ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ & ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
Τομέας Επικοινωνιών, Ηλεκτρονικής & Συστημάτων Πληροφορικής
Εργαστήριο Διαχείρισης και Βέλτιστου Σχεδιασμού Δικτύων - NETMODE
Ηρώων Πολυτεχνείου 9, Ζωγράφου, 157 80 Αθήνα, Τηλ: 210-772.1448, Fax: 210-772.1452
e-mail: maglaris@mail.ntua.gr, URL: http://www.netmode.ntua.gr

Εξέταση στο Μάθημα:
"ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ - ΕΥΦΥΗ ΔΙΚΤΥΑ"
(9ο Εξάμηνο)
Διδάσκων: Β. Μάγκλαρης
24.01.2005

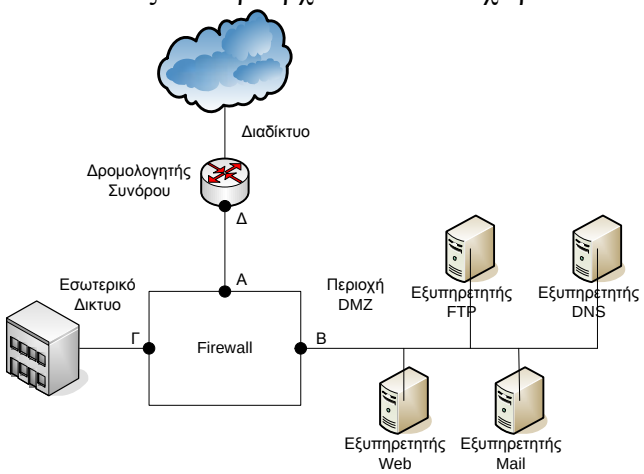
Παρακαλώ απαντήστε (χωρίς πολλά λόγια) σε όλες τις ερωτήσεις. Διάρκεια 2 ώρες.

Ανοικτά Βιβλία & Σημειώσεις. ΚΑΛΗ ΕΠΙΤΥΧΙΑ!

Οι βαθμοί θα ανακοινωθούν στο URL: www.netmode.ece.ntua.gr.

ΘΕΜΑ 1 (30%)

Στο δίκτυο του σχήματος χρησιμοποιείται ένα σύστημα Firewall για να προστατεύσει την περιοχή των εξυπηρετητών (Demilitarized Zone – DMZ) και το εσωτερικό δίκτυο ενός οργανισμού από απειλές που προέρχονται από το χώρο του Διαδικτύου.



α. Ο οργανισμός έχει αποκτήσει την περιοχή διευθύνσεων 212.5.2.0 με μάσκα 255.255.255.0. Ζητείται αυτή να κατατμηθεί με τη μέγιστη δυνατή οικονομία διευθύνσεων στα εξής υποδίκτυα (με αυτή τη σειρά):

- Ένα υποδίκτυο με 64 διαθέσιμες διευθύνσεις για το εσωτερικό δίκτυο.
- Ένα υποδίκτυο με 16 διαθέσιμες διευθύνσεις για την περιοχή DMZ.
- Ένα υποδίκτυο για τη σύνδεση Δρομολογητή - Firewall.

Από τις περιοχές που προσδιορίσατε δώστε συγκεκριμένες διευθύνσεις στα 3 Interfaces του Firewall (Α, Β και Γ) και το Interface Δ του Δρομολογητή.

β. Μια από τις πολιτικές ασφαλείας του οργανισμού έχει τη μορφή:
Στην περιοχή DMZ επιτρέπονται οι κλήσεις προς υπηρεσίες Web (TCP port 80), Mail (TCP port 25), DNS (UDP port 53) και FTP (TCP port 21) και απαγορεύονται όλες οι άλλες συνδέσεις.
Διατυπώστε την πολιτική αυτή ασφαλείας με ένα φίλτρο που περιέχει τους λιγότερους δυνατούς κανόνες της μορφής:

<RuleNo> <Action (allow/deny)> <protocol (TCP/UDP/ANY)> <srcIP/Mask(ή ANY)> <srcPort(ή ANY)> <dstIP/Mask(ή ANY)><dstPort (ή ANY)>

Επίσης να αναφέρετε σε ποιο από τα 3 interfaces του Firewall (A, B ή Γ) πρέπει να εφαρμοστεί το φίλτρο και σε ποια κατεύθυνση (IN/OUT).

ΘΕΜΑ 2 (30%)

1. Ορίσατε τα απαραίτητα αντικείμενα (objects) της SNMP MIB ενός Wireless Access Point.

Γενικές πληροφορίες:

Περιγραφή συσκευής, Υπεύθυνος διαχειριστής, Διάρκεια λειτουργίας, Χρήση κρυπτογραφίας (Off, WEP, WPA)

Πίνακας Σταθμών συνδεδεμένων στο Wireless Access Point

Φυσική διεύθυνση σταθμού (MAC address), Πακέτα από το σταθμό, Πακέτα προς το σταθμό, Ένταση σήματος λήψης.

Πίνακας Σταθμών που επιτρέπεται να συνδεθούν στο Wireless Access Point

Φυσική διεύθυνση σταθμού (MAC address)

Η περιγραφή των αντικειμένων πρέπει να ακολουθεί την ακόλουθη μορφή (όχι πλήρη περιγραφή ASN.1):

```
xObject
                SYNTAX          DisplayString
                DESCRIPTION     "Το αντικείμενο αυτό περιγράφει...."
                :: = {θέση στο δένδρο της Wireless-MIB}
```

Για τους τύπους των αντικειμένων συμβουλευτείτε το Παράρτημα Β των σημειώσεων. Θεωρήστε ότι η ζητούμενη MIB έχει ρίζα τη "Wireless-MIB".

2. Τι αλλαγές πρέπει να γίνουν στον Πίνακα Επιτρεπόμενων Σταθμών ώστε αυτός να γίνει επανεγγράψιμος και να μπορούν να προστεθούν ή να αφαιρεθούν σταθμοί;

ΘΕΜΑ 3 (20%)

Δίνεται το παρακάτω τμήμα ενός packet trace από τον υπολογιστή matrix.netmode.ece.ntua.gr (147.102.13.60):

1	**Header 1**: Source: 00:02:3f:36:0c:3a, Destination: 00:02:b3:95:bd:24, Type: IP **Header 2**: Source: 147.102.13.60, Destination: 147.102.13.10, Protocol: UDP **Header 3**: Source port: 1033, Destination port: 53 (dns) **Header 4**: Queries: mafioso.netmode.ece.ntua.gr, type A, class inet
2	**Header 1**: Source: 00:02:b3:95:bd:24, Destination: 00:02:3f:36:0c:3a, Type: IP **Header 2**: Source: 147.102.13.10, Destination: 147.102.13.60, Protocol: UDP **Header 3**: Source port: 53 (dns), Destination port: 1033 **Header 4**: Answers: mafioso.netmode.ece.ntua.gr type A, class inet, addr 147.102.13.29
3	**Header 1**: Source: 00:02:3f:36:0c:3a, Destination: ff:ff:ff:ff:ff:ff, Type: ARP **Header 2**: Protocol Type: IP, Sender MAC address: 00:02:3f:36:0c:3a, Sender IP address: 147.102.13.60, Target MAC address: 00:00:00:00:00:00, Target IP address: 147.102.13.29
4	**Header 1**: Source: 00:60:08:47:e0:40, Destination: 00:02:3f:36:0c:3a, Type: ARP **Header 2**: Protocol Type: IP, Sender MAC address: 00:60:08:47:e0:40, Sender IP address: 147.102.13.29, Target MAC address: 00:02:3f:36:0c:3a, Target IP address: 147.102.13.60
5	**Header 1**: Source: 00:02:3f:36:0c:3a, Destination: 00:60:08:47:e0:40, Type: IP **Header 2**: Source: 147.102.13.60, Destination: 147.102.13.29, Protocol: ICMP **Header 3**: Type: 8 (echo request) Code: 0
6	**Header 1**: Source: 00:60:08:47:e0:40, Destination: 00:02:3f:36:0c:3a, Type: IP **Header 2**: Source: 147.102.13.29, Destination: 147.102.13.60, Protocol: ICMP **Header 3**: Type: 0 (echo reply) Code: 0

1. Ομαδοποιήστε τα παραπάνω πακέτα σε ζεύγη ερώτησης – απάντησης του ίδιου πρωτοκόλλου.
2. Ποια πληροφορία ζητείται σε κάθε περίπτωση και μέσω ποιών πρωτοκόλλων; Ποιες είναι οι απαντήσεις σε κάθε περίπτωση;
3. Αν η παραπάνω ανταλλαγή πακέτων έχει προκληθεί από την εκτέλεση μιας και μόνο εντολής στον υπολογιστή 147.102.13.60, ποια πιστεύετε ότι είναι αυτή η εντολή;