Off the Wire: Wireless Penetration Testing Basics & Ethical Considerations

Derek E. Isaacs

CISSP, Security+, CEH, CNDA

Road Map For This Presentation

- The presentation goals
- Overview of instructional issues
- A short course on Wireless Penetration Testing
  - The security perspective
- Review of ethical issues
- Discussion & examples
- Questions

Boecore

Colorado Technical University™
TAKE YOUR CAREER TO NEW HEIGHTS®

Expectations

- This is a presentation - not a “lecture”
- Please:
  - Ask questions at the end . . .
    - ☞ Although I may not be able to provide specific details . . .
      - *Due mainly to ethical concerns!*
- I don’t have any need to plow through these slides!
  - And I will make them available to you (via an e-mail request)
    - ☞ See the final slide or the presenter at lunchtime!
- I will have failed if - I don’t make you stop and think . . .
  - (or at least make you a little uneasy . . .)

Goals (Why Am I Here?)

- Define the wireless penetration test, also called a pen test and “ethical hacking”
- Talk about the legal / ethical issues
  - ECPA considerations
- Discuss setting some boundaries . . . goals. . . limits
- Talk about when things go bad – and (yes) they will
- Walk through the major wireless pen test steps & definitions

Teaching Focus

- Computer / Information Security
  - A series of stand-alone courses and modules
    - Operating systems
    - Networking
    - Certification and accreditation

- The modules are intended to introduce “computer security” early and often throughout the curriculum
  - When you take the courses – one gets the impression that security is important, relevant, and “fun”!

I hear...and I forget
I see...and I remember
I do...and I understand

Ancient Chinese Proverb

Pedagogy Issues

- Are we training hackers?
  - No
- Does teaching someone about security vulnerabilities / exploits invite trouble?
  - Perhaps
- Do you have to study the adversary (black hat) to be a better defender (white hat)?
  - I believe so . . .
    - You need to instantiate a "*Hacker frame of mind . . .*"
- What should a "computer security" course teach?
  - Theory?
    - What theory?
  - Practice?
    - What is meant by "practice"? How to attack?
  - Tools? For what purpose?

Pedagogy Issues (continued)

- If you include practical exercises involving computer security …
  - How do you protect campus networks and machines?
    - How do you protect ‘outside’ networks where students may ‘practice’?
  - How do you distinguish between teaching the tools / techniques for legitimate defense versus those used solely for malicious purposes?
  - How much “privilege” do you grant students? Root/Admin?
  - Do teaching faculty need to be experts in security?
    - How can you limit liability ‘Off Campus’?

Goals Of The Assignment

- Get some hands-on networking experience
- Get some hands-on network monitoring and packet dissection experience
- Learn how secure different protocols are
- Learn about common attacks on clear-text protocols
- DON'T end up in jail !
  - Never test your code outside of an environment you have permission to use!

Reconnoitering

- Goal: observe network traffic, learn about different protocols
- Installed tools (must be run as root-or from Knoppix-STD):
  - Ettercap
    - Focuses on the “Network Inventory”
    - Great for probing networks and generating target lists!
  - Ethereal/Wireshark & Etherape
    - Like tcpdump, but with more smarts about protocols
    - Etherape is a graphical network traffic representation
    - Sniffer used for examining application level data (i.e passwords)!
  - Nmap
    - Focuses on the payloads and packets
    - Great for probing systems!

Dangerous Territory

- This is an area in which one could cross over to “the dark side”
  - Why would you want to actually install and test a rootkit?
  - What point is served by performing a DoS attack?
  - Why actually re-create a buffer overflow attack?
- What about testing a MITM* attack? Is there any value in that?
  *(*Man In The Middle)*
- Log analysis is a very worthwhile practical experience!
  - Nothing beats actual ‘hands-on’ for learning
    - ☞ Program analysis vs. compilation results
      - My Mies van der Rohe example . . .

A Question For You

- Should we teach someone how to write computer viruses?
- Several university CS departments do -
  - Their argument: the best (only?) way to defend against viruses is to fully understand how to write viruses (how they work)
    - We're back to that "Hacker frame of mind'
- Counter-argument
  - Doesn't teaching the "art" of virus writing make it more likely that more and newer (more clever?) viruses will be written (by those students?)
- What do you think?

My Response

- We focus on teaching about vulnerabilities and exploits, but not threats
  - We would not teach the "how-to" of virus writing
  - We'd leave that to the actual security professionals
    - We assume they have very strict rules regarding ethics / behavior
- From Gene Spafford: "A good course, taught by a competent instructor, focuses on the underlying concepts and the defenses against them."

Comparative Review

- What are the differences between a penetration yest, a vulnerability assessment and an audit?
- People sometimes use these terms interchangeably
- There are definitely some critical (and distinct) differences.

Penetration Testing

- This definition is taken from the FFIEC (Federal Financial Institutions Examination Council) Information Security booklet:

"Penetration tests, audits, and assessments can use similar sets of tools in their methodologies. The nature of the tests, however, is decidedly different. Additionally, the definitions of penetration test and assessment, in particular, are not universally held and have changed over time."

Comparisons

	Penetration Test	Vulnerability Assessment	Audit
Initial Info	Limited	Limited	Full
Outcome	Access to Internal Network	List of Vulns	Secure System
Location	Internal / External	External	On System
Time	Medium	Short	Long

Ethics

- An objectively defined standard of right and wrong
- Often idealistic principles
- In a given situation several ethical issues may be present
- Different from law – in many ways
- Laws are rules adopted and enforced by governments to codify expected behavior in modern society
- Key difference between law and ethics is that
  - law carries the sanction of a governing authority and ethics do not
- Ethics are based on cultural mores:
  - relatively fixed moral attitudes or customs of a societal group

Law vs. Ethics

Law

- Described by formal written documents
- Interpreted by courts
- Established by legislatures representing all people
- Applicable to everyone
- Priority determined by laws if two laws conflict
- Court is final arbiter for right
- Enforceable by police and courts

Ethics

- Described by unwritten principles
- Interpreted by each individual
- Presented by philosophers, religions, professional groups
- Personal choice
- Priority determined by an individual if two principles conflict
- No external arbiter
- Limited enforcement – usually the “court of public opinion”

The Ten Commandments of Computer Ethics (from the Computer Ethics Institute)

- Thou shalt not use a computer to harm other people
- Thou shalt not interfere with other people's computer work
- Thou shalt not snoop around in other people's computer files
- Thou shalt not use a computer to steal
- Thou shalt not use a computer to bear false witness
- Thou shalt not copy or use proprietary software for which you have not paid
- Thou shalt not use other people's computer resources without authorization or proper compensation
- Thou shalt not appropriate other people's intellectual output
- Thou shalt think about the social consequences of the program you are writing or the system you are designing
- Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans

Legal Issues As We Start

- First, can you do what you want to do where you want to do it?
  - Is a war-dialing legal / ethical against your own systems when going through a central office?
  - Is hacking into your own wireless system allowed for "evaluation purposes?
    - "Just because a thing can be done – doesn't necessarily mean it should be done"
      - Paraphrased from Mr. Spock – Star Trek 6 – The Undiscovered Country
- Make sure you are protected with a "Letter of Authority".
  - Protect yourself with a "Get out of jail" type letter. More on this in a minute.
- Encrypt your data. You don't want to be liable if *your* data is compromised.
  - The evidence YOU find and derive MUST be protected – otherwise YOU are now causing a data breach.

More Legalese

- Watch, and throttle if necessary, your generated network traffic…Think stealth and covert.
  - Don’t let the right hand know what the left hand is doing . . .
- Think through your actions before doing them.
  - If it seems like a dumb or silly thing to do –
    - **Don’t do it.**
- Run these tools at your own risk. I am not responsible for your actions

  {but I will send you postcards in jail ☺}

More Legalese (cont'd)

- Test your tactics and methods first on a stand-alone network with a network sniffer - and review all the source code
  - Obtain tools from the source – compile your own
    - Remember what happens when you "Assume"
  - Verify checksums from multiple sources when applicable

- Log all of your actions
  - Think like a lawyer – Evidence is essential!
    - Keep extensive records of ALL of your steps, actions, and responses!

Why Would You Want To Do a Penetration Test?

- If you only want to measure risk, think about an assessment which will give you a better review of the current security mechanisms.
- A penetration test is used to show where security fails – more specifically – how others get in
  - *Remember – it's not just hacking from outside!*
- Can test intrusion detection and incident response to activity
  - *Really a test of "What happens when I push this button?"*
- Can be used to justify the need for an upgrade, bigger budget, or to validate risk assessments.

What Are Your Boundaries?

- Be as aggressive as you can and work to be creative. Now is when you can use the “thinking out of the box” ideas.
- Don’t get tunnel vision – stay “big picture”
- Are you going to do physical penetrations?
  - Actually trying to break-in vs. wandering where you shouldn’t?

    or
  - Only electronic penetration
- What about “social engineering”?

What Are Your Boundaries? (Cont'd)

- Application and internet service providers (how can you use them?) [Remember NOT to interfere or trespass on THEIR turf]
- Externally hosted resources – observe – but don't touch
- Non-target company equipment – keep away
- All need to be addressed with each customer and agreed upon
  - In advance, in writing, with signatures and witnesses!

Penetration Testing Methodology

- Let's walk through the following major steps of a pen-test:
  - Recon / foot printing
  - Scanning
    - Enumeration
  - Exploiting / penetrating
    - Privilege escalation as required
  - Data collection aka "limited pillaging"
  - Cleaning-Up
  - Prepare & deliver report / presentation

Technique – Penetration Testing

1) Gather information
2) Scan targets & reconnoiter
3) Evaluate information
4) Exploit vulnerable services
5) Elevate access
6) Repeat

(almost like shampoo!)

Scan Target Systems

- Goal – Given a set of IP addresses, determine what services and operating systems each is running.
- Nmap – www.nmap.org
- Ettercap - http://ettercap.sourceforge.net/download.php
- Scanline – www.foundstone.com
- nikto - http://www.cirt.net/code/nikto.shtml
- Bactrack2/Bactrack3
- Auditor
- Metasploit

Developing a Methodology

- Work on establishing your own methodology using some pre-existing methodologies as guides:
  - SANS
  - Institute for Security and Open Source Methodologies (ISECOM)
  - Common Criteria
  - OSSTIM
    - More on this in a minute . . .

Developing a Methodology (Cont'd)

- Complete at least a rough draft of your methodology before starting -and finalize it after your first penetration test.
  - What worked, what didn't, and what (you think) went awry.
- Your methodology should be a living document.
  - Always growing/changing/evolving

The OSSTMM

OSSTMM – Open-Source Security Testing Methodology Manual

Version 2.2 at www.osstmm.org (this redirects to the site: http://www.isecom.org/projects/osstmm.htm)

Developed by Pete Herzog, it is a living document on how to perform a penetration test.

It defines how to go about performing a pen test, but does not go into the actual tools or techniques.

(We'd need much more than our 45 minutes to effectively indoctrinate you on this - btw . . .)

Reconnaissance and Foot Printing

- Look, but don't touch
- This is a lot of web-based searching and reviewing
- Fire-Up the browser and review:
  - Monster/HotJobs/Dice, etc.
  - All Whois (www.allwhois.com)
  - ARIN Whois (www.arin.net)
    - or APNIC, Ripe Whois, LAPNIC
  - Sam Spade Microsoft Windows application
  - Sam Spade.org
  - US SEC's Edgar database

Murphy's Law

- Everything that goes wrong on the target host, network, or on the Internet from two weeks before you plug in to two weeks after you submit the report will be your fault
  - You must have caused it somehow!
- Document everything!
  - We're back in that evidentiary 'frame of mind'
- Can you script operations to increase efficiency and reduce errors?

What Do We Want To Teach Students Regarding How To Get Access?

- Install sniffer on server or administrators network
- Have console access (local exploits or maybe there is no PW protected screen saver)
- Grab documents, configurations, any other documentation
- Grab back-up tapes or other media for review
- Make your own back-up

Wireless Network Scanning

- Hosts, services, O/S, banners, etc.
- What they (attackers) already know about you!
- Also useful to have DHCP leases, MAC/IP mappings...
- Useful for effective response:
  - New exploit affects IIS on Windows 200X
  - What computers are running Win2k03 with IIS?
- Useful tools: nmap, ettercap, Metasploit, AirMagnet

Exploit Sites …. Find Your Own!

- www.packetstormsecurity.org
- neworder.box.sk/
- www.securiteam.com/exploits
- www.hoobie.net/security/exploits/
- www.insecure.org/sploits.html
- www.astalavista.com/tools

- IRC Channels

- Usenet Groups
- Lots of others . .
  - *(remember this is an overview – not a specific "How To")*

Are You Really Vulnerable?

- In a word: Yes. ☹ Sorry.
- If you are connected to the Internet, someone could probably break into your network, if they had the desire, time and money.
- Difference between breaking into YOUR system and breaking into a system.
- Script kiddie – wants to break into a system. If your system is better protected then the next guys, your safe. (Sorry next guy.)
- Malicious ex-employee, distrusted insider, etc. – wants to break into YOUR system. These people are hard to defend against because they will spend more than 5 minutes on your system.

What Do YOU Think?

- Hacking into government systems to point out security flaws without harm to the system?
  - Ethical?
  - Not Ethical?
- Hacking into a home computer to point out security flaws?
  - Ethical?
  - Not Ethical?
- What about using your neighbors wireless?
  - Ethical?
  - Not Ethical?

What Do YOU Think?

- A student specializing in computer security creates a website similar to Braniff Airlines to demonstrate that terrorists can make fake boarding passes.
  - Ethical?
  - Not ethical?
- A data collecting company claims to keep certain information private, such as SSN and account numbers. A hacker discovers that the company did not keep its promise. The private information is actually published on the report. The hacker makes his findings public in a news outlet.
  - Ethical?
  - Not ethical?

Wireless Security

- Wireless networks becoming prevalent
- New security concerns
  - More attack opportunities
    - No need for physical access
  - Attack from a distance
    - 1km or more with good antennae
  - No physical evidence of attack
- Typical LAN protection insufficient
  - Need stronger technological measures

Practical Considerations

- Park van outside of house or office
  - With good antenna and line of sight, can be many blocks away
- Use off-the-shelf wireless card
- Monitor and inject traffic
  - Injection potentially difficult, but possible
- Software to do Fluhrer et al attack readily available

Defenses

- Various commercial 802.11 enhancements
  - Almost always, “enhanced security” means better key management
  - Does not protect against active attacks (reaction, redirection) or the Fluhrer et al attack
- Wait for next version of WEP
  - Still in progress
- Use a VPN over the wireless network
  - Assumes wireless LAN untrusted
  - Works around any security flaws

Conclusions

- Security is difficult to achieve
  - Even when good cryptography is used
- WEP is insufficient to protect privacy
  - All security goals can be compromised
  - Use other technologies to secure transmissions
- More information at:

  http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

For More Information

Boecore:

- URL: www.Boecore.com
- E-mail: Scott.Boe@Boecore.com
- These slides:
  - Send an e-mail request to:
    - Tracy.Sharples@boecore.com

Colorado Technical University:

- URL: http://www.coloradotech.edu/
- E-mail: jklag@coloradotech.edu

Boecore

Colorado Technical University™
TAKE YOUR CAREER TO NEW HEIGHTS®