**ΑΤΕΙ ΠΕΛΟΠΟΝΝΗΣΟΥ**
**ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ**
**ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ**

**ΤΙΤΛΟΣ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ**

# "Ασφάλεια δικτύων και προστασία των πληροφοριακών δεδομένων με την χρήση των «honeypots»"

**ΤΟΥ : ΣΑΛΙΑΡΑ ΝΙΚΟΛΑΟΥ**

**ΕΠΙΒΛ. ΚΑΘΗΓΗΤΗΣ : ΚΑΡΑΜΠΑΤΣΟΣ ΒΑΣΙΛΕΙΟΣ**

**ΣΠΑΡΤΗ 2016**

ΔΗΛΩΣΗ ΜΗ ΛΟΓΟΚΛΟΠΗΣ ΚΑΙ ΑΝΑΛΗΨΗΣ ΠΡΟΣΟΠΙΚΗΣ ΕΥΘΥΝΗΣ

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ενυπογράφως ότι είμαι αποκλειστικός συγγραφέας της παρούσας Πτυχιακής Εργασίας, για την ολοκλήρωση της οποίας κάθε βοήθεια είναι πλήρως αναγνωρισμένη και αναφέρεται λεπτομερώς στην εργασία αυτή. Έχω αναφέρει πλήρως και με σαφείς αναφορές, όλες τις πηγές χρήσης δεδομένων, απόψεων, θέσεων και προτάσεων, ιδεών και λεκτικών αναφορών, είτε κατά κυριολεξία είτε βάση επιστημονικής παράφρασης. Αναλαμβάνω την προσωπική και ατομική ευθύνη ότι σε περίπτωση αποτυχίας στην υλοποίηση των ανωτέρω δηλωθέντων στοιχείων, είμαι υπόλογος έναντι λογοκλοπής, γεγονός που σημαίνει αποτυχία στην Πτυχιακή μου Εργασία και κατά συνέπεια αποτυχία απόκτησης του Τίτλου Σπουδών, πέραν των λοιπών συνεπειών του νόμου περί πνευματικών δικαιωμάτων. Δηλώνω, συνεπώς, ότι αυτή η Πτυχιακή Εργασία προετοιμάστηκε και ολοκληρώθηκε από εμένα προσωπικά και αποκλειστικά και ότι, αναλαμβάνω πλήρως όλες τις συνέπειες του νόμου στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δε μου ανήκει διότι είναι προϊόν λογοκλοπής άλλης πνευματικής ιδιοκτησίας.

Όνομα και Επώνυμο Συγγραφέα (Με κεφαλαία):

…….....

Υπογραφή (Ολογράφως, χωρίς μονογραφή):

…….

Ημερομηνία (Ημέρα – Μήνας – Έτος):

……..

**ΠΕΡΙΛΗΨΗ**

Ζούμε πλέον σε μια εποχή που θέλοντας και μη, η καθημερινή επαφή με το διαδίκτυο είναι αναπόφευκτη. Σταθεροί υπολογιστές, φορητοί, tablets, και κινητά τηλέφωνα είναι συνδεδεμένα στο διαδίκτυο, και περιέχουν από καθημερινές στιγμές με φίλους σε φωτογραφίες μέχρι και τραπεζικούς λογαριασμούς για αγορές μέσω διαδικτύου. Πόσο ασφαλή είναι τα δεδομένα μας; Γιατί κάποιος άγνωστος να ασχοληθεί για να κάνει κακό σε μας;

Στην παρακάτω εργασία θα γνωρίσουμε καλύτερα το διαδίκτυο, πως ξεκίνησε και πως έχει εξελιχθεί, τι κινδύνους έχει αλλά και τι μηχανισμούς ασφάλειας μπορούμε να χρησιμοποιήσουμε, όπως για παράδειγμα τα honeypots, που αποτελούν μια νέα τεχνολογία που έχει τις δυνατότητες αν χρησιμοποιηθεί σωστά να αποτελέσει την βάση για την εξέλιξη των συστημάτων ανίχνευσης επιθέσεων.

Στο τέλος θα παρουσιάσουμε την εγκατάσταση ενός συστήματος honeypot, και την συμπεριφορά του όταν γίνει στόχος από επιθέσεις τύπου άρνησης υπηρεσίας( DDOS), αλλά και το πως θα αξιοποιήσουμε την αλληλεπίδραση του με τον επιτιθέμενο, για την άντληση χρήσιμών πληροφοριών.

## ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ

honeypots, honeynets, firewalls, DDOS Attack, κατανεμημένες επιθέσεις άρνησης υπηρεσίας, διαδίκτυο, συστήματα ανίχνευσης επιθέσεων, συστήματα πρόληψης επιθέσεων,

# Πίνακας περιεχομένων

## Πίνακας Σχημάτων

# Κεφάλαιο 1 – ΕΙΣΑΓΩΓΗ

Σύμφωνα με πρόσφατες μελέτες το διαδίκτυο απαριθμεί περισσότερες από 14,3 τρις σελίδες και πάνω από 672 Exabyte's διαθέσιμων πληροφοριών(πηγή: internetlivestats.com). Ο αριθμός των ανθρώπων που έχουν πρόσβαση είναι λίγο λιγότερος από το μισό πληθυσμό της γης ( 3 δις χρήστες ). Όσο εύκολα λοιπόν στον πραγματικό κόσμο μπορεί να εξαλειφτεί το έγκλημα και η παραβατικότητα άλλο τόσο και στο διαδίκτυο. Είναι σχεδόν αδύνατο να υπάρξει απόλυτη ασφάλεια, παρά τις σημαντικές προόδους στα συστήματα ασφάλειας η εξέλιξη των απειλών και του κακόβουλου λογισμικού θα είναι φρενήρης.

Στις μέρες μας υπάρχει ποικιλομορφία απειλών και κακόβουλου λογισμικού, μέσω των συστημάτων που έχουν πρόσβαση στο διαδίκτυο οι μολύνσεις μεταφέρονται στα συστήματα που αλληλεπιδρούν μεταξύ τους. Οι κακόβουλοι χρήστες εξαπολύουν μολύνσεις οι οποίες αναπτύσσονται στα ευάλωτα συστήματα τα οποία μεταφέρουν χωρίς την συγκατάθεση τους στη συνέχεια τις μολύνσεις στις συσκευές η στα συστήματα που θα αλληλεπιδράσουν.

Αντικείμενο της εργασίας αυτής είναι η ασφάλεια δικτύων και η προστασία των δεδομένων με την χρήση τεχνολογιών honeypot. Οι τεχνολογίες αυτές μας δίνουν την δυνατότητα μέσω ενός ασφαλούς περιβάλλοντος, να παρατηρήσουμε σε πραγματικό χρόνο επιθέσεις προς το σύστημα μας, αντλώντας πολύτιμες πληροφορίες από τον επιτιθέμενο αλλά και από τα τρωτά σημεία του συστήματος.

Στόχος είναι να εναρμονιστεί η ενεργητική ασφάλεια των υπολογιστικών συστημάτων με την παθητική. Στην τόσο απαιτητική κοινωνία που ζούμε γεμάτη από απειλές η καθημερινή αναβάθμιση της ασφάλειας των συστημάτων που εκτίθενται σε δίκτυα, είναι μονόδρομος.

Αξία δεν έχουν πλέον μόνο τα δεδομένα η οι πληροφορίες που διακινούνται αλλά και οι υπολογιστικοί πόροι όπου πολλές φορές καταστρατηγούνται για την διεκπεραίωση κακόβουλων διεργασιών. Για τον λόγο αυτό η χρήση της παθητικής ασφάλειας μας δίνει την δυνατότητα τις περαιτέρω έρευνας και αξιολόγησης των συστημάτων ενεργητικής ασφάλειας που διαθέτουμε.

Το honeypot που χρησιμοποιήθηκε είναι το HoneyBot ένα πρόγραμμα ελεύθερης άδειας, με παγκόσμιες επιτυχίες στον αγώνα κατά του κακόβουλου λογισμικού, σε συνδυασμό με εργαλεία δικτυακής ανάλυσης όπως το wireshark μπορούν να δώσουν απαντήσεις σε πολλά ερωτήματα που μας απασχολούν, όπως για παράδειγμα εάν υπάρχει συγκεκριμένο μοτίβο συμπεριφοράς στους κακόβουλους χρήστες η ακόμα τι ακριβώς γίνεται κατά την διάρκεια μιας επίθεσης.

## 1.1 Το Διαδίκτυο

Στις μέρες μας πλέον το διαδίκτυο είναι γεγονός, είναι ένα κομμάτι της καθημερινότητας και για τους περισσότερους ανθρώπους αποτελεί ένα εργαλείο, άλλες φορές δουλείας και άλλες διασκέδασης.

Ας το γνωρίσουμε όμως λίγο καλύτερα για να είμαστε και στη θέση να αντιληφθούμε την πραγματική του αξία. Το διαδίκτυο είναι ένα παγκόσμιο δίκτυο το οποίο περιλαμβάνει εκατομμύρια μικρότερα δίκτυα, υπολογιστές και άλλες συσκευές συνδεδεμένες μεταξύ τους. Μπορεί πολύ εύκολα να παρομοιαστεί με έναν ζωντανό οργανισμό καθώς το εσωτερικό του από την μία είναι πλήρως διαδραστικό, μετακινώντας οι χρήστες που το χρησιμοποιούν πληροφορίες από και προς τους υπολογιστές τους ασταμάτητα. Και από την άλλη το μέγεθος του καθημερινά αυξάνεται με γεωμετρικούς ρυθμούς.

Το internet βλέπουμε πως δεν είναι απλά ένα υπερδίκτυο υπολογιστικών συστημάτων η ένα σύνολο συνδεδεμένων υπολογιστών, ούτε όμως και μια μεγάλη ομάδα μικρότερων δικτύων. Ουσιαστικά πρόκειται για ένα αγαθό επικοινωνίας της ανθρωπότητας, ένας δίαυλος διακίνησης πληροφοριών ιδεών και δεδομένων. Είναι αμερόληπτο, δεν κάνει διακρίσεις ανάμεσα στους χρήστες, ο καθένας μπορεί να επισκεφτεί την ηλεκτρονική σελίδα της επιλογής του, ή κάποιος επαγγελματίας να επικοινωνήσει με ένα προμηθευτή που βρίσκεται σε άλλη χώρα και έχει καλύτερες πρώτες ύλες σε ποιο ανταγωνιστική τιμή από την αγορά που δραστηριοποιείται. Επίσης δεν κλείνει ποτέ και δεν ελέγχεται από κάποιον. Είναι διαθέσιμο εικοσιτέσσερις ώρες την ημέρα εφτά φορές την εβδομάδα. Για τον λόγο αυτό δεν άργησε να αξιοποιηθεί και από τις κυβερνήσεις για την διευκόλυνση της εφαρμογής της δημοκρατίας σε θέματα διαφάνειας των διαδικασιών και των θεσμών όπως για παράδειγμα σε εκλογές, όπως ακόμη προσέφερε και στον τομέα της εκπαίδευσης με την εμφάνιση των εφαρμογών τηλεκπαίδευσης πολλοί άνθρωποι που δεν μπορούσαν δυστυχώς να μετακινηθούν από το σπίτι τους κατάφεραν τελικά με την βοήθεια του διαδικτύου να σπουδάσουν, μια δυνατότητα που κάποια χρόνια πριν θα φάνταζε απίθανη. Ακόμα και στην ιατρική η προσφορά ήταν μεγάλη. Επιστήμονες απ’ όλο τον κόσμο μπόρεσαν την ίδια στιγμή από διαφορετικά μέρη να ανταλλάξουν απόψεις για σοβαρές εγχειρήσεις και περιστατικά σαν να ήταν στον ίδιο δωμάτιο. Και οι ασθενείς των ακριτικών περιοχών με τις εφαρμογές

της τηλεϊατρικής κατάφεραν να συμβουλευτούν τον γιατρό που είχαν ανάγκη όταν δεν ήταν δυνατή η φυσική παρουσία του.

Μέχρι τώρα μιλήσαμε ως επί το πλείστον για τα θετικά του διαδικτύου, καλό θα είναι όμως να αναφερθούμε και σε κάποια κομμάτια που εφιστούν την προσοχή μας. Όσο το internet είναι ελεύθερο και μπορούν όλοι να συμμετέχουν σε αυτό τόσο θα υπάρχει και η πιθανότητα ένα μέρος των χρηστών να εισέρχονται για να ενεργήσουν αθέμιτα σε βάρος άλλων ανθρώπων. Πρέπει να είμαστε προσεκτικοί σε κάθε βήμα που κάνουμε μέσα στο διαδίκτυο και να προσέχουμε τα παιδιά που πλέον στις μέρες μας έχουν πρόσβαση στην τεχνολογία από πολύ μικρή ηλικία. Σύμφωνα με πρόσφατη έρευνα που έγινε για την διείσδυση της χρήσης των υπολογιστών και του διαδικτύου στα παιδία τα αποτελέσματα ξάφνιασαν καθώς 1 στα 5 παιδιά ηλικίας 7 έως 12 ετών έχουν κινητό τηλέφωνο. Παράλληλα στις ίδιες ηλικίες η χρήση προσωπικού υπολογιστή αγγίζει το 90% με 3 στα 5 παιδία να τον χρησιμοποιούν καθημερινώς . Το ποσοστό δε που χρησιμοποιεί το διαδίκτυο ανέρχεται στο 80,6% .(Μαλλάς Δημήτης, 2015, Σε Άνοδο η χρήση του Διαδικτύου, focus Bari)Καταλαβαίνουμε λοιπόν πως είναι αναγκαίο να ελέγχεται το παιδί η ο έφηβος στις πληροφορίες που θα έχει πρόσβαση από τον γονέα κυρίως για να μη βρεθεί στη δυσάρεστη θέση σε ακατάλληλο για τον ψυχικό του κόσμο υλικό η ακόμα και στην πιθανότητα παρενόχλησης.

Το internet σήμερα έχει και κάποια παράγωγα εργαλεία τα οποία βασίζονται στην φιλοσοφία και την αρχιτεκτονική του, προσφέρουν όμως περιορισμένες δυνατότητες προσπέλασης των πληροφοριών που περιέχουν στο ευρύ κοινό. Δύο από αυτά τα παράγωγα είναι το ενδοδίκτυο ( intranet ) και το εξωτερικό δίκτυο ( extranet ). Κάτι που με μια απλή σκέψη θα φάνταζε άχρηστο αφού υπερκαλύπτεται από την δυναμική του internet το intranet τυγχάνει μεγάλης αποδοχής από μεγάλες εταιρίες όπως οι τράπεζες που θέλουν να χρησιμοποιούν ένα δίκτυο που να εξυπηρετεί μεγάλη γεωγραφική κλίμακα και πολλούς χρήστες ταυτόχρονα σε ένα εσωτερικό περιβάλλον πλήρως ελεγχόμενο με διαβαθμιζόμενη ασφάλεια στην διάθεση των πληροφοριών που περιλαμβάνει και ολοκληρωτικό αποκλεισμό των χρηστών που δεν είναι εργαζόμενοι της τράπεζας. Η χρήση του εσωτερικού δικτύου μετά από καιρό φανέρωσε κάποια κενά που έπρεπε να εξυπηρετηθούν. Για παράδειγμα γιατί κάποιος συνεργάτης προμηθευτής μιας μεταφορικής εταιρίας που χρησιμοποιεί το intranet να μην μπορεί να παραθέσει δεδομένα σχετικά με τα προϊόντα την διαθεσιμότητα του αλλά και στατιστικά στοιχεία, εμπλουτίζοντας το εσωτερικό δίκτυο με χρήσιμες πληροφορίες άμεσα διαθέσιμες ; Χάρης

αυτού αλλά και άλλων παρόμοιων ερωτημάτων αναπτύχθηκε το εξωτερικό δίκτυο extranet. Ουσιαστικά είναι ένα εσωτερικό δίκτυο με προθήκες μικρότερων εξωτερικών δικτύων όπου πάλι και εδώ τα δεδομένα είναι διαθέσιμα με κλιμακούμενη σε επίπεδα ασφάλεια για τους χρήστες που έχουν πρόσβαση στο extranet, και για τους υπόλοιπους χρήστες του διαδικτύου προστατεύονται και αποκλείονται με τη χρήση τοίχων προστασίας ( firewall).

### 1.2 Αρχιτεκτονική και Κατηγορίες Δικτύων Υπολογιστών

Η αρχιτεκτονική στο διαδίκτυο αναφέρεται στα πρότυπα εκείνα που εφαρμόζονται για να εκτελείτε επιτυχώς η επικοινωνία μεταξύ των χρηστών του υλικού αλλά και των προγραμμάτων που συνεργάζονται. Στο διαδίκτυο λειτουργεί η αρχιτεκτονική λογισμικού πελάτη εξυπηρετητή ( client – server ). Ο πελάτης ζητά μια πληροφορία έναν πόρο η έναν υπολογισμό και στη συνέχεια ένα άλλο λογισμικό ο εξυπηρετητής ή αλλιώς διακομιστής, επιστρέφει το αποτέλεσμα. Ο διακομιστής έχει την δυνατότητα να καλύψει πληθώρα πελατών και ερωτημάτων προς εκτέλεση. Οι πελάτες και οι εξυπηρετητές επικοινωνούν χρησιμοποιώντας σύνολα από κανόνες επικοινωνίας, τα λεγόμενα πρωτόκολλα. Μια απλή εμφάνιση μιας ιστοσελίδας για να επιτευχθεί πρέπει ο πελάτης ( λογισμικό ) να στείλει αίτημα στο λογισμικό εξυπηρετητή και αυτός με τη σειρά του να απαντήσει στο αίτημα αποστέλλοντας τελικά την σελίδα στον πελάτη.

Οι κατηγορίες δικτύων που χρησιμοποιούνται σήμερα ποικίλουν και διαχωρίζονται γεωγραφικά ανάλογα με την έκταση, τον τηλεπικοινωνιακό πάροχο, τις τεχνικές αποστολής των πληροφοριών, τα λειτουργικά συστήματα που περιλαμβάνουν, τα πρωτόκολλα που χρησιμοποιούν και τέλος το μοντέλο επικοινωνίας που χρησιμοποιούν. Ένα προς ένα από τα παραπάνω θα τα εξετάσουμε στη συνέχεια.

Γεωγραφικός Σχεδιασμός Δικτύων χωρίζεται σε :

- Τοπικά Δίκτυα ( LAN Local Area Network ) Περιλαμβάνουν μια ομάδα συνδεδεμένων υπολογιστών που καταλαμβάνουν μια πεπερασμένη σχετικά μικρή γεωγραφική περιοχή όπως μια αίθουσα διδασκαλίας ηλεκτρονικών υπολογιστών ή ένα κτήριο μιας επιχείρησης. Ο ποιο ουσιαστικός λόγος για να επιλεγεί ο συγκεκριμένος τύπος δικτύων είναι όταν θέλουμε να μοιράσουμε συσκευές όπως εκτυπωτές σαρωτές και άλλα εργαλεία. Λόγο της μικρής τους έκτασης και των

υψηλών ταχυτήτων που υποστηρίζουν οι καλωδιώσεις των τοπικών δικτύων υπάρχει μεγάλη ταχύτητα στις μεταφορές των πληροφοριών.

- Μητροπολιτικό Δίκτυο ( MAN Metropolitan Area Network ) Είναι ουσιαστικά ένα τοπικό δίκτυο που έχει τη δυνατότητα να εξυπηρετήσει μια ολόκληρη πόλη. Το δίκτυο λαμβάνει την κυκλοφορία των πληροφοριών από το τοπικό δίκτυο και το προωθεί σε κάποιο άλλο τοπικό δίκτυο η σε ένα δίκτυο ευρείας περιοχής. Συνδέει χιλιάδες διαφορετικά σημεία μέσα σε μια πόλη από σχολεία και νοσοκομεία μέχρι στρατόπεδα και σπίτια μέσω δικτύων οπτικών ινών.
- Δίκτυα Ευρείας Περιοχής ( WAN Wide Area Network ) Αποτελούν ένα σύνολο από υπολογιστές που μπορεί να εκτείνονται από μια μικρή πόλη ή μια χώρα μέχρι μια ήπειρο ή ολόκληρο τον κόσμο όπως για παράδειγμα το internet. Τα δίκτυα ευρείας περιοχής περιλαμβάνουν μητροπολιτικά και τοπικά δίκτυα όπως είναι φυσικά επόμενο.

### 1.2.1 Με Βάση τον Πάροχο Τηλεπικοινωνίας

- Ιδιωτικά Δίκτυα ( Private Networks ) καλούνται τα δίκτυα που περιέχουν διευθύνσεις οι οποίες δεν είναι επισκέψιμες από χρήστες που είναι εκτός του ιδιωτικού δικτύου. Οι διευθύνσεις αυτές προέρχονται από τον ιδιωτικό χώρο διευθύνσεων και οι συνδεδεμένοι υπολογιστές του δικτύου επικοινωνούν κανονικά χωρίς περιορισμούς.
- Δημόσια Δίκτυα ( Public Networks ) Είναι δίκτυα ελεύθερα στο κοινό, ο καθένας μπορεί να συνδεθεί σε αυτά, γεγονός που πρέπει να γνωρίζουμε κάθε φορά που γινόμαστε μέλος ενός τέτοιου δικτύου και να λαμβάνουμε τα κατάλληλα μέτρα προστασίας, επειδή ο κίνδυνος είναι αυξημένος. Τα δημόσια δίκτυα τα συναντάμε σε πλατείες, καφετέριες και εμπορικά κέντρα.

### 1.2.2 Με Βάση τις Τεχνικές Αποστολής των Πληροφοριών

- Δίκτυα Ακρόασης ( Broadcasting Networks ) Σε αυτή την περίπτωση των δικτύων το μέσω επικοινωνίας για όλους τους χρήστες είναι κοινό. Οι πληροφορίες που αποστέλλει ένας σταθμός γίνονται ορατές από όλους τους συνδεδεμένους χρήστες. Δε συναντάμε κόμβους επικοινωνίας όπως σε άλλες

μορφές δικτύων και υπάρχει περίπτωση πολλοί χρήστες να μοιράζονται το ίδιο μέσο μετάδοσης. Παραδείγματα τέτοιων δικτύων είναι τα δίκτυα ραδιοφώνου, τα δορυφορικά αλλά και τα τοπικά δίκτυα.

- Δίκτυα Μεταγωγής ( Switching Networks ) Η μεταφορά των δεδομένων στο συγκεκριμένο τύπο δικτύων από έναν σταθμό προς κάποιον άλλο γίνεται μέσω ενδιάμεσων κόμβων που μεσολαβούν μέχρι να φτάσει η πληροφορία στον σωστό αποδέκτη. Παράλληλα οι κόμβοι είναι κατασκευασμένοι με τέτοιο τρόπο, που μπορούν να υποστηρίξουν κατά την μεταφορά εναλλακτική διαδρομή αν η αρχική αντιμετωπίζει πρόβλημα. Οι κυριότερες τεχνικές μετάδοσης που υπάρχουν είναι τρεις : Η μεταγωγή πακέτων, η μεταγωγή κυκλώματος και η μεταγωγή μηνύματος.

### 1.2.3 Με Βάση τα Λειτουργικά Συστήματα

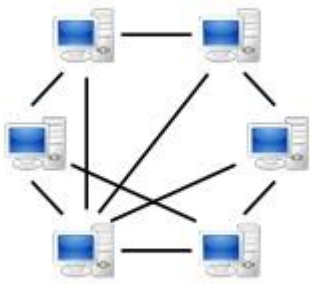
- Windows Δίκτυα : Τα δίκτυα που μπορούμε να υλοποιήσουμε με την χρήση του λειτουργικού συστήματος των windows. Υλοποιούνται είτε ασύρματα είτε ενσύρματα και υπάρχουν 5 διαφορετικές επιλογές που έχει ο χρήστης.
    1. Οικιακό Δίκτυο ( Home Network ) Η επιλογή του δικτύου αυτού είναι ποιο κατάλληλη όταν χρησιμοποιείται για οικιακή χρήση και τα μέλη του δικτύου μας είναι γνωστά και έμπιστα. Οι υπολογιστές μέλη του δικτύου βλέπουν ο ένας τον άλλο, μπορούν να μοιραστούν δεδομένα και συσκευές.
    2. Δίκτυο Εργασίας ( Work Network ) Είναι ιδανικό για μικρές επιχειρήσεις που χρειάζεται η ανταλλαγή πληροφοριών από χρήστη σε χρήστη, αλλά και η κοινή χρήση των συσκευών. Υπάρχει τέλος και η δυνατότητα της παραμετροποίησης του δικτύου για να καθορίσει το βαθμό που θα είναι διαθέσιμες οι πληροφορίες που διακινούνται στο δίκτυο από τα μέλη του.
    3. Δημόσιο Δίκτυο ( Public Network ) Το προφίλ του δικτύου που είναι κατάλληλο όταν ο υπολογιστής εισέλθει σε ένα δημόσιο δίκτυο π.χ. σε ένα εμπορικό κέντρο. Οι τεχνικές που εφαρμόζει το δίκτυο αυτό είναι για την προστασία κυρίως του υπολογιστή αφού φανερώνει όσο το δυνατόν λιγότερες πληροφορίες του υπολογιστή μας στο δίκτυο.
    4. Δίκτυα Τομέα ( Domain Network ) Χρησιμοποιούνται από μεγάλες εταιρίες όπως τράπεζες που διαθέτουν δίκτυα υπολογιστών που καλύπτουν μεγάλη

έκταση. Η τροποποίηση και η συντήρηση γίνεται από ειδικά τμήματα πληροφορικής που ασχολούνται μόνο με την σωστή διαχείριση του συστήματος.

5. Δίκτυα Hoc : Αποτελούν τα δίκτυα στα οποία δυο υπολογιστές συνδέονται ασύρματα απευθείας μεταξύ τους χωρίς την χρήση κάποιας συσκευής δρομολόγησης ( router).
    - Δίκτυα AppleTalk : Είναι τα δίκτυα υπολογιστών που κατασκεύασε η Apple για να καλύψει την ανάγκη της δικτύωσης στο λειτουργικό σύστημα macintosh.
    - Δίκτυα Novel : Στα δίκτυα αυτά συμμετέχουν υπολογιστές με DOS λειτουργικό.

### 1.2.4 Με Βάση το Πρωτόκολλο Επικοινωνίας

- Δίκτυα TCP/IP : Είναι τα δίκτυα εκείνα που υποστηρίζουν και λειτουργούν με βάση το πρωτόκολλο επικοινωνίας TCP/IP.
- Δίκτυα NET/BEUI (Net BIOS Extended User Interface ): Είναι το πρωτόκολλο που ανέπτυξε η IBM το 1985. Μπορεί να εξυπηρετήσει μέχρι 200 χρήστες αλλά δεν υποστηρίζει την δυνατότητα της δρομολόγησης γι' αυτό και δεν ανταποκρίνεται σε δίκτυα με μεγαλύτερο αριθμό υπολογιστών.



*ΣΧΗΜΑ 2.1: Δίκτυο P2P (πηγή: Wikipedia).*

### 1.2.5 Με Βάση το Μοντέλο Επικοινωνίας

- P2P ( Peer to Peer ) : Πρόκειται για ένα μοντέλο διαμοιρασμού δεδομένων απ' ευθείας από την θέση που υπάρχουν. Εμφανίστηκε λίγο πριν το 2000 από την εφαρμογή Napster, και έδωσε τη δυνατότητα στους χρήστες της να αναζητούν και να μοιράζονται δεδομένα από τους servers της εφαρμογής αλλά και από τους ίδιους τους χρήστες μέλη. Το αρνητικό είναι πως πολλές φορές τα δεδομένα προστατεύονται από πνευματικά δικαιώματα και διακινούνται χωρίς την άδεια τον δημιουργών τους. Σε αρκετές χώρες έχει απαγορευτεί το μοντέλο αυτό και οι πάροχοι τηλεπικοινωνιών το αποκλείουν.

- Πελάτη – Εξυπηρετητή ( Client – Server ) : Είναι το βασικό μοντέλο επικοινωνίας που χρησιμοποιείται στο διαδίκτυο. Και οι δύο όροι αναφέρονται σε κομμάτια λογισμικού. Ο πελάτης στέλνει ένα αίτημα προς εκτέλεση στον εξυπηρετητή – διακομιστή, και αυτός με την σειρά του απαντά με το αποτέλεσμα του ερωτήματος. Το συγκεκριμένο μοντέλο αποτελεί ένα πολύ σημαντικό επίτευγμα στις επικοινωνίες και αυτό διότι, δημιουργήθηκαν συστήματα που είναι χαμηλού κόστους με αυξημένη υπολογιστική ισχύ και απόδοση, χαμηλό κόστος συντήρησης και αναβάθμισης.

### 1.3 Βασικοί Όροι Διαδικτύου

- ISP ( Internet Service Provider ) Είναι ο τηλεπικοινωνιακός πάροχος που προσφέρει την δυνατότητα μέσο των δικτυακών υποδομών που διαθέτει, να συνδεθεί οποιοσδήποτε συνδρομητής είναι μέλος του.
- DNS (Domain Name System ) Σύστημα Ονομάτων Τομέων : Είναι ένα σύστημα ονοματοδοσίας που χρησιμοποιείται σε συνδυασμό με το πρωτόκολλο IP για να περιγράψει μια διεύθυνση με χαρακτήρες που χρησιμοποιούνται ποιο εύκολα από τον άνθρωπο αντί για αριθμούς.
- Πακέτο : Αποτελεί την ελάχιστη μονάδα πληροφορίας που διακινείτε εντός των δικτύων. Στο internet οι πληροφορίες για να αποσταλούν, χωρίζονται σε πολλά πακέτα πληροφοριών με ελάχιστο μέγεθος το καθένα. Με την μέθοδο αυτή αποστέλλονται εύκολα στον παραλήπτη όπου γίνεται και η επανασύνδεση.
- Δρομολόγηση ( Routing ) Η διαδικασία κατά την οποία επιλέγεται η κατάλληλη διαδρομή για να φτάσουν τα δεδομένα στη σωστή τοποθεσία.
- Διεύθυνση IP ( Internet Protocol address ) Είναι ένας αριθμός που αντιστοιχεί μοναδικά σε κάθε συσκευή που έχει θέση συνδεδεμένη με το διαδίκτυο. Οι ips χρησιμοποιούνται για να υπάρχει μεταξύ των συσκευών αναγνώριση και συνεργασία στα δίκτυα υπολογιστών που επισκεπτόμαστε μέσω του διαδικτυακού πρωτοκόλλου.
- Πόρτα δικτύου ( port ) Είναι ένας αριθμός μεταξύ του 0-65535 όπου δηλώνει τη μορφή μιας σύνδεσης μεταξύ ενός πελάτη και ενός εξυπηρετητή. Μερικές επίσημες πόρτες είναι η 20 ( μεταφορά δεδομένων ), 23 telnet μη κρυπτογραφημένη επικοινωνία, 80 HTTP διακίνηση ιστοσελίδων, 110 για ηλεκτρονικό ταχυδρομείο.

- Firewall: Σύστημα ελέγχου επικοινωνίας δεδομένων από το εξωτερικό δίκτυο προς τον υπολογιστή κυρίως.
- Router ( δρομολογητής ) Είναι η συσκευή που αναλαμβάνει την αποστολή τον πακέτων με την σωστή σειρά, από και προς των υπολογιστή μας.

### 1.4 Παγκόσμιος Ιστός WWW

Ο παγκόσμιος ιστός είναι μια εφαρμογή που υποστηρίζει το διαδίκτυο. Ο σκοπός της είναι να γίνεται εφικτή η ανάγνωση των εκατομμύρια εγγράφων που υπάρχουν στις σελίδες του διαδικτύου και είναι αποθηκευμένες σε χώρους αποθήκευσης ( web servers ) σε διαφορετικά σημεία σε όλο τον κόσμο. Τα έγγραφα στην ορολογία του παγκόσμιου ιστού αναφέρονται σε έγγραφα κείμενου φυσικά αλλά και σε εικόνες, κινούμενες εικόνες βίντεο και γραφικά . Οι σελίδες μπορούν να περιέχουν αναφορές σε άλλες σελίδες και ο χρήστης να μεταβαίνει αυτόματα κάνοντας "κλικ" στον αντίστοιχο υπερσύνδεσμο ( hyperlink ). Στον ιστό χρησιμοποιείται το πρωτόκολλο μεταφοράς υπερκειμένου HTTP ( Hyper Text Transfer Protocol ), υπερκείμενο λογίζεται το κείμενο που περιέχει υπερσυνδέσεις.

Για να επισκεφτούμε μια σελίδα πρέπει να γνωρίζουμε την ηλεκτρονική της διεύθυνση ή διαφορετικά το URL ( Uniform Resource Locator ). Ένα παράδειγμα είναι η σελίδα της Google : https://www.google.gr , όπου αν αναλύσουμε το συντακτικό της βλέπουμε πώς, το https αναφέρεται στο πρωτόκολλο της υπηρεσίας που χρησιμοποιεί η σελίδα, το HTTPS ( Hypertext Transfer Protocol Secure ) είναι μία έκδοση του http που αναφέραμε και ποιο πάνω αλλά με ασφάλεια για κρυπτογραφημένη επικοινωνία, παλιότερα κυρίως οι σελίδες που διαχειρίζονταν ευαίσθητες πληροφορίες υποστήριζαν το πρωτόκολλο αυτό, σήμερα πλέον είναι αρκετά διαδεδομένο. Στη συνέχεια το www αναφέρει ότι η σελίδα που ακολουθεί είναι κομμάτι του ιστού. Το google δηλώνει την διεύθυνση του web server. Το κομμάτι αυτό επικοινωνεί με ένα DNS serves όπου και γίνεται η αντιστοίχιση με την διεύθυνση IP. Το gr τέλος προσδιορίζει την καταγωγή της συγκεκριμένης τοποθεσίας την Ελλάδα δηλαδή.

Η ιστορία του μετρά από το 1989, όπου κάπου κοντά στη Γενεύη της Ελβετίας οι επιστήμονες του πειραματικού κέντρου CERN ( Conseil Europeenne pour la Recherche Nucleaire ) είχαν την ανάγκη να επικοινωνήσουν μεταξύ τους άμεσα από διαφορετικές

χώρες. Η πρόταση για διασυνδεδεμένα κείμενα σε σελίδες για την επικοινωνία της ομάδας ενάμιση χρόνο μετά είχε υλοποιηθεί.

Τέσσερα χρόνια μετά στις 23 Ιανουαρίου του 1993 ο Marc Andreessen ανακοινώνει το Mosaic. Είχε δημιουργήσει τον πρώτο περιηγητή ( browser ) με γραφικό περιβάλλον και πλέον υπήρχε η δυνατότητα στο κοινό να έχει πρόσβαση εύκολα στο internet. Το νέο μεγάλο βήμα ήταν πως ο χρήστης μπορούσε στις σελίδες που επισκέπτεται να δει και κείμενο αλλά και εικόνες. Η Microsoft δεν θα έμενε θεατής στις τεχνολογίες διαδικτύου και δυο χρόνια αργότερα ξεκίνησε να δημιουργεί τον δικό της περιηγητή με γραφικό περιβάλλον, τον γνωστό μας Internet Explorer.


*ΣΧΗΜΑ 1.2: Ο Πρώτος server του Παγκόσμιου ιστού (πηγή: Wikipedia).*

## 1.5 Ιστορικά Στοιχεία Διαδικτύου

Η πρώτη μορφή διαδικτύου που εμφανίστηκε στον κόσμο ήταν το ARPANET (Advanced Research Projects Agency Network). Ήταν ένα δίκτυο μεταφοράς πακέτων το οποίο ουσιαστικά αποτελεί τον πρόγονο του σημερινού internet, αναπτύχθηκε για να συνδέσει το υπουργείο άμυνας με τα εργαστήρια ερευνών στις Ηνωμένες Πολιτείες. Η χρηματοδότηση καλύφθηκε από το γραφείο ερευνών και αμύνης (Defense Advanced Research Projects Agency – DARPA) .

Στην ανάπτυξη του δικτύου εξέταζαν την μεταφορά δεδομένων μέσω τις διακίνησης των πακέτων. Κατά την λειτουργία αυτή τα δεδομένα προς μεταφορά εκχωρούνται σε πακέτα τα οποία μπορούν να διαμοιραστούν πολλοί χρήστες μέσω κοινής επικοινωνιακής γραμμής. Ο στόχος ήταν να δημιουργηθεί ένα διαδίκτυο που θα εξασφάλιζε την επικοινωνία μεταξύ απομακρυσμένων δικτύων ακόμη και αν κάποιος από τους ενδιάμεσους κόμβους ήταν αποσυνδεδεμένος. Στο πρωτόκολλο επικοινωνίας που χρησιμοποιήθηκε το κάθε πακέτο θα περιελάμβανε τις πληροφορίες που έπρεπε για να καταλήξει στον παραλήπτη όπου θα γίνονταν και η συνολική επανασύνδεση των πακέτων, σε δεδομένα για να μπορούν να αξιοποιηθούν.

Τα πρώτα αποτελέσματα της έρευνας απέδωσαν καρπούς το 1969 όπου και συνδέθηκαν επιτυχώς τρία πανεπιστήμια, το UCLA ( University of California Los Angeles ) το Stanford ( Stanford Research Institute ) και το πανεπιστήμιο της Utah , σε ένα δίκτυο ευρείας περιοχής (WAN, Wide Area Network ) .Στη συνέχεια συνδέθηκε και το πανεπιστήμιο Santa Barbara .

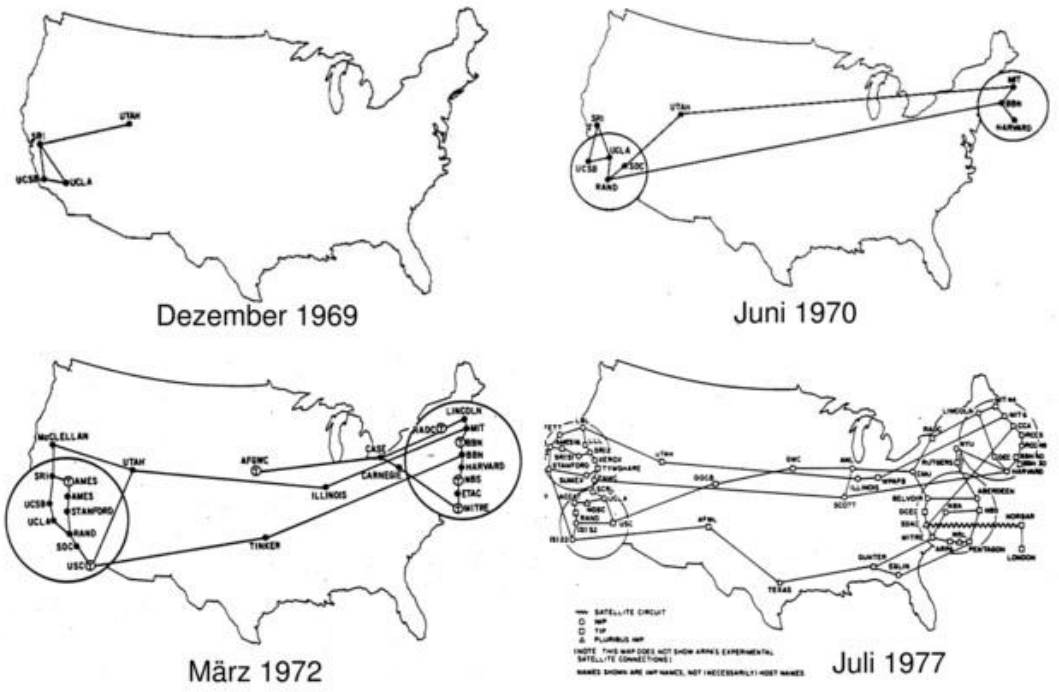
Τρία χρόνια μετά οι ερευνητές του ARPA στην πρώτη διεθνή διάσκεψη σε θέματα υπολογιστών και επικοινωνιών, παρουσίασαν στην Washington των Ηνωμένων Πολιτειών τις εξελίξεις του προγράμματος συνδέοντας χρήστες από 40 διαφορετικές τοποθεσίες.

Η επιτυχία του ARPA έδωσε το έναυσμα για περεταίρω έρευνες των επιστημών πέραν αυτών της Αμερικής σε παγκόσμιο επίπεδο πάνω στην ανάπτυξη του δικτύου. Παράλληλα τα μέλη της συνδιάσκεψης ίδρυσαν μια διεθνή ομάδα εργασίας ( IWG, Internetworking Working Group ) με σκοπό τον την οργάνωση και τον συντονισμό των διεργασιών της έρευνας.

Το νέο στοίχημα της ομάδας ARPA ήταν η αποστολή πληροφοριών και μηνυμάτων εντός του δικτύου, απευθείας όμως χρήστης με χρήστη, μια δυνατότητα που στις μέρες μας είναι γνωστή σαν ηλεκτρονικό ταχυδρομείο (email). Λίγους μήνες μετά ήταν πλέον γεγονός.

Πολύ σημαντικό ρόλο στις έρευνες για την ανάπτυξη του δικτύου είχαν και τα πρωτόκολλα επικοινωνίας (θα έχουμε την ευκαιρία να τα αναλύσουμε εκτενώς στην συνέχεια της εργασίας). Την ίδια περίπου περίοδο βλέπουμε να αναπτύσσονται τα πρώτα πρωτόκολλα host to host, μέχρι τότε το κάθε σύστημα μπορούσε να έχει πρόσβαση στις πληροφορίες του κάθε χρήστη ( host ) μόνο από ένα συγκεκριμένο απομακρυσμένο τερματικό ( remote terminal ).

Το 1983 το ARPANET διασπάστηκε σε δύο κομμάτια, στο πανεπιστημιακό στο οποίο είχαν ελεύθερη πρόσβαση οι ερευνητές και το ακαδημαϊκό κοινό και στο MILNET όπου ήταν το στρατιωτικό κομμάτι με πλήρη ελεγχόμενη πρόσβαση. Ένα χρόνο αργότερα το διαδίκτυο αριθμούσε πάνω από 1000 συνδεδεμένους κόμβους ενώ στην άλλη πλευρά του ατλαντικού, επιστήμονες από το Ισραήλ είχαν ολοκληρώσει το ταχυδρομείο φωνής (voicemail).




*ΣΧΗΜΑ 1.3: Η ανάπτυξη του ARPANET από το 1969 έως και το 1977 (πηγή: itDozent).*

### 1.6 Μοντέλο Αναφοράς OSI

Ο Διεθνής Οργανισμός Τυποποίησης ( OSI International Standards Organisation ) στα τέλη της δεκαετίας του 1980 παροτρύνε την επιστημονική κοινότητα να υιοθετήσει ένα μοντέλο επικοινωνίας επτά επιπέδων που θα καθόριζε την δικτυακή επικοινωνία δύο υπολογιστών. Η ικανότητα του ήταν, πως έδινε τη ευκαιρία σε όλα τα μέλη του δικτύου να λειτουργούν ταυτόχρονα με κάθε μέλος να μπορεί να εκτελεί τουλάχιστον ένα πρωτόκολλο δικτύωσης, χωρίς να είναι υποχρεωτικό να έχουν κοινό κατασκευαστή.

Κάθε επίπεδο του χρησιμοποιεί τις υπηρεσίες που περιέχονται στο κατώτερο επίπεδο και τις εμπλουτίζει, για να προσφέρει ποιο ολοκληρωμένα αποτελέσματα στο επόμενο επίπεδο. Αφού κάθε επίπεδο υποστηρίζει άμεσα τις υπηρεσίες του κατώτερου επιπέδου του θα υποστηρίζει και εμμέσως όλες τις υπηρεσίες των κατώτερων από αυτόν επιπέδων.

Παρόλα αυτά το TCP/IP που ήταν και προγενέστερο, είχε καταφέρει να είναι δημοφιλές και να χρησιμοποιείται σε μεγάλη έκταση. Ακόμα και μέχρι σήμερα δεν κατάφερε να χρησιμοποιηθεί ευρέως διότι επικράτησε η τάση πως οι προδιαγραφές του είναι πολύπλοκες και για να γίνει πλήρως λειτουργικό θα χρειαζόταν να πέραση πολύς καιρός. Παρακάτω θα δούμε αναλυτικά τα επίπεδα του OSI.

- $1^{ο}$ Φυσικό Επίπεδο ( Physical Layer) : Το επίπεδο αυτό ασχολείται με την μεταφορά των ακατέργαστών (raw) bits σε ένα συγκεκριμένο κανάλι επικοινωνίας. Τα υλικά μεταγωγής μπορεί να είναι, καλώδια χάλκινα η ομοαξονικά, οπτικές ίνες η ακόμα και ο αέρας.
- $2^{ο}$ Ζεύξης Δεδομένων ( Data Link Layer ) : Στο δεύτερο επίπεδο παρατηρούμε πως είναι σημαντική η εξασφάλιση της αποσφαλμάτωσης των δεδομένων που προέρχονται από το φυσικό επίπεδο, ώστε να παραληθφούν σωστά στο ανώτερο επίπεδο. Η διαδικασία που χρησιμοποιείται είναι η διάσπαση των πακέτων του αποστολέα σε ακολουθίες από bits
- $3^{ο}$ Επίπεδο Δικτύου ( Network Layer ) : Η αρμοδιότητα του επιπέδου δικτύου είναι να καθορίσει την μέθοδο δρομολόγησης, από τον αποστολέα στον παραλήπτη, και να αντιμετωπίσει τις περιπτώσεις συμφόρησης μέσο του ελέγχου ροής των πακέτων. Η ενδεχόμενες διαδρομές των πακέτων στηρίζονται τις

περισσότερες φορές σε στατικούς πίνακες, όμως κάποιες φορές ανάλογα με την κατάσταση του δικτύου μπορεί να ακολουθηθούν δυναμικά νέες.

- 4ο Μεταφοράς ( Transport Layer ) : Είναι ένα επίπεδο "από άκρο σε άκρο" ( end to end ) η λειτουργία του επιπέδου μεταφοράς έχει να κάνει με την διαχείριση των δεδομένων που προέρχονται από το ανώτερο επίπεδο, και τον διαχωρισμό τους αν είναι απαραίτητο κάτι τέτοιο, σε μικρότερα τμήματα, ώστε να μεταβαίνουν σωστά στο επίπεδο δικτύου.
- Επίπεδο 5ο Συνόδου ( Session Layer ) Το επίπεδο αυτό προσφέρει τη δυνατότητα σε χρήστες διαφορετικού υλικού να υλοποιήσουν μεταξύ τους συνδιαλέξεις (sessions). Οι συνδιαλέξεις επιτρέπουν διάφορες υπηρεσίες όπως είναι ο έλεγχος διαλόγου, η διαχείριση σκυτάλης και ο συγχρονισμός.
- Επίπεδο 6ο Παρουσίασης ( Presentation Layer ). Η ιδιότητα του επιπέδου παρουσίασης είναι το πώς θα συνταχθούν και τι σημαίνουν οι μεταδιδόμενες πληροφορίες. Είναι το πρώτο επίπεδο που συναντάμε και δεν ασχολείται με την μετάδοση των πληροφοριών όπως τα προηγούμενα επίπεδα.
- Επίπεδο 7ο Εφαρμογών ( Application Layer) Το επίπεδο αυτό με τη χρήση μίας εφαρμογής δίνει τη δυνατότητα στο χρήστη να προσπελάσει τα δεδομένα ενός δικτύου. Η εφαρμογή αυτή μπορεί να είναι ένας πλοηγός (browser). Έχει άμεση επικοινωνία με τον χρήστη που επιτυγχάνετε μέσω πρωτόκολλων εφαρμογής όπως είναι το HTTP.

### 1.7 Πρωτόκολλο Επικοινωνίας TCP/IP

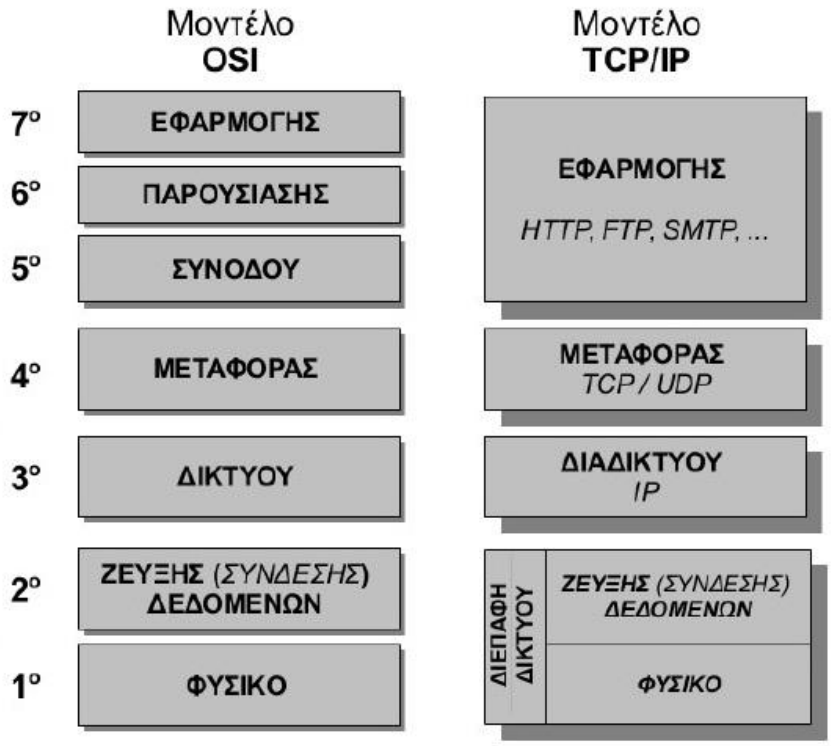
Το διαδίκτυο πλέον με την έκταση που έχει και την ποικιλομορφία των συσκευών και των δικτύων που το αποτελούν, θα έπρεπε να έχει συγκεκριμένους τρόπους επικοινωνίας που να εξασφαλίζουν την επικοινωνία μεταξύ των σταθμών όσο διαφορετικοί και είναι αυτοί.

Για τον λόγο αυτό υπάρχουν τα πρωτόκολλα. Το πρωτόκολλο στο κόσμο του διαδικτύου είναι ένα σύνολο κανόνων που διέπουν την οργάνωση της επικοινωνίας μεταξύ δύο κόμβων αλλά και την διαχείριση τυχόν σφαλμάτων που θα προκύψουν. Το ποιο σημαντικό πρωτόκολλο που λαμβάνει χώρα στις μέρες μας είναι το TCP/IP, και θα έχουμε την ευκαιρία να τα αναλύσουμε παρακάτω.

Σήμερα το πρωτόκολλο που χρησιμοποιείτε για την μεταφορά πληροφοριών και την επικοινωνία στο internet είναι το TCP ( Transmission Control Protocol ), IP ( Internet Protocol ). Δεν είναι κάτι καινούργιο καθώς ξεκίνησε να λειτουργεί την περίοδο που αναπτυσσόταν και το Arpanet, για να χρησιμοποιείται όμως ακόμη είναι ένα σημάδι που φανερώνει πόσο σημαντικό αλλά και λειτουργικό είναι. Το ουσιαστικό προσόν που έχει είναι πώς επιτρέπει την επικοινωνία μεταξύ δυο υπολογιστών ακόμα και αν είναι σε διαφορετικά δίκτυα, με διαφορετικές δυνατότητες και ανόμοια λειτουργικά συστήματα χωρίς να απαιτείτε κάποια συγκεκριμένη μετατροπή των πληροφοριών εφεξής. Έχει μια επαυξημένη έννοια καθώς πολλές φορές παρόμοια πρωτόκολλα που χρησιμοποιούνται για μεταφορά δεδομένων σε δίκτυα υπολογιστών, λογίζονται μέρη του γενικότερου πρωτοκόλλου TCP/IP. Η δομή του αποτελείτε από 4 επίπεδα και είναι τα παρακάτω:

- Επίπεδο 1$^{ο}$ Πρόσβαση στο Δίκτυο ( Network Access Layer ) Το επίπεδο αυτό έχει ως αρμοδιότητα την επικοινωνία του μέσου στο οποίο χρησιμοποιείται με το δίκτυο στο οποίο υπάγεται το μέσο. Μπορεί να ανιχνεύσει την αρχιτεκτονική που διαθέτει το δίκτυο και να επιλέξει το κατάλληλο κανάλι επικοινωνίας. Στον επίσημο ορισμό του επιπέδου αυτού δεν καθορίζεται αυστηρά τα πρωτόκολλα που αντιστοιχούν για να επιτευχθεί η επικοινωνία, και για τον λόγο αυτό αναλόγως το υλικό, το λειτουργικό και τον τύπο του δικτύου επιλέγεται κάθε φορά το ποιο σωστό.
- Επίπεδο 2$^{ο}$ Δικτύου ( Network Layer ) Στο επίπεδο αυτό λαμβάνει χώρα η δρομολόγηση και παραλαβή των πακέτων στον παραλήπτη. Σε κάθε πακέτο προς αποστολή, προσθέτει την διεύθυνση παραλαβής, ώστε να εξασφαλιστεί ότι το πακέτο θα φτάσει έστω και καθυστερημένα. Το πρωτόκολλο τέλος που χρησιμοποιείται στο επίπεδο αυτό είναι το IP.
- Επίπεδο 3$^{ο}$ Μεταφοράς ( Transport Layer ) Αρμοδιότητα του επιπέδου είναι να παραλάβει τις πληροφορίες των δεδομένων από το επίπεδο εφαρμογής, αν χρειαστεί να τις διασπάσει σε μικρότερα πακέτα, και να τα παραδώσει σωστά στο αμέσως χαμηλότερο επίπεδο δικτύου. Τα πρωτόκολλα που λειτουργούν και διασφαλίζουν τη σωστή διακίνηση των πακέτων είναι το TCP και το UDP.
- Επίπεδο 4$^{ο}$ Εφαρμογής ( Application Layer ) Είναι το υψηλότερο επίπεδο και διαχειρίζεται ενέργειες που έχουν να κάνουν με τη μεταφορά μεγάλων αρχείων με τη χρήση του πρωτόκολλου FTP, την αποστολή και λήψη μηνυμάτων του ηλεκτρονικού ταχυδρομείου ( πρωτόκολλο SMTP). Ακόμη στο επίπεδο αυτό ο

χρήστης μπορεί να επισκεφθεί ιστοσελίδες με τη βοήθεια του πρωτοκόλλου HTTP, αλλά και να συνδεθεί απομακρυσμένα με κάποια συσκευή του δικτύου ( πρωτόκολλο Telnet).




*ΣΧΗΜΑ 1.4: Παρουσίαση Πρωτοκόλλων OSI και TCP/IP (πηγή: Δίκτυα Υπολογιστών Γ' Τάξη ΕΠΑ.Λ).*

# Κεφάλαιο 2 – Κακόβουλο Λογισμικό Και Επιθέσεις

Στις μέρες μας ο όρος κακόβουλο λογισμικό ( Malicious Software ) χρησιμοποιείτε για να περιγράψει όλα εκείνα τα προγράμματα τα οποία δημιουργήθηκαν για να πραγματοποιούν αθέμιτες ενέργειες σε υπολογιστικά συστήματα, χωρίς την συγκατάθεση των διαχειριστών τους. Σημασιολογικά πάντως ο παραπάνω ορισμός είναι λάθος, καθώς αναφερόμαστε σε άυλες μορφές λογισμικού που δεν διαθέτουν βούληση για να επιλέξουν αν θα λειτουργούν θεμιτά ή αθέμιτα. Οι προγραμματιστές-δημιουργοί είναι υπεύθυνοι για τις πράξεις και τις προθέσεις των κακόβουλων προγραμμάτων.

Το κακόβουλο λογισμικό κατατάσσεται σε δυο βασικές κατηγορίες σύμφωνα με τον William Stalling, οι οποίες έχουν να κάνουν με την αυτονομία και την αναπαραγωγή. Η αυτονομία περιγράφει αν το λογισμικό μπορεί να λειτουργήσει κανονικά χωρίς να προσκολληθεί στον υπολογιστή του χρήστη ( host ), ενώ η αναπαραγωγή περιγράφει αν το λογισμικό είναι σε θέσει να πολλαπλασιαστεί από μόνο του όταν βρεθεί η κατάλληλη συνθήκη. Παράλληλα υπάρχουν και δύο είδη κακόβουλου λογισμικού, το ιομορφικό και το μη ιομορφικό.

## 2.1 Ιομορφικό

Οι ιοί είναι κομμάτια λογισμικού τα οποία προσκολλούν τον κώδικα τους σε εφαρμογές του χρήστη-ξενιστή. Πολλαπλασιάζουν τον εαυτό τους αυτοβούλως και εξαπλώνονται σε διαφορετικά σημεία του συστήματος εκτελούμενα πάντα στο παρασκήνιο για να μην γίνονται αντιληπτά. Τα στάδια λειτουργίας του ιού είναι τρία και περιγράφονται από τον κύκλο ζωής του.

- Στάδιο επώασης : Ο ιός βρίσκεται μέσα στο σύστημα του ξενιστή, όμως παραμένει ανενεργός σε κατάσταση αναμονής η οποία δεν γίνεται αντιληπτή από τα προγράμματα άμυνας του συστήματος. Για να ξεκινήσει το επόμενο στάδιο χρειάζεται ένα γεγονός, αυτό είναι είτε η εκτέλεση ενός αρχείου είτε το πέρας μίας συγκεκριμένης χρονικής διάρκειας. Πολλές φορές παρατηρείτε πως οι ιοί δεν περιλαμβάνουν την φάση της επώασης για να κερδίζουν χρόνο και αναπαράγονται με το που προσκολλήσουν στον κατάλληλο ξενιστή.

- Στάδιο αναπαραγωγής : Από τα πιο χαρακτηριστικά στάδια του κύκλου ζωής των ιών, σε αυτό το στάδιο ο ιός αντιγράφει τον εαυτό του και προσκολλάται σε κάποιο πρόγραμμα ξενιστή.
- Στάδιο ενεργοποίησης και εκτέλεσης : Το τελευταίο στάδιο του κύκλου ζωής των ιών, εδώ ο ιός εκτελεί μια ακολουθία εντολών (payload) οι οποίες κατά βάση πλήττουν το σύστημα ξενιστή ανάλογα με το περιεχόμενο των εντολών που διαθέτει, μπορεί να περιέχει από ακίνδυνα μηνύματα μέχρι καταστροφικές εντολές για την ολοκληρωτική καταστροφή ζωτικών μονάδων του συστήματος όπως είναι ο επεξεργαστής και ο σκληρός δίσκος.

Εκτός από τα τρία βασικά στάδια που αναφερθήκαμε παραπάνω κάθε ιός περιλαμβάνει τουλάχιστον δυο δευτερεύουσες λειτουργίες τις λεγόμενες υπορουτίνες.

- Υπορουτίνα αναζήτησης : Κατά την οποία ο ιός αναζητά καινούργιους ξενιστές σε τομής τοπικής αποθήκευσης και δικτύων στα οποία έχει πρόσβαση ο ξενιστής.
- Υπορουτίνα αντιγραφής : Στην οποία ο ιός δημιουργεί ένα αντίγραφο μέσω του μηχανισμού της αναπαραγωγής και το μεταθέτει στον νέο ξενιστή που βρέθηκε από την υπορουτίνα αναζήτησης.

Μερικοί ιοί υποστηρίζουν παραπάνω υπορουτίνες όπως αυτή κατά του εντοπισμού όπου εκτελούνται ενέργειες για την αποφυγή του εντοπισμού του ιού από τα συστήματα άμυνας του ξενιστή.

### 2.2 Μη Ιομορφικό

Ο όρος μη ιομορφικό χρησιμοποιείται για να περιγράψει τις υπόλοιπες κατηγορίες κακόβουλου λογισμικού οι οποίες δεν είναι στην κατηγορία των ιών. Οι ποιο γνώστες είναι οι παρακάτω.

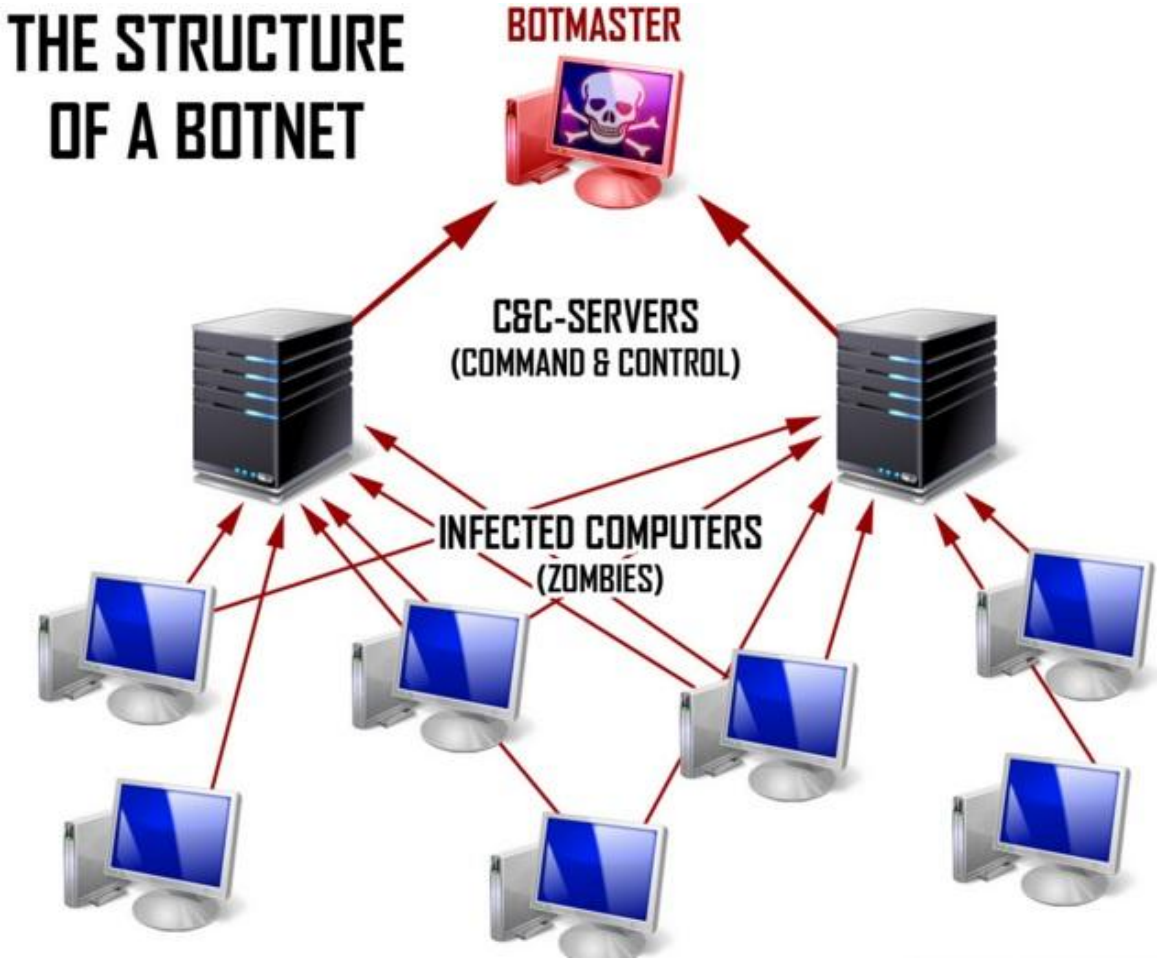
- Δούρειοι Ίπποι ( Trojan Horse ) : Εκ πρώτης όψεως χρήσιμα προγράμματα που διαθέτουν στο εσωτερικό του κώδικα που θα προκαλέσει πρόβλημα αν εκτελεστεί. Δεν έχουν τη λειτουργία της αναπαραγωγής και γι’ αυτό πρέπει να προκαλέσουν τον ίδιο τον ξενιστή να τα εγκαταστήσει εκμεταλλευόμενα την άγνοια του. Συνήθως το αποτέλεσμα από μια μόλυνση με δούρειο ίππο, είναι να δημιουργηθεί κάποιο κενό ασφάλειας και να το εκμεταλλευτεί ο επιτιθέμενος

αποκτώντας μη εξουσιοδοτημένη πρόσβαση. Υπάρχουν αρκετές κατηγορίες το στόχο που έχουν μερικές από τις οποίες είναι : Η απομακρυσμένη πρόσβαση, καταστροφή αρχείων, αποστολή μηνυμάτων, απενεργοποίηση συστημάτων άμυνας, αλλαγή τρόπου σύνδεσης στο internet με τη χρήση ακριβών συνδέσεων κλήσης ( Dial Up), κατέβασμα αρχείων. Κάποιοι από τους δούρειους ίππους που έχουν δράσει κατά καιρούς είναι οι εξής : Pest Trap, Y3K Remote Administration, Net Bus, flooder, Gromozon Trojan, Sun-7, Cuteqq_Cn, Dropper-EV, Downloader-EV, Tagasaurus.

- Σκουλήκια ( Worms ) : Αναπαράγονται με δική τους πρωτοβουλία και δρουν παρόμοια με τους ιούς ο στόχος τους είναι να μολύνουν το σύστημα του ξενιστή και στη συνέχεια να βρουν ένα νέο σύστημα για να εγκατασταθούν και να συνεχίσουν την ίδια διαδικασία. Είναι αυτόνομα δεν είναι απαραίτητος ο ξενιστής αλλά βοηθάει σημαντικά στην εξάπλωση τους. Μεταδίδονται μέσω δικτύου αλλά και από το ηλεκτρονικό ταχυδρομείο πολλές φορές. Το πρώτο σκουλήκι έδρασε το 1988 από τον Robert Morris απόφοιτο πληροφορικής του πανεπιστήμιου του Cornell. Η εξάπλωση και η ζημιές που προκάλεσε ήταν πέρα από κάθε προσδοκία του και οι συνάδελφοι δούλευαν για μέρες μέχρι να το σταματήσουν.
- Λογικές Βόμβες ( Logical Bomb ) : Είναι το παλαιότερο κακόβουλο λογισμικό. Αποτελείται από κώδικα που ενσωματώνεται σε ένα πρόγραμμα και εκτελείτε όταν γίνει αληθής κάποια συγκεκριμένη λογική συνθήκη. Ομοίως και οι χρονικές βόμβες εκτελούνται όταν έρθει η κατάλληλη χρονική στιγμή.
- Κερκόπορτες ( BackDoors) : Αποτελούν σημεία εισαγωγής στο σύστημα και προσπερνούν διαδικασίες ελέγχου οι οποίες θα τις σταματούσαν. Δημιουργήθηκαν για να είναι ποιο εύκολος ο έλεγχος σε κάποια προγράμματα δεν άργησαν όμως να εμφανιστούν και σε κακόβουλο λογισμικό. Μια κερκόπορτα όταν λειτουργεί καθιστά ευάλωτο το σύστημα σε όσους μπορούν να την διακρίνουν.
- Rootkits : Είναι σημαντικά εργαλεία για τον επιτιθέμενο, που του δίνουν την δυνατότητα να αποκρύψει τα σημάδια μιας επίθεσης, αλλά και να εγκαταστήσει μία κερκόπορτα με υψηλή διαβάθμιση δικαιωμάτων σαν του διαχειριστή. Η πόρτα θα είναι ανοιχτεί και όποτε επιθυμεί θα συνδέεται πάλι στο σύστημα επίσης θα διαθέτει και τα κατάλληλα δικαιώματα για να εγκαταστήσει επιπλέον προγράμματα υποκλοπής και παρακολούθησης.

- Βακτήρια ( Bacteria ) : Έχουν παρόμοιο τρόπο αναπαραγωγής με τους ιούς, δεν έχουν όμως ανάγκη τον ξενιστή. Ο μοναδικός σκοπός των βακτηρίων είναι αναπαραγωγή, η εφαρμογή τους δεν εκτελεί άμεσα κάποια επιζήμια ενέργεια για το σύστημα, έμμεσα όμως τα βακτήρια καταναλώνουν αρκετούς πόρους του συστήματος επηρεάζοντας την απόδοση του στην διαθέσιμη μνήμη, την ισχύ επεξεργασίας δεδομένων ή τον χώρο αποθήκευσης.
- Παραπλανητική Πληροφόρηση : Εκτός από την ανάπτυξη κακόβουλου λογισμικού ορισμένοι κατά καιρούς κατασκεύαζαν φήμες πως έχουν κυκλοφορήσει νέα ισχυρά κακόβουλα προγράμματα. Αυτό είχε σαν αποτέλεσμα να γίνονται έρευνες για να εντοπιστούν τα προγράμματα αυτά χωρίς φυσικά να βρεθεί κάτι και να χάνεται χρόνος αλλά και επεξεργαστική ισχύ.
- Bots : Τα Bots τα συναντάμε για πρώτη φορά σαν βοηθούς σε κανάλια συνομιλίας στο πρωτόκολλο IRC. Σήμερα πολλοί υπολογιστές μολύνονται από κακόβουλο λογισμικό και οργανώνονται άθελα τους σε μολυσμένα δίκτυα boot net. Τα δίκτυα αυτά ελέγχονται από τους επιτιθέμενους για την εξυπηρέτηση κακόβουλων ενεργειών όπως είναι οι επιθέσεις DDOS, και οι εξαπάτησης (phishing).
- Λογισμικό Κατασκοπείας (Spyware) : Πρόκειται για κακόβουλο λογισμικό παράνομης παρακολούθησης που εισέρχεται στο σύστημα από το δίκτυο ή από μολυσμένες συσκευές που συνδέονται με το σύστημα και λειτουργεί παρασκηνιακά ( χωρίς να φαίνεται στο περιβάλλον του χρήστη) ώστε να μην γίνεται αντιληπτό. Το spyware μαζεύει πληροφορίες και δεδομένα από τον χρήστη και τα αποστέλλει στον ιδιοκτήτη του. Τα δεδομένα αυτά μπορεί να είναι σχετικά ακίνδυνα όπως οι επιλογές του χρήστη στις σελίδες του διαδικτύου που επισκέπτεται, έως και εξαιρετικά επικίνδυνα όπως κωδικοί πρόσβασης σε λογαριασμούς και πιστωτικές κάρτες. Το λογισμικό κατασκοπίας χωρίζεται σε τρις κατηγορίες.
    1. Κατηγορία Μάρκετινγκ στην οποία το λογισμικό μαζεύει πληροφορίες από τον χρήστη με σκοπό την δημιουργία στοχευόμενων διαφημίσεων.
    2. Κατηγορία Παρακολούθησης στην οποία το λογισμικό αποκομίζει πληροφορίες για όλες τις ενέργειες που εκτελεί ή πληκτρολογεί ο χρήστης. Λογισμικό που πολλές φορές το χρησιμοποιούν και οι εταιρίες για να παρακολουθούν τους υπαλλήλους του.

3. Τρίτη Κατηγορία στην οποία το λογισμικό έχει σαν στόχο τον έλεγχο του συστήματος και την εισαγωγή του σε ένα δίκτυο μολυσμένων συστημάτων που έχει δημιουργηθεί για να καταστρατηγήσει τους υπολογιστικούς πόρους για κακόβουλες διεργασίες.




*ΣΧΗΜΑ 2.1: Η δομή ενός μολυσμένου δικτύου Botnet (πηγή: blog.tkj.se).*

## 2.3 Είδη Επιθέσεων

### 2.3.1 Επιθέσεις Άρνησης Υπηρεσίας ( DOS – Denial of Service Attacks)

Μια πολύ σημαντική κατηγορία επιθέσεων είναι αυτή την Άρνησης υπηρεσίας. Οι επιθέσεις του τύπου αυτού δεν έχουν ως στόχο να μολύνουν το σύστημα αλλά ο στόχος τους είναι η εξάντληση των επικοινωνιακών πόρων(μνήμη, bandwidth) ώστε να μην μπορεί ο σταθμός να εξυπηρετήσει του χρήστες του. Στην πράξη αυτό επιτυγχάνεται με

την μαζική αποστολή πακέτων δεδομένων, με σταθερά υψηλό ρυθμό στο σύστημα που δέχεται επίθεση, και αυτό έχει σαν αποτέλεσμα το σύστημα να μην μπορεί να ανταπεξέλθει, και να οδηγείται στην κατάρρευση. Τις περισσότερες φορές οι επιθέσεις αυτές χρησιμοποιούν κενά ασφαλείας που εμφανίζει το πρωτόκολλο TCP/IP. Κάποια γνωστά παραδείγματα είναι :

- Teardrop : Οι επιθέσεις αυτές εκμεταλλεύονται τα κενά που παρουσιάζει το πρωτόκολλο TCP/IP κατά την επανασύνδεση (reassembly) των πακέτων στην διαδικασία της λήψης τους.
- Ping of Death : Είναι ένας σχετικά παλιός τύπος επίθεσης που έχει σκοπό να κολλήσει (hang) το σύστημα ή ακόμα και να το οδηγήσει σε επανεκκίνηση, με αποτέλεσμα οι χρήστες να είναι αδύνατον να το χρησιμοποιήσουν. Στις μέρες μας έχουν βρεθεί δικλίδες ασφαλείας και τα συστήματα είναι πλέον αναβαθμισμένα και μπορούν και το αντιμετωπίζουν.
- Επίθεση Smurf: Είναι η επίθεση στην οποία στέλνεται ένας πολύ μεγάλος αριθμός από ping αιτήματα στον router, με την χρήση πλαστών IP διευθύνσεων μέσα από το ίδιο δίκτυο. Σε κάθε αίτημα που δέχεται το router εκτελεί μια ενέργεια, είτε διαμοιρασμού είτε απάντησης. Το αποτέλεσμα της επίθεσης αυτής είναι η υπερφόρτωση του δικτύου με πακέτα, και ο τερματισμός της λειτουργίας του.
- Επιθέσεις Θρυμματισμού (Fragmentation) : Αποτελούν μια νέα μέθοδο επίθεσης στην οποία, ο επιτιθέμενος επικοινωνεί με τον θύμα (μέσο του TCP/IP) και ανταλλάσει δεδομένα τα οποία τα χωρίζει σε μικρότερα κομμάτια, ο παραλήπτης μόλις λάβει τα κομμάτια, τα συνθέτει και αν δεν είναι σωστή η σύνθεση τους στέλνει μήνυμα στον αποστολέα να τα ξαναστείλει. Ο επιτιθέμενος στέλνει εσκεμμένα λάθος τα δεδομένα και διαδικασία συνεχίζεται έως ότου το θύμα αποσυνδεθεί από το δίκτυο.
- Επίθεση SYN/Land : Είναι δύο παρόμοιοι τύποι επιθέσεων η επιθέσεις SYN με την χρήση ψεύτικων IP διευθύνσεων εξαναγκάζουν το σύστημα θύμα να αναμένει επ'αόριστον μια απάντηση από την IP. Από την άλλη οι Land επιθέσεις κάνουν χρήση της ίδιας IP διεύθυνσης του συστήματος και δημιουργείται ένας ατέρμον βρόγχος επανάληψης. Το αποτέλεσμα και στις δύο περιπτώσεις είναι ο τερματισμός ή και η επανεκκίνηση.
- Βομβαρδισμός Ηλεκτρονικού Ταχυδρομείου (Email bombing) : Το είδος αυτής της επίθεσης είναι ιδιαίτερα αποτελεσματικό για συστήματα οπού διαχειρίζονται το ηλεκτρονικό ταχυδρομείο. Ο τρόπος λειτουργίας είναι απλός, ο επιτιθέμενος

στέλνει στον στόχο πάρα πολλά μηνύματα με μεγάλο μέγεθος που απαιτούν υψηλή υπολογιστική ισχύς και μεγάλο φόρτο εργασιών. Το υπολογιστικό σύστημα δεν μπορεί να ανταπεξέλθει και καταρρέει.

- Επίθεση Πλημμύρας (Port Flooding) Στην επίθεση αυτή επιλέγεται μια δικτυακή πόρτα από το υπολογιστικό σύστημα του θύματος και μέσω ενός προγράμματος που χρησιμοποιεί ο επιτιθέμενος, ανοίγει από την πόρτα που έχει επιλεγεί πάρα πολλές συνδέσεις. Οι συνδέσεις απαιτούν υπολογιστικούς πόρους για να επεξεργαστούν, και τελικά το σύστημα δεν μπορεί να ανταποκριθεί.

### 2.3.2 Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσίας ( DDOS – Distributed Denial of Service Attacks)

Οι DDOS επιθέσεις από την άλλη πλευρά αποτελούν το επόμενο βήμα των DOS επιθέσεων και έχουν πολύ μεγαλύτερη αποτελεσματικότητα. Συνήθως οι επιθέσεις εκτελούνται από μικρές ομάδες επιτιθέμενων που έχουν πρωτίστως επιτεθεί και έχουν στην κυριότητα τους μικρά δίκτυα υπολογιστών τα οποία δεν έχουν άμεση σχέση με το υπολογιστικό σύστημα θύμα. Στη συνέχεια εγκαθιστούν ένα εργαλείο για DOS επιθέσεις σε κάθε υπολογιστή, και πλέον είναι όλα έτοιμα για την επίθεση. Δίνεται εντολή για επίθεση και όλοι οι υπολογιστές των κατεχόμενων δικτύων στοχεύουν με πακέτα το θύμα. Το αποτέλεσμα είναι το υπολογιστικό σύστημα του θύματος, είτε να καταρρεύσει είτε να αργεί πάρα πολύ να ανταποκριθεί, λόγου του μεγάλου φόρτου επεξεργασίας που έχει κατακλίσει την μνήμη αλλά και τους δικτυακούς πόρους.

- Επίθεση σε υπηρεσίες ονοματολογίας ( DNS Attacks)

Σε αυτήν την κατηγορία ο κακόβουλος χρήστης αλλάζει τα στοιχεία της βάσης δεδομένων της υπηρεσίας ονοματολογίας (DNS) για την διεύθυνση μίας ιστοσελίδας στόχου. Η νέα διεύθυνση IP ορίζεται από τον επιτιθέμενο και είναι στην διακριτική του ευχέρεια που θα οδηγεί, συνεπώς όσοι χρήστες αναζητήσουν τις πληροφορίες που είχε η ιστοσελίδα αρχικά δεν θα μπορούν να τις βρουν, καθώς η ιστοσελίδα θα έχει αλλάξει περιεχόμενο.

- Επίθεση με χρήση ανιχνευτών ( Scanner Attacks )

Η χρήση των ανιχνευτών αρχικά ήταν για την έρευνα της ασφάλειας των συστημάτων από τους διαχειριστές τους. Δεν άργησαν όμως να χρησιμοποιηθούν από κακόβουλος χρήστες για επιθέσεις. Οι ανιχνευτές σαρώνουν το δίκτυο του συστήματος και αξιολογούν αν υπάρχουν τρωτά σημεία. Τα αποτελέσματα τα αξιοποιούν αναλόγως οι επιτιθέμενοι ώστε το σημείο που θα επιλεγεί για επίθεση να έχει τις περισσότερες πιθανότητες για να επιτευχθεί η είσοδος τους στο σύστημα.

- Επίθεση μέσω αδύναμης διαμόρφωσης ( weak configuration)

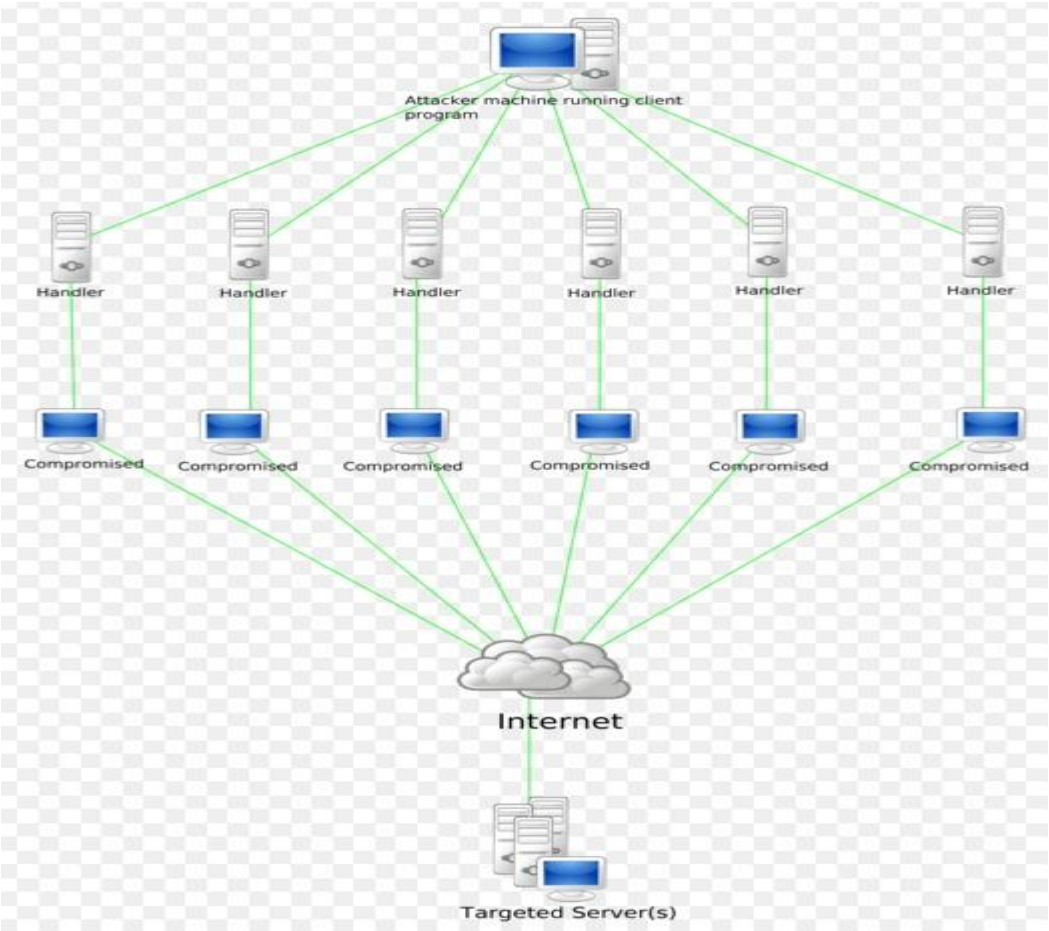
Οι επιθέσεις αυτές οφείλονται σε αμέλεια των διαχειριστών των συστημάτων. Κατά την εγκατάσταση ενός δικτυακού συστήματος υπάρχουν αρκετές παράμετροι που καλό είναι να αλλάξουν για λόγους ασφάλειας. Όταν δεν γίνει αυτό υπάρχει η πιθανότητα οι κακόβουλοι χρήστες να βρουν τους εργοστασιακούς κωδικούς των συστημάτων, και να αποκτήσουν πρόσβαση σε σημεία του δικτύου.

- Επίθεση σε σύστημα δικτυακής αρχειοθέτησης ( NFS – Network File System)

Το NFS είναι ένα δικτυακό πρωτόκολλο διαμοιρασμού αρχείων που δημιουργήθηκε από την Sun Microsystems το 1984. Μέχρι σήμερα έχει αλλάξει αρκετές φορές, όμως με απρόσεκτη χρήση ή λάθος παραμετροποίηση ενδέχεται να μοιράσει τα αρχεία σε μη εξουσιοδοτημένους χρήστες.

- Επιθέσεις ανθρώπου στη μέση MITM ( Man In The Midle Attacks )

Είναι ένας κοινός τύπος επίθεσης στις οποίες ο επιτιθέμενος μπαίνει στη μέση, μεταξύ δύο υπολογιστών που επικοινωνούν, και υποκλέπτει την επικοινωνία. Προϋπόθεση αποτελεί το γεγονός να πείσει ο κακόβουλος χρήστης και τους δύο σταθμούς που επικοινωνούν πως το κανάλι μετάβασης είναι αξιόπιστο και ασφαλές. Κατόπιν ο επιτιθέμενος έχει την δυνατότητα να αλλάξει να τροποποιήσει ή και να καταστρέψει τα μηνύματα που ανταλλάσουν οι δύο πλευρές.




*ΣΧΗΜΑ 2.2: Σχηματική απεικόνιση επίθεσης «DDOS» (πηγή: Wikimedia).*

# Κεφάλαιο 3 – Μηχανισμοί Προστασίας

## 3.1 Κρυπτογραφία και Κρυπτογράφηση Πληροφοριών

Η σημασία της επικοινωνίας και η αξία των πληροφοριών από την αρχαία εποχή έστρεψε τους ανθρώπους να ανακαλύψουν τεχνικές ώστε να μπορούν να επικοινωνήσουν και να ανταλλάξουν πληροφορίες με ασφάλεια ακόμα και αν υπάρχει περίπτωση το μήνυμα τους να υποστεί υποκλοπή. Οι Σπαρτιάτες κοντά στον $5^{ο}$ αιώνα π.χ. κατασκεύασαν την σκυτάλη, ήταν το πρώτο κρυπτογραφικό σύστημα της εποχής το οποίο λειτουργούσε με την μέθοδο της μετάθεσης. Λίγους αιώνες μετά στην περίοδο της Ρωμαϊκής αυτοκρατορίας ο γνωστός Ιούλιος Καίσαρας επινόησε μια μορφή κρυπτογράφησης μηνυμάτων με την μέθοδο της αντικατάστασης, αλλάζοντας δηλαδή τα γράμματα της πρότασης με αλλά που βρίσκονταν τρις θέσεις ποιο κάτω στο αλφάβητο. Στην εποχή μας η ραγδαία εξέλιξη της κρυπτογραφίας και τον κρυπτογραφικών συσκευών άρχισε μετά το τέλος του Α’ Παγκόσμιου πολέμου. Η πιο διάσημη συσκευή είναι η μηχανή Enigma που ανακαλύφθηκε από Γερμανούς και χρησιμοποιήθηκε πολύ στον Β’ Παγκόσμιο πόλεμο. Η μηχανή αίνιγμα ήταν μια ηλεκτρομηχανολογική μηχανή ρότορα, και μπορούσε να κρυπτογραφήσει αλλά και να αποκρυπτογραφήσει τα μηνύματα.

Η κρυπτογραφία είναι το επιστημονικό πεδίο το οποίο ασχολείται με την κρυπτογράφηση και την αποκρυπτογράφηση των πληροφοριών και γενικά έχει σαν στόχο την προάσπιση των τεσσάρων βασικών σκοπών της επικοινωνίας, που είναι η Εμπιστευτικότητα, η Ακεραιότητα, η Μη Αποποίηση ευθύνης, και Αυθεντικοποίηση.


*3.1: Η συσκευή ENIGMA μέσα σε ξύλινη θήκη μεταφοράς (πηγή: Wikipedia).*

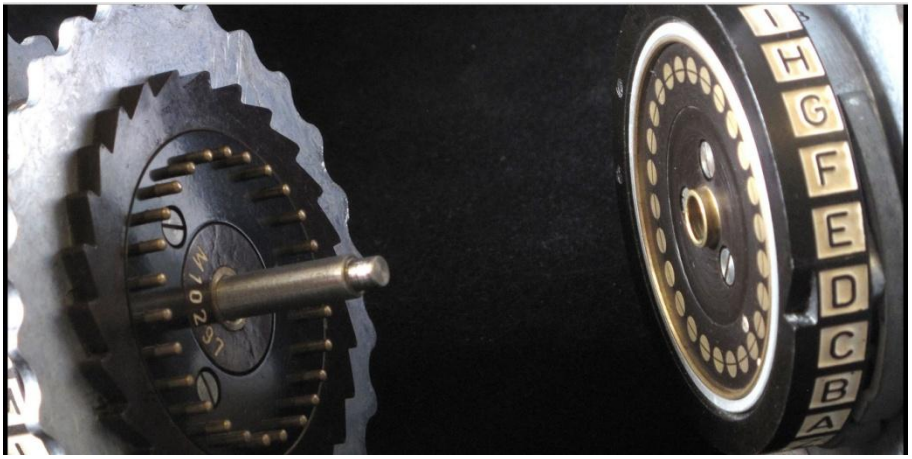
- Η Εμπιστευτικότητα διασφαλίζει πως η πληροφορία που είναι προς μετάδοση θα γίνει προσβάσιμη μόνο από τους χρήστες που κατέχουν την κατάλληλη εξουσιοδότηση. Παράλληλα ακόμα και αν παραβιαστεί η παραπάνω συνθήκη ο μη εξουσιοδοτημένος χρήστης που θα αποσπάσει την πληροφορία δεν θα είναι σε θέσει να την καταλάβει.
- Η Ακεραιότητα διασφαλίζει πως, η μεταδιδόμενη πληροφορία θα παραμείνει ως έχει και θα αλλαχθεί μόνο από εξουσιοδοτημένους χρήστες. Η αλλαγή της πληροφορίας ακόμη και αν γίνει θα αφήσει ανιχνεύσιμα σημάδια.
- Η Μη Αποποίηση Ευθύνης εξασφαλίζει την αληθή συνθήκη της ορθής αποστολής η λήψης της πληροφορίας, στο αποστολέα και στον παραλήπτη αντίστοιχα, σε βαθμό τέτοιο που αν ισχύει τότε ούτε ο ένας αλλά ούτε και ο άλλος μπορούν να αρνηθούν πως ήταν μέλη της συγκεκριμένης μετάδοσης.
- Η Αυθεντικοποίηση έχει να κάνει με την εξακρίβωση των στοιχείων του αποστολέα και του παραλήπτη, του προορισμού αλλά και τις πηγής της πληροφορίας ώστε να ισχύει η εξουσιοδότηση.

## 3.2 Είδη Κρυπτοσυστημάτων

### 3.2.1 Κλασικά Κρυπτοσυστήματα

- Αναδιάταξης : Στους αλγόριθμους αναδιάταξης ή μεταθέσεις το περιεχόμενο του μηνύματος ανασυντάσσεται κατά ομάδες και επανατοποθετείτε στο αρχικό με την νέα του μορφή.
- Αντικατάστασης : Στα συστήματα αντικατάστασης τα γράμματα που περιέχονται στα μηνύματα προς κρυπτογράφηση παίρνουν την θέση τους από άλλα γράμματα ή αλφαριθμητικούς χαρακτήρες. Παράδειγμα τέτοιου συστήματος είναι ο αλγόριθμος του Καίσαρα.
- Σημειωματάριο μιας χρήσης : Είναι το κρυπτοσύστημα που για κλειδί έχει έναν τυχαίο συνδυασμό από bits με απροσδιόριστα μεγάλο μήκος, περίπου ίσο με το μήκος του μηνύματος. Το κάθε κλειδί έχει μόνο μία χρήση και οι πληροφορίες στο εσωτερικό του κλειδιού δεν έχουν καμία σχέση μεταξύ τους.
- Ρότορες : Οι ρότορες μοιάζουν με γρανάζια και διαθέτουν μεγάλη έκταση στην δυνατότητα κρυπτογράφησης των μηνυμάτων, αφού με την χρήση ενός μόνο αλφαβήτου σε ένα ηλεκτρομηχανικό ρότορα, μπορεί να χρησιμοποιήσει 676

(26*26) αλφάβητα κρυπτογραφίας. Κλασικό παράδειγμα αποτελεί η συσκευή Enigma.




*ΣΧΗΜΑ 3.2: Δύο ρότορες της συσκευής ENIGMA (πηγή: Wikipedia).*

### 3.2.2 Μοντέρνα Κρυπτοσυστήματα

- Συμμετρικά : Τα συμμετρικά συστήματα κρυπτογράφησης είναι αυτά τα οποία χρησιμοποιούν ένα κλειδί και για τις δύο διαδικασίες(κρυπτογράφηση-αποκρυπτογράφηση). Επειδή το κλειδί είναι κοινό θα πρέπει να μετακινείτε σε ασφαλές δίαυλο επικοινωνίας. Οι συμμετρική κρυπταλγορίθμοι τέλος χωρίζονται σε δύο κατηγορίες τους, αλγόριθμους Δέσμης και τους αλγόριθμους Ροής
- Ασύμμετρα : Τα ασύμμετρα συστήματα κρυπτογράφησης η αλλιώς η κρυπτογράφηση δημοσίου κλειδιού, εφαρμόστηκε για να εξαλείψει τις άτυχες περιπτώσεις χρήσης συμμετρικών αλγόριθμου στις οποίες είχε διαρρεύσει το κλειδί. Τα κλειδιά σε αυτή αυτόν τον αλγόριθμο είναι δύο, ένα ιδιωτικό και ένα δημόσιο. Όπως προδίδουν και τα ονόματα τους το δημόσιο κλειδί είναι φανερό σε όλους ενώ το ιδιωτικό μυστικό. Η σχέση που υπάρχει μεταξύ των δύων κλειδιών είναι πώς ότι κρυπτογραφηθεί με το ένα μόνο με τη χρήση του άλλου γίνεται η αποκρυπτογράφηση.

## 3.3 Συστήματα Προστασίας

Η ραγδαία εξέλιξη της τεχνολογίας και του ίντερνετ, έδωσε πλέον ένα χαρακτήρα στην καθημερινότητα των σύγχρονων ανθρώπων όπου πολλές ώρες κάθε μέρα είναι συνδεδεμένοι σε κάποιο δίκτυο. Από το δίκτυο της εταιρίας την ανταλλαγή

μηνυμάτων ηλεκτρονικού ταχυδρομείου ως τις στιγμές χαλάρωσης σε ένα καφέ ο άνθρωπος έχει μαζί του συσκευές που είναι διαρκώς συνδεδεμένες σε κάποιο δίκτυο, ασφαλές η λιγότερο ασφαλές. Ανταλλάσει μηνύματα επισκέπτεται ηλεκτρονικές σελίδες και κάνει τις αγορές του ακόμα και από το κινητό του. Οι πληροφορίες που μοιράζεται είναι προσωπικές και ευαίσθητες και οι απειλές των επιτιθέμενων καθημερινά εξελίσσονται. Για τον λόγο αυτό η ασφάλεια των δικτύων και των υπολογιστικών συστημάτων αποκτά ακόμα μεγαλύτερη σημασία. Παρακάτω θα γνωρίσουμε εφαρμογές και συστήματα που έχουν σα στόχο την προστασία της ασφάλειας των συστημάτων, δηλαδή, της Εμπιστευτικότητας, της Ακεραιότητας και της Διαθεσιμότητας.

### 3.3.1 Συστήματα Ανίχνευσης Επιθέσεων (IDS Intrusion Detection Systems )

Τα συστήματα αυτά παρακολουθούν τις κινήσεις επικοινωνίας του δικτύου ή του συστήματος μας και τις αναλύει για τυχόν ύποπτες ενέργειες επιθέσεων. Στόχος τους είναι να ανακαλύψουν τις επιθέσεις από τα πρώτα σημάδια που θα εμφανιστούν. Οι προσπάθειες για μη εξουσιοδοτημένη πρόσβαση μπορεί να προέρχονται είτε από χρήστες που ανήκουν σε κάποιο εξωτερικό δίκτυο είτε και από χρήστες που είναι μέλη του ίδιου δικτύου αλλά δεν κατέχουν τα κατάλληλα δικαιώματα χρήσης. Τα ποιο πολλά IDS συστήματα χρησιμοποιούν την μέθοδο των υπογραφών (signatures), δηλαδή συγκρίνουν τις διαδοχικές ενέργειες που λαμβάνουν χώρα, και τις συγκρίνουν με ήδη γνωστές παράνομες. Γενικά η λειτουργία εξαντλείται στην αναζήτηση και αναγνώριση απειλών αρχικά, και στη συνέχεια με την σωστή επισήμανση των ευρημάτων στον διαχειριστή του συστήματος. Δεν έχουν δηλαδή ενεργητικό ρόλο στην καταπολέμηση των απειλών. Υπάρχουν δύο βασικοί τύποι συστημάτων ανίχνευσης απειλών, οι δικτυακοί και οι τοπικοί.

- Δικτυακά Συστήματα Ανίχνευσης ( Network IDS ) ελέγχουν την κίνηση στο δίκτυο (traffic) και την εξετάζουν για τυχόν σημάδια απειλών. Έχουν αισθητήρες σε διάφορα σημεία του δικτύου και διαθέτουν και ένα σταθμό παρακολούθησης δεδομένων εντός του δικτύου. Οι αισθητήρες σαρώνουν την κίνηση του δικτύου, και αναλύουν διεξοδικά τα δεδομένα. Αν βρεθούν

απειλές τότε αποστέλλουν της πληροφορίες που έχουν στον σταθμό παρακολούθησης.

- Τοπικά Συστήματα Ανίχνευσης ( Host IDS ) λειτουργούν όπως λέει και το όνομα τους τοπικά σε κάθε υπολογιστικό σύστημα. Είναι ποιο ευαίσθητα από τα δικτυακά συστήματα όμως για να καλύψουμε τις ανάγκες ολόκληρου του δικτύου, θα πρέπει να τα εγκαταστήσουμε σε κάθε χρήστη του δικτύου ξεχωριστά. Τα τοπικά συστήματα ανίχνευσης, παρακολουθούν διακριτικά τις ενέργειες που εκτελούνται στο σύστημα, ακόμα και αυτές στις οποίες είναι υπεύθυνος ο χρήστης για τυχόν ύποπτες κινήσεις (login, ασυνήθιστη πρόσβαση σε αρχεία).

### 3.3.2 Συστήματα Πρόληψης Επιθέσεων ( IPS Intrusion Prevention Systems)

Πρόκειται για την εξέλιξη των συστημάτων ανίχνευσης επιθέσεων. Όπως αναφέραμε και παραπάνω τα συστήματα ανίχνευσης δεν μπορούσαν να ενεργήσουν στις απειλές για να τις καταπολεμήσουν, για τον λόγο αυτό προέκυψε η ανάγκη για ένα σύστημα που θα αναγνωρίζει αλλά και θα καταπολέμα απειλές. Οι εφαρμογές IPS διαχειρίζονται την πρόσβαση με βάση την κάθε εφαρμογή που ζητά άδεια. Σε συνδυασμό με τις υπογραφές που υπάρχουν στη βάση δεδομένων επιτρέπουν ή αποκλείουν την εφαρμογή αλλά και τις ενέργειες που λαμβάνουν χώρα. Προστατεύουν από μεγάλη γκάμα κακόβουλων ενεργειών όπως είναι : οι ανωμαλίες στην κυκλοφορία του δικτύου που περιέχουν ύποπτο περιεχόμενο, επιθέσεις άρνησης εξυπηρέτησης Dos attack, υπερχείλιση ρυθμιστή Buffer overflow, νέες απειλές χωρίς να υπάρχει η αντίστοιχη υπογραφή zero day threat, ανιχνεύσεις πορτών, επιθέσεις για ηλεκτρονικό ταχυδρομείο, βάσεων δεδομένων και άλλα.

### 3.3.3 Αντιβιοτικά (Antivirus)

Είναι προγράμματα που προστατεύουν το σύστημα σε πραγματικό χρόνο από το κακόβουλο λογισμικό. Ποιο συγκεκριμένα λειτουργούν με την χρήση των υπογραφών (signatures) και με βάση αυτές συγκρίνουν κάθε ακολουθία εντολών που λαμβάνει χώρα στο σύστημα με την βάση δεδομένων των υπογραφών, αν βρεθεί κάποια αντιστοιχία τότε παρεμποδίζεται η εφαρμογή προς εκτέλεση και καταχωρείται ως κακόβουλη, αν αυτό

που πήγε να εκτελεστεί ήταν πρόγραμμα τότε αποθηκεύεται στην καραντίνα(ασφαλές σημείο του antivirus που έχει την δυνατότητα να αποθηκεύει κακόβουλο λογισμικό) και καταπολεμάτε αναλόγως. Τα αντιβιοτικά σε γενικές γραμμές είναι αρκετά αποτελεσματικά, όμως η αποτελεσματικότητα τους εξαρτάτε από το πόσο ενημερωμένη είναι η βάση δεδομένων των υπογραφών τους για την αναγνώριση του κακόβουλου λογισμικού. Αν κυκλοφορήσει ένας νέος ιός και το αντιβιοτικό δεν έχει την αντίστοιχη υπογραφή, τότε δυστυχώς αν εισέλθει στο σύστημα δεν θα αναγνωριστεί. Οι ενημερώσεις πρέπει αφενός να κυκλοφορούν άμεσα από την εταιρία που προσφέρει τα αντιβιοτικά και αφετέρου οι ενημερώσεις αυτές να εγκαθίστανται στο σύστημα μας.

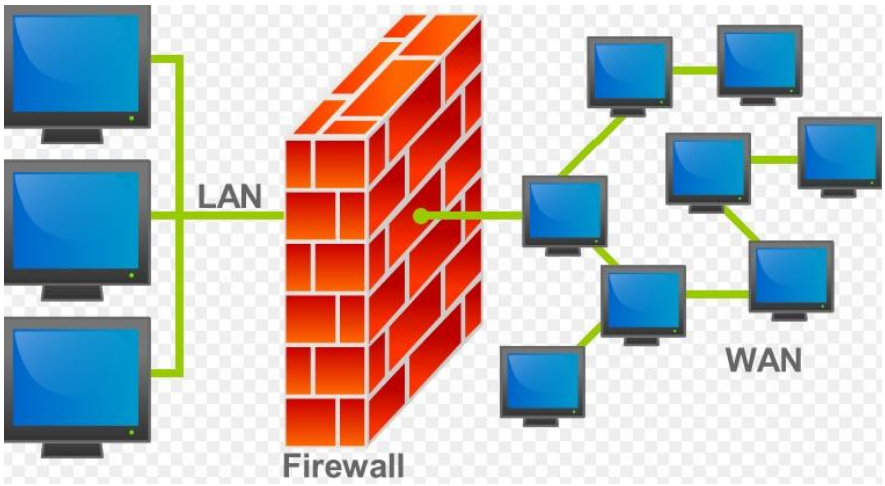
### 3.3.4 Τείχος Προστασίας ( Firewall )

Ο σκοπός της χρήσης του τείχους προστασίας είναι να αποφευχθούν επιθέσεις προς το δίκτυο μας. Είναι μια εφαρμογή ελέγχου τις κυκλοφορίας των δεδομένων μεταξύ δύο δικτύων, το ένα συνήθως είναι το διαδίκτυο όπου και χαρακτηρίζεται ως χαμηλής εμπιστοσύνης δίκτυο και το άλλο είναι το δίκτυο στο οποίο είναι εγκατεστημένο το τείχος προστασίας(τοπικό ή εταιρικό δίκτυο). Το firewall είναι ένα σύνθετο πρόγραμμα και για να λειτουργήσει σωστά απαιτεί την κατάλληλη παραμετροποίηση για να αποδώσει στον μέγιστο βαθμό, κάτι που σημαίνει πως χρειαζόμαστε μεγάλη εμπειρία για να καταγράψουμε όλες τις ανάγκες επικοινωνίας του συστήματος και να συντάξουμε τους κατάλληλους κανόνες. Η ποιο κοινή ρύθμιση είναι να απορρίπτονται όλες οι συνδέσεις προς το δίκτυο, και να επιτρέπονται μόνο αυτές που έχει δώσει έγκριση ο διαχειριστής του συστήματος. Τα πρώτα τείχη προστασίας κυκλοφόρησαν κοντά στο 1990, στις αρχές της ανάπτυξης του διαδικτύου δηλαδή, μέχρι σήμερα έχουν περάσει αρκετές γενιές, ποιο συγκεκριμένα έχουμε :

- Πρώτη Γενιά – Φίλτρα πακέτων : Ως πρώτη γένια τειχών προστασίας αναφερόμαστε στα φίλτρα πακέτων που αναπτύχθηκαν από την DEC( Digital Equipment Corporation) το 1988. Η λειτουργία τους είναι η ανάγνωση των πακέτων που κινούνται από το ένα δίκτυο στο άλλο, με στόχο αν βρεθεί κάποιο ύποπτο πακέτο που αντιστοιχεί σε γνωστό κανόνα ασφάλειας να απορριφτεί. Οι κανόνες ασφάλειας ορίζονται από τον διαχειριστή του δικτύου για το ποια πακέτα απορρίπτονται και ποια όχι.
- Δεύτερη Γενιά – Φίλτρα κατάστασης : Στη δεύτερη γενιά firewalls βλέπουμε τα φίλτρα κατάστασης που μοιάζουν πολύ με τα φίλτρα πακέτων αλλά διαθέτουν

κάποιες παραπάνω ιδιότητες όπως είναι η εξέταση των πακέτων ως προς την κατάσταση (state) την σύνδεση απ' όπου προέρχεται το κάθε πακέτο. Έχουν την ικανότητα να ξεχωρίσουν την θέση που έχουν τα πακέτα κατά την διάρκεια μιας σύνδεσης (αν είναι στην αρχή στη μέση η στο τέλος) και διαθέτουν δεδομένα για το είδος αλλά και την ποσότητα των συνδέσεων που πραγματοποιούνται ανάμεσα στα δίκτυα. Και σε αυτήν την περίπτωση ο διαχειριστής του δικτύου πρέπει να καθορίσει του κανόνες επικοινωνίας των συνδέσεων από και προς το δίκτυο.

- Τρίτη Γενιά – Επίπεδο εφαρμογών : Με βάση το μοντέλο αναφοράς OSI και το επίπεδο εφαρμογών του, οι εφαρμογές firewalls που αναπτύχθηκαν για τις ανάγκες του επιπέδου αυτού, αποτελούν την τρίτη γενιά. Πλέον οι νέες τεχνικές που διέθεταν τα τείχη προστασίας μπορούσαν να διακρίνουν ποιες εφαρμογές και πρωτόκολλα προσπαθούν να συνδεθούν με το δίκτυο μας.
- Τέταρτη Γενιά : Είναι η ποιο σύγχρονη γενιά τείχων προστασίας που κυκλοφορούν στις μέρες μας. Έχουν γραφικό περιβάλλον και δεν απαιτούν εξειδικευμένες γνώσεις για να διαμορφωθούν οι κανόνες χρήσης τους. Ακόμα και οι απλοί χρήστες μπορούν να τα παραμετροποιήσουν με βάση τις ανάγκες τους.




*ΣΧΗΜΑ 3.3: Απεικόνιση δικτύου που προστατεύεται από εξωτερικές συνδέσεις με την χρήση τείχους προστασίας (πηγή: Wikipedia).*

### 3.3.5 Λογισμικό Προστασίας από Προγράμματα Υποκλοπής ( Antispyware )

Είναι τα προγράμματα τα οποία αναλαμβάνουν να προστατεύσουν το υπολογιστικό σύστημα από κακόβουλο λογισμικό παρακολούθησης, το οποίο πολλές φορές δεν γίνεται αντιληπτό από αντιβιοτικά προγράμματα, έχουν παρόμοια λειτουργία με τα αντιβιοτικά αφού και αυτά λειτουργούν με το σύστημα των υπογραφών αλλά εξετάζουν διαφορετικές θέσεις μνήμης.

# Κεφάλαιο 4 – Τεχνολογία «HONEYPOT»

## 4.1 Εισαγωγή στα Συστήματα «HONEYPOT»

Ο τομέας της ασφάλειας των υπολογιστικών συστημάτων για χρόνια είχε επικεντρώσει το ενδιαφέρων και τις έρευνες στην εξέλιξη το συστημάτων ενεργητικής ασφάλειας. Ως συστήματα ενεργητικής ασφάλειας λογίζονται όλα εκείνα που αποτελούν την κύρια γραμμή άμυνας όπως είναι τα firewall, τα IDS και τα antivirus, τα οποία έχουν ενεργητικό και άμεσο ρόλο στην αντιμετώπιση τον εισβολών. Πλέον εδώ και λίγα χρόνια έχουν εμφανιστή συστήματα παθητικής ασφάλειας υπολογιστικών συστημάτων, τα οποία δεν έχουν άμεση συνεισφορά στην αντιμετώπιση των απειλών, προσφέρουν όμως γνώση μέσα από τις πληροφορίες που αντλούν από τους επιτιθέμενους και δίνουν τελικά υπεραξία στην έρευνες για την εξέλιξη των ενεργητικών συστημάτων.

Η τεχνολογία παθητικής ασφάλειας που θα εξετάσουμε είναι τα honeypot.Το honeypot σύμφωνα με τον ορισμό που έχει επικρατήσει είναι ένας πόρος πληροφοριακού συστήματος ο οποίος αποκτά αξία όταν ασκηθούν πάνω του μη εξουσιοδοτημένες ενέργειες. Το honeypot ουσιαστικά είναι ένα κομμάτι συστήματος στο οποίο παραδόξως θέλουμε να πέσει θύμα επίθεσης. Παρόλο που ακούγεται κάπως παράξενη η λογική αυτή, στην πράξη της μπορούμε να αποκομίσουμε χρήσιμες πληροφορίες για να αξιολογήσουμε την ενεργητική ασφάλεια αλλά και να καταγράψουμε τις μη εξουσιοδοτημένες ενέργειες δημιουργώντας μοτίβα συμπεριφοράς ανάλογα με το στιλ της επίθεσης.

Στις μέρες μας πολλές εταιρίες και οργανισμοί που θέλουν να ερευνήσουν σε θέματα ασφάλειας, προσφέρουν τις ελεύθερες διευθύνσεις από το εύρος των δικτύων τους για την ανάπτυξη honeypots. Το εύρος των διευθύνσεων που δεν χρησιμοποιείτε λέγεται και darkspace. Ο κακόβουλος χρήστης από την άλλη δεν γνωρίζει τα όρια του εκάστοτε δικτύου, που αρχίζουν δηλαδή και που τελειώνουν οι ωφέλιμες ips με αποτέλεσμα να εξαπολύει επιθέσεις και στο darkspace. Το honeypot τώρα αναλαμβάνει ένα διαδραστικού χαρακτήρα προς τον επιτιθέμενο όπως πιθανός να συμπεριφερόταν ένας φυσικός υπολογιστής του δικτύου, απαντά σε ερωτήματα και παρακολουθεί την συμπεριφορά και τις ενέργειες του. Όσες περισσότερες διευθύνσεις μπορεί να καλύψει

ένα honeypot τόσο μεγαλύτερο όγκο επιθέσεων θα διαχειριστεί και τόσες περισσότερες πληροφορίες θα συλλέξει.

Κάθε honeypot καλύπτει και από μία διεύθυνση, επόμενο είναι πως για να καλύψουμε ένα μεγάλο εύρος θα χρειαστούμε πολλά honeypots και πολλούς υπολογιστικούς πόρους για να λειτουργήσουν και να επεξεργαστούμε τις πληροφορίες που θα αποκομίσουν. Το κόστος χρήσης λοιπόν αυξάνεται, για τον λόγο αυτό λίγες επιχειρήσεις επιλέγουν να επενδύουν στο κομμάτι αυτό αν δεν έχουν άμεση σχέση με τον τομέα τις ασφάλειας.

### 4.2 Τα Πρώτα «HONEYPOTS»

Τα συστήματα honeypots κάνουν την εμφάνιση τους στο κοινό το 1992. Πρώτος ο Bill Cheswick δημοσιοποιεί σε άρθρο του "An Evening with Berferd. In Which a Cracker is Lured" την εμπειρία του με ένα επιτιθέμενο που προσπαθούσε για μήνες να αποκτήσει πρόσβαση σε αρχεία και κωδικούς του συστήματος του. Στο άρθρο του περιγράφει πως δημιούργησε ένα σύστημα που αλληλεπιδρούσε με τον επιτιθέμενο ανάλογα με τις απαιτήσεις του, και κατάφερε τελικά να τον παγιδεύσει αφού μελέτησε για αρκετό καιρό τις τεχνικές που ακολουθούσε.

*ΣΧΗΜΑ 4.1: Ένα «honeypot» μπορεί να μοιάζει "ελκυστικό" για επίθεση, κρύβει όμως κινδύνους για τον επιτιθέμενο (πηγή: Wikipedia).*

Λίγα χρόνια μετά το 1997 έχουμε την κυκλοφορία ενός ολοκληρωμένου honeypot χαμηλής αλληλεπίδρασης από τον Fred Cohen, η ονομασία του ήταν Deception Toolkit. Οι δυνατότητες που είχε η εργαλειοθήκη αυτή ήταν να αναπαριστά κάποιες δημοφιλής υπηρεσίες με καθορισμένα κενά ασφαλείας. Χρησιμοποιώντας μια μη ενημερωμένη έκδοση του sendmail και κάποια πλασματικά αρχεία με ευαίσθητες πληροφορίες χρηστών, το deception tool έδινε στους επιτιθέμενους το αρχικό κίνητρο για να ξεκινήσουν να ασχολούνται μαζί του, παράλληλα ο χρήστης του παρατηρούσε το περιεχόμενο και το είδος των επιθέσεων που μπορούσαν να αξιοποιηθούν για την αξιολόγηση του επιπέδου ασφαλείας των φυσικών συστημάτων.

Ένα χρόνο αργότερα το 1998 έκανε την εμφάνιση του το πρώτο σύστημα honeypot που μπορούσε να αντιγράψει εικονικά την μορφή ενός δικτύου υπολογιστών. Το όνομα του ήταν CyberCop Sting και προοριζόταν για περιβάλλοντα εργασίας των Windows NT. Οι

δυνατότητες του ήταν περιορισμένες, αντέγραφε διευθύνσεις IP φυσικών συστημάτων και παρείχε ευάλωτες υπηρεσίες περιορισμένων λειτουργιών. Δεν έτυχε μεγάλης αποδοχής λόγο των επιδόσεων του παρόλα αυτά το CyberCop Sting έδωσε το έναυσμα για την εξέλιξη των δικτυακών συστημάτων honeypots.

### 4.3 Τα Χαρακτηριστικά των «HONEYPOTS»

Κάθε τύπος λειτουργικού συστήματος έχει συγκεκριμένη συμπεριφορά στην επικοινωνία του με άλλες συσκευές του δικτύου. Κάθε λειτουργικό σύστημα ανάλογα με τον τύπο του έχει και διαφορετικό TCP/IP stack. Η συμπεριφορά αυτή αποτελεί και το αποτύπωμα του, η αλλιώς fingerprint. Η ανίχνευση του αποτυπώματος γίνεται αποστέλλοντας πακέτα στο σύστημα στόχο και ανιχνεύοντας τις απαντήσεις του.

Το μεγάλο θετικό που έχουν τα honeypots είναι πως μπορούν να συμπεριφερθούν μέσα στο δίκτυο ανάλογα με το λειτουργικό σύστημα η την έκδοση που θέλουμε να υιοθετήσουν. Είναι γενικά γνωστά τα fingerprints στο τι λειτουργικό σύστημα παραπέμπουν γι' αυτό και υπάρχει η δυνατότητα αυτή, να παρουσιάσουν αυτό που επιθυμεί ο διαχειριστής του honeypot. Παράλληλα εκτός από την απεικόνιση του συστήματος τα honeypot αναπαράγουν την λειτουργία συγκεκριμένων υπηρεσιών γνωστών στο ευρύ κοινό. Οι υπηρεσίες αυτές εκτελούνται με σειρές εντολών scrips. Για παράδειγμα τέτοιες υπηρεσία θα μπορούσαν να ήταν Telnet,FTP ή loging.

### 4.4 Χρήσεις των «HONEYPOTS»

Τα honeypots ανάλογα με τις δυνατότητες που έχουν αλλά και με την ιδιαίτερη αποστολή που έχει τι καθένα ξεχωριστά, επιλέγουμε να τα εφαρμόσουμε για τις ακόλουθες περιπτώσεις.

- Έρευνα: Κάθε σύστημα ανίχνευσης απειλών μπορεί να σταματήσει αποτελεσματικά κακόβουλες ενέργειες ή λογισμικό με βάση τις ως τώρα γνωστές καταγεγραμμένες απειλές. Τα honeypots αποτελούν ιδανικό εργαλείο έρευνας σε θέματα ασφάλειας. Η δομή που έχουν μας δίνει πολλές δυνατότητες στο να μελετήσουμε νέες μορφές απειλών και κακόβουλου λογισμικού, που μέχρι πριν ήταν άγνωστες.
- Έλεγχος ανεπιθύμητης αλληλογραφίας: Με την χρήση honeypots χαμηλής αλληλεπίδρασης μπορεί να ρυθμιστή η ροή μηνυμάτων στο ηλεκτρονικό

ταχυδρομείο. Το honeypot ανάλογα με τις ρυθμίσεις του, αναγνωρίζει τα μηνύματα που θέλουμε να περάσουν και για τα υπόλοιπα συνεργάζεται με φίλτρο ανεπιθύμητης αλληλογραφίας για να τα ανακόψει.

- Προστασία από επιθέσεις: Αν και συστήματα με παθητικό προσανατολισμό στην ασφάλεια, έχουν δυνατότητες να αποκλείσουν συγκεκριμένες μορφές επιθέσεων, όπως οι αυτοματοποιημένες επιθέσεις που εκτελούνται από σκουλήκια. Οι επιθέσεις αυτές ξεκινούν με σαρώσεις στο δίκτυο στόχο ψάχνοντας συγκεκριμένες αδυναμίες ή συστήματα με παλιά λειτουργικά. Το honeypot μπορεί να αλληλεπιδράσει στις αναζητήσεις αυτές και να αποπροσανατολίσει τον επιτιθέμενο δίνοντας του ψευδή στοιχεία.

### 4.5 Αρχιτεκτονική των «HONEYPOTS» στο Δίκτυο

Η τοποθέτηση και εγκατάσταση ενός honeypot αποτελεί αντικείμενο έρευνας και συνάδει με τους στόχους που έχουμε θέσει από το εγχείρημα της τεχνολογίας honeypot που έχουμε επιλέξει να εφαρμόσουμε. Οι επιλογές που έχει ο χρήστης για την τοποθέτηση του honeypot είναι τρις :

- Μετά το τείχος προστασίας.
- Μέσα στην αποστρατικοποιημένη ζώνη του δικτύου (demilitarized zone – DMZ).
- Πριν το τείχος προστασίας.

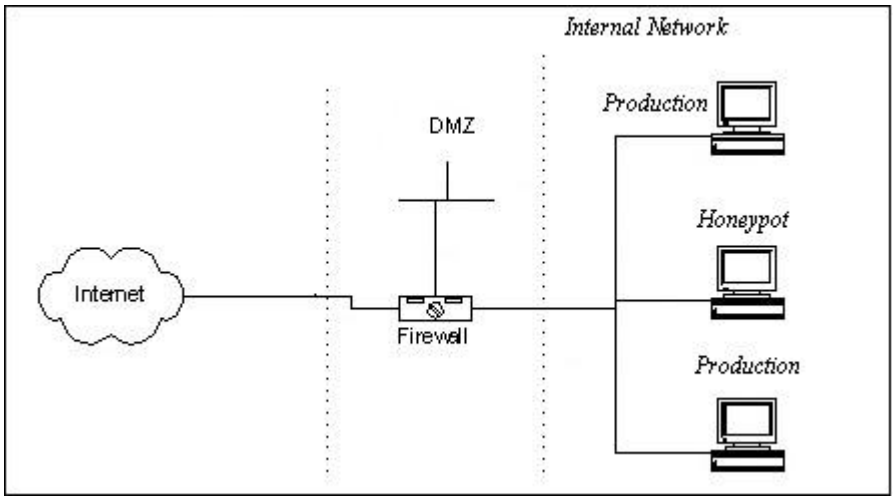
#### 4.5.1 Τοποθέτηση Μετά το Τείχος Προστασίας

Κατά την τοποθέτηση του honeypot μέσα από το τείχος προστασίας, η κίνηση του δικτύου για να αλληλεπιδράσει με το honeypot θα πρέπει να περάσει από το τείχος προστασίας. Στο σημείο αυτό προκύπτει το πρόβλημα για το πώς θα ελεγχτεί η ροή της κίνησης του δικτύου προς το honeypot χωρίς να σταματήσει στο τείχος προστασίας, και χωρίς να βλάψει το εσωτερικό του δικτύου.

Σε κάθε περίπτωση θα πρέπει να παραμετροποιηθεί κατάλληλα και με προσοχή το τείχος προστασίας για το τι είδους πληροφορίες δεν θα σταματά να εισέλθουν στο δίκτυο. Επίσης καλό θα ήταν επειδή το honeypot θα προσελκύσει κακόβουλους χρήστες, να τοποθετηθεί ένα ακόμα τείχος προστασίας το οποίο θα διαχειρίζεται την κίνηση του δικτύου από το honeypot προς το υπόλοιπο δίκτυο. Είναι πολύ σημαντικό να υπάρχουν κατάλληλα μέτρα ασφάλειας από τον διαχειριστή του συστήματος σε αυτή την

τοποθέτηση. Αν για οποιονδήποτε λόγο τυχόν απειλή που θα κατορθώσει να ξεπεράσει το honeypot θα είναι σε θέση να επιτεθεί σε ολόκληρο το υπόλοιπο δίκτυο κατά βούληση του επιτιθέμενου.

Η επιλογή της τοποθέτησης αυτής γίνεται κυρίως σε περιπτώσεις που θέλουμε να ανακαλύψουμε απειλές που βρίσκονται στο εσωτερικό του δικτύου ή όταν ο υπάρχουν αρκετές πιθανότητες απειλές να περιλαμβάνουν μηχανισμούς που να ξεπερνούν το τείχος προστασίας.

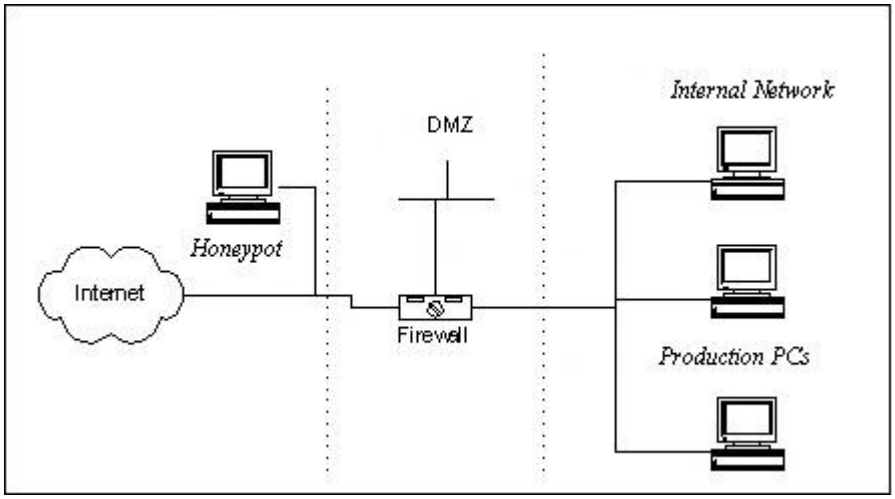



*ΣΧΗΜΑ 4.2: Τοποθέτηση «Honeypot» μετά το τείχος προστασίας, στο εσωτερικό δίκτυο.*

### 4.5.2 Τοποθέτηση Πριν το Τείχος Προστασίας

Κατά την τοποθέτηση εξωτερικά του τείχους προστασίας, το honeypot είναι εκτεθειμένο στο δίκτυο και την κίνηση του. Αποτελεί μια ξεχωριστή οντότητα στο υποδίκτυο που υπάγεται αυτό και όλες οι υπόλοιπες συσκευές – συστήματα που υπάγονται στο υποδίκτυο. Πρακτικά αυτό σημαίνει πως ο διαχειριστής δεν θα αφιερώσει χρόνο, για να ρυθμίσει το τείχος προστασίας για την λειτουργία του σε συνδυασμό με το honeypot. Η φύση του honeypot είναι να προκαλεί το ενδιαφέρον για επιθέσεις, συνεπώς η κίνηση προς το τοίχος προστασίας θα ήταν αυξημένη.

Το πιο σημαντικό μειονέκτημα για την επιλογή αυτή, είναι πως αν ο εισβολέας βρεθεί εντός του δικτύου και θέλει να αλληλεπιδράσει με το honeypot, θα συναντήσει δυσκολίες από το τείχος προστασίας, επειδή περιλαμβάνει μηχανισμούς που αναστέλλουν την εξερχόμενη κίνηση του δικτύου, από το υποδίκτυο προς το δίκτυο και συνεπώς προς το honeypot.

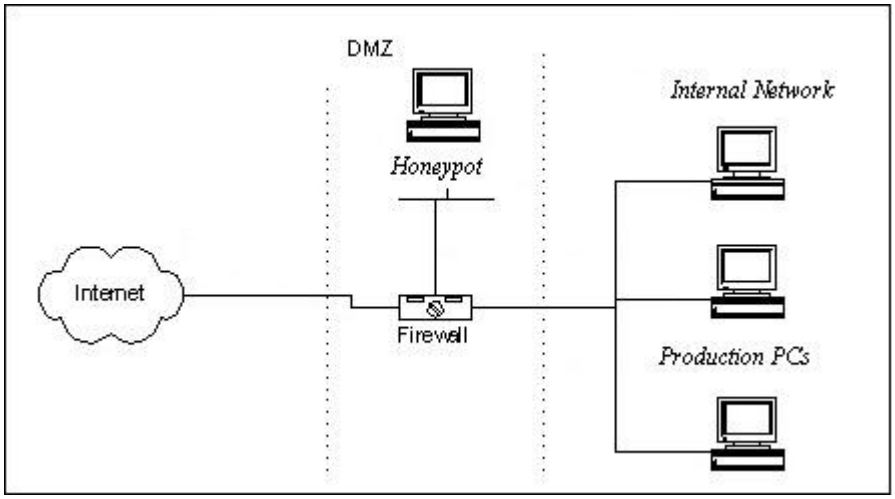



*ΣΧΗΜΑ 4.3: Τοποθέτηση «Honeypot» πριν το τείχος προστασίας.*

### 4.5.3 Τοποθέτηση στην Αποστρατικοποιημένη Ζώνη

Η αποστρατικοποιημένη ζώνη είναι ένα υπολογιστικό σύστημα το οποίο διαχειρίζεται ολόκληρη την κίνηση των δεδομένων που προέρχονται από το διαδίκτυο. Η κίνηση αυτή είναι σε πρώτο χρόνο και δεν υπάρχει κάποιου είδους έλεγχος πριν καταλήξει στο σύστημα, ακριβώς γι' αυτό η επιλογή της θέσης αυτής για το honeypot προϋποθέτει την αυστηρή παραμετροποίηση του και συχνούς ελέγχους, για να μην βλάψουν το υπολογιστικό μας σύστημα οι ενδεχόμενες απειλές.

Τις περισσότερες φορές επιλέγεται η εγκατάσταση του honeypot σε αυτή την περιοχή για να ελέγχουμε αν στη συγκεκριμένη ζώνη εμφανιστούν απειλές μη εξουσιοδοτημένης πρόσβασης ή κακόβουλου λογισμικού. Ωστόσο η περιοχή αυτή από κατασκευής δεν παρουσιάζει αυξημένη κίνηση από το δίκτυο και μόνο συγκεκριμένες υπηρεσίες επικοινωνούν μαζί της.




*ΣΧΗΜΑ 4.4: Τοποθέτηση του «Honeypot» στην αποστρατικοποιημένη ζώνη.*

### 4.6 Κατηγορίες «HONEYPOT»

Οι εφαρμογές honeypot ανάλογα με τον στόχο και τον τρόπο που λειτουργούν χωρίζονται σε δύο μεγάλες κατηγορίες.

- Με βάση τον σκοπό χρήσης
- Με βάση τον βαθμό αλληλεπίδρασης

**Με Βάση τον Σκοπό Χρήσης**

Με βάση τον σκοπό χρήσης συναντάμε δύο είδη honeypot, τα honeypot έρευνας, και τα παραγωγής honeypot.

Τα honeypot έρευνας είναι ερευνητικά συστήματα που χρησιμοποιούνται για να αποκομίσουν πληροφορίες οι διαχειριστές των συστημάτων για τον τρόπο δράσης τον κακόβουλων χρηστών, και των εφαρμογών που χρησιμοποιούν για να πετύχουν τις επιθέσεις τους. Υλοποιούνται πολλές φορές μέσα σε εικονικά συστήματα που προσομοιώνουν πλήρως τα φυσικά συστήματα, για την ελαχιστοποίηση της εξάπλωσης των απειλών, σε περιπτώσεις μόλυνσης. Δεν παρέχουν κάποια αντίσταση στις απειλές, το αντίθετο κάνουν μάλιστα, χρησιμοποιούν γνωστά κενά ασφάλειας ή παλιές εκδώσεις λογισμικών, για να προσελκύσουν τους επιτιθέμενους. Τα δεδομένα που συλλέγουν τα επεξεργάζονται πανεπιστήμια και ερευνητικά κέντρα με σκοπό την απόκτηση γνώσης, που θα εφαρμοστεί για την ανάπτυξη νέων συστημάτων άμυνας ή την αναβάθμιση των είδη υπαρχόντων.

Τα honeypot παραγωγής λειτουργούν σε συγκεκριμένα δίκτυα και σταθμούς εργασίας, με σκοπό την αξιολόγηση των συστημάτων άμυνας που διαθέτουν. Αυτό το πετυχαίνουν με την δημιουργία των honeypot, προσομοιώνοντας πλήρως τις δυνατότητες των συστημάτων που αποτελούν το δίκτυο της επιχείρησης ή του οργανισμού. Όταν θα λάβει χώρα μια επίθεση αφενός θα συλλέξουν πολύτιμα στοιχεία για την μορφή και το λογισμικό της επίθεσης και αφετέρου θα αξιολογηθεί η κατάσταση της ασφάλεια τη συγκεκριμένη χρονική περίοδο στο δίκτυο.

### 4.6.1 Χαμηλής Αλληλεπίδρασης

Στη χαμηλού επιπέδου αλληλεπίδραση honeypot, περιλαμβάνονται οι εφαρμογές που παραμετροποιούνται μέσω αρχείων script. Μπορούν να εγκατασταθούν σχετικά εύκολα σε εικονικά συστήματα. Δεν μοιάζουν με πραγματικά λειτουργικά συστήματα αντιθέτως αντιγράφουν δικτυακές υπηρεσίες. Έχουν περιορισμένη δυνατότητα να αλληλεπιδράσουν με τον εισβολέα, συνεπώς είναι και περιορισμένες οι πληροφορίες που μπορούν να αποκομίσουν. Τις περισσότερες φορές χρησιμοποιούνται για να καταγραφούν παράνομες συνδέσεις και αιτήματα στο δίκτυο εφαρμογής. Ένα παράδειγμα γνωστού honeypot χαμηλής αλληλεπίδρασης, είναι το Honeyd.

### 4.6.2 Μεσαίας Αλληλεπίδρασης

Στην κατηγορία αυτή ανήκουν τα honeypot που έχουν περισσότερους μηχανισμούς αλληλεπίδρασης με τους επιτιθέμενους. Προσφέρουν την δυνατότητα να είναι σε θέση να απαντούν στα αιτήματα, των εισβολέων με τη χρήση ψεύτικων δεδομένων με σκοπό να αποκομίσουν, ακόμα περισσότερες πληροφορίες. Όπως ακριβώς δηλαδή λειτουργούν οι δικτυακές υπηρεσίες. Μπορούν επίσης να αποθηκεύσουν κακόβουλο λογισμικό για επεξεργασία και ερευνητικούς σκοπούς. Τέλος θα πρέπει να επισημάνουμε, πως λόγω του ότι η αλληλεπίδραση είναι μεγαλύτερη από αυτήν στα χαμηλής αλληλεπίδρασης honeypot, η επικινδυνότητα αυξάνεται για το σύστημα και πρέπει να τηρούνται όλοι οι κανόνες ασφάλειας, για να μην υπάρξουν δυσάρεστες συνέπιες.

### 4.6.3 Υψηλής Αλληλεπίδρασης

Τα honeypot υψηλής αλληλεπίδρασης αποτελούν πραγματικά λειτουργικά συστήματα με ευπάθειες. "Τρέχουν" κανονικά συστήματα όπως όλα τα λειτουργικά συστήματα που γνωρίζουμε, δεν χρησιμοποιούν δηλαδή εικονικά συστήματα προσομοίωσης. Ο κακόβουλος χρήστης μπορεί να εισέλθει σε ένα ευπαθές σημείο του, και να αποκτήσει μερική ή καθολική πρόσβαση, ανάλογα πάντα με το είδος της επίθεσης αλλά και με το πόσο σοβαρό είναι το κενό της ασφάλειας. Όσο μεγαλύτερη είναι η αλληλεπίδραση με τον επιτιθέμενο τόσο περισσότερες πληροφορίες μπορούμε να αντλήσουμε, για τις τεχνικές και τις μεθόδους των επιθέσεων που εκτελεί. Άρα έχουμε περισσότερη γνώση για την κατασκευή καλύτερων, συστημάτων άμυνας και προφύλαξης. Η γνώση προκύπτει από προγράμματα παρακολούθησης που λειτουργούν εσωτερικά του honeypot, και καταγραφούν στιγμή προς στιγμή τι εκτελείται και πως.

Από την άλλη πλευρά όμως διαθέτουν αυξημένο ρίσκο ακριβώς γιατί διαθέτουν μεγάλη αλληλεπίδραση. Κάτι που σημάνει πως αν δεν προσέξει ο διαχειριστής και τελικά ο επιτιθέμενος κυριεύει το σύστημα, θα μπορεί να εξαπολύσει επιθέσεις σε άλλους υπολογιστές ή δίκτυα με την χρήση του υπολογιστή honeypot. Κάτι τέτοιο πρέπει να λογίζεται πιθανό σενάριο, και να λαμβάνονται τα κατάλληλα μέτρα όπως είναι προγράμματα ασφάλειας και τείχη προστασίας. Άλλα και το δίκτυο στο οποίο συμμετέχει είναι σημαντικό να ξέρουμε τι άλλες συσκευές περιλαμβάνει, αλλά και με τι άλλα δίκτυα επικοινωνεί ώστε να μπορούμε να υπολογίσουμε σε περίπτωση μόλυνσης τι άλλες συσκευές ή δίκτυα μπορούν να εκτεθούν στον επιτιθέμενο.

## 4.7 Πλεονεκτήματα και Μειονεκτήματα «HONEYPOT»

Τα honeypots όπως και κάθε τεχνολογία παρουσιάζουν θετικά αλλά και αρνητικά στοιχεία κατά την χρήση τους. Με βάση την μελέτη τους προκύπτουν τα παρακάτω πλεονεκτήματα αλλά και μειονεκτήματα, τα οποία εμφανίζονται σε μικρό η μεγάλο βαθμό ανάλογα με το honeypot και τις ιδιαιτερότητες που το χαρακτηρίζουν.

### 4.7.1 Πλεονεκτήματα

- Απλή λειτουργία: Σε αντίθεση με τα συστήματα ανίχνευσης επιθέσεων, τα honeypots χρησιμοποιούν πολύ λιγότερους πόρους κατά την λειτουργία τους.
  Τα εργαλεία και τα υποσυστήματα που "τρέχουν" δεν έχουν μεγάλες απαιτήσεις στη χρήση της μνήμης του συστήματος.
- Μπορούν να ανακαλύψουν νέες απειλές. Κάθε δραστηριότητα που αλληλεπιδρά με το honeypot λογίζεται σαν απειλή. Με τον τρόπο αυτόν ακόμα και αν δεν γνωρίζουμε τι είδους κακόβουλο λογισμικό είναι αυτό, υπάρχει η δυνατότητα να το μελετήσουμε.
- Μικρές απαιτήσεις συστήματος: Υπολογιστικά συστήματα με όχι τόσο δυνατούς επεξεργαστές η μεγάλης χωρητικότητας φυσικές μνήμες, μπορούν να λειτουργήσουν αρκετά honeypots.
- Υψηλή δυνατότητα αποθήκευσης δεδομένων από τις επιθέσεις ακόμα και τα δεδομένα αυτά είναι κρυπτογραφημένα από τον επιτιθέμενο.
- Δυνατότητα ανίχνευσης απειλών που βρίσκονται στο εσωτερικό του δικτύου.
- Χαμηλός αριθμός ψευδών ειδοποιήσεων (false positives): Κυρίως τα συστήματα ανίχνευσης επιθέσεων αντιμετωπίζουν συχνά αυτό το φαινόμενο από τον μεγάλο όγκο της κίνησης των δεδομένων. Πολλές από τις ειδοποίησης τους χαρακτηρίζονται ως ύποπτες χωρίς όμως πραγματικά να είναι. Στα honeypot κάθε δραστηριότητα είναι ύποπτη.
- Μικρός όγκος πληροφοριών προς επεξεργασία: Τα honeypots αποθηκεύουν πληροφορίες που προκύπτουν μόνο από δραστηριότητες που έχουν στόχο αυτά, και δεν επηρεάζονται από την κίνηση που επικρατεί στο υπόλοιπο δίκτυο

### 4.7.2 Μειονεκτήματα

- Τα honeypots προσελκύουν απειλές, υπάρχει πάντα ο κίνδυνος οι απειλές αυτές να υπερκεράσουν τους μηχανισμούς άμυνας και να μολύνουν το υπόλοιπο δίκτυο και τα συστήματα που περιλαμβάνει.
- Η αξία των honeypots έγκειται στην αλληλεπίδραση τους με τους επιτιθέμενους. Αν για οποιαδήποτε λόγο αυτή η αλληλεπίδραση χαθεί, χάνετε και η αξία των honeypot.
- Η ύπαρξη των honeypots μπορεί να αποκαλυφθεί από εξειδικευμένα εργαλεία ή έμπειρους χρήστες.

- Η προσέλκυση δικτυακής κίνησης για αλληλεπίδραση με τα honeypots αν ξεπεράσει κάποια όρια, θα προκαλεί καθυστερήσεις στην επικοινωνία των υπόλοιπων συστημάτων που τυχόν θα περιλαμβάνει το δίκτυο.

### 4.8 Τα «HONEYNETS»

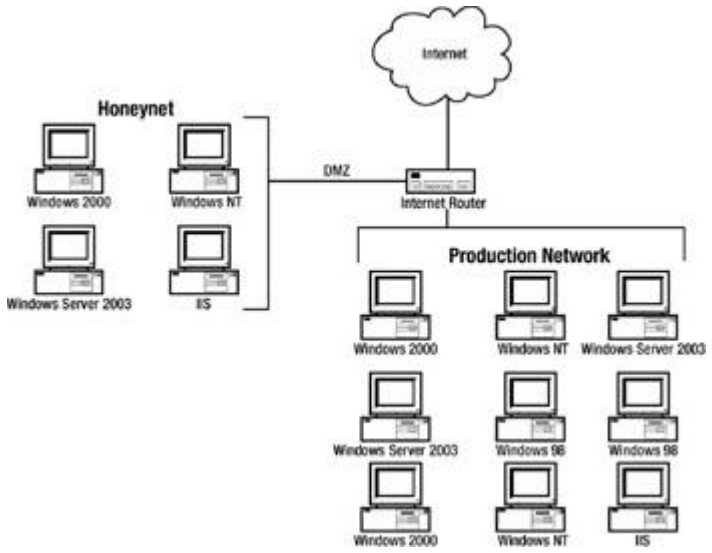
Τα honeynets αποτελούν honeypots υψηλής αλληλεπίδρασης. Είναι ένα σύνολο συστημάτων και υπηρεσιών που χαρακτηρίζονται ως μια αρχιτεκτονική. Στο εσωτερικό τους περιλαμβάνουν εικονικά συστήματα παραγωγής και υπηρεσίες όπως ακριβώς θα συναντούσε κάποιος σε οποιοδήποτε άλλο δίκτυο υπολογιστικών συστημάτων. Για τον λόγο αυτό κιόλας είναι πολύ πιο ελκυστικά από τα απλά honeypots στους επιτιθέμενους αφού προσφέρουν περισσότερες επιλογές στον κακόβουλο χρήστη, για να αλληλεπιδράσει με ένα ολόκληρο δίκτυο. Η αποστολή τους είναι να παρακολουθούν να ελέγχουν και να καταγράφουν ροές πληροφοριών από και προς το δίκτυο τους. Μπορούν άμεσα να αντιληφτούν οποιαδήποτε μη εξουσιοδοτημένη ενέργεια λάβει χώρα εντός του δικτύου. Σε κάθε περίπτωση όμως για λόγους ασφάλειας το honeynet πρέπει να είναι κατάλληλα διαχωρισμένο, αν συνυπάρχει με ένα δίκτυο παραγωγής υπολογιστών διότι ελλοχεύει πάντα ο κίνδυνος να υπάρξει η απειλή που θα μολύνει ή ακόμη και θα καταλάβει ολόκληρο το δίκτυο.

Για πρώτη φορά βλέπουμε τα honeynets κάνουν την εμφάνιση τους από μία κοινότητα ανθρώπων με όνομα Honeynet Project. Τα μέλη της ομάδας αυτής, ήθελαν να δημιουργήσουν κάτι με το οποίο θα είχαν την δυνατότητα, να ερευνήσουν και να αξιολογήσουν τις γνώσεις και τις πρακτικές που ακολουθούσαν οι κακόβουλοι χρήστες, καθώς επίσης και τα κίνητρα που τους ωθούσαν στις ενέργειες αυτές.

Εξετάζοντας ένα honeynet μπορούμε να διακρίνουμε πως υποστηρίζει μια ποικιλομορφία στα συστήματα τα οποία μπορεί να περιλαμβάνει να διαχειρίζεται καθώς και να παρακολουθεί σε πρώτο χρόνο. Οι ροές πληροφοριών που "τρέχουν" μέσα στο δίκτυο, μπορούν να εξεταστούν συνολικά ακόμα και αν προέρχονται από υπολογιστικές μονάδες του δικτύου με διαφορετικά λειτουργικά συστήματα – κάτι που αποτελεί και ένα από τα πολλά πλεονεκτήματα που παρουσιάζουν τα honeynets. Παράλληλα ο ρυθμός των δεδομένων που συλλέγονται έχει να κάνει με την έκταση του δικτύου, και το πλήθος των συσκευών που υπάρχουν μέσα σε αυτό.

Ο παραγόμενος όγκος πληροφοριών από το honeynet για να επεξεργαστεί και να αναλυθεί απαιτεί, ανάλογα με την έκταση του κατάλληλους υπολογιστικούς πόρους. Κάτι που μεταφράζεται σε έξοδα για κάθε επιχείρηση ή οργανισμού που το διαχειρίζεται. Ακόμη η εγκατάσταση και η σωστή χρήση του αποτελούν σύνθετη διαδικασία, για να καταφέρει ο διαχειριστής του honeynet να αντιλήφθη μία πιθανή απειλή, πόσο μάλλον όταν η έκταση του είναι μεγάλη.

Από την σκοπιά της ασφάλειας τα honeynet έχουν δημιουργηθεί έτσι ώστε να εκλαμβάνουν μια σύνδεση με προέλευση έξω από το δίκτυο και κατεύθυνση το εσωτερικό του honeynet ως πιθανή απειλή. Κατ' αντιστοιχία πιθανές συνδέσεις στο εσωτερικό του honeynet, από συσκευή προς συσκευή, αντιμετωπίζονται ύποπτα για το ενδεχόμενο να έχει μολυνθεί από κακόβουλο λογισμικό η συσκευή απ' όπου προέρχεται η "επιθυμία" σύνδεσης.

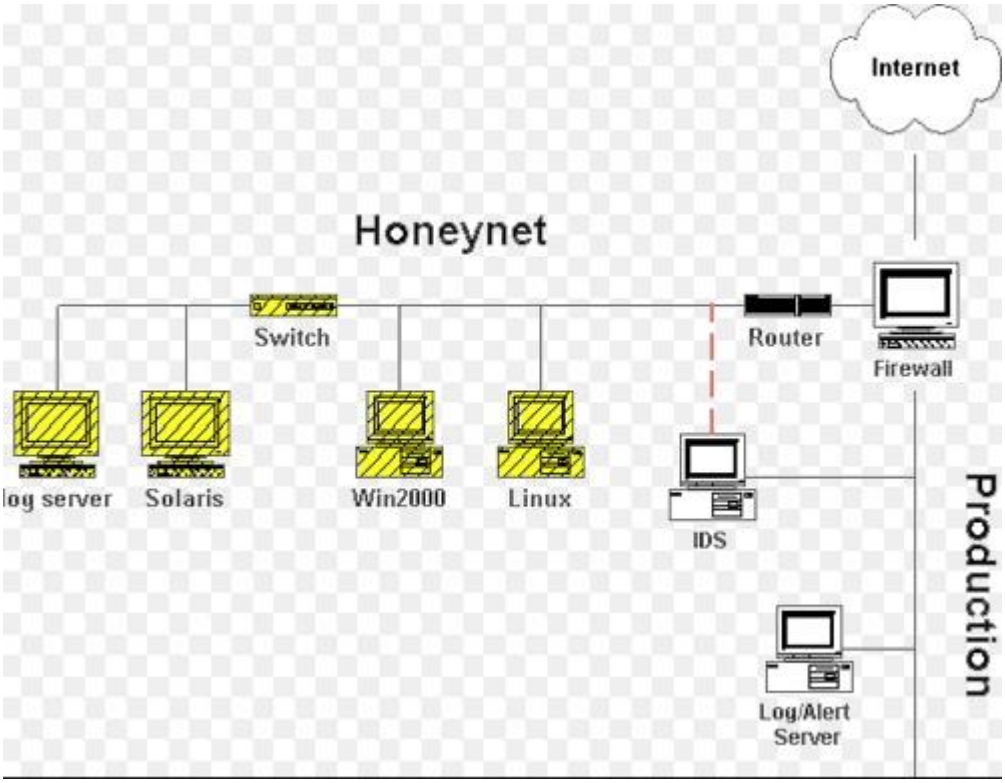



*ΣΧΗΜΑ 4.5: Απεικόνιση δικτύου «Honeynet» τοποθετημένο στην αποστρατικοποιημένη ζώνη του δικτύου (πηγή: flylib).*

### 4.8.1 «Honeynets» 1ης Γενιάς (GenI)

Αποτελούν τα πρώτα honeynets, και δημιουργήθηκαν από την ομάδα Honeynet Project στα τέλη του 20ου αιώνα. Η αποστολή τους ήταν να καλύψουν την ροή πληροφοριών στο δίκτυο που λειτουργούν, και να καταγράψουν δεδομένα για μετέπειτα επεξεργασία. Σε σχέση με τα μεμονωμένα honeypot, τα honeynets προσέλκυαν πολύ περισσότερες απειλές, ο επιτιθέμενος πλέον είχε όχι μόνο μία επιλογή, αλλά ένα δίκτυο υπολογιστικών συστημάτων για να αλληλεπιδρά. Για την καταγραφή των δεδομένων, γινόταν χρήση

ενός συστήματος ανίχνευσης επιθέσεων (IDS). Το σύστημα αυτό περιελάμβανε δύο κάρτες δικτύου, μία για την επίβλεψη του honeypot (χωρίς να φαίνεται η διασύνδεση τους με χρήση διεύθυνσης IP) και μια για την διαχείριση του ιδίου. Επίσης για μην μολυνθούν τα υπόλοιπα συστήματα του δικτύου, γινόταν χρήση δύο μηχανισμών ασφάλειας. Ο πρώτος ήταν από την χρήση του firewall, και ο δεύτερος μηχανισμός από την κατάλληλη λειτουργία του router. Τα επόμενα χρόνια με την εξέλιξη της γνώσεις των επιτιθέμενων στην εφαρμογή απειλών, τα honeynets γινόντουσαν αντιληπτά από την αρχιτεκτονική τους (Για λόγους προστασίας του δικτύου χρησιμοποιούσαν το πρωτόκολλο NAT για να αποκλείσουν συνδέσεις συσκευών στο εσωτερικό.) και σταμάτησαν να είναι αποτελεσματικά.

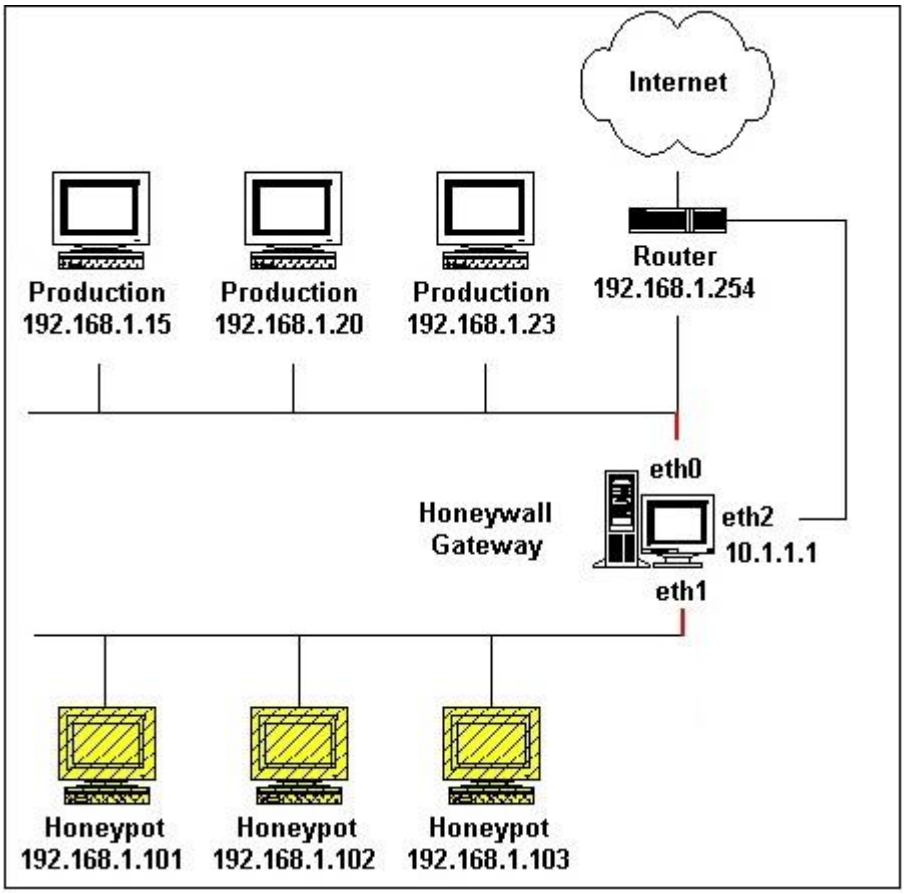



*ΣΧΗΜΑ 4.6: Απεικόνιση «Honeynet» δικτύου πρώτης γενιάς (πηγή: The Honeynet Project).*

### 4.8.2 «Honeynets» 2ης Γενιάς (GenII)

Τα honeynets δεύτερης γενιάς αποτελούν την εξέλιξη της πρώτης γενιάς honeynet και αναπτύχθηκαν επίσης από την ομάδα Honey Project το 2002. Η μεγαλύτερη ανάγκη που έδωσε και το κίνητρο για να εξελιχθεί η τεχνολογία αυτή, ήταν τα αντίμετρα. Μέθοδοι λειτουργίας και συμπεριφοράς δηλαδή κατά τις οποίες το honeynet ακολουθεί, για να μην

γίνει αντιληπτό από τους επιτιθέμενους και χάσει την αποτελεσματικότητα του. Σε αυτήν την γενιά συμπεριέλαβαν ένα σύστημα έξω από το υποδίκτυο των honeypots που ελέγχει την δραστηριότητα του δικτύου από το δεύτερο επίπεδο του πρωτοκόλλου OSI (OSI – layer 2). Το σύστημα αυτό το ονόμασαν «honeywall», διέθετε δύο κάρτες δικτύου, μία για επικοινωνία μόνο με τον διαχειριστή για λόγους ασφαλείας, και μία για επικοινωνία με το δίκτυο. Ο ρόλος του ήταν να διαχειρίζεται την κίνηση στο υποδίκτυο των honeypots, και να λειτουργεί σαν ασπίδα προστασίας σε τυχόν επιθέσεις από τα honeypots που περιλαμβάνει το υποδίκτυο στα συστήματα παραγωγής του υπόλοιπου δικτύου.

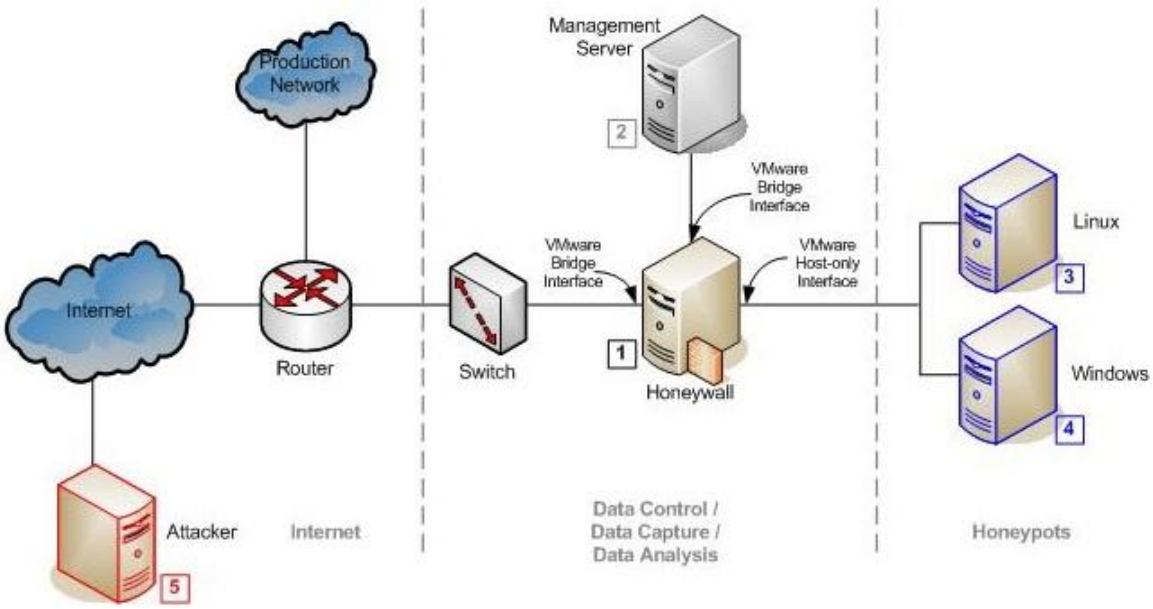



*ΣΧΗΜΑ 4.7: Απεικόνιση «Honeynet» δικτύου δεύτερης γενιάς (πηγή: The Honeynet Project).*

### 4.8.3 «Honeynets» 3ης Γενιάς (GenIII)

Η τελευταία μέχρι στιγμής γενιά honeynet, κυκλοφόρησε το 2004 με την ονομασία «Honeywall CDROM Roo» μετά από έρευνες της ομάδας Honeynet Project. Αν και τα βασικά χαρακτηριστικά της αρχιτεκτονικής στηρίχθηκαν στην δεύτερη γενιά χωρίς να

αλλάξουν, οι αλλαγές που έκαναν βελτίωσαν κατά πολύ την συμπεριφορά και την χρήση του honeynet. Πιο συγκεκριμένα με την χρήση το Honeywall CDROM Roo η δυνατότητα εγκατάστασης και λειτουργίας ενός honeynet έγινε πιο εύκολη. Υπήρχε μεγαλύτερη συμβατότητα με διαφορετικές εκδώσεις υλικού, πιο φιλικό περιβάλλον χρήσης, νέες εκδώσεις υποσυστημάτων και δυνατότητα αναβαθμίσεων.




*ΣΧΗΜΑ 4.8: Απεικόνιση ενός εικονικού δικτύου «Honeynet» τρίτης γενιάς, με δύο honeypot με διαφορετικά λειτουργικά συστήματα, Linux και Windows αντίστοιχα (πηγή: The Honeynet Project).*

## 4.9 Νομικά Ζητήματα «HONEYPOT»

Πολλές από τις ενέργειες των honeypots είναι να παρακολουθούν ροές πληροφοριών που παράγονται από την αλληλεπίδραση με τρίτους (χωρίς εκείνοι να το γνωρίζουν), ακόμα και να καταγράφουν κομμάτια η ολόκληρο το λογισμικό που επικοινωνούν. Τις περισσότερες φορές ο χαρακτήρας τους είναι ερευνητικός και ψάχνουν για κακόβουλο λογισμικό, αυτό όμως δεν μπορεί από μόνο του, να καλύψει τα νομικά κενά που προκύπτουν. Μέχρι σήμερα δεν υπάρχει κάποιο συνολικό νομικό πλαίσιο που να εφαρμόζεται από όλες τις χώρες για την ανάπτυξη και χρήση των honeypots. Κάθε χώρα ξεχωριστά ανάλογα με του νόμους της, θέτει και τα αντίστοιχα όρια στην χρήση τους. Ο

L.Spitzner στο βιβλίο του “Honeypots : Tracking a Hackers” αναφέρει για το πρόβλημα της νομιμότητας των honeypots, πως πρέπει να εξετάζονται από την πλευρά της παγίδευσης, και της ιδιωτικότητας.

### 4.9.1 Παγίδευση

Η παγίδευση, (entrapment) δεν είναι νόμιμη ενέργεια και αποτελεί ποινικό αδίκημα, το οποίο εκτελείται χωρίς δόλο από τον δράστη. Στην εφαρμογή τους τα honeypots δεν επιτίθενται κάπου, είναι συστήματα παραγωγής ή εξομοιώνουν συστήματα παραγωγής. Οι επιτιθέμενοι ψάχνουν για ευπαθή συστήματα και όταν τα ανακαλύψουν θα τους επιτεθούν κατά βούληση. Ο διαχειριστής του honeypot είναι ένας ερευνητής, δεν είναι όργανο της τάξης, στόχος του είναι η γνώση που θα αποκομίσει από την χρήση του honeypot, να εφαρμοστεί για να βελτιώσει την ενεργητική ασφάλεια του δικτύου του.

### 4.9.2 Ιδιωτικότητα

Κατά την λειτουργία των honeypots συλλέγονται δεδομένα και πληροφορίες από τους χρήστες που έρχονται σε επαφή με τα honeypots. Οι πληροφορίες αυτές αρχικά όπως και κάθε άλλη πληροφορία που διακινείται στο διαδίκτυο υπερασπίζεται από το καθεστώς της υπεράσπισης του ιδιωτικού απορρήτου που διακατέχει κάθε ελεύθερο μέλος της κοινωνίας.

Στην εφαρμογή της Αμερικάνικης νομοθεσίας για θέματα ιδιωτικού απορρήτου και χρήσης honeypot, τα πράγματα είναι διαφορετικά. Αρχικά όποιος εισέρχεται με μη εξουσιοδοτημένη πρόσβαση σε κάποιο σύστημα χάνει την ίδια στιγμή και το δικαίωμα της ιδιωτικότητας στην διακίνηση πληροφοριών. Από την άλλη η λειτουργία των honeypots ως μέσω επικοινωνίας στο διαδίκτυο δεν υποστηρίζεται από τον νόμο της προστασίας των δεδομένων, επειδή τα honeypots δεν λογίζονται ως υπηρεσίες που παρέχουν κάποιου είδος υπηρεσίας στο δίκτυο. Ουσιαστικά κατατάσσονται μαζί με όλα τα υπόλοιπα συστήματα ασφάλειας που παρακολουθούν τις ενέργειες του δικτύου.

# Κεφάλαιο 5 – Υλοποίηση «HoneyBOT»

## 5.1 Γνωριμία με το «HoneyBOT»

Το HoneyBOT είναι ένα πρόγραμμα εφαρμογής honeypot μέσης αλληλεπίδρασης φτιαγμένο για να λειτουργεί σε λειτουργικά συστήματα Windows. Πρόκειται για μια εφαρμογή δωρεάν για το κοινό, με κλειστό κώδικα που δημιουργήθηκε από την Atomic Software Solution, και δημιουργεί ένα ασφαλές περιβάλλον αποικοδόμησης και αλληλεπίδρασης μη εξουσιοδοτημένης δραστηριότητας στο δίκτυο. Έχει μεγάλη δυνατότητα καταγραφής κινήσεων από οποιοδήποτε άλλο εργαλείο ανίχνευσης απειλών. Καταγράφει την κίνηση των πακέτων, ακόμη και τα πλήκτρα που πατά ο επιτιθέμενος. Το αρχείο καταγραφής πληροφοριών που διαθέτει είναι ιδιαίτερα σημαντικό καθώς αποθηκεύονται μόνο πληροφορίες που σχετίζονται με τις επιθέσεις με ποσοστό λάθους σχεδόν μηδενικό. Με την χρήση των honeypots και συγκεκριμένα του HoneyBOT μας δίνεται η δυνατότητα να ερευνήσουμε σε πρώτο χρόνο νέες απειλές που ενδεχομένως δεν έχουν βρεθεί τρόποι καταπολέμησης ακόμη. Είναι ένα εργαλείο όπου η σωστή χρήση του θα μας δώσει τις αυριανές αναβαθμίσεις για τα συστήματα ενεργητικής ασφάλειας.

Ο τρόπος λειτουργίας είναι απλός το HoneyBOT ανοίγει μια σειρά από υποδοχές του υπολογιστή και τις προσαρμόζει ώστε να μοιάζουν με ευάλωτες υπηρεσίες. Ο επιτιθέμενος συνδέεται με αυτές τις υπηρεσίες και έχει την εντύπωση πως επιτίθεται σε κάποιον πραγματικό server. Το honeypot συλλαμβάνει με ασφάλεια όλες τις επικοινωνίες με τον εισβολέα και καταγράφει όλα τα αποτελέσματα των αναζητήσεων για μελλοντική ανάλυση. Στην περίπτωση όπου ο επιτιθέμενος προσπαθήσει να ανεβάσει κακόβουλο λογισμικό, το περιβάλλον του honeypot μπορεί να αποθηκεύει με ασφάλεια στον υπολογιστή για ποιο εκτενή ανάλυση.

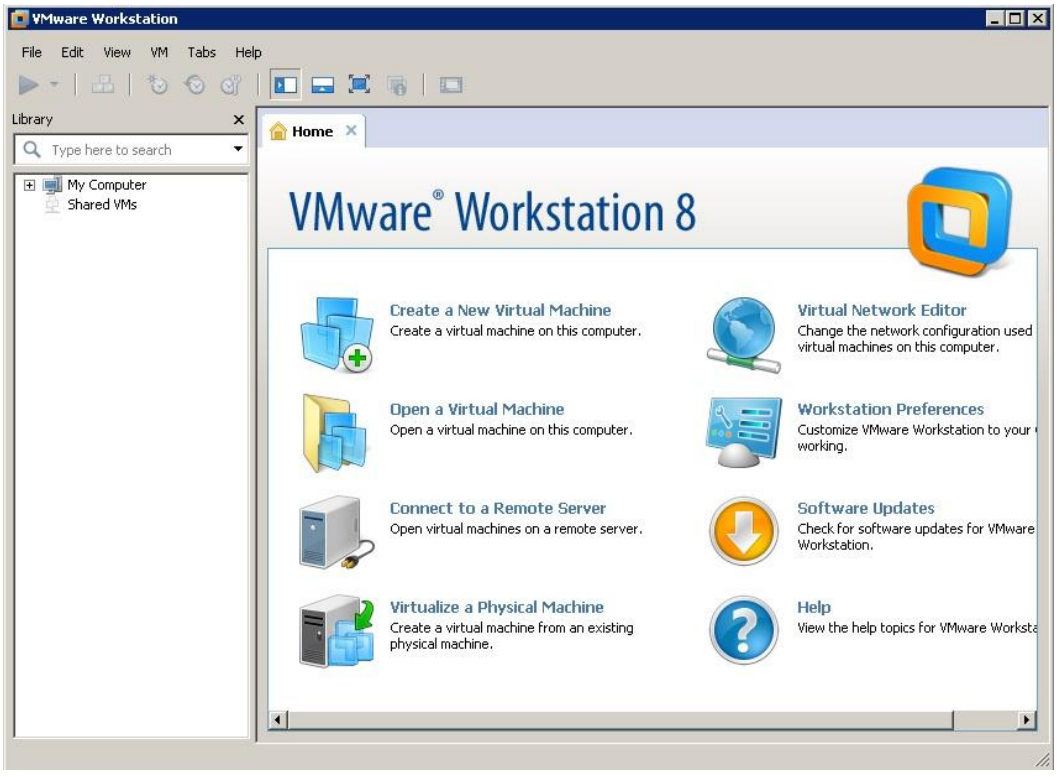
## 5.2 Υλοποίηση «HoneyBOT» σε Εικονικό Σύστημα

Η μελέτη της λειτουργίας του HoneyBOT έγινε σε εικονικό περιβάλλον με την χρήση του προγράμματος VMware, που είναι ιδανικό για την εγκατάσταση και εφαρμογή τέτοιων συστημάτων καθώς προσφέρει δυνατότητες να “τρέξουν” παράλληλα διαφορετικά λειτουργικά συστήματα ανάλογα με τις ανάγκες του χρήστη. Ακόμη έγινε χρήση του προγράμματος Wireshark για να έχουμε μια καλύτερη εικόνα για όλες τις

δικτυακές επικοινωνίες του συστήματος, και αφού λειτούργησαν όλα όπως έπρεπε, από το αρχικό σύστημα μέσω της γραμμής εντολών των Windows και με την χρήση ενός εργαλείου Perl script για επίθεση, πραγματοποιήθηκε μια DDOS επίθεση στο εικονικό σύστημα θύμα. Πάμε όμως να τα δούμε ποίο αναλυτικά όλα τα παραπάνω.

### 5.2.1 VMware

Η εταιρία VMware διαθέτει στην αγορά εργαλεία λογισμικού εικονοποίησης. Τα εργαλεία αυτά είναι πλήρως εξοπλισμένα με το κατάλληλο λογισμικό και μπορούν να εξομοιώσουν όλες τις συσκευές που διαθέτει ένας υπολογιστής από την πλευρά του υλικού( σκληρός δίσκος, κάρτα γραφικών, οδηγός δίσκων, σειριακές και παράλληλες θύρες). Ακόμη υπάρχει η δυνατότητα της επιλογής του λειτουργικού συστήματος που θέλει να δουλέψει ο χρήστης.




*ΣΧΗΜΑ 5.1: Το παράθυρο εκκίνησης της εφαρμογής VMware που χρησιμοποιήθηκε για την υλοποίηση του «honeypot».*

### 5.2.2 Wireshark

Είναι ένα εργαλείο με ελεύθερο και ανοιχτό κώδικα που μας επιτρέπει να παρακολουθούμε και να αναλύουμε το δίκτυο στο οποίο εφαρμόζεται με μεγάλη ακρίβεια και πολλές λεπτομέρειες. Το πρώτο του όνομα ήταν Ethereal, όμως για εμπορικούς λόγους άλλαξε το 2006. Οι εκδώσεις του υποστηρίζουν τα ποιο γνωστά λειτουργικά συστήματα όπως είναι τα windows, Linux, Mac OS, και Solaris. Έχει πολλές δυνατότητες ταξινόμησης και φιλτραρίσματος των πληροφοριών και προσφέρει στον χρήστη την ικανότητα να παρακολουθεί ολόκληρη την κίνηση του δικτύου, βάζοντας την κάρτα δικτύου σε ετερόκλητη λειτουργία (promiscuous mode) για την καθολική παρακολούθηση των πακέτων. Παρόλο που μέχρι σήμερα έχουν κυκλοφορήσει αρκετές αναβαθμίσεις με νεότερη την 2.0.3, στην εφαρμογή μας επιλέχτηκε η έκδοση 1.10.2 καθώς ήταν η τελευταία η οποία υποστήριζε τα windows xp professional, που εγκαταστήσαμε στο εικονικό σύστημα μας.

### 5.2.3 ActivePerl

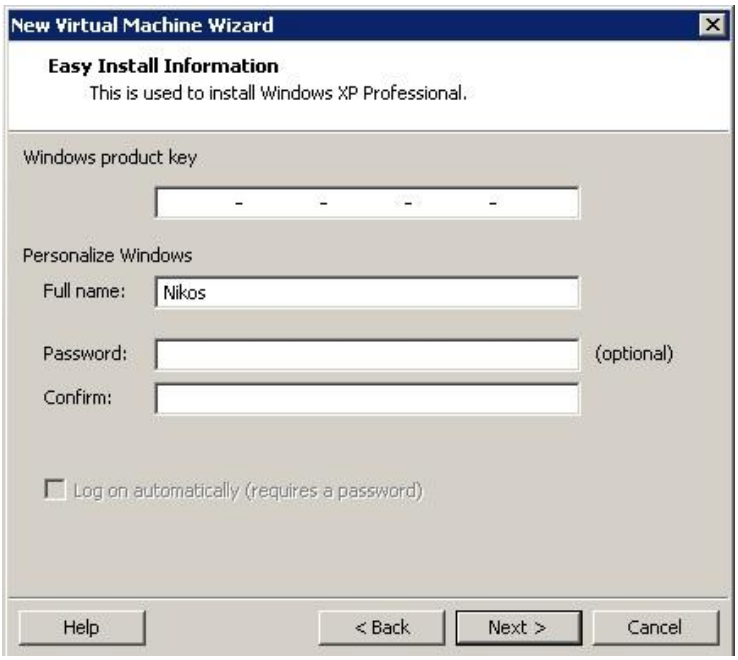
Είναι μια εφαρμογή ανοικτού κώδικα που κυκλοφορεί δωρεάν από την ActiveState και μας δίνει την δυνατότητα να εκτελέσουμε αρχεία PerlScript, αρχεία που έχουν δημιουργηθεί με την γλώσσα προγραμματισμού Perl, τα οποία είναι κομμάτια κώδικα με ποικίλες λειτουργίες ανάλογα με την συγγραφή τους.

### 5.2.4 Υλοποίηση Εικονικού Συστήματος «Honeypot»

Αρχικά εγκαταστήσαμε στο αρχικό σύστημα Windows που διαθέτουμε το πρόγραμμα για την εικονική λειτουργία συστημάτων VMware,

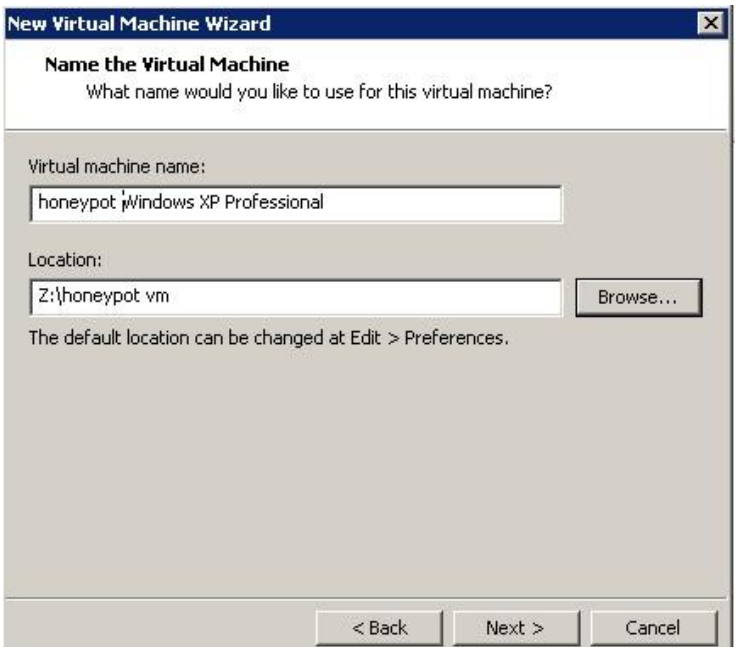
Στη συνέχεια ξεκινήσαμε την δημιουργία ενός νέου εικονικού συστήματος με λειτουργικό σύστημα Windows XP Professional.Τα χαρακτηρίστηκα που του δώσαμε ήταν μνήμη 768MB, επεξεργαστή με έναν πυρήνα, 30GB σκληρό δίσκο και κατάσταση γέφυρας στην κάρτα δικτύου(Bridged Mode). Οι υπόλοιπες συσκευές (οδηγός δίσκων, παράλληλες θύρες, κάρτα ήχου, και οθόνη) ρυθμίστηκαν από τις προεπιλεγμένες ρυθμίσεις του προγράμματος. Για όλη την διαδικασία ακολουθήθηκαν τα παρακάτω βήματα.

Βήμα 1: Εισαγωγή προφίλ χρήστη για το περιβάλλον των windows



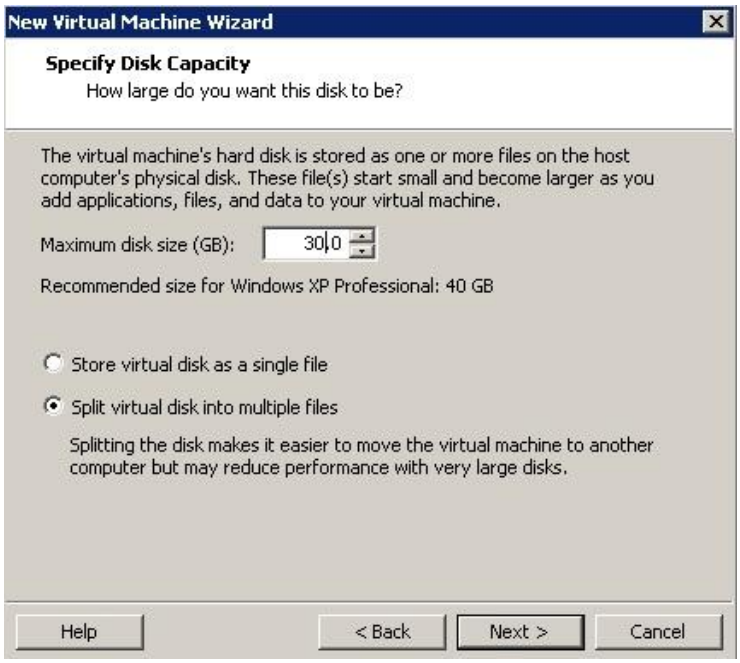

*ΣΧΗΜΑ 5.2*

Βήμα 2: Ονομασία εικονικού συστήματος και καθορισμός θέσης αποθήκευσης



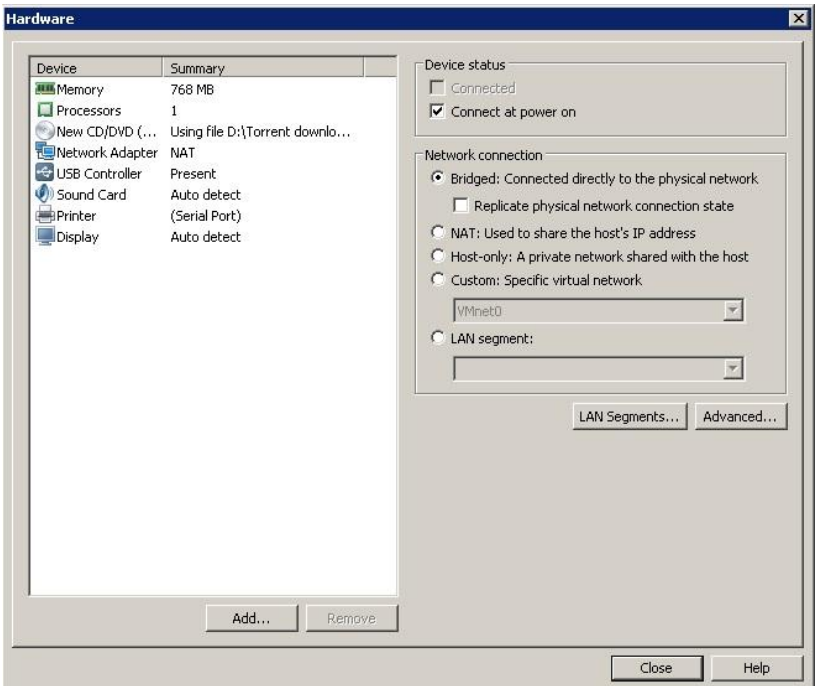

*ΣΧΗΜΑ 5.3*

Βήμα 3: Καθορισμός χωρητικότητας σκληρού δίσκου του συστήματος.



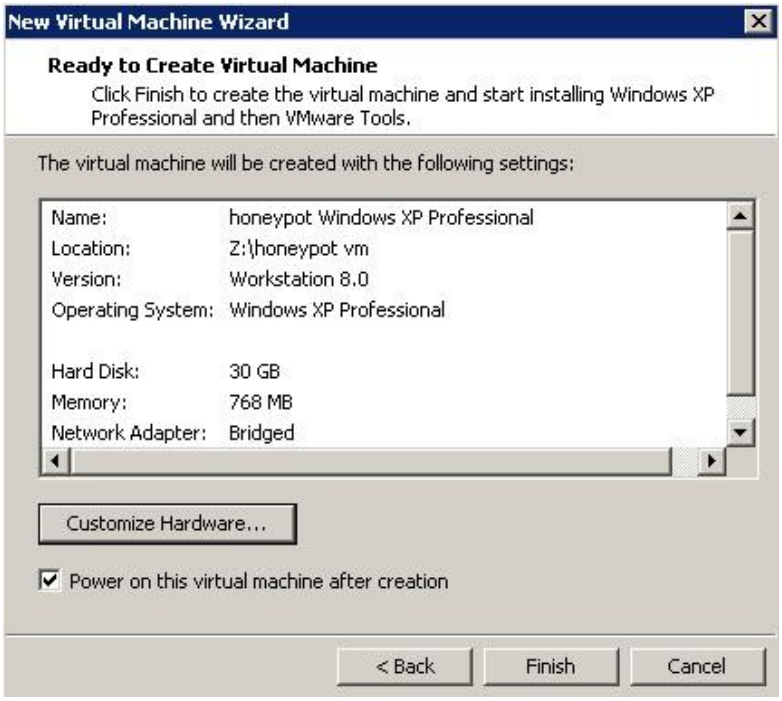

*ΣΧΗΜΑ 5.4*

Βήμα 4: Παραμετροποίηση υλικού και συσκευών του συστήματος.



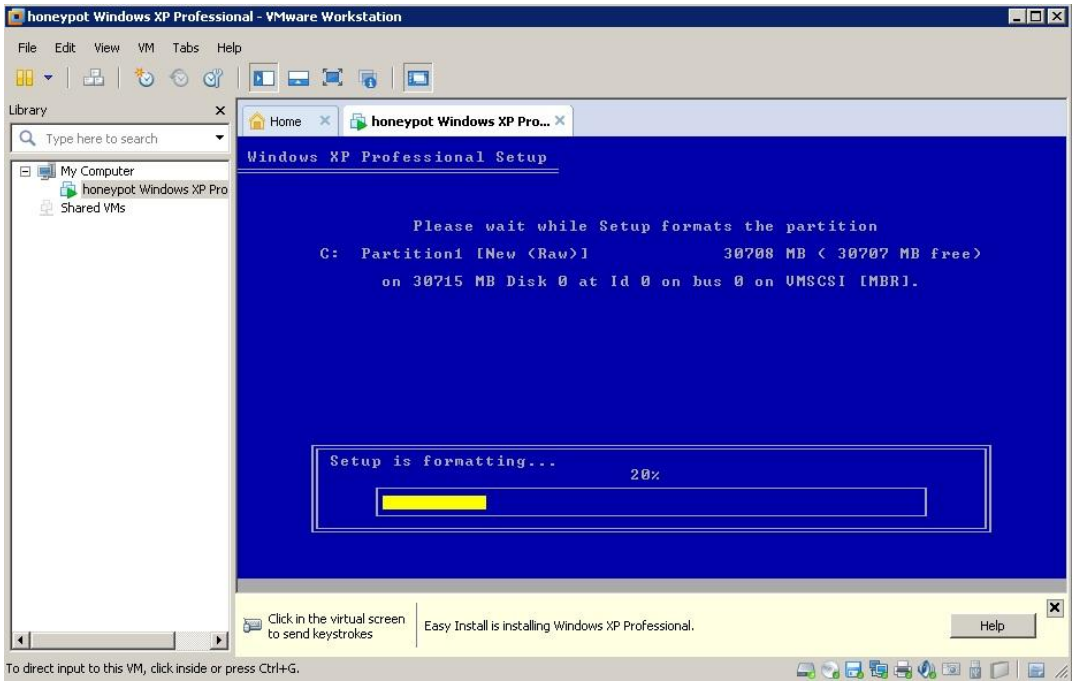

*ΣΧΗΜΑ 5.5*

Βήμα 5: Επισκόπηση ρυθμίσεων υλικού προ της δημιουργίας του συστήματος.



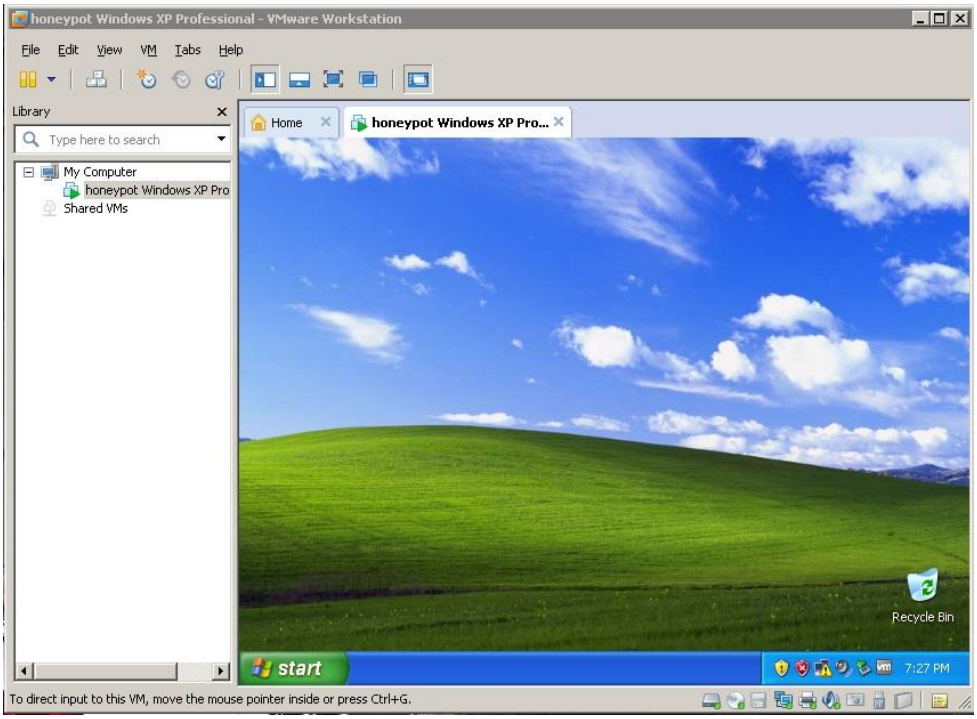

*ΣΧΗΜΑ 5.6*

Βήμα 6: Εγκατάσταση λειτουργικού συστήματος.



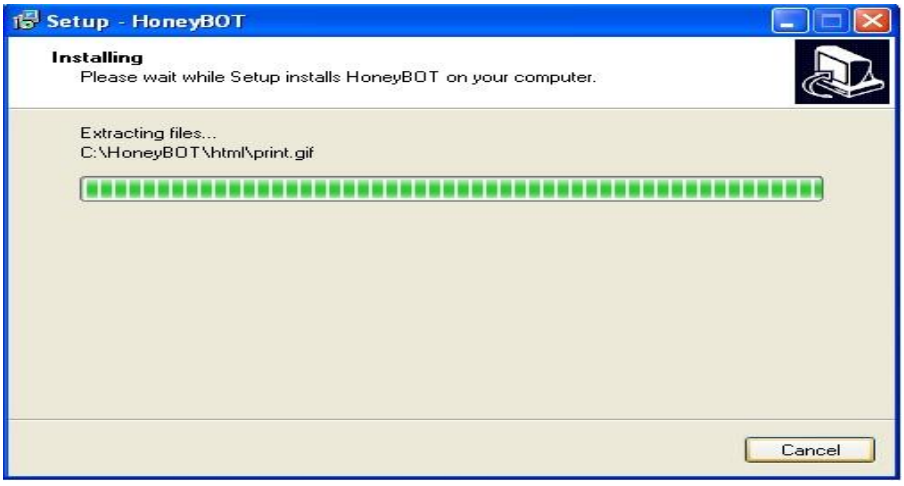

*ΣΧΗΜΑ 5.7*

Βήμα 7: Ολοκλήρωση της εγκατάστασης του εικονικού συστήματος για την εφαρμογή του «Honeypot».Το σύστημα είναι έτοιμο για την περαιτέρω εγκατάσταση των εργαλείων HoneyBot και Wireshark.



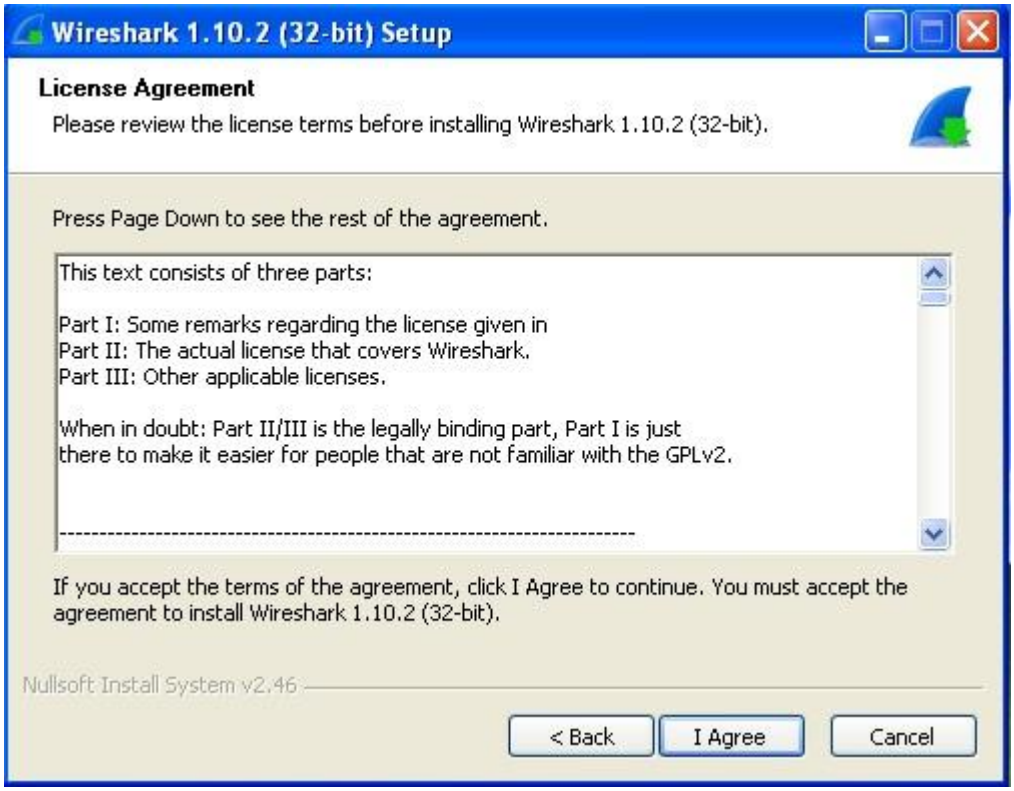

*ΣΧΗΜΑ 5.8*

Βήμα 8: Στο βήμα αυτό εγκαταστήσαμε το πρόγραμμα HoneyBOT στο εικονικό σύστημα Windows XP Professional που δημιουργήσαμε νωρίτερα. Όλες οι επιλογές της εγκατάστασης έγιναν με βάση τις προεπιλεγμένες ρυθμίσεις.




*ΣΧΗΜΑ 5.9*

Βήμα 9: Εγκατάσταση εργαλείου παρακολούθησης επικοινωνιών δικτύου Wireshark στο εικονικό σύστημα Windows XP Professional. Και στο πρόγραμμα αυτό χρησιμοποιήσαμε τις προεπιλεγμένες ρυθμίσεις για την εγκατάσταση του.




*ΣΧΗΜΑ 5.10: Εγκατάσταση εργαλείου παρακολούθησης επικοινωνιών δικτύου «Wireshark».*

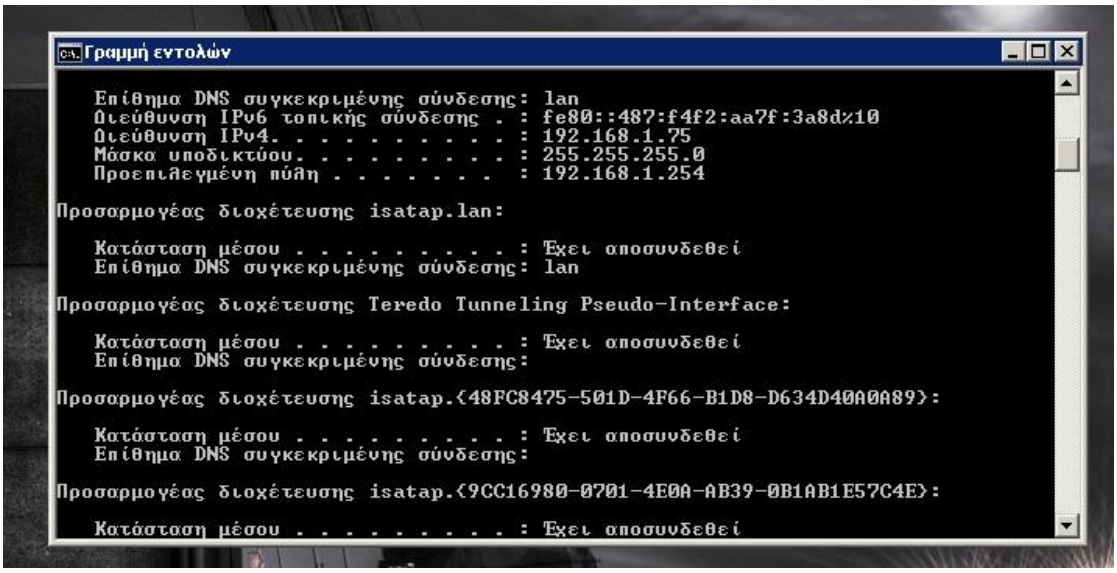
Αφού εγκαταστάθηκε και το εργαλείο Wireshark το εικονικό σύστημα είναι πλέον έτοιμο να δεχτεί και να καταγράψει την επίθεση μας.

### 5.3 Υλοποίηση DDOS Επίθεσης στο Εικονικό Σύστημα «Honeypot»

Βήμα 1: Στο φυσικό σύστημα Windows εγκαθιστούμε το πρόγραμμα Active Perl για να μπορέσουμε να εκτελέσουμε ύστερα το αρχείο με τον κώδικα της επίθεσης. Η έκδοση που διαλέξαμε ήταν η πιο αναβαθμισμένη για 64bit συστήματα. Για την εγκατάσταση επιλέγουμε τις προεπιλεγμένες ρυθμίσεις.

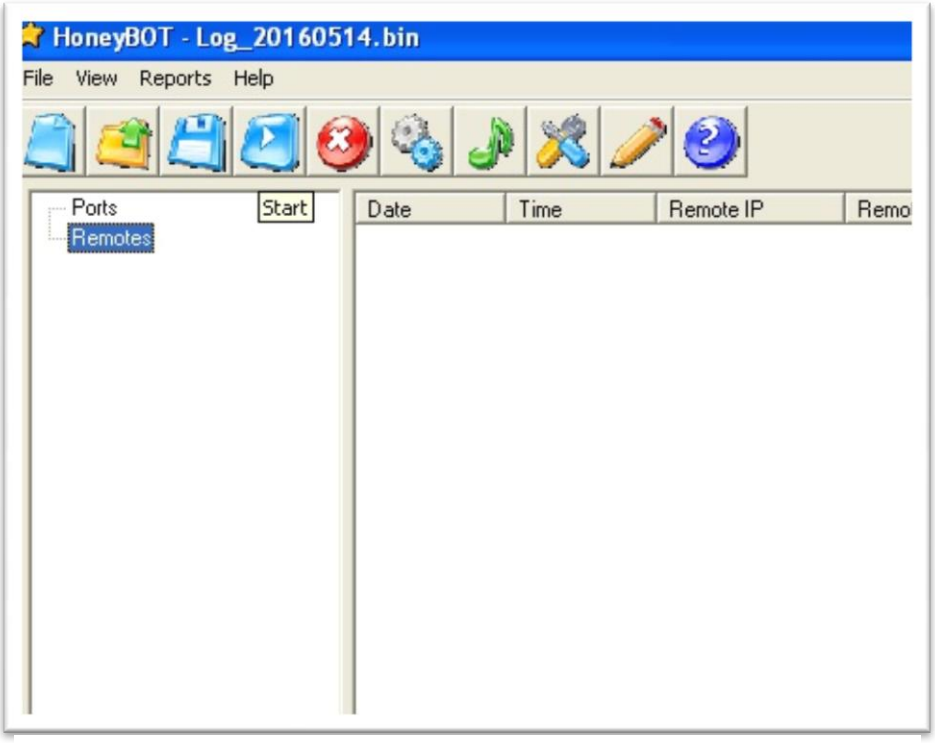

*ΣΧΗΜΑ 5.11: Εγκατάσταση προγράμματος «ActivePerl».*

Βήμα 2: Εκτελούμε από την Γραμμή εντολών των Windows την εντολή "ipconfig" για κάθε σύστημα ξεχωριστά, για να γνωρίζουμε τις IP διευθύνσεις και των δυο συστημάτων. Προκύπτουν η ***192.168.1.75*** για το φυσικό σύστημα και η ***192.168.1.82*** για το εικονικό σύστημα «Honeypot».



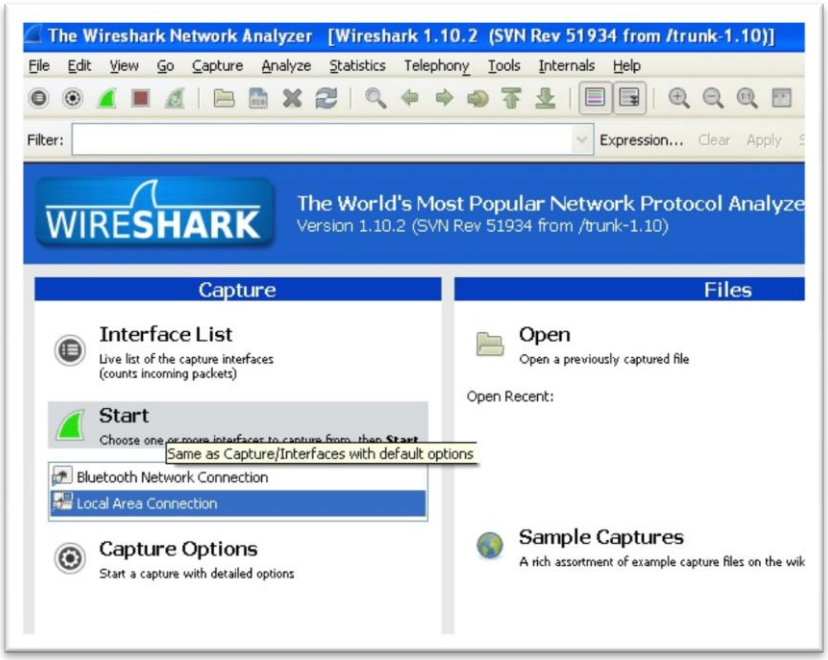

*ΣΧΗΜΑ 5.12: Αποτελέσμα εντολής "ipconfig".*

Βήμα 3: Από το εικονικό σύστημα εκκινούμε το πρόγραμμα «HoneyBOT» και επιλέγουμε την εντολή “start” για να το θέσουμε σε κατάσταση αναμονής επιθέσεων.



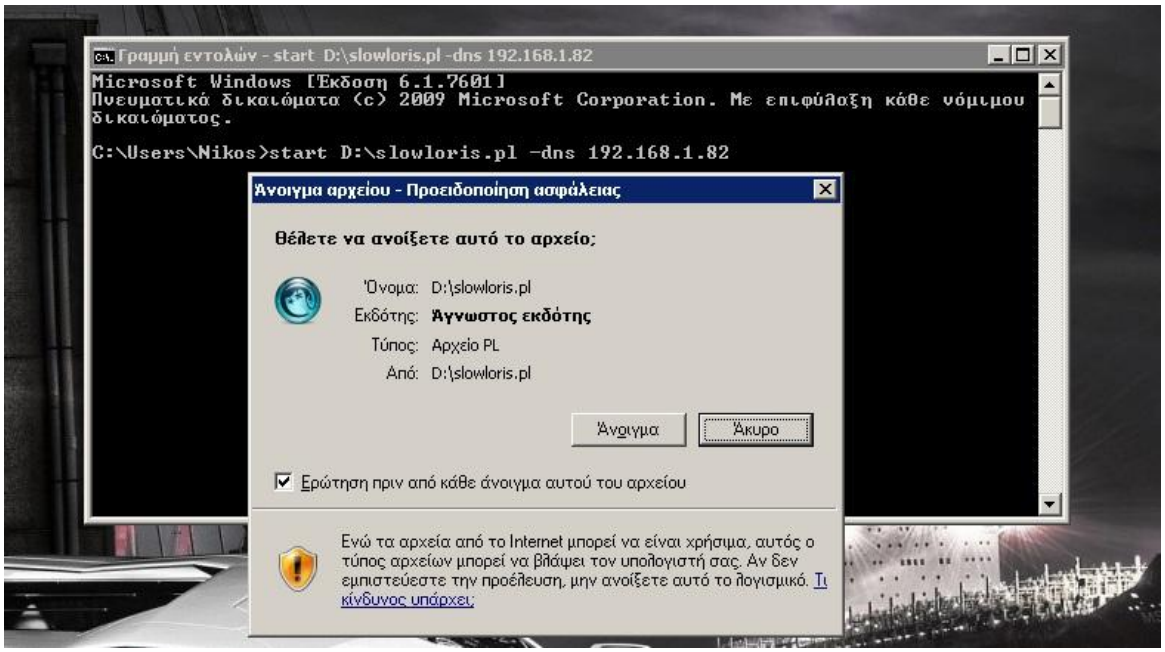

*ΣΧΗΜΑ 5.13: Εκκίνηση «HoneyBOT».*

Βήμα 4: Από το εικονικό σύστημα εκκινούμε την εφαρμογή «Wireshark», διαλέγουμε τον τύπο δικτύου που θέλουμε να ξεκινήσει να παρακολουθεί και επιλέγουμε την εντολή “start”.




*ΣΧΗΜΑ 5.14: Επιλογή σύνδεσής δίκτυου προς παρακολούθηση.*

Βήμα 5: Κάνουμε έναν τελευταίο έλεγχο στο εικονικό σύστημα για να εξακριβώσουμε πως όλα λειτουργούν όπως πρέπει, και κυρίως ελέγχουμε την λειτουργία του δικτύου για την σωστή λειτουργία της, διότι αν αντιμετωπίζει προβλήματα συνδεσιμότητας, η επίθεση μας δεν θα φτάσει ποτέ. Ενώ εκτελούνται στο εικονικό σύστημα τα προγράμματα «HoneyBOT» και «Wireshark», από το φυσικό σύστημα με την χρήση της Γραμμής εντολών των Windows πληκτρολογούμε την εντολή : ***start D:\slowloris.pl –dns 192.168.1.82*** ( D:\ είναι το σημείο όπου βρίσκεται το αρχείο αποθηκευμένο στο δίσκο, slowloris.pl είναι το όνομα του αρχείου και –dns 192.168.1.82 είναι η διεύθυνση προορισμού της επίθεσης) και πατάμε εκτέλεση. Η επίθεση πλέον είναι γεγονός.

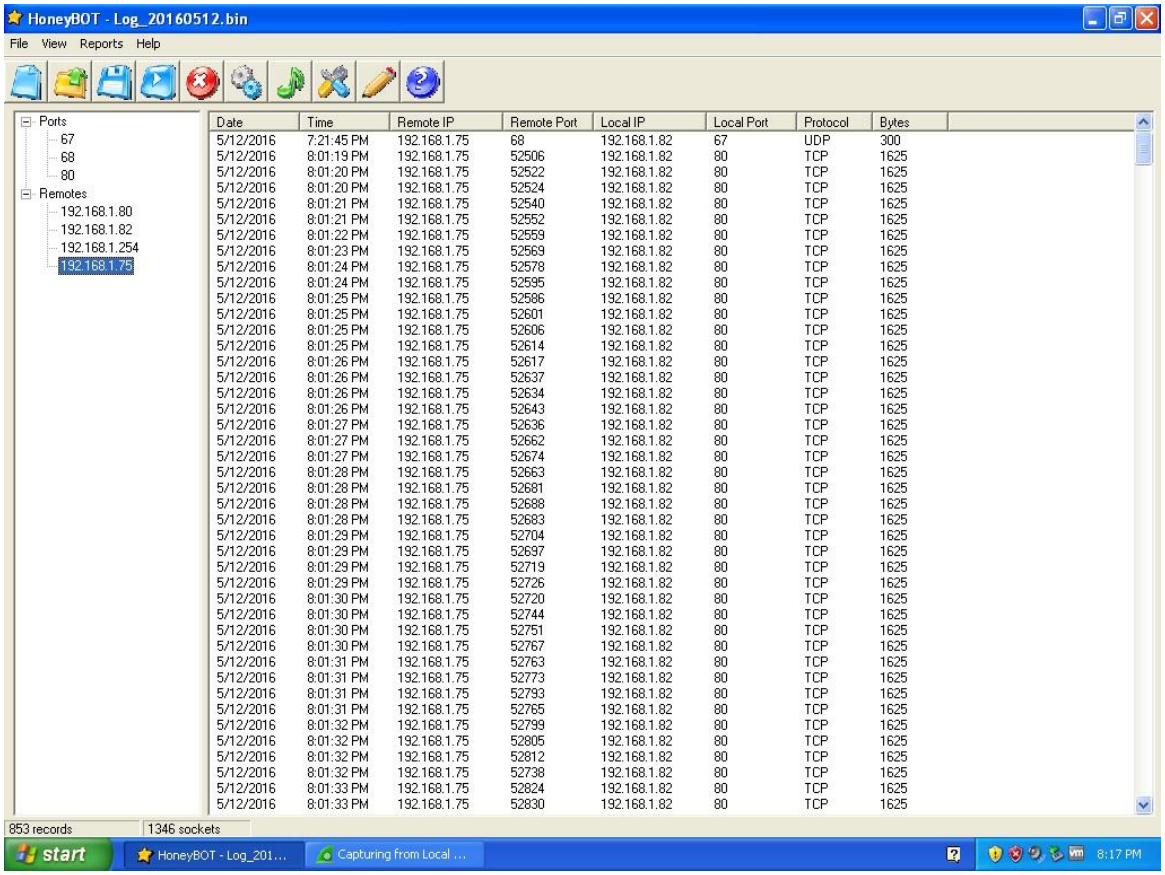



*ΣΧΗΜΑ 5.15: Εκτέλεση αρχείου «Slowloris».*

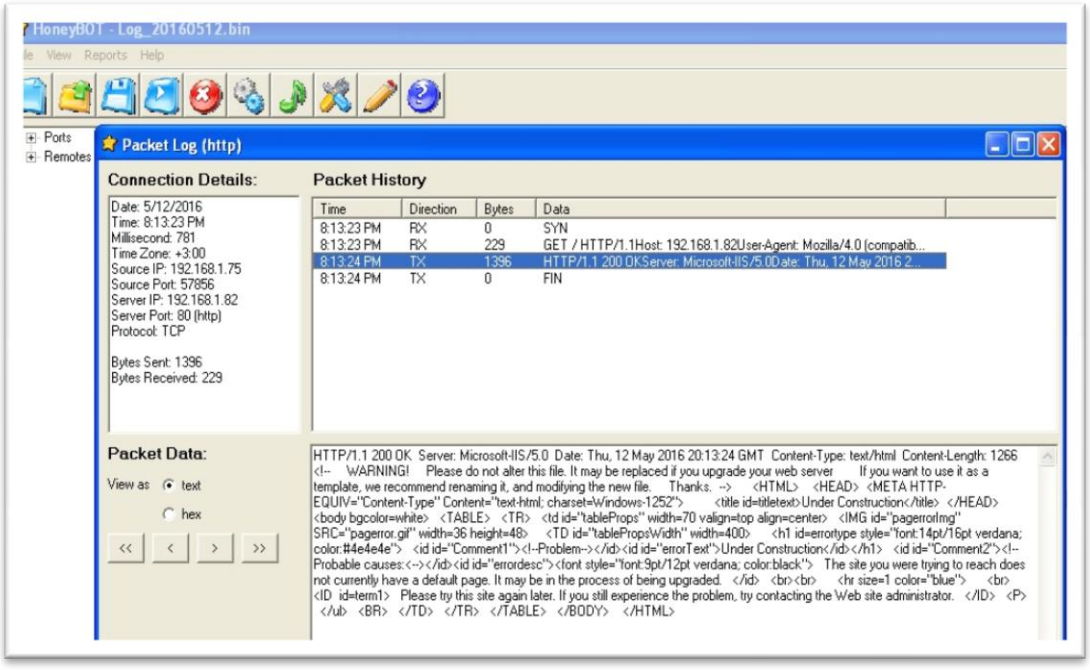
### 5.4 Καταγραφή της DDOS Επίθεσης από «HoneyBOT» και «Wireshark»

Αμέσως μετά την εκτέλεση της εντολής για DDOS επίθεση στο εικονικό σύστημα, αποστέλλονται κατά εκατοντάδες πακέτα με προορισμό το σύστημα στόχο, σε πρώτο χρόνο αυτή η αφύσικη δραστηριότητα του δικτύου γίνεται αντιληπτή από το «HoneyBOT» αλλά και φυσικά από το «Wireshark». Η επίθεση είχε χρονική διάρκεια 15 λεπτά και μέσα σε αυτή την ώρα στείλαμε πάνω από 20.000 πακέτα στο σύστημα στόχο. Επίσης η γραμμή εντολών των Windows στο φυσικό σύστημα πριν την έναρξη της επίθεσης καταλάμβανε μόλις 1Mb χώρο στη φυσική μνήμη, ενώ έφτασε τα 150Mb στη

μέγιστη τιμή της. Το «HoneyBOT» κατέγραψε 853 εγγραφές που “απάντησαν” σε 1346 υποδοχές του, οι οποίες είναι διαθέσιμες προς ανάλυση.

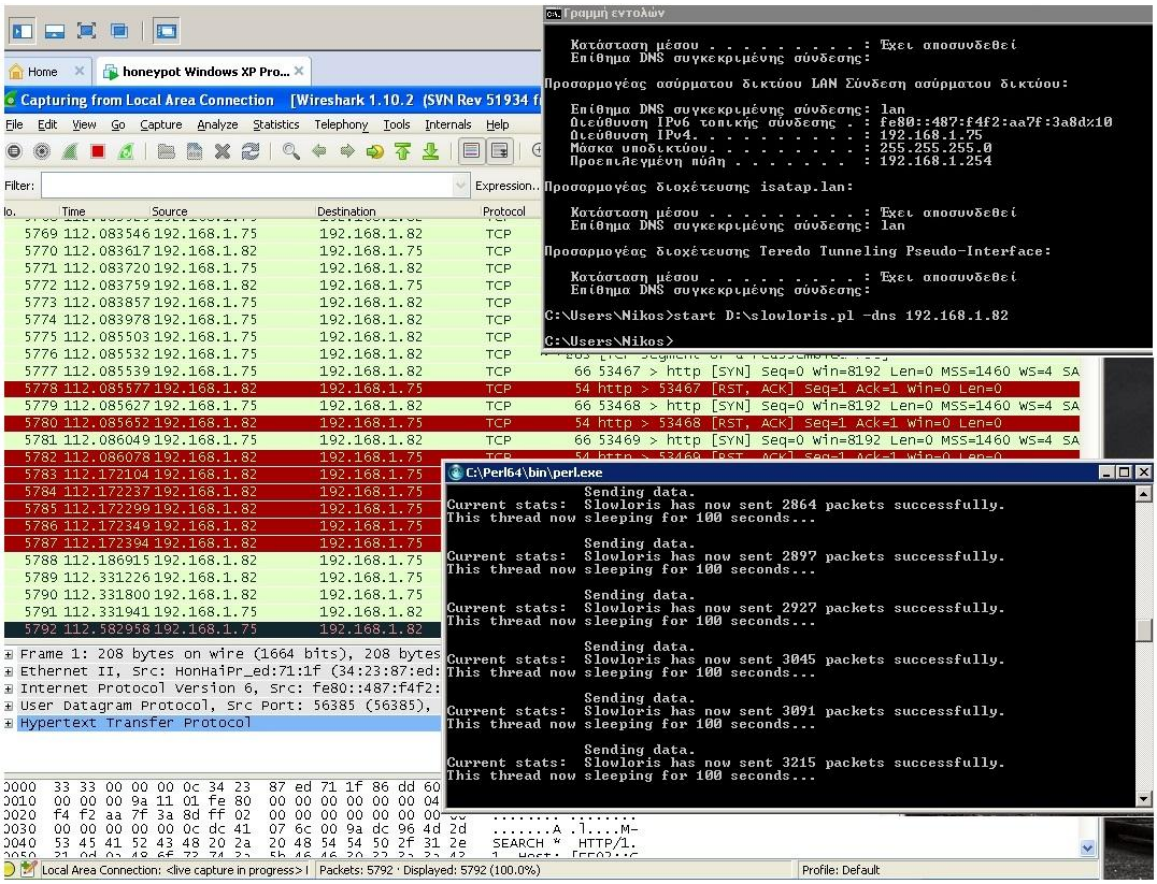



*ΣΧΗΜΑ 5.16: Σε 15 λεπτά επίθεσης βρέθηκαν πάνω από 1346 υποδοχές προς ανάλυση.*

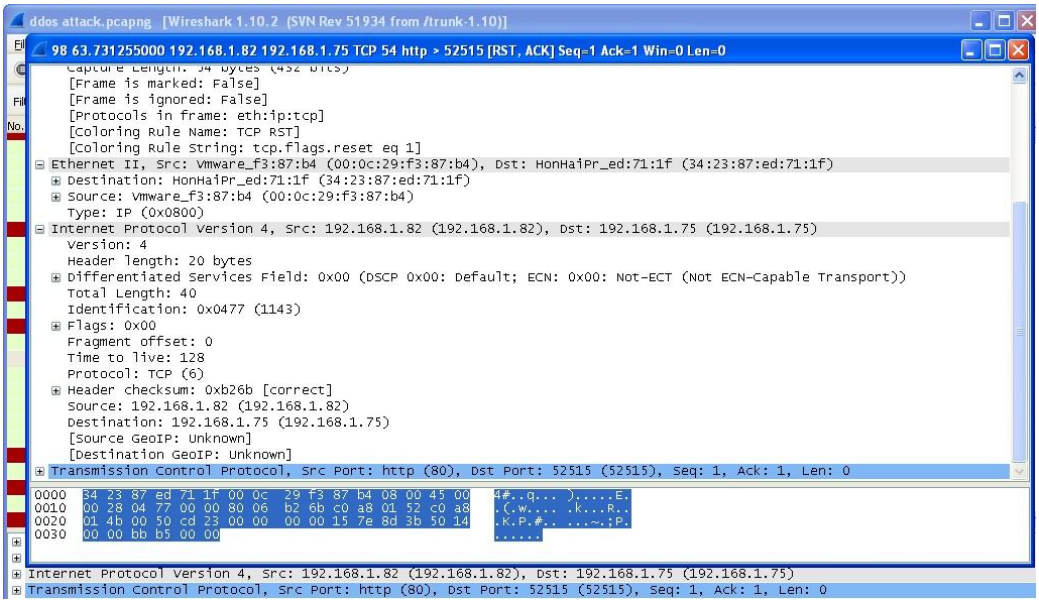



*ΣΧΗΜΑ 5.17: Στιγμιότυπο ανάλυσης πακέτου από το «HoneyBOT»*

Η επίθεση καταγράφεται και από το εργαλείο παρακολούθησης επικοινωνιών δικτύου, που μας δίνει την δυνατότητα να συλλέξουμε ενδιαφέρουσες πληροφορίες, αλλά και χρήσιμα στατιστικά στοιχεία που θα παρουσιάσουμε παρακάτω.




*ΣΧΗΜΑ 5.18: Ανάλυση επικοινωνίων δικτύου από το «Wireshark».*

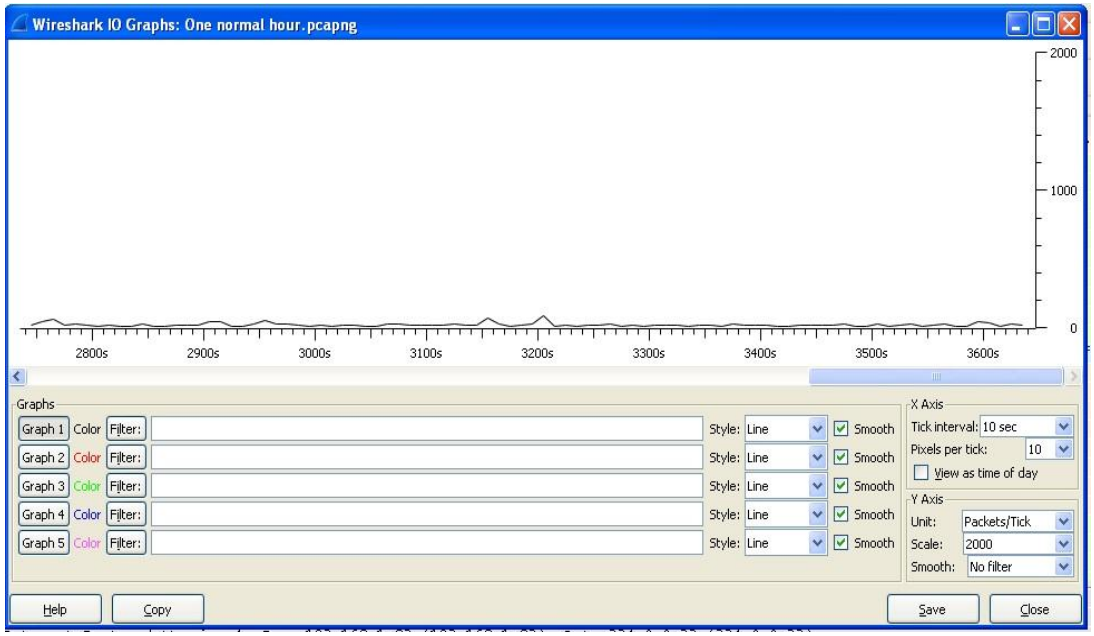



*ΣΧΗΜΑ 5.19: Ανάλυση «Wireshark» τυχαίας εγραφής από την επίθεση.*

### 5.4.1 Διαγραμματική Απεικόνιση Κίνησης Δεδομένων

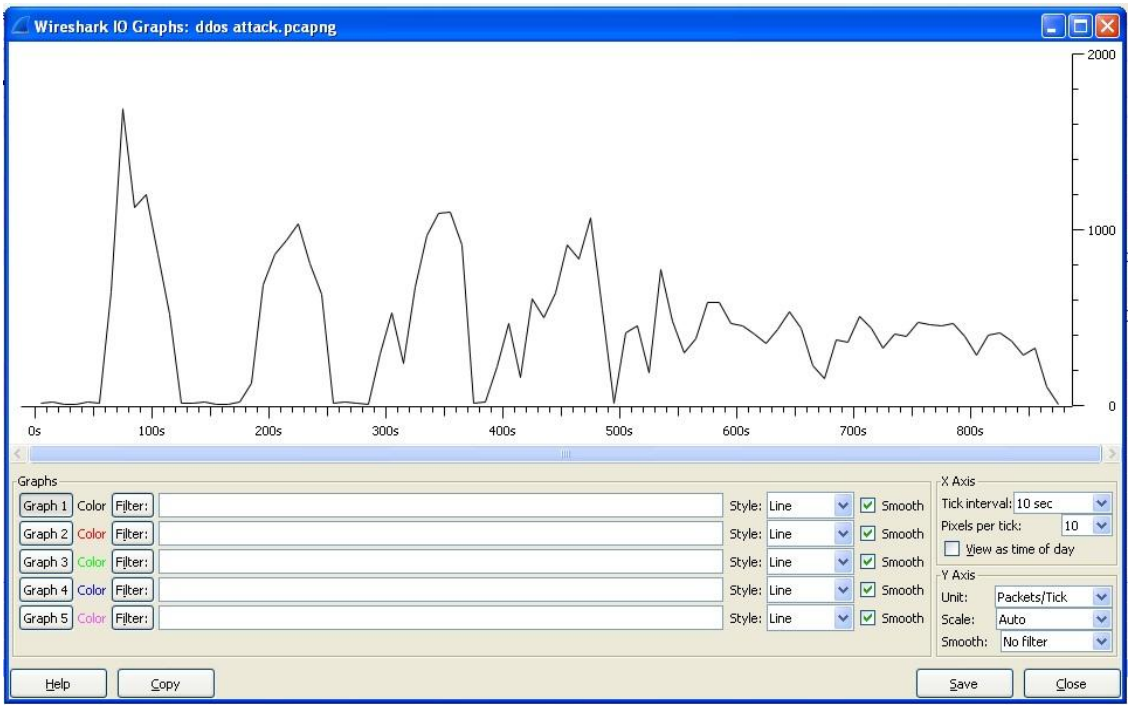
Με την βοήθεια των στατιστικών εργαλείων του προγράμματος «Wireshark» αποτυπώσαμε σε διαγράμματα την δικτυακή κίνηση των πακέτων που κατευθύνονται προς το εικονικό σύστημα «Honeypot» . Δειγματοληπτικά πήραμε τρις περιπτώσεις, η πρώτη ήταν μια τυχαία καταγραφή κίνησης δεδομένων χρονικής διάρκειας μίας ώρας, η δεύτερη ήταν η συνολική κίνηση που προέκυψε μετά από 15 λεπτά επίθεσης, και η τελευταία περίπτωση ήταν η αποτύπωση της κίνησης μετά την επίθεση σε χρονική διάρκεια  μισής ώρας.

1. Πακέτα ανά χρόνο σε διάρκεια μιας ώρας.



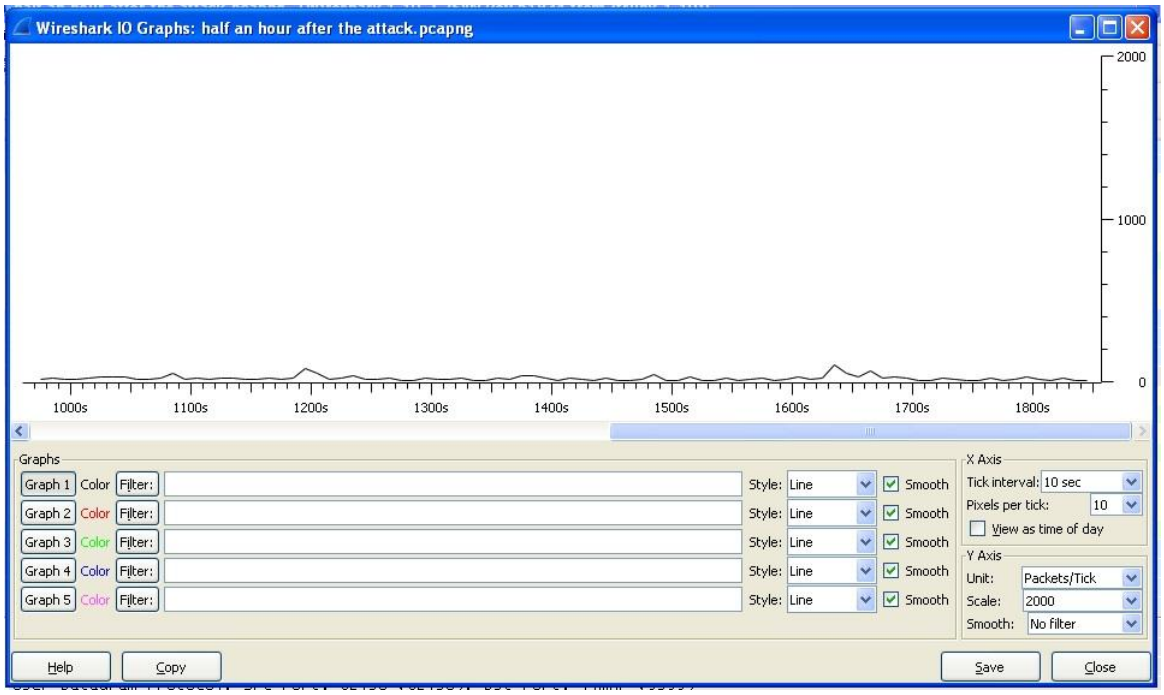

ΣΧΗΜΑ 5.20

2. Πακέτα ανά χρόνο σε 15 λεπτά DDOS επίθεσης.




ΣΧΗΜΑ 5.21

3. Πακέτα ανά χρόνο σε διάστημα μισής ώρας μετά την επίθεση




*ΣΧΗΜΑ 5.22*

Με βάση τα διαγράμματα, ακόμη και αν δεν γνωρίζαμε τον χαρακτήρα της επίθεσης DDOS και την συμπεριφορά της στο σύστημα στόχο, θα μπορούσαμε να διακρίνουμε πως, δημιουργεί μια αφύσικα έντονη επικοινωνία με το σύστημα θύμα αποστέλλοντας κατά εκατοντάδες πακέτα πληροφοριών ανά τακτά χρονικά διαστήματα. Απώτερος σκοπός είναι είτε να κολλήσει το σύστημα θύμα είτε να μην μπορεί να εξυπηρετήσει τους νομίμους χρήστες αν ο στόχος ήταν μια συγκεκριμένη υπηρεσία του συστήματος. Οι κίνδυνοι δεν σταματούν εδώ καθώς ανάλογα με της γνώσεις και τις τεχνικές του επιτιθέμενου, η επίθεση μπορεί να εξαπλωθεί και σε άλλα συστήματα αν υπάρχουν στο δίκτυο, και ο επιτιθέμενος να εκμεταλλευτεί αυτή την αστάθεια επικοινωνίας του δικτύου και να εισχωρήσει χωρίς να "καταλάβουν" πως πρόκειται για μη εξουσιοδοτημένο χρήστη στο εσωτερικό των συστημάτων με ότι αυτό συνεπάγεται.

# Κεφάλαιο 6 – Συμπεράσματα

Στην παρούσα εργασία γνωρίσαμε καλύτερα τους κινδύνους που υπάρχουν στα δίκτυα υπολογιστικών συστημάτων. Μάθαμε τρόπους και τεχνικές προστασίας των πληροφοριακών δεδομένων αλλά και των ίδιων των συστημάτων από απειλές και κακόβουλο λογισμικό. Χρησιμοποιήσαμε μια τεχνολογία, τα «Honeypots» που αν και είναι νέα ακόμη, έχει πολλές δυνατότητες και είναι πολλά υποσχόμενη για τον τομέα της ασφάλειας δικτύων και συστημάτων. Υλοποιήσαμε με την βοήθεια προγράμματος εικονοποίησης ένα εικονικό σύστημα «Honeypot» στο οποίο προσαρμόσαμε το πρόγραμμα «HoneyBOT». Εξαπολύσαμε από το φυσικό μας σύστημα επίθεση DDOS στο «Honeypot» και την καταγράψαμε τόσο μέσω του «HoneyBOT» όσο και με την βοήθεια του προγράμματος ανάλυσης επικοινωνιών δικτύου «Wireshark». Τα στοιχεία που καταγράψαμε ήταν αρκετά και λεπτομερή. Είδαμε πως η διαδικασία της επίθεσής αν και απλή στην εφαρμογή της, με μια εντολή από το πρόγραμμα Γραμμή εντολών των Windows, μέσα σε 15΄ λεπτά λειτουργίας είχε πολλαπλασιάσει τις απαιτήσεις για φυσική μνήμη συστήματος επί 150 φορές περίπου. Ένα γεγονός που μας δίνει τη δυνατότητα να κατανοήσουμε γιατί οι κακόβουλοι χρήστες έχουν ανάγκη να καταλάβουν υπό τον έλεγχο του ολόκληρα δίκτυα ηλεκτρονικών υπολογιστών, για να εξαπολύσουν μία DDOS επίθεση σε κάποια σελίδα μεγάλου οργανισμού και να την θέσουν εκτός λειτουργίας. Το «Honeypot» χωρίς να έχει αποτρεπτικό ρόλο στην εξέλιξη της επίθεσης απέδειξε πως είναι ένα εργαλείο το οποίο μπορεί να συνεισφέρει ουσιαστικά, στην έρευνα κατά των κακόβουλων ενεργειών και λογισμικού, σε καίριο τομέα της ασφάλειας όπως είναι αυτός των νέων απειλών αλλά και τεχνικών επιθέσεων. Με καθημερινή εξέλιξη και περισσότερες δυνατότητες αλλά και ποιο φιλικό περιβάλλον χρήσης τα «honeypots» χρησιμοποιούνται με ρυθμούς αριθμητικής προόδου. Είναι πλέον δεδομένο πως τα «Honeypots» θα συνδέσουν το όνομα τους με την έρευνα. Ολοένα και πιο πολλές εταιρίες που θα διαχειρίζονται ευαίσθητα δεδομένα θα έχουν «Honeypots» έρευνας να "παράγουν" γνώση για την εξέλιξη των συστημάτων ενεργητικής ασφάλειας για την προστασία των δικτύων αλλά και των υπολογιστικών συστημάτων.

# Κεφάλαιο 7 – Βιβλιογραφία


1. Κάτσικας, Σωκράτης και Γκρίτζαλης Δημήτρης και Γκρίτζαλης Στέφανος, 2004, Ασφάλεια πληροφοριακών συστημάτων, Αθήνα: Εκδόσεις Νέων Τεχνολογιών.
2. Κάτσικας, Σωκράτης, 2001, Ασφάλεια δικτύων, Πάτρα: Ελληνικό Ανοικτό Πανεπιστήμιο.
3. Δημόπουλος, Κωνσταντίνος και Παπουτσής Ιωάννης, 2005, Εισαγωγή στην πληροφορική & στον αυτοματισμό γραφείου, Αθήνα: Β. Γκιούρδας Εκδοτική.
4. Σπυράκης, Παύλος, "90 Ερωτήσεις – Απαντήσεις για το Διαδίκτυο", Το Βήμα, 1997.
5. Μαλλάς, Δημήτρης, "Με κινητό 2 στα 10 παιδιά του Δημοτικού", Ημερησία, 2014.
6. Lance, Spitzner, 2002, Honeypots: Tracking Hackers, Boston, MA: Addison-Wesley.
7. B. Cheswick, "An Evening with Berferd." 1991.
8. The Honeynet Project, "Know your Enemy" 2006. http://old.honeynet.org/
9. The Honeynet Project, "Know Your Enemy: Honeywall CDROM," 2005. http://old.honeynet.org/papers/cdrom/roo/index.html
10. The Real Time Statistics Project, "Internet Live Stats" 2015. http://www.internetlivestats.com/
11. Wikipedia, "ARPANET", https://el.wikipedia.org/wiki/ARPANET
12. Πανεπιστήμιο Μακεδονίας, "Computer Networks & Telematics Application Lab", 2016. http://conta.uom.gr/conta/ekpaideysh/seminaria/common/internet/history.htm
13. Internet Society, "Brief History of the Internet", 2016. http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet
14. Konstantope, Theodora, "Mosaic: 20 χρόνια από τη γέννηση του πρώτου αληθινού browser", 25/01/2013. http://www.techgear.gr/mosaic-web-browser-turns-20-62263/
15. Ινστιτούτο Εργασίας ΟΤΟΕ, Λεξικό, λήμμα "W", 2016. http://www.ine.otoe.gr/UplDocs/ekdoseis/leksiko/lexiko_W.pdf
16. Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, Τμήμα Δημοσιογραφίας & ΜΜΕ, OnlineLearning, 2016, http://pacific.jour.auth.gr/?page_id=152
17. Microsoft, "Choosing a network location", 2016, http://windows.microsoft.com/en-us/windows/choosing-network-location#1TC=windows-7
18. Bradley, Mitchell, "What is Ad-Hoc Mode in Wireless", adout tech, 16/12/2014, http://compnetworking.about.com/cs/wirelessfaqs/f/adhocwireless.htm
19. Margaret, Rouse, 7/2007, "Apple Talk", http://searchnetworking.techtarget.com/definition/AppleTalk
20. Margaret Rouse, 02/2007, "anti-spyware software", http://whatis.techtarget.com/definition/anti-spyware-software

21. Hafner Katie, Markoff John, 1991, “Cyberpunk: Outlaws and Hackers on the Computer Frontier, Revised”, USA, Simon & Schuster.
22. Levine John, R. LaBella, H. Owen, D. Contis, and B. Culver, 2003, “The use of honeynets to detect exploited systems across large enterprise networks”.
23. Johny Papo, 29/02/2012, “Enigma”, http://www.ww2.gr/index.php?option=articles&search=Enigma
24. Παγουρτζής Άρης, Ζάχος Στάθης, 2013, “Υπολογιστική Θεωρία Αριθμών και Κρυπτογραφία”, https://www.corelab.ntua.gr/courses/crypto/slides2013/crypto2013_pres1_classic.pdf
25. Λιμνιώτης Κώστας, 2016, “Κρυπτογραφία, Κεφάλαιο 2 Αλγόριθμοι ροής – Stream ciphers”, http://users.teilam.gr/~klimn/cryptography/Lec2.pdf
26. Χρυσίδης Αναστάσιος, 2013, “Κρυπτογραφία & Κρυπτανάλυση”, http://lyk-didym.evr.sch.gr/newschsite/files/Projects/CryprografiaB.pdf
27. K&G Digital Service, 2016, “Τι είναι το Intrusion Prevention?”, http://digiservice.gr/news/what-is--intrusion-prevention.html
28. McDowell Mindi, 04/11/2009,06/02/2013, “Understanding Denial-of-Service Attacks”, US-CERT, https://www.us-cert.gov/ncas/tips/ST04-015
29. Επιτήδειος Γιώργος, 2000, “Είδη επιθέσεων DoS (Denial of Service)”, http://www.eeei.gr/interbiz/articles/dos.htm
30. Owasp, 08/31/2015, “Man-in-the-middle attack”, https://www.owasp.org/index.php/Man-in-the-middle_attack
31. All.net, 1999, “Deception Toolkit”, http://www.all.net/dtk/