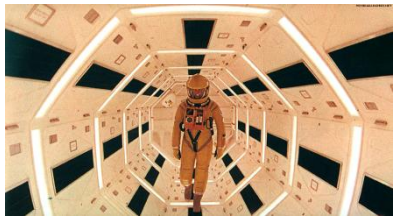



A Taste of SANS SEC575 Part III 2012: A Mobile Pen Test

Mobile Device Security and Ethical Hacking

Today's Focus: Penetration Testing Mobile Deployments

Joshua Wright
jwright@willhackforsushi.com

Outline

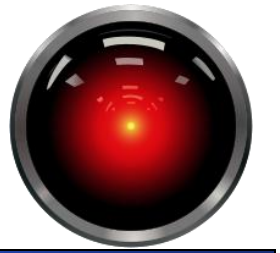
- What is SANS SEC575?
- Attacking Mobile Deployments
- Wireless Network Selection Reconnaissance
- Mobile Device Fingerprinting
- Sidejacking Mobile
- HTTP Manipulation Attacks
- Conclusion

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

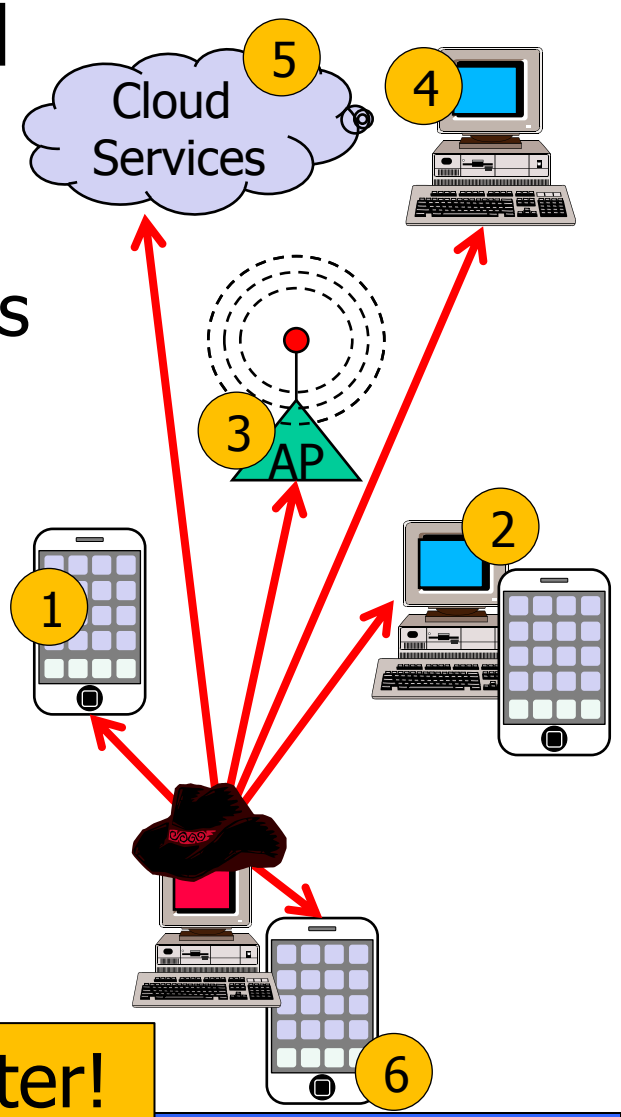
Outline

- 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

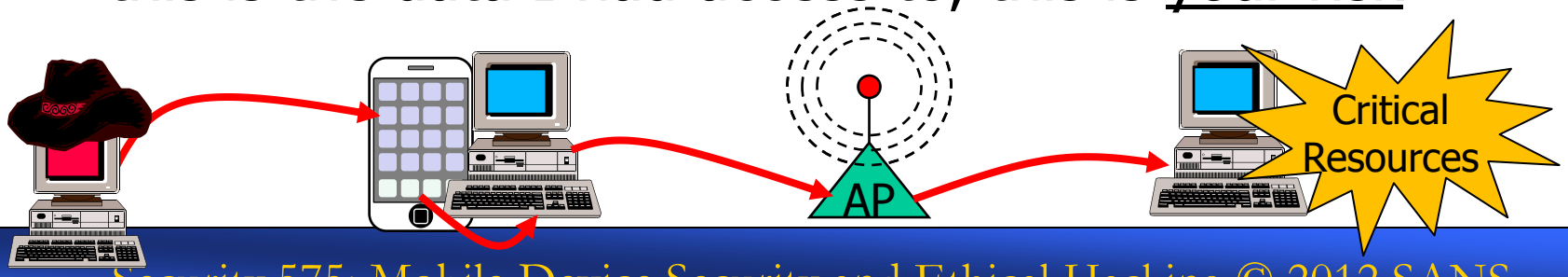
1. Wirelessly connected phones and tablets
2. Computers where mobile data is synced or backed up
3. Wireless infrastructure supporting the deployment
4. Back-end systems supporting configuration
5. Remote cloud systems
6. Physical possession of a device



Complex environments aid a pen tester!

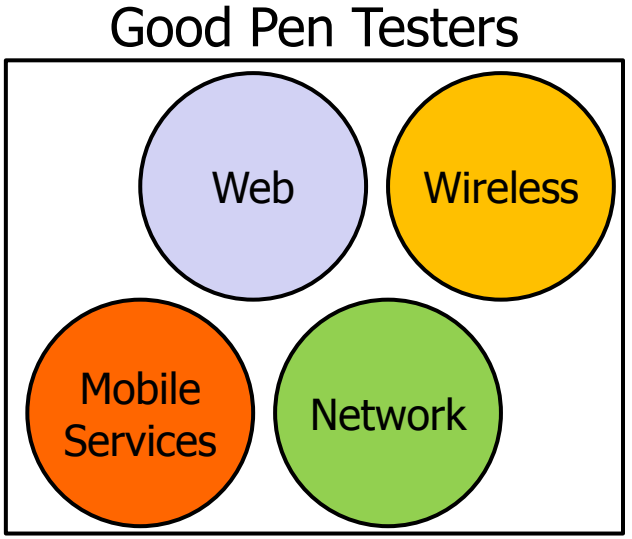
Penetration Test Benefits

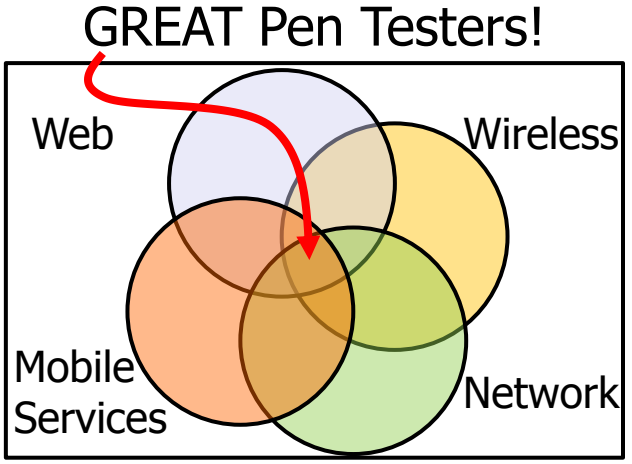
- A vulnerability assessment identifies vulnerabilities on systems, networks
  - Rates the criticality of the vulnerability based on guessed system impact
- A penetration test takes a vulnerability and exploits it
  - After exploitation, accessible data is evaluated
  - Compromised system are re-used 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.

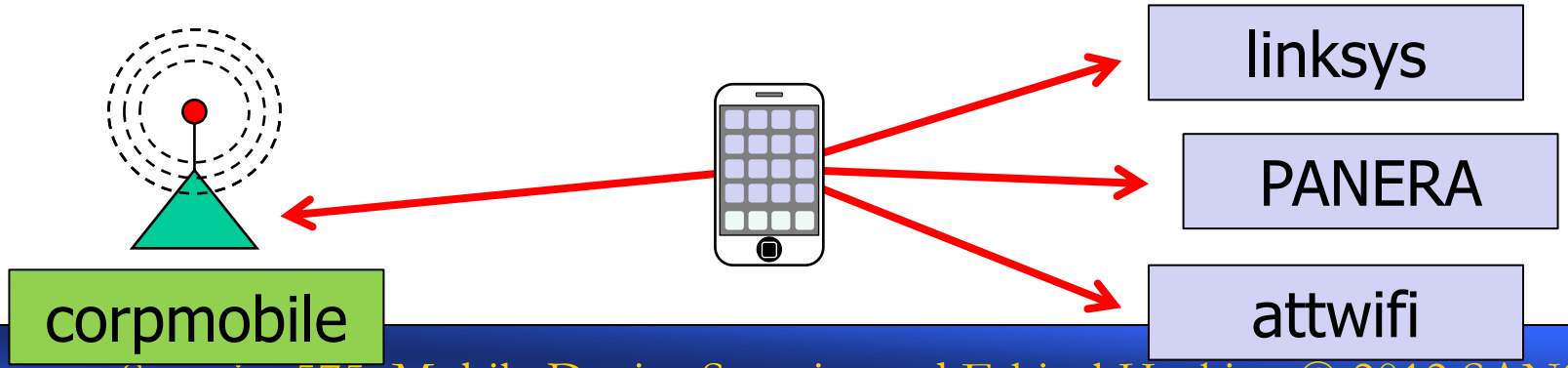
Outline

- 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



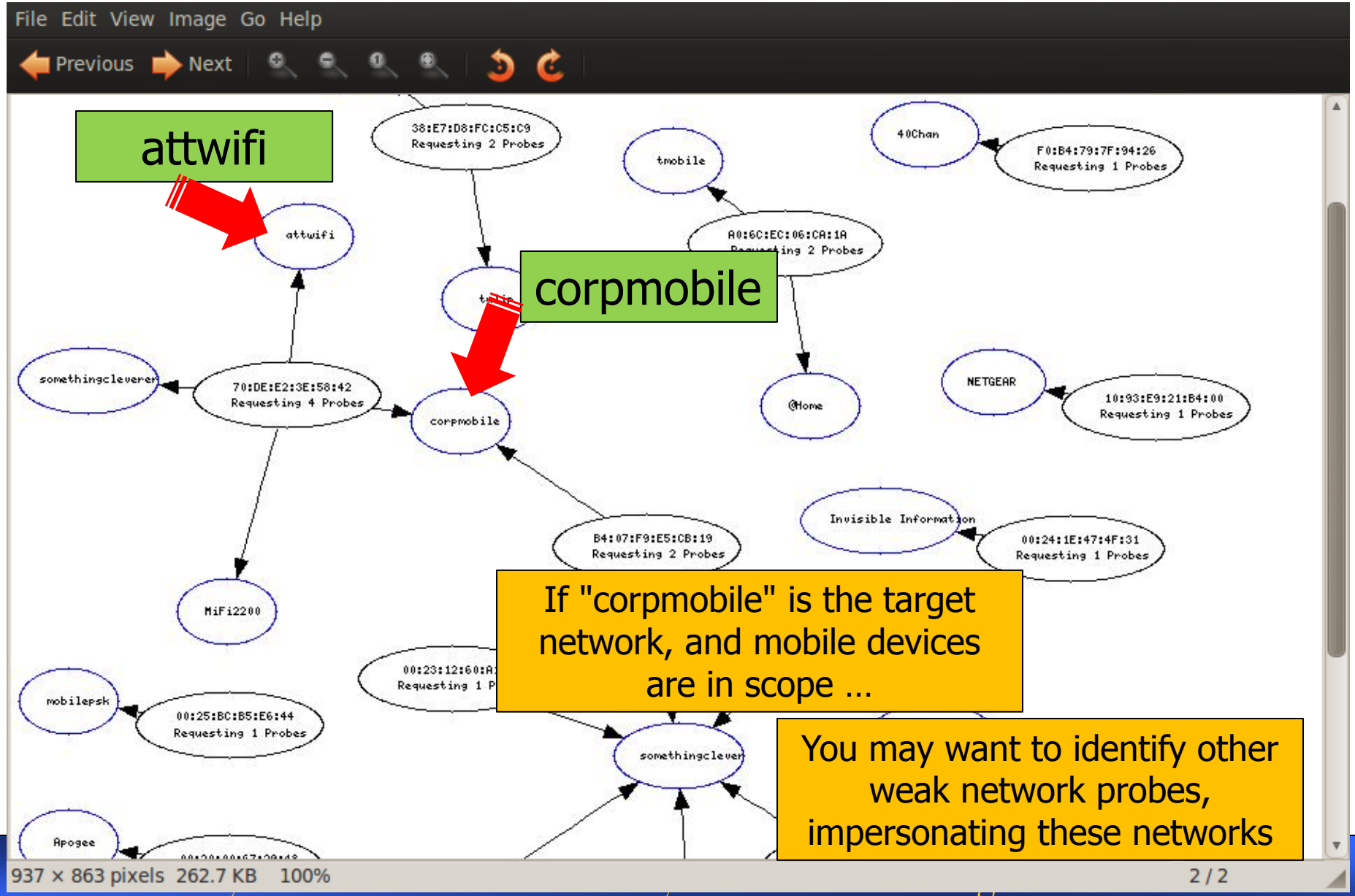
Airgraph-ng

- 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.

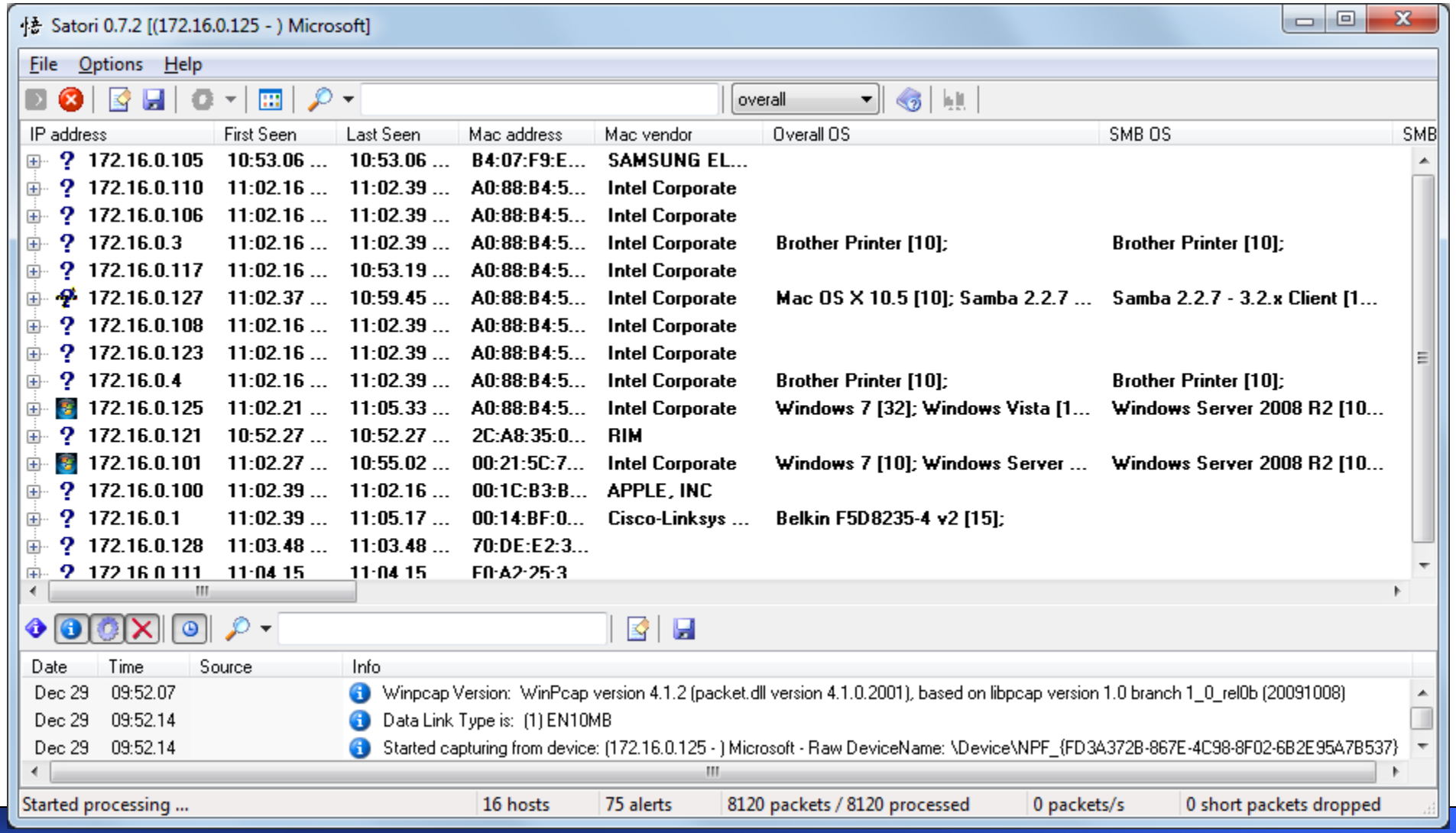
Satori

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

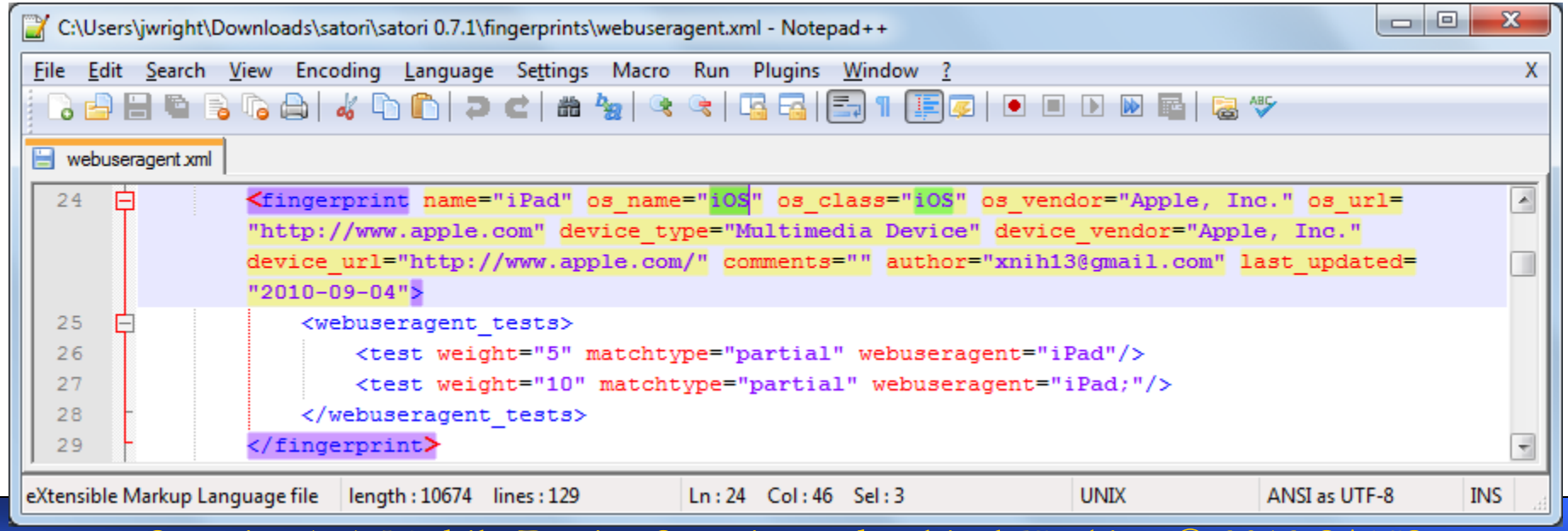
http://myweb.cableone.net/xnih/

Satori Analysis - Windows



Satori 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

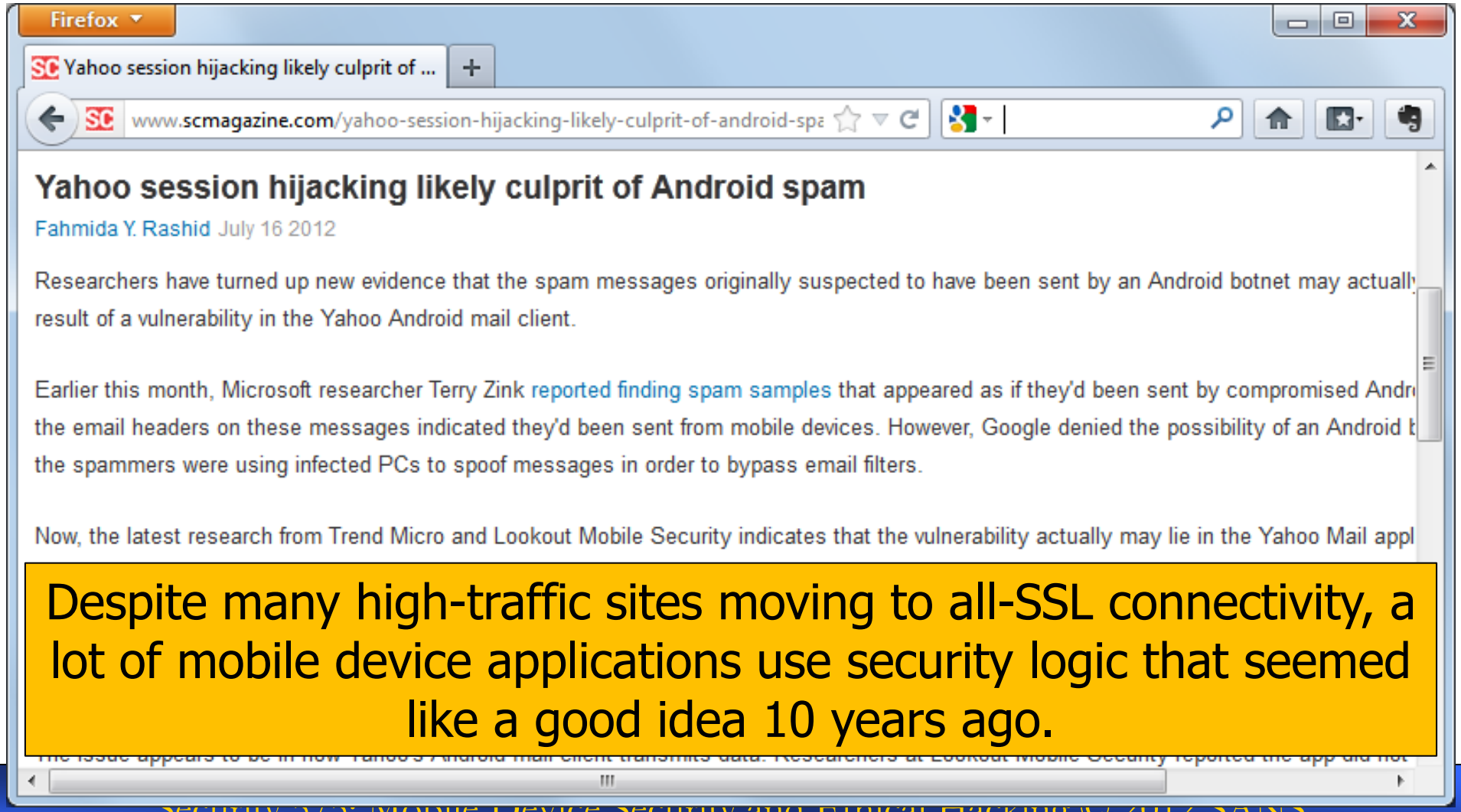


Outline

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

Welcome Back Sidejacking

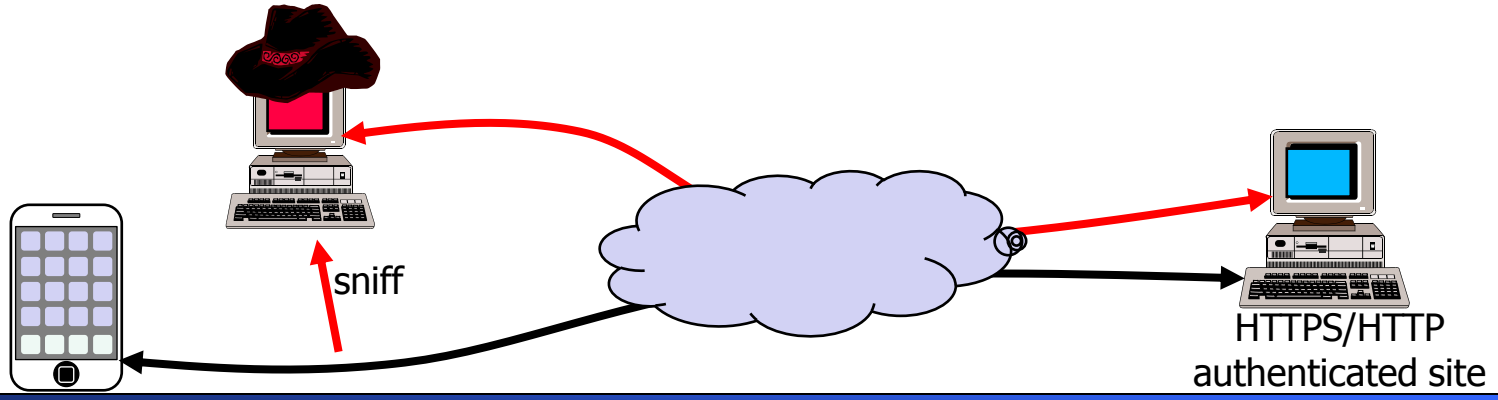
"I missed you. -Josh"



Despite many high-traffic sites moving to all-SSL connectivity, a lot of mobile device applications use security logic that seemed like a good idea 10 years ago.

Sidejacking

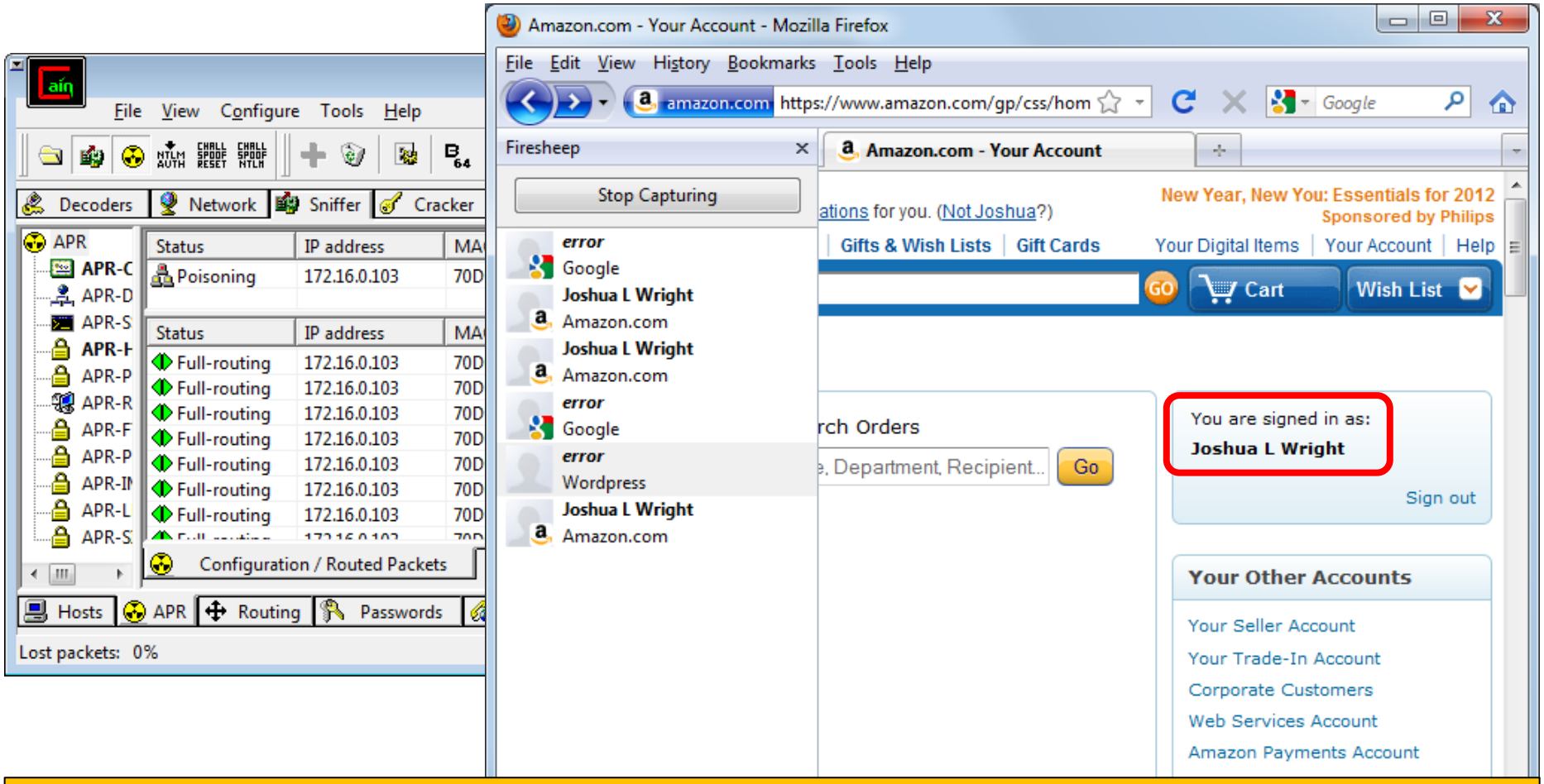
- Opportunity to access website resources impersonating the logged-in user
- Many websites begin with HTTPS authentication to protect credentials
- After authentication, a cookie is set to validate user
  - Connection is frequently redirected to HTTP
- Eavesdrop on connection, steal cookie and insert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



"*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

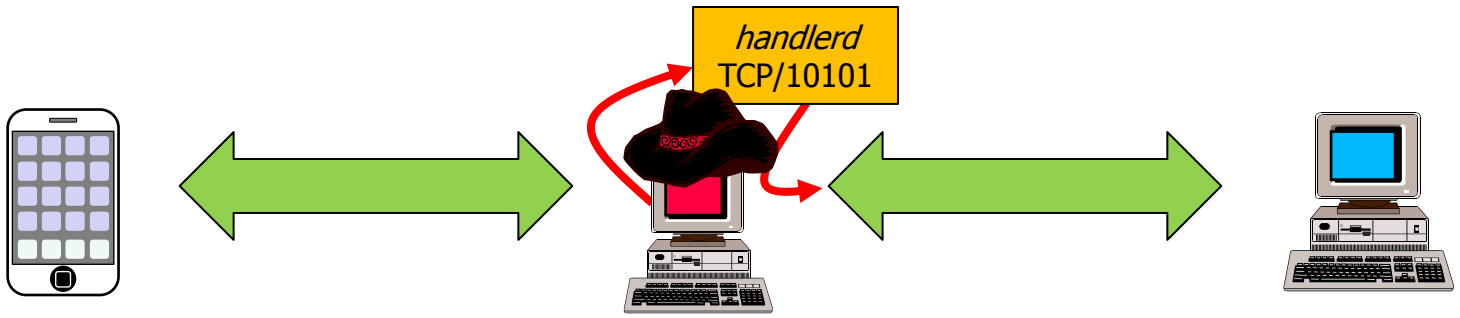
```
register({
  name: 'website.com',                          // Handler name in the sidebar
  url: 'http://www.website.com/',               // Target website URL
  domains: [ 'website.com' ],                   // The domain for matching handler
  sessionCookieNames: [ 'cookie1', 'cookie2' ], // The 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



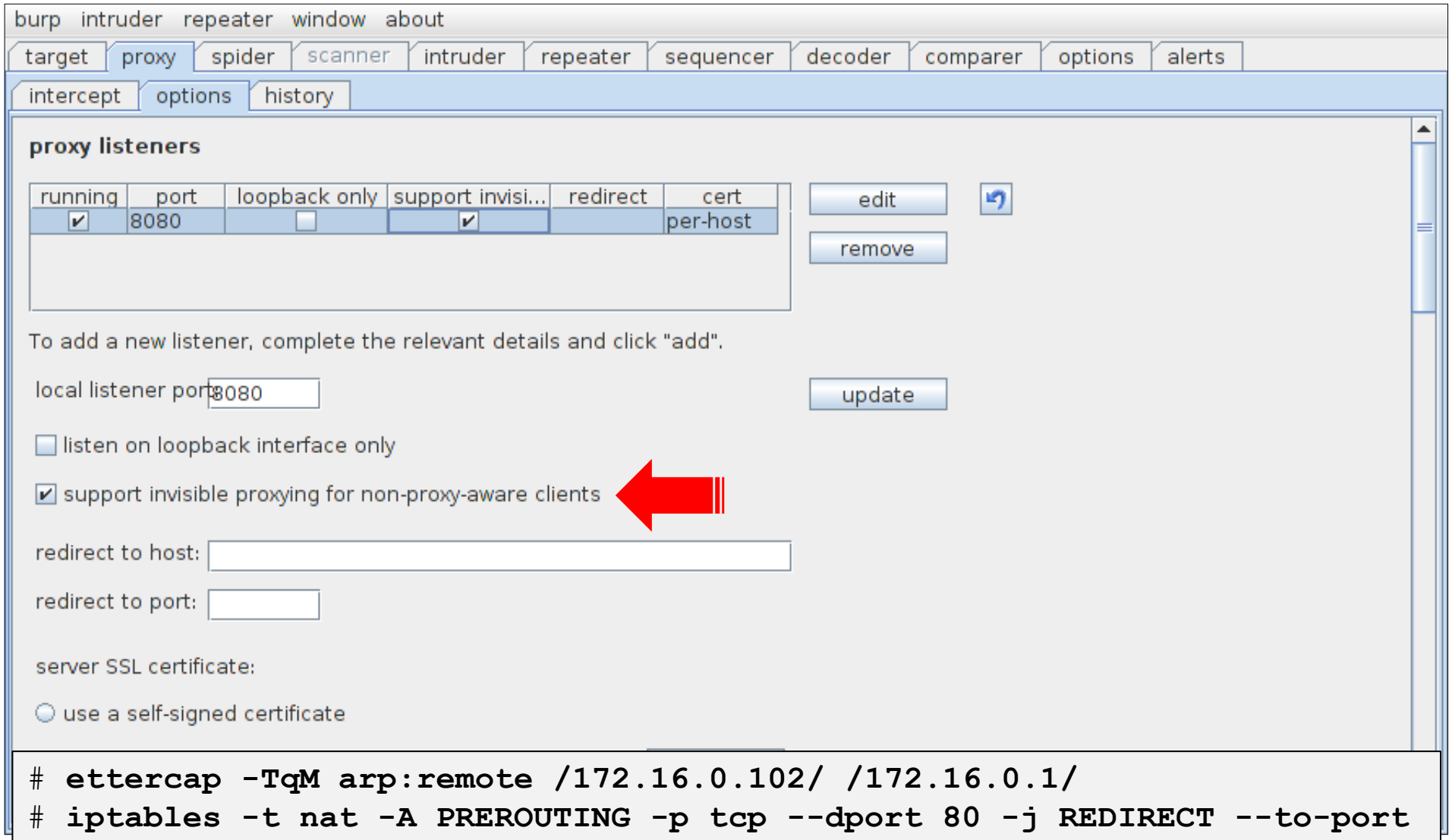
PortSwigger Burp Suite

- 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

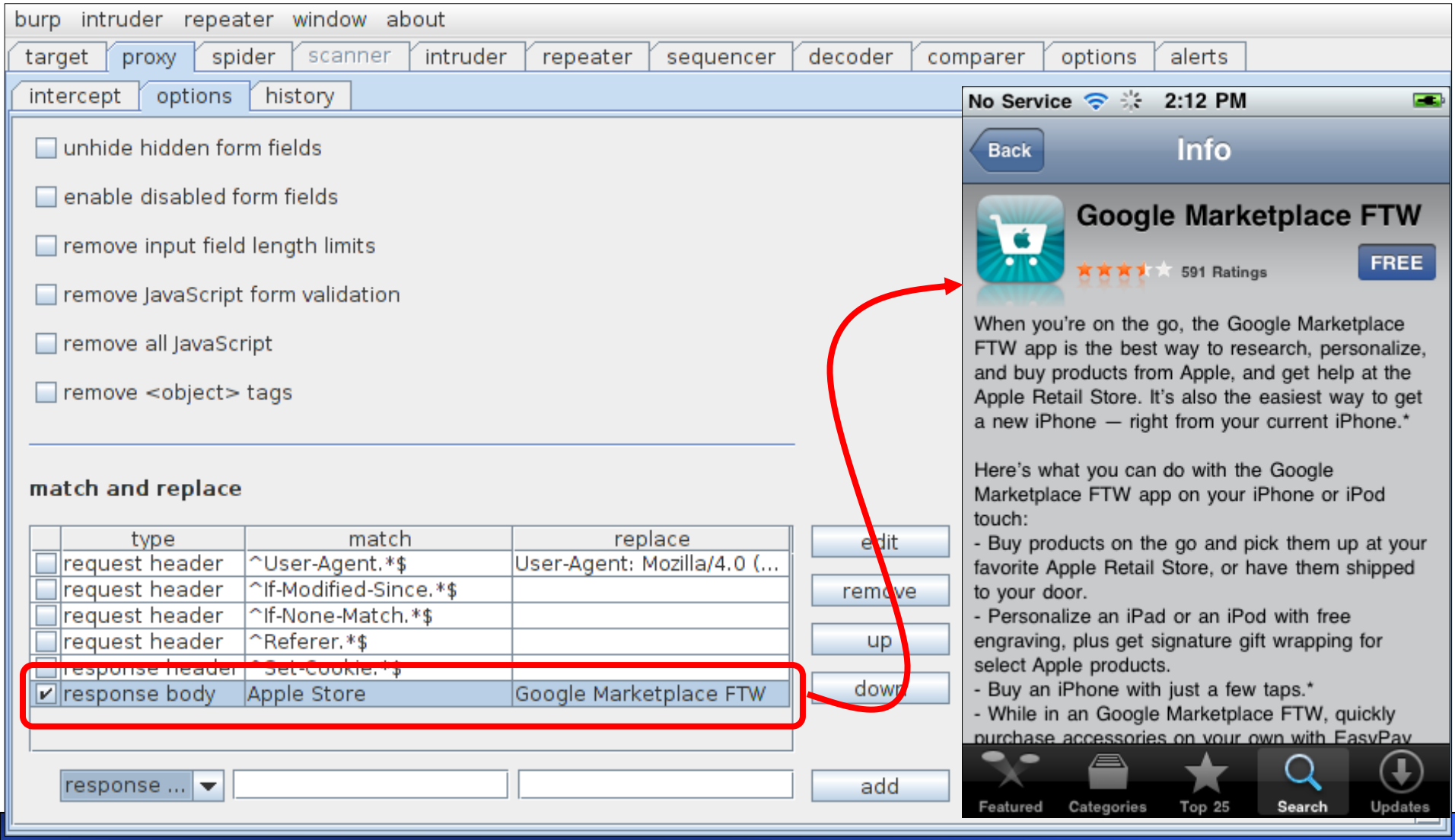



```
# ettercap -TqM arp:remote /172.16.0.102/ /172.16.0.1/
# iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port
8080
```

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



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