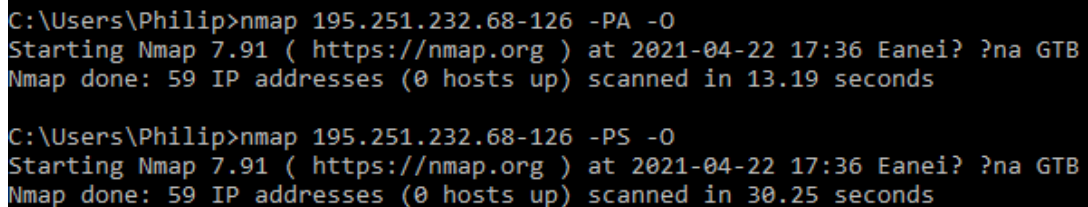


Ασφάλεια Δικτύων

Εργαστηριακή Άσκηση 1 (nmap)

1. Τα αποτελέσματα του scan για τον host περιλαμβάνουν τις θύρες που σκάνανε το nmap, την κατάστασή τους και την υπηρεσία (αν υπάρχει) που τρέχει σε κάθε μια από αυτές. Στο συγκεκριμένο output παρατηρούμε ότι οι TCP θύρες 22, 80 και 443 είναι ανοικτές και σε αυτές τρέχουν οι υπηρεσίες SSH, HTTP και HTTP αντίστοιχα. Τα βήματα του default scan είναι τα εξής:
 - i. Το nmap ελέγχει αν ο host είναι ενεργός στέλνοντας ένα ICMP Ping
 - ii. Εφόσον είναι ενεργός, εκτελεί ένα scan στις 1000 πιο γνωστές TCP θύρες.
2. Αρχικά εκτελέστηκαν οι εντολές *"nmap 195.251.232.68-126 -PA -O"* και *"nmap 195.251.232.68-126 -PS -O"*. Οι παράμετροι -PA και -PS χρησιμοποιήθηκαν ώστε το port scanning να γίνει και σε hosts που ενδεχομένως βρίσκονται πίσω από κάποιο firewall και δεν απαντούν σε ICMP Pings. Ωστόσο οι εντολές αυτές δεν επέστρεψαν αποτέλεσμα, όπως φαίνεται στην εικόνα. Έτσι τέλος χρησιμοποιήθηκε η εντολή *"nmap 195.251.232.68-126 -PN -O"*, ώστε να παραλειφθεί τελείως το βήμα του host discovery.
Το nmap μπορεί να εκτιμήσει ποιο ΛΣ τρέχει ένας host συγκρίνοντας τα αποτελέσματα του scan για εκείνον με γνωστά αποτυπώματα διαφόρων λειτουργικών συστημάτων και εξετάζοντας με ποια από αυτά ταιριάζει περισσότερο



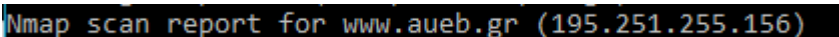
```
C:\Users\Philip>nmap 195.251.232.68-126 -PA -O
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-22 17:36 Eane1? ?na GTB
Nmap done: 59 IP addresses (0 hosts up) scanned in 13.19 seconds

C:\Users\Philip>nmap 195.251.232.68-126 -PS -O
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-22 17:36 Eane1? ?na GTB
Nmap done: 59 IP addresses (0 hosts up) scanned in 30.25 seconds
```

Εικόνα 1

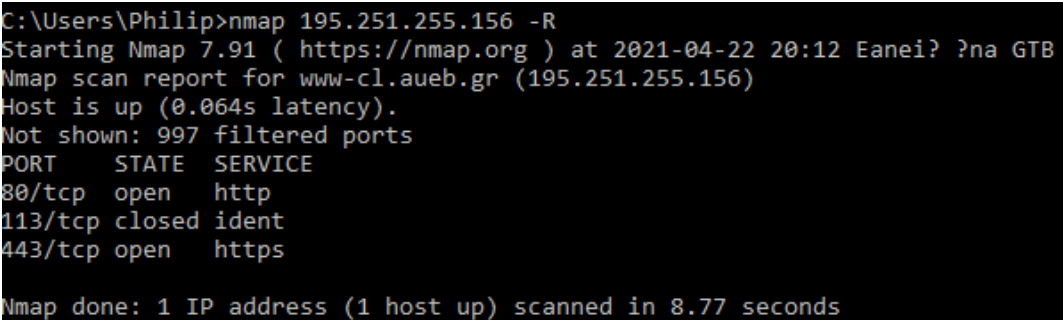
3. Η εντολή που χρησιμοποιήθηκε ήταν η *"nmap 195.251.248.128/25 -p 80"*
Οι διευθύνσεις IP των hosts που βρέθηκαν είναι οι εξής:
 - a. 195.251.248.140 (cslab.aueb.gr)
 - b. 195.251.248.143 (moniteur.aueb.gr)
 - c. 195.251.248.178 (cslab178.cs.aueb.gr)
 - d. 195.251.248.247 (cslab247.cs.aueb.gr)
 - e. 195.251.248.252 (cslab252.cs.aueb.gr)

Οι MAC διευθύνσεις δεν μπορούν να ανακτηθούν καθώς δεν βρισκόμαστε στο ίδιο υποδίκτυο που καθορίστηκε.
4. Χρησιμοποιώντας την παράμετρο -PN τα αποτελέσματα είναι περισσότερα καθώς παραλείπεται η φάση του host discovery και εκτελείται απευθείας το port scanning για όλους τους hosts που βρίσκονται στο υποδίκτυο. Έτσι επιστρέφονται και οι hosts που δεν απαντούν κανονικά σε Ping requests.

5. Η εντολή που εκτελέστηκε είναι η `"nmap 83.212.105.142 --spoof-mac 0"`
Η απόκρυψη της MAC κάνει πιο δύσκολο την ανακάλυψη της προέλευσης του scan αφού αποκρύπτει εν μέρει την ταυτότητα του μηχανήματός μας που το εκτελεί. Επίσης μας επιτρέπει να παρακάμπτουμε firewalls τα οποία ενδεχομένως δηλώνουν κανόνες για φιλτράρισμα των MAC διευθύνσεων.
Η MAC διεύθυνση μας στο ερώτημα 1 δεν ήταν ορατή από τον server καθώς βρίσκεται σε διαφορετικό LAN. Την αποκρύψαμε από τους υπόλοιπους υπολογιστές του υποδικτύου και κατ' επέκταση από το ρούτερ μας που τη χρησιμοποιεί για την δρομολόγηση της κίνησης εντός αυτού.
6. Η εντολή που χρησιμοποιήθηκε είναι η `"nmap www.aueb.gr"`
Η IP του ιστοτόπου είναι 195.251.255.156, όπως φαίνεται στην εικόνα.


Εικόνα 2

7. Εκτελέστηκαν οι εντολές `"nmap www.aueb.gr -R"` και στη συνέχεια η `"nmap 195.251.255.156 -R"`. (Σημειώνεται ότι η δεύτερη δεν έχει καταγραφεί στο αρχείο των scans)
Τα αποτελέσματα και των δύο εντολών είναι πανομοιότυπα με τα αποτελέσματα της προηγούμενης άσκησης, καθώς αφορούν τον ίδιο host, με τη διαφορά ότι ως domain name αναφέρεται το `www-cl.aueb.gr`. Κατά το rDNS Lookup γίνεται αναζήτηση για το όνομα του host με διεύθυνση 195.251.255.156 και επιστρέφεται το `www-cl.aueb.gr`, διότι σε εκείνο δείχνει ο pointer για τη συγκεκριμένη διεύθυνση στις εγγραφές του DNS Server.



```
C:\Users\Philip>nmap 195.251.255.156 -R
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-22 20:12 Eaneī? ?na GTB
Nmap scan report for www-cl.aueb.gr (195.251.255.156)
Host is up (0.064s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp    open  https

Nmap done: 1 IP address (1 host up) scanned in 8.77 seconds
```

Εικόνα 3