Kevin Wilkins, CISSP
C.T.O. iSECURE LLC

Penetration Testing and Shooting Fish in a Barrel

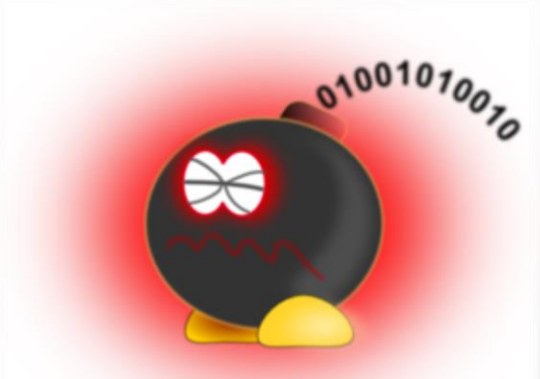
Prepared for the attendees of RSS 2016

Meetings and Greetings

- Kevin Wilkins, CISSP – Chief Technical Officer, iSecure LLC
  - Kevin Wilkins is the Chief Technology Officer (CTO) at iSecure, LLC. Mr. Wilkins oversees the implementations of Network Security product portfolios specializing in the heavily regulated environments such as PCI, SOX, HIPAA/HITECH. Mr. Wilkins has been in the IT industry since 1998 and has had extensive operational experience in Network Engineering, Systems Administration, Telecommunications, and Information Security.

Synopsys

- “Penetration Testing” is an often misunderstood term in Information Security. Sometimes a Penetration Test is requested without fully understanding the full scope that such an engagement will entail. It is often used as a buzzword or a catchall for any type of external security analysis.
- Is your organization’s security mature enough to make a Red Team test beneficial or will the result be similar to blowing a hole in the wall instead of climbing through an open window? Or will an initial assessment which is more open in nature be of more benefit?
- We will discuss the spectrum covering “White Box” Architecture Reviews, Vulnerability Assessments, and “Black Box” Penetration Testing.



iSECURE
IT Security Redefined

Synopsys

- We will also discuss how clearly defining the methodology, rules of engagement, goals of the test, and how the takeaways will be used will maximize the value of such an engagement.
- Clearly defining the expectations of an external security analysis will maximize the value of such an engagement and ensure that you are asking for the right type of service.

Why are we here?

- Organizations will often request a Penetration Test without fully understanding what it will entail and what the results will be.
- An organization engaging in a penetration test without an underlying level of Information Security maturity may see a couple of exploitable vulnerabilities revealed, but miss a bigger picture of risks.

Why are we here?

- A tester may quickly find a couple of things but not even report on all of the exposures - then call it a day. That was easy! Just like shooting fish in a barrel…
- So – let's talk about Penetration Testing as well as some other alternatives that will deliver more value depending on the current level of your Information Security program.

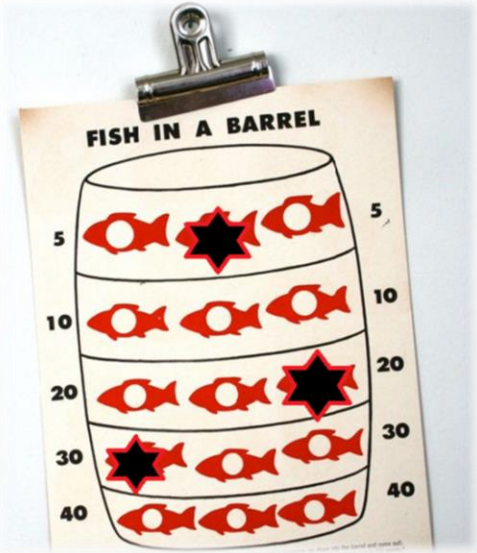
iSECURE IT Security Redefined

What is a Penetration Test?

- A penetration test involves discovering a vulnerability and demonstrating that it is exploitable.
- A penetration test is considered successful (on the part of the tester!) when some level of inappropriate access or control is gained.
- A penetration test is also successful if access credentials or information is harvested.

What is a Penetration Test? (continued)

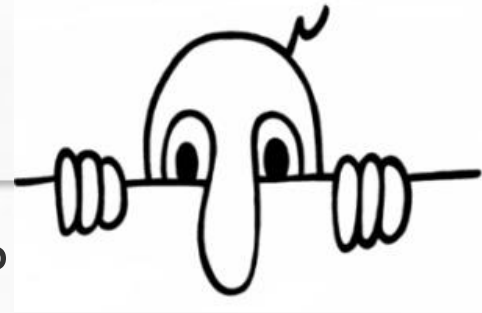
- A penetration tester will report in detail as to what resource was compromised, what methodology was used, and evidence showing that the compromise occurred.
- Although a penetration tester may take a broad view of your environment while conducting a campaign, the end result is often very narrow.
- A penetration tester may only report on one or a few workable exploits - even if many actually exist.



Is a Penetration Test what you actually want?

- Sometimes people ask for a Penetration Test when more value can be seen from a different type of engagement.
- It is good to know what you want to accomplish and select the most valuable type of engagement.
- Some qualifying questions are important to ask.

How secure do you feel your environment is?



- Do you have a well understood environment with a mature security model?
- Do you have a specific compliance requirement to conduct penetration testing?
- Or are you unsure about your security and want to run some testing to find out what needs improvement?

What are you trying to accomplish?

- Demonstrate that your environment is secure?
- Discover any specific vulnerabilities that may exist in an otherwise secure environment?
- Enumerate hosts with known vulnerabilities in order to direct a patch management program?
- Identify what may be a number of systemic weaknesses in your security posture, resulting in a number of security initiatives?
- In a spectacular way, demonstrate that your environment ISN'T secure in order to light some fires?

White Box vs. Black Box

- There is a spectrum of assessment types that may be useful.
- White Box testing is generally a more open and consultative engagement where the assessor as upfront answers to questions and works with the subject to evaluate their security and provide recommendations. Specific tests may take place with full knowledge of the environment.
- Black Box testing involves a more blind approach with limited foreknowledge. The purpose is to play the role of an attacker, or Red Team, to discover vulnerabilities as presented to an outsider.

Wow, Options!

iSECURE
IT Security Redefined

Information Security Architecture Review

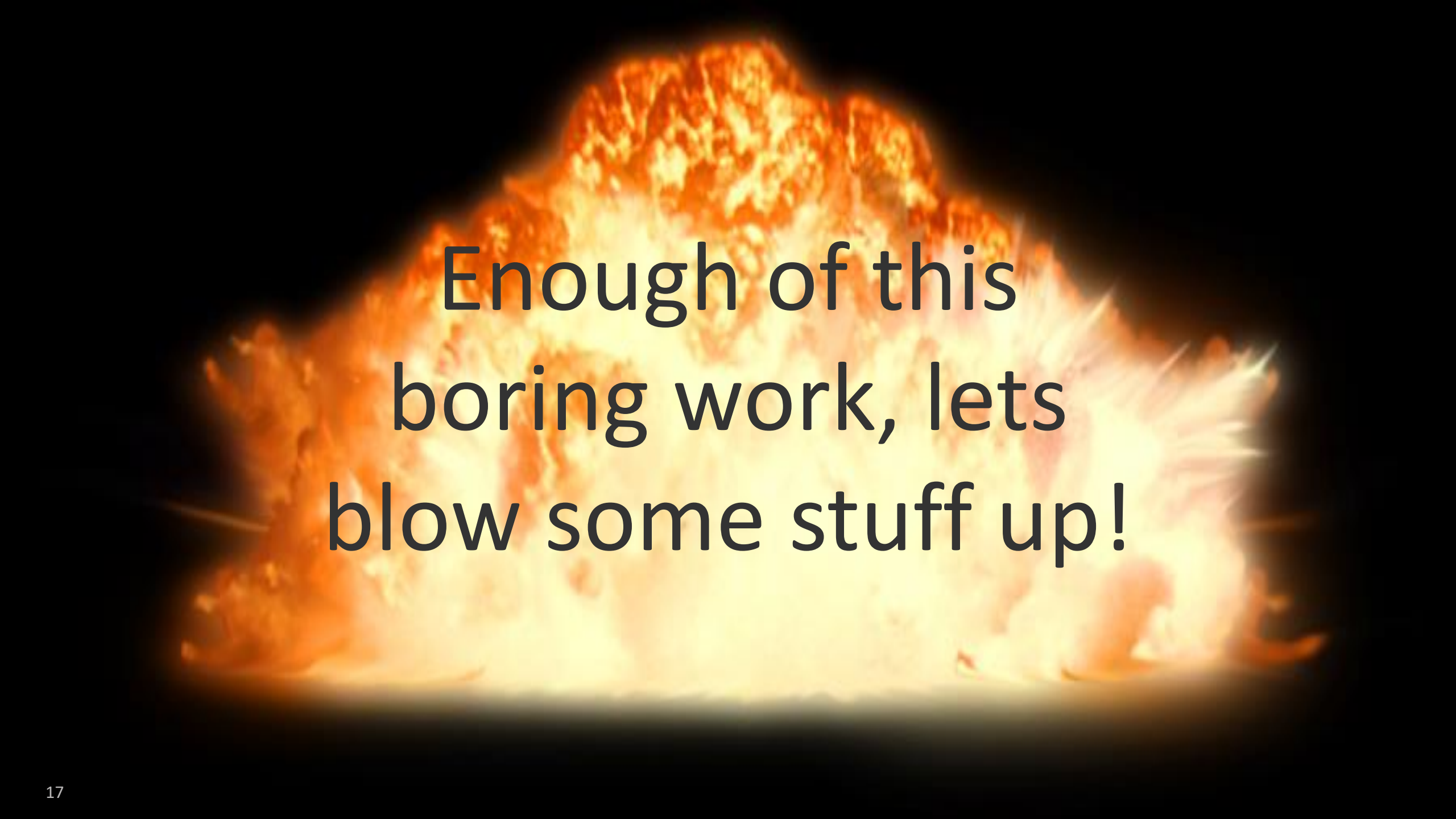
- An Information Security Architecture Review is a White Box assessment with the most open of formats. It is very consultative and collaborative.
- The assessor will discuss with the subject their organization's philosophies and practices surrounding Information Security and Governance.
- What Technical Controls exist and how are they configured?
- What Policies and Procedures exist to maintain a secure environment? Is there a regime of internal Audits to ensure compliance to Policies and Procedures?
- This type of engagement will yield a very broad list of attainable improvements.

Vulnerability Scan and Validation

- A Vulnerability Scan and Validation is also a “White Box” assessment, but more focused on exposed systems and services.
- Target subnets will be identified. Hosts and services will be discovered, then probed for more information. The list of exposed services will then be compared to a database of know exploits.
- Vulnerable, unpatched, and misconfigured services will be reported on.
- Sometimes a cycle of “validation” will be used to eliminate false positives.
- Hopefully a Vulnerability Scan is being used to verify the success of a patch and system management process to see what’s slipping through, not to drive the process itself!
- (We should be patching already, with or without a scan…)

Dynamic Web Application Testing

- A bit more “Black Box” – almost a Penetration Test but focused on a single published Web Application instead of an organization’s broader footprint.
- The server will be tested for vulnerable software and configurations.
- The application’s logic and interactive features will be thoroughly tested. Form inputs and queries will be tested for SQL injection, cross site scripting, authentication, authorization, buffer overruns, etc.
- Both an authenticated and non-authenticated context will be tested.
- This type of test is used to assess the running functions of live application or pre-deployment.
- (See also - Secure Software Development Life Cycle and Static Code Analysis)


Enough of this
boring work, lets
blow some stuff up!

Penetration Testing

- A “Red Team” test! Very exciting. Will you get to use the Big Board?
- Best for organizations that are confident in their Information Security architecture and process.
- While many testers and the hackers they are emulating will try to remain undetected, you can also turn this into a Blue Team exercise – can you track the progression of the test and take steps to defeat it in real-time?
- There is still a fair amount of homework in setting up a Penetration Test. Establishing a clear understanding of Scope and the Rules of Engagement is Critical!

Rules of Engagement

- What Kind of Penetration Tests are you Running?
  - Social Engineering and Phishing
  - Account Takeover
  - Network/Host/Service Based
  - Internal or External
  - Application Testing
  - Wireless and Physical
  - Denial of Service (Yikes!)

iSECURE IT Security Redefined

Rules of Engagement (continued)

- Scope of a Penetration Test
  - What IP addresses, systems, networks, applications, and personnel are in-scope? Enumerate them!
  - When will the Penetration Test take place? Define both specific dates and times of day for Penetration Test activity.
- What are some other aspects of your testing theory?
  - Do you notify your Security Team or test their response?
  - Do you bypass your IPS to just test target hosts or are you testing the IPS as well?

Rules of Engagement (continued)

- Get out of jail free!
  - Have a clear agreement between the tester and the subject organization acknowledging that a test is taking place and who is authorized to conduct it.
  - Make sure the person authorizing the test is authorized to do so! The tester will want to have this agreement and multiple points of contact available.

When am I getting paid for this?!?

Rules of Engagement (continued)

- Liability and Regulation
  - What if the tester actually causes damage to the subject environment? Is the tester liable for this damage or has the tester been held harmless?
  - What if the tester successfully ex-filtrates protected/confidential information? The tester must protect this information with the same level of care expected of the subject organization make full disclosure to the subject organization.
  - The tester must keep confidential any other aspects of the discovered vulnerabilities and exploits.

Rules of Engagement (continued)

- Be Nice! (Or at least civilized…)
  - A tester may install back doors and establish remote access, but must not leave this back door accessible to others or leave a system more vulnerable than when they started.
  - A tester should work deliberately and document every step. This helps validate the evidence of breach and provide more valuable reporting. It also helps backtrack the exploit and ensures any trail left by the tester has been cleaned.

Questions?

Kevin Wilkins
Chief Technology Officer
585-419-8258
Kevin.Wilkins@isecurenet.net

www.isecurenet.net