Basic Packet Capture with Snort

לאחר התקנת snort על מחשב linux (השתמשתי ב C9) התחלתי להקליט את התקשורת ע"י הרצת הפקודה:

snort –i eth0 –v

כאשר i eth0– מגדיר את הממשק שבו אני מעוניין להסניף (פעולה זו נחוצה מפני שזו הפעם הראשונה שאני מסניף, מכאן ואילך אין צורך להשתמש שוב בדגל הזה, אלא אם ארצה להקליט מממשק אחר).

```
sudo - "dvir570-p ×    bash - "ubuntu@ ×
TCP Options (3) => NOP NOP TS: 887906704 912383792
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
05/18-08:51:11.199535 10.240.1.209:34090 -> 172.17.0.42:22
TCP TTL:63 TOS:0x8 ID:31251 IpLen:20 DgmLen:116 DF
***AP*** Seq: 0xEDDFDA9  Ack: 0x748430B8  Win: 0x15E  TcpLen: 32
TCP Options (3) => NOP NOP TS: 887906704 912383792
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

(snort_decoder) WARNING: IP dgm len > captured len
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
05/18-08:51:11.200202 10.240.1.209:34090 -> 172.17.0.42:22
TCP TTL:63 TOS:0x8 ID:31252 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xEDDFDE9  Ack: 0x74843BB8  Win: 0x15E  TcpLen: 32
TCP Options (3) => NOP NOP TS: 887906704 912383792
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

05/18-08:51:11.202420 172.17.0.42:22 -> 10.240.1.209:34090
TCP TTL:64 TOS:0x8 ID:28784 IpLen:20 DgmLen:996 DF
***AP*** Seq: 0x74843BB8  Ack: 0xEDDFDA9  Win: 0x732  TcpLen: 32
TCP Options (3) => NOP NOP TS: 912383793 887906704
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

05/18-08:51:11.242778 172.17.0.42:22 -> 10.240.1.209:34090
TCP TTL:64 TOS:0x8 ID:28785 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x74843F68  Ack: 0xEDDFDE9  Win: 0x732  TcpLen: 32
TCP Options (3) => NOP NOP TS: 912383804 887906704
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
05/18-08:51:11.246150 10.240.1.209:34090 -> 172.17.0.42:22
TCP TTL:63 TOS:0x8 ID:31253 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xEDDFDE9  Ack: 0x74843F68  Win: 0x15E  TcpLen: 32
TCP Options (3) => NOP NOP TS: 887906716 912383793
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

בסיום ההקלטה ע"י לחיצה על ctrl+C נקבל סיכום על ההקלטה.

בסיכום זה מופיעים פרטים כמו משך זמן ההקלטה, קצב ממוצע של פקטות שהוסנפו, משקל ההסנפה (כמה זכרון היה בשימוש),סך כל הפקטות שנקלטו וסייוג של הפקטות לפי פורטוקולים כך שנוכל לדעת כמה פקטות הוסנפו מכל פרוטוקול.

```
bash - "dvir570-p ×    bash - "ubuntu@ ×
===============================================================================
Run time for packet processing was 334.859490 seconds
Snort processed 2600 packets.
Snort ran for 0 days 0 hours 5 minutes 34 seconds
   Pkts/min:          520
   Pkts/sec:            7
===============================================================================
Memory usage summary:
  Total non-mmapped bytes (arena):       782336
  Bytes in mapped regions (hblkhd):      21590016
  Total allocated space (uordblks):      677792
  Total free space (fordblks):           104544
  Topmost releasable block (keepcost):   101168
===============================================================================
Packet I/O Totals:
   Received:         2609
   Analyzed:         2601 ( 99.693%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            8 (  0.307%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:         2600 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:         2597 ( 99.885%)
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:            0 (  0.000%)
        TCP:         2575 ( 99.038%)
        IP6:            3 (  0.115%)
    IP6 Ext:            5 (  0.192%)
   IP6 Opts:            2 (  0.077%)
      Frag6:            0 (  0.000%)
      ICMP6:            3 (  0.115%)
       UDP6:            0 (  0.000%)
       TCP6:            0 (  0.000%)
```

בהרצת הפקודה

snort –dv

הודפס לטרמינל גם התוכן של הפקטות עצמן משכבת האפליקציה:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
05/18-09:17:57.937154 10.240.1.209:34090 -> 172.17.0.42:22
TCP TTL:63 TOS:0x8 ID:32527 IpLen:20 DgmLen:116 DF
***AP*** Seq: 0xEDEA5D9  Ack: 0x74931258  Win: 0x15E  TcpLen: 32
TCP Options (3) => NOP NOP TS: 888308388 912785475
4F 4C 7D 45 C8 D3 FE DC 25 69 A4 4E 64 D0 4E 94  OL}E....%i.Nd.N.
E9 38 DE 0D AD 9A 32 9D 5B CF 5D 24 8E 20 78 DA  .8....2.[.]$. x.
E6 90 54 7F 1B 1F 1E 30 38 DF 26 A6 AD DD 63 91  ..T....08.&...c.
18 D0 E8 1D 3E 37 AB 88 E1 03 45 0B 5E 45 77 22  ....>7....E.^Ew"

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

ע"י הרצת הפקודה

snort –h נוכל לראות את כל הדגלים שאנו יכולים להוסיף:

```
-A         Set alert mode: fast, full, console, test or none  (alert file alerts only)
           "unsock" enables UNIX socket logging (experimental).
-b         Log packets in tcpdump format (much faster!)
-B <mask>  Obfuscated 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
-D         Run Snort in background (daemon) mode
-e         Display the second layer header info
-f         Turn off fflush() calls after binary log writes
-F <bpf>   Read BPF filters from file <bpf>
-g <gname> Run snort gid as <gname> group (or gid) after initialization
-G <0xid>  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>  Checksum mode (all,noip,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
-M         Log messages to syslog (not alerts)
-m <umask> Set umask = <umask>
-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 explicit snaplen of packet (default: 1514)
-q         Quiet. Don't show banner and status report
```

בהרצת הפקודה

snort –K ascii

ההקלטה נכתבה לתוך קבצי לוגים בתקייה var/log/snort מסווגת לפי כתובת ה ipaddress שמעורבות ב-session, הפורטים והפרוטוקול שהיה בשימוש:

```
root@dvir570-python-6094507:/var/log/snort/172.17.0.42# cat TCP\:34090-22
05/18-09:33:28.516221 172.17.0.42:22 -> 10.240.1.209:34090
TCP TTL:64 TOS:0x8 ID:32209 IpLen:20 DgmLen:660 DF
***AP*** Seq: 0x74B589B8  Ack: 0xEDF52E9  Win: 0x732  TcpLen: 32
TCP Options (3) => NOP NOP TS: 913018122 888541023
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

05/18-09:33:29.539502 172.17.0.42:22 -> 10.240.1.209:34090
TCP TTL:64 TOS:0x8 ID:32210 IpLen:20 DgmLen:244 DF
***AP*** Seq: 0x74B58C18  Ack: 0xEDF52E9  Win: 0x732  TcpLen: 32
TCP Options (3) => NOP NOP TS: 913018378 888541033
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

05/18-09:33:30.556045 172.17.0.42:22 -> 10.240.1.209:34090
TCP TTL:64 TOS:0x8 ID:32211 IpLen:20 DgmLen:180 DF
***AP*** Seq: 0x74B58CD8  Ack: 0xEDF52E9  Win: 0x732  TcpLen: 32
TCP Options (3) => NOP NOP TS: 913018632 888541289
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

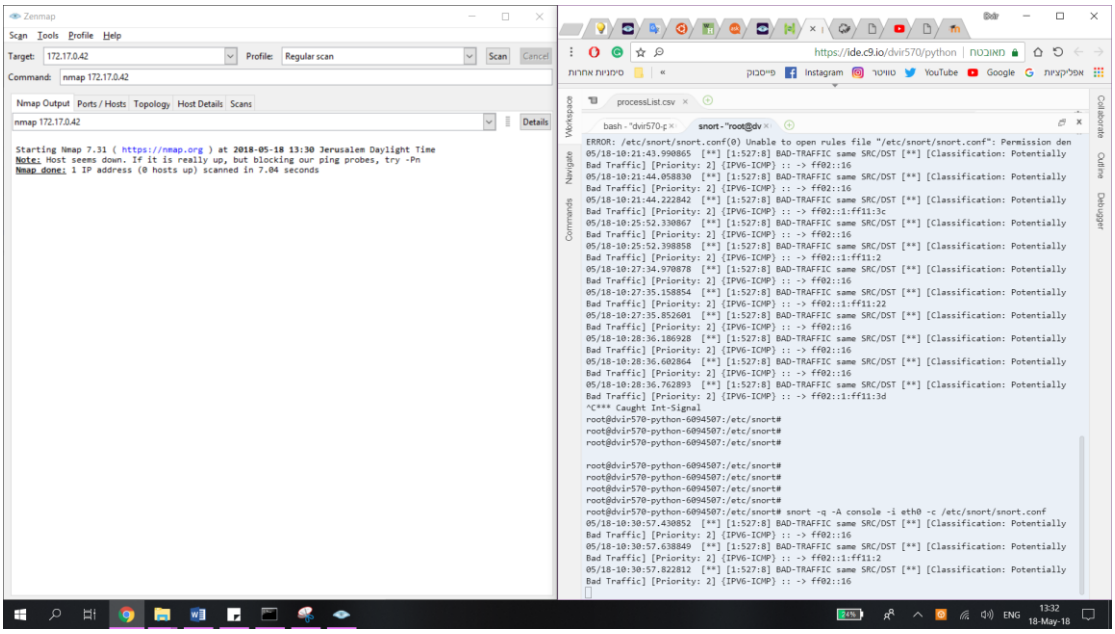
הדגל A- מקבל מצב התראה (fast, full, none, and unsock), וישנה בקובץ הקונפיגורציה בהתאם למצב שנבחר את מצב ההתראה עבור הדגימה. לפי המצב שיבחר יווצרו התראות מתאימות.

IDS Alerts

בהרצת הפקודה

snort -q -A console -i eth0 -c /etc/snort/snort.conf

וביצוע של סריקת פורטים ממכונה אחרת על המחשב ע"י הכלי nmap הביא לתוצאה הבאה:



בתמונה זו ניתן לראות שהודפס למסך ה-console התראות על אירועים חריגים בגלל שעשיתי סריקת פורטים על המחשב.

תמונות של כמה מהחוקים שסופקו:

icmp.rules

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP ISS Pinger"; itype:8; content:"ISSPNGRQ"; depth:32; reference:arachnids,158; classtype:attempted-recon; sid:465; rev:3;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP L3retriever Ping"; icode:0; itype:8; content:"ABCDEFGHIJKLMNOPQRSTUVWABCDEFGHI"; depth:32; reference:arachnids,311; classtype:attempted-recon; sid:466;
 rev:4;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Nemesis v1.1 Echo"; dsize:20; icmp_id:0; icmp_seq:0; itype:8; content:"|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00|"; reference:arachn
ids,449; classtype:attempted-recon; sid:467; rev:3;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING NMAP"; dsize:0; itype:8; reference:arachnids,162; classtype:attempted-recon; sid:469; rev:3;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP icmpenum v1.1.1"; dsize:0; icmp_id:666 ; icmp_seq:0; id:666; itype:8; reference:arachnids,450; classtype:attempted-recon; sid:471; rev:3;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP redirect host"; icode:1; itype:5; reference:arachnids,135; reference:cve,1999-0265; classtype:bad-unknown; sid:472; rev:4;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP redirect net"; icode:0; itype:5; reference:arachnids,199; reference:cve,1999-0265; classtype:bad-unknown; sid:473; rev:4;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP superscan echo"; dsize:8; itype:8; content:"|00 00 00 00 00 00 00 00|"; classtype:attempted-recon; sid:474; rev:4;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP traceroute ipopts"; ipopts:rr; itype:0; reference:arachnids,238; classtype:attempted-recon; sid:475; rev:3;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP webtrends scanner"; icode:0; itype:8; content:"|00 00 00 00|EEEEEEEEEEEE"; reference:arachnids,307; classtype:attempted-recon; sid:476; rev:4;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Source Quench"; icode:0; itype:4; classtype:bad-unknown; sid:477; rev:2;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Broadscan Smurf Scanner"; dsize:4; icmp_id:0; icmp_seq:0; itype:8; classtype:attempted-recon; sid:478; rev:3;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING speedera"; itype:8; content:"89|3A 3B|<=>?"; depth:100; classtype:misc-activity; sid:480; rev:5;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP TJPingPro1.1Build 2 Windows"; itype:8; content:"TJPingPro by Jim"; depth:32; reference:arachnids,167; classtype:misc-activity; sid:481; rev:5;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING WhatsupGold Windows"; itype:8; content:"WhatsUp - A Netw"; depth:32; reference:arachnids,168; classtype:misc-activity; sid:482; rev:5;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING CyberKit 2.2 Windows"; itype:8; content:"|AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA|"; depth:32; reference:arachnids,154; classtype:misc-act
ivity; sid:483; rev:5;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING Sniffer Pro/NetXRay network scan"; itype:8; content:"Cinco Network, Inc."; depth:32; classtype:misc-activity; sid:484; rev:4;)
alert icmp any any -> any any (msg:"ICMP Destination Unreachable Communication Administratively Prohibited"; icode:13; itype:3; classtype:misc-activity; sid:485; rev:4;)
alert icmp any any -> any any (msg:"ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited"; icode:10; itype:3; classtype:misc-activity; sid:486; rev:4;)
alert icmp any any -> any any (msg:"ICMP Destination Unreachable Communication with Destination Network is Administratively Prohibited"; icode:9; itype:3; classtype:misc-activity; sid:487; rev:4;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP digital island bandwidth query"; content:"mailto|3A|ops@digisle.com"; depth:22; classtype:misc-activity; sid:1813; rev:5;)
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Large ICMP Packet"; dsize:>800; reference:arachnids,246; classtype:bad-unknown; sid:499; rev:4;)
```

dns.rules

```
#----------
# DNS RULES
#----------

alert tcp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"DNS zone transfer TCP"; flow:to_server,established; content:"|00 00 FC|"; offset:15; reference:arachnids,212; reference:cve,1999-0532; reference:nessus,10595;
 classtype:attempted-recon; sid:255; rev:13;)
alert udp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"DNS zone transfer UDP"; content:"|00 00 FC|"; offset:14; reference:arachnids,212; reference:cve,1999-0532; reference:nessus,10595; classtype:attempted-recon;
sid:1948; rev:6;)


alert tcp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"DNS named authors attempt"; flow:to_server,established; content:"|07|authors"; offset:12; nocase; content:"|04|bind|00|"; offset:12; nocase; reference:arachni
ds,480; reference:nessus,10728; classtype:attempted-recon; sid:1435; rev:7;)
alert udp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"DNS named authors attempt"; content:"|07|authors"; offset:12; nocase; content:"|04|bind|00|"; offset:12; nocase; reference:arachnids,480; reference:nessus,107
28; classtype:attempted-recon; sid:256; rev:6;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"DNS named version attempt"; flow:to_server,established; content:"|07|version"; offset:12; nocase; content:"|04|bind|00|"; offset:12; nocase; reference:arachni
ds,278; reference:nessus,10028; classtype:attempted-recon; sid:257; rev:9;)
alert udp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"DNS named version attempt"; content:"|07|version"; offset:12; nocase; content:"|04|bind|00|"; offset:12; nocase; reference:arachnids,278; reference:nessus,100
28; classtype:attempted-recon; sid:1616; rev:7;)



alert udp $EXTERNAL_NET 53 -> $HOME_NET any (msg:"DNS SPOOF query response PTR with TTL of 1 min. and no authority"; content:"|85 80 00 01 00 01 00 00 00 00|"; content:"|C0 0C 00 0C 00 01 00 00 00|<|00 0F|";
classtype:bad-unknown; sid:253; rev:4;)
alert udp $EXTERNAL_NET 53 -> $HOME_NET any (msg:"DNS SPOOF query response with TTL of 1 min. and no authority"; content:"|81 80 00 01 00 01 00 00 00 00|"; content:"|C0 0C 00 01 00 01 00 00 00|<|00 04|"; clas
stype:bad-unknown; sid:254; rev:4;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"DNS EXPLOIT named 8.2->8.2.1"; flow:to_server,established; content:"../../../"; reference:bugtraq,788; reference:cve,1999-0833; classtype:attempted-admin; sid
:258; rev:6;)
```

ועוד חוקים נוספים..