Next-Generation Penetration Testing

Benjamin Mossé, MD, Mossé Security

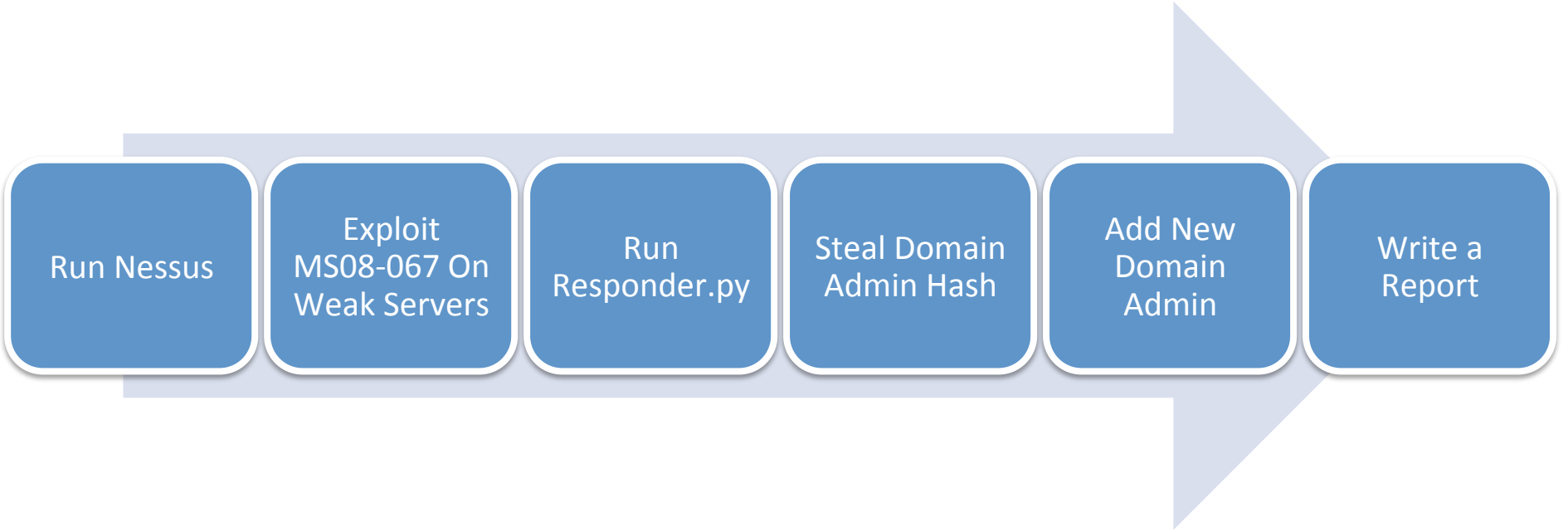
NATIONAL CONFERENCE 2015
TRUST IN INFORMATION SECURITY
13th -15th OCTOBER

About Me

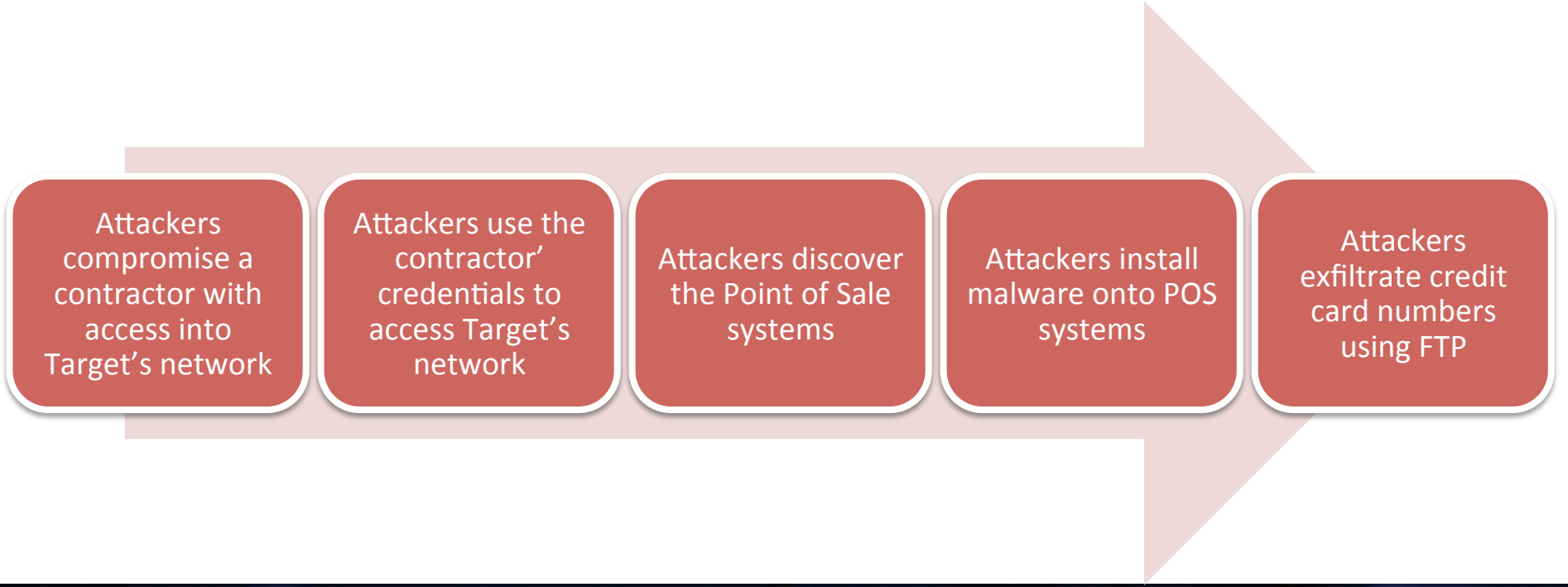
- Managing Director of Mossé Security
- Creator of an Mossé Cyber Security Institute - in Melbourne
- +30,000 machines compromised during penetration testing
- +300 penetration tests delivered
- +150 security advisories published
- Was the lead developer of the Browser Exploitation Framework

As a team, Mossé Security has compromised +100,000 machines during engagements.

Traditional Penetration Testing Kill Chain



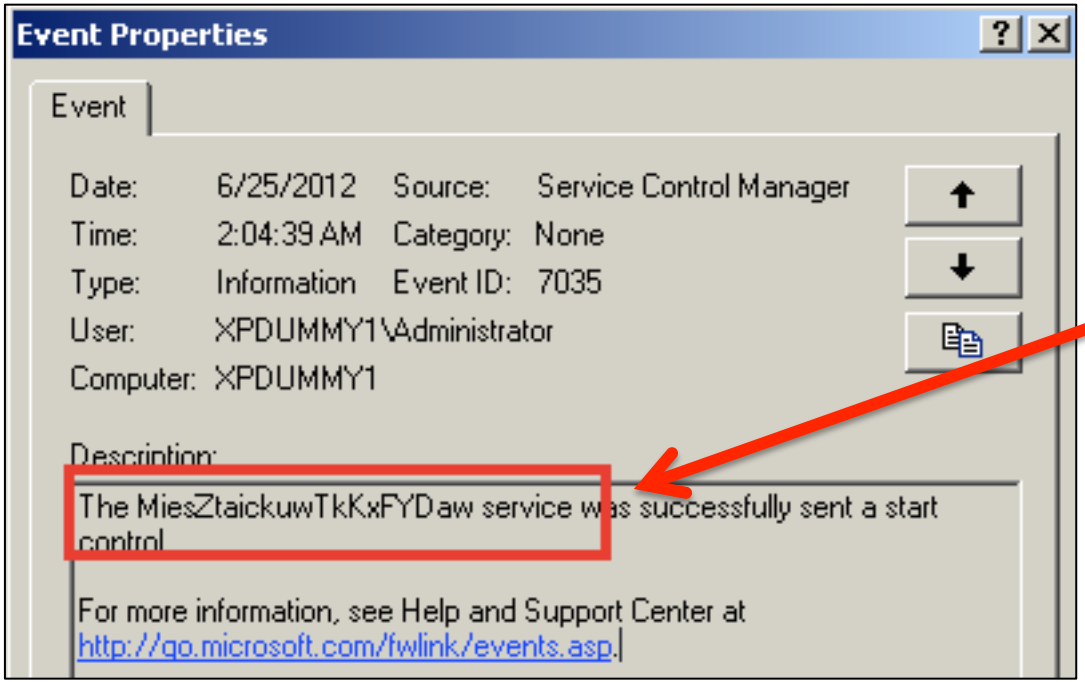
Breach: Target USA Kill Chain



Speed vs. Stealth

Traditional penetration testing = hack clients as fast as possible.

Real attackers want to get away with the crime.



Metasploit
PSEXEC

70-80% of penetration testing tools are simple to detect. That's why real attackers don't use them.

** PSEXEC is one of the most common tools to remotely execute binaries on Windows machines.

Threat Actor: Desert Falcons
Cyber mercenaries operating from the Middle East
~30 members working in three teams across multiple countries
Spear phishing, social engineering and drive-by-download
Bespoke backdoors and spyware for desktop and mobile OS
Interested in personal data, audio recordings, SMS, passwords and keystrokes

Threat Actor: Hacking Team
Zero day exploits in IE, Flash, and the Windows Kernel
Spying software for Android, iOS, Blackberry and Windows Mobile
Rootkits and backdoors for all major operating systems
Sophisticated C&C communication network across multiple channels

THE HACKING SUITE FOR GOVERNMENTAL INTERCEPTION

"If you want to defend against APT-level actors, you need to use a Red Team that maintains and uses kits at least at Hacking Team's level." – Dino A. Dai Zovi

Traditional Penetration Testing
Goal: Identify high-risk vulnerabilities
Philosophy: Obtain the broadest coverage of testing at minimum cost
Methodology: • Vulnerability Scanning • Vulnerability Scanning + Validation using Metasploit • Compromising the network using “pentest tools”
Delivery: • Mostly performed in silos as an assurance exercise • Once or twice a year conducted against the entire network

Next Generation Penetration Testing
Goal: Build the strongest case against an organisation's security plan
Philosophy: Simulate realistic threat actors
Methodology: • Use similar techniques, processes and tools as they would • Attempt to reach the same objectives they have
Delivery: • Any time, any where, against anything - so long as it fits the attack scenario(s)

Comparing Methodologies

Traditional Penetration Testing
Network Reconnaissance
Vulnerability Scanning / Discovery
External Exploitation
Privilege Escalation
Post-Exploitation

VS.

Next Generation Penetration Testing
Threat Actor Profile Design
Attack Scenario Design
Threat Actor TTPs Design
Attack Scenario Execution
Actions on Objectives

Metaphor: “pop shells”

Metaphor: “Realistic attack scenarios”

Case Study: Corporate Espionage

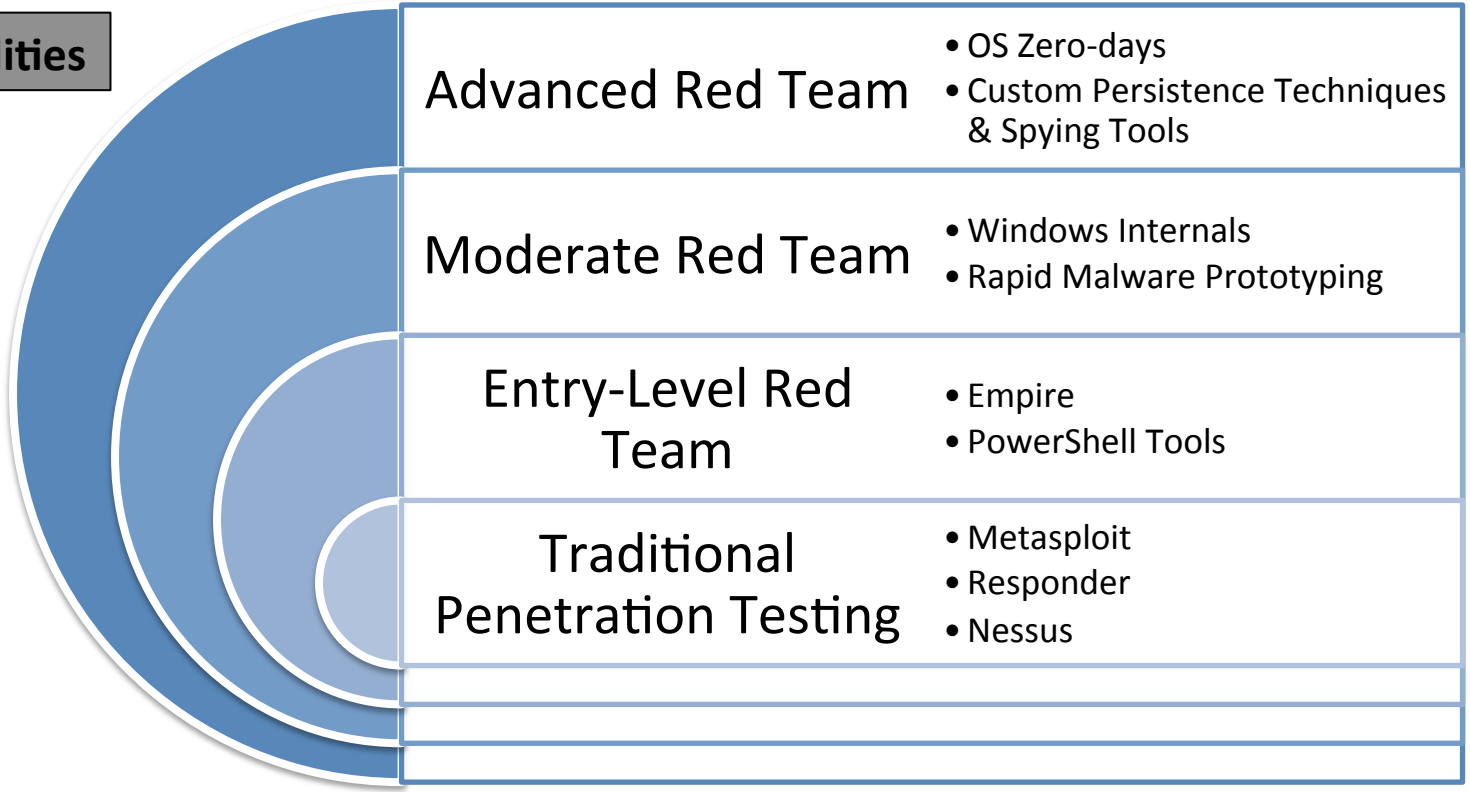
CONFIDENTIAL COMMUNICATION

SUBJECT TO LEGAL PROFESSIONAL PRIVILEGE

HOW TO MEASURE A RED TEAM'S SUCCESS:

Immediate business executive impact

Comparing Capabilities



"You must use a Red Team that can simulate the big breaches in your industry to defend your networks against the level of attacker that is after you."

Traditional vs. Next Generation

Traditional
Security architecture
Find and fix vulnerabilities
Focus on technology
Justify ROI by de-risking IT assets
Measure success by reducing the number of vulnerabilities in assets

VS.

Next Generation
Resilience
Detect, respond and retaliate against threat actors
Focus on people and processes
Justify ROI by demonstrating capability to counter threat actors
Measure success by the speed of detecting and neutralizing attacks that matter

Next Generation Penetration Testing also allows organisations to safely test their retribution tactics and strategies

Retribution: Real consequences for hacking us.

- When do we call law enforcement?
- When do we reverse engineer all their malware and C2 and burn it to the ground?
- When do we find who they are and publish that information online?
- When do we hack back?

If the client can't survive a traditional corporate network penetration test, why bother with a Red Team?

Traditional penetration testing does not generate sufficient C-Level involvement and it drives security investments in the wrong places

i.e. Fixing vulnerabilities instead of adjusting the organisation's security plan.

Cost of purchasing Next Generation Penetration Testing

	Criminal Enterprise	Espionage Campaign	State-Sponsored APT
Estimated cost of a breach	1 – 10M	10 – 100M	< 100M
Cost to simulate	~ $50,000 AUD	~ $100,000 AUD	~ $250,000 AUD
Cost Breach vs. Simulation	4%	1%	0.25%

** Dollar figures presented are based on the professional experience and the opinion of the speaker.

The 50k minimum price point for Next Generation Penetration Testing is the main hold-up for most organisations.

Automate attack scenarios with Python and/or Powershell to commoditize network and OS penetration testing

Summary

- Next Generation Penetration Testing is better at measuring the effectiveness of our security plan because it is more realistic and holistic.
- Next Generation Penetration Testing generates much greater business executive impact compared to traditional penetration testing.
- The greater the complexity to defend an organization, the greater the ROI on Next Generation Penetration Testing Exercises.
- Automate attack scenarios to test security technologies, and use Next Gen to test people and processes.

Questions?

(benmosse@mosse-security.com)