ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

UNIVERSITY OF PIRAEUS

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΜΑΘΗΜΑ: «ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ (8ο ΕΞΑΜΗΝΟ)»

ΚΑΘΗΓΗΤΕΣ: ΚΟΤΖΑΝΙΚΟΛΑΟΥ ΠΑΝΑΓΙΩΤΗΣ

ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ:

ΔΗΜΗΤΡΕΛΛΟΣ ΠΑΝΑΓΙΩΤΗΣ, Π17026

ΚΑΡΑΜΠΟΪΚΗΣ ΝΙΚΟΛΑΟΣ, Π17040

ΡΟΥΝΤΟΥ ΑΝΝΑ-ΦΑΝΗ, Π17113

5η Άσκηση – Υλοποίηση και δοκιμή IDS

1.

Ξεκινώντας κατεβάζουμε το snort με την εντολή:

$sudo apt install snort

```
zastava-ceo@zastavaceo-VirtualBox:~$ sudo apt install snort
Reading package lists... Done
Building dependency tree
Reading state information... Done
snort is already the newest version (2.9.7.0-5build1).
The following packages were automatically installed and are no longer required:
  libfprint-2-tod1 libllvm10
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 4 not upgraded.
zastava-ceo@zastavaceo-VirtualBox:~$
```

Ύστερα ανοίγουμε το Configuration του Snort με την εντολή:

$sudo gedit /etc/snort/snort.conf

Εκεί αλλάζουμε τα:

ipvar HOME_NET 192.168.2.9/32

ipvar EXTERNAL_NET ! $HOME_NET

var WHITE_LIST_PATH /etc/snort/rules/iplists

var BLACK_LIST_PATH /etc/snort/rules/iplists

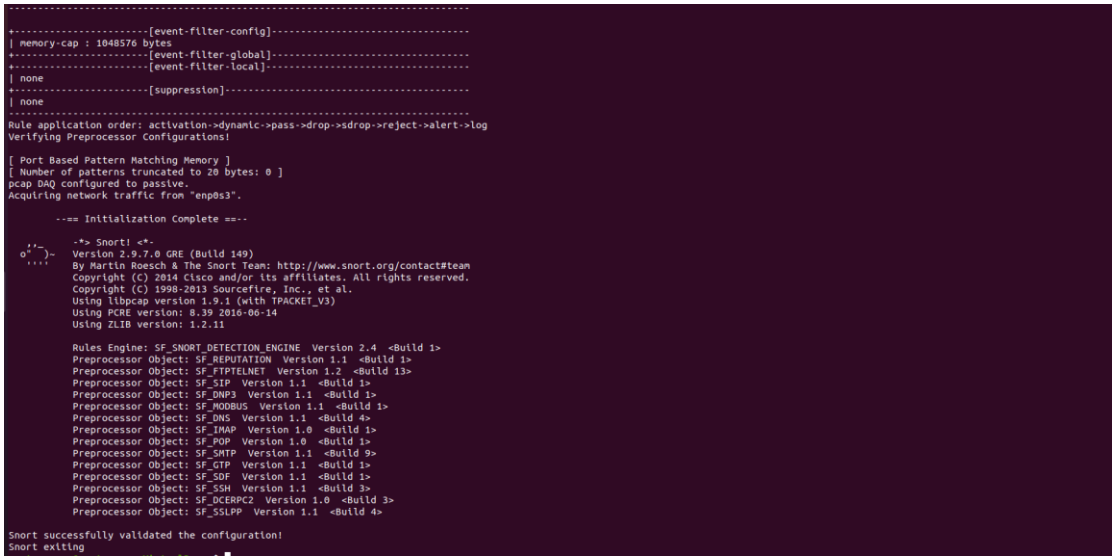
```
50 #
51 #ipvar HOME_NET any
52 ipvar HOME_NET 192.168.2.9/32
53 # Set up the external network addresses. Leave as "any" in most situations
54 #ipvar EXTERNAL_NET any
55 # If HOME_NET is defined as something other than "any", alternative, you can
56 # use this definition if you do not want to detect attacks from your internal
57 # IP addresses:
58 ipvar EXTERNAL_NET !$HOME_NET
59
```

```
114 var RULE_PATH /etc/snort/rules
115 var SO_RULE_PATH /etc/snort/so_rules
116 var PREPROC_RULE_PATH /etc/snort/preproc_rules
117
```

```
var WHITE_LIST_PATH /etc/snort/rules/iplists
var BLACK_LIST_PATH /etc/snort/rules/iplists
```

Για το testing θα χρησιμοποιήσω την εντολή:

$sudo snort -T -c /etc/snort/snort.conf -i enp0s3



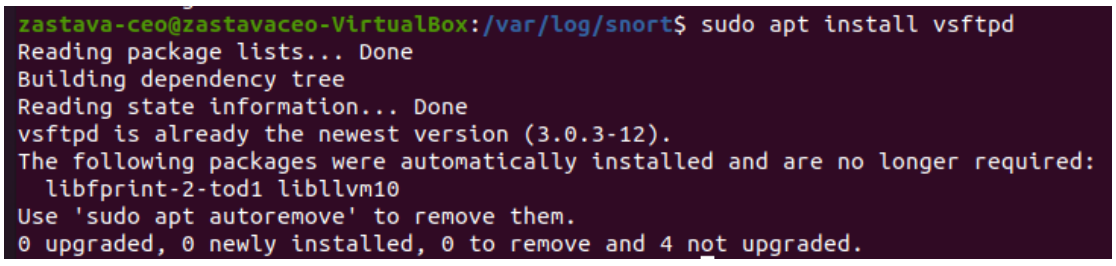
Αμέσως μετά ανοίγουμε το αρχείο /etc/snort/rules/local.rules και εισχωρούμε την δική μας εντολή:

alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP test"; sid:10000001; rev:001;)

```
1 # $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
2 # ----------------
3 # LOCAL RULES
4 alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP test"; sid:10000001; rev:001;)
5 # ----------------
6 # This file intentionally does not come with signatures.  Put your local
7 # additions here.
```

Ήρθε η ώρα να κατεβάσουμε τον FTP Server μας με την εντολή:

$ sudo apt install vsftpd



```
zastava-ceo@zastavaceo-VirtualBox:/var/log/snort$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.2.9  netmask 255.255.255.0  broadcast 192.168.2.255
        inet6 fe80::be23:aa6c:f558:715f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:39:c7:d6  txqueuelen 1000  (Ethernet)
        RX packets 165891  bytes 186627273 (186.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 81082  bytes 9072434 (9.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 106818  bytes 58034315 (58.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 106818  bytes 58034315 (58.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Πλέον στο δεύτερο μηχάνημά μας (Kali) ανοίγω το Metasploit ώστε να κάνω το Bruteforce attack στο FTP Server του Ubuntu και εισχωρώντας τα σωστά credentials ξεκινάω να κάνω την επίθεση.

```
msf > use auxiliary/scanner/ftp/ftp_login
msf auxiliary(ftp_login) > search user_file /usr/share/wordlists
[!] Module database cache not built yet, using slow search
^C[-] Error while running command search:
msf auxiliary(ftp_login) > set user_file /usr/share/wordlists/rockyou.txt
user_file => /usr/share/wordlists/rockyou.txt
msf auxiliary(ftp_login) > set pass_file /usr/share/wordlists/rockyou.txt
pass_file => /usr/share/wordlists/rockyou.txt
```

```
msf auxiliary(ftp_login) > set rhosts 192.168.2.9
rhosts => 192.168.2.9
msf auxiliary(ftp_login) > run

[*] 192.168.2.9:21        - 192.168.2.9:21 - Starting FTP login sweep
[!] 192.168.2.9:21        - No active DB -- Credential data will not be saved!
[-] 192.168.2.9:21        - 192.168.2.9:21 - LOGIN FAILED: 123456:123456 (Incorrect: )
[-] 192.168.2.9:21        - 192.168.2.9:21 - LOGIN FAILED: 123456:12345 (Incorrect: )
[-] 192.168.2.9:21        - 192.168.2.9:21 - LOGIN FAILED: 123456:123456789 (Incorrect:
 )
[-] 192.168.2.9:21        - 192.168.2.9:21 - LOGIN FAILED: 123456:password (Incorrect:
)
[-] 192.168.2.9:21        - 192.168.2.9:21 - LOGIN FAILED: 123456:iloveyou (Incorrect:
)
[-] 192.168.2.9:21        - 192.168.2.9:21 - LOGIN FAILED: 123456:princess (Incorrect:
)
[-] 192.168.2.9:21        - 192.168.2.9:21 - LOGIN FAILED: 123456:1234567 (Incorrect: )
[-] 192.168.2.9:21        - 192.168.2.9:21 - LOGIN FAILED: 123456:rockyou (Incorrect: )
[-] 192.168.2.9:21        - 192.168.2.9:21 - LOGIN FAILED: 123456:12345678 (Incorrect:
)
[-] 192.168.2.9:21        - 192.168.2.9:21 - LOGIN FAILED: 123456:abc123 (Incorrect: )
[-] 192.168.2.9:21        - 192.168.2.9:21 - LOGIN FAILED: 123456:nicole (Incorrect: )
```

Μέχρι αυτήν την ώρα δεν έχουμε παρατηρήσει κάτι καινούριο στο ubuntu μηχάνημά μας.

2.

Εκτελώντας το Snort με την εντολή:

$ sudo snort -A console -i enp0s3 -c /etc/snort/snort.conf

```
+----------------------[event-filter-config]---------------------------------
| memory-cap : 1048576 bytes
+----------------------[event-filter-global]---------------------------------
+----------------------[event-filter-local]----------------------------------
| none
+----------------------[suppression]-----------------------------------------
| none
--------------------------------------------------------------------------------
Rule application order: activation->dynamic->pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!

[ Port Based Pattern Matching Memory ]
[ Number of patterns truncated to 20 bytes: 0 ]
pcap DAQ configured to passive.
Acquiring network traffic from "enp0s3".
Reload thread starting...
Reload thread started, thread 0x7f5e8288f700 (49974)
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.7.0 GRE (Build 149)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.4  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
Commencing packet processing (pid=49969)
```

Παρατηρούμε ότι πλέον σκάει στο τερματικό μας συνεχώς το alert που δημιουργήσαμε πρίν, αφού λαμβάνουμε πλέον πολλά requests από το Kali μηχάνημα

```
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
Commencing packet processing (pid=49969)
06/07-21:35:39.948893  [**] [1:10000001:1] FTP test [**] [Priority: 0] {TCP} 192.168.2.12:35017 -> 192.168.2.9:21
06/07-21:35:39.949175  [**] [1:10000001:1] FTP test [**] [Priority: 0] {TCP} 192.168.2.12:35017 -> 192.168.2.9:21
06/07-21:35:39.953295  [**] [1:10000001:1] FTP test [**] [Priority: 0] {TCP} 192.168.2.12:35017 -> 192.168.2.9:21
06/07-21:35:39.953527  [**] [1:10000001:1] FTP test [**] [Priority: 0] {TCP} 192.168.2.12:35017 -> 192.168.2.9:21
06/07-21:35:39.954192  [**] [1:10000001:1] FTP test [**] [Priority: 0] {TCP} 192.168.2.12:35017 -> 192.168.2.9:21
06/07-21:35:42.715718  [**] [1:10000001:1] FTP test [**] [Priority: 0] {TCP} 192.168.2.12:42069 -> 192.168.2.9:21
06/07-21:35:42.716661  [**] [1:10000001:1] FTP test [**] [Priority: 0] {TCP} 192.168.2.12:42069 -> 192.168.2.9:21
06/07-21:35:42.720055  [**] [1:10000001:1] FTP test [**] [Priority: 0] {TCP} 192.168.2.12:42069 -> 192.168.2.9:21
06/07-21:35:42.720446  [**] [1:10000001:1] FTP test [**] [Priority: 0] {TCP} 192.168.2.12:42069 -> 192.168.2.9:21
06/07-21:35:42.721059  [**] [1:10000001:1] FTP test [**] [Priority: 0] {TCP} 192.168.2.12:42069 -> 192.168.2.9:21
06/07-21:35:42.752773  [**] [1:10000001:1] FTP test [**] [Priority: 0] {TCP} 192.168.2.12:35017 -> 192.168.2.9:21
06/07-21:35:45.223631  [**] [1:10000001:1] FTP test [**] [Priority: 0] {TCP} 192.168.2.12:34015 -> 192.168.2.9:21
06/07-21:35:45.223859  [**] [1:10000001:1] FTP test [**] [Priority: 0] {TCP} 192.168.2.12:34015 -> 192.168.2.9:21
06/07-21:35:45.226875  [**] [1:10000001:1] FTP test [**] [Priority: 0] {TCP} 192.168.2.12:34015 -> 192.168.2.9:21
06/07-21:35:45.227196  [**] [1:10000001:1] FTP test [**] [Priority: 0] {TCP} 192.168.2.12:34015 -> 192.168.2.9:21
06/07-21:35:45.227796  [**] [1:10000001:1] FTP test [**] [Priority: 0] {TCP} 192.168.2.12:34015 -> 192.168.2.9:21
06/07-21:35:45.265464  [**] [1:10000001:1] FTP test [**] [Priority: 0] {TCP} 192.168.2.12:42069 -> 192.168.2.9:21
06/07-21:35:48.475559  [**] [1:10000001:1] FTP test [**] [Priority: 0] {TCP} 192.168.2.12:34799 -> 192.168.2.9:21
06/07-21:35:48.475768  [**] [1:10000001:1] FTP test [**] [Priority: 0] {TCP} 192.168.2.12:34799 -> 192.168.2.9:21
06/07-21:35:48.478568  [**] [1:10000001:1] FTP test [**] [Priority: 0] {TCP} 192.168.2.12:34799 -> 192.168.2.9:21
06/07-21:35:48.478878  [**] [1:10000001:1] FTP test [**] [Priority: 0] {TCP} 192.168.2.12:34799 -> 192.168.2.9:21
06/07-21:35:48.479353  [**] [1:10000001:1] FTP test [**] [Priority: 0] {TCP} 192.168.2.12:34799 -> 192.168.2.9:21
06/07-21:35:48.518733  [**] [1:10000001:1] FTP test [**] [Priority: 0] {TCP} 192.168.2.12:34015 -> 192.168.2.9:21
```

3.

Εισχωρούμε τους κανόνες που βρίσκουμε στο site του snort και ξαναδοκιμάζουμε την επίθεση. Αν και κάναμε αρκετές δοκιμές δεν καταφέραμε να ενεργοποιήσουμε κάποιον νέο κανόνα.

```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP test"; sid:10000001; rev:001;)
# protocol verification
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP MDTM overflow attempt"; flow:to_server,established; content:"MDTM"; nocase; isdataat:100,relative; pcre:"/^MDTM\s[^\n]{100}/smi";
  reference:bugtraq,9751; reference:cve,2001-1021; reference:cve,2004-0330; reference:nessus,12080; classtype:attempted-admin; sid:2546; rev:5;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP XMKD overflow attempt"; flow:to_server,established; content:"XMKD"; nocase; isdataat:100,relative; pcre:"/^XMKD\s[^\n]{100}/smi";
  reference:bugtraq,7909; reference:cve,2000-0133; reference:cve,2001-1021; classtype:attempted-admin; sid:2373; rev:4;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP NLST overflow attempt"; flow:to_server,established; content:"NLST"; nocase; isdataat:100,relative; pcre:"/^NLST\s[^\n]{100}/smi";
  reference:bugtraq,10184; reference:bugtraq,7909; reference:bugtraq,9675; reference:cve,1999-1544; classtype:attempted-admin; sid:2374; rev:6;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP ALLO overflow attempt"; flow:to_server,established; content:"ALLO"; nocase; isdataat:100,relative; pcre:"/^ALLO\s[^\n]{100}/smi";
  reference:bugtraq,9953; classtype:attempted-admin; sid:2449; rev:1;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP RNTO overflow attempt"; flow:to_server,established; content:"RNTO"; nocase; isdataat:100,relative; pcre:"/^RNTO\s[^\n]{100}/smi";
  reference:bugtraq,8315; reference:cve,2000-0133; reference:cve,2001-1021; reference:cve,2003-0466; classtype:attempted-admin; sid:2389; rev:7;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP STOU overflow attempt"; flow:to_server,established; content:"STOU"; nocase; isdataat:100,relative; pcre:"/^STOU\s[^\n]{100}/smi";
  reference:bugtraq,8315; reference:cve,2003-0466; classtype:attempted-admin; sid:2390; rev:4;)
alert tcp any any -> any any (msg:"mpla mpla"; sid:1000001;)
alert tcp $HOME_NET 21 -> $EXTERNAL_NET any (msg:"ET SCAN Potential FTP Brute-Force attempt"; flow:from_server,established; content:"530 "; pcre:"/530\s+(Login|User|Failed|Not)/smi";
  classtype:unsuccessful-user; threshold: type threshold, track by_dst, count 1, seconds 30; sid:2002383; rev:10; fwsam: dst, 24 hours
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP APPE overflow attempt"; flow:to_server,established; content:"APPE"; nocase; isdataat:100,relative; pcre:"/^APPE\s[^\n]{100}/smi";
  reference:bugtraq,8315; reference:bugtraq,8542; reference:cve,2000-0133; reference:cve,2003-0466; classtype:attempted-admin; sid:2391; rev:7;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP RETR overflow attempt"; flow:to_server,established; content:"RETR"; nocase; isdataat:100,relative; pcre:"/^RETR\s[^\n]{100}/smi";
  reference:bugtraq,8315; reference:cve,2003-0466; reference:cve,2004-0287; reference:cve,2004-0298; classtype:attempted-admin; sid:2392; rev:7;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP STOR overflow attempt"; flow:to_server,established; content:"STOR"; nocase; isdataat:100,relative; pcre:"/^STOR\s[^\n]{100}/smi";
  reference:bugtraq,8668; reference:cve,2000-0133; classtype:attempted-admin; sid:2343; rev:3;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP CEL overflow attempt"; flow:to_server,established; content:"CEL"; nocase; isdataat:100,relative; pcre:"/^CEL\s[^\n]{100}/smi";
  reference:arachnids,257; reference:bugtraq,679; reference:cve,1999-0789; reference:nessus,10009; classtype:attempted-admin; sid:337; rev:12;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP XCWD overflow attempt"; flow:to_server,established; content:"XCWD"; nocase; isdataat:100,relative; pcre:"/^XCWD\s[^\n]{100}/smi";
  reference:bugtraq,8704; reference:bugtraq,11542; classtype:attempted-admin; sid:2344; rev:2;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP CWD overflow attempt"; flow:to_server,established; content:"CWD"; nocase; isdataat:100,relative; pcre:"/^CWD\s[^\n]{100}/smi"; reference:bugtraq,
  1227; reference:bugtraq,1690; reference:bugtraq,6869; reference:bugtraq,7251; reference:bugtraq,7950; reference:bugtraq,11069; reference:cve,1999-0219; reference:cve,1999-1058; reference:cve,-
  1999-1510; reference:cve,2000-1035; reference:cve,2000-1194; reference:cve,2001-0781; reference:cve,2002-0126; reference:cve,2002-0405; classtype:attempted-admin; sid:1919; rev:21;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP CMD overflow attempt"; flow:to_server,established; content:"CMD"; nocase; isdataat:100,relative; pcre:"/^CMD\s[^\n]{100}/smi";
  classtype:attempted-admin; sid:1621; rev:10;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP STAT overflow attempt"; flow:to_server,established; content:"STAT"; nocase; isdataat:100,relative; pcre:"/^STAT\s[^\n]{100}/smi";
  reference:bugtraq,3507; reference:bugtraq,8542; reference:cve,2001-0325; reference:cve,2001-1021; reference:url,labs.defcom.com/adv/2001/def-2001-31.txt; classtype:attempted-admin; sid:1379; rev:12;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE CHMOD overflow attempt"; flow:to_server,established; content:"SITE"; nocase; content:"CHMOD"; distance:0; nocase; isdataat:100,relative;
  pcre:"/^SITE\s+CHMOD\s[^\n]{100}/smi"; reference:bugtraq,10181; reference:bugtraq,9483; reference:bugtraq,9675; reference:cve,1999-0838; reference:nessus,12037; classtype:attempted-admin; sid:2340;
  rev:7;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE CHOWN overflow attempt"; flow:to_server,established; content:"SITE"; nocase; content:"CHOWN"; distance:0; nocase; isdataat:100,relative;
  pcre:"/^SITE\s+CHOWN\s[^\n]{100}/smi"; reference:bugtraq,2120; reference:cve,2001-0065; classtype:attempted-admin; sid:1562; rev:11;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE NEWER overflow attempt"; flow:to_server,established; content:"SITE"; nocase; content:"NEWER"; distance:0; nocase; isdataat:100,relative;
  pcre:"/^SITE\s+NEWER\s[^\n]{100}/smi"; reference:bugtraq,229; reference:cve,1999-0800; classtype:attempted-admin; sid:1920; rev:6;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE CPWD overflow attempt"; flow:established,to_server; content:"SITE"; nocase; content:"CPWD"; distance:0; nocase; isdataat:100,relative;
  pcre:"/^SITE\s+CPWD\s[^\n]{100}/smi"; reference:bugtraq,5427; reference:cve,2002-0826; classtype:misc-attack; sid:1888; rev:8;)
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE EXEC format string attempt"; flow:to_server,established; content:"SITE"; nocase; content:"EXEC"; distance:0; nocase; pcre:"/-
```

Παρακάτω θα εξηγήσουμε κάποιες άγνωστες λέξεις που βλέπουμε μέσα στους κανόνες.

PCRE: Το pcre λειτουργεί σαν εργαλείο ανίχνευσης συγκεκριμένων λέξεων/γραμμάτων, αναλόγως πως θα το ορίσουμε εμείς.

Classtype: Το classtype μας δείχνει τι τύπου είναι η δραστηριότητα που ψάχνουμε.

Content: Το content μας βοηθάει να βρούμε τα συγκεκριμένα μοτίβα που θέλουμε να ελέγξουμε αν εμπεριέχει το payload.

Isdataat: Το isdataat μας επιβεβαιώνει αν το payload είναι στην θέση που του δώσαμε.

Nocase: Με το nocase επιτυγχάνουμε να αναζητήσουμε συγκεκριμένο μοτίβο αγνοώντας κάθε περίπτωση.

Flow: Με το flow καταφέρνουμε να χρησιμοποιήσουμε τον κανόνα μόνο όταν εμείς θέλουμε μία συγκεκριμένη κυκλοφορία και όχι για κάθε κυκλοφορία.

Με τις παραπάνω πληροφορίες μπορούμε πλέον να αναλύσουμε κάποιους από τους κανόνες:

alert tcp $EXTERNAL_NET any -> $HOME_NET 3535 (msg:"FTP RMD / attempt"; flow:to_server,established; content:"RMD"; nocase; pcre:"/^RMD\s+\x2f$/smi"; reference:bugtraq,9159; classtype:attempted-dos; sid:2335; rev:2;) για παράδειγμα αυτός ο κανόνας ψάχνει συγκεκριμένο pattern σε επιθέσεις dos.

alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP large PWD command"; flow:to_server,established; dsize:10; content:"PWD"; nocase; classtype:protocol-command-decode; sid:1624; rev:6;) ο συγκεκριμένος κανόνας προσπαθεί να ανιχνεύσει τις επιθέσεις που προσπαθούν να αποσπάσουν πληροφορίες σχετικά με το path του προγράμματος.

alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP PASS overflow attempt"; flow:to_server,established,no_stream; content:"PASS"; nocase; isdataat:100,relative; pcre:"/^PASS\s[^\n]{100}/smi"; reference:bugtraq,10078; reference:bugtraq,10720; reference:bugtraq,1690; reference:bugtraq,3884; reference:bugtraq,8601; reference:bugtraq,9285; reference:cve,1999-1519; reference:cve,1999-1539; reference:cve,2000-1035; reference:cve,2002-0126; reference:cve,2002-0895; classtype:attempted-admin; sid:1972; rev:16;)
Και αυτό ο κανόνας κάνει alert για κάθε επίθεση μέσω overflow.

4.

Η αξιομνημόνευτη διαφορά του snort με το inline snort είναι πως το inline χρησιμοποιεί κάποια daq modules όπου είναι συσκευές οι οποίες ελέγχουν την ροή των πακέτων ανάμεσα στο computer και στον αισθητήρα. Κάποιες από τις δυνατότητές του είναι να κάνει drop τα πακέτα που θεωρεί πως δεν πρέπει να φτάσουν στο μηχάνημά μας και να τα φιλτράρει καλύτερα. Μερικά από τα modules που υποστηριζει το snort inline είναι τα afpacket-lpq-nfq-ip firewall.