

575.6

Capture the Flag

SANS

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP and PMBOK are registered marks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.

SANS

Capture the Flag

© 2019 Joshua Wright & NVISO | All Rights Reserved | Version E02_01

Welcome to SANS Security 575.6. Today you will work individually or as part of a team to complete a series of challenges that closely resemble the responsibilities of a lead mobile device security analyst. This final book in the 575 series describes the challenge you will be facing, provides the Rules of Engagement, and provides a description of how to conduct the exercise. This session will center on the hands-on application of tools and techniques we've discussed throughout the class.

TODAY'S ACTIVITIES

Brief presentation of the workshop describing the scenario and goals for today

Hands-on workshop using guided questions and analysis exercises

Wrap-up at 1:00 for a final debriefing where all exercises will be reviewed

Today's Activities

Today we'll be participating in the hands-on final workshop event. First, we'll start with a brief presentation of the workshop describing the scenario we've outlined and the goals for today. This presentation will take approximately 30 minutes.

Once the presentation is complete, you will start the hands-on workshop using guided questions and analysis exercises. This will take the majority of the time today, stopping at 1:00 p.m. for a final debriefing. During this debriefing, all the exercises will be reviewed and questions will be answered.

TEAMS

Recommend working in a team of three or four people

Can divide questions for analysis within the team or assign to smaller groups

Recommend top-of-the-hour debriefing to discuss findings, challenges for each task

Review your findings with the team for consensus prior to submitting an answer

Teams

For the best workshop experience, we recommend that everyone work in teams of three to four people. Within the team, you can work together with other analysts to answer questions and complete analysis tasks as a single team (each person working on the same question) or divide up the responsibilities of the team with smaller groups to assess some of the more complex analysis tasks in parallel.

We also recommend that each team take a 5–10-minute break at the top of every hour to discuss findings, challenges, and problem areas for each task. Talking a problem out with other people on the team can be a tremendously useful exercise, allowing you to take a step back from the problem while seeking the advice of other analysts.

Prior to submitting the answer to a question or analysis task, we recommend that the team review the answer as a whole and approve the response. This will help avoid the loss of points from the submission of incorrect answers.

YOUR POSITION

You are the chief mobile device security analyst for Gamera Aeronautic Systems Corporation (GAS)

You and your team are responsible for multiple facets of a mobile device deployment

The GAS CSO, Mike Hottaire, has assigned your team several tasks to complete

- Including analysis and penetration testing tasks



Your Position

In this workshop, you are the chief mobile device security analyst for Gamera Aeronautic Systems Corporation (GAS). You and your team are responsible for multiple facets of a mobile device deployment, reporting to the GAS CSO, Mike Hottaire. Mike has assigned your team several tasks to complete, ranging from simple question-and-answer tasks to more complex analysis and penetration tasks.

RESOURCES

You will likely use many of the tools we used in class for the workshop

- Windows and Linux

Internet access is also available with caveats

- We cannot guarantee that the provider network will not go down, but we'll do our best

If you get completely stuck, see an instructor

- No promises for support, but we'll be reasonable, while fair to the other teams

Resources

To complete the analysis tasks Mike has assigned to you, you will use many of the tools we used in the course. You will likely use both Windows and Linux for the analysis tasks.

Throughout the workshop, you will also have access to the internet, with caveats. Notably, we cannot guarantee that the provider network will not go down during the workshop, but we will do our best to ensure you have access to internet search engines and other online resources.

If you and your team get completely stuck on an analysis exercise, please see an instructor for assistance. We are not promising to give you hints or answers, but we'll be reasonable in providing guidance while being fair to the other teams.

WORKSHOP PLATFORM

Mike Hottaire has submitted your analysis tasks in a tiered hierarchy

- Achieve a minimum score for the level to gain access to the next tier

We'll be using the NetWars platform for questions and scoring

- Designed by the Counter Hack Challenges team, www.counterhackchallenges.com
 - Ed Skoudis, Tom Hessman, Jake Medin, Joshua Wright, Jeff McJunkin, and Daniel Pendolino

Workshop Platform

GAS CSO Mike Hottaire has submitted the analysis tasks you need to complete in a tiered hierarchy. You'll start with Level 1 questions, moving up to the next level after achieving a minimum score defined for each level.

Throughout the workshop, we'll use the NetWars platform for the delivery of questions and validation of responses, as well for scoring each team. The NetWars platform was designed by the Counter Hack Challenges team (www.counterhackchallenges.com) consisting of Ed Skoudis, Tom Hessman, Jake (Tim) Medin, Joshua Wright, Jeff McJunkin, and Daniel Pendolino.

NETWARS SCORING

All scoring is maintained by the scoring server located at <https://netwars-e02.sec575.org>

Each level has a set of questions

- Flag, literal, or multiple-choice questions

Flags are taken from various challenge questions

- Sometimes the flag is preceded with "flag:"
- Sometimes the flag is an answer you discover
- Read the questions carefully for guidance

Know a SHA1 hash:
40 characters in
length, 0–9 and a–f

```
da39a3ee5e6b4b0d3255bfef95601890afd80709
```

NetWars Scoring

All scoring in the workshop is maintained by the scoring server at <https://netwars-e02.sec575.org>. After logging into the scoring server, you will see the questions for your level achievement and be able to submit your responses. Your answers to the questions will gain or cost you points. You can also monitor the score of other teams from the scoring server as well.

Each level in the workshop has a set of questions you will answer. Some questions will be multiple choice, but many will require an answer that represents a literal value (such as a word or a group of words) or a flag. Flags are taken from the various challenge questions, sometimes preceded with the string "flag:". Sometimes a flag is a string or other answer you discover by completing the analysis task. Read each question carefully for guidance on what should be submitted for the answer.

Some exercises will require you to find a flag value in a file, program, or other network resource. Flags are in SHA1 hash format, as shown on this page. The SHA1 flags are 40 characters in length, consisting of hexadecimal characters (0–9 and a–f).

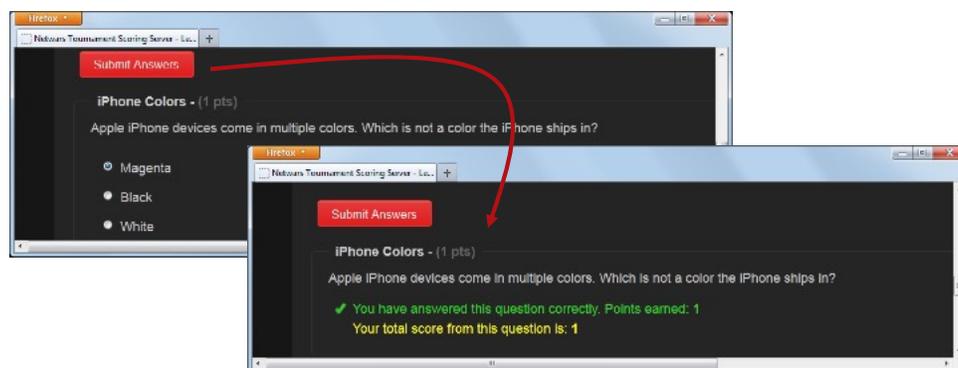
SAMPLE QUESTION (1)

Multiple questions are listed per level

Answer any question and click Submit

- Unanswered questions are ignored

Order of answers changes for multiple-choice questions!



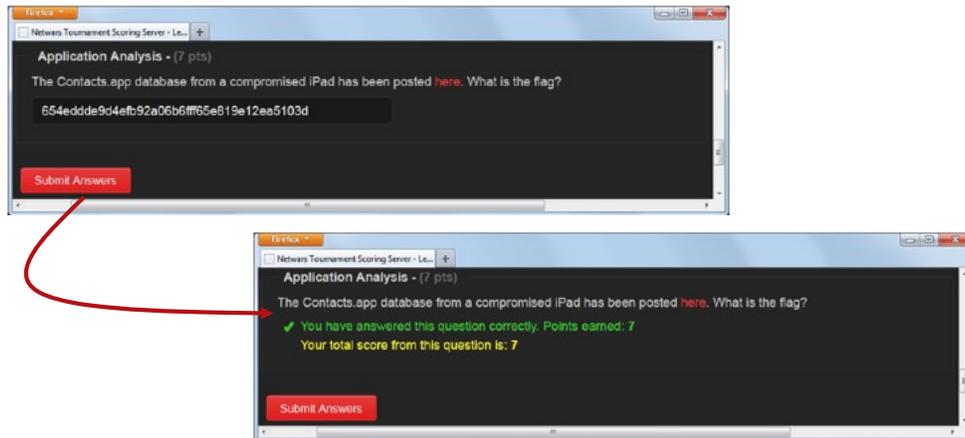
Sample Question (1)

This page has an example question from the NetWars scoring engine. The participant reviews the question and selects the answer he or she thinks is correct. At any time, there will be multiple questions that are accessible; answer the question and submit your answer by clicking the "Submit Answers" button. You can answer one or more questions each time you click submit; questions that have not been answered are ignored by the scoring engine, allowing you to answer them at a later time.

Note that for multiple-choice questions, the order of answers will change each time the page is retrieved (and for different people on the same team).

SAMPLE QUESTION (2)

Some questions will ask for a flag (40 characters) or a literal value



Sample Question (2)

The sample question on this page is a flag question where the participant is challenged to gather data from a linked resource and identify the flag. Remember that flag values are 40-character SHA1 hashes, as shown here.

Other questions will require a literal value, such as one or more words, an IP address, or any other string value.

POINT VALUE OF ANALYSIS TASKS

Each of Mike Hottaire's analysis tasks or questions is given a number of points

- 1 to 15 based on difficulty

Answer correctly to get the points

- No penalty for one wrong guess (mulligan)
- Decrement one point for each additional wrong guess (no more than three)

Please don't brute force answers

- It's a waste of time, and Mike Hottaire will think poorly of you during your next compensation review

Point Value of Analysis Tasks

Each of Mike Hottaire's analysis tasks or questions is assigned a number of points between 1 and 15 that are rewarded for a correct answer. Answer a question correctly to gain the point value assigned to the question.

The first wrong answer for each question will not decrement points. Additional wrong answers for each question will decrement one point for each incorrect response, up to three points total.

Please don't attempt to brute force the answers. It is not permitted within the scope of this workshop and, furthermore, will make Mike Hottaire think less of you.

RULES OF ENGAGEMENT

No denial-of-service attacks

No "dangerous" attacks

- Don't risk bringing down our machines!
- Do not change the configuration of target machines (hardening or weakening)
- If you gain access to a machine, don't delete items or plant false flags

You need to help keep the infrastructure running

Attack only the target infrastructure

- You are not allowed to attack other testers
- No attacks against other team scores or account logins

Rules of Engagement

During this workshop, participants are forbidden from performing denial-of-service attacks or otherwise dangerous attacks that threaten the stability of the systems supporting the assessment. Do not risk bringing down our machines and avoid excessive system use (such as excessive disk I/O or CPU-intensive activities). If you gain access to a system, don't delete items or plant false flags on the system. We need your help to keep the workshop infrastructure running!

In the workshop, you are allowed to attack only the target infrastructure identified in the question presented by the scoring server. You are not allowed to attack other testers on your team or other teams. You are not allowed to attack the scoring server, including any attempts to access other team scores or account logins.

MONITORING SERVICES

We will monitor services throughout the day

- Some systems will come down periodically for maintenance ... this happens in real life too
- We will announce systems going down to let you know that they will be offline temporarily

If you notice a service go down, let the course instructor know

We will attempt to resume service as quickly as possible

Monitoring Services

Throughout the day, we will monitor services supporting the workshop to ensure their availability. We might need to take systems temporarily offline to restore their functionality and will notify the workshop participants accordingly.

If you notice a service that goes down, let the course instructor know. We will attempt to resume service as quickly as possible.

WINNING

A perfect game is 100 points

- The first team to 100 points or the team with the highest score at the end of the game wins

Be careful about answering questions too quickly and losing points

Confer with your teammates to validate answers to avoid costly mistakes

Winning

To win the SEC575 challenge, your team must be the first to achieve a score of 100 points (a perfect game) or be the highest scoring team at the end of the game.

In past challenges, some teams racked up points very quickly, but they might have lost a few points for wrong answers. Even when teams finish early, they are not automatic winners because teams who finish later with a higher score (closer to perfect) can be declared the winner.

Be careful about answering questions too quickly because this can easily lead to point loss. To avoid costly mistakes, confer with your teammates to validate your answers before you submit them.

FORMYOURTEAMS

Form your teams (up to four people per team) and choose a team name

Each team will be given an account to log in to the NetWars scoring server

- Decide to share or control access to the scoring server as a team

<https://netwars-e02.sec575.org>

Form Your Teams

In a minute, you will be asked to form your teams (no more than five people per team) and choose a PG-appropriate team name. Each team will be given an account to log in to the NetWars scoring server at the URL on this page.

As a team, decide whether you will share the login credentials for the scoring server with the team or appoint one person who is responsible for submitting answers and distributing analysis tasks.

ANY QUESTIONS?

Ask any questions now prior to the opening of the scoring server

If there are no further questions, let one representative come up from each team

We will announce when the scoring server is officially open

Have fun, take a break when you need it, and enjoy

Any Questions?

At this point, ask any questions prior to the opening of the scoring server. Once the question and answer phase is done, one representative from each team should see the instructor for credentials to the scoring server while the rest of the team prepares its systems for analysis. We will make an announcement when the scoring server is officially open.

During the workshop, have fun and enjoy. If you need to take a break, get a beverage or a snack; if you need to walk around and think for a few minutes, please feel free, but be respectful of the other teams and do not disturb their analysis work.

This page intentionally left blank.

Index

/data/data	2:66, 4:136
oxCAFEBABE	3:19

A

adb backup	2:81
adb devices	1:92, 2:59
adb install	1:92, 4:42, 4:139, 5:129
adb logcat	1:92, 2:79-80, 4:13, 4:127, 4:130
adb pull	1:92, 3:7, 3:81
adb push	1:92, 2:55, 2:60, 4:67, 5:129
adb shell	1:92, 1:112, 1:118, 2:59-60, 4:67, 4:139, 5:129
adb uninstall	1:92, 4:42, 4:139
Address Space Layout Randomization	1:31, 1:35, 1:37, 1:68, 3:14
am force-stop	1:118
Android Account Isolation	1:58
Android Activity	1:119, 4:126, 5:119
Android App Manipulation	1:3, 4:2, 4:27-29, 4:43, 4:47
Android App Signature Verification	1:67
Android Application Files	2:65
Android AVD Manager	1:86, 1:88-89
Android Backup	2:2, 2:81-82, 2:84
Android Backup Access	2:82
Android Classes.dex	2:67, 3:8-9, 3:78, 3:89-90, 3:97, 4:40-41
Android Debug Bridge	1:89, 1:92
Android Debug Detection	4:137
Android Emulator	1:86, 1:90-91, 4:27, 5:129, 5:145
Android Fake Installers	2:129
Android Filesystem Files	1:92, 2:64-65, 2:68, 2:77, 3:89
Android Intent	1:106, 4:2, 4:11, 4:13, 4:15, 4:91
Android Key Store	4:135-136, 4:139
Android Normal Permissions	1:61, 1:63-64, 1:115, 2:134, 5:120
Android Nougat	1:52, 5:96-97, 5:99-100
Android Obfuscation	3:47, 3:49-54, 3:69-72, 3:102, 4:138
Android Platform Releases	1:52, 1:91
Android Ransomware	2:133
Android Runtime (ART)	1:54, 1:61
Android SDK Manager	1:87, 1:92

Android Smart Lock	2:20-21
Android Software Updates, Fragmentation	1:8, 1:51-52, 1:57, 1:67, 1:71-78, 1:80-81, 2:48-49, 2:52, 2:55, 2:113, 2:128, 2:137, 2:143, 2:147, 3:32, 3:61-62, 4:100, 5:132, 5:135, 5:144
Android Studio	1:86, 1:89, 3:49, 3:55-56, 3:59, 3:61, 3:64, 3:67, 3:69-70, 3:72, 3:93-94, 4:137-138
Android Tech Specs	1:51
Android WebView Vulnerability	1:8, 4:136
Android wpa_supplicant.conf	2:68
AndroidManifest.xml	1:59-60, 1:64, 1:117, 2:67, 2:72, 2:131, 3:8, 3:56, 3:78, 3:89-90, 3:97, 4:31, 4:37, 4:40-41, 4:131, 4:137, 5:114, 5:119
Apkmonk	3:7, 3:78, 3:89, 3:96
Apktool	3:101, 4:31, 4:37-38, 4:43, 4:77, 5:96, 5:131
Apple App Store	1:10, 1:39, 1:42-43, 1:45, 1:107, 2:33, 2:41, 2:93, 2:102, 2:127, 2:140-141, 2:150, 3:16-17, 3:77
Apple Pay	2:107
Apple System Log (ASL)	1:43, 4:21, 4:106
Apple Transport Security (ATS)	4:20, 5:84, 5:107
Application Signing	1:67
Application System Log (ASL)	1:31, 1:35, 1:37, 1:43, 1:68, 3:8-9, 3:14, 4:31-32, 4:106, 4:120
archtype.c	3:20
ARP Spoofing	5:28-32, 5:37, 5:39-40, 5:48
Aurora Feint	1:42
AXMLPrinter2	2:72, 4:137

B

backup.ab File	2:81-82
Baksmali	4:31, 4:37
BigBoss Recommended Tools	2:43
BIND_DEVICE_ADMIN permission	1:65-66
Bing Translate	1:107
BlackBerry App World	2:127
Bluetooth Low Energy	1:8
Bold Like Us (BLU)	2:51-58
Boot ROM	1:31, 1:53, 1:71, 2:34, 2:53
Bring Your Own Device (BYOD)	1:8, 2:26, 2:146

Browser User-Agent	1:105
Burp Decoder	5:21
Burp Repeater	5:104
Burp Suite	5:53-56, 5:60, 5:87-88, 5:92, 5:103, 5:105
Burp Suite, Match and Replace	5:56-57, 5:60, 5:103
Burp Suite, Transparent Proxy	5:53-54, 5:60, 5:103
Busybox	4:95, 4:134

C

Cain	5:31-37, 5:42, 5:47-48, 5:70, 5:79, 5:103
Captive Portal	5:98
Certificate Pinning	4:65-66, 4:79, 4:86, 4:95, 4:108-112, 5:59-60, 5:81, 5:86, 5:92-93, 5:100-102
Certificate Validation	1:39, 1:67, 2:34, 2:146, 4:107-112, 4:124, 4:132-133, 4:140, 5:65, 5:69, 5:79, 5:86, 5:99, 5:102, 5:107, 5:114
CFBundleUrlSchemes	4:104
CFNetwork.framework	3:22
ChatterBotFactory	3:84
Chrome APK Downloader	3:7
Chrome URL Handler Vulnerability	1:105
Client Side Injection Attacks	5:124, 5:136
config.xml	5:96, 5:99
ContactsContract	3:12
Container MDM	5:135
Cross Site Scripting (XSS)	1:105, 5:106, 5:124, 5:136
Cycript	4:49-53, 4:55-60, 4:62-63, 4:121-122
Cydia	2:35-39, 2:41-42, 2:44, 4:21, 4:48-50, 4:62, 4:67, 4:110-111, 4:121, 5:92
Cydia Substrate	4:48-50, 4:62, 4:110-111, 4:121

D

Dalvik Bytecode	3:47, 3:82, 4:30-38, 4:43
Dalvik Executable	1:51, 1:54-56, 2:65, 2:67, 3:8-10, 3:70-71, 3:78, 3:89-90, 3:97, 4:29-30, 4:40-41, 4:77
Dalvik Instructions	1:54-56, 3:10, 3:25, 3:47, 3:70, 4:29, 4:34-35
Dalvik Runtime	1:54-56, 1:68, 4:30, 4:32-36, 4:43

Data Execution Prevention	1:31, 1:35, 1:37-38, 1:68
dd (Utility)	1:37, 2:82, 2:111
Device Passcode	1:65, 1:70, 2:6-7, 2:19, 2:26, 2:109
DEX2JAR	3:10, 4:77
Digital Millenium Copyright Act (DMCA)	2:30, 3:5
Dropbox Application	2:74, 2:103, 2:137
Drozer Framework	4:2, 4:6-13, 4:124, 4:126-128, 4:131, 4:137
Dumpdecrypted	2:140, 3:18, 4:120

E

ec_gid, ec_uid	5:70
Eclipse IDE	4:37, 4:137-138
Encryption	1:31, 1:40, 1:70, 2:71, 2:73, 2:75, 2:78, 2:81, 2:86, 2:89, 2:101, 2:117, 2:133, 2:140, 3:18, 3:27, 3:69, 3:108, 4:77, 4:119, 4:135, 4:138, 5:17, 5:59-60, 5:64, 5:83-84, 5:94, 5:113
Encryption, Android	1:70, 2:71, 2:73, 2:75, 2:78, 2:81, 2:133, 3:27, 3:69, 3:108, 4:77, 4:135, 4:138, 5:59, 5:83, 5:94, 5:113
Encryption, iOS	1:31, 1:40, 2:101, 2:140, 3:27, 3:108, 5:17, 5:83-84
Enterprise Certificate, Apple	2:140-142
Ettercap	5:31, 5:36-48, 5:51-52, 5:54, 5:69-71, 5:73, 5:76-79, 5:103
Evil Bank	1:5, 1:27
Executable and Linkable Format (ELF)	1:51
ext4 filesystem	1:51

F

Facebook	1:60, 1:100, 1:102-103, 2:69, 2:98, 2:134, 2:138, 3:91, 4:20, 4:22, 4:24, 4:105-106, 4:125, 4:131, 5:76, 5:121-122, 5:125
FanReact	3:96-102
Filesystem Application Modeling	3:4
Find My iPhone	2:23
Foncy Malware	2:130-132
Forbes	1:8, 2:8, 2:15
Forensics	2:8, 4:116, 5:18, 5:113, 5:146

ForeSee (vendor)	4:126, 4:128
Four Goats, OWASP Project	4:9-13

G

gdb	1:89, 2:43, 3:18, 4:22, 4:29, 4:48, 4:120-121
getSubscriberId	3:9
Google Bouncer	2:144, 5:124
Google Play	1:10, 1:52, 1:87, 1:90, 2:60, 2:127-128, 2:133, 2:137, 2:143-144, 3:7, 3:41, 3:77, 3:81, 4:137, 4:139, 5:95, 5:124
GPWN Mailing List	5:143, 5:146

H

Hacking Team Malware, iOS	3:40, 5:113-114, 5:132
Hashcat	2:116
Hopper	3:26
HTTP Parameter Tampering	5:103
HTTP Transaction Replay	5:103-104
HTTPS Intercept	5:60, 5:86

I

iBoot	1:31, 2:34
iCloud	2:23, 2:107-108, 5:17
iCloud, Keychain	2:107
Ida Pro	3:26, 4:69, 4:104
Identity Management	1:14
IEEE OUI	2:106, 3:80-82, 3:84, 3:86-87, 5:19, 5:22
iExplorer	2:114-115, 4:115
iFunBox	2:44, 4:110, 4:112, 4:115
Info.plist	2:97, 2:109-110, 2:142, 4:104, 5:84
Instagram Application	5:83, 5:125
International Mobile Equipment Identifier	1:60, 2:109, 3:12, 4:121, 5:21-22
iOS Action Extension	1:106-107, 4:104
iOS Address Book	1:42
iOS App Extensions	1:106
iOS App Manipulation	1:3, 4:2, 4:27-28, 4:47-48, 4:63, 4:110

iOS Application Bundle	2:102
iOS Backup, Directory	2:108-109
iOS Data Protection	2:86-88
iOS Debug Detection	4:120
iOS Dictionary Data	2:106
iOS Document Provider Extension	1:106
iOS Filesystem	2:101, 3:17
iOS Filesystem Files	2:101, 3:17
iOS Keyboards	1:45
iOS Keychain Accessibility	2:90, 4:118
iOS Method Swizzling	4:58-59, 4:61-62
iOS Passcode Bypass	2:7
iOS Phone Number	1:43, 2:93-94, 2:105, 2:109, 2:138, 4:133
iOS Photo Editing Extension	1:106
iOS Privilege Model	1:41
iOS Screen Snapshots	2:104
iOS Screenshots	2:74, 2:104, 2:142, 4:23
iOS Share Extension	1:106-107, 4:104
iOS Simulator	1:85-86, 1:93-94
iOS Software Maintenance	1:46
iOS SpringBoard	2:44, 2:142, 4:49, 4:111, 5:92
iOS Tech Specs	1:30
iOS Today Extension	1:106, 2:90, 4:118
iOS Touch ID	2:14, 2:107, 2:117, 4:86, 4:95
iOS Visual Voicemail	2:105
iPhoneDevWiki	1:101, 4:55
iptables	5:51-54, 5:60, 5:70, 5:95, 5:103
iTunes	1:46, 2:8, 2:37-38, 2:45, 2:101-102, 2:107-109, 2:111, 2:114, 2:116-118, 4:118, 5:12
itunes_backup2hashcat	2:116

J

Jabberwacky	3:83-85
Jadx	3:10-12, 3:27, 3:47, 3:50, 3:52, 3:54-57, 3:59, 3:71-72, 3:82-83, 3:93, 3:108, 4:105, 4:124, 4:128, 4:131, 4:136, 4:138
Jailbreak	2:5, 2:28, 2:30-37, 2:39-41, 2:44-45, 2:91, 2:127, 2:141, 2:145, 2:150, 4:18, 4:28, 4:54-55, 4:61, 4:67, 4:84, 4:110, 5:134
Jailbreak Detection	4:21, 4:28, 4:61, 4:65-66, 4:79
Jarsigner	4:40-41, 4:139, 5:96, 5:131

JD-GUI 3:10, 4:30

K

keychain_dumper 2:91, 4:23, 4:117, 4:119

Keytool 4:39, 4:139-140, 5:131

Kindle Fire 1:71

Koodous Service 3:34, 3:40

L

LiberiOS (jailbreak) 2:35, 2:37

Linux ip_forward parameter 5:70-71

lipo Tool 1:52, 1:54, 2:21, 3:20

Lost/Stolen 2:4-6, 2:19, 2:23-26, 2:116

M

Mach-O 1:30, 1:93, 3:16-20, 3:23, 3:25, 3:27,
3:108, 4:52, 4:120

Man in the Middle Attacks 3:99, 4:111, 5:28, 5:31-44, 5:48, 5:50-54,
5:57, 5:59-60, 5:64, 5:67-76, 5:78-79,
5:98-100, 5:103, 5:107

Mandatory Access Control 1:69

Mddata File 2:109, 2:111

Metasploit 4:6, 4:17, 4:25, 5:116-118, 5:120, 5:122-
123, 5:128-129, 5:131

Metasploit Framework 4:6, 4:17, 4:25, 5:116-118, 5:120, 5:122-
123, 5:128-129, 5:131

Meterpreter 5:2, 5:116-123, 5:129-131, 5:138

Mobile Malware 1:3, 1:10, 1:13, 1:39, 1:66, 1:84, 2:2, 2:31,
2:123-135, 2:138-139, 2:141-143, 2:147,
2:149, 3:33, 3:40-42, 4:69, 5:111, 5:114,
5:130, 5:132, 5:134

Mobile Malware Incentives 2:124

Mobile Problems and Opportunities 1:5, 1:7

Mobile Transaction Authorization 2:125

Number (MTAN)

MobileIron 5:135

mogoRoad 2:138

Msfvenom 5:116-117, 5:120-122, 5:124

N

NDIS	1:73, 2:8-9, 5:79
Network Impersonation	5:103
Network Manipulation Attacks	5:2, 5:27-28, 5:39, 5:50, 5:103
Network Traffic Manipulation	5:2, 5:50-51
NetworkMiner	5:18-20, 5:25
Newsstand App, iOS	1:85, 5:132
NeXT	1:30
Nexus 7	3:81, 5:128
NFC	1:8, 1:50, 1:63
Ninja Slider Application	3:8-9, 4:31
Nitro JIT	1:39
Nmap	5:44, 5:129
NSUserDefaults	2:92, 4:119

O

Obfuscated Applications	1:3, 3:2, 3:47, 3:49-54, 3:64-66, 3:70-71, 3:74, 3:94, 4:138, 5:21
Objective-C	1:32-34, 1:39, 1:54, 3:14-16, 3:23-25, 3:27, 3:76, 3:108, 4:48-51, 4:58, 4:62-63, 4:109, 4:121
ooVoo	2:44, 2:102, 4:102-108, 4:112-118, 4:120, 4:122-123, 4:141
Open Handset Alliance (OHA)	1:50, 1:52-53, 1:71, 1:73
Open Web Application Security Project (OWASP)	4:9-13, 4:100
OpenFeint	2:138
OpenSSH	2:43
openssl	2:82, 4:132
otool	3:13, 3:15, 3:22, 3:25, 3:27, 3:108, 4:103
otool Tool	3:13, 3:15, 3:22, 3:25, 3:27, 3:108, 4:103
Ouija App	3:80-82, 3:84, 3:86-87

P

Pandora Application	3:21, 4:56-58
Penetration Test, Benefits	5:6, 5:139
Penetration Test, Effectiveness	1:12, 5:64, 5:78, 5:136
Penetration Test, Roles	5:8, 5:139

Penetration Test, Scoping	5:78-79
Penetration Test, Value	4:75, 5:4, 5:8, 5:139
PennyTalk Mobile App	3:17
Personal Information Exfiltration	1:10, 2:124, 2:147
PhoneGap	3:2, 3:47, 3:76, 3:94-103, 3:107, 4:101
Plist File	2:92, 2:95-97, 2:102-103, 2:109-110, 2:116, 2:119, 2:140-142, 4:23, 4:86, 4:104, 4:119, 5:84
plutil Tool	2:110
Position-Independent Executable (PIE)	1:54, 3:95, 4:103, 5:129
Privilege Management Models	1:38, 1:41, 1:43, 1:50, 1:53, 1:55-56, 1:58- 59, 1:61-66, 1:69, 1:113, 2:28, 2:47, 2:76, 2:131, 2:137, 2:143, 2:146, 3:102, 4:95, 4:137, 5:114, 5:134
Procyon	3:57-58, 4:30

Q

QEMU	1:86, 1:89
QNX	4:65

R

Rasticrac	2:140
Real APK Leecher	3:7
Reconstructed Code	3:10, 3:47, 3:54-56, 3:59, 3:61, 3:70-72, 3:82-83, 3:93-94
Reflective Programming Language	4:48-49
Remote Access Trojan (RAT)	1:3, 3:42, 5:2, 5:111-124, 5:128-136, 5:138
resources.arsc	2:67, 3:8, 3:90, 3:97, 4:40-41
Return-Oriented Programming	1:35
RFID	1:8, 1:50, 1:63
RockYou, Wordlist	2:9, 2:116
Runtime Modification, Detection	4:121
Rvictl	4:113, 5:12-13

S

Sandbox	1:41, 1:55, 4:110
Script (Key Derivation Function)	4:95
SELinux	1:69

Short Code SMS	2:126, 2:128-130, 2:132, 2:138, 2:146-147
Sidejacking	4:24, 4:133
Sideloadng	2:137, 2:145
Simple Certificate Enrollment Protocol (SCEP)	5:65
Simplify Tool	1:67, 3:70-72, 4:27
Siri	2:16
Skype	1:60, 4:102, 5:125
Skype Application	1:60, 4:102, 5:125
Smali	3:70, 3:108, 4:30-33, 4:37-38, 4:42-43, 5:121, 5:131
sms send	4:13, 5:119
SMSManager	2:132, 3:12, 4:13
SQL Injection	3:99, 5:106
SQLite	1:109, 1:113, 2:43, 2:65-66, 2:70, 2:73-76, 2:89, 2:92-94, 2:111-112, 2:115, 2:119, 3:22, 4:23, 4:86, 4:115-116
SQLiteSpy	2:74, 2:94, 2:112, 2:115, 4:23
SSL Kill Switch	4:111-112, 5:102, 5:107
SSL MitM	4:111, 5:67, 5:69-71, 5:75
Sslstrip	5:73-79
Strings	2:77, 2:100, 3:9, 3:17, 3:21, 3:60, 3:65, 3:69-71, 3:92, 4:19, 4:22, 4:81-82, 4:130, 5:17, 5:21, 5:23, 5:56
SuperSU	2:50, 2:53, 2:55, 2:58-59, 5:122
suspendstate.plist	2:95, 2:97
Svpeng Malware, Android	2:133
Swift	1:32-34, 3:14-15, 3:76, 4:51, 4:62

T

TCP Stream	5:15
TCP/31415	4:8-9
Tcpdump	1:89, 4:113, 5:11, 5:13-14, 5:17, 5:23
Team Win Recovery Project (TWRP)	2:48, 2:53, 2:57-58
Toast	2:132, 4:34
TowelRoot	4:134
Twitter	1:100, 1:111, 2:9, 2:69, 2:138, 3:98, 4:104, 5:144, 5:146

U

Unity	1:8, 1:10-12, 1:14, 1:25, 1:32-33, 1:37, 1:42, 1:71, 1:73, 2:5, 2:10-12, 2:19, 2:31, 2:104, 2:116-117, 2:119, 2:126, 2:129, 2:138, 2:142, 3:22, 3:25, 3:32, 3:47-48, 3:76-81, 3:87-89, 3:92-95, 3:103, 4:6, 4:25, 4:49, 4:64-65, 4:100-101, 5:27-28, 5:37, 5:40-41, 5:50, 5:78-79, 5:86, 5:89, 5:113, 5:120, 5:123-125, 5:129, 5:145-146
URL Handler	1:100, 1:102, 1:105, 4:20, 4:104-105, 4:141
User Credential Theft	2:124-125, 2:147
UsesCleartextTraffic Flag, Android	5:85

V

VMware	1:89, 1:91, 1:93
--------	------------------

W

War on Cleartext Traffic	5:83
WEP	2:68
Windows Internet Connection Sharing	1:4, 2:67, 2:116, 3:42, 5:18
Wireshark	5:15-16, 5:18
Words with Friends App	4:60
WPA-PSK, WPA2-PSK	2:68

X

Xamarin	3:2, 3:47, 3:76, 3:88-94, 3:103, 3:105, 4:101
XCode	1:39, 1:85, 1:93, 2:96, 2:99, 2:140, 2:142, 3:16, 3:20, 3:25, 4:103, 4:106, 4:113, 4:120, 5:12
XMPP Protocol	4:113-114
XNU	1:30

Y

YiSpecter Malware	2:141-142
-------------------	-----------

Z

Zillow	4:125-128, 4:130-134, 4:136-139, 4:141
Zitmo Malware	2:125
Zygote	1:53, 1:55, 1:68, 1:110