Midterm Assignment

Threats and Countermeasures — Released: 01Mar2025
COMP-5830/-6830 — Due: 08Mar2025at 11:59pm CT

This project must be completed individually

For your midterm, you will demonstrate your ability to conduct the initial stages of a penetration test against a target network and communicate the results of that test with the customer. In this scenario, the customer has contracted you to perform this test independently and without the cooperation of the customer's IT department. Using the MITRE ATT&CK framework, you are expected to evaluate the customer's network with a primary focus on its security-related aspects and then write a short (3–5 page) report to submit to your customer as a work-product. In addition to serving as a description of the network's state (including documentation of any weaknesses/vulnerabilities found), this report should also sufficiently communicate the importance of your findings and appropriate suggestions for mitigating/remediating any issues you identify.

You are being provided with three (3) OVAs which collectively constitute the customer's network. Each VM is configured to operate independent of the others and there are no direct dependencies between them (e.g., VM-A does not rely on an API from VM-B to function). The midterm can be completed by either running all three VMs concurrently or incrementally by running/interacting with one at a time.

To be clear, you **are** expected to conduct an independent penetration test of the customer's network and the scenario for this midterm is **entirely independent** from the PenTest Report Review scenario. Additionally, you should expect to encounter services/protocols/applications/etc. which are foreign and unknown to you. This is intentional as it requires you to independently learn and incorporate new information in the context of this assignment. The ideas, concepts, and approaches discussed/demonstrated in-class remain applicable.

Scope and Allowed-Actions

This assignment is explicitly scoped to the target network contained in the provided OVAs. 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 VMs in that both the provided VM 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 and testing of any network service, network endpoints, etc.
- Attempts to inject malicious data into the target devices (SQL-injection, shell-injection, . . .)

- Attempts to exploit known or suspected vulnerabilities
- Attempts to escalate privileges up to and including to `root` access
- 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

As seen previously, you are being provided pre-configured OVAs 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).

Context and Assumptions

OSINT

A portion of your Reconnaissance Phase has already been completed by a co-worker and passed to you on their last day of employment (i.e., are no-longer available to consult). This information is contained in a separate document available via the course website and you **are not** expected to locate any scenario-specific information outside of the provided VMs. This provided OSINT information is expected to aid you in completion of this assignment.

Power-Cycling

You may assume that your customer will power-cycle their devices arbitrarily during your pen-test. If you wish, you may simulate this by powering the devices off/on via either the operating system or VirtualBox's UI. When powering-off via the UI (i.e., clicking "X" on the window), it is recommended that you elect to "Send the Shutdown Signal" which will give the VM to shutdown gracefully and lessen the chances of corruption caused by partial disk-writes.

Console Access

You **may not** assume that you have console access to the customer's network devices. To simulate this, you are **forbidden** from interacting with the VMs via any non-network channel with the exception of powering off/on via the VirtualBox UI as stated above. This *explicitly* prevents you from logging-in to the VM via VirtualBox's UI if you obtain a username/password combination. This **does not** prohibit you from leveraging such username/password combinations in furtherance of your objectives, only forces you to do so via network interaction from your Kali VM.

What is "Enough"

You should assume that each device on the customer's network has at least one weakness that should be discussed in your report. Additionally, you should assume that `root` access can be achieved on each device on the customer's network. Students in the undergrad section are expected to identify and inform the customer of their ability to achieve `root`-access on **at least one (1) device**. Students in the graduate section are expected to identify and inform the customer of their ability to achieve `root`-access on **at least two (2) devices**.

Submission Details & Grading

You will write a 3–5 page PenTest Report to communicate your findings to your customer and submit it as a single PDF document via Canvas. In addition to the technical details contained in it, this report will be graded based on its coverage, presentation, appropriateness, and overall suitability for the given scenario. As discussed in-class, this report is you **communicating with your customer** and not you communicating with your professor/instructor/colleague/friend and should be written as such.

Other than the limitation of 5 pages max, there are no specific requirements related to formatting, structure, or tone and you are free to make those choices as you see fit. You should, however, be aware that your formatting, structure, and tone will impact your grade as these aspects heavily impact both the presentation of and ability to communicate information

Appendices If you wish, you may attach an arbitrary number of clearly-marked appendices to your report as addition pages in the PDF. While these appendices *do not* count towards your 5 page limit, you *may not* assume that they will be read. All information you believe your customer should be explicitly aware of should be contained in the initial 3–5 page PenTest Report and any appendices you choose to include should be done so as ancillary/auxiliary/supplemental information.

VM Disk Crypto Key

`CdHzqD5Eas2UYVEiEYb2y4Fz`

The above disk crypto key is the same for all OVAs provide.

ERRATA

None