**Introduction to Documentation and Reporting**

Strong documentation and reporting skills are incredibly beneficial in any area of Information Technology or Information Security, and mastering these skills can help us quickly progress in our careers. Being highly technical is great and essential, but without soft skills to back up our technical pwning skills, we won't be as effective whether we are writing internal policies and procedures, technical documentation, penetration test reports, or other types of client deliverables.

There is no "one size fits all" for notetaking and preparing reports, but there are fundamental principles that must be followed to be successful. This module will explore different styles from notetaking tools, organizing our evidence on our testing VM, writing up Executive Summaries for non-technical audiences, and documenting Attack Chains and technical findings. We attempted to provide a generic formula that anyone can use to achieve success while sprinkling in tips, tricks, and best practices that we have learned from around 25 combined years in various client-facing technical consulting and managerial roles.

One crucial consideration for us as testers is a penetration test is a snapshot in time of the target network's security status. We should include an overview section in our report that talks about the type of work performed, who performed it, source IP addresses used in testing, and any special considerations (i.e., testing performed remotely over VPN or from a host within the client's network). This overview should also state that our testing was performed during a specific period and that any changes to in-scope systems and resultant vulnerabilities would not be captured in this report deliverable. We could state: "All testing activities were performed between January 7, 2022 and January 19, 2022." We could also add a disclaimer, such as "This report represents a snapshot in time during the aforementioned testing period, and Acme Consulting, LLC cannot attest to the state of any client-owned information assets outside of this testing window."

**Documentation & Reporting in Practice**

You may be thinking "this will be a boring module.", or "how could we possibly make an entire course on this topic?". While documentation and reporting is not the most exciting topic and certainly not as satisfying as pwning a box or getting DA in a lab or real-world network, these are critical skills for anyone in a consulting role. Below are a few examples of times in our careers when neat and thorough documentation and detailed reporting rescued us from what could have escalated into a rather unpleasant situation.

**Scenario 1 - The Case of an Exploding VM**

During one particularly lengthy engagement (a nearly month-long External Penetration Test), I signed on for the day, and my VM would not load up properly. I spent a while trying to recover the file system, but it was completely gone. Luckily I had been taking excellent, detailed project notes using a local copy of OneNote on my base workstation. My team at the time used a shared storage solution for all projects, and we had an automated script to sync our data to share at the end of testing, both for QA and archive purposes. On a tip from a more senior teammate, I had been backing up my testing evidence to this share at the end of every working day. Therefore once I built a new VM (from a template that I kept), all I had to do was sync my project data, and I was back to testing without any interruptions. If I had not been following a defined process, the result could have been catastrophic, losing weeks of work and potentially losing a client for the company or even my job.

**Scenario 2 - Ping of Death**

I knew this one Internal Penetration Test would be difficult starting from the initial scoping call. One member of the client's internal IT team was very hostile and questioned everything, suspicious of the team's skills, and very protective of a set of critical servers (whose IP addresses were not in the scope of testing). During the enumeration phase of testing, I received an email and call from the client asking to stop all testing as we had brought down multiple critical servers that were sensitive to any type of scanning. I produced all log data, scope files, and timestamped raw scan data. The IP addresses of the affected hosts were in my scans, but they were also included in the scope file, which the client had confirmed. In this case, I had done nothing wrong as I was testing the scope I was given (and confirmed) and had not performed any reckless testing activities. There was a lesson learned that I added to my processes, though. After this, I made sure to ask clients for a specific list of any individual IP addresses and host names that should be explicitly excluded from any scans or other testing activity. In this situation, I had strong documentation to back up what activities had been performed, and written confirmation of the in-scope IP address ranges from the client. However, I found an opportunity to refine my processes further and grow as a consultant.

**Scenario 3 - Slow as Molasses**

In this last example, I was performing an Internal Penetration Test onsite at a client's headquarters building, seated in an area of the office where IT staff sat. Seated behind me was a particularly hostile network administrator who had been skeptical of our abilities and tools since the kickoff call, stating that previous penetration tests from other companies had slowed the network down massively due to inexperienced and reckless testers. Less than 20 minutes into testing, this network admin had sent emails to the entire distribution list and came over to my desk telling me that our scans had slowed the network to a halt, and he had blocked our source IP addresses. We then went through an exercise of sharing our scanning output, showing that we had followed best practices and nothing we had done would explain the network slowdown. Another admin, meanwhile, determined that debug mode had been enabled on every network device, which, combined with normal Nmap scans, was enough to overwhelm the devices and cause slowdowns. Once this was disabled, testing proceeded with no issues. In this case, our documentation backed up our actions and forced the customer to investigate further. Had we not had any (or poor) documentation, then the blame could have easily been placed on us, and it could have greatly impacted the client relationship and our reputation.

These stories illustrate the importance of strong documentation. We need to be able to justify our actions and, if asked, be able to produce evidence for the client to attempt to troubleshoot an issue. It is not uncommon for any network issues during a penetration test to be blamed on the tester regardless of whether it is a result of their activities. We want to be in a strong position to cover ourselves and assist our clients. Furthermore, we never want to scramble to re-do testing after losing evidence or ask a client for more time because we were not diligent in our notetaking and organization.

**About this Module**

We've included a sample Obsidian notebook and a sample Internal Penetration Test report (in both MS Word and PDF formats - zip password hackthebox) that can be downloaded from the Resources tab in the top right of this or any other module section. These are great supplementary resources to keep for yourselves but also helpful to have on hand while working through the content.

There are many opportunities in this module to practice the skills being taught, but none of them are mandatory to complete the module. To get the most value out of this module, we recommend (obviously) taking detailed notes and using the tips and tricks to see where there may be holes or inefficiencies in your processes. Once you figure this out, we hope you will find ways to be more productive and reduce the reporting burden because, let's be honest, no one enjoys reporting; we tolerate it as a necessary evil. Once you are done with this module, it is worth practicing these tips on real-world engagements, or, if you're not yet working in a consulting role, practice your documentation and reporting skills against training targets and labs.

We include a pre-configured attack host and a small lab with this module that you can use to simulate an Internal Penetration Test. Take advantage of this and use it to practice as much as you want until you are comfortable identifying all the findings and develop a documentation style that fits your workflow.

Throughout the module you may see us throwing around terms like "an internal" or "an external". In these cases we are referring to an Internal Penetration Test or External Penetration Test, respectively.

We've tried to make this typically dull topic more engaging than usual, so strap in. It's going to be a wild ride down the rabbit hole of documentation and reporting!