Εργαστηριακή Άσκηση 8
TELNET, FTP και TFTP

Ο σκοπός αυτής της εργαστηριακής άσκησης είναι η εξέταση πρωτοκόλλων εφαρμογής που χρησιμοποιούνται για την πρόσβαση και μεταφορά αρχείων από/προς απομακρυσμένους υπολογιστές. Στο πλαίσιο αυτό, θα εξετάσετε τα TELNET, FTP και TFTP, με τη βοήθεια του αναλυτή πρωτοκόλλων Wireshark.

Για τις παρακάτω ασκήσεις απαντήστε στο συνοδευτικό φυλλάδιο, το οποίο θα υποβάλλετε ως αρχείο pdf.

1. TELNET

Το TELNET είναι ένα πρωτόκολλο που χρησιμοποιείται για διαδραστική αμφίδρομη πρόσβαση σε δικτυωμένες μηχανές μέσω μιας σύνδεσης εικονικού τερματικού. Το βασικό πρωτόκολλο ορίζεται στο RFC 854 και διάφορες επεκτάσεις του στα RFC 855 έως 861. Το όνομά του προέρχεται από τη σύντμηση των λέξεων TELetype NETwork. Υλοποιεί ένα εικονικό τηλέτυπο, η βασική λειτουργία του οποίου είναι η μεταφορά χαρακτήρων ASCII. Οι χαρακτήρες μεταφέρονται ως byte των 8-bit. Ο χαρακτήρας που "πιέζει" ο χρήστης στο πληκτρολόγιο μεταφέρεται ως έχει στο απομακρυσμένο μηχάνημα και, εάν έχει ζητηθεί, επαναλαμβάνεται (echoed) από το απομακρυσμένο μηχάνημα και εμφανίζεται στην οθόνη του χρήστη. Το byte 0xff (IAC –Interpret as Command) σηματοδοτεί ότι ο επόμενος χαρακτήρας είναι εντολή TELNET. Μέσω των εντολών γίνεται διαπραγμάτευση επιλογών μεταξύ των δύο μερών. Βασικές εντολές του TELNET είναι οι "will", "won't", "do" and "don't". Η εντολή "will" δηλώνει την επιθυμία χρήσης ή επιβεβαιώνει τη χρήση της επιλογής που δηλώνει ο κωδικός που την ακολουθεί. Η εντολή "Won't" δηλώνει άρνηση της χρήσης ή άρνηση της συνέχισης χρήσης της επιλογής που την ακολουθεί. Η εντολή "Do" ζητά από την άλλη πλευρά να χρησιμοποιήσει ή να επιβεβαιώσει ότι χρησιμοποιεί την επιλογή που την ακολουθεί. Η εντολή "Don't" ζητά από την άλλη πλευρά να σταματήσει να χρησιμοποιεί ή να επιβεβαιώσει ότι δεν θα χρησιμοποιήσει στη συνέχεια την επιλογή που την ακολουθεί. Στην ιστοσελίδα https://www.eventhelix.com/Networking/Telnet.pdf θα βρείτε ένα πλήρες παράδειγμα ανταλλαγής εντολών κατά τη σύνδεση με telnet ενός πελάτη σε ένα εξυπηρετητή.

Η λέξη telnet επίσης αναφέρεται στο πρόγραμμα λογισμικού που υλοποιεί την πλευρά πελάτη του πρωτοκόλλου. Το πρόγραμμα telnet υπάρχει σχεδόν σε όλα τα λειτουργικά συστήματα. Παρέχει πρόσβαση σε διεπαφή γραμμής εντολών (CLI – Command-Line Interface) απομακρυσμένων υπολογιστών και δικτυακών εξοπλισμών. Ο χρήστης για να συνδεθεί στην απομακρυσμένη μηχανή δίνει ένα όνομα και ένα συνθηματικό. Το TELNET εξ ορισμού δεν κρυπτογραφεί την πληροφορία που στέλνεται πάνω από τη σύνδεση. Είναι επομένως δυνατό να υποκλέψει κανείς τα ονόματα χρηστών και τα συνθηματικά με τη βοήθεια ενός αναλυτή πρωτοκόλλων. Επειδή ως πρωτόκολλο εμφανίζει σημαντικά προβλήματα ασφαλείας, δεν συνιστάται η χρήση του για απομακρυσμένη πρόσβαση σε υπολογιστές και έχει αντικατασταθεί από το SSH.

Με τη βοήθεια του Wireshark, θα καταγράψετε την κίνηση ενώ κάνετε χρήση της υπηρεσίας Telnet του υπολογιστή edu-dy.cn.ntua.gr (147.102.40.15). Εάν χρησιμοποιείτε λειτουργικό σύστημα Windows θα πρέπει ρητά να ενεργοποιήσετε την εφαρμογή πελάτη telnet από το *Turn Windows features on or off*. Σε συστήματα Unix/Linux, εάν δεν υπάρχει, θα χρειαστεί να την εγκαταστήσετε. Εφαρμόστε φίλτρο σύλληψης `host 147.102.40.15` για να παρατηρείτε μόνο την κίνηση που σχετίζεται με το edu-dy.cn.ntua.gr. Για τη χρήση της υπηρεσίας Telnet πληκτρολογήστε `telnet edu-dy.cn.ntua.gr` σε ένα παράθυρο εντολών. Στην προτροπή `login:` πληκτρολογήστε `abcd` ακολουθούμενο από `<Enter>`, ενώ στην προτροπή `Password:` πληκτρολογήστε `efgh` ακολουθούμενο από `<Enter>`. Σημειώνεται ότι ο χρήστης abcd δεν υπάρχει στον συγκεκριμένο εξυπηρετητή και η

αναγνώριση του χρήστη θα αποτύχει. Στη συνέχεια πληκτρολογήστε <Ctrl>+] και στην προτροπή που θα εμφανισθεί δίνετε την εντολή quit για έξοδο.

1.1 Ποιο πρωτόκολλο μεταφοράς χρησιμοποιεί το TELNET (TCP ή UDP);
1.2 Καταγράψτε τις θύρες του πρωτοκόλλου μεταφοράς που χρησιμοποιούνται για την επικοινωνία.
1.3 Ποια από τις παραπάνω θύρες αντιστοιχεί στο πρωτόκολλο εφαρμογής TELNET;
1.4 Εφαρμόστε ένα φίλτρο απεικόνισης ώστε να παραμείνουν μόνο τα τεμάχια που σχετίζονται με το πρωτόκολλο εφαρμογής TELNET. Ποια είναι η σύνταξή του;

Εντοπίστε το **πρώτο** μήνυμα TELNET που μεταφέρει την προτροπή για login. *[Υπόδειξη: Για να το εντοπίσετε, επιλέξτε το πρώτο μήνυμα TELNET, από το μενού Edit → Find Packet… ενεργοποιήστε την επιλογή String (αντί για Display filter), στο πεδίο αναζήτησης πληκτρολογήστε login, επιλέξτε Packet Details για αναζήτησε στο πεδίο δεδομένων, και τέλος πατήστε το Find]*.

1.5 Καταγράψτε τις εντολές (command) TELNET τύπου echo και τον αποστολέα τους, μεταξύ του υπολογιστή σας και του edu-dy.cn.ntua.gr, που προηγούνται του μηνύματος αυτού.
1.6 Ζητά ο edu-dy.cn.ntua.gr από τον υπολογιστή σας να επαναλαμβάνει (echo) τους χαρακτήρες που λαμβάνει; Εάν ναι, δέχεται ο υπολογιστής σας να τους επαναλαμβάνει;
1.7 Ζητά ο edu-dy.cn.ntua.gr από τον υπολογιστή σας να μην επαναλαμβάνει (echo) τους χαρακτήρες που λαμβάνει; Εάν ναι, δέχεται ο υπολογιστής σας να μην τους επαναλαμβάνει;
1.8 Προτίθεται ο edu-dy.cn.ntua.gr να επαναλαμβάνει τους χαρακτήρες που λαμβάνει από τον υπολογιστή σας;

Εντοπίστε το μήνυμα TELNET από τον υπολογιστή σας προς τον edu-dy.cn.ntua.gr που μεταφέρει τον πρώτο χαρακτήρα "a" του ονόματος χρήστη.

1.9 Έχει προηγηθεί του μηνύματος αυτού εντολή TELNET με την οποία ο υπολογιστής σας ζητά την επανάληψη των χαρακτήρων από τον edu-dy.cn.ntua.gr;

Από το μενού *Analyze* επιλέγοντας *Follow TCP Stream*, εμφανίζεται παράθυρο όπου μπορείτε να παρατηρήσετε ολόκληρη τη ροή κίνησης TCP κατά την επικοινωνία. Με μπλε χρώμα παρουσιάζεται η κίνηση από την πλευρά του εξυπηρετητή, ενώ με κόκκινο η δική σας. Εντοπίστε την πρώτη προτροπή login (εν ανάγκη μεγεθύνετε το παράθυρο ώστε να δείτε το τέλος των γραμμών όπου εμφανίζονται οι χαρακτήρες ASCII).

1.10 Τι συμβαίνει κατά τη μεταφορά του ονόματος χρήστη που αποστείλατε μετά την πρώτη προτροπή login;
1.11 Εξηγήστε το φαινόμενο που παρατηρείτε στο προηγούμενο ερώτημα με βάση την απάντηση στα ερωτήματα 1.8 και 1.9.
1.12 Κλείστε τώρα το παράθυρο Follow TCP Stream και εφαρμόζοντας φίλτρο απεικόνισης εντοπίστε τα πακέτα IPv4 που μεταφέρουν μηνύματα TELNET από τον υπολογιστή σας προς τον εξυπηρετητή. Ποια είναι η σύνταξή του;
1.13 Πόσα πακέτα IPv4 χρειάζονται για να μεταφερθεί η πληροφορία για το όνομα (abcd) του χρήστη;
1.14 Πόσα πακέτα IPv4 χρειάζονται για να μεταφερθεί η πληροφορία για τον κωδικό του χρήστη (efgh);

Ακυρώστε το προηγούμενο φίλτρο απεικόνισης και εφαρμόστε νέο ώστε να παρατηρείτε και τα μηνύματα TELENT που στέλνει ο εξυπηρετητής.

1.15 Ο εξυπηρετητής στέλνει την ηχώ των χαρακτήρων efgh του κωδικού χρήστη προς τον πελάτη;
1.16 Παρατηρήσατε εντολή TELNET “Don’t Echo” πριν τη μεταφορά του κωδικού;
1.17 Εάν η απάντηση στην προηγούμενη ερώτηση είναι όχι, γιατί δεν εμφανίζεται στην οθόνη ο κωδικός;
1.18 Σχολιάστε την ασφάλεια της υπηρεσίας Telnet.

2. FTP

Το File Transfer Protocol (FTP) είναι ένα πρωτόκολλο του διαδικτύου που χρησιμοποιείται για τη μεταφορά αρχείων μεταξύ ενός πελάτη και ενός εξυπηρετητή. Υλοποιεί μια αρχιτεκτονική πελάτη-εξυπηρετή χρησιμοποιώντας δύο συνδέσεις TCP, μία ελέγχου και μία μεταφοράς δεδομένων. Το βασικό πρωτόκολλο ορίζεται στο RFC 959 και διάφορες επεκτάσεις του στα RFC 2228 και RFC 2640. Η λέξη ftp επίσης αναφέρεται στο πρόγραμμα λογισμικού που υλοποιεί την πλευρά πελάτη του πρωτοκόλλου. Οι πρώτες εφαρμογές ftp ήταν προγράμματα γραμμής εντολών (CLI) και υπάρχουν σχεδόν σε όλα τα λειτουργικά συστήματα. Σήμερα θα βρείτε πολλές εφαρμογές ftp με γραφικό περιβάλλον. Επίσης έχει ενσωματωθεί στους πλοηγούς ιστού ενεργοποιούμενο για URI που αρχίζουν με ftp:// αντί για http://. Όμως στις πρόσφατες εκδόσεις του Firefox και Chrome απαιτείται η ύπαρξη εξωτερικού προγράμματος όπως το WinSCP ή FileZilla για τον χειρισμό τέτοιων URI. Εμφανίζει και αυτό σημαντικά προβλήματα ασφάλειας, για αυτό συχνά η μετάδοση κρυπτογραφείται με SSL/TLS, FTP Secure (FTPS), ή αντικαθίσταται από το SSH File Transfer Protocol (SFTP). Όπως και στο telnet οι χρήστες για να συνδεθούν στον εξυπηρετητή δίνουν όνομα και συνθηματικό. Επιπλέον επιτρέπεται και η ανώνυμη πρόσβαση (όνομα χρήστη anonymous, συνθηματικό οτιδήποτε), εάν ο εξυπηρετητής ρυθμισθεί κατάλληλα.

Στο FTP ορίζονται δύο τρόποι λειτουργίας (modes): α) ο *ενεργός* (active mode) και β) ο *παθητικός* (passive mode). Και στους δύο τρόπους λειτουργίας, το FTP χρησιμοποιεί μία συγκεκριμένη θύρα (ftp) για τις εντολές ελέγχου. Η θύρα για τη μεταφορά δεδομένων (ftp-data) είναι συγκεκριμένη στην περίπτωση του ενεργού τρόπου λειτουργίας, ενώ προσδιορίζεται δυναμικά στην περίπτωση του παθητικού τρόπου. Δείτε μια αναλυτική περιγραφή των δύο τρόπων λειτουργίας και άλλες πληροφορίες για το FTP στην ιστοσελίδα http://slacksite.com/other/ftp.html. Οι προδιαγραφές του πρωτοκόλλου FTP ορίζουν μια σειρά από εντολές, για τις οποίες μπορείτε να βρείτε πληροφορίες στην ιστοσελίδα http://www.networksorcery.com/enp/protocol/ftp.htm. Πρέπει να σημειωθεί ότι οι εντολές αυτές δεν υποστηρίζονται στο σύνολό τους από όλες τις υλοποιήσεις προγραμμάτων εξυπηρετητών ή πελατών FTP. Είναι ακόμη σημαντικό να διευκρινιστεί η διαφορά μεταξύ εντολής του *πρωτοκόλλου* FTP και εντολής του *προγράμματος φλοιού* ftp. Κάθε εντολή του προγράμματος φλοιού ftp επιτελεί μια συγκεκριμένη λειτουργία του πρωτοκόλλου FTP και για τον σκοπό αυτό μεταφράζεται σε μία ή περισσότερες εντολές του πρωτοκόλλου, που μεταφέρονται σε αντίστοιχα μηνύματα FTP. Καθώς χρησιμοποιείτε το πρόγραμμα φλοιού ftp, μπορείτε οποιαδήποτε στιγμή να πληκτρολογήσετε help από την προτροπή ftp>, προκειμένου να δείτε τις διαθέσιμες εντολές του προγράμματος. Στην ιστοσελίδα https://www.eventhelix.com/Networking/ftp/Ftp.pdf θα βρείτε ένα παράδειγμα χρήσης του FTP για σύνδεση με εξυπηρετητή, εμφάνιση των περιεχομένων του φακέλου όπου έγινε η σύνδεση, αλλαγή του τρέχοντος φακέλου, κατέβασμα αρχείου και κλείσιμο της σύνδεσης.

Για τη συνέχεια συνδεθείτε μέσω OpenVPN στο εσωτερικό δίκτυο του ΕΜΠ όπως στην Εργαστηριακή Άσκηση 5. Το πρόγραμμα θα δημιουργήσει μια εικονική διεπαφή, που τυπικά έχει την ονομασία TAP ή TUN, με διεύθυνση IPv4 από το χώρο των διευθύνσεων 147.102.0.0/16 του Ιδρύματος. Οι καταγραφές που θα κάνετε παρακάτω θα γίνουν στη συγκεκριμένη διεπαφή και όχι σε αυτή της κάρτας δικτύου του υπολογιστή σας.

Με τη βοήθεια του Wireshark, θα καταγράψετε την κίνηση ενώ κάνετε χρήση της υπηρεσίας FTP του υπολογιστή edu-dy.cn.ntua.gr (147.102.40.15) χρησιμοποιώντας τον ενεργό τρόπο λειτουργίας. Όπως πριν, εφαρμόστε φίλτρο σύλληψης για να παρατηρείτε μόνο την κίνηση που σχετίζεται με το edu-dy.cn.ntua.gr. Αρχίστε μια καταγραφή και σε ένα παράθυρο εντολών πληκτρολογήστε ftp –d edu-dy.cn.ntua.gr σε περιβάλλον Windows (ή ftp –A –d edu-dy.cn.ntua.gr σε περιβάλλον Linux). Στην προτροπή User: πληκτρολογήστε anonymous, ενώ στην προτροπή Password: πληκτρολογήστε labuser@cn. Αφού συνδεθείτε, δώστε τις εντολές help και remotehelp (ή rhelp σε συστήματα Linux). Στη συνέχεια δώστε την εντολή ls για να δείτε τα περιεχόμενα του τρέχοντος καταλόγου και πληκτρολογήστε bye για έξοδο.

2.1 Καταγράψτε τη σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε ώστε να συλλαμβάνονται μόνο τα πακέτα που περιλαμβάνουν τη διεύθυνση IP του edu-dy.cn.ntua.gr.
2.2 Τι σημαίνει το –d στη γραμμή εντολής που πληκτρολογήσατε; *[Υπόδειξη: Πληκτρολογήστε ftp -help στη γραμμή εντολών]*.
2.3 Ποιο πρωτόκολλο μεταφοράς χρησιμοποιεί το FTP (TCP ή UDP);
2.4 Καταγράψτε τις θύρες (πηγής και προορισμού) που χρησιμοποιούνται για την επικοινωνία FTP τόσο για τις εντολές ελέγχου όσο και για τη μεταφορά δεδομένων. *[Υπόδειξη: Χρησιμοποιήστε φίλτρο απεικόνισης tcp.flags.syn==1 ώστε να παραμείνουν μόνο τεμάχια των τριπλών χειραψιών με τη σημαία SYN ενεργοποιημένη]*.
2.5 Από ποια πλευρά (του πελάτη ή του εξυπηρετητή) γίνεται η σύνδεση TCP για τη μεταφορά *δεδομένων* FTP;
2.6 Καταγράψτε τις εντολές FTP που έστειλε ο πελάτης στον εξυπηρετητή. *[Υπόδειξη: Χρησιμοποιήστε φίλτρο απεικόνισης ftp.request==1]*.
2.7 Εμφανίζονται αυτές οι εντολές FTP στις πληροφορίες αποσφαλμάτωσης (debugging) στην οθόνη του προγράμματος φλοιού ftp και με ποιον τρόπο;
2.8 Με ποια εντολή του πρωτοκόλλου FTP μεταφέρεται το όνομα χρήστη;
2.9 Πόσα πακέτα χρειάζονται για να μεταφερθεί το όνομα του χρήστη;
2.10 Με ποια εντολή του πρωτοκόλλου FTP μεταφέρεται ο κωδικός χρήστη;
2.11 Πόσα πακέτα IP χρειάζονται για να μεταφερθεί ο κωδικός του χρήστη;
2.12 Περιγράψτε μια ομοιότητα και μια διαφορά στον τρόπο λειτουργίας των πρωτοκόλλων FTP και TELNET σε σχέση με ό,τι παρατηρήσατε για τη μεταφορά του ονόματος και του κωδικού χρήστη.
2.13 Η εντολή help του προγράμματος φλοιού ftp μεταφράζεται σε εντολή του πρωτοκόλλου FTP;
2.14 Βάσει των αποτελεσμάτων από την εκτέλεση της εντολής remotehelp (rhelp) που πληκτρολογήσατε στο παράθυρο της γραμμής εντολών, καταγράψτε δύο εντολές FTP που δεν υποστηρίζονται από τον εξυπηρετητή.

Εφαρμόστε τώρα το φίλτρο απεικόνισης ftp ώστε να εμφανισθεί όλος ο διάλογος (μεταξύ του υπολογιστή σας και του εξυπηρετητή) στη σύνδεση ελέγχου FTP.

2.15 Πόσα πακέτα, σχετικά με την εντολή remotehelp (rhelp), στάλθηκαν από τον υπολογιστή σας και πόσα από τον εξυπηρετητή;
2.16 Πώς δηλώνει ο εξυπηρετητής ότι τελείωσε η αποστολή πακέτων σχετικών με την εντολή remotehelp (rhelp); *[Υπόδειξη: Αναζητήστε τη λέξη hyphen στην παράγραφο FTP Replies στο RFC 959.]*
2.17 Εντοπίστε στη λίστα καταγεγραμμένων πακέτων του Wireshark το μήνυμα FTP που μεταφέρει την εντολή PORT. Τι παριστάνουν οι 4 πρώτοι δεκαδικοί αριθμοί;

Οι δύο τελευταίοι δεκαδικοί αριθμοί της εντολής PORT ορίζουν τη θύρα που ανακοινώνει ο πελάτης στον εξυπηρετητή προκειμένου να λάβει εκεί δεδομένα από αυτόν, την οποία έχετε καταγράψει προηγουμένως στην απάντηση της ερώτησης 2.4.

2.18 Πώς προκύπτει αυτός ο αριθμός αυτής της θύρας από τα δεδομένα της εντολής PORT; *[Υπόδειξη: Συμβουλευτείτε το παράδειγμα που περιγράφεται στην ενότητα "The FTP PORT Command" στην ιστοσελίδα http://slacksite.com/other/ftp.html]*.
2.19 Ποια εντολή του πρωτοκόλλου FTP εμφανίζει τα περιεχόμενα του τρέχοντος καταλόγου;
2.20 Γιατί η εντολή PORT του πρωτοκόλλου FTP προηγείται της εντολής της ερώτησης 2.19;
2.21 Σε ποια εντολή του πρωτοκόλλου FTP μεταφράζεται η εντολή bye του προγράμματος φλοιού ftp;
2.22 Με ποιο μήνυμα αποκρίνεται ο εξυπηρετητής FTP στην εντολή bye του προγράμματος φλοιού ftp;
2.23 Εφαρμόστε φίλτρο απεικόνισης ώστε να παραμείνουν μόνο τεμάχια με τη σημαία FIN ενεργοποιημένη. Ποια είναι η σύνταξή του;

2.24 Από ποια πλευρά (του πελάτη ή του εξυπηρετητή) γίνεται η απόλυση των συνδέσεων TCP που αφορούν τις εντολές *ελέγχου* και μηνύματα *δεδομένων* του FTP;

Στη συνέχεια θα παρατηρήσετε την κίνηση όταν χρησιμοποιείτε τον παθητικό τρόπο λειτουργίας του ftp. Αρχίστε μια νέα καταγραφή με το Wireshark και συνδεθείτε με anonymous ftp στο edu-dy.cn.ntua.gr χρησιμοποιώντας το γραφικό περιβάλλον του υπολογιστή σας. Σε Windows ανοίξτε τον File Explorer, κάντε κλικ στο Quick Access και γράψτε ftp://edu-dy.cn.ntua.gr. Σε περιβάλλον Linux, εάν δεν υπάρχει, εγκαταστήστε ένα πελάτη ftp όπως π.χ. FileZilla ή Nautilous, δώστε edu-dy.cn.ntua.gr ως προορισμό και επιλέξτε anonymous πρόσβαση. Αφού εμφανισθεί στην οθόνη η λίστα των αρχείων του edu-dy.cn.ntua.gr κλείστε το παράθυρο και σταματήστε την καταγραφή.

2.25 Καταγράψτε τις θύρες (πηγής και προορισμού) που χρησιμοποιούνται για την επικοινωνία FTP τόσο για τις εντολές *ελέγχου* όσο και για τη μεταφορά *δεδομένων*. *[Υπόδειξη: Χρησιμοποιήστε φίλτρο απεικόνισης ώστε να παραμείνουν μόνο τεμάχια των τριπλών χειραψιών με τη σημαία SYN ενεργοποιημένη]*.

2.26 Καταγράψτε τις εντολές FTP που έστειλε ο πελάτης στον εξυπηρετητή. *[Υπόδειξη: Χρησιμοποιήστε φίλτρο απεικόνισης ftp.request.command]*.

2.27 Αν η σύνδεση στον εξυπηρετητή FTP γινόταν με χρήση της διεύθυνσης ftp://user:password@edu-dy.cn.ntua.gr, στην καταγραφή ως όνομα χρήστη θα βλέπατε το user και ως κωδικό χρήστη το password. Στη δική σας περίπτωση, ποιο όνομα και ποιος κωδικός χρήστη χρησιμοποιήθηκε;

2.28 Ποια εντολή του πρωτοκόλλου FTP χρησιμοποιήθηκε για την εμφάνιση της λίστας αρχείων;

2.29 Καταγράψτε το μήνυμα με το οποίο αποκρίνεται ο εξυπηρετητής στην εντολή PASV. *[Υπόδειξη: Εφαρμόστε νέο φίλτρο απεικόνισης ώστε να βλέπετε και τις αποκρίσεις στις εντολές FTP]*.

2.30 Από ποια πλευρά (του πελάτη ή του εξυπηρετητή) γίνεται η εγκατάσταση της σύνδεσης TCP που αφορά τα μηνύματα *δεδομένων* του FTP; *[Υπόδειξη: Χρησιμοποιήστε φίλτρο απεικόνισης ώστε να παραμείνουν μόνο τεμάχια με τη σημαία SYN ενεργοποιημένη]*.

2.31 Για τη μεταφορά *δεδομένων* FTP, ο εξυπηρετητής δεν χρησιμοποιεί τη θύρα 20. Ποια θύρα του εξυπηρετητή χρησιμοποιείται και πώς προκύπτει ο αριθμός της από τα στοιχεία της απάντησης που καταγράψατε στην ερώτηση 2.29;

2.32 Πώς προκύπτει ο αριθμός θύρας της σύνδεσης TCP για μεταφορά *δεδομένων* FTP στην πλευρά του πελάτη;

Εφαρμόστε τώρα το φίλτρο απεικόνισης ftp-data ώστε να εμφανισθεί η ανταλλαγή δεδομένων μέσω της σύνδεσης δεδομένων FTP.

2.33 Πόσα μηνύματα *δεδομένων* FTP στάλθηκαν από τον εξυπηρετητή και ποιο το μέγεθος των δεδομένων που μεταφέρουν;

2.34 Δικαιολογήστε το μέγεθος του πρώτου από τα προηγούμενα μηνύματα *δεδομένων* FTP.

2.35 Από ποια πλευρά (του πελάτη ή του εξυπηρετητή) γίνεται η απόλυση των συνδέσεων TCP που αφορούν τις εντολές *ελέγχου* του FTP;

2.36 Από ποια πλευρά (του πελάτη ή του εξυπηρετητή) γίνεται η απόλυση της σύνδεσης TCP που αφορά τα μηνύματα *δεδομένων* FTP;

3. TFTP

Το Trivial FTP (TFTP) είναι ένα απλό πρωτόκολλο για μεταφορά αρχείων που ορίζεται στο RFC 1350. Χρησιμοποιείται από ένα πελάτη για να λάβει ή να στείλει κάποιο αρχείο σε εξυπηρετητή TFTP. Λόγω της απλότητάς του υλοποιείται εύκολα και σε λίγες γραμμές κώδικα. Αρχικά χρησιμοποιήθηκε σε συνδυασμό με το BOOTP από υπολογιστές κατά την εκκίνησή τους για να λάβουν την εικόνα του λειτουργικού τους συστήματος από κάποιον εξυπηρετητή στο τοπικό δίκτυο. Παρότι δεν χρησιμοποιείται πλέον για μεταφορά αρχείων στο διαδίκτυο, η χρήση του για κατέβασμα εικόνων firmware και αρχείων διάρθρωσης δικτυακών συσκευών, όπως δρομολογητές,

τείχη προστασίας κλπ είναι διαδεδομένη καθώς δεν απαιτείται όνομα χρήστη και συνθηματικό για την πρόσβαση στον εξυπηρετητή.

Εάν χρησιμοποιείτε λειτουργικό σύστημα Windows θα πρέπει ρητά να ενεργοποιήσετε την εφαρμογή πελάτη tftp από το *Turn Windows features on or off*. Επίσης θα πρέπει να προσθέσετε κανόνα στο τείχος προστασίας που να επιτρέπει την κίνηση που παράγεται από το εκτελέσιμο πρόγραμμα tftp.exe. Σε συστήματα Unix/Linux, εάν δεν υπάρχει, θα χρειαστεί να την εγκαταστήσετε.

Παραμένοντας συνδεδεμένοι μέσω OpenVPN στο εσωτερικό δίκτυο του ΕΜΠ, καταγράψτε με τη βοήθεια του Wireshark την κίνηση ενώ κάνετε χρήση της υπηρεσίας TFTP του υπολογιστή edu-dy.cn.ntua.gr (147.102.40.15). Εάν το Wireshark δεν αποκωδικοποιεί τα μηνύματα TFTP ίσως χρειαστεί να εγκαταστήσετε την προηγούμενη ευσταθή έκδοση 3.4. Όπως πριν, εφαρμόστε φίλτρο σύλληψης για να παρατηρείτε μόνο την κίνηση που σχετίζεται με το edu-dy.cn.ntua.gr. Για τη χρήση της υπηρεσίας TFTP στα Windows πληκτρολογήστε `tftp edu-dy.cn.ntua.gr get rfc1350.txt` σε ένα παράθυρο εντολών. Σε περιβάλλον Unix/Linux πληκτρολογήστε `tftp edu-dy.cn.ntua` και μετά `get rfc1350.txt`. Αφού σταματήσετε την καταγραφή κίνησης, εφαρμόστε το φίλτρο απεικόνισης για να παρατηρείτε μόνο την κίνηση (πακέτα IPv4) που σχετίζεται με το edu-dy.cn.ntua.gr.

3.1 Ποιο πρωτόκολλο μεταφοράς χρησιμοποιεί το TFTP (TCP ή UDP);
3.2 Καταγράψτε τις θύρες (πηγής και προορισμού) του πρωτοκόλλου μεταφοράς που χρησιμοποιούνται για την *πρώτη* επικοινωνία του πελάτη με τον εξυπηρετητή TFTP.
3.3 Καταγράψτε τις θύρες (πηγής και προορισμού) του πρωτοκόλλου μεταφοράς που χρησιμοποιούνται κατά τη μεταφορά δεδομένων.
3.4 Ποια από τις παραπάνω θύρες αντιστοιχεί στο πρωτόκολλο εφαρμογής TFTP;
3.5 Πώς προκύπτουν οι αριθμοί θυρών που χρησιμοποιούνται κατά τη μεταφορά δεδομένων; *[Υπόδειξη: Δείτε παράγραφο για το Initial Connection Protocol στο RFC 1350]*.
3.6 Η μεταφορά του αρχείου rfc1350.txt γίνεται σε δυαδικό (binary) τρόπο (mode) ή ASCII;
3.7 Σε ποιο μήνυμα TFTP μεταξύ πελάτη – εξυπηρετητή καθορίζεται αυτό και με ποιο τρόπο;
3.8 Καταγράψτε όλους του τύπους μηνυμάτων TFTP που παρατηρήσατε.
3.9 Το πρωτόκολλο μεταφοράς UDP είναι αναξιόπιστο καθώς δεν παρέχει μηχανισμό επιβεβαιώσεων, όπως το TCP. Πώς αντιμετωπίζει το πρόβλημα αυτό το TFTP;
3.10 Ποιος τύπος μηνύματος TFTP και ποιο πεδίο της επικεφαλίδας χρησιμοποιείται για τον σκοπό αυτό;
3.11 Ποιο είναι το μέγεθος των μηνυμάτων TFTP (πλην του τελευταίου) που μεταφέρουν τα προς μετάδοση δεδομένα;
3.12 Ποιο είναι το μέγεθος των δεδομένων που μεταφέρονται από αυτά τα μηνύματα TFTP;
3.13 Πώς αντιλαμβάνεται ο πελάτης το τέλος της μετάδοσης δεδομένων; *[Υπόδειξη: Αναζητήστε τον όρο Normal Termination στο RFC 1350]*.

Όνοματεπώνυμο: Νικόλας Μπέλλος	**Ομάδα:** 3
Όνομα PC/ΛΣ: BELLOS-DELL-G3	**Ημερομηνία:** 20 / 12 / 2021
Διεύθυνση IP: 147 . 102 . 136 . 53	**Διεύθυνση MAC:** 7C - 2A - 31 - 40 - C9 - AF

Εργαστηριακή Άσκηση 8
TELNET, FTP και TFTP

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

1

1.1 Το πρωτόκολλο TCP

1.2 Χρησιμοποιούνται οι θύρες 23 και 52117

1.3 Η θύρα 23

1.4 Display filter : telnet

1.5 Commands : Will Echo, Won't Echo, Do Echo, Don't Echo

1.6 Δεν υπάρχει κάποιο Do Echo προς τον υπολογιστή μου, οπότε δεν ζητάει (Υπάρχει ωστόσο Will Echo)

1.7 Ναι, το ζητάει και ο υπολογιστής μου απαντάει με Won't Echo, επομένως δέχεται

1.8 Όχι, δεν προτίθεται γιατί δεν υπάρχει Will Echo από τον εξυπηρετητή

1.9 Ναι, ο υπολογιστής μου στέλνει Do Echo

1.10 Ο εξυπηρετητής επαναλαμβάνει τους χαρακτήρες

1.11 Λόγω του Do Echo από τον υπολογιστή μου, ο εξυπηρετητής αποδέχθηκε αυτή την εντολή

1.12 Display filter : telnet and ip.src == 192.168.1.9

1.13 5 πακέτα

1.14 5 πακέτα

1.15 Όχι, δεν στέλνει

1.16 Όχι

1.17 Γιατί το εικονικό τερματικό αναγνωρίζει ότι πρόκειται για κωδικό

1.18 Δεν παρέχει κρυπτογράφιση των πακέτων και επομένως δεν είναι ασφαλή υπηρεσία (σε αντίθεση πχ με το SSH)

2

2.1 Capture filter : host 147.102.40.15

2.2 Επιτρέπει το debugging

2.3 Το TCP

2.4 Source Port: 52474

Destination Port: 21

2.5 Του πελάτη

2.6 OPTS, USER, PASS, HELP, PORT, NLST, QUIT

2.7 Εμφανίζονται με ένα βελάτι στα αριστερά τους

2.8 Με την USER

2.9 1 πακέτο

2.10 Με την PASS

2.11 1 πακέτο

2.12 Ομοιότητα : Δεν είναι κρυπτογραφημένα, Διαφορά : Το FTP τα μεταφέρει ως ένα πακέτο, ενώ το TELNET ως πολλαπλά πακέτα

2.13 Οχι, δεν μεταφράζεται

2.14 ascii, verbose

2.15 1 από τον υπολογιστή μου και 9 από τον εξυπηρετητή

2.16 Υπάρχει κενό αντί για παύλα “-” μετά το κωδικό στο τελευταίο πακέτο

2.17 Την IP του αποστολέα

2.18 2 τελευταίοι αριθμοί του PORT : 206, 129.

Ο αριθμός της θύρας προκύπτει ως : 206 * 256 + 129

2.19 Η NLST

2.20 Γιατί πρέπει να έχει υπολογιστεί πρώτα η κατάλληλη πόρτα

2.21 QUIT

2.22 221 Goodbye.

2.23 Display filter : tcp.flags.fin == 1

2.24 Του εξυπηρετητή

2.25 Source Port: 21

Destination Port: 50751

2.26 USER, PASS, opts, stst, site, PWD, TYPE, PASV, LIST

2.27 anonymous και IEUser

2.28 LIST

2.29 227 Entering Passive Mode (147,102,40,15,80,164).

2.30 Του πελάτη

2.31 2 τελευταίοι αριθμοί του PORT : 80, 164.

Χρησιμοποιεί τη πόρτα 80*256+164=20644

2.32 Γίνεται επιλογή από τις διαθέσιμες πόρτες

2.33 2 μηνύματα, μεγέθους 536bytes και 490 byte.

2.34 Πρόκειται για το μέγιστο μέγεθος δεδομένων λόγω της MTU

2.35 Του πελάτη

2.36 Του εξυπηρετητή

3

3.1 Το UDP

3.2 Source Port: 54916, Destination Port: 69

3.3 Source Port: 50352, Destination Port: 54916

3.4 Η 69

3.5 Από το UDP Header

3.6 ASCII

3.7 Στο Read request, με πεδίο Transfer Type: netascii

3.8 Read Request, Data Packet, Error Code

3.9 Επαναλαμβάνει τα δεδομένα που στέλνει

3.10 Read Request

3.11 558 bytes

3.12 512 bytes

3.13 Από το 'Null Destination File'