

Εθνικό Μετσόβιο Πολυτεχνείο
Δίκτυα Υπολογιστών
Χειμερινό Εξάμηνο 2022-2023

Όνομα:

Ιωάννης Μπασδέκης - 03119198



8η Εργαστηριακή Αναφορά

Μέρος 1ο

1.1) tcp

1.2) 23 και 55141

1.3) 23 port (πασίγνωστη θύρα TELNET)

1.4) telnet

1.5) Server: will , do

Client: won't , do

1.6) Ναι ζητάει αλλά ο υπολογιστής μου δεν δέχεται

1.7) Όχι

1.8) Ναι

1.9) Ναι

1.10) Υπάρχει echoing στους χαρακτήρες του ονόματος login από τον εξυπηρετητή σε εμάς (τιμή : aabbbccdd) λαμβάνεται όμως το abcd

1.11) Ο εξυπηρετητής ζητάει να κάνει echo και ο υπολογιστής μας στέλνει do echo επομένως γίνεται echo απο την μεριά του εξυπηρετητή

1.12) ip.src == 192.168.0.106 and telnet

1.13) 5 πακέτα (4 για τα δεδομένα 1 για το CR)

1.14) 5 πακέτα (4 για τα δεδομένα 1 για το CR)

1.15) Όχι

1.16) Όχι

1.17) Μάλλον εξ αιτίας της υλοποίησης του telnet όταν πρόκειται για password δεν γίνεται echo

1.18) Δεν γίνεται encryption οπότε με τεχνικές hacking (spoofing , man in the middle) ή ακόμα και να δωθεί καταλάθος κάπως κάποιο πακέτο σε εμάς μπορούμε να βρούμε τα δεδομένα ενός χρήστη. Άρα είναι πολύ ευάλωτη και για αυτό χρησιμοποιούμε το SSH

Μέρος 2ο

2.1) host 147.102.40.15

2.2) debug

2.3) tcp

2.4) ελέγχου : 21 -> 62789

data : 22065 -> 62792

(χρησιμοποιώ ncftp γιατί το mac δεν έχει την εντολή ftp)

2.5) Από εμάς στον εξυπηρετητή

2.6) USER, PASS, PWD, FEAT, HELP SITE, CLNT NcFTP 3.2.6

macosx12.0.1, HELP, OPTS MLST

type;size;modify;UNIX.mode;perm;UNIX.owner;UNIX.group; , PASV , MLSD , QUIT

2.7) Στο τέρμιναλ μετά την εντολή

2.8) USER

2.9) 1

2.10) PASS

2.11) 1

2.12) χρησιμοποιούν και τα δύο εντολές για μεταφορά. Στο ftp το user και το pass μεταφέρονται σαν ένα πακέτο χωρίς δυνατότητα echo ενώ στο telnet μεταφέρονται ένας ένας οι χαρακτήρες και υπάρχει επιλογή για echo

2.13) όχι

2.14) AUTH, CONF

2.15) 9 response απο τον εξυπηρετητη και 2 tcp ack απο εμάς

2.16) Το τελευταίο πακέτο ξεκινάει με το response code 214 αλλα χωρις το hyphen

2.17) Δεν μου το εμφανίζει εμένα αλλα με βάση μελέτης στο Ίντερνετ βρήκα ότι οι πρώτοι 4 αριθμοί δηλώνουν την IPv4 του πελάτη

2.18) Η θύρα είναι ο 5ος αριθμός επά 256 + τον 6ο αριθμό

2.19) MLSD

2.20) Γιατί πρώτα πρέπει να εγκατασταθεί η σύνδεση ftp για να μπορούμε να δούμε τους καταλόγους του server

2.21) QUIT

2.22) 221 Goodbye

2.23) tcp.flags.fin == 1

2.24) από την μεριά του πελάτη

2.25) ελέγχου : 21 -> 61329
data : 19545-> 61330

2.26) USER, SYST, PASS, PWD, TYPE I, CWD, PASV, PORT, LIST, RETR

2.27) User: anonymous
Pass : cfnetwork@apple.com

2.28) LIST

2.29) 227 Entering passive mode

2.30) client side

2.31)

2.32)

2.33) 8 πακέτα από 524 bytes εκτός του τελευταίου

2.34) Περιορισμένα από την MTU

2.35) Απο την πλευρά του εξυπηρετητή

2.36) Απο την πλευρά του εξυπηρετητή

Μέρος 3ο

3.1) udp

3.2) 57789 , 80

3.3) 69 , 51443 , 67823

3.4) 69

3.5) είναι τυχαία επιλεγμένες κατα την εκκίνηση της σύνδεσης (TID)

3.6) ASCII

3.7) στο header του TFTP στο πεδίο type με το πακέτο RRQ που στέλνουμε

3.8) RRQ , DATA , ACK

3.9) Για όλα τα datagrams που λαμβάνουμε στέλνουμε πίσω ένα ACK

3.10) TFTP ACK → Opcode: 4, Block: (acknowledged block number)

3.11) 516 bytes (524 bytes UDP datagram)

3.12) 512

3.13) Αν το μήκος είναι λιγότερο από 512 bytes