Know your enemy!

- Understand their Business
- Probe the network
  - What are they about?
  - Use Social Media
- Do the boring homework
  - Hacking is only easy in Hollywood

Presentation date 24/04/2011
Know your own skills!

• Understand who you are!
• This is not fun or treated as such by authorities.
• Set yourself a goal
• Learn on your machine
• Know your limits – Stick to them!
Know the punishment!

- The bigger the fish, the bigger the stick!
- Can any hacking be called fun?
  - Neighbours wi-fi
  - Will you like what you find out?
- Do you really want to go down this route?
• I run automated tools – I am a hacker...
  – Can you cover your tracks?
  – These tools have signatures

• Police will knock on your door with a warrant and seize everything.
  – Not a game

Do not Get Caught
**Self Defence**

**Vulnerable points with methods of attack**

- Eyes — fist, fingers
- Ears — flat of hand
- Bridge of nose — back fist, head
- Chin — kick, fist, elbow
- Windpipe — fist, elbow, chop
- Solar plexus — kick, knee, fist
- Groin — kick, knee, fist
- Knee — kick to front or side
- Shin — kick
- Instep — stamp on

- Do not pick the 7ft 350 lbs ninja to fight (unless you're that good)
- Actions have a purpose
  - Random arm/leg movements ineffective.
- What are the consequences.

Presentation date 24/04/2011
• Don't attack the 7ft ninja...
• Create a plan
  – Stick to it
  – Step through it
• Take notes as you go
• You will get arrested if you do more then a probe
  – Maybe even then?
• All systems have a fatal flaw
• If you are good enough you may find it.
  – What do you do with this info?
  – Google pay for defects found...
• An attack at this point is illegal
  – Not recommended

See – I told you I could do it!
### Mapping from 2007 to 2010 Top 10

<table>
<thead>
<tr>
<th>OWASP Top 10 – 2007 (Previous)</th>
<th>OWASP Top 10 – 2010 (New)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2 – Injection Flaws</td>
<td>A1 – Injection</td>
</tr>
<tr>
<td>A1 – Cross Site Scripting (XSS)</td>
<td>A2 – Cross Site Scripting (XSS)</td>
</tr>
<tr>
<td>A7 – Broken Authentication and Session Management</td>
<td>A3 – Broken Authentication and Session Management</td>
</tr>
<tr>
<td>A4 – Insecure Direct Object Reference</td>
<td>A4 – Insecure Direct Object References</td>
</tr>
<tr>
<td>A5 – Cross Site Request Forgery (CSRF)</td>
<td>A5 – Cross Site Request Forgery (CSRF)</td>
</tr>
<tr>
<td>&lt;was T10 2004 A10 – Insecure Configuration Management&gt;</td>
<td>A6 – Security Misconfiguration (NEW)</td>
</tr>
<tr>
<td>A10 – Failure to Restrict URL Access</td>
<td>A7 – Failure to Restrict URL Access</td>
</tr>
<tr>
<td>&lt;not in T10 2007&gt;</td>
<td>+ A8 – Unvalidated Redirects and Forwards (NEW)</td>
</tr>
<tr>
<td>A8 – Insecure Cryptographic Storage</td>
<td>A9 – Insecure Cryptographic Storage</td>
</tr>
<tr>
<td>A9 – Insecure Communications</td>
<td>A10 – Insufficient Transport Layer Protection</td>
</tr>
<tr>
<td>A3 – Malicious File Execution</td>
<td>&lt;dropped from T10 2010&gt;</td>
</tr>
<tr>
<td>A6 – Information Leakage and Improper Error Handling</td>
<td>&lt;dropped from T10 2010&gt;</td>
</tr>
</tbody>
</table>

**What does all this mean?**
Select target
- Pick a suitable target, there are several criteria you can apply.
- Attacks should not be random events
- Pick a victim within your capabilities
- Improve your skills constantly
- READ READ READ READ
- Sign up to security blog sites,
- Keep up to date on zero days and version update releases

What would a white hat do here? Test what he is allowed to access
What would a black hat do here? Scan to gather as many victims as possible
Justify benefit
- There must be a gain in your action
- Less and less common to attack with aim of destruction
- Be sure you will be happy with the result if you get your wish?

What would a white hat do here? Find the problem and report it
What would a black hat do here? Fun and profit!
Learn application flow
- Discover the business logic
- Figure out what the application wants you to do and document it.
- Be able to describe action/response for every click

What would a white hat do here? Learn about the allowed area
What would a black hat do here? Learn as much as possible and share it
Probe architecture and design
- Figure out what components are used
- Get details on version numbers and products
- Check for default usernames and password
- Check ports

What would a white hat do here? Stick to the allowed areas
What would a black hat do here? Go to town... Do everything, everywhere...

Golden Rule: 4
Identify entry points based on components
- Map on paper the application as you understand it
- Compose potential attack vectors
- Decide the best route to achieve the predetermined goal

What would a white hat do here? Stick to the testplan...
What would a black hat do here? Everything, everywhere...
Chart attack vector matrix on each component
- Using a predefined attack matrix, select attacks suitable for component.
- Generate a complete list and develop a testing plan.

What would a white hat do here? “You are supposed to test only this...”
What would a black hat do here? “w0w! Machines all over the place!...”
Carry out simplified to complex probes

- Starting with the most simple test cases develop an attack story
- Treat the results of simple test as clues to the next step
- Gradually increase the complexity of the probes.

What would a white hat do here? No problems found in the allowed areas
What would a black hat do here? Nothing in that service, but there I hit the spot!
Analyse results

- Chart out the results you are getting
- Do they help you achieve the goal
- if not, why not?
- Was you testing methodology sufficient to achieve the goal based on your findings?
- Should you relook at how you achieve goal
  - link in chain V one time hit.

What would a white hat do here? The goal is to find a problem
What would a black hat do here? while 1; FUN_AND_PROFIT!
Build valid attacks based on derived benefit

- Based on your finding derive clean and clear steps to reproduce the issue.
- Stabilize the attack
- Look for variants that give the same result.

What would a white hat do here? Theoretical attacks on allowed services
What would a black hat do here? A bunch of exploits all over the place!
Contact Admin – let them know.

- It is important that you contact the owners of the application to let them know about the issue.
- Currently it is recommended that 180 days is enough notice (Responsible Disclosure)
  - This notice period is not legal protection for you
- You should not post the defect on any forums.
- If you are lucky the admins will fix the issue and after that give you credit publicly. Without contacting law enforcement.

What would a white hat do here? Responsible disclosure...
What would a black hat do here? Carry on the hack, expose it to others (forums, hacktivism, trading, fun and profit!)
• Select target
• Justify benefit
• Learn application flow
• Probe architecture and design
• Identify entry points based on components
• Chart attack vector matrix on each component
• Carry out simplified to complex probes
• Analyse results
• Build valid attacks based on derived benefit
• Contact Admin – let them know.

The Golden Rules

project date 20/09/2007
• Do you take the white or the black pill?
  – How deep into the rabbit hole do you want to go?