Social Engineering to Improve Security Awareness

SECURE MENTEM

- Ira Winkler, CISSP
- +1-443-603-0200
- ira@securementem.com

Penetration Tests are a Waste of Money

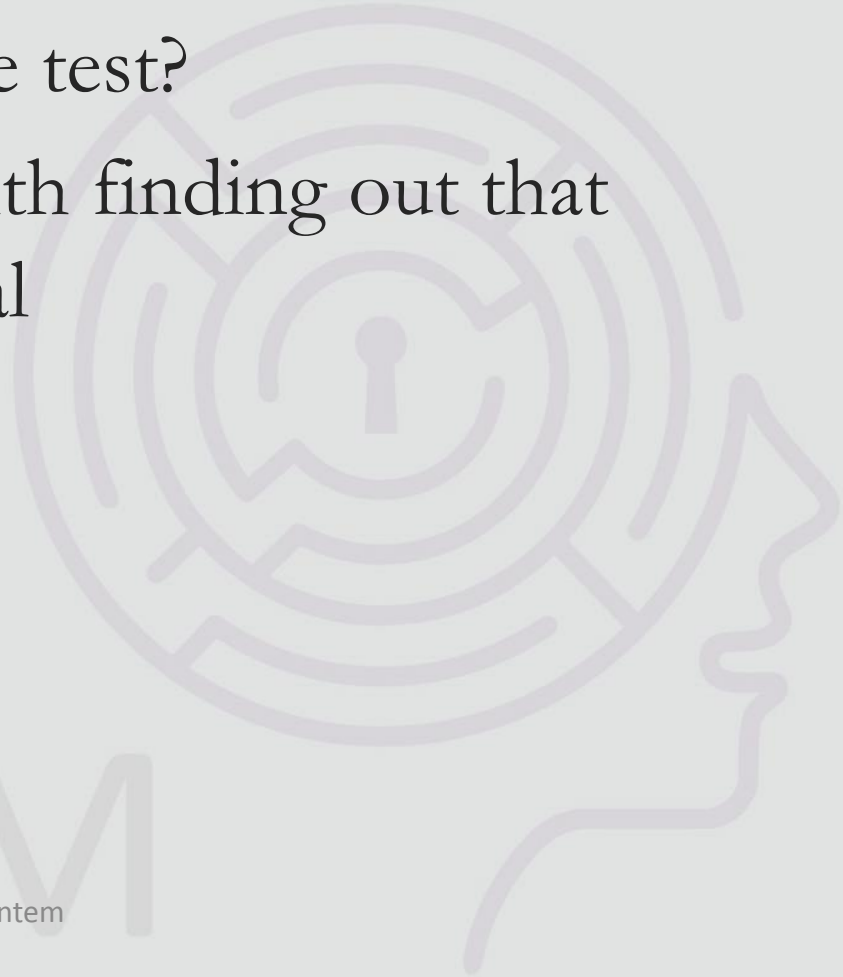
- I made my reputation by performing a wide variety of pentest, Social Engineering, Espionage Simulations
- Took over banks EFT systems
- Plant malware in the power grid
- Stole billions of dollars of IP
- Had the ability to cripple Global 50 companies
- Etc.

The Reality

- I could have given my clients 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

Is 10% a Failure?

- Depends on your goal
- What is the purpose of the test?
- There is nothing wrong with finding out that security has achieved a goal



What is the Job of a Security Professional?

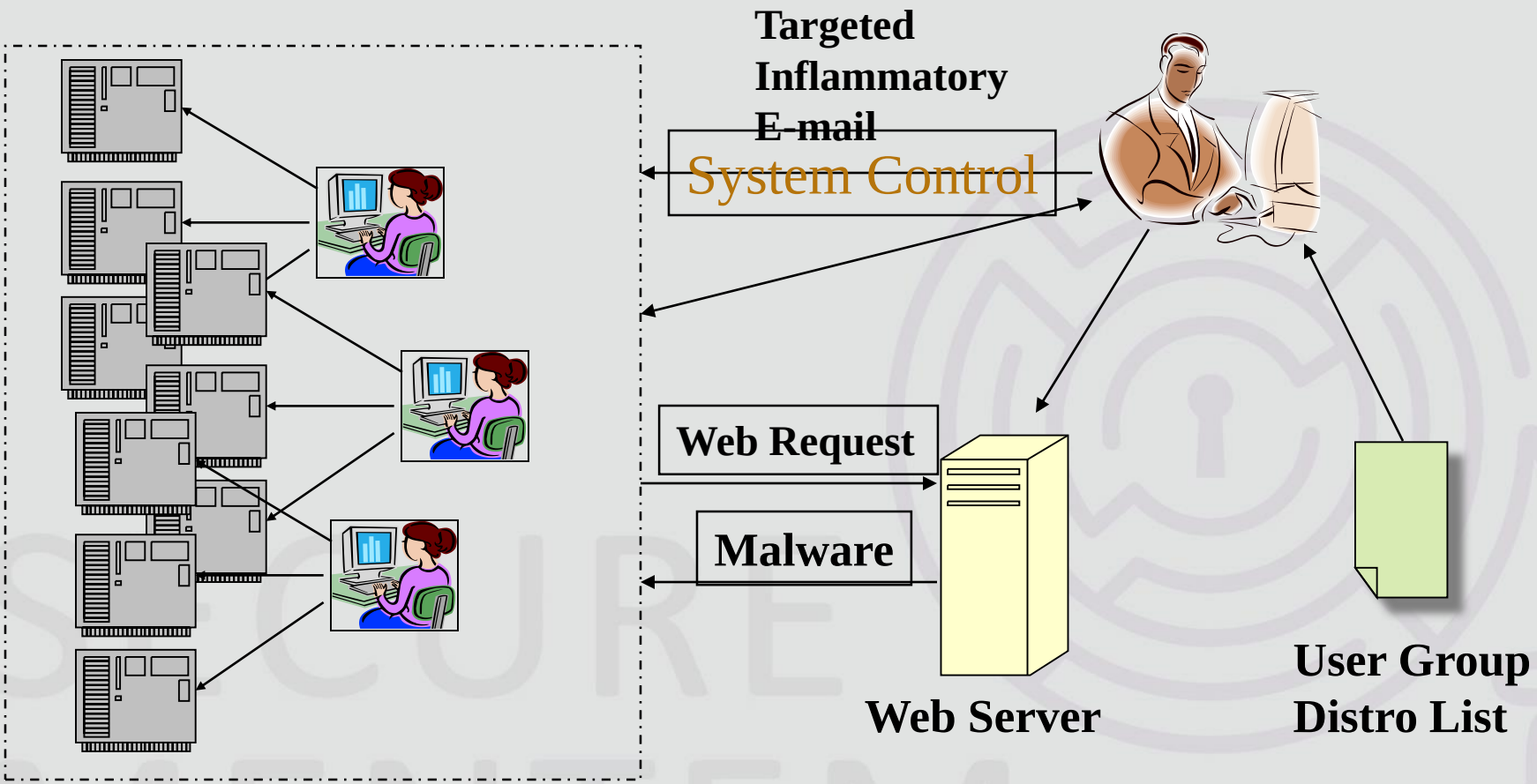
- Security professionals secure things
- They don't break things
- The goal is to leave things better than they are

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



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?

Interesting Test

- Penetration test involved targeting HQ of Fortune 500 company
- Walked by reception desk
- Called operator as CIO to get badges issued
- Went to reception desk
- Guard took pictures, recommended server room access

The Call

- Three weeks after the test I get a call from the physical security manager
- Demanded to know who issued the badge

Response

- Told him I had no idea if he was whom he says he was
- Told him to ask the CIO to call me if he wanted the information
- Advised him that the fact that he didn't know who issued me a badge was worse than issuing the badge
- Said I would tell the CIO that if he called

What Did All That Prove?

- There was no formal process in place to issue and track badges
- There was no process in place to track controlled area permissions
- Did I need to do all that to find this out?

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

Training vs. Awareness

- Basic, but needs to be said
- Training is providing a fixed body of knowledge and testing for comprehension
  - Actually short term memory
- Usually required by compliance and regulatory standards
- Seems to be the case for 75+% of "Security Awareness Programs"

Training

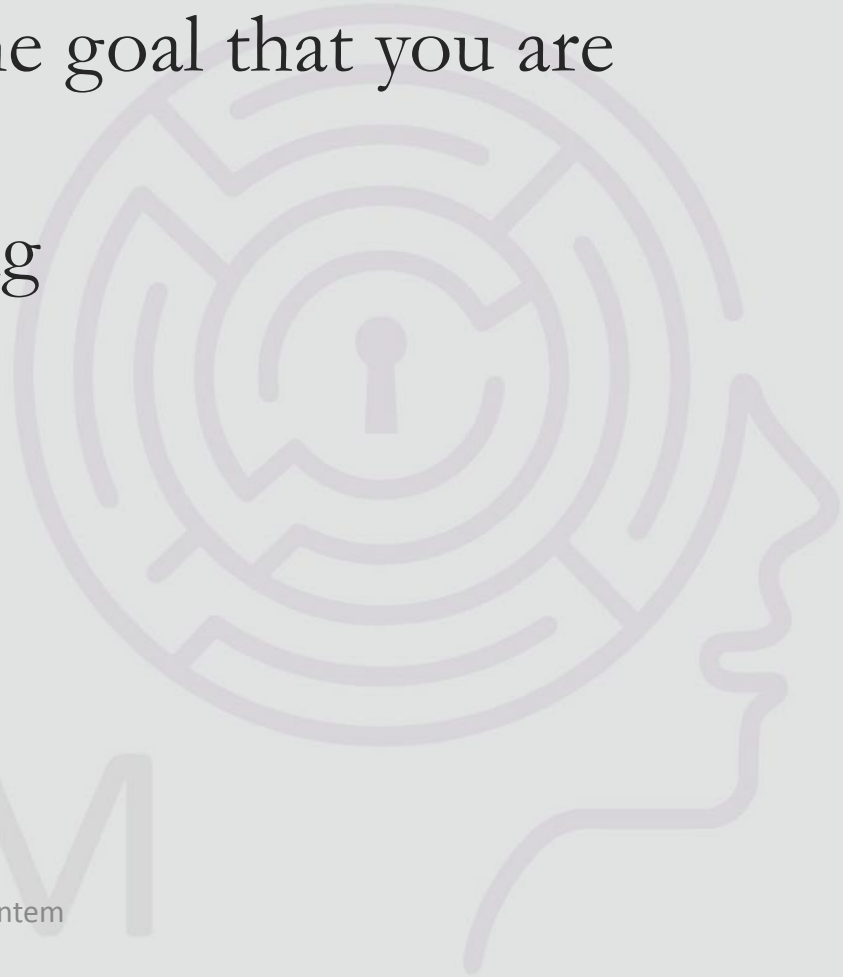
- Definition per NIST 800-50
- Usually CBT
- Sometimes attendance at events
- Metrics involves percentage of employees completing the training
  - Hopefully they pass the test

What is Awareness?

- The purpose of awareness is to create behavior change
- Behavior change improves security culture
- Employees do the right thing by default
  - It creates Common Knowledge
- Security incidents are reduced
- Culture was top concern at recent CISO event

Measuring Awareness

- Different measures for different purposes
- You need to understand the goal that you are trying to measure
- Requires proactive planning



What is Social Engineering?

- Manipulating people to get them to take actions they shouldn't otherwise take
- Phishing is a form of Social Engineering
- USB drops are also a form of Social Engineering
- You can call it Human Assessments if you want a term, but that wont fly in a Hackers track

Constructing for Generalizability

- The goal is to provide a repeatable test that determines the state of consistent behaviors (aka awareness) 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

Structure the Report in Advance

- You want to have tables already laid out
- 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

Achieving Your Goals

Do You Have a Goal?

- Serious question
- Do you want to decrease incidents?
  - By how much?
- Is there a desired behavior you want to increase or decrease?
- In the absence of a stated goal, it is hard to say you are successful unless you just want to decrease things
- Pick easy goals at first

Real Metrics

- Awareness is to change behaviors
- You need to test root behaviors to know if awareness efforts are having an effect
- Behaviors need to reflect specific targets of the awareness campaign

Root Behaviors

- Secure Mentem identified 17 unique behavioral topics and 7 compliance topics
- Each behavioral topic is embodied by one or more behaviors
- Compliance topics can sometimes be measured by behaviors, sometimes knowledge

Behavior Metric Samples

Look for Organic Resources

- Guards
- Access controls
  - Physical and technical
- Computer and network technologies
- Audit staff

Phishing

- Already well known to do phishing simulations
- Track statistics
- Can be deceiving
  - Not everyone likes cats
- Better to integrate complexity into the strategy to raise the bar

Physical Security

- Tailgating
  - Counting
  - Simulating
- Clean desk policies
  - Walkthroughs

Social Engineering, Phishing, and other Pentests

Metrics Should Integrate Statistics

- Social engineering, phishing, etc. should be repeatable
- Testing should "purposefully" examine all parts of an organization
- Remember that the goal is not to break an organization, but fix it
  - You need to have valid data, not random "gotchas"
  - Unless you need the gotchas, which most organizations don't
- Complexity introduced over time

Conclusions

- Metrics are very often overlooked
- Goals are good – Make sure you have some
- Metrics can study components and topics
- Metrics will help you justify your efforts
- Metrics will help you keep and improve your budget
- It helps you do a better job

Additional Resources

- www.securementem.com for paper
- CSO magazine – csoonline.com

For More Information

Ira@securementem.com
+1-443-994-0245
www.facebook.com/ira.winkler
@irawinkler
www.linkedin.com/in/irawinkler