MADSecurity

Making A Difference

Penetration Testing! The Nitty Gritty…

Jeremy Conway

Partner/CTO

Before I Start…

What qualifies me to speak about this?

MADSecurity
Making A Difference

It's all important and relevant!

Brief History… The Past!

- US Active Army
- DoD Contractor
- NASA Contractor
- Commercial Security Vendor
- Founder of Cyber Security Company

Sort of just fell into it!

MAD Security
Making A Difference

MADSecurity
Making A Difference

20+ years of Invaluable Experiences with a wide range of Cyber Security Issues and Situations!

But you know what the definition of experience is, right?

Experience is…

Something You Don’t Get Until Just After You Need It!

The Present… Partner / CTO

MAD Security

Making A Difference

Advancing the Mission of Cyber Security through Integrated & Innovative Solutions!

Our Experience…

Wide Range of Organizations

From SMB to Fortune 100

In All Verticals

Financial, Retail, Health Care, Education, Manufacturing, Energy, Utilities, and Government Sectors!

MADSecurity
Making A Difference

The Future…

Share our Experiences

and Expertise with

EVERYONE

that will listen!

We don’t have all the answers,
but we have seen a lot!

So what qualifies me to answer this?

Experience…

Everything in this presentation is based on first hand experience and my own data!

Disclaimer:

Random Internet Gathered Statistics not included!

What is Penetration Testing?

A test evaluating the strengths of all security controls for a computer system.

Penetration Tests evaluate ***procedural*** *and* ***operational*** *controls as well as* ***technological*** *controls!*

What is the Intent of a Pen Test?

Determine feasibility of an ***attack*** *and the amount of* ***business impact*** *of a successful exploit of an attack.*

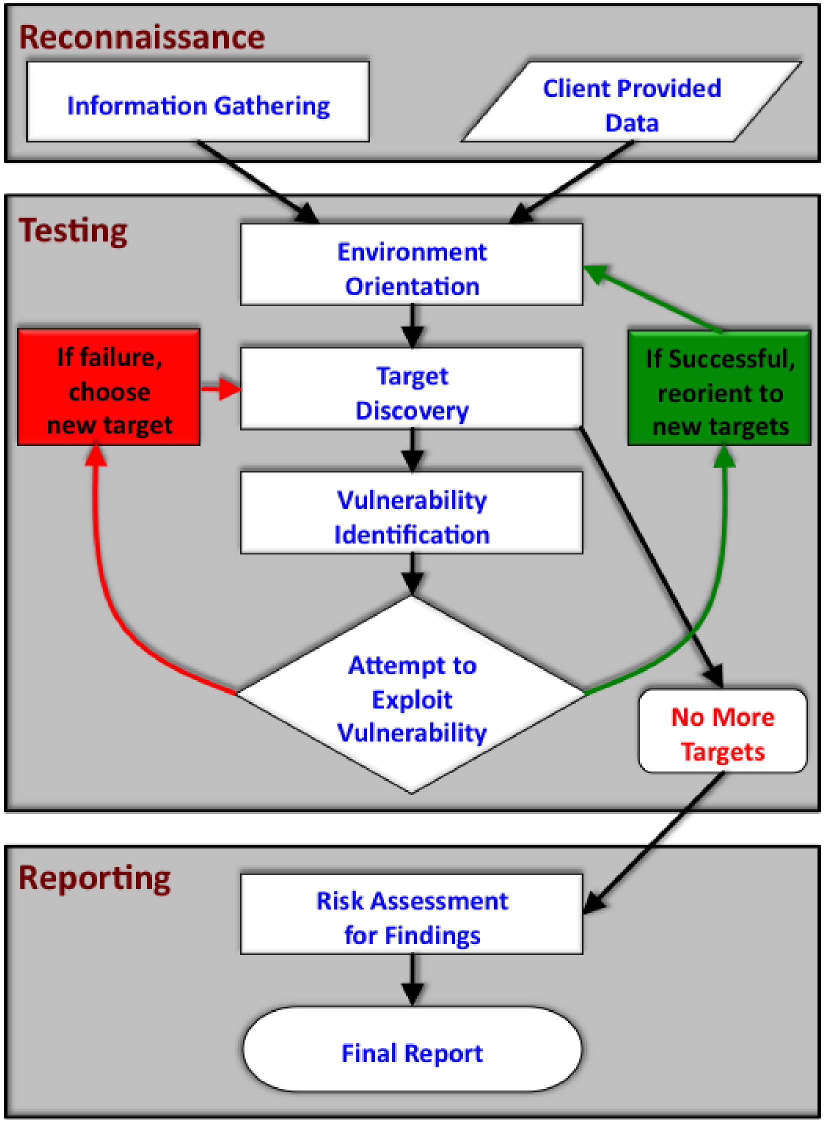
The Goal is to demonstrate…

BUSINESS RISK!

MADSecurity

Making A Difference

Our Pen Testing Methodology


Reconnaissance
Information Gathering
Client Provided Data
Testing
Environment Orientation
If failure, choose new target
Target Discovery
If Successful, reorient to new targets
Vulnerability Identification
Attempt to Exploit Vulnerability
No More Targets
Reporting
Risk Assessment for Findings
Final Report

- Based upon best practices from:
  - NIST
  - OSSTM
  - OWASP
  - Experience
- Provides:
  - Repeatability
  - Reliability
  - Quality
  - Minimal Risk
  - Complete Understanding

MADSecurity
Making A Difference

NIST 800-115 Methodology

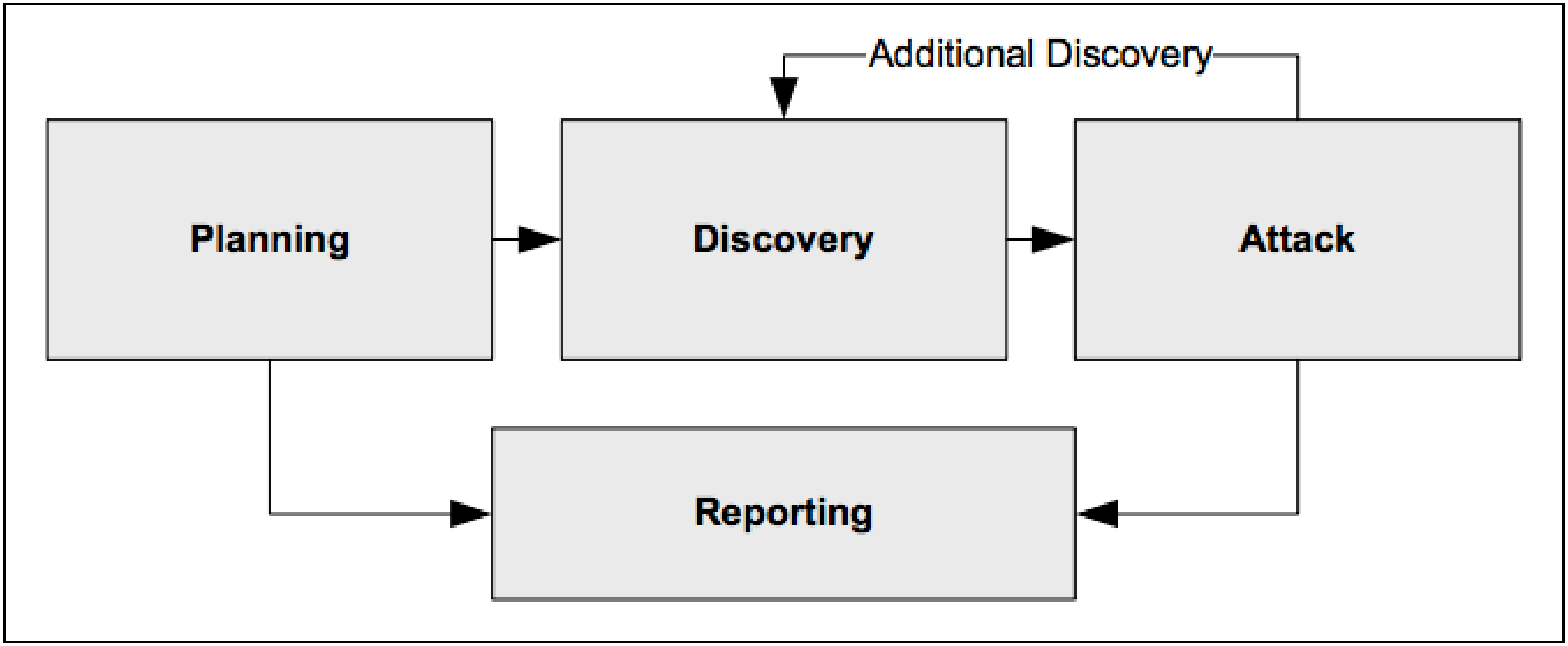
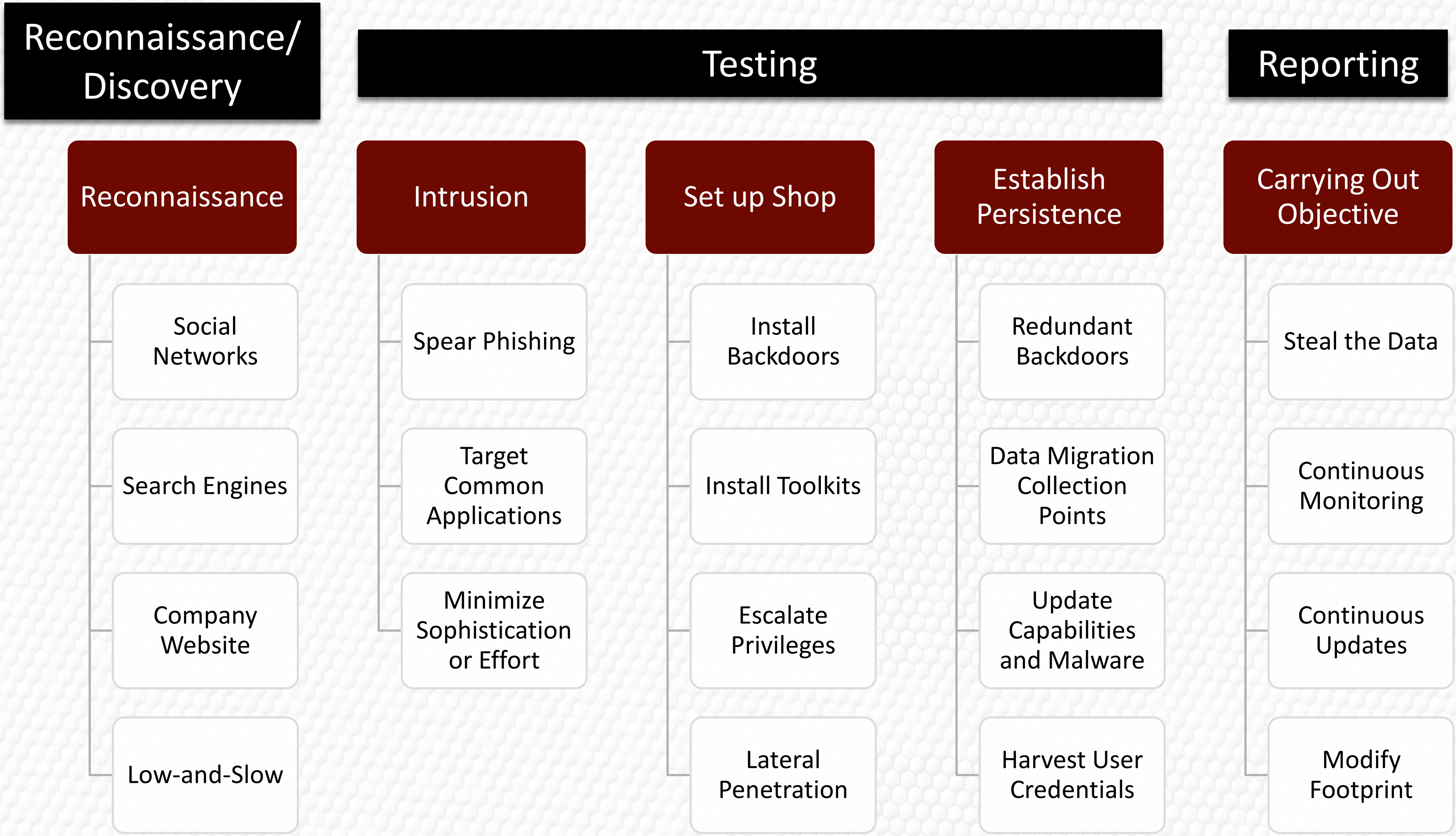


Figure 5-1. Four-Stage Penetration Testing Methodology

General APT Methodology



Reconnaissance/ Discovery

- Reconnaissance
  - Social Networks
  - Search Engines
  - Company Website
  - Low-and-Slow

Testing

- Intrusion
  - Spear Phishing
  - Target Common Applications
  - Minimize Sophistication or Effort
- Set up Shop
  - Install Backdoors
  - Install Toolkits
  - Escalate Privileges
  - Lateral Penetration
- Establish Persistence
  - Redundant Backdoors
  - Data Migration Collection Points
  - Update Capabilities and Malware
  - Harvest User Credentials

Reporting

- Carrying Out Objective
  - Steal the Data
  - Continuous Monitoring
  - Continuous Updates
  - Modify Footprint

MADSecurity

Making A Difference

Approaches to Pen Testing

Black Box

No specific knowledge of the structure of the target

White Box

Complete knowledge of the structure of the target

Grey Box

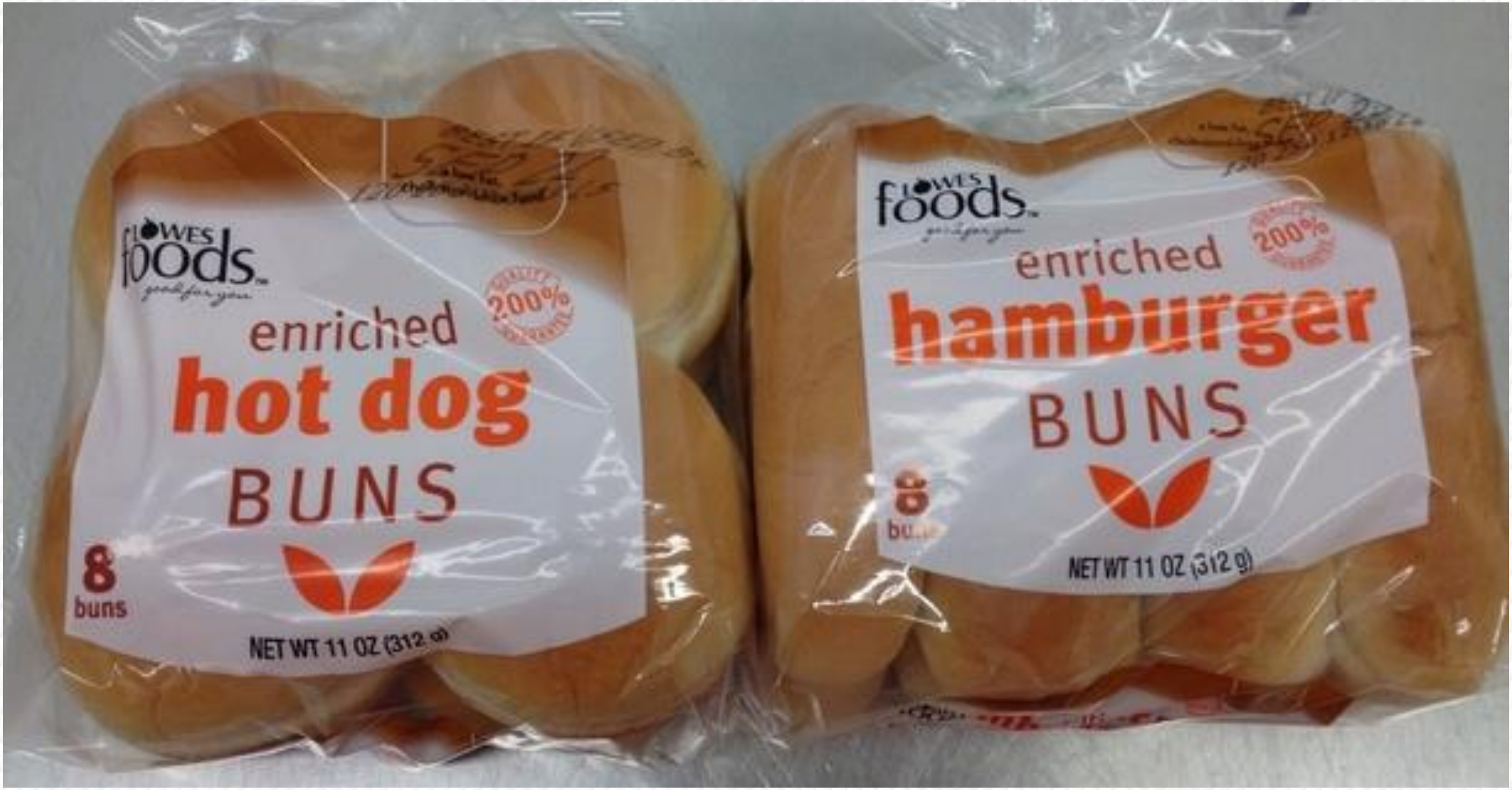
Limited knowledge of the structure of the target

Making Penetration Testing a Success!

How to successfully procure and carry out a penetration test!

MADSecurity
Making A Difference

The goal is to avoid this!



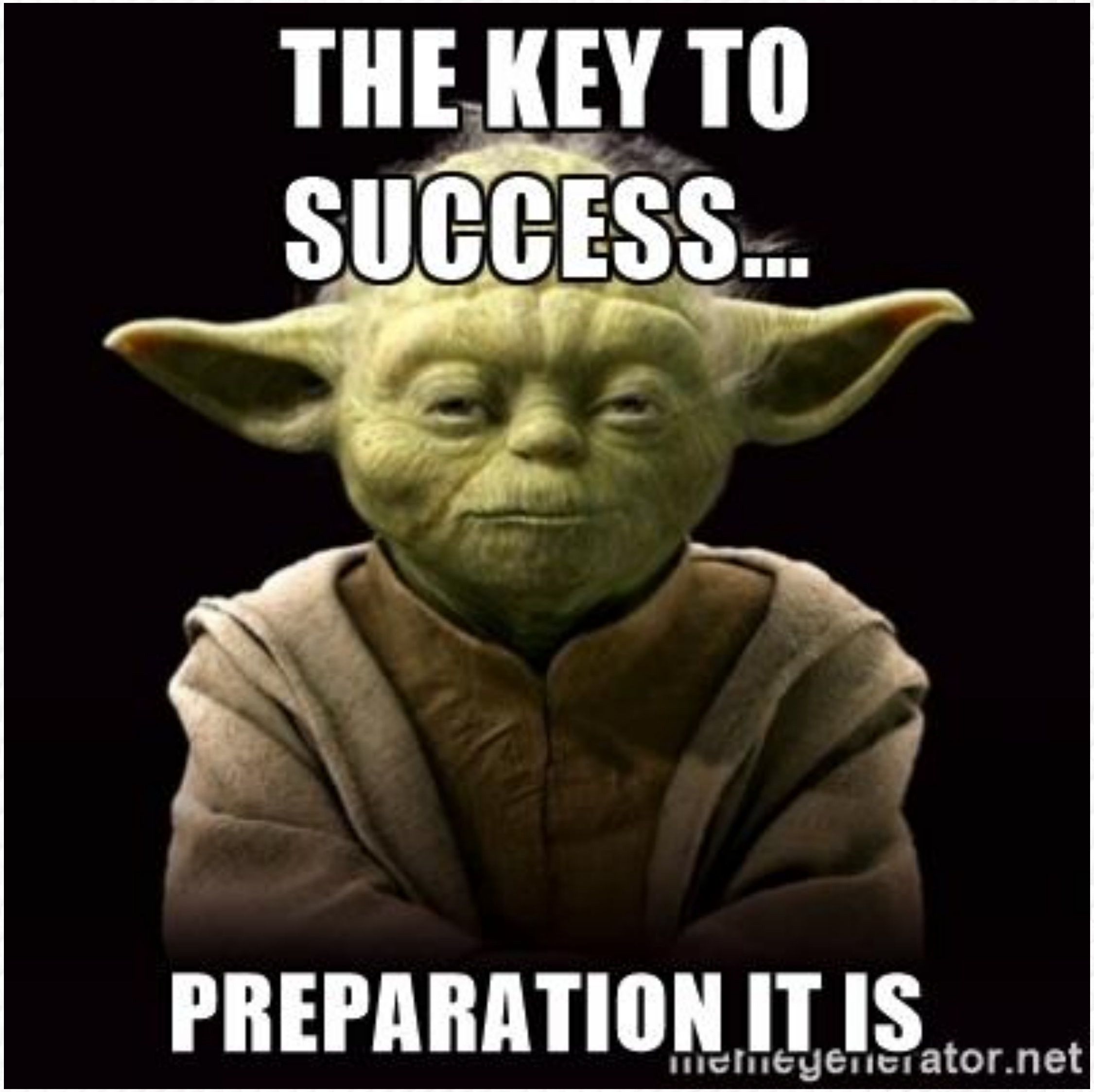
Simply put…

Penetration testing is not a straightforward process nor a panacea for all ills!

Three main phases of an engagement.

- *Preparation*
- *Execution*
- *Delivery*

Yoda knows!



MADSecurity
Making A Difference

Pre-Engagement Steps

- *Type of Test*
- *Testing Approach*
- *Scoping*
- *Dealing with 3rd Parties*
- *Rules of Engagement*
- *Communication Plan*

Types of Penetration Tests

- *External Network*
- *Internal Network*
- *Social Engineering*
- *Web Application or Service*
- *Mobile Application or Service*
- *Wireless*
- *VoIP and Telecom*
- *Embedded Systems*
- *Endpoint*
- *Applications*
- *Red Team*

Testing Approach

- *Black box*
  - *Reconnaissance information is important to the assessment*
  - *Time intensive for assessment team*
- *White box*
  - *Thoroughness is important to the assessment*
  - *Time intensive for both assessment team and customer*
- *Grey box*
  - *Most popular, cost effective, and well balanced*

MADSecurity
Making A Difference

Scoping

- Network Pen Testing
  - Number of Networks and Domains
  - Number of Live IPs
  - Services Footprint and Saturation
- Social Engineering
  - Number of Users Targeted
  - Number of Scenarios
  - Physical Locations
- Wireless
  - Number of SSIDS
  - Number of Access Points
  - Physical Location Specifications (size, locations, multitenant building)
  - Clients in scope

Scoping

- *Web Applications and Web Services*
  - *Platform, framework, and/or languages used*
  - *Client side technologies (Flash, Java Applet, Silverlight, AJAX)*
  - *Environments to test (production, staging, testing, etc)*
  - *Number of account roles to be assessed*
  - *Type of authentication used*
  - *Number of dynamic pages*
  - *Number of API functions or methods*
  - *Backend data storage (database, NoSQL, files, etc)*
- *Mobile Applications and Mobile Services*
  - *Same as Web Applications and Web Services*
  - *Client Authentication (client side certificates)*

Dealing with 3rd Parties

Numerous situations are common now with third parties.

Must get third party permissions!

- *Cloud Services*
  - *Biggest issue is shared data storage (multiple organizations on a single service)*
  - *Most cloud services have published guidance on Pen Testing, FOLLOW IT*
- *ISP*
  - *Verify Terms of Service*
  - *Could block or disable service*
- *MSSPs*
  - *Depends on testing goals (Response time, detection capabilities in scope)*
  - *Testing their devices they need to be notified typically under Terms of Service*

Rules of Engagement

Defines how the testing will occur

- *Timeline – Schedule, Testing Windows*
- *Locations for onsite testing*
- *Sensitive data handling and disclosure process*
- *Preferred method of secure communication*
- *If VPN or remote appliance is used, data security and storage*
- *Evidence handling and sanitization after testing*
- *Level of exploitation*
- *Post exploitation activities and pivoting*
- *Handling legacy or critical systems*

Rules of Engagement

Defines how the testing will occur

- *Critical and high risk findings disclosures*
- *Dealing with shunning and/or security controls*
- *Incident response process (will customer be reacting and changing environment?)*
- *Steps to disclose discovery of previous or active compromise*
- *Handling Passwords, is cracking allowed*
- *Testing information needed, IPs and equipment requirements*

Communications Plan

Establishes lines of communication

--- can be a part of the ROE

- *Emergency points of contact information both client and assessment team*
- *Preferred method for secure communications*
- *Status meetings schedules*
- *Defined status update prompts*
  - *Risk level of finding*
  - *Risk level of performing an exploit*
- *Delivery method of report*

Execution Phase

Assessment is executed and should follow the defined pre-engagement processes!

Delivery Phase

Reporting and Documentation Structure

- *Executive Summary*
- *Scope definition*
- *Assessment Methodology*
- *Risk determination and definitions*
- *High level Strengths and Weaknesses*
- *Overall Findings Statistics*
- *Sections for each assessment type*
- *Assessment type overview/narrative*

Delivery Phase

Reporting and Documentation Structure

- *Detailed findings with:*
  - *Finding Name*
  - *Affected hosts/devices*
  - *Risk Level (Impact and Likelihood values)*
  - *Detailed explanation*
  - *Detailed risk explanation and definition*
  - *Detailed remediation recommendations and steps*
- *Appendixes with supplemental data and information*
  - *Exploitation Artifacts*
  - *Password Analysis*
  - *Hardening guides and recommendations*
  - *Fingerprinting and network mapping results*
  - *Automated vulnerability scan results*
  - *Glossary of terms*

Delivery Phase

- *Report Rendering Presentation*
- *Remediation testing and scheduling*

MADSecurity
Making A Difference

Common Penetration Testing Mistakes:

- *Restrictions:*
  - *Testing to non production systems*
  - *The hours of testing*
  - *The length of the test*
- *Not Allowing Exploitation*
- *Not scoping correctly:*
  - *Missing IPs/Networks*
  - *Incorrect testing type or approach selected*
- *Changing the Rules during testing*
- *Only performing it externally*
- *Not including Social Engineering*
- *Focusing on Technical Issue and Not Business Risk*

Most common and costly mistake!

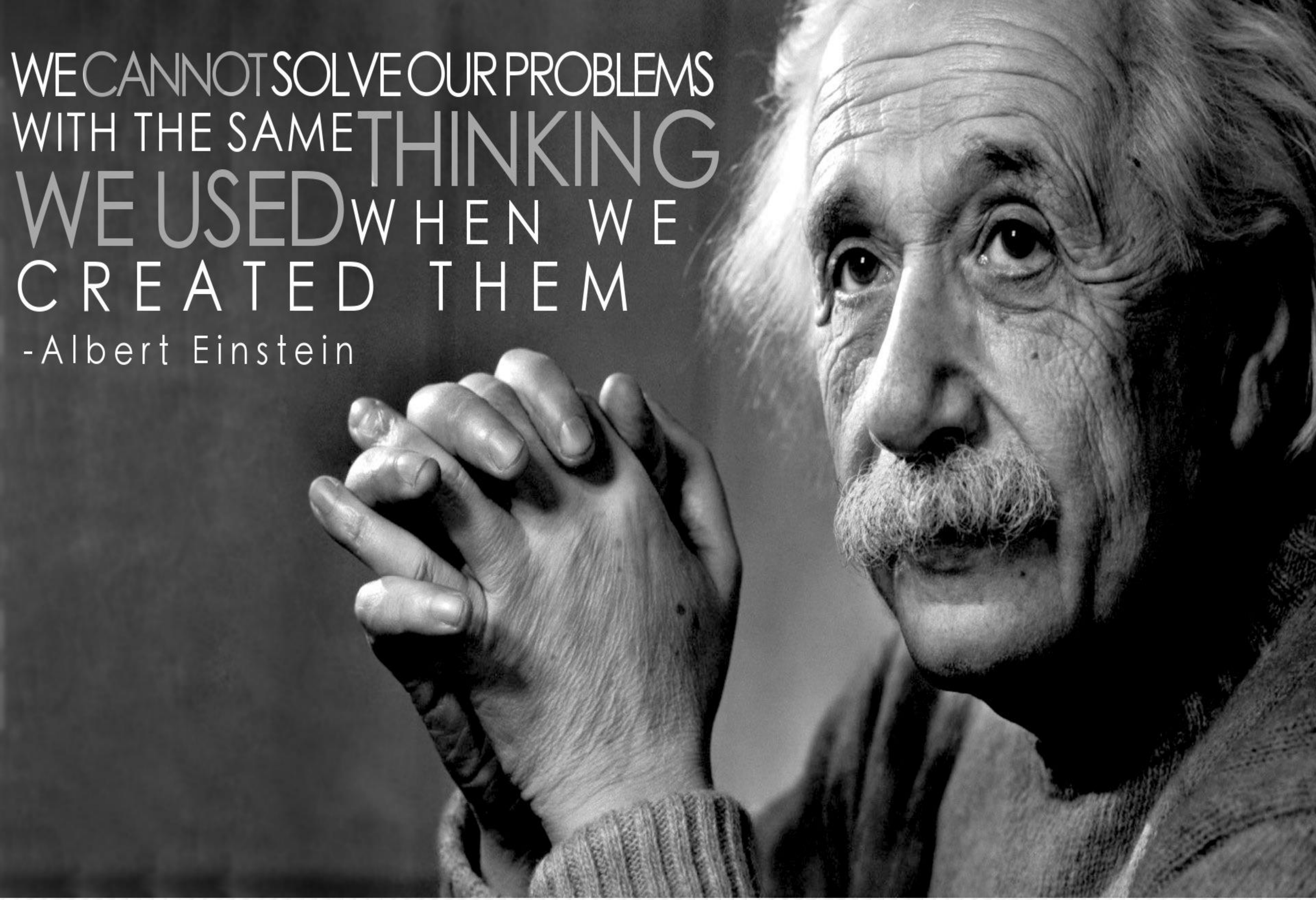
*Losing sight that the assessment is to test the security controls of the environment and **NOT** to assess the assessment teams skillset!*

MADSecurity
Making A Difference

2nd Most common and costly mistake!

Dismissing findings because:

- *Lack of understanding*
- *Fear of asking questions or seeking clarification*
- *Assuming security controls will mitigate without testing*
- *Can’t reproduce the finding*



WE CANNOT SOLVE OUR PROBLEMS WITH THE SAME THINKING WE USED WHEN WE CREATED THEM

-Albert Einstein

Albert Einstein

MADSecurity

Making A Difference

Questions?