1η ΕΡΓΑΣΙΑ ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ:

1)
α)
Με την εντολή nmap IP σκανάρουμε την δωσμένη IP αν είναι ανοιχτή.Ο τρόπος για να δούμε άν είναι ανοιχτή στέλνεται ένα ping αίτημα στην συγκεκριμένη IP και πρέπει να υπάρξει απάντηση για να βεβαιώσουμε ότι η IP είναι ανοιχτή.Αν η IP είναι ανοιχτή σκανάρονται οι TCP PORTS(kAI OI 1000).Από τα αποτελέσματα λοιπόν βλέπουμε οτι η ip είναι ανοιχτή(HOST IS UP).Επίσης,πραγματοποιώντας το σκανάρισμα και στις 1000 TCP PORTS βλέπουμε ότι μόνο 3 πόρτες είναι ανοιχτές.Το οποίο φαίνεται και από το state τους αλλά επίσης και απο το μήνυμα (NOT SHOWN) που εμφανίζει ποιες πόρτες είναι κλειστές.Στην προκειμένη περίπτωση οι κλειστές πόρτες είναι 997.

2)
Οι εντολές που χρησιμοποιήσα,ήταν οι:nmap -O -PN 195.251.232.68-126.

Ο τρόπος εντοπισμού του λειτουργικού συστήματος γίνεται ως εξής:
Με την εντολή OS DETECTION στέλνονται TCP,UDP πακέτα στο απομακρυσμένο host.Στην συνέχεια το NMAP τσεκάρει ένα-ένα τα bits που έρχονται ώς απάντηση.Στην συνέχεια το NMAP συγκρίνει τα αποτελέσματα με το -os database και ελέγχει αν ταιριάζουν.Κάθε fingerprint στην ουσία περίεχει μία φόρμα περιγραφής του OS και ένα classification που μας δίνει πληροφορίες για το vendor name,underlying OS,OS generation καθώς και για τον τύπο της συσκευής.

Η εντολή -PN στην ουσία παραλείπει το βήμα να ελέγξει αν η IP είναι ανοιχτή και πάει κατευθείαν να δει αν το HOST είναι UP.

3)Η εντολή που χρησιμοποιήσα ήταν:nmap -p 80 195.251.248.128/25

Για κάθε ένα από τα αποτελέσματα οι IP ADDRESSES φαίνονται παρακάτω:
a)cslab.aueb.gr (195.251.248.140)
b)moniteur.aueb.gr (195.251.248.143)
c)cslab178.cs.aueb.gr (195.251.248.178)
d)cs.aueb.gr (195.251.248.247)
e)cslab252.cs.aueb.gr (195.251.248.252)
Με κόκκινο χρώμα είναι οι IP

Τα windows είναι:2
και τα linux:9 το οποίο φαίνεται από την εντολή Running (JUST GUESSING)

4)
Η εντολη nmap IP και η -PN διαφέρουν στα εξής σημεία.
Η απλή εντολή NMAP στέλνει αίτημα ping στην IP και περιμένει να απαντήσει για να δεί αν είναι ανοιχτή ή όχι.Στην συνέχεια αν είναι ανοιχτή κάνει tcp port scanning εμφανίζοντας τις ανοιχτες tcp ports.

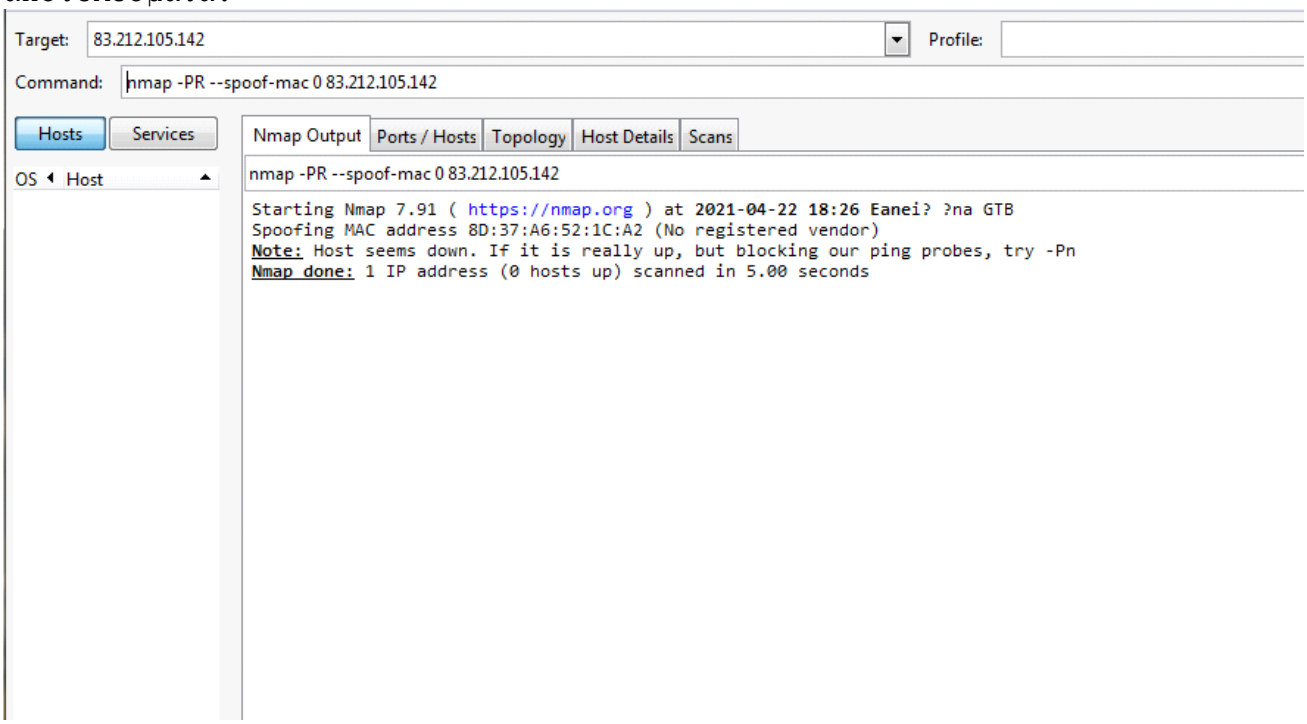
Αντίθετα, η εντολη -PN(NO PING) κάνει port scanning παραλείποντας να ελέγξει αν η IP είναι ανοιχτή πραγματοποιώντας μόνο έλεγχο για να δει αν το host είναι UP ή όχι.

Στην ουσία η εντολή -PN ειναι αρκετά χρήσιμη καθως με την απλή εντολή nmap μπορεί να υπάρχει firewall μεταξύ εμάς και του host ή ακόμα και ο host ναι

κλειστός καθώς επίσης και να μην υπάρχει ανταπόκριση.Οπότε για αυτό το -PN είναι μία πολυ χρήσιμη εντολή.

5)

Η εντολή που χρησιμοποιήσα ήταν η:nmap -PR 83.212.105.142
Καθώς απο ψάξιμο σε διάφορες πηγές αναφερόταν ότι mac spoofing μπορούσε να πραγματοποιηθεί με ένα ARP PING SCAN.Ωστόσο μετά από λίγο παρατήρησησα ότι έπρεπε να προστεθεί και η εντολή --spoof -mac0,αλλά δυστηχώς δεν πρόλαβα την προθεσμία και δεν κατάφερα να το συμπεριλάβω στα σκαναρίσματα του zip αρχείου.Τρέχοντας ωστόσο την ολοκληρωμένη εντολή στο zenmap είχα τα εξής αποτελέσματα.

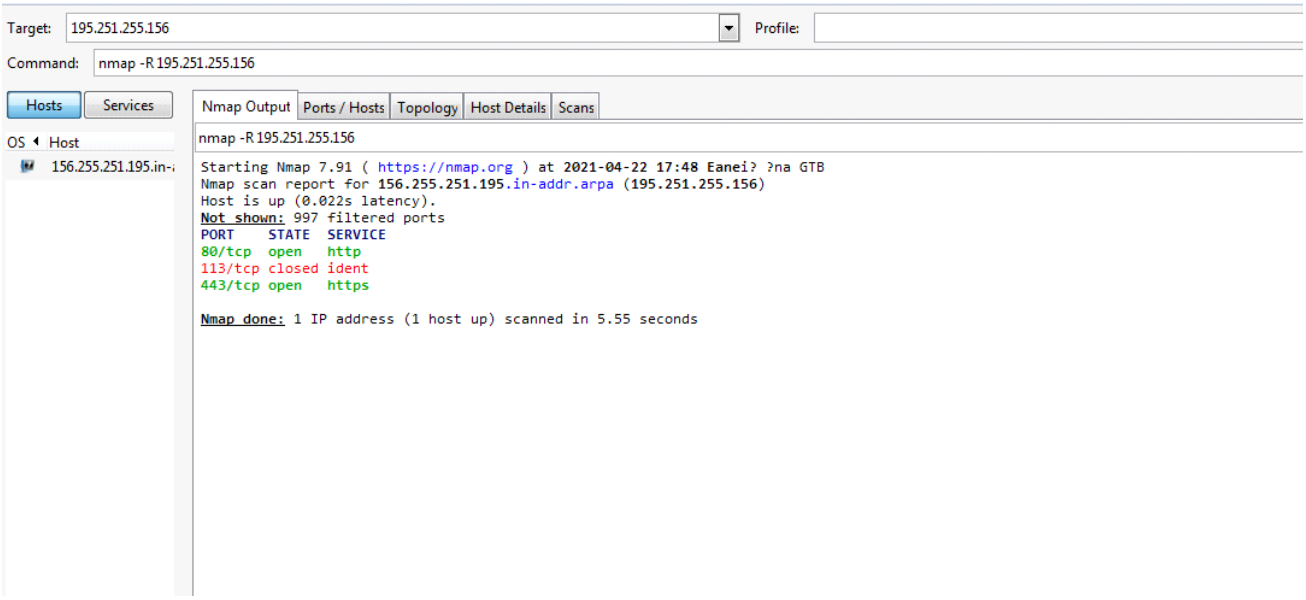


Πλεονεκτήματα:
Η MAC διεύθυνση είναι ορατή στο τοπικό δίκτυο.Οπότε πραγματοποιώντας mac spoofing κατα κάποιο τρόπο κρύβω την ταυτοτήτά μου.

Στο ερώτημα 1 η MAC ADDRESS δεν είναι ορατή στην IP ADDRESS:83.212.105.142 και την αποκρύψαμε από το τοπικό μας δίκτυο.

6)Η εντολή που χρησιμοποιήσα ήταν η:nmap -sL www.aueb.gr,όπου στην ουσία σκανάρεται το domain name του www.aueb.gr και βρίσκεται η ip του.
Η ip του www.aueb.gr είναι:www.aueb.gr (195.251.255.156).

7)Η εντολή που χρησιμοποιήσα ήταν:



Σε αναζήτηση που πραγματοπιήσα στο internet διαπίστωσα ότι η εντολή για να πραγματοποιήσω reverse DNS είναι η nmap -R IP

-R (DNS resolution for all targets)

Tells Nmap to *always* do reverse DNS resolution on the target IP addresses. Normally reverse DNS is only performed against responsive (online) hosts.

Στην ουσία με το reverse DNS είναι η τακτική που προσδιορίζεται το domain name στην προκειμένη περίπτωση το www.aueb.gr μέσα από την IP.Δηλαδή,μέσα απο την ip να οδηγούμε στο domain name.

Ωστόσο,παρά το ψάξιμο που έκανα στο internet και βάζοντας την εντολή που βρήκα στο ZenMap παρατήρησα ότι η ip που βρήκα για το www.aueb.gr δεν με οδηγεί στο συγκεκριμένο domain name.