Reporting

Contents

Overview

This document is intended to define the base criteria for penetration testing reporting. While it is highly encouraged to use your own customized and branded format, the following should provide a high level understanding of the items required within a report as well as a structure for the report to provide value to the reader.

Report Structure

The report is broken down into two (2) major sections in order to communicate the objectives, methods, and results of the testing conducted to various audiences.

The Executive Summary

This section will communicate to the reader the specific goals of the Penetration Test and the high level findings of the testing exercise. The intended audience will be those who are in charge of the oversight and strategic vision of the security program as well as any members of the organization which may be impacted by the identified/confirmed threats. The executive summary should contain most if not all of the following sections:

Background:

The background section should explain to the reader the overall purpose of the test. Details on the terms identified within the Pre Engagement section relating to risk, countermeasures, and testing goals should be present to connect the reader to the overall test objectives and the relative results.

(Example: (CLIENT) tasked <Pentester> with performing an internal/external vulnerability assessment and penetration testing of specific systems located in (logical area or physical location). These systems have been identified as (risk ranking) and contain (data classification level) data which, if accessed inappropriately, could cause material harm to (Client). In an effort to test (CLIENT's) ability to defend against direct and indirect attack, <Pentester> executed a comprehensive network vulnerability scan, Vulnerability conformation(<-insert attack types agreed upon->) exploitation of weakened services, client side attacks, browser side attacks (etc) The purpose of this assessment was to verify the effectiveness of the security controls put in place by (CLIENT) to secure business-critical information. This report represents the findings from the assessment and the associated remediation recommendations to help CLIENT strengthen its security posture.

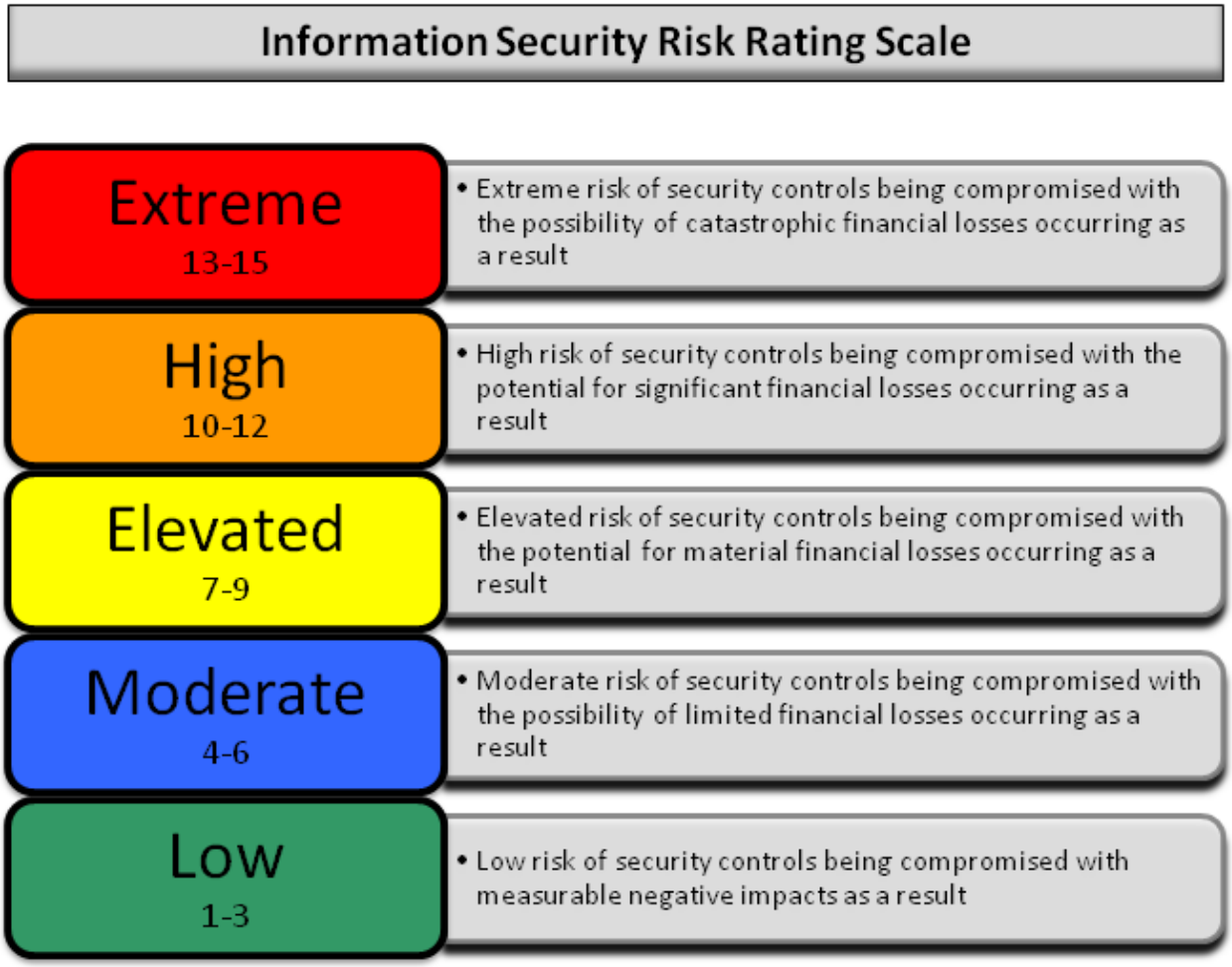
- If objectives were changed during the course of the testing then all changes must be listed in this section of the report. Additionally, the letter of amendment should be included in the appendix of the report and linked to from this section.

Overall Posture:

This area will be a narrative of the overall effectiveness of the test and the pentesters ability to achieve the goals set forth within the pre engagement sessions. A brief description of the Systemic (ex. Systemic issue= Lacking Effective Patch Management Process vs. Symptomatic= Found MS08-067 missing on xyz box) issues identified through the testing process as well as the ability to achieve access to the goal information and identify a potential impact to the business.

Risk Ranking/Profile:

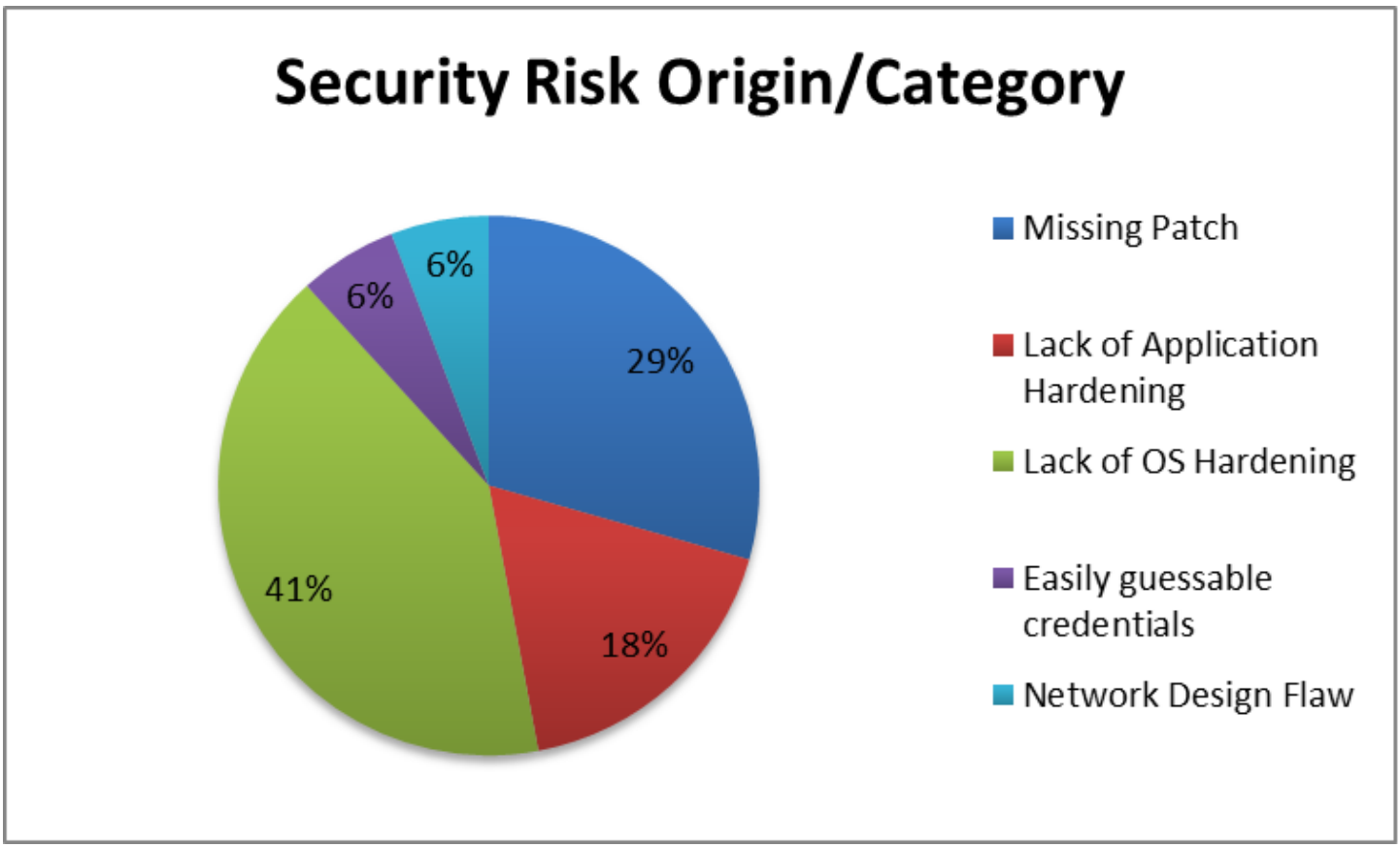
The overall risk ranking/profile/score will be identified and explained in this area. In the pre engagement section the Pentester will identify the scoring mechanism and the individual mechanism for tracking/grading risk. Various methods from FAIR, DREAD, and other custom rankings will be consolidated into environmental scores and defined.



The "Overall Risk Score" for the (CLIENT) is currently a Seven (7). This rating implies an ELEVATED risk of security controls being compromised with the potential for material financial losses. The consultant determined this risk score based on one high risk and several medium risk vulnerabilities, along with the success of directed attack. The most severe vulnerability identified was the presence of default passwords in the corporate public facing website which allowed access to a number of sensitive documents and the ability to control content on the device. This vulnerability could lead to theft of user accounts, leakage of sensitive information, or full system compromise. Several lesser severe vulnerabilities could lead to theft of valid account credentials and leakage of information.

General Findings:

The general findings will provide a synopsis of the issues found during the penetration test in a basic and statistical format. Graphic representations of the targets tested, testing results, processes, attack scenarios, success rates, and other trendable metrics as defined within the pre engagement meeting should be present. In addition, the cause of the issues should be presented in an easy to read format. (ex. A graph showing the root cause of issues exploited)



If defined within the Pre engagement exercise, this area should also include metrics which depict the effectiveness of the countermeasures within the environment. (ex.. we ran x attacks and IPS blocked y. Other countermeasures should also have similar metrics of design vs. effectiveness.)

Recommendation Summary:

The recommendation section of the report should provide the reader with a high level understanding of the tasks needed to resolve the risks identified and the general level of effort required to implement the resolution path suggested. This section will also identify the weighting mechanisms used to prioritize the order of the road map following.

Strategic Roadmap:

Roadmaps should include a prioritized plan for remediation of the insecure items found and should be weighed against the business objectives/ level of potential impact. This section should map directly to the goals identified as well as the threat matrix created in the PTES-Threat modeling section. By breaking up into predefined time/objective based goals, this section will create a path of action to follow in various increments. Example:

Completed at the time of this assessment
Tasks
Identify internal security point of contact • Identify current resources to dedicate the task of resolving security concerns within the environment. The remediation process should be owned and supported by senior staff in order to effectively manage its completion. • Secure appropriate funding for initial program review and 3rd party assessment
Identify Current Security State of security • This task will be performed at an executive level. CLIENT will identify the proper ownership and executive support channel to champion this effort. In addition, CLIENT will need to take inventory of the "Security Management Chain of Command", Policy, Procedure, and Compliance tracking sophistication.

One (1) to Three (3) Months
Tasks
Create Remediation Strategy • Leverage results found within the Penetration Test to create a full remediation strategy • This assessment report will provide the basis for this action. It must now be formalized and approved by the CLIENT Security Team.
Create Information Security Council/Task Force • To gain better traction in the remediation and security onboarding process, CLIENT should create a specific ISEC council to aid in remediation and adequately involve each individual team. • The council should consist of Management of each individual business unit • ….
Begin Security Project planning • Assign Executive owners of security for CLIENT • …
Prioritize Remediation Events • Leverage results found within Penetration Test to gain understanding of the tasks needed to be performed in order to resolve the risks identified. • Assign priority listing to remediation tasks that will provide the highest level of impact and largest reduction of identified risk. • Start process with server patching to gain quick increases in environment security.
Patch Services • **Specific things to be fixed/how…** • …
Harden Servers • … • …

Three (3) to Twelve (12) Months
Tasks
Security Self Assessment Adequate security of information and the systems that process it is a fundamental management responsibility. CLIENT officials must understand the current status of their information security program and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level. Self-assessments provide a method for CLIENT officials to determine the current status of their information security programs and, where necessary, establish a target for improvement. A good guide for this is **NIST SP 800-53a**: found at http://csrc.nist.gov/publications/PubsDrafts.html. Another approach would be to run the **Microsoft Security Assessment Tool** : found at http://www.microsoft.com/technet/security/tools/msat/default.mspx
Twelve (12) Months+
Tasks
Perform 3rd Party Assessment of Information Security and Compliance with 27001/2 (or any other compliance control set chosen). • Perform a Corporate wide assessment of CLIENT's ability to defend against targeted & generic attacks • Identify the root cause of compliance gaps • Identify strategy for using the output of the assessment to facilitate a security baseline Begin remediation planning/budgeting

Technical Report

This section will communicate to the reader the technical details of the test and all of the aspects/components agreed upon as key success indicators within the pre engagement exercise. The technical report section will describe in detail the scope, information, attack path, impact and remediation suggestions of the test.

Introduction:

The introduction section of the technical report is intended to be an initial inventory of:

- Personnel involved in the testing from both the Client and Penetration Testing Team
- Contact information
- Assets involved in testing
- Objectives of Test
- Scope of Test
- Strength of Test
- Approach
- Threat/Grading Structure

This section should be a reference for the specific resources involved in the testing and the overall technical scope of the test.

Information Gathering:

Intelligence gathering and information assessment are the foundations of a good penetration test. The more informed the tester is about the environment, the better the results of the test will be. In this section, a number of items should be written up to show the CLIENT the extent of public and private information available through the execution of the Intelligence gathering phase of PTES. At a minimum, the results identified should be presented in 4 basic categories:

Passive Intelligence:

Intelligence gathered from indirect analysis such as DNS,Google dorking for IP/infrastructure related information. This section will focus on the techniques used to profile the technology in the CLIENT environment WITHOUT sending any traffic directly to the assets.

Active Intelligence:

This section will show the methods and results of tasks such as infrastructure mapping, port scanning, and architecture assessment and other foot printing activities. This section will focus on the techniques used to profile the technology in the CLIENT environment by sending traffic DIRECTLY to the assets.

Corporate Intelligence:

Information about the structure of the organization, business units, market share, vertical, and other corporate functions should be mapped to both business process and the previously identified physical assets being tested.

Personnel Intelligence:

Any and all information found during the intelligence collection phase which maps users to the CLIENT organization. This section should show the techniques used to harvest intelligence such as public/private employee depots, mail repositories, org charts and other items leading to the connection of employee/company.

Vulnerability Assessment:

Vulnerability assessment is the act of identifying the POTENTIAL vulnerabilities which exist in a TEST and the threat classification of each threat. In this section, a definition of the methods used to identify the vulnerability as well as the evidence/classification of the vulnerability should be present. In addition this section should include:

- Vulnerability Classification Levels
- Technical Vulnerabilities

    - OSI Layer Vulns
    - Scanner Found
    - Manually identified
    - Overall Exposure
- Logical Vulnerabilities
    - NON OSI Vuln
    - Type of vuln
    - How/Where it is found
    - Exposure
- Summary of Results

Exploitation/ Vulnerability Confirmation:

Exploitation or Vulnerability confirmation is the act of triggering the vulnerabilities identified in the previous sections to gain a specified level of access to the target asset. This section should review, in detail, all of the steps taken to confirm the defined vulnerability as well as the following:

- Exploitation Timeline
- Targets selected for Exploitation
- Exploitation Activities
    - Directed Attack
        - Target Hosts unable to be Exploited
        - Target Hosts able to be Exploited
            - Individual Host Information
            - Attacks conducted
            - Attacks Successful
            - Level of access Granted +escalation path
            - Remediation
                - Link to Vuln section reference
                - Additional Mitigating technique
                - Compensating control suggestion
- Indirect Attack
    - Phishing
        - Timeline/details of attack
        - Targets identified
        - Success/Fail ratio
        - Level of access granted
    - Clientside
        - Timeline/details of attack
        - Targets identified
        - Success/Fail ratio
        - Level of access granted
    - Browser Side
        - Timeline/details of attack
        - Targets identified
        - Success/Fail ratio
        - Level of access granted

Post Exploitation:

One of the most critical items in all testing is the connection to ACTUAL impact on the CLIENT being tested. While the sections above relay the technical nature of the vulnerability and the ability to successfully take advantage of the flaw, the Post Exploitation section should tie the ability of exploitation to the actual risk to the business. In this area the following items should be evidenced through the use of screenshots, rich content retrieval, and examples of real world privileged user access:

- Privilege Escalation path
  - Technique used
- Acquisition of Critical Information Defined by client
- Value of information
- Access to core business systems
- Access to compliance protected data sets
- Additional Information/Systems Accessed
- Ability of persistence
- Ability for exfiltration
- Countermeasure Effectiveness

    This section should cover the effectiveness of countermeasures that are in place on the systems in scope. It should include sections on both active (proactive) and passive (reactive) countermeasures, as well as detailed information on any incident response activities triggered during the testing phase. A listing of countermeasures that were effective in resisting assessment activities will help the CLIENT better tune detection systems and processes to handle future intrusion attempts.

  - Detection Capability
    - FW/WAF/IDS/IPS
    - Human
    - DLP
    - Log
  - Response & effectiveness

Risk/Exposure:

Once the direct impact to the business is qualified through the evidence existing in the vulnerability, exploitation and post exploitation sections, the risk quantification can be conducted. In this section the results above are combined with the risk values, information criticality, corporate valuation, and derived business impact from the pre engagement section. This will give the CLIENT the ability to identify, visualize and monetize the vulnerabilities found throughout the testing and effectively weight their resolution against the CLIENTS business objectives. This section will cover the business risk in the following subsections:

- Evaluate incident frequency
  - probable event frequency
  - estimate threat capability (from 3 - threat modeling)
  - Estimate controls strength (6)
  - Compound vulnerability (5)
  - Level of skill required
  - Level of access required
- Estimate loss magnitude per incident
  - Primary loss
  - Secondary loss

    - Identify risk root cause analysis
        - Root Cause is never a patch
        - Identify Failed Processes
- Derive Risk
    - Threat
    - Vulnerability
    - Overlap

Conclusion:

Final overview of the test. It is suggested that this section echo portions of the overall test as well as support the growth of the CLIENT security posture. It should end on a positive note with the support and guidance to enable progress in the security program and a regimen of testing/security activity in the future to come.
