



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Τμήμα Πληροφορικής



Εργασία Μαθήματος **Ασφάλεια Δικτύων**

Άσκηση <<αριθμός άσκησης>>	5- snort
Όνομα φοιτητή – Αρ. Μητρώου (όλων σε περίπτωση ομαδικής εργασίας)	Κουσουνής Κωνσταντίνος p14086
Ημερομηνία παράδοσης	04-06-2019

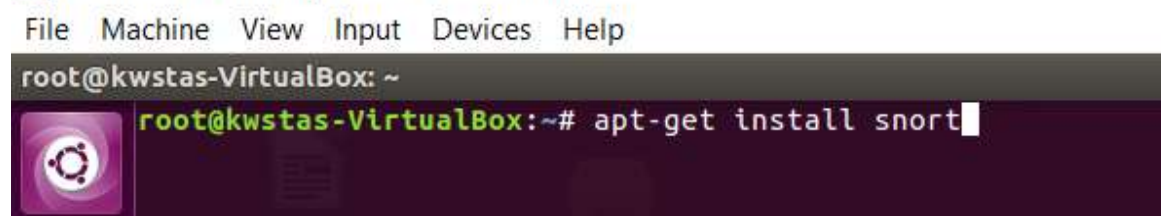


Εγκαταστήστε το λογισμικό ανίχνευσης εισβολών snort. Στη συνέχεια εκτελέστε τις ακόλουθες λειτουργίες:

- Γράψτε (ή ενεργοποιήστε) κανόνες για τις ακόλουθες ενέργειες:
- - Έλεγχος για XMAS scan από το εξωτερικό δίκτυο
 - Έλεγχος για SSH brute force attack και καταγραφή όσων IP διευθύνσεων κάνουν περισσότερες από 3 προσπάθειες σύνδεσης το λεπτό
- Ξεκινήστε το snort σε alert mode (snort -q -A console -i eth0 -c /etc/snort/snort.conf).
- Δοκιμάστε να κάνετε XMAS scan και SSH brute force ώστε να επαληθεύσετε τα alert.

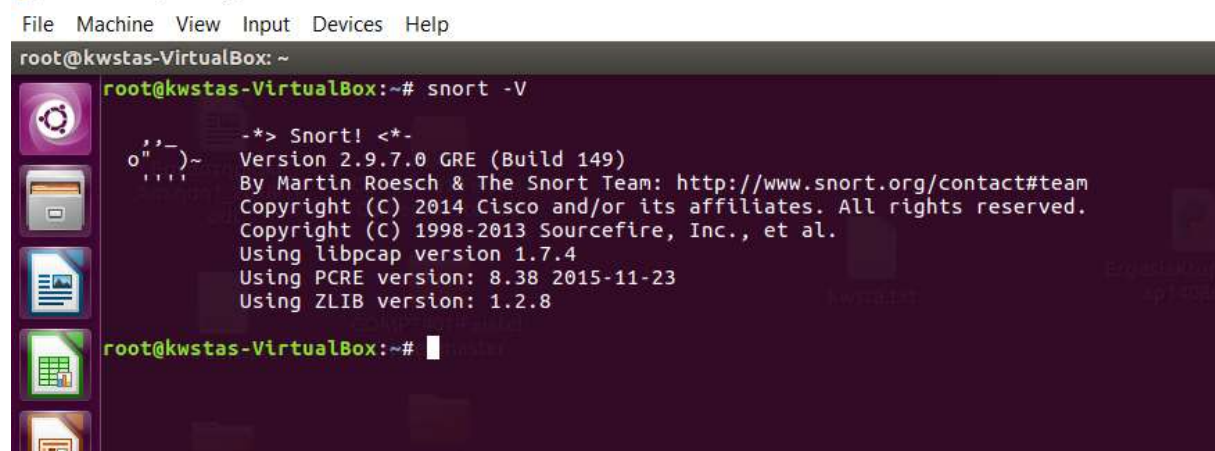
Εγκαταστήστε το λογισμικό ανίχνευσης εισβολών snort. Στη συνέχεια εκτελέστε τις ακόλουθες λειτουργίες:

Testbed [kallimig] - Oracle VM VirtualBox



Θα κάνουμε εγκατάσταση του snort σε ένα μηχάνημα kali Linux

Με την εντολή **apt-get install snort**



Βλέπουμε την έκδοση του snort που κάναμε εγκατάσταση με την εντολή **snort -V**.

Όπως βλέπουμε έχουμε την έκδοση snort 2.9.7.0.5



Κάναμε εγκατάσταση του snort σε ubuntu.

Γράψτε (ή ενεργοποιήστε) κανόνες για τις ακόλουθες ενέργειες:

- Έλεγχος για XMAS scan από το εξωτερικό δίκτυο

Όπως ξέρουμε η tcp επικοινωνία ακολουθεί τρεις διαφορετικούς τρόπους χειραψίας για να πραγματοποιηθεί η σύνδεση με ένα διαφορετικό μηχάνημα.

Στην συνέχεια ανοίγουμε το αρχείο που περιέχει τους κανόνες
/etc/snort/rules

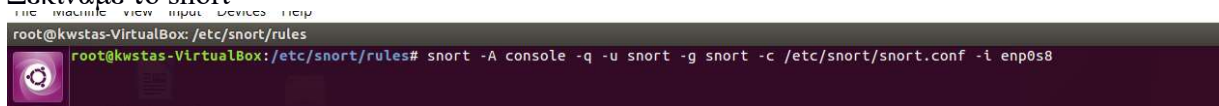
Ανοίγουμε το αρχείο **local.rules**

Δίνουμε την εντολή

alert tcp any any -> 192.168.205.5 22 (msg:"Nmap XMAS Tree Scan"; flags:FPU; sid:1000006; rev:1;)



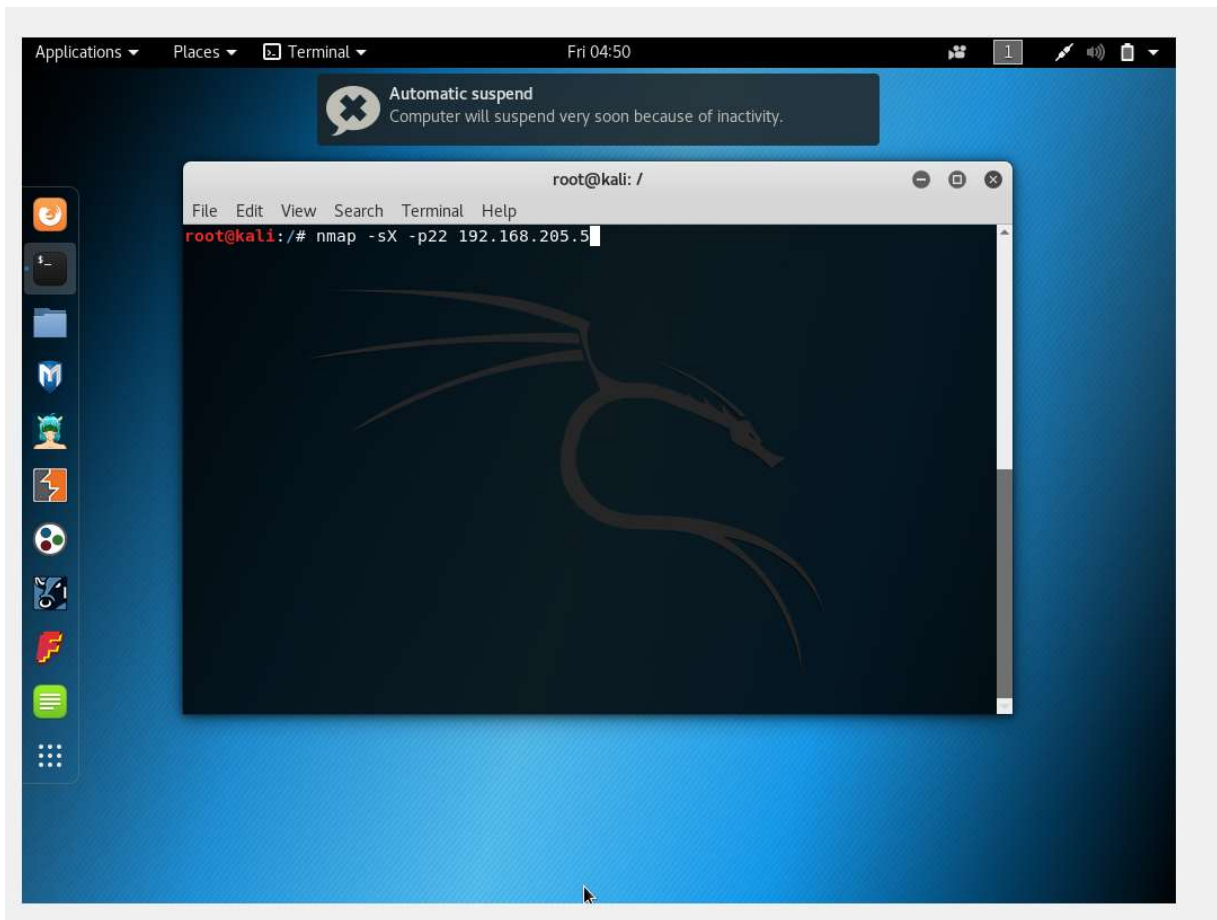
Ξεκινάμε το snort



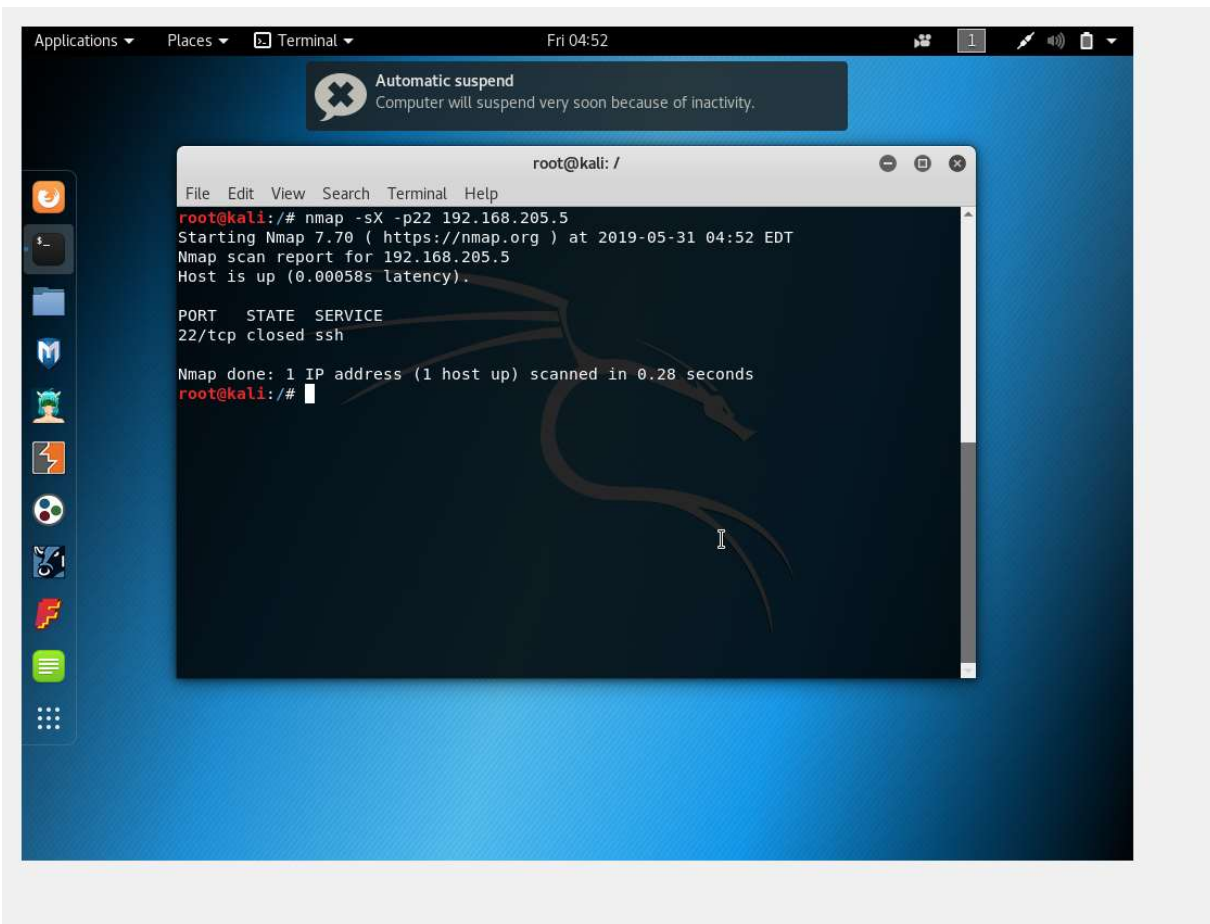
Snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -I enp0s8

S

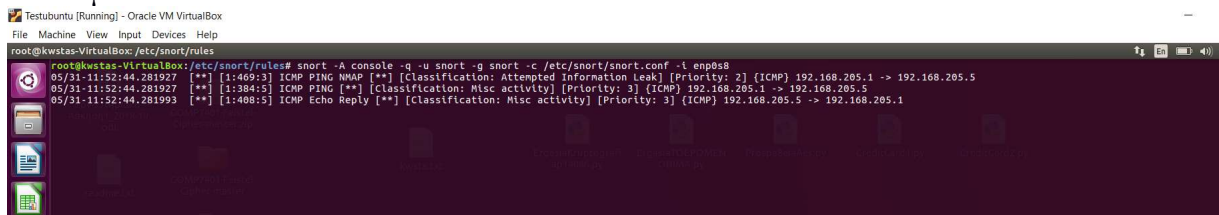
Ανοίγουμε ένα Kali Linux μηχάνημα που θα είναι ο επιτιθέμενος με ip διαφορετική του μηχανήματος μας.



Με την εντολή `nmap -sX -p22 192.168.205.5` κάνουμε xmas scan.



Κάναμε επίθεση στο μηχάνημα μας και αν πάμε στο θύμα στο ubuntu μηχάνημα μας μπορούμε να δούμε



Όπως βλέπουμε μας ενημερώνει ότι κάποιος χρησιμοποίησε το Nmap για να επικοινωνήσει με το μηχάνημα μας.



Έλεγχος για SSH brute force attack και καταγραφή όσων IP διευθύνσεων κάνουν περισσότερες από 3 προσπάθειες σύνδεσης το λεπτό.

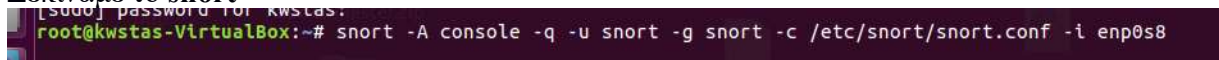
Δίνουμε την εντολή



```
alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"ET SCAN
Potential SSH Scan"; flow:to_server; flags:S,12; threshold: type both,
track by_src, count 3, seconds 60;
reference:url,en.wikipedia.org/wiki/Brute_force_attack;
reference:url,doc.emergingthreats.net/2001219; classtype:attempted-
recon; sid:2001219; rev:20; metadata:created_at 2010_07_30,
updated_at 2010_07_30;)
```

Ειδοποίηση όταν η συχνότητα συνδέσεων από μια συγκεκριμένη πηγή υπερβεί τις 3 συνδέσεις μέσα σε ένα λεπτό.

Ξεκινάμε το **snort**



Snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -I enp0s8



```
Applications ▾ Places ▾ Terminal ▾ Sat 05:10
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ssh -p 22 192.168.205.5
^Z
[4]+ Stopped                  ssh -p 22 192.168.205.5
root@kali:~# ssh -p 22 192.168.205.5
ssh: connect to host 192.168.205.5 port 22: Connection timed out
root@kali:~# ssh -p 22 192.168.205.5
root@192.168.205.5's password:
Permission denied, please try again.
root@192.168.205.5's password:
Permission denied, please try again.
root@192.168.205.5's password:
Permission denied (publickey,password).
root@kali:~# ssh -p 22 192.168.205.5
root@192.168.205.5's password:
Permission denied, please try again.
root@192.168.205.5's password:
Permission denied, please try again.
root@192.168.205.5's password:
Permission denied (publickey,password).
root@kali:~# ssh -p 22 192.168.205.5
^Z
[5]+ Stopped                  ssh -p 22 192.168.205.5
root@kali:~# ssh -p 22 192.168.205.5
^Z
[6]+ Stopped                  ssh -p 22 192.168.205.5
root@kali:~# ssh -p 22 192.168.205.5
```

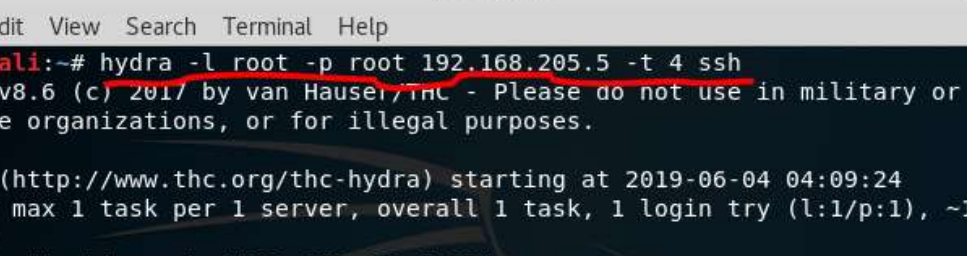
Κάνοντας από τον επιτιθέμενο μια ssh επίθεση μας ειδοποιεί το σύστημα μας.

```
Testubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kostas-VirtualBox: /etc/snort/rules# snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -l enp0s8
06/01-12:09:28.897386  [**] [1:2061219:20] ET SCAN Potential SSH Scan [**] [Classification: Attempted Information Leak] [Priority: 2] (TCP) 192.168.205.1:22050 -> 192.168.205.5:22
```

Στην συνέχεια με την βοήθεια του εργαλείου Hydra θα πραγματοποιήσουμε brute force επίθεση στο σύστημα μας.

Hydra -l root -p root 192.168.205.5 -t 4 ssh

Στην ip 192.168.205.5 πραγματοποιούμε επίθεση για να βρούμε τον κωδικό.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# hydra -l root -p root 192.168.205.5 -t 4 ssh  
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret  
service organizations, or for illegal purposes.  
  
Hydra (http://www.thc.org/thc-hydra) starting at 2019-06-04 04:09:24  
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try pe  
r task  
[DATA] attacking ssh://192.168.205.5:22/  
1 of 1 target completed, 0 valid passwords found  
Hydra (http://www.thc.org/thc-hydra) finished at 2019-06-04 04:09:26  
root@kali:~#
```

Όπως μπορούμε να δούμε το snort μας ειδοποιεί για την ssh επίθεση που γίνεται.