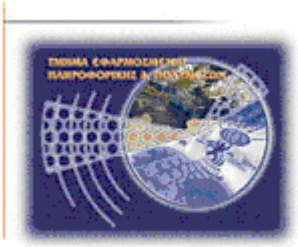
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων



Πτυχιακή εργασία

Υλοποίηση διεξαγωγής ελέγχου ασφαλείας σε υπολογιστικό σύστημα βασισμένης στη μεθοδολογία OSSTMM

Χρυσοβαλάντης Εμμανουήλ Παπαδάκης (ΑΜ: 1633)
epp1633@epp.teiher.gr

Ηράκλειο – 28/04/09

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

***Υπεύθυνη Δήλωση**: Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Εφαρμοσμένης Πληροφορικής και Πολυμέσων του Τ.Ε.Ι. Κρήτης.*

Ευχαριστίες

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον επόπτη καθηγητή της εργασίας μου κύριο Χαράλαμπο Μανιφάβα, για την εμπιστοσύνη που μου έδειξε αναθέτοντάς μου αυτή την εργασία, για την πολύτιμη βοήθεια και καθοδήγησή του καθ' όλη τη διάρκειά της και κυρίως για την ευκαιρία που μου έδωσε να ασχοληθώ με ένα πολύ ενδιαφέρον αντικείμενο.

Πίνακας Περιεχομένων

Πίνακας Εικόνων

Κεφάλαιο 1 Εισαγωγή

1.1 Γενικά

Η διεξαγωγή ελέγχου ασφάλειας είναι ουσιαστικά η αποτίμηση των μέτρων ασφαλείας ενός δικτύου ή ενός συστήματος, με σκοπό: την βελτίωση της ασφάλειας του, τον σχεδιασμό διαδικασιών για την αποφυγή ανεπιθύμητων καταστάσεων, τον σχεδιασμό και την υλοποίηση τρόπων για την διασφάλιση των δεδομένων, και τέλος την εκπαίδευση των χρηστών του δικτύου ή του συστήματος με την χρήση πολιτικών ασφάλειας.

1.2 Σκοπός

Για τον έλεγχο αυτό εφαρμόστηκε το πρότυπο Open Source Security Testing Methodology Manual (OSSTMM, http://www.osstmm.org). Ο έλεγχος του δικτύου ή του συστήματος περιλαμβάνει τα παρακάτω:

- Έρευνα σχετικά με το υπό δοκιμή δίκτυο
  - Πληροφορίες για το δίκτυο
- Ανίχνευση των πορτών
  - Προσδιορισμός της κατάστασης των πορτών στις οποίες ακούν διάφορες υπηρεσίες
- Προσδιορισμός των υπηρεσιών
  - Εντοπισμός των υπηρεσιών που “τρέχουν” πίσω από τις πόρτες
- Προσδιορισμός του συστήματος
  - Εντοπισμός του λειτουργικού συστήματος του Server
- Προσδιορισμός των αδυναμιών του συστήματος
  - Έρευνα και επαλήθευση των ευπαθειών
- Προσδιορισμός του δρομολογητή που χρησιμοποιεί το σύστημα
  - Έλεγχος του δρομολογητή
- Προσδιορισμός του firewall και της κατάστασης των πορτών
  - Έλεγχος του τείχους προστασίας
- Ανακάλυψη των κωδικών όσο αφορά λογαριασμούς χρηστών και αρχείων
  - Σπάσιμο κωδικών

Τέλος, η εργασία αυτή θα υλοποιήσει αντίμετρα σε κάθε ενότητα ώστε η διαθέσιμη πληροφορία να μην είναι ικανοποιητική όσο αφορά την χρησιμότητά της σε έναν επιτιθέμενο.

1.3 Σχεδιάγραμμα Αναφοράς

Αριθμός κεφαλαίου	Τίτλος	Σύντομη περιγραφή
1	Εισαγωγή	Περιγραφή Κεφαλαίου.
2	Internet Security	Περιγραφή Κεφαλαίου.
3	Πρωτότυπα Κείμενα	Περιγραφή Κεφαλαίου.
4	Βιβλιογραφία	Περιγραφή Κεφαλαίου.
Παράρτημα Α	Συντομογραφίες	Περιγραφή Κεφαλαίου.
Παράρτημα Β	Παρουσίαση	Περιγραφή Κεφαλαίου.
Παράρτημα Γ	Δημοσίευση	Περιγραφή Κεφαλαίου.

Κεφάλαιο 2 Internet Security

2.1 Network Surveying

2.1.1 Περιγραφή

Μια έρευνα δικτύου χρησιμεύει συχνά ως μια εισαγωγή στα συστήματα που εξετάζονται. Ορίζεται καλύτερα ως ο συνδυασμός συλλογής δεδομένων, πληροφοριών, και πολιτικού ελέγχου. Είναι συχνά ενδεδειγμένος από μια νομική σκοπιά για να καθορίσει ακριβώς βάσει του νόμου για το ποια συστήματα θα πρέπει να εξεταστούν, αν πρόκειται για third-party συγγραφέα ή και ακόμα αν πρόκειται για το διαχειριστή του συστήματος δεν θα μπορεί να αρχίσει με συγκεκριμένα ονόματα συστημάτων ή με διευθύνσεις IP. Σε αυτήν την περίπτωση θα πρέπει να γίνει έρευνα και ανάλυση. Σκοπός αυτής της άσκησης είναι να βρεθεί ο αριθμός των συστημάτων του δικτύου που μπορούν να εξεταστούν, χωρίς την παραβίαση των νόμιμων ορίων για αυτά που θα γίνει η εξέταση. Ως εκ τούτου, η έρευνα του δικτύου είναι ένας τρόπος για να ξεκινήσει κάποιος έλεγχος, κ΄ ένας άλλος είναι να είναι γνωστό το εύρος των IP που θα εξεταστούν. Σε αυτήν την ενότητα, καμία παρείσφρυση δεν εκτελείται άμεσα στα συστήματα εκτός από τις θέσεις που θεωρούνται ημι-δημόσια περιοχή.

Σε νομικά πλαίσια, η ημι-δημόσια περιοχή είναι ένα κατάστημα που προσκαλεί για την πραγματοποίηση αγορών. Το κατάστημα μπορεί να ελέγξει την πρόσβασή και μπορεί να αρνηθεί την είσοδο σε ορισμένα άτομα, αλλά για το μεγαλύτερο μέρος είναι ανοικτό στο ευρύ κοινό. Αυτό είναι το parallel στο ηλεκτρονικό εμπόριο ή και στον ιστοχώρο.

Η έρευνα δικτύων είναι μια αφετηρία, όπου ολοένα και περισσότεροι hosts εντοπίζονται κατά τη διάρκεια της εξέτασης. Σημειώνεται ότι οι hosts που ανακαλύπτονται αργότερα μπορούν να εισαχθούν στην εξέταση ως ένα υποσύνολο της καθορισμένης δοκιμής και συχνά μόνο με την άδεια ή τη συνεργασία με την εσωτερική ομάδα ασφαλείας του στόχου.

Αναμενόμενα αποτελέσματα:

- Τα ονόματα των περιοχών
- Τα ονόματα των Server
- Τις διευθύνσεις IP
- Το χάρτη του δικτύου
- Πληροφορίες για ISP/ASP
- Τους κατόχους των συστημάτων και των υπηρεσιών
- Κάτοχοι των συστημάτων
- Πιθανούς περιορισμούς δοκιμών

Βήματα που εφαρμόζονται για την έρευνα ενός δικτύου:

Απαντήσεις κεντρικών Server:

- Εξέταση των Domain registry πληροφοριών των Server.

- *Πληροφορίες για μια IP διεύθυνση ή ένα όνομα χώρου. Όπως το όνομα του ιδιοκτήτη, τη διεύθυνση, τον διαχειριστή του ονόματος κτλ.*

- Εύρεση του φάσματος των IP.
  - *Το εύρος των διευθύνσεων ip που είναι παρακρατημένο για απόδοση σε τοπικά δίκτυα.*

- Εξέταση των πρωτεύων, των δευτερεύων Server και των ISP για hosts και υποπεριοχές.
  - *Σε ποιο Server ανήκει κάποιο domain και ποιος πάροχος το φιλοξενεί.*

Εξέταση του outer wall του δικτύου:
- Χρήση πολλαπλών ιχνών στην gateway για τον καθορισμό του outer network layer και των router.
  - *Το χάρτη δικτύου που παρουσιάζει μια κατανοητή γραφική προβολή όλων των συσκευών του δικτύου και του τρόπου σύνδεσής τους.*

Εξέταση των διαδρομών από τον οργανισμό που είναι ο στόχος μας:
- Αναζήτηση web logs και intrusion logs για ίχνη των συστημάτων του στόχου.
- Αναζήτηση board και newsgroup postings για τα ίχνη των Server πίσω στο δίκτυο του στόχου.
  - *Πηγές που να αναφέρουν διαδικτυακές επιθέσεις όσο αφορά το στόχο.*

Διαρροές πληροφοριών (Δεν πραγματοποιήθηκε):
- Εξέταση του πηγαίου κώδικα του web server του στόχου, τα script των server των εφαρμογών και των εσωτερικών συνδέσεων.
- Εξέταση των email headers, των bounced mails και των αποδείξεων των ιχνών του server.
- Αναζήτηση των newsgroups για τις ταχυδρομημένες πληροφορίες του στόχου.
- Αναζήτηση των βάσεων δεδομένων εργασίας και εφημερίδων για θέσεις IT μέσα στην οργάνωση σχετικά με το υλικό και το λογισμικό.
- Αναζήτηση υπηρεσιών P2P για συνδέσεις στο δίκτυο του στόχου και για στοιχεία σχετικά με την οργάνωση.

Πληροφορίες:
- *Για το DNS, το Server, το range των IP, τον παρόχο κ. α χρησιμοποιήσαμε το πρόγραμμα Visual Route και μια σελίδα του διαδικτύου www.ripe.net και η διαδικασία περιγράφεται στην ενότητα 1.1.2*

- *Για τυχόν διαδικτυακές παραβιάσεις που έγιναν στα δύο πανεπιστημιακά ιδρύματα έγινε αναφορά στην ενότητα 1.1.3*

2.1.2 Examine the outer wall of the network

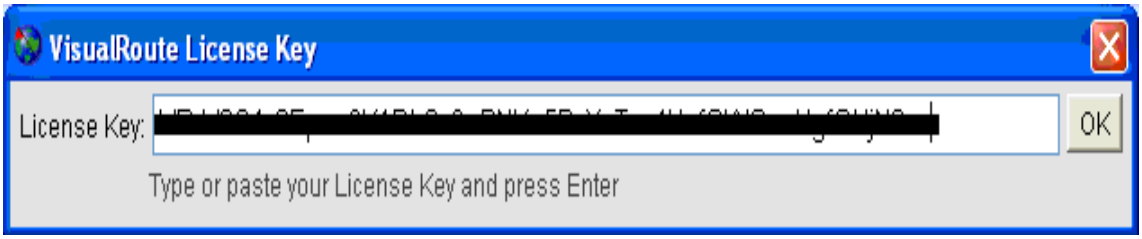
Visual Route

Το Visual Route είναι μια γραφική traceroute, ping και whois εφαρμογή η οποία επισημαίνει τις IP διευθύνσεις και τα domain της προέλευσης τους και απεικονίζει τα αποτελέσματα σε ένα γραφικό παγκόσμιο χάρτη. Μπορεί να προσδιορίσει τη φυσική

θέση της διεύθυνσης σε επίπεδο πόλεων και παρέχει τον κάτοχο και την επίτευξη της επικοινωνίας μέσω ενσωματωμένων Whois lookup. Το Visual Route βοηθάει επίσης στην ανάλυση των προβλημάτων συνδεσιμότητας στο Internet, επιτρέποντας την ανίχνευση και την τεκμηρίωση της αιτίας για τη φτωχή συνδεσιμότητα του Internet για το αν οφείλεται στον πάροχο ή σε άλλα προβλήματα του δικτύου.

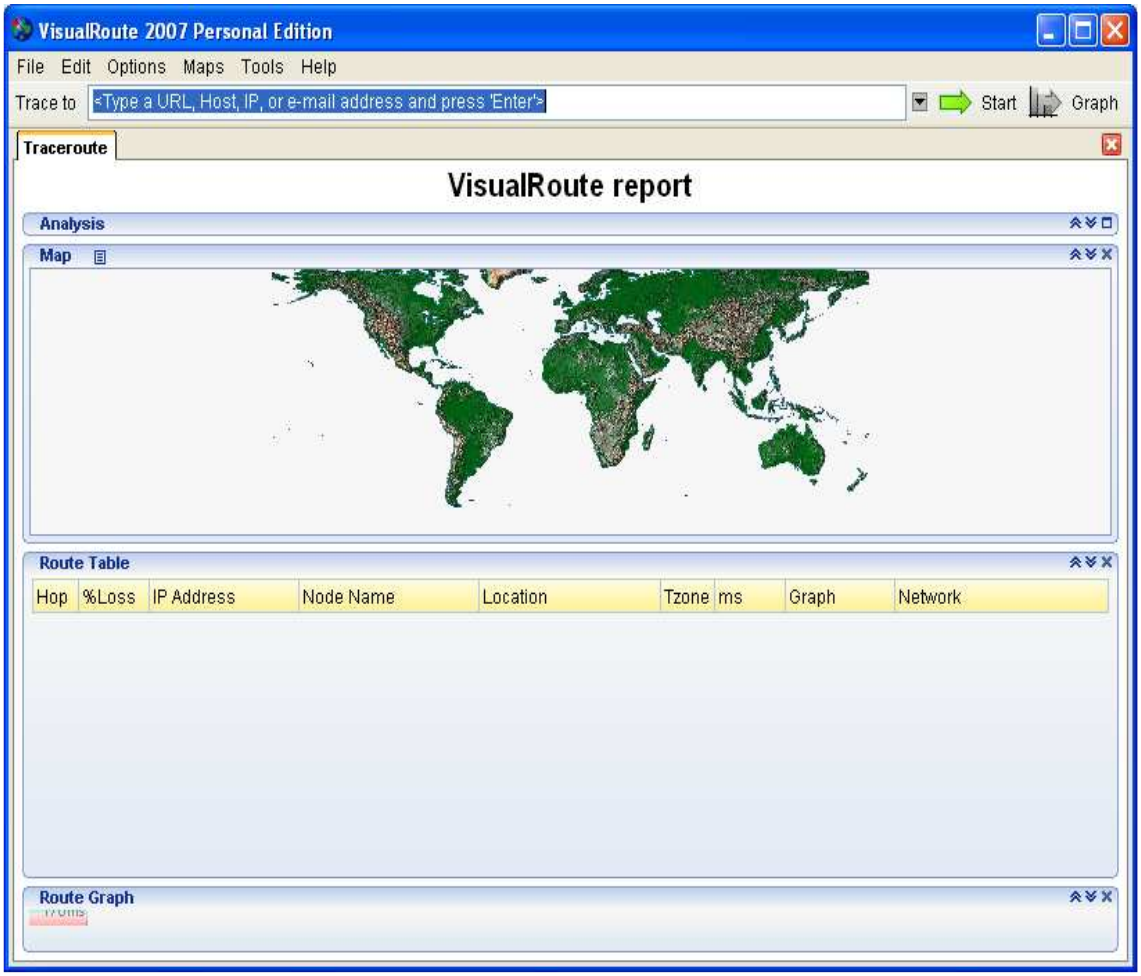
Download: http://www.filestube.com/2935d4da80c2672403e9/go.html

Παρακάτω γίνεται η τοποθέτηση του κωδικού που μας στάλθηκε ηλεκτρονικά για να χρησιμοποιήσουμε την πλήρη έκδοση του προγράμματος.



Εικόνα 1 Visual Route : Εισαγωγή Lisence Key

Έπειτα θα ανοίξουμε το πρόγραμμα. Στο πεδίο κειμένου trace το θα πληκτρολογήσουμε τη διεύθυνση όπου θα γίνει η ανίχνευση της προέλευσης της. Συγκεκριμένα η ανίχνευση θα γίνει για δύο διαδικτυακούς τόπους.

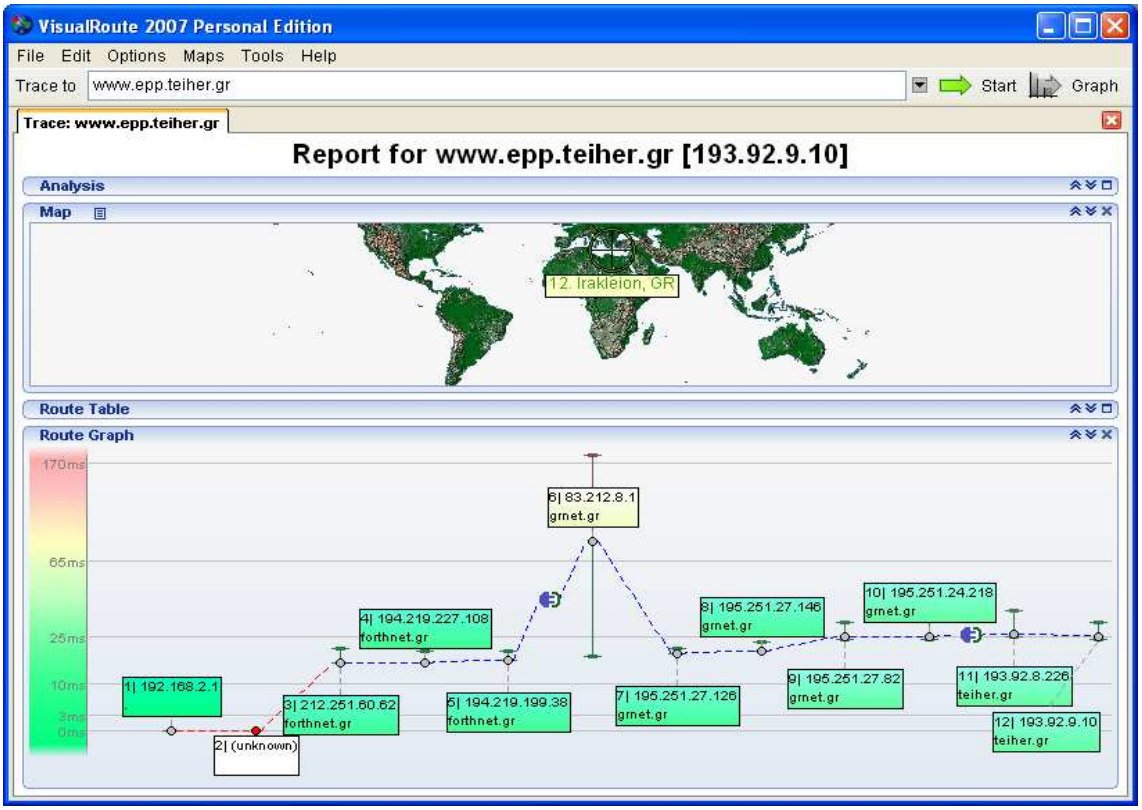


Εικόνα 2 Visual Route : Απεικόνιση του προγράμματος

Στην πρώτη περίπτωση θα πληκτρολογήσουμε τη σελίδα του τμήματος της Εφαρμοσμένης Πληροφορικής και Πολυμέσων του ΤΕΙ Κρήτης όπως παρακάτω και θα επιλέξουμε "Start" για να ξεκινήσει η διαδικασία της ανίχνευσης.

Εικόνα 3 Visual Route : Πληκτρολόγηση www.epp.teiher.gr

Παρακάτω λοιπόν έχουμε το αποτέλεσμα της ανίχνευσης όπου παρουσιάζεται η πλήρης διαδρομή (χάρτης) του αιτήματος που στέλνεται όταν θέλουμε να παρουσιαστεί η συγκεκριμένη σελίδα στον υπολογιστή μας.



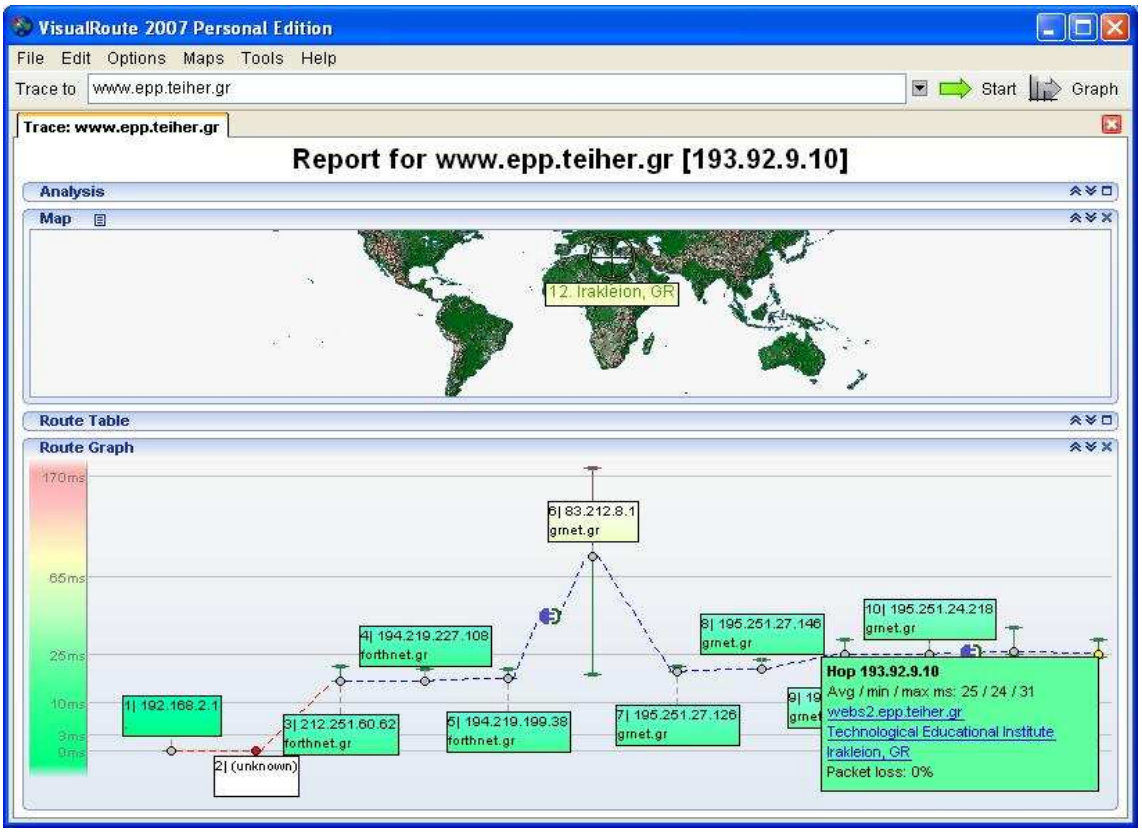
Εικόνα 4 Visual Route : Χάρτης δικτύου με τα hops

2.1.3 Name Server Responses

Κάνοντας απλά mouse over πάνω από την IP address του http: //www.epp.teiher.gr δηλαδή την 193.92.9.10 μπορούμε να πάρουμε πληροφορίες για

- Το Domain Name System
- Το όνομα του δικτύου

Αυτά παρουσιάζονται στην εικόνα που ακολουθεί:

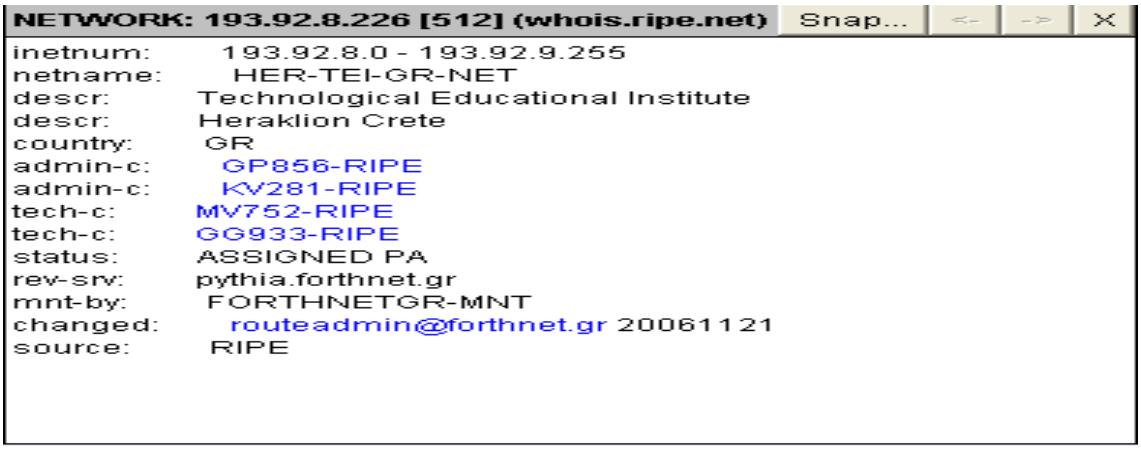


Εικόνα 5 Visual Route : Πληροφορίες του DNS και του δικτύου

Επιλέγοντας την περιγραφή του δικτύου θα ανακτήσουμε γενικότερες πληροφορίες σχετικά με αυτό. Παρακάτω εμφανίζονται πληροφορίες σχετικά με

- Το range των διευθύνσεων IP του δικτύου
- Την περιγραφή του δικτύου
- Τη χώρα όπου βρίσκεται
- Τα κωδικά ονόματα των Administrative Contacts
- Τα κωδικά ονόματα των Technical Contacts
- Την κατάσταση
- Το server όπου έχει ανέβει η σελίδα
- Τον πάροχο(ISP)
- Το πότε έγινε τροποποίηση
- Την πηγή των πληροφοριών

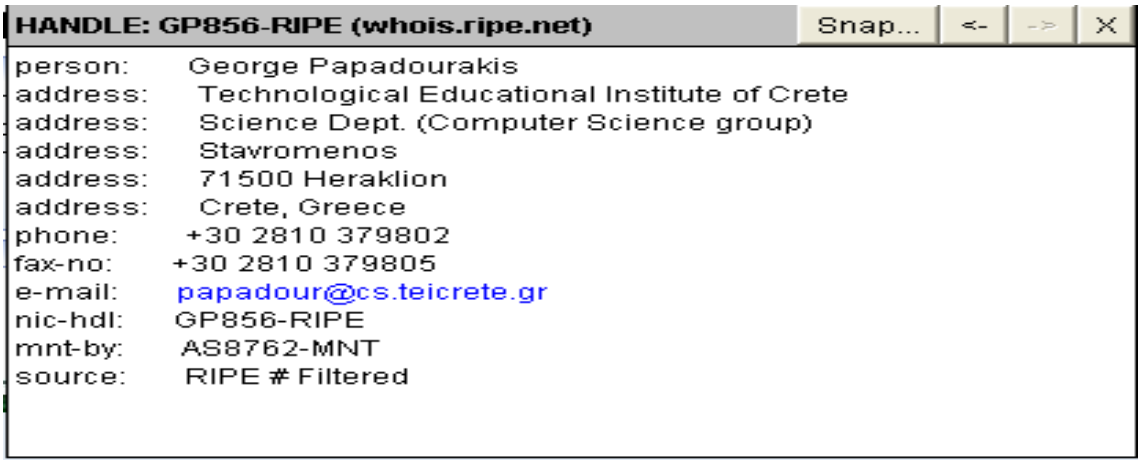
- Network:



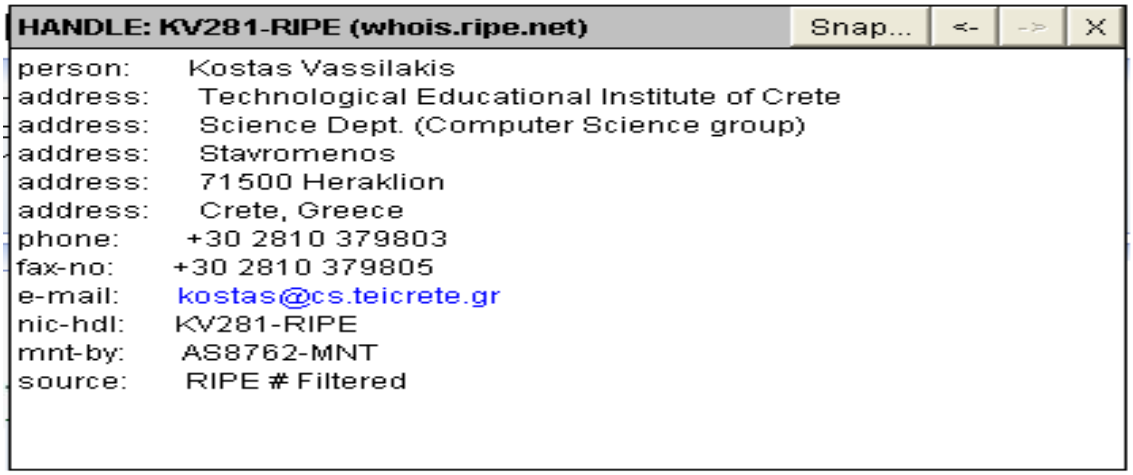
Εικόνα 6 Visual Route : Πληροφορίες του δικτύου

Κλικάροντας τα κωδικά ονόματα των Administrative Contacts και των Technical Contacts ενημερωνόμαστε γι αυτούς. Έχουμε λοιπόν για τους:

- Admin-c:

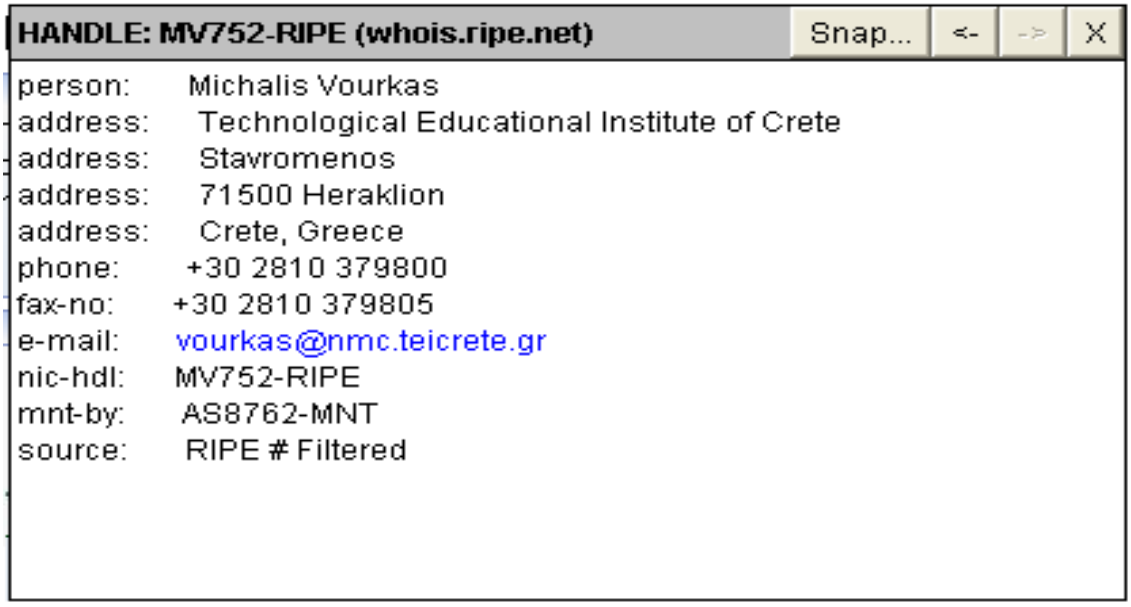


Εικόνα 7 Visual Route : Πληροφορίες του Admin-C

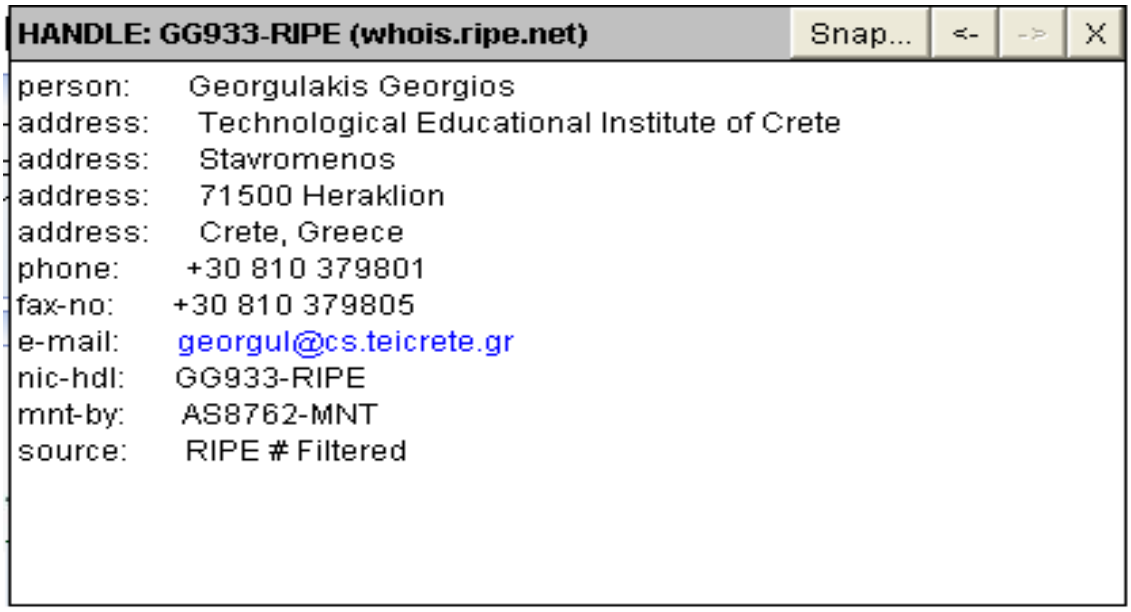


Εικόνα 8 Visual Route : Πληροφορίες του Admin-C

- Tech-c:



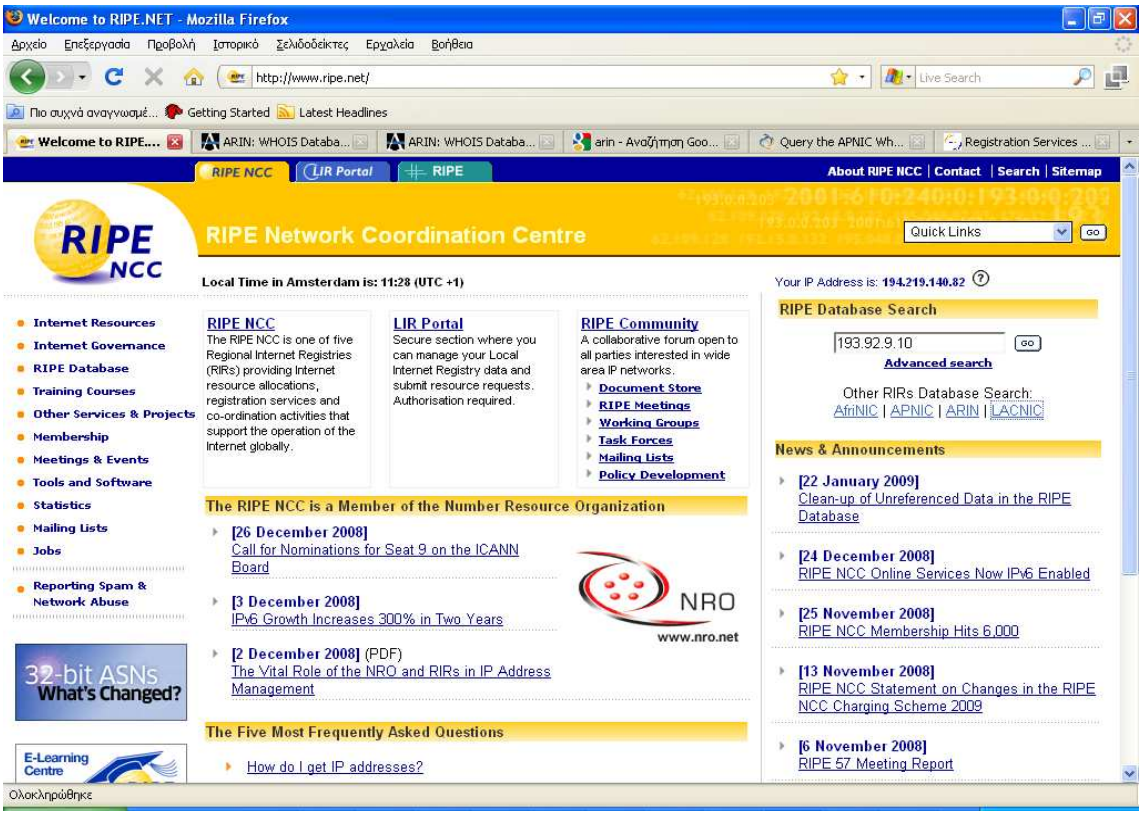
Εικόνα 9 Visual Route : Πληροφορίες του Tech-C



Εικόνα 10 Visual Route : Πληροφορίες του Tech-C

Για την ανάκτηση περισσότερων πληροφοριών σχετικά με τον κόμβο μπορούμε να μεταβούμε στην παρακάτω σελίδα: http://www.ripe.net/

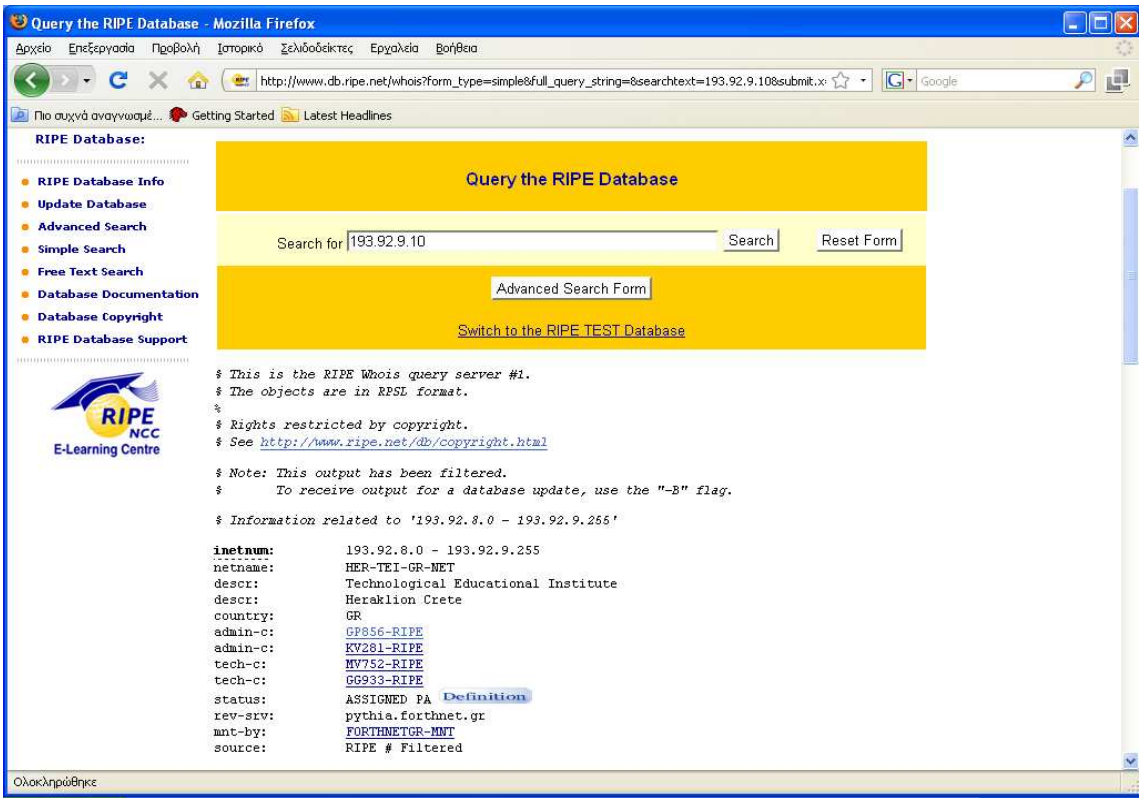
Στην παρακάτω σελίδα στο πεδίο textfield RIPE Database Search πληκτρολογούμε τη διεύθυνση IP “193.92.9.10” που έχουμε ανακτήσει από το χάρτη του Visual Route και επιλέγοντας “Go” θα ξεκινήσει η ανάκτηση των πληροφοριών.



Εικόνα 11 Visual Route : Παρουσίαση της σελίδας της μεθόδου Whois

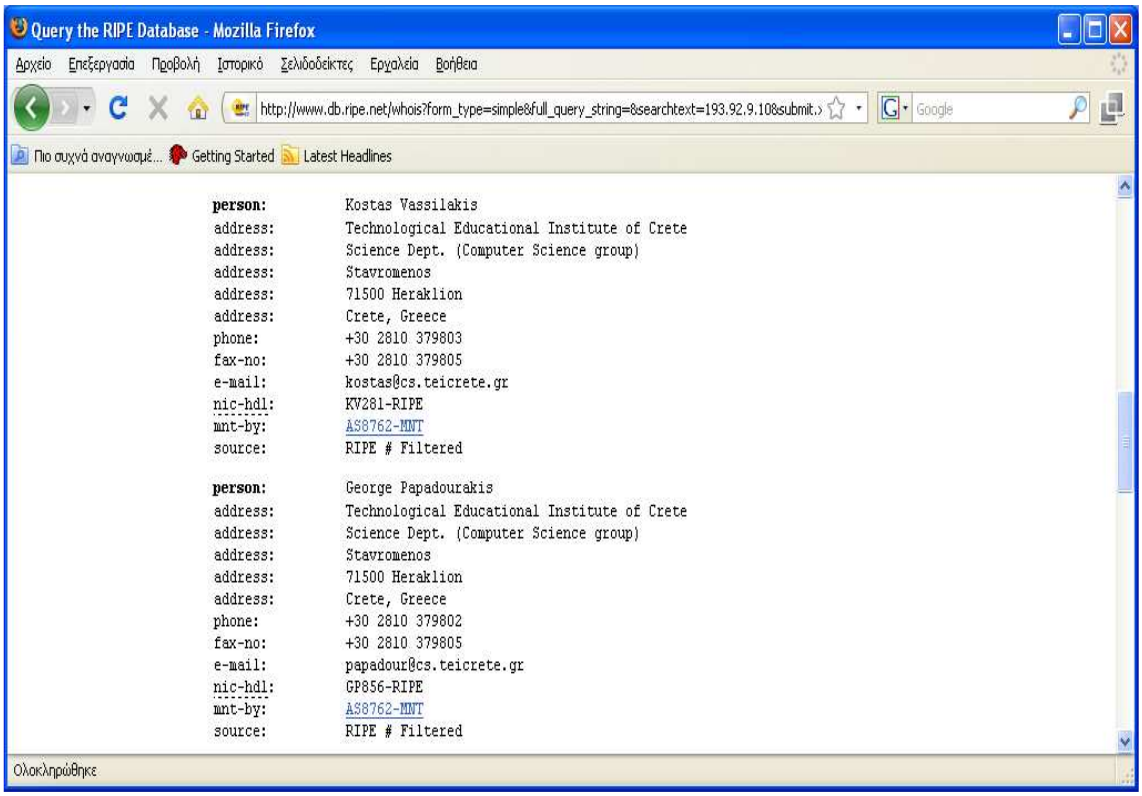
Τα αποτελέσματα που ανακτάμε παρουσιάζονται στις παρακάτω εικόνες:

- Network:



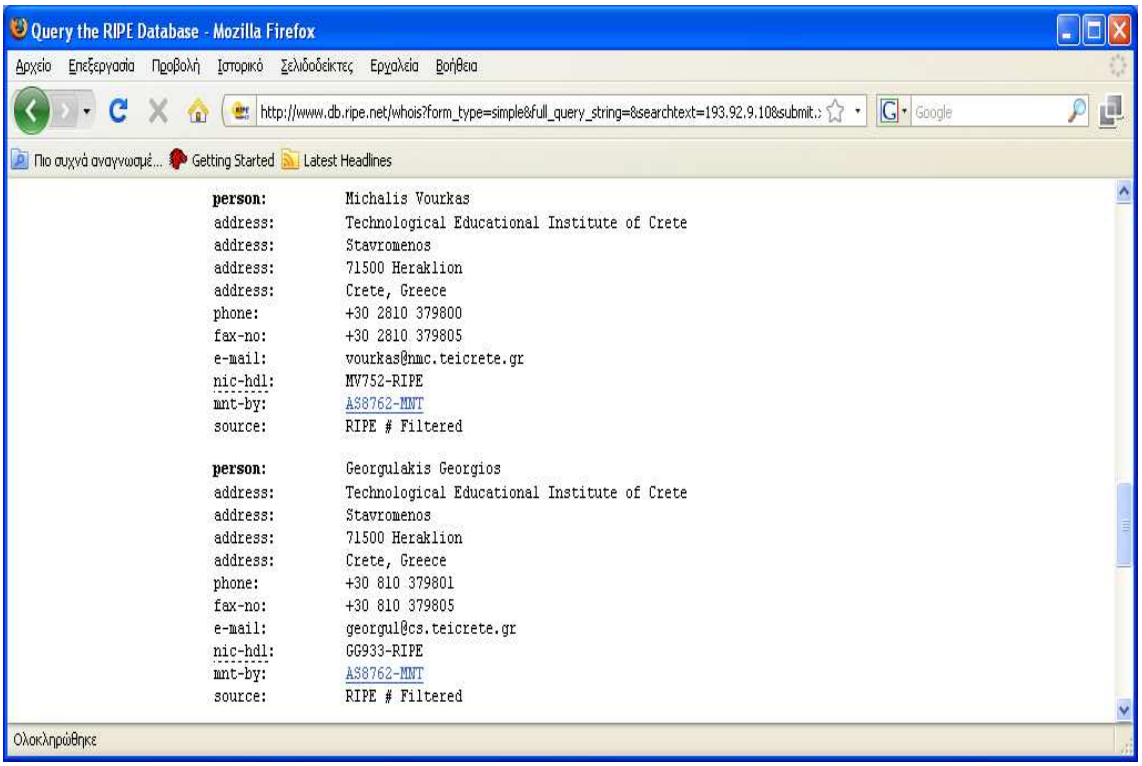
Εικόνα 12 Visual Route : Αναλυτικές πληροφορίες του δικτύου

- Admin –c:



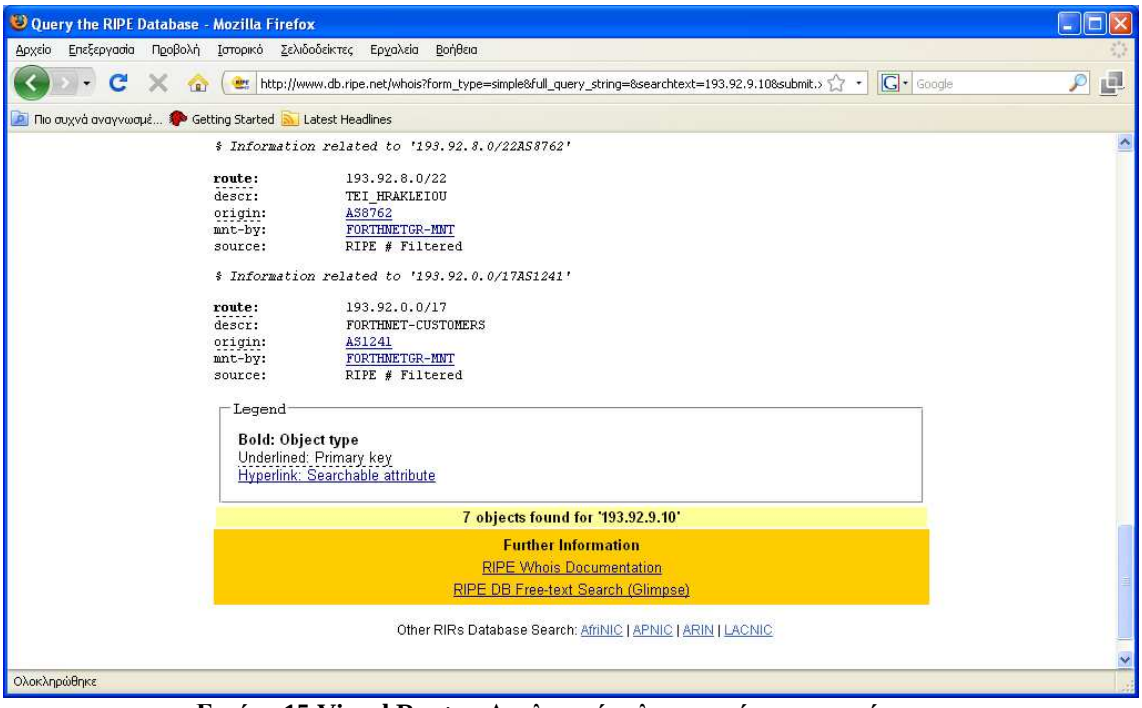
Εικόνα 13 Visual Route : Αναλυτικές πληροφορίες των Admin-C

- Tech-c:



Εικόνα 14 Visual Route : Αναλυτικές πληροφορίες των Tech-C

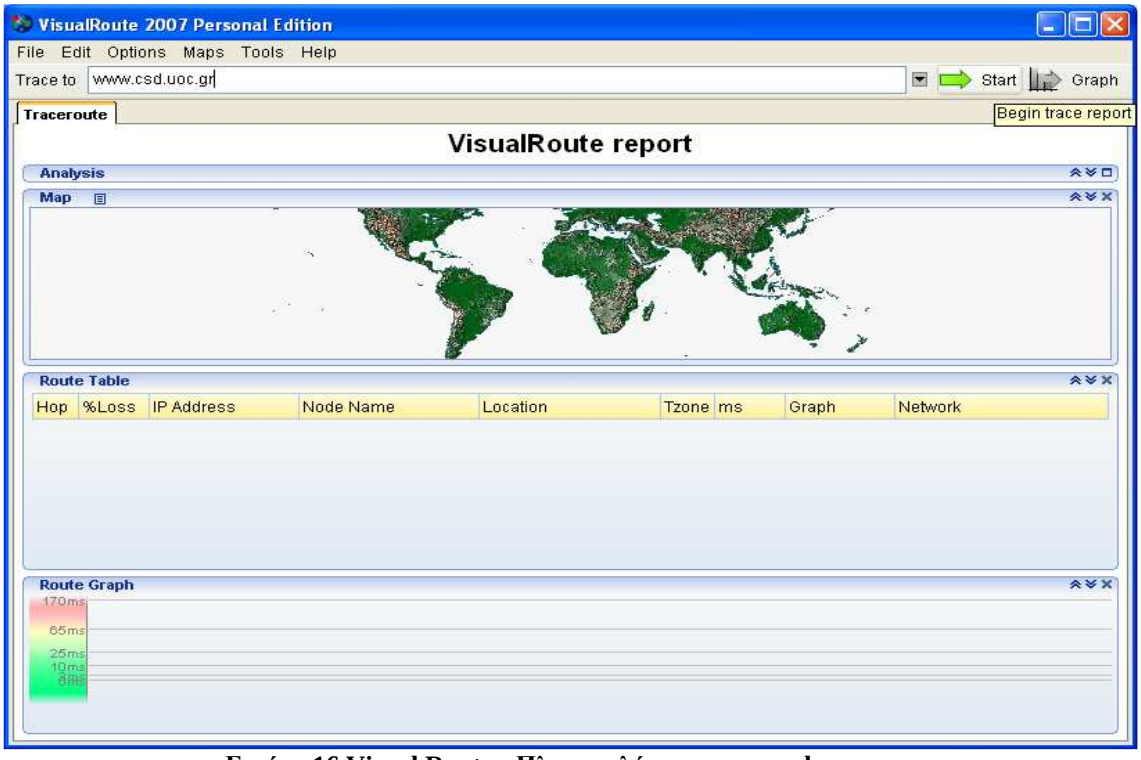
- Route:



Εικόνα 15 Visual Route : Αναλυτικές πληροφορίες του παρόχου

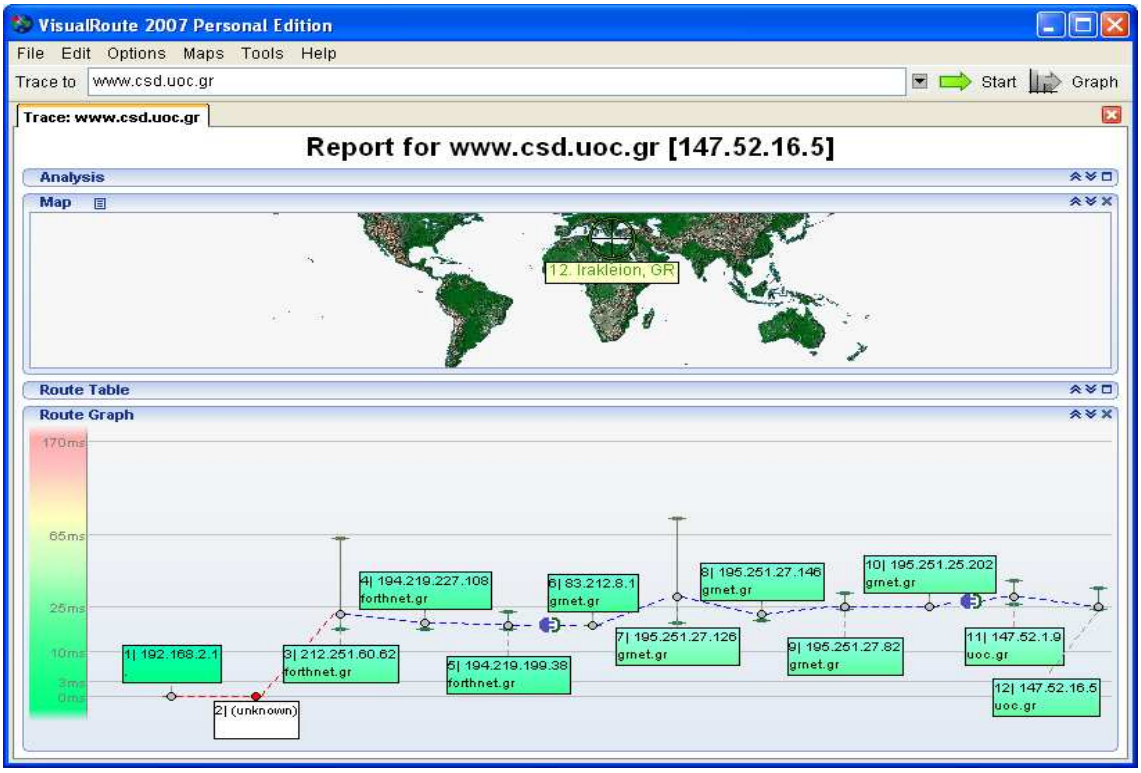
Εφαρμόζοντας τα ίδια βήματα και με την ίδια σειρά θα γίνει ανίχνευση στην σελίδα του τμήματος Επιστήμης των Υπολογιστών του Πανεπιστημίου Κρήτης http://www.csd.uoc.gr. Παρακάτω παρουσιάζονται τα αποτελέσματα της ανίχνευσης.

Πληκτρολογούμε τη διεύθυνση:



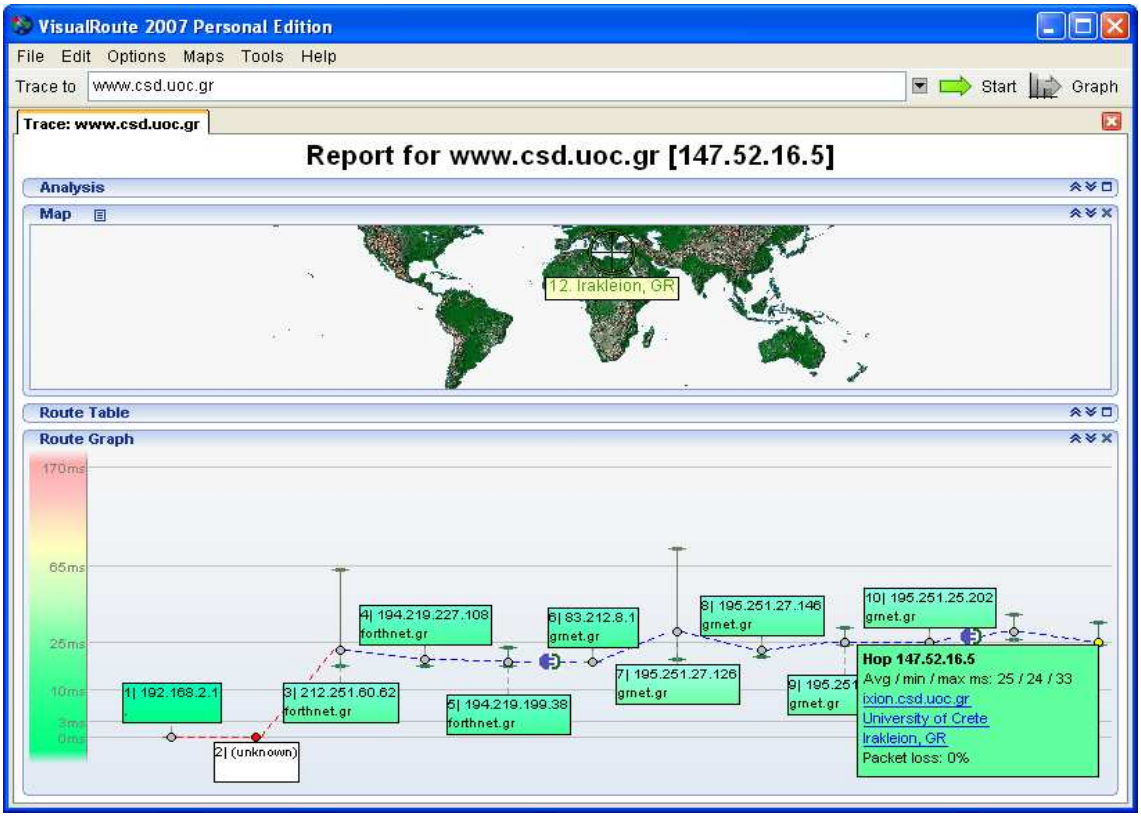
Εικόνα 16 Visual Route : Πληκτρολόγηση www.csd.uoc.gr

- Χάρτης της διαδρομής:



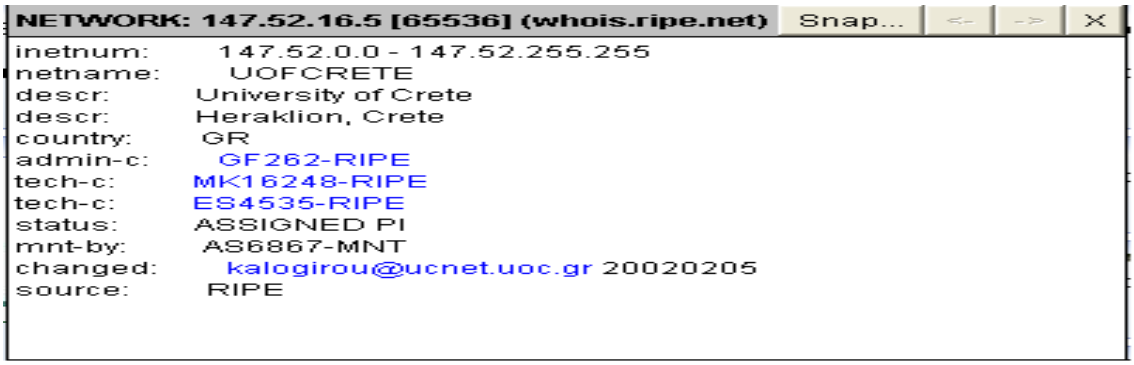
Εικόνα 17 Visual Route : Χάρτης δικτύου με τα hops

- Πληροφορίες για τον DNS και το όνομα του δικτύου:



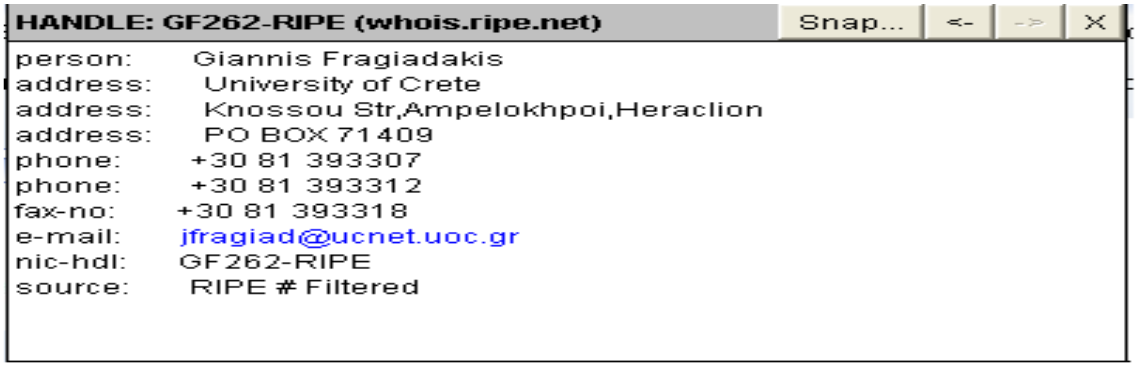
Εικόνα 18 Visual Route : Πληροφορίες του DNS και του δικτύου

- Network:



Εικόνα 19 Visual Route : Πληροφορίες του Admin-C

- Admin-c:



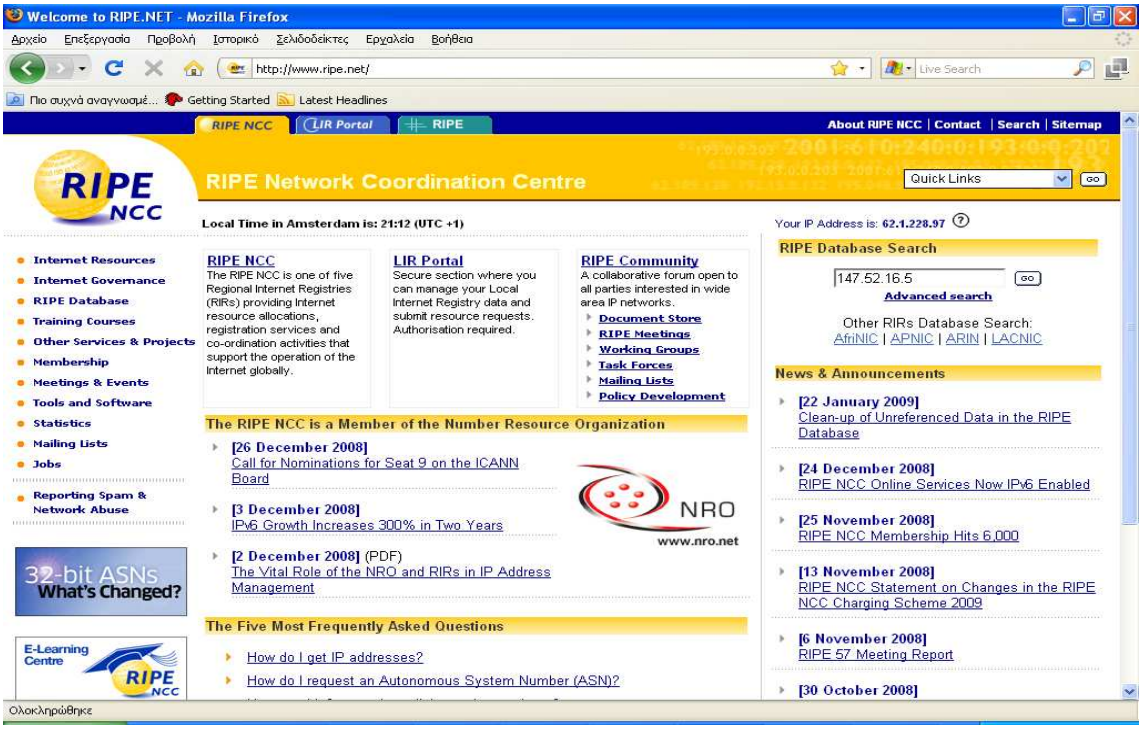
Εικόνα 20 Visual Route : Πληροφορίες του Tech-C

- Tech-c:

Εικόνα 21 Visual Route : Πληροφορίες του Tech-C

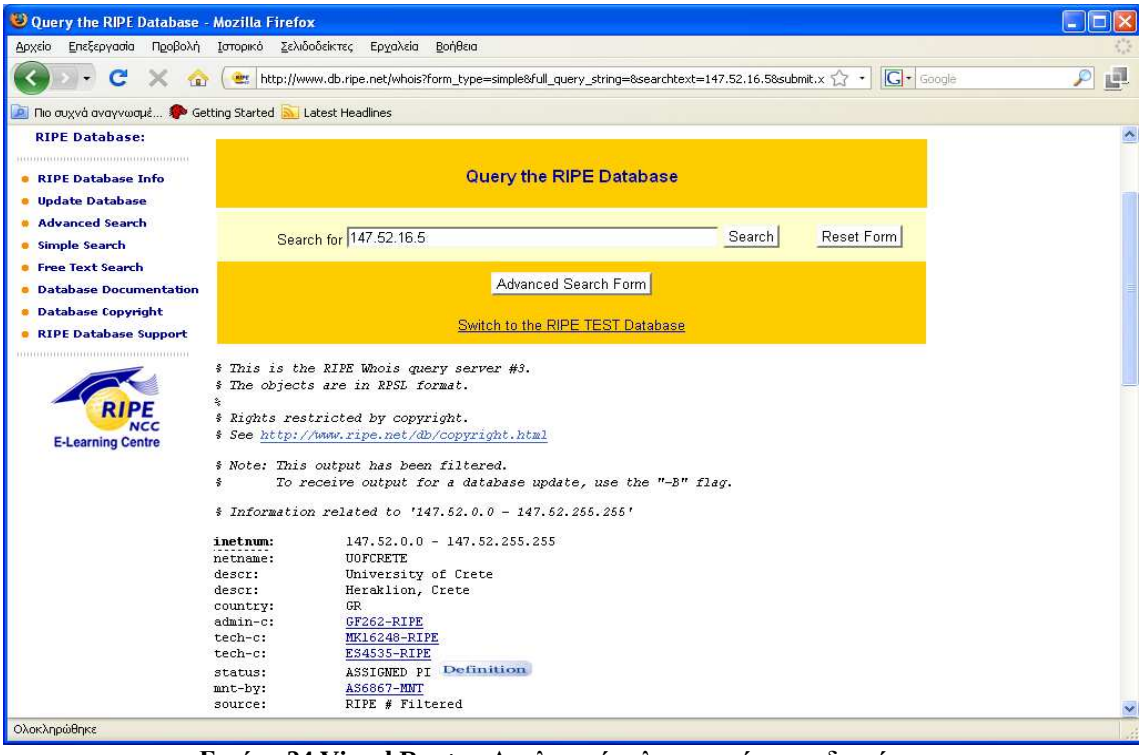
Εικόνα 22 Visual Route : Πληροφορίες του Tech-C

Ομοίως όπως και παραπάνω στο πεδίο textfield RIPE Database Search πληκτρολογούμε τη διεύθυνση IP “147.52.16.5” που έχουμε ανακτήσει από το χάρτη του Visual Route και επιλέγοντας “Go” θα ξεκινήσει η ανάκτηση των πληροφοριών αυτή τη φορά για το τμήμα της Επιστήμης των Υπολογιστών.



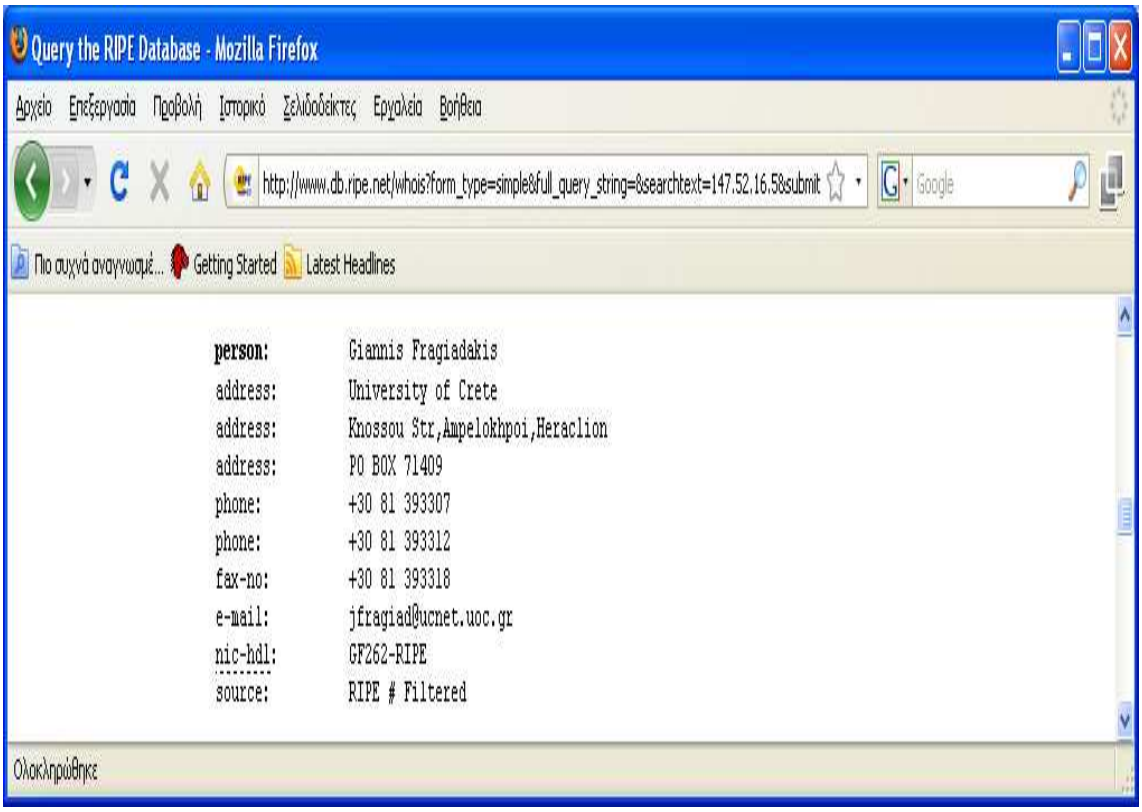
Εικόνα 23 Visual Route : Παρουσίαση της σελίδας της μεθόδου Whois

- Network



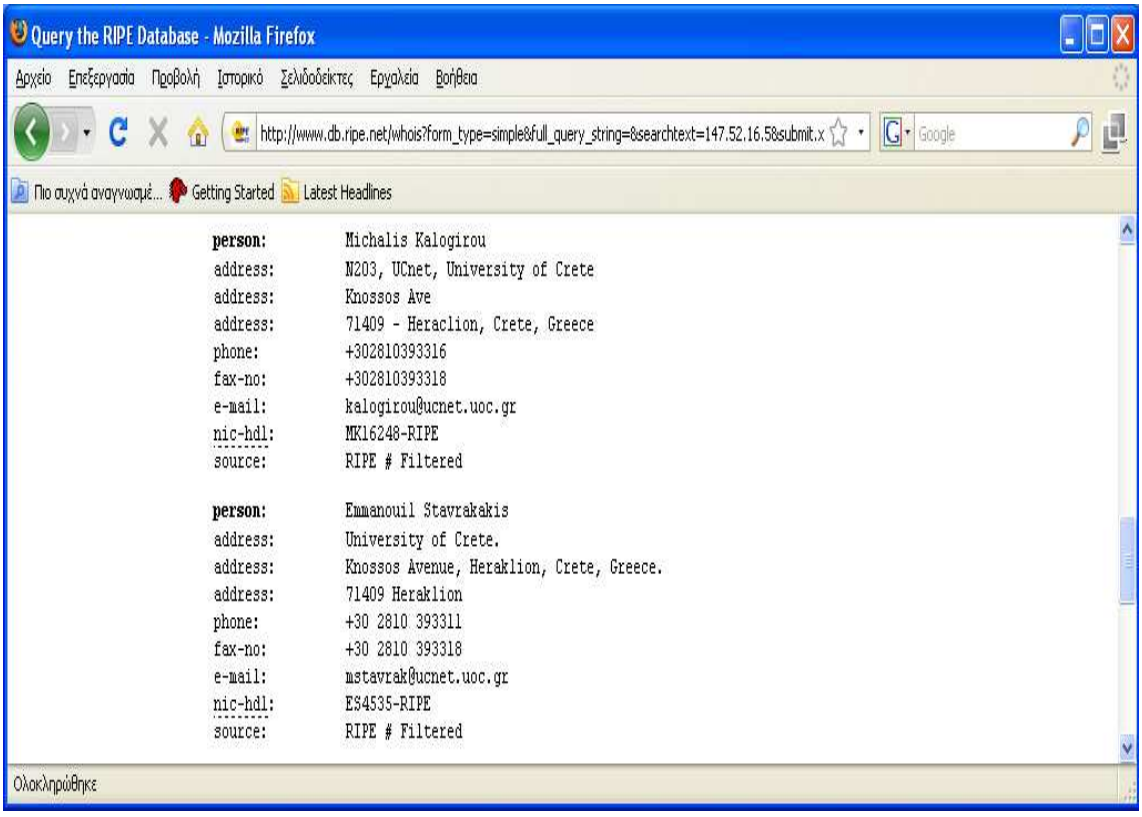
Εικόνα 24 Visual Route : Αναλυτικές πληροφορίες του δικτύου

- Admin –c:



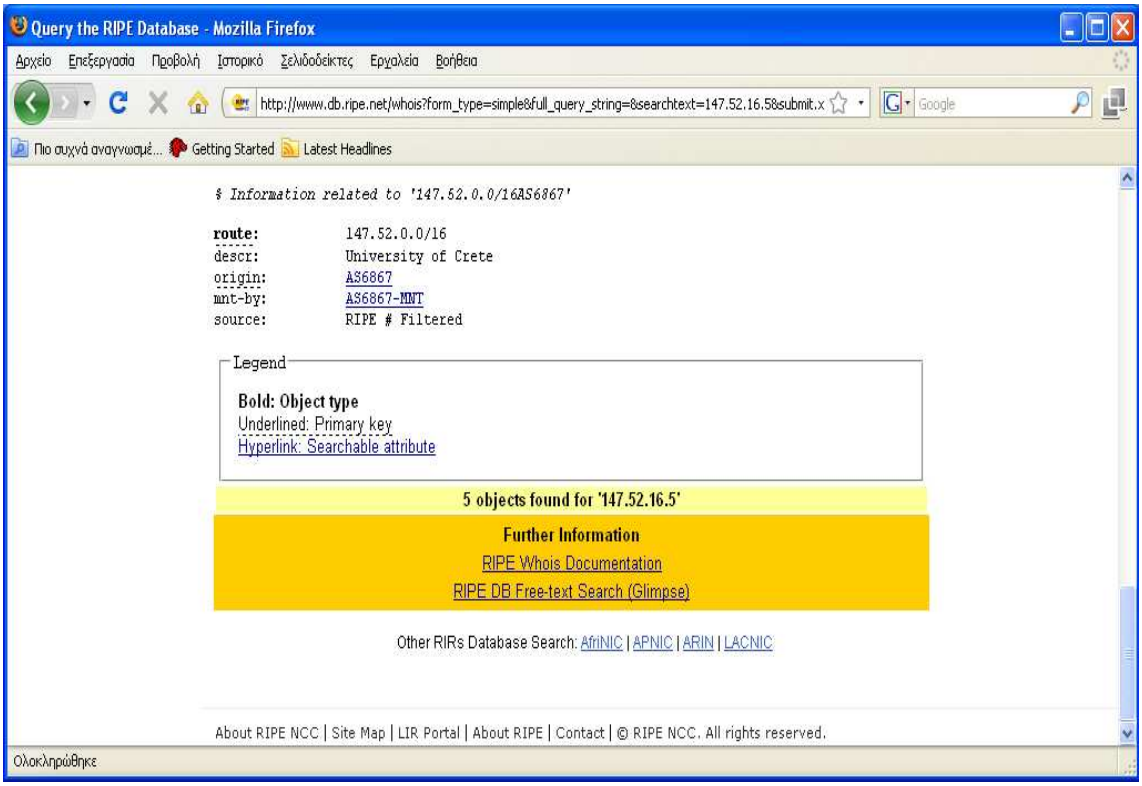
Εικόνα 25 Visual Route : Αναλυτικές πληροφορίες του Admin-C

- Tech –c:



Εικόνα 26 Visual Route : Αναλυτικές πληροφορίες των Tech-C

- Route:



Εικόνα 27 Visual Route : Αναλυτικές πληροφορίες του παρόχου

2.1.4 Examine tracks from the target organization

Όσο αφορά τις διαδικτυακές επιθέσεις, δεν βρέθηκαν αναφορές μέσω του Διαδικτύου που να αναφέρουν τυχόν επιθέσεις που έχουν δεχτεί αυτά τα δύο τμήματα.

2.2 Port Scanning

2.2.1 Περιγραφή

Το Port Scanning είναι η διαδικασία της εισβολής στις πόρτες ενός συστήματος σε επίπεδο μεταφοράς και δικτύου. Αυτή η ενότητα απαριθμεί ενεργές ή προσβάσιμες υπηρεσίες Internet όπως και ενέργειες που διαπερνούν το τείχος προστασίας για να βρουν επιπλέον ενεργά συστήματα. Αυτό το μικρό δείγμα των πρωτοκόλλων που παρουσιάζεται εδώ είναι για τη σαφήνεια του καθορισμού των πορτών. Πολλά πρωτόκολλα δεν υπάρχουν εδώ. Η ανίχνευση για διαφορετικά πρωτόκολλα θα εξαρτηθεί από τον τύπο και τις υπηρεσίες συστημάτων που προσφέρει. Μια πιο ολοκληρωμένη λίστα από πρωτόκολλα μπορούμε να βρούμε στην ενότητα του Test References.

Κάθε Διαδικτυακό σύστημα έχει 65.536 TCP και UDP πιθανές πόρτες (συμπεριλαμβάνεται και η πόρτα 0). Εντούτοις, δεν είναι πάντα απαραίτητο να ελέγχουμε όλες τις πόρτες σε όλα τα συστήματα. Αυτό αφήνεται στην κρίση της ομάδας δοκιμής. Οι αριθμοί των πορτών που είναι σημαντικοί για έλεγχο σύμφωνα με την υπηρεσία παρατίθενται με το στόχο. Επιπλέον αριθμοί πορτών για ανίχνευση θα πρέπει να παρθούν από το Consensus Intrusion Database Project Site.

Αναμενόμενα αποτελέσματα:

- Ανοιχτές, κλειστές ή φιλτραρισμένες πόρτες
- Διευθύνσεις IP από ενεργά συστήματα
- Εσωτερική εξέταση των δικτύων των συστημάτων
- Λίστα από ανιχνευμένα tunneled και encapsulated πρωτόκολλα
- Λίστα από ανιχνευμένα πρωτόκολλα δρομολόγησης που υποστηρίζονται
- Ενεργά συστήματα
- Χάρτης δικτύου

Βήματα που εφαρμόζονται για την ανίχνευση πορτών:

Έλεγχος σφαλμάτων:

- Έλεγχος της διαδρομής στο δίκτυο που είναι ο στόχος μας για την απώλεια πακέτων.
- Μέτρηση του ποσοστού round-trip time των πακέτων.
- Μέτρηση του ποσοστού αποδοχής και απάντησης πακέτων στο δίκτυο που είναι ο στόχος μας.
- Μέτρηση της ποσότητας των αρνήσεων απώλειας ή σύνδεσης πακέτων στο δίκτυο που είναι ο στόχος μας.

Απαρίθμηση πορτών:

- Χρήση των TCP SYN (Half-Open) ανιχνεύσεων για την απαρίθμηση των πορτών οι οποίες είναι ανοιχτές, κλειστές ή φιλτραρισμένες στις προεπιλεγμένες πόρτες του TCP testing στο Appendix B για όλους τους σταθμούς του δικτύου.

- Χρήση ανιχνεύσεων UDP για την απαρίθμηση των πορτών που είναι ανοιχτές ή κλειστές στο προεπιλεγμένο UDP testing ports στο Appendix B αν το UDP δεν έχει φιλτραριστεί ακόμα.

Απαρίθμηση συστημάτων (Δεν πραγματοποιήθηκε) :

- Συλλογή των broadcast απαντήσεων από το δίκτυο
- Έλεγχος του τείχους προστασίας με σετ πακέτων TTLs που έχουν στρατηγική για όλες τις διευθύνσεις IP.
- Χρήση ICMP και αντίστροφα name lookups για τον καθορισμό της ύπαρξης όλων των μηχανών σε ένα δίκτυο.
- Χρήση της πηγαίας πόρτας 80 του TCP και του ACK στις πόρτες 3100-3150, 10001-10050, 33500-33550 και 50 τυχαίες πόρτες πάνω από 35000 για όλους τους σταθμούς του δικτύου.
- Χρήση των τεμαχίων του TCP σε αντίστροφη διάταξη με ανιχνεύσεις FIN, NULL, and XMAS στις πόρτες 21, 22, 25, 80, και 443 για όλους τους σταθμούς του δικτύου.
- Χρήση του TCP SYN στις πόρτες 21, 22, 25, 80, και 443 για όλους τους σταθμούς του δικτύου.
- Χρήση των προσπαθειών σύνδεσης DNS σε όλους τους σταθμούς του δικτύου
- Χρήση FTP και Proxies για την επίτευξη ανιχνεύσεων στο εσωτερικό του DMZ στις πόρτες 22, 81, 111, 132, 137, και 161 για όλους τους σταθμούς του δικτύου.

Επαλήθευση των διαφόρων απαντήσεων του πρωτοκόλλου (Δεν πραγματοποιήθηκε):

- Έλεγχος και εξέταση της χρήσης των πρωτοκόλλων κυκλοφορίας και δρομολόγησης.
- Χρήση και εξέταση της χρήσης των μεταβλητών πρωτοκόλλων.
- Χρήση και εξέταση της χρήσης των κρυπτογραφημένων πρωτοκόλλων.

Επαλήθευση του επιπέδου των απαντήσεων των πακέτων (Δεν πραγματοποιήθηκε) :

- Προσδιορισμός της προβλεψιμότητας της ακολουθίας του TCP.
- Προσδιορισμός της προβλεψιμότητας των αριθμών της ακολουθίας του TCP.
- Προσδιορισμός της ακολουθίας Generation predicatbility
- Προσδιορισμός του up-time του συστήματος.
- Χρήση των τεμαχίων του TCP σε αντίστροφη διάταξη για την απαρίθμηση των πορτών και των υπηρεσιών για το υποσύνολο των πορτών στο προεπιλεγμένο Packet Fragment testing ports στο Appendix B για όλους τους σταθμούς του δικτύου.

Πληροφορίες:

- *Για τον έλεγχο των σφαλμάτων και την απαρίθμηση των κόμβων ενός δικτύου χρησιμοποιήσαμε το πρόγραμμα Ping Tester και η διαδικασία περιγράφεται στην ενότητα 1.2.2 .*
- *Για την απαρίθμηση των πορτών και των υπηρεσιών χρησιμοποιήσαμε τα προγράμματα Superscan και Scanline όπου οι διαδικασίες περιγράφονται στις ενότητες 1.2.3 και 1.2.4*

2.2.2 Error Checking

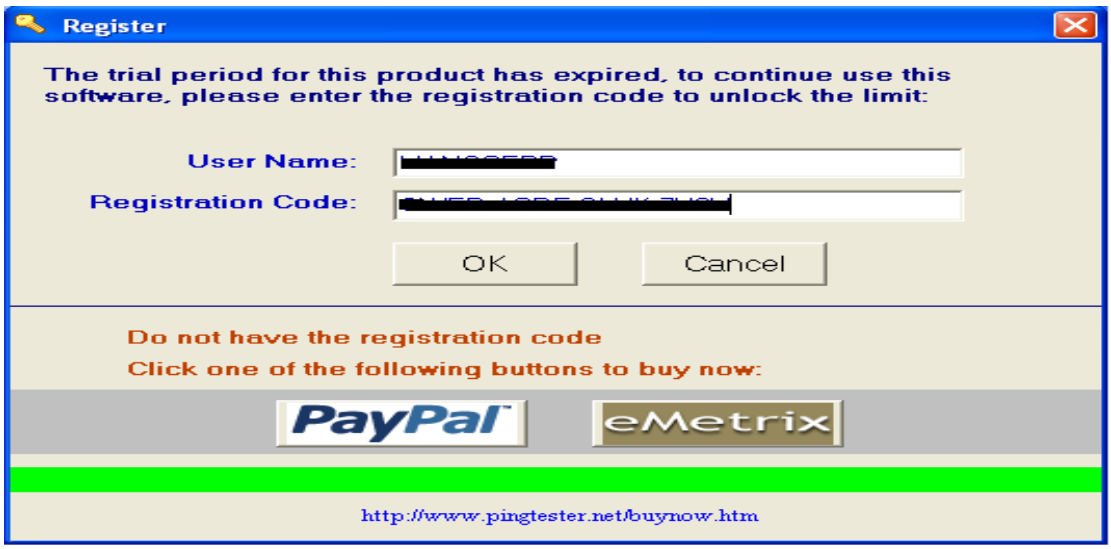
Το ping[1] είναι μια μέθοδος για τον εντοπισμό της διαθεσιμότητας και της απόδοσης ενός απομακρυσμένου πόρου του δικτύου. Θεωρείται ότι αποτελεί το ακρωνύμιο των λέξεων "Packet INternet Groper". Διαδικασία με την οποία επιβεβαιώνεται η σύνδεση με έναν απομακρυσμένο υπολογιστή π.χ. μέσω Internet ή τοπικού δικτύου.

Ping Tester

Το ping tester μπορεί να αποθηκεύσει μια λίστα από διευθύνσεις IP και εντολές δοκιμής δικτύων για να αυξήσει την αποδοτικότητα εργασίας, την υλοποίηση των τεστ ping και trace με ένα μόνο κλικ, ping sweep σε υποδίκτυα ή στους ενδιάμεσους κόμβους μιας λίστας συνεχόμενα. Τα αποτελέσματα μπορούν να αποθηκευτούν σε αρχεία τύπου txt ή Excel και μπορεί να διαμορφώσει και στατιστικά στοιχεία ώστε να γνωρίζουμε την κατάσταση του δικτύου κάθε στιγμή. Επίσης με το ip scanner που διαθέτει μπορούμε να σαρώσουμε ένα εύρος ip και να δούμε ποιες από αυτές χρησιμοποιούνται.

Download: http://www.pingtester.net/

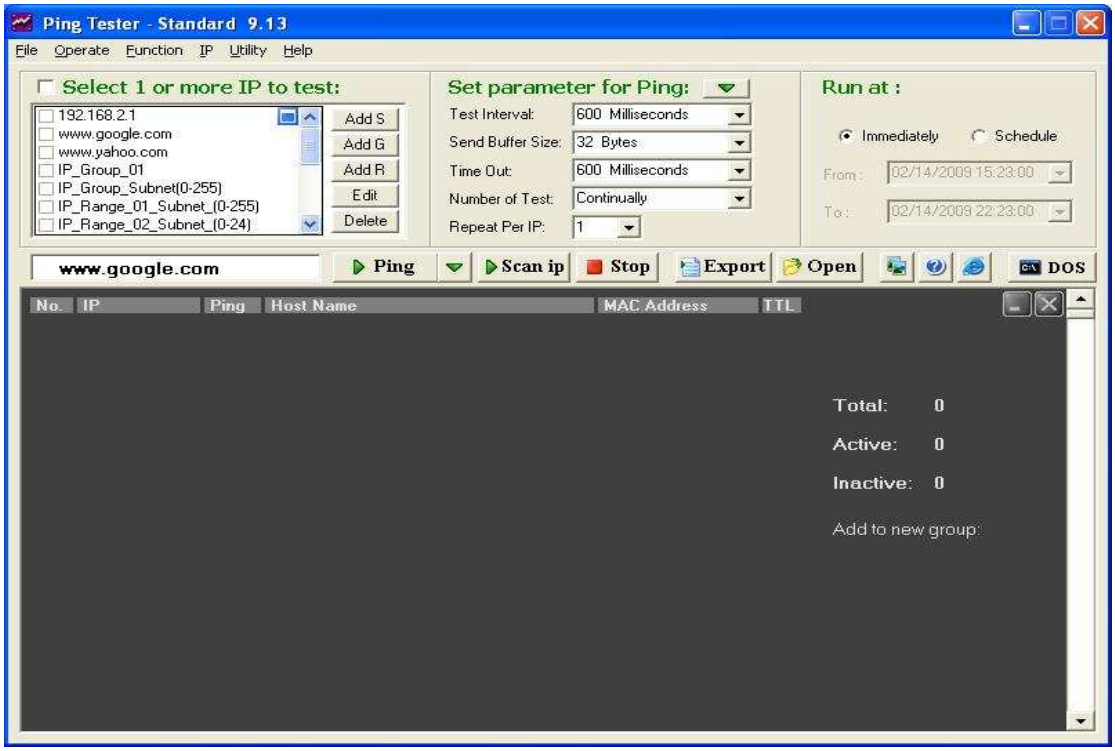
Στη συνέχεια γίνεται η τοποθέτηση του κωδικού που μας στάλθηκε ηλεκτρονικά για να χρησιμοποιήσουμε την πλήρη έκδοση του προγράμματος.



Εικόνα 28 Ping Tester : Πληκτρολόγηση User Name και Registration Code

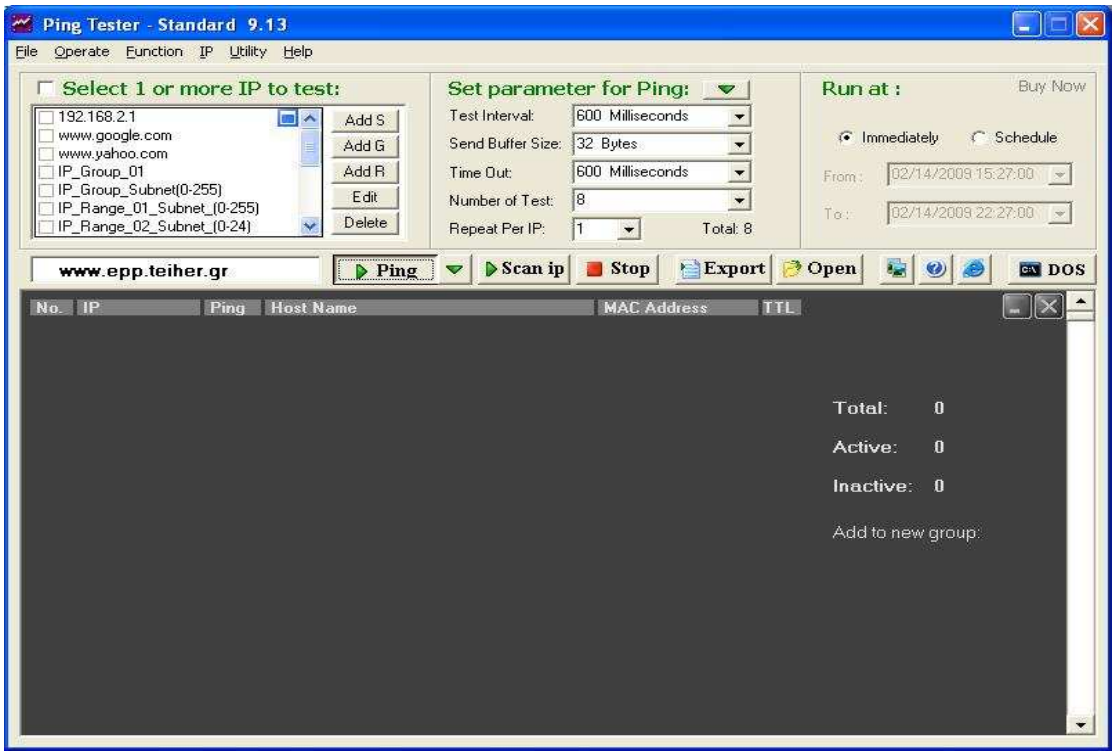
Ανοίγουμε λοιπόν το πρόγραμμα και συναντάμε το παρακάτω παράθυρο.

[1] http://el.wikipedia.org/wiki/Ping



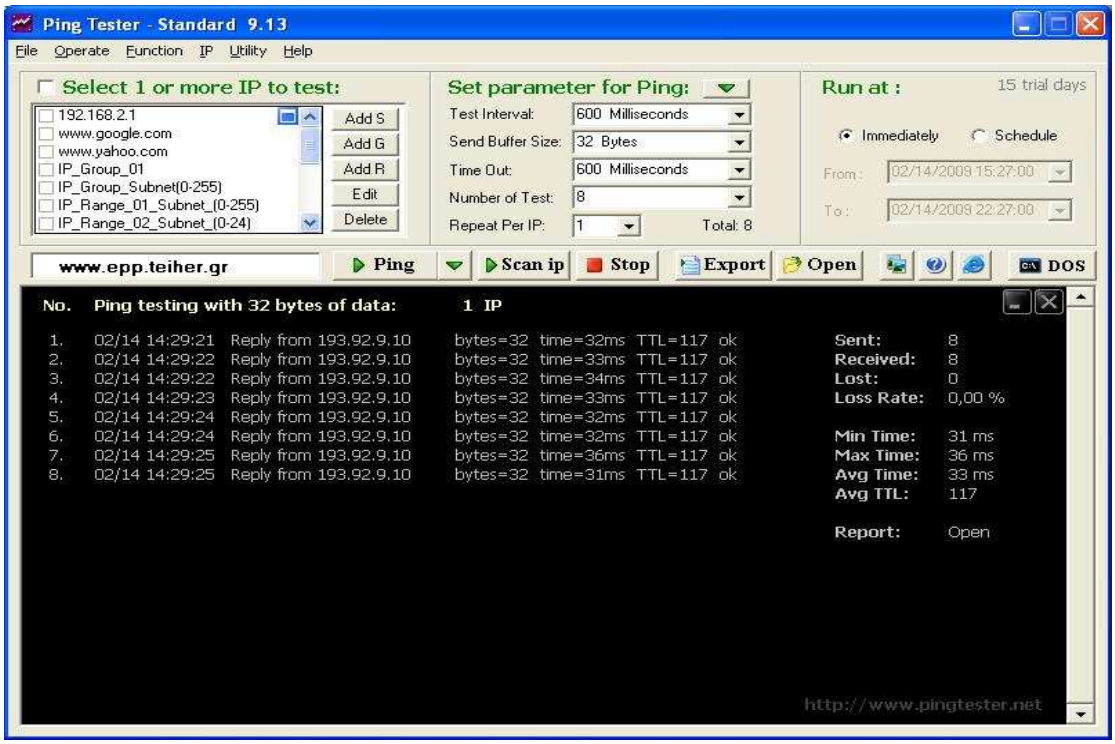
Εικόνα 29 Ping Tester : Απεικόνιση του προγράμματος Ping Tester

Θα πρέπει να πληκτρολογήσουμε www.epp.teiher.gr στο πεδίο κειμένου όπως ακολουθεί και αφού ρυθμίσουμε πρώτα κάποιες παραμέτρους όπως παρακάτω επιλέγουμε Ping.



Εικόνα 30 Ping Tester : Πληκτρολόγηση www.epp.teiher.gr και επιλογή μεθόδου

Έχουμε λοιπόν τα εξής αποτελέσματα:



Εικόνα 31 Ping Tester : Αποτελέσματα του Ping

- Το μέγεθος της απάντησης που αποστέλλεται.
- Το round trip-time που είναι ο χρόνος που απαιτείται μέχρι να σταλεί το πακέτο από τον Server και υπολογίζεται σε ms.
- Το TTL όπου είναι το χρονικό διάστημα ή ο αριθμός των κόμβων από τους οποίους πρέπει να περάσει κάποιο πακέτο πριν απορριφθεί από το δίκτυο. Οι κυριότερες χρήσεις του είναι στα πακέτα IP και στις καταχωρήσεις των διαφόρων DNS servers.
- Τον αριθμό των πακέτων που:
    - Εστάλησαν
    - Ελήφθησαν
    - Χάθηκαν

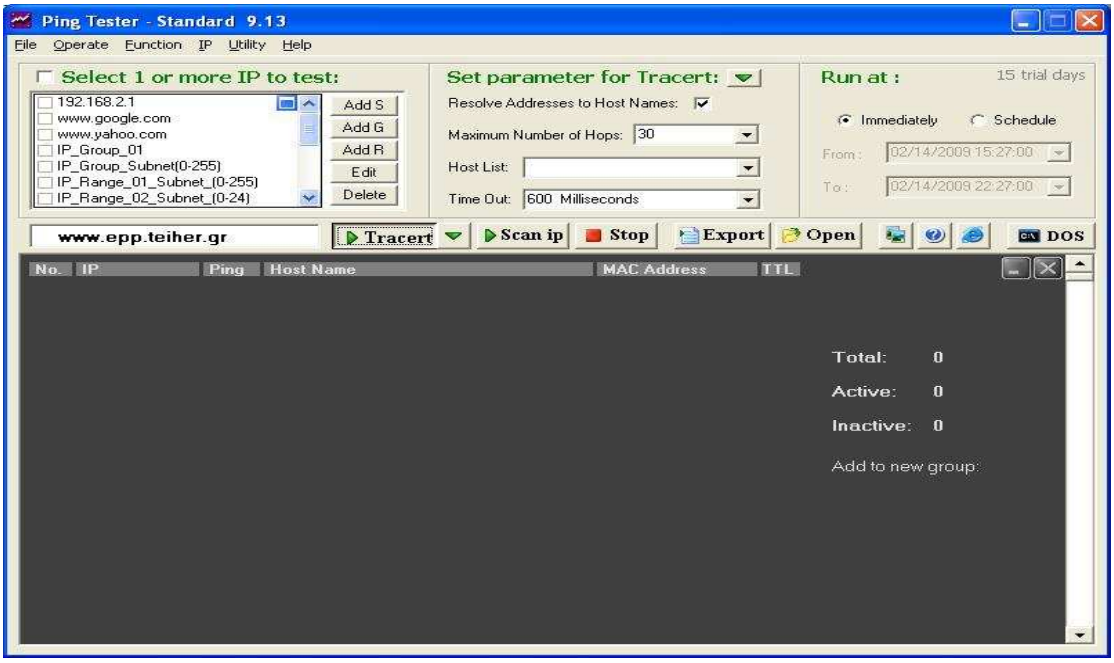
- Το ποσοστό της απώλειας των πακέτων.

- Τους χρόνους που απαιτήθηκαν μέχρι να σταλεί το πακέτο της απάντησης, συγκεκριμένα τον:
    - Ελάχιστο
    - Μέγιστο
    - Μέσο όρο

Σειρά έχει τώρα η μέθοδος tracert όπου μπορεί να παρουσιάσει την πορεία ενός πακέτου πληροφοριών που ξεκινάει από κάποιο υπολογιστή και καταλήγει σε ένα συγκεκριμένο προορισμό. Μπορεί να απαριθμήσει όλους τους δρομολογητές από όπου περνά έως ότου φτάσει στον προορισμό του, ή αποτύχει οπότε και

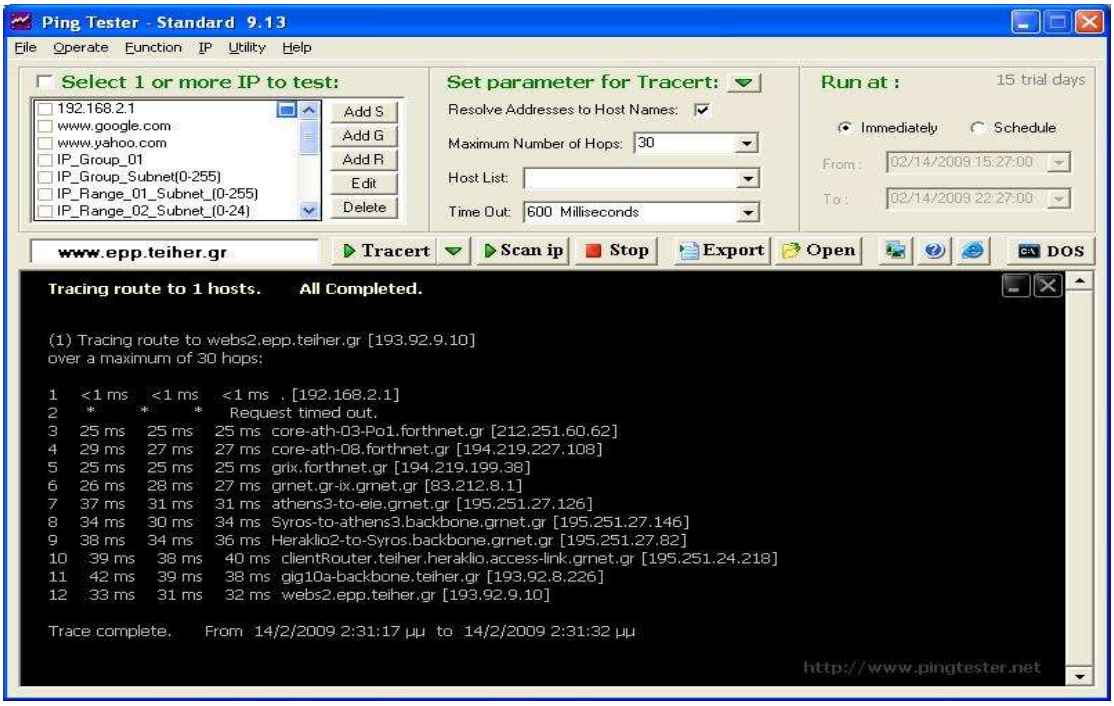
απορρίπτεται. Επιπλέον, εκφράζει τον χρόνο που χρειάζεται κάθε ' hop' από δρομολογητή σε δρομολογητή.

Συμπληρώνοντας ξανά στο πεδίο κειμένου http://www.epp.teiher.gr. Αφού ρυθμίσουμε πρώτα κάποιες παραμέτρους επιλέγουμε “Tracert” .



Εικόνα 32 Ping Tester : Πληκτρολόγηση www.epp.teiher.gr και επιλογή μεθόδου

Έχουμε λοιπόν τα παρακάτω αποτελέσματα:



Εικόνα 33 Ping Tester : Αποτελέσματα του Tracert

- Το σύνολο των κόμβων που προσπέλασε.
- Την πλήρη διαδρομή που ακολούθησε το πακέτο ώσπου να φτάσει στον προορισμό του.
- Το χρόνο της απάντησης από κάθε κόμβο για κάθε μια προσπάθεια από τις τρεις που έγιναν συνολικά.

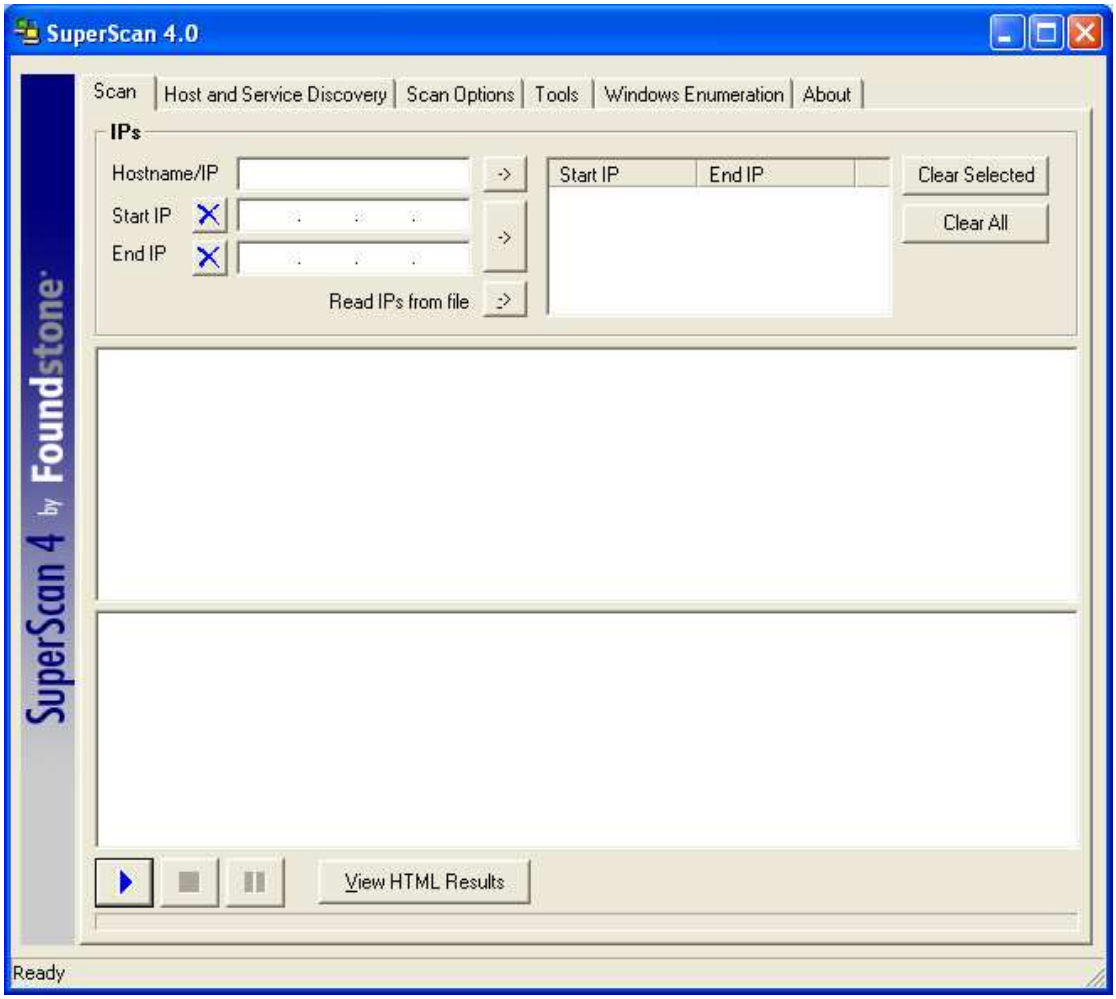
2.2.3 Enumerating ports

Superscan 4

Είναι κατασκευασμένο από την εταιρεία FoundStone και είναι ένας σαρωτής Θυρών.Ο κώδικας του δεν είναι "ανοικτός" στους χρήστες που το χρησιμοποιούν. Μπορεί να χρησιμοποιηθεί για σάρωση Θυρών όσο και για την διαδικασία με την οποία επιβεβαιώνεται η σύνδεση με έναν απομακρυσμένο υπολογιστή(Packet INternet Goper) και τέλος την αντιστοίχηση μιας διεύθυνσης IP η ιστοσελίδας σε ένα εξυπηρετητή.

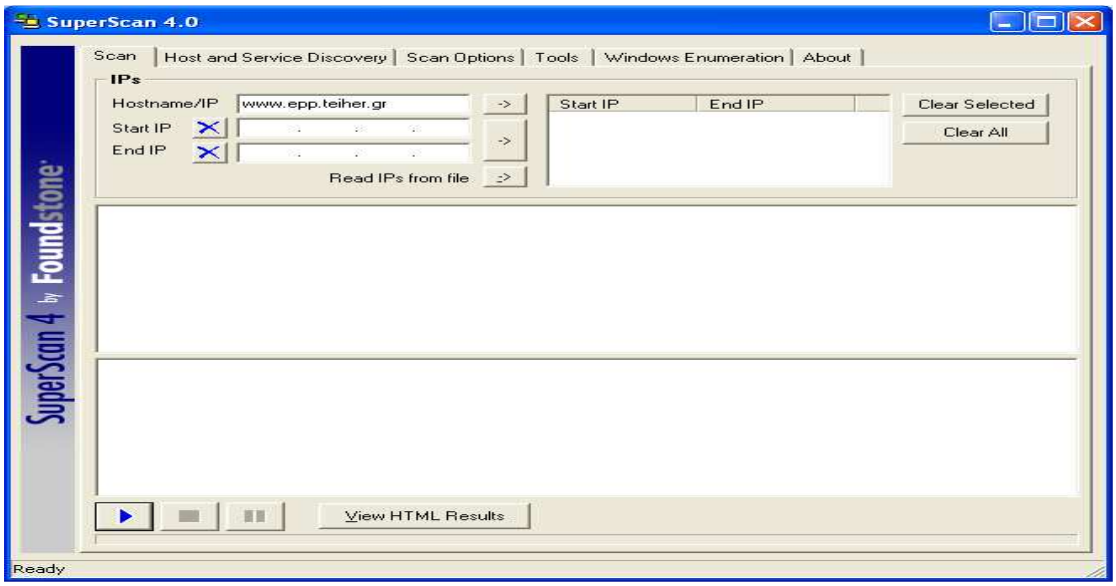
Download: http://www.foundstone.com/us/resources/proddesc/superscan4.htm

Ξεκινάμε με το άνοιγμα του προγράμματος.



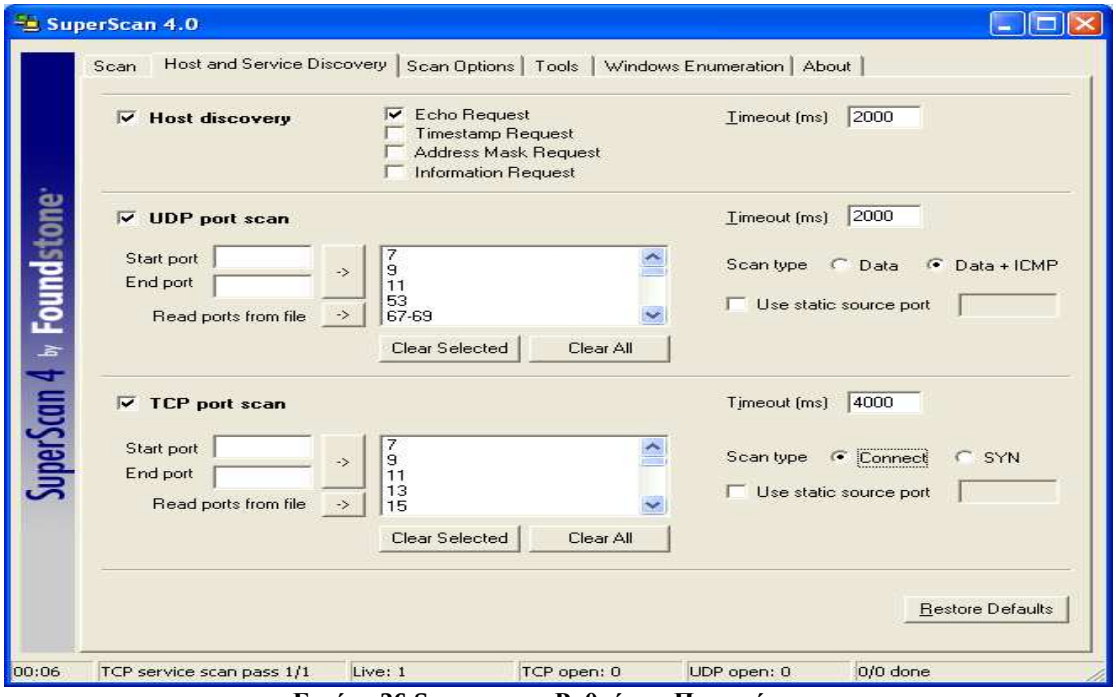
Εικόνα 34 Superscan : Απεικόνιση του προγράμματος

Στην καρτέλα Scan στο πεδίο κειμένου Hostname/IP θα πληκτρολογήσουμε τη σελίδα του τμήματος http://www.epp.teiher.gr όπως ακολουθεί:



Εικόνα 35 Superscan : Πληκτρολόγηση www.epp.teiher.gr

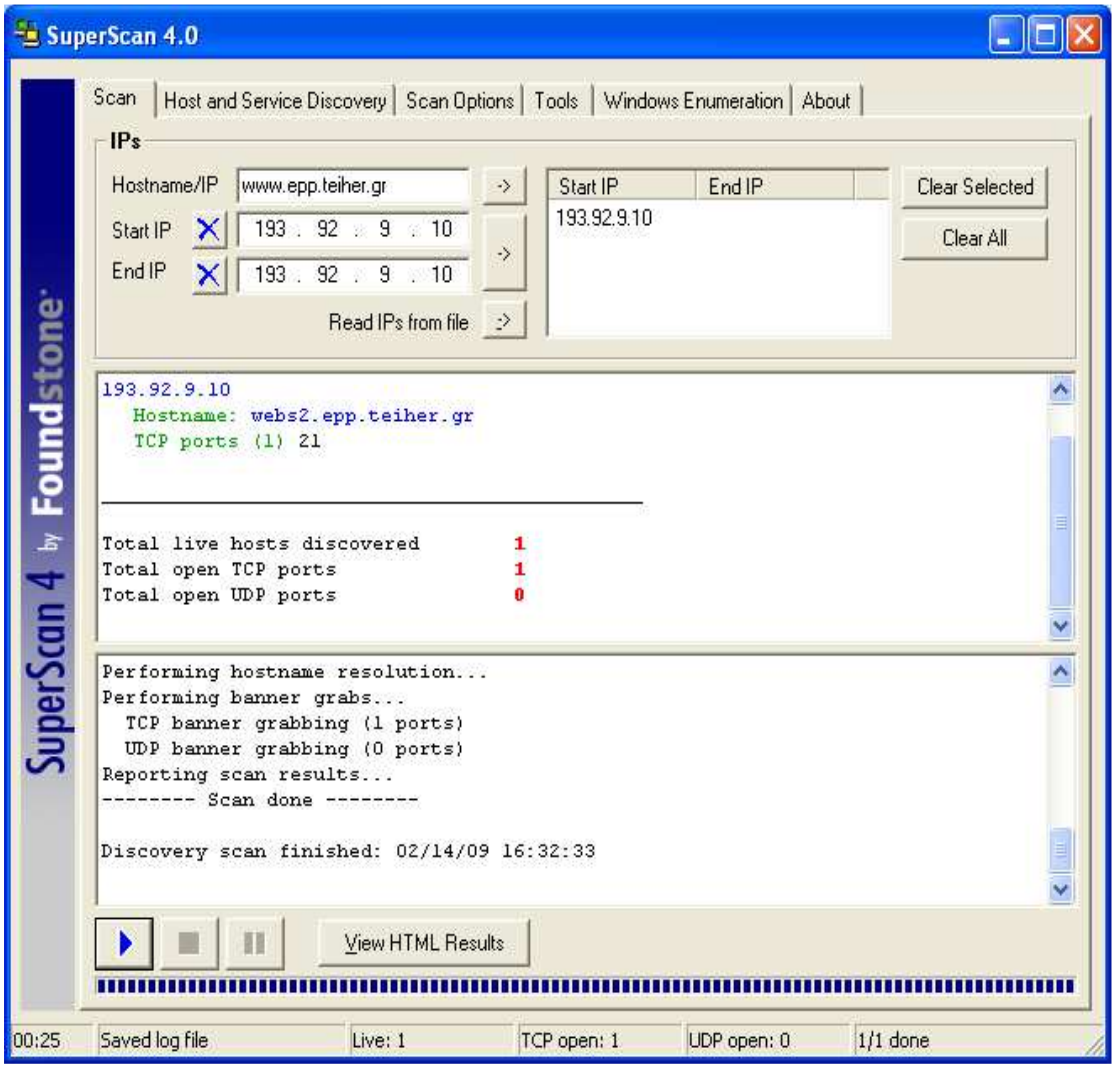
Στη συνέχεια στην καρτέλα Host and Service Discovery θα ρυθμίσουμε μερικές παραμέτρους όπως παρακάτω στην εικόνα ώστε να πάρουμε τα επιθυμητά αποτελέσματα. Ο λόγος που έγιναν αυτές οι ρυθμίσεις έγκειται στο ότι με την επιλογή DATA + ICMP στο UDP port scan στέλνει όχι μόνο UDP πακέτα στις πόρτες που επιδιώκουν απαντήσεις από υπηρεσίες που τρέχουν στις γνωστές πόρτες αλλά με το τα πακέτα ICMP στέλνει και άλλου είδους πακέτα που αν τα επεξεργαστούνε οι πόρτες τις βλέπει σαν ανοικτές. Μερικές φόρες μπορεί να δώσει και λανθασμένα αποτελέσματα για μερικές πόρτες. Στο TCP port scan σε επιλογή CONNECT κάνει την πλήρη ανάλυση των Θυρών.



Εικόνα 36 Superscan : Ρυθμίσεις Παραμέτρων

Στη συνέχεια επιστρέφουμε στην αρχική καρτέλα και επιλέγουμε “Start”.

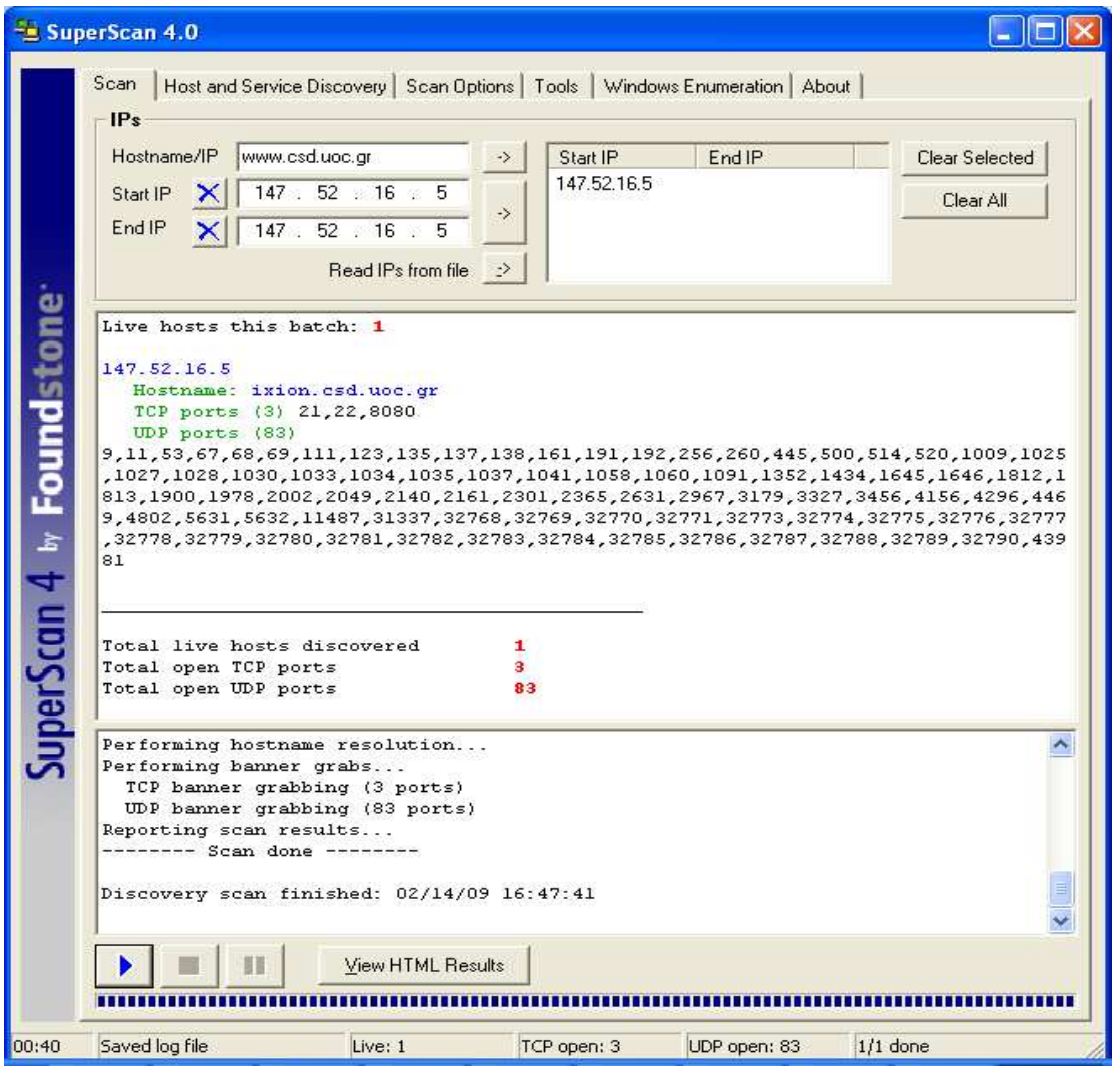
Παρουσιάζονται λοιπόν τα αποτελέσματα:



Εικόνα 37 Superscan : Παρουσίαση αποτελεσμάτων για epp

- Hostname: webs2.epp.teiher.gr
- IP Address: 193.92.9.10
- TCP open ports (1)
- UDP open ports (0)

Έπειτα θα αντικαταστήσουμε το Hostname/IP με http://www.csd.uoc.gr και θα αλλάξουμε τις ρυθμίσεις από τις default όπως προηγουμένως και θα επιλέξουμε Start όπως παρακάτω:



Εικόνα 38 Superscan : Εφαρμογή και παρουσίαση αποτελεσμάτων για csd

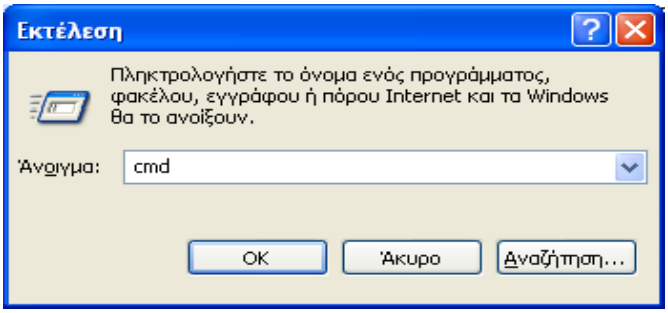
- Hostname: ixion.csd.uoc.gr
- IP Address:147.52.16.5
- TCP open ports (3)
- UDP open ports (83)

Scanline

Είναι ένα πρόγραμμα ανίχνευσης πορτών που τρέχει σε γραμμή εντολών σε όλες τις πλατφόρμες των Windows. Μπορεί να επιτύχει το ICMP "pinging",το ICMP TimeStamp scanning, μπορεί να δείξει το χρόνο των απαντήσεων του host και των αριθμό αυτών, το TCP scanning, το simple UDP scanning, τα banner grabbing και hostname resolving. Η ανίχνευση εκτελείται σε μια ιδιαίτερα γρήγορη παράλληλη μόδα χωρίς προσφυγή στη χρησιμοποίηση των πολλαπλάσιων νημάτων. Μπορεί να χειριστεί τους τεράστιους αριθμούς και τις σειρές των διευθύνσεων IP χωρίς κανένα πρόβλημα.

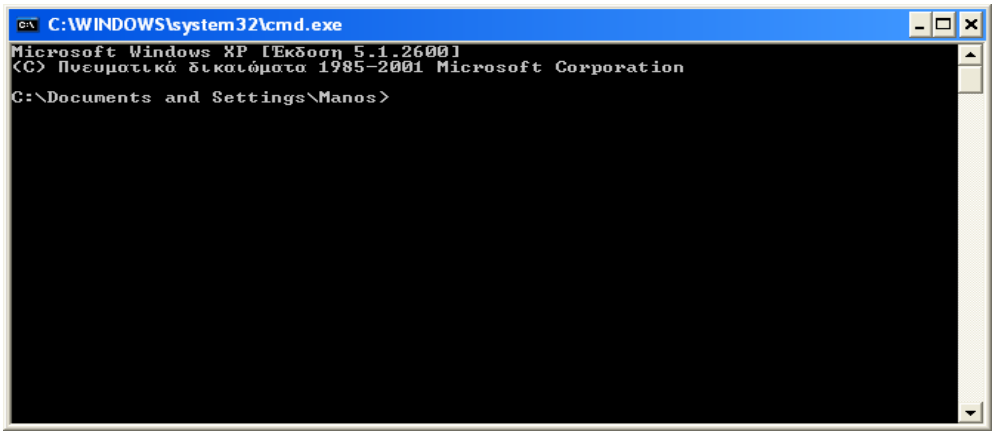
Download: http://www.scanwith.com/ScanLine_download.htm

Επειδή το πρόγραμμα τρέχει σε γραμμή εντολών MS-DOS ας δούμε πως θα ξεκινήσει. Επιλέγουμε έναρξη και μετά εκτέλεση. Έτσι έχουμε το παρακάτω παράθυρο όπου θα γράψουμε cmd για να μεταβούμε στο παράθυρο του MS-DOS.



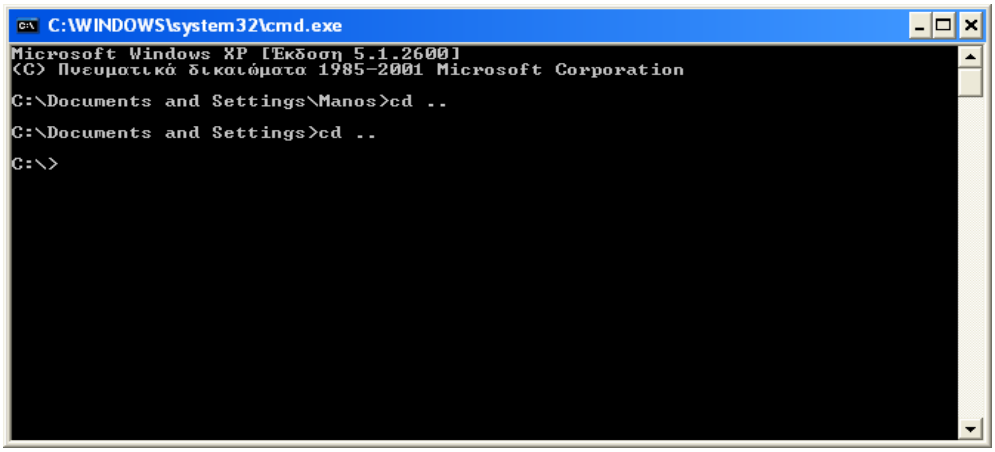
Εικόνα 39 Πληκτρολόγηση cmd

Έτσι έχουμε το παράθυρο του MS-DOS:



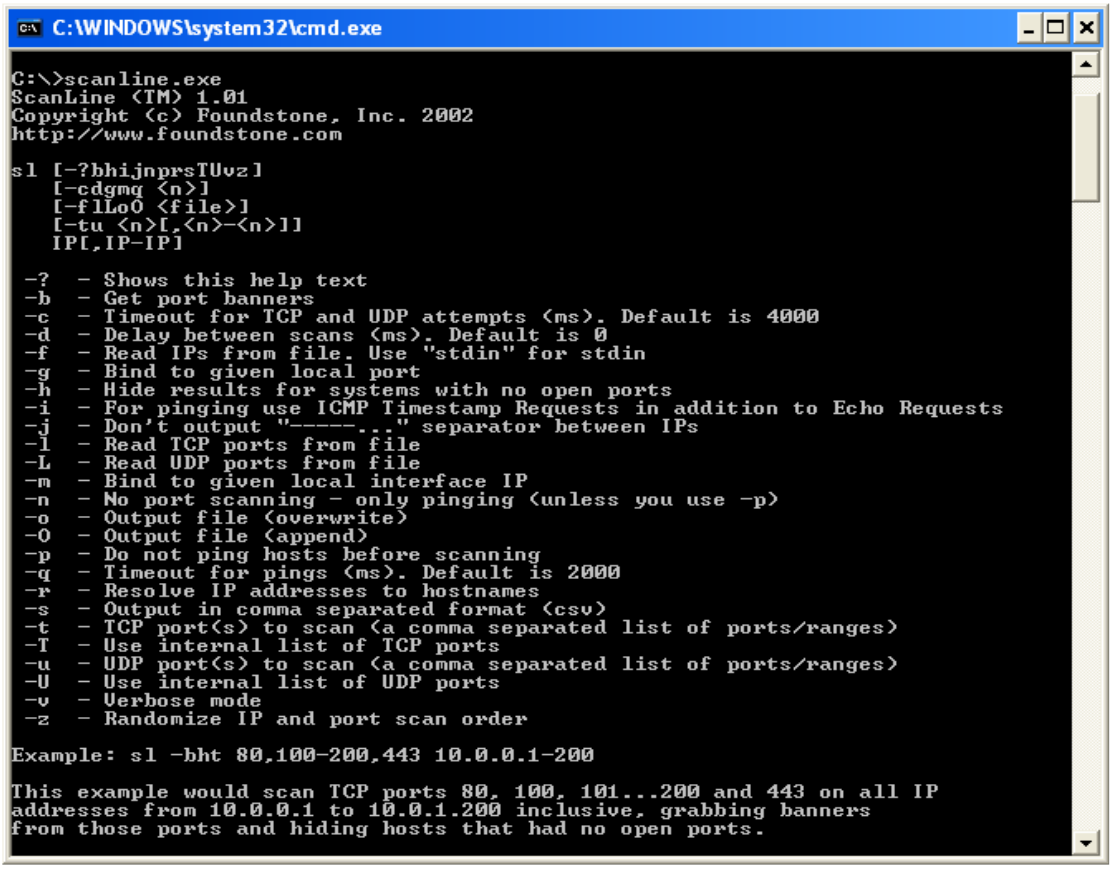
Εικόνα 40 Παράθυρο MS-DOS

Αν χρησιμοποιήσουμε τις εντολές και τις διαδρομές των φακέλων με τις σωστές ονομασίες θα είμαστε έτοιμοι να χρησιμοποιήσουμε το πρόγραμμα. Στην προκειμένη περίπτωση θα αλλάξουμε το directory ώστε να πάμε στο σημείο όπου έχουμε αποθηκεύσει το Scanline. Στην προκειμένη περίπτωση το έχουμε αποθηκεύσει στο C.



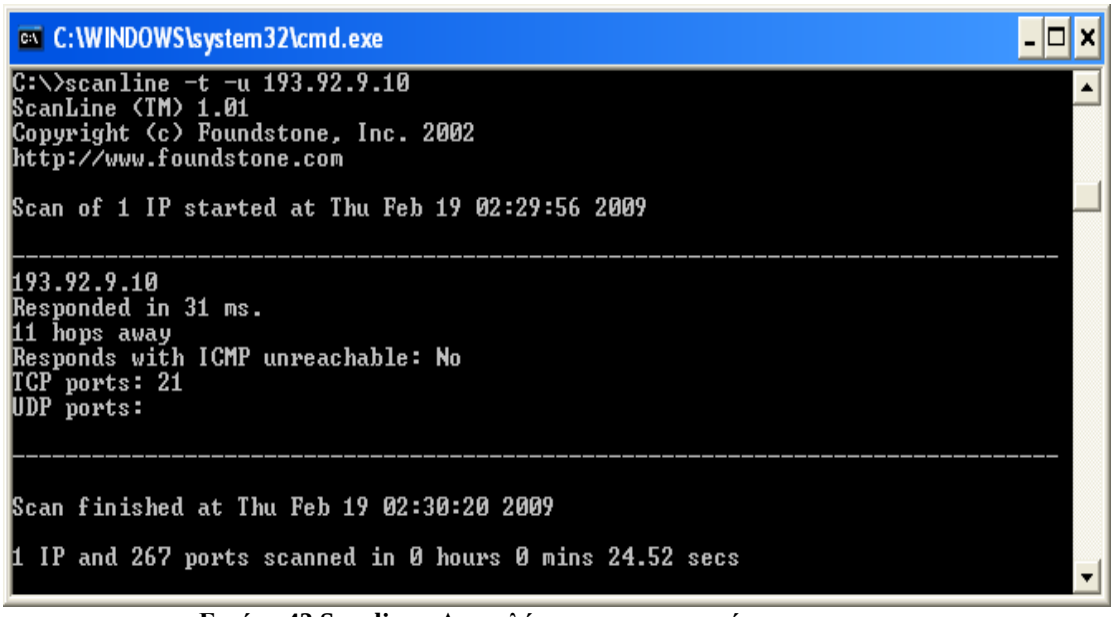
Εικόνα 41 Αλλαγή directory

Τρέχουμε λοιπόν το scanline.exe όπως παρακάτω και εμφανίζονται όλες οι τεχνικές που υποστηρίζει το συγκεκριμένο πρόγραμμα:



Εικόνα 42 Scanline : Εκτέλεση του αρχείου scanline.exe

Στη συνέχεια πληκτρολογούμε την εντολή “scanline –t –u 193.92.910” όπου ορίζουμε να εκτελεστούν οι τεχνικές TCP Scan και UDP Scan στην IP διεύθυνση του www.epp.teiher.gr. Η διαδικασία και τα αποτελέσματα παρουσιάζονται παρακάτω:

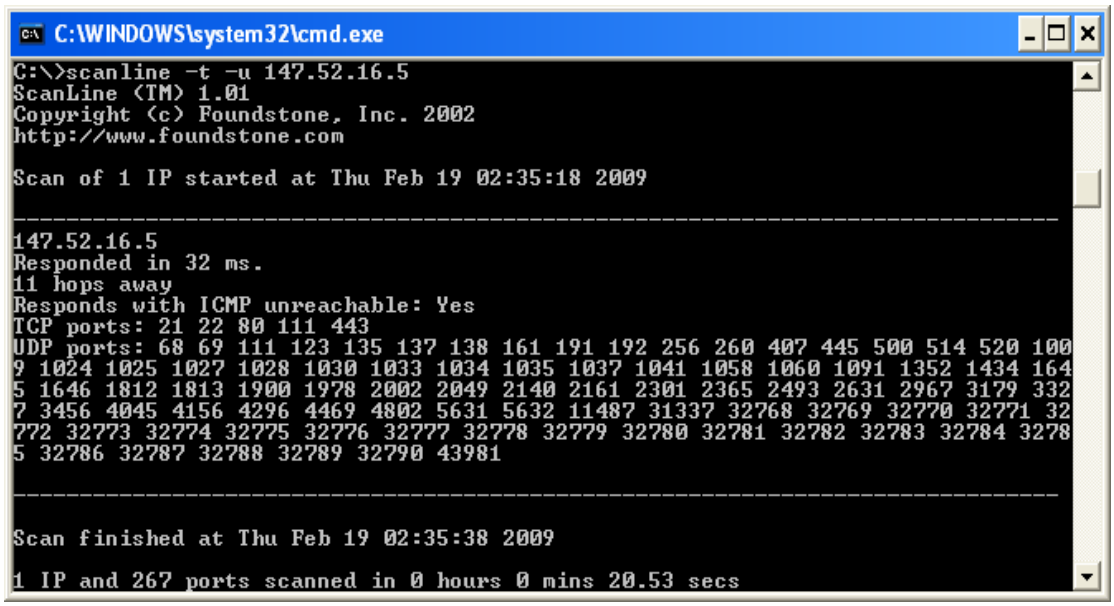


Εικόνα 43 Scanline : Αποτελέσματα του προγράμματος για epp

Έχουμε λοιπόν :

- Τον αριθμό των hops
- Τις ανοιχτές πόρτες TCP
- Τις ανοιχτές πόρτες UDP
- Το χρόνο που υλοποιήθηκε η ανίχνευση

Η διαδικασία θα εφαρμοστεί και για το http://www.csd.uoc.gr με τα ίδια βήματα και με την ίδια σειρά. Άρα έχουμε:



Εικόνα 44 Scanline : Αποτελέσματα του προγράμματος για csd

2.3 Services Identification

2.3.1 Περιγραφή

Αυτός είναι ένας ενεργός έλεγχος της εφαρμογής του listening πίσω από την υπηρεσία. Σε μερικές περιπτώσεις υπάρχουν περισσότερες από μία εφαρμογές πίσω από μια υπηρεσία όπου μία εφαρμογή λειτουργεί σαν listener και οι υπόλοιπες θεωρούνται συστατικά της εφαρμογής του listener. Ένα καλό παράδειγμα γι αυτό είναι η εφαρμογή PERL η οποία εγκαθίσταται για χρήση σε δικτυακές εφαρμογές. Σε αυτήν την περίπτωση η υπηρεσία του listening είναι το HTTP και το περιεχόμενο είναι το PERL.

Αναμενόμενα αποτελέσματα:

- Τύποι της υπηρεσίας
- Τύπος της εφαρμογής της υπηρεσίας και την έκδοση του Patch
- Χάρτης δικτύου

Βήματα που εφαρμόζονται για τον προσδιορισμό των υπηρεσιών:

- Αντιστοίχιση κάθε ανοιχτής πόρτας σε μια υπηρεσία και ένα πρωτόκολλο.
- Έλεγχος για τις τελευταίες ενημερώσεις που έγιναν στα Patch. (Δεν πραγματοποιήθηκε)
- Έλεγχος της εφαρμογής πίσω από την υπηρεσία και την έκδοση του Patch που χρησιμοποιεί banners ή fingerprinting. (Δεν πραγματοποιήθηκε)
- Έλεγχος της εφαρμογής στο σύστημα και την έκδοση του. (Δεν πραγματοποιήθηκε)
- Προσδιορισμός και έλεγχος της υπηρεσίας remapping ή του επαναπροσανατολισμού του συστήματος. (Δεν πραγματοποιήθηκε)
- Έλεγχος των περιεχομένων της υπηρεσίας του listening. (Δεν πραγματοποιήθηκε)
- Χρήση των UDP-based υπηρεσιών και Trojan requests σε όλα τα συστήματα του δικτύου. (Δεν πραγματοποιήθηκε)

Πληροφορίες:

- *Για την απαρίθμηση των υπηρεσιών χρησιμοποιήσαμε τα πρόγραμμα Nmap, και οι διαδικασία περιγράφεται στην ενότητα 1.3.2*

2.3.2 Services Identification

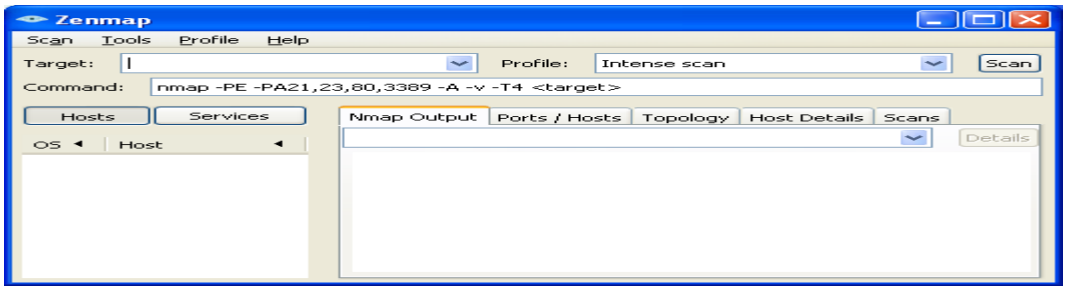
Network Mapper

Είναι ένα «πολυεργαλείο», ανοικτού λογισμικού, το οποίο μπορεί να «χαρτογραφήσει», ένα εύρος διευθύνσεων ή ένα υποδίκτυο. Ακόμα μπορεί να αναζητήσει πόσα μηχανήματα υπάρχουν και ποίες θύρες (ports) είναι «ενεργές» σε κάθε μηχάνημα, δηλαδή τι υπηρεσίες υπάρχουν, όπως επίσης και να αναγνωρίσει το λειτουργικό σύστημα του κάθε μηχανήματος.Αυτή τη στιγμή το nmap διατίθεται σε εκδώσεις συμβατές με τα πιο διαδεδομένα λειτουργικά συστήματα όπως: Linux, FreeBSD, OpenBSD, NetBSD, Solaris, IRIX, HP-UX, Sun OS, Mac OS X, Amiga και Microsoft Windows.

Download: http://nmap.org/download.html

Ξεκινάμε λοιπόν το τεστ για το τμήμα της Εφαρμοσμένης Πληροφορικής και Πολυμέσων του ΤΕΙ Κρήτης.

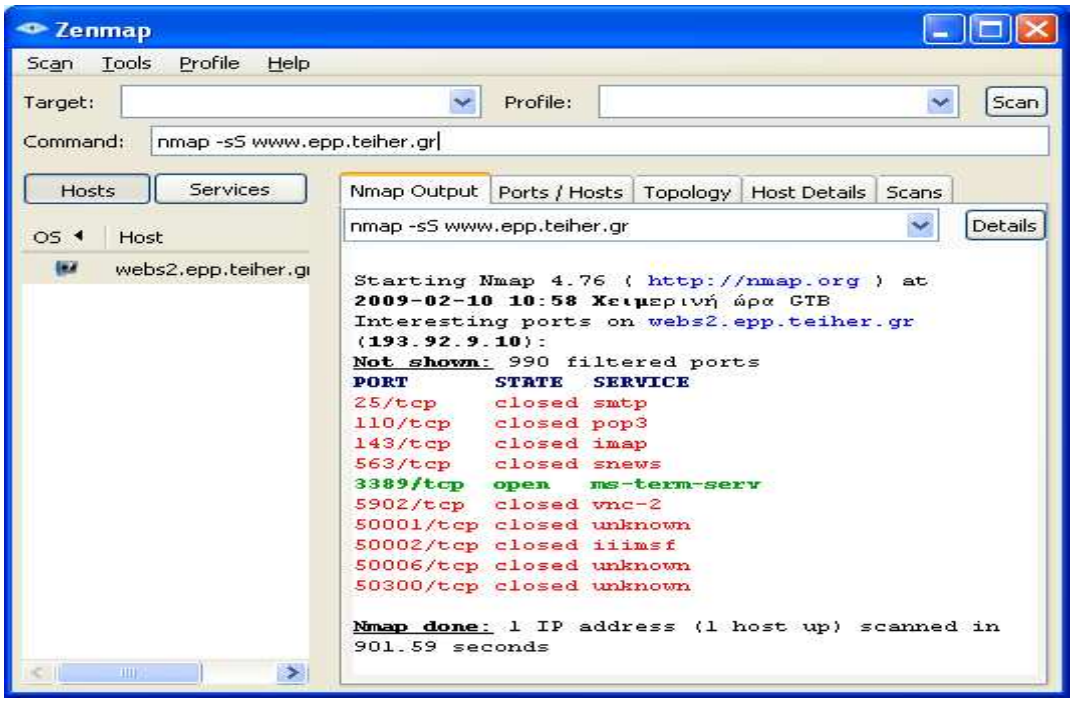
Στη συνέχεια ανοίγουμε το πρόγραμμα:



Εικόνα 45 Nmap : Απεικόνιση του προγράμματος Nmap

Εφόσον θέλουμε να εφαρμόσουμε την μέθοδο **TCP SYN Scan**[2] στο πεδίο κειμένου Command θα πληκτρολογήσουμε την εντολή όπως ακολουθεί**.** Πατώντας "Scan" θα ξεκινήσει η διαδικασία:

- Με την παράμετρο –sS το nmap στέλνει αρχικά ένα SYN στο απομακρυσμένο μηχάνημα και περιμένει από αυτό ένα SYN-ACK. Αν το απομακρυσμένο μηχάνημα απαντήσει με SYN-ACK τότε η συγκεκριμένη πόρτα είναι ενεργή. Το nmap αμέσως στέλνει ένα πακέτο RESET πριν ολοκληρωθεί το TCP three-way handshake. Αν αρχικά το nmap δεν λάβει τίποτα από το απομακρυσμένο μηχάνημα ή λάβει RESET τότε η πόρτα δεν είναι ενεργή.



Εικόνα 46 Εφαρμογή της μεθόδου TCP SYN Scan για epp

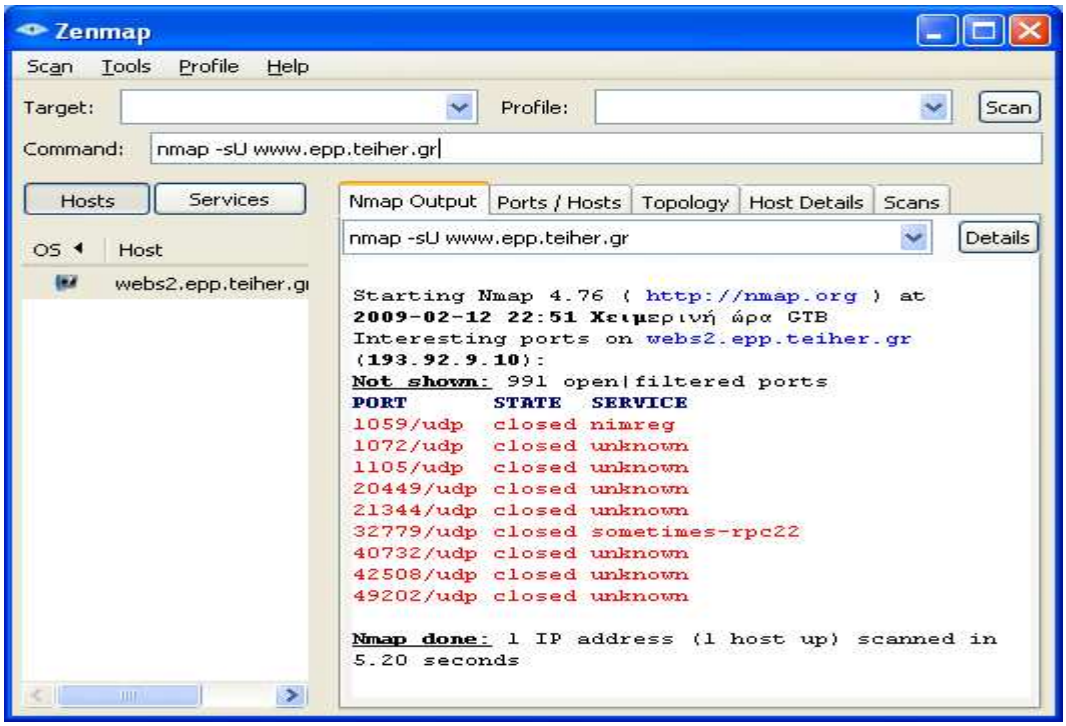
[2] http://en.wikipedia.org/wiki/Port_scanning#TCP.2FIP_basic_knowledge

Μετά την ολοκλήρωση της διαδικασίας της επίθεσης θα λάβουμε τα αποτελέσματα που παρουσιάζονται στην παραπάνω εικόνα. Πληροφορούμαστε λοιπόν για:

- Τις φιλτραρισμένες πόρτες.
- Την πόρτα στην οποία έγινε η επίθεση.
- Την κατάσταση της όπου μπορεί να είναι
    - Open (Όταν σε εκείνη την πόρτα τρέχει μια διαδικασία που να ακούει τις συνδέσεις στη συγκεκριμένη πόρτα).
    - Closed (Όταν σε εκείνη την πόρτα δεν τρέχει κάποια διαδικασία που να ακούει τις συνδέσεις στη συγκεκριμένη πόρτα).
    - Filtered (Όταν το firewall μπλοκάρει την επίθεση και δεν ξέρουμε αν εκείνη η πόρτα είναι ανοιχτή ή κλειστή).

Στη συνέχεια θέλουμε να εφαρμόσουμε τη μέθοδο **UDP Scan**[3] οπότε στο πεδίο κειμένου Command αυτή τη φορά θα πληκτρολογήσουμε μια άλλη εντολή όπως παρακάτω και πατώντας "Scan" θα ξεκινήσει η διαδικασία της επίθεσης:

- Με την παράμετρο –sU το nmap αποστέλλει UDP πακέτα σε κάθε μηχάνημα που θέλουμε να ανιχνεύσουμε αν υπάρχουν ενεργές UDP υπηρεσίες. Αν ο παραλήπτης επιστρέψει μήνυμα ICMP Port Unreachable, το nmap θα θεωρήσει πως η θύρα είναι ανενεργή. Διαφορετικά θα το θεωρήσει ενεργό.
  Σε αυτή την τεχνική, η πιθανότητα για λανθασμένες εκτιμήσεις είναι μεγάλη. Ακόμα, δεν μπορούμε να έχουμε πληροφορίες για την έκδοση της υπηρεσίας.



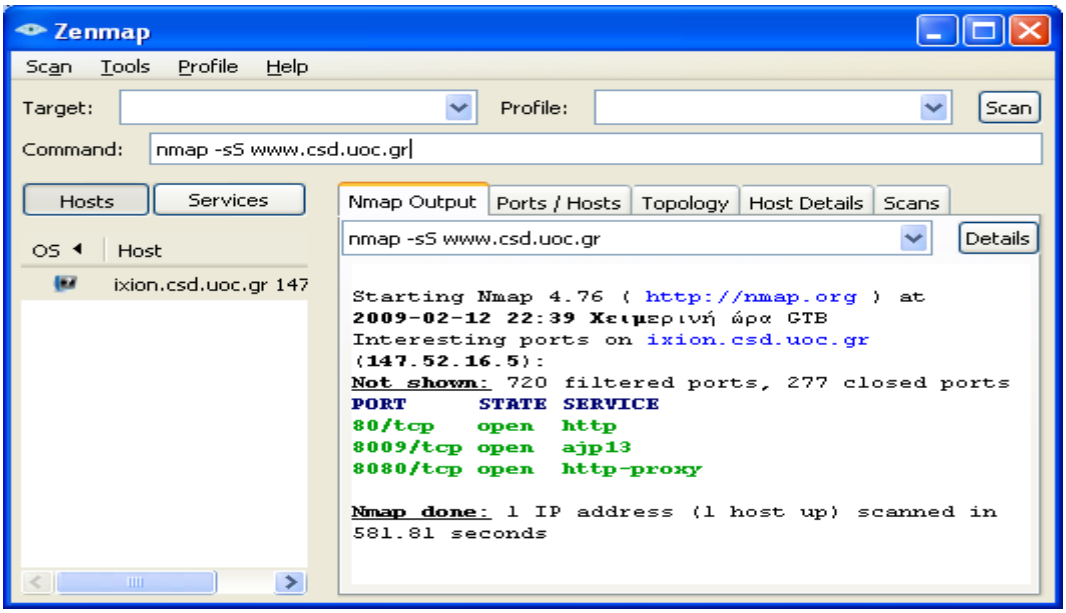
Εικόνα 47 Nmap : Εφαρμογή της μεθόδου UDP Scan για epp

Αφού ολοκληρωθεί και αυτή η διαδικασία της επίθεσης συλλέγουμε πάλι τα αποτελέσματα που αναφέρονται παραπάνω.

[3] http://en.wikipedia.org/wiki/Port_scanning#TCP.2FIP_basic_knowledge

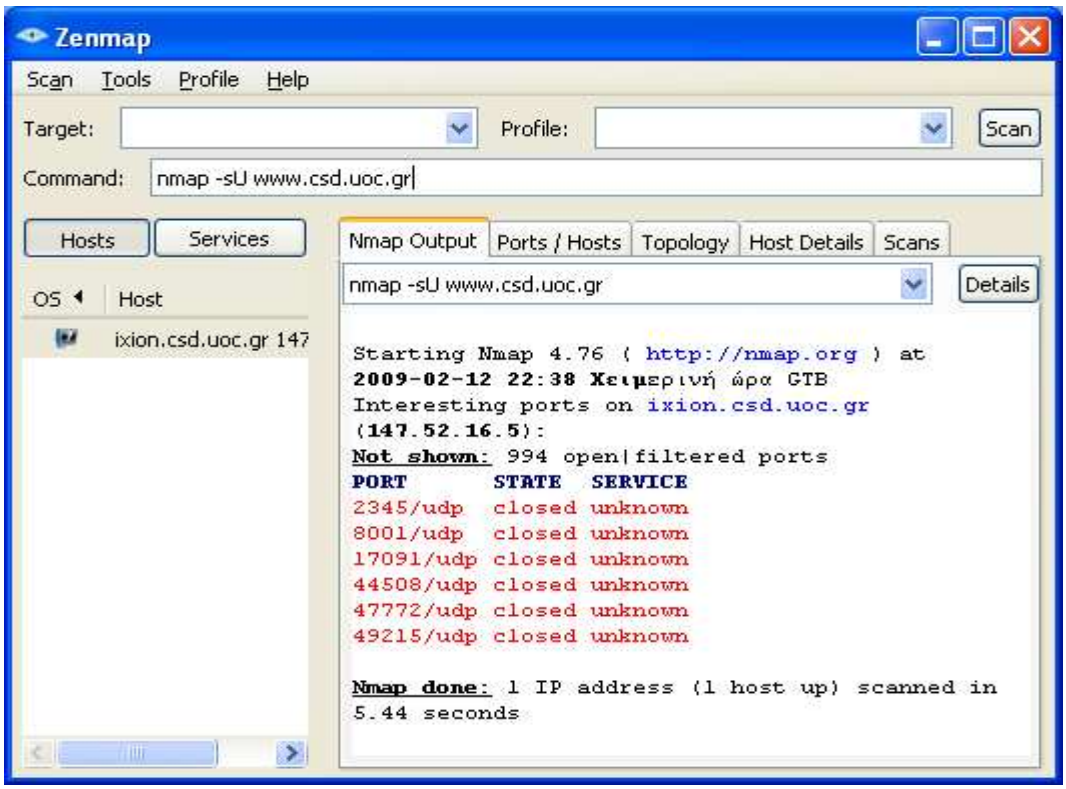
Σειρά έχει τώρα το τμήμα της Επιστήμης των Υπολογιστών του Πανεπιστημίου Κρήτης. Οι επιθέσεις θα εκτελεστούν εφαρμόζοντας τα ίδια βήματα και με την ίδια σειρά. Έχουμε λοιπόν:

- TCP SYN Scan



Εικόνα 48 Nmap : Εφαρμογή της μεθόδου TCP SYN Scan για epp

- UDP Scan



Εικόνα 49 Nmap : Εφαρμογή της μεθόδου UDP Scan για csd

2.4 System Identification

2.4.1 Περιγραφή

Το fingerprinting σε ένα συστήμα είναι ένας ενεργός έλεγχος για απαντήσεις οι οποίες μπορούν να προσδιορίσουν το λειτουργικό του σύστημα και την έκδοση του.

Αναμενόμενα αποτελέσματα:

- Τύπος του λειτουργικού συστήματος
- Έκδοση του Patch
- Τύπος του συστήματος
- Απαρίθμηση του συστήματος
- Εσωτερική διευθυνσιοδότηση των δικτύων του συστήματος

Βήματα που εφαρμόζονται για τον προσδιορισμό του συστήματος:

- Εξέταση των απαντήσεων του συστήματος για να καθοριστεί ο τύπος του λειτουργικού συστήματος και η έκδοση του patch.
- Έλεγχος του προβλεπόμενου αριθμού ακολουθίας του TCP για κάθε “ζωντανό” χρήστη στο δίκτυο. (Δεν πραγματοποιήθηκε)
- Αναζήτηση “job postings” για πληροφορίες του server και της εφαρμογής του στόχου. (Δεν πραγματοποιήθηκε)
- Αναζήτηση “tech bulletin boards” και “newsgroups” του server και της εφαρμογής του στόχου. (Δεν πραγματοποιήθηκε)
- Αντιστοίχιση των πληροφοριών που συλλέχθηκαν με τις απαντήσεις του συστήματος για πιο ακριβή αποτελέσματα. (Δεν πραγματοποιήθηκε)

Πληροφορίες:

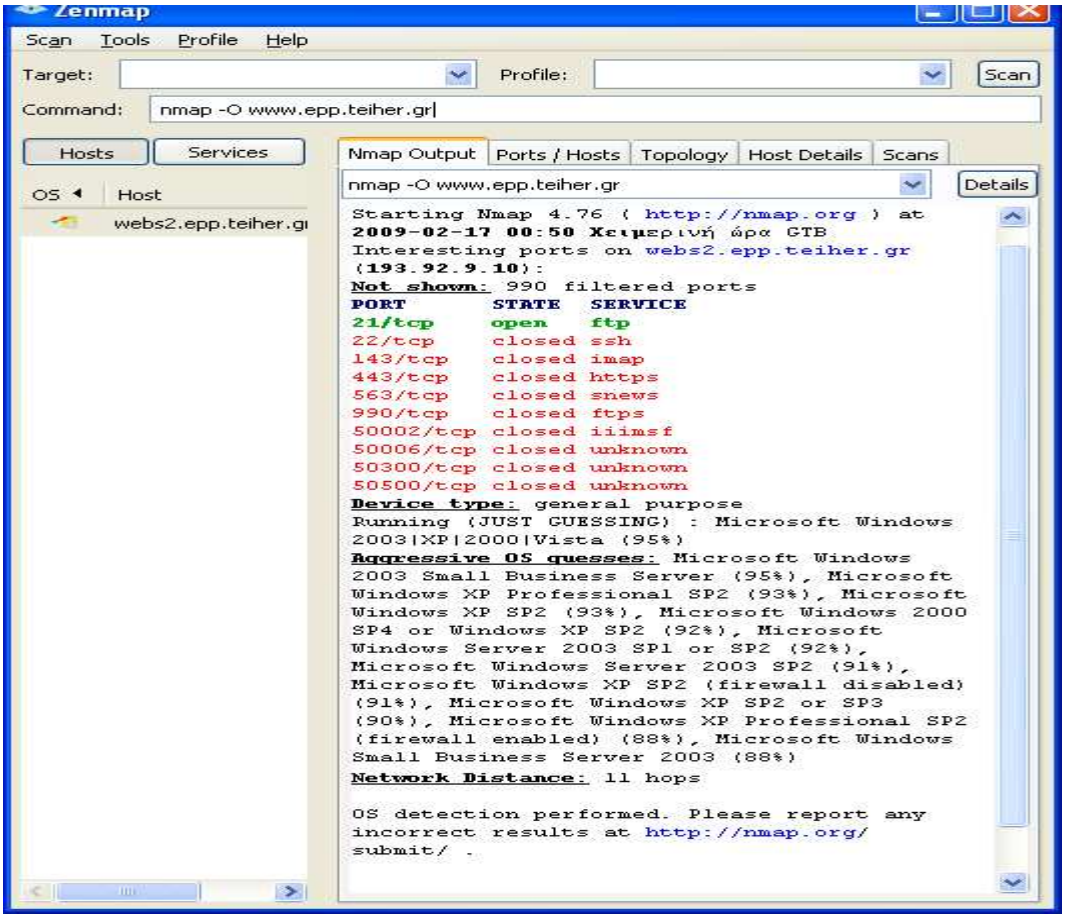
- *Για την ανίχνευση του λειτουργικού συστήματος χρησιμοποιήθηκε το πρόγραμμα Nmap και η διαδικασία περιγράφεται στην ενότητα 1.4.2*

2.4.2 Operating System Identification

Ανοίγουμε πάλι το πρόγραμμα nmap για να αρχίσουμε την διαδικασία εντοπισμού του λειτουργικού συστήματος στον Server του www.epp.teiher.gr .

Όπως βλέπουμε παρακάτω παρουσιάζεται η εντολή που πρέπει να πληκτρολογήσουμε ώστε να ξεκινήσει η διαδικασία. Μετά την πληκτρολόγηση της εντολής επιλέγουμε “Start” .

- Με την παράμετρο -O ενεργοποιούνται οι τεχνικές ανίχνευσης του λειτουργικού συστήματος.



Εικόνα 50 Nmap: Ενεργοποίηση τεχνικών ανίχνευσης για epp

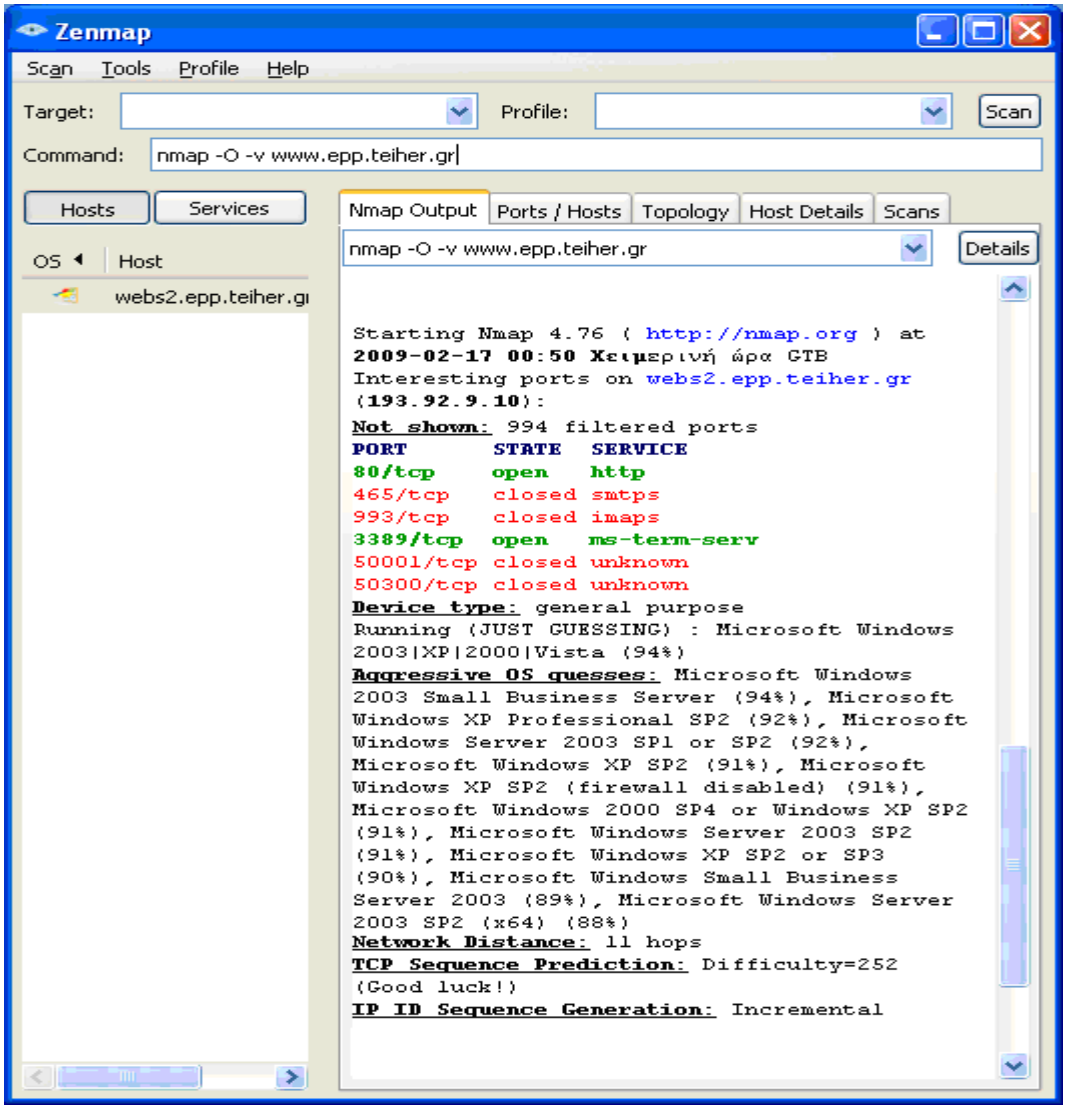
Παραπάνω παρουσιάζονται:

- οι πόρτες
- η κατάστασή τους
- οι υπηρεσίες που υποστηρίζονται από αυτές
- Device type: of the host you scanned to get this fingerprint (if known). If the device type doesn't appear in the dropdown list, or you feel a special device type is necessary, please put the information in the Notes field.
- Aggressive OS guesses: This option can make certain scans (especially SYN scans against heavily filtered hosts) much faster. It is recommended for impatient folks with a fast net connection. Insane is only suitable for very fast networks or where you don't mind losing some information. It times out hosts in 15 minutes and won't wait more than 0.3 seconds for individual probes. It does allow for very quick network sweeps though.
- Distance: The node places its distance in number of hops to the destination of the request in the hop count field of intermediate reply before broadcasting the message.

Για την ανάκτηση περισσοτέρων πληροφοριών μπορούμε να χρησιμοποιήσουμε μια άλλη εντολή όπως ακολουθεί.

- Με την παράμετρο -v, έχουμε την αναλυτική παρουσίαση των αποτελεσμάτων, την ανάκτηση χρήσιμων πληροφοριών που μπορούν να

φανούν χρήσιμες για να εντοπιστούν απομακρυσμένα μηχανήματα που μπορούν να χρησιμοποιηθούν στα **Idle Scans**[4].



Εικόνα 51 Nmap: Αναλυτική παρουσίαση των αποτελεσμάτων για epp

- TCP Sequence Prediction: is an attempt to predict the sequence number used to identify the packets in a TCP connection, which can be used to counterfeit packets. The attacker hopes to correctly guess the sequence number to be used by the sending host. If they can do this, they will be able to send counterfeit packets to the receiving host which will seem to it to originate from the sending host, even though the counterfeit packets may in fact originate from some third host controlled by the attacker. If an attacker can cause delivery of counterfeit packets of this sort, he or she may be able to cause various sorts of mischief, including the injection into an existing TCP connection of data of the attacker's choosing, and the premature closure of an existing TCP connection by the injection of counterfeit packets with the FIN bit set.Theoretically, other information such as timing differences or information from lower protocol layers could allow the receiving host to distinguish

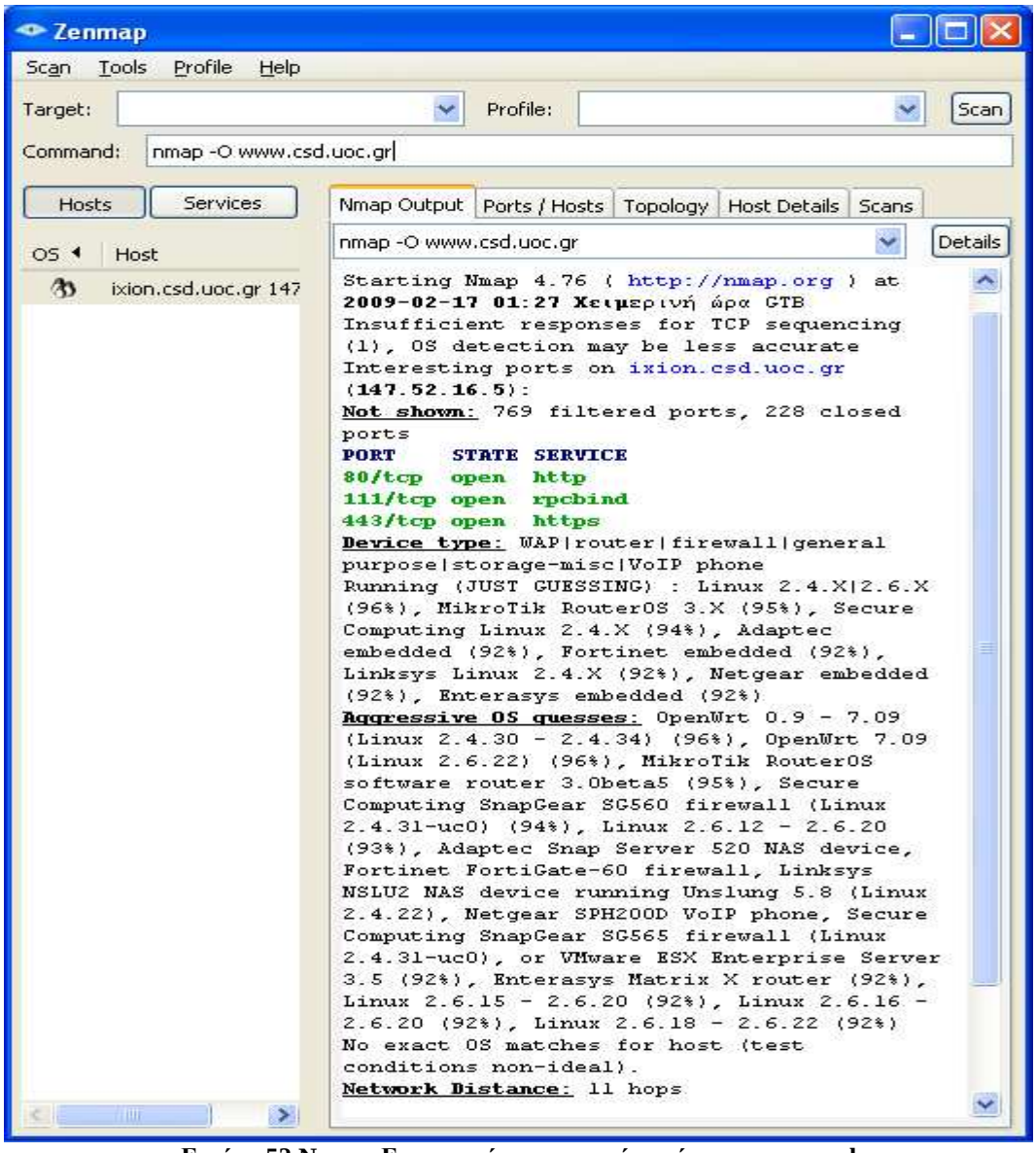
[4] http://en.wikipedia.org/wiki/Idle_scan

authentic TCP packets from the sending host and counterfeit TCP packets with the correct sequence number sent by the attacker. If such other information is available to the receiving host, if the attacker cannot also fake that other information, and if the receiving host gathers and uses the information correctly, then the receiving host may be fairly immune to TCP sequence prediction attacks. Usually this is not the case, so the TCP sequence number is the primary means of protection of TCP traffic against these types of attack.

- IP ID Sequence Generation: IPID classes Nmap understands include "incremental" (most machines), "duplicated IPID" (mostly stupid devices like printers), "Broken little-endian incremental" (Windows), "Randomized" (OpenBSD), and "Random positive increments

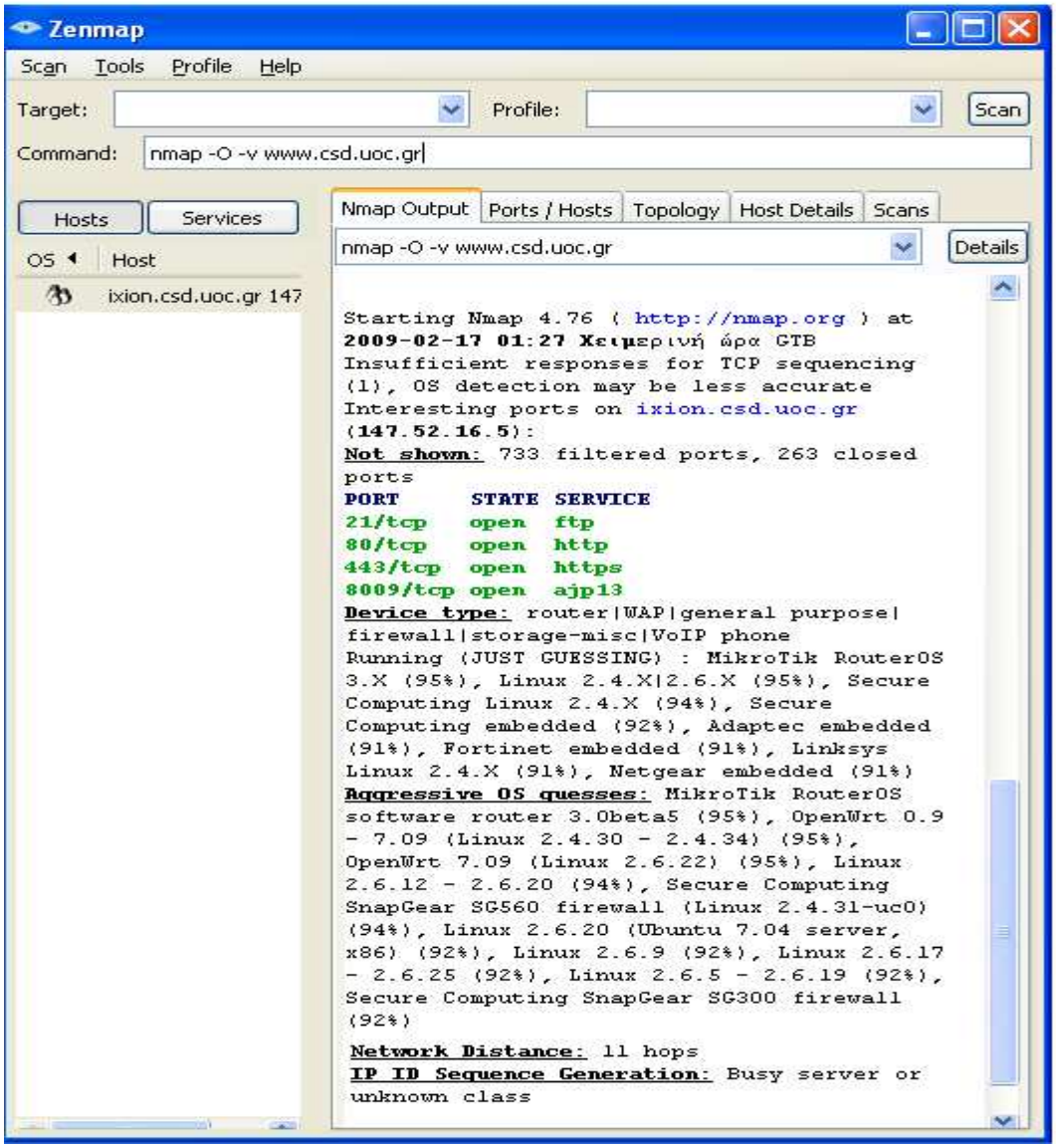
Ακολουθεί η ίδια διαδικασία αυτή τη φορά για το http://www.csd.uoc.gr.

- Παράμετρος: -O



Εικόνα 52 Nmap: Ενεργοποίηση τεχνικών ανίχνευσης για csd

- Παράμετρος: -O –v



Εικόνα 53 Nmap: Αναλυτική παρουσίαση των αποτελεσμάτων για csd

2.5 Vulnerability Research and Verification

2.5.1 Περιγραφή

Σκοπός αυτής της ενότητας είναι ο προσδιορισμός, η κατανόηση και η επαλήθευση των αδυναμιών, των misconfigurations και των vulnerabilities σε έναν οικοδεσπότη ή σε ένα δίκτυο.

Η έρευνα που περιλαμβάνεται στην εύρεση των ευπαθειών είναι απαραίτητα ενεργή μέχρι την παράδοση της έκθεσης. Αυτό περιλαμβάνει την έρευνα online βάσεων δεδομένων και των καταλόγων αλληλογραφίας συγκεκριμένα για τα συστήματα και το δίκτυο που εξετάζονται. Μην περιορίστείτε στον Ιστό, εξετάστε χρησιμοποιώντας IRC, ομάδες πληροφόρησης, και υπόγειες περιοχές FTP.

Η δοκιμή για τις ευπάθειες που χρησιμοποιούν τα αυτοματοποιημένα εργαλεία είναι ένας ικανός τρόπος να καθοριστούν οι υπάρχουσες τρύπες και το επίπεδο του Patch των συστημάτων. Αν και πολλοί αυτοματοποιημένοι ανιχνευτές είναι αυτήν την περίοδο στην αγορά και υπόγεια, είναι σημαντικό για τον ελεγκτή να προσδιορίσει και να ενσωματώσει τα ισχύων underground scripts / exploits σε αυτήν την δοκιμή. Εντούτοις, η μη-αυτοματοποιημένη επαλήθευση είναι απαραίτητη για την εξάλειψη των ψεύτικων θετικών, για την επέκταση του πεδίου χάραξης, και της ανακάλυψη της ροής στοιχείων μέσα και έξω από το δίκτυο. Η μη-αυτοματοποιημένη δοκιμή αναφέρεται σε ένα πρόσωπο ή τα πρόσωπα που χρησιμοποιούν τη δημιουργικότητα, την εμπειρία και την ευστροφία στον υπολογιστή για να εξετάσει το δίκτυο στόχων.

Αναμενόμενα αποτελέσματα:

- Τύπος της εφαρμογής ή της υπηρεσίας
- Εκδόσεις του Patch για τα συστήματα και τις εφαρμογές
- Λίστα από πιθανές αρνήσεις των ευπαθειών της υπηρεσίας
- Λίστα από περιοχές που ελέγχονται με αόρατη ή ορατή πρόσβαση
- Λίστα από τις πραγματικές ευπάθειες μείων τις ψεύτικες θετικές
- Λίστα των Internal ή των DMZ συστημάτων
- Λίστα του mail, του server και άλλων γνωστών συμβάσεων
- Χάρτης δικτύου

Βήματα που εφαρμόζονται για τον προσδιορισμό των ευπαθειών του συστήματος:

- Προσθήκη των τωρινών διάσημων scanner, hacking tools και χρήση αυτών.
- Εκτίμηση του στόχου εναντίων των τωρινών διάσημων σαρωτών.
- Προσπάθεια καθορισμού της ευπάθειας από τον τύπο των συστημάτων και της εφαρμογής.
- Προσπάθεια αντιστοίχισης των ευπαθειών με τις υπηρεσίες. (Δεν πραγματοποιήθηκε)
- Προσπάθεια καθορισμού του τύπου και της υπηρεσίας της εφαρμογής από την ευπάθεια. (Δεν πραγματοποιήθηκε)
- Εκτέλεση δοκιμών με τουλάχιστον δύο αυτοματοποιημένους σαρωτές ευπάθειας.
- Προσδιορισμός όλων των ευπαθειών σύμφωνα με τις εφαρμογές. (Δεν πραγματοποιήθηκε)

- Προσδιορισμός όλων των ευπαθειών σύμφωνα με τα λειτουργικά συστήματα. (Δεν πραγματοποιήθηκε)
- Προσδιορίστε όλων των ευπαθειών παρόμοια ή όπως τα συστήματα που μπορούν επίσης να έχουν επιπτώσεις στα συστήματα στόχων. (Δεν πραγματοποιήθηκε)
- Εξέταση όλων των ευπαθειών που βρίσκονται στη διάρκεια της ερευνητικής φάσης άθλου για ψεύτικα θετικά και ψεύτικα αρνητικά. (Δεν πραγματοποιήθηκε)
- Εξέταση όλων των θετικών. (Δεν πραγματοποιήθηκε)

Πληροφορίες:

- *Για την ανίχνευση των ευπαθειών των συστημάτων χρησιμοποιήθηκαν τα προγράμματα Nessus κ' Retina και η διαδικασία περιγράφεται στην ενότητα 1.5.2*

2.5.2 Vulnerability Scanning

Nessus

Το nessus είναι το πιο γνωστό εργαλείο διείσδυσης το οποίο παρέχεται υπό το καθεστώς του ανοικτού λογισμικού. Επίσης είναι ολοκληρωμένο εργαλείο διείσδυσης παρέχοντας όλες τις απαραίτητες λειτουργίες καλύπτοντας ταυτόχρονα όλες τις απαιτήσεις. Χαρακτηριστικά, το nessus παρέχει μια ολοκληρωμένη μηχανή για «port scanning» και αναγνώριση υπηρεσιών, ημιαυτοματοποιημένο μηχανισμό για την ενημέρωση για νέου είδους επιθέσεις, δημιουργία εύκολων και ευανάγνωστων αναφορών για την κατάσταση των υπό εξέταση μηχανημάτων και τέλος μια εξειδικευμένη γλώσσα για τη συγγραφή «σεναρίων» επίθεσης. Τέλος επιτρέπει τον έλεγχο οποιασδήποτε IP διεύθυνσης χωρίς την ανάγκη κάποιας ειδικής αδείας χρήσης, αφού παρέχεται κάτω από την GNU GPL.

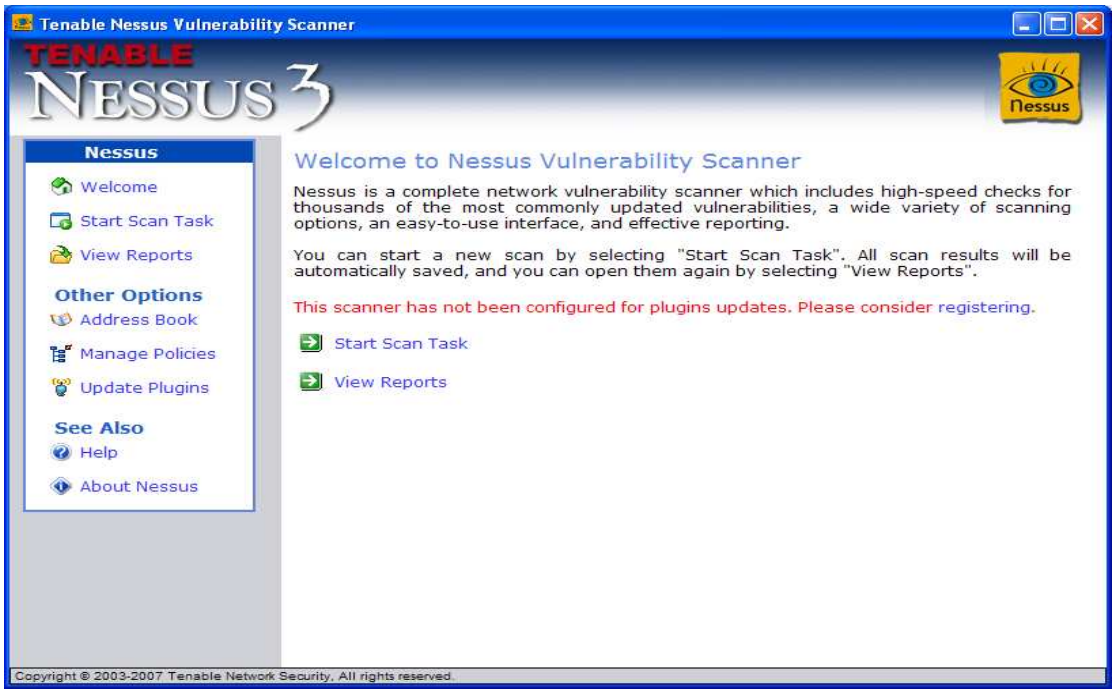
Download: http://www.nessus.org/download/

Παρακάτω γίνεται η τοποθέτηση του κωδικού που μας στάλθηκε ηλεκτρονικά για να χρησιμοποιήσουμε την πλήρη έκδοση του προγράμματος.

Εικόνα 54 Nessus : Εισαγωγή License Key

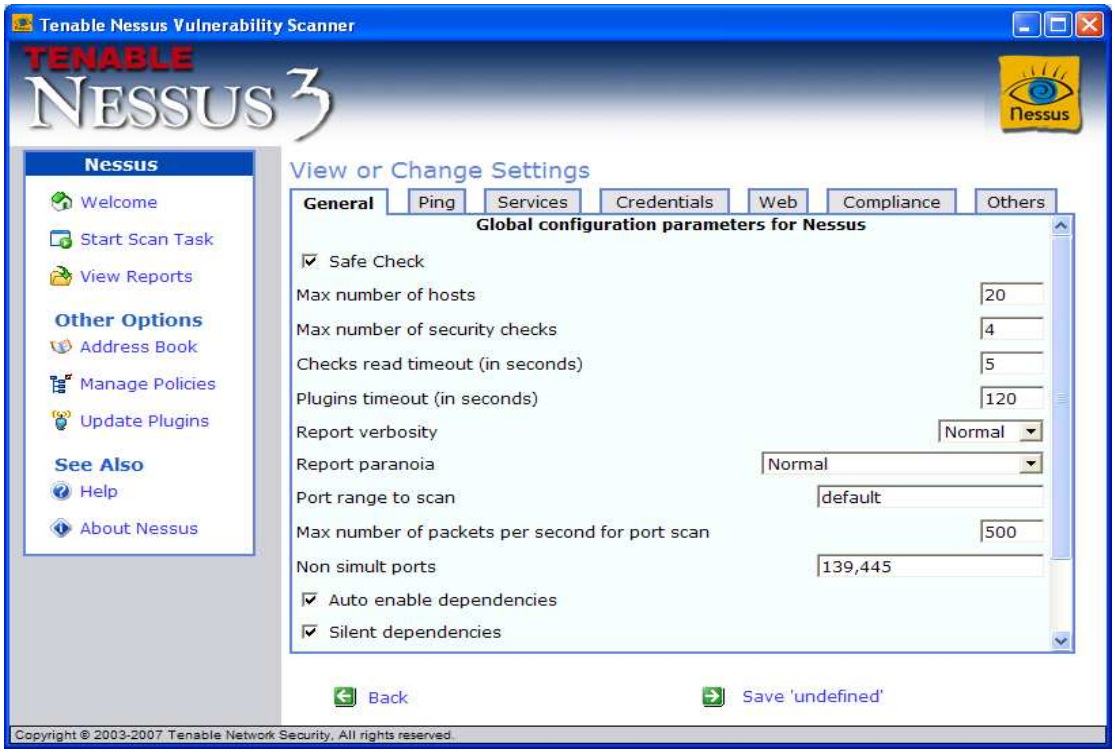
Πρέπει να αναφέρουμε πως η εκτέλεση της διαδικασίας έγινε σε εσωτερικό δίκτυο του epp λόγω του ότι το Nessus δεν έβρισκε αδυναμίες μέσω Ιντερνετ.

Ξεκινάμε με το άνοιγμα του προγράμματος.



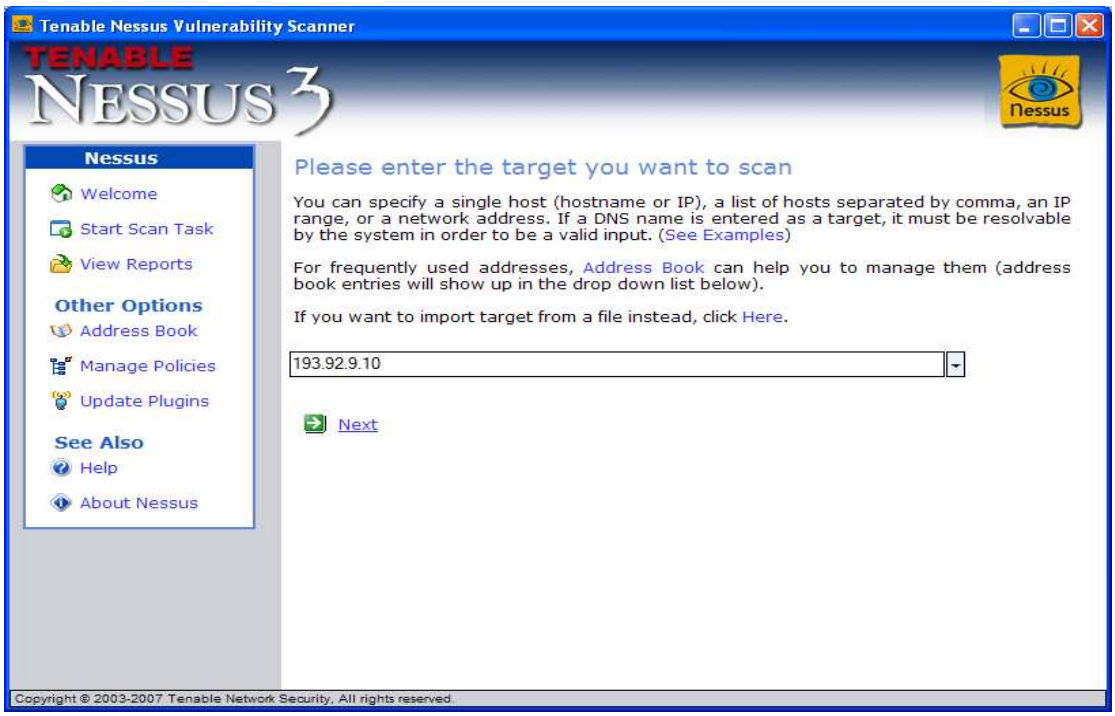
Εικόνα 55 Nessus: Απεικόνιση του προγράμματος

Επιλέγοντας την καρτέλα Manage Policies όπως ακολουθεί μπορούμε να κάνουμε τις κατάλληλες αλλαγές ως προς τον τρόπο εύρεσης των αδυναμιών του συστήματος. Αναφορικά θα στηθούμε σε μερικές από αυτές στην γενική καρτέλα του προγράμματος. αφού και οι προεπιλεγμένες τιμές που έχει δώσει ο κατασκευαστής αρκούν για να πάρουμε τα επιθυμητά αποτελέσματα.



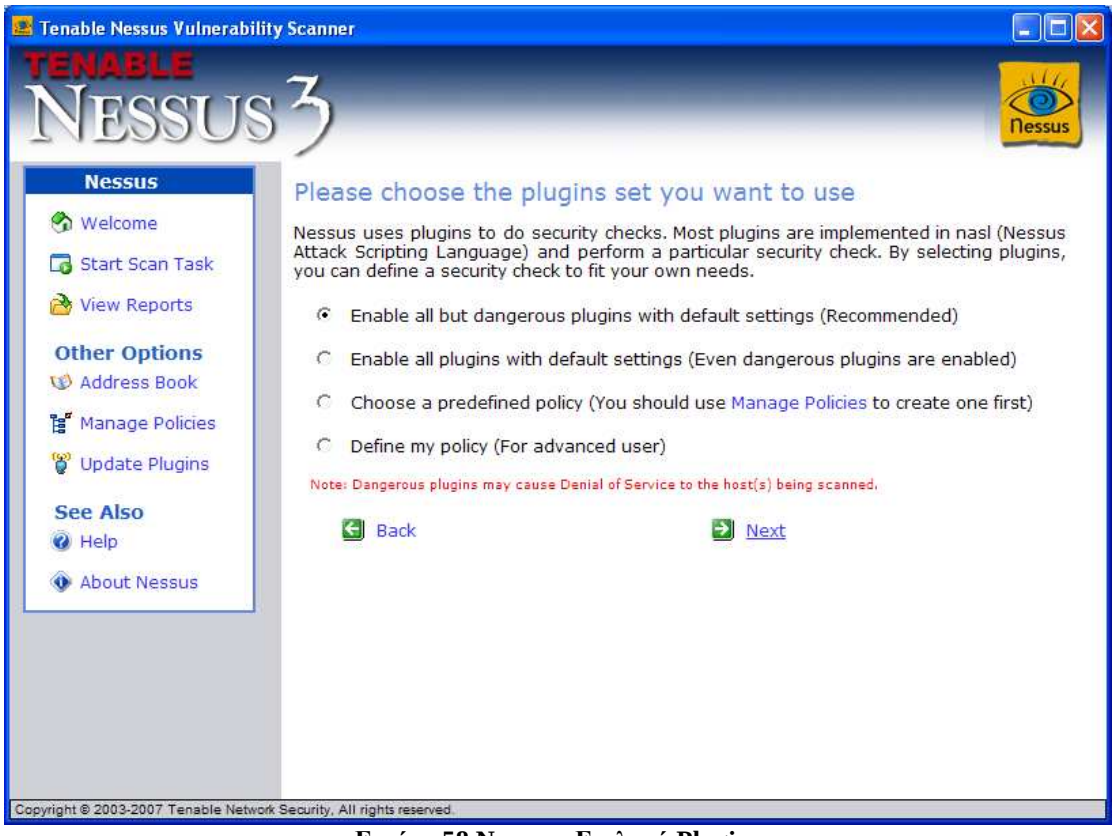
Εικόνα 56 Nessus: Manage Policies

Αφού επιστρέψουμε στην καρτέλα Start Scan Task στο πεδίο κειμένου θα πληκτρολογήσουμε την IP διεύθυνση του στόχου μας που είναι η "193.92.9.10" για το http://www.epp.teiher.gr. Στη συνέχεια επιλέγουμε "next" :



Εικόνα 57 Nessus: Προσθήκη διεύθυνσης IP για epp

Παρακάτω αφού επιλέξουμε τα κατάλληλα plugins όπως ακολουθεί επιλέγουμε Next.

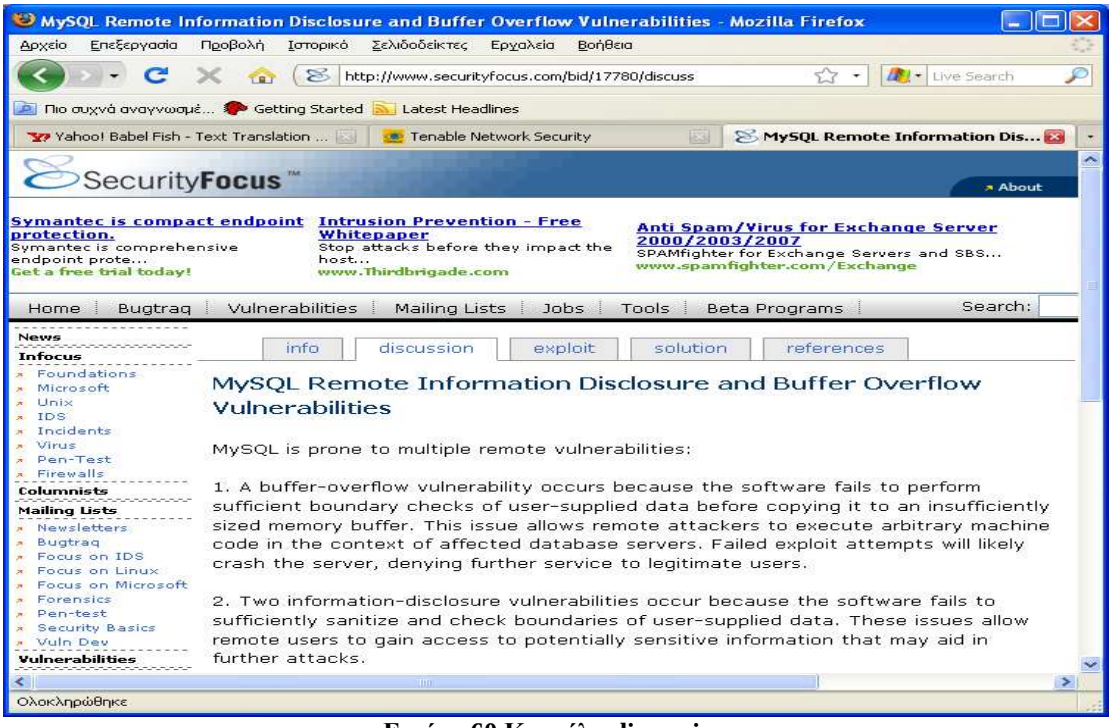


Εικόνα 58 Nessus: Επιλογή Plugins

Το Plugin είναι ένα απλό πρόγραμμα που ελέγχει για μια δεδομένη ρωγμή. Υπάρχουν αυτήν την περίοδο 25245 διαφορετικά **plugins**[5] που χρησιμοποιούνται από το Nessus, για την κάλυψη τοπικών και μακρινών ρωγμών που περιγράφονται από κάποιο **CVE**[6]. π. χ στο plugin 21632 αντιστοιχεί το CVE-2006-1516.

Εικόνα 59 Plugin MySQL Anonymous Login Handshake Remote Information Disclosure

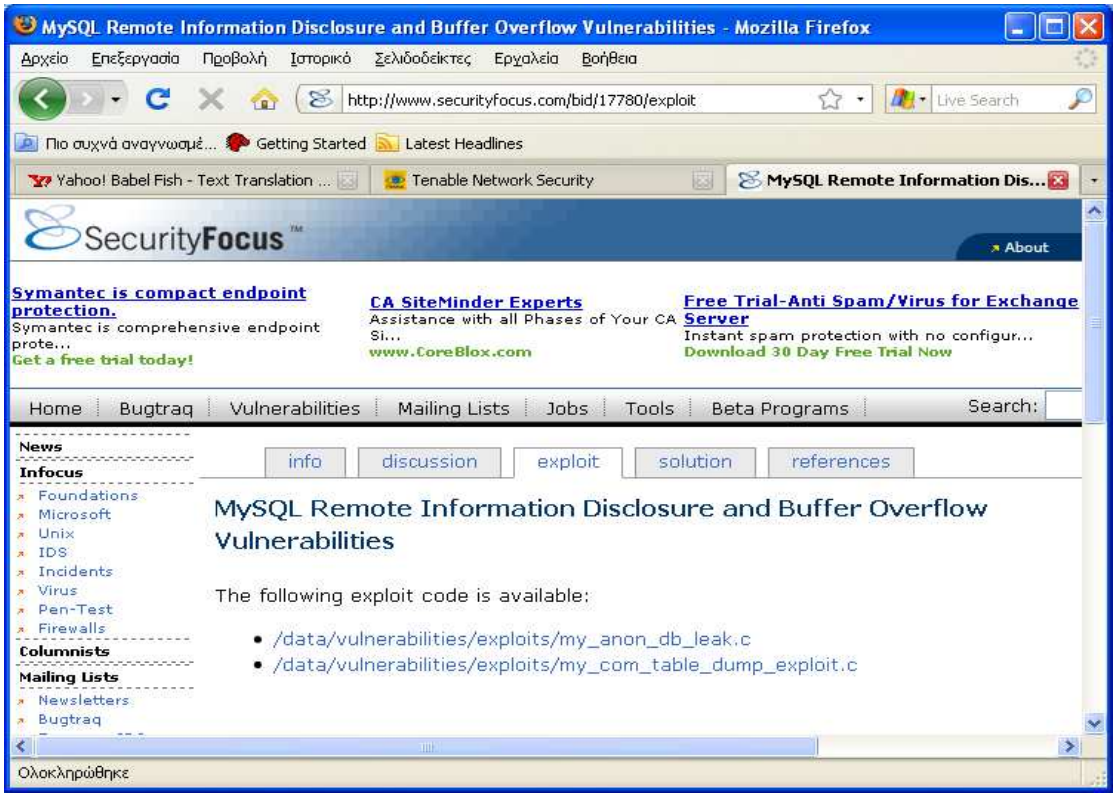
Επιλέγουμε το Bugtraq ID 17780 και έχουμε στην καρτέλα discussion γενικότερες πληροφορίες για το συγκεκριμένο CVE:



Εικόνα 60 Καρτέλα discussion

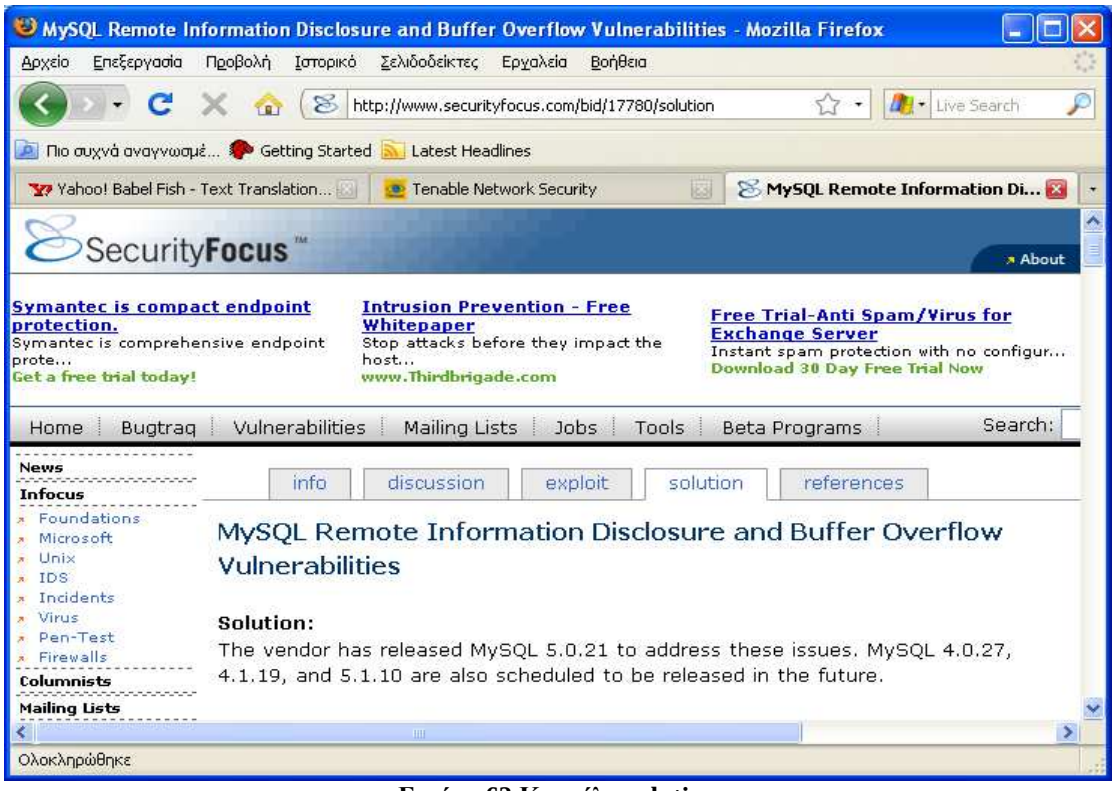
[5] http://www.nessus.org/plugins/index.php?view=all
[6] http://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

Στην καρτέλα exploit βρίσκουμε τον κώδικα που μπορούμε να χρησιμοποιήσουμε για να εκμεταλλευτούμε τη συγκεκριμένη αδυναμία:



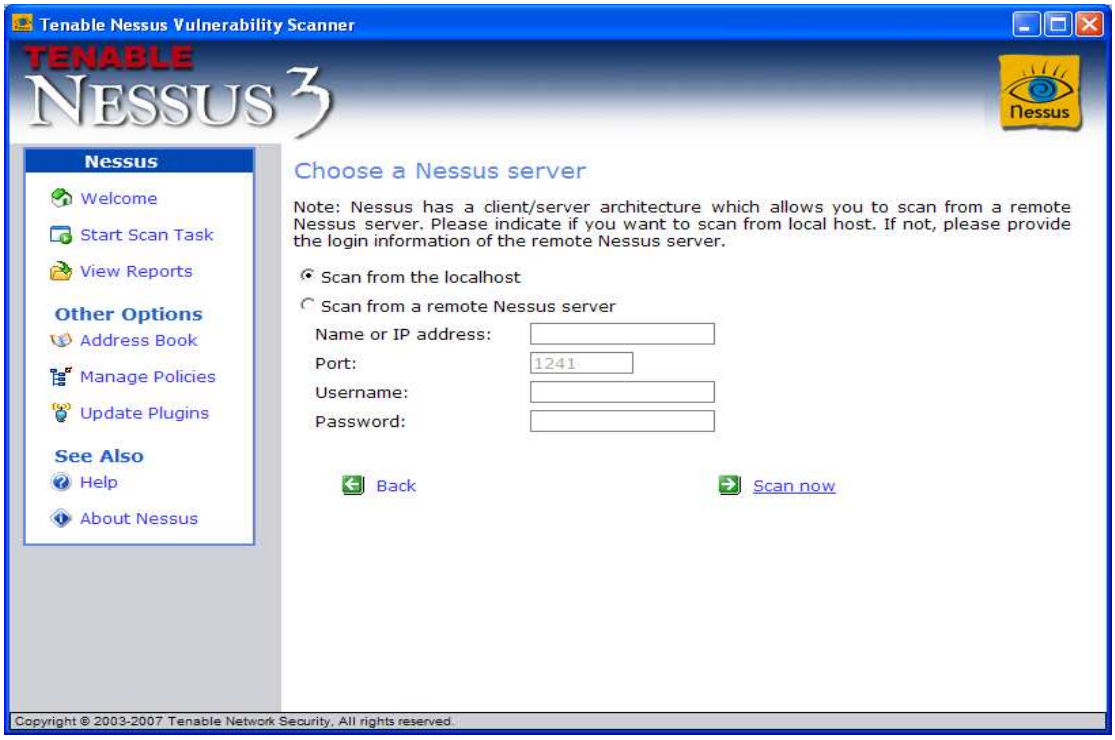
Εικόνα 61 Καρτέλα exploit

Τέλος παρουσιάζεται η επίλυση της αδυναμίας:



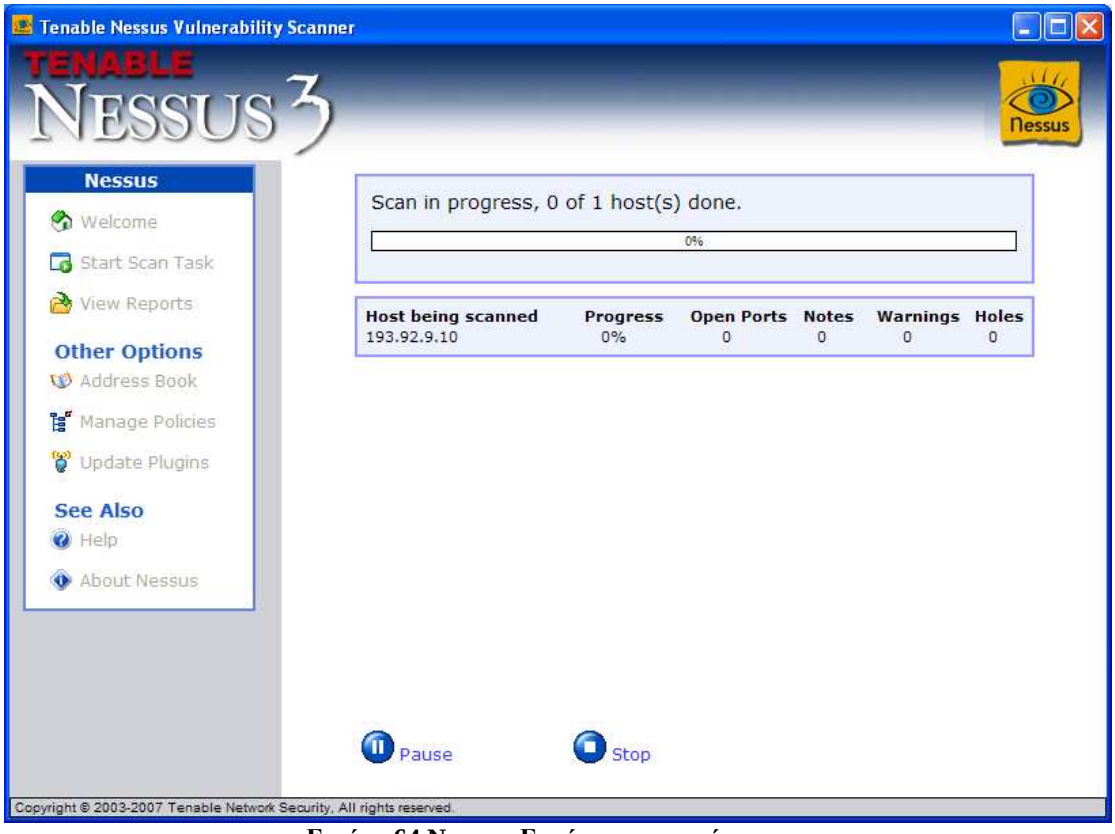
Εικόνα 62 Καρτέλα solution

Στη συνέχεια επιλέγεται το σημείο απ' όπου θα ξεκινήσει η επίθεση. Μετά επιλέγουμε Scan now.



Εικόνα 63 Nessus: Επιλογή θέσης εκκίνησης

Και η διαδικασία ξεκινάει:

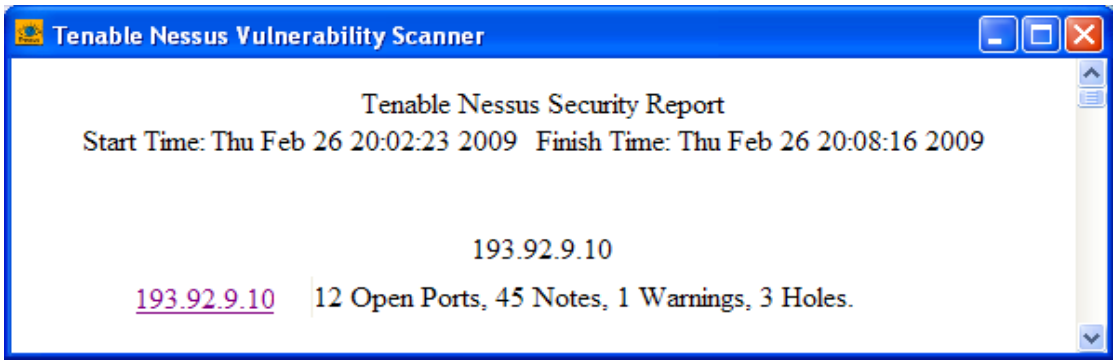


Εικόνα 64 Nessus: Εκκίνηση της ανίχνευσης

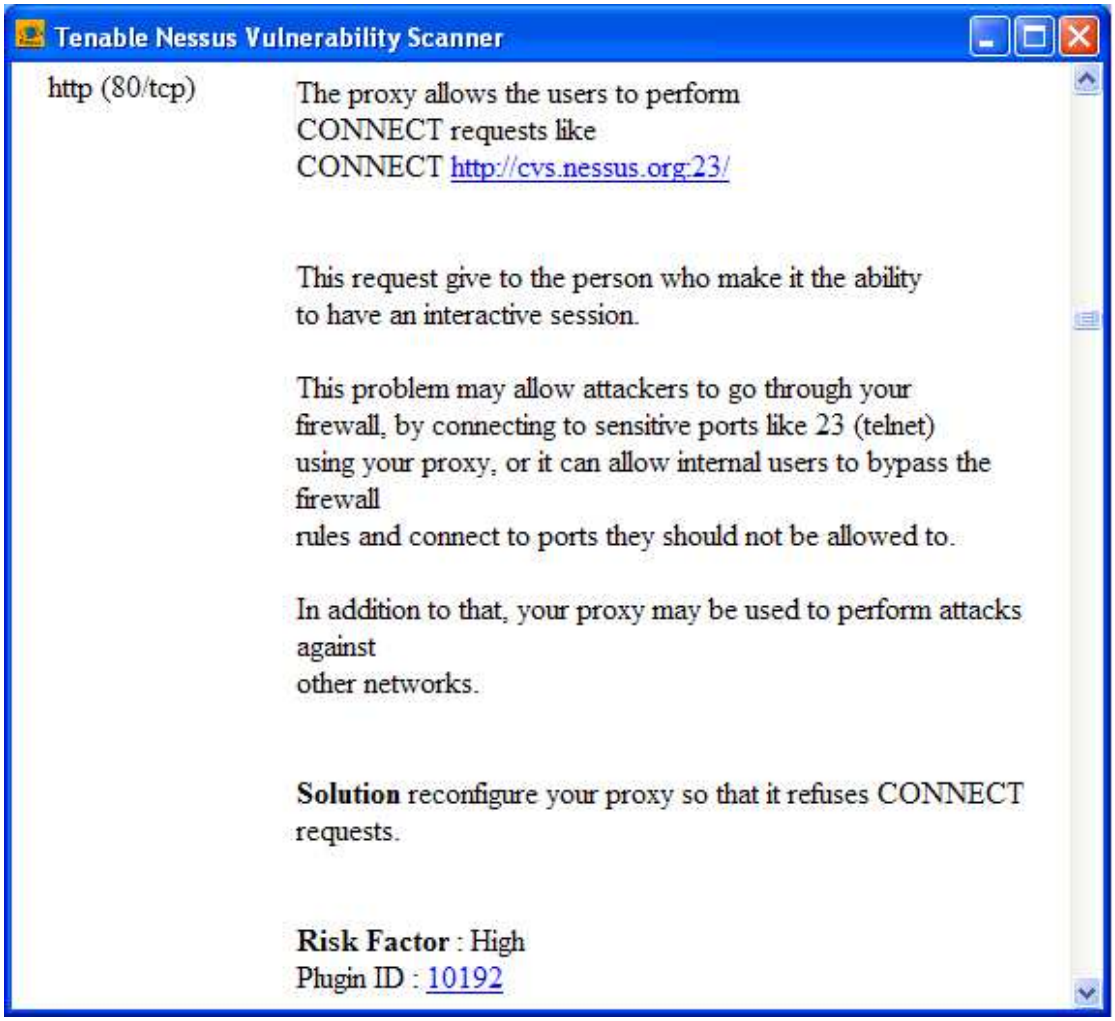
Τέλος στην παρακάτω ενότητα παρουσιάζονται τα αποτελέσματα της συννημένης αναφοράς του προγράμματος όπου το Risk Factor (κατάσταση επικινδυνότητας) είναι High ή Critical. Η ιεραρχία παρουσιάζεται παρακάτω:

Ιεραρχία κατάστασης επικνδυνότητας

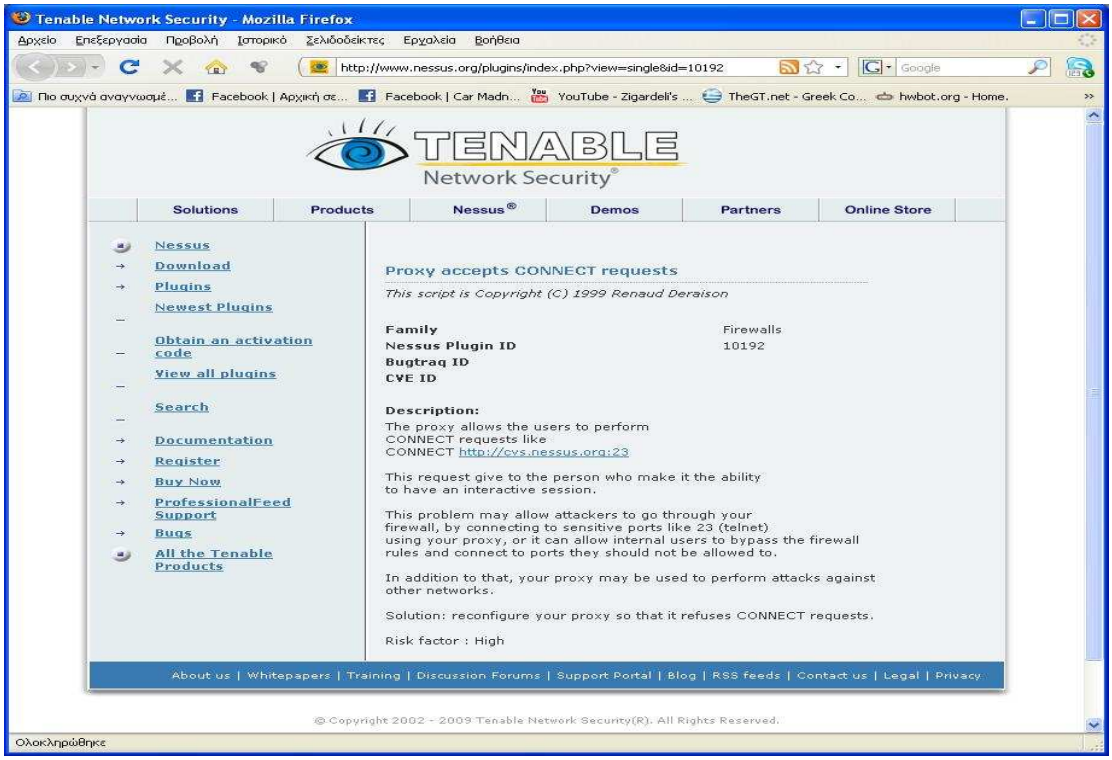
- Low
- Medium
- High
- Critical



Εικόνα 65 Nessus: Open Ports, Notes, Warnings, Holes



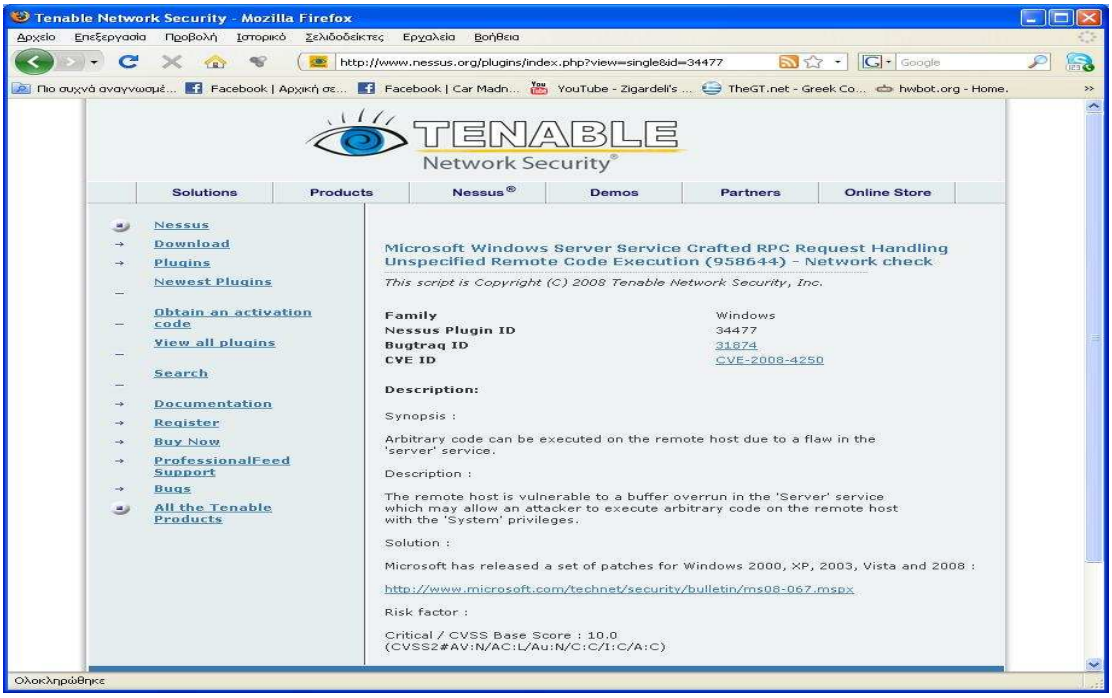
Εικόνα 66 Nessus: http(80/tcp)



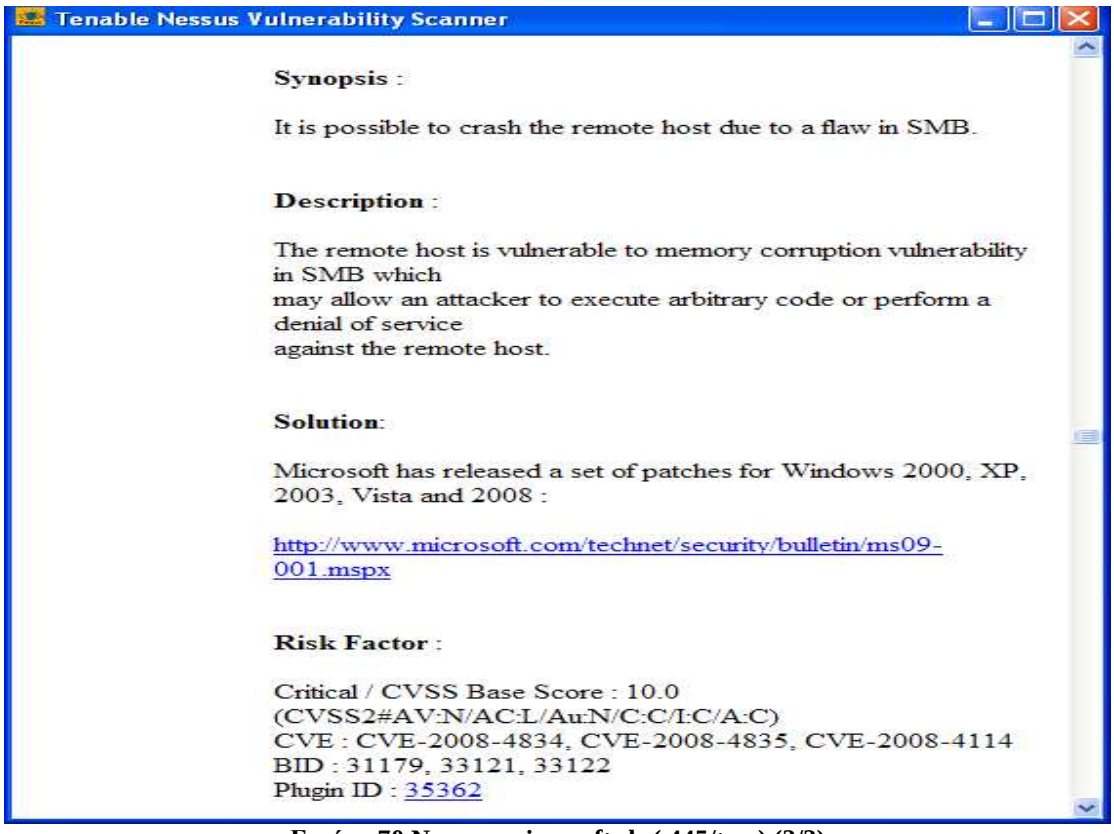
Εικόνα 67 Plugin ID : 10192

Εικόνα 68 Nessus: microsoft-ds (445/tcp)(1/2)

- CVE-2008-4250: The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalization, as exploited in the wild by Gimmiv.A in October 2008, aka "Server Service Vulnerability."



Εικόνα 69 Plugin ID : 34477

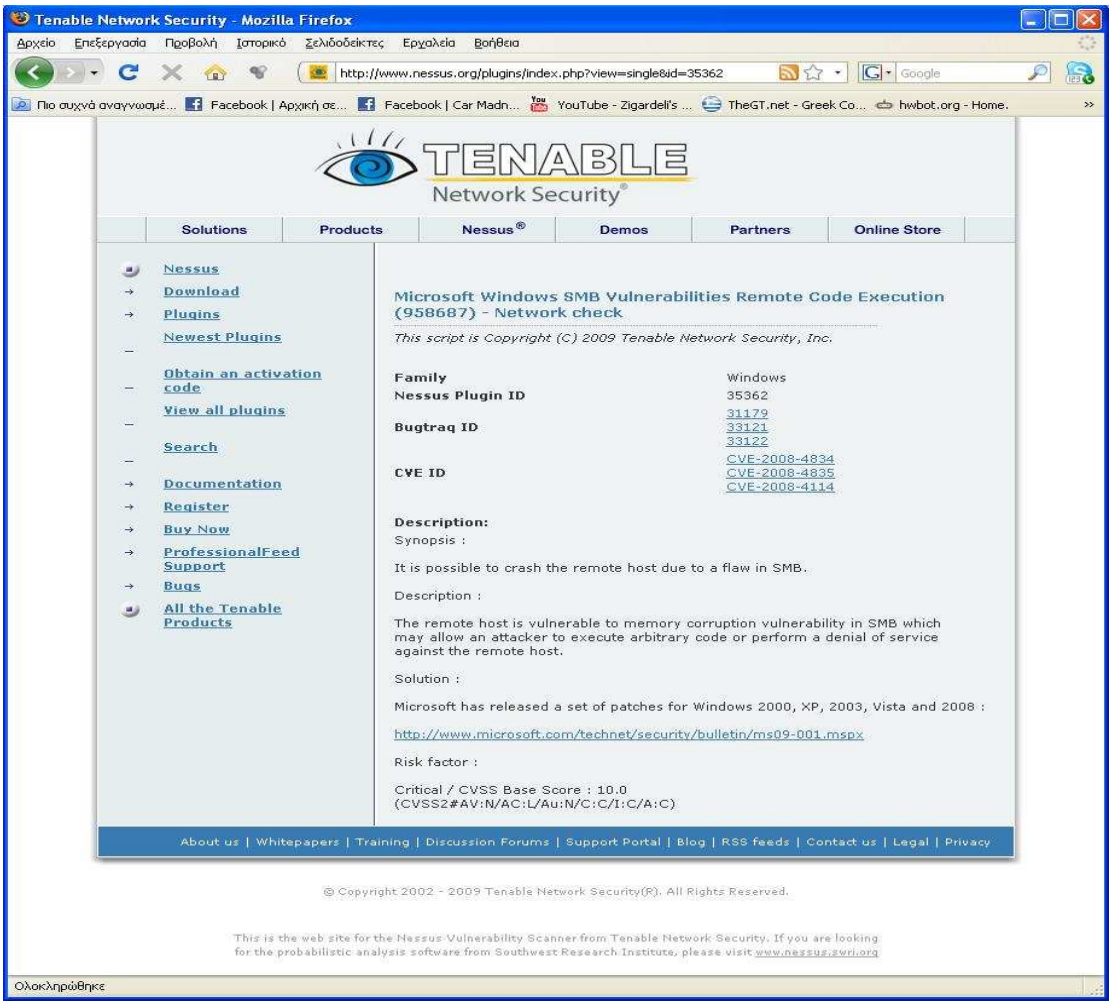


Εικόνα 70 Nessus: microsoft-ds (445/tcp) (2/2)

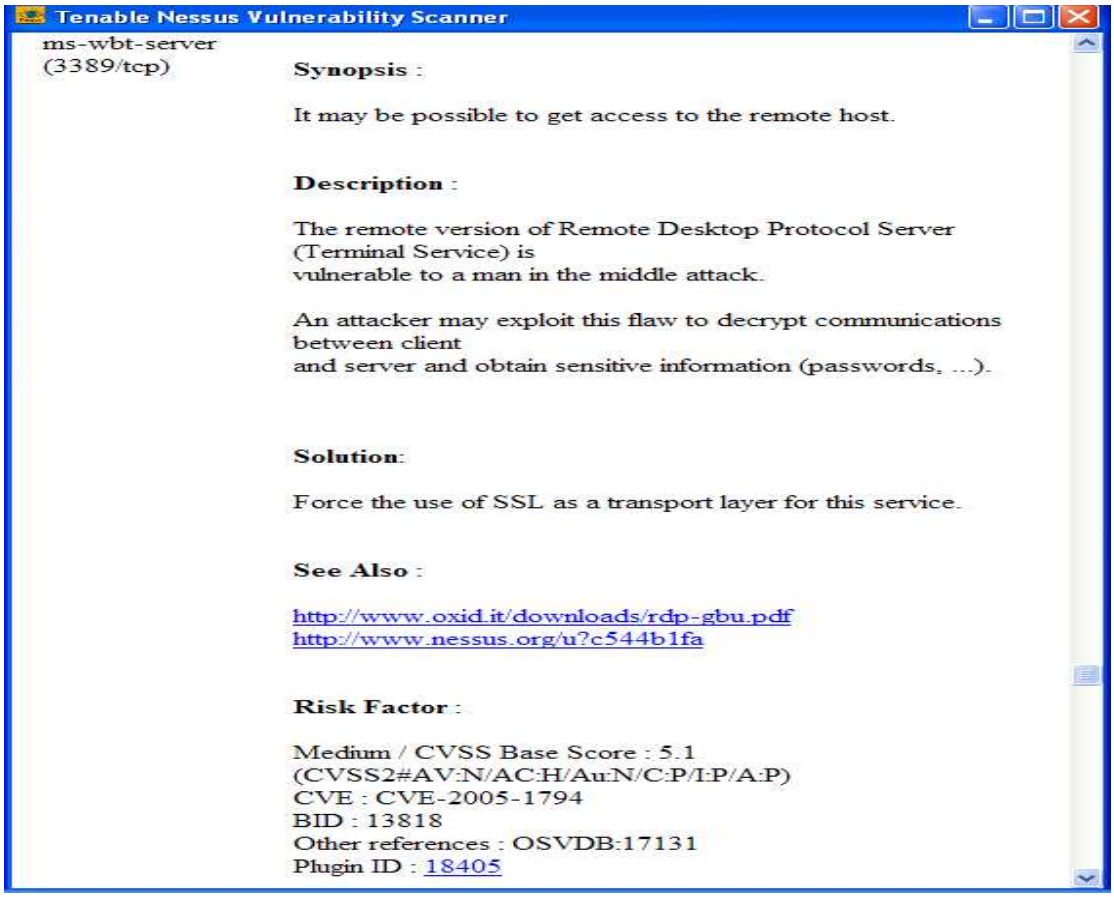
- CVE-2008-4834: Buffer overflow in SMB in the Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2 allows remote attackers to execute arbitrary code via malformed values of unspecified "fields inside the SMB packets" in an NT Trans request, aka "SMB Buffer Overflow Remote Code Execution Vulnerability."

- CVE-2008-4835: SMB in the Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote attackers to execute arbitrary code via malformed values of unspecified "fields inside the SMB packets" in an NT Trans2 request, related to "insufficiently validating the buffer size," aka "SMB Validation Remote Code Execution Vulnerability."

- CVE-2008-4114: srv.sys in the Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote attackers to cause a denial of service (system crash) or possibly have unspecified other impact via an SMB WRITE_ANDX packet with an offset that is inconsistent with the packet size, related to "insufficiently validating the buffer size," as demonstrated by a request to the \PIPE\lsarpc named pipe, aka "SMB Validation Denial of Service Vulnerability."

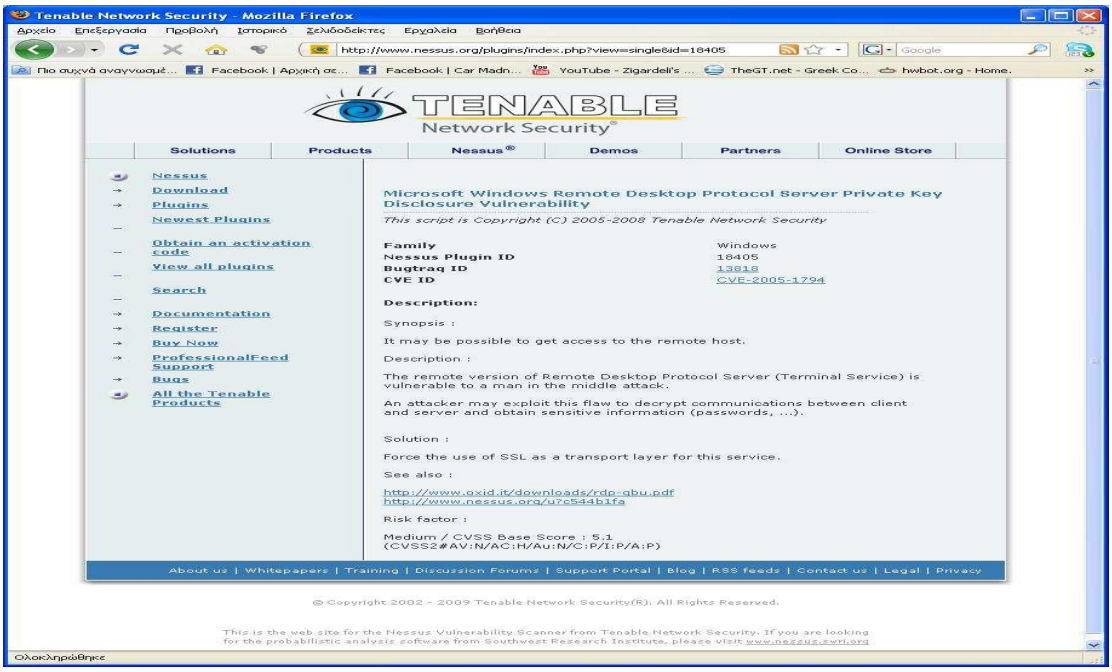


Εικόνα 71 Plugin ID : 35362



Εικόνα 72 Nessus: ms-wbt-server (3389/tcp)

- CVE-2005-1794: Microsoft Terminal Server using Remote Desktop Protocol (RDP) 5.2 stores an RSA private key in mstlsapi.dll and uses it to sign a certificate, which allows remote attackers to spoof public keys of legitimate servers and conduct man-in-the-middle attacks.



Εικόνα 73 Plugin ID : 18405

Για την εύρεση των:

- Discussion
- Exploit
- Solution

Θα επισκεπτόμαστε τη σελίδα http://www.nessus.org/plugins/index.php?view=search όπου πληκτρολογώντας το Plugin ID θα επιλέγουμε Bugtraq ID και θα παραπεμπόμαστε στη σελίδα όπου θα πληροφορούμαστε για τα παραπάνω.

Retina 5

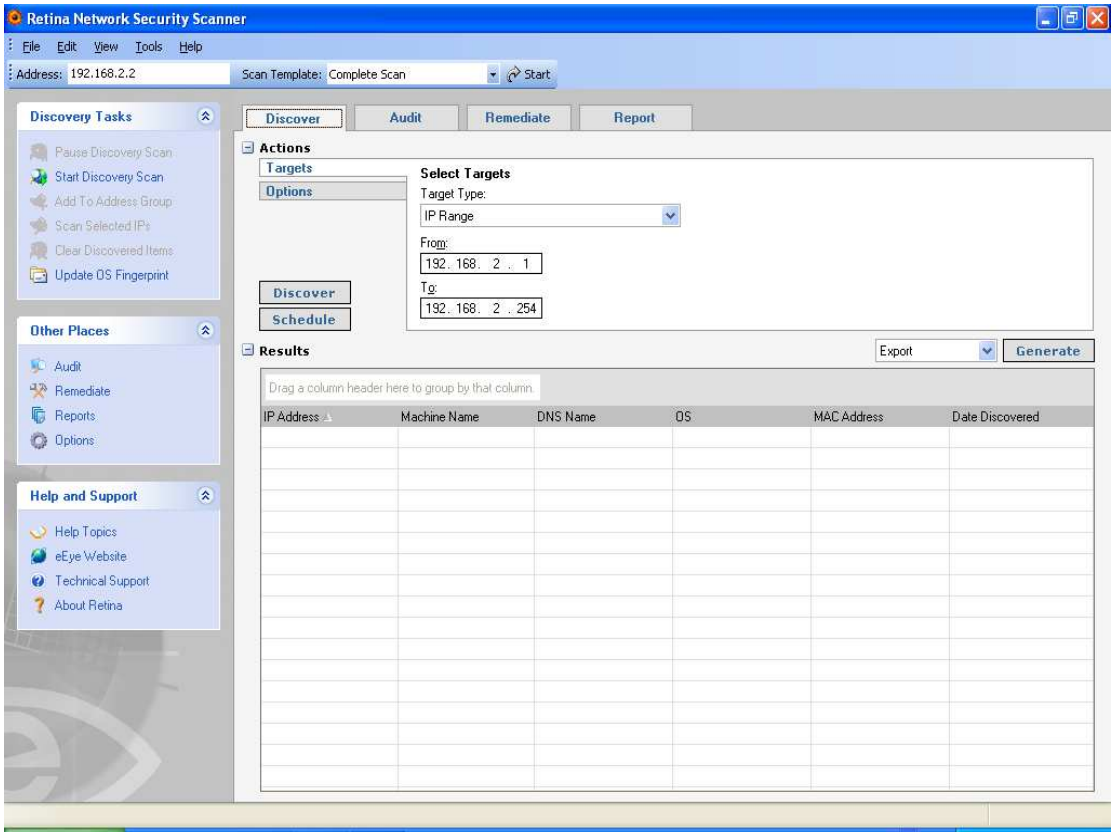
Το Retina είναι ένα network security scanner που έχει δημιουργηθεί από την eEye Digital Security. Το Retina είναι ένα βραβευμένο σύστημα διείσδυσης το οποίο είναι γνωστό για την ακρίβεια και την ταχύτητα του. Παρέχει μηχανισμούς για τη μορφοποίηση του προγράμματος ανάλογα με τις απαιτήσεις του κάθε οργανισμού. Παρέχει προηγμένη μηχανή για scanning καθώς και μια κατανοητή βάση δεδομένων η οποία αποθηκεύει τις γνώστες αδυναμίες ασφαλείας και η οποία ανανεώνεται αυτόματα με νέες απειλές. Επίσης μπορεί να αναγνωρίσει διάφορες συσκευές δικτύου καθώς και μη-εξουσιοδοτημένα προγράμματα όπως P2P, malware, spyware etc. Τέλος το Retina υποστηρίζει ελέγχους ασφάλειας σε διαφορετικά λειτουργικά συστήματα, παρέχει δυνατότητες για τη δημιουργία προσωπικών ελέγχων ασφαλείας καθώς και προσαρμοσμένες αναφορές ασφάλειας. Το Retina είναι ένα σύστημα ελέγχου ασφαλείας το οποίο προορίζεται κυρίως για οργανισμούς και δεν παρέχει τη δυνατότητα ελέγχου οποιασδήποτε IP διεύθυνσης.

Download: http://www.softpedia.com/get/Security/Security-Related/Retina-Network-SecurityScanner.shtml

Παρακάτω γίνεται η τοποθέτηση του κωδικού που μας στάλθηκε ηλεκτρονικά για να χρησιμοποιήσουμε την πλήρη έκδοση του προγράμματος

Εικόνα 74 Εισαγωγή License Key

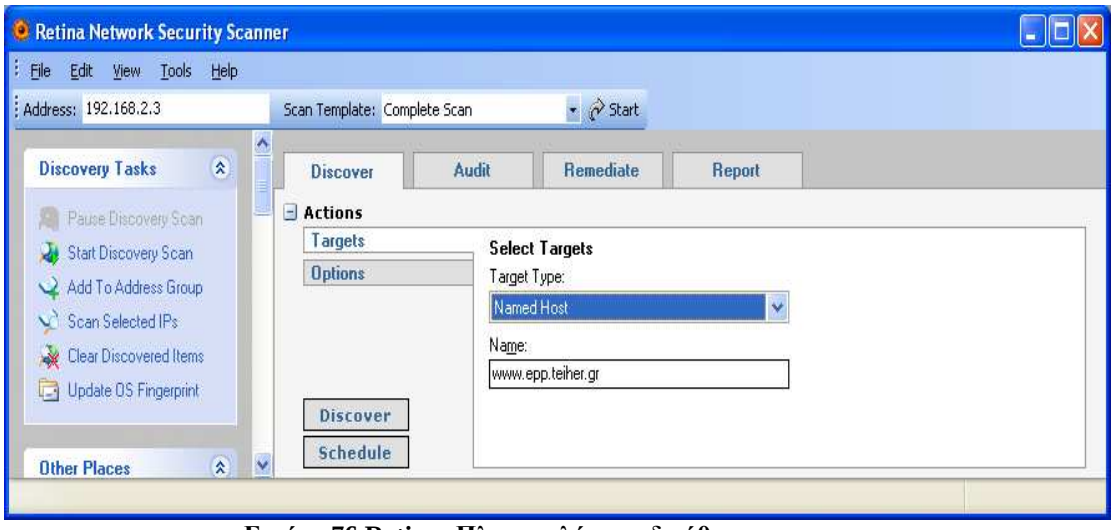
Ξεκινάμε με το άνοιγμα του προγράμματος:



Εικόνα 75 Retina: Απεικόνιση του προγράμματος Retina

Συνεχίζουμε με την αλλαγή των παραμέτρων (για το epp) στην καρτέλα **Discover**[7] στην επιλογή:

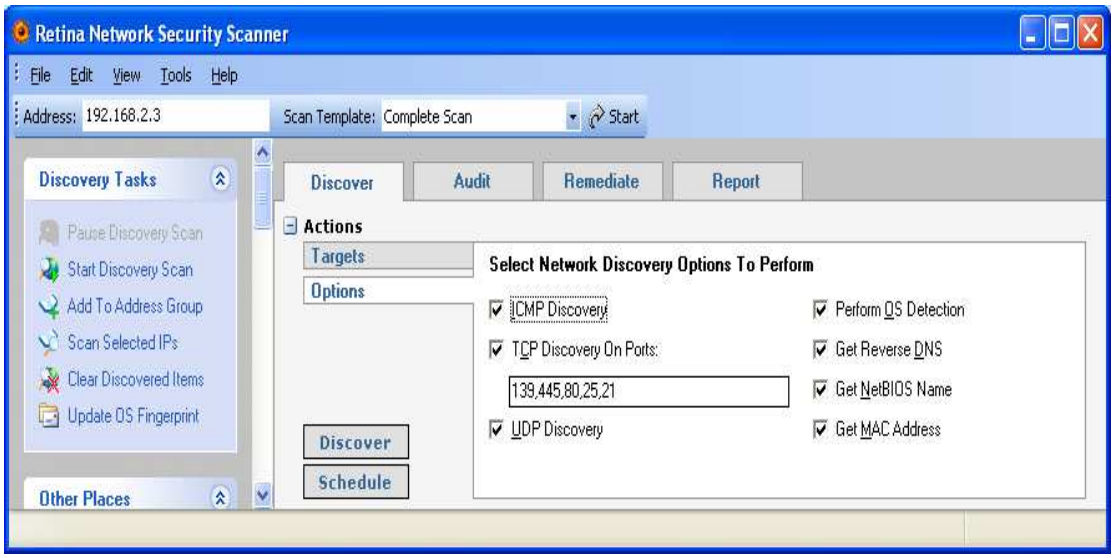
- Targets



Εικόνα 76 Retina: Πληκτρολόγηση διεύθυνσης του epp

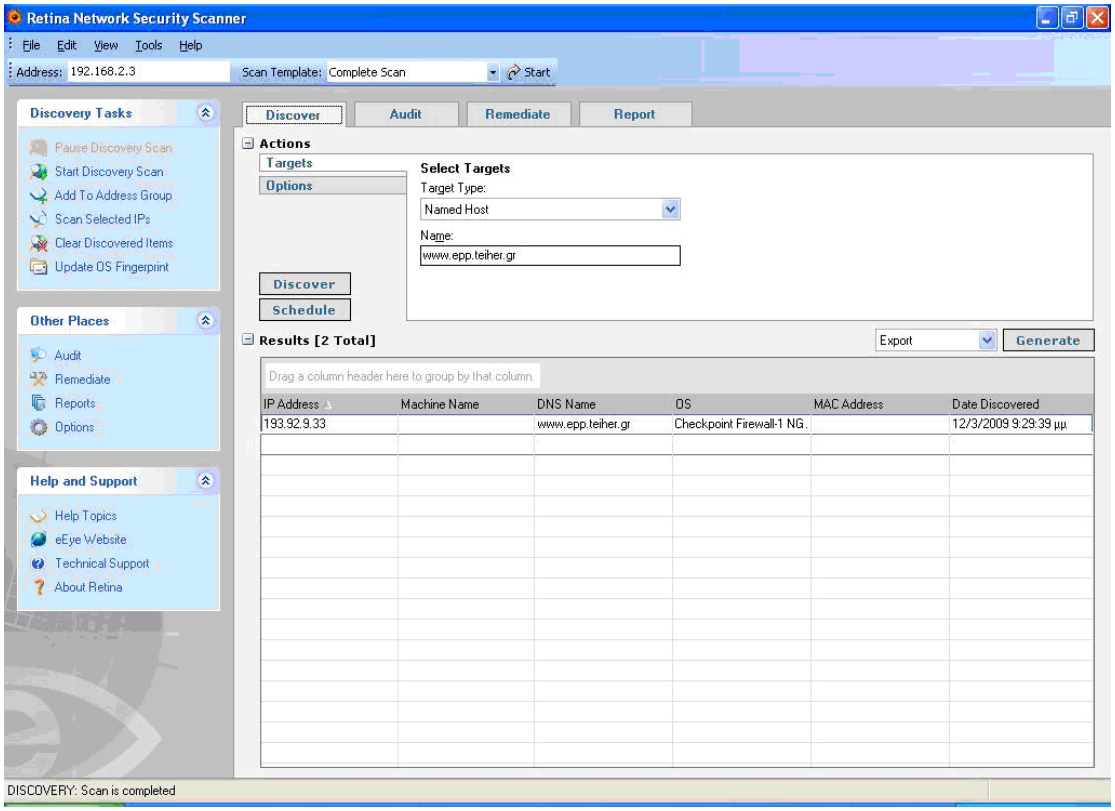
[7] The Discover tab provides the ability to scan unlimited IPs to discover network machines—PCs, routers, printers, and so on

- Options



Εικόνα 77 Retina: Ρυθμίσεις της παραμέτρου Options στην καρτέλα Discover

Επιλέγοντας Discover έχουμε:



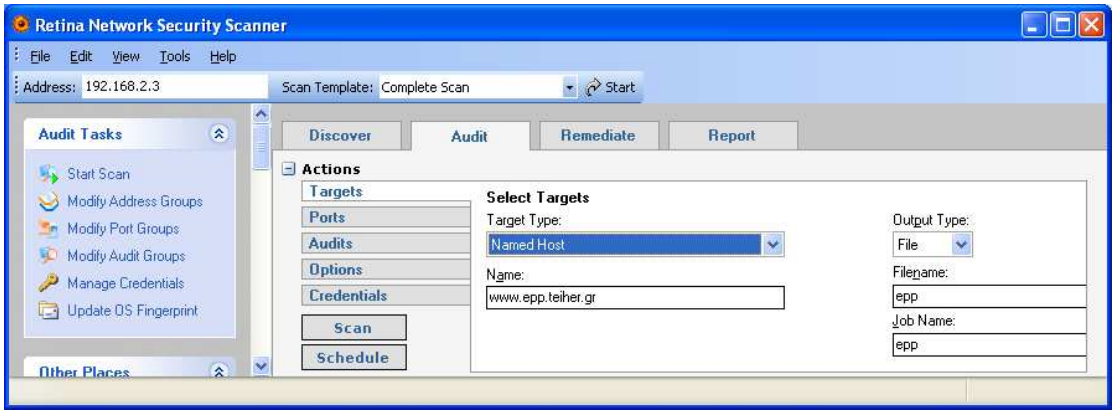
Εικόνα 78 Retina: Επιλογή Discover

Έτσι πληροφορούμαστε για:

- Τη διεύθυνση IP
- Το όνομα του DNS
- Το λειτουργικό σύστημα

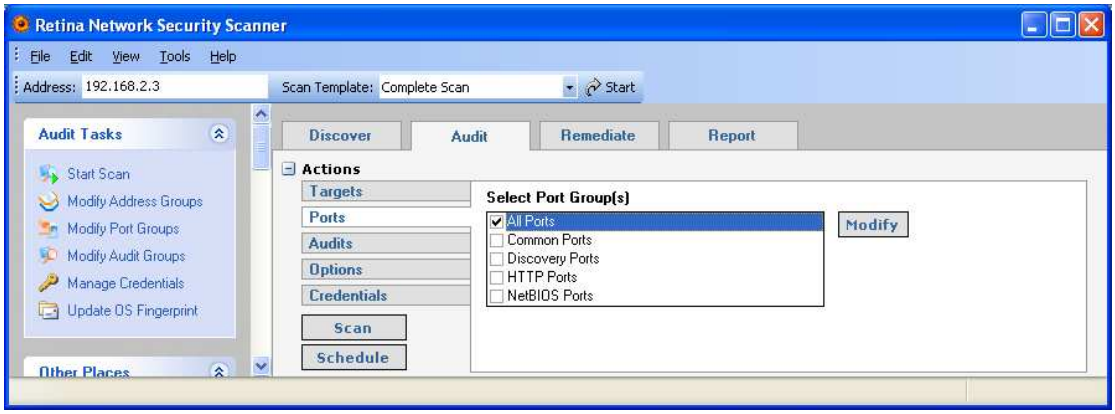
Στην καρτέλα **Audit**[8] στην επιλογή:

- Targets



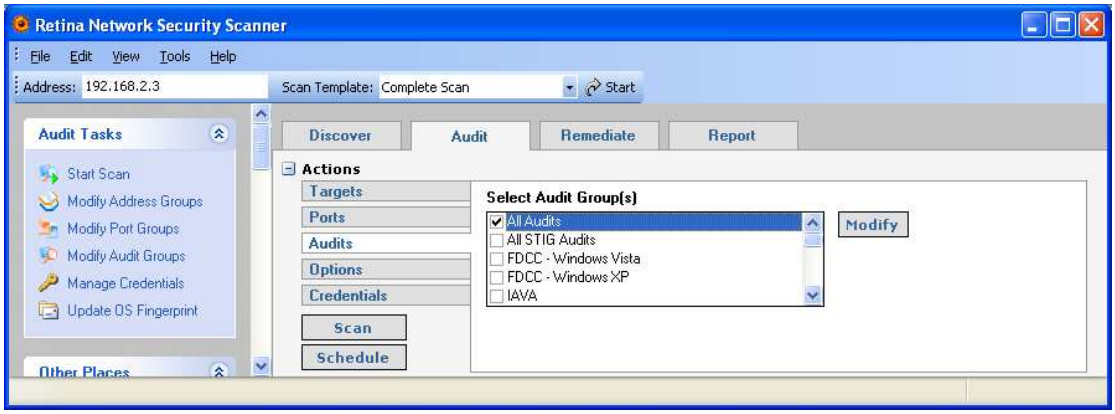
Εικόνα 79 Retina: Ρυθμίσεις της παραμέτρου Targets στην καρτέλα Audit

- Ports



Εικόνα 80 Retina: Ρυθμίσεις της παραμέτρου Ports στην καρτέλα Audit

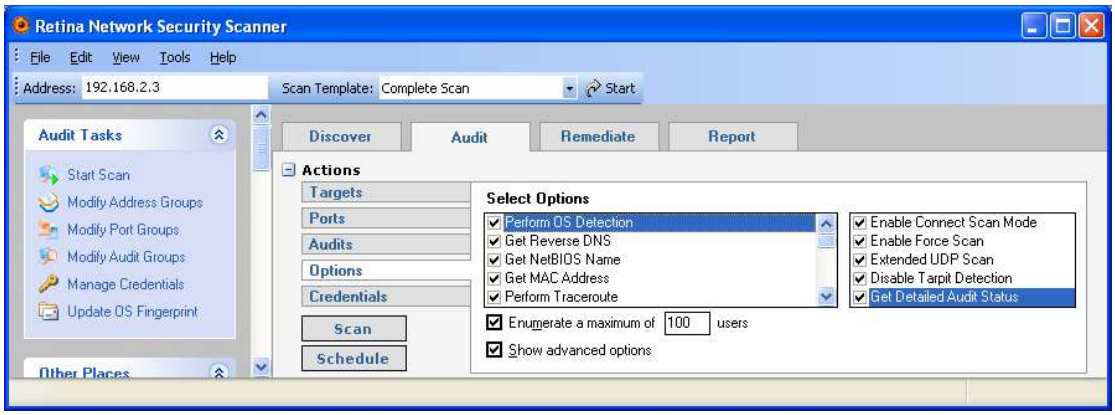
- Audits



Εικόνα 81 Retina: Ρυθμίσεις της παραμέτρου Audits στην καρτέλα Audit

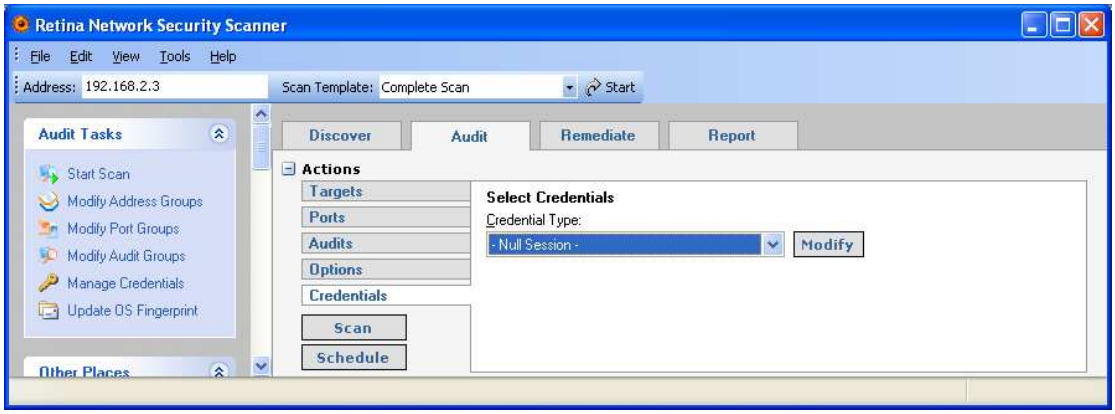
[8] The Audit tab is an option you can select to scan for all known open ports and services on the specified target IP address(es).

- Options



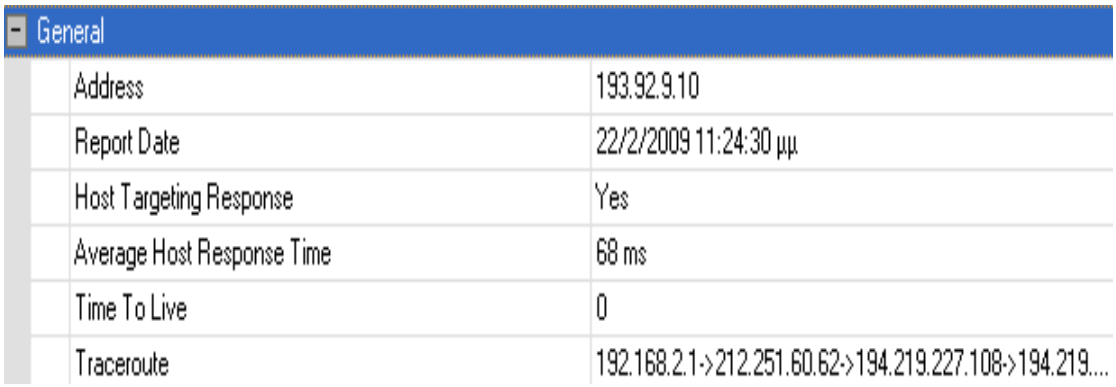
Εικόνα 82 Retina: Ρυθμίσεις της παραμέτρου Options στην καρτέλα Audit

- Credentials



Εικόνα 83 Retina: Ρυθμίσεις της παραμέτρου Credentials στην καρτέλα Audit

Αφού εκτελεστούν οι παραπάνω ρυθμίσεις πατάμε “Start” . Όταν εκτελεστεί η διαδικασία στην καρτέλα Audit ->Scanned Ips παρουσιάζονται τα αποτελέσματα:

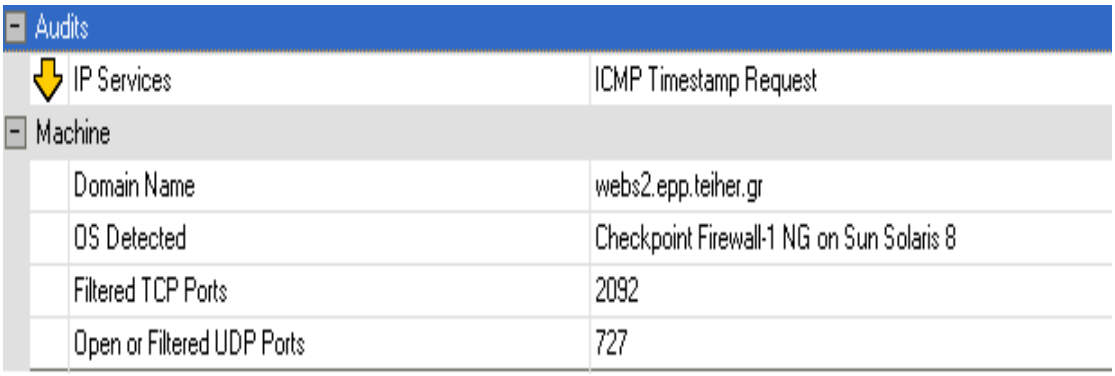


Εικόνα 84 Retina: General

Πληροφορούμαστε για:

- Την IP διεύθυνση
- Την ημερομηνία της αναφοράς
- Αν λάβαμε απάντηση από τον host
- Το μέσο όρο πού έλαβε χρόνο η απάντηση

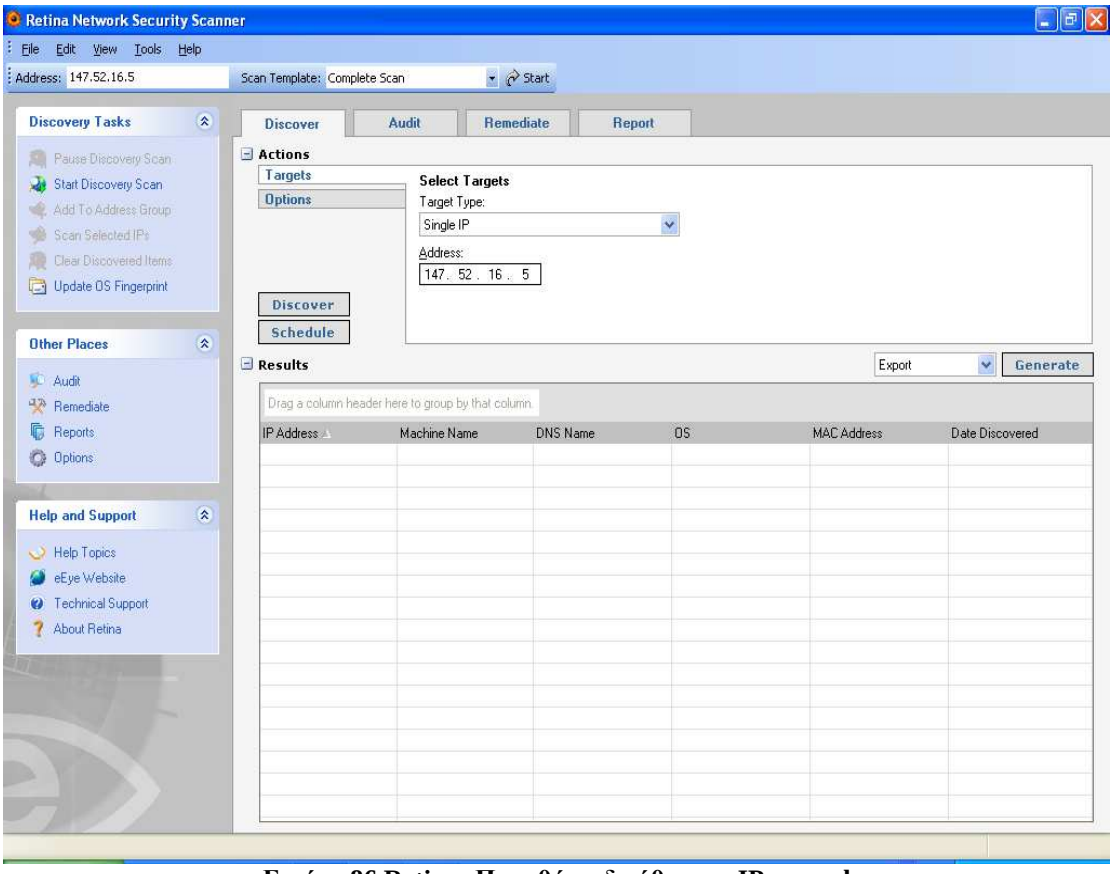
- Το TTL
- Το χάρτη της διαδρομής



Εικόνα 85 Retina: Audits, Machine

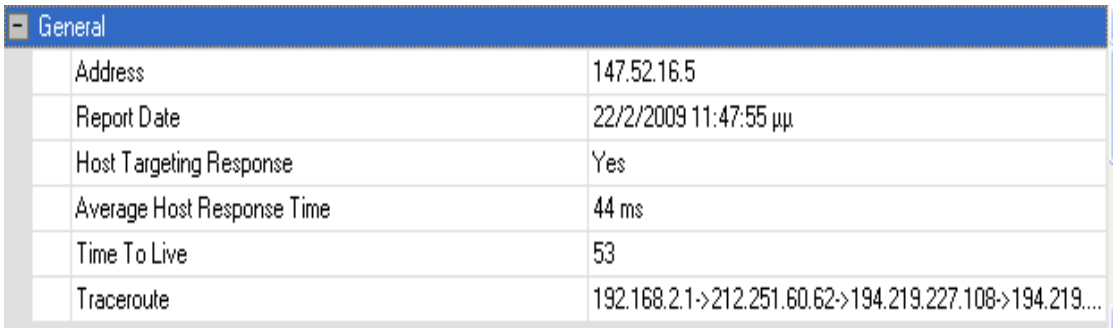
- Τις υπηρεσίες IP
- Το όνομα του Server
- Το λειτουργικό σύστημα
- Τις φιλτραρισμένες πόρτες TCP
- Τις ανοιχτές ή φιλτραρισμένες πόρτες UDP

Τηρώντας τα βήματα και τη σειρά αυτών θα εφαρμόσουμε τη διαδικασία για το csd. Η μόνη διαφορά είναι ότι στην καρτέλα Discover και Audit αλλάζει η διεύθυνση, πατώντας “Scan” θα ξεκινήσει και πάλι η διαδικασία της ανίχνευσης:



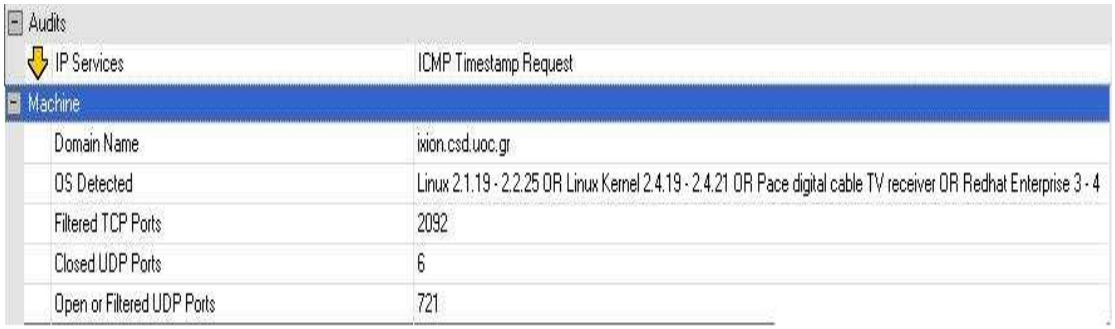
Εικόνα 86 Retina: Προσθήκη διεύθυνσης IP για csd

Ακολουθούν τα αποτελέσματα της ανίχνευσης:



General	
Address	147.52.16.5
Report Date	22/2/2009 11:47:55 μμ
Host Targeting Response	Yes
Average Host Response Time	44 ms
Time To Live	53
Traceroute	192.168.2.1->212.251.60.62->194.219.227.108->194.219....

Εικόνα 87 Retina: General



Audits	
IP Services	ICMP Timestamp Request
Machine	
Domain Name	ixion.csd.uoc.gr
OS Detected	Linux 2.1.19 - 2.2.25 OR Linux Kernel 2.4.19 - 2.4.21 OR Pace digital cable TV receiver OR Redhat Enterprise 3 - 4
Filtered TCP Ports	2092
Closed UDP Ports	6
Open or Filtered UDP Ports	721

Εικόνα 88 Retina: Audits, Machine

2.6 Firewall Testing

2.6.1 Περιγραφή

Το firewall ελέγχει το ρυθμό της κίνησης μεταξύ του τοπικού/εταιρικού δικτύου, του DMZ, και του Διαδικτύου. Λειτουργεί σε μια πολιτική ασφάλειας και χρησιμοποιεί ACLs (AccessControl Lists). Αυτή η ενότητα έχει ως σκοπό να βεβαιώσει ότι μόνο αυτός που έχει άδεια μπορεί να επιτραπεί ρητώς στο δίκτυο, κάθε άλλος θα πρέπει να αμφισβητηθεί. Επιπλέον με τον έλεγχο μπορεί να γίνει κατανοητή η ρύθμιση του firewall και η χαρτογράφηση που παρέχει μέσς των server και των υπηρεσιών που τρέχουν πίσω από αυτόν.

Αναθεωρώντας τα log του server απαιτείται ο έλεγχος των δοκιμών που εκτελούνται με την παρουσία του Διαδικτύου ειδικά σε περιπτώσεις όπου τα αποτελέσματα των δοκιμών δεν είναι αμέσως ορατά με τον έλεγχο.

Αναμενόμενα αποτελέσματα:

- Πληροφορίες του firewall ως υπηρεσία και σύστημα.
- Πληροφορίες για τα χαρακτηριστικά γνωρίσματα που εφαρμόζονται στο firewall.
- Περίληψη της πολιτικής ασφαλείας δικτύων από το ACL. (Δεν πραγματοποιήθηκε)
- Λίστα των τύπων των πακέτων που μπορούν να εισαχθούν στο δίκτυο. (Δεν πραγματοποιήθηκε)
- Λίστα των τύπων των πρωτοκόλλων με την πρόσβαση μέσα στο δίκτυο
- Λίστα από τα ενεργά συστήματα που βρέθηκαν.
- Λίστα των πακέτων που εισήχθησαν στο δίκτυο από τον αριθμό της πόρτας. (Δεν πραγματοποιήθηκε)
- Λίστα των πρωτοκόλλων που εισήχθησαν στο δίκτυο.
- Λίστα των ανεξακρίβωτων πορειών στο δίκτυο. (Δεν πραγματοποιήθηκε)

Βήματα που εφαρμόζονται για τον προσδιορισμό του firewall του συστήματος:

Προσδιορισμός του firewall και των χαρακτηριστικών του (Δεν πραγματοποιήθηκε):

- Προσδιορισμός του τύπου του δρομολογητή με τις πληροφορίες που συλλέγονται.
- Προσδιορισμός του router για το αν παρέχει NAT (Network Address Translation).
- Προσδιορισμός των διεισδύσεων από τα στρατηγικά καθορισμένα πακέτα TTL (Firewalking) που πραγματοποιήθηκαν στην ενότητα Port Scanning.

Έλεγχος της ρύθμισης ACL του firewall: (Δεν πραγματοποιήθηκε)

- Εξέταση του ACL ενάντια στη γραπτή πολιτική ασφαλείας ή ενάντια στον κανόνα " Deny All " .
- Έλεγχος για το αν το firewall είναι έξοδος φιλτράροντας την τοπική κυκλοφορία δικτύων.
- Έλεγχος για το αν το firewall εκτελεί την υποκριτική ανίχνευση διευθύνσεων

- Έλεγχος των διεισδύσεων από την αντίστροφη ανίχνευση που ολοκληρώνεται στην ενότητα Port Scanning.
- Εξέταση των εξερχομένων ικανοτήτων του firewall από το εσωτερικό.
- Καθορισμός των επιτυχιών των διάφορων απαντήσεων των πακέτων δακτυλοσκοπώντας τις μεθόδους μέσω του firewall.
- Έλεγχος της βιωσιμότητας της ανίχνευσης SYN health μέσω του firewall για την απαρίθμηση.
- Προσδιορισμός της χρήσης της ανίχνευσης με συγκεκριμένες πηγές πορτών μέσω του firewall για την απαρίθμηση.
- Προσδιορισμός της δυνατότητας του firewall για την αντιμετώπιση των επικαλυμμένων τεμαχίων όπως αυτά που χρησιμοποιούντα στην επίθεση Teardrop.
- Προσδιορισμός της δυνατότητας του firewall για την αντιμετώπιση των μικροσκοπικών τεμαχισμένων πακέτων.
- Προσδιορισμός της δυνατότητας της αντιπυρικής ζώνης να ρυθμιστεί μια τρέχουσα σειρά πακέτων SYN που μπαίνουν (flooding).
- Εξέταση της απάντησης του firewall στα πακέτα με το σύνολο σημαιών RST.
- Εξέταση της διαχείρισης του firewall στα τυποποιημένα πακέτα UDP.
- Έλεγχος της δυνατότητας του firewall στις τεχνικές απαρίθμησης οθόνης χρησιμοποιώντας τα πακέτα ACK.
- Έλεγχος της δυνατότητας του firewall στις τεχνικές απαρίθμησης οθόνης χρησιμοποιώντας τα πακέτα FIN.
- Έλεγχος της δυνατότητας του firewall στις τεχνικές απαρίθμησης οθόνης χρησιμοποιώντας τα πακέτα NULL.
- Έλεγχος της δυνατότητας του firewall στις τεχνικές απαρίθμησης οθόνης μετρώντας το μέγεθος των παραθύρων των πακέτων (WIN).
- Έλεγχος της δυνατότητας του firewall στις τεχνικές απαρίθμησης οθόνης χρησιμοποιώντας όλες τις καθορισμένες σημαίες (XMAS).
- Έλεγχος της δυνατότητας του firewall στις τεχνικές απαρίθμησης οθόνης χρησιμοποιώντας IPIDs
- Έλεγχος της δυνατότητας του firewall στις τεχνικές απαρίθμησης οθόνης χρησιμοποιώντας πρωτόκολλα encapsulated.
- Προσδιορισμός του robustness του firewall και της ευαισθησίας στην άρνηση των επιθέσεων υπηρεσιών με τις συνεχείς συνδέσεις TCP,
- Προσδιορισμός του robustness του firewall και της ευαισθησίας στην άρνηση των επιθέσεων υπηρεσιών με τις χρονικές συνδέσεις TCP.
- Προσδιορισμός του robustness του firewall και της ευαισθησίας στην άρνηση των επιθέσεων υπηρεσιών με τις χρονικές συνδέσεις UDP.
- Προσδιορισμός των απαντήσεων του firewall σε όλους τους τύπους πακέτων ICMP

Ανασκόπηση των log του firewall (Δεν πραγματοποιήθηκε):

- Εξέταση της διαδικασίας logging του firewall.
- Έλεγχος των ανιχνεύσεων TCP και UDP στα logs του server.
- Έλεγχος των αυτοματοποιημένων ανιχνεύσεων ευπάθειας.
- Έλεγχος των ανεπαρκών logs των υπηρεσιών.

Πληροφορίες:

- *Για τον έλεγχο του firewall χρησιμοποιήσαμε τα προγράμματα Nmap, Scanmetender και η διαδικασία περιγράφεται στην ενότητα 1.6.2*

2.6.2 Firewall features identification

Scanmetender

Το Scanmetender Standard είναι ένας πολυσύνθετος ανιχνευτής TCP/UDP και μία σουίτα ασφαλείας, που προσφέρει ένα καλό και χρήσιμο γραφικό περιβάλλον με επαγγελματικές μεθόδους. Το εργαλείο αυτό δεν είναι μόνο ικανό να ανιχνεύει πόρτες, αλλά ακόμα και να τις κλείνει. Είναι πιθανόν μια καλή επιλογή για ανιχνευτή θυρών.

Download: http://www.download.com/Scanmetender-Standard/3000-2094_4-10425122.html

- Ο απλούστερος τρόπος για να ανιχνεύσουμε τον τύπο ενός firewall είναι να εξετάσουμε αν είναι ανοιχτές συγκεκριμένες πόρτες, καθώς συγκεκριμένα firewall μπορούν να αναγνωριστούν από τις εξορισμού ανοιχτές πόρτες. Για παράδειγμα:
  - Το Firewall-1 της CheckPoint εξορισμού ακούει στις TCP πόρτες 256, 257 και 258.
  - Το Firewall NG της Checkpoint εξορισμού ακούει στις TCP πόρτες 18210, 18211, 18186, 18190, 18191 και 18192.
  - Ενώ ο Microsoft Proxy Server εξορισμού ακούει στις TCP πόρτες 1745 και 1080.

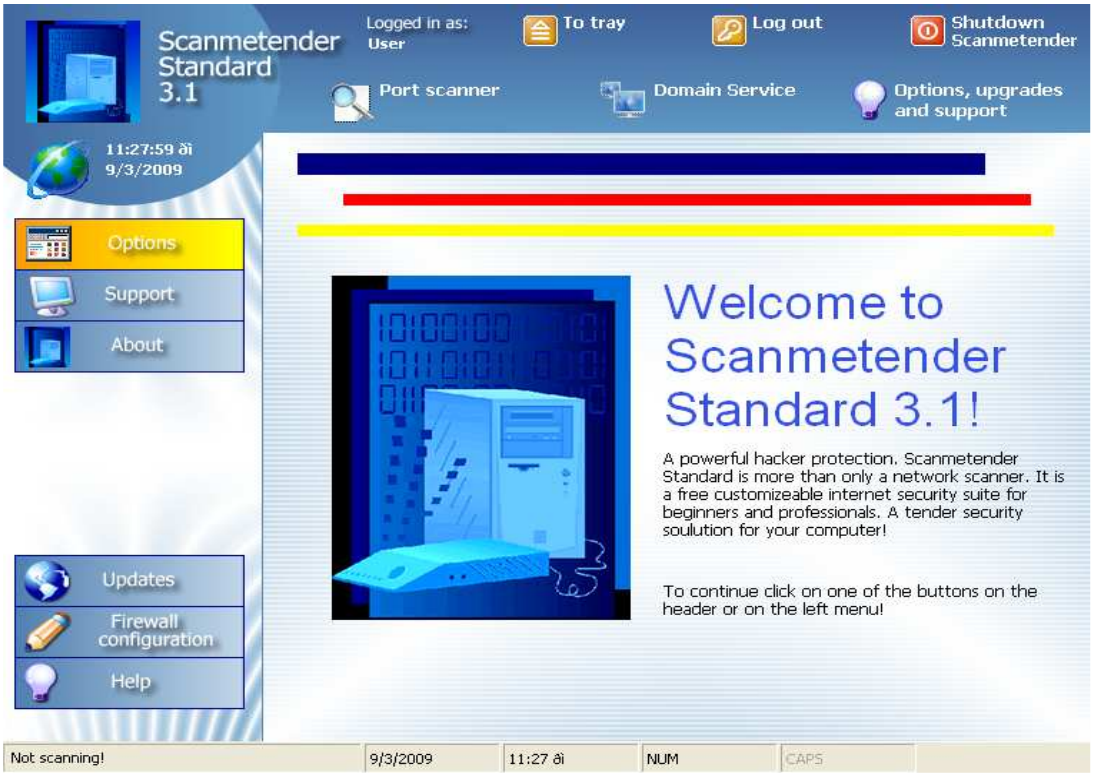
Ανοίγουμε το πρόγραμμα και συναντάμε την παρακάτω εικόνα:

Εικόνα 89 Απεικόνιση του προγράμματος Scanmetender

Στη συνέχεια επιλέγουμε Options, upgrades and support:

Εικόνα 90 Scanmetender: Επιλογή Options, upgrades and support

Επιλέγουμε Options ώστε να ρυθμίσουμε τις παραμέτρους για την ανίχνευση στο παράθυρο που ακολουθεί:



Εικόνα 91 Scanmetender:Επιλογή Options

Αρχικά θα μεταβούμε στην καρτέλα Scan και μετά θα επιλέξουμε Enter an IP ώστε να καθορίσουμε την IP διεύθυνση όπου θα γίνει η επίθεση.

Εικόνα 92 Scanmetender: Ρύθμιση παραμέτρων

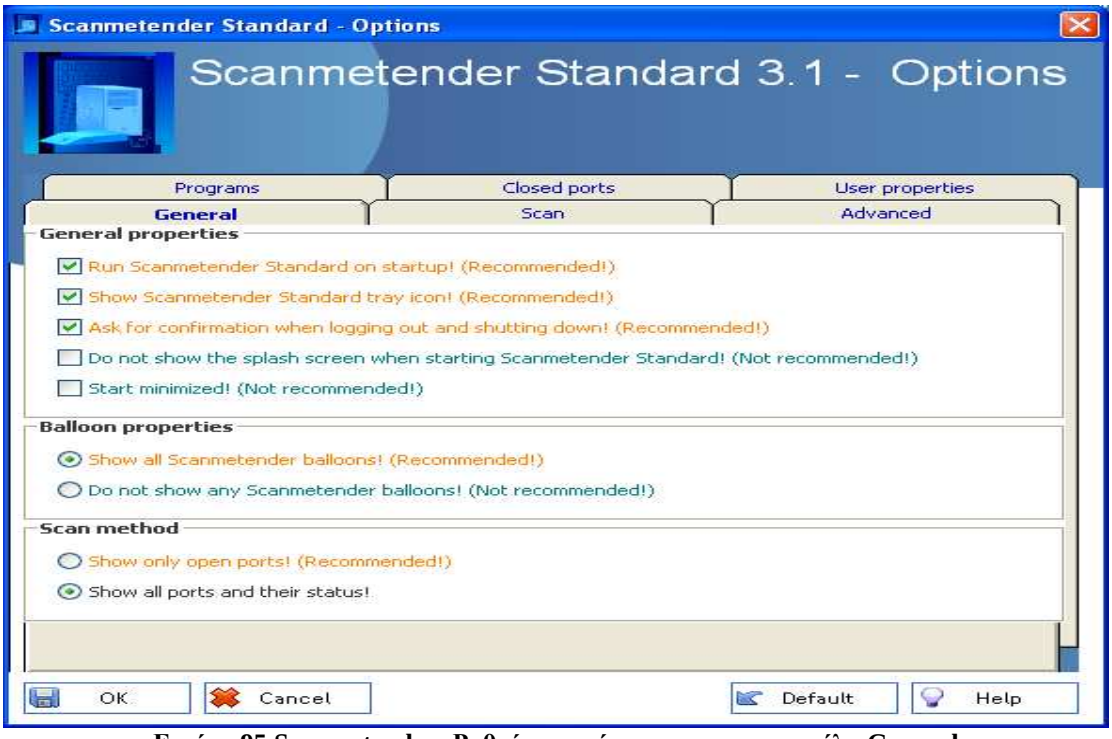
Έτσι στο επόμενο παράθυρο πληκτρολογούμε την IP διεύθυνση και πατάμε OK:

Εικόνα 93 Scanmetender: Εισαγωγή διεύθυνσης IP

Επιστρέφοντας στο προηγούμενο παράθυρο θα ορίσουμε το εύρος των πορτών όπου θα επιτευχθεί η επίθεση και επιλέγουμε OK.

Εικόνα 94 Scanmetender: Ρυθμίσεις ανίχνευσης στην καρτέλα Scan

Στην καρτέλα General έχουμε όλες τις default ρυθμίσεις εκτός από την παράμετρο Scan method:



Εικόνα 95 Scanmetender: Ρυθμίσεις ανίχνευσης στην καρτέλα General

Έπειτα θα επιλέξουμε Port Scanner όπως παρακάτω:

Εικόνα 96 Scanmetender: Επιλογή Port Scanner

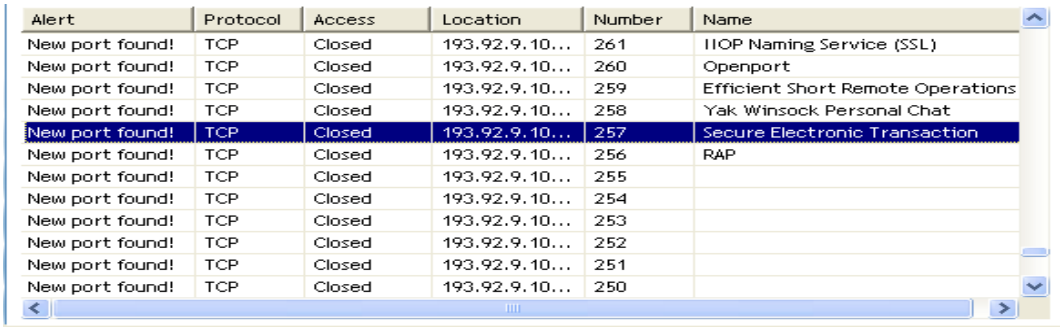
Μετά επιλέγουμε Scan όπως ακολουθεί:

Εικόνα 97 Scanmetender: Επιλογή Scan

Τέλος στο αρχικό παράθυρο αφού ορίσουμε το πρωτόκολλο της ανίχνευσης επιλέγουμε “Start scan” και η διαδικασία ξεκινάει (για epp) :

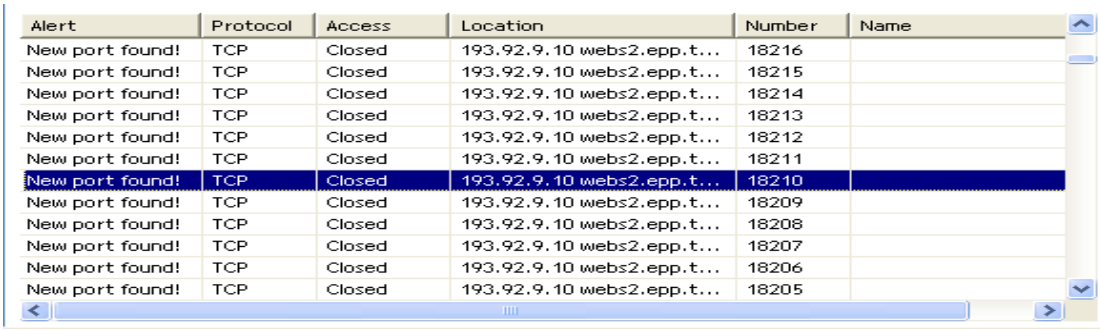
Εικόνα 98 Scanmetender: Εκκίνηση της διαδικασίας

Εφόσον ολοκληρωθεί η διαδικασία παρακάτω παρουσιάζεται για κάθε πόρτα ποια υπηρεσία τρέχει:



Alert	Protocol	Access	Location	Number	Name
New port found!	TCP	Closed	193.92.9.10...	261	IIOP Naming Service (SSL)
New port found!	TCP	Closed	193.92.9.10...	260	Openport
New port found!	TCP	Closed	193.92.9.10...	259	Efficient Short Remote Operations
New port found!	TCP	Closed	193.92.9.10...	258	Yak Winsock Personal Chat
New port found!	TCP	Closed	193.92.9.10...	257	Secure Electronic Transaction
New port found!	TCP	Closed	193.92.9.10...	256	RAP
New port found!	TCP	Closed	193.92.9.10...	255	
New port found!	TCP	Closed	193.92.9.10...	254	
New port found!	TCP	Closed	193.92.9.10...	253	
New port found!	TCP	Closed	193.92.9.10...	252	
New port found!	TCP	Closed	193.92.9.10...	251	
New port found!	TCP	Closed	193.92.9.10...	250	

Εικόνα 99 Scanmetender: Ports 256, 257, 258, 259 του epp για firewall -1



Alert	Protocol	Access	Location	Number	Name
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18216	
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18215	
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18214	
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18213	
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18212	
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18211	
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18210	
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18209	
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18208	
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18207	
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18206	
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18205	

Εικόνα 100 Scanmetender: Ports 18210, 18211 του epp για firewall NG (1/2)

Alert	Protocol	Access	Location	Number	Name
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18193	
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18192	
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18191	
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18190	
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18189	
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18188	
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18187	
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18186	
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18185	
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18184	
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18183	
New port found!	TCP	Closed	193.92.9.10 webs2.epp.t...	18182	

Εικόνα 101 Scanmetender: Ports 18186, 18190, 18191, 18192 του epp για firewall NG (2/2)

Alert	Protocol	Access	Location	Number	Name
New port found!	TCP	Closed	193.92.9.10...	1086	
New port found!	TCP	Closed	193.92.9.10...	1085	
New port found!	TCP	Closed	193.92.9.10...	1084	Anasoft License Manager
New port found!	TCP	Closed	193.92.9.10...	1083	Anasoft License Manager
New port found!	TCP	Closed	193.92.9.10...	1082	
New port found!	TCP	Closed	193.92.9.10...	1081	
New port found!	TCP	Closed	193.92.9.10...	1080	Socks
New port found!	TCP	Closed	193.92.9.10...	1079	
New port found!	TCP	Closed	193.92.9.10...	1078	
New port found!	TCP	Closed	193.92.9.10...	1077	
New port found!	TCP	Closed	193.92.9.10...	1076	
New port found!	TCP	Closed	193.92.9.10...	1075	

Εικόνα 102 Scanmetender: Port 1080 του epp για firewall Proxy server

Alert	Protocol	Access	Location	Number	Name
New port found!	TCP	Closed	193.92.9.10...	1751	SwiftNet
New port found!	TCP	Closed	193.92.9.10...	1750	Simple Socket Library's PortMaster
New port found!	TCP	Closed	193.92.9.10...	1749	aspenpservices
New port found!	TCP	Closed	193.92.9.10...	1748	oraclepem1
New port found!	TCP	Closed	193.92.9.10...	1747	ftrapidp2
New port found!	TCP	Closed	193.92.9.10...	1746	ftrapidp1
New port found!	TCP	Closed	193.92.9.10...	1745	remotepwinsock
New port found!	TCP	Closed	193.92.9.10...	1744	ncpmpft
New port found!	TCP	Closed	193.92.9.10...	1743	Cinema Graphics License Manager
New port found!	TCP	Closed	193.92.9.10...	1742	3
New port found!	TCP	Closed	193.92.9.10...	1741	ciscopnetpmgmt
New port found!	TCP	Closed	193.92.9.10...	1740	encore

Εικόνα 103 Scanmetender: Port 1745 του epp για firewall Proxy Server

Έχουμε λοιπόν για την πόρτα :

- 256: **Route Access Protocol**[9]
- 257: **Secure Electronic Transaction**[10]
- 258: **Yak Winsock Personal Chat**[11]
- 1080: **Socks**[12]
- 1745: **Remotewinsock**[13]

[9] http://www.networksorcery.com/enp/protocol/rap.htm
[10] http://en.wikipedia.org/wiki/Secure_electronic_transaction
[11] http://vbnet.mvps.org/code/internet/chat.htm
[12] http://en.wikipedia.org/wiki/SOCKS
[13] http://www.auditmypc.com/port/tcp-port-1745.asp

Στη συνέχεια η διαδικασία εφαρμόζεται για το csd τηρούμε τα βήματα και τη σειρά τους και αλλάζουμε τη διεύθυνση IP σε “147.52.16.5” και έχουμε :

Alert	Protocol	Access	Location	Number	Name
New port found!	TCP	Closed	147.52.16.5...	266	
New port found!	TCP	Closed	147.52.16.5...	265	
New port found!	TCP	Closed	147.52.16.5...	264	
New port found!	TCP	Closed	147.52.16.5...	263	HDAP
New port found!	TCP	Closed	147.52.16.5...	262	Arcisdms
New port found!	TCP	Closed	147.52.16.5...	261	IIOP Naming Service (SSL)
New port found!	TCP	Closed	147.52.16.5...	260	Openport
New port found!	TCP	Closed	147.52.16.5...	259	Efficient Short Remote Operations
New port found!	TCP	Closed	147.52.16.5...	258	Yak Winsock Personal Chat
New port found!	TCP	Closed	147.52.16.5...	257	Secure Electronic Transaction
New port found!	TCP	Closed	147.52.16.5...	256	RAP
New port found!	TCP	Closed	147.52.16.5...	255	

Εικόνα 104 Scanmetender : Ports 256, 257, 258, 259 του csd για firewall -1

Alert	Protocol	Access	Location	Number	Name
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18217	
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18216	
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18215	
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18214	
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18213	
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18212	
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18211	
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18210	
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18209	
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18208	
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18207	
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18206	

Εικόνα 105 Scanmetender : Ports 18210, 18211 του csd για firewall NG (1/2)

Alert	Protocol	Access	Location	Number	Name
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18194	
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18193	
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18192	
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18191	
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18190	
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18189	
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18188	
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18187	
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18186	
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18185	
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18184	
New port found!	TCP	Closed	147.52.16.5 ixion.csd.uo...	18183	

Εικόνα 106 Scanmetender : Ports 18186, 18190, 18191, 18192 του csd για firewall NG (2/2)

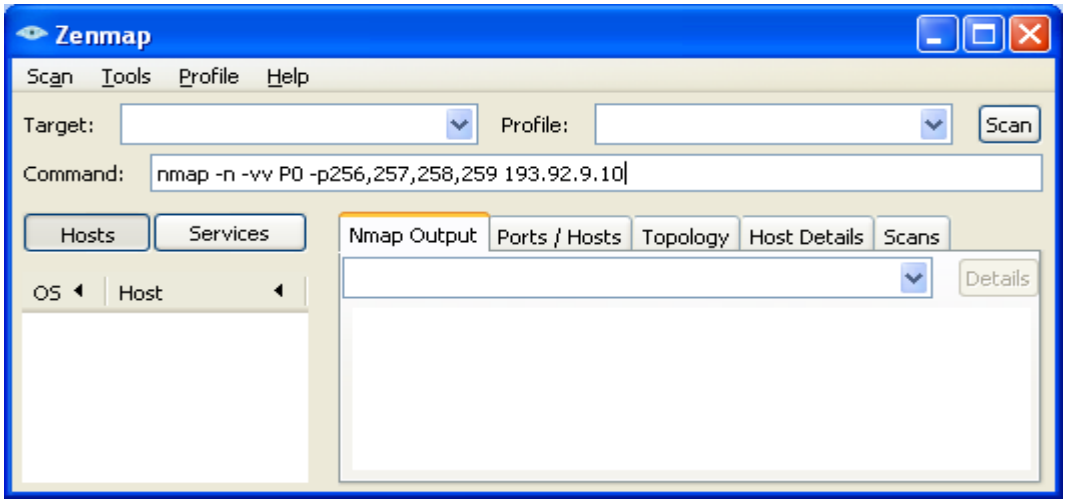
Alert	Protocol	Access	Location	Number	Name
New port found!	TCP	Closed	147.52.16.5...	1085	
New port found!	TCP	Closed	147.52.16.5...	1084	Anasoft License Manager
New port found!	TCP	Closed	147.52.16.5...	1083	Anasoft License Manager
New port found!	TCP	Closed	147.52.16.5...	1082	
New port found!	TCP	Closed	147.52.16.5...	1081	
New port found!	TCP	Closed	147.52.16.5...	1080	Socks
New port found!	TCP	Closed	147.52.16.5...	1079	
New port found!	TCP	Closed	147.52.16.5...	1078	
New port found!	TCP	Closed	147.52.16.5...	1077	
New port found!	TCP	Closed	147.52.16.5...	1076	
New port found!	TCP	Closed	147.52.16.5...	1075	
New port found!	TCP	Closed	147.52.16.5...	1074	

Εικόνα 107 Scanmetender : Port 1080 του csd για firewall Proxy Server

Alert	Protocol	Access	Location	Number	Name
New port found!	TCP	Closed	147.52.16.5...	1750	Simple Socket Library's PortMaster
New port found!	TCP	Closed	147.52.16.5...	1749	aspenpservices
New port found!	TCP	Closed	147.52.16.5...	1748	oraclepem1
New port found!	TCP	Closed	147.52.16.5...	1747	ftrapidp2
New port found!	TCP	Closed	147.52.16.5...	1746	ftrapidp1
New port found!	TCP	Closed	147.52.16.5...	1745	remotepwinsock
New port found!	TCP	Closed	147.52.16.5...	1744	ncpmpft
New port found!	TCP	Closed	147.52.16.5...	1743	Cinema Graphics License Manager
New port found!	TCP	Closed	147.52.16.5...	1742	3
New port found!	TCP	Closed	147.52.16.5...	1741	ciscopnetpmgmt
New port found!	TCP	Closed	147.52.16.5...	1740	encore
New port found!	TCP	Closed	147.52.16.5...	1739	webaccess

Εικόνα 108 Εικόνα 85 Scanmetender : Port 1745 του csd για firewall Proxy Server

Στη συνέχεια ανοίγουμε το πρόγραμμα nmap και με τα ανάλογα ορίσματα μπορούμε να ελέγξουμε αν υπάρχουν τα συγκεκριμένα firewall. Για να ελέγξουμε αν το firewall που χρησιμοποιείται είναι το Firewall -1 πληκτρολογούμε στο Command την εντολή όπως παρακάτω (για epp) :

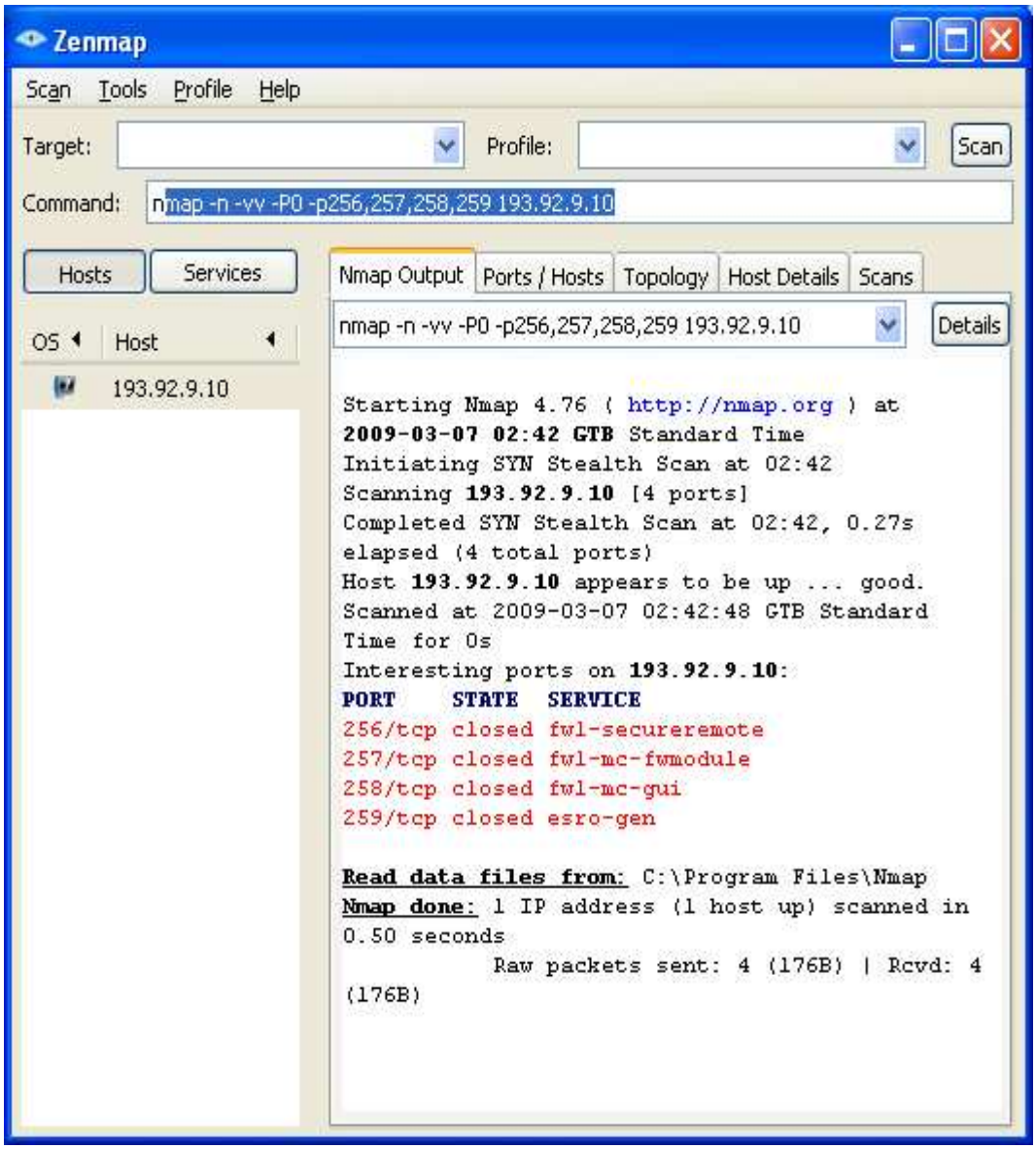


Εικόνα 109 Nmap: Πληκτρολόγηση της εντολής του epp για firewall -1

Με τις παραμέτρους:

- –n δεν θα γίνει ανάλυση του DNS
- -vv έχουμε μια πάρα πολύ λεπτομερή παρουσίαση των αποτελεσμάτων.
- -PO κάνουμε ping .
- -p η ανίχνευση γινεται σε συγκεκριμένες πόρτες.

Επιλέγοντας “Scan” θα ξεκινήσει η διαδικασία όπου θα πάρουμε τα παρακάτω αποτελέσματα:

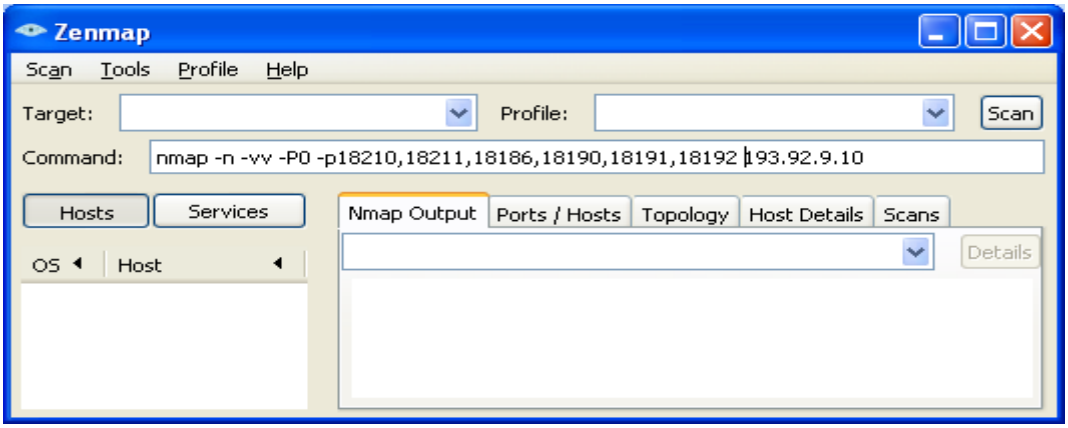


Εικόνα 110 Nmap: Παρουσίαση αποτελεσμάτων της ανίχνευσης του epp για firewall -1

Πληροφορούμαστε για:

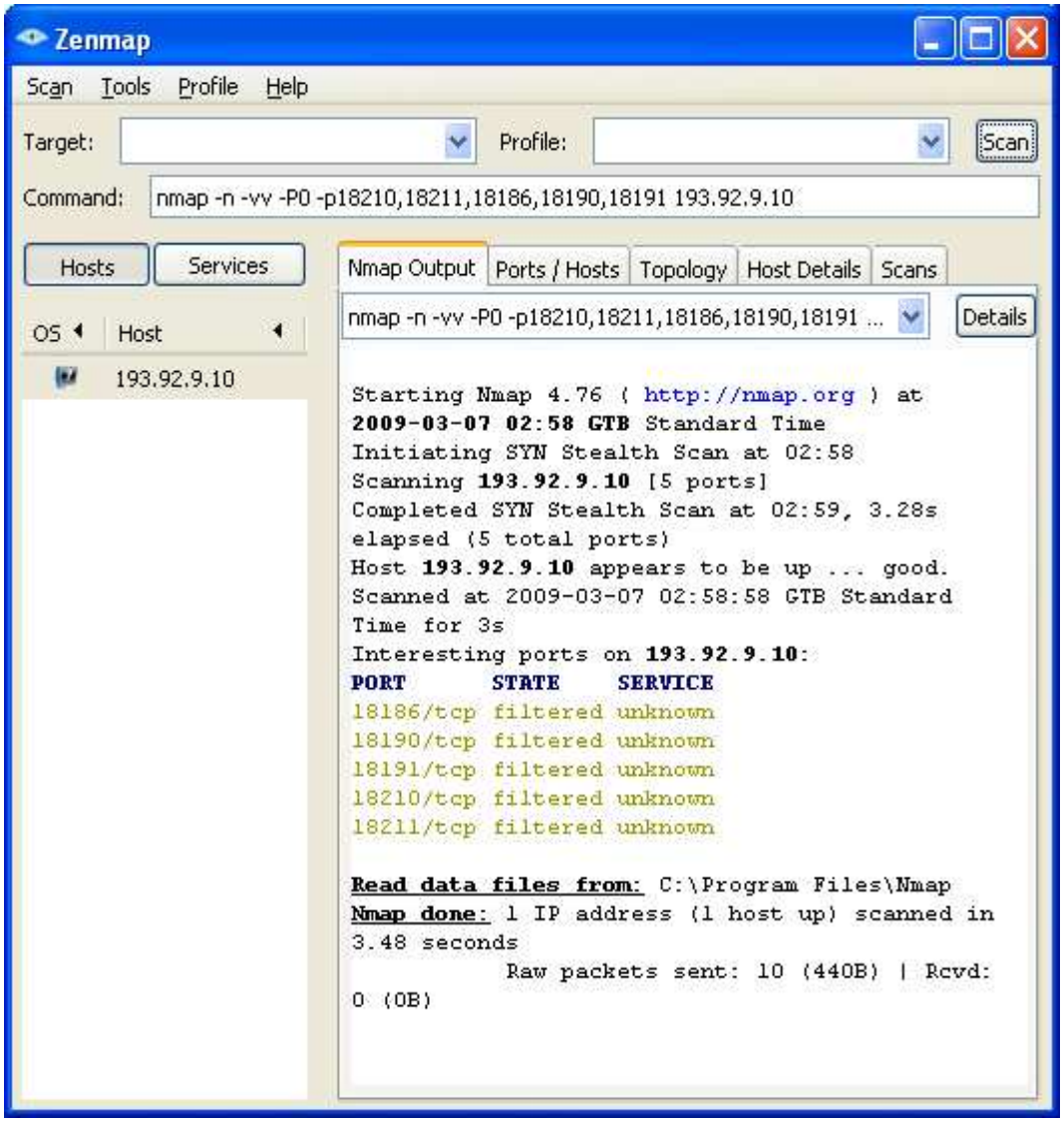
- Τον τύπο της ανίχνευσης (SYN Stealth Scan) όπου εντοπίζει ενεργές πόρτες χωρίς να εγκαθιδρύσει σύνδεση.
- Την πόρτα στην οποία έγινε η επίθεση.
- Την κατάσταση της.
- Την υπηρεσία που τρέχει πίσω από τη συγκεκριμένη πόρτα.

Για να ελέγξουμε αν το firewall που χρησιμοποιείται είναι το Firewall NG πληκτρολογούμε στο Command την εντολή όπως παρακάτω:



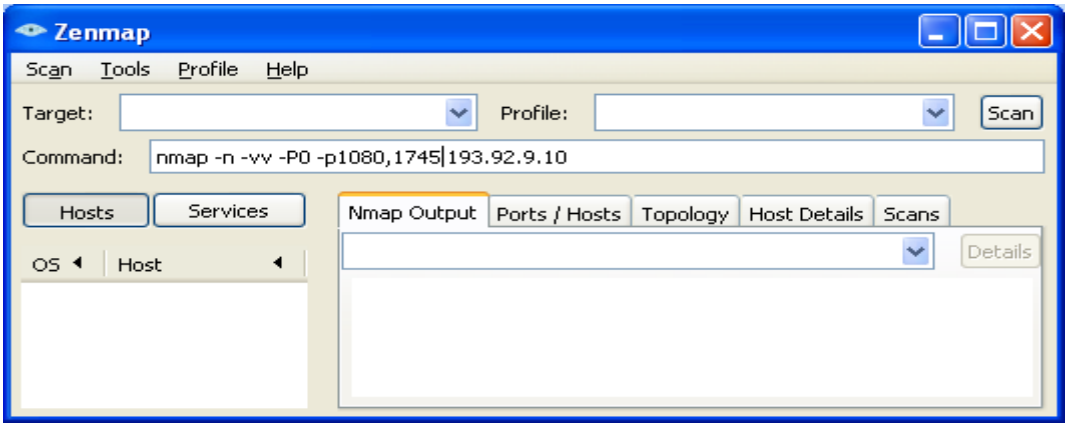
Εικόνα 111 Nmap: Πληκτρολόγηση της εντολής του epp για firewall NG

Έχουμε λοιπόν τα παρακάτω αποτελέσματα:



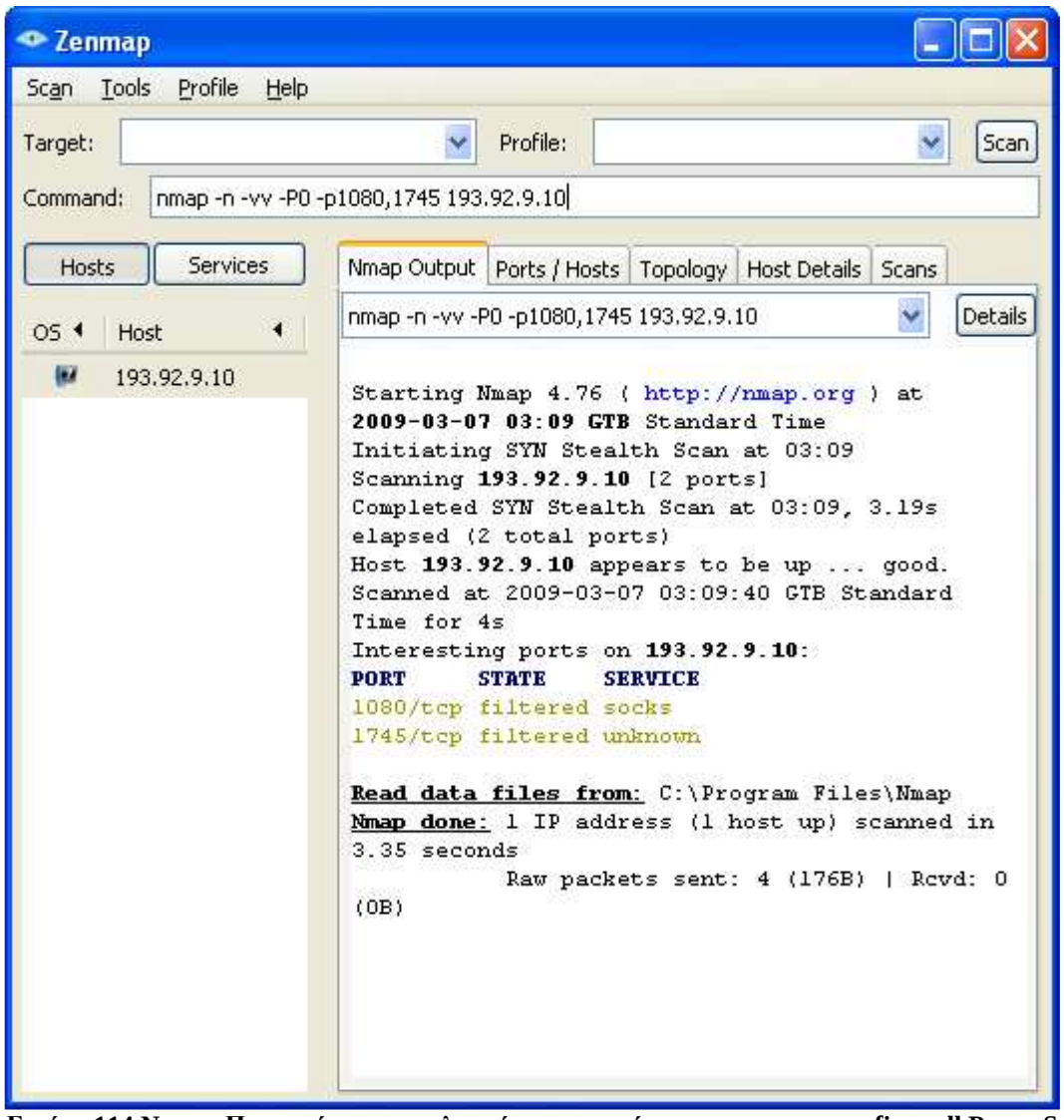
Εικόνα 112 Nmap: Παρουσίαση αποτελεσμάτων της ανίχνευσης του epp για firewall NG

Για να ελέγξουμε αν το firewall που χρησιμοποιείται είναι το Microsoft Proxy Server πληκτρολογούμε στο Command την εντολή όπως παρακάτω:



Εικόνα 113 Nmap: Πληκτρολόγηση της εντολής του epp για firewall Proxy Server

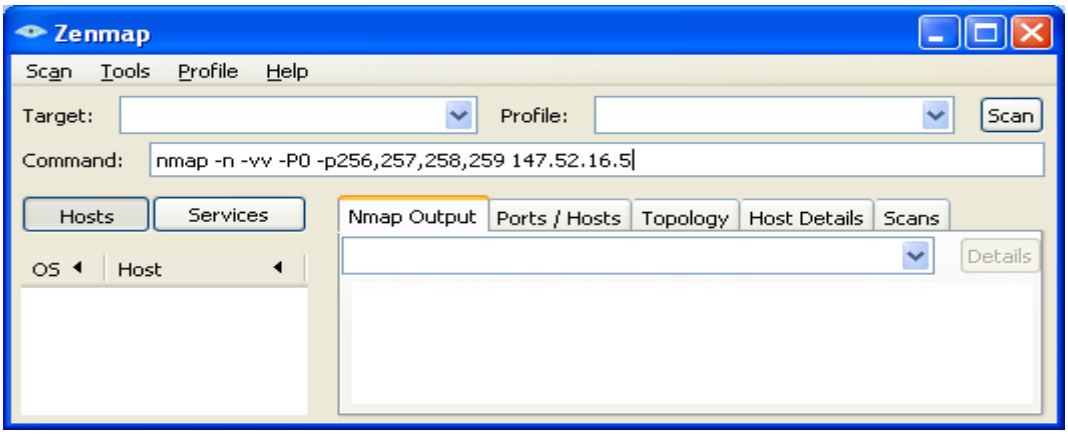
Έχουμε λοιπόν τα αποτελέσματα που ακολουθούν:



Εικόνα 114 Nmap: Παρουσίαση αποτελεσμάτων της ανίχνευσης του epp για firewall Proxy Server

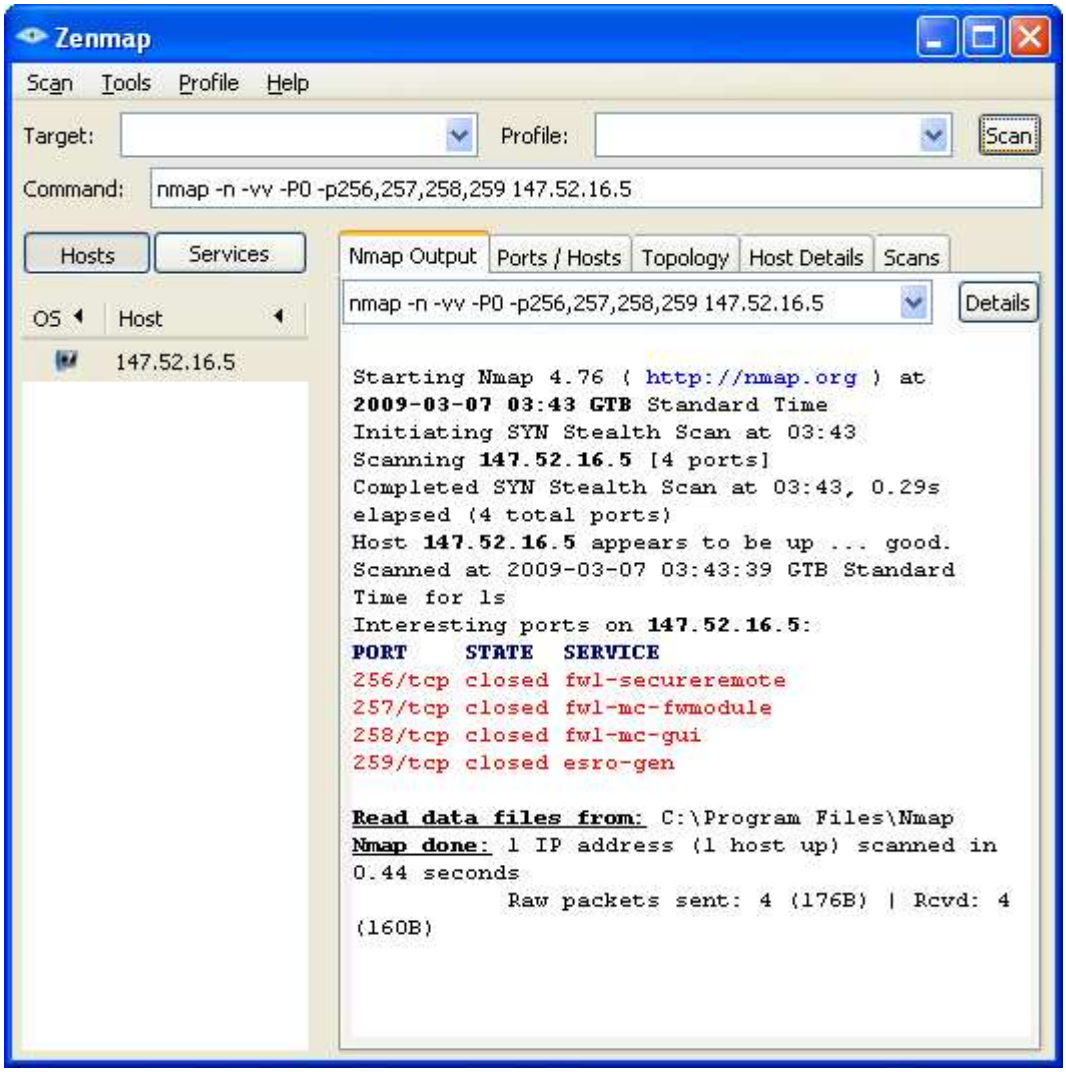
Τηρώντας τα ίδια βήματα και τη σειρά τους η διαδικασία θα εφαρμοστεί και για το csd.

- Checkpoint Firewall -1



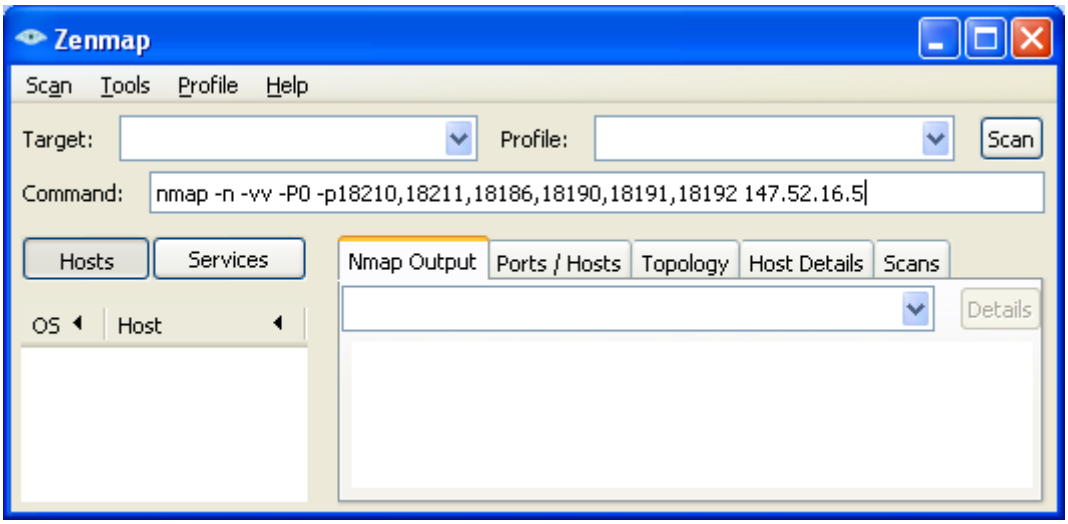
Εικόνα 115 Nmap: Πληκτρολόγηση της εντολής του csd για firewall -1

- Αποτελέσματα



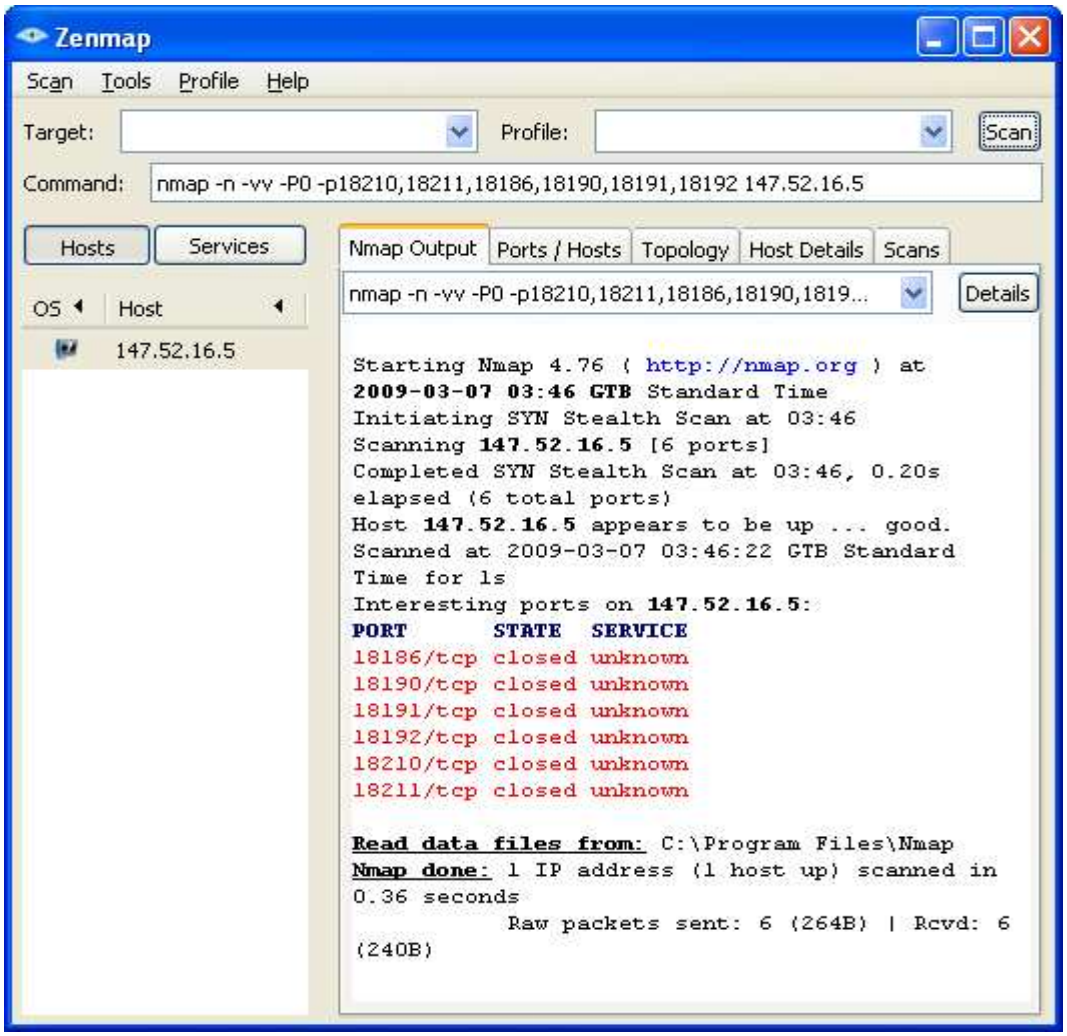
Εικόνα 116 Nmap: Παρουσίαση αποτελεσμάτων της ανίχνευσης του csd για firewall -1

- Checkpoint firewall NG



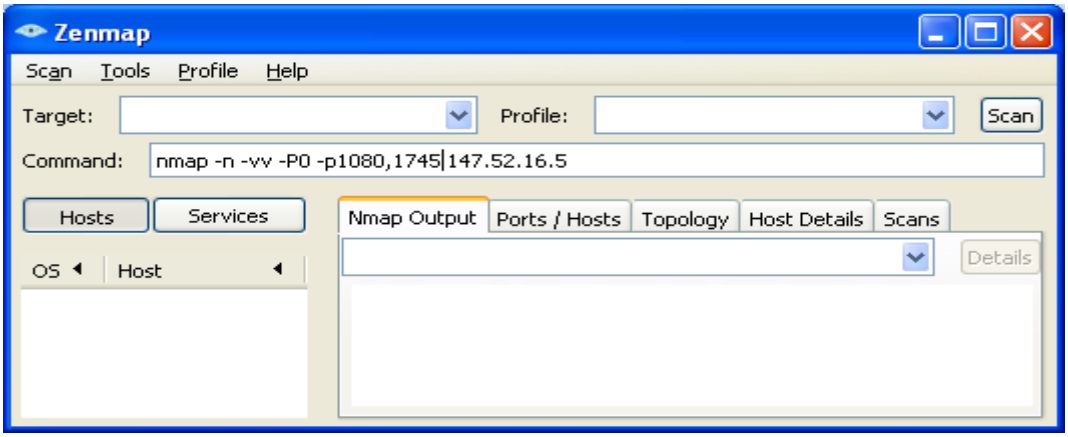
Εικόνα 117 Nmap: Πληκτρολόγηση της εντολής του csd για firewall NG

- Αποτελέσματα



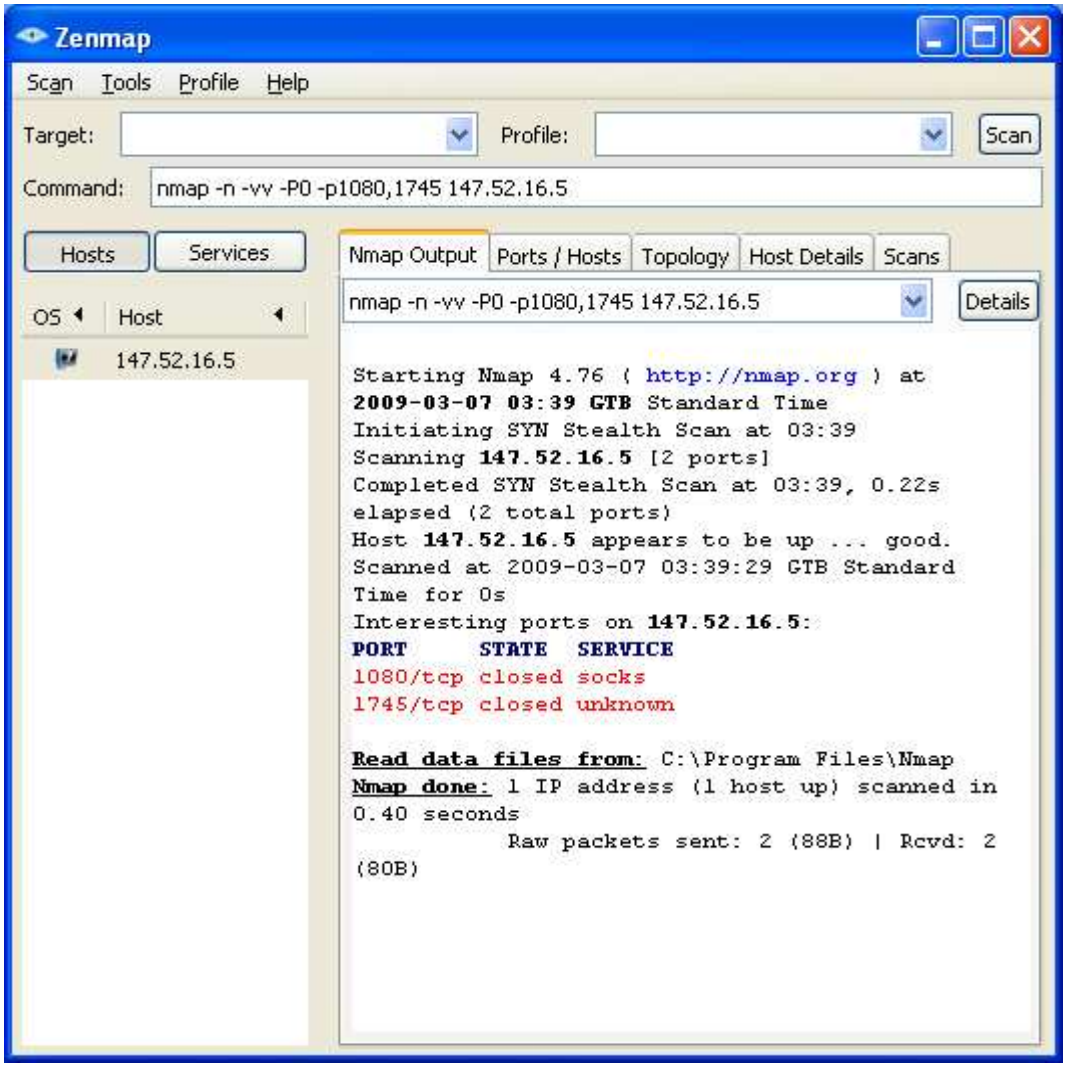
Εικόνα 118 Nmap: Παρουσίαση αποτελεσμάτων της ανίχνευσης του csd για firewall NG

- Microsoft Proxy Server



Εικόνα 119 Nmap: Πληκτρολόγηση της εντολής του csd για firewall Proxy Server

- Αποτελέσματα



Εικόνα 120 Nmap : Παρουσίαση αποτελεσμάτων της ανίχνευσης του cad για firewall Proxy Server

Με βάση τα αποτελέσματα συμπαιρένουμε λοιπόν πως και οι δυο Server χρησιμοποιούν το τείχος προστασίας: Checkpoint firewall -1.

2.6.3 Checkpoint firewall -1 vulnerabilities

- Remote Management
  - There is a weakness in the logic used for firewall to firewall communications - the IP of the supposed real management console is not checked at layer 3, but instead at layer 7. This means that if someone can authenticate to a firewall module somehow, they can come from any arbitrary IP and trick the firewall module into thinking that the attacker's machine is its management console.

- S/Key
  - The S/Key authentication mechanism used by 4.0 and below (default for v.3.0, but also used occasionally in 4.0) can be trivially brute-forced. This, combined with the first finding, means that an attacker could have all they need to remotely control your firewall - provided you are using S/Key authentication, set by your $FWDIR/lib/control.map file, and that your policy allows connections to TCP port 256 (i.e., "Accept Firewall-1 Control Connections" box is checked in the firewall properties dialog.) In their example, Thomas Lopatic of TUV Data Protect issued the command to remotely unload the firewall policy so that he could then circumvent all security controls.

- fwn1
  - fwn1 authentication was also found to be trivially cracked using other methods, allowing the same remote policy unloading capabilities.

- fwa1 fw-to-fw authentication
  - They also broke fwa1 fw-to-fw authentication, but since that authentication also includes some encrypted communications, they were not able to fully authenticate. Thus, 4.1 looks "okay" for now (since some 4.0 and all 4.1 versions use fwa1 by default).

- FTP PORT and PASV command
  - Another variant of both the FTP PORT and PASV command handling vulnerabilities was also found, which allowed vulnerable servers behind the firewall to be compromised under certain conditions.

- one -way connection
  - There is also a problem with one-way connection handling, in which fw-1 really allows two-way traffic if TCP header and TCP payload are split into two separate packets.

- FWZ
  - Found problems with FWZ encapsulation which could allow connection spoofing.

- RSH Error
  - They also figured out that RSH Error connections weren't properly handled, which allowed them to connect to certain protected hosts via any UDP port (assuming spoof tracking was not turned on).

- spoof tracking
  - Found a problem with fw-1's spoof tracking, in which you could use multicast addressing to connect to protected hosts, under certain circumstances.

- "fastmode" services
  - They also pointed out the security vulnerabilities inherent to the use of "fastmode" services.

2.7 Password Cracking

2.7.1 Περιγραφή

Το password cracking είναι μια διαδικασία επικύρωσης της «ισχύος» ενός συνθηματικού μέσω της χρήσης αυτοματοποιημένων εργαλείων ανάκτησης συνθηματικών τα οποία εκθέτουν είτε τις εφαρμογές με αδύναμους κρυπτογραφικούς αλγόριθμους, είτε τη λανθασμένη εφαρμογή αυτών, ή και τους αδύναμους κωδικούς λόγω ανθρώπινων παραγόντων. Αυτή η ενότητα δεν θα πρέπει να συγχέεται με την επαναφορά κωδικών μέσω sniffing ,η οποία μπορεί να έχει μια πιο απλή σημασία της υπονόμευσης της ασφάλειας συστημάτων, εξαιτίας μη κρυπτογραφημένων μηχανισμών γνησιότητας, και όχι της ίδιας της αδυναμίας του συνθηματικού. [Σημείωση: Αυτή η ενότητα μπορεί να περιέχει μη-αυτοματοποιημένες τεχνικές εύρεσης συνθηματικών, οι οποίες χρησιμοποιούν προεπιλεγμένους συνδυασμούς όνομα χρήστη και συνθηματικού σε λειτουργικά συστήματα π.χ.Username:System,Password:Test ή εύκολα στην εύρεση συνθηματικών από λάθος χειρισμό του χρήστη(π.χ. Username: joe, Password: joe). Αυτός μπορεί να είναι αρχικά ένας τρόπος ώστε να γίνει εφικτή η πρόσβαση σε ένα σύστημα, ίσως και σαν administrator ή σαν root access. Πέρα από τις μη-αυτοματοποιημένες τεχνικές ευρέσεως συνθηματικού με απλούς ή μη-αυτοματοποιημένους συνδυασμούς, η θηριώδεις δύναμη των κωδικών σε εφαρμογές όπως το Telnet χρησιμοποιώντας scripts ή custom programs, είναι σχεδόν ακατόρθωτο εξαιτίας των προστατευμένων τιμών του timeout, ακόμα και με την πολύ-συνδεσιμότητα.

Έχοντας αποκτήσει administrator ή root δικαιώματα σε ένα υπολογιστικό σύστημα, το password cracking μπορεί να συμβάλλει στην απόκτηση πρόσβασης και σε επιπρόσθετα συστήματα ή και εφαρμογές και είναι μια έγκυρη τεχνική που μπορεί να χρησιμοποιηθεί σε συστήματα μόχλευσης διαμέσου ενός τεστ ασφαλείας. Λεπτομερές ή corporate - wide password cracking μπορεί επίσης να εφαρμοστεί ως μια απλή μετά-δραστήρια άσκηση και μπορεί να προβάλλει την ανάγκη για ισχυρότερους αλγόριθμους κρυπτογράφησης για την αποθήκευση των συνθηματικών σε συστήματα σε βασικά συστήματα, καθώς και να προβάλλει την ανάγκη για την ενίσχυση της χρήσης ισχυρότερων συνθηματικών μέσω αυστηρότερης πολιτικής, αυτόματης παραγωγής, ή σφραγισμένης γνησιότητας των ενοτήτων(PAMs).

Αναμενόμενα αποτελέσματα:

- Το αρχείο των συνθηματικών να είναι ”σπασμένο” ή ”μη σπασμένο”
- Λίστα καταγεγραμμένων ταυτοτήτων με συνθηματικό χρήστη ή συστήματος
- Λίστα συστημάτων ευαίσθητα σε επιθέσεις
- Λίστα από έγγραφα ή αρχεία ευαίσθητα σε επιθέσεις
- Λίστα συστημάτων με ταυτότητες χρήστη ή συστήματος που χρησιμοποιούν τους ίδιους κωδικούς

Βήματα που εφαρμόζονται για την ανάκτηση των συνθηματικών:

- Αναζήτηση του αρχείου των συνθηματικών του συστήματος που αποθηκεύει τα ονόματα των χρηστών και τους αντίστοιχους κωδικούς τους
    - Σε UNIX συστήματα το αρχείο μπορεί να είναι είτε το etc/password είτε το etc/shadow

  - Σε UNIX συστήματα αυτό συμβαίνει για να επιτευχθεί η γνησιότητα του SMB, τα συνθηματικά NT μπορούν να βρεθούν στο etc/smbpasswd
  - Σε NT συστήματα το αρχείο μπορεί να είναι στο /winnt/repair/Sam._(ή και σε άλλο που όμως είναι δυσκολότερη η ανάκτηση των συνθηματικών)
- Υλοποιούμε μια επίθεση της μορφής dictionary στο αρχείο με τα συνθηματικά
- Υλοποιούμε μια επίθεση της μορφής brute-force στο αρχείο με τα συνθηματικά, όσο ο χρόνος και οι κύκλοι της επεξεργασίας το επιτρέπουν
- Χρήση των ανακτημένων συνθηματικών ή των παραλλαγών τους για την πρόσβαση σε επιπλέον συστήματα ή διαδικασίες
- Χρήση αυτοματοποιημένων προγραμμάτων(password crackers) σε μη κρυπτογραφημένα αρχεία τα οποία αντιμετωπίζονται(αρχεία όπως PDF ή Word)σε μια προσπάθεια να αποκτήσουν περισσότερη νοημοσύνη και να επισημάνουν την ανάγκη για ισχυρότερη κρυπτογράφηση σε αρχεία και σε συστήματα αρχείων

Πληροφορίες:

- *Για την ανάκτηση των κωδικών σε αρχεία PDF χρησιμοποιήσαμε το πρόγραμμα PDF Password Cracker Pro και η διαδικασία περιγράφεται στην ενότητα 1.7.2*

- *Για την ανάκτηση των κωδικών των χρηστών σε Windows χρησιμοποιήσαμε το πρόγραμμα Cain & Avel και η διαδικασία περιγράφεται στην ενότητα 1.7.3*

- *Για την ανάκτηση των κωδικών των χρηστών σε Unix χρησιμοποιήσαμε το πρόγραμμα John the Ripper και η διαδικασία περιγράφεται στην ενότητα 1.7.4*

2.7.2 Password Cracking on PDF files

Pdf Password Cracker Pro

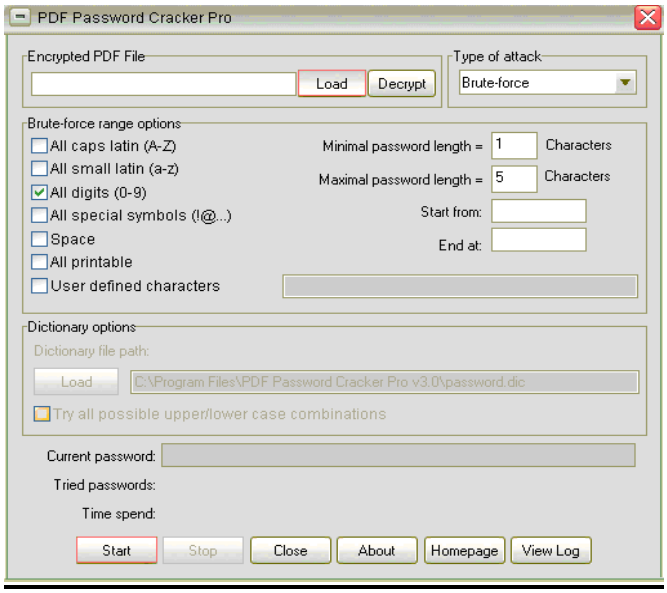
Το PDF Password Cracker Pro επιτρέπει την αναζήτηση κωδικών του κατόχου και των χρηστών αυτού με την εφαρμογή επιθέσεων τύπου brute-force και dictionary attack, αποτελεσματικά βελτιστοποιημένο για ταχύτητα. Ακόμα παρέχει την επίθεση αναζήτησης κλειδιού, η οποία εγγυάται την αποκρυπτογράφηση(άσχετα από το μήκος και την πολυπλοκότητα του κωδικού πρόσβασης) των αρχείων PDF που χρησιμοποιούν κρυπτογράφηση 40-bit.

Download: http://www.download.com/PDF-Password-Cracker-Pro/3000-2092_4-10558411.html

Παρακάτω γίνεται η τοποθέτηση του κωδικού που μας στάλθηκε ηλεκτρονικά για να χρησιμοποιήσουμε την πλήρη έκδοση του προγράμματος.

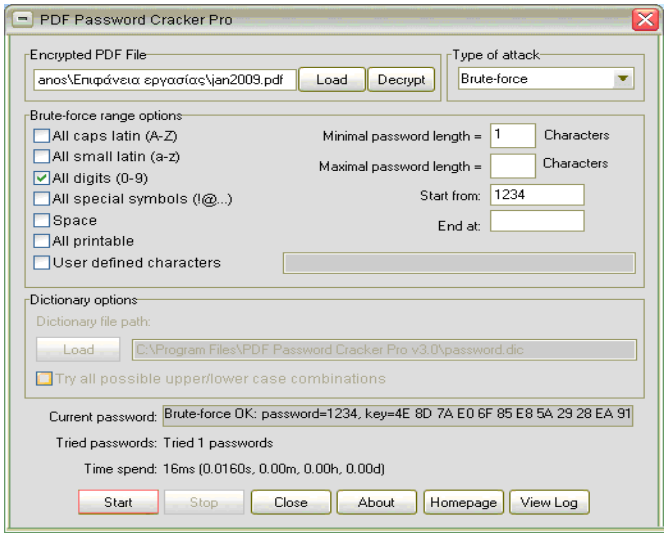
Εικόνα 121 Pdf Password Cracker Pro : Εισαγωγή License Key

Στη συνέχεια ανοίγουμε το πρόγραμμα και συναντάμε την παρακάτω εικόνα όπου σε αυτό το σημείο θα πρέπει να ορίσουμε το αρχείο από το οποίο θα γίνει η ανάκτηση του κωδικού, τον τύπο της επίθεσης, την πολυπλοκότητα και το μήκος του κωδικού. Τέλος θα επιλέξουμε “Start” και η διαδικασία ανάκτησης του κωδικού θα ξεκινήσει.



Εικόνα 122 Pdf Password Cracker Pro : Απεικόνιση του προγράμματος και ρύθμιση παραμέτρων

Στην παρακάτω εικόνα βλέπουμε ότι έχουν εφαρμοστεί όσα αναφέρθηκαν παραπάνω. Τώρα παρατηρούμε στο πεδίο κειμένου Current Password ότι περιγράφει το είδος της επίθεσης που εφαρμόστηκε τον κωδικό και το κλειδί. Άρα έχουμε καταφέρει να ανακτήσουμε τα δεδομένα που θέλαμε



Εικόνα 123 Pdf Password Cracker Pro : Εμφάνιση αποτελεσμάτων

Εδώ παρουσιάζεται η αναφορά της διαδικασίας που εκτελέσαμε.

File name	jan2009
File type	pdf
Crack time	0.015 sec
Username	-----
Password	12345

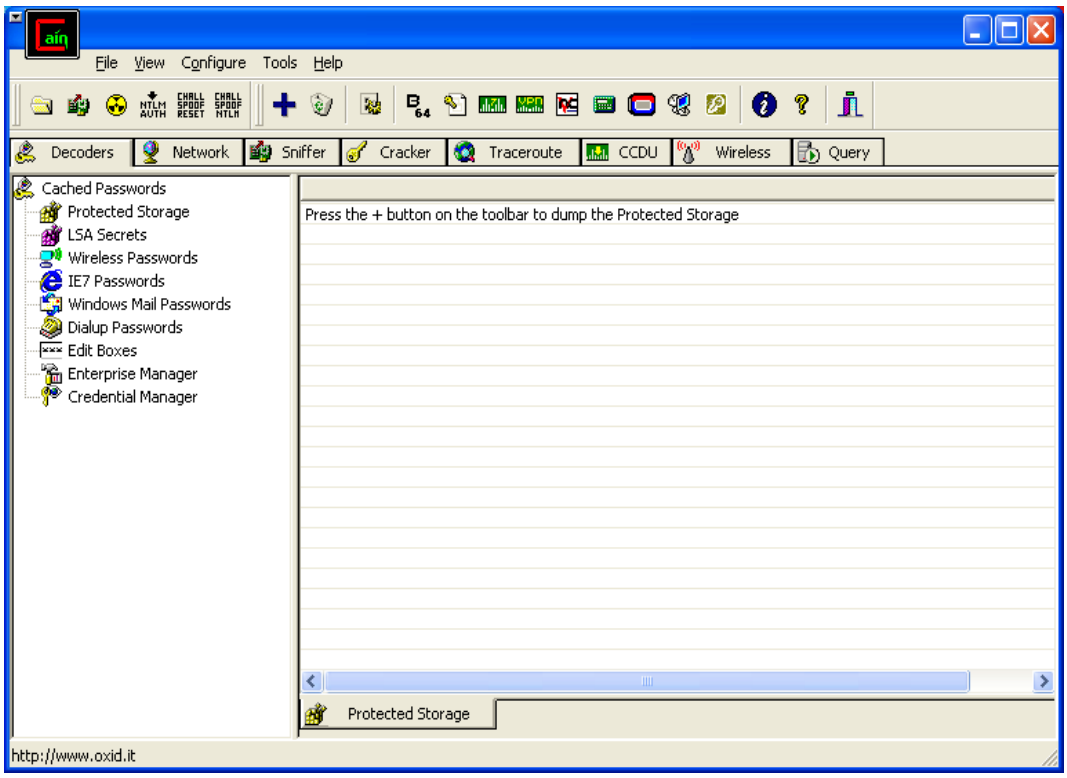
2.7.3 Password Cracking on Windows

Cain & Avel

Είναι ένα ελεύθερο εργαλείο ανάκτησης κωδικών πρόσβασης για τα λειτουργικά συστήματα της Microsoft. Επιτρέπει την εύκολη αποκατάσταση των διάφορων κωδικών πρόσβασης με την καταγραφή (Sniff) του δικτύου, σπάσιμο των κρυπτογραφημένων κωδικών πρόσβασης χρησιμοποιώντας τις επιθέσεις με χρήση λεξικού , ανακατωμένοι κωδικοί πρόσβασης αποκωδικοποίησης, αποκάλυψη παραθύρων κωδικού πρόσβασης, αποκάλυψη των εναποθηκευμένων κωδικών πρόσβασης και ανάλυση των πρωτοκόλλων δρομολόγησης. Ο κώδικας πηγής δεν παρέχεται.

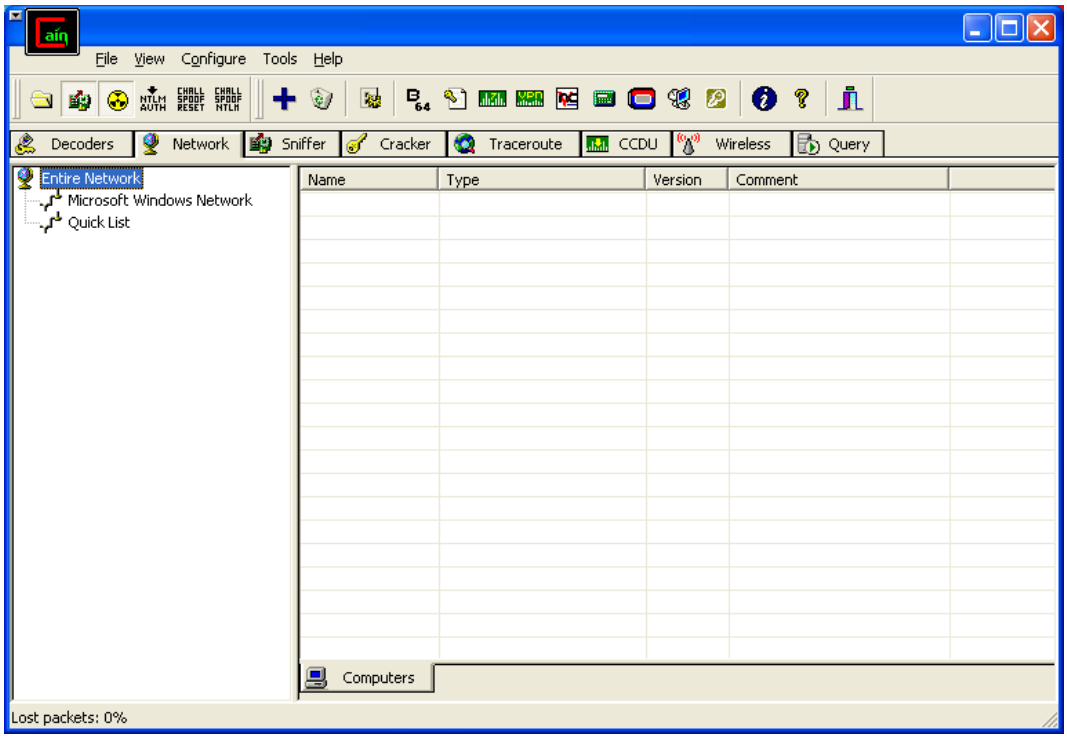
Download: http://www.oxid.it/cain.html

Ανοίγουμε το πρόγραμμα το οποίο απεικονίζεται ως εξής:



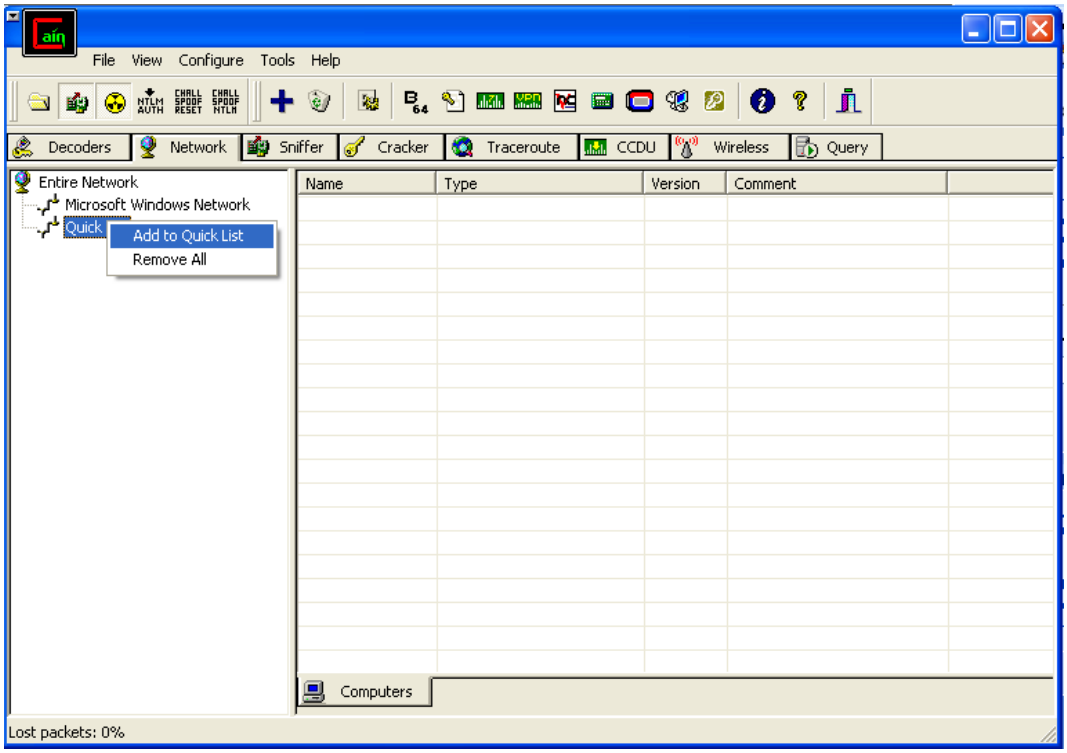
Εικόνα 124 Cain & Avel : Απεικόνιση του προγράμματος

Εφόσον η επίθεση που θέλουμε να εφαρμόσουμε θα πραγματοποιηθεί σε τοπικό επίπεδο θα πρέπει να επιλεγεί η καρτέλα Network. Κατόπιν θα εμφανιστούν οι επιλογές Microsoft Windows Network και Quick List.



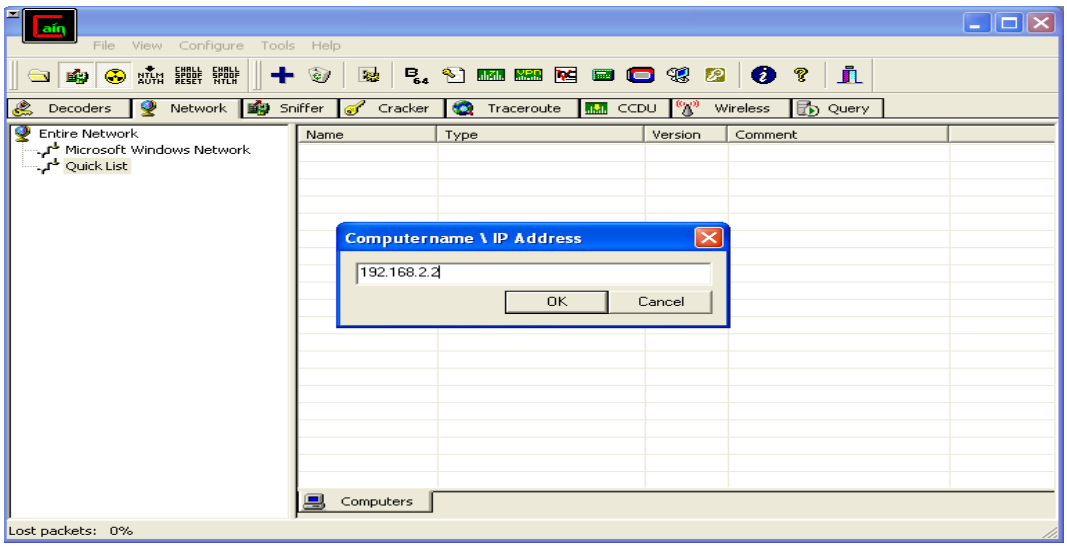
Εικόνα 125 Cain & Avel : Επιλογή της καρτέλας Network

Όπως βλέπουμε και στην παρακάτω εικόνα θα πρέπει να επιλέξουμε Add to Quick List ώστε να προσθέσουμε την διεύθυνση IP στην οποία θα γίνει η επίθεση.



Εικόνα 126 Cain & Avel : Επιλογή πρόσθεσης μιας IP διεύθυνσης στη λίστα

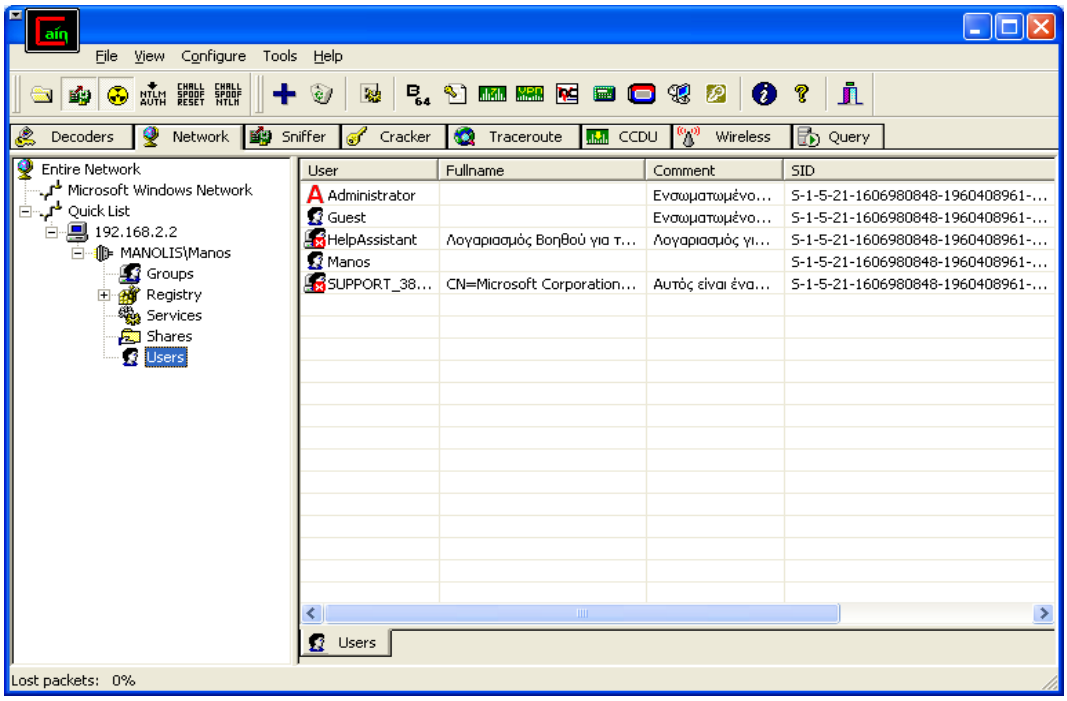
Έτσι εμφανίζεται το επόμενο παράθυρο που πληκτρολογούμε την ζητούμενη διεύθυνση IP.



Εικόνα 127 Cain & Avel : Πληκτρολόγηση διεύθυνσης IP

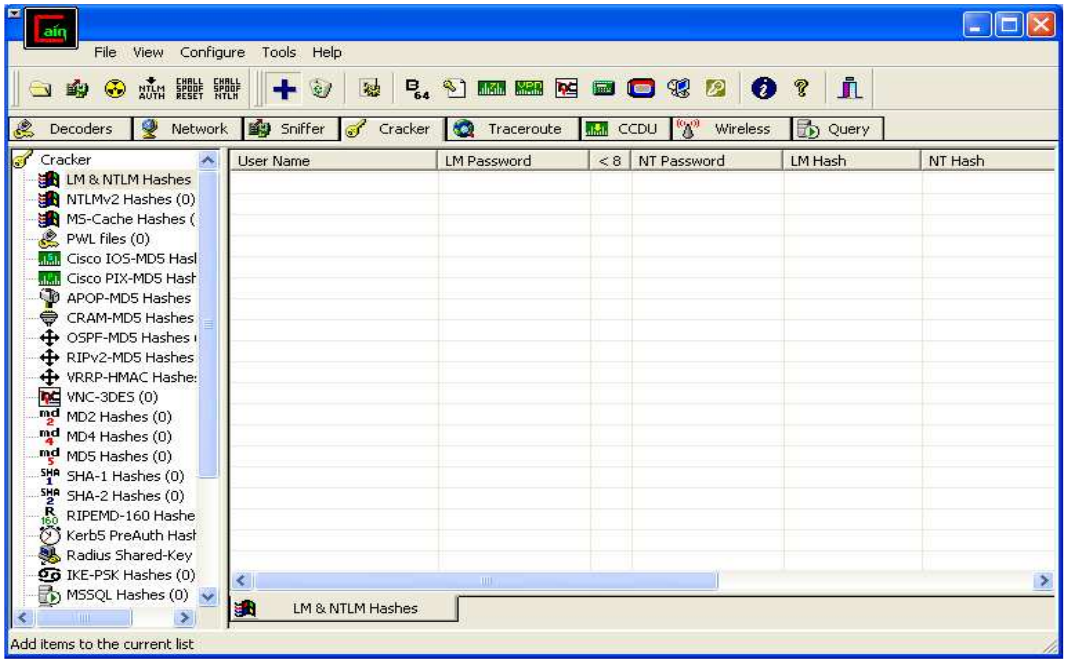
Αφού προστεθεί στη λίστα μας θα επιλέξουμε Users όπου θα εμφανιστούν τα ονόματα των χρηστών που έχουν λογαριασμό σε εκείνο τον υπολογιστή. Οι λογαριασμοί αυτοί (σε Windows) βρίσκονται στο αρχείο Sam.

- Το αρχείο Security Account Manager είναι μια βάση δεδομένων όπου αποθηκεύεται ως αρχείο registry σε Windows NT, Windows 2000 και σε επόμενες εκδόσεις των Windows. Αποθηκεύει τους κωδικούς των χρηστών σε hashed format (σε LM και NTLM hash). Δεδομένου ότι μια hash λειτουργία είναι μονόδρομη, αυτό παρέχει κάποιο μέτρο ασφάλειας για την αποθήκευση των κωδικών πρόσβασης.



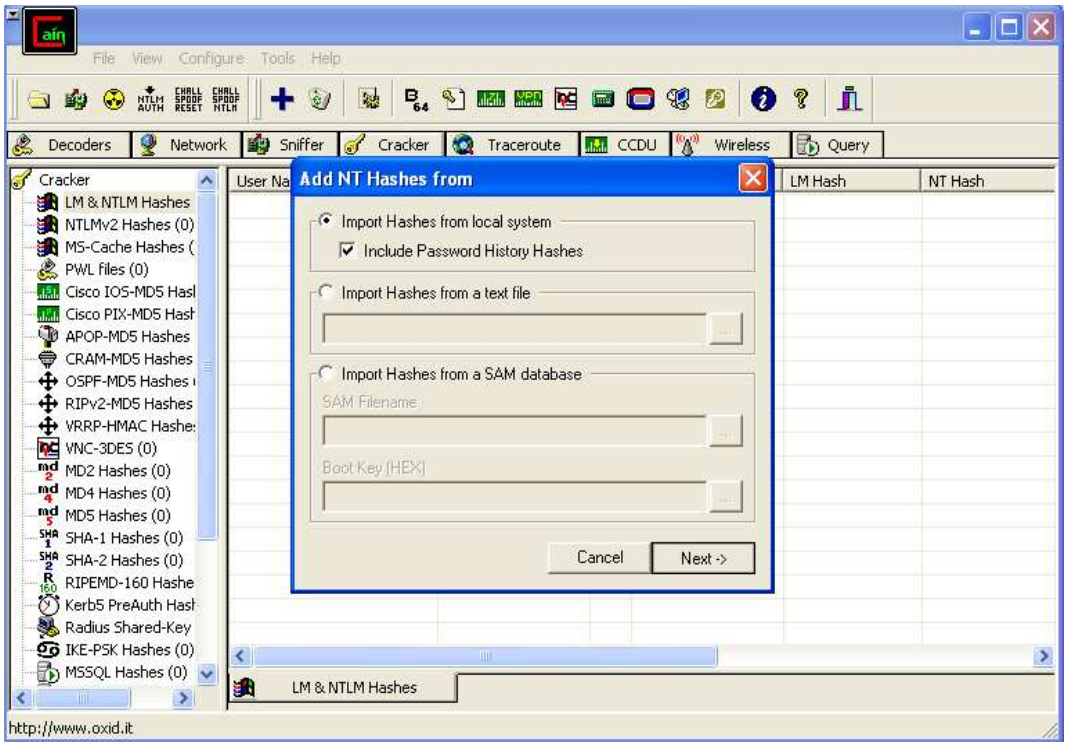
Εικόνα 128 Cain & Avel : Εμφάνιση των λογαριασμών των χρηστών του Η/Υ

Προχωράμε λοιπόν στο μέρος όπου θα ανακτήσουμε τους κωδικούς πρόσβασης των αντίστοιχων συνθηματικών. Έτσι λοιπόν σε αυτό το σημείο επιλέγουμε την επιλογή Cracker όπου εκεί θα εισαγάγουμε το αρχείο με τα συνθηματικά όπου θα ανακτηθούν το αρχείο Sam δηλαδή. Έχουμε λοιπόν προσδιορίσει στο πρόγραμμα τι θέλουμε να κάνουμε, για να προστεθεί το αρχείο θα πρέπει να κλικάρουμε το «+».



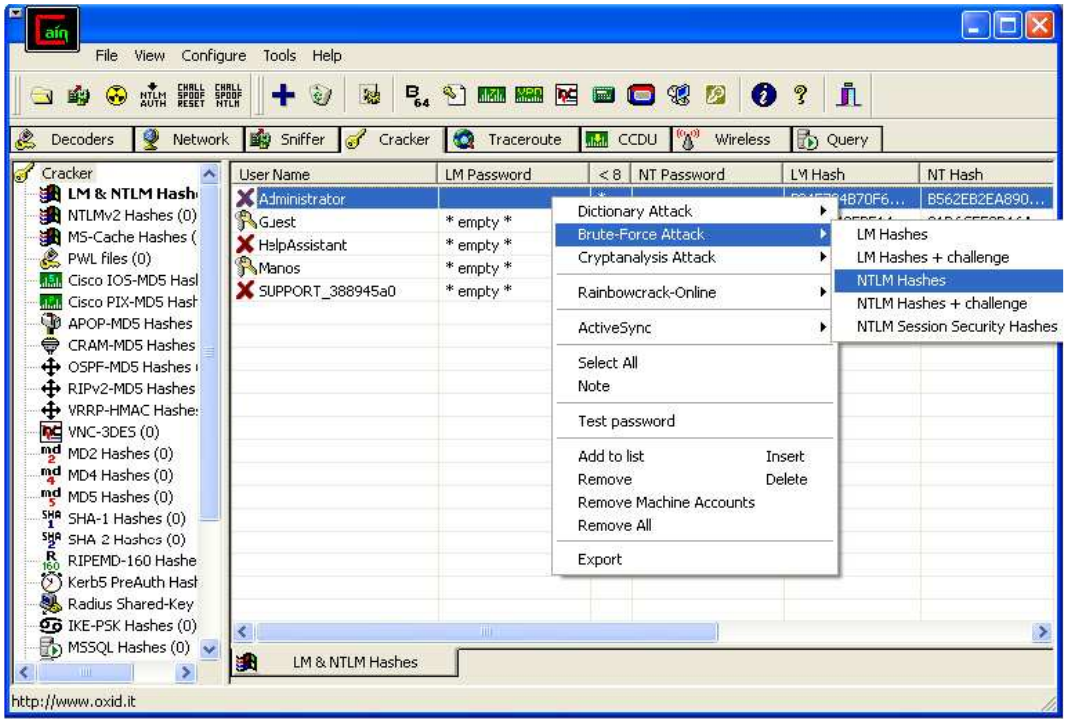
Εικόνα 129 Cain & Avel : Επιλογή της καρτέλας Cracker

Στο παράθυρο που εμφανίζεται προσδιορίζουμε ότι θα εισαγάγουμε τα στοιχεία που είναι σε hash format από το αρχείο Sam. Επιλέγουμε Next.



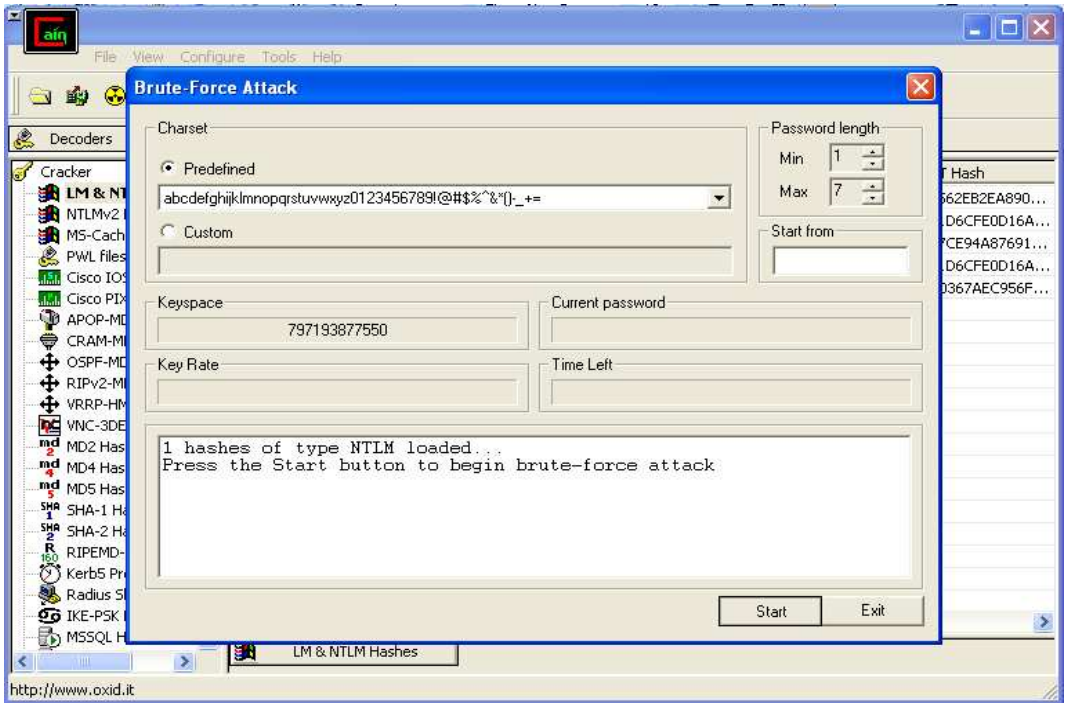
Εικόνα 130 Cain & Avel : Εισαγωγή αρχείων τύπου hash

Έτσι παρατηρούμε πως τα συνθηματικά του αρχείου Sam έχουν εισαχθεί στο Cracker μέρος του προγράμματος. Τώρα για όποιο username θέλουμε να ανακτηθεί ο αντίστοιχος κωδικός θα κάνουμε δεξί κλικ σε αυτό θα επιλέξουμε το είδος της επίθεσης και το format που έχουν οι κωδικοί.



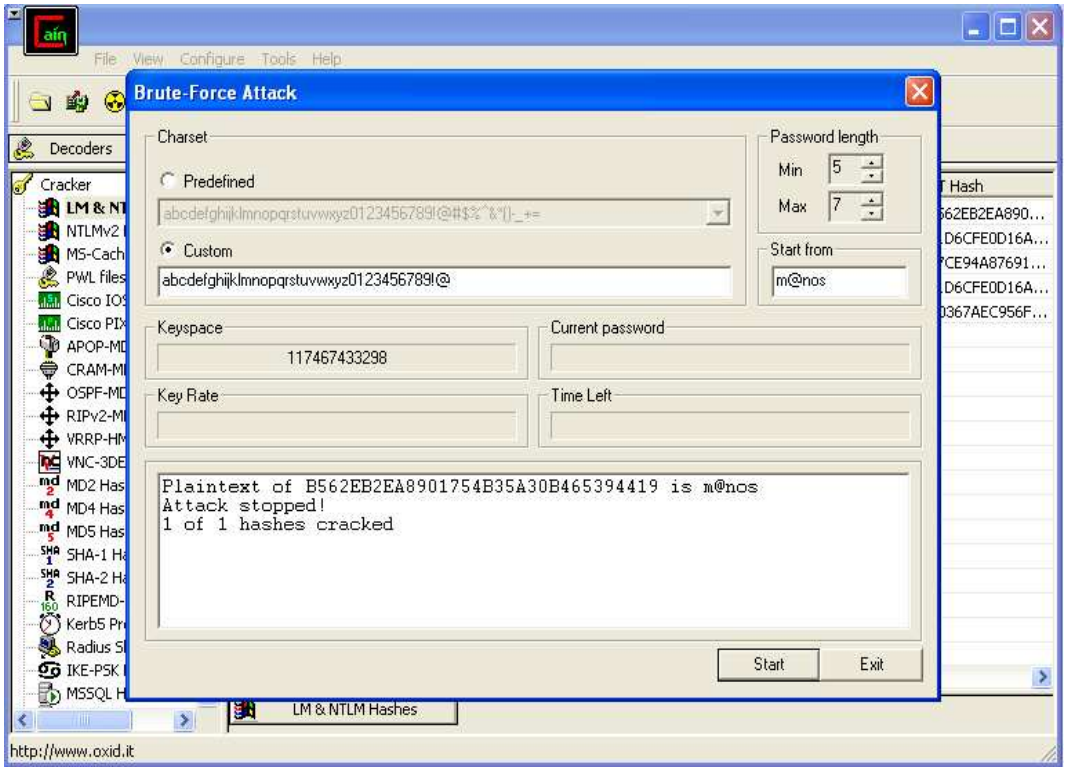
Εικόνα 131 Cain & Avel : Προσδιορισμός της επίθεσης

Στο επόμενο παράθυρο που εμφανίζεται καθορίζουμε το μήκος και την πολυπλοκότητα του κωδικού του κωδικού αν αυτό είναι εφικτό. Στη συνέχεια επιλέγουμε το Start ώστε να αρχίσει η διαδικασία της ανάκτησης του κωδικού.



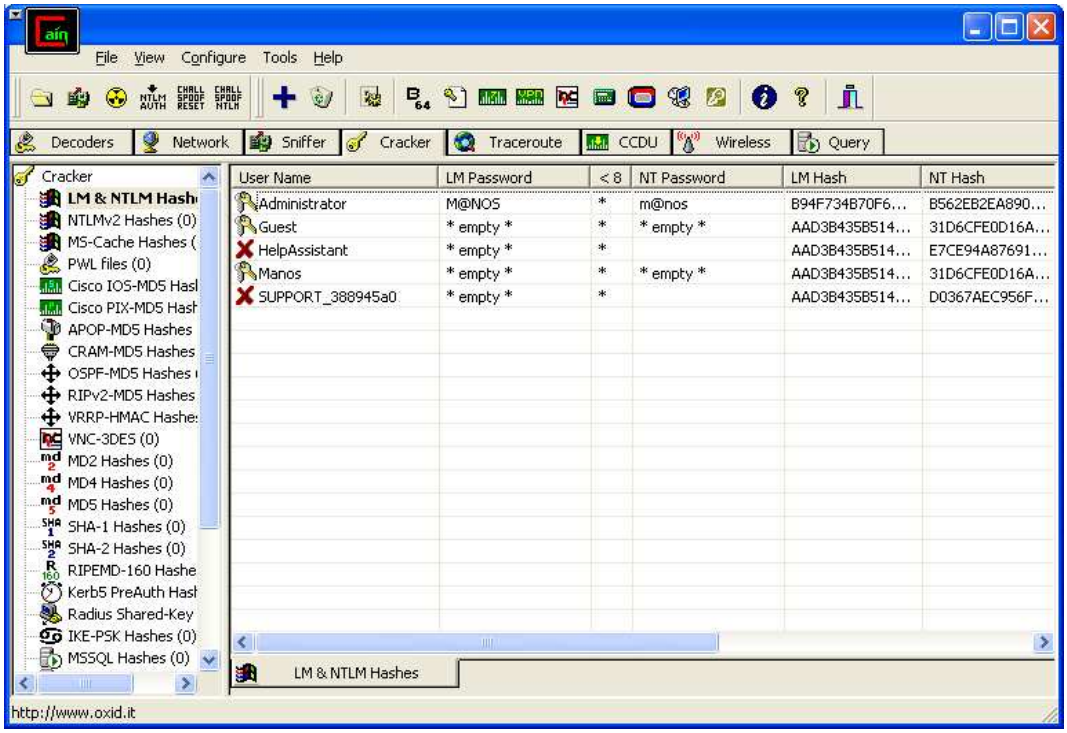
Εικόνα 132 Cain & Avel : Ρύθμιση ιδιοτήτων κωδικού

Η διαδικασία έχει ολοκληρωθεί, αφού έχουν ανακτηθεί τα στοιχεία που επιθυμούσαμε. Επιλέγουμε Exit.



Εικόνα 133 Cain & Avel : Εύρεση του κωδικού

Το πρόγραμμα επιστρέφει αυτόματα στο Cracker μέρος του προγράμματος όπου τα πεδία LM Password, NT Password, LM Hash και NT Hash είναι πλέον συμπληρωμένα με τα στοιχεία που αναζητούσαμε και όχι κενά.



Εικόνα 134 Cain & Avel : Παρουσίαση του αποτελέσματος

Εδώ παρουσιάζεται η αναφορά της διαδικασίας που εκτελέσαμε.

IP Address	192.168.2.2
Service Port	23
Service Type	
Protocol	Telnet
File name	sam
File type	Windows
Crack time	20 sec
Login Names	Administrator Guest stHelpAssistant Manos SUPPORT_388945a0
Passwords	m@nos

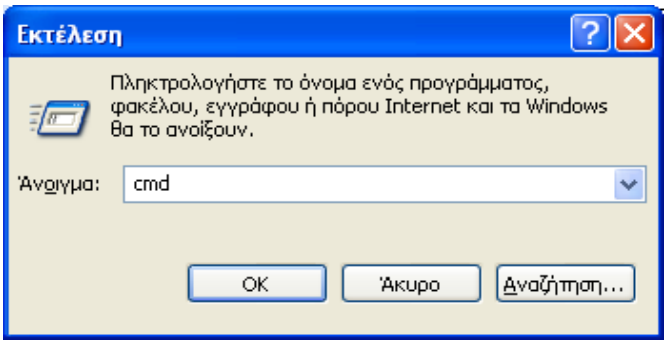
2.7.4 Password Cracking on Unix

John the Ripper

Είναι ένα βοήθημα για το σπάσιμο των κωδικών πρόσβασης μόνο μέσου λεξικού, το οποίο έχει δημιουργηθεί από την Solar Designer. Είναι ένα εργαλείο γραμμής εντολών ,σχεδιασμένο κυρίως για το σπάσιμο αρχείων κωδικών πρόσβασης του UNIX αλλά μπορεί να χρησιμοποιηθεί και για το σπάσιμο κρυπτογραφημένων κωδικών πρόσβασης του LanMan για Windows. Εκτός του ότι τρέχει σε πολλές αρχιτεκτονικές και υποστηρίζει πολλούς διαφορετικούς αλγόριθμους κρυπτογράφησης, είναι εξαιρετικά γρήγορο και δωρεάν. Επίσης στις παλιότερες εκδόσεις του προγράμματος, οι κωδικοί πρόσβασης που παράγει διατηρούν αναγραφή πεζών-κεφαλαίων χαρακτήρων, κάτι τέτοιο μπορεί να δημιουργήσει προβλήματα εάν ο πραγματικός κωδικός πρόσβασης περιέχει συνδυασμούς πεζών-κεφαλαίων.

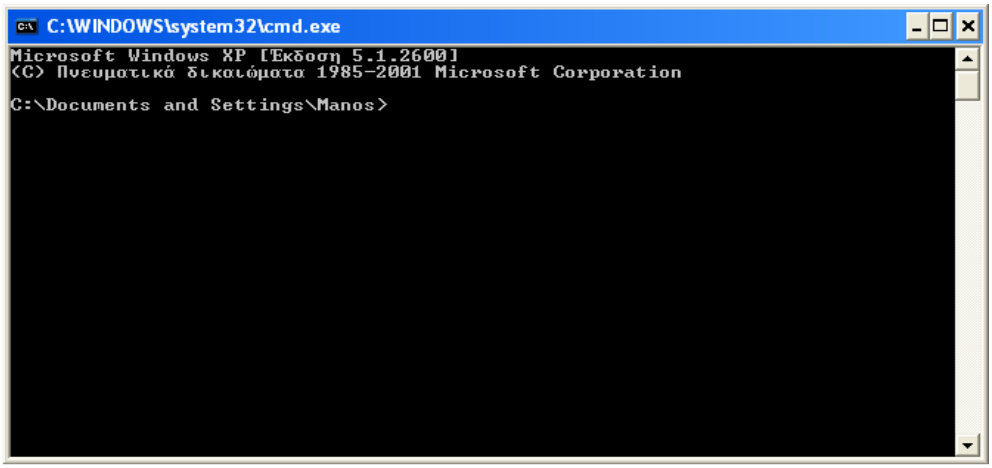
Download: http://www.openwall.com/john/

Επειδή το πρόγραμμα τρέχει σε γραμμή εντολών MS-DOS ας δούμε πως θα ξεκινήσει. Επιλέγουμε έναρξη και μετά εκτέλεση. Έτσι έχουμε το παρακάτω παράθυρο όπου θα γράψουμε cmd για να μεταβούμε στο παράθυρο του MS-DOS.



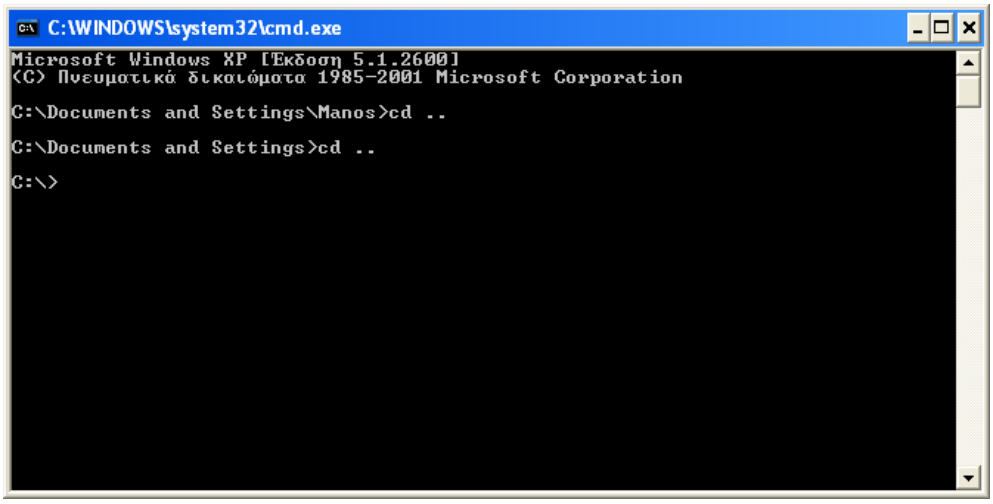
Εικόνα 135 Πληκτρολόγηση cmd

Έτσι έχουμε το παράθυρο του MS-DOS



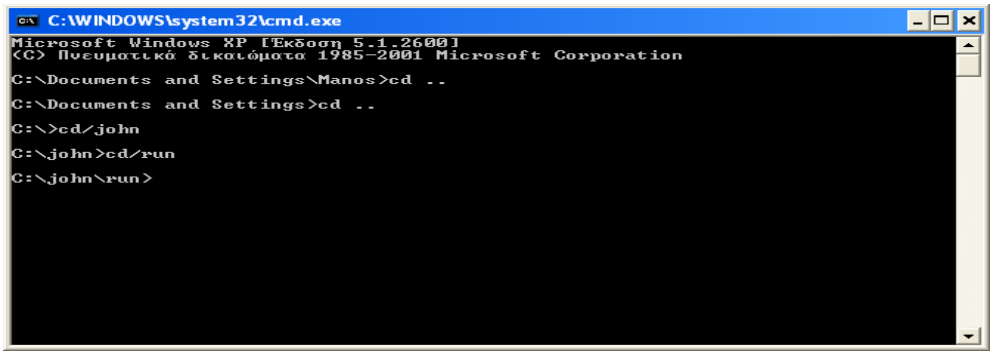
Εικόνα 136 Παράθυρο MS-DOS

Αν χρησιμοποιήσουμε τις εντολές και τις διαδρομές των φακέλων με τις σωστές ονομασίες θα είμαστε έτοιμοι να χρησιμοποιήσουμε το πρόγραμμα. Στην προκειμένη περίπτωση θα αλλάξουμε το directory ώστε να πάμε στο σημείο όπου έχουμε αποθηκεύσει το John The Ripper. Με την επιλογή Το έχουμε αποθηκεύσει στο C



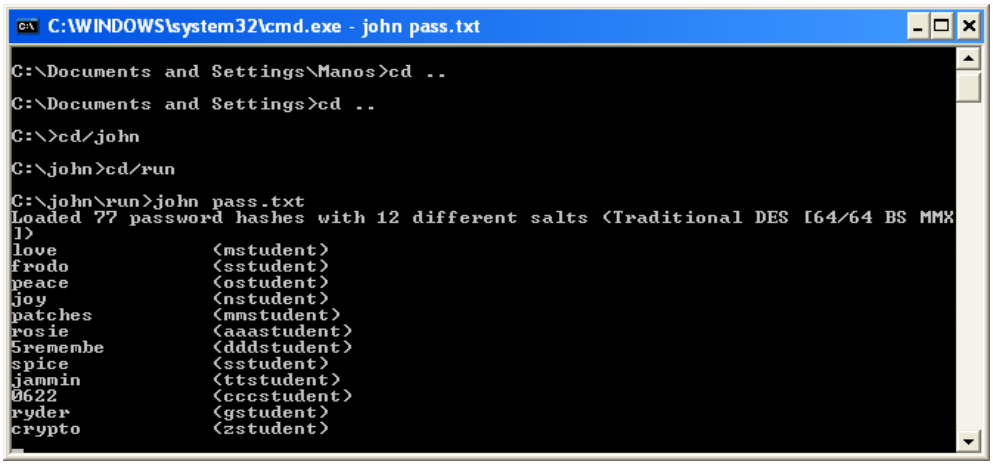
Εικόνα 137 Αλλαγή directory

Πάμε στο φάκελο Run ώστε να τρέξουμε το .exe



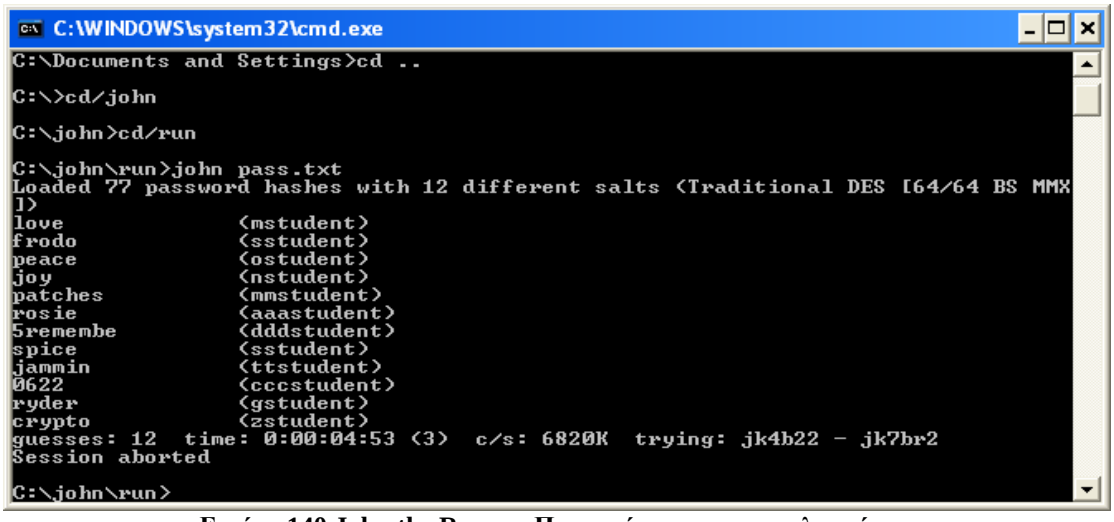
Εικόνα 138 Άνοιγμα φακέλου Run

Επίσης σε αυτό το φάκελο βρίσκεται το αρχείο pass.txt με όλα τα κρυπτογραφημένα στοιχεία, τα οποία θα πρέπει να αποκρυπτογραφηθούν με τον εξής τρόπο (john pass.txt) όπως βλέπουμε και στην εικόνα



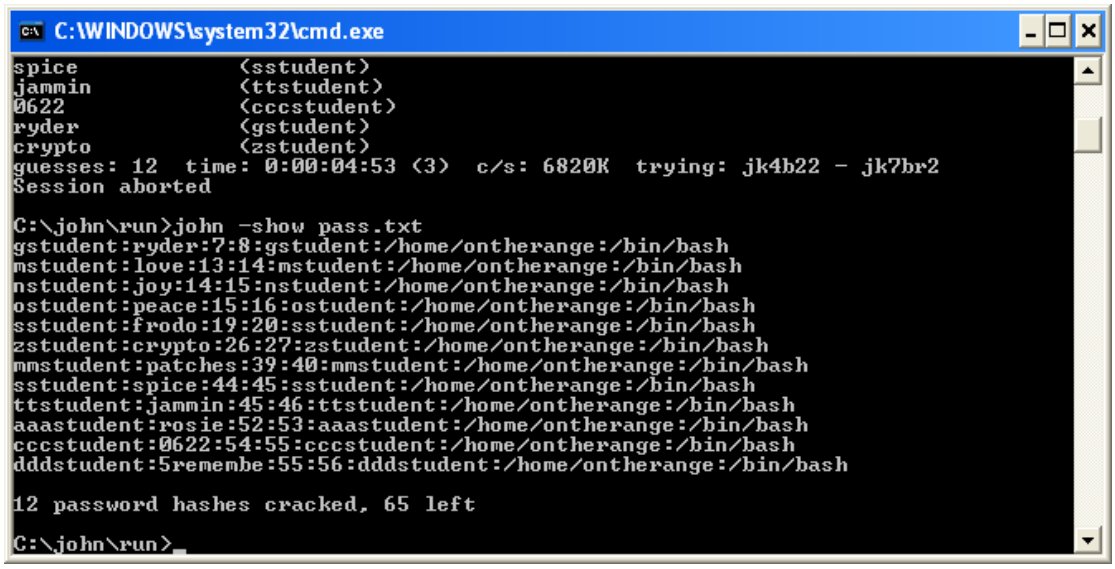
Εικόνα 139 John the Rpper : Εκτέλεση του αρχείου pass.txt

Αφού περιμένουμε να ολοκληρωθεί η διαδικασία(μπορεί και να διακοπεί όπως γίνεται και στην προκειμένη περίπτωση με Ctrl + C), παίρνουμε τα παρακάτω αποτελέσματα.



Εικόνα 140 John the Rpper : Παρουσίαση των αποτελεσμάτων

Τέλος για να δούμε όλα τα cracked passes γράφουμε στη γραμμή εντολών (john –show.pass.txt)



Εικόνα 141 John the Rpper : Παρουσίαση όλων των cracked passes

Εδώ παρουσιάζεται η αναφορά της διαδικασίας που εκτελέσαμε.

File name	pass
File type	txt
Crack time	4m & 53s
Username	Παρουσιάζονται στην παραπάνω εικόνα
Password	Παρουσιάζονται στην παραπάνω εικόνα

2.8 Denial of Service Testing

2.8.1 Περιγραφή

Το Denial of Service[14] (DOS) είναι μια κατάσταση όπου μια περίσταση, είτε σκόπιμα είτε τυχαία αποτρέπει το σύστημα από τη λειτουργία του όπως θα έπρεπε. Σε ορισμένες περιπτώσεις, το σύστημα μπορεί να λειτουργεί ακριβώς όπως είχε σχεδιαστεί, ωστόσο, ποτέ δεν είχε την πρόθεση να χειρίζεται το φορτίο, το πεδίο εφαρμογής, είτε τις παράμετροι που επιβάλλει.

Είναι πολύ σημαντικό ότι το DOS λαμβάνει πρόσθετη υποστήριξη από την οργάνωση και παρακολουθείται στενά. Οι επιθέσεις Flood και Distributed (DDoS) συγκεκριμένα δεν εξετάζεται και απαγορεύεται για να εξεταστεί σύμφωνα με αυτό το εγχειρίδιο. Αυτές πάντα θα προκαλλούν ορισμένα προβλήματα και συχνά όχι μόνο στο στόχο αλλά και σε όλους τους δρομολογητές και στα συστήματα.

Αναμενόμενα αποτελέσματα:

- Λίστα των αδύναμων σημείων στην παρουσία Διαδικτύου συμπεριλαμβανομένων των ενιαίων σημείων της αποτυχίας
- Καθιέρωση μιας βασικής γραμμής για κανονική χρήση
- Λίστα των συμπεριφορών του συστήματος σε βαριά χρήση
- Λίστα των τρωτών συστημάτων DOS

Βήματα που εφαρμόζονται για τον έλεγχο DOS:

- Ελέγχος των λογαριασμών των διαχειριστών και των αρχείων και των πόρων των συστημάτων για το εάν εξασφαλίζονται κατάλληλα και όλη η πρόσβαση χορηγείται με " List Prevelege ".
- Έλεγχος των περιορισμών έκθεσης των συστημάτων στα μη-εμπιστευόμενα δίκτυα.
- Έλεγχος για ότι οι βασικές γραμμές καθιερώνονται για την κανονική δραστηριότητα των συστημάτων.
- Έλεγχος για το ποιες διαδικασίες είναι σε θέση να ανταποκριθούν στην ανώμαλη δραστηριότητα.
- Έλεγχος των απαντήσεων στις προσποιούμενες αρνητικές επιθέσεις πληροφοριών (προπαγάνδα).
- Έλεγχος βαρέων φορτίων δικτύου και διακομιστή.

Πληροφορίες:

- *Για το Denial of Service χρησιμοποιήσαμε τα προγράμματα Udp Flood, DoS HTTP και η διαδικασία περιγράφεται στην ενότητα 1.6.2*

2.8.2 Denial of Service Testing

Udp Flood

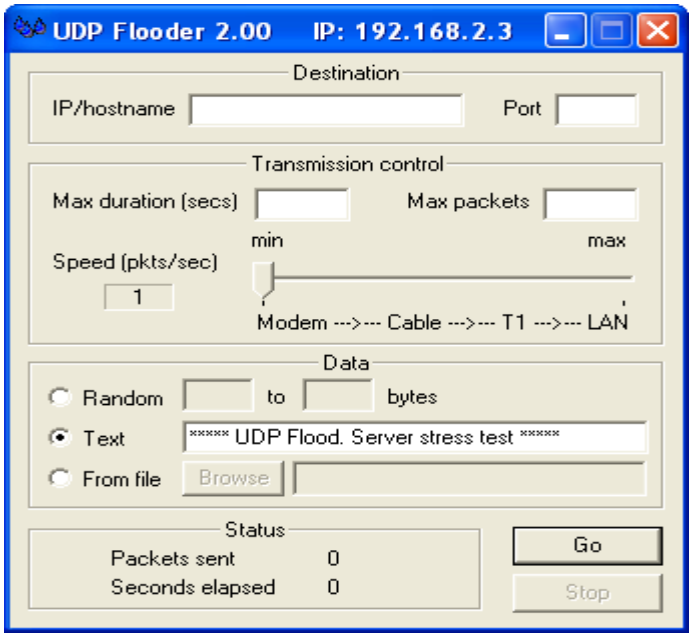
Το UDPFlood είναι ένας αποστολέας πακέτων UDP. Στέλνει πακέτα UDP σε μια καθορισμένη IP διεύθυνση και πόρτα σε κάποιο συγκεκριμένο χρονικό διάστημα. Τα

[14] http://en.wikipedia.org/wiki/Denial-of-service_attack

πακέτα μπορεί να είναι μια συμβολοσειρά, ένας αριθμός από τυχαία bytes, δεδομένα από κάποιο αρχείο. Είναι χρήσιμο εργαλείο για τον έλεγχο του Server.

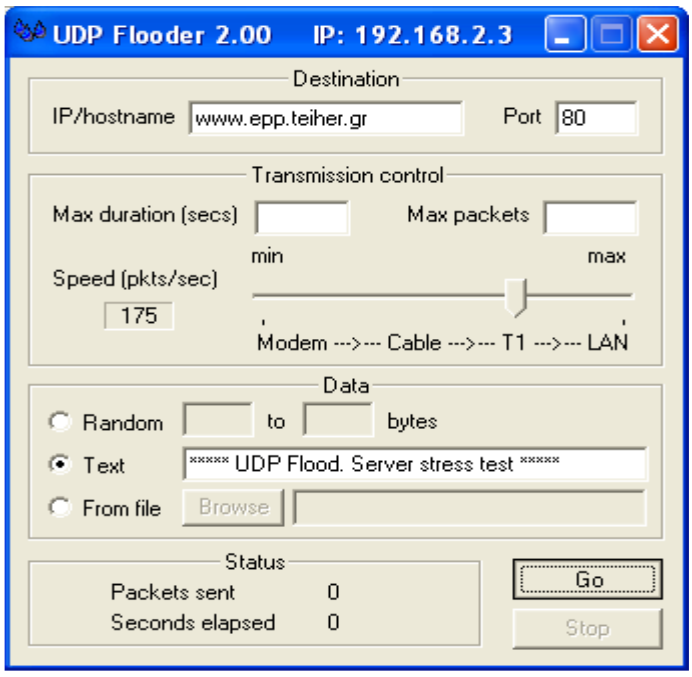
Download:http://www.topshareware.com/hacking-tool-denial-of-service-attack/downloads/1.htm

Ξεκινάμε με το άνοιγμα του προγράμματος:



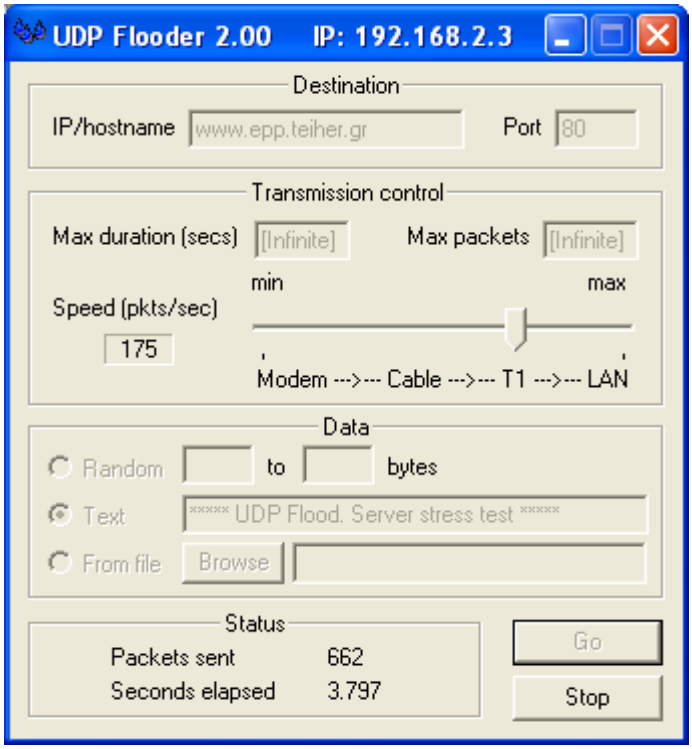
Εικόνα 142 UDP Flooder : Εκκίνηση του προγράμματος

Στυ συνέχεια θα ρυθμίσουμε τις παραμέτρους του προγράμματος. Επιλέγοντας “Go” θα ξεκινήσει η διαδικασία (για epp):



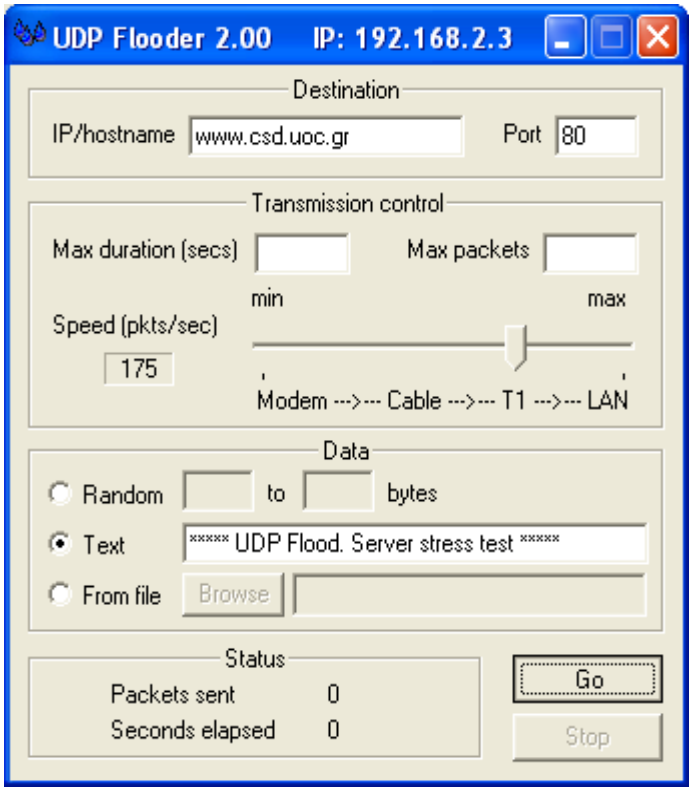
Εικόνα 143 UDP Flooder : Ρύθμιση παραμέτρων για epp

Εκκίνηση της διαδικασίας:

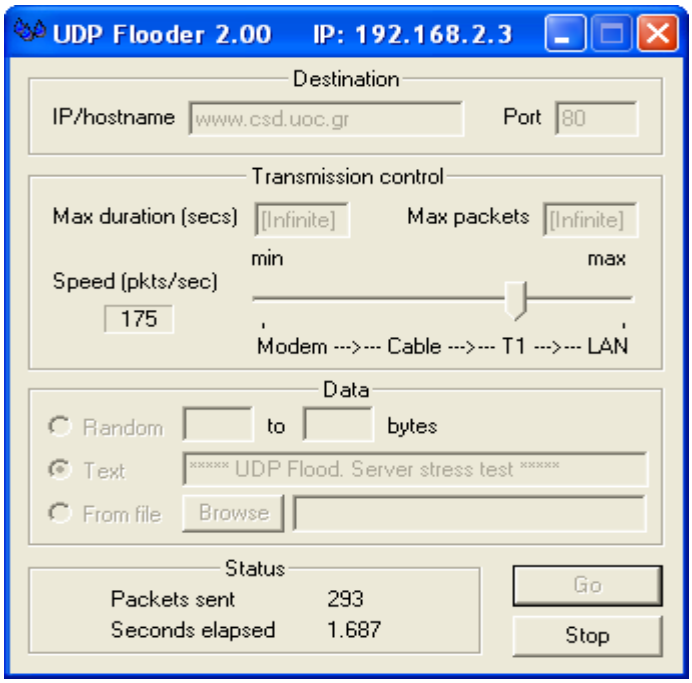


Εικόνα 144 UDP Flooder : Server stressing για epp

Με αυτόν τον τρόπο λοιπόν επιτυγχάνεται το "κρασάρισμα" του Server. Με τα ίδια βήματα και την ίδια σειρά η διαδικασία θα γίνει και για το csd.



Εικόνα 145 UDP Flooder : Ρύθμιση παραμέτρων για csd



Εικόνα 146 UDP Flooder : Server stressing για csd

DoS HTTP

Το DosHttp χρησιμοποιεί πολλαπλά ασύγχρονα socket[15] για να επιτύχει μια αποτελεσματική HTTP πλυμμήρα πακέτων (UDP flood[16]) . Μπορεί να χρησιμοποιηθεί ταυτόχρονα σε πολλαπλούς clients για να εξομειώσει επιθέσεις τύπου Denial Of Service.

Download: http://www.filebuzz.com/fileinfo/51184/DoSHTTP.html

Ανοίγοντας το πρόγραμμα έχουμε:

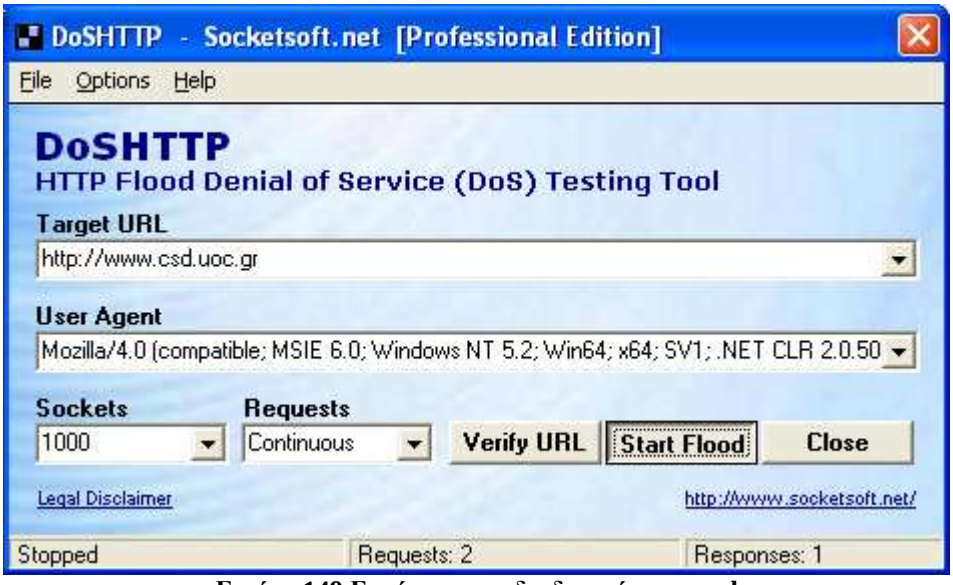
Εικόνα 147 DoSHTTP : Εκκίνηση του προγράμματος

[15] http://en.wikipedia.org/wiki/Internet_socket
[16] http://en.wikipedia.org/wiki/UDP_flood_attack
http://www.cert.org/advisories/CA-1996-01.html

Στο πεδίο κειμένου Target URL πληκτρολογούμε τη διεύθυνση του epp και επιλέγουμε “Start Flood” ώστε να ξεκινήσει η αποστολή των πακέτων ώσδτε να επιτευχθεί το “κρασάρισμα” του Server.

Εικόνα 148 DoSHTTP : Εκκίνηση της διαδικασίας για epp

Με τον ίδιο τρόπο η διαδικασία θα γίνει για το csd:



Εικόνα 149 Εκκίνηση της διαδικασίας για csd

2.9 Wireless Networks Testing

2.9.1 Περιγραφή

Αυτή είναι μια μέθοδος για τον έλεγχο της πρόσβασης σε WLAN 802.11 τα οποία γίνονται ολοένα και περισσότερο δημοφιλείς. Εντούτοις, μερικά αρκετά ανησυχητικά προβλήματα ασφαλείας είναι κοινά κατά την εφαρμογή αυτών των τεχνολογιών. Αυτό είναι κυρίως επειδή αυτά τα δίκτυα πολύ γρήγορα και εύκολα ρίχνονται μαζί, αλλά τα μέτρα ασφάλειας δεν είναι μέρος της προεπιλογής της οργάνωσης. Υπάρχουν μερικά βασικά πράγματα που μπορούν να γίνουν για να βελτιώσουν την ασφάλεια και λίγο περισσότερα δραστικά μέτρα που μπορούν να ληφθούν για να καταστήσουν τα WLANs αρκετά ασφαλή.

Προδιαγραφές 802.11:

- Φυσικό επίπεδο: Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), infrared (IR).
- Προεπιλεγμένη κρυπτογράφηση: RC4-based stream encryption algorithm για εμπιστευτικότητα, πιστοποίηση, και ακεραιότητα. Περιορισμένη διαχείριση κλειδιών.
- Φάσμα λειτουργίας: Περίπου 150 πόδια σε εσωτερικούς χώρους και 1500 πόδια σε εξωτερικούς χώρους.

Εφαρμογές:

- **802.11a**
  - Λειτουργεί στην περιοχή συχνοτήτων των 5 GHz
  - Δεν είναι συμβατό με 802.llb ή 802.11g υλικό
  - Μέγιστη ταχύτητα των 54 Mbps

- **802.11b**
  - Λειτουργεί στην περιοχή συχνοτήτων των 2.4 GHz
  - Επί του παρόντος, το ευρύτερα διαδεδομένο πρότυπο
  - Μέγιστη ταχύτητα των 11 Mbps

- **802.11g**
  - Λειτουργεί στην περιοχή συχνοτήτων των 2.4 GHz
  - Η καθορισμένη μέγιστη ταχύτητα των 54Mbps
  - Αναμένεται να είναι συμβατό με το υλικό 802.11b

Αξιολόγηση των επιχειρησιακών αναγκών, των πρακτικών, και των πολιτικών:

- Έλεγχος για το ότι η οργάνωση έχει μια επαρκή πολιτική ασφαλείας που εξετάζει τη χρήση της ασύρματης τεχνολογίας, συμπεριλαμβανομένης της χρήσης 802.11

Αξιολόγηση των Hardware, Firmware, Updates:

- Εκτέλεση μιας πλήρης απογραφής όλων των ασύρματων συσκευών στο δίκτυο.

Αξιολόγηση του ελέγχου προσπέλασης, της ασφάλειας περιμέτρου, και της δυνατότητας αναχαίτισης ή παρεμπόδισης της επικοινωνίας:

- Καθορισμός του επιπέδου των φυσικών ελέγχων προσπέλασης στα σημεία πρόσβασης και συσκευών που ελέγχει (keyed locks, card badge readers, cameras...).

Αξιολόγηση των διοικητικών προσβάσεων στις ασύρματες συσκευές:

- Καθορισμός για το εάν τα σημεία πρόσβασης κλείνουν κατά τη διάρκεια των μερίδων της ημέρας όταν δεν θα είναι σε λειτουργία.

Αξιολόγηση της διαμόρφωσης, της επικύρωσης και της κρυπτογράφησης των ασύρματων δικτύων:

- Έλεγχος για το ότι το καθορισμένο προσδιοριστικό υπηρεσιών προεπιλογής του σημείου πρόσβασης (SSID) έχει αλλάξει.

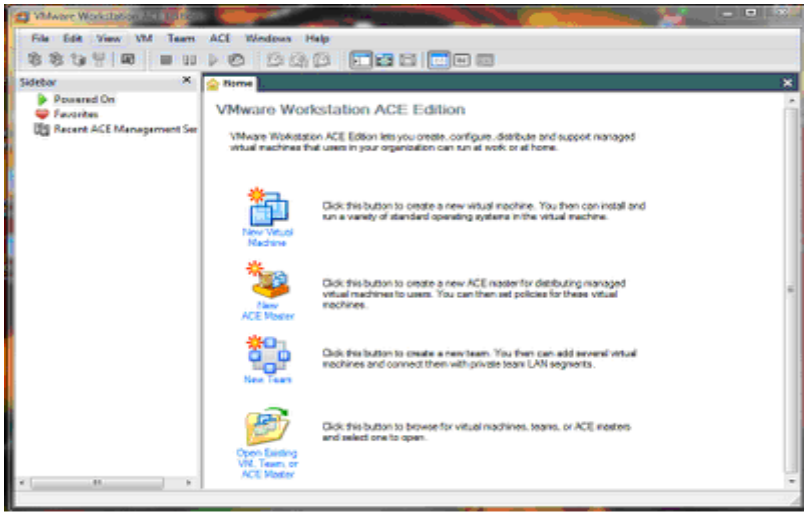
Αξιολόγηση των αύρματων πελατών:

- Έλεγχος ότι όλοι οι ασύρματοι πελάτες εγκαθιστούν το antivirus λογισμικό.

2.9.2 Wireless Networks Testing

Η διαδικασία μπορεί να πραγματοποιηθεί μόνο μέσα από κάποια διανομή των Linux. Αυτό που υλοποιήθηκε είναι η εγκατάσταση διανομών Linux σε ένα Virtual Machine (Vmware[17]) που τρέχει σε Windows και η χρήση των προγραμμάτων μέσα από αυτό. Βεβαίως αυτό δεν θα μπορούσε να υλοποιηθεί αν η ασύρματη κάρτα δικτύου που χρησιμοποιήσαμε (WUSB45GR της LINKSYS) δεν είχε USB Interface.

Ξεκινάμε με το άνοιγμα του προγράμματος:



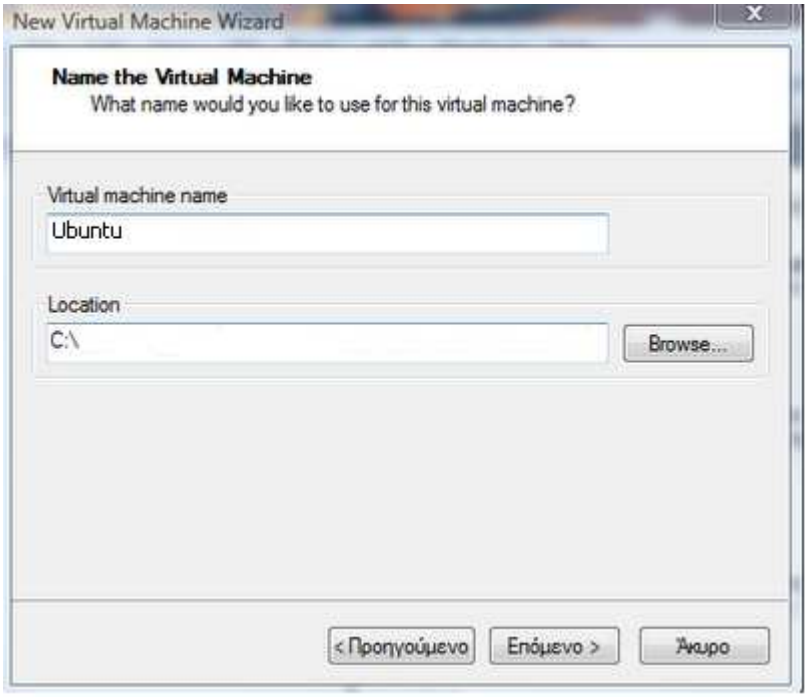
Εικόνα 150 Vmware : Εκκίνηση του προγράμματος

[17] http://en.wikipedia.org/wiki/VMware
http://www.remote-exploit.org/backtrack_download.html

Πατάμε την επιλογή New virtual Machine και έχουμε τις επιλογές που βλέπετε δοκιμάσουμε να περάσουμε τα Linux .

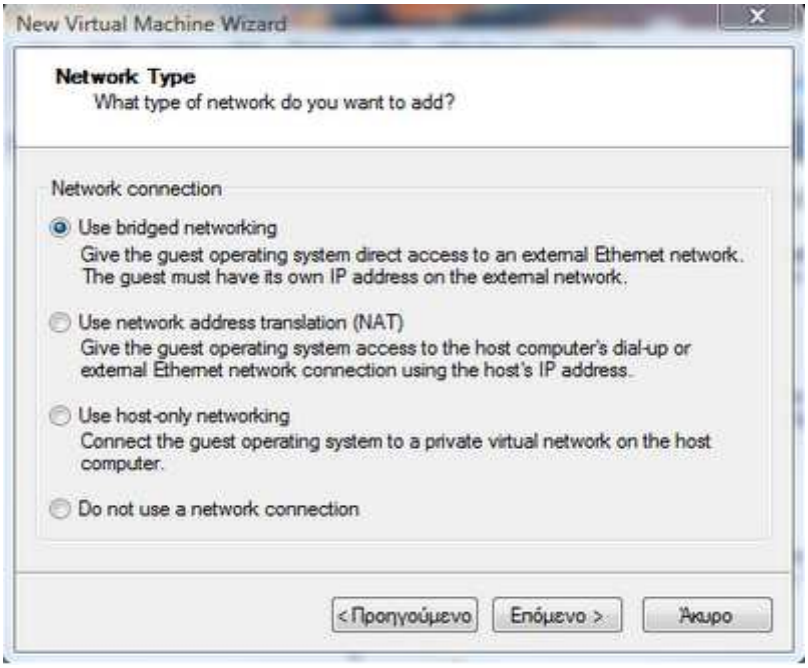
Εικόνα 151 VMware : Επιλογή εικονικού λειτουργικού συστήματος

Το αφήνουμε ως έχει, ή αν θέλετε μπορείτε να αλλάξετε την διαδρομή location



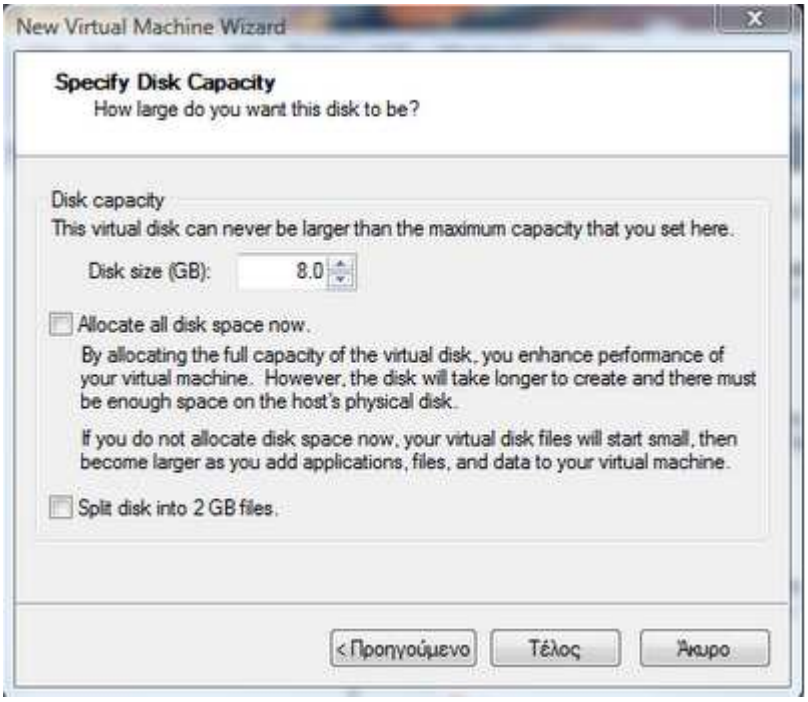
Εικόνα 152 VMware : Καθορισμός προορισμού αποθήκευσης

Το αφήνουμε όπως είναι:



Εικόνα 153 VMware : Επιλογή σύνδεσης δικτύου

Εδώ εάν θέλουμε αλλάζουμε την χωρητικότητα που θέλουμε να έχει ο εικονικός δίσκος:



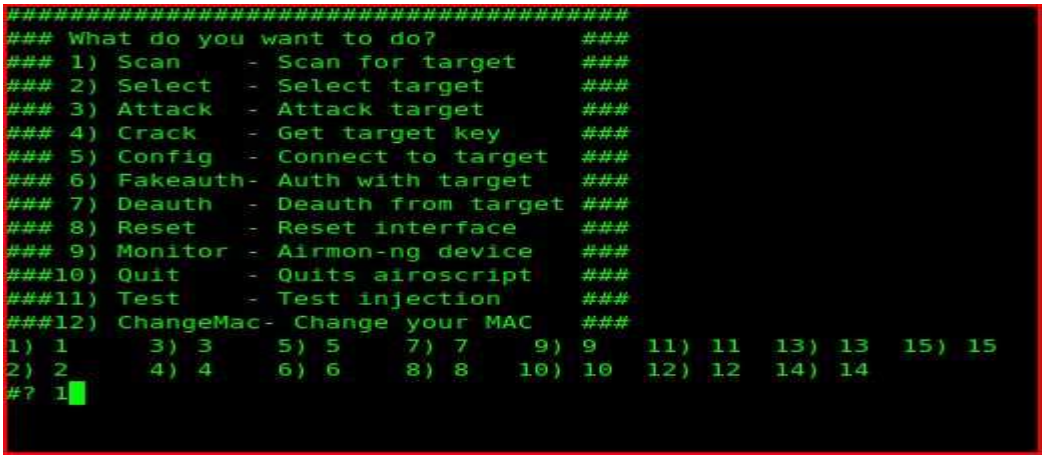
Εικόνα 154 VMware : Προσδιορισμός χωρητικότητας εικονικού δίσκου

Στη συνέχεια τρέχουμε το πρόγραμμα Airoscript όπου είναι (ένα Linux script), το οποίο επιτρέπει να γίνει η επίθεση πολύ πιο γρήγορα χωρίς να χρειάζεται να πληκτρολογούμε και να κρατάμε σημειώσεις.

Ανοίγουμε λοιπόν το πρόγραμμα:

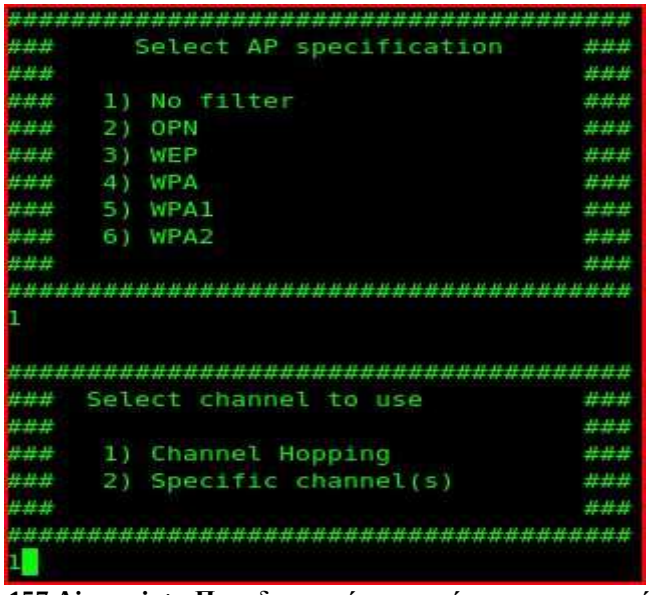
Εικόνα 155 Airoscript : Εκκίνηση του προγράμμτος

Στη συνέχεια θα επιλέξουμε να κάνουμε scan στην περιοχή



Εικόνα 156 Airoscript : Επιλογή της περιοχής που θα γίνει η ανίχνευση

Τέλος θα επιλέξουμε τις παραμέτρους του scan και η διαδικασία ξεκινάει:



Εικόνα 157 Airoscript : Προσδιορισμός παραμέτρων για την ανίχνευση

Η διαδικασία ολοκληρώνεται:

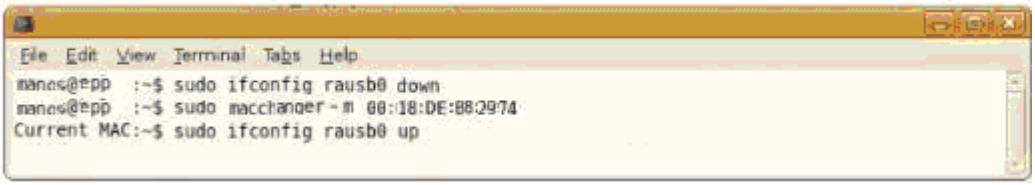
Εικόνα 158 Παρουσίαση αποτελεσμάτων

Πληροφορούμαστε λοιπόν για τα παρακάτω:

- Ότι υπάρχει ένα Access Point(AP) στην περιοχή με όνομα: MANOS_WiFi.
- Τη MAC Address του interface: 00:60:4C:E2:4A:C7 που χρησιμοποιεί
- Ότι ένας client με MAC 00:18:DE:B8:29:74 είναι συνδεδεμένος με το AP

Επόμενο βήμα είναι να αλλάξουμε τη MAC Address του interface μας στη MAC Address του συνδεδεμένου client με στόχο να μπορούμε να στείλουμε τα ARP πακέτα που διαβάζουμε, ώστε να δημιουργήσουμε κίνηση.

Για να το κάνουμε αυτό, έχουμε εγκαταστήσει στο λειτουργικό μας την εφαρμογή macchanger[18].Ανοίγουμε λοιπόν το πρόγραμμα και πληκτρολογούμε τις παρακάτω εντολές όπως ακολουθεί:



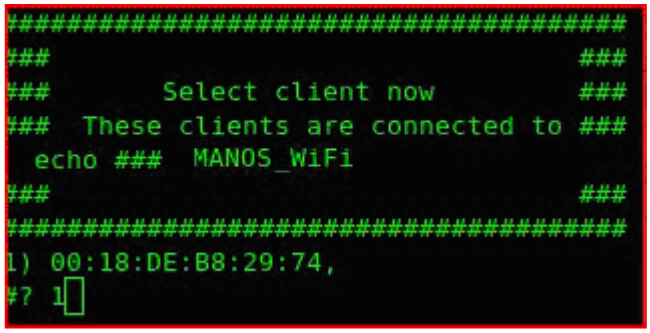
Εικόνα 159 Macchanger : Αλλαγή MAC Address

Επιστρέφουμε πάλι στο Airoscript και υλοποιούμε όλα τα προηγούμενα βήματα από την αρχή και προχωρούμε στην επομένη σελίδα που είναι η επιλογή του θύματος:

Εικόνα 160 Airoscript : Επιλογή του θύματος (1/3)

[18] http://www.maxi-pedia.com/download+macchanger

Εικόνα 161 Airoscript : Επιλογή του θύματος (2/3)



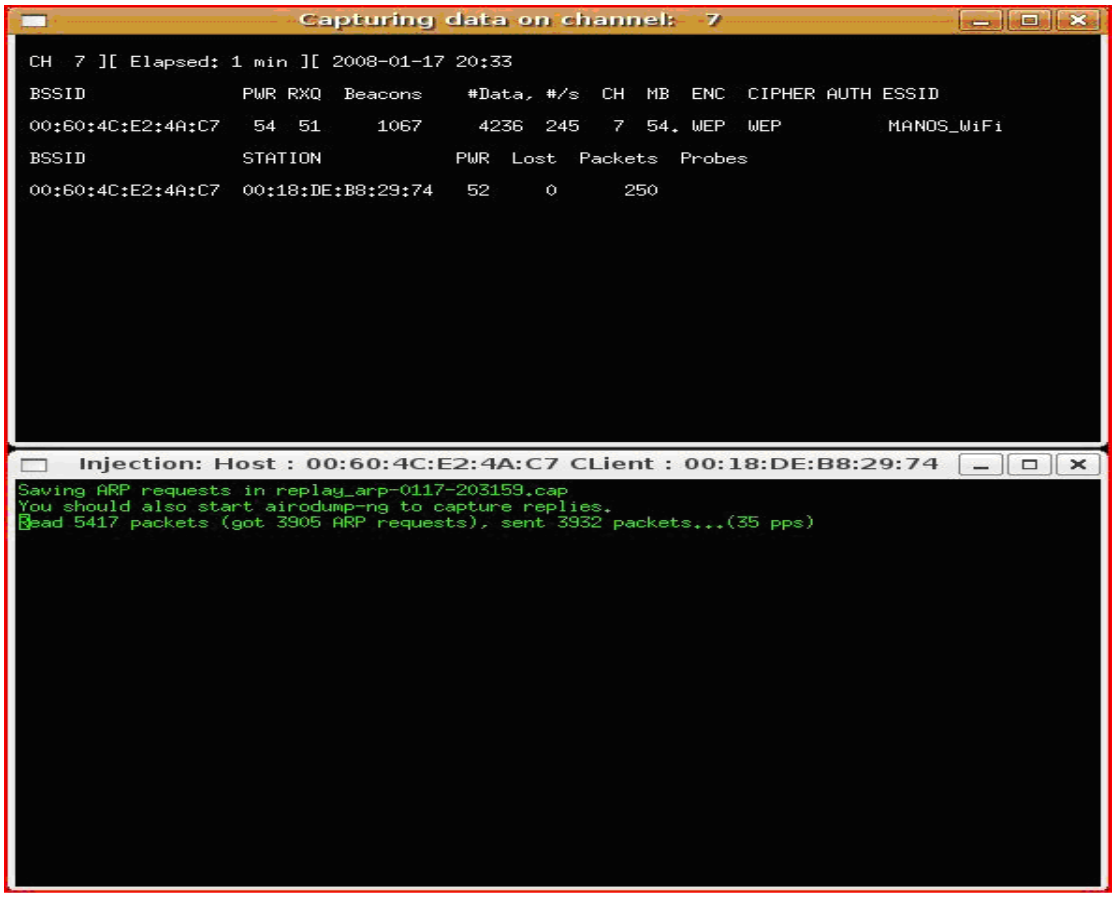
Εικόνα 162 Airoscript : Επιλογή του θύματος (3/3)

Και αφού επιλέξαμε το θύμα με τις κατάλληλες παραμέτρους επιλέγουμε και την επίθεση:

- Η καλύτερη επίθεση που μπορούμε να επιλέξουμε στην περίπτωση που έχουμε έναν client συνδεδεμένο με το AP είναι η ARP replay.

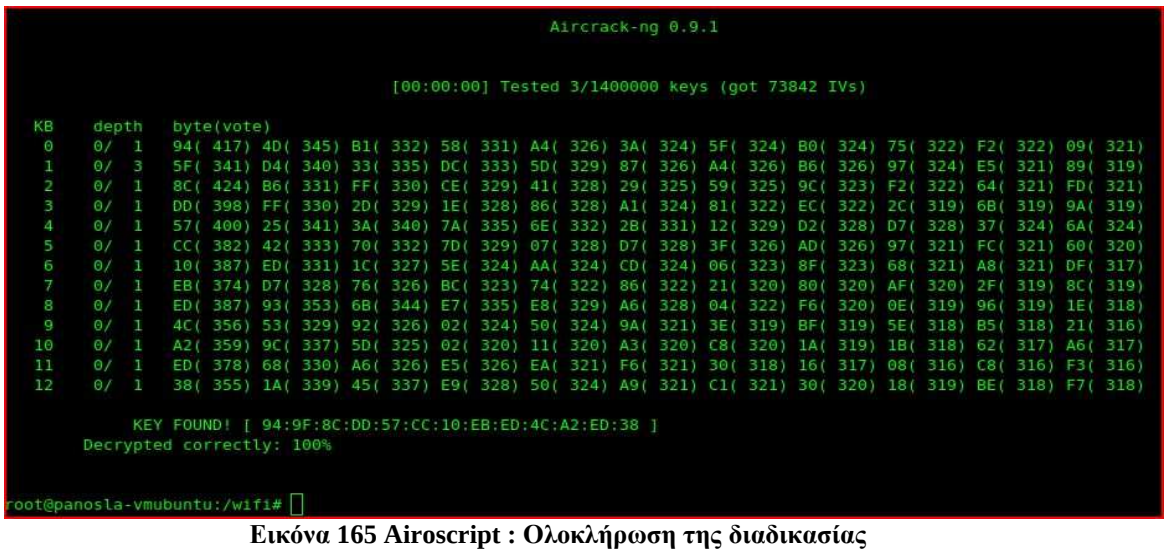
Εικόνα 163 Airoscript : Επιλογή της επίθεσης

Ξεκινάμε την επίθεση λοπόν:



Εικόνα 164 Εκκίνηση της επίθεσης

Αυτό που παρατηρούμε είναι ότι μπορεί να περάσει αρκετή ώρα μέχρι να πάρουμε το πρώτο πακέτο αλλά από ‘κει πέρα όλα τα υπόλοιπα έρχονται με μεγάλο ρυθμό. Όταν συγκεντρώσουμε περίπου 80.000 πακέτα –περίπου 3 λεπτά- για WEP 104BIT μπορούμε να αρχίσουμε το σπάσιμο του κλειδιού με το Aircrack:



Εικόνα 165 Airoscript : Ολοκλήρωση της διαδικασίας

Η επίθεση μας είναι επιτυχής και το κλειδί σωστό.

Κεφάλαιο 3 Πρωτότυπα Κείμενα

3.1 Περιγραφή

Παρακάτω παρουσιάζεται το αγγλικό παράρτημα των προαναφερθέντων κεφαλαίων.

3.1.1 Network Surveying

A network survey serves often as an introduction to the systems to be tested. It is best defined as a combination of data collection, information gathering, and policy control. Although it is often advisable from a legal standpoint to define contractually exactly which systems to test if you are a third-party auditor or even if you are the system administrator, you may not be able to start with concrete system names or IP addresses. In this case you must survey and analyze. The point of this exercise is to find the number of reachable systems to be tested without exceeding the legal limits of what you may test. Therefore the network survey is just one way to begin a test; another way is to be given the IP range to test. In this module, no intrusion is being performed directly on the systems except in places considered a quasi-public domain.

In legal terms, the quasi-public domain is a store that invites you in to make purchases. The store can control your access and can deny certain individuals entry but for the most part is open to the general public (even if it monitors them). This is the parallel to an e-business or web site.

Although not truly a module in the methodology, the network survey is a starting point. Often more hosts are detected during actual testing. Please bear in mind that the hosts discovered later may be inserted in the testing as a subset of the defined testing and often only with permission or collaboration with the target organization's internal security team.

Expected Results:

- Domain Names
- Server Names
- IP Addresses
- Network Map
- ISP / ASP information
- System and Service Owners
- Possible test limitations

Tasks to perform for a thorough network survey include:

Name server responses:

- Examine Domain registry information for servers.
- Find IP block owned.
- Question the primary, secondary, and ISP name servers for hosts and sub domains.

Examine the outer wall of the network:

- Use multiple traces to the gateway to define the outer network layer and routers.

Examine tracks from the target organization:

- Search web logs and intrusion logs for system trails from the target network.
- Search web logs and intrusion logs for system trails from the target network.

Information Leaks

- Examine target web server source code and scripts for application servers and internal links.
- Examine e-mail headers, bounced mails, and read receipts for the server trails.
- Search newsgroups for posted information from the target.
- Search job databases and newspapers for IT positions within the organization relating to hardware
  and software.
- Search P2P services for connections into the target network and data concerning the organization.

3.1.2 Port Scanning

Port scanning is the invasive probing of system ports on the transport and network level. Included here is also the validation of system reception to tunneled, encapsulated, or routing protocols. This module is to enumerate live or accessible Internet services as well as penetrating the firewall to find additional live systems. The small sample of protocols here is for clarity of definition. Many protocols are not listed here. Testing for different protocols will depend on the system type and services it offers. For a more complete list of protocols, see the Test References section. Each Internet enabled system has 65,536 TCP and UDP possible ports (incl. Port 0). However, it is not always necessary to test every port for every system. This is left to the discretion of the test team. Port numbers that are important for testing according to the service are listed with the task. Additional port numbers for scanning should be taken from the Consensus Intrusion Database Project Site.

Expected Results:
Open, closed or filtered ports
IP addresses of live systems
Internal system network addressing
List of discovered tunneled and encapsulated protocols
List of discovered routing protocols supported
Active services
Network Map

Tasks to perform for a thorough Port Scan:
Error Checking:

- Check the route to the target network for packet loss
- Measure the rate of packet round-trip time
- Measure the rate of packet acceptance and response on the target network
- Measure the amount of packet loss or connection denials at the target network

Enumerating Ports:

- Use TCP SYN (Half-Open) scans to enumerate ports as being open, closed, or filtered on the default TCP testing ports in Appendix B for all the hosts in the network.
- Use UDP scans to enumerate ports as being open or closed on the default UDP testing ports in Appendix B if UDP is NOT being filtered already. [Recommended: first test the packet filtering with a very small subset of UDP ports.]

Enumerate Systems:

- Collect broadcast responses from the network
- Probe past the firewall with strategically set packet TTLs (Firewalking) for all IP addresses.
- Use ICMP and reverse name lookups to determine the existence of all the machines in a network.
- Use a TCP source port 80 and ACK on ports 3100-3150, 10001-10050, 33500-33550, and 50 random ports above 35000 for all hosts in the network.
- Use TCP fragments in reverse order with FIN, NULL, and XMAS scans on ports 21, 22, 25, 80, and 443 for all hosts in the network.

- Use a TCP SYN on ports 21, 22, 25, 80, and 443 for all hosts in the network.
- Use DNS connect attempts on all hosts in the network.
- Use FTP and Proxies to bounce scans to the inside of the DMZ for ports 22, 81, 111, 132, 137, and 161 for all hosts on the network.

Verifying Various Protocol Response:

- Verify and examine the use of traffic and routing protocols.
- Verify and examine the use of non-standard protocols.
- Verify and examine the use of encrypted protocols.

Verifying Packet Level Response

- Identify TCP sequence predictability.
- Identify TCP ISN sequence numbers predictability.
- Identify IPID Sequence Generation predicatbility.
- Identify system up - time.

- Use TCP fragments in reverse order to enumerate ports and services for the subset of ports on the default Packet Fragment testing ports in Appendix B for all hosts in the network.

3.1.3 Services Identification

This is the active examination of the application listening behind the service. In certain cases more than one application exists behind a service where one application is the listener and the others are considered components of the listening application. A good example of this is PERL installed for use in a Web application. In that case the listening service is the HTTP daemon and the component is PERL.

Expected Results:
Service Types
Service Application Type and Patch Level
Network Map

Tasks to perform for a thorough service probe:

- Match each open port to a service and protocol.
- Identify server uptime to latest patch releases.
- Identify the application behind the service and the patch level using banners or fingerprinting.
- Verify the application to the system and the version.
- Locate and identify service remapping or system redirects.
- Identify the components of the listening service.
- Use UDP-based service and trojan requests to all the systems in the network.

3.1.4 System Identification

System fingerprinting is the active probing of a system for responses that can distinguish its operating system and version level.

Expected Results:
OS Type
Patch Level
System Type
System enumeration
Internal system network addressing

Tasks to perform for a thorough Password Cracking verification:

- Examine system responses to determine operating system type and patch level.
- Examine application responses to determine operating system type and patch level.
- Verify the TCP sequence number prediction for each live host on the network.
- Search job postings for server and application information from the target.
- Search tech bulletin boards and newsgroups for server and application information from the target.
- Match information gathered to system responses for more accurate results.

3.1.5 Vulnerability Research and Verification

The focus of this module is in the identification, understanding, and verification of weaknesses, misconfigurations and vulnerabilities within a host or network.
Research involved in finding vulnerabilities is necessary up until the delivery of the report. This involves searching online databases and mailing lists specific to the systems and network being tested. Do not confine yourself to the web, consider using IRC, Newsgroups, and underground FTP sites. Testing for vulnerabilities using automated tools is an efficient way to determine existing holes and system patch level. Although many automated scanners are currently on the market and in the underground, it is important for the tester to identify and incorporate the current underground scripts/exploits into this testing. However, manual verification is necessary for eliminating false positives,
expanding the hacking scope and discovering the data flow in and out of the network. Manual testing refers to a person or persons at the computer using creativity, experience, and ingenuity to test the target network.

Expected Results:
Type of application or service by vulnerability
Patch levels of systems and applications
List of possible denial of service vulnerabilities
List of areas secured by obscurity or visible access
List of actual vulnerabilities minus false positives
List of Internal or DMZ systems
List of mail, server, and other naming conventions
Network map

Tasks to perform for a Vulnerability Research and Verification:

- Integrate the currently popular scanners, hacking tools, and exploits into the tests.
- Measure the target organization against the currently popular scanning tools.
- Attempt to determine vulnerability by system and application type.
- Attempt to match vulnerabilities to services.
- Attempt to determine application type and service by vulnerability.
- Perform redundant testing with at least 2 automated vulnerability scanners.
- Identify all vulnerabilities according to applications.
- Identify all vulnerabilities from similar or like systems that may also affect the target systems.
- Verify all vulnerabilities found during the exploit research phase for false positives and false negatives.
- Verify all positives (be aware of your contract if you are attempting to intrude or might cause a
  denial of service).

3.1.6 Firewall Testing

The firewall controls the flow of traffic between the enterprise network, the DMZ, and the Internet. It operates on a security policy and uses ACLs (Access Control Lists). This module is designed to assure that only that which should be expressly permitted be allowed into the network, all else should be denied. Additionlly, the tester is to understand the configuration of the firewall and the mapping it provides through to the servers and services behind it. Reviewing the server logs is needed to verify the tests performed on the Internet presence especially in cases where results of the tests are not immediately visible to the tester. Many unknowns are left to the analyst who has not reviewed the logs.

Expected Results:
Information on the firewall as a service and a system
Information on the features implemented on the firewall
Outline of the network security policy by the ACL
List of the types of packets which may enter the network
List of the types of protocols with access inside the network
List of live systems found
List of packets which entered the network by port number
List of protocols which entered the network
List of unmonitored paths into the network

Tasks to perform for a thorough router ACL test:
Firewall and features Identification:

- Verify the router type with information collected from intelligence gathering.
- Verify if the router is providing network address translation (NAT)
- Verify the penetrations from strategically determined packet TTL settings (Firewalking) completed in the Port Scanning module.

Verify firewall ACL configuration:

- Test the ACL against the written security policy or against the "Deny All" rule.
- Verify that the firewall is egress filtering local network traffic
- Verify that the firewall is performing address spoof detection
- Verify the penetrations from inverse scanning completed in the Port Scanning module.
- Test the firewall outbound capabilities from the inside.
- Determine the success of various packet response fingerprinting methods through the firewall.
- Verify the viability of SYN stealth scanning through the firewall for enumeration.
- Measure the use of scanning with specific source ports through the firewall for enumeration.
- Measure the ability of the firewall to handle overlapped fragments such as that used in the TEARDROP attack.
- Measure the ability of the firewall to handle tiny fragmented packets
- Test the firewall’s ability to manage an ongoing series of SYN packets coming in (flooding).

- Test the firewall's response to packets with the RST flag set.
- Test the firewall's management of standard UDP packets.
- Verify the firewall's ability to screen enumeration techniques using ACK packets.
- Verify the firewall's ability to screen enumeration techniques using FIN packets.
- Verify the firewall's ability to screen enumeration techniques using NULL packets.
- Verify the firewall's ability to screen enumeration techniques measuring the packet window size (WIN).
- Verify the firewall's ability to screen enumeration techniques using all flags set (XMAS).
- Verify the firewall's ability to screen enumeration techniques using IPIDs.
- Verify the firewall's ability to screen enumeration techniques using encapsulated protocols.
- Measure the robustness of firewall and it's susceptibility to denial of service attacks with sustained TCP connections.
- Measure the robustness of firewall and it's susceptibility to denial of service attacks with temporal TCP connections.
- Measure the robustness of firewall and it's susceptibility to denial of service attacks with streaming UDP.
- Measure the firewall's response to all types of ICMP packets.

Verify firewall ACL configuration:

- Test the firewall logging process.
- Verify TCP and UDP scanning to server logs.
- Verify automated vulnerability scans.
- Verify services' logging deficiencies.

3.1.7 Password Cracking

Password cracking is the process of validating password strength through the use of automated password recovery tools that expose either the application of weak cryptographic algorithms, incorrect implementation of cryptographic algorithms, or weak passwords due to human factors. This module should not be confused with password recovery via sniffing clear text channels, which may be a more simple means of subverting system security, but only due to unencrypted authentication mechanisms, not password weakness itself. [Note: This module could include manual password guessing techniques, which exploits default username and password combinations in applications or operating systems (e.g. Username: System Password: Test), or easy-to-guess passwords resulting from user error (e.g. Username: joe Password: joe). This may be a means of obtaining access to a system initially, perhaps even administrator or root access, but only due to educated guessing. Beyond manual password guessing with simple or default combinations, brute forcing passwords for such applications as Telnet, using scripts or custom programs, is almost not feasible due to prompt timeout values, even with multi-connection (i.e. simulated threading) brute force applications.]

Once gaining administrator or root privileges on a computer system, password cracking may assist in obtaining access to additional systems or applications (thanks to users with matching passwords on multiple systems) and is a valid technique that can be used for system leverage throughout a security test. Thorough or corporate-wide password cracking can also be performed as a simple after-action exercise and may highlight the need for stronger encryption algorithms for key systems storing passwords, as well as highlight a need for enforcing the use of stronger user passwords through stricter policy, automatic generation, or pluggable authentication modules (PAMs).

Expected Results:
Password file cracked or uncracked
List of login IDs with user or system passwords
List of systems vulnerable to crack attacks
List of documents or files vulnerable to crack attacks
List of systems with user or system login IDs using the same passwords

Tasks to perform for a thorough Password Cracking verification:

- Obtain the password file from the system that stores usernames and passwords
  - For Unix systems, this will be either /etc/passwd or /etc/shadow
  - For Unix systems that happen to perform SMB authentication, you can find NT passwords in /etc/smbpasswd
  - For NT systems, this will be /winnt/repair/Sam._ (or other, more difficult to obtain variants)
  -
- Run an automated dictionary attack on the password file
- Run a brute force attack on the password file as time and processing cycles allow
- Use obtained passwords or their variations to access additional systems or applications

- Run automated password crackers on encrypted files that are encountered (such as PDFs or Word documents) in an attempt to gather more intelligence and highlight the need for stronger document or file system encryption.

3.1.8 Denial of Service Testing

Denial of Service (DoS) is a situation where a circumstance, either intentionally or accidentally, prevents the system from functioning as intended. In certain cases, the system may be functioning exactly as designed however it was never intended to handle the load, scope, or parameters being imposed upon it.

It is very important that DoS testing receives additional support from the organization and is closelymonitored. Flood and Distributed (DDoS) attacks are specifically not tested and forbidden to be tested as per this manual. Well resourced floods and DDoS attacks will ALWAYS cause certain problems and often not just to the target but also to all routers and systems between the tester and the target.

Expected Results:
List weak points in the Internet presence including single points of failure
Establish a baseline for normal use
List system behaviors to heavy use
List DoS vulnerable systems

Tasks to perform for a thorough DOS test:

- Verify that administrative accounts and system files and resources are secured properly and all access is granted with "Least Privilege".
- Check the exposure restrictions of systems to non-trusted networks
- Verify that baselines are established for normal system activity
- Verify what procedures are in place to respond to irregular activity.
- Verify the response to SIMULATED negative information (propaganda) attacks.
- Test heavy server and network loads.

3.1.9 Wireless Networks Testing

This is a method for testing access to 802.11 WLANs, which are becoming increasingly popular. However, some fairly alarming security problems are common when implementing these technologies. This is mainly because these networks are very quickly and easily thrown together, but security measures are not part of the default setup. There are some basic things that can be done to improve security and some more drastic measures that can be taken to make WLANs fairly secure.

802.11 Specifications:

Physical Layer: Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), infrared (IR)
Default encryption: RC4-based stream encryption algorithm for confidentiality, authentication and integrity. Limited Key management.
Operating Range: About 150 feet indoors and 1500 feet outdoors.

Implementations:

802.11a

- Operates in the 5GHz frequency range
- Not compatible with 802.llb or 802.11g hardware
- Maximum speed of 54Mbps

802.11b

- Operates in the 2.4GHz frequency range
- Currently the most widely deployed standard
- Maximum speed of 11Mbps

802.11g

- Operates in the 2.4 GHz frequency range
- Maximum speed of 54Mbps standard
- Expected to be backward compatible with the 802.11b hardware

Evaluate Business Needs, Practices, and Policies:

- Verify that the organization has an adequate security policy that addresses the use of wireless technology, including the use of 802.11.

Evaluate Hardware, Firmware, and Updates.

- Perform a complete inventory of all wireless devices on the network.

Evaluate Access Control, Perimeter Security, and Ability to Intercept or Interfere with
Communication:

- Determine the level of physical access controls to access points and devices controlling them (keyed locks, card badge readers, cameras...).

Evaluate Administrative Access to Wireless Devices:

- Determine if access points are turned off during portions of the day when they will not be in use.

Evaluate Configuration, Authentication and Encryption of Wireless Networks:

- Verify that the access point's default Service Set Identifier (SSID) has been changed.

Evaluate Wireless Clients:

- Verify that all wireless clients have antivirus software installed

Κεφάλαιο 4 Συμπεράσματα

4.1 Αποτελέσματα Εργασίας

Με τη διεξαγωγή ελέγχου ασφαλείας που υλοποιήθηκε σε αυτήν την πτυχιακή καταλήξαμε στα παρακάτω :

1. Με τη χρήση συγκεκριμένων εφαρμογών μπορούμε να βρούμε αδυναμίες στο εκάστοτε λειτουργικό σύστημα όπου εκμεταλλευόμενοι αυτές του τις αδυναμίες μπορούμε να του προκαλέσουμε ζημιά.
2. Με την εφαρμογή μετρών προστασίας είναι δυνατή η μείωση του κινδύνου όχι όμως και της πλήρως εξάλειψης του. του εφαρμόσουμε τα συγκεκριμένα μέτρα προστασίας .

4.2 Μελλοντική Έρευνα

Θα πρέπει λοιπόν με το σχεδιασμό και την υλοποίηση διαδικασιών να βελτιώνουμε συνεχώς την ασφάλεια του δικτύου ή του συστήματος, να επιδιώκουμε την αποφυγή ανεπιθύμητων καταστάσεων, να διασφαλίζουμε τα δεδομένα και τις πληροφορίες και να εκπαιδεύουμε τους χρήστες του δικτύου ή του συστήματος με την χρήση πολιτικών ασφαλείας.

Βιβλιογραφία

- Hacking Exposed 5th Edition
- Open-Source Security Testing Methodology Manual
- Security Power Tools

Παράρτημα Α Συντομογραφίες

ACK	ACKnowledge
ACL	Access Control List
AES	Advanced Encryption Standard
ASP	Active Server Page
CS	Client/Server
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DMZ	Data Management Zone
DNS	Domain Name System
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
ID	Identification Number
IP	Internet Protocol
ISP	Internet Service Provider
MSDOS	MicroSoft Disk Operating System
MAC	Media Access Control
OS	Operating System
PING	Packet INternet Groper
SP	Service Pack
SYN	SYNchronize
TCP	Transmission Control Protocol
TTL	Time To Live
UDP	User Datagram Protocol