NMAP

Tutorial and Examples

Γιώργος Καππές

NMAP TUTORIAL

Το nmap είναι ένα δικτυακό εργαλείο ανάλυσης δικτύων. Σχεδιάστηκε έτσι ώστε να ελέγχει μεγάλα δίκτυα, ωστόσο λειτουργεί τέλεια και για έναν host. Χρησιμοποιεί RAW IP πακέτα έτσι ώστε να ανακαλύψει τους host που είναι σε λειτουργία στο δίκτυο, τις υπηρεσίες και τον τύπο του λειτουργικού συστήματος που τρέχουν, τι είδους firewall χρησιμοποιούνται στο δίκτυο και πολλά άλλα.

1. **Καθορισμός στόχων**

Μερικές φορές μπορεί να θέλουμε να αναλύσουμε ένα ολόκληρο δίκτυο και άλλες φορές κάποιον συγκεκριμένο host. Το nmap υποστηρίζει την CIDR διευθυνσιοδότηση δίνοντάς μας έτσι τη δυνατότητα να χρησιμοποιήσουμε το πρόθεμα /numbits έτσι ώστε να ελέγξουμε ένα ολόκληρο δίκτυο. Για παράδειγμα η διεύθυνση 192.168.10.0/24 περιέχει 256 hosts, από 192.168.10.0 (δυαδικός: **11000000 10101000 00001010** 00000000) μέχρι και 192.168.10.255 (δυαδικός: **11000000 10101000 00001010** 11111111). Να επισημάνουμε ότι το /24 μας λέει ότι τα πρώτα 24 bits της διεύθυνσης IP θα συμβολίζουν τη διεύθυνση του δικτύου.
Έτσι αν θέλουμε να ελέγξουμε το παραπάνω δίκτυο θα δώσουμε κάτι σαν:

```
nmap 192.168.10.0/24
```

Μπορούμε επίσης να παραλείψουμε ορισμένες διευθύνσεις ώστε να κάνουμε τον έλεγχο πιο αποδοτικό. Για παράδειγμα αν στο παραπάνω δίκτυο θα θέλαμε να παραλείψουμε τις διευθύνσεις που τελειώνουν σε 0 ή 255 θα τρέχαμε:

```
nmap 192.168.10.1-254
```

Αν πάλι θέλουμε να ελέγξουμε όλες τις διευθύνσεις του Internet που τελειώνουν σε 18.87 τότε θα τρέχαμε:

```
nmap 0-255.0-255.12.37
```

Στο σημείο αυτό να επισημάνουμε ότι για να ελέγξουμε μια IPv6 διεύθυνση θα πρέπει να εισάγουμε ολόκληρη τη διεύθυνση ή το αντίστοιχο hostname. Μια άλλη επιλογή που μας δίνει το nmap είναι να διαβάζουμε τις διευθύνσεις στόχους από αρχείο. Για να το πετύχουμε αυτό εκτελούμε:

```
nmap –iL
```

όπου filename το αρχείο που περιέχει τις διευθύνσεις μας. Τέλος μπορούμε να ελέγξουμε τυχαίους host τους οποίους το nmap θα επιλέξει για εμάς. Το μόνο που χρειάζεται είναι να δώσουμε στο nmap τον αριθμό των τυχαίων host που θέλουμε να δημιουργήσει:

```
nmap -iR
```

2. Εύρεση host

Αφού έχουμε προσδιορίσει στο nmap το δίκτυο ή τον host που θέλουμε να ελέγξει, θα πρέπει αρχικά το nmap να ελέγξει ποιοι host του δικτύου ή αν ο συγκεκριμένος host που δώσαμε είναι σε λειτουργία. Με αυτό τον τρόπο μειώνουμε τον αριθμό των host που θα ελέγξει το nmap σε αυτούς που είναι σε λειτουργία κάνοντας έτσι τον έλεγχο πιο αποδοτικό. Ας δούμε τώρα με ποιους τρόπους μπορούμε να ανακαλύψουμε έναν "ζωντανό" host.

Ping Scan

- **Επιλογή: -sP**

Αυτή η επιλογή λέει στο nmap να εκτελέσει μόνο ping scan, και στη συνέχεια να τυπώσει τον αριθμό των hosts που ανταποκρίθηκαν. Κανένας επιπλέον έλεγχος δε πραγματοποιείται (όπως port scanning, ή εύρεση του λειτουργικού συστήματος). Αυτός ο έλεγχος μας είναι χρήσιμος όταν θέλουμε να μάθουμε τον αριθμό των host που είναι σε λειτουργία μέσα σε ένα δίκτυο χωρίς να τραβήξουμε την προσοχή. Η μέθοδος αυτή συνήθως ονομάζεται και ping sweep και είναι πιο αξιόπιστη από το να εκτελέσουμε ping σε μια broadcast διεύθυνση, διότι πολλοί host αγνοούν τα broadcast πακέτα.
Η επιλογή -sP στέλνει μία αίτηση echo request στη θύρα 80 εξ ορισμού. Όταν το πρόγραμμα εκτελείται από απλούς χρήστες χωρίς επιπλέον δικαιώματα, τότε στέλνεται ένα SYN πακέτο. Διαφορετικά, όταν το nmap εκτελείται από το χρήστη root, τότε στέλνεται στον στόχο ένα πακέτο ARP request. Να σημειώσουμε ότι δε μπορούμε να συνδυάσουμε αυτή την μέθοδο με της μεθόδους που θα δούμε στη συνέχεια. Ωστόσο, μπορούμε αρχικά να εκτελέσουμε αυτή τη μέθοδο για να μάθουμε τους ενεργούς host και στη συνέχεια να εκτελέσουμε σε αυτούς ενέργειες όπως port scanning ή service detection.

Παράδειγμα:

```
cronos:/home/giorgos# nmap -sP 192.168.1.1

Starting Nmap 4.62 ( http://nmap.org ) at 2009-08-18
13:37 EEST
Host 192.168.1.1 appears to be up.
MAC Address: 00:21:29:78:15:8B (Unknown)
```

```
Nmap done: 1 IP address (1 host up) scanned in 13.202
seconds
```

TCP Syn Ping

- **Επιλογή: -PS**

Αυτή η επιλογή στέλνει ένα άδειο IP πακέτο με ενεργοποιημένο το SYN flag. Η εξ ορισμού θύρα αποστολής είναι η 80 ωστόσο ο χρήστης μπορεί να δώσει σαν παράμετρο μια λίστα από δικές του επιθυμητές θύρες. Για παράδειγμα: -PS22 για την πόρτα 22 και -PS22-25,80,113,1050,35000 για τις πόρτες 22 έως και 25, την 80, την 113, την 1050, και την 35000.
Αν η απομακρυσμένη πόρτα είναι κλειστή τότε έρχεται πίσω σε μας ένα πακέτο RST (connection reset), διαφορετικά, αν η πόρτα είναι ανοικτή ο υπολογιστής στόχος θα εκτελέσει το 2ο βήμα της 3-way handshake του TCP στέλνοντας πίσω σε μας ένα SYN/ ACK πακέτο. Ωστόσο, αυτό που μας ενδιαφέρει στην παρούσα φάση δεν είναι αν η απομακρυσμένη πόρτα βρέθηκε κλειστή η ανοικτή, αλλά η ύπαρξη του συγκεκριμένου host. Έτσι, ακόμα κι αν η πόρτα ήταν κλειστή, αν λάβουμε το πακέτο RST, τότε κατευθείαν ο host στόχος θα έχει υποδηλώσει την ύπαρξή του.

Παράδειγμα:

```
cronos:/home/giorgos# nmap -PS21,100-110 192.168.1.1

Starting Nmap 4.62 ( http://nmap.org ) at 2009-08-18
13:38 EEST
Interesting ports on 192.168.1.1:
Not shown: 1713 closed ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https
MAC Address: 00:21:29:78:15:8B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 14.763
seconds
```

TCP ACK Ping

- **Επιλογή: -PA**

Η τεχνική αυτή είναι σχεδόν ίδια με την τεχνική που περιγράψαμε παραπάνω. Η μόνη διαφορά είναι ότι στέλνεται ένα άδειο πακέτο TCP στο οποίο έχει τεθεί η επιλογή ACK.

Στέλνοντας ένα ACK πακέτο στο στόχο προσποιούμαστε ότι επιβεβαιώνουμε δεδομένα μιας σύνδεσης TCP, ωστόσο τέτοια σύνδεση δεν υπάρχει και γι' αυτό ο στόχος θα μας απαντήσει με ένα πακέτο RST και θα υποδηλώσει έτσι την ύπαρξή του. Η default θύρα που χρησιμοποιείται είναι η 80 αλλά μπορούμε να καθορίσουμε εμείς σε ποια θύρα θέλουμε να σταλεί το πακέτο όπως και παραπάνω.
Ο λόγος για τον οποίο το nmap προσφέρει και SYN και ACK pings είναι για να διαπεράσει τα firewall. Υπάρχει η περίπτωση κάποιος διαχειριστής να προγραμματίσει το firewall έτσι ώστε να πετάει τα πακέτα SYN που απευθύνονται σε κλειστές πόρτες και να μη στέλνει πίσω πακέτα RST. Σε μία τέτοια περίπτωση η τεχνική SYN Ping δε θα μας έδινε το σωστό αποτέλεσμα γιατί θα υπέθετε πως ο host είναι απενεργοποιημένος. Ωστόσο, και η τεχνική ACK ping έχει τα προβλήματά της. Ένα θέμα που προκύπτει με την αποστολή ψεύτικων ACK πακέτων χωρίς να υπάρχει η σύνδεση, είναι ότι ισχυρά firewall, όπως το iptables αν ρυθμιστούν κατάλληλα μπορούν να πετάνε απρόσμενα πακέτα όπως τα ACK που στέλνει το nmap χωρίς να υπάρχει η σύνδεση. Μια αποτελεσματική τεχνική που συνήθως χρησιμοποιούμε είναι να συνδυάζουμε τις επιλογές -PS και -PA.

Παράδειγμα:

```
cronos:/home/giorgos# nmap -PA 192.168.1.1

Starting Nmap 4.62 ( http://nmap.org ) at 2009-08-18
14:38 EEST
Interesting ports on 192.168.1.1:
Not shown: 1713 closed ports
PORT STATE SERVICE
80/tcp open http

443/tcp open https
MAC Address: 00:21:29:78:15:8B (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 14.771
seconds

cronos:/home/giorgos# nmap -PA -PS 192.168.1.1

Starting Nmap 4.62 ( http://nmap.org ) at 2009-08-18
14:38 EEST
Interesting ports on 192.168.1.1:
Not shown: 1713 closed ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https
MAC Address: 00:21:29:78:15:8B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 14.772
seconds
```

UDP Ping

- **Επιλογή: -PU**

Με τη μέθοδο αυτή το nmap στέλνει στο στόχο άδεια πακέτα UDP. Σαν default χρησιμοποιείται η πόρτα 31338, αλλά μπορούμε να καθορίσουμε άλλες επιθυμητές πόρτες όπως και παραπάνω.
Αν το πακέτο UDP συναντήσει μια κλειστή πόρτα, τότε θα μας σταλεί ένα μήνυμα ICMP (port unreachable). Αυτό κατευθείαν θα σημαίνει ότι ο host είναι ενεργοποιημένος. Ωστόσο σε αντίθεση με τις προηγούμενες μεθόδους αν το πακέτο συναντήσει μια ανοικτή πόρτα, οι περισσότερες υπηρεσίες απλά θα αγνοήσουν το πακέτο και δε θα στείλουν πίσω κάποιο μήνυμα ICMP κι έτσι δε μπορούμε να γνωρίζουμε αν ο host είναι ενεργός ή όχι. Αυτός είναι και ο λόγος που η default θύρα της συγκεκριμένης μεθόδου είναι η 31338 διότι είναι απίθανο κάποιο μηχάνημα να έχει αυτή τη θύρα ανοικτή. Έτσι σαν συμβουλή χρησιμοποιείστε μαζί με την επιλογή -PU θύρες που είναι πολύ απίθανο να βρεθούν ανοικτές, όπως για παράδειγμα η 55515.

Παράδειγμα:

```
cronos:/home/giorgos# nmap -PU scylla.cs.uoi.gr

Starting Nmap 4.62 ( http://nmap.org ) at 2009-08-18
15:40 EEST
Interesting ports on scylla.cs.uoi.gr (195.130.121.45):
Not shown: 1694 closed ports
PORT STATE SERVICE
22/tcp open ssh
25/tcp filtered smtp
79/tcp filtered finger
80/tcp open http
110/tcp open pop3
111/tcp filtered rpcbind
139/tcp filtered netbios-ssn
143/tcp open imap
443/tcp open https
445/tcp filtered microsoft-ds
512/tcp filtered exec
513/tcp filtered login
514/tcp filtered shell
762/tcp filtered quotad
800/tcp filtered mdbs_daemon
2003/tcp filtered finger
3306/tcp open mysql
4045/tcp filtered lockd
6000/tcp open X11
```

```
27000/tcp open flexlm0
32772/tcp open sometimes-rpc7

Nmap done: 1 IP address (1 host up) scanned in 53.492
seconds
```

No Ping

- **Επιλογή: -PN**

Αυτή η επιλογή παρακάμπτει την αναζήτηση για ενεργούς host και εκτελεί ελέγχους όπως port scanning σε κάθε host.

3. Port Scanning

Το nmap χωρίζει τις θύρες σε 6 κατηγορίες:

- **open.** Μια εφαρμογή τρέχει πίσω από τη θύρα και δέχεται συνδέσεις.
- **closed.** Η θύρα είναι ανοικτή, αλλά δεν υπάρχει κάποια εφαρμογή που να τη χρησιμοποιεί.
- **Filtered.** Το nmap δε μπορεί να αποφασίσει αν η θύρα είναι ανοικτή γιατί κάποια φίλτρα πακέτων εμποδίζουν τα πακέτα του να φτάσουν στον προορισμό.
- **Unfiltered.** Η θύρα είναι προσβάσιμη αλλά το nmap δε μπορεί να αποφασίσει αν είναι ανοικτή ή όχι.
- **open|filtered.** Το nmap δεν είναι δυνατό να αποφασίσει αν η συγκεκριμένη πόρτα είναι ανοικτή ή φιλτραρισμένη.
- **closed|filtered.** Το nmap δεν είναι δυνατό να αποφασίσει αν η συγκεκριμένη πόρτα είναι κλειστή ή φιλτραρισμένη.

TCP SYN Scan

- **Επιλογή: -sS**

Πρόκειται για τη default μέθοδο που χρησιμοποιεί το nmap. Μπορεί να εκτελεστεί πάρα πολύ γρήγορα και δεν εντοπίζεται εύκολα από firewalls, αφού δεν ολοκληρώνει το TCP three-way handshake και δεν καταγράφεται από τον host-στόχο.
Η μέθοδος αυτή συχνά αναφέρεται και ως half-open scanning , αφού δεν δημιουργείται TCP σύνδεση. Το nmap στέλνει ένα πακέτο SYN και περιμένει απάντηση. Αν φτάσει πίσω ένα πακέτο SYN/ ACK τότε η πόρτα είναι σε κατάσταση listening, διαφορετικά αν φτάσει ένα πακέτο RST η πόρτα είναι σε κατάσταση non-listening. Αν δεν έρθει καμιά απάντηση

μετά από ορισμένες προσπάθειες ή έρθει κάποιο μήνυμα σφάλματος ICMP η πόρτα χαρακτηρίζεται ως filtered.

Παράδειγμα:

```
cronos:/home/giorgos# nmap -sS scylla.cs.uoi.gr

Starting Nmap 4.62 ( http://nmap.org ) at 2009-08-18
16:04 EEST
Interesting ports on scylla.cs.uoi.gr (195.130.121.45):
Not shown: 1694 closed ports
PORT STATE SERVICE
22/tcp open ssh
25/tcp filtered smtp
79/tcp filtered finger
80/tcp open http
110/tcp open pop3
111/tcp filtered rpcbind
139/tcp filtered netbios-ssn
143/tcp open imap
443/tcp open https
445/tcp filtered microsoft-ds
512/tcp filtered exec
513/tcp filtered login
514/tcp filtered shell
762/tcp filtered quotad
800/tcp filtered mdbs_daemon
2003/tcp filtered finger
3306/tcp open mysql
4045/tcp filtered lockd
6000/tcp open X11
27000/tcp open flexlm0
32772/tcp open sometimes-rpc7

Nmap done: 1 IP address (1 host up) scanned in 49.964
seconds
```

TCP Connect Scan

- **Επιλογή: -sT**

Η μέθοδος αυτή χρησιμοποιείται όταν δεν είναι διαθέσιμη η SYN Scan ή αν εκτελούμε το nmap από κάποιον χρήστη με περιορισμένα δικαιώματα. Είναι πιο αργή, αφού μεταφέρονται περισσότερα πακέτα και συνήθως καταγράφεται από το απομακρυσμένο

σύστημα, αφού ολοκληρώνεται το TCP three-way handshake και πραγματοποιείται η σύνδεση.

Παράδειγμα:

```
cronos:/home/giorgos# nmap -sT scylla.cs.uoi.gr

Starting Nmap 4.62 ( http://nmap.org ) at 2009-08-18
16:09 EEST
Interesting ports on scylla.cs.uoi.gr (195.130.121.45):
Not shown: 1693 closed ports
PORT STATE SERVICE
22/tcp open ssh
25/tcp filtered smtp
79/tcp filtered finger
80/tcp open http
110/tcp open pop3
111/tcp filtered rpcbind
139/tcp filtered netbios-ssn
143/tcp open imap
443/tcp open https
445/tcp filtered microsoft-ds
512/tcp filtered exec
513/tcp filtered login
514/tcp filtered shell
731/tcp filtered netviewdm3
762/tcp filtered quotad
800/tcp filtered mdbs_daemon
2003/tcp filtered finger
3306/tcp open mysql
4045/tcp filtered lockd
6000/tcp open X11
27000/tcp open flexlm0
32772/tcp open sometimes-rpc7

Nmap done: 1 IP address (1 host up) scanned in 55.395
seconds
```

UDP SCAN

- **Επιλογή: -sU**

Οι περισσότερες υπηρεσίες στο internet τρέχουν κάτω από TCP, ωστόσο έχουν αρχίσει να εμφανίζονται πλέον και πολλές που χρησιμοποιούν το UDP. Μερικά τέτοια παραδείγματα

είναι οι υπηρεσίες DNS, SNMP, και DHCP. Επειδή το UDP scanning είναι πιο αργό και πιο δύσκολο από το TCP scanning, πολλοί διαχειριστές αγνοούν τις UDP πόρτες. Οι hackers όμως δε τις αγνοούν!
Το UDP scanning μπορεί να συνδυαστεί και με το TCP scanning δίνοντας τις κατάλληλες επιλογές στο nmap, για παράδειγμα:

```
nmap -sS -sU 192.169.1.1
```

XMAS Scan

- **Επιλογή: -sX**

Αυτή η μέθοδος περιλαμβάνει την αποστολή TCP πακέτων με τις σημαίες FIN, URG, PUSH ενεργοποιημένες. Αν ληφθεί ένα πακέτο RST, η θύρα θεωρείται κλειστή, διαφορετικά θεωρείται open|filtered. Το πλεονέκτημα αυτής της μεθόδου είναι ότι μπορεί να παρακάμψει non-statefull firewalls και packet filtering routers. Άλλο ένα πλεονέκτημα είναι ότι αυτή η μέθοδος εντοπίζεται πιο δύσκολα και από τη μέθοδο SYN Scanning που είδαμε παραπάνω.

Παράδειγμα:

```
cronos:/home/giorgos# nmap -sX 192.168.1.1

Starting Nmap 4.62 ( http://nmap.org ) at 2009-08-18
16:29 EEST
All 1715 scanned ports on 192.168.1.1 are open|filtered
MAC Address: 00:21:29:78:15:8B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 36.993
seconds
```

FIN Scanning

- **επιλογή: -sF**

Σε αυτή τη μέθοδο στέλνεται ένα πακέτο FYN στο στόχο. Αν ο στόχος είναι ενεργός, αλλά δεν ακούει στη συγκεκριμένη πόρτα, θα ανταποκριθεί με ένα πακέτο RST, διαφορετικά, αν ακούει στη συγκεκριμένη θύρα δε θα ανταποκριθεί. Σημειώστε ότι τα Microsoft Windows στέλνουν RST πακέτα σε όλες τις περιπτώσεις.

Παράδειγμα:

```
cronos:/home/giorgos# nmap -sF 192.168.1.1

Starting Nmap 4.62 ( http://nmap.org ) at 2009-08-18
16:32 EEST
All 1715 scanned ports on 192.168.1.1 are open|filtered
MAC Address: 00:21:29:78:15:8B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 36.966
seconds
```

NULL Scanning

- **Επιλογή: -sN**

Αυτή η μέθοδος στέλνει στο host στόχο ένα πακέτο με όλες τις σημαίες κεφαλίδας απενεργοποιημένες. Αν ο host ακούει στην συγκεκριμένη θύρα δε θα απαντήσει. Διαφορετικά θα στείλει πίσω ένα πακέτο RST.

Παράδειγμα:

```
cronos:/home/giorgos# nmap -sN 192.168.1.1

Starting Nmap 4.62 ( http://nmap.org ) at 2009-08-18
16:34 EEST
All 1715 scanned ports on 192.168.1.1 are open|filtered
MAC Address: 00:21:29:78:15:8B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 36.977
seconds
```

ACK Scanning

- **Επιλογή: -sA**

Η μέθοδος αυτή διαφέρει από τις υπόλοιπες αφού δεν ανακαλύπτει ανοικτές θύρες. Χρησιμοποιείται για να προσδιορίσει κατά πόσο το firewall του στόχου είναι stateful ή όχι και ποιες θύρες είναι σε κατάσταση filtered.

Παράδειγμα:

```
cronos:/home/giorgos# nmap -sA scylla.cs.uoi.gr

Starting Nmap 4.62 ( http://nmap.org ) at 2009-08-18
16:38 EEST
Interesting ports on scylla.cs.uoi.gr (195.130.121.45):
Not shown: 1703 unfiltered ports
PORT STATE SERVICE
25/tcp filtered smtp
79/tcp filtered finger
111/tcp filtered rpcbind
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
512/tcp filtered exec
513/tcp filtered login
514/tcp filtered shell
762/tcp filtered quotad
800/tcp filtered mdbs_daemon
2003/tcp filtered finger
4045/tcp filtered lockd

Nmap done: 1 IP address (1 host up) scanned in 59.733
seconds
```

IDLE Scanning

- **Επιλογή: -sI**

Πρόκειται για μια προχωρημένη μέθοδο κατά την οποία χρησιμοποιείται ένας τρίτος host που λειτουργεί σαν zombie και ο host στόχος καταγράφει τη διεύθυνση του zombie και όχι τη δική μας. Έτσι πρόκειται για μία τυφλή επίθεση. Περισσότερες πληροφορίες και οδηγίες μπορείτε να βρείτε στο: http://nmap.org/book/idlescan.html

4. Καθορισμός θυρών

Εξ ορισμού το nmap ελέγχει τις πρώτες 1024 θύρες, αλλά και μεγαλύτερες θύρες που περιέχονται στο αρχείο nmap-services και εξυπηρετούν γνωστές υπηρεσίες. Αν θέλουμε να δώσουμε μια δική μας ακολουθία από πόρτες μπορούμε να χρησιμοποιήσουμε την επιλογή **-p** ακολουθούμενη από το εύρος θυρών που θέλουμε. Για παράδειγμα:

```
-p 1-1025, 5000, 5100-5400, 6800
```

5. Εύρεση υπηρεσιών που εκτελούνται στον host

Το nmap μπορεί αν μας εμφανίσει τις υπηρεσίες και τις εκδόσεις τους που τρέχουν στις πόρτες που βρέθηκαν ανοικτές. Για να ενεργοποιήσουμε τη συγκεκριμένη μέθοδο δίνουμε στο nmap την επιλογή -**sV**

Παράδειγμα:

```
cronos:/home/giorgos# nmap -sV scylla.cs.uoi.gr

Starting Nmap 4.62 ( http://nmap.org ) at 2009-08-18
16:58 EEST
Interesting ports on scylla.cs.uoi.gr (195.130.121.45):
Not shown: 1691 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh SunSSH 1.0.1 (protocol 2.0)
25/tcp filtered smtp
79/tcp filtered finger
80/tcp open http Apache httpd 2.2.6 ((Unix) mod_ssl/2.2.6
OpenSSL/0.9.8h DAV/2 PHP/5.2.5)
110/tcp open pop3
111/tcp filtered rpcbind
139/tcp filtered netbios-ssn
143/tcp open imap UW imapd 2001.295
287/tcp filtered unknown
443/tcp open ssl/http Apache httpd 2.2.6 ((Unix)
mod_ssl/2.2.6 OpenSSL/0.9.8h DAV/2 PHP/5.2.5)
445/tcp filtered microsoft-ds
512/tcp filtered exec
513/tcp filtered login
514/tcp filtered shell
603/tcp filtered mnotes
757/tcp filtered unknown
762/tcp filtered quotad
800/tcp filtered mdbs_daemon
2003/tcp filtered finger
3306/tcp open mysql MySQL 5.0.27
4045/tcp filtered lockd
6000/tcp open X11?
27000/tcp open flexlm FlexLM license manager
32772/tcp open rpcbind
```

```
1 service unrecognized despite returning data. If you
know the service/version, please submit the following
fingerprint at http://www.insecure.org/cgi-bin/servicefp-
submit.cgi :
SF-Port110-TCP:V=4.62%I=7%D=8/18%Time=4A8AB41B%P=i686-pc-
linux-gnu%r(NULL,
SF:6A,"\+OK\x20scylla\.cs\.uoi\.gr\x20Solstice\x20Interne
t\x20Mail\x20Serv
SF:er\x20\x20POP3\x201\.0\.2\x20at\x20Tue,\x2018\x20Aug\x
202009\x2017:00:5
SF:6\x20\+0300\x20\(EEST\)\r\n")%r(GenericLines,7D,"\+OK\
x20scylla\.cs\.uo
SF:i\.gr\x20Solstice\x20Internet\x20Mail\x20Server\x20\x2
0POP3\x201\.0\.2\
SF:x20at\x20Tue,\x2018\x20Aug\x202009\x2017:00:56\x20\+03
00\x20\(EEST\)\r\
SF:n-ERR\x20Null\x20command\r\n");

Service detection performed. Please report any incorrect
results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 245.487
seconds
```

6. Εύρεση λειτουργικού συστήματος

Επιπλέον, το nmap μπορεί να εντοπίσει και το λειτουργικό σύστημα που τρέχει ο host στόχος. Αν θέλουμε να πραγματοποιήσουμε αυτόν τον έλεγχο χρησιμοποιούμε την επιλογή **–O.**

Να σημειώσουμε ότι χρησιμοποιώντας την επιλογή **-A** το nmap εκτελεί αυτόματα εύρεση υπηρεσιών και λειτουργικού συστήματος ταυτόχρονα.

Παράδειγμα:

```
cronos:/home/giorgos# nmap -O scylla.cs.uoi.gr

Starting Nmap 4.62 ( http://nmap.org ) at 2009-08-18
17:04 EEST
Interesting ports on scylla.cs.uoi.gr (195.130.121.45):
Not shown: 1694 closed ports
PORT STATE SERVICE
22/tcp open ssh
25/tcp filtered smtp
79/tcp filtered finger
```

```
80/tcp open http
110/tcp open pop3
111/tcp filtered rpcbind
139/tcp filtered netbios-ssn
143/tcp open imap
443/tcp open https
445/tcp filtered microsoft-ds
512/tcp filtered exec
513/tcp filtered login
514/tcp filtered shell
762/tcp filtered quotad
800/tcp filtered mdbs_daemon
2003/tcp filtered finger
3306/tcp open mysql
4045/tcp filtered lockd
6000/tcp open X11
27000/tcp open flexlm0
32772/tcp open sometimes-rpc7
Device type: general purpose
Running (JUST GUESSING) : Sun Solaris 10|9|8 (92%)
Aggressive OS guesses: Sun Solaris 10 (x86) (92%), Sun
Solaris 9 or 10 (92%), Sun Solaris 9 or 10 (SPARC) (91%),
Sun Solaris 9 (x86) (89%), Sun Solaris 10 (SPARC) (89%),
Sun Solaris 8 (SPARC) (87%)
No exact OS matches for host (test conditions non-ideal).
Uptime: 110.265 days (since Thu Apr 30 10:43:52 2009)
Network Distance: 11 hops

OS detection performed. Please report any incorrect
results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 62.824
seconds
```

7. Χρόνος και απόδοση

Το nmap μας προσφέρει 6 timing teplates τα οποία μπορούμε να τα χρησιμοποιήσουμε και να βελτιώσουμε την απόδοση. Μπορούμε να καθορίσουμε ένα timing template με την επιλογή **-T** ακολουθούμενη από τον αριθμό ή το όνομα του template. Τα διαθέσιμα templates είναι:

- **paranoid (0):** Χρησιμοποιείται για IDS envasion
- **sneeky (1):** Παρόμοιο με το paranoid.

- **polite (2):** Καθυστερεί τον έλεγχο έτσι ώστε να καταναλώσει λιγότερο bandwidth του δικτύου.
- **normal(3):** Το default template
- **aggressive(4):** Κάνει τον έλεγχο ταχύτερο υποθέτοντας ότι βρίσκεστε σε ένα γρήγορο και αξιόπιστο δίκτυο.
- **insane (5):** Υποθέτει ότι βρίσκεστε σε ένα πάρα πολύ γρήγορο και αξιόπιστο δίκτυο και θυσιάζει ένα ποσοστό της ακρίβειας των αποτελεσμάτων για την ταχύτητα του ελέγχου.

Όταν ελέγχουμε κόμβους στο εσωτερικό μας δίκτυο είναι εύλογο να χρησιμοποιήσουμε την επιλογή aggressive επειδή τα τοπικά δίκτυα είναι γρήγορα και ασφαλή. Όταν ελέγχουμε απομακρυσμένα δίκτυα, τότε αν μας ενδιαφέρει η αξιοπιστία των αποτελεσμάτων πρέπει να χρησιμοποιήσουμε είτε το normal είτε το polite template.

Χρήση:

---

nmap -T1 ...
nmap -T insane ...
nmap -T 2

Παράδειγμα:

```
cronos:/home/giorgos# nmap -sS -T4 scylla.cs.uoi.gr

Starting Nmap 4.62 ( http://nmap.org ) at 2009-08-18
17:32 EEST
Warning: Giving up on port early because retransmission
cap hit.
Interesting ports on scylla.cs.uoi.gr (195.130.121.45):
Not shown: 1694 closed ports
PORT STATE SERVICE
22/tcp open ssh
25/tcp filtered smtp
79/tcp filtered finger
80/tcp open http
110/tcp open pop3
111/tcp filtered rpcbind
139/tcp filtered netbios-ssn
143/tcp open imap
443/tcp open https
445/tcp filtered microsoft-ds
512/tcp filtered exec
513/tcp filtered login
514/tcp filtered shell
762/tcp filtered quotad
800/tcp filtered mdbs_daemon
```

```
2003/tcp filtered finger
3306/tcp open mysql
4045/tcp filtered lockd
6000/tcp open X11
27000/tcp open flexlm0
32772/tcp open sometimes-rpc7

Nmap done: 1 IP address (1 host up) scanned in 51.739
seconds
```

Εκτελώντας το παραπάνω παράδειγμα με το template insane παρατηρούμε ότι οι πόρτες που ανακαλύπτει το nmap είναι πολύ λιγότερες:

```
cronos:/home/giorgos# nmap -sS -T 5 scylla.cs.uoi.gr

Starting Nmap 4.62 ( http://nmap.org ) at 2009-08-18
17:34 EEST
Warning: Giving up on port early because retransmission
cap hit.
Interesting ports on scylla.cs.uoi.gr (195.130.121.45):
Not shown: 1234 closed ports, 472 filtered ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
110/tcp open pop3
143/tcp open imap
443/tcp open https
3306/tcp open mysql
6000/tcp open X11
27000/tcp open flexlm0
32772/tcp open sometimes-rpc7

Nmap done: 1 IP address (1 host up) scanned in 31.938
seconds
```

8. Ολοκληρωμένο παράδειγμα

Έστω ότι θέλουμε να ελέγξουμε τις πόρτες από την 22 μέχρι και την 425 σε όλα τα τα hosts που βρίσκονται στο τοπικό μας δίκτυο και είναι ενεργοποιημένα. Επιπλέον θέλουμε να πάρουμε πληροφορίες για τις υπηρεσίες που τρέχουν και τα λειτουργικά συστήματα που χρησιμοποιούνται. Να σημειώσουμε ότι το τοπικό μας δίκτυο περιλαμβάνει τις διευθύνσεις: 192.168.1.0/24.

Στον παρακάτω έλεγχο θα χρησιμοποιήσουμε το template aggressive εφόσον ελέγχουμε μηχανήματα μέσα στο τοπικό μας δίκτυο που είναι ένα ethernet και ως γνωστόν το ethernet χαρακτηρίζεται από ταχύτητα και αξιοπιστία.

```
cronos:/home/giorgos# nmap -PS -sS -p22-425 -sV -O -T4 192.168.1.0/24

Starting Nmap 4.62 ( http://nmap.org ) at 2009-08-18 17:45 EEST
Interesting ports on 192.168.1.1:
Not shown: 403 closed ports
PORT STATE SERVICE VERSION
80/tcp open http?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port80-TCP:V=4.62%I=7%D=8/18%Time=4A8ABEA3%P=i686-pc-linux-gnu%r(GetReq
SF:uest,157,"HTTP/1\.0\x20401\x20Unauthorized\r\nServer:\x20\r\nDate:\x20T
SF:ue,\x2018\x20Aug\x202009\x2016:45:58\x20GMT\r\nWWW-Authenticate:\x20Bas
SF:ic\x20realm=\"Linksys\x20WAG54G2\x20\"\r\nContent-Type:\x20text/html\r\
SF:nConnection:\x20close\r\n\r\n\n401\x20Unauthorized
```