Ασφάλεια Δικτύων

Εργαστηριακή Άσκηση 1 (nmap)

Διογένης Τσολάκου - 3170164

1) Το συγκεκριμένο scan μας δείχνει τα open ports του στόχου (host) που προσδιορίσαμε, αποκρύπτοντας όσα ports είναι filtered.

Ο τρόπος που λειτουργεί στη συγκεκριμένη περίπτωση είναι ο εξής :

1. Επειδή δίνουμε IP address δεν κάνει DNS lookup.

2. Κάνει ping τον στόχο με ένα πακέτο ICMP echo request κι ένα TCP ACK στην θύρα 80

3. Κάνει ένα TCP port scan στις 1000 πιο δημοφιλής σύμφωνα με το nmap-services

4. Τέλος τυπώνει τα αποτελέσματα

Αυτά τα βήματα μπορούμε επίσης να τα δούμε προσθέτοντας την παράμετρο "-v", δηλαδή verbose ώστε να τυπώσει περισσότερες λεπτομέρειες το scan.

2) Για το συγκεκριμένο scan χρησιμοποιήθηκε η εντολή :

nmap -O -Pn 195.251.232.68-126

ώστε να κάνουμε OS detection με το -O και χωρίς host discovery με -Pn.

Συνολικά υπήρχαν 2 host με Windows και 9 με Linux. Ως Linux θεωρήθηκαν και κάποιοι host που είχαν αναγνωριστεί και ως Grandstream embedded καθώς είχαν ίδιο ποσοστό matching (86%).

Ο τρόπος με τον οποίο το nmap αναγνωρίζει το OS (fingerprinting) είναι η ανάλυση κάθε bit των απαντήσεων που στέλνει ο στόχος ώστε να βρει

ιδιαιτερότητες σε αυτές τις απαντήσεις και να τις συγκρίνει με τη βάση δεδομένων του.

3) Η εντολή που χρησιμοποιήθηκε ήταν η :

nmap -p 80 195.251.248.128/25

Από τις 128 IP διευθύνσεις 5 hosts ήταν up και οι IP τους ήταν οι εξής :

- 195.251.248.140

- 195.251.248.143 , η port 80 ήταν filtered

- 195.251.248.178

- 195.251.248.247 , η port 80 ήταν κλειστή

- 195.251.248.252

Ο λόγος που δεν βλέπουμε MAC διευθύνσεις είναι καθώς για να δούμε MAC διευθύνσεις πρέπει να κάνουμε scan σε επίπεδο τοπικού δικτύου, layer 2, από τη στιγμή που τα πακέτα μας πάνε σε απομακρυσμένο host μέσω του router γίνονται layer 3 και δεν μπορούμε να δούμε την MAC του host.

4) Με την παράμετρο -Pn το nmap δεν θα κάνει ping, αλλά θα κάνει SYN scan που είναι λιγότερο "θορυβώδες", τους host και τους θεωρεί όλους up, οπότε εκτός από τις 5 διευθύνσεις που μας επέστρεψε στο (3), που ήταν όντως up, θα μας επιστρέψει όλες τις 128 διευθύνσεις με τις port 80 ως filtered.

5) Η εντολή που εκτελέστηκε ήταν η εξής :

nmap --spoof-mac 0 83.212.105.142

Η απόκρυψη της MAC στη συγκεκριμένη περίπτωση δεν μας προσφέρει κάποιο πλεονέκτημα μιας και όπως αναφέρθηκε παραπάνω τα πακέτα πάνε σε

απομακρυσμένο host. Σε άλλες περιπτώσεις, όπως π.χ. την διείσδυση σε τοπικό δίκτυο ενός οργανισμού είτε μας δίνει πρόσβαση αν αυτή έχει περιοριστεί σε συγκεκριμένες διευθύνσεις MAC είτε αποποιούμαστε της ευθύνης μιας και η συσκευή μας έχει διαφορετική πραγματική MAC.

Όπως αναφέρθηκε η MAC εμφανίζεται μόνο σε layer 2, οπότε στο (1) ο server δεν έβλεπε την MAC μας, σ' αυτό το ερώτημα την αποκρύψαμε από το router.

6) Η εντολή που εκτελέστηκε ήταν η εξής :

nmap --traceroute www.aueb.gr

και η IP είναι η 195.251.255.156

Απλούστερα θα μπορούσε να είχε χρησιμοποιηθεί η παράμετρος -sL αντί της --traceroute.

7) Η εντολή που χρησιμοποιήθηκε ήταν η εξής :

nmap -R --system-dns 195.251.255.156

Το αποτέλεσμα στο οποίο καταλήγουμε είναι το www-cl.aueb.gr αντί του www.aueb.gr που δώσαμε στο (6). Αυτό συμβαίνει καθώς μας επιστρέφει την reverse DNS εγγραφή που αντιστοιχεί στην IP.