RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Making Penetration Tests Actually Useful

SESSION ID: STU-M07A

Ira Winkler

President
Secure Mentem

Penetration Tests are a Waste of Money

- I made my reputation by performing a wide variety of pentest, Social Engineering, Espionage Simulations
- Took over banks EFT systems
- Plant malware in the power grid
- Stole billions of dollars of IP
- Had the ability to cripple Global 50 companies
- Etc.

The Reality

- I could have given my clients most of the same recommendations without doing all of that
- Sometimes, they needed proving
- For the most part though, the actual penetration was a waste of time and effort

What is the Job of a Security Professional?

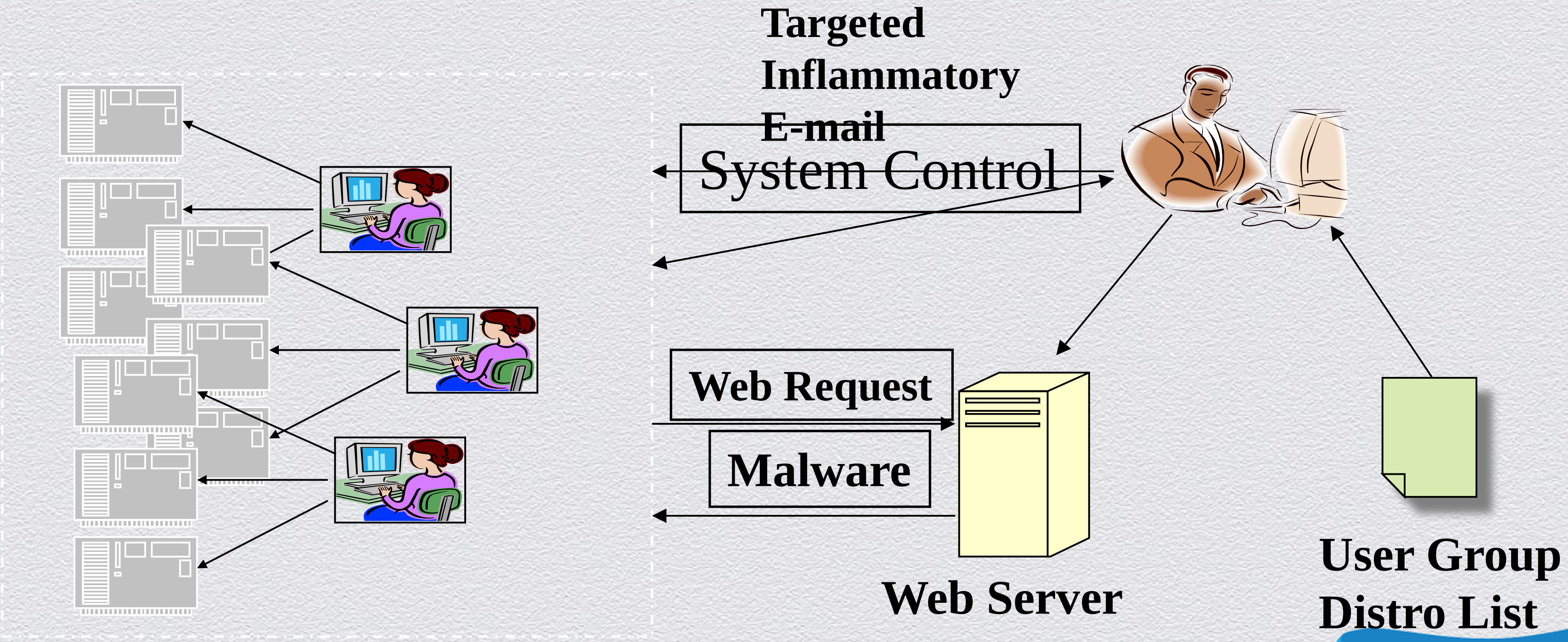
- Security professionals secure things
- They don’t break things
- The goal is to leave things better than they are

Penetration Tests are a Game of “Gotchas”

- Too many people who perform pentests want to parade around a set of trophies
- That is only OK if the customer wants to prove that they have problems or a potential value
- But even then that should not be the only goal
- They usually know that they have problems

Gotchas are Worthless!

Case Study



Targeted
Inflammatory
E-mail
System Control
Web Request
Malware
Web Server
User Group
Distro List

What Did That Prove?

- SCADA systems open to viruses
- There is one port open to the outside world
- Control and business networks overlap
- Employees susceptible to spearphishing taking advantage of pending merger
- Which of those things warranted all of that effort?

What Should Penetration Tests Be?

- A deeper Vulnerability Assessment
- A chance to see the reality of security as it is practiced in the organization
- A systematic approach to identifying consistent vulnerabilities across an organization

Constructing for Generalizability

- The goal is to provide a repeatable test that determines the state of consistent technical and human behaviors across an organization
- Should be able to measure across an organization to determine if there are different behaviors in different areas
- Takes into account demographics and job functions
- Determining if there are technical countermeasures that can offset poor awareness consistently

Proactive Data Collection is Key

- Too many people research a target to find pretexts that will work
- Examining the structure, business needs, business areas, locations, job functions, is even more critical
- You are assessing the organization, not shooting for gotchas…unless that is the specific goal

What Does It Take to be Caught?

- Detection is more important than prevention
- If caught, does the organization react correctly?
- Need to systematically raise attack sophistication levels to determine at what level the organization fails
- This way you can determine where you need to start
- Finds flaws in detection

Structure the Report in Advance

- You want to have tables already laid out
- Ensure systematic examination of the network architecture
- For the human element, tables involve locations, job functions, gender, etc.
- Looking for observations proactively

Pretexts Must be Specifically Defined

- Scripts and sophistication levels must be standardized
- You are establishing a baseline level
- Deviating from the defined levels means that you are not getting consistent results or know how to improve
- Can better target awareness training
- You need to constantly raise awareness levels
  - Standard phishing campaigns don’t do it

Conclusions

- Penetration tests need to be more than a game of “gotchas”
- Penetration tests need to be designed proactively to provide value
- Design for repeatability
- Target sophistication levels, lower to higher
- There is nothing wrong with being caught
- You want to see where you can get caught

For More Information

Ira@securementem.com

+1-443-994-0245

www.facebook.com/ira.winkler

@irawinkler

www.linkedin.com/in/irawinkler