

# Open Source Penetration Testing for 2010

Presented by Rick Deacon

ISACA

January 21, 2010

# Bio

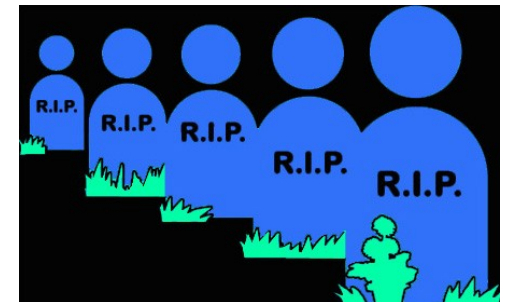
- Security Analyst/Penetration Tester at Hurricane Labs
- Information Security for 4+ years
- Presented at DEFCON 15
- Published in 2600

# Quick Agenda

- What This is About
- 2009 Overview
- Security Outlook for 2010
- The Open Source Toolbox for 2010
- What We Can Do
- Closing
- Questions

# So What Happened?

- SSL Is Broken
  - TLS/SSLv3 Renegotiation, MITM Attacks
- Predators are prey
  - Encryption is important
- Social Networks boom
  - Facebook, Twitter
- Slew of Buffer Overflows
  - Firefox, Microsoft, etc.
- Smart Phone Security(or lack there of) begins...
- Malware



# What's Up in 2010?

- SQL/XSS Attacks are less prominent
  - Better protection and countermeasures
  - More knowledge
- Buffer Overflow type attacks remain high priority
- Physical hardware hacking stays in scope but has less focus

# On to the big stuff...

The "Hot Items" of 2010

- Little explanation
- Some remediation techniques



# The Hot Items

- The Zero Day Exploit
  - These attacks are targeted on up to date software
  - Released at conferences/on forums/chats
  - Happens daily
  - Patches often take a while
    - But they are getting better!
  - Host firewalls for servers are a good starting point for protection

# The Hot Items

- Windows 7
  - "Reworked" Vista
  - Supposedly the most secure version yet
  - Will be riddled with holes/vulnerable services
  - Keeping up with patches and user awareness are a good start here



# The Hot Items

- Social Engineering
  - The rise of the misinformed employee
    - Or maybe just the exploitation?
  - Social Engineering outlines and toolkits (ie, SET)
  - Logins, password, physical information, data leakage, phishing scams
  - Opens the possibility of other types of exploitation
  - The only protection here is education



# The Hot Items

- Network Connected Devices
  - Not necessarily a new threat but one that will emerge
  - Vendors aren't prepared for these attacks
  - If it communicates... it can be hacked
  - Patches, access control and best practices win this one



# The Hot Items

- The Cloud
  - Cloud Computing on the rise in general
  - Seems less secure than once thought
    - Encryption needed for all communication
    - Data physical location(Recovery)
    - Audit Refusal
  - Understand your Service Level Agreement, use cryptography



# The Hot Items

- Virtualization
  - Also on the rise for the past few years
  - Best practices and access control not in place
  - Could allow malicious users to "break out" of the VM environment
  - Software vulnerabilities
  - More virtualization will make this a bigger target
  - Patches and best practices

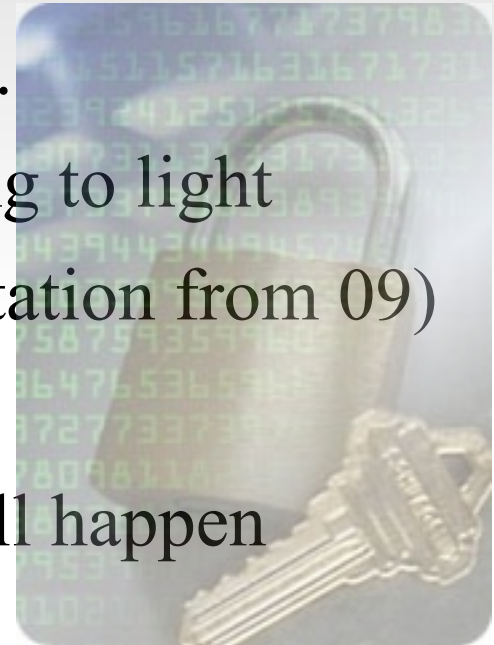
# The Hot Items



- Client Side Attacks
  - Occurs on the client/user's computer
    - Eventually uses the client as a means to get to the "better" stuff
  - Includes exploitation of vulnerabilities/Zero Day exploits
  - IE, Firefox, automatic software updates, multimedia software...
  - Client firewalls can help, proper access controls

# The Hot Items

- Cryptography
  - GSM(Cell Phones), SSL/TLS, etc.
  - Vulnerabilities/exploitation coming to light
  - MITM attacks grow(TLS Renegotiation from 09)
  - Sites will mandate SSL (Gmail)
  - Hopefully newer, better crypto will happen



# The Hot Items

- Smart Phones & Mobile Devices
  - Hold a lot more data than you think about
  - Worms/Viruses that target these devices
    - Most recently stealing bank data
  - E-mails/Calendar/Client Doc's
  - Apps could be untrustworthy
  - Watch what you keep on your phone
  - Encrypt data
  - Trusted applications



# The Hot Items

- Social Networking

The Facebook logo, consisting of the word "facebook" in white lowercase letters on a blue rectangular background.

- Debatedly the hottest item
- Privacy, Client Side Attacks, Info Leakage, Web App Security, Social Engineering, Mobile Devices, oh my...
- Needs much attention with the recent growth
- Users use it without thinking of many of the repercussions that their actions involve
- Data thrown around that normally would seem harmless
- User education and business policies for all are necessary

The Twitter logo, featuring the word "twitter" in a light blue, rounded, lowercase font with a white outline.



# The Tools

- Open Source tools can help determine what your problems will be **before someone else does**
- Penetration testing whether internal or external is a good start
- New tools and old tools combined will give us the insight needed to prepare for the issues of 2010

# What's that do?

- Nmap – Open Source port scanner at heart
  - Around for years, most popular
  - A lot more than just port scan – fingerprint, evasion techniques, custom scripting
  - What it will help us test:
    - Zero Day Exploits, Network Connected Devices, Client Side Attacks, Windows 7, everything :)
  - More information/download from <http://www.nmap.org>

# What's that do?

- OpenVAS – Open Source vulnerability scanner
  - Alternative to Nessus
  - Gives a general idea of what vulnerabilities exist on your network
  - Requires manual testing as well for accuracy
  - Slight learning curve
  - What it will help us test:
    - Many things (assuming the plugins exist)
    - Write your own plugins
  - More information: <http://www.openvas.org/>



# What's that do?

- Metasploit – Exploitation Framework
  - Developed for penetration testing to exploit known vulnerabilities
  - Updated often with the newest vulns
  - Lets you see the practicality of an attack and what it will do to your systems
  - Fun stuff!
  - What will this help us test:
    - Zero Day, Windows 7, Client Side Attacks
  - More info at <http://www.metasploit.com/>



# What's that do?

- TCPDump, Wireshark
  - Packet capture tools(others exist)
  - Existed for a long time
  - Essential to any sort of network troubleshooting
  - Also good for penetration testing
    - Analyze data passed over network
    - Sniff passwords, authentication
    - View web traffic
  - Helps us with:
    - Network Connected Devices, Cryptography attacks
  - More info at <http://www.tcpdump.org>, <http://www.wireshark.org>



# What's that do?

- Social Engineering Framework
  - Social Engineering Toolkit(SET)
  - Lets you test your users' security knowledge
  - Assists with all facets of Social Engineering
  - <http://www.social-engineer.org>
- Vulnerability Databases
  - OSVDB, Offensive Security, Security Focus, etc.
  - Keep on top of latest vulnerabilities
  - Downloadable exploits usable for testing

# Where's that leave us?

- That leaves us kind of up in the air for some stuff...
  - Cloud Computing, Virtualization, Smart Phones/Mobile Devices, Network Connected Devices...
- Tools exist but they're still being developed
- This is the reason WHY they're on the hot list for 2010
- Time for research and development...

# I Want It All!

- A good "hacker" starting place is Backtrack
- Open Source Penetration Testing Linux distro
- Based on Ubuntu
- Simple to download/install/use
- Can be booted as a LiveCD or installed
- Excellent development work



# The Testing Procedure

- So now that we have our tools in place...
- Perform all your testing in a lab/with permission
- Take your time
- Record all data
- Solutions? Share them!



# The Users

- A number of the 2010 outlook issues involve human error
- Pen test the people as well
- User awareness, password policies, basic computer knowledge, social networking(if allowed) awareness, phishing scam detection...
- Have some fun with this one



# The Next Step

- Need more assurance?
  - Hire a third party for a penetration test
- Stay updated on all patches and updates
- Stay on top of security research and trends
- Educate your users
- Be aware of your network as a whole

# Summary

- Penetration Testing can help you plan ahead
- 2010 Security Outlook is well informed
- 2009 left us with some interesting stuff
- 2010 probably won't disappoint.  
... but let's hope it does

# Contact/Questions

- Contacting me:
  - rick@hurricanelabs.com
  - rickdeaconx@gmail.com
  - @rickdeaconx on Twitter

Questions?