OPFOR 4Ever

Presented by:

Tim Maletic & Chris Pogue

OPFOR 4Ever

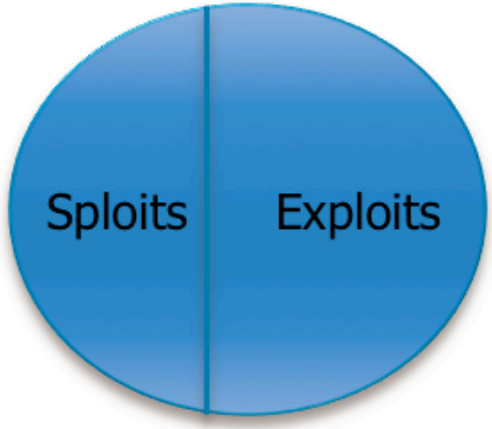
- OPFOR: Opposing Forces
- OPFOR Works Both Ways
  - Use OPFOR to not just improve IR & Forensics, but also pentesting
- OPFOR All the Time
  - Bring OPFOR mentality to all infosec attack & defense exercises
  - The Attack and Defense communities must be in a constant mode of information sharing and training

Plan of Attack

- Introductions
  - Sniper Forensics + Real-World Pentesting ~= OPFOR 4Ever
- Sniper Forensics
- Real-World Penetration Testing
- Proof-of-concept
  - Pentester vs IDS
  - Pentester vs Forensics Analyst
- Post-mortem

State of the Industry

- Incident Response & Forensics
  - Still working to escape the old power-down-image-everything mindset
  - Still struggling to build expertise in the workforce
- Penetration Testing
  - Sploit happy
  - Loosing connection to actual attack patterns



ex·ploit /ik'sploit/

Verb: Make full use of and derive benefit from (a resource): "500 companies sprang up to exploit this new technology".

Trustwave SpiderLabs

Trustwave

A Crash Course in Sniper Forensics

Trustwave SpiderLabs

Trustwave

SNIPER FORENSICS

http://dcdrawings.blogspot.com/

Trustwave SpiderLabs

Trustwave

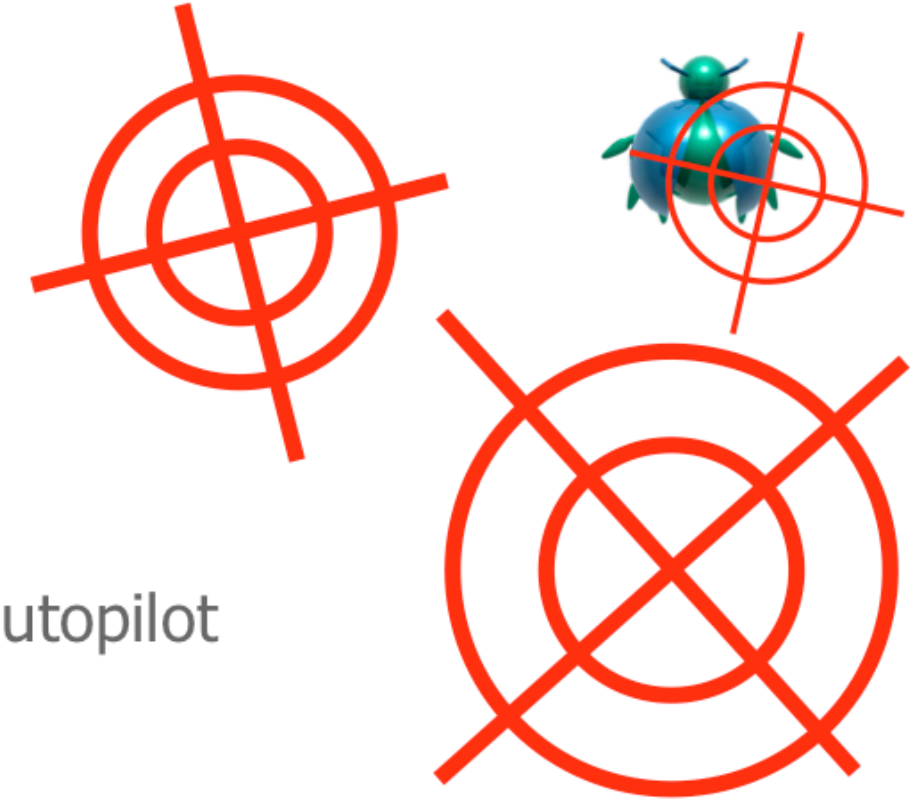
Emerging Threats and Threat Vectors

- 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…

Shotgun Forensics

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



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

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"

Guiding Principles

- Locard's Exchange Principle
- Occam's Razor
- The Alexiou Principle

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

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

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?

Real-World Penetration Testing

Trustwave SpiderLabs

Trustwave

How Whitehats Choose Exploits

- Back in the day
  - Vendor ratings
    - Microsoft, Oracle, etc.
  - Industry ratings
    - ISAC's for industry verticals
  - Independent ratings
    - CERT (now US-CERT)
- Now
  - CVSS

How Blackhats Choose Exploits

- Safety
- Power
- Invisibility
- Frequency

Notice the Difference?

- Whitehat metrics are
  - Based on vulnerabilities
  - Focused on public-facing attack surfaces
  - Atomic
- Blackhat methods are
  - Based on attacks
  - Focused on internal network attacks
  - Complex

Fixing CVSS

- CVE != Vulnerability
- Most critical attack surface is internal
- Modeling atomic attacks is too simple

Our New Goals

- Stealth (safety is implied here)
- Demonstration of multi-step attacks
- Blended methods (external > social > internal)
- Data exfiltration
- Use of Blackhat's tools and methods

The Old Goal

The New Goal

The Real-World Pentesting Movement

- HD & Valsmith @ Defcon 15
  - "Tactical Exploitation": a compilation of attack techniques that "do not rely on exploiting known vulnerabilities"
- HD @ Sector 2010
  - "Beyond Exploits: Real-world Penetration Testing": "[Exploits] are just one vector you can swap in [to the metasploit framework]. They're basically replaceable. They don't really matter."

The Real-World Pentesting Movement

- Valsmith @ carnalownage May 10, 2011
  - "Frameworks and How I Hack Currently": "I don't use exploits much anymore."
- Dave @ Daily Dave, May 11 2011
  - "Exploits Are Important"
- Haron Meer @ 44Con September 2011
  - "Penetration Testing Considered Harmful": we're all a 0day away from getting owned, and penetration testing won't prevent that.

Lazy Pentester vs IDS

Trustwave SpiderLabs

Trustwave

Demo #1a

Lazy Pentester vs Forensics Analyst

Trustwave SpiderLabs

Trustwave

Demo #1b

Trustwave SpiderLabs

Trustwave

Real-World Pentester vs IDS

Trustwave SpiderLabs

Trustwave

Demo #2a

Real-World Pentester vs Forensics Analyst

Trustwave SpiderLabs

Trustwave

Demo #2b

Trustwave SpiderLabs

Trustwave

Conclusions

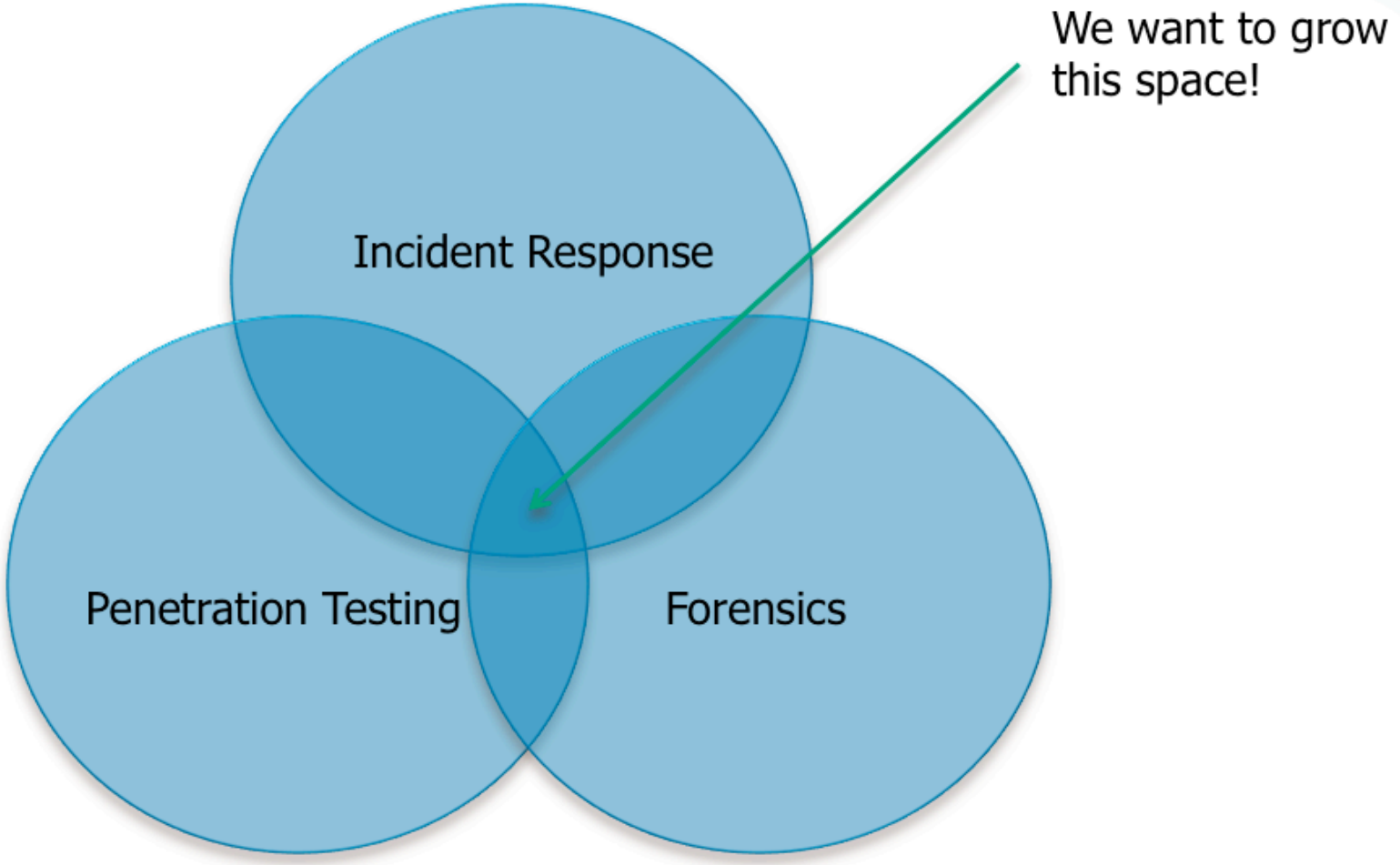
Forensics Conclusions

- Attack #1 touched more that 400 files.
- Created 133 new files.
- Showed IOCs indicating downloads.
- Attack #2 access a single, existing ntuser.dat file and created only two prefetch files.
- Showed IOCs within the event logs showing that the winexesvc service executed, but that's it.

Top 5 Ways to Get Caught

5. Create new user accounts
4. Use password brute-forcers
3. Push shellcode or a port scan past a network monitor
2. Let anti-virus see your password dumper
1. **Crash your target**

Infosec Mashup



Trustwave SpiderLabs

Trustwave

Other Ways to Collaborate

- JTF Missions
  - Are there IOCs that pre-date the pentest compromise?
- Incident Ready to Eat
  - Custom, pre-exploited virtual training lab
- Future Projects
  - Further analysis of common penetration testing methods
  - Development of stealthier attacks and better detection
  - Pentest automation

Thanks!

Questions?

cpogue@trustwave.com
tmaletic@trustwave.com

http://blog.spiderlabs.com

Twitter: @SpiderLabs

Trustwave SpiderLabs

Trustwave