Εργαστηριακή Άσκηση 8
TELNET, FTP και TFTP

Ο σκοπός αυτού του εργαστηρίου είναι η εξέταση πρωτοκόλλων εφαρμογής που χρησιμοποιούνται ευρύτατα στο διαδίκτυο για την πρόσβαση και μεταφορά αρχείων από/προς απομακρυσμένους υπολογιστές. Στο πλαίσιο αυτό, θα εξετάσετε τις υπηρεσίες TELNET, FTP και TFTP, με τη βοήθεια του αναλυτή πρωτοκόλλων Wireshark. Εδώ θα χρησιμοποιήσετε τη λειτουργία *Capture* με φίλτρο, ώστε τα πλαίσια που καταγράφονται να περιέχουν κάποια συγκεκριμένα χαρακτηριστικά. Υπενθυμίζεται ότι το φίλτρο απεικόνισης *(Display)*, που επιλέγετε από το μενού *Analyze,* μπορεί να (απ)ενεργοποιηθεί οποιαδήποτε στιγμή κατά τη διάρκεια της καταγραφής, καθώς επίσης και μετά την ολοκλήρωση αυτής, προκειμένου να αποκρύπτει (αποκαλύπτει) κάποια από τα συλληφθέντα πλαίσια, ενώ το φίλτρο σύλληψης, που επιλέγετε από το μενού *Capture*, ενεργοποιείται πάντοτε **πριν** ξεκινήσει η διαδικασία καταγραφής, με αποτέλεσμα να καταγράφεται μόνο ένα μέρος των διερχόμενων πλαισίων.

1. Υπηρεσία TELNET – TELecommunication NETwork (RFC 854)

Με τη βοήθεια του Wireshark, καταγράψτε την κίνηση ενώ κάνετε χρήση της υπηρεσίας Telnet του υπολογιστή `edu-dy.cn.ntua.gr` (`147.102.40.9`). Εφαρμόστε φίλτρο σύλληψης `host 147.102.40.9` 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 `Microsoft Telnet>` 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;

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

1.4 Παρατηρήστε τις λεπτομέρειες του πακέτου που ακολουθεί και καταγράψτε την εντολή (command) TELNET που μεταφέρει.
1.5 Τι σημαίνει η εντολή αυτή για τα δεδομένα που ακολουθούν. *[Υπόδειξη: Ανατρέξατε στο RFC 857(http://www.faqs.org/rfcs/rfc857.html) για τη χρήση των εντολών "echo"]*.

Από το μενού *Analyze* επιλέγοντας *Follow TCP Stream*, εμφανίζεται παράθυρο όπου μπορείτε να παρατηρήσετε ολόκληρη τη ροή της 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 μεγεθύνατε το παράθυρο ώστε να δείτε το τέλος των γραμμών όπου εμφανίζονται οι χαρακτήρες ASCII).

1.6 Τι συμβαίνει κατά τη μεταφορά του ονόματος χρήστη που αποστείλατε μετά την πρώτη προτροπή login;

1.7 Εξηγείστε το φαινόμενο που παρατηρείτε στο προηγούμενο ερώτημα με βάση την απάντηση στα ερωτήματα 1.4 και 1.5.
1.8 Κλείστε τώρα το παράθυρο Follow TCP Stream και εντοπίστε τα πακέτα IP όπου μεταφέρεται η πληροφορία για το όνομα (`abcd`). Πόσα πακέτα IP χρειάζονται για να μεταφερθεί το όνομα χρήστη; *[Υπόδειξη: αναζητείστε μόνο μεταξύ των μηνυμάτων* `Telnet data` *… που ακολουθούν το μήνυμα telnet που περιέχει την προτροπή login, αφού προηγουμένως εφαρμόσετε φίλτρο απεικόνισης* `ip.dst==147.102.40.9`*]*.
1.9 Εντοπίστε τα πακέτα IP όπου μεταφέρεται η πληροφορία για τον κωδικό του χρήστη (`efgh`). Πόσα πακέτα IP χρειάζονται για να μεταφερθεί ο κωδικός του χρήστη;

Ακυρώστε το προηγούμενο φίλτρο απεικόνισης `ip.dst==147.102.40.9`.

1.10 Ο εξυπηρετητής στέλνει την ηχώ των χαρακτήρων `efgh` του κωδικού χρήστη προς τον πελάτη;
1.11 Παρατηρήσατε εντολή (command) TELNET "Don't Echo" πριν τη μεταφορά του κωδικού;
1.12 Εάν η απάντηση στην προηγούμενη ερώτηση είναι όχι, γιατί δεν εμφανίζεται στην οθόνη ο κωδικός;
1.13 Σχολιάστε την ασφάλεια της υπηρεσίας Telnet.

2. Υπηρεσία FTP – File Transfer Protocol (RFC 959)

Η άσκηση αυτή αναλύει, μεταξύ άλλων, τους δύο τρόπους λειτουργίας της υπηρεσίας FTP: α) τον *ενεργό* (active mode) και β) τον *παθητικό* (passive mode). Η υπηρεσία FTP έχει την ιδιαιτερότητα να χρησιμοποιεί δύο θύρες, μία για "δεδομένα" και μία για "εντολές". Η θύρα για τις εντολές ελέγχου (ftp) είναι συγκεκριμένη. Η θύρα για τη μεταφορά δεδομένων (ftp-data) είναι συγκεκριμένη στην περίπτωση του ενεργού τρόπου λειτουργίας, ενώ στην περίπτωση παθητικού τρόπου λειτουργίας προσδιορίζεται δυναμικά. Μια αναλυτική περιγραφή των δύο τρόπων λειτουργίας και άλλες πληροφορίες για το FTP μπορείτε να βρείτε στην ιστοσελίδα: http://www.troubleshootingnetworks.com/ftpinfo.html.

Τα Windows παρέχουν δύο διαφορετικά προγράμματα – πελάτες, καθένα από τα οποία χρησιμοποιεί διαφορετικό τρόπο λειτουργίας (mode) του FTP: το ένα είναι το πρόγραμμα φλοιού `ftp`, ενώ το άλλο βρίσκεται ενσωματωμένο στον Internet Explorer. Άλλωστε, οι περισσότεροι πλοηγοί ιστού διαθέτουν τη δυνατότητα FTP, και την ενεργοποιούν για διευθύνσεις URI που αρχίζουν με `ftp://` (αντί για `http://`).

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.

Με τη βοήθεια του Wireshark, θα καταγράψετε την κίνηση ενώ κάνετε χρήση της υπηρεσίας FTP του υπολογιστή `edu-dy.cn.ntua.gr` (`147.102.40.9`). Όπως πριν, εφαρμόστε φίλτρο σύλληψης για να παρατηρείτε μόνο την κίνηση που σχετίζεται με το `edu-dy.cn.ntua.gr`. Αρχίστε μια καταγραφή και πληκτρολογήστε `ftp –d edu-dy.cn.ntua.gr` σε ένα παράθυρο εντολών. Στην προτροπή `User:` πληκτρολογήστε `anonymous`, ενώ στην προτροπή `Password:`

πληκτρολογήστε `labuser@cn`. Αφού συνδεθείτε, δώστε τις εντολές `help` και `remotehelp`. Στη συνέχεια δώστε την εντολή `ls` για να δείτε[1] 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: Χρησιμοποιείστε φίλτρο απεικόνισης* `tcp.flags.syn==1` *ώστε να παραμείνουν μόνο τεμάχια των τριμερών 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 (6 συνολικά) που έστειλε ο πελάτης στον εξυπηρετητή. *[Υπόδειξη: Χρησιμοποιείστε 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 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, 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;
2.17 Εντοπίστε 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 στην οποία ο πελάτης αναμένει να λάβει δεδομένα. Τον αριθμό αυτό, τον έχετε καταγράψει προηγουμένως στην απάντηση της ερώτησης 2.4.

2.18 Πώς προκύπτει αυτός ο αριθμός από τα δεδομένα της εντολής PORT; *[Υπόδειξη: Συμβουλευτείτε το παράδειγμα που περιγράφεται στην ενότητα "The FTP PORT Command" στην* http://www.troubleshootingnetworks.com/ftpinfo.html*]*.

[1] Αν εμφανιστεί παράθυρο σχετικό με το τείχος πυρασφάλειας (firewall) των Windows πατήστε OK.

2.19 Ποιο τρόπο λειτουργίας (ενεργό ή παθητικό) του πρωτοκόλλου FTP υλοποιεί η εντολή φλοιού `ftp`;

2.20 Στο πρόγραμμα φλοιού `ftp` η εντολή `ls` προκαλεί την εντολή NLST του πρωτοκόλλου FTP. Γιατί η εντολή FTP τύπου PORT προηγείται της NLST;

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 της σύνδεσης TCP που αφορά τα μηνύματα *δεδομένων* του FTP;

Κατόπιν, αρχίστε μια νέα καταγραφή με το Wireshark και με τη βοήθεια του MS Internet Explorer[2], επισκεφθείτε το `ftp://edu-dy.cn.ntua.gr` 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: Χρησιμοποιείστε φίλτρο απεικόνισης ώστε να παραμείνουν μόνο τεμάχια των τριμερών χειραψιών με τη σημαία SYN ενεργοποιημένη]*.

2.26 Αν η σύνδεση στον εξυπηρετητή FTP γινόταν με χρήση της διεύθυνσης `ftp://user:password@edu-dy.cn.ntua.gr`, ο Internet Explorer θα χρησιμοποιούσε ως όνομα χρήστη το `user` και ως κωδικό χρήστη το `password`. Στη δική σας περίπτωση, ποιο όνομα και ποιος κωδικός χρήστη χρησιμοποιήθηκε; *[Υπόδειξη: Χρησιμοποιείστε φίλτρο απεικόνισης `ftp.request.command`]*.

2.27 Ποια εντολή του πρωτοκόλλου FTP, αντίστοιχη της NLST, χρησιμοποιεί ο Internet Explorer για την εμφάνιση των περιεχομένων ενός καταλόγου;

2.28 Εντοπίστε το μήνυμα FTP που μεταφέρει την εντολή PASV. Ποιο τρόπο λειτουργίας (ενεργό ή παθητικό) του πρωτοκόλλου FTP υλοποιεί ο Internet Explorer;

2.29 Καταγράψτε το μήνυμα με το οποίο αποκρίνεται ο εξυπηρετητής; *[Υπόδειξη: Εφαρμόστε νέο φίλτρο απεικόνισης ώστε να παραμείνουν μόνο μηνύματα σχετικά με 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: Χρησιμοποιείστε 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 χρησιμοποιείται και πώς προκύπτει ο αριθμός της από τα στοιχεία της απάντησης του εξυπηρετητή που καταγράψατε στην ερώτηση 2.29;

2.32 Πώς προκύπτει ο αριθμός της θύρας πηγής της σύνδεσης TCP που αφορά τα μηνύματα *δεδομένων* του FTP;

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

2.33 Πόσα μηνύματα δεδομένων στάλθηκαν από τον εξυπηρετητή FTP και ποιο το μέγεθος των δεδομένων αυτών;

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

[2] Αν εμφανιστεί παράθυρο σχετικό με την ενεργοποίηση του φίλτρου Phishing του Internet Explorer, επιλέξτε 'Turn on automatic Phishing Filter' και πατήστε OK.

3. Υπηρεσία TFTP – Trivial FTP (RFC 1350)

Με τη βοήθεια του Wireshark, καταγράψτε την κίνηση ενώ κάνετε χρήση της υπηρεσίας TFTP του υπολογιστή `edu-dy.cn.ntua.gr` (`147.102.40.9`). Για τη χρήση της υπηρεσίας TFTP πληκτρολογήστε `tftp edu-dy.cn.ntua.gr get rfc1350.txt` σε ένα παράθυρο εντολών. Αφού σταματήσετε την καταγραφή κίνησης, εφαρμόστε το φίλτρο απεικόνισης για να παρατηρείτε μόνο την κίνηση (πακέτα IP) που σχετίζεται με το `edu-dy.cn.ece.ntua.gr`.

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

Όνοματεπώνυμο:	Όνομα PC:
Ομάδα:	Ημερομηνία:
Διεύθυνση IP: . . .	Διεύθυνση MAC: - - - - -

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 .....

1.2 .....

1.3 .....

1.4 .....

1.5 .....

.....

.....

1.6 .....

.....

.....

1.7 .....

.....

.....

1.8 .....

1.9 .....

1.10 .....

1.11 .....

1.12 .....

.....

.....

1.13 .....

.....

.....

2

2.1 .....

2.2 .....

2.3 .....

2.4 .....

2.31 .....

.....

2.32 .....

.....

2.33 .....

.....

2.34 .....

3

3.1 .....

3.2 .....

3.3 .....

3.4 .....

3.5 .....

3.6 .....

.....

3.7 .....

3.8 .....

.....

3.9 .....

.....

.....

3.10 .....

3.11 .....

3.12 .....

.....

.....