**Types of Reports**

Our report structure will differ slightly depending on the assessment we are tasked to perform. In this module, we will mainly focus on an Internal Penetration Test report where the tester achieved Active Directory (AD) domain compromise during an Internal Penetration Test. The report we will work with will demonstrate the typical elements of an Internal Penetration Test report. We will discuss aspects of other reports (such as additional appendices that may be included in an External Penetration Test report). It's not uncommon to see an External Penetration Test report that resulted in internal compromise with an attack chain and other elements we will cover. The main difference in our lab is that we will not include OSINT data/publicly available information such as email addresses, subdomains, credentials in breach dumps, domain registration/ownership data, etc., because we are not testing against an actual company with an internet presence. While there are some veteran players that have staying power like Have I Been Pwned, Shodan, and Intelx, OSINT tools are also generally very fluid, so by the time this course is published, the best tool or resource to collect that information may have changed. Instead, we list some common types of information targeted to assist in a penetration test and leave it to the reader to test and discover which tools or APIs provide the best results. It's always a good idea not to be reliant on any one tool, so run multiple and see what the difference in data is.

* Public DNS and domain ownership records
* Email Addresses
  + You can then use these to check if any have been involved in a breach or use Google Dorks to search for them on sites like Pastebin
* Subdomains
* Third-party vendors
* Similar domains
* Public cloud resources

These types of information gathering are covered in other modules such as [Information Gathering - Web Edition](https://academy.hackthebox.com/course/preview/information-gathering---web-edition), [OSINT: Corporate Recon](https://academy.hackthebox.com/course/preview/osint-corporate-recon), and [Footprinting](https://academy.hackthebox.com/course/preview/footprinting) and are outside the scope of this module.

**Differences Across Assessment Types**

Before walking through the various types of reports available and then digging into the components of a Penetration Test report, let's define a few key assessment types.

**Vulnerability Assessment**

Vulnerability assessments involve running an automated scan of an environment to enumerate vulnerabilities. These can be authenticated or unauthenticated. No exploitation is attempted, but we will often look to validate scanner results so our report may show a client which scanner results are actual issues and which are false positives. Validation may consist of performing an additional check to confirm a vulnerable version is in use or a setting/misconfiguration is in place, but the goal is not to gain a foothold and move laterally/vertically. Some customers will even ask for scan results with no validation.

**Internal vs External**

An external scan is performed from the perspective of an anonymous user on the internet targeting the organization's public systems. An internal scan is conducted from the perspective of a scanner on the internal network and investigates hosts from behind the firewall. This can be done from the perspective of an anonymous user on the corporate user network, emulating a compromised server, or any number of different scenarios. A customer may even ask for an internal scan to be conducted with credentials, which can lead to considerably more scanner findings to sift through but will also produce more accurate and less generic results.

**Report Contents**

These reports typically focus on themes that can be observed in the scan results and highlight the number of vulnerabilities and their severity levels. These scans can produce a LOT of data, so identifying patterns and mapping them to procedural deficiencies is important to prevent the information from becoming overwhelming.

**Penetration Testing**

Penetration testing goes beyond automated scans and can leverage vulnerability scan data to help guide exploitation. Like vulnerability scans, these can be performed from an internal or external perspective. Depending on the type of penetration test (i.e., an evasive test), we may not perform any kind of vulnerability scanning at all.

A penetration test may be performed from various perspectives, such as "black box," where we have no more information than the name of the company during an external or a network connection for an internal, "grey box" where we are given just in-scope IP addresses/CIDR network ranges, or "white box" where we may be given credentials, source code, configurations, and more. Testing can be performed with zero evasion to attempt to uncover as many vulnerabilities as possible, from a hybrid evasive standpoint to test the customer's defenses by starting out evasive and gradually becoming "noisier" to see at what level internal security teams/monitoring tools detect and block us. Typically once we are detected in this type of assessment, the client will ask us to move to non-evasive testing for the remainder of the assessment. This is a great assessment type to recommend to clients with some defenses in place but not a highly mature defensive security posture. It can help to show gaps in their defenses and where they should concentrate efforts on enhancing their detection and prevention rules. For more mature clients, this type of assessment can be a great test of their defenses and internal procedures to ensure that all parties perform their roles properly in the event of an actual attack.

Finally, we may be asked to perform evasive testing throughout the assessment. In this type of assessment, we will try to remain undetected for as long as possible and see what kind of access, if any, we can obtain while working stealthily. This can help to simulate a more advanced attacker. However, this type of assessment is often limited by time constraints that are not in place for a real-world attacker. A client may also opt for a longer-term adversary simulation that may occur over multiple months, with few company staff aware of the assessment and few or no client staff knowing the exact start day/time of the assessment. This assessment type is well-suited for more security mature organizations and requires a bit of a different skill set than a traditional network/application penetration tester.

**Internal vs External**

Similar to vulnerability scanning perspectives, external penetration testing will typically be conducted from the perspective of an anonymous attacker on the internet. It may leverage OSINT data/publicly available information to attempt to gain access to sensitive data via applications or the internal network by attacking internet-facing hosts. Internal penetration testing may be conducted as an anonymous user on the internal network or as an authenticated user. It is typically conducted to find as many flaws as possible to obtain a foothold, perform horizontal and vertical privilege escalation, move laterally, and compromise the internal network (typically the client's Active Directory environment).

**Inter-Disciplinary Assessments**

Some assessments may require involvement from people with diverse skillsets that complement one another. While logistically more complex, these tend to organically be more collaborative in nature between the consulting team and the client, which adds tremendous value to the assessment and trust in the relationship. Some examples of these types of assessments include:

**Purple Team Style Assessments**

As the name implies, this is a combined effort between the blue and red teams, most commonly a penetration tester and an incident responder. The general concept is that the penetration tester simulates a given threat, and the incident responder works with the internal blue team to review their existing toolset to determine whether alerting is properly configured or if adjustments are needed to enable correct identification.

**Cloud Focused Penetration Testing**

While heavily overlapping with a conventional penetration test, an assessment with a cloud focus will benefit from the knowledge of someone with a background in cloud architecture and administration. It can often be as simple as helping to articulate to the penetration tester what is possible to abuse with a particular piece of information that was discovered (like secrets or keys of some sort). Obviously, when you start introducing less conventional infrastructure like containers and serverless apps, the approach to testing those resources requires very specific knowledge, likely a different methodology and toolkit entirely. As the reporting for these types of assessments is relatively similar to conventional penetration tests, they are mentioned in this context for awareness, but technical details about testing these unique resources is outside the scope of this course.

**Comprehensive IoT Testing**

IoT platforms typically have three major components: network, cloud, and application. There are folks who are very specialized in each one of these that will be able to provide a much more thorough assessment together rather than relying on one person with only basic knowledge in each area. Another component that may need to be tested is the hardware layer, which is covered below. Similar to cloud testing, there are aspects of this testing that will likely require a specialized skill set outside the scope of this course, but the standard penetration testing report layout still lends itself well to presenting this type of data nonetheless.

**Web Application Penetration Testing**

Depending on the scope, this type of assessment may also be considered an inter-disciplinary assessment. Some application assessments may only focus on identifying and validating the vulnerabilities in an application with role-based, authenticated testing with no interest in evaluating the underlying server. Others may want to test both the application and the infrastructure with the intent of initial compromise being through the web application itself (again, perhaps from an authenticated or role-based perspective) and then attempting to move beyond the application to see what other hosts and systems behind it exist that can be compromised. The latter type of assessment would benefit from someone with a development and application testing background for initial compromise and then perhaps a network-focused penetration tester to "live off the land" and move around or escalate privileges through Active Directory or some other means beyond the applications itself.

**Hardware Penetration Testing**

This type of testing is often done on IoT-type devices but can be extended to testing the physical security of a laptop shipped by the client or an onsite kiosk or ATM. Each client will have a different comfort level with the depth of testing here, so it's vital to establish the rules of engagement before the assessment begins, particularly when it comes to destructive testing. If the client expects their device back in one piece and functioning, it is likely inadvisable to try desoldering chips from the motherboard or similar attacks.

**Draft Report**

It is becoming more commonplace for clients to expect to have a dialogue and incorporate their feedback into a report. This may come in many forms, whether they want to add comments about how they plan to address each finding (management response), tweak potentially inflammatory language, or move things around to where it suits their needs better. For these reasons, it's best to plan on submitting a draft report first, giving the client time to review it on their own, and then offering a time slot where they can review it with you to ask questions, get clarification, or explain what they would like to see. The client is paying for the report deliverable in the end, and we must ensure it is as thorough and valuable to them as possible. Some will not comment on the report at all, while others will ask for significant changes/additions to help it suit their needs, whether it be to make it presentable to their board of directors for additional funding or use the report as an input to their security roadmap for performing remediation and hardening their security posture.

**Final Report**

Typically, after reviewing the report with the client and confirming that they are satisfied with it, you can issue the final report with any necessary modifications. This may seem like a frivolous process, but several auditing firms will not accept a draft report to fulfill their compliance obligations, so it's important from the client's perspective.

**Post-Remediation Report**

It is also common for a client to request that the findings you discovered during the original assessment be tested again after they've had an opportunity to correct them. This is all but required for organizations beholden to a compliance standard such as PCI. You **should not** be redoing the entire assessment for this phase of the assessment. But instead, you should be focusing on retesting only the findings and only the hosts affected by those findings from the original assessment. You also want to ensure that there is a time limit on how long after the initial assessment we perform remediation testing. Here are some of the things that might happen if you don't.

* The client asks you to test their remediation several months or even a year or more later, and the environment has changed so much that it's impossible to get an "apples to apples" comparison.
* If you check the entire environment for new hosts affected by a given finding, you may discover new hosts that are affected and fall into an endless loop of remediation testing the new hosts you discovered last time.
* If you run new large-scale scans like vulnerability scans, you will likely find stuff that wasn't there before, and your scope will quickly get out of control.
* If a client has a problem with the "snapshot" nature of this type of testing, you could recommend a Breach and Attack Simulation (BAS) type tool to periodically run those scenarios to ensure they do not continue popping up.

If any of these situations occur, you should expect more scrutiny around severity levels and perhaps pressure to modify things that should not be modified to help them out. In these situations, your response should be carefully crafted to be both clear that you’re not going to cross ethical boundaries (but be careful about insinuating that they’re asking you to do something intentionally dishonest, indicating that they are dishonest), but also commiserate with their situation and offer some ways out of it for them. For example, if their concern is being on the hook with an auditor to fix something in an amount of time that they don’t have, they may be unaware that many auditors will accept a thoroughly documented remediation plan with a reasonable deadline on it (and justification for why it cannot be completed more quickly) instead of remediating and closing the finding within the examination period. This allows you to keep your integrity intact, fosters the feeling with the client that you sincerely care about their plight, and gives them a path forward without having to turn themselves inside out to make it happen.

One approach could be to treat this as a new assessment in these situations. If the client is unwilling, then we would likely want to retest just the findings from the original report and carefully note in the report the length of time that has passed since the original assessment, that this is a point in time check to assess whether ONLY the previously reported vulnerabilities affect the originally reported host or hosts and that it's likely the client's environment has changed significantly, and a new assessment was not performed.

In terms of report layout, some folks may prefer to update the original assessment by tagging affected hosts in each finding with a status (e.g., resolved, unresolved, partial, etc.), while others may prefer to issue a new report entirely that has some additional comparison content and an updated executive summary.

**Attestation Report**

Some clients will request an Attestation Letter or Attestation Report that is suitable for their vendors or customers who require evidence that they've had a penetration test done. The most significant difference is that your client will not want to hand over the specific technical details of all of the findings or credentials or other secret information that may be included to a third party. This document can be derived from the report. It should focus only on the number of findings discovered, the approach taken, and general comments about the environment itself. This document should likely only be a page or two long.

**Other Deliverables**

**Slide Deck**

You may also be requested to prepare a presentation that can be given at several different levels. Your audience may be technical, or they may be more executive. The language and focus should be as different in your executive presentation as the executive summary is from the technical finding details in your report. Only including graphs and numbers will put your audience to sleep, so it's best to be prepared with some anecdotes from your own experience or perhaps some recent current events that correlate to a specific attack vector or compromise. Bonus points if said story is in the same industry as your client. The purpose of this is not fear-mongering, and you should be careful not to present it that way, but it will help hold your audience's attention. It will make the risk relatable enough to maximize their chances of doing something about it.

**Spreadsheet of Findings**

The spreadsheet of findings should be pretty self-explanatory. This is all of the fields in the findings of your report, just in a tabular layout that the client can use for easier sorting and other data manipulation. This may also assist them with importing those findings into a ticketing system for internal tracking purposes. This document should *not* include your executive summary or narratives. Ideally, learn how to use pivot tables and use them to create some interesting analytics that the client might find interesting. The most helpful objective in doing this is sorting findings by severity or category to help prioritize remediation.

**Vulnerability Notifications**

Sometimes during an assessment, we will uncover a critical flaw that requires us to stop work and inform our clients of an issue so they can decide if they would like to issue an emergency fix or wait until after the assessment is over.

**When to Draft One**

At a minimum, this should be done for any finding that is directly exploitable that is exposed to the internet and results in unauthenticated remote code execution or sensitive data exposure, or leverage weak/default credentials for the same. Beyond that, expectations should be set for this during the project kickoff process. Some clients may want all high and critical findings reported out-of-band regardless of whether they're internal or external. Some folks may need mediums as well. It's usually best to set a baseline for yourself, tell the client what to expect, and let them ask for modifications to the process if they need them.

**Contents**

Due to the nature of these notifications, it's important to limit the amount of fluff in these documents so the technical folks can get right to the details and begin fixing the issue. For this reason, it's probably best to limit this to the typical content you have in the technical details of your findings and provide tool-based evidence for the finding that the client can quickly reproduce if needed.