Contents

Σύνοψη Απαιτήσεων

- Διατίθενται προς χρήση 126 συνολικά διευθύνσεις, που κυμαίνονται από 83.112.8.128 έως 83.112.8.255.
- Τμήματα: Πέντε
- Κεντρικοί υπολογιστές τουλάχιστον ανά τμήμα: 12

Στρατηγικές για υποδικτύωση

Πρέπει να λάβουμε υπόψη ένα μέγεθος υποδικτύου που επιτρέπει τουλάχιστον 14 διευθύνσεις (12 κεντρικούς υπολογιστές + 2 για δίκτυο και μετάδοση) προκειμένου να υποστηρίζονται επιπλέον τουλάχιστον 12 κεντρικοί υπολογιστές σε κάθε τμήμα σε επιπλέον διευθύνσεις για διευθύνσεις δικτύου και εκπομπής σε κάθε υποδίκτυο.

Υπολογισμός του μικρότερου υποδικτύου

Ένα /28 υποδίκτυο είναι το μικρότερο υποδίκτυο που υποστηρίζει 14 διευθύνσεις και προσφέρει τις ακόλουθες δυνατότητες:

- Μάσκα υποδικτύου: 255.255.255.240
- Δίκτυα: 16 διευθύνσεις συνολικά — 14 χρησιμοποιήσιμες + 2 για δίκτυο και εκπομπή

Εκχώρηση υποδικτύων:

Ας υπολογίσουμε πόσα από αυτά τα υποδίκτυα μπορούν να χωρέσουν στο δίκτυό μας /25, δεδομένου του μεγέθους υποδικτύου /28:Οκτώ υποδίκτυα συνολικά είναι δυνατά (που κυμαίνονται από /25 έως πολλαπλά /28s).Έτσι, μπορούμε να χωρίσουμε το δίκτυό μας /25 σε οκτώ πιο διαχειρίσιμα /28 δίκτυα. Με πέντε από αυτά τα υποδίκτυα που χρησιμοποιούνται για τα τμήματα και άλλα τρία υποδίκτυα διαθέσιμα για οποιαδήποτε μελλοντική τμηματοποίηση (όπως διαχείριση IT, Wi-Fi επισκέπτη ή επέκταση), καθένα από αυτά τα υποδίκτυα θα είναι περισσότερο από αρκετό για να καλύψει τις ανάγκες κάθε τμήματος.

Παράδειγμα, Μονάδα διαμόρφωσης υποδικτύου

- Τμήμα 1: 83.112.8.128/28

83.112.8.129 - 83.112.8.142 είναι το χρησιμοποιήσιμο εύρος.

- Τμήμα 2: 83.112.8.144/28 είναι ο κωδικός του τμήματος.

83.112.8.145–83.112.8.158 είναι το χρησιμοποιήσιμο εύρος.

- Τμήμα 3: 83.112.8.160/28 είναι ο κωδικός του τμήματος.

Το χρησιμοποιήσιμο εύρος είναι 83.112.8.161 έως 83.112.8.174

- Τμήμα 4: 83.112.8.176/28
  83.112.8.177 - 83.112.8.190 είναι το χρησιμοποιήσιμο εύρος
- Τμήμα 5: 83.112.8.192/28

Εύρος χρήσης: 83.112.8.193 έως 83/112.8.206.

Οι υπόλοιπες διευθύνσεις, οι οποίες είναι 83.112.8.208/28 έως 83.112.8.255, μπορούν πλέον να χρησιμοποιηθούν για διαφορετικές χρήσεις.

Συνοψίζοντας

Η μάσκα υποδικτύου **255.255.255.240 (/28)** κάνει αποτελεσματική χρήση του διαθέσιμου εύρους διευθύνσεων IP, επιτρέπει μελλοντική τμηματοποίηση ή επέκταση δικτύου και προσφέρει την απαιτούμενη ευαισθησία για την κάλυψη της απαίτησης κάθε τμήματος για τουλάχιστον 12 κεντρικούς υπολογιστές. Με την εγγύηση ότι κάθε τμήμα έχει ένα αποκλειστικό τμήμα δικτύου, αυτή η διαμόρφωση βελτιώνει τη διαχειρισιμότητα και την ασφάλεια του συνολικού σχεδιασμού του δικτύου. Με βάση την επιλογή μας να χρησιμοποιήσουμε υποδίκτυα /28 εντός του μεγαλύτερου δικτύου /25, ας δούμε τις ιδιαιτερότητες των διευθύνσεων δικτύου για κάθε ένα από τα πέντε τμήματα. 16 διευθύνσεις IP μπορούν να φιλοξενηθούν από κάθε υποδίκτυο /28, εκ των οποίων οι 14 μπορούν να χρησιμοποιηθούν από κεντρικούς υπολογιστές μετά την αφαίρεση των διευθύνσεων δικτύου και εκπομπής.

Ανάλυση της εκχώρησης υποδικτύου /28

Θα ξεκινήσουμε τον υποδικτύωμα στο 83.112.8.128, την αρχή του μπλοκ /25 που μας έχει εκχωρηθεί. Αυτός είναι ο τρόπος με τον οποίο εκχωρείται και υπολογίζεται κάθε υποδίκτυο:

Τμήμα 1: 83.112.8.128/28

- Διεύθυνση δικτύου: 83.112.8.128
- Εύρος χρησιμοποιήσιμων κεντρικών υπολογιστών: 83.112.8.129–83.112.8.142
- Διεύθυνση Broadcast: 83.112.8.143

Τμήμα 2: 83.112.8.144/28 είναι ο κωδικός του τμήματος.

- Διεύθυνση δικτύου: 83.112.8.144
- Το εύρος των χρησιμοποιήσιμων κεντρικών υπολογιστών είναι 83.112.8.145 έως 83.112.8.158.
- Διεύθυνση εκπομπής: 83.112.8.159

Τμήμα3: 83.112.8.160/28 είναι ο κωδικός του τμήματος.

- Εύρος κεντρικού υπολογιστή που μπορεί να χρησιμοποιηθεί: 83.112.8.161 έως 83.112.8.174
- Διεύθυνση δικτύου: 83.112.8.160
- Διεύθυνση Broadcast: 83.112.8.175

Τμήμα 4:Κωδικός τμήματος 83.112.8.176/28

- Διεύθυνση δικτύου: 83.112.8.176
- Εύρος χρησιμοποιήσιμων κεντρικών υπολογιστών: 83.112.8.177 έως 83.112.8.190
- Διεύθυνση εκπομπής: 83.112.8.191

Τμήμα 5: 83.112.8.192/28

- Διεύθυνση Δικτύου: 83.112.8.192
- Εύρος κεντρικού υπολογιστή που μπορεί να χρησιμοποιηθεί: 83.112.8.193 to 83.112.8.206
- Διεύθυνση broadcast: 83.112.8.207

Επεξήγηση των υπολογισμών

1. **Μέγεθος υποδικτύου**: Υπάρχουν 16 διευθύνσεις IP σε κάθε υποδίκτυο /28.
2. **Διευθύνσεις εκπομπής και δικτύου**: Κάθε υποδίκτυο έχει μια δεσμευμένη διεύθυνση για το δίκτυο στην αρχή και μια διεύθυνση εκπομπής στο τέλος.
3. **Χρησιμοποιήσιμες διευθύνσεις κεντρικού υπολογιστή**: Οι κεντρικοί υπολογιστές μπορούν να χρησιμοποιούν διευθύνσεις που βρίσκονται μεταξύ των διευθύνσεων εκπομπής και του δικτύου.
4. **Αύξηση**: Κάθε νέο υποδίκτυο ξεκινά αμέσως μετά τη διεύθυνση εκπομπής του προηγούμενου υποδικτύου.

83.112.8.128/28 - Network 1: 83.112.8.128 to 83.112.8.143 (Department 1)
83.112.8.144/28 - Network 2: 83.112.8.144 to 83.112.8.159 (Department 2)
83.112.8.160/28 - Network 3: 83.112.8.160 to 83.112.8.175 (Department 3)
83.112.8.176/28 - Network 4: 83.112.8.176 to 83.112.8.191 (Department 4)
83.112.8.192/28 - Network 5: 83.112.8.192 to 83.112.8.207 (Department 5)

Αυτή η δομή παρέχει ένα μοναδικό τμήμα δικτύου για κάθε τμήμα, διευκολύνοντας τη διαχείριση του δικτύου, βελτιώνοντας την ασφάλεια και εξασφαλίζοντας αρκετό χώρο διευθύνσεων για τις απαιτήσεις κάθε τμήματος.

Επισκόπηση Σχεδιασμού Δικτύου

1. **Διεύθυνση & VLAN**: Κάθε τμήμα θα έχει ένα μοναδικό υποδίκτυο και ένα μοναδικό VLAN. Αυτό βοηθά στην τμηματοποίηση του δικτύου, βελτιώνει την ασφάλεια διαχωρίζοντας την κίνηση τμημάτων και διαχειρίζεται αποτελεσματικά τους τομείς μετάδοσης.
2. **Εναλλαγή και δρομολόγηση**:Η δρομολόγηση μεταξύ VLAN θα πρέπει να αντιμετωπίζεται από διακόπτες επιπέδου 3 στο επίπεδο πυρήνα για να είναι δυνατός ο αποτελεσματικός έλεγχος και παρακολούθηση της κυκλοφορίας μεταξύ διαφόρων VLAN.

3. **Ασφάλεια**: Για να διαχειριστείτε και να ασφαλίσετε την κυκλοφορία μεταξύ διαφόρων τμημάτων δικτύου, εφαρμόστε μέτρα ασφαλείας όπως τείχη προστασίας, λίστες ελέγχου πρόσβασης (ACL) και χάρτες πρόσβασης VLAN (VACL).
4. **Ασύρματα δίκτυα:** Διαμορφώστε ασφαλή σημεία ασύρματης πρόσβασης (WAP) για κάθε τμήμα, βεβαιωθείτε ότι η ασύρματη κίνηση χωρίζεται επίσης σε τμήματα αντιστοιχίζοντας τα SSID σε αντίστοιχα VLAN.
5. **Πλεονασμός και αξιοπιστία**: Χρησιμοποιήστε πρωτόκολλα όπως το Spanning Tree Protocol (STP) για να αποτρέψετε τους βρόχους δικτύου και να ενσωματώσετε τον πλεονασμό χρησιμοποιώντας διπλές συνδέσεις από τους μεταγωγείς στο κεντρικό δίκτυο.

Ολοκληρωμένο διάγραμμα δικτύου με διεύθυνση IP

Με βάση τα υποδίκτυα /28 που προσδιορίστηκαν προηγουμένως, η διαμόρφωση δικτύου για κάθε τμήμα αντιπροσωπεύεται οπτικά από το διάγραμμα δικτύου και τη στρατηγική κατανομής IP παρακάτω:

Εκχώρηση Διεύθυνσης IP

- Τμήμα Πωλήσεων: VLAN 10

Δίκτυο: 83.112.8.128/28
Εύρος χρήσης: 83.112.8.129 - 83.112.8.142

- Τμήμα Εξυπηρέτησης: VLAN 20

Δίκτυο: 83.112.8.144/28
Εύρος χρήσης: 83.112.8.145 - 83.112.8.158

- Τμήμα Διαχείρισης: VLAN 30

Δίκτυο: 83.112.8.160/28
Εύρος χρήσης: 83.112.8.161 - 83.112.8.174

- Τμήμα Ηλεκτρονικού Εμπορίου: VLAN 40

Δίκτυο: 83.112.8.176/28
Εύρος χρήσης: 83.112.8.177 - 83.112.8.190

- Τμήμα Μάρκετινγκ: VLAN 50

Δίκτυο: 83.112.8.192/28
Εύρος χρήσης: 83.112.8.193 - 83.112.8.206

Διαμόρφωση και συσκευές για δίκτυα

Κύριος διακόπτης:
Μοντέλο: Διακόπτης Layer 3 υψηλής χωρητικότητας.
Τα χαρακτηριστικά περιλαμβάνουν ACL που σχετίζονται με την ασφάλεια και δρομολόγηση VLAN.

Διακόπτες πρόσβασης:
Υπάρχουν διακόπτες ειδικά για κάθε όροφο ή τμήμα.
συνδέεται μέσω ανοδικών συνδέσεων gigabit στον πυρήνα.

Τείχος προστασίας: Βρίσκεται στην άκρη του δικτύου. ελέγχει και φιλτράρει την κυκλοφορία, τόσο την εισερχόμενη όσο και την εξερχόμενη.

Διακομιστές DHCP: Ρύθμιση για αυτόματη εκχώρηση διευθύνσεων IP σε κάθε VLAN.

Σημεία ασύρματης πρόσβασης:
Το WPA2-Enterprise προστατεύει τα σημεία ασύρματης πρόσβασης. Ένα μοναδικό VLAN αντιστοιχίζεται σε κάθε WAP ανάλογα με το τμήμα και την τοποθεσία του.

Κίνδυνοι:

Υπάρχουν αρκετοί εγγενείς κίνδυνοι ασφάλειας κατά την υλοποίηση ενός δικτύου σε ένα πολυτμηματικό επιχειρηματικό περιβάλλον, όπως αυτό που περιγράψατε για το κτήριο

πέντε τμημάτων σας. Η αποτελεσματική αντιμετώπιση αυτών των απαιτήσεων για μια διεξοδική προσέγγιση στην ασφάλεια του δικτύου. Θα παραθέσω μερικούς τυπικούς κινδύνους για την ασφάλεια του δικτύου παρακάτω μαζί με προτάσεις για τη μείωσή τους:

1. Μη εξουσιοδοτημένη πρόσβαση: Οι μη εξουσιοδοτημένοι χρήστες ενδέχεται να έχουν πρόσβαση σε ευαίσθητα δεδομένα ή να παρεμβαίνουν στις υπηρεσίες δικτύου λόγω αδύναμων διαδικασιών ελέγχου ταυτότητας ή ανεπαρκών ελέγχων πρόσβασης.

Λύση:
Ισχυρός έλεγχος ταυτότητας: Χρησιμοποιήστε έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA) για να αποκτήσετε πρόσβαση σε ζωτικής σημασίας επιχειρηματικές εφαρμογές και συσκευές δικτύου.
- Λίστες ελέγχου πρόσβασης (ACL): Για να περιορίσετε την πρόσβαση σε τμήματα δικτύου ανάλογα με το ρόλο ή το τμήμα, χρησιμοποιήστε ACL σε διακόπτες και δρομολογητές.
-Ασφαλή ασύρματα δίκτυα: Διαχωρίστε τα δίκτυα επισκεπτών από τα εσωτερικά δίκτυα και χρησιμοποιήστε το WPA3 για WiFi.

2. Εσωτερικές απειλές:
Κίνδυνος: Τα μέλη του προσωπικού ενδέχεται σκόπιμα ή ακούσια να κάνουν κατάχρηση της πρόσβασής τους στο δίκτυο για να κλέψουν πληροφορίες ή να διαταράξουν το σύστημα.
Λύση:
Αρχή Ελάχιστων Προνομίων: Βεβαιωθείτε ότι τα συστήματα και οι χρήστες έχουν μόνο την ελάχιστη πρόσβαση που απαιτείται για την εκτέλεση των καθηκόντων τους.
Behavior Analytics: Χρήστης και οντότητα: Χρησιμοποιήστε συστήματα ασφαλείας που είναι σε θέση να προσδιορίζουν τα περίεργα πρότυπα συμπεριφοράς που υποδεικνύουν εσωτερικές απειλές.

3. Επιθέσεις κακόβουλου λογισμικού και ransomware:
Κίνδυνος: Ενώ το ransomware κρυπτογραφεί σημαντικά δεδομένα και απαιτεί λύτρα για να τα ξεκλειδώσει, το κακόβουλο λογισμικό μπορεί να παρέμβει στις λειτουργίες, να καταλάβει συστήματα ή να κλέψει ευαίσθητα δεδομένα.

Λύση:
Endpoint Protection: Εγκαταστήστε λογισμικό αιχμής κατά του κακόβουλου λογισμικού με συχνές ενημερώσεις και σάρωση σε πραγματικό χρόνο.

Ασφάλεια email: Μειώστε την έκθεσή σας σε επιθέσεις phishing χρησιμοποιώντας πύλες ηλεκτρονικού ταχυδρομείου που ελέγχουν τα συνημμένα και τους συνδέσμους για κακόβουλο περιεχόμενο.

Τακτικά αντίγραφα ασφαλείας:Για να διευκολύνετε την ανάκτηση σε περίπτωση επίθεσης ransomware, κρατήστε τακτικά, ασφαλή αντίγραφα ασφαλείας σημαντικών δεδομένων.

4**. Κατανεμημένες επιθέσεις άρνησης υπηρεσίας (DDoS) και άρνησης υπηρεσίας (DoS):**
Κίνδυνος: Αυτές οι επιθέσεις προσπαθούν να υπερφορτώσουν τους πόρους του δικτύου έτσι ώστε οι εξουσιοδοτημένοι χρήστες να μην μπορούν να έχουν πρόσβαση σε αυτούς.

Λύση: Για να αντέχετε τις επιθέσεις, δημιουργήστε το δίκτυο με περιττές διαδρομές και βασικά στοιχεία.

Φιλτράρισμα κυκλοφορίας: Χρησιμοποιήστε δρομολογητές και τείχη προστασίας για να εξαλείψετε πιθανή κυκλοφορία DDoS σύμφωνα με ανωμαλίες και γνωστές υπογραφές επίθεσης.

5.Παραβίαση δεδομένων
Κίνδυνος: Ο ανεπαρκής χειρισμός ή τα ακατάλληλα διαμορφωμένα δίκτυα θα μπορούσαν να αποκαλύψουν ακούσια ευαίσθητες πληροφορίες.
Λύση:
Αποτροπή απώλειας δεδομένων (DLP): Χρησιμοποιήστε όργανα DLP για να παρακολουθείτε και να διαχειρίζεστε τα δεδομένα που διακινούνται μέσω του δικτύου.
Κρυπτογράφηση: Για να αποφύγετε την ανεπιθύμητη πρόσβαση, κρυπτογραφήστε κρίσιμα δεδομένα τόσο κατά τη μεταφορά όσο και σε κατάσταση ηρεμίας.

6.Υποκλοπή δικτύου
Κίνδυνος: Ευαίσθητες πληροφορίες ενδέχεται να κλαπούν από χάκερ εάν καταφέρουν να υποκλέψουν δεδομένα που κινούνται στο δίκτυο.
Λύση:
Κρυπτογράφηση: Κατά τη μετάδοση δεδομένων, χρησιμοποιήστε ισχυρά πρωτόκολλα κρυπτογράφησης όπως IPsec, HTTPS και SSL/TLS.
Ασφαλής Υποδομή Δικτύου: Διαχωρίστε και ασφαλίστε την κυκλοφορία δικτύου χρησιμοποιώντας VLAN και VPN.

7. Αποτυχίες ρύθμισης παραμέτρων και διαχείρισης ενημερώσεων κώδικα

Κίνδυνος: Απαρχαιωμένο λογισμικό ή ακατάλληλα διαμορφωμένες συσκευές δικτύου ενδέχεται να έχουν κενά ασφαλείας που θα μπορούσαν να εκμεταλλευτούν οι χάκερ.

Λύση:
Τακτικές ενημερώσεις και διαχείριση ενημερώσεων κώδικα: Βεβαιωθείτε ότι ενημερώνετε το λογισμικό και το υλικολογισμικό σε τακτική βάση για να αντιμετωπίζετε γνωστά τρωτά σημεία.
Έλεγχοι διαμόρφωσης: Βεβαιωθείτε ότι οι διαμορφώσεις συσκευών δικτύου συμμορφώνονται με τις οδηγίες ασφαλείας του οργανισμού, αναθεωρώντας τις τακτικά.

Εκτός από τις τεχνολογικές λύσεις, η εκπαίδευση των μελών του προσωπικού σχετικά με τις βέλτιστες πρακτικές ασφάλειας και η διατήρηση μιας κουλτούρας με επίγνωση της ασφάλειας είναι επίσης απαραίτητη για την εφαρμογή αυτών των μέτρων ασφαλείας. Είναι δυνατό να διασφαλιστεί ότι κάθε τμήμα του δικτύου είναι ασφαλές από νέες απειλές με τη διενέργεια τακτικών ελέγχων ασφαλείας και ελέγχων συμμόρφωσης.

Χρήση Εργαλείου Wireshark

α. Δώστε τη διεύθυνση IP του διακομιστή DNS στο δίκτυο

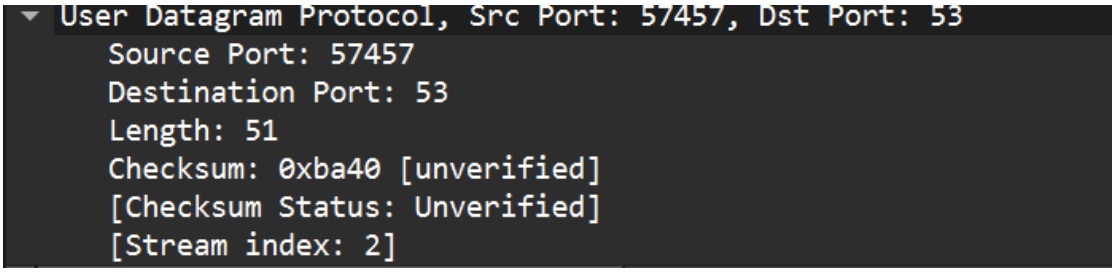
Βήματα για την ανάλυση πακέτων της IP του διακομιστή DNS
Επισκόπηση του ζητήματος:
Χρησιμοποιώντας το δεδομένο αρχείο καταγραφής πακέτων (pcapng), καθορίστηκε αρχικά η διεύθυνση IP του διακομιστή DNS του δικτύου.

Εξαγωγή δεδομένων: Για να βρούμε πακέτα που σχετίζονται με το πρωτόκολλο DNS, ανοίξαμε και εξετάσαμε το αρχείο καταγραφής πακέτων (pcapng).

Αναγνώριση πακέτων DNS: Επικεντρωθήκαμε σε πακέτα UDP που χρησιμοποιούν τη θύρα 53, η οποία είναι η τυπική θύρα που χρησιμοποιείται για αιτήματα και απαντήσεις DNS.

Το πακέτο πρωτοκόλλου UDP (αριθμός πρωτοκόλλου 17).
53 είναι η θύρα προορισμού. είναι η προεπιλεγμένη θύρα DNS.
192.168.2.9 είναι η διεύθυνση πηγής και 192.168.2.1 είναι η διεύθυνση προορισμού.

Η διεύθυνση προορισμού (192.168.2.1) αυτού του πακέτου είναι η διεύθυνση IP του DNS server στο δίκτυο, καθώς όλες οι DNS αιτήσεις αποστέλλονται σε αυτήν τη διεύθυνση για να λάβουν απαντήσεις.



Ακολουθούν οι έγκυροι διακομιστές ονομάτων και οι διευθύνσεις IP τους:

1. adns1.berkeley.edu

   - IPv4: 128.32.136.3

   - IPv6: 2607:f140:ffff:fffe::3

2. adns2.berkeley.edu

   - IPv4: 128.32.136.14

   - IPv6: 2607:f140:ffff:fffe::e

3. aodns1.berkeley.edu

   - IPv4: 192.35.225.133

   - IPv6: 2607:f010:3f8:8000:0:ff:fe00:53

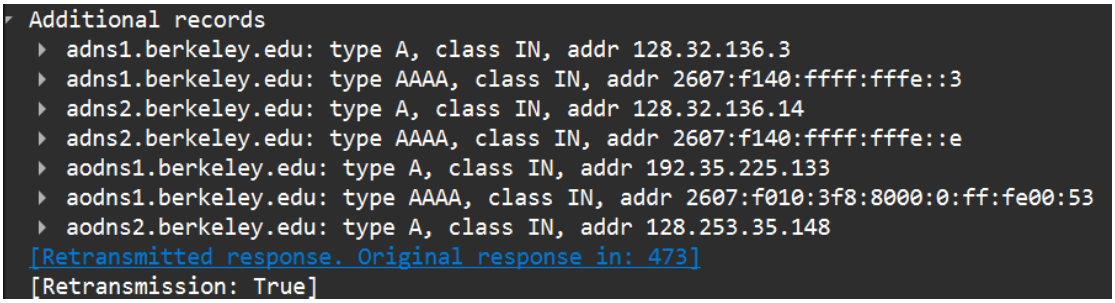
4. aodns2.berkeley.edu

   - IPv4: 128.253.35.148

Αυτοί είναι οι έγκυροι διακομιστές ονομάτων για τον τομέα "berkeley.edu" που θα χειρίζονται ερωτήματα DNS για αυτόν τον τομέα.

Λόγος επιλογής πλασίου 474 για την απάντηση:

Το πλαίσιο 474 περιλαμβάνει την ενότητα "Authoritative nameservers" που απαριθμεί τους εξουσιοδοτημένους ονοματολογικούς servers και τις διευθύνσεις τους.

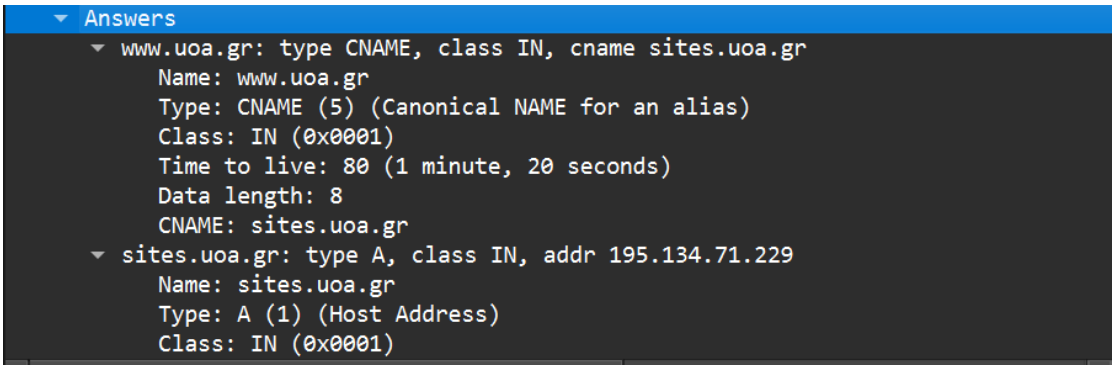


Δώστε τη διεύθυνση IP του διακομιστή web που φιλοξενεί την ιστοσελίδα www.uoa.gr

Ο διακομιστής που φιλοξενεί την ιστοσελίδα «www.uoa.gr» έχει διεύθυνση IP 195.134.71.229.

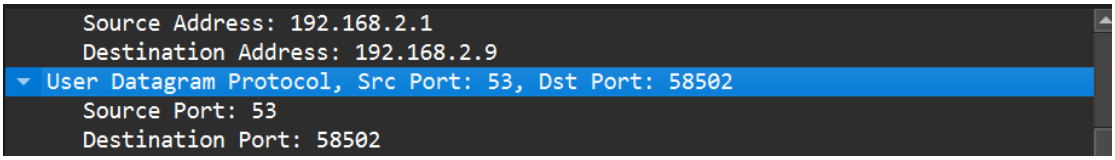
Η τελική απάντηση για το "www.uoa.gr" βρίσκεται στο πλαίσιο 892. Υποδεικνύει ότι η διεύθυνση IP είναι 195.134.71.229 και ότι είναι ένα CNAME για το "sites.uoa.gr".

Οι υπόλοιπες εγγραφές ενδέχεται να περιλαμβάνουν ενδιάμεσους ή διαφορετικούς τύπους εγγραφών που παραλείπουν την τελική διεύθυνση IP.



Δηλώστε τη θύρα επικοινωνίας με τον διακομιστή DNS για το ερώτημα του διεύθυνση της ιστοσελίδας www.uoa.gr

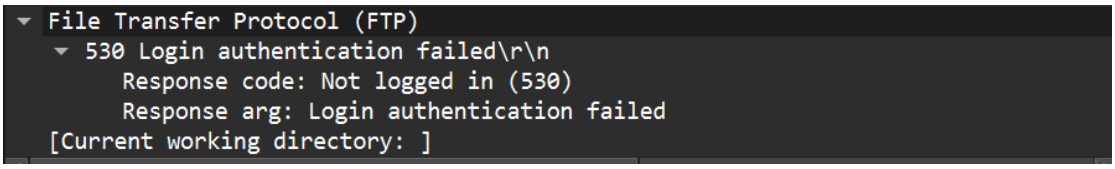
Η θύρα 53 είναι η καθιερωμένη θύρα που χρησιμοποιείται για την επικοινωνία με τους διακομιστές DNS για την αποστολή και λήψη αιτημάτων και απαντήσεων DNS.



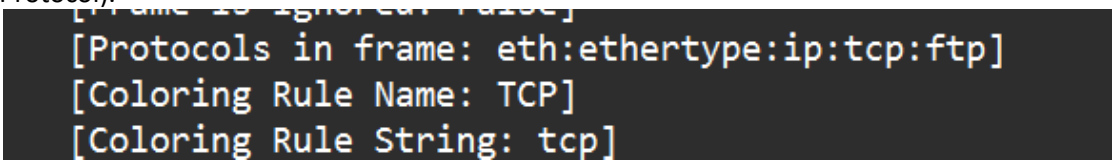
Ποιο όνομα χρήστη χρησιμοποιήθηκε για την επικοινωνία με τον κεντρικό υπολογιστή με διεύθυνση IP του 172.16.137.53;

Ποιο πρωτόκολλο επικοινωνίας χρησιμοποιήθηκε; Ήταν η σύνδεση επιτυχημένη ή όχι;

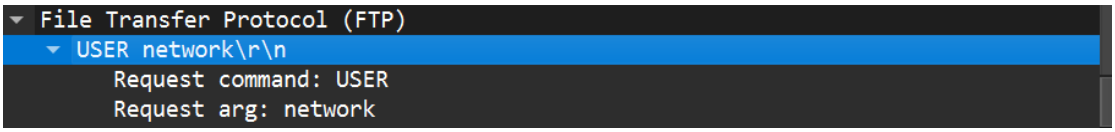
Η σύνδεση δεν ήταν επιτυχής, όπως υποδεικνύεται από το πλαίσιο 1433 που δείχνει την απάντηση 530 Ο έλεγχος ταυτότητας σύνδεσης απέτυχε.



Το πρωτόκολλο επικοινωνίας που χρησιμοποιήθηκε είναι το TCP μέσω FTP (File Transfer Protocol).

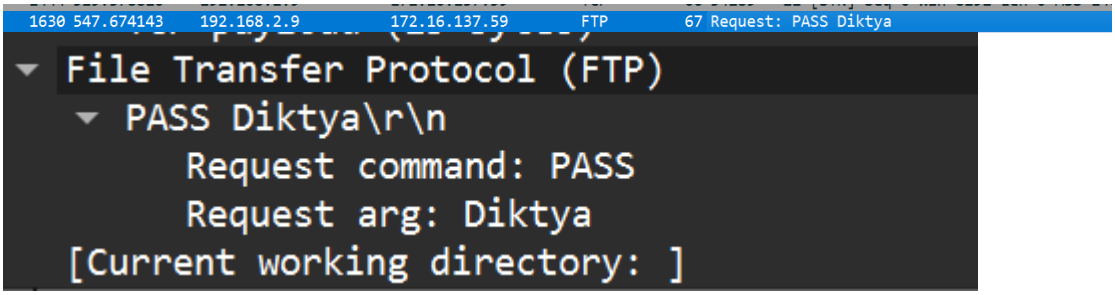


Το όνομα χρήστη που χρησιμοποιήθηκε για την επικοινωνία με τον κεντρικό υπολογιστή με διεύθυνση IP 172.16.137.53 είναι “network”



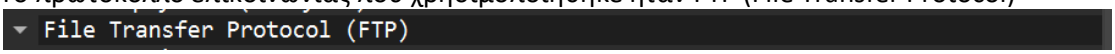
Ποιος είναι ο κωδικός πρόσβασης που χρησιμοποιείται για τη σύνδεση με τον κεντρικό υπολογιστή με διεύθυνση IP 172.16.137.59;

Ο κωδικός πρόσβασης που χρησιμοποιήθηκε ήταν "diktya".



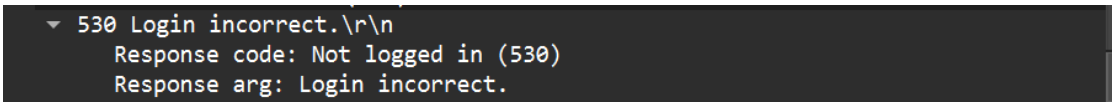
Ποιο πρωτόκολλο επικοινωνίας χρησιμοποιήθηκε;

Το πρωτόκολλο επικοινωνίας που χρησιμοποιήθηκε ήταν FTP (File Transfer Protocol)



Ήταν η σύνδεση επιτυχημένη ή όχι;

Η σύνδεση δεν ήταν επιτυχής.



Εντολή για να αναζητήσουμε τα αρχεία με IP172.16.137.59 : ip.addr == 172.16.137.59

Δηλώστε τις θύρες και στις δύο πλευρές της επικοινωνίας με τον κεντρικό υπολογιστή με διεύθυνση IP 172.16.137.59.

Θύρα προέλευσης:
Στη μεριά του πελάτη (192.168.2.9) που επικοινωνεί με τον διακομιστή (172.16.137.59), η θύρα προέλευσης είναι η 54289.

Θύρα προορισμού:
Στη μεριά του διακομιστή (172.16.137.59), η θύρα προορισμού είναι η 21, που είναι η τυπική θύρα για το πρωτόκολλο FTP.

Πόσα byte μεταφέρθηκαν σε αυτήν την επικοινωνία;

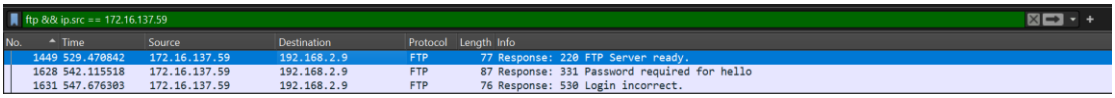
Θα προσθέσουμε τα πακέτα: 1446: 54 bytes ,1630: 67 bytes , 1631: 76 bytes , 1632: 54 bytes , 1634: 54 bytes , 1633: 60 bytes , 1633: 60 bytes με μια απλή πρόσθεση βγάζουμε άθροισμα ***365 bytes***.

Ποιο πρωτόκολλο Transport Layer χρησιμοποιήθηκε για τις συνδέσεις FTP;

Για τη σύνδεση FTP, το πρωτόκολλο επιπέδου μεταφοράς που χρησιμοποιήθηκε είναι το TCP (Transmission Control Protocol). Το TCP είναι το πρωτόκολλο που χρησιμοποιείται για αξιόπιστες μεταφορές δεδομένων και είναι το πρωτόκολλο που χρησιμοποιείται από το FTP για τη μεταφορά αρχείων.

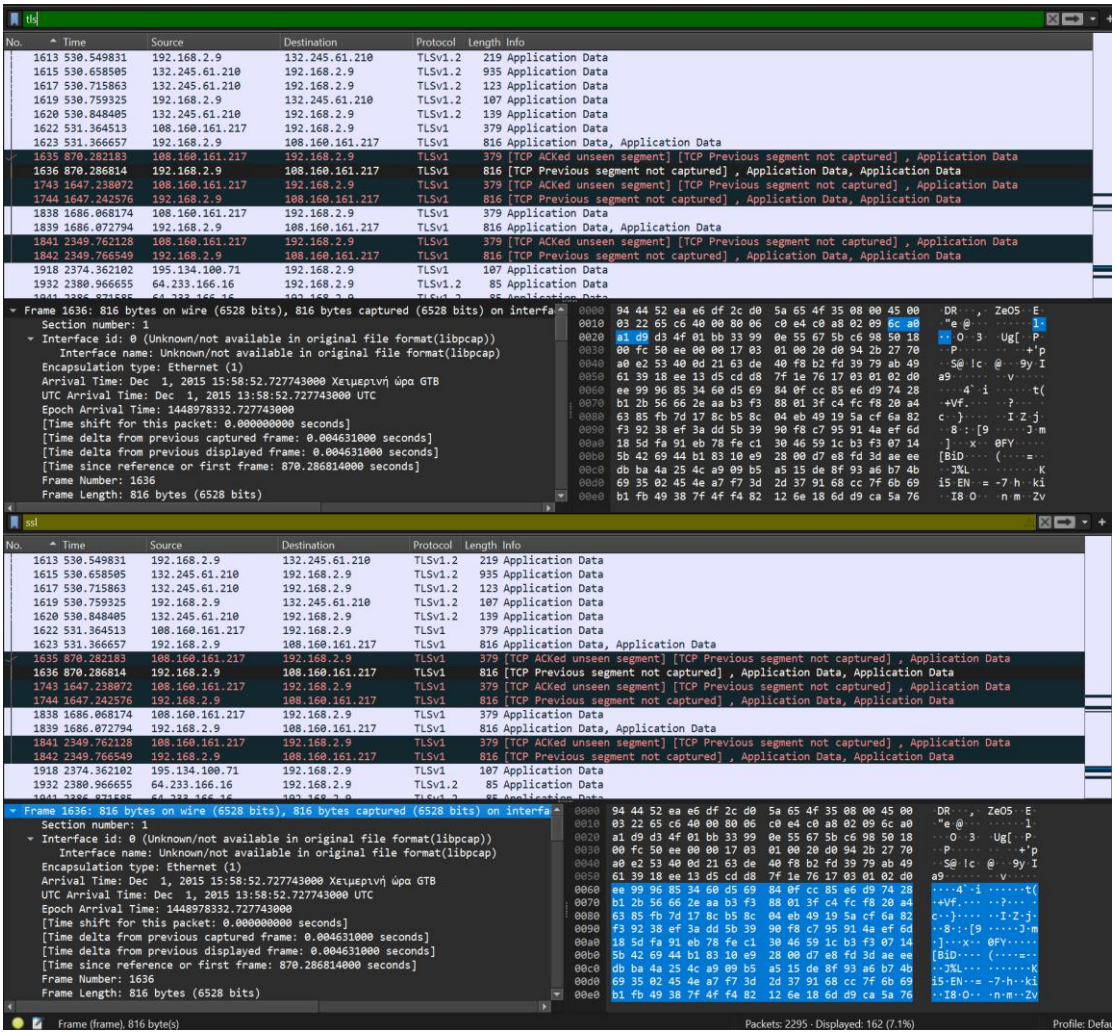
Πόσα byte ελήφθησαν από τον διακομιστή ftp με διεύθυνση IP

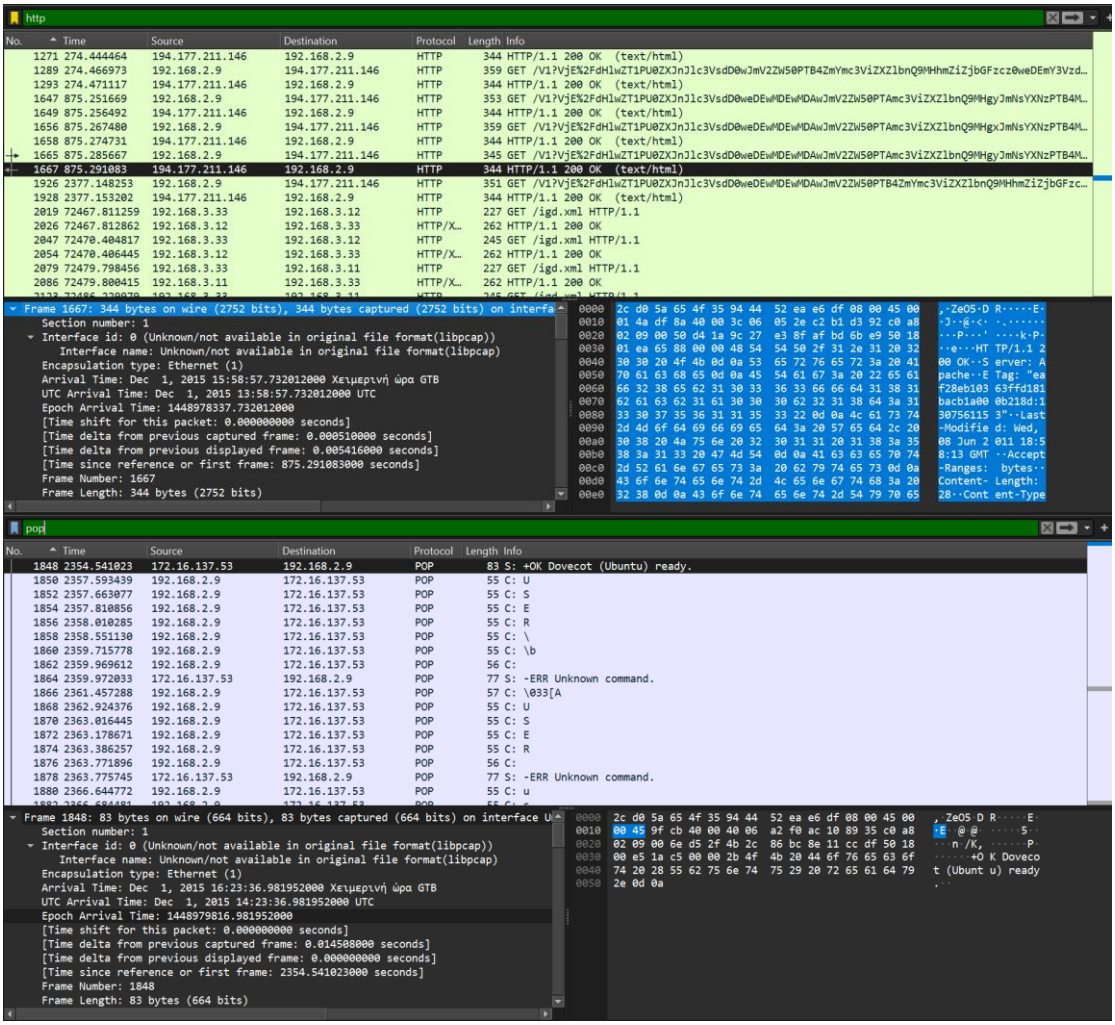
172.16.137.53;



Θα προσθέσουμε τα τρία length 77 + 87 + 76 = 240 bytes

Εκτός από το SMTP, χρησιμοποιήσαμε άλλο πρωτόκολλο επιπέδου εφαρμογής για να στείλουμε μία ηλεκτρονική διεύθυνση? Αν ναι, τότε ποια;





Όπως βλέπουμε τα πρωτόκολλα που χρησιμοποιήσαμε ήταν το pop,http,ssl και tls.

Bibliography

Comer, Douglas E, Δίκτυα και διαδίκτυα υπολογιστών Και εφαρμογές τους στο Internet, ISBN13: 9789604610402, Εκδ. Κλειδάριθμος, 2007. PETERSON, DAVIE, Δίκτυα Υπολογιστών, ISBN13: 9789604612666, Εκδ. Κλειδάριθμος, 2010. James Kurose, Keith Ross, Computer Networking: A Top-Down Approach (7th Edition), Pearson 2016. Comer, D E. (2015) Internetworking with TCP/IP (6th Edition), Prentice Hall