Εργαστήριο 2
Ασκήσεις: Διαχείριση Δικτύου (nmap, netstat)

Εργαλείο nmap (network mapper)

Το εργαλείο nmap είναι ένα ανοικτού κώδικα εργαλείο για την εξερεύνηση του δικτύου και τον έλεγχο της ασφάλειας. Το nmap είναι ένα από τα πολυτιμότερα και πιο γνωστά εργαλεία για τους διαχειριστές συστημάτων. Λειτουργεί ως σαρωτής ασφαλείας και χρησιμοποιείται για να ανακαλύψει κεντρικούς υπολογιστές και τις υπηρεσίες σε ένα δίκτυο υπολογιστών, δημιουργώντας έτσι ένα "χάρτη" του δικτύου. Η λειτουργία του παρέχει στο χρήστη μια αναλυτική εικόνα, του προς ελέγχου δικτύου φανερώνοντας πιθανά προβλήματα και ελλείψεις ασφάλειας. Στο εργαστήριο αυτό θα το χρησιμοποιήσετε για να σαρώσετε τη μηχανή σας και να ελέγξετε για το αν υπάρχουν ανοικτές θύρες (π.χ. η θύρα 22 του πρωτοκόλλου ssh) και ποιες είναι αυτές. Αν μια θύρα είναι ανοικτή, αυτό προφανώς σημαίνει ότι τρέχει κάποια υπηρεσία που «ακούει» στη θύρα αυτή. Γενικά, δεν υπάρχει λόγος να τρέχουν διάφορες επιπλέον υπηρεσίες, πέραν από αυτές που μας χρειάζονται σε μια μηχανή, γιατί μέσω των θυρών τους δύναται να εισέλθουν κακόβουλοι χρήστες.

Εργαλείο netstat (network statistics)

Το εργαλείο netstat είναι ένα χρήσιμο εργαλείο ελέγχου σε μια μηχανή:

- για την προβολή της δικτυακής δραστηριότητας. Μέσω της εντολής netstat -a μπορείτε να δείτε τις εισερχόμενες/εξερχόμενες τοπικές/διαδικτυακές συνδέσεις. Πιο συγκεκριμένα μπορείτε να δείτε όλα τα sockets[1] σε κατάσταση σύνδεσης ή σε κατάσταση αναμονής για σύνδεση). Μέσω της εντολής netstat -l μπορείτε να δείτε τα sockets που είναι σε κατάσταση αναμονής για σύνδεση, listening sockets.
- για την προβολή των πινάκων δρομολόγησης (routing tables) μέσω netstat -r,
- για την προβολή στατιστικών σχετικά με τις διεπαφές (interfaces) μέσω netstat -i
- και άλλα ενδιαφέροντα στοιχεία για τις δικτυακές διασυνδέσεις.

Η εντολή αυτή είναι σημαντική για κάθε χρήστη, καθώς μπορεί να δει εάν κάποιο trojan ή spyware, πραγματοποιεί συνδέσεις στη μηχανή του χωρίς να το γνωρίζει. Στο εργαστήριο αυτό μπορείτε να χρησιμοποιήσετε το εργαλείο για να δείτε στοιχεία για τις διεπαφές της μηχανής σας.

Χρήσιμες εντολές

Με τη βοήθεια των εντολών nmap, netstat μέσω του terminal μπορείτε να δείτε ποιες υπηρεσίες τρέχουν στη μηχανή σας (localhost – συζητούμε γι' αυτό πιο κάτω) και σε ποιες θύρες ακούνε. Οι πιο κάτω εντολές παρουσιάζουν πως μπορείτε να δείτε τις τρέχουσες υπηρεσίες της μηχανής σας:

- `nmap localhost`

  Το εργαλείο nmap είναι ένα ανοικτού κώδικα εργαλείο για την εξερεύνηση του δικτύου και τον έλεγχο της ασφάλειας. Το nmap είναι ένα από τα πολυτιμότερα και πιο γνωστά εργαλεία για τους διαχειριστές συστημάτων. Λειτουργεί ως σαρωτής ασφαλείας και χρησιμοποιείται για να ανακαλύψει κεντρικούς υπολογιστές και τις υπηρεσίες σε ένα δίκτυο υπολογιστών, δημιουργώντας έτσι ένα "χάρτη" του δικτύου. Η λειτουργία του παρέχει στο χρήστη μια αναλυτική εικόνα, του προς ελέγχου δικτύου φανερώνοντας πιθανά προβλήματα και ελλείψεις

1 Socket (υποδοχή) ονομάζεται το τερματικό σημείο (endpoint) ενός αμφίδρομου διαύλου επικοινωνίας (two-way communication link) μεταξύ 2 διεργασιών που επικοινωνούν μέσω του δικτύου (είτε βρίσκονται πάνω στην ίδια μηχανή ή βρίσκονται σε ξεχωριστές μηχανές).

ασφάλειας. Στο εργαστήριο αυτό θα το χρησιμοποιήσετε για να σαρώσετε τη μηχανή σας και να ελέγξετε για το αν υπάρχουν ανοικτές θύρες και ποιες είναι αυτές. Αν μια θύρα είναι ανοικτή, αυτό σημαίνει ότι τρέχει κάποια υπηρεσία που «ακούει» στη θύρα αυτή.

```
Starting Nmap 7.92 ( https://nmap.org ) at 2024-09-12 09:16 EEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000051s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
631/tcp  open  ipp
3389/tcp open  ms-wbt-server
5910/tcp open  cm
5911/tcp open  cpdlc

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

Από όσο βλέπετε, οι υπηρεσίες που τρέχουν στην πιο πάνω μηχανή είναι η ssh (ασφαλής απομακρυσμένη πρόσβαση στη TCP θύρα 22), η rpcbind (υπηρεσία για Remote Procedure Calls στη TCP θύρα 111), η ipp (internet printing protocol – CUPS service) η ms-wbt-server (υπηρεσία που υλοποιήθηκε από τη Microsoft για να επιτρέπει συνδέσεις πάνω πρωτοκόλλου Remote Desktop Protocol στη θύρα 3389 – απομακρυσμένη σύνδεση με γραφικό περιβάλλον), η cm (υπηρεσία content management στη θύρα 5910) και η cpdl (υπηρεσία Controller Pilot Data Link Communication στη θύρα 5911).

- `nmap <IP-address or Domain-name>`

Μπορείτε να δείτε τις ανοικτές θύρες και άλλων μηχανών που βρίσκονται είτε σε απομακρυσμένο δίκτυο ή στο τοπικό δίκτυο.
Αν δοκιμάσετε να δείτε τις πληροφορίες μιας μηχανής στο εργαστήριο που βρίσκεστε π.χ. 103ws11 χρησιμοποιώντας την εντολή `nmap 103ws11` και λάβετε τα πιο κάτω

```
Starting Nmap 7.92 ( https://nmap.org ) at 2024-09-12 11:44 EEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.03 seconds
```

τότε μπορεί είτε η μηχανή να είναι εκτός λειτουργίας (down) ή η μηχανή σας να νομίζει ότι η άλλη μηχανή είναι εκτός λειτουργίας. Αυτό συμβαίνει διότι η nmap αρχικά ξεκινά να κάνει ping την άλλη μηχανή (στέλνοντας μηνύματα κυρίως ICMP ή TCP ή ARP) για να διαπιστώσει αν είναι «ζωντανή» (alive) η άλλη μηχανή. Αν δεν υπάρχει απόκριση από την άλλη μηχανή (μπορεί να φταίει το γεγονός ότι κάποιος μηχανισμός του δικτύου όπως ένα firewall απορρίπτει αυτά τα πακέτα και δεν φτάνουν ποτέ στην άλλη μηχανή) τότε η μηχανή σας υποθέτει ότι δεν είναι «ζωντανή» και σταματάει η διαδικασία σάρωσης των θυρών της άλλης μηχανής. Στην περίπτωση αυτή μπορούμε να δοκιμάσουμε την παράμετρο `-Pn` λέει στην nmap να υποθέσει ότι η άλλη μηχανή είναι ζωντανή (δηλ. να μην μπει στη διαδικασία ping) και να προχωρήσει απευθείας στη σάρωση των θυρών της. Με την εντολή `nmap -Pn 103ws11` μπορούμε να λάβουμε απάντηση αν όντως είναι ζωντανή η άλλη μηχανή:

```
Nmap scan report for 103ws11 (10.16.13.152)
Host is up (0.021s latency).
```

```
rDNS record for 10.16.13.152: 103ws11.in.cs.ucy.ac.cy
Not shown: 979 filtered tcp ports (no-response), 18 filtered tcp ports
(host-unreach)
PORT     STATE  SERVICE
22/tcp   open   ssh
3389/tcp open   ms-wbt-server
9090/tcp closed zeus-admin

Nmap done: 1 IP address (1 host up) scanned in 12.63 seconds
```

Όπως φαίνεται από την πιο πάνω απόκριση, η άλλη μηχανή (103ws11) έχει 2 θύρες ανοικτές και 1 κλειστή προς το έξω κόσμο.

- `nestat`

Η εντολή αυτή ανάλογα με τις παραμέτρους που δέχεται σαν όρισμα μπορεί να εκτυπώσει τις δικτυακές συνδέσεις της τοπικής μηχανής, τους πίνακες δρομολόγησης, στατιστικά για τις διεπαφές (interfaces) της τοπικής μηχανής κ.α. Αν δεν δοθεί κανένα όρισμα εκτυπώνει τις ενεργές συνδέσεις.

- `netstat -lntp`

Η εντολή αυτή παρουσιάζει τα sockets που είναι σε κατάσταση αναμονής (listening sockets) για σύνδεση (-l), παρουσιάζοντας τις υπηρεσίες με τον αριθμό της θύρας στην οποία ακούνε (-n) (sshd=22, ms-wbt-server=3389), τις ταυτότητες (PID) των διεργασιών (-p) και έχουν σχέση με το πρωτόκολλο tcp (-t).

```
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program
name
tcp        0      0 0.0.0.0:55011           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5910          0.0.0.0:*               LISTEN      662741/Xvnc
tcp        0      0 127.0.0.1:5911          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::59501                :::*                    LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
tcp6       0      0 ::1:3350                :::*                    LISTEN      -
tcp6       0      0 ::1:5911                :::*                    LISTEN      -
tcp6       0      0 ::1:5910                :::*                    LISTEN      662741/Xvnc
tcp6       0      0 :::111                  :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::3389                 :::*                    LISTEN      -
```

Στη στήλη Local Address, η διεύθυνση 127.0.0.1 (localhost ή loopback address) είναι η διεύθυνση της τοπικής μηχανής και χρησιμοποιείται συνήθως για τη διάγνωση και αντιμετώπιση προβλημάτων αλλά και για τοπική σύνδεση σε εξυπηρετητές (servers) που τρέχουν πάνω στην ίδια τη μηχανή. Για παράδειγμα, όταν εγκαταστήσουμε ένα server στην τοπική μηχανή για να επικοινωνήσουμε μαζί του χρειαζόμαστε το IP του και αυτό είναι το 127.0.0.1. Στην πιο πάνω εικόνα, ο IPP server για εκτυπώσεις ακούει (LISTEN) στο 127.0.0.1:631 που συνεπάγεται ότι δέχεται συνδέσεις (αιτήσεις) στη θύρα 631 μόνο αν προέρχονται από την ίδια μηχανή (127.0.0.1). Δεν μπορεί να απαντήσεις σε αιτήσεις που προέρχονται από άλλες μηχανές (δηλ. με IP εκτός από το 127.0.0.1).
Εκτός από την διεύθυνση 127.0.0.1, μια μηχανή μπορεί να έχει και άλλες IP διευθύνσεις που δίνονται από τα δίκτυα στα οποία συνδέεται η μηχανή. Αν η μηχανή έχει 2 διεπαφές

(interfaces ή κάρτες δικτύου) και μέσω αυτών συνδέεται σε 2 διαφορετικά δίκτυα τότε κατά συνέπεια θα έχει επιπλέον 2 διευθύνσεις IP π.χ. 192.168.1.10 και 10.0.2.7 (που εκχωρούνται συνήθως από τους routers κάθε δικτύου).
Η διεύθυνση 0.0.0.0 που φαίνεται στην πιο πάνω εικόνα αντιστοιχεί σε όλες οι διευθύνσεις IPv4. Με απλά λόγια, ο SSH server που ακούει στο 0.0.0.0:22 δέχεται συνδέσεις (αιτήσεις) στη θύρα 22 από οποιαδήποτε IPv4 διεύθυνση.
Η διεύθυνση ::: που φαίνεται στην πιο πάνω εικόνα αντιστοιχεί σε όλες οι διευθύνσεις IPv6. Με απλά λόγια, οι SSH & MS WBT servers που ακούνε στο :::22 και :::3389 αντίστοιχα δέχονται συνδέσεις (αιτήσεις) στη θύρα 22 και 3389 αντίστοιχα από οποιαδήποτε IPv6 διεύθυνση.

- `netstat -i`

Για να δείτε ποιες διεπαφές έχει η μηχανή σας εκτελέστε την πιο πάνω εντολή:

```
Kernel Interface table
Iface             MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eno1             1500 29506884      0      0 0      30036817      0      0      0 BMRU
lo              65536    73958      0      0 0         73958      0      0      0 LRU
```

Η διαπαφή (lo), loopback interface, που αναφέραμε ήδη πιο πάνω, είναι μια εικονική διεπαφή δικτύου την οποία μια μηχανή χρησιμοποιεί για να επικοινωνήσει με τον εαυτό της. Η διεπαφή eno1 είναι η διεπαφή δικτύου (onboard Network Interface Card, με απλά λόγια η κάρτα ethernet) για τη διασύνδεση της μηχανής με τον έξω κόσμο. Σε άλλες μηχανές, μπορεί να δείτε διεπαφές με όνομα eth1 (που αντιστοιχεί και πάλι σε κάρτα Ethernet) και wlan0 (κάρτα ασύρματου δικτύου π.χ. wifi). Αν υπάρχουν 2 κάρτες Ethernet, η πρώτη μπορεί να έχει το όνομα eth1 και η άλλη το eth2 κ.ο.κ.

- `netstat -s`

Η πιο πάνω εντολή ανακτά και παρουσιάζει δικτυακά στατιστικά ανά πρωτόκολλο επικοινωνίας όπως φαίνεται πιο κάτω (παρουσιάζεται ένα υποσύνολο των αποτελεσμάτων της εντολής διότι ολόκληρη η απόκριση της εντολής είναι μακροσκελής):

```
Ip:
    Forwarding: 2
    13087002 total packets received
    139 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    13081717 incoming packets delivered
    9692439 requests sent out
    90 dropped because of missing route
    OutTransmits: 9692439
Icmp:
    25865 ICMP messages received
    0 input ICMP message failed
    ICMP input histogram:
        destination unreachable: 11
        echo requests: 25854
    25860 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
```

```
        destination unreachable: 6
        echo replies: 25854
IcmpMsg:
        InType3: 11
        InType8: 25854
        OutType0: 25854
        OutType3: 6
Tcp:
    7439 active connection openings
    102 passive connection openings
    3174 failed connection attempts
    199 connection resets received
    8 connections established
    13038124 segments received
    30047053 segments sent out
    59635 segments retransmitted
    1 bad segments received
    8408 resets sent
```

Ερωτήσεις

Με βάση τις πιο πάνω πληροφορίες απαντήστε τις ερωτήσεις:

1) Εκτυπώστε όλες τις πληροφορίες για τις ενεργές συνδέσεις της μηχανής σας που χρησιμοποιούν το πρωτόκολλο TCP

2) Εκτυπώστε μόνο τα ονόματα (domain name) των μηχανών που είναι ενεργά συνδεδεμένες με τη μηχανή σας.

3) Εκτυπώστε μόνο τα ονόματα (domain name) των μηχανών που είναι ενεργά συνδεδεμένες με τη μηχανή σας έτσι ώστε το κάθε όνομα να εμφανίζεται μόνο μια φορά αλλά να φαίνεται και ο αριθμός των συνδέσεων της κάθε μηχανής.

4) Εκτυπώστε το όνομα της διεπαφής (interface) που έχει λάβει τα πιο πολλά πακέτα καθώς και τον αριθμό των εισερχόμενων πακέτων.

5) Έστω ότι σας ενδιαφέρουν οι ανοικτές θύρες των υπηρεσιών της μηχανής σας. Να γράψετε σε αρχείο με το όνομα open_ports ΜΟΝΟ τους αριθμούς των θυρών, τη μία δίπλα στην άλλη χωρισμένες με κενό (space) π.χ. `22 11 631 3389 5910 5911`

6) Εκτυπώστε τις ανοικτές θύρες των υπηρεσιών της μηχανής σας. Θα πρέπει να τυπώσετε ΜΟΝΟ τα ονόματα των υπηρεσιών το ένα κάτω από το άλλο π.χ.

```
ssh
rpcbind
ipp
ms-wbt-server
cm
cpdlc
```

7) Τα αρχεία καταγραφής συμβάντων (log files) περιέχουν εξαιρετικά χρήσιμες πληροφορίες για τη εύρυθμη λειτουργία ενός server (εξυπηρετητή). Για παράδειγμα, στα λειτουργικά συστήματα τύπου Red Hat όπως είναι το CentOS τα log files του Web (HTTP) server βρίσκονται στον κατάλογο /var/log/apache2. Μέσα στο φάκελο αυτό μπορείτε να διαφόρων ειδών log files όπως για παράδειγμα error logs και access logs.
Μέσα στα error logs ένας server βάζει διάφορες διαγνωστικές πληροφορίες για τη λειτουργία του και καταγράφει σφάλματα που παρουσιάζονται κατά την διάρκεια των αιτήσεων που δέχεται. Είναι η πρώτη πηγή πληροφοριών που θα κοιτάξει ο διαχειριστής όταν συμβεί ένα πρόβλημα κατά την εκκίνηση του server ή με τη λειτουργία του server γενικότερα διότι συχνά περιέχει λεπτομέρειες σχετικά με το τι πήγε λάθος και πώς μπορεί να διορθωθεί. Μια τυπική γραμμή ενός τέτοιου αρχείου είναι:

```
wpbfl2-45.gate.net [29:23:56:12] "GET /Access/ HTTP/1.0" 200 2376
```

Μέσα στα access logs ο Apache server καταγράφει όλες τις αιτήσεις που δέχεται. Περιέχει τον αποστολέα και το περιεχόμενο της κάθε αιτήσεως. Από τα περιεχόμενα των αρχείων αυτών μπορεί μετά από περαιτέρω ανάλυση να παραχθούν χρήσιμα στατιστικά.
Επειδή στις μηχανές των εργαστηρίων δεν τρέχει κάποιος HTTP server, δεν υπάρχουν διαθέσιμα log files, οπότε θα κατεβάσουμε δεδομένα από μια ιστοσελίδα που περιέχει traces από access logs. Πιο συγκεκριμένα θα κατεβάσουμε ένα access log file από ένα HTTP server που βρίσκεται στο Research Triangle Park, NC στην Αμερική και περιέχει πληροφορίες αιτήσεων προς τον server για ένα 24 ωρο. Διαβάστε περισσότερα στοιχεία για το συγκεκριμένο access log file εδώ. Κατεβάστε το (με την εντολή wget) στη μηχανή σας και αποσυμπιέστε (με την εντολή zcat):

```
wget ftp://ita.ee.lbl.gov/traces/epa-http.txt.Z

zcat epa-http.txt.Z > epa-http.txt
```

α) Τυπώστε τα ονόματα (domain names) των 10 μηχανών που έκαναν τις πιο πολλές αιτήσεις GET στον HTTP server (μπορείτε να τυπώσετε και τον αριθμό των αιτήσεων).

β) Τυπώστε τα ονόματα (domain names) των 10 μηχανών που έκαναν τις πιο πολλές αιτήσεις POST στον HTTP server (μπορείτε να τυπώσετε και τον αριθμό των αιτήσεων).