

2η ΕΡΓΑΣΙΑ ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ:

IP:83.212.110.46

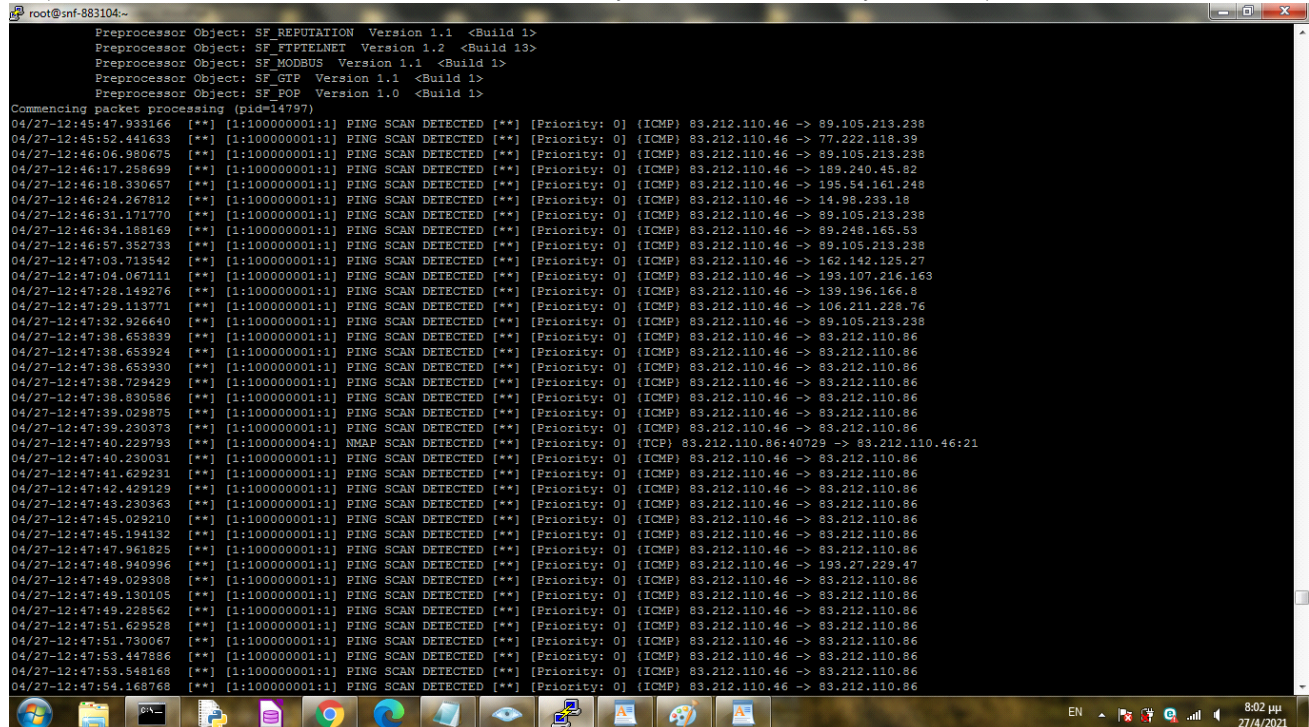
Άσκηση 1)

Ο κανόνας που χρησιμοποίησα ήταν ο:

```
alert icmp any any -> any any (msg:"PING SCAN  
DETECTED";sid:100000001;rev:001;).
```

Όπως φαίνεται και από το αρχείο rules που ανέβασα.

Παραθέτω τα screenshots και από τις δύο επιθέσεις που έγιναν:



```
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Commencing packet processing (pid=14797)
04/27-12:45:47.993166 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 89.105.213.238
04/27-12:45:52.441693 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 77.222.118.99
04/27-12:46:06.980675 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 89.105.213.238
04/27-12:46:17.258899 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 189.240.45.82
04/27-12:46:18.330657 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 195.54.161.248
04/27-12:46:24.267812 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 14.98.239.18
04/27-12:46:31.171770 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 89.105.213.238
04/27-12:46:34.188169 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 89.248.165.53
04/27-12:46:57.352733 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 89.105.213.238
04/27-12:47:03.713542 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 162.142.125.27
04/27-12:47:04.067111 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 193.107.216.163
04/27-12:47:28.149276 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 139.196.166.8
04/27-12:47:29.113771 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 106.211.228.76
04/27-12:47:32.926640 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 89.105.213.238
04/27-12:47:38.653839 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
04/27-12:47:38.653924 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
04/27-12:47:38.653930 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
04/27-12:47:38.729429 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
04/27-12:47:38.830586 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
04/27-12:47:39.029875 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
04/27-12:47:39.230373 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
04/27-12:47:40.229793 ** [1:100000004:1] NMAP SCAN DETECTED ** [Priority: 0] (TCP) 83.212.110.86:40729 -> 83.212.110.46:21
04/27-12:47:40.230031 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
04/27-12:47:41.629231 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
04/27-12:47:42.428129 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
04/27-12:47:43.230363 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
04/27-12:47:45.029210 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
04/27-12:47:45.194132 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
04/27-12:47:47.961825 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
04/27-12:47:48.940996 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 193.27.229.47
04/27-12:47:49.029308 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
04/27-12:47:49.130105 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
04/27-12:47:49.228562 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
04/27-12:47:51.629528 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
04/27-12:47:51.730067 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
04/27-12:47:53.447886 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
04/27-12:47:53.548168 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
04/27-12:47:54.168768 ** [1:100000001:1] PING SCAN DETECTED ** [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
```


ping.
Όπως βλέπουμε λ

Άσκηση 2)

Στην 2 χρησιμοποίησα τους 2 κανόνες

```
alert tcp any any -> any 443 (msg:"HTTPS  
DETECTED";content:"admin@site.gr";sid:100000002;rev:001;)
```

```
alert tcp any any -> any 80 (msg:"HTTP  
DETECTED";content:"admin@site.gr";sid:100000003;rev:001;)
```

Ο λόγος που χρησιμοποίησα δύο κανόνες ήταν διότι τα http,https έχουν διαφορετικό port destination 443,80 αντίστοιχα.Οπότε θεώρησα ως πιο σωστό να γράψω δυο κανόνες που να συμπεριελάμβανε και τις δύο πόρτες για να λάβω υπόψη μου όλες τις περιπτώσεις.Στο content έβαλα "admin@site.gr" καθώς θέλουμε να ανιχνεύσουμε πακέτο προς http,https και περιλαμβάνει payload στο "admin@site.gr".

Κάποια screenshot που μου εμφανίστηκαν στην επίθεση είναι:

```
04/27-12:47:54.356512  [**] [1:100000006:1] SCAN DETECTED [**] [Priority: 0] (ICMP) 83.212.110.46 -> 195.251.255.77  
04/27-12:47:54.356512  [**] [1:100000001:1] PING SCAN DETECTED [**] [Priority: 0] (ICMP) 83.212.110.46 -> 195.251.255.77  
04/27-12:47:55.629088  [**] [1:100000001:1] PING SCAN DETECTED [**] [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86  
04/27-12:47:56.829298  [**] [1:100000001:1] PING SCAN DETECTED [**] [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86  
04/27-12:47:57.049496  [**] [1:100000003:1] HTTP DETECTED [**] [Priority: 0] (TCP) 195.251.255.77:52767 -> 83.212.110.46:80  
04/27-12:47:57.049736  [**] [1:100000006:1] SCAN DETECTED [**] [Priority: 0] (ICMP) 83.212.110.46 -> 195.251.255.77  
04/27-12:47:57.049736  [**] [1:100000001:1] PING SCAN DETECTED [**] [Priority: 0] (ICMP) 83.212.110.46 -> 195.251.255.77  
04/27-12:47:57.111443  [**] [1:100000002:1] HTTPS DETECTED [**] [Priority: 0] (TCP) 195.251.255.77:52767 -> 83.212.110.46:443
```

```
04/27-12:58:56.613521  [**] [1:100000001:1] PING SCAN DETECTED [**] [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86  
04/27-12:58:57.714617  [**] [1:100000001:1] PING SCAN DETECTED [**] [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86  
04/27-12:58:59.207899  [**] [1:100000003:1] HTTP DETECTED [**] [Priority: 0] (TCP) 195.251.255.77:35304 -> 83.212.110.46:80  
04/27-12:58:59.208126  [**] [1:100000006:1] SCAN DETECTED [**] [Priority: 0] (ICMP) 83.212.110.46 -> 195.251.255.77  
04/27-12:58:59.208126  [**] [1:100000001:1] PING SCAN DETECTED [**] [Priority: 0] (ICMP) 83.212.110.46 -> 195.251.255.77  
04/27-12:58:59.250758  [**] [1:100000002:1] HTTPS DETECTED [**] [Priority: 0] (TCP) 195.251.255.77:35304 -> 83.212.110.46:443
```

όπου φαίνονται οι επιθέσεις http,https.

Άσκηση 3)

Στην άσκηση 3 ο κανόνας που χρησιμοποίησα ήταν:

```
alert tcp any any -> any 21 (msg:"NMAP SCAN  
DETECTED";flags:S;sid:100000004;rev:001;).
```

Σαν port destination έβαλα 21 καθώς στην άσκηση υπάρχει περιορισμός να εμφανίζονται max 10 alerts σε κάθε scan.Σκεπτόμενος ότι αν έπιανα και τις 100 πόρτες τότε για κάθε scan θα εμφανιζόντουσαν πάρα πολλά alerts το οποίο δεν το θέλουμε στην προκειμένη περίπτωση.Ετσι,θεώρησα ως καλύτερη προσέγγιση να πάρω μια τυχαία από τις 100 τις πιο γνωστές που σκανάρει το NMAP για αυτό τον λόγο διάλεξα την port 21.

Ακολουθεί screenshot με το μήνυμα(NMAP SCAN DETECTED),που πληρεί τον περιορισμό των max 10 alerts.

```
04/27-12:47:39.029875  [**] [1:100000001:1] PING SCAN DETECTED [**] [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86  
04/27-12:47:39.230373  [**] [1:100000001:1] PING SCAN DETECTED [**] [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86  
04/27-12:47:40.229793  [**] [1:100000004:1] NMAP SCAN DETECTED [**] [Priority: 0] (TCP) 83.212.110.86:40729 -> 83.212.110.46:21  
04/27-12:47:40.230031  [**] [1:100000001:1] PING SCAN DETECTED [**] [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
```

Άσκηση 4)

Στην άσκηση 4 οι κανόνες που χρησιμοποίησα είναι:

```
alert tcp any any -> 195.251.248.0/21 any (msg:"SCAN
DETECTED";sid:100000005;rev:001;)
```

```
alert icmp any any -> 195.251.248.0/21 any (msg:"SCAN
DETECTED";sid:100000006;rev:001;)
```

Ο λόγος που χρησιμοποίησα δύο κανόνες είναι διότι η εκφώνηση λέει να ανιχνεύεται οποιοσδήποτε κίνηση προς την **ip 195.251.248.0/21**. Οπότε σκέφτηκα ότι έπρεπε να χρησιμοποιήσω δύο κανόνες.

A) Έναν κανόνα που να ανιχνεύει τα ping (Ο πρώτος κανόνας ICMP).

B) Έναν κανόνα που να ανιχνεύει τα scans tcp(Δεύτερος κανόνας TCP).

Σαν ip destination έβαλα την **ip 195.251.248.0/21** καθώς η εκφώνηση αναφέρει να ανιχνεύεται **οποιαδήποτε** κίνηση προς το ip range του ΟΠΑ (195.251.248.0/21).

Παραθέτω σε screenshot τα alerts που εμφανίστηκαν κατά την επίθεση.

```
04/27-12:58:56.494887 0000000006:1 SCAN DETECTED [**] [Priority: 0] (ICMP) 83.212.110.46 -> 195.251.255.77
04/27-12:58:56.494887 0000000001:1 PING SCAN DETECTED [**] [Priority: 0] (ICMP) 83.212.110.46 -> 195.251.255.77
04/27-12:58:56.613521 0000000001:1 PING SCAN DETECTED [**] [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
04/27-12:58:57.714617 0000000001:1 PING SCAN DETECTED [**] [Priority: 0] (ICMP) 83.212.110.46 -> 83.212.110.86
04/27-12:58:59.207899 0000000003:1 HTTP DETECTED [**] [Priority: 0] (TCP) 195.251.255.77:35304 -> 83.212.110.46:80
04/27-12:58:59.208126 0000000006:1 SCAN DETECTED [**] [Priority: 0] (ICMP) 83.212.110.46 -> 195.251.255.77
04/27-12:58:59.208126 0000000001:1 PING SCAN DETECTED [**] [Priority: 0] (ICMP) 83.212.110.46 -> 195.251.255.77
04/27-12:58:59.250758 0000000002:1 HTFS DETECTED [**] [Priority: 0] (TCP) 195.251.255.77:35304 -> 83.212.110.46:443
04/27-12:58:59.250953 0000000006:1 SCAN DETECTED [**] [Priority: 0] (ICMP) 83.212.110.46 -> 195.251.255.77
```

```
04/27-12:47:54.356332 [[**] [1:1000000001:1] PING SCAN DETECTED [[**] [Priority: 0] {ICMP} 195.251.255.77 -> 83.212.110.46  
04/27-12:47:54.356512 [[**] [1:1000000006:1] SCAN DETECTED [[**] [Priority: 0] {ICMP} 83.212.110.46 -> 195.251.255.77  
04/27-12:47:54.356512 [[**] [1:1000000001:1] PING SCAN DETECTED [[**] [Priority: 0] {ICMP} 83.212.110.46 -> 195.251.255.77  
04/27-12:47:55.629088 [[**] [1:1000000001:1] PING SCAN DETECTED [[**] [Priority: 0] {ICMP} 83.212.110.46 -> 83.212.110.86  
04/27-12:47:56.829298 [[**] [1:1000000001:1] PING SCAN DETECTED [[**] [Priority: 0] {ICMP} 83.212.110.46 -> 83.212.110.86  
04/27-12:47:57.049496 [[**] [1:1000000003:1] HTTP DETECTED [[**] [Priority: 0] {TCP} 195.251.255.77:52767 -> 83.212.110.46:80  
04/27-12:47:57.049736 [[**] [1:1000000006:1] SCAN DETECTED [[**] [Priority: 0] {ICMP} 83.212.110.46 -> 195.251.255.77  
04/27-12:47:57.049736 [[**] [1:1000000001:1] PING SCAN DETECTED [[**] [Priority: 0] {ICMP} 83.212.110.46 -> 195.251.255.77  
04/27-12:47:57.111443 [[**] [1:1000000002:1] HTTPS DETECTED [[**] [Priority: 0] {TCP} 195.251.255.77:52767 -> 83.212.110.46:443  
04/27-12:47:57.111643 [[**] [1:1000000006:1] SCAN DETECTED [[**] [Priority: 0] {ICMP} 83.212.110.46 -> 195.251.255.77
```

Άσκηση 5)

α) Σύμφωνα με τις διαφάνειες του μαθήματος του snort, αναφέρεται ότι υπάρχει κάποια προκαθορισμένη σειρά με την οποία το detection engine σκανάρει τους κανόνες. Αναλυτικότερα, η σειρά με την οποία σκανάρει τους κανόνες είναι: 1) alert 2) pass 3) log.

Οπότε ο κανόνας `pass ip any any -> any any (msg:"Allowed";sid:1001;)`

στην προκειμένη περίπτωση θα εκτελεστεί μετά το alert. Άρα λαμβάνοντας υπόψη όλα τα παραπάνω και να προστεθεί ο κανόνας αυτός **δεν θα έχει καμία επίδραση** στους δικούς μου κανόνες (alert).

 $\beta)$

Ο κανόνας λειτουργεί ως εξής:

Το drop στην αρχή του κανόνα κάνει block και log τα πακέτα. Αντίθετα, το alert εμφανίζει μια ειδοποίηση (alert) και στην συνέχεια κάνει log το πακέτο. Στην προκειμένη περίπτωση λοιπόν γίνονται block και μετά log τα αντίστοιχα πακέτα, τα οποία μπορούν να έρθουν από οποιαδήποτε ip, port source και destination. Στην ουσία λοιπόν ο συγκεκριμένος κανόνας θα μπλοκάρει το συγκεκριμένο tls.

