Getting Started In Information Security

© 2006 Mikael Albrecht

Paul Asadoorian

Security Weekly | Tenable Security
http://securityweekly.com | http://www.tenable.com

```
# whoami
```

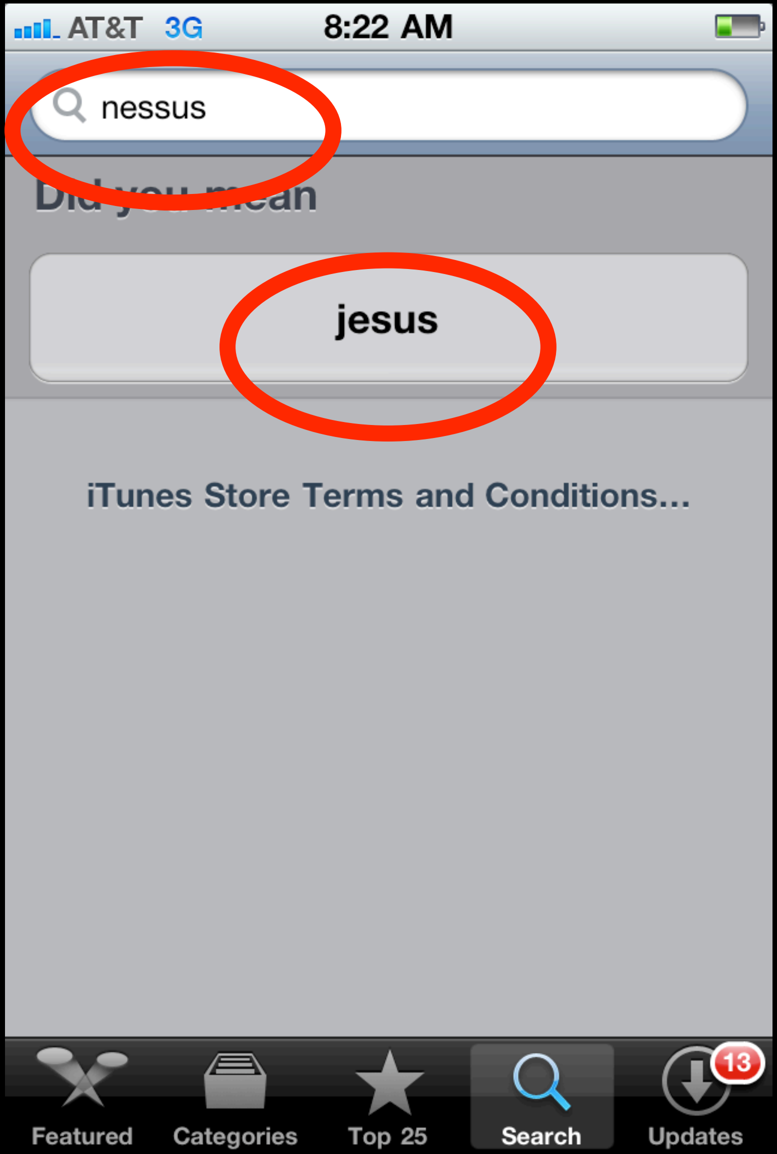
tenable
network security

Podcast
tenable.com/podcast

Tenable Network Security

- Local company in Columbia, MD
- Flagship product is Nessus, a vulnerability scanner
  - Founder wrote Nessus as a college project!
- Nessus is freely available for home use, feel free to download and use it
- Enterprise products allow organizations to correlate vulnerability data with system and network logs

Nessus®
vulnerability scanner



nessus

Did you mean

jesus

Security Weekly

http://www.securityweekly.com

Formerly “PaulDotCom”

- I provided a monthly briefing for systems administrators at a university
- Podcasts became popular, and I said “I can do that!”
- Episode 1 was recorded at a security conference in October 2005
- We just recorded episode 367
- We’ve won “Best security podcast” for the 4 time

Our First Podcast Setup Was Worse Than This

Security Weekly Today

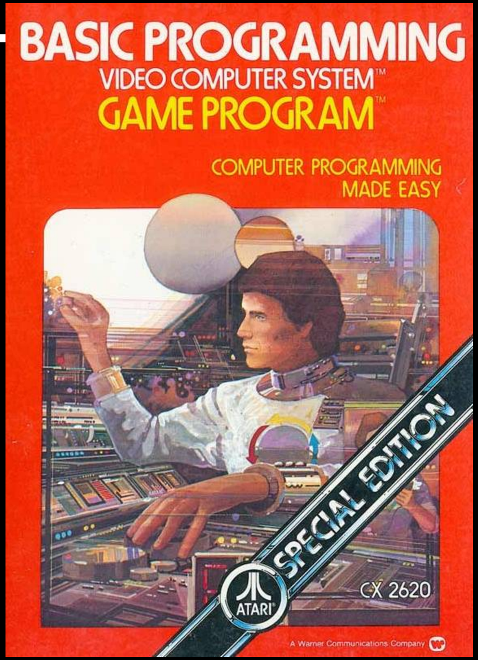
- 1100 sq. ft studio, 5 HD cameras, 3 sets
- 2 production assistants, 1 audio engineer, 1 executive producer, interns

Surround yourself with smart people

Lineco /pH Testing Pen

How I Got My Start

- The firewall administrator got sick, so I stepped in
- Fell in love with security, took all of my effort and put to use all of my skills
- I went to a SANS training conference, then studied for a certification
- I received honors for my paper on intrusion detection and write-up of buffer overflows
- Began working for SANS and writing articles



I stink at math

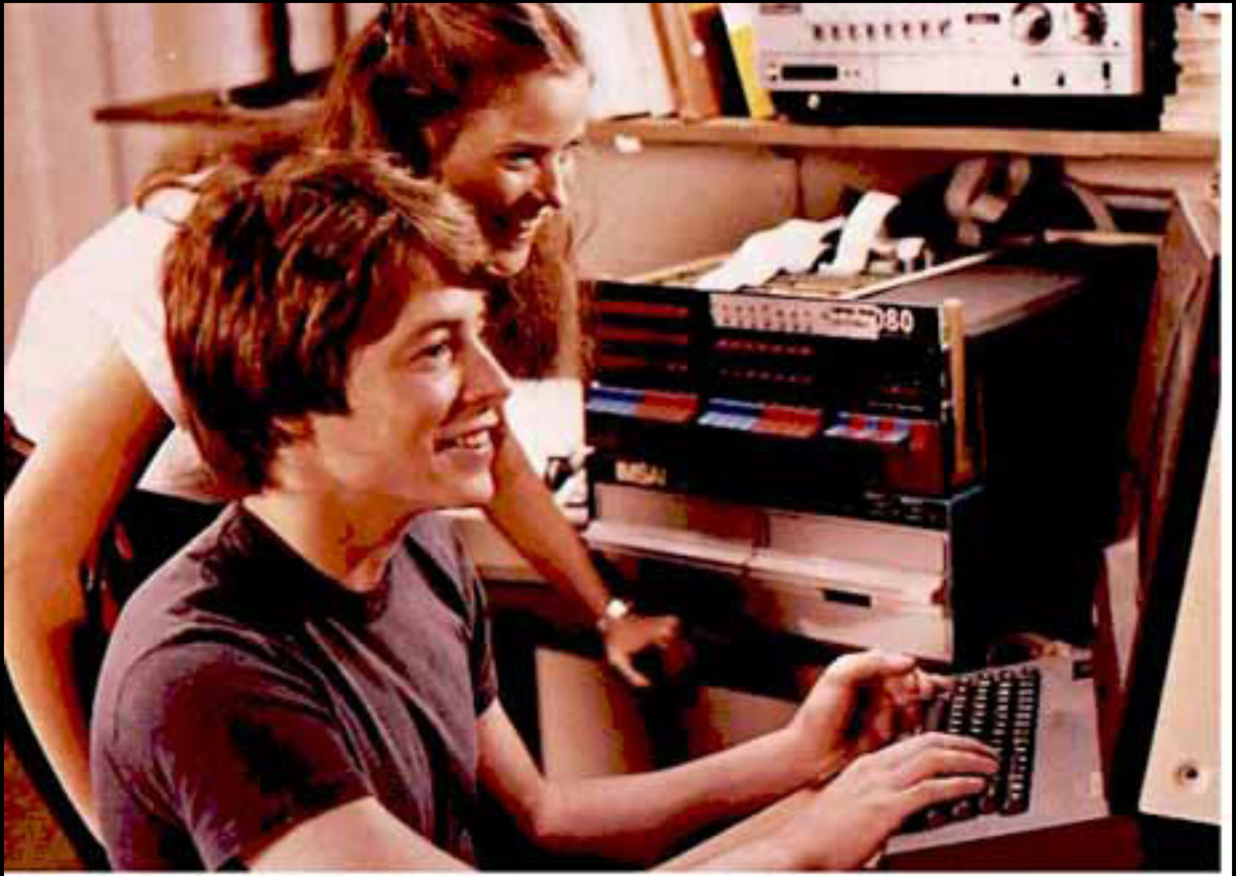
“How to become a hacker in 8 steps”

1. Embody the “hacker spirit”
2. Setup a home hacking lab
3. Work in the IT department
4. Attend local user groups & security conferences
5. Read security blogs & listen to podcasts
6. Write about security
7. Socially network yourself
8. Get hacked

How NOT to become a hacker

- Choosing a really cool NIM like “ZeroCool”
- Write 3v3ryth1ng in 1337sp3@k (translated: Write everything in “leetspeak”)
- Break into your friends computers and change their backgrounds to images of Barney and blast “Wrecking Ball” 24/7
- Violate state, federal, or international law
- Wear black all the time
- Take the “8 steps to becoming a hacker” seminar you found on the Internet

The “hacker spirit”

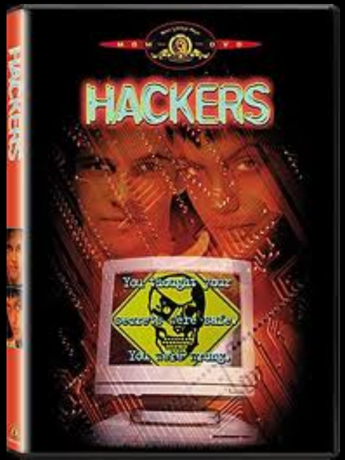


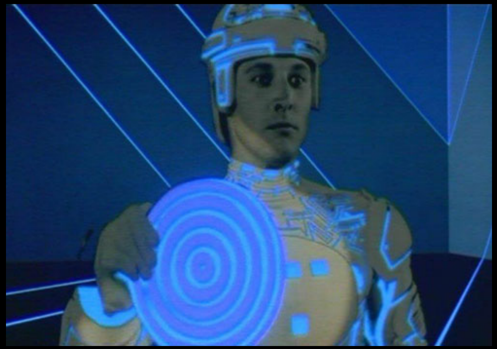
“Would you like to play global thermonuclear war?”

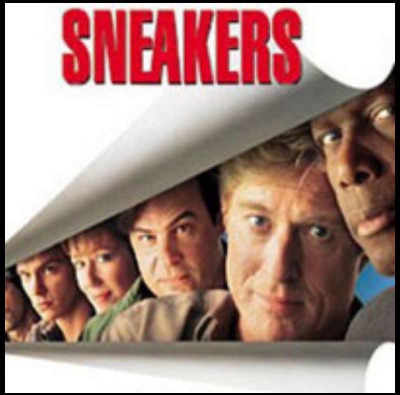
Before we go any further...

Top ten best/worst hacker movies of all time:

1. **War Games** - My parents wouldn’t let me get a modem
2. **Sneakers** - “It’s all about the information”
3. **Tron** - Cool body suits
4. **Hackers** - Angelina Jolie, do I need to say more?
5. **Swordfish** - Halle Berry, notice a trend?







JOHN HUGH HALLE DON
TRAVOLTA/JACKMAN/BERRY/CHEADLE
Log on. Hack in. Go anywhere. Steal everything.
SWORDFISH
PASSWORD ACCEPTED

Continued...

6. **The Net** - Ruining people’s lives is not cool
7. **The Matrix** - Believe whatever you want to believe
8. **Johnny Mnemonic** - Don’t format my brain
9. **Antitrust** - More about software than hacking
10. **Takedown** - Read the book instead

So You've Watched 10 movies

- Hopefully not in one sitting, but whatever
- What does it mean to be a hacker? (Note: it should have nothing to do with rollerblades or "hacking the gibson")
- Hacking really means being curious and exploring that curiosity
- Making things do stuff they were not intended to do

Be curious about technology!

Setup A Home Hacking Lab

Preferably **NOT** in your Mom’s living room, like I did…

Computers Are Cheap

- You can find old computers everywhere
- Set them up, install Linux on them (thats free too)
- You can find archives of old software to exploit:
  - www.oldapps.com
- VMware is also free, cheap, and easy to use
  - This also helps you learn virtualization
  - QEMU, Virtual box, Xen are other great options

Work In the IT Department

"Hello IT, did you turn it off then on again?"

By The Way...

- Paul’s Top 5 Hacker TV Shows:

1. **The IT Crowd** - British people are funny
2. **Tiger Team** - Don’t forget your USB cable
3. **Prototype This** - Build it!
4. **Battlestar Galactica** - Yea, its a stretch...
5. **Hak.5** - Technology and hacking stuff

*Honorable Mentions: Myth Busters and To Catch A Thief! and when you’re older, Archer

Seriously, Get A Job

- There is not better preparation for information security than working in the IT department
- Programming experience helps too, depends on where you want your career to go
- Ideally you work on the help desk, networking, systems administration
- Then move into security with a solid foundation of skills and experiences

Go To The Con

Just don’t pass out at the con (when you are of legal drinking age of course)

No Shortage of Cons

- Shmoocon
- Defcon
- Toorcon
- Quahogcon
- Brucon
- SOURCE
- Bsides
- Cansecwest
- HOPE
- Blackhat
- Derbycon
- and more...

Local Groups

- Defcon groups - DC<your area code>
- ISSA
- ISACA
- NAISG
- 2600 groups
- Infraguard chapters
- OWASP meetings
- Bsides presenting program

http://site.infosecmentors.com/

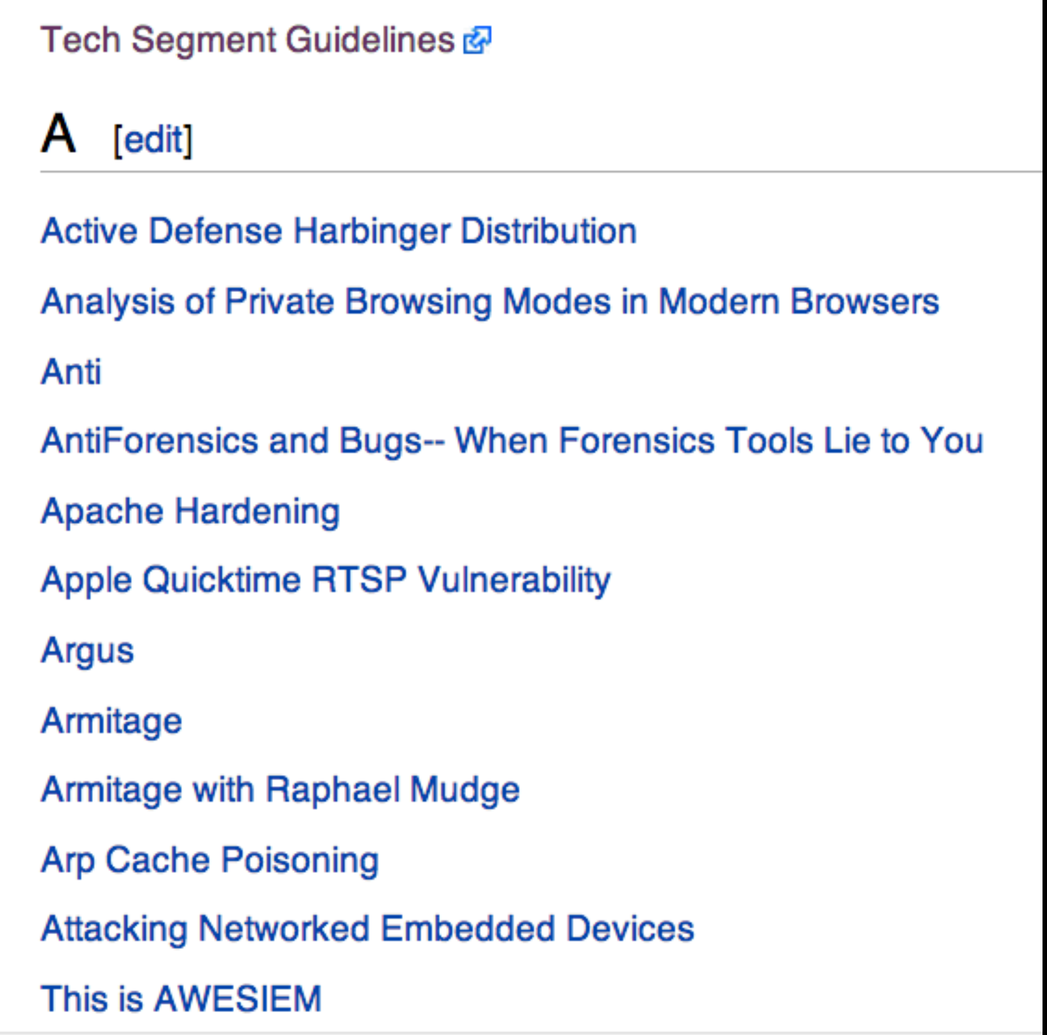
Read & Listen to Everything

Listen to Security Podcasts

- We do a weekly show called **Security Weekly (www.securityweekly.com)**
- Several others:
  - Risky Business
  - Liquid Matrix
  - Southern Fried Podcast
  - Network Security Podcast
  - Go to http://getmon.com/ for a complete list

Security Weekly: Tech Segments

- http://wiki.securityweekly.com/wiki/index.php/TechSegments
- We teach you how to do stuff
- Most recently we talked about how our web site got hacked (more on that later)
- We are always looking for technical segments



Tech Segment Guidelines

A [edit]

Active Defense Harbinger Distribution

Analysis of Private Browsing Modes in Modern Browsers

Anti

AntiForensics and Bugs-- When Forensics Tools Lie to You

Apache Hardening

Apple Quicktime RTSP Vulnerability

Argus

Armitage

Armitage with Raphael Mudge

Arp Cache Poisoning

Attacking Networked Embedded Devices

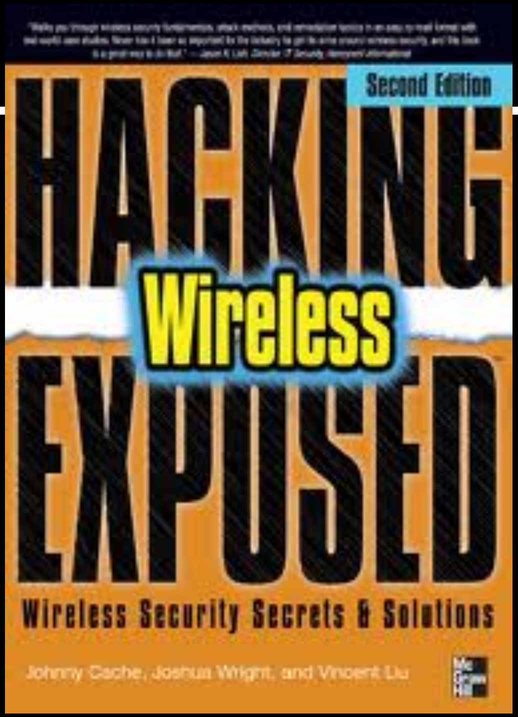
This is AWESIEM

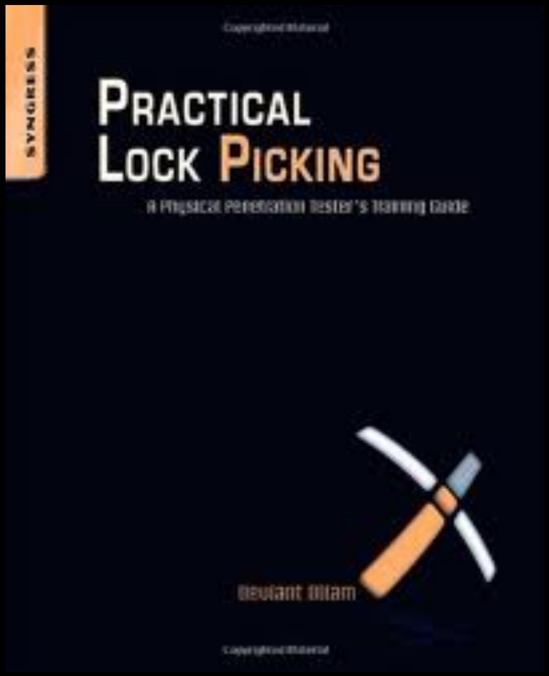
Security Weekly: Interviews

- Hundreds of interviews! Get the index here:
- http://wiki.pauldotcom.com/wiki/index.php/Interviews
- Two must watch for you:
  - Brian Snow
  - Eve Adams (http://securityweekly.com/2014/03/episode-364-eve-adams-interview.html)

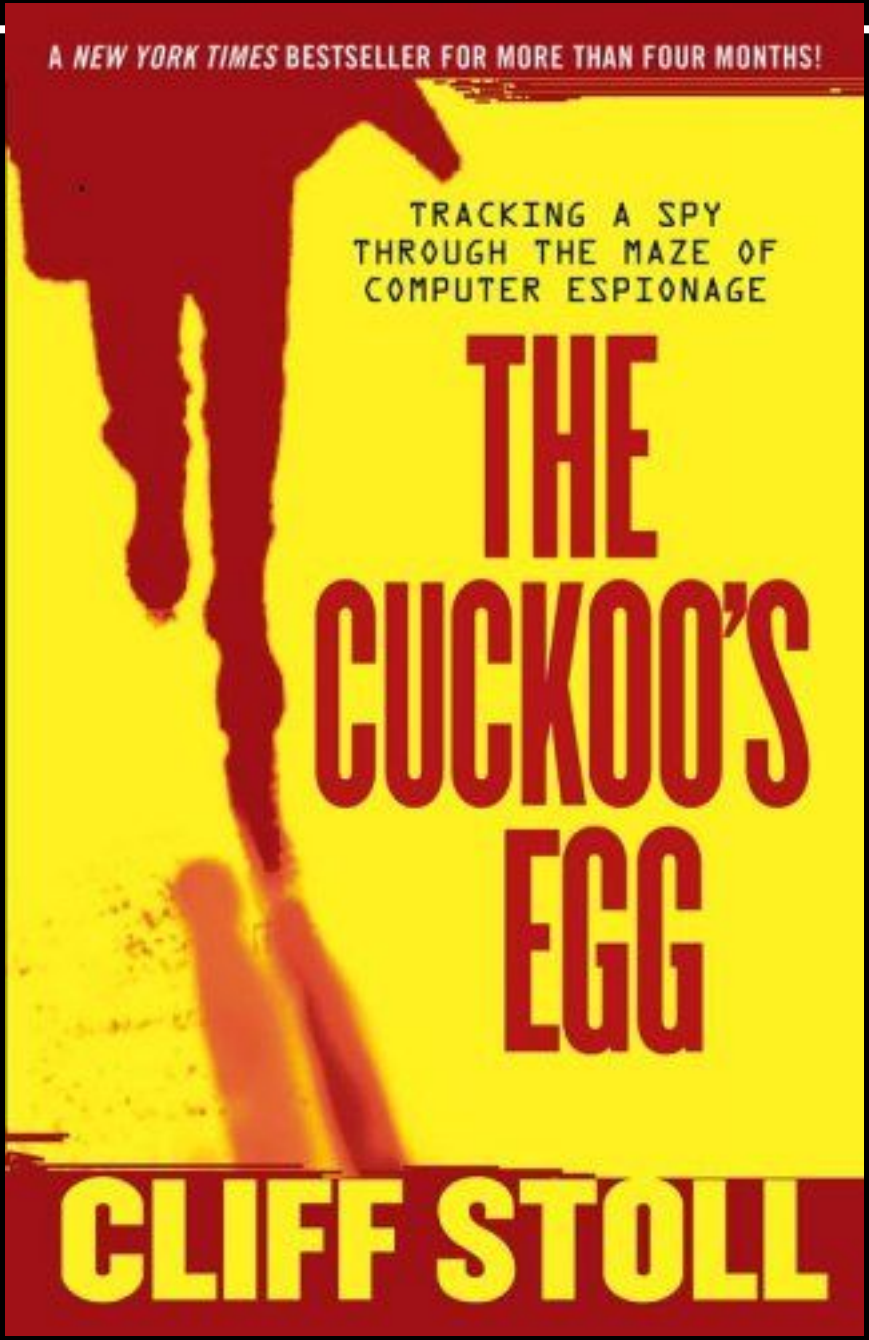
Read Stuff

- Blogs
  - I subscribe to over 500 blogs
  - You should too
  - Read them, assimilate knowledge
  - http://securityweekly.com/PaulFeeds.opml
- Books
  - So many great books, Wireless Hacking Exposed and Lockpicking by Deviant Ollom
  - I co-authored a book called “WRT54G Ultimate Hacking” and “Offensive Countermeasres: The Art Of Active Defense”


Second Edition
HACKING
Wireless
EXPOSED
Wireless Security Secrets & Solutions
Johnny Cache, Joshua Wright, and Vincent Liu
Mc Graw Hill



My Favorite Hacking Book


A NEW YORK TIMES BESTSELLER FOR MORE THAN FOUR MONTHS!
TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE
THE CUCKOO'S EGG
CLIFF STOLL

Write About Security

Speaking at conferences is cool too! (not so cool 1 week out from ACL surgery)

Start a Blog!

- Write about your experiences
- The best blogs are the “notes” of the author on how they got stuff working
- Don’t be afraid to write about stuff:
  - Setup a Linux system and write about how you configured it
  - Put custom firmware on home routers and write about it
  - Use tools like Nmap, write about it

Submit Articles

- Take on a project that creates a new project, or extends an existing one
- There are tons of online publications that would be happy to publish you
- In fact, if you write a post PaulDotCom would be happy to post it to our blog
- Or, help you get it published on another site

Don’t Be Afraid to Talk

- Submit a talk to a conference
- Don’t think this is something you cannot attain
- There are tons of conferences looking for “fresh” talent
- Submitting to a conference is good practice

Socially Network Yourself

How not to socially network yourself:

Remember, whatever you put on the Internet is public forever

Social Network Productivity

- Twitter
  - LOTS of security professionals on Twitter
  - Many events, like CCDC, are “live Tweeted”
  - Several events have a “Tweetup”
- Facebook
  - Most users BY FAR
  - Can be productive
  - Don’t play farmville

PaulDotCom On Facebook

- PaulDotCom Fan Page
  - https://www.facebook.com/pages/PaulDotCom-Security/56074056651
- PaulDotCom Facebook Group
  - https://www.facebook.com/group.php?gid=6678027341

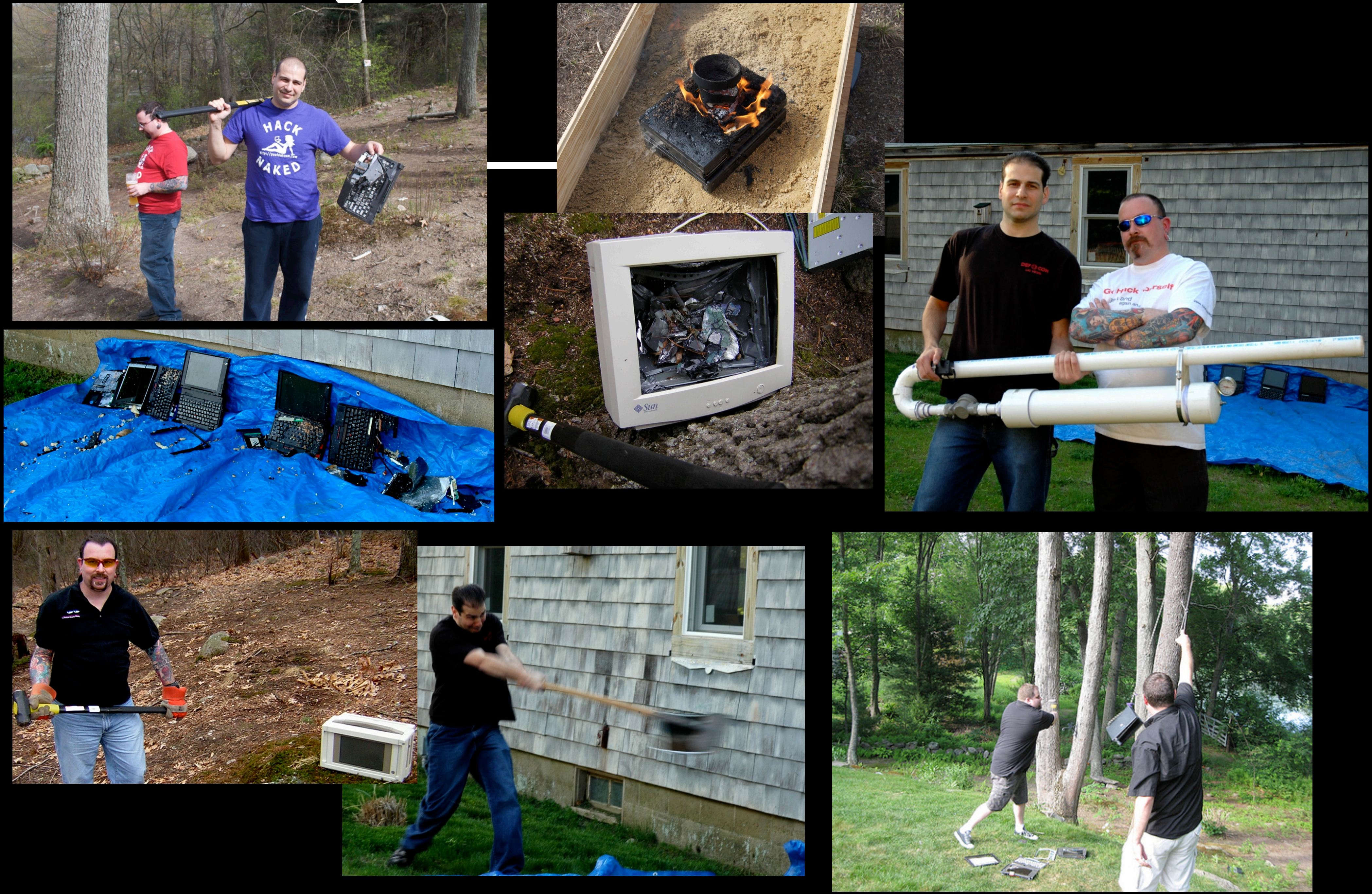
Get Hacked

No seriously, the best security people I know got started ‘cuz they got hacked

No Seriously, Get Hacked

- Attend CCDC and get attacked and hacked in a controlled environment
- Or just run a system that gets hacked
  - Friend had Red Hat systems that kept serving files via FTP
  - First week as sysadmin, had to deal with Sysadmind
  - So many security pros say, “I had a machine, it got hacked, I got sucked into security, been there since”
- Our web site got hacked, read about it here: http://wiki.pauldotcom.com/wiki/index.php/Episode366#Tech_Segment:_Wordpress_Defacement:_Lessons_Learned

Computer Destruction



BLACK HILLS INFORMATION SECURITY

http://www.blackhillsinfosec.com

tenable network security

http://tenable.com/careers

Security Weekly

THESE SLIDES: http://securityweekly.com/gettingstarted.pdf

Join Our Mailing List: http://securityweekly.com/insider

Podcasts/Blogs/Videos: http://securityweekly.com

Contact Me: paul@securityweekly.com