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: 772.1448, Fax: 772.1452
e-mail: maglaris@mail.ntua.gr

Παρασκευή, 7 Φεβρουαρίου 2014

Διαχείριση Δικτύων – Ευφυή Δίκτυα

6η Ομάδα Ασκήσεων

Άσκηση 1

Ζητείται η συγγραφή μιας MIB για ένα σύστημα firewall. Το συγκεκριμένο σύστημα είναι ένας υπολογιστής με περισσότερα του ενός δικτυακά interfaces. Όλα τα interfaces υποστηρίζουν το IP πρωτόκολλο και ο υπολογιστής λειτουργεί ως δρομολογητής (προωθεί πακέτα μεταξύ των interfaces).
Η λειτουργία του συστήματος ως firewall έγκειται στην εφαρμογή φίλτρων στα πακέτα που διέρχονται από τα interfaces. Ένα φίλτρο είναι ένα σύνολο από κανόνες που καθορίζουν αν ένα πακέτο επιτρέπεται να διέλθει από το interface ή εάν πρέπει να απορριφθεί. Κάθε interface μπορεί να μην εφαρμόζει κανένα φίλτρο (όλα τα πακέτα διέρχονται ελεύθερα), να εφαρμόζει ένα φίλτρο στα εισερχόμενα από το δίκτυο πακέτα, να εφαρμόζει ένα φίλτρο στα εξερχόμενα προς το δίκτυο πακέτα ή να εφαρμόζει δύο φίλτρα (ένα σε κάθε κατεύθυνση).

Κάθε φίλτρο αποτελείται από ένα σύνολο κανόνων της παρακάτω μορφής:

```
<RuleNo> <Action> <Protocol> <SrcIP> <SrcMask> <DstIP> <DstMask> <SrcPort> <DstPort>
```

όπου:

RuleNo:	Αύξων αριθμός κανόνα (για το συγκεκριμένο φίλτρο)
Action:	Pass ή Drop (καθορίζει αν το διερχόμενο πακέτο θα προωθηθεί ή θα απορριφθεί)
Protocol:	IP, ICMP, TCP, UDP
SrcIP:	Source IP address του πακέτου
SrcMask:	Subnet mask που εφαρμόζεται στο Source IP address του πακέτου
DstIP:	Destination IP address του πακέτου
DstMask:	Subnet mask που εφαρμόζεται στο Destination IP address του πακέτου
SrcPort:	Source port του πακέτου (μπορεί να είναι αριθμός X ή εύρος X-Y)
DstPort:	Destination port του πακέτου (μπορεί να είναι αριθμός X ή εύρος X-Y)

Κάθε πακέτο που διέρχεται από το interface εξετάζεται διαδοχικά από όλους τους κανόνες του φίλτρου κατά αύξουσα σειρά RuleNo. Σε κάθε κανόνα εξετάζονται οι επικεφαλίδες του πακέτου και συγκρίνονται με τα αντίστοιχα πεδία του κανόνα (Protocol, SrcIP, κλπ). Εάν η σύγκριση είναι επιτυχής εφαρμόζεται το action του κανόνα (το πακέτο είτε προωθείται είτε απορρίπτεται οριστικά). Διαφορετικά εξετάζεται ο επόμενος κανόνας.
Η MIB που ζητείται θα πρέπει να περιλαμβάνει αντικείμενα που θα περιγράφουν τα φίλτρα, τους κανόνες τους και τις συσχετίσεις τους με τα interfaces. Φροντίστε να

μην περιλαμβάνεται περιττή πληροφορία για τα interfaces, καθώς το σύστημα υποστηρίζει ήδη την MIB-II. Επιπλέον ζητούνται και τα παρακάτω στοιχεία:

- Για κάθε κανόνα των φίλτρων να καταγράφεται πόσες φορές ενεργοποιήθηκε το action του.
- System Group που να περιέχει τις παρακάτω πληροφορίες: όνομα του συστήματος, email του διαχειριστή και χρόνο λειτουργίας του firewall.

Να παραδοθεί το σχήμα (σε μορφή δένδρου) και ο κώδικας της MIB. Η κωδικοποίηση θα πρέπει να γίνει τουλάχιστον με SNMPv2 SMI (RFCs 1901-1908). Τοποθετήστε τη MIB σε οποιοδήποτε σημείο του δένδρου αντικειμένων SNMP κάτω από το .iso αλλά δώστε συγκεκριμένες αριθμήσεις (Object IDs – OIDs) στα αντικείμενα σας.

Άσκηση 2.1

Στη άσκηση αυτή θα γίνει εξοικείωση με το εργαλείο Nagios, το οποίο αποτελεί ένα από τα πλέον διαδεδομένα Service Monitoring Tools. Στον υπολογιστή maria.netmode.ntua.gr έχει εγκατασταθεί το εργαλείο Nagios και έχει παραμετροποιηθεί κατάλληλα για να παρακολουθεί την κατάσταση ορισμένων από τους servers, τους δικτυακούς εκτυπωτές και τα switches του εργαστηρίου NETMODE, καθώς και ορισμένων άλλων απομακρυσμένων servers (εκτός του εργαστηρίου).
Στην άσκηση αυτή καλείστε μέσα από το web interface του Nagios να περιγράψετε την παραμετροποίηση που έχει γίνει από το διαχειριστή του μηχανήματος. Το web interface του Nagios βρίσκεται στο παρακάτω URL:

```
http://maria.netmode.ntua.gr/nagios/
```

και είναι προσβάσιμο (read-only access) με τα παρακάτω στοιχεία:

```
username: netmg
password: netmg
```

Ειδικότερα ζητάμε να απαντηθούν τα παρακάτω:

1. Πόσες και ποιες ομάδες δικτυακών συσκευών έχουν οριστεί.
2. Ποιες συγκεκριμένες συσκευές περιλαμβάνει η κάθε ομάδα και ποιες υπηρεσίες παρακολουθούνται σε κάθε συσκευή.
3. Πόσες και ποιες ομάδες υπηρεσιών έχουν οριστεί. Ποιες συσκευές περιλαμβάνει η κάθε ομάδα υπηρεσιών.
4. Ποιες από τις υπηρεσίες των συσκευών που παρακολουθούνται δεν στέλνουν ειδοποιήσεις στον διαχειριστή.
5. Ποιες από τις υπηρεσίες σε κάθε συσκευή βρίσκονται σε κατάσταση “WARNING”.
6. Ποιες από τις υπηρεσίες σε κάθε συσκευή βρίσκονται σε κατάσταση “CRITICAL”.
7. Πότε ξεκίνησε να «τρέχει» το Nagios Tool και πόσο χρόνο είναι ενεργό.
8. Για κάθε υπηρεσία σε κάθε συσκευή να αναφέρετε κάθε πότε πραγματοποιείται η μέτρηση (time-interval).

Άσκηση 2.2

Σημείωση:

- Για να εκτελέσετε τα plug-ins του Nagios, τα οποία είναι αυτόνομα προγράμματα, θα πρέπει να είστε στο φάκελο "/usr/local/libexec/nagios".

- Για περισσότερες πληροφορίες για τα plugins του Nagios εκτελέστε την κάθε εντολή-plugin με παράμετρο `--help`. (π.χ. `check_ping --help`).

- Ο κατάλογος με τα plugins του Nagios βρίσκεται στο directory: /usr/local/libexec/nagios.

Από το command line στον υπολογιστή maria.netmode.ntua.gr ζητούνται να εκτελεστούν οι παρακάτω εντολές για τα μηχανήματα www.imperial.ac.uk και www.harvard.edu, οι οποίες χρησιμοποιούν συγκεκριμένο plug-in του Nagios.

```
check_ping -4 –H <hostname> –w 50.0,50% -c 100.0,90%
check_ping -4 –H <hostname> –w 100.0,50% -c 200.0,90%
check_ping -4 –H <hostname> –w 200.0,50% -c 300.0,90%
```

1. Εξηγείστε για ποιο λόγο τα μηχανήματα www.imperial.ac.uk και www.harvard.edu βρίσκονται στην κατάσταση WARNING και CRITICAL αντίστοιχα όπως δηλώνεται στο web interface του Nagios.

2. Με βάση τις τιμές για το PING που έχει συλλέξει το Nagios, σε ποιες τιμές θεωρείτε ότι μπορεί να κυμαίνονται τα αντίστοιχα thresholds που έχουν οριστεί από τον διαχειριστή ώστε τα μηχανήματα να βρίσκονται σε αυτές τις καταστάσεις;

3. Δοκιμάστε να πειραματιστείτε και με άλλα plugins του Nagios και σημειώστε στις αναφορές σας την σύνταξη των εντολών που χρησιμοποιήσατε κατά την κλήση των plug-ins καθώς και τα αποτελέσματα που σας επέστρεψαν.