Penetration Test Report Review Assignment

Threats and Countermeasures — Released: 22Feb2025
COMP-5830/-6830 — Due: 03Mar2025at 11:30 CT

This project must be completed individually

For this assignment, you are required to review the provided test report and provide feedback to the original customer on its contents. In this scenario, the customer has contracted a separate entity to conduct a surface-level penetration test of their network, received their report, was unsure as to its veracity, and has now contracted you to evaluate the report itself. You are expected to read/analyze the provided report (separate doc) and use the available network (OVA provided) to both A) confirm/refute assertions made by the report's author and B) provided feedback to the customer on the report overall. You **are not** expected to conduct an independent penetration test of the customer's network but **you are** expected to perform many of the associated actions with penetration tests to evaluate the report's contents.

While you are provided a single OVA, it is configured to have *multiple IP addresses* as would be found on a realistic network. You should treat each IP **as a separate device** on the customer's network. While it would be more accurate to package as multiple OVAs, the network is packaged as a single VM in order to greatly reduce the resource requirements and potential for unintended behavior caused by virtualisation.

Scope and Allowed-Actions

This assignment is explicitly scoped to the target network contained in the provided OVA. Due to its construction and use of local VMs, it is highly unlikely that any out-of-scope network/device will be negatively impacted **when the correct local configuration is present**. This configuration is identical to that which we have used in-class to interact with VM in that both the provided OVA and your Kali VM are only using **Internal Network** virtual NICs. While a set of explicitly in-scope actions are listed below, they *are not an all-inclusive enumeration* and only meant to give you a very good "feel" for what the bounds of the engagement are. If you have questions about whether an action is allowed or not, you should contact Dr. Springall **before you perform that action** for clarification either in-person (3101H Shelby Center) or remotely (334-844-6660).

Explicitly In-Scope Actions:

- Reasonable-rate scanning/enumeration/interrogation of devices
- Reasonable-rate scanning/enumeration/interrogation of available services
- Reasonable-rate online/brute-force password guessing
- Arbitrary and in-depth exploration, evaluation, and testing of any network service, network endpoints, etc.
- Modifying or attempting to modify files or process on the target network's devices

It should be noted that any excessive-rate action is likely to result in unintended, non-deterministic, and/or unexplainable behavior due to congestion of the virtual network and/or resource competition. In order to avoid this, ensure that all actions (scans, enumerations, brute-force interrogation, etc.) are limited to a reasonable-rate, repeatable, and their results are explainable.

Broken VMs and Getting Help

You are being provided a pre-configured OVA representing the customer's network in its entirety. If there is concern that an action may have significantly altered or damaged ("bricked") a device of interest, you can delete the currently-used VM and re-import the OVA to revert to its initial state. Dr. Springall is available to answer questions and assist in advanced troubleshooting either in-person (3101H Shelby Center, before/during/after lecture) or via phone (334-844-6660).

Submission Details

In order to ensure your sufficient understanding of the target network and analyzed of the provided report, you will submit a Canvas Quiz with answers to specific questions for a grade. While you will only have **one (1) attempt** at this Canvas Quiz, all questions contained in it are listed below*. Each question will be short-answer and you can respond in either a small number of sentences (order 1–5) or a small number of bullet points. It is *highly recommended* that you construct your answers in a local file (e.g., a `.txt`) and then copy-paste your responses into Canvas. The use of "rich-text" elements (e.g., bold, underline, images, etc.) is not forbidden but it should be noted that A) it is not required and B) it creates the opportunity for unexpected presentation when grading.

Canvas Quiz Questions

1. Evaluate the report's coverage. Did you locate any devices that were not discussed in the report? Did the report discuss any devices that you were not able to locate?
2. How would you rate the Executive Summary portion? Does it sufficiently describe the rest of the report's contents? Is it targeted to the correct audience?
3. How useful is the Methodology portion? Does it describe the process that was take to a sufficient degree? Are there any elements which should have been included or excluded?
4. With regard to the findings/assessment of Server 1 (192.168.66.5), what elements were you able to confirm as accurate?
5. With regard to the findings/assessment of Server 1 (192.168.66.5), what elements were you able to refute as inaccurate?
6. With regard to the findings/assessment of Server 1 (192.168.66.5), what elements were you able unable to confirm or refute?
7. With regard to the findings/assessment of Server 1 (192.168.66.5), were you able to locate any services which are omitted?
8. With regard to the "Risks" portion of Server 1 (192.168.66.5), is this an accurate characterization of the dangers posed by the vulnerabilities?
9. With regard to the "Recommendations" portion of Server 1 (192.168.66.5), are they actionable? If so, are they sufficient to mitigate those risks?
10. With regard to the findings/assessment of Server 2 (192.168.66.119), what elements were you able to confirm as accurate?
11. With regard to the findings/assessment of Server 2 (192.168.66.119), what elements were you able to refute as inaccurate?

*The device-specific questions are identical across all devices listed in the report and separated as answers may or may not differ.

12. With regard to the findings/assessment of Server 2 (192.168.66.119), what elements were you able unable to confirm or refute?
13. With regard to the findings/assessment of Server 2 (192.168.66.119), were you able to locate any services which are omitted?
14. With regard to the "Risks" portion of Server 2 (192.168.66.119), is this an accurate characterization of the dangers posed by the vulnerabilities?
15. With regard to the "Recommendations" portion of Server 2 (192.168.66.119), are they actionable? If so, are they sufficient to mitigate those risks?
16. With regard to the findings/assessment of Server 3 (192.168.66.254), what elements were you able to confirm as accurate?
17. With regard to the findings/assessment of Server 3 (192.168.66.254), what elements were you able to refute as inaccurate?
18. With regard to the findings/assessment of Server 3 (192.168.66.254), what elements were you able unable to confirm or refute?
19. With regard to the findings/assessment of Server 3 (192.168.66.254), were you able to locate any services which are omitted?
20. With regard to the "Risks" portion of Server 3 (192.168.66.254), is this an accurate characterization of the dangers posed by the vulnerabilities?
21. With regard to the "Recommendations" portion of Server 3 (192.168.66.254), are they actionable? If so, are they sufficient to mitigate those risks?
22. Overall, how would you rate the *structure* and *presentation* of the provided report and why? This includes not only the information presented/omitted but also the way in which that information is provided to the customer.
23. Overall, how would you rate the *usefulness* of this report to the customer?
24. What advice would you give to the report's author on improving the structure/presentation of future reports?
25. If asked, would you recommend the customer retain the same penetration testing organization for future engagements or search for a different provider? Why?

VM Disk Crypto Key

`qi4oaMDEjYZpgqza2uLQSS5U`

ERRATA

- 26Feb2025: Correct server #s in questions (IPs unchanged and remain correct)