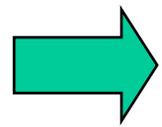

The Bad Guys Are Winning... So Now What?

Ed Skoudis
v1Q13

```
$ cut -f5 -d: /etc/passwd |  
grep -i skoudis
```

- Ed Skoudis
- Started infosec career at Bellcore in 1996 working for phone companies... eventually got into...
 - Pen tests
 - Incident response
 - Digital forensics
- SANS Instructor
 - Author of classes for Incident Handling and Network Penetration Testing
- Counter Hack Founder -- Cyber Foundations, Cyber Quests, and NetWars
- InGuardians Co-Founder -- Infosec research and consulting
- Researcher -- Malware, Virtual Machine Security Issues, Penetration Testing, Cyber Attacks and Defenses
- Blogger -- CommandLineKungFu.com
- Author -- *Counter Hack Reloaded* and *Malware: Fighting Malicious Code*

Outline



State of the Hack

- Some of the Implications...
 - For Pen Testers & Red Teamers
 - For Enterprise Security Professionals
 - For the Military
- Q&A

This Presentation

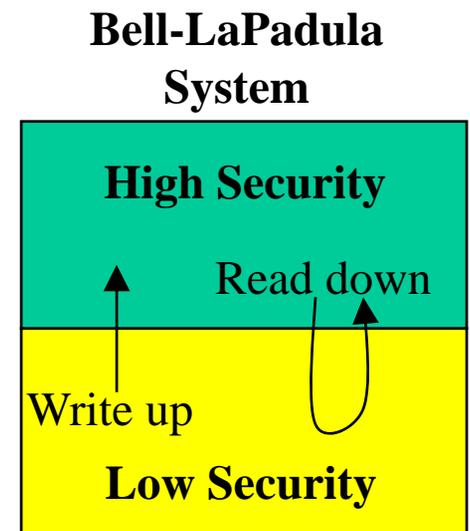
- Based on discussions and brainstorming with some of the best penetration testers, computer attackers, and defenders I know
- I've been working in computer security for > 16 years...
 - Pen tests, incident response, digital forensics, security architecture
- ...Trying to get a feel for evolutionary trends in that time
- This talk may be controversial
- I'm not expecting you to agree with me
- I'm not sure I even agree with myself on all of this... but it's got me thinking, and I hope you find these concepts worth at least considering

State of the Hack

- Thesis:
 - A sufficiently determined, but not necessarily well-funded, attacker can break into almost any modern organization
 - Gaining control of critical systems within the organization
 - Exfiltrating sensitive information
 - Acting unnoticed for sufficient periods of time to damage that organization

Why Is This So? Vulnerabilities

- Increased attack surface
 - Client-side exploitation
 - Browsers (IE, Firefox, Chrome, Safari), document rendering programs (Adobe Reader, Word, Excel), media players (Real Player, Windows Media Player), program execution environments (Java, Flash, HTML5), etc.
 - Wireless (almost) everywhere
 - Wifi, Bluetooth, ZigBee, etc.
 - Webification of most applications
 - Web 2.0 – publishing content everywhere, scripting everything, social-networking-a-rama
 - Cross-Site Scripting and Cross-Site Request Forgery
 - On critical infrastructure devices and control systems!
 - SQL Injection still rampant (sad, sad, sad)
 - Such attacks can be combined together
 - See the *Pen Test Perfect Storm Trilogy* of webcasts by Josh Wright, Kevin Johnson, and Ed Skoudis
 - Six webcasts total... maybe more!



More Why Is This So?

Repeated Mistakes

- We're not learning from the mistakes of the past
 - Buffer overflow & SQLi vulns still prevalent
 - Misconfigurations abound
 - Comprehensive patching processes remain elusive
 - New languages and environments to run them are embedded in nearly everything
 - General-purpose computer systems are hungry to run code...
 - ...and attackers are happy to provide it

Why Is This So?

Asymmetry and Botnets

- Computer attackers have always benefited from the fact that they only need to find one way in, while the “good guys” need to block almost every avenue in...
- ...or at least police every entry point
- A crucial asymmetry in offense vs. defense...
 - Making attackers’ jobs easier than defenders’
- Plus, with the rise of the botnet and mobile device infections, attackers increasingly have computer firepower that matches or even exceeds the target organization

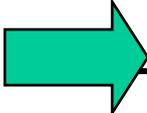
Outline

- State of the Hack
- Some of the Implications...
 - ➔ For Pen Testers and Red Teamers
 - For Enterprise Security Professionals
 - For the Military
- Q&A

Implications for Penetration Testers and Red Teamers

- If a test scope is defined broadly enough, we almost always get in
 - Sure, if you take all of the interesting attack vectors off the table, you may thwart us... but not the real bad guys
 - “Just look at these four servers... see what you can do...”
 - The real attackers aren’t limited that way
- So what? If pen testers can’t help target organizations actually improve their security, they’re just showing off
 - Thus, it is more important than ever to express findings in business terms and potential mission impacts... and to emphasize the appropriate defenses

Outline

- State of the Hack
- Some of the Implications...
 - For Pen Testers and Red Teamers
 -  – For Enterprise Security Professionals
 - For the Military
- Q&A

Implications for Enterprise Security Personnel

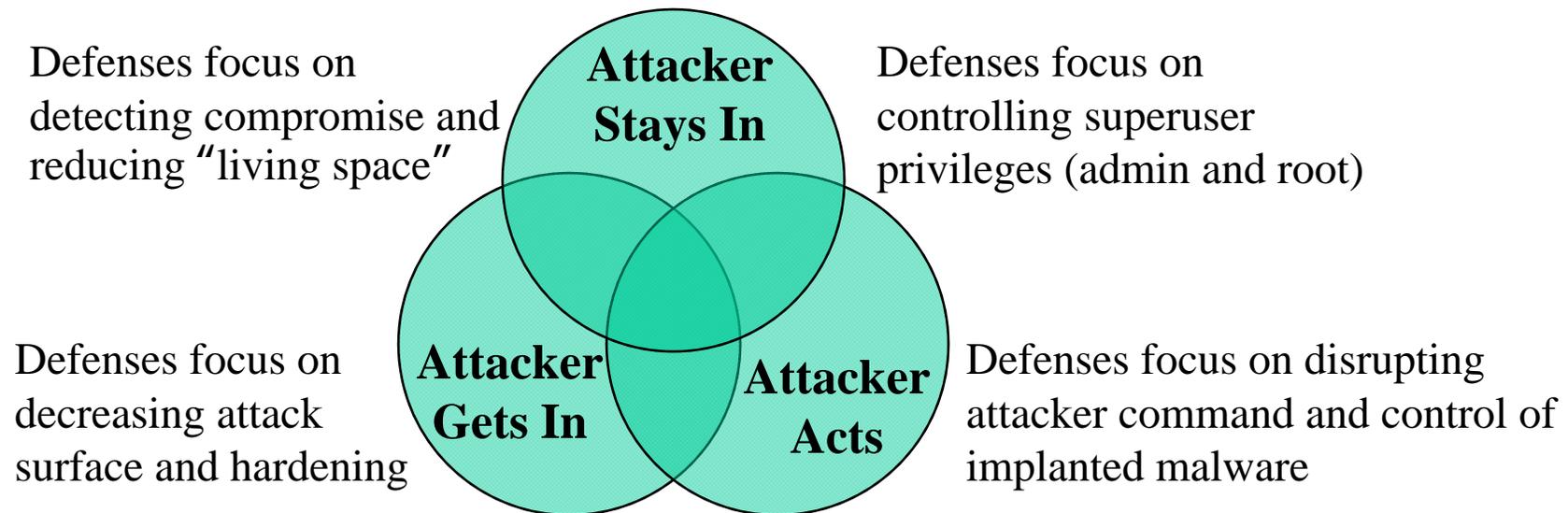
- Most enterprises spend the vast majority of their infosec resources on prevention
 - Firewalls, anti-virus, system hardening, patching, etc.
 - Even audit and vuln assessment are a form of prevention – proactively finding flaws and fixing them before exploitation
- But, if exploitation has already occurred, your preventative measures have already failed... that gets back to the main thesis



Implications for Enterprises...

So What?

- We should divert some enterprise security resources from prevention to...
- ...detection and eradication
- Where has the bad guy already compromised me?
- How can I get rid of or disrupt attackers in our midst?

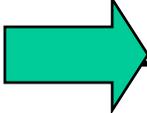


* Hat tip for diagram idea to NIAEC, Wende.Peters@jhuapl.edu

Implications for Enterprises... How?

- Intrusion Detection Systems
 - Not just Intrusion Prevention Systems... they often are tuned to a point where they can be dodged
- Log Analysis
 - Sounds painful, but a lot can be gained from it
- Looking for anomalous traffic
- Honeypots (honeyd, thp) and tarpits (Labrea)
- Then, clean up – re-imaging has good benefits
- Also, such detection and eradication efforts can provide insight in how to better position preventative measures (i.e., iterate to improve)
 - Also, by detecting and eradicating, you are preventing the attacker from acting... so you can still call this expense “prevention” if you want/must

Outline

- State of the Hack
- Some of the Implications...
 - For Pen Testers and Red Teamers
 - For Enterprise Security Professionals
 -  – For the Military
- Q&A

Implications for the Military

- It is widely rumored and in some cases actually reported that major government, military, and civilian infrastructure systems have been compromised
- So what?
 - Significant kinetic effects are possible
- Operational and strategic military goals are achievable via cyber means, often at lower cost and ***potentially*** lower physical risk than traditional military strikes

Cyber Attacks As Precursors to Or Defusers of Kinetic Attacks

- Before kinetic attacks occur, an actor could prepare the battlefield with cyber attack
 - Disable critical infrastructure
 - Alter it so that it doesn't function properly
- A cyber attack could incite the following kinetic warfare...
- ...Or inhibit it
 - A country under cyber attack can respond with cyber attack if it has the capabilities...
 - Otherwise, it may be forced to respond kinetically
- More rungs on the escalation ladder... That's a *good* thing

Difficulty of Attribution

- Direct attribution in the cyber world can be very difficult if the attacker is clever and desires anonymity
- A large nation could attack another one and deny action
- A small actor could incite two larger players into a conflict
- Some countries have stated that they consider a cyber attack on their territory to be the equivalent of the use of WMD against them... and they will respond *in kind*
- Would a country be willing to engage militarily without knowing *for sure* who triggered a cyber attack?
- Sometimes, though, attribution is not difficult at all

A

B

C

Conclusions

- The world is changing...
- More reliance on IT... more reliance on information security professionals
- But, infosec itself is rapidly evolving, possibly in ways that aren't all rainbows and unicorns
- For red teamers & pen testers:
 - Define scope to match real-world attacks... so:
 - You should almost always get in
- For enterprise infosec professionals:
 - Look to see where you are owned
 - Detection is critical... redirect some resources
- For military:
 - It's a brave-new world
 - Get ready for increased military engagement in cyber space

