

A Taste of SANS SEC575 Part III

2012: A Mobile Pen Test

Mobile Device Security and Ethical Hacking

Today's Focus: Penetration Testing Mobile
Deployments

Joshua Wright
jwright@willhackforsushi.com

Outline

What is SANS SEC575?

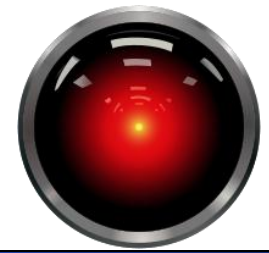
- Attacking Mobile Deployments
- Wireless Network Selection Reconnaissance
- Mobile Device Fingerprinting
- Sidejacking Mobile
- HTTP Manipulation Attacks
- Conclusion

What is SEC575?

- A brand new 6-day course offering by SANS
- "Mobile Device Security and Ethical Hacking"
- Combining policy, architecture, defense and penetration testing
 - Hands-on exercises throughout, culminating in an in-depth Mobile Device Security Challenge event
- Covering Apple iOS (iPhone, iPad, iTouch), Android, BlackBerry and Windows Phone
- Written by Joshua Wright with leadership by Ed Skoudis as curriculum lead and advisor

Building the skills necessary for effective mobile device security

Last Time *at the Movies*



- In Part I of this series, we saw "Invasion of the Mobile Phone Snatchers"
 - We looked at the threat of mobile device theft
- In Part II, we saw "A Mobile Malware Connection"
 - We looked at the growth and exposure to mobile malware threats

Parts I and II posted at www.willhackforsushi.com

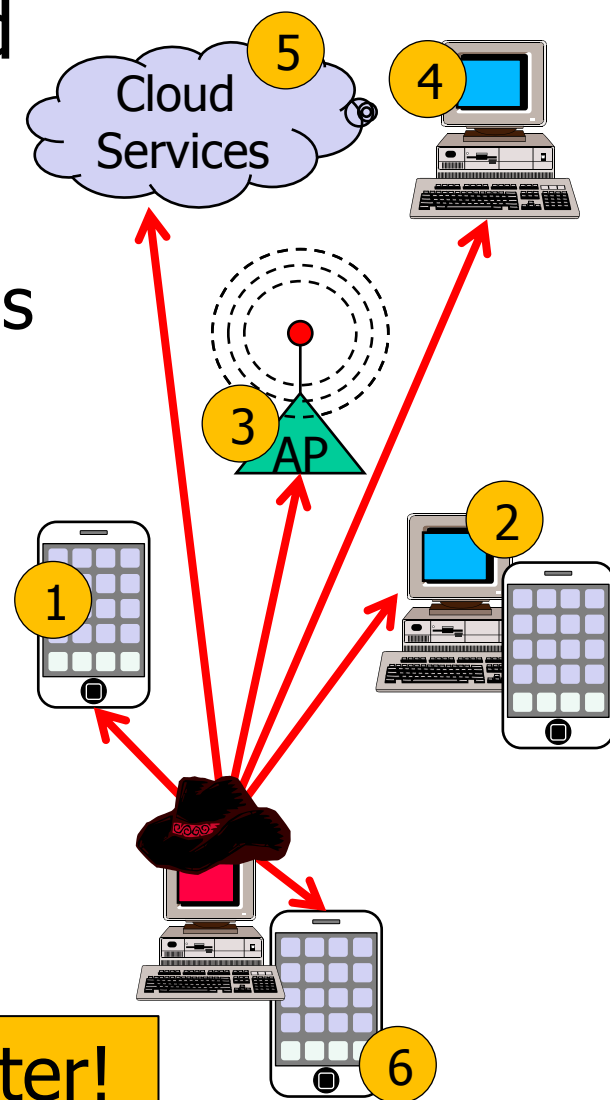
Outline

- What is SANS SEC575?
- ➔ Attacking Mobile Deployments
 - Wireless Network Selection Reconnaissance
 - Mobile Device Fingerprinting
 - Sidejacking Mobile
 - HTTP Manipulation Attacks
- Conclusion

Attacking Mobile Deployments

Several components are targeted

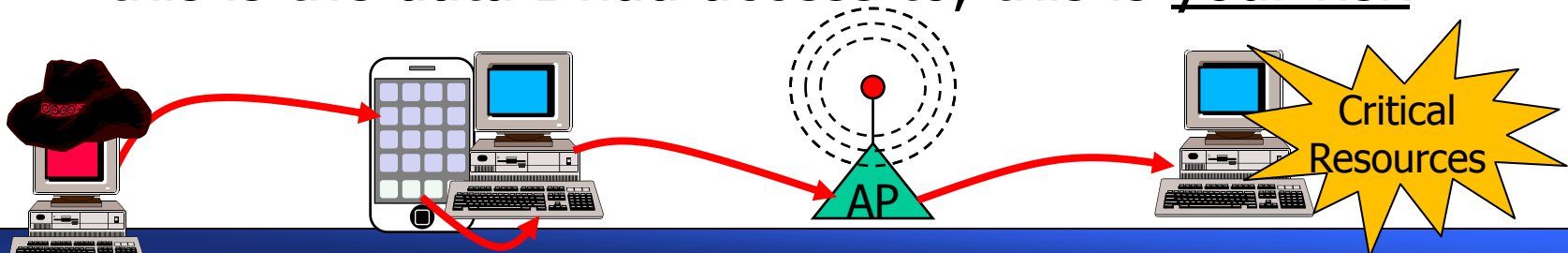
1. Wirelessly connected phones and tablets
2. Computers where mobile data is synced or backed up
3. Wireless infrastructure supporting the deployment
4. Back-end systems supporting configuration
5. Remote cloud systems
6. Physical possession of a device



Complex environments aid a pen tester!

Penetration Test Benefits

- A vulnerability assessment identifies vulnerabilities on systems, networks
 - Rates the criticality of the vulnerability based on guessed system impact
- A penetration test takes a vulnerability and exploits it
 - After exploitation, accessible data is evaluated
 - Compromised system are re-used for pivoting to access other resources
- More accurately reflects what an attacker does
- Provides definitive results: this is how I got access, this is the data I had access to, this is your risk

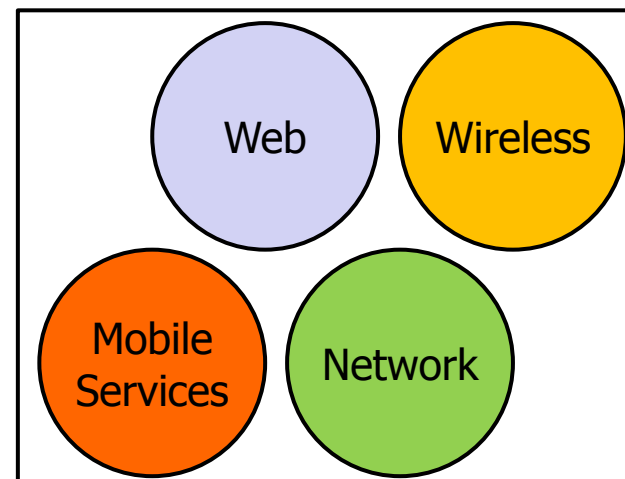


Effective Penetration Testing

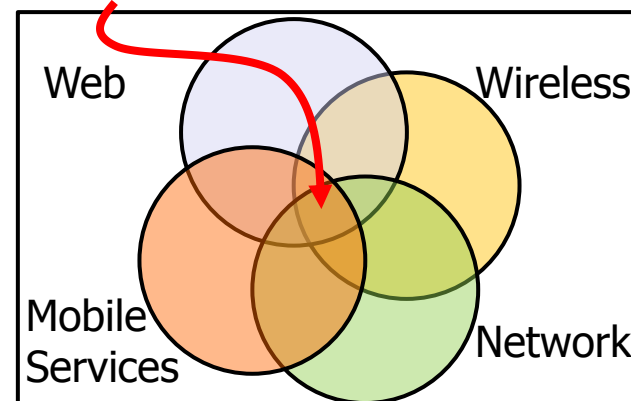
- Mobile penetration testing requires cross-functional skills
- If you want to be a good pen tester you can test web, wireless, network and mobile services independently
- If you want to be a great pen tester, you must integrate testing
 - Pivoting from one platform to another

Pen Test Perfect Storm: Combining attack vectors across multiple focus areas.

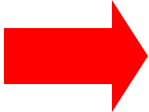
Good Pen Testers



GREAT Pen Testers!



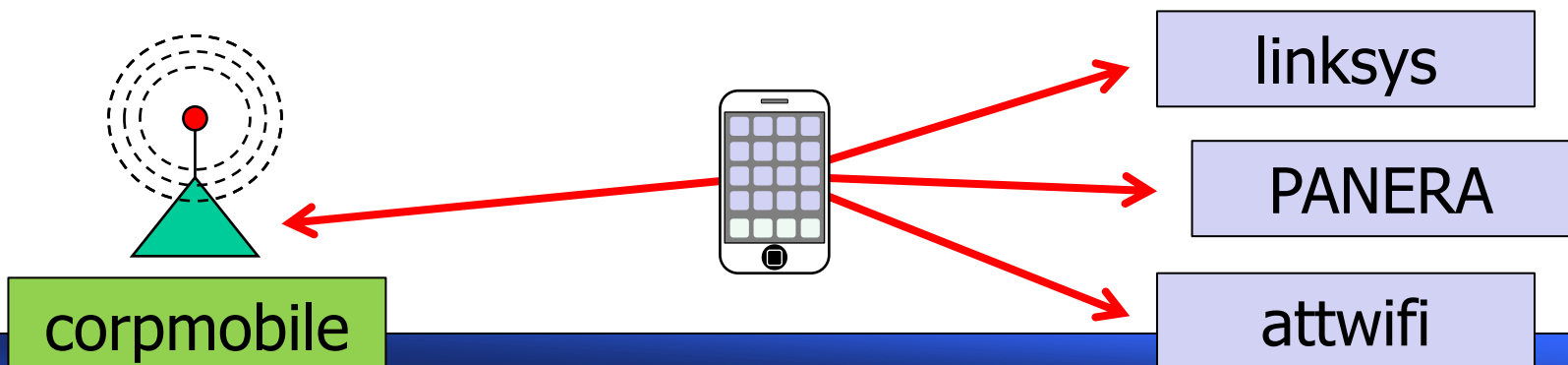
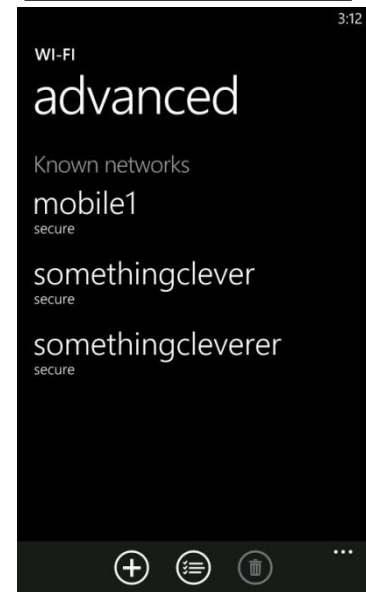
Outline

- What is SANS SEC575?
- Attacking Mobile Deployments
-  Wireless Network Selection Reconnaissance
- Mobile Device Fingerprinting
- Sidejacking Mobile
- HTTP Manipulation Attacks
- Conclusion

Preferred Network List

- List of preferred networks configured on the target device
 - Currently connected network is typically the more preferred available
- Other configured networks are also interesting in a penetration test
- iOS simple interface exposure

Windows
Phone PNL



Airgraph-ng

- Python script to plot Client Probe Graph (CPG) map
 - Client MAC addresses connected to probed network SSID's
- Reads the CSV output from Airodump-ng
- Airodump-ng can parse libpcap files to create CSV files for Airgraph-ng

Airodump-ng will start, terminate with CTRL+C after you see "Finished reading from input file"

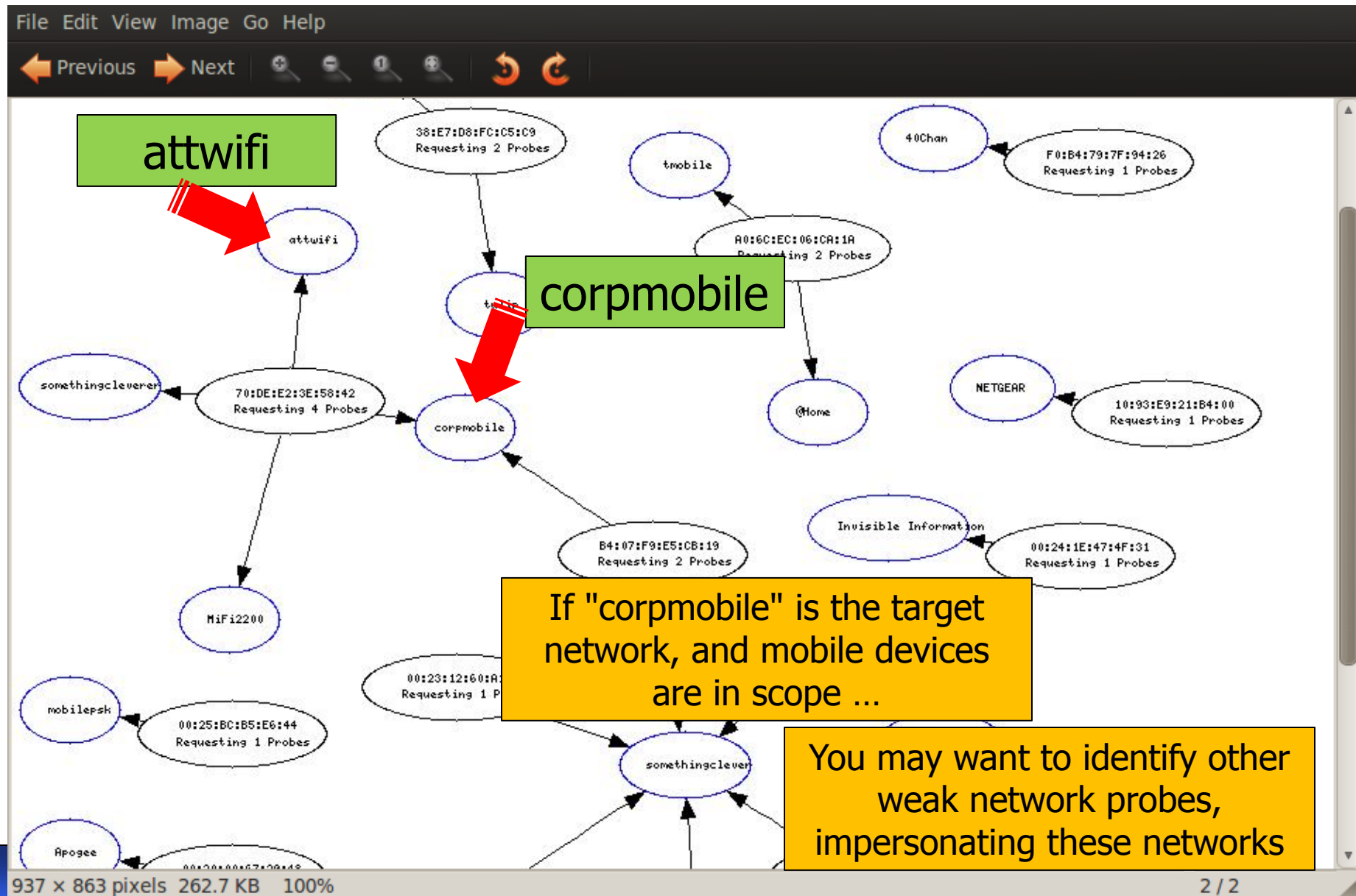
```
# airodump-ng -r Kismet-20110920-11-50-58-1.pcapdump -w Cust01
```

```
# airgraph-ng -i Cust01-01.csv -g CPG -o cust01-cpg.png
```

```
**** WARNING Images can be large! ****
```

```
Creating your Graph using Cust01-01.csv and outputting to cust01-cpg.png  
Depending on your system this can take a bit. Please standby.....  
Graph Creation Complete!
```

Client Probe Graph



Open Network Impersonation

- Devices may probe for open networks that are not available
 - Identified with Airgraph-ng or Kismet
 - Looking for common hotspots or default/open networks
- Become any open network by assuming the SSID
 - Reliably, using any SOHO AP
- Integrated WiFi and 3G/4G devices provide Internet access
- May need to deauth devices from the corporate network to force a roaming event



Limited device resources may lead to a DoS event.

Outline

- What is SANS SEC575?
- Attacking Mobile Deployments
- Wireless Network Selection Reconnaissance
- ➔ Mobile Device Fingerprinting
 - Sidejacking Mobile
 - HTTP Manipulation Attacks
 - Conclusion

Active Fingerprinting

- Active fingerprinting techniques do not work well on mobile devices
- Primarily due to lack of listening TCP ports required for fingerprinting
 - Also lack of uniqueness in TCP stack between mobile and traditional platforms

```
# nmap -F -O 172.16.0.105 | grep -A1 Running
```

```
Running: Microsoft Windows 2008|7|Longhorn|Vista
```

```
Too many fingerprints match this host to give specific OS details
```

```
#
```

```
# nmap -F -O 172.16.0.123 | grep -A1 Running
```

```
Running: Apple iOS 4.X, Apple Mac OS X 10.6.X|10.5.X, Apple iPhone OS  
1.X|2.X|3.X, VMware ESX Server 3.X
```

```
Too many fingerprints match this host to give specific OS details
```

Windows Phone 7.5

Apple iOS 5.0

Mobile device fingerprinting will primarily rely on passive analysis techniques.

Satori



Special thanks to
Eric Kollmann!

- Free, closed-source passive fingerprinting tool
 - Linux and Windows GUI
- Leverages several analysis techniques:
 - TCP/IP stack fingerprinting (p0f)
 - DHCP/bootp analysis
 - HTTP User-Agent and Server tags
 - Proprietary protocols and other techniques
- Currently lacks fingerprints for many mobile devices
- Extensible through plaintext XML files
 - Can manually add signatures as needed

<http://myweb.cableone.net/xnih/>

Satori Analysis - Windows

Satori 0.7.2 [(172.16.0.125 -) Microsoft]

File Options Help

overall

IP address	First Seen	Last Seen	Mac address	Mac vendor	Overall OS	SMB OS	SMB
172.16.0.105	10:53.06 ...	10:53.06 ...	B4:07:F9:E...	SAMSUNG EL...			
172.16.0.110	11:02.16 ...	11:02.39 ...	A0:88:B4:5...	Intel Corporate			
172.16.0.106	11:02.16 ...	11:02.39 ...	A0:88:B4:5...	Intel Corporate			
172.16.0.3	11:02.16 ...	11:02.39 ...	A0:88:B4:5...	Intel Corporate	Brother Printer [10];	Brother Printer [10];	
172.16.0.117	11:02.16 ...	10:53.19 ...	A0:88:B4:5...	Intel Corporate			
172.16.0.127	11:02.37 ...	10:59.45 ...	A0:88:B4:5...	Intel Corporate	Mac OS X 10.5 [10]; Samba 2.2.7 ...	Samba 2.2.7 - 3.2.x Client [1...	
172.16.0.108	11:02.16 ...	11:02.39 ...	A0:88:B4:5...	Intel Corporate			
172.16.0.123	11:02.16 ...	11:02.39 ...	A0:88:B4:5...	Intel Corporate			
172.16.0.4	11:02.16 ...	11:02.39 ...	A0:88:B4:5...	Intel Corporate	Brother Printer [10];	Brother Printer [10];	
172.16.0.125	11:02.21 ...	11:05.33 ...	A0:88:B4:5...	Intel Corporate	Windows 7 [32]; Windows Vista [1...	Windows Server 2008 R2 [10...	
172.16.0.121	10:52.27 ...	10:52.27 ...	2C:A8:35:0...	RIM			
172.16.0.101	11:02.27 ...	10:55.02 ...	00:21:5C:7...	Intel Corporate	Windows 7 [10]; Windows Server ...	Windows Server 2008 R2 [10...	
172.16.0.100	11:02.39 ...	11:02.16 ...	00:1C:B3:B...	APPLE, INC			
172.16.0.1	11:02.39 ...	11:05.17 ...	00:14:BF:0...	Cisco-Linksys ...	Belkin F5D8235-4 v2 [15];		
172.16.0.128	11:03.48 ...	11:03.48 ...	70:DE:E2:3...				
172.16.0.111	11:04.15 ...	11:04.15 ...	F0:A2:25:3...				

Winpcap Version: WinPcap version 4.1.2 (packet.dll version 4.1.0.2001), based on libpcap version 1.0 branch 1_0_rel0b (20091008)

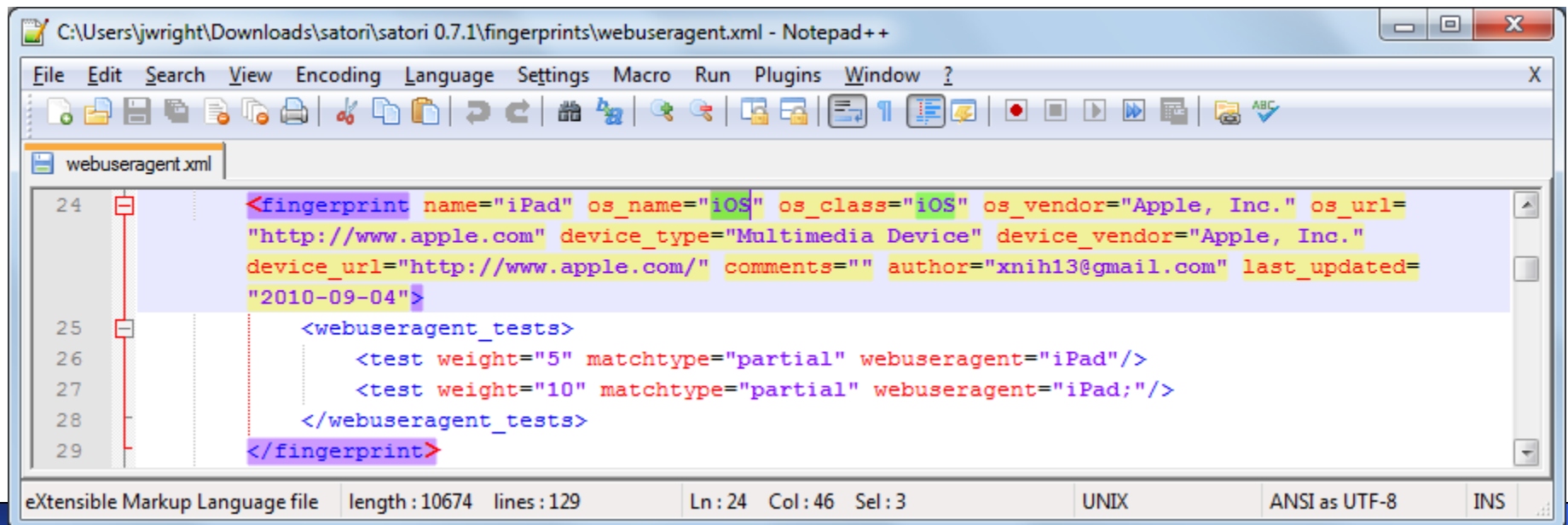
Data Link Type is: (1) EN10MB

Started capturing from device: (172.16.0.125 -) Microsoft - Raw DeviceName: \Device\NPF_{FD3A372B-867E-4C98-8F02-6B2E95A7B537}

Started processing ... 16 hosts 75 alerts 8120 packets / 8120 processed 0 packets/s 0 short packets dropped

Satori Fingerprints

- Stored in the fingerprints/ directory
- Edit XML files with an ASCII editor
 - Preferably one that supports XML syntax highlighting such as Notepad++
- Add new signatures as needed

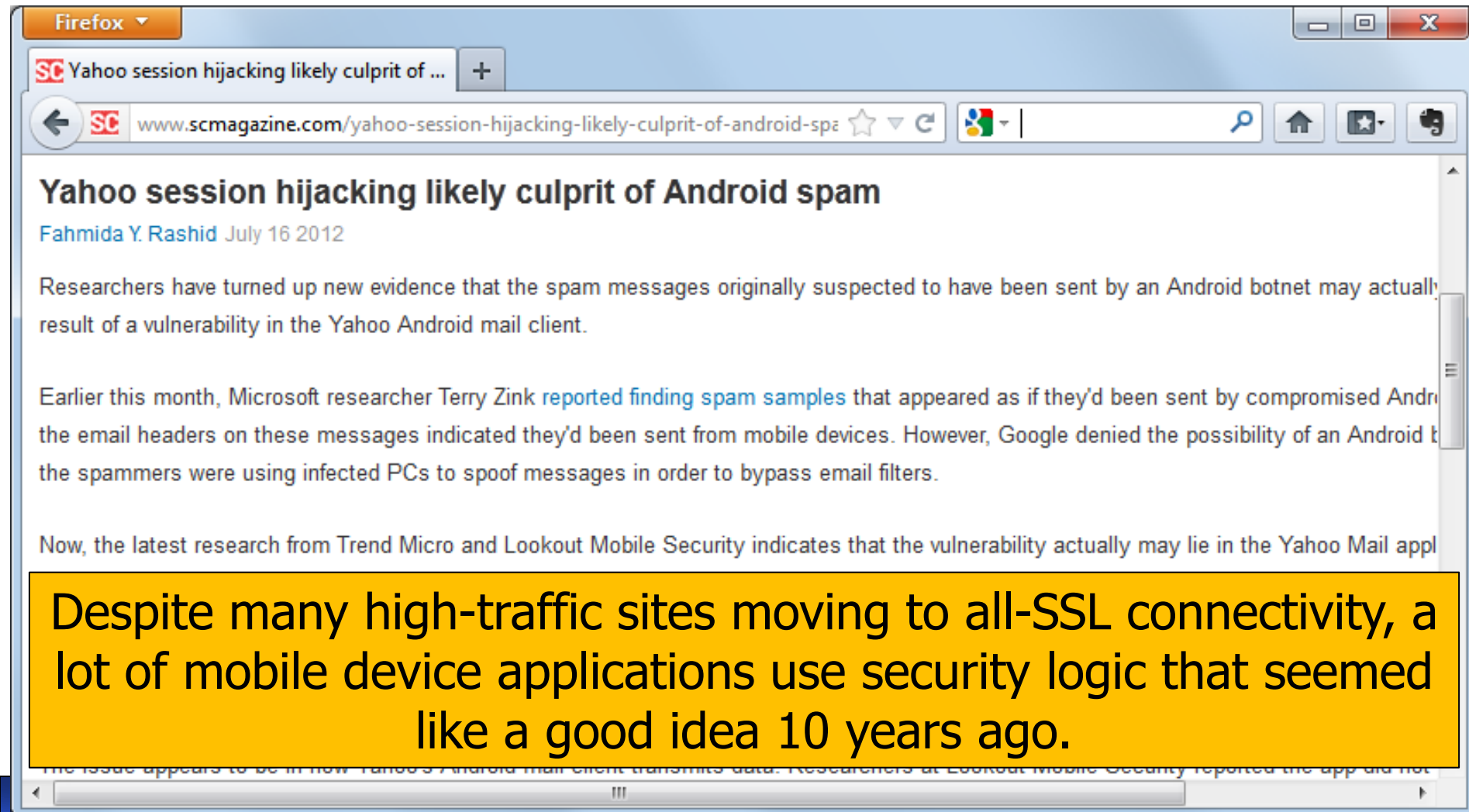
A screenshot of the Notepad++ application window. The title bar shows the file path: C:\Users\jwright\Downloads\satori\satori 0.7.1\fingerprints\webuseragent.xml - Notepad++. The menu bar includes File, Edit, Search, View, Encoding, Language, Settings, Macro, Run, Plugins, Window, and ?. The toolbar contains various icons for file operations and editing. The main text area shows an XML file named webuseragent.xml with syntax highlighting. The XML content includes a <fingerprint> element for an iPad, with attributes for os_name, os_class, os_vendor, os_url, device_type, device_vendor, device_url, comments, author, and last_updated. Below this is a <webuseragent_tests> section containing two <test> elements with weight and matchtype attributes. The status bar at the bottom displays 'eXtensible Markup Language file', 'length: 10674 lines: 129', 'Ln: 24 Col: 46 Sel: 3', 'UNIX', 'ANSI as UTF-8', and 'INS'.

Outline

- What is SANS SEC575?
- Attacking Mobile Deployments
- Wireless Network Selection Reconnaissance
- Mobile Device Fingerprinting
-  Sidejacking Mobile
- HTTP Manipulation Attacks
- Conclusion

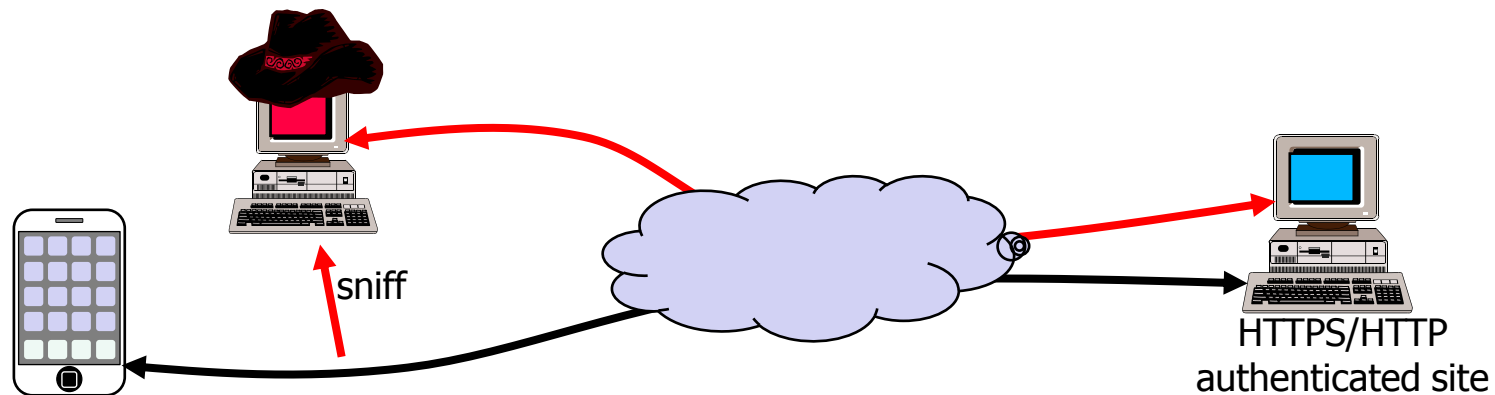
Welcome Back Sidejacking

"I missed you. -Josh"



Sidejacking

- Opportunity to access website resources impersonating the logged-in user
- Many websites begin with HTTPS authentication to protect credentials
- After authentication, a cookie is set to validate user
 - Connection is frequently redirected to HTTP
- Eavesdrop on connection, steal cookie and insert in local browser to access target site



Sidejacking with Firesheep

- Plugin for Firefox 3.6.12 browser
 - Not updated for newer browsers, little ongoing maintenance in public source repository
- Designed for WiFi sniffing and user impersonation
- Ease of use raised awareness of Sidejacking flaw
 - Publicized cases of celebrity sidejacking
 - Many sites transitioned to HTTPS for all traffic
- Extensible with additional handlers

Cain and Firesheep

The image displays two overlapping windows. The background window is Mozilla Firefox showing the Amazon.com 'Your Account' page. The foreground window is Cain and Abilene (Cain), a network sniffing tool. The 'Network' tab in Cain shows a list of captured packets. The 'Firesheep' window, which is a plugin for Firefox, shows a list of captured sessions. The session for 'Joshua L Wright' is highlighted, and the 'Amazon.com' session is selected. The Amazon page shows the user is signed in as 'Joshua L Wright'.

Cain and Abilene (Cain) - Network Tab

Status	IP address	MA
Full-routing	172.16.0.103	70D
Full-routing	172.16.0.103	70D
Full-routing	172.16.0.103	70D
Full-routing	172.16.0.103	70D
Full-routing	172.16.0.103	70D
Full-routing	172.16.0.103	70D
Full-routing	172.16.0.103	70D
Full-routing	172.16.0.103	70D
Full-routing	172.16.0.103	70D
Full-routing	172.16.0.103	70D

Firesheep - Captured Sessions

Session Name	Session ID	Session Type
error		Google
Joshua L Wright		Amazon.com
Joshua L Wright		Amazon.com
error		Google
error		Wordpress
Joshua L Wright		Amazon.com
Joshua L Wright		Amazon.com

Amazon.com - Your Account - Mozilla Firefox

Amazon.com - Your Account - Mozilla Firefox

File Edit View History Bookmarks Tools Help

amazon.com https://www.amazon.com/gp/css/hom

Stop Capturing

Gifts & Wish Lists Gift Cards Your Digital Items Your Account Help

GO Cart Wish List

Search Orders

You are signed in as: **Joshua L Wright**

Sign out

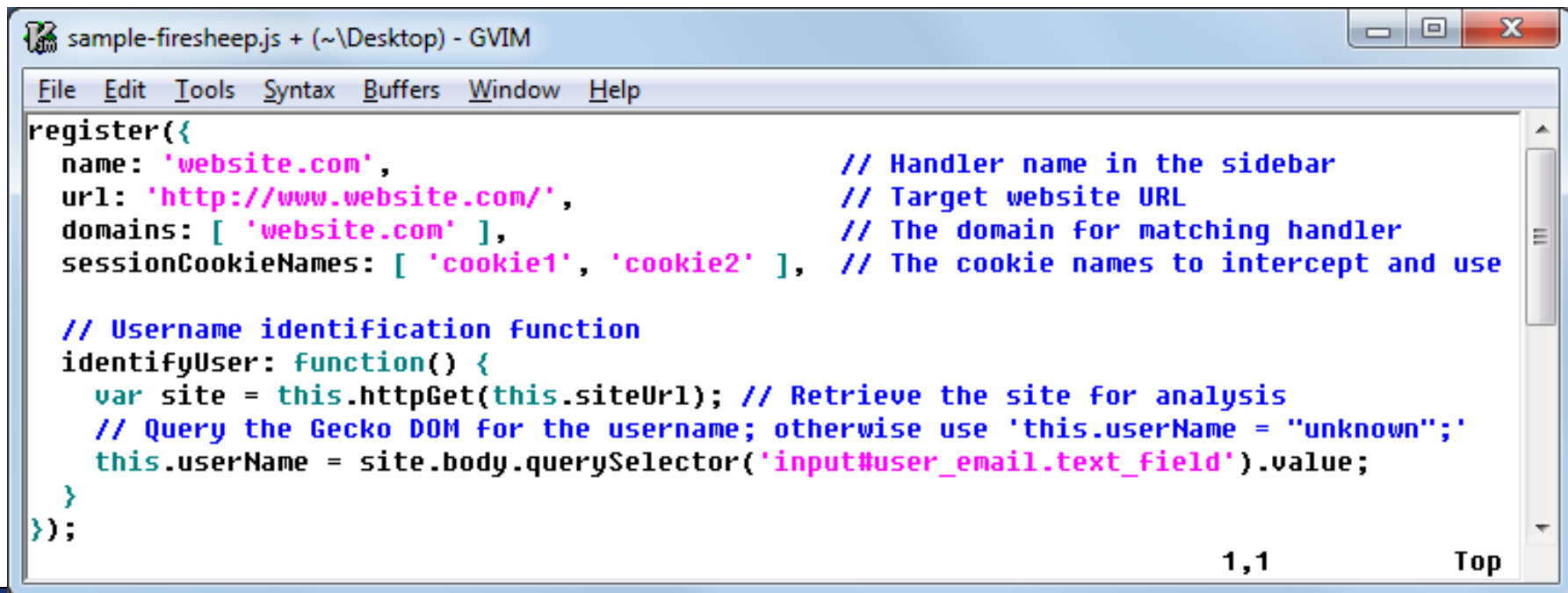
Your Other Accounts

- Your Seller Account
- Your Trade-In Account
- Corporate Customers
- Web Services Account
- Amazon Payments Account

"*error*" indicates that the Firesheep session handler was unable to obtain a valid username. Does not interfere with successful exploitation.

Writing Firesheep Handlers

1. Setup mobile browser with proxy
2. Login to target site
3. Access HTTP resource after logging in, identify cookies, URL and username element



```
sample-firesheep.js + (~\Desktop) - GVIM
File Edit Tools Syntax Buffers Window Help
register({
  name: 'website.com',           // Handler name in the sidebar
  url: 'http://www.website.com/', // Target website URL
  domains: [ 'website.com' ],    // The domain for matching handler
  sessionCookieNames: [ 'cookie1', 'cookie2' ], // The cookie names to intercept and use

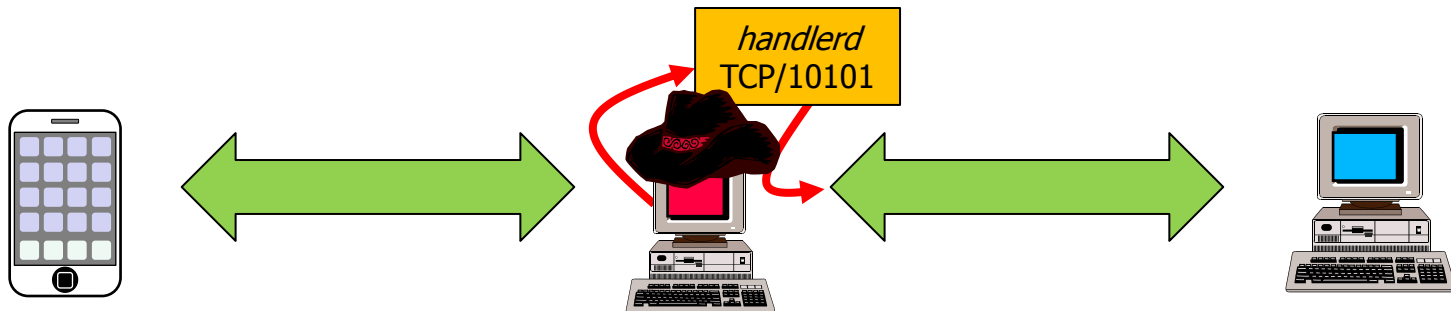
  // Username identification function
  identifyUser: function() {
    var site = this.httpGet(this.siteUrl); // Retrieve the site for analysis
    // Query the Gecko DOM for the username; otherwise use 'this.userName = "unknown";'
    this.userName = site.body.querySelector('input#user_email.text_field').value;
  }
});
1,1 Top
```

Outline

- What is SANS SEC575?
- Attacking Mobile Deployments
- Wireless Network Selection Reconnaissance
- Mobile Device Fingerprinting
- Sidejacking Mobile
-  HTTP Manipulation Attacks
- Conclusion

MitM User Space Tools

- Ettercap establishes the MitM
 - Kernel forwards packets between source and destination
- Linux firewall can reconfigure traffic to send to a local user space process
 - Manipulate and view rules with the "iptables" command
 - Capture packets before forwarding with the "PREROUTING" rule list (chain)
- Allows developers to receive, log, modify and forward packets



PortSwigger Burp Suite

- Sophisticated web scanner with free and commercial versions
 - Written in Java, runs on most platforms
- Supports transparent proxy
 - Standard proxy server, but does not require the client to be reconfigured
- Can be used with iptables for monitoring, manipulating HTTP/HTTPS transactions

<http://portswigger.net/burp> *

* Seriously, learn to use this tool. It's well worth your time.

Burp Suite Transparent Proxy

burp intruder repeater window about

target proxy spider scanner intruder repeater sequencer decoder comparer options alerts

intercept options history

proxy listeners

running	port	loopback only	support invis...	redirect	cert
☒	8080	☐	☒		per-host



To add a new listener, complete the relevant details and click "add".

local listener port:

☐ listen on loopback interface only

☒ support invisible proxying for non-proxy-aware clients 

redirect to host:

redirect to port:

server SSL certificate:

☐ use a self-signed certificate

```
# ettercap -TqM arp:remote /172.16.0.102/ /172.16.0.1/
# iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 8080
```

Burp Suite Proxy Match and Replace

- Burp Suite proxy supports modifying data in real-time
- Differentiates requests and responses, header and body content
- Supports regular expressions for complex matching
- Automatically URL-encodes data as necessary
- Updates Content-Length header as needed

Match and Replace Example

burp intruder repeater window about

target proxy spider scanner intruder repeater sequencer decoder comparer options alerts

intercept options history

- ☐ unhide hidden form fields
- ☐ enable disabled form fields
- ☐ remove input field length limits
- ☐ remove JavaScript form validation
- ☐ remove all JavaScript
- ☐ remove <object> tags

match and replace

	type	match	replace
☐	request header	^User-Agent.*\$	User-Agent: Mozilla/4.0 (...)
☐	request header	^If-Modified-Since.*\$	
☐	request header	^If-None-Match.*\$	
☐	request header	^Referer.*\$	
☐	response header	^Set-Cookie.*\$	
☒	response body	Apple Store	Google Marketplace FTW

response ...

edit remove up down add

No Service 2:12 PM

Back Info

Google Marketplace FTW 591 Ratings **FREE**

When you're on the go, the Google Marketplace FTW app is the best way to research, personalize, and buy products from Apple, and get help at the Apple Retail Store. It's also the easiest way to get a new iPhone — right from your current iPhone.*

Here's what you can do with the Google Marketplace FTW app on your iPhone or iPod touch:

- Buy products on the go and pick them up at your favorite Apple Retail Store, or have them shipped to your door.
- Personalize an iPad or an iPod with free engraving, plus get signature gift wrapping for select Apple products.
- Buy an iPhone with just a few taps.*
- While in an Google Marketplace FTW, quickly purchase accessories on your own with EasyPay

Featured Categories Top 25 Search Updates

Practical Attacks with Burp

Match and Replace

1. Rewrite <FORM> target to send content to your server
2. Replace an App Store download with a different app
3. Deliver a BeEF hook to control the remote mobile browser
4. Inject malicious certificate content to aid in SSL attacks

Outline

- What is SANS SEC575?
- Attacking Mobile Deployments
- Wireless Network Selection Reconnaissance
- Mobile Device Fingerprinting
- Sidejacking Mobile
- HTTP Manipulation Attacks

 Conclusion

Essential Skill Development

- Few penetration testers are able to leverage the eccentricities of mobile devices to their advantage
- Skill at pen testing mobile deployments is a great way to differentiate you from your peers
- Likely a requirement for many organizations to be compliant with PCI
- Unique opportunities and unique challenges compared to traditional pen testing

SANS Security 575: Building the skills necessary for effective mobile device security

Resources

- Airodump-ng - <http://www.aircrack-ng.org>
- Satori - <http://myweb.cableone.net/xnih>
- Yahoo! Mail Client Vulnerability -
<http://blog.mylookout.com/blog/2012/07/05/our-thoughts-on-the-android-spam-botnet/>
- Firefox 3.6.12 -
<https://ftp.mozilla.org/pub/mozilla.org/firefox/releases/3.6.12/>
- Firesheep -
<https://github.com/codebutler/firesheep/downloads>
- Burp Suite - <http://portswigger.net/burp>

SANS Security 575: Mobile Device Security and Ethical Hacking

- SANS Conference Events
 - VA Beach 8/20 - 8/25 (Joshua Wright)
 - Las Vegas 9/17 - 9/22 (Joshua Wright)
 - Baltimore 10/15 - 10/20 (Joshua Wright)
 - London 11/26 - 12/1 (Raul Siles)

Visit www.sec575.org for upcoming courses and instructor announcements!

Special vLive Offer!

- Live instruction over the Internet with Joshua Wright and Peter Szczepankiewicz
 - Monday and Wednesday nights 7-10 ET
 - Starting 9/4, ending 10/10
- All sessions are recorded to make-up or listen again for 4 months
- Complete with labs, demos and everything you would expect at a conference event



Special: Register by 7/25 with reg code
"0710_MBAIR" and get a free 11"
MacBook Air! Ends this Wednesday!

<http://tinyurl.com/cafr4fe>