the “\” and putting decompress_swf and decompress_pdf in comments. Also, put the preprocessors in comments. Also, put the preprocessor bo in comments Delete comment from preprocessor sfportscan.

  g. Set path to white list and black list. Create a new white list and black list. Save these files in rules directory.

  h. Customize rule set in snort.conf file by replacing the forward slash “/” with backslash “\”.

  i. : Open the command prompt and go to “C:\Snort\bin” and type “snort –W” to check the available interface.

  j. Execute the Snort tool in the command prompt by typing “snort –i 2 –c C:\Snort\etc\snort.conf”.

- To write rules to detect scanning attack :

  a. After running Snort in IDS mode, the next step is to write rules in “local.rules” file. For example, the following rules can be added to detect SYN attack, UDP scan, PINK scan, FIN scan, NULL scan, XMAS scan, and TCP scan.

    - alert tcp any any -> any any (msg: "SYN attack"; flags: S,12; sid: 10000005;) 22

- alert udp any any -> 192.168.43.160 any (msg: "UDP Scan"; sid: 10001;rev: 1;)
- alert icmp any any -> 192.168.43.160 any (msg: "PING Scan"; dsize:0;sid:10002; rev: 1;)
- alert tcp any any -> $HOME_NET any (msg: "FIN Scan"; flags: F; sid: 10003;rev: 1;)
- alert tcp any any -> $HOME_NET any (msg: "NULL Scan"; flags: 0; sid: 10004;rev: 1;)
- alert tcp 192.168.43.160 any -> $HOME_NET 22 (msg: "XMAS Scan"; flags: FPU; sid: 10005;rev: 1;)
- alert tcp 192.168.43.160 any -> 192.168.43.160 any (msg: "TCP Scan"; flags: S,12; sid: 10006;rev: 1;)

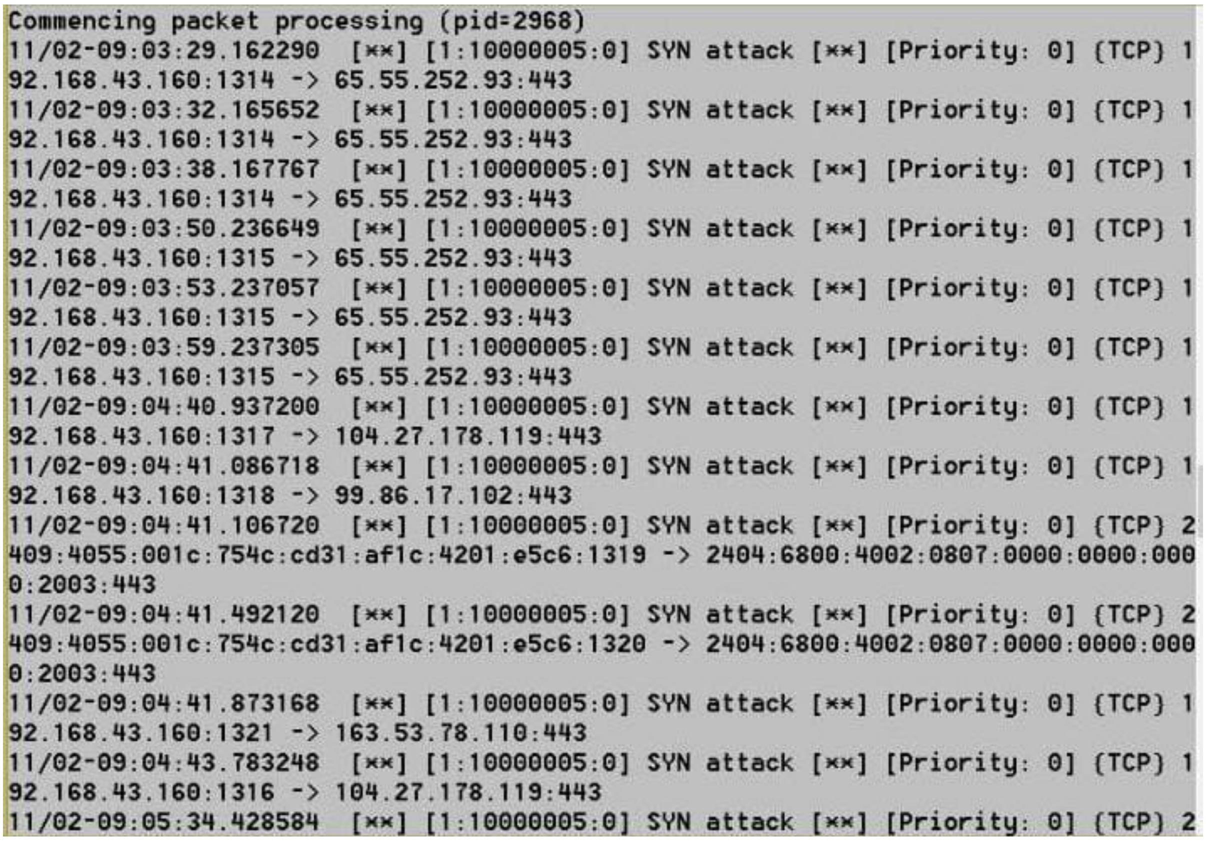
b. Execute Snort in IDS mode by typing “snort –i 1 –c C:\Snort\etc\snort.conf –A console” in the command prompt and press Enter.

c. Perform network scanning attacks with nmap by typing “nmap –p 1-65535 –v 192.168.43.160” in the command prompt as shown in Figure 41 where p is the port number and v is the verbose mode. The network scanning attacks can be performed with Zenmap tool.

d. The network scanning attacks are detected by Snort IDS.

The following countermeasures must be followed:

- Always disable SNMP and SMB on hosts if not using it for a particular period of time.
- Block the SNMP ports (UDP ports 161 and 162) and SMB ports (TCP port 139 and 445) at the network perimeter.
- There’s technically a “U” that’s part of the solution: upgrade. Upgrading systems (at least the ones you can) to 27 SNMP version 3 and SMB version 2 can resolve many of the well-known SNMP and SMB security weaknesses.



```
Commencing packet processing (pid=2968)
11/02-09:03:29.162290  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 1
92.168.43.160:1314 -> 65.55.252.93:443
11/02-09:03:32.165652  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 1
92.168.43.160:1314 -> 65.55.252.93:443
11/02-09:03:38.167767  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 1
92.168.43.160:1314 -> 65.55.252.93:443
11/02-09:03:50.236649  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 1
92.168.43.160:1315 -> 65.55.252.93:443
11/02-09:03:53.237057  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 1
92.168.43.160:1315 -> 65.55.252.93:443
11/02-09:03:59.237305  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 1
92.168.43.160:1315 -> 65.55.252.93:443
11/02-09:04:40.937200  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 1
92.168.43.160:1317 -> 104.27.178.119:443
11/02-09:04:41.086718  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 1
92.168.43.160:1318 -> 99.86.17.102:443
11/02-09:04:41.106720  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 2
409:4055:001c:754c:cd31:af1c:4201:e5c6:1319 -> 2404:6800:4002:0807:0000:0000:000
0:2003:443
11/02-09:04:41.492120  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 2
409:4055:001c:754c:cd31:af1c:4201:e5c6:1320 -> 2404:6800:4002:0807:0000:0000:000
0:2003:443
11/02-09:04:41.873168  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 1
92.168.43.160:1321 -> 163.53.78.110:443
11/02-09:04:43.783248  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 1
92.168.43.160:1316 -> 104.27.178.119:443
11/02-09:05:34.428584  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 2
```

CONCLUSION :

Thus the intrusion detection system using the snort has been configured and executed successfully.Thus ,this snort software has been used to detect whether intrusion has occurred.