ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ: ΜΟΡΦΕΣ, ΤΕΧΝΟΛΟΓΙΕΣ, ΑΝΤΙΜΕΤΡΑ ΚΑΙ ΣΥΝΕΠΕΙΕΣ

ΚΑΡΑΤΣΗ ΑΝΑΣΤΑΣΙΑ ΑΜ 2830
ΝΙΚΟΛΑΟΥ ΑΝΤΩΝΙΟΣ ΑΜ: 2731

ΕΠΙΒΛΕΠΩΝ: ΠΑΡΑΣΚΕΥΑΣ ΜΙΧΑΗΛ

ΠΑΤΡΑ 2022

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Οι ηλεκτρονικοί υπολογιστές και η ανάπτυξη του διαδικτύου είναι από τα σημαντικότερα τεχνολογικά επιτεύγματα. Ο παγκόσμιος ιστός παρέχει άπειρες δυνατότητες στην ανθρώπινη καθημερινότητα. Ωστόσο, μέσω των πληροφοριακών δεδομένων που ανταλλάσσονται, εκθέτονται συχνά προσωπικά στοιχεία ή δεδομένα που οδηγούν στον εντοπισμό αυτών. Ορισμένοι γνώστες της τεχνολογίας γνωρίζοντας αυτή την κατάσταση, το εκμεταλλεύονται διαπράτοντας απάτες και παράνομες ενέργειες. Στην παρούσα εργασία γίνεται μία προσπάθεια παρουσίασης του ηλεκτρονικού εγκλήματος, του νομικού πλαισίου που το διέπει και των αντίμετρων. Στο ερευνητικό μέρος θα πραγματοποιηθεί μία MITM επίθεση.

Λέξεις - Κλειδιά: ηλεκτρονικό έγκλημα, διαδικτυακή απάτη, υπολογιστής, επίθεση.

ABSTRACT

Computers and the development of the internet are among the most important technological achievements. The World Wide Web offers endless possibilities in human daily life. However, through the information exchanged, personal data or data that lead to their identification are often exposed. Some techies, aware of this situation, exploit it by committing scams and illegal activities. In the present work, an attempt is made to present cybercrime, the legal framework that governs it and the countermeasures. A MITM attack will take place in the research part.

Keywords: cybercrime, cyber fraud, computer, attack.

ΕΙΣΑΓΩΓΗ

Ένα από τα σημαντικότερα τεχνολογικά επιτεύγματα είναι το διαδίκτυο και οι ηλεκτρονικοί υπολογιστές. Όλοι οι τομείς της ανθρώπινης καθημερινότητας έχουν αλλάξει μετά την εμφάνιση του παγκόσμιου ιστού. Στην εποχή μας συντελείται η λεγόμενη ψηφιακή επανάσταση εξαιτίας του συγκερασμού της τηλεπικοινωνίας, των οπτικοακουστικών μέσων και της πληροφορικής. Οι ηλεκτρονικές επικοινωνίες έχουν εισβάλλει στην καθημερινή ζωή των ανθρώπων.

Μια πληθώρα ενεργειών μπορούν να πραγματοποιηθούν από απόσταση, όπως συναλλαγές με ιδιωτικούς και δημόσιους φορείς, ηλεκτρονικές αγορές και πολλά άλλα, τα οποία εξοικονομούν στον άνθρωπο χρήματα και χρόνο. Κατά τη διάρκεια αυτών, το άτομο εκθέτει προσωπικά του στοιχεία ή δεδομένα τα οποία μπορούν να οδηγήσουν σε προσωπικές πληροφορίες.

Η Κοινωνία της Πληροφορίας και η είσοδος στο διαδίκτυο εκτός από τα πλεονεκτήματα που παρέχουν στον άνθρωπο και στο κράτος, καλλιεργούν το κατάλληλο πλαίσιο για να αναπτυχθούν νέες μορφές εγκλήματος.

Κάποια από αυτά είναι πολύ σοβαρά, κάποια λιγότερο. Η Ευρώπη και η Ελλάδα, όπως συμβαίνει με τις περισσότερες χώρες διεθνώς, έχουν θεσπίσει ένα νομοθετικό πλαίσιο για την προστασία των χρηστών των ηλεκτρονικών μέσων μέσα από το διαδίκτυο.

Στόχος της παρούσας εργασίας είναι να παρουσιάσει τις βασικές πτυχές του ηλεκτρονικού εγκλήματος και εν συνεχεία να παρουσιάσει μία διαδικτυακή επίθεση.

Αρχικά, στο πρώτο κεφάλαιο παρουσιάζεται το ηλεκτρονικό έγκλημα. Δίνεται ο ορισμός του, τα χαρακτηριστικά, η ιστορική του πορεία και οι διακρίσεις στις οποίες υπόκειται.

Στο δεύτερο κεφάλαιο καταγράφονται οι μορφές του ηλεκτρονικού εγκλήματος. Ειδικότερα, οι γνήσιες μορφές και τα ηλεκτρονικά εγκλήματα μέσω ηλεκτρονικών υπολογιστών.

Το τρίτο κεφάλαιο αναφέρεται στη χρησιμοποίηση της τεχνολογίας στο πεδίο της ανίχνευσης ηλεκτρονικών εγκλημάτων. Συγκεκριμένα, στα συστήματα που μπορούν να χρησιμοποιηθούν για την ανίχνευση και τον έλεγχο. Επίσης, παρουσιάζεται το ευρωπαϊκό και το ελληνικό νομικό πλαίσιο.

Η βιβλιογραφική ανασκόπηση ολοκληρώνεται με το τέταρτο κεφάλαιο, στο οποίο καταγράφονται κάποια από τα αντιμετρα του ηλεκτρονικού εγκλήματος, όπως η ταυτοπροσωπία, το λογισμικό και οι πολιτικές ασφαλείας.

Ακολουθεί το πρακτικό μέρος, στο οποίο παρουσιάζεται κατόπιν εφαρμογής μία επίθεση. Ειδικότερα, μία Man In The Middle (MITM) Attack. Στο συγκεκριμένο είδος ένας επιτιθέμενος/Hacker παρεμβάλλεται στην μετάδοση των πακέτων μεταξύ δύο μερών.

ΚΕΦΑΛΑΙΟ 1^{Ο} ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

1.1 ΕΝΝΟΙΟΛΟΓΙΚΗ ΠΡΟΣΕΓΓΙΣΗ

Τα τελευταία χρόνια, η τεχνολογία έκανε τεράστια βήματα προόδου και έγινε προσιτή στον καθένα. Αυτό είχε ως αποτέλεσμα να σημειωθούν πολύ σημαντικές αλλαγές σε όλους σχεδόν τους τομείς της ζωής του ανθρώπου. Η εργασία, η εκπαίδευση, η διασκέδαση, ακόμα και ο τρόπος που αντιλαμβανόμαστε τα πράγματα είναι πια διαφορετικός, λόγω των νέων δυνατοτήτων που αποκτήσαμε. Εκτός όμως από τις ευεργετικές για τη ζωή μας αλλαγές, η τεχνολογία έδωσε τα μέσα και το έδαφος για αναπτυχθούν και νέες μορφές εγκλήματος, που γενικά ορίζονται ως «Ηλεκτρονικό Έγκλημα».

Η χρήση των ηλεκτρονικών υπολογιστών για παράνομη δράση παρουσιάστηκε από την αρχή σχεδόν της ανάπτυξής τους και ήδη από τη δεκαετία του 1970 οδήγησε πολλά κράτη να λάβουν μέτρα και να νομοθετήσουν σχετικά με αυτή. Αργότερα όμως, με τη δημιουργία του internet, παρατηρήθηκαν και φαινόμενα εκμετάλλευσής του που δεν μπορούν να χαρακτηριστούν ως παράνομες πράξεις μέσω υπολογιστή. Γι αυτό, πρέπει να διαχωρίζονται οι πράξεις ηλεκτρονικού εγκλήματος από αυτές του λεγόμενου διαδικτυακού (cyber crime).

Είναι φανερό λοιπόν ότι οι παράνομες συμπεριφορές που έχουν σχέση με το διαδίκτυο έχουν τόσες πολλές μορφές και επιδιώξεις, ώστε είναι δύσκολο να υπάρξει ένας συνολικός ορισμός που να τις περιλαμβάνει όλες. Υπάρχει και η άποψη ότι το «ιντερνετικό» έγκλημα είναι σαν το κοινό ηλεκτρονικό έγκλημα και η μόνη διαφορά είναι το περιβάλλον στο οποίο διαπράττεται, αλλά μάλλον δεν ισχύει, γιατί ενώ υπάρχουν παράνομες πράξεις που μπορούν να τελεστούν και στα δύο περιβάλλοντα, κάποιες άλλες αφορούν αποκλειστικά τον κόσμο του διαδικτύου.

Επομένως, το πρώτο βήμα για να οριστούν οι έννοιες του διαδικτυακού και του ηλεκτρονικού εγκλήματος, είναι ο διαχωρισμός αυτών των δύο εννοιών, θεωρώντας το διαδικτυακό έγκλημα ως μια πιο συγκεκριμένη μορφή του ηλεκτρονικού. Η προσπάθεια για έναν κοινό ορισμό θα οδηγούσε

σε μια πολύ γενική και αόριστη έννοια που θα έπρεπε να περιλαμβάνει όλους τους τύπους εγκληματικότητας μέσω του internet. Έτσι, σε μια προσπάθεια να περιγραφούν με πιο ακριβή τρόπο αυτές οι έννοιες, θα μπορούσαμε να πούμε ότι ηλεκτρονικό έγκλημα είναι οι αξιόποινες πράξεις (παράνομες, ανήθικες και χωρίς δικαίωμα συμπεριφορές κ.τ.λ.) που μπορούν να τελεστούν χρησιμοποιώντας τις γενικότερες δυνατότητες ενός υπολογιστή, ενώ διαδικτυακό έγκλημα αυτές που μπορούν να γίνουν χρησιμοποιώντας αποκλειστικά το διαδίκτυο (Αγγελής, 2000).

Βέβαια, αυτές οι διατυπώσεις σε καμία περίπτωση δεν μπορούν να θεωρηθούν ορισμοί, γιατί δεν οριοθετούν με ακρίβεια τις ποινικά κολάσιμες συμπεριφορές, όπως απαιτεί η ποινική δικαιοσύνη. Είναι πράξεις χωρίς συγκεκριμένες και αντικειμενικά μετρήσιμες επιπτώσεις και γι αυτό το λόγο αόριστες. Οπότε οι έννοιες αυτές λειτουργούν κυρίως ως κατευθύνσεις και εναπόκειται στο νομοθετικό και δικαστικό σώμα κάθε χώρας η περαιτέρω διασαφήνιση και λεπτομερειακή περιγραφή για το τι ακριβώς συνιστά παρανομία και το πώς τιμωρείται (Μυλωνόπουλος, 2000).

1.2 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Το φαινόμενο του ηλεκτρονικού εγκλήματος εμφανίστηκε στη δεκαετία του 1970 και γρήγορα προβλημάτισε τους νομοθέτες, γιατί οι υφιστάμενοι νόμοι δεν μπορούσαν να αντιμετωπίσουν τη μορφή του νέου αυτού τρόπου παραβατικής συμπεριφοράς και τα χαρακτηριστικά της. Γι’ αυτό το λόγο τα αρμόδια όργανα κάθε χώρας φρόντισαν να επιφέρουν τις αλλαγές που έπρεπε, ώστε να προσαρμοστούν στα νέα δεδομένα.

Με την εξέλιξη όμως της τεχνολογίας και τη σύνδεση των υπολογιστών παγκοσμίως, προέκυψαν πολύπλοκα νομικά θέματα και έγινε ακόμα πιο απαραίτητη η ανάγκη αντιμετώπισης του εγκλήματος αυτού του τύπου, που έπαιρνε συνεχώς νέες μορφές. Οπότε οι νέες νομοθετικές παρεμβάσεις είχαν ως γνώμονα να αναλύσουν τα χαρακτηριστικά του και να καταδείξουν τις συνέπειες και το πόσο επικίνδυνο μπορεί να γίνει (Αγγελής, 2000).

Ένα από τα βασικά γνωρίσματα του εγκλήματος μέσω του διαδικτύου, που τα διαφοροποιεί από το κοινό έγκλημα, είναι η απόσταση μεταξύ του θύτη και του θύματος, η έλλειψη άμεσης επαφής. Δεν πρόκειται για έλλειψη βίας, αλλά για βία διαφορετικού τύπου. Για παράδειγμα, ο δράστης ενός ηλεκτρονικού εγκλήματος δεν κάνει διάρρηξη στο σπίτι του θύματος, προκειμένου να κλέψει τα ηλεκτρονικά αρχεία του, αλλά το κάνει από απόσταση, εισβάλλοντας στον υπολογιστή του θύματος, σπάζοντας τους κωδικούς πρόσβασης στο ηλεκτρονικό του σύστημα. Ούτε καταστρέφει τον υπολογιστή του θύματος παίρνοντας τον σκληρό δίσκο του, αλλά μέσω ενός κακόβουλου λογισμικού, που το ίδιο το θύμα ενεργοποιεί άθελά του (Κιούπης, 2000).

Η έλλειψη σωματικής βίας σε τέτοιου είδους πράξεις, θα μπορούσε να οδηγήσει κάποιον στη σκέψη ότι πρόκειται για ήπια εγκληματικότητα, όμως αυτό δεν ισχύει. Τα θύματα συνήθως δεν έχουν καμία δυνατότητα να αντιμετωπίσουν τις εισβολές αυτές, πολύ συχνά μάλιστα δεν αντιλαμβάνονται καν τις επιθέσεις κι όταν ακόμα το κάνουν, είναι πολύ δύσκολο να εντοπιστούν οι δράστες. Πρόκειται για εγκλήματα με πολύ μεγάλο βαθμό ατιμωρησίας.

Επίσης, πρόκειται για διεθνή εγκλήματα, που μπορούν να συμβούν από κάθε γωνιά του πλανήτη, χάρη στο internet. Η σύνδεσή των υπολογιστών έχει ξεπεράσει στην ουσία τα εθνικά σύνορα. Οι δράστες έχουν τους τρόπους να αλλάζουν τον τόπο απ' τον οποίο τελείται το έγκλημα ή να εκμεταλλεύονται την πολυπλοκότητα του δικτύου ώστε να είναι πολύ δύσκολο να εντοπιστεί ο τόπος και οι ίδιοι. Και υπό την έννοια αυτή η εγκληματικότητα αυτού του τύπου συνιστά κίνδυνο για τη διεθνή κοινότητα γενικά.

Βασική διαφοροποίηση μεταξύ του διαδικτυακού και του ηλεκτρονικού εγκλήματος, είναι η ταυτότητα των θυμάτων, που, ενώ στο ηλεκτρονικό έγκλημα είναι συγκεκριμένη, στο διαδικτυακό είναι συνήθως τυχαία και τα θύματα είναι άγνωστα και δεν έχουν στοχοποιηθεί από πριν. Αυτή είναι και μία βασική αιτία που τα περισσότερα διαδικτυακά εγκλήματα δεν καταγγέλλονται.

Αυτό, σε συνδυασμό με τη δυσκολία εντοπισμού του τόπου απ' τον οποίο τελέστηκε η παράνομη πράξη, ειδικά αν πρόκειται για χώρα διαφορετική απ' τη χώρα του θύματος, κάνει πολύ δύσκολη και την έρευνα για το έγκλημα και τη διαλεύκανση των υποθέσεων αυτών (Αγγελής, 2000).

Μεγάλη δυσκολία επίσης υπάρχει στην προσπάθεια ταυτοποίησης του τύπου του δράστη τέτοιων εγκλημάτων, του «προφίλ» του. Πολύ λίγες περιπτώσεις φτάνουν στη δικαιοσύνη, κάτι που έχει ως συνέπεια να υπάρχουν ελλιπή στοιχεία για τη σχετική έρευνα. Τα εγκλήματα είναι, όπως προαναφέρθηκε, πολύ περισσότερα σε σχέση με αυτά που καταγγέλλονται. Η εύκολη χρήση του internet έχει δώσει τη δυνατότητα στον καθένα να το χρησιμοποιήσει με τέτοιο τρόπο. Και η παγκόσμια γνώση πάνω στη χρήση του συνεχώς διευρύνεται.

Όλα αυτά σημαίνουν ότι οι δράστες των διαδικτυακών εγκλημάτων δεν περιορίζονται σε έναν μικρό αριθμό ειδικών πάνω στο αντικείμενο, που έχουν συγκεκριμένες γνώσεις και ανεπτυγμένο πνευματικό επίπεδο. Θύτης μπορεί να είναι οποιοσδήποτε κατέχει έναν υπολογιστή και μια σύνδεση τηλεφώνου με πρόσβαση στο διαδίκτυο. Κι αυτό αποδεικνύεται αν δούμε στοιχεία σχετικά με το αδίκημα της δυσφήμισης, που είναι απ' τα πιο διαδεδομένα, αφού δε χρειάζεται ούτε πολύς χρόνος ούτε ειδικές γνώσεις για να τελεστεί, είναι εξαιρετικά απλό και παρόλα αυτά δε μπορεί να αντιμετωπιστεί εύκολα από τα συστήματα ασφαλείας (Αγγελής, 2000).

1.3 ΙΣΤΟΡΙΚΗ ΑΝΑΣΚΟΠΗΣΗ

Για τη μελέτη της εξέλιξης του ηλεκτρονικού εγκλήματος, από την εμφάνισή του έως και σήμερα, θα ήταν χρήσιμη μια ιστορική αναδρομή, με στόχο να μας διαφωτίσει για την πορεία, τις διαφορετικές μορφές που απέκτησε όσο αναπτυσσόταν, τις νομοθετικές παρεμβάσεις με τις οποίες έγινε προσπάθεια να αντιμετωπιστεί, την τεχνολογία που επιστρατεύθηκε γι' αυτό, το «προφίλ» των δραστών σε κάθε περίπτωση.

Στη δεκαετία του 1980 εμφανίστηκε το «πρωτόκολλο X.25». Οι υπολογιστές που το χρησιμοποιούσαν (Apple, PC XT/PC AT, Sinclair Spectrum), χρησιμοποιώντας μια τηλεφωνική σύνδεση και μια συσκευή που ονομάστηκε modem, μπορούσαν να επικοινωνήσουν μεταξύ τους. Με αυτό τον τρόπο, και μέσω των Bulletin Board Service (BBSs), μπορούσαν να ανταλλάξουν πληροφορίες μεταξύ τους, με ένα απλό τηλεφώνημα από το modem ενός χρήστη σε κάποιον τηλεφωνικό αριθμό. Όταν κάποιος χρήστης συνδεόταν σε κάποια BBSs, αμέσως έβλεπε πληροφορίες που τον βοηθούσαν να συνδεθεί σε αυτή. Η σύνδεση επιτυγχανόταν όταν το modem του άλλου υπολογιστή απαντούσε στο τηλεφώνημα και μέσω BBS ο χρήστης μπορούσε να διαβάσει και να κατεβάσει (download) αρχεία ή διάφορες πληροφορίες ή να ανεβάσει (upload) αυτός, χρησιμοποιώντας κάποια πρωτόκολλα λειτουργίας.

Αρχικά, με αυτό τον τομέα ασχολήθηκαν εταιρίες, πανεπιστήμια και σταδιακά όλο και περισσότεροι ιδιώτες. Σχεδόν αμέσως όμως εμφανίστηκαν και οι λεγόμενοι hackers, οι οποίοι κατάφερναν να συνδεθούν σε υπολογιστές στους οποίους δεν ήταν ελεύθερη η πρόσβαση σε όλους, όπως πανεπιστημίων ή υπολογιστών του στρατού, μια και τα μέτρα ασφαλείας σ' αυτόν τον τομέα ήταν ελάχιστα ή ανύπαρκτα.

Τα πρώτα κρούσματα hacking στη Μεγάλη Βρετανία σημειώθηκαν περίπου στο 1983-85 και αφορούσαν προσπάθειες, που πολλές μάλιστα ήταν επιτυχημένες, να προκληθούν ζημιές σε διάφορους υπολογιστές πανεπιστημίων ή να υποκλαπούν σημαντικές πληροφορίες. Έτσι, το 1984 ιδρύθηκε στη New Scotland Yard το πρώτο τμήμα δίωξης ηλεκτρονικού εγκλήματος. Η Μεγάλη Βρετανία ήταν και η χώρα που θέσπισε πρώτη νομοθεσία για την προστασία των ηλεκτρονικών δεδομένων (Data Protection Act, 1984).

Επίσης, την ίδια χρονιά κυκλοφόρησε περιοδικό σχετικό με το hacking, the hacker's handbook, που γνώρισε μεγάλη επιτυχία.

Κατά τη διάρκεια του δεύτερου μισού της ίδιας δεκαετίας, αναπτύχθηκαν και εξελίχτηκαν πολύ οι λεγόμενοι υπολογιστικοί ιοί (computer viruses), όπως ο ιός «Aids», που ήταν υπεύθυνος για την πρώτη εκτεταμένη μόλυνση υπολογιστών, καθώς κυκλοφόρησε σε δισκέτα από πολλά περιοδικά με θέμα τους υπολογιστές. Ο δημιουργός του τον χρησιμοποίησε για να εκβιάσει τα θύματα, ζητώντας χρήματα για να διορθώσει τη βλάβη που προκαλούσε στα υπολογιστικά συστήματα.

Η ανάπτυξη του ηλεκτρονικού εγκλήματος και η φύση του ανάγκασε τα διάφορα κράτη να λάβουν μέτρα για να το αντιμετωπίσουν. Έτσι, το 1989 γίνεται η πρώτη προσπάθεια σε πανευρωπαϊκό επίπεδο για να αντιμετωπιστεί νομικά. Έως τότε, πολύ λίγες χώρες είχαν ήδη θεσπίσει νόμους για κάποιες μορφές του, όπως οι Η.Π.Α., η Αγγλία, η Ανατολική και Δυτική Γερμανία, η Δανία, η Γαλλία, η χώρα μας, η Ιαπωνία, ο Καναδάς και η Αυστρία. Δημιουργήθηκε μία επιτροπή, με την ονομασία Legal Affairs Committee, με εκπροσώπους από τις ευρωπαϊκές χώρες, με σκοπό τη δημιουργία ενός ενιαίου νομοθετικού πλαισίου, που θα επέτρεπε την πιο αποτελεσματική και γρήγορη αντίδραση σε πράξεις που συνιστούσαν ηλεκτρονικά εγκλήματα. Οι εκπρόσωποι της επιτροπής αυτής είχαν συνειδητοποιήσει ότι το ηλεκτρονικό έγκλημα ξεπερνά τα εθνικά σύνορα των διαφόρων χωρών και γι’ αυτό το λόγο ήταν απαραίτητη η δημιουργία κοινής νομοθεσίας. Το πόρισμά της είναι γνωστό ως Council of Europe Recommendation R. Το ίδιο έτος κυκλοφόρησε κι ένα βιβλίο (The Cuckoo’s Egg), στο οποίο καταγραφόταν η πρώτη περίπτωση διεθνούς κατασκοπείας μέσω υπολογιστών (Κιούπης, 2000).

Στη δεκαετία του 1990, ιδρύεται το πρώτο παγκόσμιο κέντρο συντονισμού της ασφάλειας των υπολογιστών, στο Software Engineering Institute του πανεπιστημίου Carnegie Melon, των Ηνωμένων Πολιτειών Αμερικής, γνωστό και σαν Computer Emergency Response Team/Coordination Center (CERT/CC).

Την ίδια εποχή, το διαδίκτυο, χρησιμοποιώντας την υπηρεσία World Wide Web (WWW), που επέτρεπε τη δημιουργία και αναπαραγωγή αρχείων εικόνων, βίντεο, ήχου αλλά και υπερκειμένου

(Hypertext) στις σελίδες των διακομιστών (servers), γνωρίζει τεράστια ανάπτυξη και εξαπλώνεται παντού. Η ανάπτυξη όμως αυτή φέρνει και το πορνό στο διαδίκτυο, τη δημοσίευση τρομοκρατικών προκηρύξεων, τη δημιουργία και ανταλλαγή παράνομων πειρατικών λογισμικών για υπολογιστές.

Επίσης, τότε καταγράφεται και η πρώτη υπόθεση βιομηχανικής κατασκοπείας. Ο θύτης, Kevin Mitnick, αμερικάνος hacker, κατηγορήθηκε για πρόκληση βλάβης σε υπολογιστικά συστήματα και οικονομικές ζημίες δισεκατομμυρίων δολαρίων και κατέληξε στη φυλακή.

Στα μέσα της δεκαετίας του ’90 αναπτύσσονται ραγδαία οι παροχές υπηρεσιών internet (Internet Service Providers – ISPs) και εμφανίζονται οι πρώτες εμπορικές εταιρείες του διαδικτύου (e-commerce). Ταυτόχρονα, δημιουργείται το πρώτο εργαλείο προστασίας υπολογιστών, το SATAN (Security Administrator Tool for Analyzing Networks). Η εφαρμογή αυτή έβρισκε τα αδύνατα σημεία των υπολογιστικών συστημάτων, που θα μπορούσαν να γίνουν πύλη εισόδου των hackers. Αλλά ενώ κυκλοφόρησε για να συνδράμει όσους διαχειρίζονταν τα δίκτυα αυτά, σύντομα αποτέλεσε εργαλείο για τους hackers, που το χρησιμοποίησαν με αντίστροφο σκοπό. Την ίδια εποχή, αρχίζει, με επίκεντρο τη Μεγάλη Βρετανία, η προσπάθεια δημιουργίας ενός προτύπου που θα υποδείκνυε στις εταιρίες τρόπους ασφάλειας για τα συστήματά τους (BS 7799).

Προς το τέλος της δεκαετίας του ’90, το ηλεκτρονικό έγκλημα πήρε νέες απειλητικές μορφές. Η κυκλοφορία του πρώτου macro-virus, ιού δηλαδή που προσέβαλε και μη εκτελέσιμα αρχεία, όπως τα έγγραφα του word ή του excel, με το όνομα «Melissa», προκάλεσε μεγάλες οικονομικές απώλειες σε υπολογιστικά συστήματα σε όλο τον κόσμο. Ταυτόχρονα, βγήκαν σε κυκλοφορία στο διαδίκτυο εργαλεία με τα οποία οποιοσδήποτε μπορούσε να εκμεταλλευτεί τα κενά ασφάλειας ενός υπολογιστή (freeware tools). Επίσης, με τη δημιουργία των CD-R, που επέτρεπαν την αναπαραγωγή δίσκων οπτικού υλικού, η παράνομη αντιγραφή ψηφιακού περιεχομένου πήρε τεράστιες διαστάσεις. Όλες αυτές οι νέες μορφές ηλεκτρονικού εγκλήματος δημιούργησαν αβεβαιότητα για την ασφάλεια και το μέλλον των υπολογιστικών συστημάτων, ακόμα και αυτών που θα μπορούσαν να επηρεάσουν την

παγκόσμια ασφάλεια, όπως για παράδειγμα κέντρα ελέγχου πυραυλικών συστημάτων ή ακόμα και πυρηνικών.

Στη δεκαετία του 2000, μεγάλη αναστάτωση προκάλεσε το λεγόμενο «millennium bug» ή ιός του 2000, που σύμφωνα με φήμες θα κατέστρεφε ολοσχερώς τους περισσότερους υπολογιστές του πλανήτη, χωρίς όμως τελικά να ισχύει κάτι τέτοιο. Αντίθετα, μεγάλα προβλήματα σε εκατομμύρια χρήστες παγκοσμίως προκάλεσε ένας άλλος ιός, με την ονομασία «I love you virus» ή «love bug», όπως και οι ιοί «Code Red» και «Nimda6».

Το 2001 έχουμε την πρώτη διεθνή συνθήκη αναφορικά με το ηλεκτρονικό έγκλημα (Cyber Crime Convention 2001), στην οποία συμμετείχε και η Ελλάδα. Παράλληλα, υπήρχε έντονη φημολογία για την παρακολούθηση και καταγραφή, από τις Η.Π.Α., των τηλεφωνικών συνδιαλέξεων και συνομιλιών, θέμα που πήρε την ονομασία «Carnivore» και επιβεβαιώθηκε με στοιχεία από απόρρητα έγγραφα της Υπηρεσίας Εθνικής Ασφάλειας των Η.Π.Α. (NSA) που δημοσίευαν κάποιοι hackers. Παρόμοια θέματα υπήρξαν και στην Ευρώπη, με το σύστημα παρακολούθησης «Echelon».

Η τρομοκρατική επίθεση του 2011 κατά στόχων στις Η.Π.Α. έπαιξε καθοριστικό ρόλο στις εξελίξεις που ακολούθησαν, αφού αποδείχτηκε ότι τα τρομοκρατικά χτυπήματα σχεδιάστηκαν με κρυπτογραφημένα μηνύματα και ότι οι δράστες χρησιμοποίησαν το hacking για να πάρουν τις πληροφορίες που χρειάζονταν για να τα οργανώσουν. Και γι' αυτό η 11^{η} Σεπτεμβρίου 2011 θεωρείται ημερομηνία σταθμός για όλες τις μελλοντικές εξελίξεις πάνω στο θέμα της ασφάλειας των πληροφοριών και του ηλεκτρονικού εγκλήματος γενικότερα.

1.4 ΔΙΑΚΡΙΣΕΙΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Το ηλεκτρονικό έγκλημα διακρίνεται σε κατηγορίες, ανάλογα με το περιβάλλον στο οποίο τελείται και τον τρόπο. Οι κατηγορίες είναι:

1. Σε ηλεκτρονικό και κοινό περιβάλλοντα χώρο:

Μέσω του διαδικτύου δεν γίνονται μόνο εγκλήματα που αφορούν στην αποκλειστική χρήση των computer, αλλά και αδικήματα του κοινού ποινικού δικαίου. Η τεχνολογία προσέφερε νέα όπλα και νέους τρόπους παράνομης δραστηριότητας, διευρύνοντας τα όρια της εγκληματικότητας. Όταν λοιπόν ένα έγκλημα σχετίζεται με το διαδίκτυο αλλά είναι «κοινό» έγκλημα, αντιμετωπίζεται με αυτό τον τρόπο, και η σχέση του διαδικτύου θεωρείται απλά ως εναλλακτική μέθοδος δράσης, το μέσο με το οποίο τελείται.

Για παράδειγμα, αδικήματα όπως αυτά της εξύβρισης ή της συκοφαντικής δυσφήμισης, της απάτης, της πλαστογραφίας, της εκβίασης, της απειλής, ή της κλοπής πνευματικής ιδιοκτησίας συμβαίνουν και στο διαδίκτυο αλλά και έξω απ' αυτό. Σε τέτοιες περιπτώσεις, η υπάρχουσα νομοθεσία καλύπτει σε μεγάλο βαθμό τους τρόπους εγκληματικής συμπεριφοράς, αφού περιγράφει με ακρίβεια τα χαρακτηριστικά που τους καθιστούν παράνομους, με την επιφύλαξη βέβαια για το πόσο ολοκληρωμένες και επαρκείς είναι αυτές οι περιγραφές αν δεν λαμβάνουν υπόψη και την παράμετρο του διαδικτύου, που ίσως θα μπορούσε να επηρεάσει τη βαρύτητα των εγκλημάτων και τις ποινές των δραστών.

Για τους λόγους αυτούς, τα διαδικτυακά εγκλήματα πρέπει να θεωρούνται ως ιδιαίτερη μορφή και να εξετάζονται ξεχωριστά. Σε σχέση με τα κοινά ποινικά αδικήματα, παρουσιάζουν αρκετές και καθοριστικές διαφορές. Μέσω του διαδικτύου οι δράστες μπορούν να διαπράξουν τα ίδια αδικήματα σε πολύ μεγάλο αριθμό ατόμων, που δεν είναι προκαθορισμένα αλλά συνήθως τυχαίοι στόχοι, από διάφορα μέρη του κόσμου, με μεγάλη ταχύτητα, εκμεταλλευόμενοι την απρόσωπη και αυτοματοποιημένη λειτουργία των υπολογιστών.

Για παράδειγμα, μία περίπτωση συκοφαντικής αρθρογραφίας σε μια εφημερίδα ή ένα περιοδικό, θα διαβαστεί από όσους επιλέξουν να αγοράσουν το έντυπο. Αντίθετα, αν το άρθρο αυτό δημοσιευτεί σε έναν δημοφιλή διαδικτυακό τόπο, θα διαβαστεί από πολύ περισσότερους ανθρώπους. Άρα, η σχετική νομοθεσία πρέπει να μεριμνήσει και για την τιμωρία της εκμετάλλευσης της τεχνολογίας

προς αυτή την κατεύθυνση, αλλά και για την πρόληψη τέτοιων αδικημάτων. Στην Ελλάδα, αυτό έγινε με το άρθρο 386Α του Ποινικού Κώδικα, που καθόρισε το αδίκημα απάτης με υπολογιστή.

2. Σε ηλεκτρονικό περιβάλλοντα χώρο:

Η δεύτερη κατηγορία ηλεκτρονικού εγκλήματος αφορά σε όσα παίρνουν υπόσταση αποκλειστικά με τη χρήση υπολογιστή. Σε αντίθεση με τα διαδικτυακά, δεν είναι απαραίτητη η χρήση του διαδικτύου για να τελεστούν. Και σε σχέση με την πρώτη κατηγορία ηλεκτρονικών εγκλημάτων, η σημαντική διαφορά συνίσταται στο ότι ο υπολογιστής δεν είναι πια το μέσο ή ένα από τα μέσα με τα οποία γίνεται το έγκλημα, αλλά ο παράγοντας που είναι απαραίτητος για να έχει αντικειμενική υπόσταση. Χωρίς τη χρήση του υπολογιστή δηλαδή δεν υφίσταται έγκλημα (Αγγελής, 2000).

Για παράδειγμα, σε αυτή την κατηγορία περιλαμβάνονται οι αξιόποινες πράξεις που περιγράφονται στα άρθρα 370Β και 370Γ του Ποινικού Δικαίου της Ελλάδας, σύμφωνα με τα οποία η άνευ δικαιώματος πρόσβαση σε δεδομένα υπολογιστικών συστημάτων είναι παράνομη και αξιόποινη πράξη (Κιούπης, 2000).

Άλλα αδικήματα της κατηγορίας αυτής είναι η αλλοίωση, η διαγραφή, η αχρήστευση, η μεταβολή και η απόκρυψη ηλεκτρονικών δεδομένων (άρθρο 303a του Ποινικού Κώδικα της Γερμανίας). Και εκτός απ' τους διάφορους εθνικούς νόμους, υπάρχει και η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση των διαδικτυακών εγκλημάτων (Convention on Cybercrime), που στο άρθρο 4 του Β' κεφαλαίου αναφέρεται στην αθέμιτη τροποποίηση δεδομένων.

3.Σε κυβερνοχώρο:

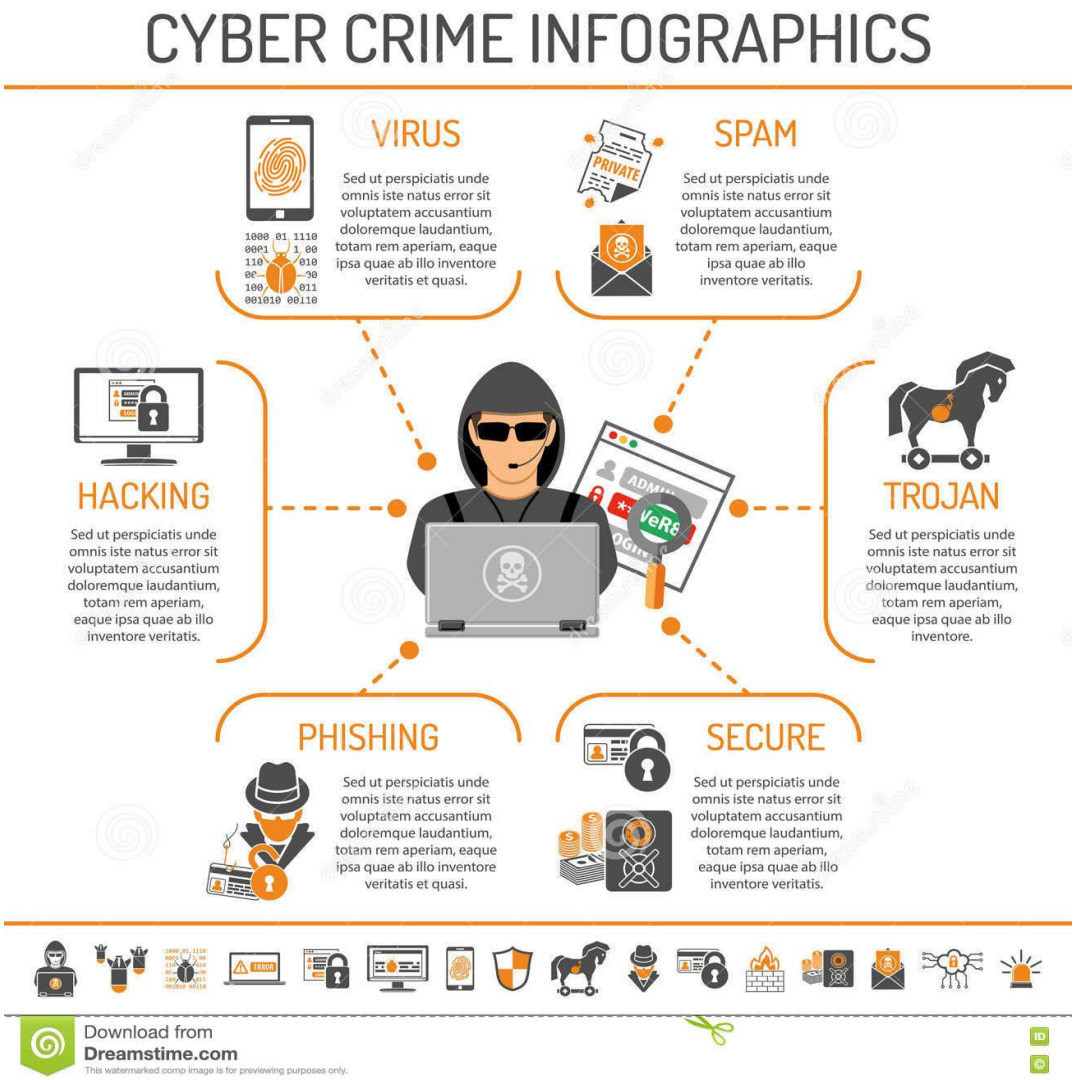
Όπως αναφέρθηκε παραπάνω, τα διαδικτυακά εγκλήματα δεν ταυτίζονται με τα ηλεκτρονικά, αφού για να τελεστούν απαιτείται η χρήση του διαδικτύου κι όχι απλά του υπολογιστή και υπό αυτό το πρίσμα αποτελούν τμήμα της έννοιας του ηλεκτρονικού εγκλήματος, που είναι ευρύτερη. Αν δηλαδή ο υπολογιστής από τον οποίο τελείται ένα αδίκημα δεν έχει σύνδεση με το διαδίκτυο ή δεν το χρησιμοποιεί για το αδίκημα, το έγκλημα είναι ηλεκτρονικό και όχι διαδικτυακό (Παπανικολάου, 2006).

Στην κατηγορία των εγκλημάτων του κυβερνοχώρου ανήκουν αδικήματα όπως η μόλυνση υπολογιστών με ιούς, η εισβολή, χωρίς εξουσιοδότηση, σε πληροφοριακά συστήματα, η μεταβίβαση αποκρυπτογραφημένων κειμένων χωρίς τη σχετική άδεια γι' αυτό. Επίσης, όσα αναφέρονται στα άρθρα 2 έως 10 της Σύμβασης του Συμβουλίου της Ευρώπης για την καταπολέμηση της εγκληματικότητας στο διαδίκτυο. Επιπλέον, πρέπει να αναφερθεί η τάση που υπάρχει τα τελευταία χρόνια στους κόλπους της δικαιοσύνης που τείνει να ενοποιήσει τα διαδικτυακά με τα ηλεκτρονικά εγκλήματα και τα κατηγοριοποιεί με μια ευρύτερη έννοια, ως «εγκλήματα πληροφορικής».

Τέλος, να σημειωθεί η προσπάθεια της δικαιοσύνης στις διατάξεις της να χρησιμοποιεί όσο το δυνατόν πιο ευρείς και ουδέτερους όρους για να οριοθετήσει τεχνολογικά χαρακτηριστικά, ώστε η συνεχής εξέλιξη της τεχνολογίας να μην τις καταστήσει ανενεργές και ξεπερασμένες.

ΚΕΦΑΛΑΙΟ 2Ο ΜΟΡΦΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

2.1 ΓΝΗΣΙΕΣ ΜΟΡΦΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ



2.1.1 ΕΠΙΘΕΣΗ ΑΡΝΗΣΗΣ ΕΞΥΠΗΡΕΤΗΣΗΣ

Επιθέσεις άρνησης εξυπηρέτησης ονομάζονται οι απόπειρες εισβολής σε ένα υπολογιστή να σκοπό να απορροφήσουν όλους τους πόρους του για να μη μπορεί να συνδεθεί ομαλά και να συνεργαστεί με άλλους υπολογιστές. Δηλαδή να εμποδίσουν τη σύνδεση αυτού του υπολογιστή με

διάφορες υπηρεσίες, να διακόψουν τη ροή πληροφοριών και γενικά να υποβαθμίσουν την ποιότητα των υπηρεσιών του. Οι πιο σημαντικές τεχνικές που χρησιμοποιούνται για αυτές τις επιθέσεις είναι οι SYN Flood Attacks, Ping of death, Fragmentation, αλλά υπάρχουν και άλλες, όπως οι port flooding, UDP Flood Attacks, ICMP Flood Attacks, OOB Attacks, Smurf Attacks, Fraggle Attacks και Papasmurf Attacks, Teardrop attacks κ.α.

Η συγκεκριμένη μορφή ηλεκτρονικού εγκλήματος μπορεί να συνοψιστεί σε 4 στάδια. Στο πρώτο, ο επιτιθέμενος τοποθετεί ένα πρόγραμμα απομακρυσμένης διαχείρισης σε έναν υπολογιστή με ευρυζωνική σύνδεση στο internet και έπειτα προσπαθεί να συνδεθεί με αυτό τον υπολογιστή. Δεύτερο στάδιο, η εντολή του εισβολέα να του αποσταλεί το ping (διαδικτυακή εφαρμογή που ενημερώνει το χρήστη για την προσβασιμότητα σε μια διεύθυνση). Με αυτό τον τρόπο, ο χρήστης μπορεί να λειτουργεί τον υπολογιστή από απόσταση, μέσω άλλου. Στο τρίτο βήμα, ο υπολογιστής – θύμα της επίθεσης απαντά στα ping, χωρίς όμως να συνδέεται με τον υπολογιστή που επιτίθεται. Έτσι, ο επιτιθέμενος συνεχίζει να στέλνει νέα ping και χρησιμοποιεί όλους τους πόρους του θύματος για την εξυπηρέτησή τους, με αποτέλεσμα να μη μπορεί να ανταποκριθεί στα αιτήματα που διεκπεραίωνε πριν την επίθεση.

2.1.2 HACKING

Hacking ονομάζεται η απόπειρα πρόσβασης σε ξένους υπολογιστές με σκοπό την εκμετάλλευσή τους από απόσταση. Οι hackers στοχεύουν συνήθως σε συγκεκριμένα υπολογιστικά συστήματα, αφού πρώτα βρουν ευάλωτα σημεία εισόδου και άλλες φορές αποκτούν την απόλυτη διαχείριση των συστημάτων αυτών, που τους καθιστά ικανούς να προβούν σε σοβαρές αλλοιώσεις, άλλοτε εισβάλλουν με δικαιώματα απλού χρήστη.

Οι πιο συνηθισμένες τεχνικές που χρησιμοποιούν οι hackers είναι:

- Η εκμετάλλευση των cookies (μικρών αρχείων που τοποθετούνται στον υπολογιστή όταν επισκέπτεται διάφορες διαδικτυακές σελίδες). Μέσα στα cookies, υπάρχουν προσωπικά στοιχεία του χρήστη, κωδικοί πρόσβασης υπηρεσιών, του ηλεκτρονικού του ταχυδρομείου κ.τ.λ.

- Ανιχνευτές δικτυακών πακέτων. Χρησιμοποιώντας τις εφαρμογές λογισμικού packet sniffers, οι hackers εντοπίζουν όλα τα πακέτα του διαδικτύου και επιτίθενται σε όσα δεν είναι προστατευμένα ή κρυπτογραφημένα. Με αυτό τον τρόπο, αποκτούν πρόσβαση σε κωδικούς πιστωτικών καρτών ή άλλων τέτοιων προσωπικών δεδομένων.

- Ανίχνευση δικτυακών υπηρεσιών συστημάτων. Με αυτή την τεχνική οι hackers αποκομίζουν πληροφορίες σχετικά με την άμυνα του συστήματος στο οποίο σκοπεύουν να επιτεθούν. Κάνοντας ερωτήματα σε διάφορους servers για τις υπηρεσίες που παρέχουν και τα επίπεδα ασφάλειάς τους (port scanning), συγκεντρώνουν πληροφορίες και έπειτα επιτίθενται στα αδύνατα σημεία του συστήματος ή εντοπίζουν λογαριασμούς που δεν έχουν προστασία και είναι εύκολοι στόχοι.

- Πλαστές διευθύνσεις. Αυτές χρησιμοποιούνται ως πηγή, για να δώσουν αληθοφάνεια και αξιοπιστία σε πλαστές πληροφορίες και μηνύματα. Επίσης, λειτουργούν ως κλειδί για την είσοδο σε διάφορες υπηρεσίες.

- Επιθέσεις σε επίπεδο εφαρμογής. Πολλές εφαρμογές του διαδικτύου, όπως για παράδειγμα οι φυλλομετρητές, είναι ευάλωτες σε τέτοιες επιθέσεις.

2.1.3 SPAMMING

Spam λέγεται η μαζική αποστολή διαφόρων μηνυμάτων, κυρίως διαφημιστικού χαρακτήρα, για διάφορες υπηρεσίες ή προϊόντα. Είναι μια απλή διαδικασία, που προϋποθέτει τη συλλογή των διευθύνσεων των διαφημιζομένων (συνήθως γίνεται με στοιχεία από καταλόγους με εταιρείες που διαθέτουν και ηλεκτρονικό κατάστημα) και τη χρήση ενός λογιστικού harvester που συλλέγει διευθύνσεις στις οποίες θα αποσταλούν τα μηνύματα.

2.1.4 ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ

Πρόκειται για μια από τις πιο συνηθισμένες μορφές διαδικτυακού εγκλήματος. Σκοπός των λογισμικών αυτών είναι η εισβολή σ' έναν ηλεκτρονικό υπολογιστή είτε για να αλλοιώσει, είτε να διαγράψει προγράμματα και δεδομένα, είτε να τα κλέψει, είτε να τον καταστρέψει εντελώς ώστε να μην είναι πλέον λειτουργικός. Ο Simrod διακρίνει 3 τύπους τέτοιων κακόβουλων λογισμικών:

Α) Οι ιοί. Πρόκειται για προγράμματα, που μέσω του διαδικτύου εγκαθίστανται σε κάποιον υπολογιστή με σκοπό να εκτελέσουν εντολές χωρίς να φαίνεται η παρουσία τους. Με αυτό τον τρόπο, το ανυποψίαστο θύμα της επίθεσης μεταδίδει άθελά του τον ιό σε κάποιον άλλο υπολογιστή με τον οποίο θα συνδεθεί, είτε μέσω ταχυδρομείου είτε με κάποιον άλλο τρόπο, και δημιουργείται μια αλυσίδα που μολύνει και προκαλεί βλάβες σε πολλούς υπολογιστές.

Κυριότεροι τύποι ιών είναι οι:

-Boot Sector Virus: Οι ιοί αυτού του τύπου επηρεάζουν τον κώδικα του υπολογιστικού συστήματος, εντοπίζοντάς τον στις λειτουργίες της εκκίνησης, στη βοηθητική μνήμη ή στο Master Boot Record (MBR) του σκληρού δίσκου. Με αυτό τον τρόπο, οι ιοί αυτοί μολύνουν κάθε δίσκο ή δισκέτα που θα εκκινήσει στον υπολογιστή αυτό.

-File infectors ή αλλιώς parasitic viruses: Ιοί που στοχεύουν σε εκτελέσιμα προγράμματα στα οποία προσθέτουν κακόβουλο πρόγραμμα, οδηγώντας τα σε ενέργειες που δεν θα έπρεπε να κάνουν. Επηρεάζουν αρχεία με επεκτάσεις .com, .sys, .old, .exe.

-Multi-partite viruses: Οι ιοί αυτοί συνδυάζουν τα χαρακτηριστικά των δύο πρώτων τύπων. Μπορούν να επηρεάσουν και εκτελέσιμα αρχεία και τη λειτουργία εκκίνησης.

-Flash Bios και ιοί link: Οι flash bios ιοί επιτίθενται στο λογισμικό BIOS που βρίσκεται στη μητρική πλακέτα των υπολογιστών, και το τροποποιούν, προκαλώντας σοβαρές βλάβες που φτάνουν μέχρι και την αχρήστευσή τους, αφού δεν μπορούν καν να εκκινήσουν. Οι ιοί τύπου link επιφέρουν

τροποποιήσεις στο αρχείο file allocation table (FAT) με τέτοιο τρόπο, ώστε ο χρήστης να προσπαθεί να εκτελέσει ένα πρόγραμμα κι αντί αυτού να εκτελείται το περιεχόμενο του ιού.

- Companion viruses: Ιοί που στοχεύουν στο σύστημα DOS των υπολογιστών. Η μετάδοσή τους γίνεται με εξωτερικά αποθηκευτικά μέσα και τα αρχεία που εισάγονται «κρύβονται» στη μνήμη του υπολογιστή.

-Macro viruses: Πρόκειται για ιούς που έχουν σχέση με προγράμματα αυτοματισμού γραφείων.

Β) Τα σκουλήκια. Είναι προγράμματα παρόμοια με τους ιούς, που όμως δεν χρειάζονται κάποιο αρχείο για να επισυναφθούν, ούτε κάποια ενέργεια από τον χρήστη – θύμα για να επηρεάσουν τον υπολογιστή του. Εισβάλλουν στους υπολογιστές μέσω του internet, διαφοροποιούν ή καταστρέφουν αρχεία και μετά στέλνουν αντίγραφά τους σε άλλους υπολογιστές, δημιουργώντας αλυσίδα καταστροφών. Μια τέτοια τεράστια αλυσίδα δημιούργησε το σκουλήκι με την ονομασία Code Red II, που κατάφερε να μολύνει 359 χιλιάδες υπολογιστές σε 14 μόλις ώρες, με οικονομικό αντίκτυπο στα θύματα πάνω από δύο δις δολάρια.

Γ) Δούρειοι Ίπποι, Spyware, Adware, Dialers, λογικές και ωρολογιακές βόμβες, τεχνικές απόκρυψης ιών και φάρσες.

Οι Δούρειοι ίπποι είναι κακόβουλα λογισμικά που πήραν αυτή την ονομασία γιατί λειτουργούν όπως τον Δούρειο Ίππο της Ιλιάδας. Ο Οδυσσέας έκανε στους Τρώες ένα φαινομενικά άκακο δώρο για να τους ευχηθεί καλή τύχη, στην πραγματικότητα όμως αυτό ήταν το μέσο για να καταληφθεί η Τροία. Με τον ίδιο τρόπο, οι δούρειοι ίπποι μοιάζουν σαν ένα απλό πρόγραμμα, μέσα τους όμως κρύβουν λειτουργίες που δεν φαίνονται. Όταν εγκατασταθούν στον σκληρό δίσκο του υπολογιστή-θύματος, δίνουν τη δυνατότητα στον δράστη να τον ελέγξει από μακριά, να αποκτήσει πρόσβαση σε προσωπικά στοιχεία, όπως κωδικούς πρόσβασης και πιστωτικών καρτών ή ακόμα και να ενεργοποιήσει την άρνηση εξυπηρέτησης.

Υποκατηγορία των δούρειων ίππων είναι τα προγράμματα spyware και adware. Πρόκειται επίσης για προγράμματα κακόβουλου λογισμικού, εκτός από τις περιπτώσεις που η ύπαρξή τους περιλαμβάνεται στους όρους χρήσης που αποδέχεται ο χρήστης μπαίνοντας σε μια ιστοσελίδα. Συνήθως χρησιμοποιούνται με σκοπό τη διαφήμιση προϊόντων ή διαφόρων sites του διαδικτύου, δημιουργώντας λογαριασμούς στους οποίους αποστέλλουν διαφημιστικά μηνύματα. Η λειτουργία τους μπορεί να βλάψει κάποιον υπολογιστή επιβραδύνοντάς τον, καταστρέφοντας αρχεία ή αποσυντονίζοντας το λειτουργικό του σύστημα.

Οι dialers είναι μια μορφή spyware προγραμμάτων, που επιχειρούν να αποσυνδέσουν το χρήστη απ' την κανονική σύνδεση με το internet και να τον συνδέσουν με γραμμές υψηλής χρέωσης. Με αυτό τον τρόπο ευνοούνται τα sites στα οποία γίνονται αυτές οι συνδέσεις και γι αυτό οι dialers συνήθως βρίσκονται σε συγκεκριμένες ιστοσελίδες με ύποπτο λογισμικό.

Λογικές βόμβες ονομάζονται κάποια προγράμματα που όταν εγκατασταθούν σ' έναν υπολογιστή περιμένουν μια συγκεκριμένη ενέργεια για να ξεκινήσουν την κακόβουλη λειτουργία τους. Όταν γίνει αυτό, μπορεί να εξαπολύσουν έναν ιό στο σύστημα, που θα διαγράψει αρχεία, θα σταματήσει τη λειτουργία του υπολογιστή ή θα προκαλέσει άλλες βλάβες. Στις περιπτώσεις που η ενεργοποίησή τους έχει σχέση με την ώρα ή κάποια ημερομηνία και έχει οριστεί από πριν, λέγονται ωρολογιακές βόμβες γιατί λειτουργούν με αντίστοιχο τρόπο.

Οι φάρσες είναι προγράμματα που προκαλούν ψεύτικους συναγερμούς για την ύπαρξη κακόβουλου λογισμικού στον υπολογιστή του θύματος. Δεν προκαλούν άμεση βλάβη, ωστόσο οι χρήστες που λαμβάνουν αυτές τις προειδοποιήσεις αναγκάζονται να διαγράψουν αρχεία που νομίζουν ότι είναι μολυσμένα.

Οι ιοί καταπολεμούνται με «αντιβιοτικά» λογισμικά (antivirus), που παράγουν οι διάφορες εταιρίες που δραστηριοποιούνται στον τομέα της προστασίας των υπολογιστών. Παρόλα αυτά,

υπάρχουν και αόρατοι (stealth) ιοί, που είναι κατασκευασμένοι με τρόπο που προβλέπει τις ενέργειες αυτών των λογισμικών και τις παρακάμπτουν, μένοντας ενεργοί χωρίς να εντοπίζονται.

Τέλος, οι πολυμορφικοί ιοί (self-mutating, polymorphic), είναι προγράμματα που δημιουργούν κόπιες του εαυτού τους που είναι διαφορετικές μεταξύ τους. Τα αντίγραφα αυτά εμποδίζουν τα αντιβιοτικά να τους εντοπίσουν.

2.1.5 ΠΕΙΡΑΤΕΙΑ ΔΙΑΔΙΚΤΥΑΚΩΝ ΔΙΕΥΘΥΝΣΕΩΝ

Η παράνομη αυτή δραστηριότητα συνέβαινε κυρίως στην πρώτη περίοδο ανάπτυξης του internet, όταν ακόμα δεν είχαν κατοχυρωθεί οι διευθύνσεις των διαφόρων εταιρειών. Οι δράστες στην ουσία καπηλεύονταν μια διαδικτυακή διεύθυνση, συνήθως εταιριών μεγάλου κύρους, και στη συνέχεια, ή έδιναν πίσω τη διεύθυνση στην εταιρία αυτή, έναντι αμοιβής, ή χρησιμοποιούσαν το κύρος της εταιρείας για να δώσουν βαρύτητα σε συκοφαντικές ή προσβλητικές δημοσιεύσεις.

2.1.6 ΠΕΙΡΑΤΕΙΑ ΛΟΓΙΣΜΙΚΩΝ

Ο όρος πειρατεία λογισμικού σημαίνει την παράνομη διακίνηση ή αναπαραγωγή προγραμμάτων υπολογιστή άνευ δικαιώματος, ενέργεια που προσκρούει στο νόμο για την προστασία της πνευματικής περιουσίας. Οι εταιρείες που δημιουργούν τα διάφορα λογισμικά προσπαθούν να εμποδίσουν την παράνομη αναπαραγωγή τους, εισάγοντας σ' αυτά δικλείδες ασφαλείας και γνησιότητας, όμως δεν έχουν καταφέρει να εμποδίσουν τους hackers, που έχουν τη δυνατότητα να παρακάμψουν αυτά τα μέτρα (cracking) και να αντιγράψουν τα προγράμματα. Η πειρατεία είναι πολύ συχνό φαινόμενο τα τελευταία χρόνια και η δράση της έχει σταθεροποιηθεί σε υψηλά ποσοστά, όπως δείχνουν και στοιχεία ερευνών από εταιρείες παραγωγής λογισμικού όπως η Business Software Alliance.

2.1.7 ΕΠΙΘΕΣΗ ΔΙΑΔΙΚΤΥΑΚΩΝ ΤΟΠΩΝ

Η επίθεση σε κάποια συγκεκριμένη ιστοσελίδα θεωρείται από τα λεγόμενα «γνήσια» ηλεκτρονικά εγκλήματα. Στόχοι συνήθως είναι σελίδες υπηρεσιών ή διαφόρων κυβερνητικών

φορέων ή και εφημερίδων και σκοπός η διαφοροποίηση του περιεχομένου τους. Οι επιθέσεις αυτές γίνονται γρήγορα αντιληπτές και αντιμετωπίζονται, ωστόσο αν οι αλλοιώσεις του περιεχομένου είναι εκτεταμένες, αναγκάζουν τους διαχειριστές να διακόψουν τη λειτουργία του διαδικτυακού τόπου μέχρι να διορθώσουν τα προβλήματα.

2.1.8 PHISING

Ένας νέος τρόπος παράνομης απόκτησης προσωπικών ή οικονομικών στοιχείων είναι το λεγόμενο phishing. Συνήθεις στόχοι του είναι κερδοσκοπικοί οργανισμοί που έχουν αυτά τα στοιχεία στην κατοχή τους. Οι phishers χρησιμοποιούν τη μέθοδο του spam ή bots για να συνδεθούν αυτόματα με τα θύματά τους και να επικοινωνήσουν ως εκπρόσωποι του οργανισμού του οποίου έχουν οικειοποιηθεί παράνομα τα στοιχεία. Οι χρήστες παγιδεύονται λαμβάνοντας e-mail από κάποιον οργανισμό ή υπηρεσία που εμπιστεύονται, στην πραγματικότητα όμως τα λαμβάνουν από τον δράστη. Έπειτα, με διάφορα τεχνάσματα, όπως την πρόφαση επιβεβαίωσης του κωδικού πρόσβασης σ' ένα λογαριασμό ή κάποιο password για την είσοδο σε κάποια υπηρεσία, προσπαθούν να οδηγήσουν τα θύματα στην αποκάλυψη προσωπικών ή οικονομικών στοιχείων ή άλλων πληροφοριών (κωδικών τραπεζικών λογαριασμών ή πρόσβασης σε υπηρεσίες, αριθμών πιστωτικών καρτών κ.α.), ώστε να τα εκμεταλλευτούν, άμεσα ή έμμεσα (Παπαδόπουλος, 2005).

«Ο όρος phishing χρησιμοποιήθηκε για πρώτη φορά το 1996 από hackers που στόχευαν λογαριασμούς νόμιμων χρηστών της εταιρίας AOL (America On Line), τους οποίους ήλεγχαν χρησιμοποιώντας passwords νόμιμων συνδρομητών χωρίς να γίνονται αντιληπτοί. Τότε έγινε και η πρώτη αναφορά γι' αυτήν, σε διαδικτυακό τόπο που είχε θέμα το hacking. Η πρώτη αναφορά για το phishing σε Μέσο Ενημέρωσης έγινε τον Μάρτιο του '97.

Το phishing είναι μέθοδος διαδικτυακής απάτης που συνδυάζει την κακόβουλη χρήση της τεχνολογίας που στοχεύει (technical deceit) και εφαρμοσμένων πρακτικών εξαπάτησης (social engineering practices). Ο phischer εμφανίζεται ως εκπρόσωπος ενός έμπιστου οργανισμού, συνήθως

μάλιστα επικοινωνεί με το θύμα ζητώντας με κάποια πρόφαση πληροφορίες προσωπικού ή οικονομικού περιεχομένου (τηλέφωνα, passwords, τραπεζικά στοιχεία κ.α.), για να αποκομίσει τα στοιχεία που χρειάζεται. Στη συνέχεια, επικαλείται προβλήματα που τάχα διαπιστώνει σχετικά με τον τραπεζικό λογαριασμό ή τις κάρτες του θύματος και δίνει ψεύτικες πληροφορίες για δήθεν παρακολούθηση του λογαριασμού αυτού για ύποπτες συναλλαγές. Έτσι το θύμα, αφού πειστεί για την αξιοπιστία του συνομιλητή του, μοιράζεται ευαίσθητες προσωπικές πληροφορίες ή οδηγείται ακόμα και σε περιουσιακή διάθεση και οικονομική βλάβη, σε όφελος φυσικά του δράστη.

Ο πιο συνηθισμένος τρόπος επαφής hacker-θύματος είναι τα e-mail. Χρησιμοποιούνται όμως και τα μέσα άμεσης επικοινωνίας, το τηλέφωνο, πλαστές ιστοσελίδες και αμφίβολης ασφάλειας ή παραβιασμένοι από τους θύτες servers. Μέσω του ηλεκτρονικού ταχυδρομείου, οι επιθέσεις phishing γίνονται με την αλληλογραφία, που υποτίθεται ότι έρχεται από γνήσια και έγκυρη πηγή, τη χρήση ηλεκτρονικής αλληλογραφίας HTML, και αντίγραφα στα οποία έχουν γίνει τροποποιήσεις σε περιεχόμενα URLs και hyperlinks, τη χρήση ιών και σκουληκιών που εισβάλλουν στον υπολογιστή του θύματος ως συνημμένα στην αλληλογραφία, με τη χρήση anti-spam εργαλείων, με εξατομικευμένη αλληλογραφία, τη χρήση ηλεκτρονικής αλληλογραφίας με τροποποιημένη ένδειξη αποστολέα «Mail From:», που σε συνδυασμό με τη χρήση Open Mail Relays servers κρύβουν την προέλευσή της.

Οι επιθέσεις τύπου phishing που χρησιμοποιούν ως μέσο επικοινωνίας με το θύτη πλαστές ιστοσελίδες, γίνονται με τις παρακάτω μεθόδους:

- Χρησιμοποιώντας ψεύτικες διαφημιστικές πινακίδες, που ονομάζονται banners, ώστε να παρακινηθούν οι επισκέπτες της ιστοσελίδας και να πατήσουν κλικ πάνω σε αυτές.

- Ένα άλλο εργαλείο που χρησιμοποιούν είναι τα διαδικτυακά bugs, που διερευνούν τις συνήθειες των επισκεπτών της σελίδας και τον αριθμό των επισκεπτών της.

- Με τη χρήση των frameless windows (pop-ups), που αποκρύπτουν την πραγματική προέλευση του μηνύματος που στέλνει ο phisher.

- Με κακόβουλο λογισμικό που είναι ενσωματωμένο στην ιστοσελίδα και εγκαθιστά στα computer των επισκεπτών της λογισμικό της αρεσκείας του θύτη, όπως ιούς, σκουλήκια, spyware, δούρειους ίππους, keyloggers, back-doors, spyware, exploits, rootkits, dialers κ.α.

- Με την εισαγωγή hyperlinks σε ιστοσελίδες με μεγάλη επισκεψιμότητα.

- Με την κατάχρηση των προδιαγραφών σχέσεων εμπιστοσύνης που υπάρχουν σε ιστοσελίδες φυλλομετρητών στο internet, ώστε μέσω αυτών των σελίδων να εγκαταστήσουν στους υπολογιστές των πελατών τους εκτελέσιμα λογισμικά στους τόπους αποθήκευσης του συστήματός τους» (Παπαδόπουλος, 2005).

2.2 ΗΛΕΚΤΡΟΝΙΚΑ ΕΓΚΛΗΜΑΤΑ ΜΕΣΩ ΥΠΟΛΟΓΙΣΤΩΝ

Η δεύτερη βασική μορφή ηλεκτρονικής εγκληματικότητας περιλαμβάνει αδικήματα που τελούνταν και πριν την εμφάνιση των ηλεκτρονικών υπολογιστών και του διαδικτύου, που όμως, από την εμφάνισή τους και έπειτα, χρησιμοποιήθηκαν γι' αυτό το σκοπό και πια συντελούν με μεγάλο βαθμό στην τέλεσή τους.

2.2.1 ΔΙΑΔΙΚΤΥΑΚΗ ΑΠΑΤΗ

Βασικός σκοπός των μορφών απάτης είναι η απόσπαση χρηματικών ποσών από τα θύματα. Μέσω του διαδικτύου, ο πιο εύκολος τρόπος είναι με το ηλεκτρονικό ταχυδρομείο. Πρώτο βήμα αυτής της μεθόδου είναι η μαζική αποστολή e-mail, με περιεχόμενο που θα γίνει πιστευτό και θα έχει κάποιο ενδιαφέρον για τα θύματα. Για παράδειγμα, συχνό φαινόμενο είναι η αποστολή μηνυμάτων που κάποιος δήθεν κάτοικος χώρας της Αφρικής ζητά βοήθεια ώστε να καταφέρει να εξασφαλίσει τα χρήματα που απαιτούνται για να εγκαταλείψει τη χώρα του και να μετακινηθεί στη χώρα του θύματος. Ως αιτίες γι' αυτή την ενέργεια αναφέρονται οι πόλεμοι, που μαστίζουν τις αφρικανικές χώρες, κάποια προσωπική τραγωδία ή φυσική καταστροφή. Κοινός παρανομαστής όλων των αιτιών που μπορεί να αναφερθούν, ότι είναι ικανές να ευαισθητοποιήσουν κάποιον που θα διαβάσει το μήνυμα. Κι έπειτα, διατυπώνεται η απαίτηση δημιουργίας ενός τραπεζικού λογαριασμού, με συνδικαιούχους τον θύτη και το θύμα, ώστε η οικονομική βοήθεια να έχει τη μορφή δανείου που θα ξεπληρωθεί όταν θα είναι δυνατό. Φυσικά, σκοπός του θύτη είναι να πάρει τα χρήματα και να κλείσει τον λογαριασμό.

Παρόμοιο παράδειγμα διαδικτυακής απάτης είναι το ΛΟΤΤΟ της Ισπανίας. Αφρικανοί που ζούσαν στην Ισπανία απέστειλαν μηνύματα σε διάφορους πολίτες, ενημερώνοντάς τους ότι δήθεν κέρδισαν το ΛΟΤΤΟ και ζητούσαν αριθμούς λογαριασμών για να κατατεθούν τα κέρδη και τα διαδικαστικά έξοδα και άλλα προσωπικά στοιχεία.

Η ταχεία εξάπλωση του ηλεκτρονικού εμπορίου τα τελευταία χρόνια έφερε αύξηση στον αριθμό των ηλεκτρονικών εγκλημάτων που αφορούν τις πιστωτικές κάρτες. Με την απλούστευση

ορισμένων τραπεζικών διαδικασιών και τη δυνατότητα εμπορικών συναλλαγών από απόσταση, χρησιμοποιώντας απλά τον τραπεζικό λογαριασμό, παρατηρήθηκε η διαρροή τέτοιων λογαριασμών στο internet. Το εργαλείο «web sniffer», που έχει τη δυνατότητα να παρακολουθήσει τη μετάδοση δεδομένων στο διαδίκτυο και να ανακτήσει αυτόματα τραπεζικούς λογαριασμούς, την έκανε μια σχετικά απλή διαδικασία.

2.2.2 ΞΕΠΛΥΜΑ ΧΡΗΜΑΤΟΣ

Ξέπλυμα χρήματος ονομάζεται η προσπάθεια κάποιου να κρύψει εισοδήματα που απέκτησε με παράνομο τρόπο και η μετατροπή τους σε εισοδήματα που φαίνεται ως νόμιμο. Η διαδικασία αυτή ξεκινά δίνοντας άλλη μορφή, πιο νομιμοφανή, στα χρήματα. Έπειτα, κόβεται η ανιχνεύσιμη σύνδεση της παράνομης πηγής με τα χρήματα, τα οποία απλώνονται σε διάφορες συναλλαγές, ώστε να μην είναι συγκεντρωμένα και ολοκληρώνεται με την εκ νέου μετατροπή τους, σε νόμιμο πια εισόδημα. Η ανωνυμία που προσφέρει το διαδίκτυο για τις συναλλαγές είναι σύμμαχος προς την κατεύθυνση αυτή.

2.2.3 ΚΛΟΠΗ ΤΑΥΤΟΤΗΤΑΣ

Η κλοπή ταυτότητας αποτελεί ένα από τα πιο σοβαρά και τα πιο επικίνδυνα για το θύμα αδικήματα. Οι δράστες αποκτούν προσωπικά στοιχεία του θύματος με διάφορους τρόπους, είτε μέσω διαδικτύου, είτε με πιο «παραδοσιακούς» τρόπους όπως μια κοινή κλοπή ενός λογαριασμού που περιέχει προσωπικά στοιχεία ή ακόμα και της ίδιας της ταυτότητας, κι έπειτα χρησιμοποιούν τα στοιχεία αυτά για να δημιουργήσουν πλαστούς λογαριασμούς, πιστωτικές κάρτες ή και πλαστές ταυτότητες για δική τους χρήση.

2.2.4 CYBER TERRORISM

Η Κυβερνο-τρομοκρατία (Cyber Terrorism) είναι το είδος τρομοκρατίας που περιορίζεται στο διαδίκτυο, προκαλεί όμως σοβαρές συνέπειες. Οι επιθέσεις αυτές εκμεταλλεύονται την ανωνυμία και τη δυσκολία που υπάρχει να ανιχνευτούν οι κινήσεις κάποιου στο internet και οργανώνονται με αυτό τον τρόπο. Σύμφωνα με το F.B.I., διαδικτυακή τρομοκρατία είναι η πολιτικά υποκινούμενη,

προσχεδιασμένη επίθεση σε υπολογιστές, προγράμματα υπολογιστών, ευαίσθητες πληροφορίες και δεδομένα που έχουν ως αποτέλεσμα την άσκηση βίας από μυστικούς πράκτορες ή υπερεθνικές ομάδες σε άμαχο πληθυσμό.

2.2.5 ΔΙΑΔΙΚΤΥΑΚΗ ΠΑΡΕΝΟΧΛΗΣΗ

Όπως η πορνογραφία, έτσι και η απλή παρενόχληση ήταν κοινωνικό φαινόμενο και πριν τη δημιουργία του διαδικτύου. Μέσω του internet όμως, με e-mail ή τα social media, το φαινόμενο έχει πάρει μεγάλες διαστάσεις. Μέσω του ταχυδρομείου στέλνονται μαζικά μηνύματα από δύσκολα εντοπίσιμες πηγές. Τα μηνύματα αυτά μπορεί να έχουν άμεσο χαρακτήρα, στοχευμένο ή έμμεσο, δηλαδή να στέλνονται μηνύματα που προσβάλλουν ή απειλούν τυχαία πρόσωπα.

2.2.6 ΠΟΡΝΟΓΡΑΦΙΚΟ ΥΛΙΚΟ

Η παράνομη διακίνηση πορνογραφίας προϋπήρχε του διαδικτύου, με τη χρήση του όμως γνώρισε μεγάλη αύξηση. Το πορνογραφικό υλικό μπορεί να έχει τη μορφή βίντεο ή φωτογραφιών και είναι εύκολα προσβάσιμο σε οποιονδήποτε. Να σημειωθεί εδώ και το φαινόμενο της παιδικής πορνογραφίας, που όπως είναι φυσικό ανησυχεί και ευαισθητοποιεί ιδιαίτερα τους αρμόδιους φορείς για την καταπολέμηση του ηλεκτρονικού εγκλήματος.

Προστάτεψε
το παιδί σου από το
ηλεκτρονικό έγκλημα

2.3 ΑΛΛΕΣ ΜΟΡΦΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Ένα μέσο απ' το οποίο μπορούν να διαπραχθούν ηλεκτρονικά εγκλήματα είναι τα κινητά τηλέφωνα, αφού με την εφαρμογή Bluetooth έχουν τη δυνατότητα να ανακτήσουν δεδομένα. Επίσης, είναι υπεύθυνα για τηλεφωνικές υποκλοπές ή την παγίδευση θυμάτων που κάνουν κλήσεις με υπέρογκες χρεώσεις.

Τα τηλεπικοινωνιακά δίκτυα έχουν γνωρίσει τεράστια εξέλιξη και έχουν εξαπλωθεί παντού. Συνεχώς προσθέτουν νέες εφαρμογές στις υπηρεσίες που παρέχουν, ταυτόχρονα όμως μέσω αυτών γίνονται ευαίσθητα σε επιθέσεις.

Τα Α.Τ.Μ. των τραπεζών είναι άλλο ένα πιθανό εργαλείο εγκλήματος, γιατί είναι ευάλωτα στις προσπάθειες υποκλοπής των password των πελατών, είτε με τη χρήση κάμερας είτε με ειδικούς

μηχανισμούς που μπλοκάρουν τις πιστωτικές κάρτες. Τέλος, μια ευρηματική μέθοδος υποκλοπής είναι η τοποθέτηση ψεύτικων πλήκτρων πάνω στα πραγματικά ώστε να υποκλαπούν οι κωδικοί τραπεζικών λογαριασμών.

Χαρακτήρα εργαλείου του ηλεκτρονικού εγκλήματος μπορούν να αποκτήσουν ακόμα και τα ηλεκτρονικά παιχνίδια. Η σύνδεση των παικτών σε servers του διαδικτύου και τα προγράμματα ανάλυσης και επεξεργασίας δεδομένων που χρησιμοποιούν τα καθιστούν ευάλωτα στο hacking και τις συνέπειες που μπορεί να έχει.

Τα τελευταία χρόνια, σύμφωνα με στοιχεία των αστυνομικών υπηρεσιών, είναι μεγάλη η αύξηση των εγκλημάτων του κοινού ποινικού δικαίου που ευνοούνται πολύ απ' το διαδίκτυο, όπως η διακίνηση ναρκωτικών ουσιών, η προτροπή σε αυτοκτονία ή η διευκόλυνσή της με διάφορους τρόπους, το εμπόριο οργάνων ή ακόμα και παιδιών, γι αυτό τα αδικήματα αυτά θεωρούνται μορφές ηλεκτρονικού εγκλήματος. Το διαδίκτυο σ' αυτές τις περιπτώσεις είναι το μέσο που φέρνει σε επαφή ανθρώπους με τέτοιους σκοπούς, που βρίσκουν θύματα ή ομοϊδεάτες σε θεματικά διαδικτυακά groups συζητήσεων ή στα μέσα κοινωνικής δικτύωσης. Για παράδειγμα, έχει καταγραφεί η περίπτωση ανήλικου μαθητή που αυτοκτόνησε με φυτοφάρμακο που του πρότεινε κάποιος 25άχρονος συνομιλητής του σε κάποιο chat room.

Κυβερνοσφετερισμός (cybersquatting)

Κυβερνοσφετερισμός λέγεται το ηλεκτρονικό έγκλημα που αφορά την αυθαίρετη κατοχύρωση και χρήση νόμιμων ηλεκτρονικών διευθύνσεων (domain name) εμπορικών εταιρειών και επιχειρήσεων. Όταν συμβεί αυτό, η επιχείρηση, αν και κατέχει νόμιμα τη διεύθυνση αυτή, δεν μπορεί πια να τη χρησιμοποιήσει, χάνει στην ουσία το δικαίωμα να υπάρχει στο διαδίκτυο με την επωνυμία της. Η φήμη της εταιρείας αμαυρώνεται και οι συνέπειες έχουν και οικονομικό αντίκτυπο.

Ο τρόπος προστασίας των domain names εξαρτάται από τη διατύπωσή τους. Αν πρόκειται για διεύθυνση με ένα όνομα, την προστατεύουν τα άρθρα 57 και 58 του Αστικού Κώδικα για το δικαίωμα στην προσωπικότητα. Αν το domain name αφορά επωνυμία μιας επιχείρησης, τυχόν επιθέσεις σε αυτό εμπίπτουν στο άρθρο 58 του Α.Κ. και στο άρθρο 13 του νόμου 1146/1914. Το συγκεκριμένο άρθρο ισχύει και στις περιπτώσεις που μια ηλεκτρονική διεύθυνση είναι εικονικό κατάστημα.

ΚΕΦΑΛΑΙΟ 3^{Ο} Η ΧΡΗΣΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΣΤΗΝ ΑΝΙΧΝΕΥΣΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

3.1 ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΠΙΘΕΣΕΩΝ

Η εξιχνίαση του ηλεκτρονικού εγκλήματος είναι δύσκολη διαδικασία που συχνά απαιτεί χρονοβόρες έρευνες για να εντοπιστούν τα ηλεκτρονικά ίχνη του εγκλήματος. Τρόποι για την ανακάλυψη των ιχνών παράνομων δραστηριοτήτων είναι ο εντοπισμός IP, οι προειδοποιήσεις, τα αρχεία καταγραφής, τα emails, οι συναγερμοί, οι αναφορές και τα honeypots.

Ο εντοπισμός του IP του δράστη μιας ηλεκτρονικής παράνομης πράξης, δηλαδή η αποτύπωση του ίχνους της ηλεκτρονικής του διεύθυνσης, είναι πολύ σημαντική μέθοδος για να εντοπιστούν άτομα που μπαίνουν χωρίς δικαίωμα πρόσβασης σε κάποιον υπολογιστή ή σύστημα υπολογιστών. Φυσικά, οι πεπειραμένοι δράστες τέτοιων ηλεκτρονικών υποθέσεων δεν χρησιμοποιούν την IP τους κατά την τέλεση αυτών των πράξεων, αλλά ψεύτικες ή πλαστές IP, για να μην μπορούν να εντοπιστούν. Αυτό μπορεί να γίνει με πολύ απλό τρόπο, με την πλαστογράφηση της ηλεκτρονικής τους διεύθυνσης μέσω του domain name system, ή αλλιώς, συστήματος ονόματος χώρου. Ο καλύτερος τρόπος αντιμετώπισης αυτών των πλαστών IP είναι η χρήση των λεγόμενων firewalls, που μπορούν να στείλουν ηλεκτρονικά μηνύματα σε συγκεκριμένους παραλήπτες, που εναντίον των οποίων έχουν εντοπιστεί τέτοιες επιθέσεις. Αυτά τα μηνύματα ενημερώνουν τους διαχειριστές των υπολογιστών και καταγράφουν και αποθηκεύουν κάθε παράνομη κίνηση σε ειδικά αρχεία.

Οι προειδοποιήσεις (alerts) είναι εργαλεία που χρησιμοποιούνται από τους διαχειριστές των πληροφοριακών συστημάτων. Όταν υπάρξει κάποια επίθεση, οι διαχειριστές ειδοποιούνται μέσω email και με αυτό τον τρόπο έχουν τη δυνατότητα έγκαιρης και αποτελεσματικής αντιμετώπισης μιας πιθανής βλάβης, εξαιτίας π.χ. κάποιου κακόβουλου λογισμικού.

Τα αρχεία καταγραφής (log files) μπορούν να αποθηκεύουν τις σχετικές με τη λειτουργία του συστήματος πληροφορίες. Αν ένας υπολογιστής ή δίκτυο υπολογιστών που δεχτεί επίθεση δεν έχει

συγκεκριμένη και καθορισμένη πολιτική σε σχέση με την ασφάλεια των χρηστών τους, τότε τα αρχεία καταγραφής παραμένουν κενά, ενώ την ευθύνη για τον καθορισμό των πολιτικών αντιμετώπισης θα έχουν οι διαχειριστές του συστήματος. Στην περίπτωση που υπάρχει και εφαρμόζεται συγκεκριμένη πολιτική, τότε τα αρχεία καταγραφής είναι πολύ πιο χρήσιμα στην αντιμετώπιση των επιθέσεων. Με τον έλεγχο αυτών των αρχείων οι ελεγκτικές αρχές μπορούν να ερευνήσουν τις ενέργειες κάθε χρήστη και την εξουσιοδότηση που είχε ο καθένας, ώστε να βρεθούν οι υπαίτιοι κάποιας επίθεσης.

Ο έλεγχος των email, ή μηνυμάτων του ηλεκτρονικού ταχυδρομείου, είναι ο πιο συνηθισμένος τρόπος εντοπισμού των δραστών ηλεκτρονικών εγκλημάτων, αφού η αποστολή τους είναι ο συνηθέστερος τρόπος τέλεσης των εγκλημάτων αυτών, είτε γιατί περιέχουν απειλή, είτε με την αποστολή ιών με σκοπό την καταστροφή των αρχείων του ατομικού ή εταιρικού υπολογιστή. Η έρευνα των email στηρίζεται στο ότι ένα ηλεκτρονικό μήνυμα, για να φτάσει από τον αποστολέα στον παραλήπτη, περνάει από ενδιάμεσους σταθμούς, άλλους ηλεκτρονικούς υπολογιστές, που προσθέτουν πληροφορίες στο μήνυμα, και κυρίως στην επικεφαλίδα του. Στην αναζήτηση, λοιπόν, της διαδρομής του μηνύματος, οι καταγραφές αυτές, με την εξέταση της αντίστροφης πορείας του μηνύματος, βοηθούν στον εντοπισμό της ηλεκτρονικής διεύθυνσης του αποστολέα (Βαφόπουλος, 2012).

Οι συναγερμοί (alarm) είναι πολύ χρήσιμα εργαλεία, καθώς δίνουν τη δυνατότητα αποτροπής μιας ηλεκτρονικής επίθεσης, γιατί προειδοποιούν τους διαχειριστές για την επίθεση ή την προσπάθεια εισβολής στο πληροφοριακό σύστημα πριν καν αυτή εκδηλωθεί.

Οι αναφορές (reports) δίνουν πληροφορίες για απόπειρες λήψης παράνομης εξουσιοδότησης για την πρόσβαση σε έναν υπολογιστή ή σε ένα δίκτυο και πιθανές ηλεκτρονικές επιθέσεις.

Τέλος, το λεγόμενο honeypot είναι το πιο νέο και σύγχρονο όπλο των ελεγκτικών αρχών για να εντοπίζουν και να εξιχνιάζουν τα ηλεκτρονικά εγκλήματα. Πρόκειται για συστήματα που έχουν τη μορφή πραγματικών συστημάτων, αλλά χρησιμοποιούνται για να παραπλανήσουν τους δράστες και να τους οδηγήσουν σε απόπειρες να τα παραβιάσουν. Με αυτό τον τρόπο, τα honeypots παρακολουθούν τις ενέργειες που γίνονται και καταγράφουν τη μέθοδο των επιθέσεων. Μια άλλη πιο εξελιγμένη μορφή honeypots είναι τα honeynets, τα οποία δημιουργούν ολοκληρωμένα αντίγραφα συστημάτων παραγωγής και δικτύων (Blake et al., 2008).

3.2 ΣΥΣΤΗΜΑΤΑ ΕΛΕΓΧΟΥ

Όλα σχεδόν τα πληροφοριακά συστήματα χρησιμοποιούν βάσεις δεδομένων. Το ίδιο συμβαίνει και με τα υπολογιστικά συστήματα. Αυτές οι βάσεις απαιτούν τη μεγαλύτερη δυνατή ασφάλεια και ειδικά και πολύπλοκα εργαλεία, ανάλογα και με τη δομή και τους μηχανισμούς από τους οποίους αποτελούνται, για να την εξασφαλίσουν. Προστασία χρειάζονται και τα δεδομένα που βρίσκονται σε αυτές τις βάσεις, καθώς είναι ευαίσθητα και πολύ σημαντικά για τη σωστή λειτουργία τους.

Η προστασία των βάσεων δεδομένων είναι πολλών ειδών: Καταρχάς η φυσική προστασία, δηλαδή η προφύλαξη της βάσης δεδομένων και του υπολογιστή στον οποίο είναι εγκατεστημένη από φυσική φθορά. Έπειτα, η εξασφάλιση της λογικής ακεραιότητας, ώστε η μεταβολή ενός πεδίου να μην οδηγήσει σε αλυσιδωτές βλάβες όλης της βάσης με απρόβλεπτο αποτέλεσμα, αλλά με σωστό σχεδιασμό του συστήματος να περιοριστεί και να απομονωθεί κάθε τυχόν πρόβλημα.

Επίσης, ο σωστός έλεγχος πρόσβασης κάθε χρήστη στα δεδομένα που είναι εξουσιοδοτημένος να έχει πρόσβαση κι όχι σε περισσότερα. Πολύ σημαντική είναι και η ταυτοποίηση κάθε χρήστη πριν του επιτραπεί η είσοδος στη βάση δεδομένων. Αυτό συνήθως γίνεται με κωδικούς εισόδου, ενώ σε πιο εξελιγμένα συστήματα χρησιμοποιούνται κι άλλες μέθοδοι, όπως οι βιομετρικές.

Τέλος, μέρος της προστασίας της βάσης δεδομένων ενός πληροφοριακού συστήματος είναι και η διαθεσιμότητα, δηλαδή η επιβεβαίωση της δυνατότητας πρόσβασης στα δεδομένα τη στιγμή που θα θελήσει κάποιος εξουσιοδοτημένος χρήστης. Όλοι αυτοί οι παράγοντες είναι κρίσιμοι για την υγεία και την καλή λειτουργία των συστημάτων, προστατεύουν τα δεδομένα και τις απόρρητες πληροφορίες και υλοποιούνται με το σωστό σχεδιασμό όλου του συστήματος, που μηδενίζει ή περιορίζει πολύ την πιθανότητα δυσλειτουργίας.

Ο σχεδιασμός ενός συστήματος που περιέχει βάσεις δεδομένων γίνεται με τα εξής στάδια:

● Προκαταρκτική ανάλυση, δηλαδή ανάλυση των απαιτήσεων ασφάλειας για τις συγκεκριμένες βάσεις δεδομένων και εξέταση όλων των πιθανών κινδύνων που μπορεί να αντιμετωπίσουν, όπως κακόβουλα λογισμικά, προβλήματα συμβατότητας και εξουσιοδότησης, η φυσική ασφάλεια των βάσεων κ.ά.

● Ανάλυση των απαιτήσεων ασφαλείας, που σημαίνει ότι στη φάση αυτή γίνεται ο προσδιορισμός των χρηστών των βάσεων και της εξουσιοδότησης που θα έχουν στα δεδομένα των βάσεων.

● Δημιουργία και σχεδίαση του λογικού μοντέλου με το οποίο θα λειτουργήσει η βάση δεδομένων. Ο όρος μοντέλο περιλαμβάνει τη διαδικασία και τους τρόπους πρόσβασης στη βάση, τα υποκείμενα και τα αντικείμενά της και γενικά όλο τον τρόπο λειτουργίας της.

● Σχεδιασμός του λογικού μοντέλου και ενσωμάτωσή του στο γενικό μοντέλο δεδομένων που μπορεί να υποστηρίξει το σύστημα της βάσης δεδομένων.

● Τέλος, ο φυσικός σχεδιασμός. Σε αυτό το στάδιο καθορίζονται παράγοντες του συστήματος όπως η απόδοση, η προσαρμοστικότητα, η ευελιξία, οι τρόποι αντίδρασης σε τυχόν υπερφόρτωση κ.ά.

3.3 ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ

3.3.1 ΣΤΗΝ ΕΥΡΩΠΗ

Οι διαστάσεις που πήραν, τα τελευταία 50 χρόνια, η ανάπτυξη και η χρήση των ηλεκτρονικών υπολογιστών και η ένταξή τους, ως εργαλεία, στα πλαίσια της λειτουργίας ιδιωτικών και κρατικών φορέων, κίνησε το ενδιαφέρον της Διεθνούς Κοινότητας, αφού, όπως έγινε γρήγορα φανερό, η σταδιακή μεταφορά των κοινωνικών δραστηριοτήτων σε ψηφιακό περιβάλλον θα αύξανε το ποσοστό της διαδικτυακής και ηλεκτρονικής έναντι της συμβατικής εγκληματικότητας.

Γι' αυτό, ήδη πριν το 2000, πολλές ανεπτυγμένες χώρες προσπάθησαν να δημιουργήσουν νομοθετικό πλαίσιο που θα ήλεγχε τις πράξεις που έχουν σχέση με το διαδίκτυο. Η αρχή είχε γίνει ακόμα νωρίτερα, όπως για παράδειγμα με το «Electronic Privacy Act» του 1986 στις Ηνωμένες Πολιτείες ή το «Computer Misuse Act» (1990) στην Αγγλία, που ήταν νομοθεσίες που ασχολούνταν με θέματα που αφορούσαν τη χρήση των δικτύων και των ηλεκτρονικών υπολογιστών.

Η σταδιακή άρση των περιορισμών του διαδικτύου και η ελεύθερη πρόσβαση όλων σε αυτό έκαναν πιο επιτακτική την ανάγκη για ισχυρή νομοθεσία. Έτσι, το καλοκαίρι του 1997 η Γερμανία καθιέρωσε νόμο που ρύθμιζε τις γενικές συνθήκες σχετικά με τις υπηρεσίες επικοινωνίας και πληροφόρησης, προβλέποντας αλλαγές στον Ποινικό Κώδικα και κυρώσεις για τις παράνομες πράξεις του διαδικτύου. Λίγο αργότερα, με το «No Electronic Theft Act», οι Ηνωμένες Πολιτείες της Αμερικής κατέστησαν παράνομες ενέργειες που παραβίαζαν την πνευματική ιδιοκτησία στο διαδίκτυο.

Η ανάπτυξη της τεχνολογίας και του διαδικτύου απασχόλησε, όπως ήταν φυσικό, και την Ευρωπαϊκή Ένωση. Αφού αναγνωρίστηκε η μορφή του ηλεκτρονικού εγκλήματος ως έγκλημα που δεν έχει σύνορα, και αφού τονίστηκε η αναγκαιότητα για συνεργασία μεταξύ των κρατών - μελών, ώστε να αντιμετωπισθεί, το Ευρωπαϊκό Συμβούλιο εξέδωσε τη σύσταση No. R (89) 935, που αφορούσε εγκλήματα που είχαν σχέση με τους ηλεκτρονικούς υπολογιστές, τη σύσταση No. R (95)

1336 που διευθετούσε ποινικά και δικονομικά ζητήματα που συνδέονταν με την πληροφορική, και τη σύσταση REC (2001) 837, που ρύθμιζε την παροχή υπηρεσιών που είχαν σχέση με τη μετάδοση πληροφοριών και προστάτευε τους χρήστες από επικίνδυνο ή βλαβερό περιεχόμενο.

Ένα πολύ σημαντικό βήμα για τη διεθνή αντιμετώπιση του ηλεκτρονικού εγκλήματος έγινε στις 23-11-2001, όταν, μετά από διαβουλεύσεις ειδικής επιτροπής που διήρκεσαν τέσσερα χρόνια, καταρτίστηκε η υπ' αριθμόν 185 «Σύμβαση για το Κυβερνοέγκλημα», στη Βουδαπέστη. Η σύμβαση, όπως αναφέρθηκε και στην εισαγωγή της, είχε σκοπό την προαγωγή, κατά προτεραιότητα, μιας κοινής πολιτικής, με στόχο την προστασία της κοινωνίας από το έγκλημα του διαδικτύου, μεταξύ άλλων, υιοθετώντας κατάλληλα νομοθετικά κείμενα και προωθώντας την διακρατική συνεργασία».

Πιο συγκεκριμένα, η σύμβαση περιλαμβάνει διατάξεις που καλύπτουν σε μεγάλο βαθμό το ποινικό σκέλος των ηλεκτρονικών εγκλημάτων και διακρίνεται σε τρία μέρη:

Στο πρώτο μέρος συμπεριελήφθησαν διατάξεις που αφορούν το ουσιαστικό ποινικό Δίκαιο, με τις οποίες οριοθετήθηκαν συγκεκριμένες ποινικές πράξεις εναντίον των πληροφοριακών συστημάτων, εγκλήματα που έχουν σχέση με τη χρήση των ηλεκτρονικών υπολογιστών και τα πνευματικά δικαιώματα. Πολύ σημαντική ρύθμιση ήταν η ταυτοποίηση του αδικήματος της παράνομης πρόσβασης σε ηλεκτρονικούς υπολογιστές, που περιγράφτηκε στο άρθρο 2 της σύμβασης.

Το δεύτερο μέρος περιείχε δικονομικές διατάξεις που είχαν σχέση με τη συλλογή αποδεικτικών στοιχείων σε ηλεκτρονική μορφή, όπως για παράδειγμα μέτρα για τη γρήγορη προστασία και τη μερική γνωστοποίηση δεδομένων, την έρευνα και κατάσχεση δεδομένων και τη διαταγή επίδειξής τους. Τέλος, στο τρίτο μέρος της σύμβασης περιλαμβάνονται διατάξεις που ρύθμιζαν τη διεθνή δικαστική συνεργασία μεταξύ των αρμοδίων Αρχών, την έκδοση

κατηγορουμένων, την παροχή πληροφοριών και την τύχη των δεδομένων στις περιπτώσεις κατάσχεσής τους.

Στη Σύμβαση του Βουκουρεστίου έχουν προσχωρήσει ως σήμερα 65 χώρες, γεγονός που αποδεικνύει το πόσο σημαντική αποδείχτηκε. Κατά τη διάρκεια των εργασιών για τη διαμόρφωσή της, αναδείχτηκε η μεγαλύτερη ίσως δυσκολία για την καταπολέμηση του ηλεκτρονικού εγκλήματος και τον έλεγχο των παράνομων πράξεων στο διαδίκτυο, που είναι η πολυπλοκότητα στη θέσπιση οποιουδήποτε νόμου σχετικά με το θέμα αυτό, τόσο λόγω του διεθνούς χαρακτήρα των εγκλημάτων αυτών, όσο και λόγω των δυσκολιών που προκύπτουν από την ταυτοποίηση των απαιτούμενων τεχνικών εννοιών.

Ταυτόχρονα, η σύμβαση ανέδειξε την ανάγκη θέσπισης νέων νόμων για την αντιμετώπιση των νέων μορφών εγκληματικότητας, που το παραδοσιακό Ποινικό Δίκαιο δεν μπορούσε να ελέγξει. Επίσης, οι διαβουλεύσεις και η έρευνα προκειμένου να διαμορφωθεί η σύμβαση συνέβαλαν στην οριοθέτηση και τη διεθνή χρήση όρων, σε σχέση με το ηλεκτρονικό έγκλημα, όπως τα δεδομένα και το υπολογιστικό σύστημα, οι πάροχοι υπηρεσιών διαδικτύου, τα δεδομένα κίνησης κ.ά.

Τέλος, ο τεράστιος διεθνής αντίκτυπος της σύμβασης κατέστησε τα αρμόδια όργανα της Ευρωπαϊκής Ένωσης ως σημαντικούς και μόνιμους αρωγούς στην καταπολέμηση του ψηφιακού εγκλήματος.

Μετά τη Σύμβαση της Βουδαπέστης, η Ευρωπαϊκή Επιτροπή ασχολήθηκε με τις επιθέσεις στα πληροφοριακά συστήματα και υπέβαλε πρόταση για τη δημιουργία νομοθετικού πλαισίου σχετικά με το θέμα. Έτσι, το 2005, μετά από αρκετές τροποποιήσεις, εκδόθηκε η Απόφαση – Πλαίσιο 2005/222/ΔΕΥ.

Σε αυτήν υπήρξε για πρώτη φορά επίσημη διατύπωση για τους όρους «σύστημα πληροφοριών», «ηλεκτρονικά δεδομένα» και την πρόσβαση σε αυτά «χωρίς δικαίωμα». Επίσης,

εισήχθη ο όρος «μέτρα ασφαλείας» για τις περιπτώσεις παράνομης πρόσβασης στα πληροφοριακά συστήματα.

Πιο συγκεκριμένα, ενώ το προκαταρκτικό κείμενο της απόφασης προέβλεπε την ποινικοποίηση της παράνομης πρόσβασης, ακόμα και δίχως αυτή να θεωρείται κρίσιμη, σε πληροφοριακά συστήματα, αν αυτά προστατεύονταν από ειδικά μέτρα, στο τελικό κείμενο προστέθηκε η προϋπόθεση της παράβασης των μέτρων ασφαλείας, ώστε να θεωρηθεί παράνομη πράξη. Δηλαδή, το αδίκημα συνδέθηκε με κάποια πρότερη ενέργεια των διαχειριστών ή των κατόχων των παραβιασμένων συστημάτων, ενώ οι ποινές για τις μικρής σημασίας παραβιάσεις τέθηκαν στη διακριτική ευχέρεια της νομοθεσίας του κάθε κράτους-μέλους.

Η Απόφαση-Πλαίσιο 2005/222/ΔΕΥ δεν έλυσε τα προβλήματα που δημιουργήθηκαν με το ηλεκτρονικό έγκλημα και γι' αυτό εφαρμόστηκε λιγότερο από δέκα χρόνια. Η Ε.Ε., στην προσπάθειά της να καταπολεμήσει πιο αποφασιστικά το διαδικτυακό έγκλημα και τις επιθέσεις στα πληροφοριακά συστήματα, εξέδωσε την Οδηγία 2013/40/ΕΕ.

Εκεί τονίστηκε και πάλι η σημασία της Σύμβασης της Βουδαπέστης, που θεωρήθηκε η βάση στην οποία στηρίζεται κάθε νομοθετική ρύθμιση για το ηλεκτρονικό έγκλημα. Όπως ξεκάθαρα αναφέρεται στην Οδηγία, η σύμβαση της Βουδαπέστης είναι το βασικό νομικό πλαίσιο για την καταπολέμηση του ηλεκτρονικού εγκλήματος και των επιθέσεων κατά των πληροφοριακών συστημάτων.

Η οδηγία αυτή, αφού εξειδίκευσε και διεύρυνε το περιεχόμενο της Σύμβασης της Βουδαπέστης και της Απόφασης είναι, και σήμερα, το πιο πλήρες νομοθετικό υπερεθνικό πλαίσιο κατά του ηλεκτρονικού εγκλήματος. Το κείμενο της οδηγίας θεωρείται ο οδηγός για την καταπολέμησή του παγκοσμίως, αφού, πέρα από τα κράτη που την έχουν προσυπογράψει, άλλα

εκατόν σαράντα περίπου έχουν στηρίξει τη σχετική τους νομοθεσία πάνω στις συγκεκριμένες αρχές της.

3.3.2 ΣΤΗΝ ΕΛΛΑΔΑ

Στην Ελλάδα, συνέπεια της Οδηγίας 2013/40/ΕΕ, υπήρξε η θέσπιση του Ν.4411/2016, με τον οποίον έγιναν μέρος της εθνικής νομοθεσίας οι διατάξεις της Σύμβασης. Ο νόμος επέφερε πολλές αλλαγές στον Ποινικό Κώδικα της χώρας, ώστε να ελεγχθεί όσο ήταν δυνατόν η νέα μορφή εγκληματικότητας. Πολύ σημαντική είναι η εισαγωγή, στο άρθρο 13 ΠΚ, του ορισμού των όρων «πληροφοριακό σύστημα» και «ψηφιακά δεδομένα». Με αυτό τον τρόπο, αφενός, εκφράστηκε με σαφή τρόπο η διαπίστωση ότι το ηλεκτρονικό έγκλημα δεν είναι μεμονωμένο φαινόμενο που μπορεί να αντιμετωπιστεί εύκολα με νέες διατάξεις, αλλά μια νέα μορφή εγκληματικότητας, για την οποία απαιτείται πιο σύγχρονο Ποινικό Δίκαιο (ένδειξη γι αυτό είναι η εισαγωγή του όρου «πληροφοριακό σύστημα» στα α. 348Α και 348Β ΠΚ, με σκοπό να εναρμονιστούν οι παλιές με τις νέες διατάξεις). Αφετέρου, με την καθιέρωση των όρων αυτών στη νομοθεσία μας έγινε η σύνδεσή της με την ευρωπαϊκή νομοθεσία και κατέστη ευκολότερο να συμμετέχει και η χώρα μας στη διαβούλευση και την ανταλλαγή απόψεων για τα συγκεκριμένα θέματα σε επίπεδο Ευρωπαϊκής Ένωσης.

Επίσης, ο νόμος Ν.4411/2016 εισήγαγε στο υπάρχον εθνικό νομοθετικό πλαίσιο μια σειρά από νέες διατάξεις σχετικά με την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριακών συστημάτων. Με αυτό τον τρόπο, για πρώτη φορά στην Ελλάδα, θεωρήθηκαν ως παράνομες πράξεις η παράνομη πρόσβαση σε υπολογιστές (α. 370Γ παρ. 2 ΠΚ), η παράνομη παρακολούθηση και υποκλοπή διαβιβάσεων δεδομένων (α. 370Δ ΠΚ), η εμπόδιση της λειτουργίας πληροφοριακών συστημάτων (α. 292Β ΠΚ) και οι σχετικές προπαρασκευαστικές πράξεις (α. 292Γ ΠΚ), όπως και οι σχετικές με τις προηγούμενες πράξεις προπαρασκευαστικές πράξεις (α.370Ε ΠΚ).

Επίσης, ο νόμος θέσπισε διατάξεις που είχαν στόχο τη βελτίωση και τον εκσυγχρονισμό του υπάρχοντος Ποινικού Δικαίου, ώστε να είναι δυνατή η εφαρμογή του σε ψηφιακό περιβάλλον. Τέτοιες ήταν η διάταξη για την προσέλκυση παιδιών για γενετήσιους λόγους (α. 348Β ΠΚ), για την απάτη μέσω της χρήσης ηλεκτρονικού υπολογιστή και η διάταξη για την φθορά ηλεκτρονικών δεδομένων (α. 381Α ΠΚ) και τις προπαρασκευαστικές πράξεις αυτής (α. 381Β ΠΚ). Με τις αλλαγές αυτές η νομοθεσία κατάφερε να προσφέρει στις δικαστικές αρχές ένα σχετικά πλήρες νομικό πλαίσιο για τον έλεγχο των παράνομων ενεργειών στο διαδίκτυο, ενώ παράλληλα εναρμονίστηκε με την ευρωπαϊκή φιλοσοφία σε αυτά τα θέματα.

3.4 ΕΛΛΗΝΙΚΕΣ ΑΡΧΕΣ ΕΠΟΠΤΕΙΑΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Στη χώρα μας, η εποπτεία για τα θέματα ασφάλειας και την προστασία στο διαδίκτυο και τις επικοινωνίες, γίνεται από τρεις ανεξάρτητες Αρχές: Την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ), την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.) και την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.). Και οι τρεις Αρχές έχουν τη δυνατότητα να επιβάλλουν όρους για την τήρηση του απορρήτου των τηλεπικοινωνιών στις εταιρείες που έχουν άδεια για τη χρήση τηλεπικοινωνιών δραστηριοτήτων και σε αυτές υπάγονται και όσοι παρέχουν Υπηρεσίες Διαδικτύου (ISP’s).

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα θεσπίστηκε με τον νόμο Ν.2472/1997 και καθήκον της είναι ο έλεγχος της τήρησης του απορρήτου στο διαδίκτυο. Σύμφωνα με το νόμο Ν.2774/1999 «Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα», οι ιστοσελίδες που συγκεντρώνουν προσωπικά στοιχεία του εκάστοτε επισκέπτη τους, όπως τηλέφωνα, ονόματα, διευθύνσεις e-mail κ.τ.λ., έχουν υποχρέωση από το νόμο να τον ενημερώνουν για το λόγο που συλλέγονται τα στοιχεία αυτά και για το αν μεταβιβάζονται σε τρίτους.

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Ε.Τ.) είναι η εθνική ρυθμιστική ανεξάρτητη Αρχή για θέματα τηλεπικοινωνιών. Έχει έδρα την Αθήνα και οικονομική και διοικητική αυτοτέλεια. Οι αρμοδιότητές της συνίστανται στη χορήγηση αδειών σε πάροχους Τηλεπικοινωνιακών Υπηρεσιών, στους οποίους περιλαμβάνονται και οι πάροχοι Υπηρεσιών Διαδικτύου (ISP's), η ρύθμιση κι ο έλεγχος του τηλεπικοινωνιακού τομέα και η γενικότερη εποπτεία της αγοράς τηλεπικοινωνιών.

Τα μέλη της διορίζονται από τον Υπουργό Μεταφορών και Επικοινωνιών, αφού πρώτα γίνει προεπιλογή από την Διάσκεψη των Προέδρων της Βουλής, με αυξημένη πλειοψηφία των τεσσάρων πέμπτων των μελών της. Τα μέλη της συνήθως είναι πρόσωπα με κύρος, κοινωνική αποδοχή, επιστημονική κατάρτιση και άριστη επαγγελματική ικανότητα σε τεχνικούς, οικονομικούς ή νομικούς τομείς. Όσο διαρκεί η θητεία τους, τα μέλη είναι δεσμευμένα να τηρούν αρχεία ενεργειών, ώστε να αποδεικνύεται εύκολα η αντικειμενικότητα και αμεροληψία τους. Επίσης, είναι υποχρεωμένα να τηρούν, για 4 χρόνια μετά την αποχώρησή τους (εκούσια ή ακούσια) από την Αρχή, δηλώσεις εμπιστευτικότητας για εμπορικές πληροφορίες.

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) ξεκίνησε τη λειτουργία της το 2003 με τον νόμο Ν.3115/2003. Στόχο της ανεξάρτητης Αρχής αποτελεί η προστασία του απορρήτου των επιστολών και η ελεύθερη επικοινωνία και ανταπόκριση με οποιονδήποτε άλλο τρόπο. Στην προστασία του απορρήτου των επικοινωνιών συμπεριλαμβάνεται και ο έλεγχος για την εφαρμογή των όρων και της διαδικασίας άρσης του απορρήτου. Επίσης, τμήμα των αρμοδιοτήτων της είναι το δικαίωμα να αποδέχεται και να εξετάζει καταγγελίες, να εκδίδει κανονιστικά κείμενα και να διενεργεί ελέγχους.

Πιο συγκεκριμένα, η Α.Δ.Α.Ε. μπορεί:

● Να κάνει, αυτεπάγγελτα ή μετά από καταγγελία, τακτικούς ή έκτακτους ελέγχους σε εγκαταστάσεις, αρχεία, τεχνικό εξοπλισμό, τράπεζες δεδομένων και έγγραφα της Εθνικής Υπηρεσίας Πληροφοριών, οργανισμών, άλλων δημόσιων υπηρεσιών, επιχειρήσεων του ευρύτερου δημόσιου τομέα και ιδιωτικών επιχειρήσεων που ασχολούνται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση και την επικοινωνία.

● Να προσκαλεί σε ακρόαση τους νόμιμους εκπροσώπους των προαναφερθεισών διοικήσεων δημόσιων ή ιδιωτικών φορέων και εταιριών, ή τους νόμιμους υπαλλήλους τους.

● Να έχει τη δυνατότητα συνεργασίας με άλλες Αρχές της χώρας και με αντίστοιχες άλλων κρατών, καθώς και με ευρωπαϊκούς ή διεθνείς οργανισμούς.

● Να προσφέρει γνωμοδοτήσεις και να διατυπώνει συστάσεις και οδηγίες για τη λήψη μέτρων που θα διασφαλίσουν το απόρρητο των τηλεπικοινωνιών ή τις διαδικασίες για τις περιπτώσεις που απαιτείται η άρση του.

ΚΕΦΑΛΑΙΟ 4^{Ο} ΑΝΤΙΜΕΤΡΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

4.1 ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ - ΤΑΥΤΟΠΡΟΣΩΠΙΑ

Αυθεντικοποίηση λέγεται η διαδικασία με την οποία γίνεται η ταυτοπροσωπία ενός χρήστη, αποτρέποντας την πρόσβαση και την παρέμβαση χωρίς εξουσιοδότηση σε ένα πληροφοριακό σύστημα. Η ταυτότητα του χρήστη επιβεβαιώνεται συνήθως με τη χρήση κωδικών πρόσβασης ή κάποια «έξυπνη κάρτα» που λειτουργεί ως κλειδί σε έναν υπολογιστή.

Οι μέθοδοι αυτοί όμως δεν είναι απόλυτα ασφαλείς, γι' αυτό, για συστήματα που απαιτούν μεγαλύτερη ασφάλεια, ή εξελιγμένα συστήματα με απόρρητες και ευαίσθητες πληροφορίες, η ταυτοποίηση γίνεται με βάση τα φυσικά χαρακτηριστικά των εξουσιοδοτημένων χρηστών, όπως τα δακτυλικά τους αποτυπώματα.

Κωδικοί πρόσβασης

Οι κωδικοί πρόσβασης είναι ο πιο συνηθισμένος τρόπος για την προστασία των υπολογιστών και των αρχείων τους, λόγω του ότι είναι εξαιρετικά απλός κι εύκολος στη χρήση. Για την ενεργοποίησή τους αρκεί η εισαγωγή του ονόματος χρήστη (username) και του κωδικού ασφαλείας (password) που είναι μοναδικά για τον κάθε χρήστη, εύκολο να τα απομνημονεύσει και να τα αλλάξει αν το κρίνει σκόπιμο.

Παρόλα αυτά, η απλότητα της μεθόδου αυτής είναι και το βασικό της μειονέκτημα, αφού πλέον υπάρχουν τα εργαλεία λογισμικού για την εύκολη κλοπή των κωδικών. Επίσης, σε συστήματα που οι κωδικοί καθορίζονται από τον ίδιο το χρήστη, οι επίδοξοι δράστες εκμεταλλεύονται την τάση των χρηστών να επιλέγουν κωδικούς που είναι εύκολο να απομνημονευτούν ή που σημαίνουν κάτι για αυτούς, όπως ημερομηνίες γενεθλίων, αριθμούς τηλεφώνου κ.ά. και με αυτόν τον τρόπο μαντεύουν τους κωδικούς χωρίς να χρειαστεί να εφαρμόσουν κάποια άλλη διαδικασία.

Στις περιπτώσεις που οι κωδικοί πρόσβασης των χρηστών καθορίζονται από τους διαχειριστές του πληροφοριακού συστήματος, η υφαρπαγή τους είναι γενικά πιο δύσκολη. Αλλά υπάρχουν και οι περιπτώσεις που οι χρήστες εμπιστεύονται τους κωδικούς τους σε τρίτους, όπως για παράδειγμα για κάποια εξυπηρέτηση, που μπορεί να γίνει αιτία για να διαρρεύσει ένα κωδικός.

Άλλος τρόπος είναι η παρακολούθηση των πακέτων που διακινούνται μέσω internet ή η σύνδεση ενός κεντρικού υπολογιστή με έναν απομακρυσμένο, που για να γίνει απαιτείται η εισαγωγή κωδικού. Τέλος, ένας κωδικός πρόσβασης μπορεί να υποκλαπεί όταν το αρχείο του διακομιστή στο οποίο αποθηκεύεται για να γίνεται η ταυτοποίηση του χρήστη δεν έχει επαρκή ασφάλεια.

Βιομετρικές τεχνικές

Βιομετρία ονομάζεται η επιστήμη που ταυτοποιεί άτομα με τη χρήση της ψηφιακής τεχνολογίας. Στόχος της είναι η επαλήθευση της ταυτότητας κάποιου χρήστη με βάση τα μοναδικά του χαρακτηριστικά και οι μέθοδοί της θεωρούνται αρκετά ασφαλείς για την προστασία αρχείων δεδομένων.

Βιομετρικές τεχνικές θεωρούνται οι εξής:

- Δακτυλικά αποτυπώματα.

Τα αποτυπώματα είναι σχεδόν απόλυτα μοναδικό χαρακτηριστικό για κάθε άνθρωπο, αφού η πιθανότητα ύπαρξης ολόιδιου αποτυπώματος είναι περίπου 1 στο ένα δισεκατομμύριο. Για αυτό το λόγο είναι μία πολύ αξιόπιστη μέθοδος ταυτοποίησης. Τα αποτυπώματα του χρήστη λαμβάνονται με scanner, υπέρυθρες ακτίνες και τεχνολογίες σιλικόνης.

- Αναγνώριση προσώπου (face recognition).

Η μέθοδος αυτή στηρίζεται σε συγκεκριμένα χαρακτηριστικά του προσώπου του κάθε χρήστη. Βαρύτητα δίνεται σε χαρακτηριστικά που αλλάζουν δύσκολα στο χρόνο, όπως το σχήμα του στόματος, το περίγραμμα των ματιών, οι αποστάσεις μεταξύ του στόματος, των ματιών και των φρυδιών. Πρόκειται για αρκετά αξιόπιστη μέθοδο, που όμως δεν είναι εύκολο να εφαρμοστεί σε μεγάλη κλίμακα και πολλές φορές αποδεικνύεται ότι δεν είναι πρακτική.

● Σάρωση φωνής.

Βιομετρική μέθοδος με την οποία η ταυτοποίηση γίνεται με την αναγνώριση ενός ηχητικού σήματος που δίνει ο χρήστης με μια λέξη ή φράση-κλειδί. Το πλεονέκτημα αυτής της τεχνικής είναι η δυνατότητα ταυτοποίησης και από απόσταση, χωρίς τη φυσική παρουσία του χρήστη, αλλά με τη χρήση ενός μικροφώνου ή τηλεφώνου.

● Σάρωση ίριδας και αμφιβληστροειδή χιτώνα.

Η ίριδα είναι το έγχρωμο μέρος του ματιού και είναι μοναδική για κάθε άνθρωπο, αφού ο γενετικός της κώδικας περιλαμβάνει 250 διαφορετικά χαρακτηριστικά, που κάνουν μηδενική την πιθανότητα να είναι απόλυτα όμοια σε δύο διαφορετικούς ανθρώπους. Για αυτό θεωρείται μία απόλυτα σίγουρη μέθοδος ταυτοποίησης.

Εξίσου αξιόπιστη θεωρείται και η μέθοδος σάρωσης του αμφιβληστροειδούς χιτώνα. Και αυτό το μέρος του ματιού είναι μοναδικό για κάθε άνθρωπο και μάλιστα παραμένει ίδιο σε όλη τη διάρκεια της ζωής του, εκτός από μερικές σπάνιες εξαιρέσεις που έχουν σχέση με σοβαρές βλάβες στο μάτι. Το μειονέκτημα αυτής της μεθόδου είναι ότι θεωρείται πολύ δύσκολη στην εφαρμογή.

● Σάρωση χεριού.

Η μέθοδος αυτή σαρώνει και αναγνωρίζει το χέρι του χρήστη με τον ίδιο τρόπο που γίνεται και η αναγνώριση προσώπου. Τα σημεία στα οποία δίνει έμφαση είναι η απόσταση μεταξύ των

κλειδώσεων, το μήκος των δακτύλων και το σχήμα των αρθρώσεων. Θεωρείται μία σχετική φτηνή αλλά όχι απόλυτα αξιόπιστη μέθοδος ταυτοποίησης και γι' αυτό χρησιμοποιείται κυρίως σε εφαρμογές που δεν απαιτούν πολύ ψηλά επίπεδα ασφάλειας.

● Σάρωση υπογραφής.

Θεωρητικά, η υπογραφή κάθε ανθρώπου είναι μοναδική, και σε αυτό στηρίζεται η συγκεκριμένη μέθοδος. Παρότι πάντοτε υπάρχει ο κίνδυνος της πλαστογραφίας, θεωρείται αρκετά αξιόπιστη γιατί εξετάζονται πολλοί παράγοντες, όπως η πίεση και η δύναμη που εξασκεί κάποιος όταν υπογράφει και η ταχύτητα με την οποία το κάνει. Πάντως, πρόκειται για τεχνική με περιορισμένη εφαρμογή, που όμως μπορεί στο μέλλον να γίνει πολύ χρήσιμη, ειδικά για να πιστοποιείται η αυθεντικότητα επίσημων εγγράφων.

● Σάρωση πατήματος πλήκτρου (keystroke dynamics).

Η μέθοδος αυτή στηρίζεται στον τρόπο που δακτυλογραφεί ο κάθε χρήστης. Εξετάζει παράγοντες όπως τη δύναμη που χρησιμοποιεί, την ταχύτητα δακτυλογράφησης, τον χρόνο που χρειάζεται για να δακτυλογραφήσει μια συγκεκριμένη συνθηματική λέξη ή φράση, τη συχνότητα λαθών, το χρονικό διάστημα μεταξύ του πατήματος των διαφορετικών πλήκτρων κ.ά.

Από αυτές τις βιομετρικές τεχνικές, κάποιες είναι απόλυτα αξιόπιστες, κάποιες λιγότερο και κάποιες μοιάζουν ευφάνταστες και δύσκολες στην εφαρμογή. Όλες έχουν κοινό χαρακτηριστικό το γεγονός ότι δεν στηρίζονται σε κωδικούς ή αριθμούς, αλλά στα χαρακτηριστικά του κάθε χρήστη. Επειδή αυτά είναι μοναδικά για τον καθένα και δεν μπορούν να αντιγραφούν ή να υποκλαπούν, η βιομετρία συνεχίζει την έρευνα για τη δημιουργία νέων τέτοιων τεχνικών. Κάποιες από αυτές, που ίσως μας απασχολήσουν στο μέλλον, είναι η σάρωση κάποιας φλέβας, η οσμή, η ταυτοποίηση με βάση το σχήμα του αυτιού, της γεωμετρίας του δακτύλου, του νυχιού ή του βηματισμού του κάθε χρήστη.

4.2 ΛΟΓΙΣΜΙΚΟ ΑΣΦΑΛΕΙΑΣ

Το επίπεδο προστασίας των υπολογιστών εξαρτάται σε μεγάλο βαθμό από τα λογισμικά ασφαλείας που χρησιμοποιούν. Τα δύο πιο διαδεδομένα είδη εφαρμογών για το σκοπό αυτό είναι τα antivirus και τα firewalls.

1) Antivirus

Οι περισσότερες επιθέσεις σε πληροφοριακά συστήματα γίνονται με τη χρήση ιών. Η σοβαρότητα των επιθέσεων αυτών ποικίλλει, καθώς υπάρχουν σχετικά ανώδυνοι ιοί αλλά και κάποιοι που μπορούν να προκαλέσουν ανεπανόρθωτες βλάβες σε ένα υπολογιστή ή σε ολόκληρα δίκτυα υπολογιστών. Έτσι, η εγκατάσταση καλών λογισμικών που αντιμετωπίζουν τους ιούς αποτελεσματικά είναι απαραίτητη. Τα αντιβιοτικά δημιουργούνται μετά τη δημιουργία κάθε νέου ιού και έχουν στόχο να τον αντιμετωπίσουν. Κι αυτή είναι μια συνεχής διαδικασία, αφού νέοι επικίνδυνοι ιοί δημιουργούνται συνεχώς.

Τα antivirus λογισμικά λειτουργούν σε τρία στάδια.

- Στο πρώτο στάδιο γίνεται η ανίχνευση των ιών που έχουν εισβάλει στον υπολογιστή. Η διαδικασία αυτή γίνεται είτε αυτόματα, δηλαδή με τη συνεχή ανίχνευση του συστήματος και την ταχύτερη δυνατή αναγνώριση κάποιου ιού, είτε με τη βούληση του χρήστη που θέτει σε λειτουργία τη διαδικασία ανίχνευσης.
- Το δεύτερο στάδιο είναι ο καθορισμός της ταυτότητας και του τύπου του ιού. Από αυτά εξαρτάται η βλάβη που μπορεί να προκαλέσει και ο τρόπος αντιμετώπισής του.
- Το τελικό στάδιο αφορά τον καθαρισμό του συστήματος από τον ιό. Το αντιβιοτικό εντοπίζει τα αρχεία που έχουν μολυνθεί και ο χρήστης παίρνει οδηγίες για τη διαγραφή, επιδιόρθωση ή απομόνωσή τους, ώστε να εμποδίσει μεγαλύτερη εξάπλωση.

Κάθε antivirus, από τη στιγμή που θα εγκατασταθεί, προσφέρει κάποια βασική προστασία στο χρήστη του υπολογιστή. Επειδή όμως παράγονται και κυκλοφορούν διαρκώς νέοι ιοί, οι εταιρίες που δημιουργούν τα λογισμικά προστασίας δίνουν τη δυνατότητα στους χρήστες να ενημερώνουν on line τη βάση δεδομένων του αντιβιοτικού που χρησιμοποιούν, ώστε να παρέχουν προστασία και για τους νέους ιούς.

Οι ιοί αναγνωρίζονται από τα μοναδικά χαρακτηριστικά που έχει ο καθένας απ' αυτούς, την υπογραφή ή το αποτύπωμά τους, όπως αλλιώς λέγεται. Αυτά τα μοναδικά χαρακτηριστικά καταγράφονται και αποθηκεύονται στα λογισμικά προστασίας και με αυτό τον τρόπο αναγνωρίζονται οι απειλές που θα εμφανίσει η σάρωση του υπολογιστή. Μόλις αναγνωριστεί ο ιός, ειδοποιείται ο χρήστης και ακολουθεί η διαδικασία καθαρισμού. Άρα, είναι φανερό ότι το πιο καθοριστικό στοιχείο για την καλή προστασία ενός συστήματος είναι η όσο το δυνατόν πιο πλήρης καταχώρηση των πιθανών απειλών στη βάση δεδομένων του antivirus.

Όταν εμφανίζεται ένας νέος ιός, σε μικρό χρονικό διάστημα ενημερώνεται και η βάση δεδομένων των εταιριών δημιουργίας λογισμικού προστασίας. Ωστόσο, μέχρι να ενημερωθούν πλήρως οι βάσεις δεδομένων των προγραμμάτων των εταιριών αυτών μεσολαβεί ένα εύλογο χρονικό διάστημα, κατά το οποίο ο ιός μπορεί να εξαπλωθεί σε χιλιάδες υπολογιστές.

Κατά τη διάρκεια αυτού του κενού ολοκληρωμένης προστασίας, οι εταιρίες προσπαθούν να αντιμετωπίσουν τις συνέπειες των νέων ιών με άλλες τεχνικές που έχουν αναπτυχθεί τα τελευταία χρόνια. Από αυτές, οι δύο πιο διαδεδομένες είναι η ευρετική ανάλυση και ο έλεγχος ακεραιότητας.

Ευρετική Ανάλυση (heuristic)

Με τη τεχνική της ευρετικής ανάλυσης, το antivirus δεν ψάχνει την υπογραφή των ιών, ώστε να τους ταυτίσει με κάποιον που υπάρχει στη βάση δεδομένων του, αλλά κάνει έλεγχο στα αρχεία που χρησιμοποιεί το υπολογιστικό σύστημα και μετά προσδιορίζει αν ο κώδικας των αρχείων αυτών

έχει εντολές που προέρχονται από ιούς. Έτσι διαπιστώνει την ύπαρξη ιών χωρίς να έχει την ανάγκη να είναι καταγεγραμμένοι αυτοί στη βάση δεδομένων του προγράμματός του. Με αυτή την τεχνική ανιχνεύονται οι ιοί κατά 60-90%, χωρίς να υπάρχει η ανάγκη να έχουν καταγραφεί ήδη στα δεδομένα του προγράμματος, γεγονός που μηδενίζει και το χρόνο αντίδρασης, που είναι η βασική αιτία που χρησιμοποιείται η συγκεκριμένη μέθοδος.

Έλεγχος Ακεραιότητας (Integrity Check)

Ο έλεγχος ακεραιότητας είναι μια μέθοδος που μπορεί να ανιχνεύσει ιούς χωρίς να τους αναγνωρίσει.

Γίνεται σε δύο φάσεις:

Στην πρώτη, όλα τα αρχεία του υπολογιστικού συστήματος καταμετρώνται και υπολογίζεται ένα άθροισμα, που είναι ένας μοναδικός αριθμός για κάθε αρχείο. Έτσι, όλες οι ανεπιθύμητες τροποποιήσεις κάθε αρχείου μεταβάλλουν το νούμερο αυτό, που αποθηκεύεται σε μια βάση δεδομένων.

Στη δεύτερη φάση, γίνεται νέος υπολογισμός των αθροισμάτων και έπειτα σύγκριση με την πρώτη μέτρηση. Οποιαδήποτε διαφορά σημαίνει ότι ενδέχεται να οφείλεται στην παρουσία κάποιου ιού. Να σημειώσουμε πάντως εδώ ότι αυτές οι δύο μέθοδοι λειτουργούν πιο αποτελεσματικά όταν εφαρμόζονται συνδυαστικά.

Κριτήρια επιλογής λογισμικού ανίχνευσης ιών

Στις μέρες μας υπάρχουν πάρα πολλά λογισμικά ανίχνευσης ιών και η επιλογή του καταλληλότερου πρέπει να γίνεται λαμβάνοντας υπόψη κάποια κριτήρια. Τα κυριότερα είναι η δυνατότητα προστασίας σε πραγματικό χρόνο, η δυνατότητα αυτόματης ενημέρωσης της βάσης δεδομένων του, η χαμηλή κατανάλωση πόρων του υπολογιστή, το εύχρηστο interface, η καλή

προστασία της ηλεκτρονικής αλληλογραφίας, η δυνατότητα προγραμματισμένων ελέγχων, η καταγραφή συμβάντων και τέλος η δυνατότητα εκκίνησης του προγράμματος με τη χρήση δισκέτας.

2) Firewalls

Ο όρος firewall μας φέρνει στο νου ένα τοίχος προστασίας και με αυτή την έννοια χρησιμοποιήθηκε, σαν ένα τοίχος που χωρίζει δυο σημεία με σκοπό να αποτρέψει την επέκταση της φωτιάς, σε περίπτωση πυρκαγιάς. Έτσι περίπου είχε χρησιμοποιηθεί ο ίδιος όρος στον μηχανοκίνητο αθλητισμό, μόνο που εκεί περιέγραφε το περίβλημα στα ντεπόζιτα των αγωνιστικών αυτοκινήτων, τα οποία είναι φτιαγμένα ώστε να αποτρέπουν την είσοδο της φωτιάς στο χώρο των εύφλεκτων καυσίμων. Παρόμοια έννοια απέκτησε και η χρήση του στους υπολογιστές: firewall θεωρείται η συσκευή ή το εργαλείο λογισμικού που παρακολουθεί τα πακέτα που προσπαθούν να εισέλθουν ή να εξέλθουν από έναν εσωτερικό δίσκο ή από έναν υπολογιστή. Πραγματικά λοιπόν λειτουργεί σαν ένα τοίχος που προστατεύει το εσωτερικό του υπολογιστή και τα δεδομένα του από το «έξω» απ' αυτόν, που είναι ο χώρος του internet.

Οι βασικές λειτουργίες ασφάλειας που πραγματοποιούν τα firewalls είναι οι εξής:

● Packet filtering (φιλτράρισμα πακέτων).

Η διαδικασία επιτρέπει ή απαγορεύει αντίστοιχα την κίνηση πακέτων που διακινούνται στο internet σύμφωνα με την πολιτική ασφάλειας του οργανισμού ή μη.

● Application proxy gateways (πύλες εφαρμογών).

Μέσω αυτών των πυλών προσφέρονται διάφορες υπηρεσίες στους εσωτερικούς χρήστες, ενώ την ίδια στιγμή οι hosts προστατεύονται από εξωτερικές απειλές. Σε αυτή την περίπτωση, ο τρόπος λειτουργίας του firewall εξαρτάται από την πολιτική ασφάλειας του οργανισμού.

Οι πολιτικές ασφάλειας έχουν δύο μορφές:

Πολιτική προκαθορισμένης άδειας χρήσης (allow-everything-not-specifically-denied). Με την εφαρμογή της συγκεκριμένης πολιτικής, η κυκλοφορία των πακέτων και η εκτέλεση διαφόρων εφαρμογών είναι ελεύθερη, με εξαίρεση τις περιπτώσεις στις οποίες υπάρχει κάποια ρητή απαγόρευση.

Πολιτική προκαθορισμένης απαγόρευσης χρήσης (deny-everything-not-specifically-allowed). Με αυτή την πολιτική, το firewall μπλοκάρει κάθε κυκλοφορία πακέτων και κάθε εκτέλεση εφαρμογής εκτός από αυτές που έχουν προκαθοριστεί. Η συγκεκριμένη πολιτική προσφέρει πολύ μεγαλύτερη ασφάλεια σε σχέση με την πρώτη, αλλά πολλές φορές δεν επιτρέπει καμία ελευθερία στους χρήστες.

Η κατακόρυφη αύξηση του ηλεκτρονικού εγκλήματος στην εποχή μας έχει καταστήσει τα firewalls αναγκαία για κάθε υπολογιστή. Η τεχνολογία τους βελτιώνεται συνέχεια, τα firewalls μπορούν πια να κάνουν πολλές εργασίες ταυτόχρονα, προσφέροντας όλο και μεγαλύτερη ασφάλεια σε όσους τα χρησιμοποιούν.

Οι βασικές τεχνικές προστασίας τους μπορούν να διακριθούν στις εξής:

● Πύλες φιλτραρίσματος (packet filtering gateways), που είναι η πιο απλή διαδικασία που επιτελούν τα firewalls. Ο διαχειριστής έχει προκαθορίσει τους κανόνες που επιθυμεί ο ίδιος και τα firewalls φιλτράρουν τα πακέτα που διακινούνται στο internet με βάση τους κανόνες αυτούς. Ένα πακέτο δηλαδή που θα περάσει από το firewall είτε θα γίνει δεκτό είτε θα απορριφθεί. Τα κριτήρια του φιλτραρίσματος μπορεί να είναι η IP του αποστολέα και του παραλήπτη, η θυρίδα προέλευσης και προορισμού ή το πρωτόκολλο επικοινωνίας που χρησιμοποιείται. Το μειονέκτημα αυτής της τεχνικής είναι το γεγονός ότι στις διευθύνσεις IP εξετάζονται μόνο οι επικεφαλίδες από τις οποίες αντλούνται οι πληροφορίες δρομολόγησης (κι όχι το περιεχόμενο), που στη συνέχεια αξιολογούνται για να γίνουν αποδεκτές ή να απορριφθούν.

● Πύλες εφαρμογών (application gateways). Κύριο χαρακτηριστικό της εφαρμογής αυτής είναι η λειτουργία μια διαμεσολαβητικής υπηρεσίας, που χρησιμοποιεί ένα πακέτο λογισμικού proxy server. Το πακέτο λειτουργεί ως διακομιστής για τους εσωτερικούς χρήστες και ως πελάτης για τους εξωτερικούς. Οι υπηρεσίες proxy μπορούν να παρεμβάλλονται ανάμεσα στα πρωτόκολλα επικοινωνίας και με αυτόν τον τρόπο έχουν τον έλεγχο των επικοινωνιών. Έτσι, αν ένας εξωτερικός χρήστης ζητήσει πρόσβαση σε μια υπηρεσία του εσωτερικού δικτύου, θα συνδεθεί πρώτα με την υπηρεσία proxy. Εκεί θα εξεταστεί η ταυτότητα και η πιστοποίησή του και έπειτα θα του επιτραπεί η πρόσβαση στην υπηρεσία που ζήτησε. Με αυτόν τον τρόπο οι πύλες εφαρμογών κάνουν έλεγχο των πακέτων που δρομολογούνται, εμποδίζοντας επιθέσεις IP και DNS spoofing. Ως προς αυτό, είναι πιο αποτελεσματικές από τις πύλες φιλτραρίσματος, αλλά απαιτούν πιο πολύ χρόνο.

● Υβριδικές πύλες (hybrid gateways). Η τεχνική των υβριδικών πυλών συνδυάζει την αξιοπιστία των πυλών εφαρμογών με την ταχύτητα των πυλών φιλτραρίσματος, και τα υβριδικά firewalls θεωρούνται τα πιο εξελιγμένα. Η πιο σύγχρονη μορφή τους (Stateful Inspection), προσθέτει στο φιλτράρισμα μια υπηρεσία που ελέγχει το εσωτερικό των πακέτων με βάση προηγούμενες επικοινωνίες. Οι πληροφορίες που συγκεντρώνονται από αυτούς τους ελέγχους αποθηκεύονται σε μια βάση δεδομένων με συνεχή ανανέωση και τα δεδομένα των εισερχόμενων πακέτων συγκρίνονται με τα προηγούμενα για να γίνουν αποδεκτά ή να απορριφθούν.

4.3 CRYPTOGRAPHY

Με τον όρο κρυπτογραφία αναφερόμαστε στην πανάρχαια μέθοδο που χρησιμοποιούσε κώδικες- σύμβολα, όπου το καθένα από αυτά είχε αντιστοιχία με ένα από τα γράμματα του αλφάβητου. Η κρυπτογραφία είναι κλάδος της κρυπτολογίας, η οποία ορίζεται στην Wikipedia ως η επιστήμη που έχει ως αντικείμενο μαθηματικούς μετασχηματισμούς με σκοπό να εξασφαλίσει την αλήθεια της πληροφορίας, ενώ η κρυπτανάλυση ασχολείται με το να αποκρυπτογραφήσει, να αναλύσει και να «σπάσει» τους αλγορίθμους που κρυπτογραφούνται.

Η κρυπτογράφηση έχει ως σκοπό την εμπιστευτικότητα, την ακεραιότητα, την αυθεντικοποίηση καθώς και τη μη αποποίηση της παραλαβής – αποστολής (confidentiality, integrity, authentication, non repudiation). Με την κρυπτογράφηση μετατρέπεται η πληροφορία από την κανονική μορφή σε κωδικό. Η αποκρυπτογράφηση, λοιπόν, είναι η διαδικασία κατά την οποία ο γρίφος μετατρέπεται σε κατανοητή μορφή.

Η διαδικασία αυτή απαιτεί τέσσερα στάδια:

- αρχικό μήνυμα
- ένα κρυπτογραφικό σύστημα το οποίο αποτελείται από κάποιον αλγόριθμο κρυπτογράφησης καθώς και από ένα αλγόριθμο για την αποκρυπτογράφηση
- ένα κρυπτογραφημένο κείμενο το οποίο δημιουργείται από τον αλγόριθμο της κρυπτογράφησης του αρχικού κειμένου, προτού αποσταλεί στον αποδέκτη
- ένα «κλειδί» αποτελούμενο από κάποια σειρά συμβόλων, το οποίο χρησιμοποιούν οι αλγόριθμοι για την κρυπτογράφηση και την αποκρυπτογράφηση

Υπάρχουν δυο κύριες κατηγορίες κρυπτογραφίας:

1. η συμμετρική κρυπτογραφία, (με κάποιο ιδιωτικό κλειδί)
2. η ασύμμετρη κρυπτογραφία, (με ιδιωτικό και δημόσιο κλειδί)

Αυτό που χαρακτηρίζει την συμμετρική κρυπτογραφία είναι η ύπαρξη μόνο ενός κλειδιού το οποίο κρυπτογραφεί και το ίδιο αποκρυπτογραφεί. Ο πομπός χρησιμοποιεί το κλειδί για να κρυπτογραφήσει το μήνυμα και το στέλνει κρυπτογραφημένο στον αποδέκτη μέσω κάποιου διαύλου επικοινωνίας. Όταν ο αποδέκτης λάβει το μήνυμα το αποκρυπτογραφεί με το ίδιο κλειδί, το οποίο πρέπει να το παίρνει ο ενδιαφερόμενος με κάποιον ασφαλή τρόπο.

Πιο ασφαλής, όμως, είναι η ασύμμετρη από τη στιγμή που υπάρχουν δυο κλειδιά, ένα δημόσιο, γνωστό από όλους, το οποίο αξιοποιείται με σκοπό την κρυπτογράφηση, και ένα ιδιωτικό

το οποίο γνωρίζει μόνο αυτός που θα αποκρυπτογραφήσει το μήνυμα. Στην δεύτερη περίπτωση, δεν σημαίνει ότι αυτός που γνωρίζει το ένα κλειδί μπορεί να γνωρίζει το άλλο και για την ανταλλαγή δεν χρειάζεται ένας ασφαλής τρόπος επικοινωνίας. Έτσι, τη στιγμή που κάποιος θέλει να πάρει κρυπτογραφημένο μήνυμα, θα δώσει στον πομπό το κλειδί που είναι δημόσιο για να γίνει η αποκρυπτογράφηση με τη χρήση, στη συνέχεια του κλειδιού που είναι ιδιωτικό και το γνωρίζει μόνο αυτός. Εδώ απαιτούνται μεγαλύτερα κλειδιά σε σχέση με αυτά της συμμετρικής κρυπτογραφίας.

Υπάρχουν όμως και κάποια προβλήματα. Στη συμμετρική κρυπτογραφία αδύναμο σημείο θεωρείται να βρεθεί ο πιο ασφαλής τρόπος επικοινωνίας ενώ στην ασύμμετρη κρυπτογραφία χρειάζονται πιο μεγάλα κλειδιά με σκοπό τη αποκρυπτογράφηση και έτσι η όλη διαδικασία καθίσταται χρονοβόρα.

Εδώ η λύση δίνεται από έναν υβριδικό τρόπο κρυπτογράφησης που είναι ο συνδυασμός των προαναφερθέντων. Αξιοποιείται η ασύμμετρη με σκοπό την ανταλλαγή μεταξύ των ενδιαφερομένων του κλειδιού και μετά την ολοκλήρωση της διαδικασίας γίνεται η παραλαβή από τους χρήστες μέσα από έναν ασφαλή δίαυλο επικοινωνίας. Για την πραγματοποίηση της επικοινωνίας αξιοποιείται η συμμετρική κρυπτογράφηση. Ένα δεύτερο πρόβλημα που προκύπτει είναι η δυσκολία πιστοποίησης όσον αφορά την αυθεντικότητα των κλειδιών που είναι δημόσια. Είναι ιδιαίτερα σημαντική η εξακρίβωση της αυθεντικότητας γιατί όταν γίνεται η επαλήθευση, ο ενδιαφερόμενος χρειάζεται να είναι απόλυτα σίγουρος ότι το κλειδί της επαλήθευσης είναι το αληθινό κλειδί αυτού που υπογράφει.

Για αυτό χρειάζεται συνεχώς ο χρήστης να προσπαθεί να εξακριβώσει την αυθεντικότητα του κλειδιού με την βοήθεια της αρχής πιστοποίησης που δίνει την δυνατότητα εξακρίβωσης των δημόσιων κλειδιών. Βάζει υπογραφή με το προσωπικό ιδιωτικό κλειδί στα δημόσια κλειδιά και προσθέτει και άλλα στοιχεία. Το σημείο των δεδομένων, τα οποία υπογράφονται από μέρους της αρχής πιστοποίησης, καλείται «πιστοποιητικό», με την δυνατότητα επαλήθευσης με την βοήθεια του

δημόσιου κλειδιού που παρέχει η αρχή πιστοποίησης. Επιπλέον, κατά την κρυπτογράφηση υπάρχει ο κίνδυνος επίθεσης στην κρυπτανάλυση.

Οι μέθοδοι που χρησιμοποιούνται καθώς και οι τεχνικές που έχει η κρυπτοανάλυση είναι τα σημαντικότερα όργανα όσων επιτίθενται απέναντι σε αυτά της κρυπτογράφησης. Βασικό ρόλο για αυτού του είδους την επίθεση έχει το υλικό που χρησιμοποιείται από τον δράστη. Όταν αυτός που κάνει την επίθεση κατέχει κάποιο κρυπτογραφημένο υλικό, υπάρχει απειροελάχιστη πιθανότητα να γίνει αποκωδικοποίηση, εκτός κι αν ταυτόχρονα γνωρίζει και το αρχικό υλικό.

Στην περίπτωση αυτή μπορεί εύκολα να ανακαλύψει το κλειδί. Όμως χρειάζεται πολλή προσπάθεια και πολύς χρόνος με αποτέλεσμα να είναι πιο ασφαλές το σύστημα. Αν και είναι δύσκολο να παραβιαστούν οι αλγόριθμοι, υπάρχουν πιθανότητες να γίνει, αν κάποιος αφιερώσει πολύ χρόνο, εφαρμόζοντας πολλά κλειδιά και στο τέλος μπορεί να ανακαλύψει το σωστό.

4.4 ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ

Για να αντιμετωπιστούν όλοι αυτοί οι κίνδυνοι για την ασφάλεια των κωδίκων εφαρμόζονται πολιτικές ασφάλειας από τους αρμόδιους οργανισμούς. Οι πολιτικές ασφαλείας αναφέρονται σε ένα γραπτό κείμενο που ορίζει τους κανόνες οι οποίοι εφαρμόζονται με σκοπό την διασφάλιση του συστήματος πληροφορίας του αρμόδιου οργανισμού από τυχόν κινδύνους. Το κείμενο πολιτικής ασφαλείας συντάσσεται σε δυο στάδια:

1^{ο} στάδιο: πριν συνταχθεί το κείμενο, παρατίθενται οι τυχόν κίνδυνοι που προκύπτουν για την ασφάλεια του οργανισμού με ποσοτική ανάλυση για τους κινδύνους. Πιο συγκεκριμένα ορίζεται:

- ποιο μπορεί να είναι το είδος του κινδύνου για την ασφάλεια του οργανισμού
- ποιες οι πιθανότητες να παρουσιαστεί κάποιος κίνδυνος
- ποιο το κόστος που θα προκύψει για τον οργανισμό αν παρουσιαστεί κίνδυνος

Παράλληλα γίνεται και ποιοτική ανάλυση η οποία δεν βασίζονται στη βάση των πιθανοτήτων, παρά σε άλλους παράγοντες που είναι οι τυχόν απειλές ή τα δεδομένα του συστήματος τα οποία το απογυμνώνουν απέναντι στις απειλές.

2^{ο} στάδιο: συντάσσεται το κείμενο για την πολιτική ασφάλεια που χωρίζεται θα πρέπει σε δυο κύρια έγγραφα. Έτσι, το πρώτο παρουσιάζει κάποιες γενικές πολιτικές ενώ το δεύτερο ορίζει τις συγκεκριμένες διαδικασίες. Για την τέλεσή του απαιτείται γνώση κι εμπειρία αλλά και κανόνες γραμμένους σε γλώσσα απλή, κατανοητή σε όλους.

ΚΕΦΑΛΑΙΟ 5ο ΠΡΑΚΤΙΚΟ ΜΕΡΟΣ

Man In the middle Attack

Τα πακέτα ARP(Address Resolution Protocol)

Το Πρωτόκολλο Ανάλυσης Διεύθυνσης Address Resolution Protocol (ARP) είναι το πρωτόκολλο επικοινωνίας που χρησιμοποιείται για την αντιστοίχηση της διεύθυνσης επιπέδου σύνδεσης (παραδείγματος χάριν την φυσικη διεύθυνση MAC) με το αντίστοιχο IP. Το πρωτόκολλο ARP εγκαθιδύθηκε το 1982 στο RFC (Request For Comments) 826 .

Το πρωτόκολο ARP διακρίνεται σε σε 4 κατηγορίες λειτουργιών:

1.Στην περίπτωση επικοινωίας μεταξύ δύο υπολογιστών που βρίσκονται στο ίδιο δίκτυο με στόχο την ανταλλαγή πακέτων
2.Στην περίπτωση όπου δυο ξένοι υπολογιστές που βρίσκονται σε διαφορετικά δίκτυα επικοινωνούν με μία πύλη/δρομολογητήγητή(gateway/router)
3.Στην περίπτωση όπου ένας δρομολογητής καλείται να προωθήσει ένα πακέτο κάποιου host μέσω ενός άλλου δρομολογητή.
4.Στην περίπτωση όπου ένας δρομολογητής κληθεί να προωθήσει ένα πακέτο ενός υπολογιστή σε έναν άλλο υπολογιστή, με τον οποίο βρίσκονται στο ίδιο δίκτυο.
Η πρώτη κατηγορία αφορά την περίπτωση όπου δυο host βρίσκονται στο ίδιο φυσικό δίκτυο (physical network, π.χ. συνδεδεμένοι με ένα καλώδιο Ethernet). Οι λοιπές τρεις κατηγορίες αφορούν την περίπτωση όπου δυο ξένοι υπολογιστές χωρίζονται σχεδόν πάντα από πάνω από τρεις κόμβους.

Δομή ARP πακέτων

Παρακάτω παρουσιάζονται τα πακέτα του ARP

Τύπος υλικού (hardware type)
Ένας αριθμός προσδιορίζεται σε κάθε πρωτόκολλο του στρώματος συνδέσμου και γράφεται στο πεδίο αυτό.
Τύπος πρωτόκολλου **(protocol type)**
Ένας αριθμός προσδιορίζεται σε κάθε πρωτόκολλο που αντιγράφεται στο πεδίο αυτό.
Μέγεθος τύπου υλικού (hardware length)
Μέγεθος σε bytes της διεύθυνσης υλικού για διευθύνσεις Ethernet.
Μέγεθος τύπου πρωτόκολλου
Μέγεθος σε bytes της διεύθυνσης λογικού τύπου, για διευθύνσεις IPv4.

Ενέργεια (operation)
Καθορίζει την ενέργεια που εκτελεί ο αποστολέας:
1. για ερώτημα
2. για απάντηση.

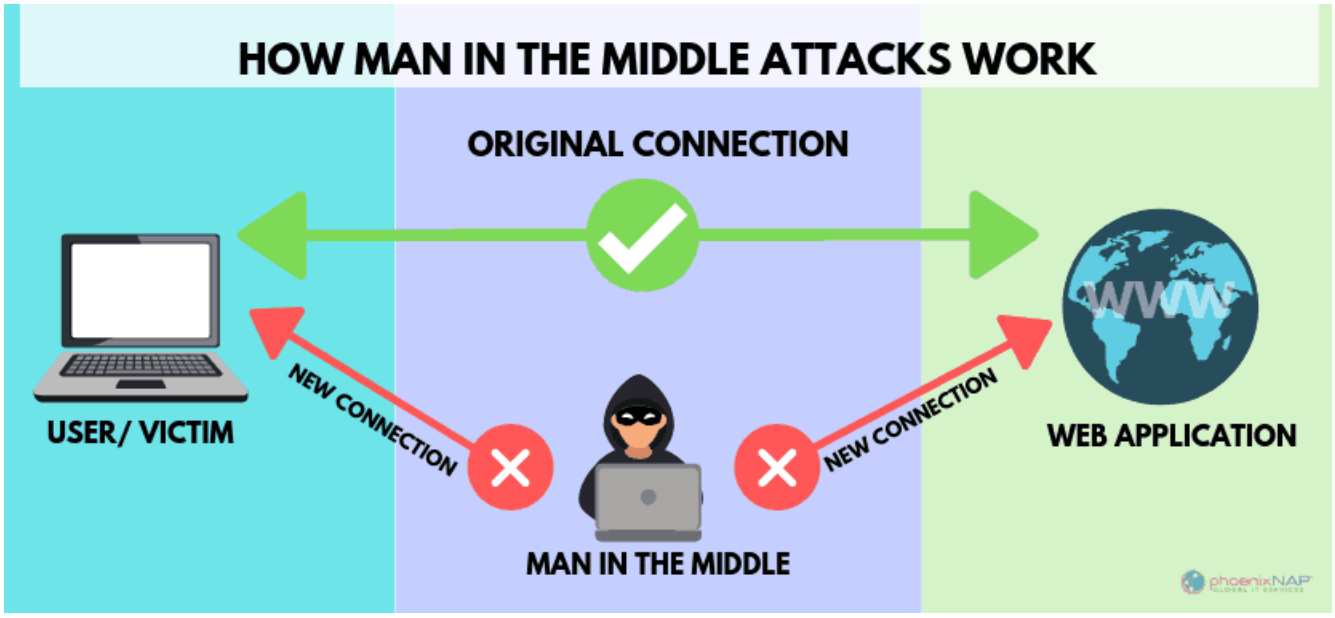
Διεύθυνση υλικού αποστολέα (sender hardware address)
Διεύθυνση υλικού του αποστολέα. Το μέγεθος του πεδίου αυτού δεν είναι σταθερό ˙ εξαρτάται από το υλικό που χρησιμοποιείται.
Διεύθυνση πρωτοκόλλου αποστολέα (sender protocol address)
Διεύθυνση πρωτοκόλλου του αποστολέα. Το μέγεθος του πεδίου αυτού δεν είναι σταθερό ˙ εξαρτάται από το πρωτόκολλο που χρησιμοποιείται.
Διεύθυνση υλικού παραλήπτη (target hardware address)
Διεύθυνση υλικού του **τελικού** παραλήπτη. Το μέγεθος του πεδίου αυτού δεν είναι σταθερό ˙ εξαρτάται από το υλικό που χρησιμοποιείται. Εαν η ενέργεια είναι ερώτημα, το πεδίο αυτό είναι άγνωστο και εξ ορισμού τιμή είναι

Διεύθυνση πρωτοκόλλου παραλήπτη (target protocol address)Διεύθυνση πρωτοκόλλου του **τελικού** παραλήπτη. Το μέγεθος του πεδίου αυτού δεν είναι σταθερό ˙ εξαρτάται από το πρωτόκολλο που χρησιμοποιείται.

Man In The Middle (MITM) Attack

Στο συγκεκριμένο είδος επίθεσης ένας τρίτος (επιτιθέμενος/Hacker) παρεμβάλλεται στην μετάδοση των πακέτων μεταξύ δύο μερών, σύνηθως μεταξύ του διαμεσολαβητή (router) και ενός host (θύμα). Για να το πετύχει αυτό ο επίτιθέμενος στέλνει ένα πλασματικό ARP πακέτο στον router δηλώνοντας ότι εκείνος έχει το IP του host στον οποίο επιτίθεται και έπειτα ο επιτιθέμενος δηλώνει στον host με ένα δεύτερο ARP πακέτο ότι εκείνος είναι το router. Επιτυγχάνοντας την σύζευξη ο επιτιθέμενος αποκτά πρόσβαση σέ όλα τα πακέτα που μεταδίδονται μεταξύ του host και του router. Η επίθεση αυτή χρησιμοποιεί δύο βασικές αδυναμίες του πρωτοκόλλου ARP:

1. Αρχικά οι Clients (συσκευές) μπορούν να δεχθούν αποκρίσεις (responses) χωρίς να στείλουν requests(αίτημα για arp πακέτο)
2. Οι Clients δεν ελέγχουν τα responses που δέχονται ως προς την εγκυρότητα



Εικόνα 1: Εικόνα για MITM

Υλοποίηση MITM επίθεσης

Εργαλία Υλοποίησησης

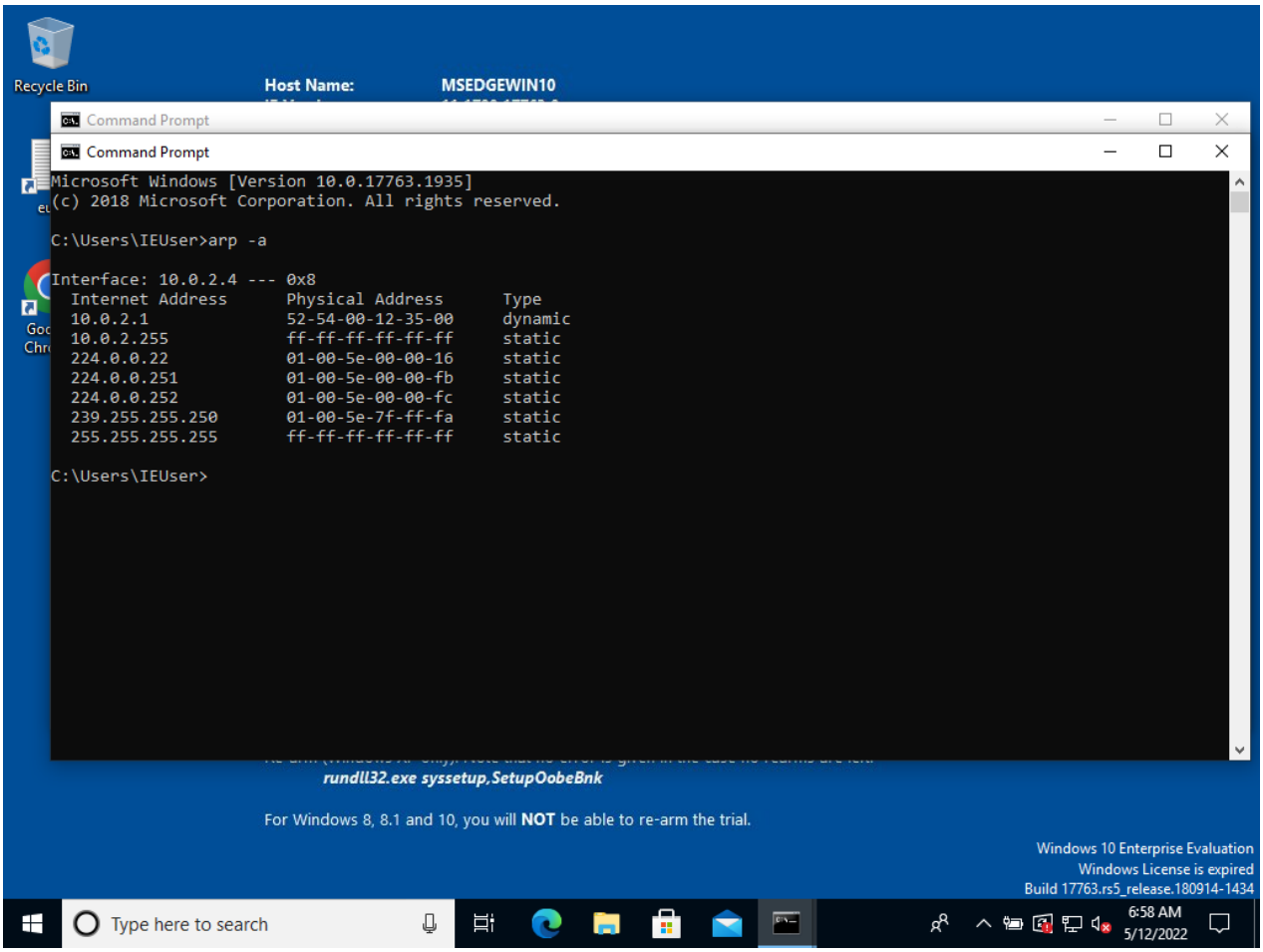
Για την υλοποίηση της επίθεσης χρησιμοποιήσαμε το λογισμικό Debian Linux 64-bit (Kali) σε Oracle VM VirtualBox και η επίθεση πραγματοποιήθηκε σε λογισμικό Windows 10 (64-bit). Για την υλοποίηση χρησιμοοποιήθηκε framework το Bettercap που είναι ενσωματομένο στο Kali Linux.

Υλοποίηση

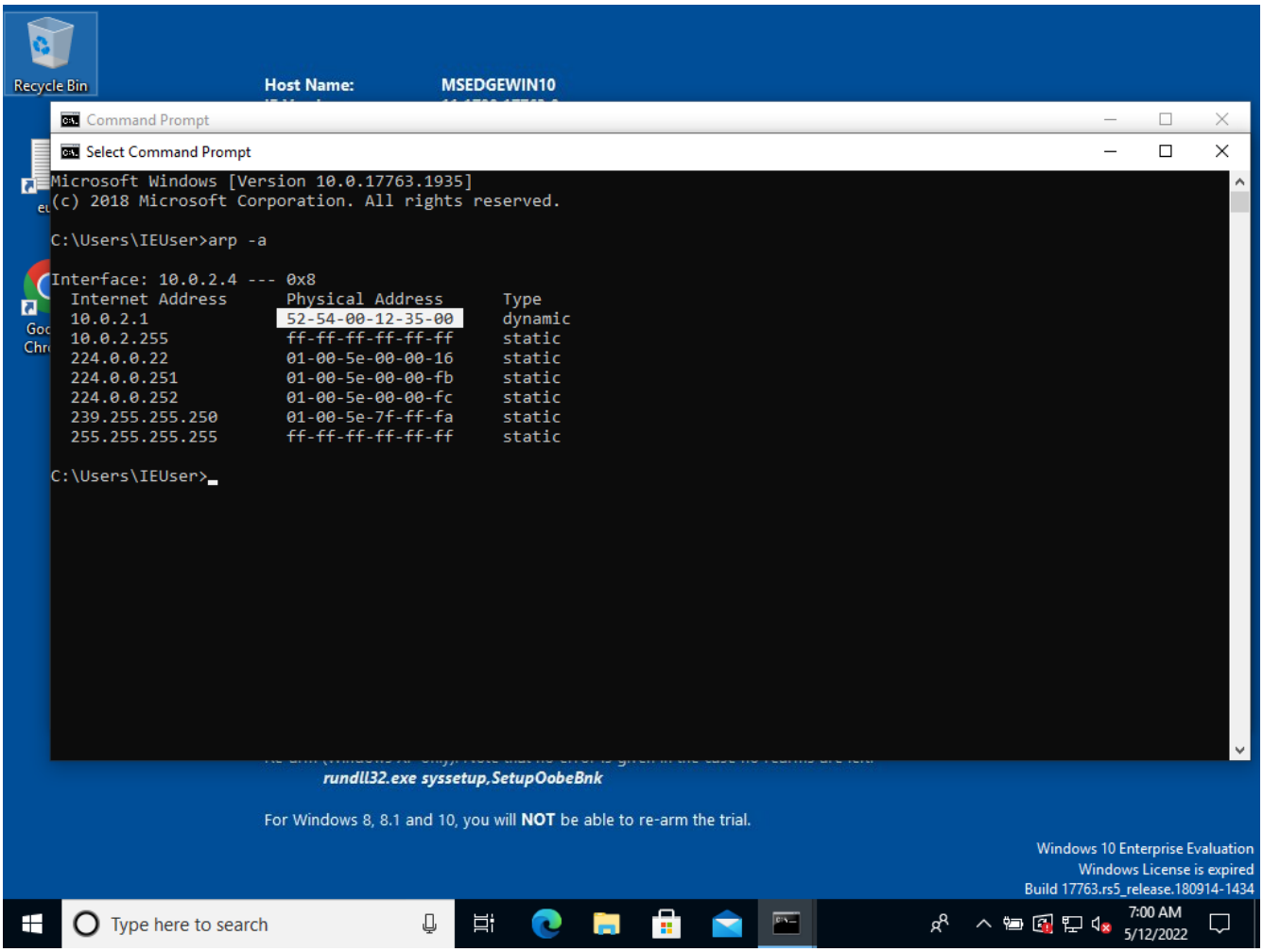
1. Αρχικά ανοίγουμε τα Virtual machines και στο windows machine δίνουμε την εντολή

```
arp -a
```

όπως φαίνεται και στην παρακάτω εικόνα.

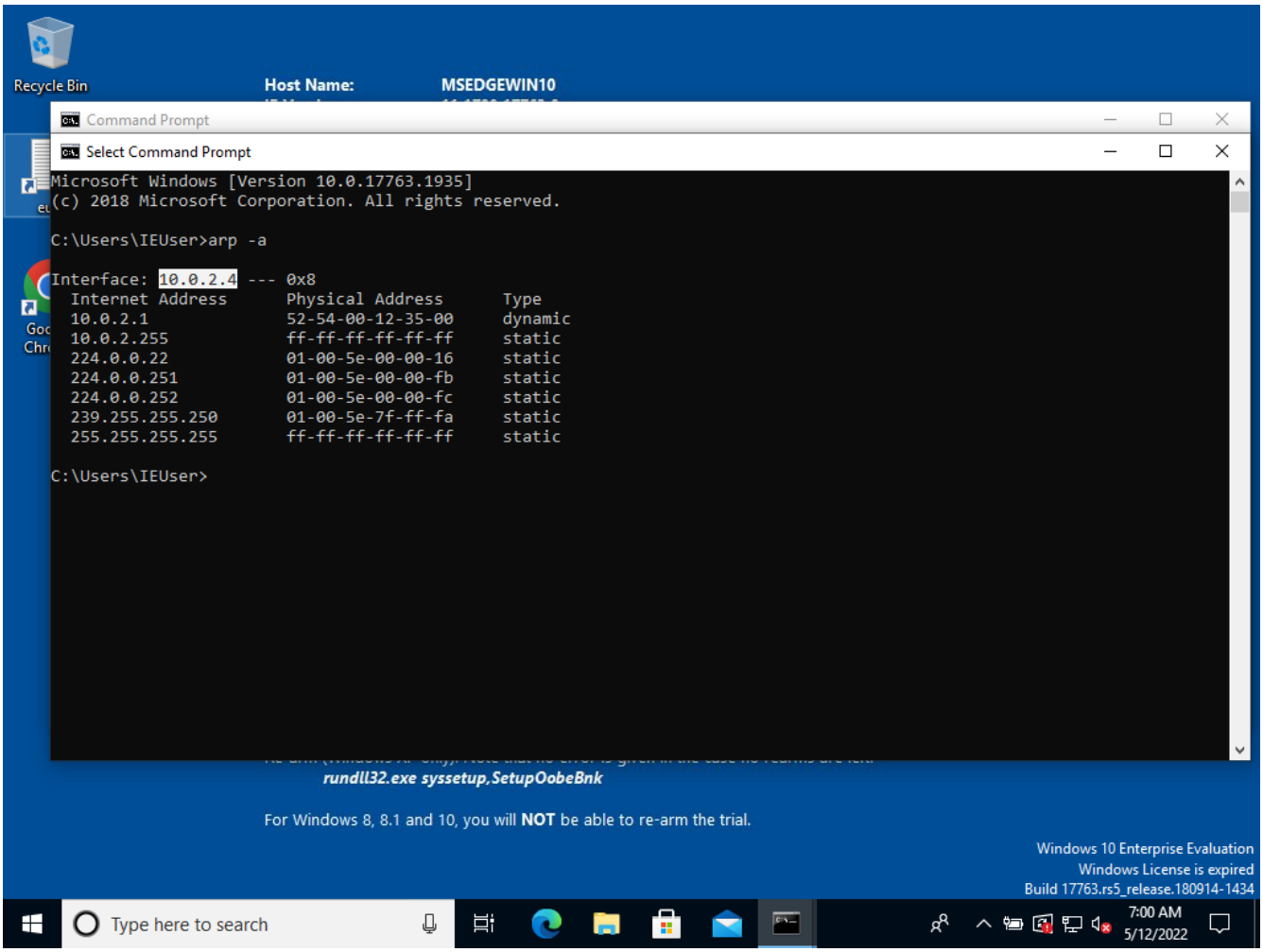


Εικόνα 2: Έλεγχος IP και MAC από τον host (δέκτης επίθεσης)



Εικόνα 3: Έλεγχος IP και MAC από τον host (δέκτης επίθεσης) 2

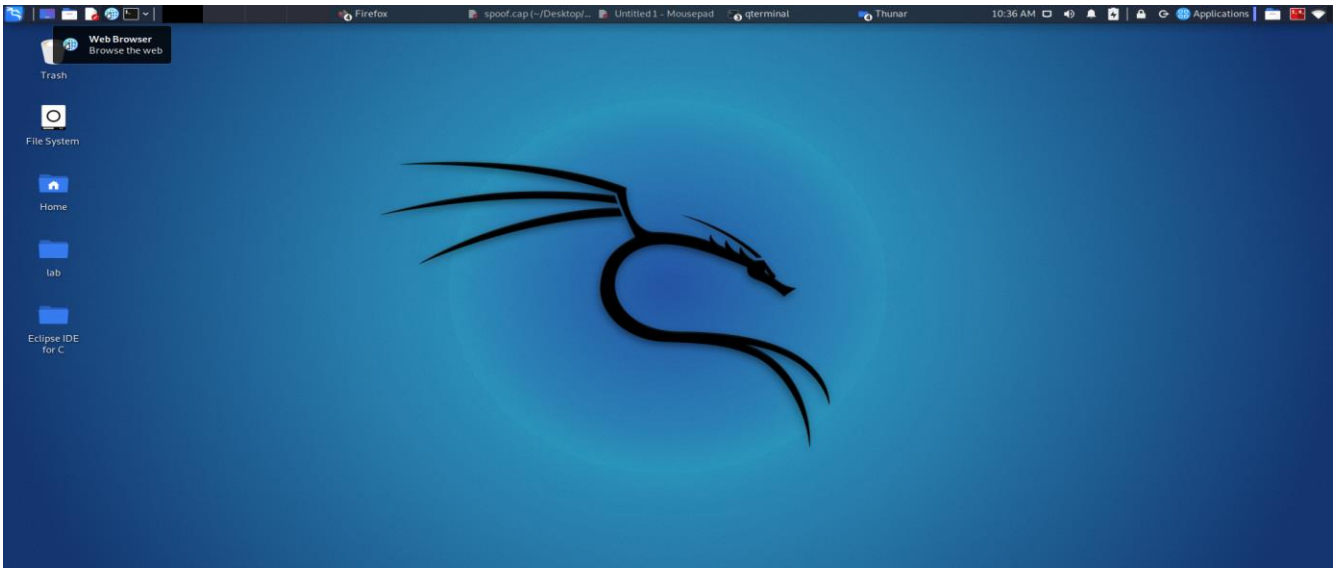
Στο IP 10.0.2.1 βρίσκεται το router με φυσική διεύθυνση MAC: 52-54-00-12-35-00



Εικόνα 4: Έλεγχος IP και MAC από τον host (δέκτης επίθεσης) 3

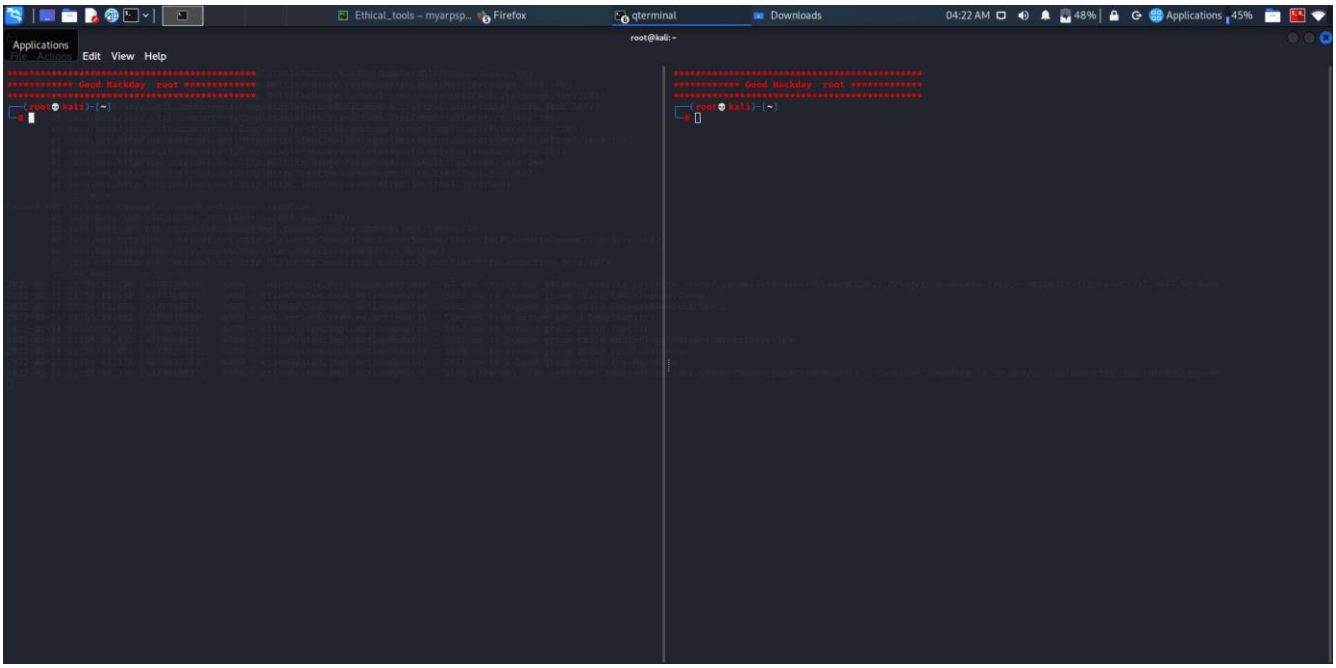
Στο IP 10.0.2.4 είναι συνδεδεμένη η συσκευή που θα δεχθεί την επίθεση (το Windows 10 machine)

Έπειτα ανοίγουμε την μηχανή Kali Linux.

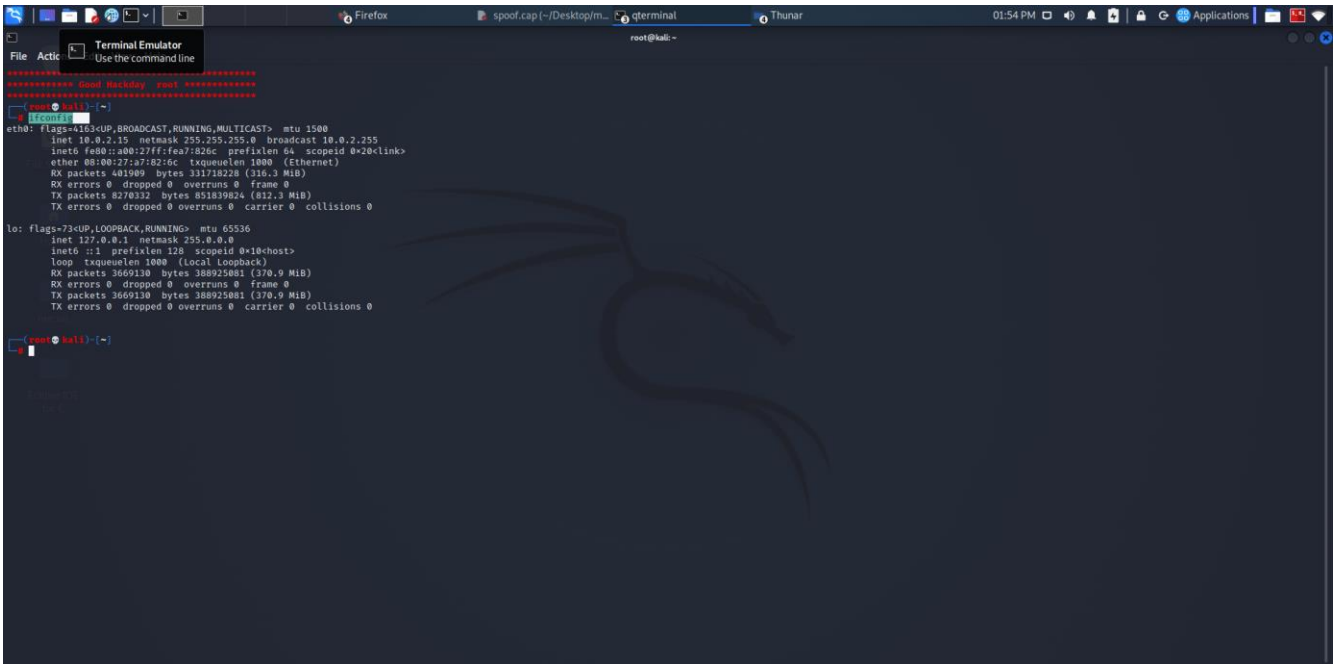


Εικόνα 5: Αρχική μηχανής Kali

Ανοίγουμε το Terminal και χρησιμοποιούμε την ipconfig ώστε να δούμε το network interface όπως φαίνεται παρακάτω:



Εικόνα 6: Terminal Kali



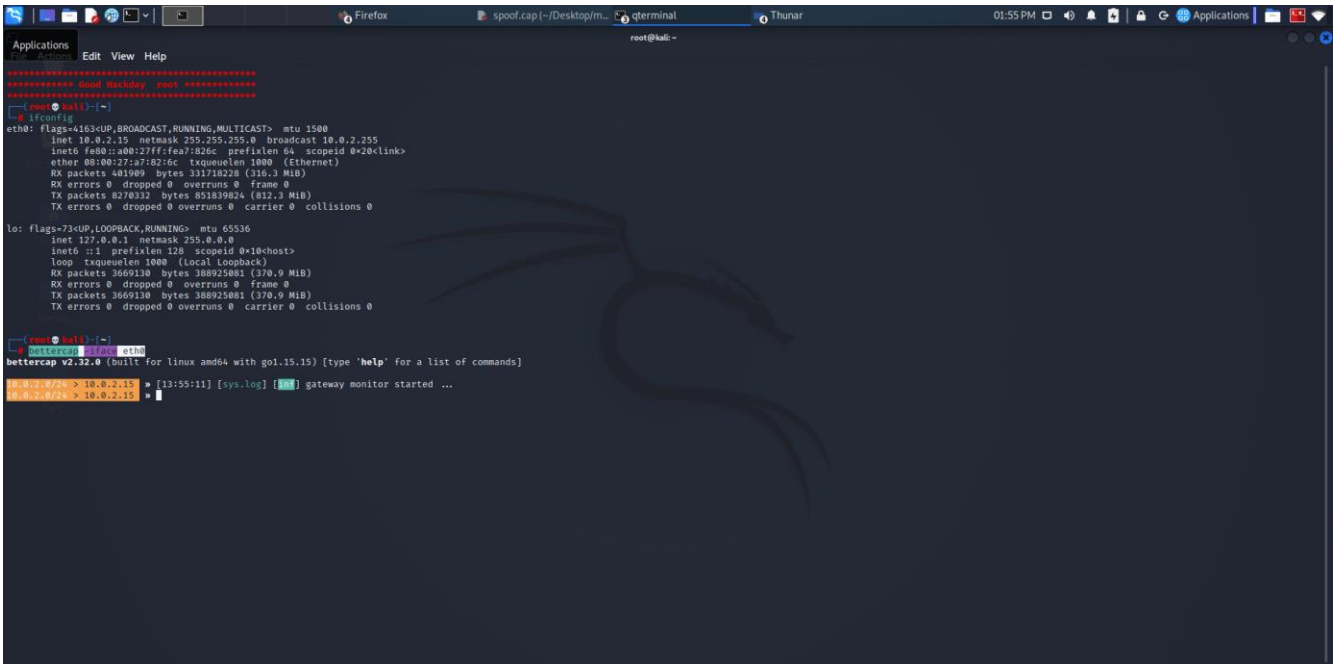
Εικόνα 7: ifconfig για έλεγχο του network interface

Παρατηρούμε ότι το eth0 είναι το network (Ethernet) interface μας.

Πληκτρολογούμε την εντολή

```
bettercap -iface eth0
```

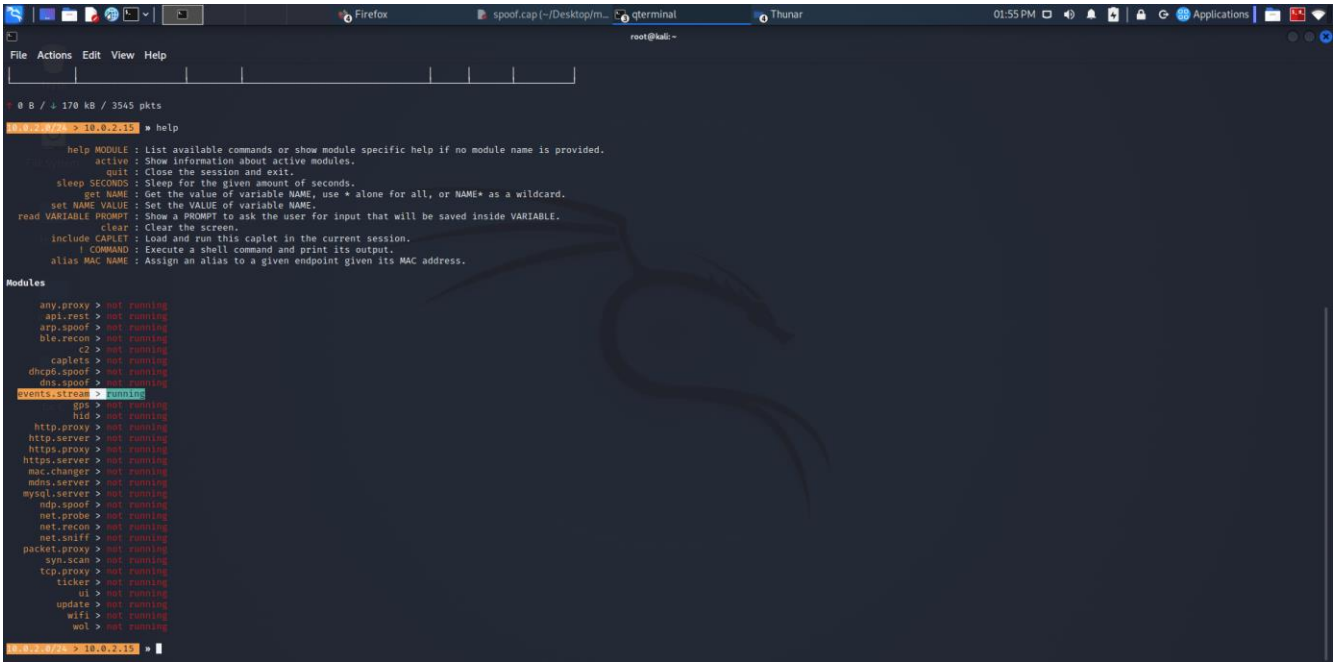
Όπως φαίνεται και στον παρακατω πίνακα



Εικόνα 8: Ενεργοποίηση bettercap
Με την εντολή

```
help
```

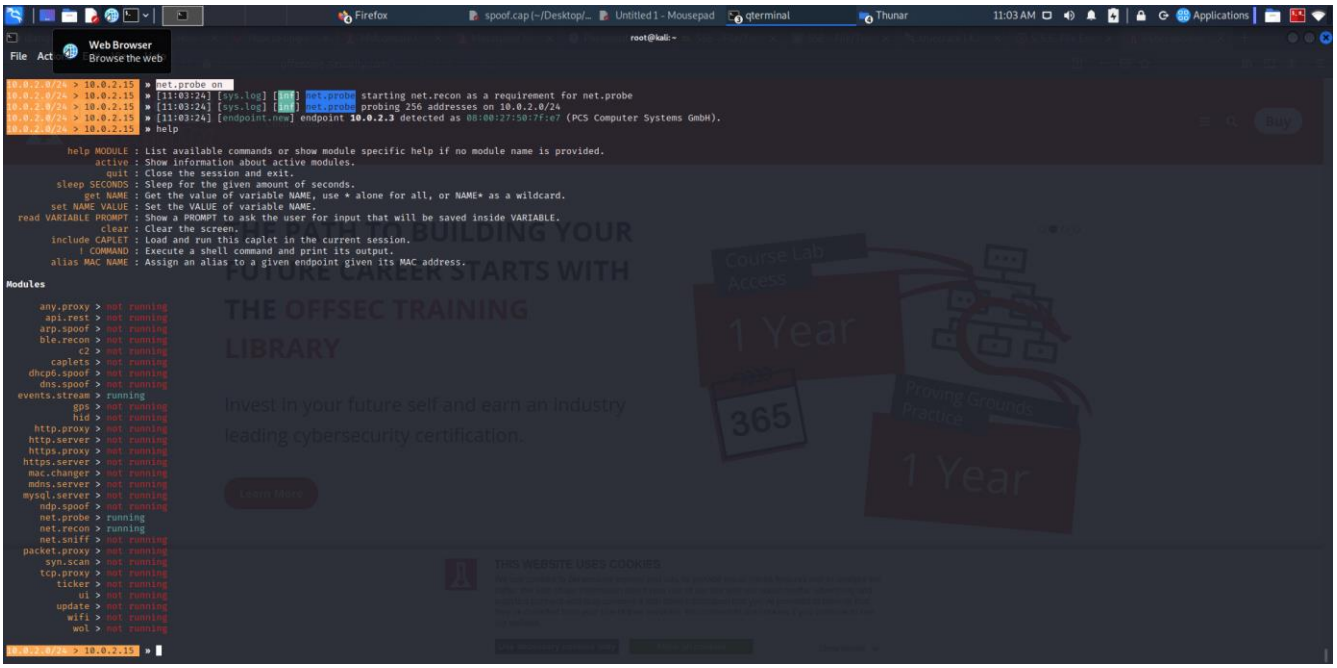
βλέπουμε τις λειτουργίες του bettercap που είναι ενεργές:



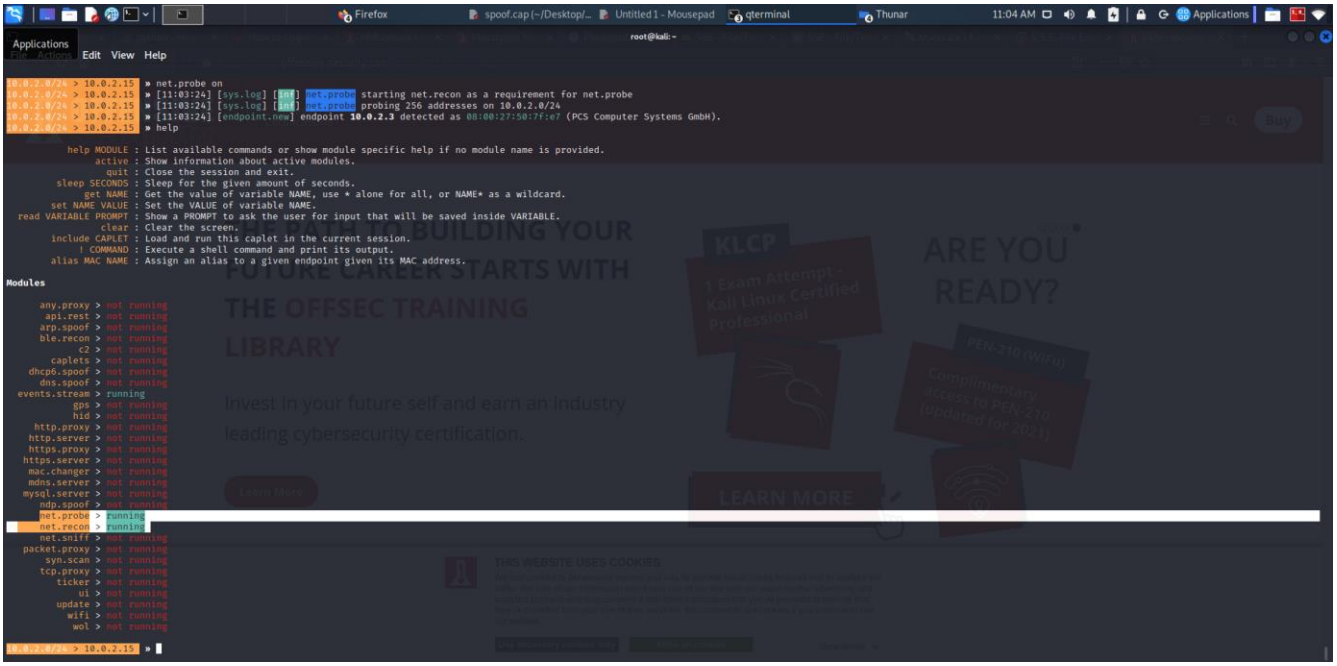
Εικόνα 9: Εντολή help

Το πρώτο μας βήμα είναι να ενεργοποιήσουμε την λειτουργία net.probe μέσω της εντολής

```
net.probe on
```



Εικόνα 10: Ενεργοποίηση net.probe



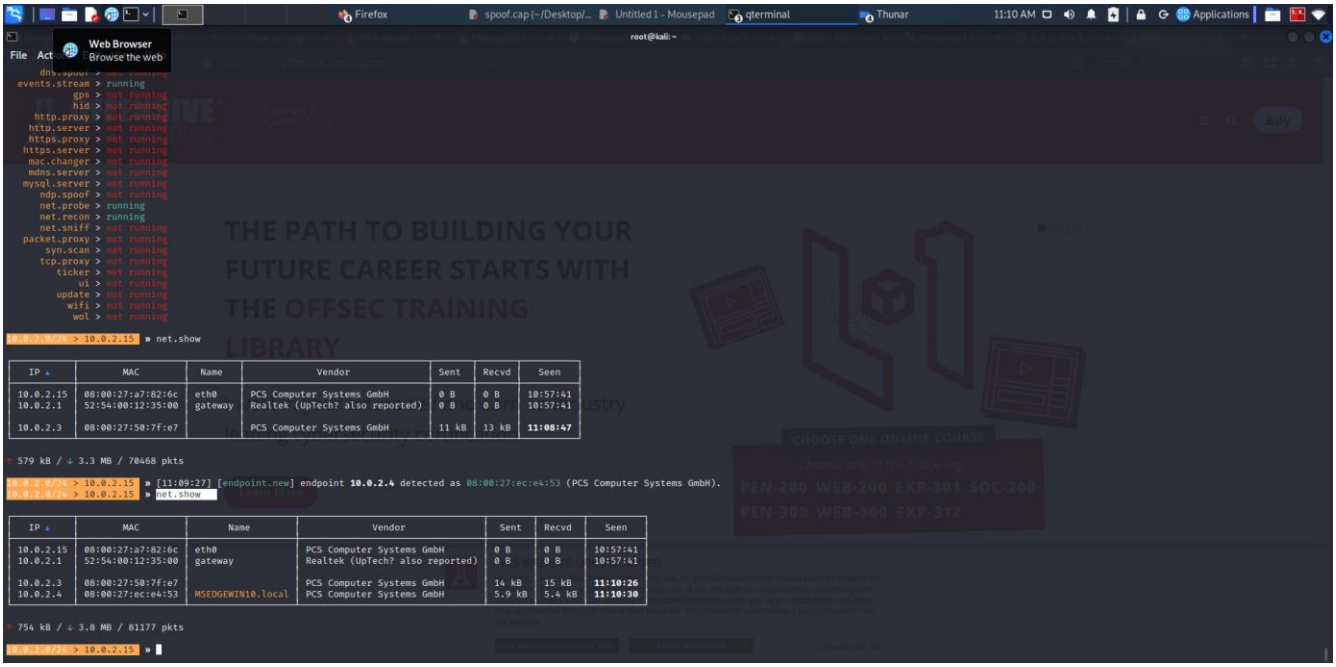
Εικόνα 11: Έλεγχος διαδικασιών μέσω help

Με την εντολή help λοιπόν βλέπουμε ότι ενεργοποιήθηκε η λειτουργία net.probe ώστε να γίνει δυνατή η μετάδοση πακέτων.

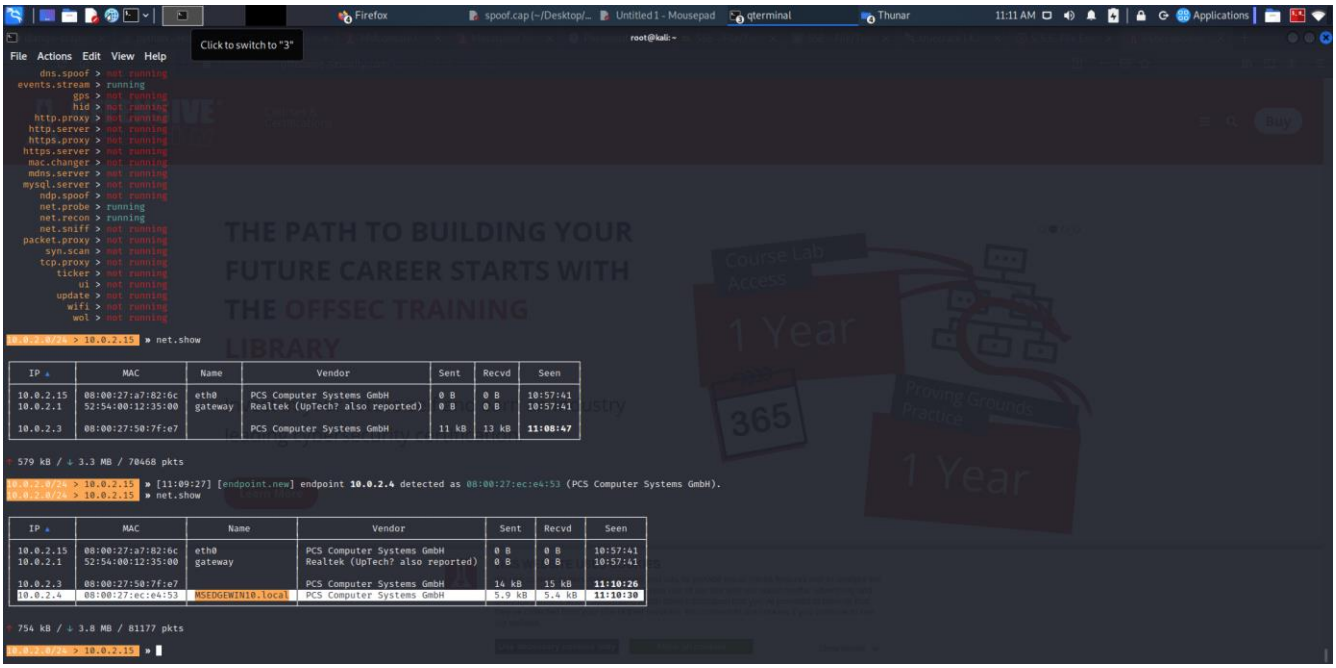
Έπειτα με την εντολή

```
net.show
```

βρίσκουμε το IP και το MAC της συσκευής στην οποία θέλουμε να επιτεθούμε πριν ενεργοποιήσουμε την λειτουργία arp.spoof για να ξεκινήσουμε την επίθεση.



Εικόνα 12: Εντολή net.show



Εικόνα 13: Έυρεση του αποδέκτη της επίθεσης

Παρατηρούμε ότι βρίσκουμε το MAC του IP 10.0.2.4 το οποίο όπως είδαμε ανήκει στην συσκεύη που σκοπεύουμε να επιτεθούμε. Χρησιμοποιούμε μετά τις παρακάτω εντολές για να ρυθμίσουμε την λειτουργία arp.spoof.

Παρατηρούμε ότι το MAC της μηχανής Kali που χρησιμοποιούμε είναι 08:00:27:a7:82:6c είναι το πρώτο MAC που θα εμφανιστεί κατά το net.show και βρίσκεται στο IP 10.0.2.15.

```
set arp.spoof.fullduplex true
set arp.spoof.targets 10.0.2.4
arp.spoof on
```

Η εντολή

```
set arp.spoof.fullduplex true
```

χρησιμοποιηται ώστε να πει στο bettercap ότι θα πρέπει να γίνεται παράλληλα ροή πακέτων από και προς το router και από και προς τον 10.0.2.4.

Με την εντολή :

```
set arp.spoof.targets 10.0.2.4
```

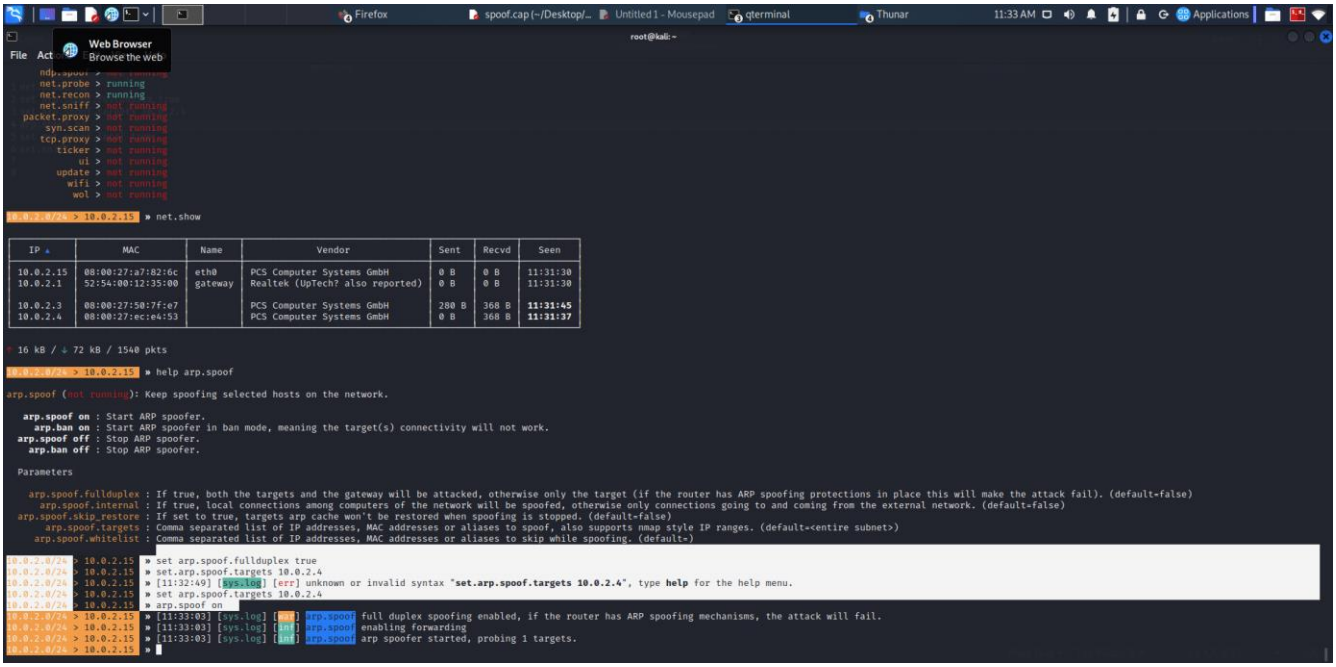
θέτουμε ως στόχο για επίθεση (target) τον 10.0.2.4 (το Bettercap μας δίνει την δυνατότητα να πραγματοποιήσουμε μαζική επίθεση σε διαφορετικά IP θέτοντας απλά περισσότερους στόχους π.χ θα μπορούσαμε να γράψουμε set arp.spoof.targets 10.0.2.4,10.0.2.3 και να επιτεθούμε ταυτόγχρονα στα IP 10.0.2.4 και 10.0.2.3)

τέλος με την εντολή

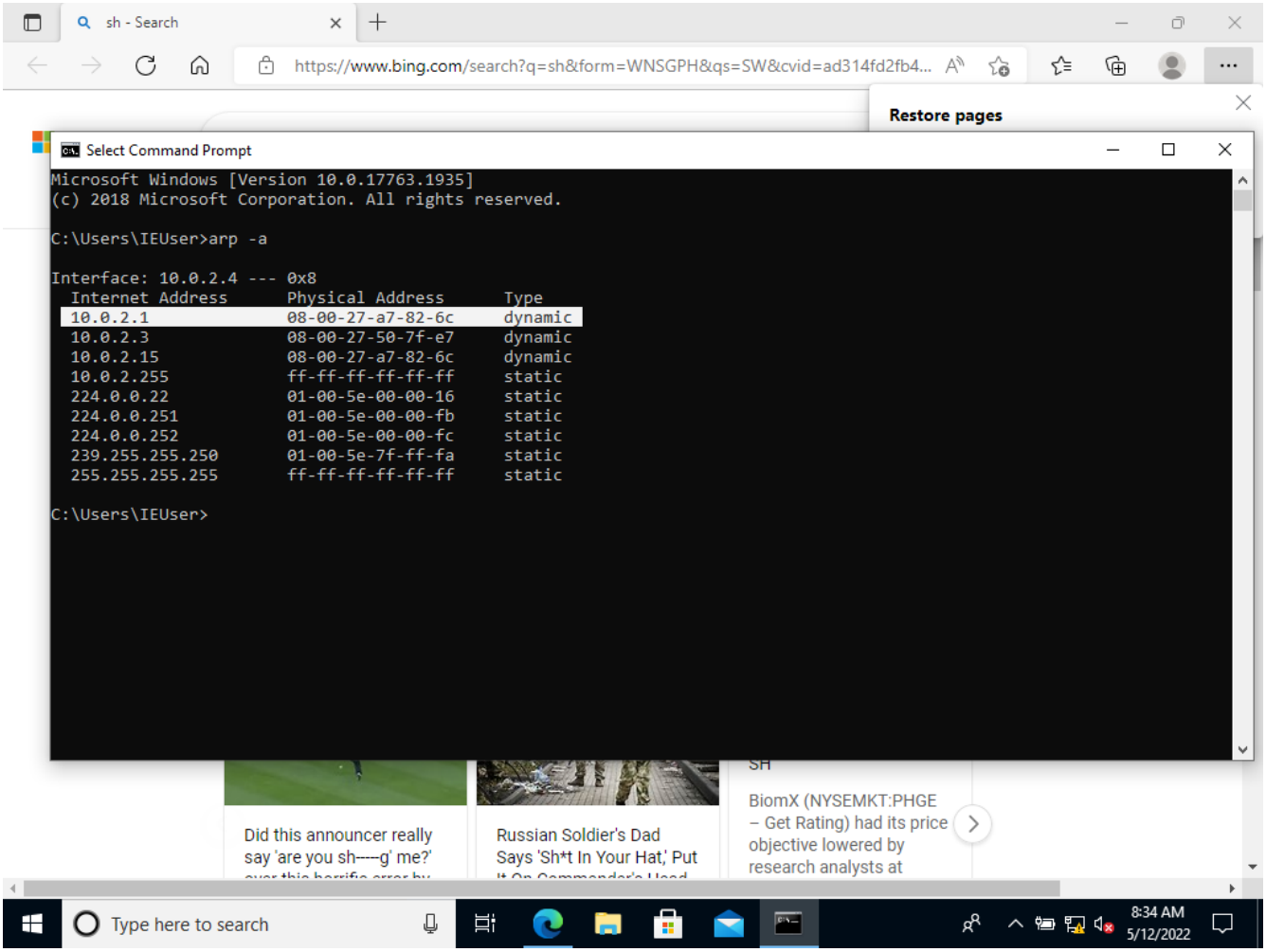
arp.spoof on

ενεργοποιούμε την λειτουργία arp.spoof και έτσι η συσκευή Kali linux λειτουργεί ως ενδιάμεσος των router και windows 10 (10.0.2.4).

Στις παρακάτω εικόνες βλέπουμε την σειρά εντολών καθώς και την διαφοροποίησει στο MAC του router που βλέπει η συσκευή windows 10 μέσω του arp -a.



Εικόνα 14: Ενεργοποίηση και ρύθμιση του arp.spoof



Εικόνα 15: Επιβεβαίωση της αλλάγής του MAC

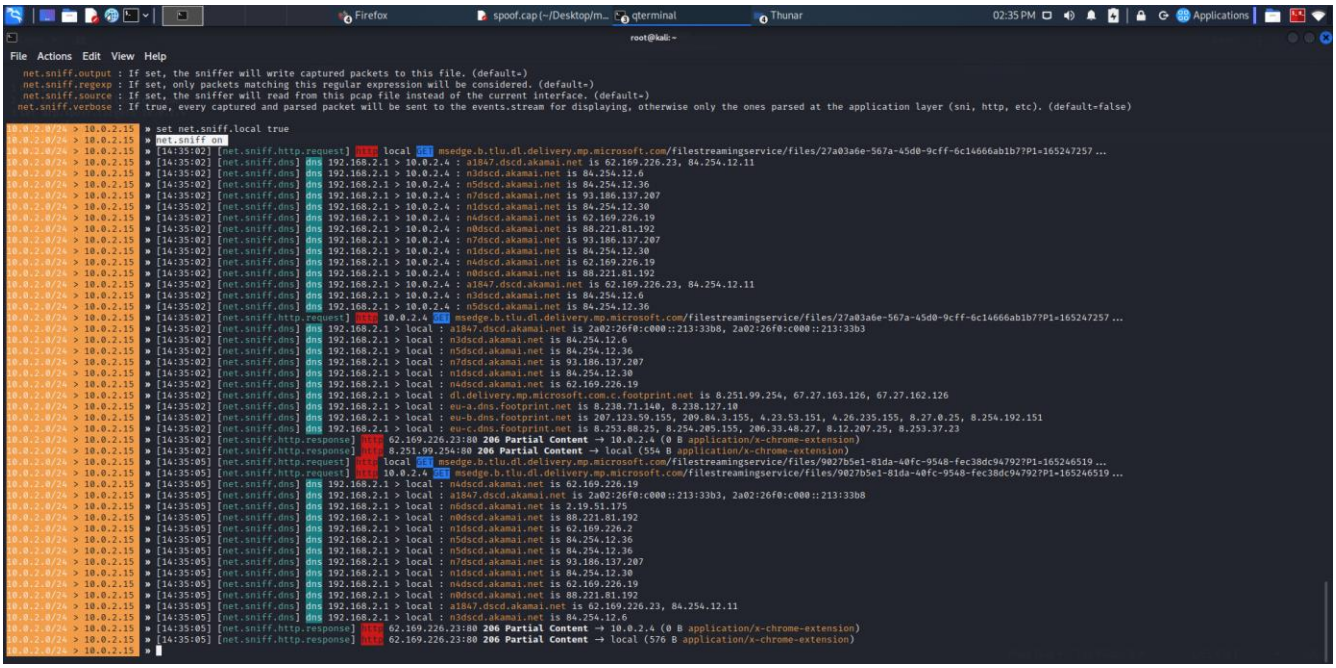
Παρατηρούμε ότι στο IP του router που είναι το 10.0.2.1 (πάντα είναι το πρώτο IP του δικτύου) η μηχανή του windows 10 (δέκτης επίθεσης) βλέπει το MAC του Kali Linux δλδ το 08:00:27:a7:82:6c.

Πλέον οι συσκευές είναι διασυνδεδεμένες και μπορούμε να κάνουμε υποκλοπή των πακέτων της συσκευής windows 10 από την μηχανή Kali.

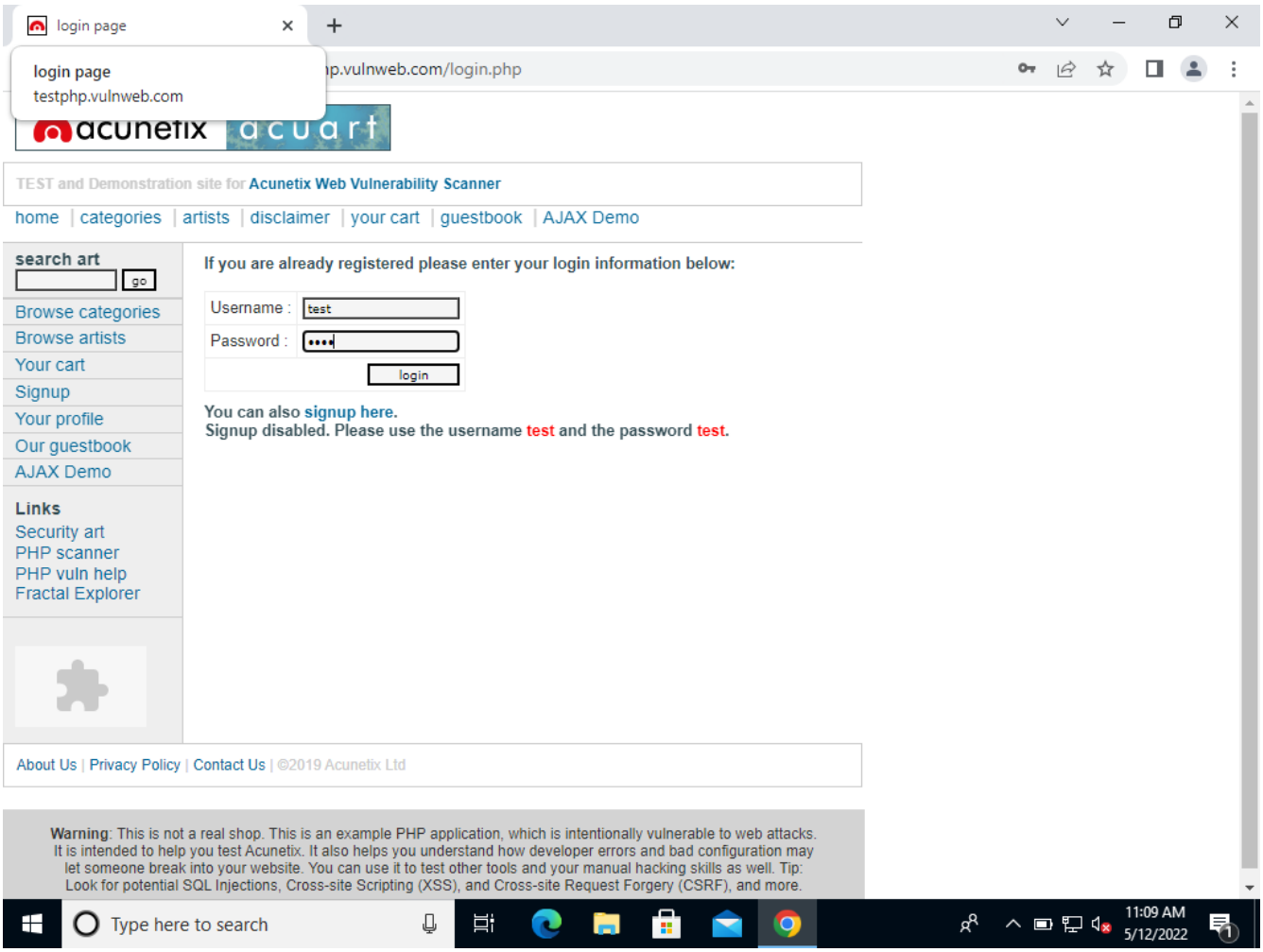
Για να το επιτύχουμε αυτό χρησιμοποιούμε τις εντολές

```
set net.sniff.local true
net.sniff on
```

μέσω της εντολής **net.sniff.local** άν είναι true, θα εξετάσει τα πακέτα που κινούνται από και προς αυτόν τον υπολογιστή, διαφορετικά θα τα παρακάμψει. Με αυτόν τον τρόπο κατβάζουμε τα πακέτα τα οποία ανήκουν στο πρωτόκολλο HTTPS μέσω του εργαλείου sslstrip (η διαφορά του πρωτοκόλου HTTPS από το HTTP είναι ότι τα πακέτα έρχονται κρυπτογραφημένα στο HTTPS αλλά μέσω της διαδικασίας που περιγράψαμε και κάποιων τροποποιήσεων στα πακέτα caplets επιτυγχάνουμε την αποκρυπτογράφησει των αρχείων αυτών και την παράκαμψη του πρωτοκόλλου HTTPS).
Με την ενολή **net.sniff on** ενεργοποιούμε την λειτουργία net.sniff. Στις παρακάτω φωτογραφίες παρουσιάζονται τα στοιχεία της επίθεσης.

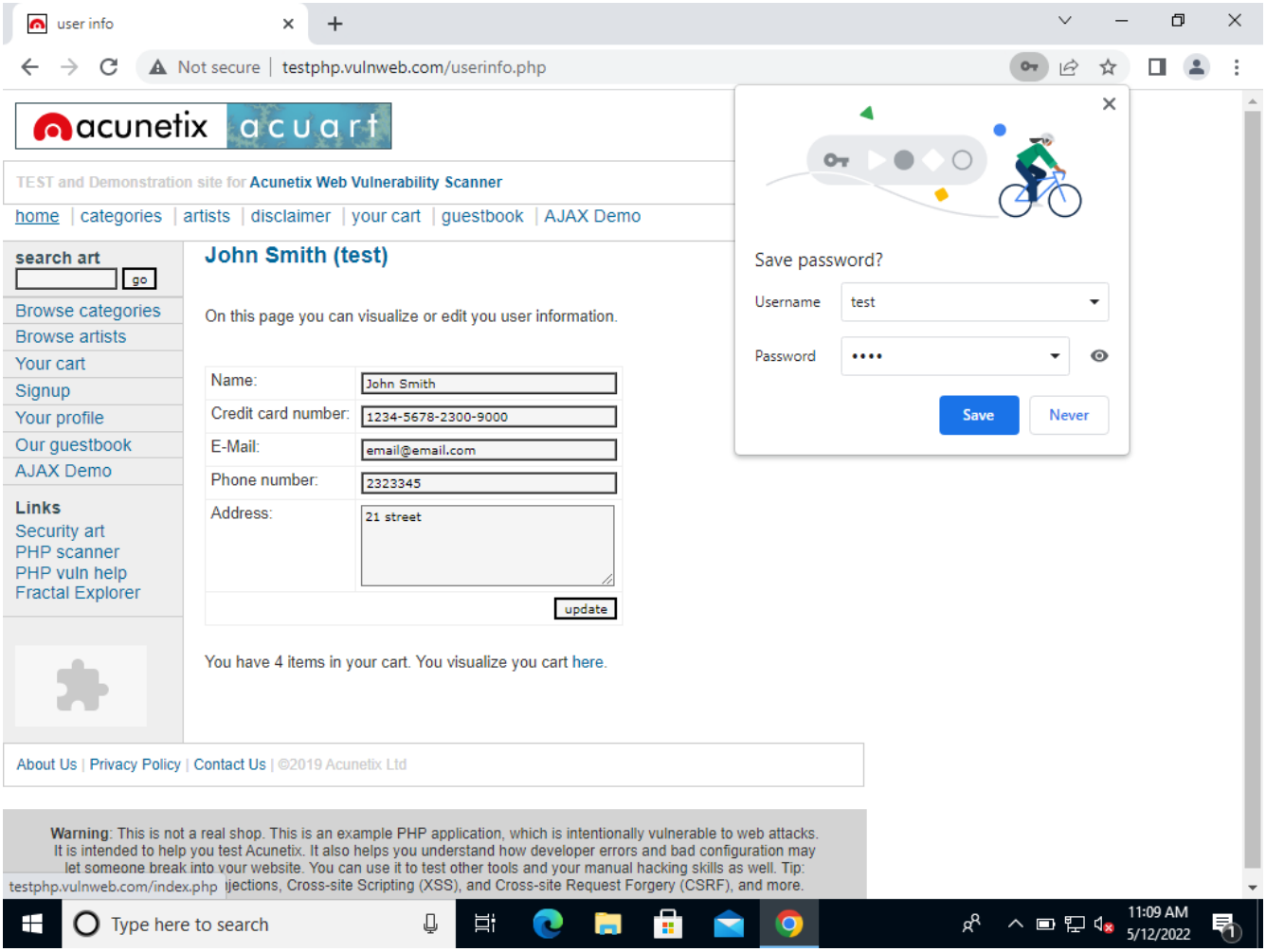


Εικόνα 16: Ενεργοποίηση και ρύθμιση του net.sniff

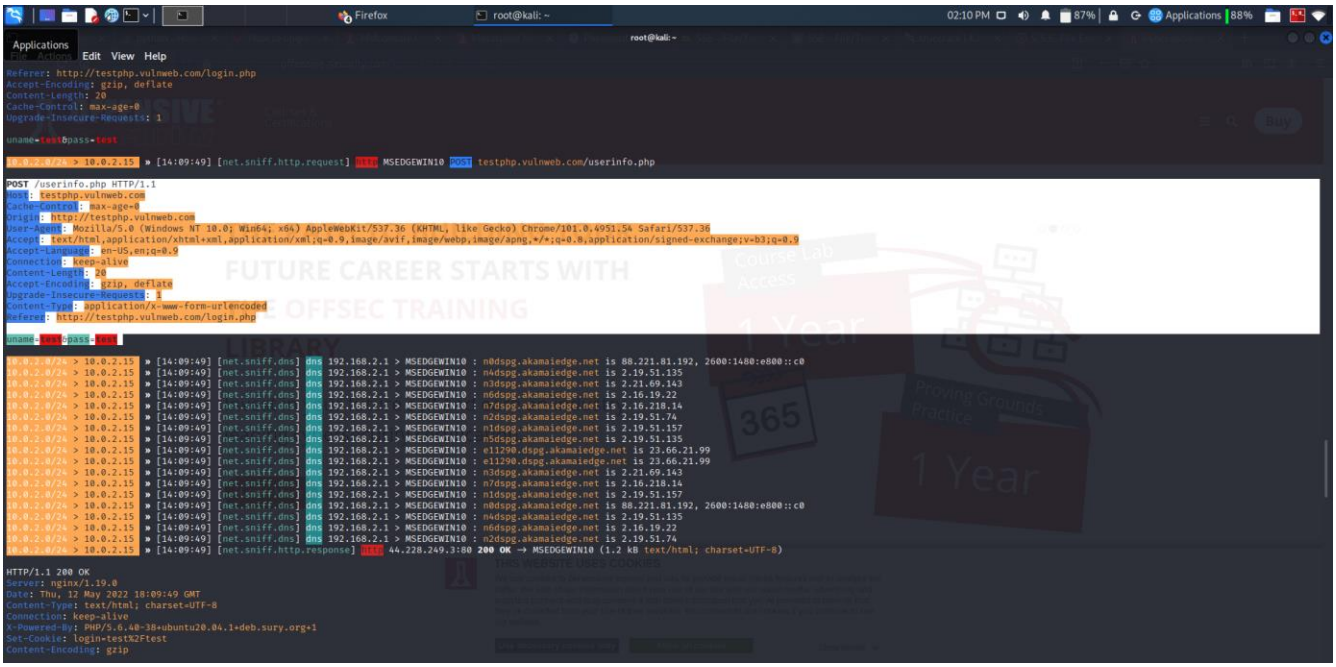


Εικόνα 17: Http ιστοσελίδα στην μηχανή windows 10 για έλεγχο του sniffing

Στην παραπάνω εικόνα φαίνεται η ιστοσελίδα που ανοίξαμε στο windows 10 για να ελέγξουμε την επίθεση σε http πρωτόκολλο στην απο κάτω εικόνα παρουσιάζεται η ιστοσελίδα που ανοίγει αφού πληκτρολογήσουμε το username:test και password:test.



Εικόνα 18: Ιστοσελίδα http Μετά τους κωδικούς για έλεγχο



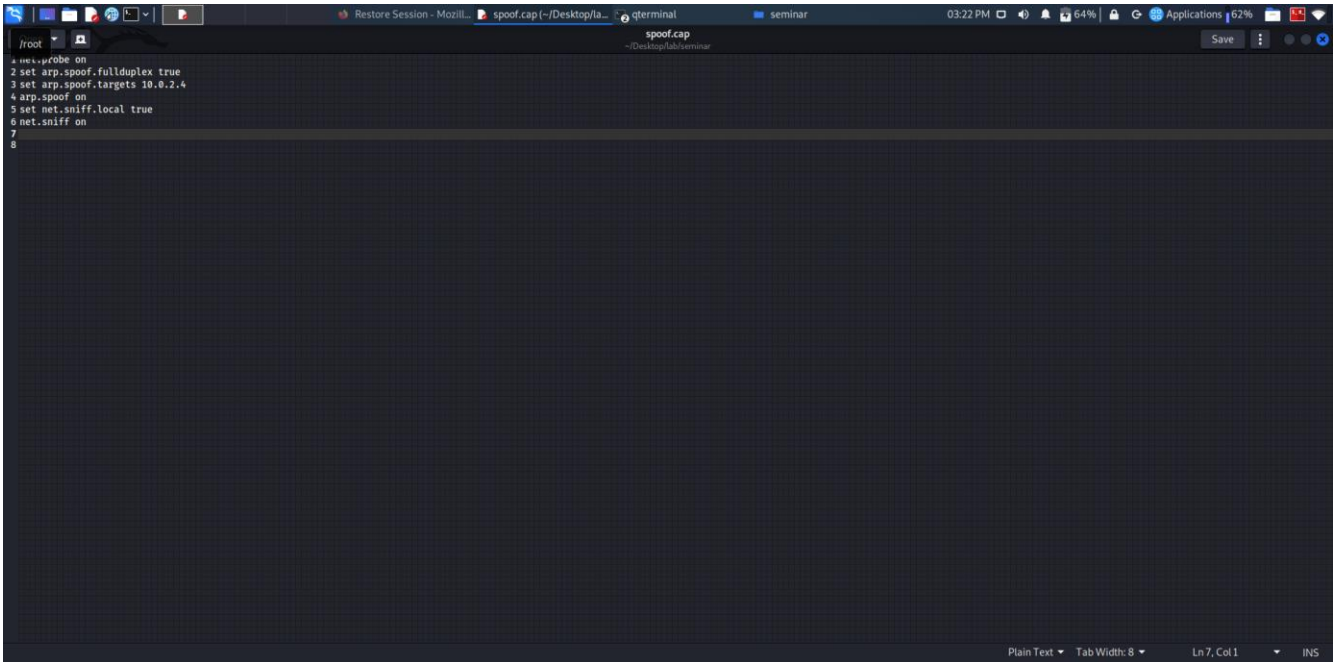
Εικόνα 19: Αποτέλεσμα sniffing

Στην παραπάνω εικόνα βλέπουμε το πακέτο που αναγνώρισε το bettercap κατά την υποκλοπή (sniffing) όπως φαίνεται βλέπουμε και τα username και password.

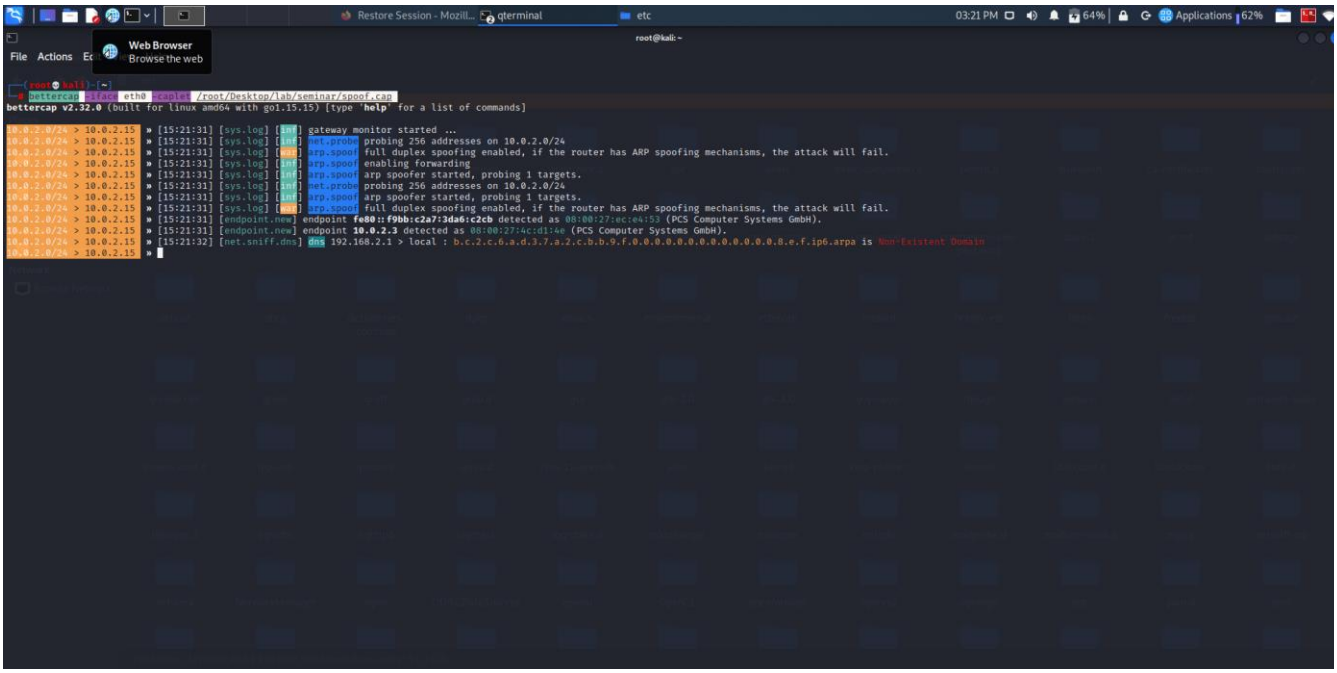
Τέλος μπορούμε να οργανώσουμε τις εντολέςς σε ένα αρχείο .cap, με την παρακάτω διαδικασία:

1. Ανοίγουμε τον text editor
2. Γράφουμε τις εντολές με την σειρά που είπαμε
3. Αποθηκεύουμε το αρχείο στην μορφή name.cap όπου το name το αντικαθιστούμε με οποιοδήποτε όνομα θέλουμε να χρησιμοποιήσουμε
4. Τέλος τρέχουμε την παρακάτω εντολή

```
bettercap -iface eth0 -caplet ~/name.cap
```



Εικόνα 20: Το .cap file



Εικόνα 21: Ενεργοποίηση του Bettercap μέσω του .cap file

Συμπεράσματα

Παραπάνω είδαμε μία απλή υλοποίηση MITM επίθεσης με την χρήση εργαλειών του Debian Linux(Kali) απέναντι σε ένα windows 10 machine. Η έκθεση του σύγχρονου ανθρώπου στο διαδίκτυο και η ανάγκη για χρήση ολοενα και περισσότερων εργαλείων αυξάνεται ραγδαία τις τελευταίες δεκαετίες με αποτέλεσμα ο τομέας της ασφάλειας των δεδομένων σε ψηφιακό επίπεδο να είναι απαραίτητο αγαθό. Καθώς τα σύγχρονα συστήματα γίνονται ολοένα και πιο ισχυρά δημιουργούνται στον αντίποδα αντίστοιχα εργαλεία που χρησιμοποιούν τα κενά (vulnerabilities) που υπάρχουν στο εκάστωτε σύστημα καθώς ως ώρας δεν έχει κατασκευαστεί κάποιο απόλυτα ασφαλές σύστημα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΕΛΛΗΝΟΓΛΩΣΣΗ

Αγγελής Ι., «Διαδίκτυο (Internet) και ποινικό δίκαιο – Έγκλημα στον κυβερνοχώρο (Cybercrime – Internet Crime)», ΠοινΧρ Ν/2000.

Αραβαντινού Βασιλείου Θ., «Η προστασία προσωπικού χαρακτήρα από την αθέμιτη επεξεργασία τους με ηλεκτρονικό υπολογιστή – Συμβολή στην Δικαιοκυβερνητική», Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή 1997.

Βλαχόπουλου Κ., Ηλεκτρονικό Έγκλημα, Εκδ. Νομική Βιβλιοθήκη 2007.

Βλαχόπουλος Κωνσταντίνος, «Ηλεκτρονικό Έγκλημα», Νομική Βιβλιοθήκη, Αθήνα 2007.

Κιούπης Δημήτρης, «Ποινικό Δίκαιο και Internet», Εκδ. Αντ. Ν. Σάκκουλα, 1999.

Κιούπης Δ., «Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα – Κενά και αδυναμίες της ποινικής νομοθεσίας», Υπεράσπιση 2000.

Μυλωνόπουλος Χρήστος, «Ποινικό Δίκαιο – Ειδικό Μέρος», Εκδ. Π.Ν. Σάκκουλας, 2000.

Παπαδόπουλος, Νομικά προβλήματα στην άρση του απορρήτου στην Ελλάδα (Άρση του ανοήτου στην άρση του απορρήτου στην Ελλάδα), ΔiΜΕΕ 1/2005.

Παπανικολάου, Σύνταγμα και Αυτοτέλεια του Αστικού Δικαίου (2006).

ΞΕΝΟΓΛΩΣΣΗ

Barrett, N. (1997). Digital crime: policing the cybernation. Kogan Page.

Blake, K. W., Converse, V. K., Edmark, R. O. N., & Garrison, J. M. (2008). U.S. Patent No. 7,412,723. Washington, DC: U.S. Patent and Trademark Office.

Council of Europe. Octopus Programme. (2005). Organised crime in Europe: the threat of cybercrime: situation report 2004. Council of Europe.

Cyber Crime. Κινητοποιήσεις Ευρωπαϊκής Ένωσης σχετικά με το Ηλεκτρονικό Έγκλημα (https://electroniccrime.wordpress.com/).