Getting A Better Pen Test (And Improve Your Security Jedi Skills In The Process)

So you can be just like this guy...

Paul Asadoorian (paul@pauldotcom.com)
John Strand (john@pauldotcom.com)
Speaking Handicap
“Product Evangelist” - Use, beat up, maim, torture, extend or otherwise abuse products and tell people about it.
“Podcast” – Bunch of people get together, talk about stuff, drink beer and oh yea there are microphones.
Corrupting the youth of America since 2005.
You can hire us to do penetration tests...
“Penetration Testing” - Find weaknesses in your defenses and architecture, tell you about them. Drink lots of Red Bull and listen to techno music.
So you know where I stand on important issues

```python
#!/usr/bin/env python

beer = "G. Schneider and Sons"
if beer == 'Coors Light':
    sys.exit()
print beer
```

:%s/emacs/vim/g
I wasn’t kidding about the Star Wars thing...

Take your son to work day
Outline

**Episode 1** - Top five mistakes penetration testers make

**Episode 2** - Top five questions you must ask penetration testers

**Episode 3** - Elements of a great penetration test

**Episode 4** - Signs you are not ready for a penetration test

**Episode 5** - Things you must do before a penetration test

**Episode 6** - Advanced things you can do before a penetration test (provided you did everything in Episode 5)
Episode 1

The Phantom Menaces of Penetration Testing
Top Five Pen Tester Mistakes

1. Testing “stuff” you already know is broken (and have a plan to fix)
2. Relying solely on automated tools
3. Believing the Shell is the end, not the beginning
4. Improper scoping of the penetration test
5. Providing Lame defensive recommendations
1. “We know the Wifi is broken”

⚠️ If you know protections are not in place, then don’t have someone test it!

⚠️ However, make sure you understand the risk

⚠️ Could a hole in your Wifi lead to your death star exploding?

http://pauldotcom.com
2. “We’ve Had A Pen Test...”
Scanning != Pen Test

⚠️ Its not a penetration test if they run an automated vulnerability scanner and hand you the results

⚠️ However, if you have never run a vulnerability scan before, this is not a bad thing

⚠️ Same goes for web application testing

⚠️ Intelligence gathering, vulnerability identification, exploitation, post-exploitation and threat modeling

If you don’t want to know about vulnerabilities in your network, you should not have a penetration test.
3. I got shell...

- Simply gaining access to a system is just that, unauthorized access
- What you can do from there, or post-exploitation, that matters
- Sometimes you do want to just prove you got shell
- Other times you have goals, such as access to sensitive information or potential disruptions of business continuity

Han Solo Shell
4. Scoping A Penetration Test

⚠️ These are not the systems you are looking for...
Those were the systems I was looking for!
Scope Without Denial

⚠️ “No one would use THOSE systems to attack us...”
Provide Excellent Recommendations

“You should apply some patches...”

http://pauldotcom.com
5. “Apply patches”

Penetration Tester: “I found this vulnerability”

You: “Okay, what should I do about it?”

Penetration Tester: “You should apply patches”

You: “Gee, thanks.”

Recommendations include how the vulnerability and exploitation affects your organization

Low, Medium and High relate to the vulnerability, not to the risk presented to your organization
Episode 2

Attacking The Penetration Testers
5 Questions For Penetration Testers

1. Do you prefer to scan production or DEV/QA environments?
2. How do you plan to scope the web application test?
3. What does your report format look like?
4. How will you test the system(s) that crash if you send them packets?
5. How will you test the IPS and our incident response program?
Episode 3

A guy can only be called "Annie" so many times before he snaps.

 Revenge of the Penetration Testers
Always test the DEV/QA environments where possible, especially when testing web applications.

Scoping web applications requires knowing the number of input fields, and obtaining multiple sets of credentials.

There is nothing wrong with changing the scope to see what an attacker would do on the inside.

So as to not waste time and money, agree on whether IPS will be on or off. Typically one set of tests for each condition (but OFF FIRST).
Keys To A Great Report

- Description of the problem and conditions found
- A list of hosts and/or applications containing the problem
- The impact of the vulnerability and exploitation on the organization
- Information on how to reproduce the condition
- Background information about the techniques
- A section for management response

Key to every teenage boy loving Star Wars for life

http://pauldotcom.com
Value of Penetration Testing

- Fully understand and manage risk
- Testing of your defenses and procedures
- Put context around all your vulnerabilities, show what attackers can do with them and link them together
- Put the “rubber to the road” and go above and beyond traditional auditing
- Understand who, why and how attackers will come after your organization
Episode 4

A New Hope For Securing Your Network?
You May Not Be Ready If...

⚠️ Do you have a patch management system?

⚠️ Does it include 3rd party software?

⚠️ Does it encompass all systems? (Red Hat, Microsoft, etc..)

⚠️ Do you have a well-defined process for applying patches?

http://pauldotcom.com
You May Not Be Ready If...(2)

Do you have dedicated employees to security and/or systems management?

Do you have a vulnerability management program which includes remediation tracking?

Is security part of development and QA programs?

Do you test software and devices before they go into production?

http://pauldotcom.com
Episode 5

The Defenders Strike Back
Getting Ready For A Pen Test

Network vulnerability scanning - The “point and shoot” of vulnerability scans.

Passive vulnerability “scanning” - Hiding in the bushes with a telephoto lens.

Local patch checking - Walking into the place and taking a full inventory.

http://pauldotcom.com
Getting Ready For A Pen Test (2)

🎯 Configuration/Compliance Auditing - Taking inventory, but comparing it to a shopping lists.

🎯 Identify Undesirable Conditions - Extra stuff, such as secret tunnels, hidden rooms, etc...
Passive Vulnerability Discovery

- Identify vulnerabilities on systems that are firewalled and/or unmanaged

- **Example:** A web browser leaks the version when they browse the web

- **Example:** An embedded system may initiate a software update and leak the version number

- **Example:** Users run applications on a virtual machine to get around software restrictions on the host OS
Local Patch Checking

⚠️ Log into the system and determine if patches are applied

Example: Every day Nessus logs into my systems and checks that all the Linux software updates are applied. If patches are available, I get an email.

Example: Log into all of your desktop computers on the network, make sure they are up-to-date on Adobe software. *You will get lots of email!
Anti-Virus Software

“The Armor is too thick!”

http://pauldotcom.com
Anti-Virus Software
You should have it, however, realize that through “magic” it can be bypassed.

Changing the binaries around, different encoding can all bypass anti-virus software.

Running the malware through an SMB or WEBDAV share can do the trick as well: http://pauldotcom.com/2012/05/remote-malware-deployment-and.html
Keep Sysadmins In Check

http://pauldotcom.com
Find Open Shares

http://pauldotcom.com
Find Exploitable Vulnerabilities

All vulnerabilities that have associated exploits and either an exploits is exists or is not required.
In Summary...

- Apply patches to all systems and software according to a proven process
- Scan across the network to find new systems with vulnerabilities
- Scan existing systems for missing patches and mis-configuration
- Monitor the network for hidden vulnerable systems and applications
- Use Anti-Virus software and keep it up-to-date
- Scan for open shares and default passwords

http://pauldotcom.com
Episode 6

It's a Trap!

The Return Of “Hacking Back”
Create “Honeypots”

```bash
@echo off
for /L %%i in (1,1,1) do @for /f "tokens=3" %%j in ('netstat -nao ^| find ^": 3333^"') do@for /f "tokens=1 delims=:" %%k in ("%%j") do netsh advfirewall firewall add rulename="WTF" dir=in remoteip=%%k localport=any protocol=TCP action=block

[root@linux ~]# while [ 1 ] ; echo "started" ; do IP=`nc -v -l -p 2222 2>&1 1> /dev/null | grep from | cut -d[ -f 3 | cut -d] -f 1`; iptables -A INPUT -p tcp -s ${IP} -j DROP ; done
```
Create Infinitely Recursive Directories

```bash
C:\Users\John>cd \nC:\>mkdir \goaway
C:\>cd goaway

C:\goaway>mklink /D dir1 c:\goaway\ 
symbolic link created for dir1 <<==>> c:\goaway\ 
```

```
Directory of C:\goaway\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1\dir1
10/01/2011 07:29 AM <DIR> .
10/01/2011 07:29 AM <DIR> ..
10/01/2011 07:29 AM <SYMLINK> dir1 [c:\goaway\]

 0 File(s) 0 bytes
Total Files Listed:
 0 File(s) 0 bytes
96 Dir(s) 8,044,331,008 bytes free
```

```
C:\goaway>mklink /D dir2 c:\goaway\ 
```
Make A Web Labyrinth

[root@OCM labyrinth]# wget -r http://127.0.0.1/labyrinth

2011-01-18 09:25:43--  http://127.0.0.1/labyrinth/ODM5MDYyNg/MTk4MzEzOTY
Connecting to 127.0.0.1:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3448 (3.4K) [text/html]
Saving to: “127.0.0.1/labyrinth/ODM5MDYyNg/MTk4MzEzOTY”

100%[================================================================]=> 3,448  ---K/s in 0s

2011-01-18 09:25:43 (478 MB/s) - “127.0.0.1/labyrinth/ODM5MDYyNg/MTk4MzEzOTY” saved [3448/3448]

2011-01-18 09:25:43--  http://127.0.0.1/labyrinth/ODM5MDYyNg/MTExMTQ1NQ
Connecting to 127.0.0.1:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2983 (2.9K) [text/html]
Saving to: “127.0.0.1/labyrinth/ODM5MDYyNg/MTExMTQ1NQ”

100%[================================================================]=> 2,983  ---K/s in 0s
Implement Wireless Trap

**Step 1**: Setup a hidden SSID ("private" or "guest")

**Step 2**: Use a captive portal when people connect to it

**Step 3**: Portal login page contains Beef hook or SET exploit (use your warning banner!)

**Step 4**: Collect information about attacker (dissolvable agents)

**Step 5**: (OPTIONAL) Ban Wifi Mac on WIPS and/or Wireless network (works until they change it)
Make An Evil Java App

⚠️ Embed a malicious Java Application in a non-production web server
  • Usually in a directory that is noindex and/or nofollow in robots.txt

⚠️ The attacker/victim will get a pop-up asking if they want to open the Java application

⚠️ They will, attackers tend to be very curious

⚠️ The payload can be flexible (Shell, Rootkit, VNC)

⚠️ You can automatically run enumeration scripts when the attacker/victim runs the application
The Point Is...

⚠️ You may not be ready for a penetration test, and that’s okay

⚠️ Good vulnerability management is key to your success

⚠️ There are good and bad penetration tests

⚠️ Ask the right questions to weed out the bad ones

⚠️ Make attackers and pen testers alike work harder by using offensive countermeasures
Listen

- http://pauldotcom.com/podcast
- Podcast in iTunes (audio/video)

Watch

- Live! http://pauldotcom.com/live
- “TV” http://pauldotcom.blip.tv
Participate

- Discussion List: http://mail.pauldotcom.com
- Chat: irc.freenode.net #pauldotcom

Read

- Newsletter: http://pauldotcom.com/insider
- Blog: http://pauldotcom.com
- Technical Library: http://pauldotcom.com/wiki

50 Must-Read IT Blogs 2012
BizTech magazine recognizes 50 smart, useful and informative blogs in IT and small business.

If you like your IT security advice bare and without preservatives, then Paul Asadoorian, a product evangelist for Tenable Network Security, is the guy you want to talk to. As part of his robust security blog, Paul runs a vlog called Hack Naked TV, which is a name that, thankfully, is more figurative than literal.

Follow: @pauldotcom | Read the blog: pauldotcom.com
Want More?
(Shameless Plug)

OFFENSIVE COUNTERMEASURES: DEFENSIVE TACTICS THAT ACTUALLY WORK

Coming Soon...
Time for Questions?

We send slides and presentation updates to the PaulDotCom Insider. Go to http://pauldotcom.com/insider or scan the QR code above!