Bringing Sexy Back
Breaking in with Style…
Pentest? Really?!?!

- Pentest has been getting a bad rap lately.
- The demand hasn’t dropped off…
- Testers hate doing it because it’s boring.
Why is pentesting boring?

It's seldom about 0day, it's most about lame php bugs or password cracking…
Why is pentesting boring?

Customers don’t understand them. I once was hired to do a pen test on a Class C that had nothing on it.
Why is pentesting boring?

Watching scanners run is boring…
Where is the excitement?

This can’t be it, there must be more to this than some scanners, password crackers, and out of date software. Where is the mystery, the intrigue, the fun stuff?
We have two ways pen testing can be interesting, easy, and surprisingly successful.
1. iPhone in a box.
iPhone in a box is simple

• Step 1 – Get a Box
• Step 2 – Put your iPhone in a Box
• Step 3 – Mail the box
Step 1 – Get a box
• Get a box.
  – We used the original iPhone box.
  – It doesn’t look very suspicious
  – And it’s the perfect size for everything we need to fit inside.
Step 2 - Put your iPhone in the box
All the materials...
Battery problems?

• The iPhone will last a day or so if it is on constantly and scanning.

• Batteries to the Rescue!
  – APC makes mobile batteries…
Battery Problems?

• We have found that with a fully charged battery an iPhone can run for 5 days with activity.
Back to the box…

• The default box has enough room for the phone, the battery, and the cables.
• It requires some cutting of plastic
  – Easy to do with any knife
Cutting, Cutting, Cutting
All done…
Now for the plastic...
Fits like a glove!
Disable the autolock and poweroff..
Box built, now what?
Configure the iPhone

• Jailbreak the iPhone
• Install SSH and the BSD subsystems…
• Install tcpdump, APLogger, and anything else you might use…
• Do some custom stuff…
What is custom?

• How it connects to you…
  – You can’t SSH to the phones IP address…
  – So you can have it connect to you…
  – Write a program that behaves like shellcode
    • Starting a process with a shell
    • Redirect standard in and out to a shell
    • Connect to a predetermined address at specific time intervals
    • You can use Netcat to list on the receiving host.
• This process is croned to run every hour on the hour.
• When you get a connection you are inside the network!
• Manually do scans and connect to access points/Other machines.
Set it all up and seal the box up...
Step 3 – Mail the box
Demo of iPhone connection software
2. Phish for it…
• The easiest way to break in to Windows is to ask nicely…
• A good phishing site isn’t after passwords…
• Installing software is far more useful.
There has been a number of vulnerable ActiveX controls lately that allow for the download and execution of arbitrary programs.

An ActiveX control like this could greatly benefit a test.
• Grab a CMS, configure it to look like a benefit management company.
• Configure the main page to prompt visitors to install a “secure” ActiveX control.
• Download and install the trojan.
• Safeguards have to be put in place
  – It can’t infect any site visitor
  – The trojan has to delete itself and the ActiveX control after a period of time.
  – Log everything on the victim machine…
Pen Phising Demo
Thank you.

http://erratasec.blogspot.com
http://www.erratasec.com