Christopher Pogue is the Managing Consultant of the SpiderLabs Incident Response and Digital Forensics team. Having served as a US Army Signal Corps Warrant Officer, he worked on digital forensic investigations and as Cyber Security Instructor. Pogue joined the IBM Internet Security Systems (ISS) X-Force after leaving the military. As a Penetration Tester and Forensic Investigator with IBM, he performed over 300 penetration tests and 50 investigations. In his role with SpiderLabs, Pogue leads the team that performs investigations all over the United States, Central and South America, and the Caribbean Islands. He also assists local, state, and federal law enforcement agencies with cases involving digital media.

Tim Maletic is a Senior Security Consultant within the Penetration Testing team at Trustwave's SpiderLabs. Tim has been working in IT since the birth of the web, and has been focused full-time on information security since 2001. Prior to joining Trustwave, Tim held positions as Senior UNIX Engineer, Senior Security Engineer, and Information Security Officer.

Welcome!

We're very excited to have this opportunity to share some ideas about pushing incident response, forensics, and penetration testing to the next level.

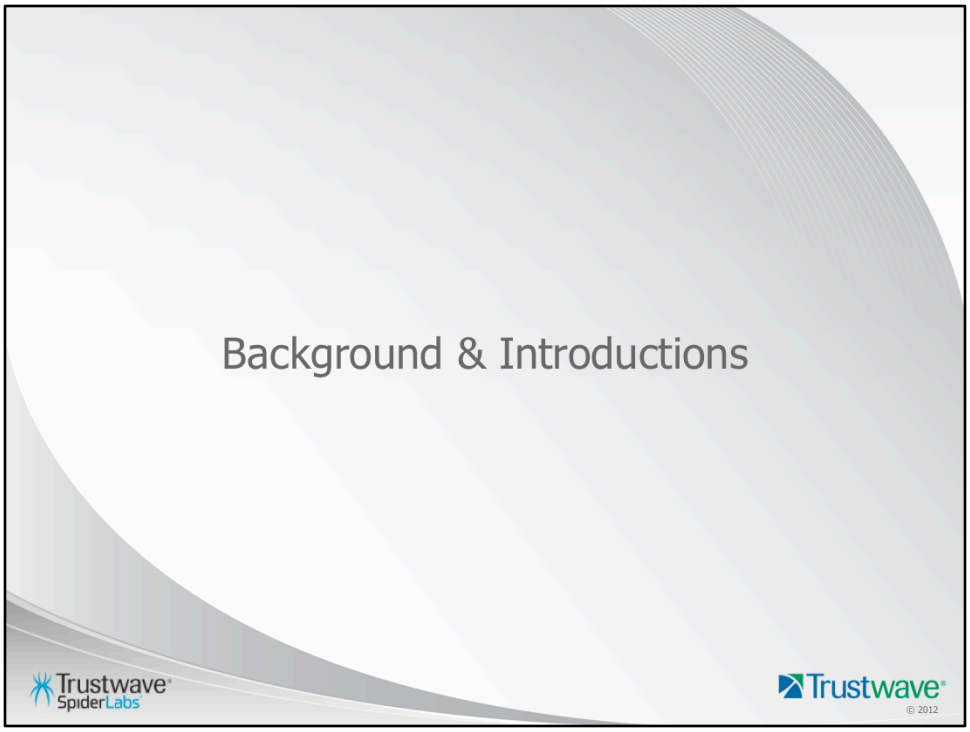
We are honored, and humbled, to present to a DEF CON audience. Our mission is to inspire network defenders and attackers to work more closely together to make each other better.

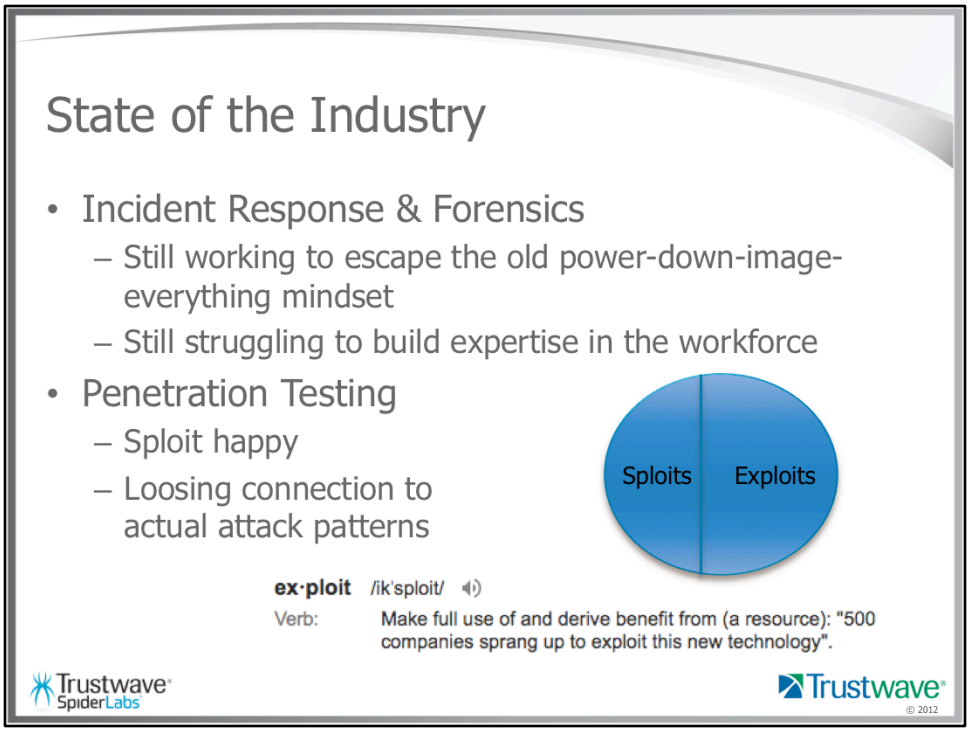
We'll finish off the session with a giant group hug and a few rounds of "Kum ba ya"! ☺

But first we're going to introduce ourselves and our methods and the problems we see ourselves trying to address. We'll then give a quick, advanced introduction to the forensics methodology we call "Sniper Forensics". We'll follow that up with our contributions to what we're calling the "Real-World Penetration Testing" movement.

Next we're going to show how we are applying these ideas in context by stepping through some sample attacks that do and do not exemplify our methods.

Then we'll wrap-up with the hugs and songs.


Background & Introductions
Trustwave SpiderLabs
Trustwave
© 2012



State of IR & Forensics

• Fighting the uphill battle of completely changing the mindset of the digital forensic discipline

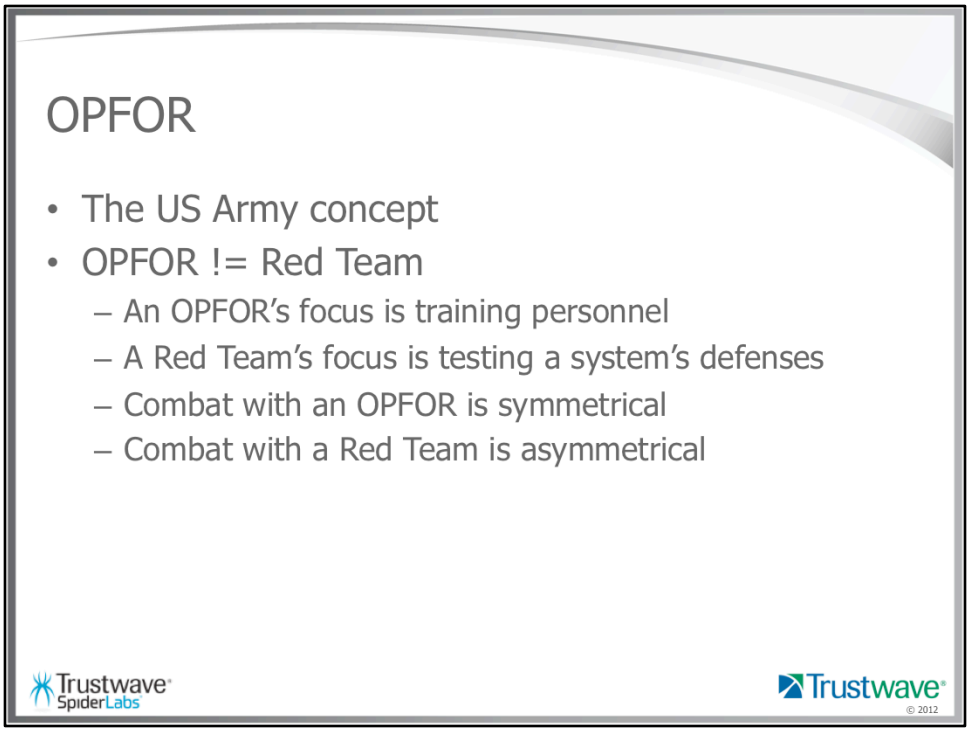
• Cops are good at being cops, WE are good at being computer engineers – every so often, we get hybrids – LEs who are actually techie

• Constantly evolving data sample – new systems mean new attacks – means research – if I haven't seen it before…then what?

• Proof of concept exercises with Pentest…opens Forensics up to the larger world of digital whodunit

State of pentesting

- We are sploit happy. I use "sploit" to mean exploits that take advantage of memory corruption bugs. About 75% of the stuff living under the exploit tree in metasploit. I am re-appropriating the term "exploit" to mean all the exploits that aren't "sploits". Note that this is usage is running opposite to current trends. But I think it's important. Language shapes our reality. If you heard Richard Thieme yesterday then I can rest my case. More on this later.
- I'm going to be arguing throughout this talk that we can – mostly – ignore sploits and instead focus on exploits.
- The way we scope and perform and document penetration tests are pushing us further and further away from modeling real-world attacks.
- The genesis of the OPFOR idea was simple. I presented to Grrcon on the results of a pet project to catalog SpiderLabs' most successful (i.e., most commonly used and productive) internal network attack techniques. A couple talks later, my friend Tim Crothers, then doing Incident Response for GE gave an awesome presentation where he stepped through keystrokes captured from a live C&C server of an attacker manually exploiting an internal network. There was a high degree of overlap between the attacker's methods, and the methods I was recommending, and I thought that fact was very interesting. So here we are.



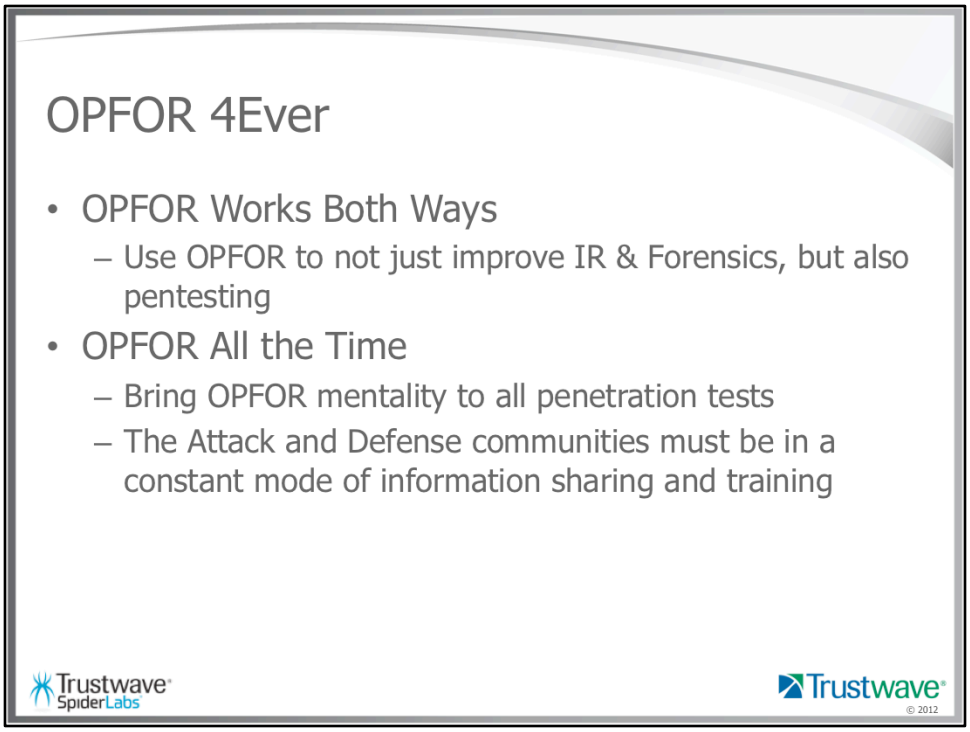
When I explained what I wanted to do to Chris, he said: "Oh, OPFOR. Cool." I'm not ex-military, and I'm not a computer gamer, so I had to go look that up. Is there anyone *else* in this room who would have to look that acronym up? I thought not.

But I know how to use google, so I read up on some unclassified US Army training manuals on OPFOR. An OPFOR is basically what we think of as a red team. But of course as applied by the US Army, it's huge. They'll represent real opponents or fictional opponents. They get accredited. They're just one part of an exercise that also includes political, social, geographical and other elements. In fact, information warfare tactics may be one part of an OPFOR exercise.

In contrast, a Red Team typically consists of a much smaller number of players, and targets not a military force, but an organization, facility or security system. A straightforward example is the use of a Red Team to test TSA procedures at a particular airport. The goal of a Red Team is to measure the state of the system. Is it prepared to defend against attack type X?

I prefer the goal of the OPFOR, which is essentially training – giving human beings something that's as close to real-world experience as we can get.

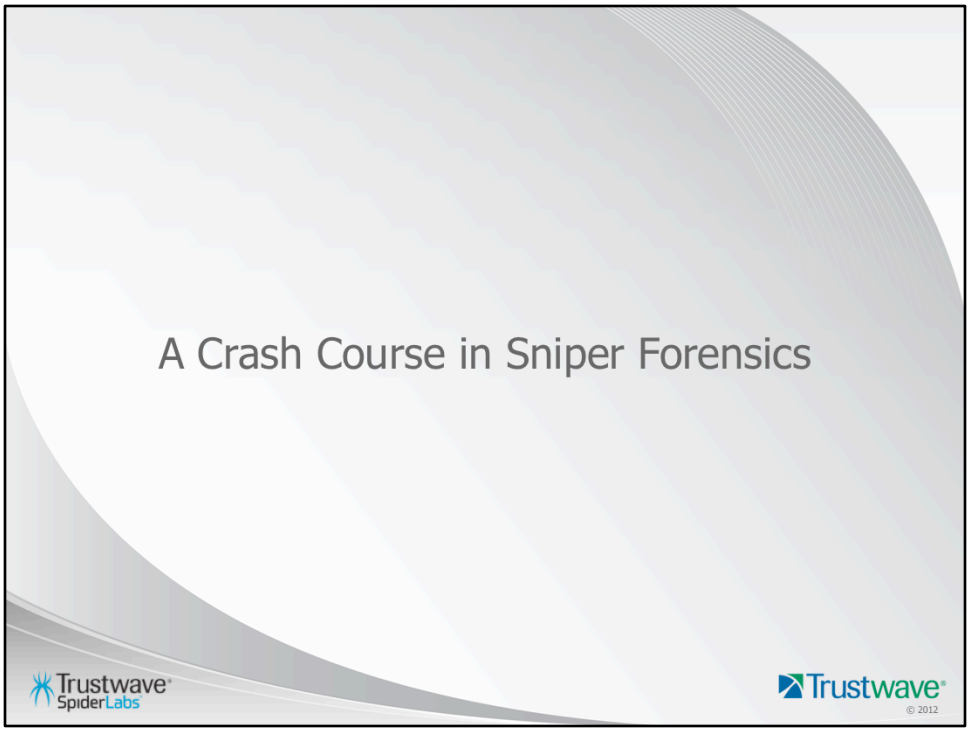
The asymmetrical nature of dealing with a Red Team more naturally lines up with attacks of opportunity, where early detection is the key. As targeted attacks become more common, I think we'll see a move to the OPFOR concept where the Blue Team must take the battle to

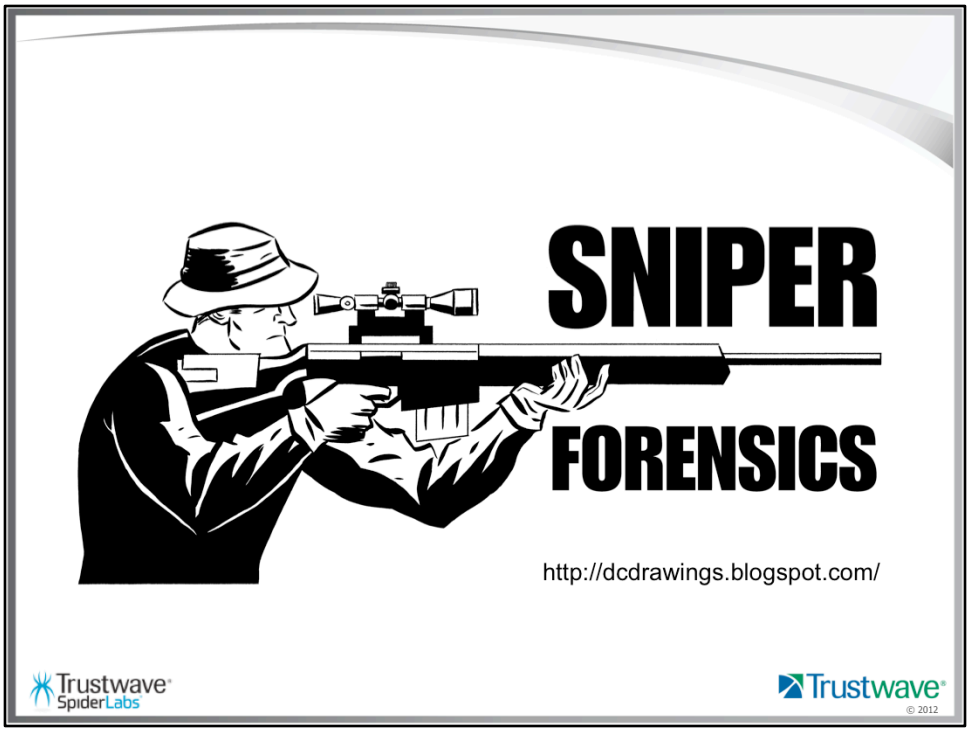


By "OPFOR 4Ever", we mean applying the OPFOR concept to information security attack and defense so as to create a continuous feedback loop between these two communities.

Pentesters train defenders, but equally the defenders must train the opposing force.

Also, we're not talking about some once-a-year exercise, but a constant mode of operation. For organizations with both attack and defense capabilities, this is simply a call for more communication and cross-training. For organizations with only one capability or the other, it means finding ways to interact with the wider community to share results and learn from others.

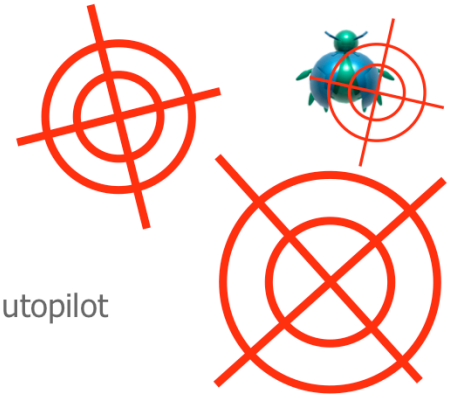

A Crash Course in Sniper Forensics
Trustwave SpiderLabs
Trustwave
© 2012


SNIPER
FORENSICS
http://dcdrawings.blogspot.com/
Trustwave SpiderLabs
Trustwave
© 2012


Emerging Threats and Threat Vectors
• Organic Persistent Threat
– Constantly evolving
– Highly motivated, funded, and organized
• A Laser vs Big Rock
– Efficient, targeted, and deadly accurate
– Messy, haphazard, more or less accurate (sort of)
• Target Selection
– Compromised data can be monetized
– Best return on investment for attackers
– Pivot attacks can lead to deeper penetration
*Advanced attacks, need an equally advanced investigation approach…enter Sniper Forensics…
Trustwave SpiderLabs
Trustwave
© 2012

Shotgun Forensics

- The process of taking a haphazard, unguided approach to forensic investigations:
  - "Old school"
  - Image everything
  - Reliance on tools – autopilot
  - Pull the plug



Trustwave SpiderLabs

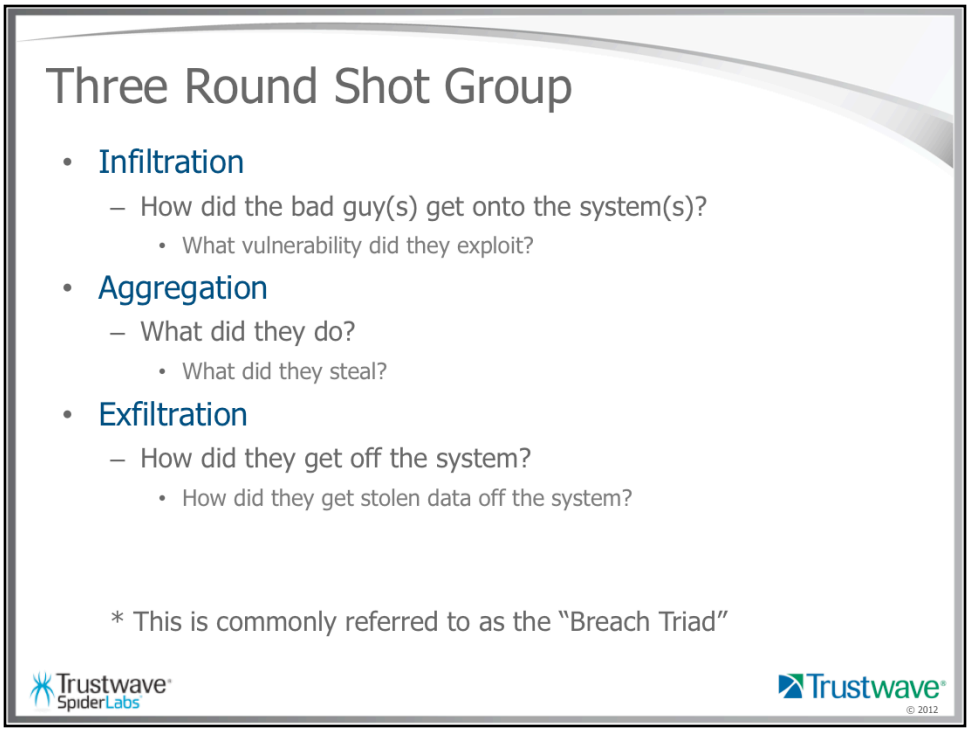
Trustwave

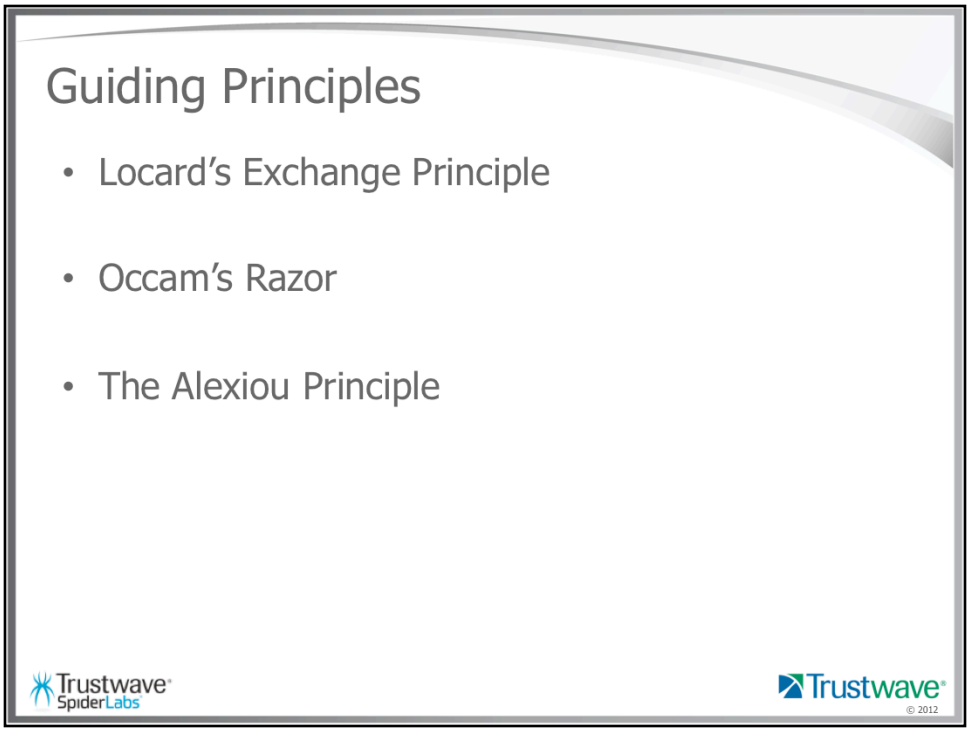
Sniper Forensics

- The process of taking a targeted, deliberate approach to forensic investigations:
  - Create an investigation plan
  - Apply sound logic
    - Locard
    - Occam
    - Alexiou
  - Extract what needs to be extracted, nothing more
  - Allow the data to provide the answers
  - Report on what was done
  - Answer the questions

Trustwave SpiderLabs

Trustwave


Three Round Shot Group
Infiltration
How did the bad guy(s) get onto the system(s)?
What vulnerability did they exploit?
Aggregation
What did they do?
What did they steal?
Exfiltration
How did they get off the system?
How did they get stolen data off the system?
* This is commonly referred to as the "Breach Triad"
Trustwave SpiderLabs
Trustwave
© 2012


Guiding Principles
• Locard's Exchange Principle
• Occam's Razor
• The Alexiou Principle
Trustwave SpiderLabs
Trustwave
© 2012

Locard's Exchange Principle

- Established by Edmund Locard (1877-1966)
- Regarded as the father of modern forensics
- Uses deductive reasoning
  - All men are mortal
  - Socrates is a man
  - Therefore, Socrates is mortal

Edmund Locard

Trustwave SpiderLabs

Trustwave

Occam's Razor

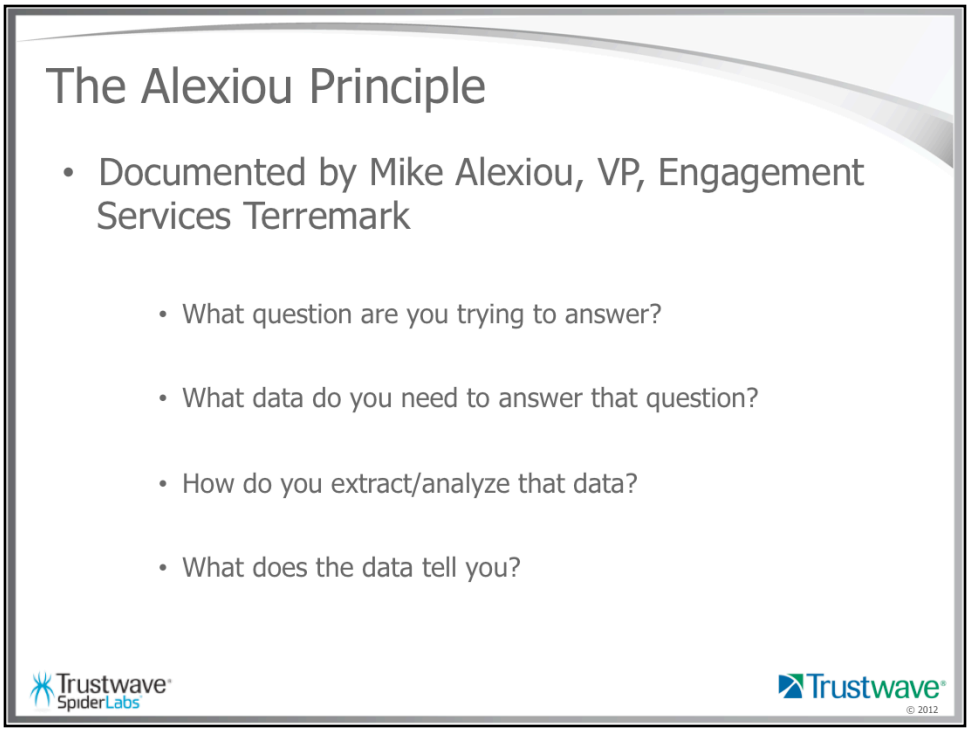
- Establish by William of Occam
  - 13th century Franciscan Friar
  - Major contributor to medieval thought
  - Student of Aristotelian logic

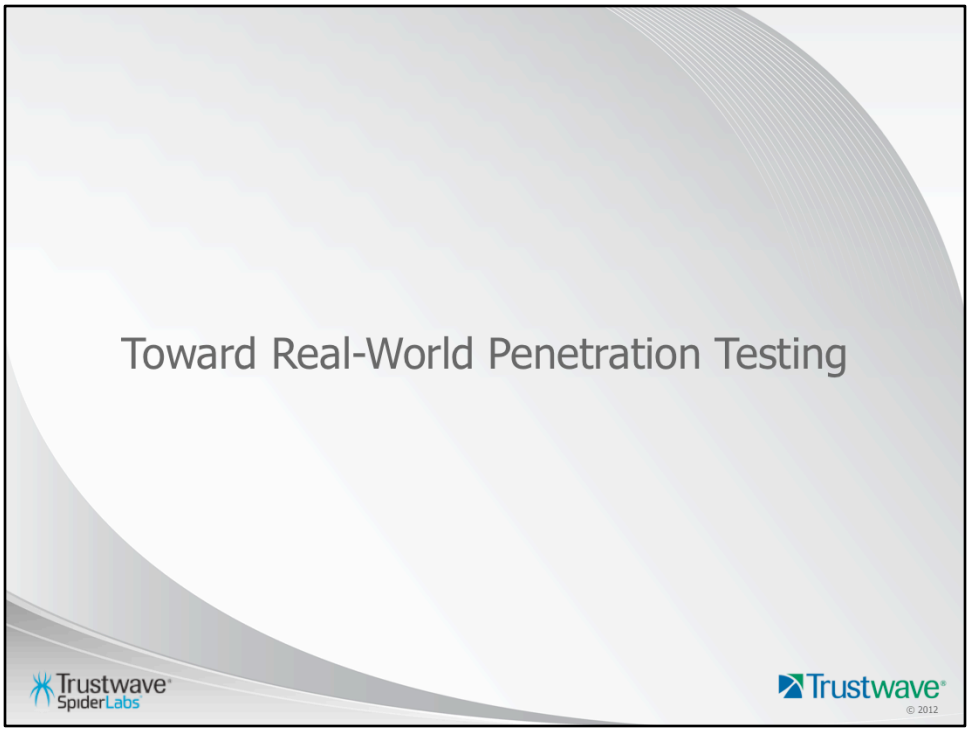
William of Occam

- The simplest answer is usually right
  - The modern KISS principle
    - "Keep It Simple Stupid"
  - Don't speculate
  - Let the data be the data

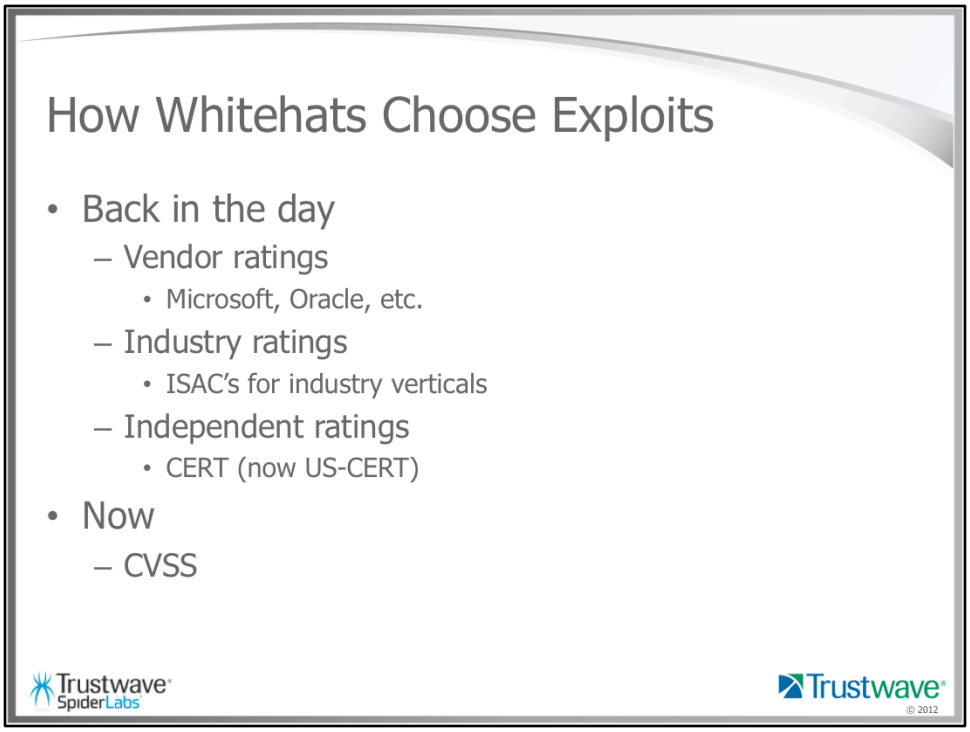
Trustwave SpiderLabs

Trustwave


The Alexiou Principle
• Documented by Mike Alexiou, VP, Engagement Services Terremark
• What question are you trying to answer?
• What data do you need to answer that question?
• How do you extract/analyze that data?
• What does the data tell you?
Trustwave SpiderLabs
Trustwave
© 2012



First let me explain what I mean by "real-world" here. We have to remember that a penetration test is a model of something else, and its value is related to how close or far away the model is from reality. So by "real-world pentesting" I don't mean "pentesting like the real pentesters do it". I mean "pentesting like the real attackers do it". Or simply a return to the roots, where we pay particular attention to the differences between the model and the real world.

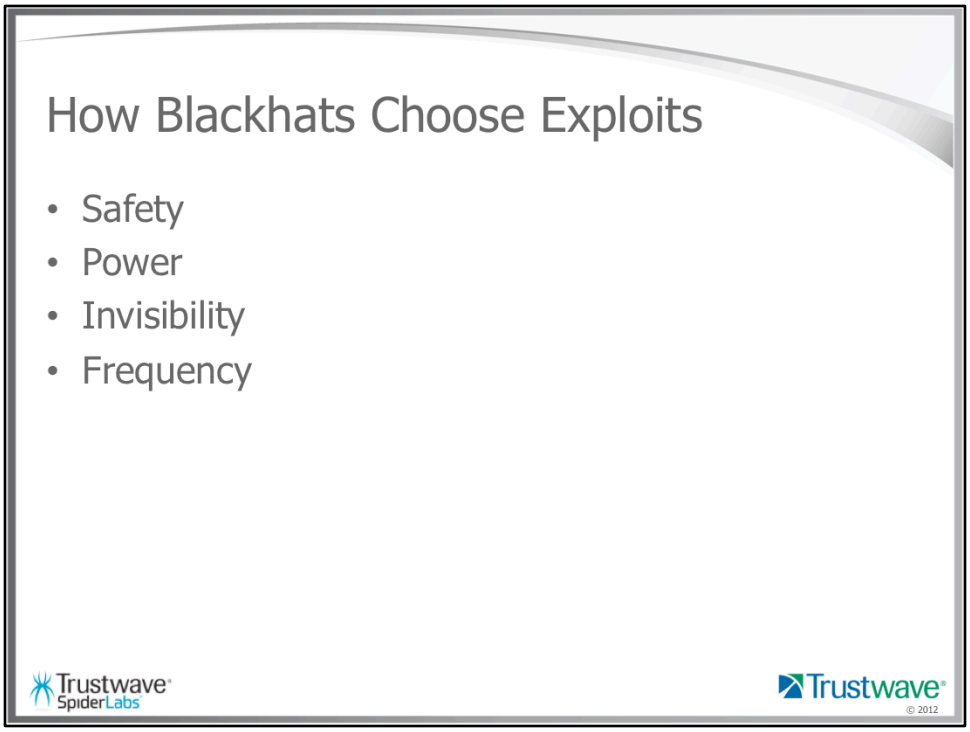


Consider how white hats choose exploits to defend against.

Over the years there have been many systems proposed to rank the severity of a vulnerability. Microsoft still ranks their patches as Critical, Important, Moderate, or Low.

CERT once used a number between 0-180 based on factors like: is it known, is it being exploited, is the Internet at risk, and so on?

But now we have one scoring system to rule them all: CVSS.

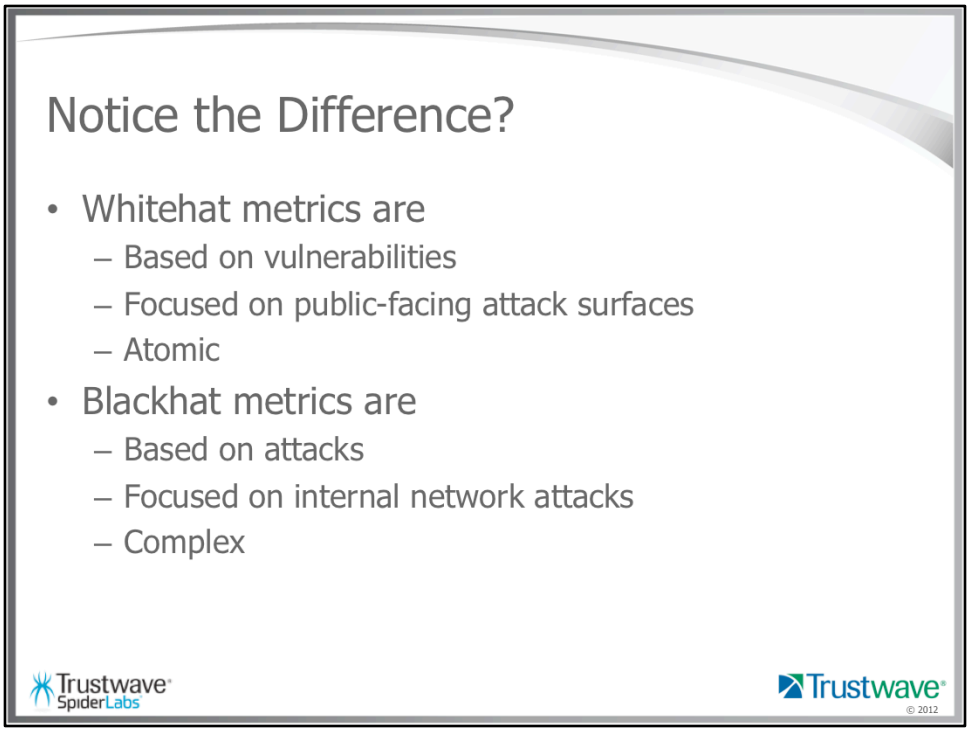


Based on my observations from my pentesting experience, and cross-referenced against research from the incident response community, I see…

Four of the biggest factors are:

- Safety: the attack doesn't harm the target – ever (for 2 reasons: stealth + reusability)
- Power: the attack gives the attacker leverage to carry out further attacks
- Invisibility: the attack may be detectable, but is rarely detected (in time)
- Frequency: the attack targets a relatively common vulnerability in a relatively common target

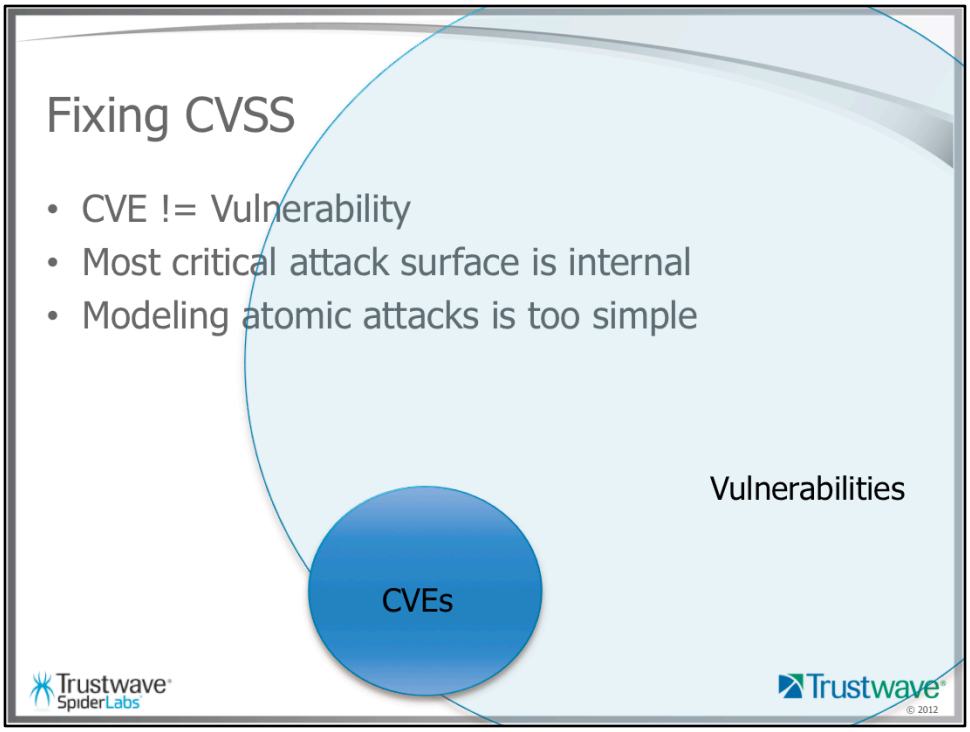
Notice that Safety, Power, and Invisibility are completely missed by CVSS.



If you spend much time looking at CVE data, it's easy to slip into the view that "vulnerability" == "that which can be patched". But there's a trivial proof that this is false.

It's past time we turned more attention to vulnerabilities that only exist on internal networks. If there's a moral to be learned from the 2011 RSA hack, it's that we are *all* one phishing campaign away from a remote-controlled instance of BackTrack on our network.

And for an example of attack-chains, think about the lowly NetBIOS null session enumeration attack and what you can do with that data.

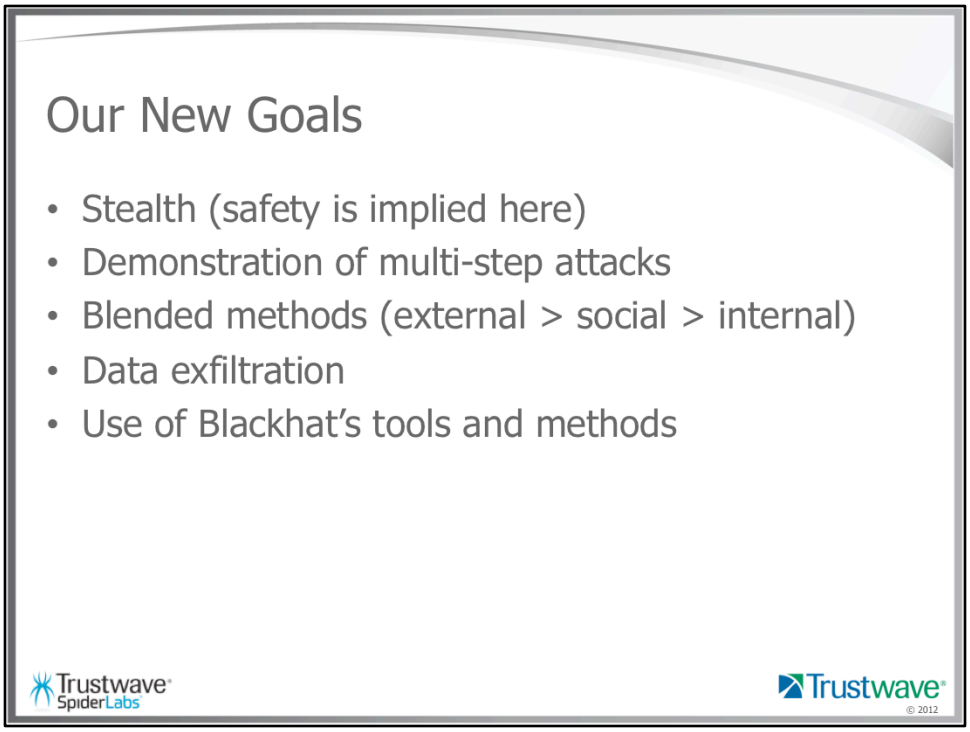


In the last couple months the CVE database crossed the 50,000 vulnerability threshold. But there are vastly more vulnerabilities than there are CVEs. Here's one example: ARP cache poisoning. (It achieved CVE candidate status in 1999, and never got beyond that.) CVSS is focused on vulns that have sploits, and so is missing what I think is the most important part of the picture.

CVSS needs a way to distinguish whether the vuln is exploitable over the Internet vs. over an internal network, and then focus energy on cataloging internal vulns.

CVSS needs combinatorics – some way to show how a chain of "low-risk" vulnerabilities can lead to a major problem. Something, perhaps, like an upside-down attack tree.

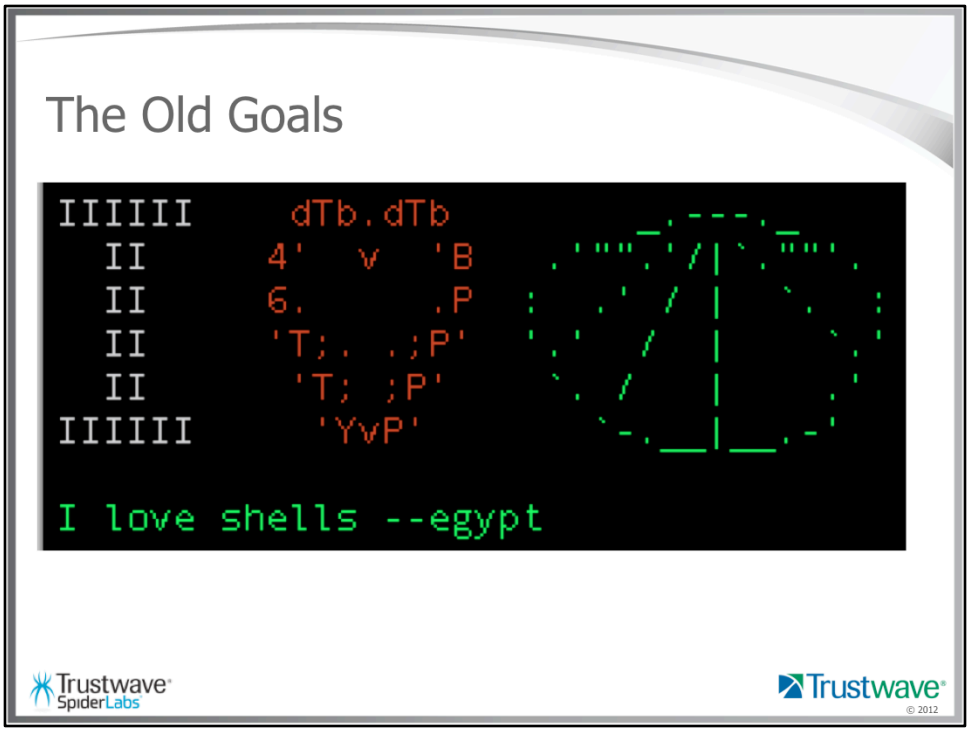
(I don't believe CAPAC is the answer here. The "attack patterns" covered by CAPAC are not the "chain of separate attacks" I'm speaking of here, but are instead something like "the pattern all SQL injection attacks follow".)



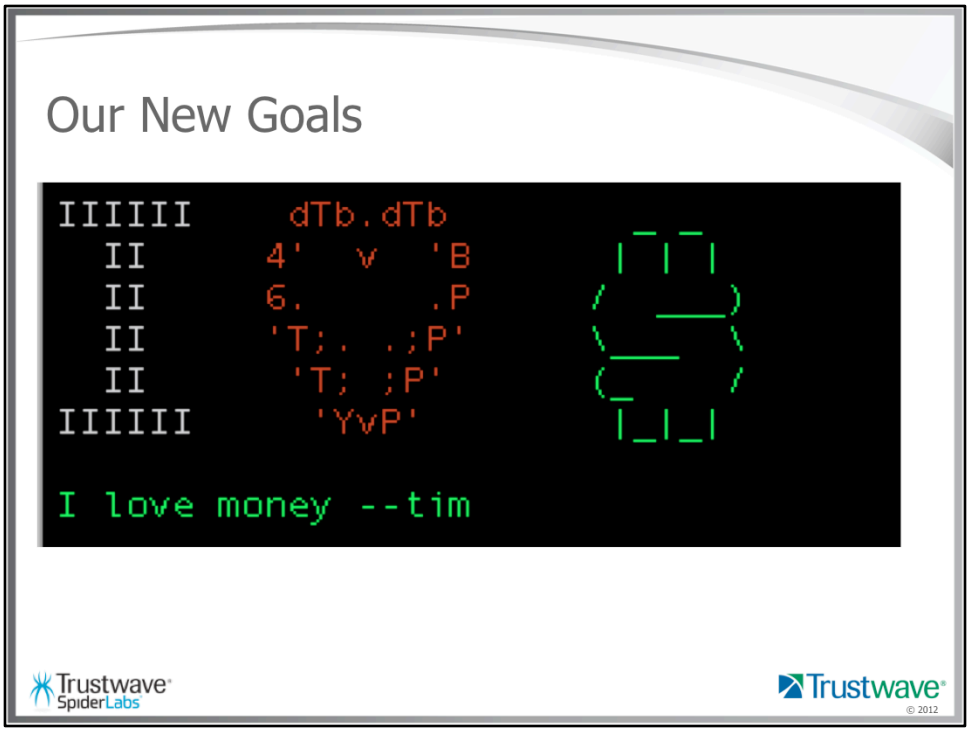
Our new goals are using principles of stealth to mimic real attacks. Real attacks are blended, and exfiltrate data.

Safety is implied – we sort of get it for free, since you can't be stealthy is safety isn't a concern. But we get other benefits from safety. We get to expand our pentest scope to a realistic class of targets, since we'll be able to convince our clients that safety is the first priority.

Think of the airsoft guns and biodegradable ammo used by today's OPFORs. We don't want to take down the people we're trying to train. But on the other hand you do work together to set realistic boundaries. You don't run an OPFOR exercise in an urban area.



Yes, shells are cool. But we shouldn't be getting paid pentest consulting dollars to produce shells.



Blackhats don't heart shells. They heart credit cards. They heart RSA secrets. They heart product designs. They heart data that can be monetized.

Those of you who heart shells may be thinking "why try to make pentests more like actual attacks?"

- Because doing so places the focus back on the data
- Because doing so allows your incident responders to see more realistic data
- Because we want the pentesters scope equivalent to the blackhats scope (which we get by sticking to the rule of "safety first")

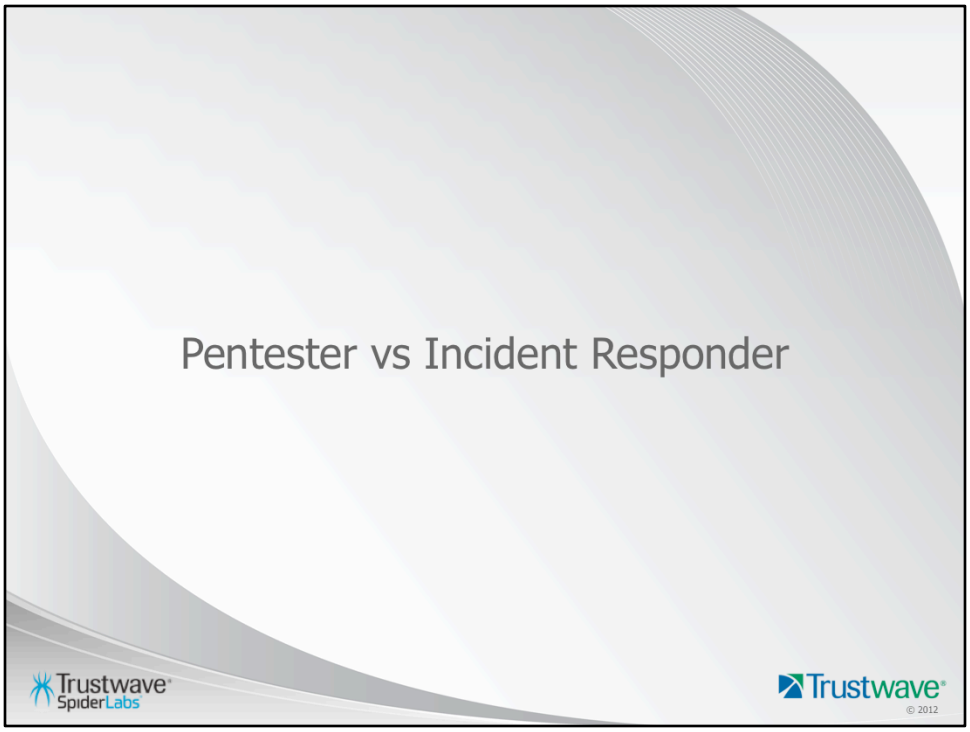
Of course I'm not alone in calling for more realistic penetration testing. Much of my thinking on this topic has been influenced by HD Moore's and Valsmith's classes on "Tactical Exploitation". I'm not sure when they started these classes up, but they presented on it at DEF CON 15. HD carried on this theme is his talk at SECTOR 2010.

Notice what these guys say about "exploits" – or what I'm calling "sploits".

Valsmith brings this up again in 2011, and irks Dave Aitel enough to make him respond.

Valsmith points out how the exploits he favors – logic flaws, bad protocol design and such – have a much longer shelf-life than sploits have. This is because sploits get patched. Because memory corruption bugs are relatively easy to patch versus protocol design issues. This lines up nicely with one of the recurring themes from the SpiderLabs Global Security Report: by focusing on exploits, instead of sploits, we are frequently taking advantage of ancient flaws, like ARP and NetBIOS. Oh, and passwords.

Haron Meer's talk from 44Con is a good example of someone arguing explicitly for real-world penetration testing *and* the use of sploits. But I don't want the debate to revolve around the "sploits are good" vs "sploits are bad" argument. What I'm arguing for is "safety first", so if you can convince me your sploit won't knock over my target, I'll happily use it. Meer's solution is for sploits is to be able to play them like a trump card in a hybrid table-top exercise. His reasoning stems from his analysis of the economics of 0days, but it works just a well if your concern is stealth and safety.

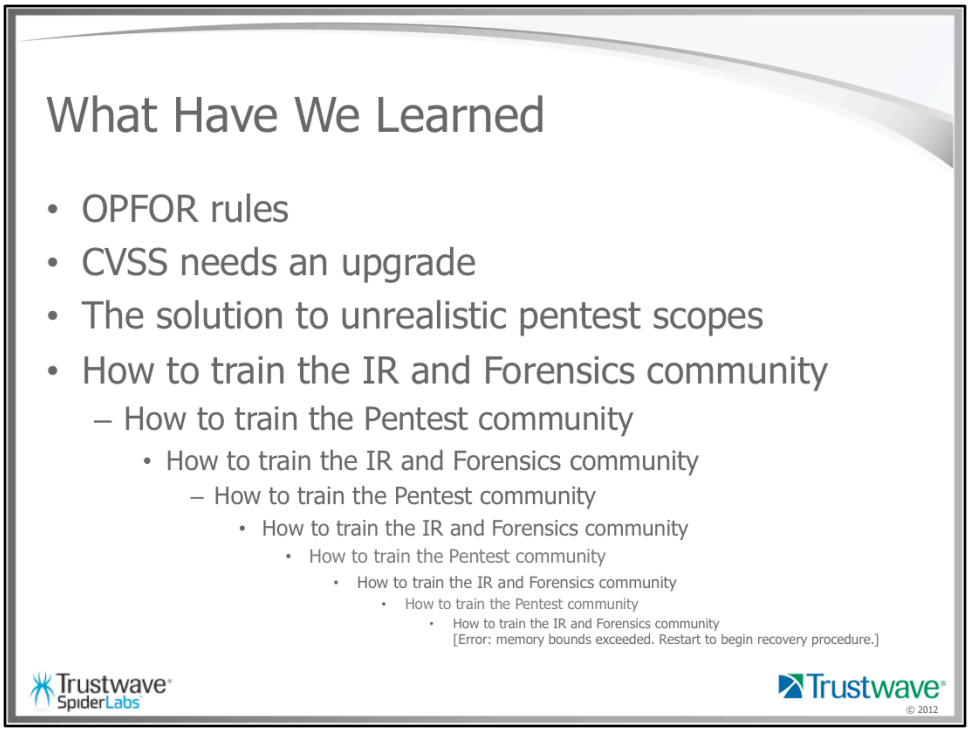

Pentester vs Incident Responder
Trustwave SpiderLabs
Trustwave
© 2012

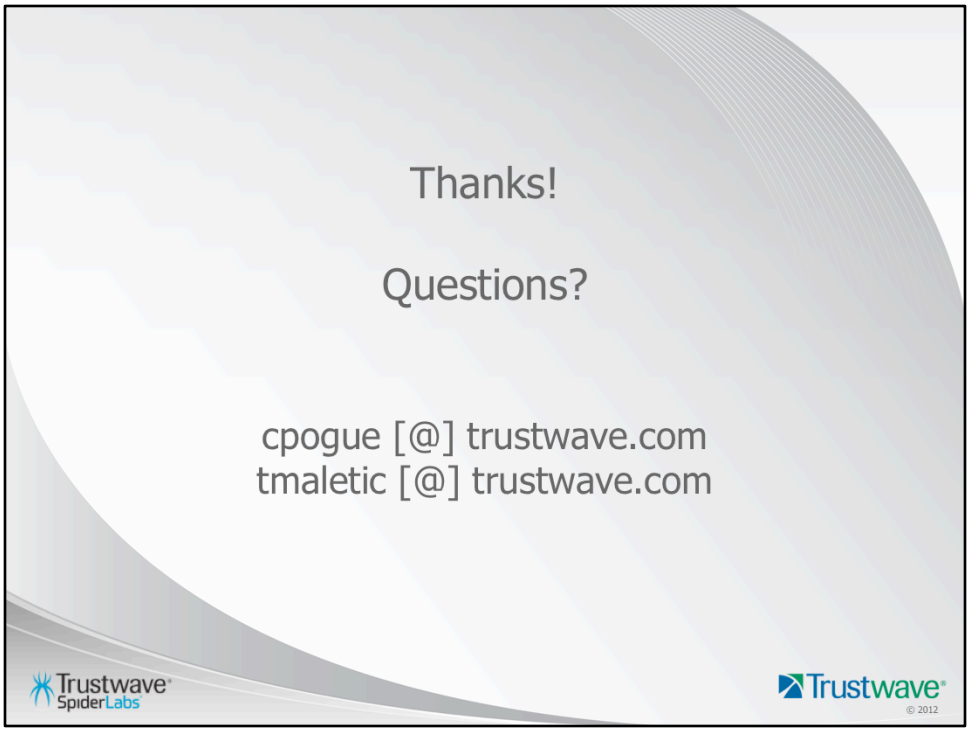

Demo #1
Trustwave SpiderLabs
Trustwave
© 2012


Demo #2
Trustwave SpiderLabs
Trustwave
© 2012


Demo #3
Trustwave SpiderLabs
Trustwave
© 2012


Conclusions
Trustwave SpiderLabs
Trustwave
© 2012


What Have We Learned
• OPFOR rules
• CVSS needs an upgrade
• The solution to unrealistic pentest scopes
• How to train the IR and Forensics community
– How to train the Pentest community
• How to train the IR and Forensics community
– How to train the Pentest community
• How to train the IR and Forensics community
• How to train the Pentest community
• How to train the IR and Forensics community
• How to train the Pentest community
• How to train the IR and Forensics community
• How to train the IR and Forensics community
[Error: memory bounds exceeded. Restart to begin recovery procedure.]
Trustwave SpiderLabs
Trustwave
© 2012

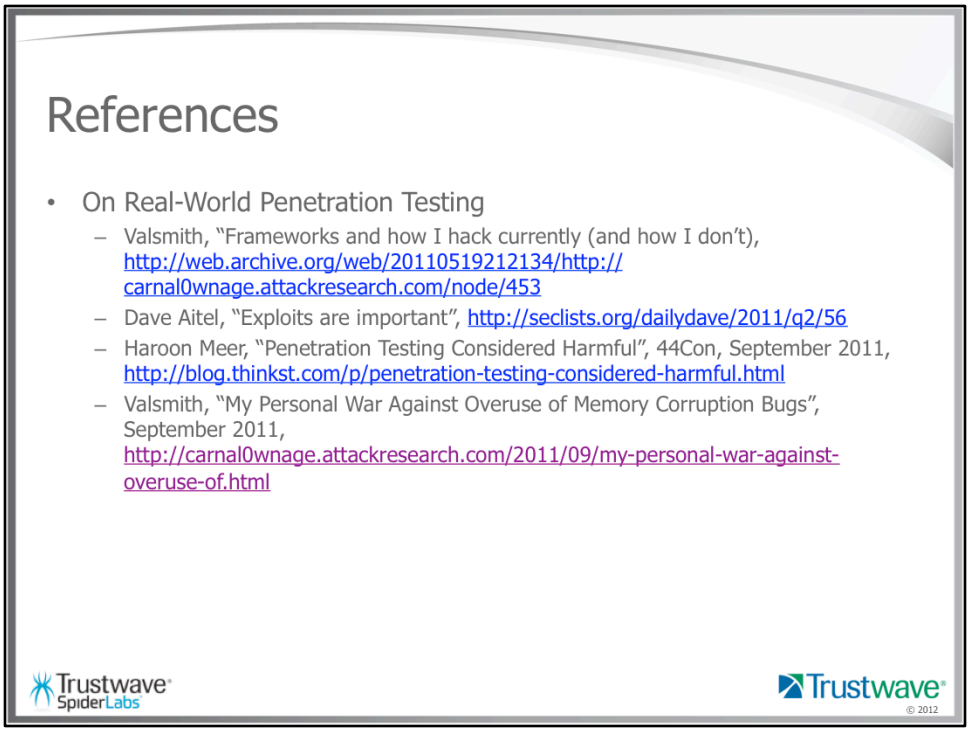

Thanks!
Questions?
cpogue [@] trustwave.com
tmaletic [@] trustwave.com
Trustwave SpiderLabs
Trustwave
© 2012


Resources
• Download the Global Security Report:
http://www.trustwave.com/GSR
• Read our Blog:
http://blog.spiderlabs.com
• Follow us on Twitter:
@SpiderLabs
Trustwave SpiderLabs
Trustwave
© 2012

References

- On OPFOR
  - Army Regulation 350-2, "Opposing Force (OPFOR) Program", http://armypubs.army.mil/epubs/pdf/r350_2.pdf
  - Army Training Circular 7-100.2, "Opposing Force Tactics", https://armypubs.us.army.mil/doctrine/DR_pubs/dr_aa/pdf/tc7_100x2.pdf
- On Real-World Penetration Testing
  - HD Moore & Valsmith, "Tactical Exploitation", DEF CON 15, http://www.defcon.org/images/defcon-15/dc15-presentations/Moore_and_Valsmith/Whitepaper/dc-15-moore_and_valsmith-WP.pdf
  - HD Moore, "Beyond Exploits: Real-World Penetration Testing", SECTOR 2010, http://vimeo.com/28291771

Trustwave SpiderLabs


References
• On Real-World Penetration Testing
– Valsmith, "Frameworks and how I hack currently (and how I don't), http://web.archive.org/web/20110519212134/http://carnal0wnage.attackresearch.com/node/453
– Dave Aitel, "Exploits are important", http://seclists.org/dailydave/2011/q2/56
– Haroon Meer, "Penetration Testing Considered Harmful", 44Con, September 2011, http://blog.thinkst.com/p/penetration-testing-considered-harmful.html
– Valsmith, "My Personal War Against Overuse of Memory Corruption Bugs", September 2011, http://carnal0wnage.attackresearch.com/2011/09/my-personal-war-against-overuse-of.html
Trustwave SpiderLabs
Trustwave
© 2012