RSAConference2016
Abu Dhabi | 15–16 November | Emirates Palace

SESSION ID: CIN-W05

Operationally Focused Pentesting

Greg Anderson
Technical Account Manager
Qualys, Inc.
@pghsec

Mike Cook
Cyber Security Researcher and Pentester
CERT Division of the Software Engineering Institute at Carnegie Mellon University

Pentesting is in high demand

- A decade of high-profile data breaches has resulted in governments, regulators, and the public demanding greater due diligence in organizations' security programs

Governance

Regulations

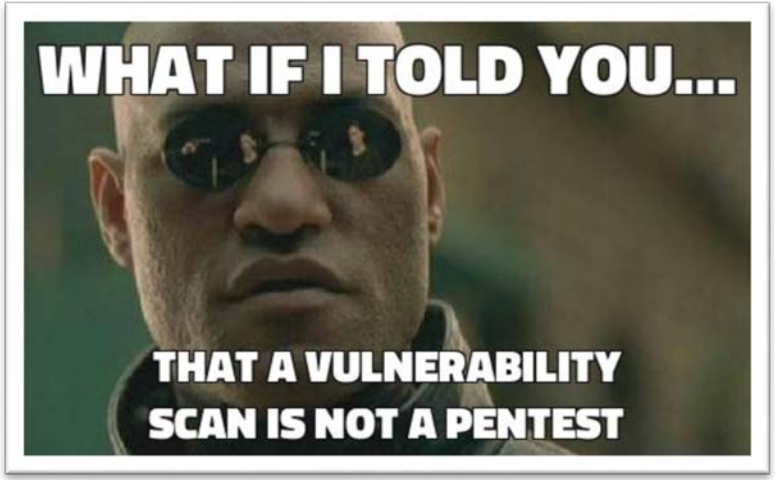
Media Coverage

The Problem with High Demand

- There is currently no universally accepted standard for a quality pentest
- As a result, a pentest means different things to different people
- This makes consistent delivery, output, and value difficult to achieve

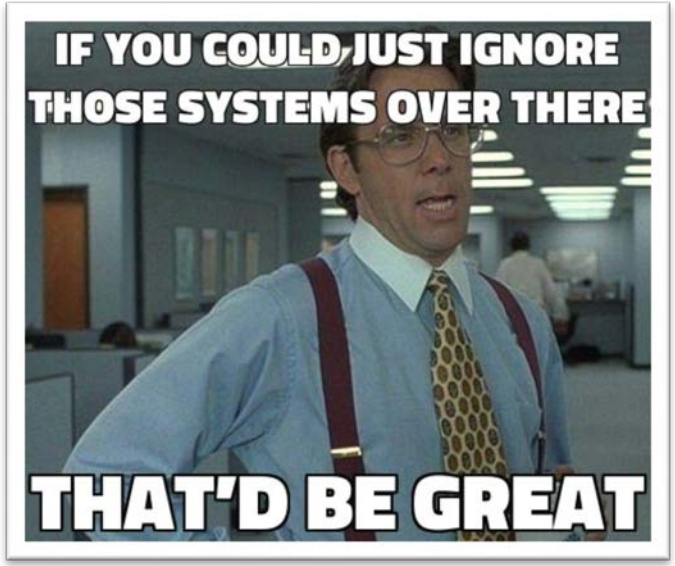
The Problem with High Demand

- The worst case:
  - Vulnerability scans passed off as pentests
    - Exploitability not tested
    - Does not model attacker behavior
    - No correlation to business impact
- Example:
  - Pentest report regurgitates vulnerability scan report results.



The Problem with High Demand

- The compliance case:
  - Scope is so constrained that attack path isn't realistic
    - Does not model attacker behavior
    - May exclude a viable attack path



The Problem with High Demand

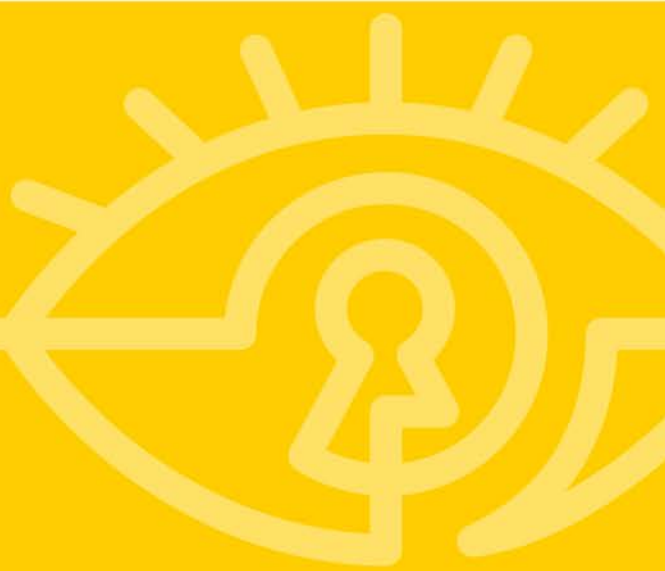
- Example:
  - Our team was contracted to target a sensitive system and see if we could access and exfiltrate PII data.
  - Standard for the assessment type was to start by performing a phishing assessment.
  - Discovered that scope was limited to only those IP addresses associated with the target system and excluded all user workstations.
  - No logical path from our foothold to the target system network within the authorized scope.

The Problem with High Demand

- The typical case:
  - Too narrowly focused on technology instead of business operations
    - Difficult to demonstrate business impact

The Problem with High Demand

- Ultimately, these cases create a negative perception of pentesting as a whole
  - Minimal business value
  - Unjustifiably high-cost
  - Combative relationships
  - Don't live up to potential



The Real Value of a Pentest

The Real Value of a Pentest

- When performed properly, pentesting can provide unparalleled value compared to paper-based risk management practices alone
- Current risk analysis methods are subjective
- Inputs like probability, likelihood, impact, threat actors, etc. are all subject to interpretation
- Making accuracy, consistency, and repeatability difficult

The Real Value of a Pentest

- Additionally, some inputs are volatile by their very nature
  - Likelihood can increase as exploit kits are released and as access and deployment become easier
  - The impact of an attack may differ between the middle and end of a fiscal quarter
  - Threat actors can change rapidly

The Real Value of a Pentest

- Pentesting can add objectivity to risk analysis methods by validating an organization's conclusions about risk
  - Likelihood can be validated based on the complexity of the exploit or attack path
  - Impact can be validated based on the attackers ability to move laterally to high-value assets

The Real Value of a Pentest

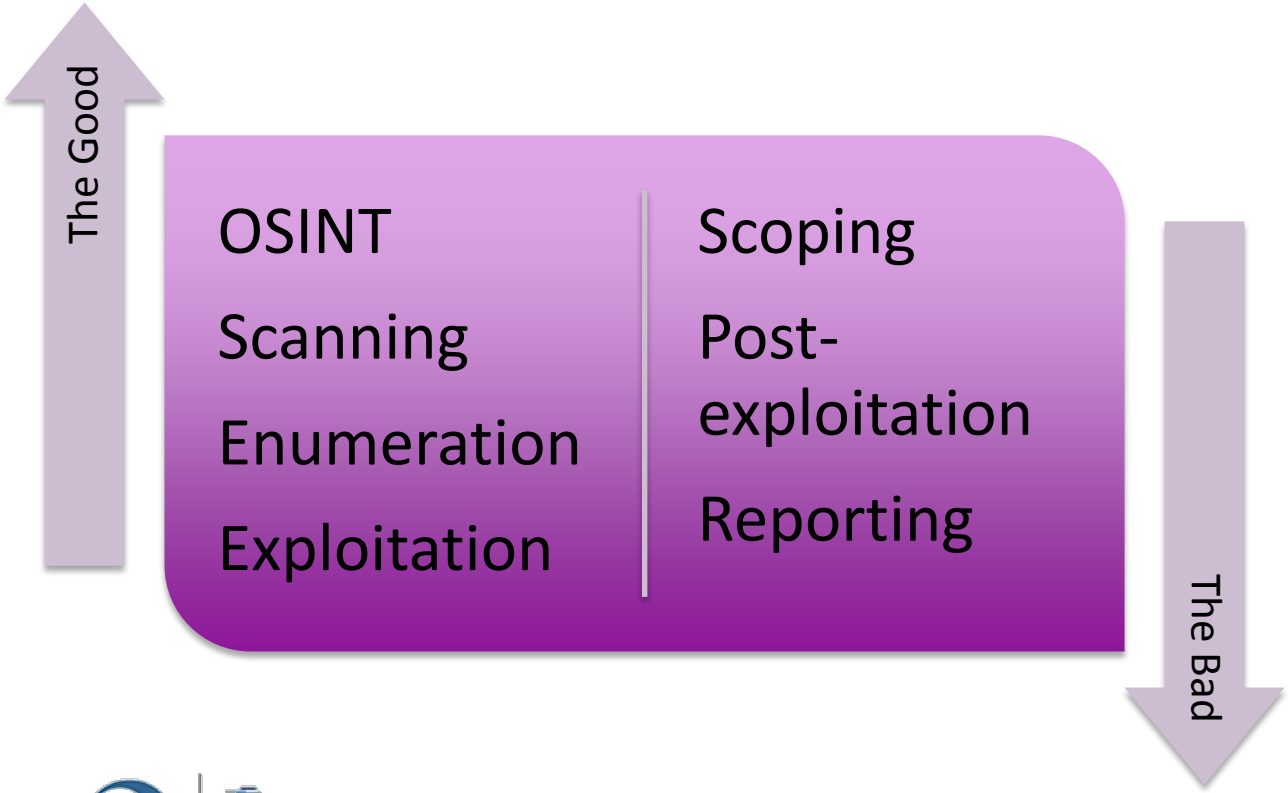
- Ongoing cycles of risk analysis and pentesting can help build discipline and maturity into an organization's risk management program

Bridging the Gap Between Perception and Reality

Bridging the Gap

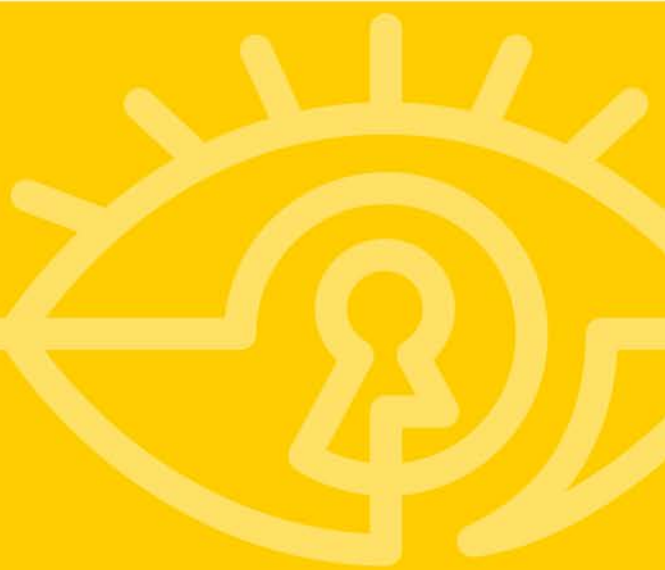
- While the real-world potential value of pentests are high, current standards leave much to be desired.
- As both pentesters and consumers of pentests we need to raise our standards and expectations respectively.
- To do so, we need to carefully consider both the strengths and weaknesses of our pentests and be willing to perform and demand the necessary improvements

Bridging the Gap



Bridging the Gap

- Bottom Line:
  - Pentests require a great deal of technical prowess
  - However, they are also a business service
  - As such, pen-testers need to be just as proficient in their understanding of business, IT, and security operations as they are in their technical abilities.



Goal Oriented Pentesting

Goal Oriented Pentesting

- Often times, pentest goals are poorly defined.
- Ambiguous statements like “hack us”, “phish us”, or “get shell” are not sufficient goals.
  - In these cases, it is difficult to know when the goal is achieved
  - The goal may mean different things to different people

Goal Oriented Pentesting

- Goal Oriented Pentesting is intended to remove this ambiguity by defining goals that are

Goal Oriented Pentesting

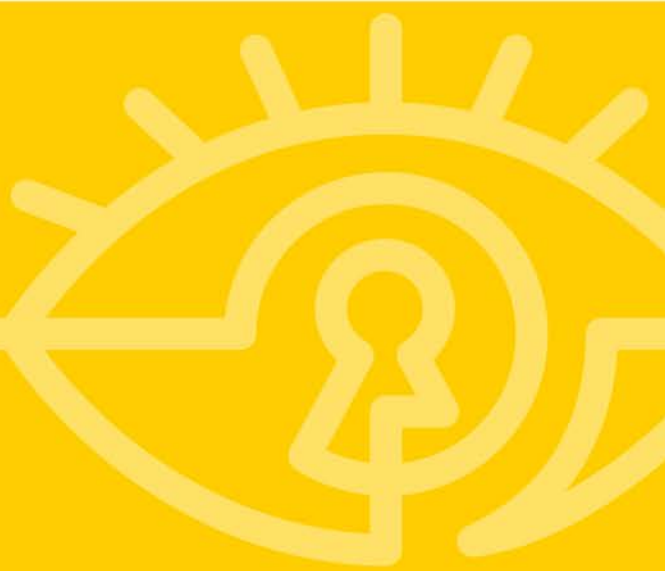
- Examples:
  - Demonstrate the ability to exfiltrate PII from the HRIS via an external network attack within a two-week engagement
  - Compromise domain admin credentials via a 30-day reconnaissance and phishing campaign targeting IT personnel
  - Gain undetected system-level access to the ICS network via a 90-day red team engagement

Goal Oriented Pentesting

- Goals discussions should begin prior to defining scope
- Think about:
  - What do you hope to gain from the pentest?
  - What are your top security concerns?
  - What are your most critical assets?
  - What are the organization's greatest security strengths?

Goal Oriented Pentesting

- Why are goals important?
  - Manages expectations
  - Provides a clear objective for the pentester
  - Can help to align the pentest with risk management objectives



Strategic Lateral Movement

Strategic Lateral Movement

- There is a misconception that a pentester's objective is to find all of the vulnerabilities
- This quantity over quality approach results in a very weak pentest and is an inefficient use of resources
- Quantifying exploitable vulnerabilities is the job of your vulnerability management program, not your pentester

Strategic Lateral Movement

- Instead, the pentester's objective is to find relationships between technical and operational weakness that reveal business risks
- This is accomplished by
  - Understanding business operations
  - Identifying high-value targets
  - Demonstrating the business impact of the compromise

Strategic Lateral Movement

- Understanding business operations
  - Who are their customers?
  - How do they generate revenue?
  - What do their investors value?
- Much of this information can be obtained through their website, annual reports, and market analysts.

Strategic Lateral Movement

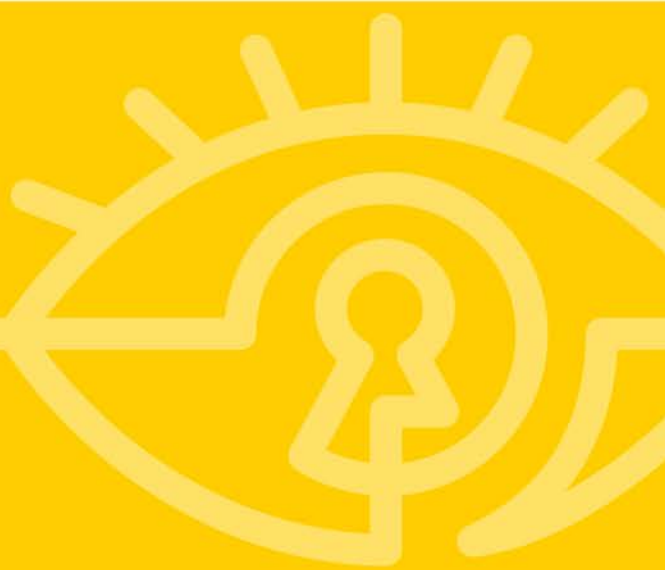
- Identifying high-value targets
  - Based on your new understanding of the business, what systems or functions are critical to their operations?
  - Where would a data exfiltration have the most impact?
  - Do they have data with high-integrity requirements?
  - How would a disruption of certain functions impact their business

Strategic Lateral Movement

- Demonstrating business impact
  - Loss of revenue is not the only motivator
    - Safety
    - Productivity
    - Production Capacity
    - Privacy
    - SEO

Strategic Lateral Movement

- Gaining shell, root, or even domain admin credentials is not the end of a pentest.
- This level of access is only the beginning of where business impact is identified

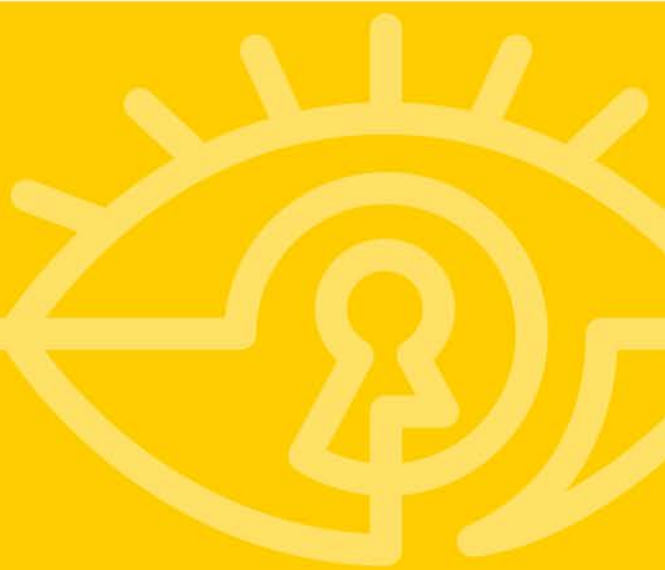


Case Study #1

Goal Oriented Pentesting and Strategic Lateral Movement

Case Study #1

- Contracted to perform both a resilience assessment and a penetration test for a customer.
- Prior to the assessments the customer identified their critical assets and top concerns which were based on their industry and the location of their operations.
  - Access to Industrial Control Systems
  - Resilience of Field Communications
  - Hacktivists
  - Phishing Attacks
- Our customer was able make informed decisions regarding its security dollars and resources because we:
  - Focused on Applicable Scenarios
  - Simulated Identified Threat Actors, and
  - Tailored Our Objectives



Focus Less on Technology

Focus Less on Technology

- While pen-tests are technical by nature, most technical findings are merely symptoms of deficiencies in broader operational controls.
- Often times however, pen-testers focus so heavily on the technical details that their recommendations are nothing more than band-aide solutions that fail to address the operational root cause of the technical finding.

Focus Less on Technology

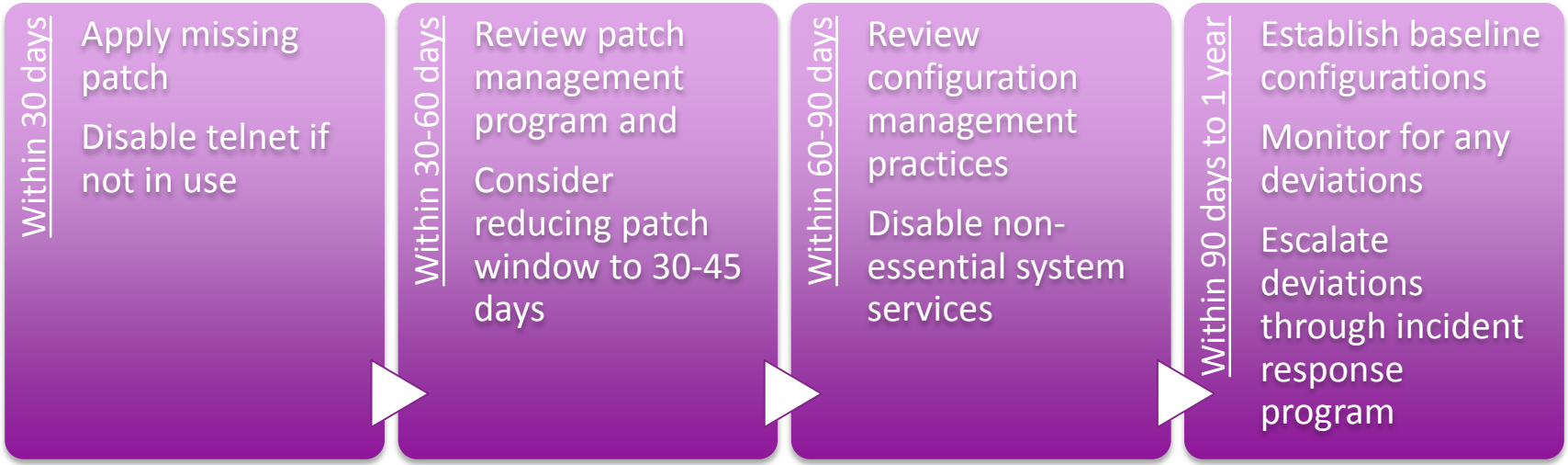
- Let's say that a pen-tester takes advantage of an SSH vulnerability on a system accepting both telnet and SSH connections. The patch for the SSH vulnerability was released over two months ago
- In this case, a typical pentester recommendation would be:
  - Apply the missing SSH patch
  - Disable telnet if not in use

Focus Less on Technology

- The problem here is that this approach does not address the root cause of the finding
  - Why is a there two-month old exploitable vulnerability?
  - Why are both telnet and ssh enable?
- The recommendation only addresses this one system
- However, chances are high that similar conditions are present on other systems.

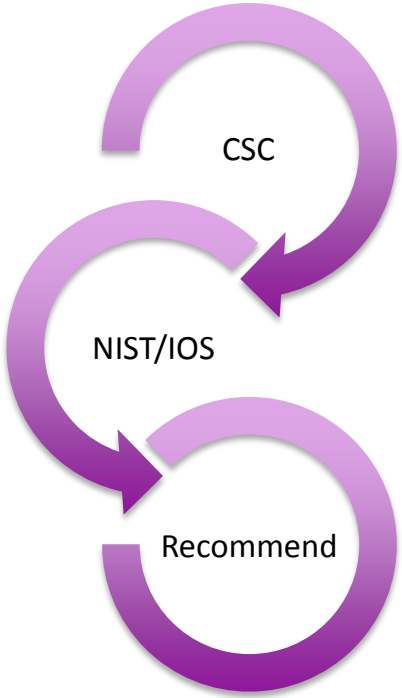
Focus Less on Technology

- A better approach:



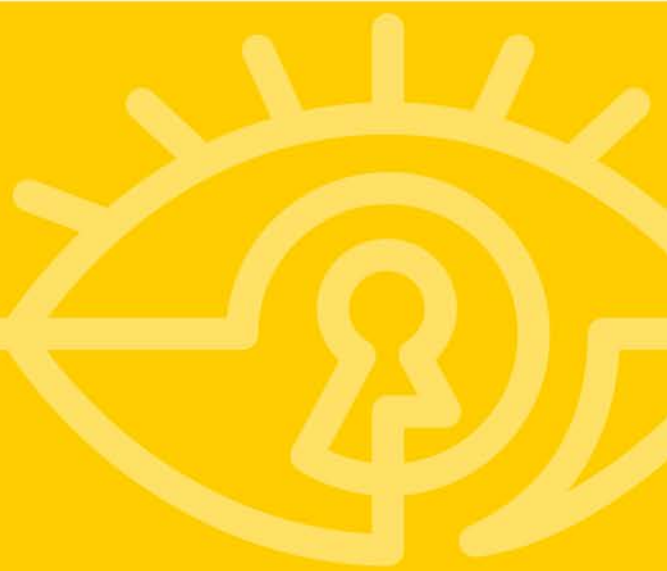
Focus Less on Technology

- Where to get started
  - Critical Controls for Effective Cyber Defense are 100% Technical
  - NIST 800-53 and ISO 20772 are more management and operational
  - Leverage mappings to correlate CSC with NIST/ISO to make related operational and management recommendations



Focus Less on Technology

- Benefits of this approach:
  - Addresses the finding beyond the superficial patch/config fix
  - Addresses potentially unidentified vulnerabilities
  - Provides a remediation roadmap
  - Identifies preventative, detective, and response controls



Understand the Audience

Understand the Audience

- A single pentest report has multiple audiences that include
  - Executives
  - Managers
  - Technical staff
- Each of these audiences has different needs which should be addressed accordingly
- However, many pentest reports read as if the audience were other pentesters

Understand the Audience

- The good news, is that many pentest reports are structured properly, the content and language just need to be tuned to the appropriate audience.

Executive Summary

Main Body

Appendices

Understand the Audience

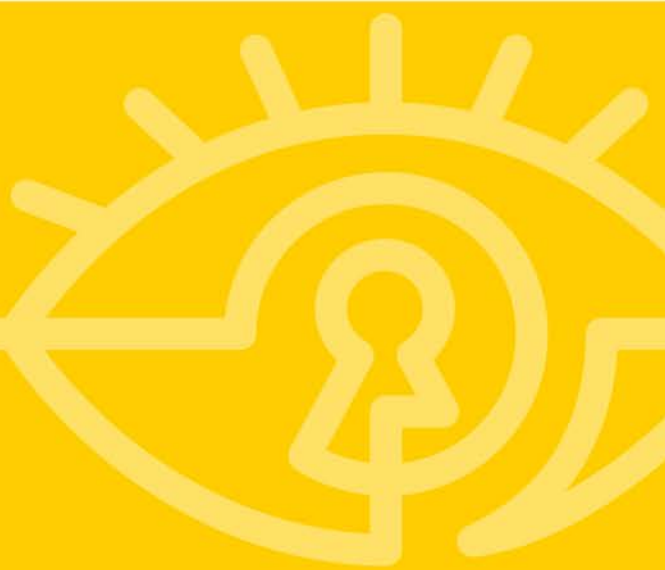
- Executive Summary
  - Audience: Executives
  - Concerns: Business impact & remediation strategy
- Approach
  - Express business impact using appropriate terminology
  - Relate findings to the goals of the pentest
  - Recommendations should be strategic (i.e. programs not systems)

Understand the Audience

- Main Body
  - Audience: Management (often managers of technical staff)
  - Concerns: Remediation measures
- Approach
  - Summarize technical findings (ID, title, severity)
  - Provide a time-bound remediation roadmap
    - Critical findings, quick-win operational findings, long-term sustainable programs

Understand the Audience

- Appendices
  - Audience: Technical Staff
  - Concerns: Technical findings and fixes
- Approach
  - Provide a detailed attack narrative
  - Provide detailed findings
    - Be carful to tailor severity, description, and recommendations appropriately

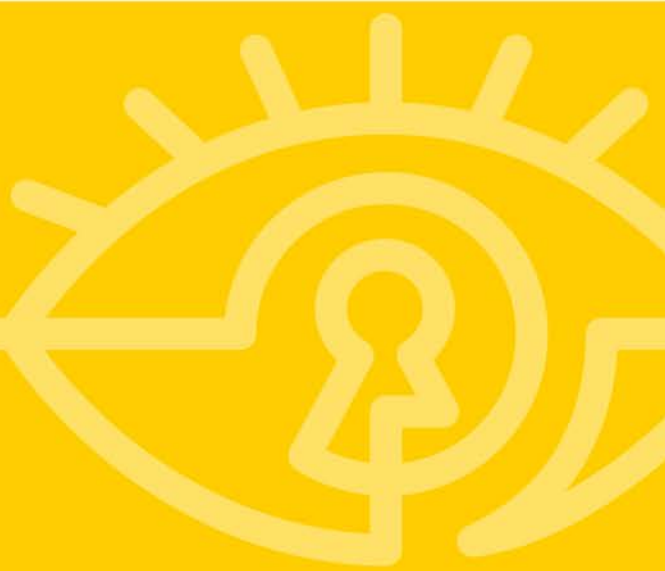


Case Study #2

Focusing Less on Technology and Understanding Your Audience

Case Study #2

- Was tasked with directing remediation efforts following a pentest
- The pentest report was barely usable
  - Provided no sense of conclusion on overall security posture
  - Was both too detailed and not detailed enough
  - Provided no prioritization other then severity ratings
- Had to perform our own analysis and conclusions
  - Root cause analysis
  - Prioritization
  - Framing of the results
- All the pentester provided was data; we had to turn it in to information



Applications

As a Pentester

- Engage you clients upfront regarding their expectations surrounding the pentest
- Instead of focusing your reconnaissance efforts on personnel and technology, begin gathering information on the business as a whole
- Target assets that contribute to the organization's mission
- Focus your reporting more on root-causes rather than quick fixes

As a Consumer of Pentests

- Review your last few pentest reports and ask yourself
  - What was the goal of this pentest and was in understood by all parties?
  - How do the results of the pentest relate to your organization's mission?
  - Were you left with a clear understanding of how to address the root-cause of the findings across your organization?
- Consider addressing these shortcomings for your next pentest