Are You Vulnerable?
The Tiger Team Approach
Purpose and Scope

- To present a best practice approach to securing your company
- To present real life examples of vulnerability assessment successes
Don’t try this at home

Get written permission before trying any of these techniques

The main difference between a tiger team and a burglar is permission
Juggling Tasks

Physical

Cyber

Regular Work

Privacy

Not Secure

Too Secure
Adversary Theft Path

Design and Evaluation of Physical Security Systems – Published by Butterworth-Heinemann
- Lock, Light & Limit Access
- View from bad guy’s perspective
What needs to be protected?

- Laptop = $1000
- SSN numbers - $2 each
- Breach notification - $18 - $209 per identity
- Bot herders can make $50k per month
- Copper - $3.20 /lb
Who are the bad guys?

- **Insiders**
  - Former or disgruntled employees
  - Click happy employees

- **Outsiders**
  - Thieves
  - Extremists / Terrorists
  - Hackers
  - Meth Heads
- Password site:yoursite.com
- Filetype:doc site:yoursite.com classified
- Google Street View
Insider Threat

- 60 percent of ex-employees leave with insider information
  - Enforce termination procedures
  - Limit access to those who need it

- View your network from an insider’s perspective
  - Video: Lock your PC

- How many of your employees will click on an email I send them?

Locks keep honest people honest

Lock videos on the Internet

http://www.youtube.com/whitehat1969
Tools of the Trade
DISCOVERY

Sometimes, the greatest treasures are found beneath piles of trash.
Techniques

- Social engineering
- Social networking
- Lock by-passing
- Thumb drive sprinkle
- Dumpster diving
- Tailgating
- Out of office message
- Black box
- Unlocked PC’s & cabinets
- Unused network jacks
- Keyloggers
Step 0: Attacker Places Content on Trusted Site
Step 1: Client-Side Exploitation Example

- Exploit client-side vulnerability to install and run code on unpatched victim machine
Step 2: Establish Reverse Shell Backdoor Using HTTPS
Step 3 & 4: Dump Hashes and Use Pass-the-Hash Attack to Pivot
Step 5: Pass the Hash to Compromise Domain Controller
Video

www.youtube.com/whitehat1969
An Ounce of Prevention

$9
Password Cracking

- Identify weak or default passwords
- Verify the use of complex passwords

<table>
<thead>
<tr>
<th>Characters (complex)</th>
<th>Estimated time to crack</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>6 minutes</td>
</tr>
<tr>
<td>8</td>
<td>2.34 hours</td>
</tr>
<tr>
<td>14</td>
<td>9 hours</td>
</tr>
<tr>
<td>15</td>
<td>209 days</td>
</tr>
</tbody>
</table>
password
Summer13
P@swordCompl3x
juggle13 google