Penetration Test Reporting[€]

An Attempt To Simplify The Process

By

A'mmer Almadani

mad_dev@linuxmail.org

PENBANG

WEARING A WHITE HAT IS A CHOICE

€ The content is subject to change as newer versions are released. Check http://penbang.sysbase.org/pen_test_report/ for the latest version

Disclosure[1]:

The disclosure is an integral part of your report; legality and legitimacy of your conduct must be documented before any information retaining the test is released. It is important to familiarize yourself with legal terms, especially if opting for a Grey[2] test. In case of a White[3] test, simply mention that you were contacted to conduct a vulnerability assessment by X company/individual on their system/systems[4].

Proposed Structure of The Disclosure

- Name the rules of conduct[5]
- Specify the IP address you used[6]
- State the duration of the test.
  - If the employer demanded a time frame, state it as a goal
  - If the employer did not specify a time frame to abide by, state the time it took you/attacker to accomplish the goal/goals
- Specify the type of test[7]; Internal/External
  - Network Service Test
  - Client-Side Test
  - Web Application Test
  - Wireless Security Test
  - Social Engineering Test
- Set Goals; they could be set by the employer
  - What will the attacker achieve
- State that you delivered all drives used in the process[8]
- If the disclosure is for a Grey test, append a statement of altruism[9]

Summary:

This is what matters from a managerial standpoint.

Proposed Structure of The Summary

- Define all technical terms
- Explain what was concluded
  - Briefly mention the method of attack and its result
  - Highlight the scope[10] and why was it chosen
- Do not add sensitive information here. If such information is necessary, redact them in all versions except in the document securely delivered to the PERSON in charge. In case it is a Grey report, avoid adding them.

1 Disclosure: The report disclosure; it should not be confused with the Non-Disclosure Agreement(NDA).
2 Grey: When a test is conducted without prior consent, yet the goal is altruistic.
3 White: When a test is conducted with prior consent; if you were hired.
4 Based on the assumption that you have proof of ownership.
5 For example: No DDOS Attack or entry point must be through the web service
6 If using a static IP address. If the test was conducted using various proxies, state the use of proxies.
7 The list is not conclusive. Retrieved from http://www.pen-tests.com/types-of-penetration-tests.html
8 Some clients prefer that debugged data, sensitive information, and the drive used to conduct the assessment be delivered with the report. If such a client is encountered, state the delivery accompanied with a reference to the signed receipt; a document signed by the client stating the they have received the drive.
9 Justify your reasons; pragmatism is preferable
10 Scope: Your entry point/points. There could be several independent entry points i.e. SSH Brute-Forcing and a Web Application Vulnerability at the same time. If you were successful at all of them, "Divide and Summarize"

Body:

This is usually the most hindering part of being a pen-tester[11]. The reason resides in documenting the process while it is in action. The body of the report should be meticulous and straightforward. Here you are free to dive into technical linguistics, seeing as how it will probably be read by the head of the IT department. However, adding footnotes with definitions is a notable effort. The body contains everything you did to reach your final risk statement.

Proposed Structure of The Body

- Divide the body into sections according to the scope
- Name the vulnerability and laconically describe the process
- If the attack leads to another, in the same scope; categorize the section
  - This includes server access and root access
- Using screen-shots may help in explaining the process
- Reference all scripts, programs, and exploits
- Use the "Step-By-Step" method
- For each attack
  - Why – Why did you choose this entry point
  - How – How did you exploit it
  - What – What did you achieve

Conclusion:

Proposed Structure of The Conclusion

- State the goals
- State whether or not the goals were met
- State how the goals were met

Assessment & Risk Statement:

Proposed Structure of The Assessment & Risk Statement

- List appropriate recommendations based on your findings[12]
- Define your recommendations[13]
- State your personal opinion as the final risk assessment statement[14]

11 pen-tester: Penetration Tester
12 Listing the recommendations should not include the explanations
13 If you recommended stricter accessibility, explain how to achieve it
14 The statement by which the client should act upon

Additional Notes:

- Append any changes you made to the client's system
- Detail the exploits you used and vulnerabilities you discovered
- Choose an appropriate `Font`[15]
- Avoid copy-and-paste; if you must, read through it first[16]
- Third-Person language
- Add a signature of some sorts to authenticate the report[17]
- There should be at least 3 drafts before the final report

Addendum:

This guide is not conclusive nor should it be heeded as the industry standard or relied upon to the extent of fulfillment.

TODO:

1. Define the Summary
2. Define the Conclusion
3. Define the Assessment & Risk Statement
4. Append an example

15 Social-Engineering

16 You will encounter many similar occurrences where the same exploit is successful; copying-and-pasting sections from another report is understandable. However, mentioning wrong company-specific information is not acceptable by any standard

17 Not necessary. However, adding it will authenticate the report and imply a professional attitude