

Ethical Hacking...

Mind the Gap with Business



ISACA Round Table 10/2011 - Xavier Mertens

\$ whoami

- Xavier Mertens
- Security Consultant @ Telenet (C-CURE)
- CISSP, CISA, CeH
- Security Blogger
- Volunteer for security projects:



\$ cat disclaimer.txt

“The opinions expressed in this presentation are those of the speaker and do not reflect those of past, present or future employers, partners or customers”

Agenda

- You said “ethical hacking”?
- Some frameworks
- The process
- Some tips

**You said “Ethical
Hacking”?**

“Ethic”

“A set of moral principles of right and wrong that are accepted by an individual or a social group”



“Hacking”

“Practice of modifying computer hardware/software or any other electronic device to accomplish a goal outside of the creator’s original purpose. People who engage in computer hacking activities are often called ‘hackers’.”



Hackers are good guys

The term 'hacker' has been misrepresented in popular media for a long time!

“Hacking has nothing to do with criminal activities such as identity theft and electronic trespassing! Rather, it [hacker] has been coined at the Massachusetts Institute of Technology (MIT) as a term for curious individuals for whom every device or piece of software is full of exciting challenges to develop potential improvements or discover alternative uses.”



But some derive...

Hacking can be used to break into computers for personal or commercial gains or for malicious activities.

Those are called “Black Hats”



Can hacking be “ethical”?

Yes, of course!

Using the same tools and techniques as bad guys, security vulnerabilities are discovered then disclosed and patched (sometimes ;-)



Ethical Hacking is...

An individual who is usually employed with the organization and who can be trusted to undertake an attempt to penetrate computer systems using the same methods as a Hacker.

Ethical hacking is:

- Legal
- Granted by the target
- Scope clearly defined / NDA
- Non destructive

Also Known As...

- Pentesting
- White-hat hacking
- Red-teaming



Communities

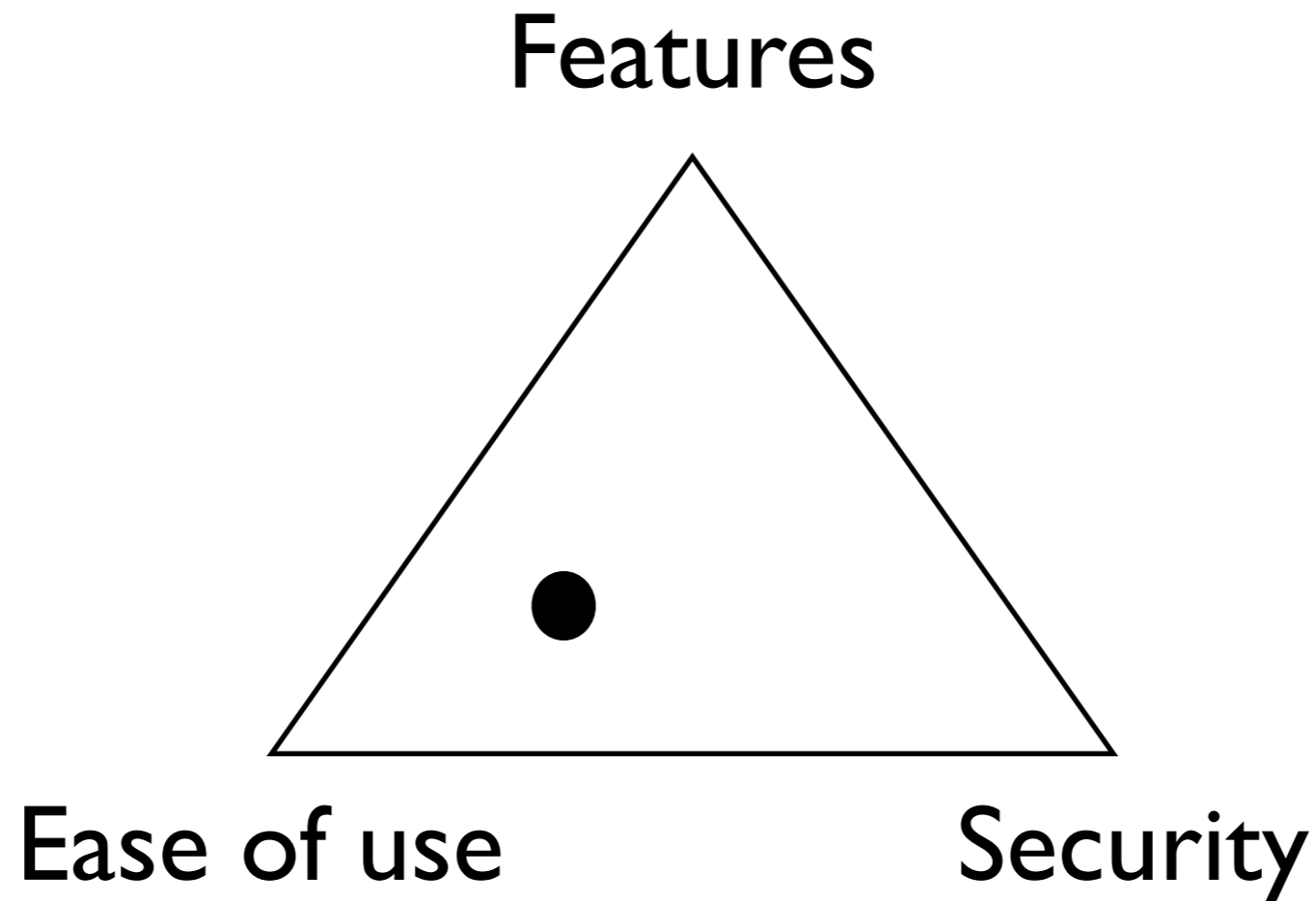
Security conference tries to create bridges between the various actors active in computer security world, included but not limited to hackers, security professionals, security communities, non-profit organizations, CERTs, students, law enforcement agencies, etc.....



Security Researchers

- Develop tools to understand how attacks work and how to reproduce it
- Search for software vulnerabilities with the debate of full-disclosure vs. responsible-disclosure
- Prosecuted in some countries
- Research is mandatory!

Why are we vulnerable?



New features/ease of use reduce the security or at least increase the attack surface!

Nothing new...

- Confidentiality
- Integrity
- Availability

Some Testing Frameworks

OSSTMM

- “Open Source Testing Methodology Manual”
- Based on a scientific method
- Divided in 4 groups: Scope, Channel, Index & Vector
- <http://www.isecom.org/osstmm>



ISSAF

- “Information Systems Security Assessment Framework”
- Focus on 2 areas: Technical & Managerial
- <http://www.oissg.org/issaf>



OWASP Top Ten

- Open Web Application Security Project
- Focus on the application layer (websites)
- <http://www.owasp.org/>



PTES

- “Penetration Testing Execution Standard”
- It is a new standard (Alpha) designed to provide both businesses and security service providers with a common language and scope for performing penetration testing
- <http://www.pentest-standard.org>



Forget the frameworks!

- Ethical hacking is highly technical
- Use your imagination!
- Be “vicious”!
- Think as a “bad boy”!



Let's use a standard

- Check-lists suxx!
- Reporting a list of CVE's or MS security bulletins is irrelevant
- Need of translation from technical risks into business risks
 - Loss of profit
 - Loss of confidentiality
 - Hit the management!

The Process

Process

- Preparation
- Reconnaissance
- Scanning
- Gaining access
- Maintaining access
- Clearing tracks
- Reporting

Preparation

- Define a clear scope with the customer
- Contract
 - Protection against legal issues
 - Definition of limits and danger
 - Which tests are permitted
 - Time window / Total time
- Key people
- NDA



Some scope examples

- An business application
- Physical security
- Wi-Fi
- DMZ
- A website
- ...



Reconnaissance

- Active / Passive
- Information gathering
- Target discovery
- Enumeration



Scanning

- Based on data collected during the reconnaissance phase
- Searching for vulnerabilities to attack the target



Gaining Access

- “Target Exploration”
- Exploitation of the discovered vulnerabilities
- Privilege escalation



Maintaining Access

- Trying to gain/keep the ownership of the compromised system
- Zombie systems



Covering Tracks

- Clear all trace of the attack
- Log files
- Tunneling
- Steganography



Reporting

- Critical step!
- At all levels, keep evidences (logs, screenshots, recordings)
- Use a mind-mapping software
- Think to the target audience while writing your report



Some Tips

Internet is your friend!

- Google! All the required information is online
- Documents meta-data (FOCA)
- Social engineering (**WE**'re the weakest link)
 - Maltego / Facebook / LinkedIn
- Fuzzing

Build Your Toolbox

- There exists specialized Linux distributions like BackTrack or Samurai
- Physical tools (cables, converters, lock-picking kits)
- Software tools
(We are all lazy people)



Keep in mind...

- Information is never far-away (often public)
- Broaden your mind (react as your victim)
- Everything is a question of time! (\$\$\$)
- Do not criticize customer. If they fail, don't laugh!
- Use your imagination
- Be vicious!

Conclusions

Why EH is good?

- Address your security from an attacker perspective
- Some audit results might give a false sense of security
- Protect company values
- Preserve corporate image and customer loyalty

Thank You!
Q&A?

<http://blog.rootshell.be>

<http://twitter.com/xme>