Pentesting 101 Part 3: Executing the Scope-of-Work & Penetration Testing

labs.lares.com/pentesting-101-pt3

Steve Spence March 5, 2024

It's time to test some pens ...

Following our previous posts, Part1 & Part 2, let's continue building on what we have learned and moving towards our end goal.

So, a quick recap!

- We posed and answered the question: what is Penetration Testing?
- We've identified your driving factors, why you need to conduct a penetration test, and any required testing types.
- We've identified our engagement prereqs and the scope of the penetration testing engagement.

Now, we are, or rather should be, at the stage where we have everything we need to conduct our engagement.

In part 1 of the series, we posed and answered the question: What is a Penetration test? Using the following answer to serve as a generic base:

> A method for gaining assurance in the security of an IT system/environment, by attempting to breach some or all of that system's/environment's security, using the same tools and techniques as an adversary might.

Here at Lares, we do just this with our penetration testing, attempt to circumvent security controls and gain unauthorized access to an environment, system or service, from an adversarial stance, as a threat actor. Ultimately, it seeks to identify exposures, weaknesses, misconfigurations, and vulnerabilities, which consequently allow/facilitate the exploitation of given systems, infrastructure, applications, or networks.

These attack vectors and exploits will attempt to gain control and further penetrate/compromise the network. With the aim to gain an understanding of the extent of exposure, risk, and compromise to which our clients are face, as a result of the infrastructure, services and security maturity in play. Doing so allows us to understand the true impact to any client organization or what it will likely be, e.g., a postulated threat.

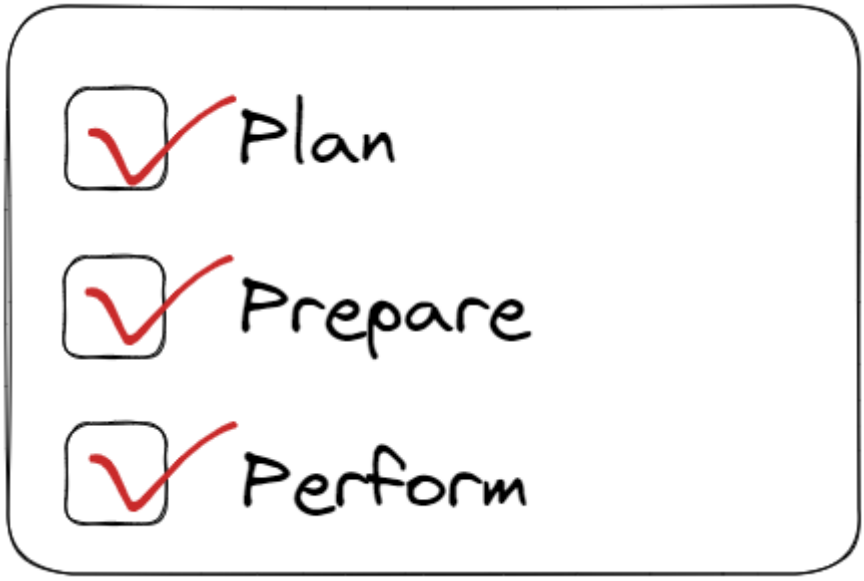
I hear you asking how we do this ... well simply put, we execute our engagements with a detailed methodology, which follows many repeatable steps that can be used no matter the type of engagement.

Methodology Overview

As I mentioned, a methodology, sometimes referred to as the ‘stages of a penetration test’, can be broken down into the following five steps/stages/phases:

- Planning & Reconnaissance
- Discovery/Enumeration (Automated & Manual)
- Attack Simulation & Exploitation (Automated & Manual)
    - Command & Control (optional)
    - Exfiltration (optional)
- Analysis & Reporting
- Client Debrief

However, let's take a moment or two to revisit a crucial stage of the overall penetration testing process, ‘**Pre-engagement**’ activities.



Setting up for Success!

The first element of any penetration test should always be pre-engagement with the customer. This is where we define the engagement parameters, e.g., Plan, Prepare & Perform, ultimately setting the engagement up for success! Here are a few key points to tick: a pre-engagement checklist.

- Meet with the engagement point-of-contact, commonly referred to as the “PoC”.
- Meet with the customer's security team/technical liaison.
- Ensure there is a description, known as the Statement-of-Work, for the testing types/activities highlighted within the Scope of Work document.
    - Statement of Work: Summary describing the overall work to be carried out.
    - Scope of Work (SoW): The actual specifics, e.g., IPs, Domains, Environments, Type of testing/scenarios.

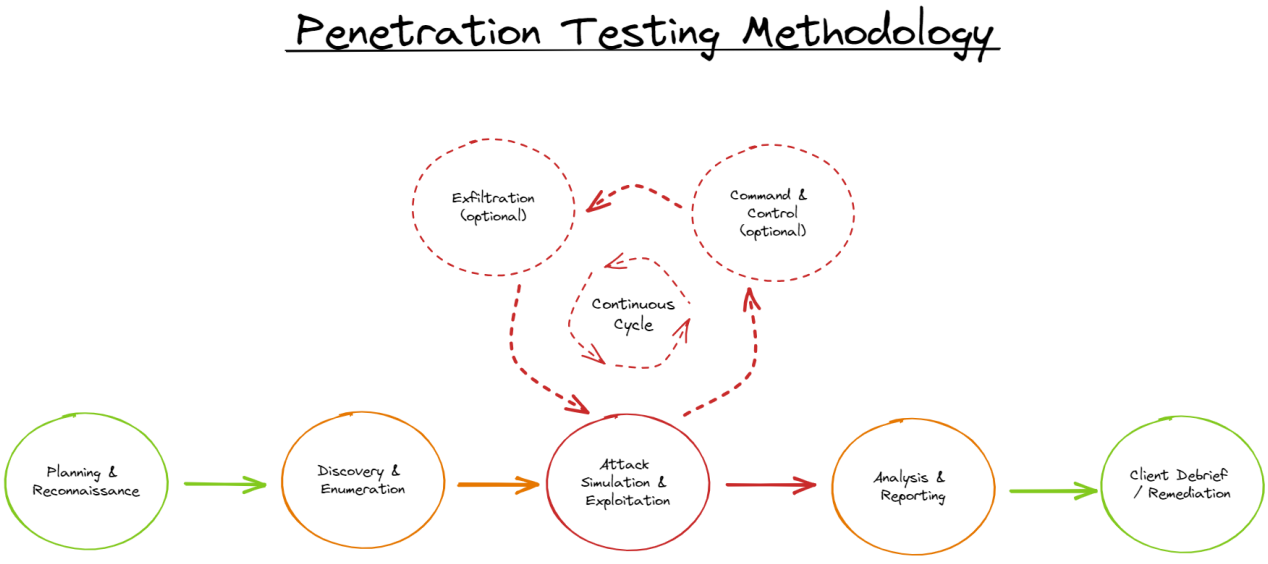
        Note: I see lots of folks use these headings interchangeably, which is not correct and can lead to complications/confusion.

- Ideally, there should be no deviation from the scope document. Where a new testing requirement has been identified, a procedure relating to SoW changes or additional work must be followed prior to any new or undefined work being undertaken. Doing so will keep everyone right.
- Confirm connectivity, access and any credentials required/provided for testing purposes are working correctly/as expected.
- Ensure there is an agreed method to communicate with the PoC's, both primary and secondary (if required), along with establishing a communal & line of communication throughout the testing,
    - Ensure that where details for any technical PoC exist they are also added into any communications.
    - Ensure that the necessary communications with any involved security team are established, if different from your point of contact.
- Where on-site testing site is applicable, or where multiple on-site locations are in scope, then an onsite point-of-contact must be nominated for each site in scope.
- Again, include these PoCs in any engagement's communications (as applicable).
- Prior to the engagement/testing commencing on the agreed start date, a final authorization to test will be sought via email. This is in order to verify there have been no changes and/or issues with any of the scoped items for review.

So, now we have revisited the pre-engagement activities and double checked that we're good to go e.g., get to the fun stuff, lets provide some context around each of the steps/stages/phases outlined in the **Methodology Overview** and set some expectations around what to expect.

A not-so-linear process ...

With all that said, the penetration testing methodology, or rather the one that I will lay out and step through, describing as a linear model isn't necessarily the best way to describe it; a more accurate representation would look like this *(everyone loves a diagram)*:



Basic Penetration Testing Methodology

I should state, at this stage at least, that whilst the methodology depicted in the diagram above can be applied across several different engagement types, the actual activities/actions, taken for example, for a **Red** or **Purple** team engagement, each would significantly differ in execution, due to the engagement deliverables or objectives. So, it is essential to remember this and understand the differences. As such, this post won't cover the specifics of a Red & Purple team engagement.

Planning & Reconnaissance

This can differ depending on engagement type and objectives, but in a general sense this can be framed as conducting initial reconnaissance & target confirmation phase of a penetration test.

The test team will perform activities to enumerate, identify, and confirm information relating to the engagement target(s) or specific environment(s) in a non-invasive or passive manner.

This phase can or will be conducted in a variety of ways, some examples of which are detailed below:

- Customer-supplied information, i.e., target lists, IP ranges, URLs.
- Use and reference publicly available information sources such as domain name registrars, corporate information disclosed as a matter of public record and/or social media platforms.
- Publicly available data breach information, e.g., emails, passwords, usernames etc.

Note: *The points detailed above are not exhaustive, and any source that discloses information regarding a target and/or environment can or may be used to some extent.*

Discovery/Enumeration (Automated & Manual)

This step involves taking the information and data gathered above and then using it more actively, meaningfully and strategically, e.g., interacting with the target resources and services. This step will typically involve activities such as:

- Port scanning
- Banner grabbing
- Vulnerability assessment & mapping
- User verification/validation
- Security misconfiguration verification/validation
- Password analysis & reuse

Essentially, the test team will look to validate any of their findings/observations for the services and capabilities, which would ultimately be presented to a threat actor for any of the given assets/applications/environments in scope.

Example Enumeration and Discovery:

The test team has identified and confirmed a selection of servers as target assets.

- They will then attempt to identify a list of services running on the host(s).
  For internal network environments this could be done via passive monitoring of the network or be achieved with active scanning techniques such as port scanning.
- Further targeted manual testing and probing of any applications, networks, services and/or devices in scope will be conducted. This is to provide continuity of testing as well as determine or identifying exact versions of software or hardware (where possible) in use on the asset(s) in scope.
- The test team will now determine whether any of these services are vulnerable and furthermore, whether any consequent issues identified are associated with publicly disclosed vulnerabilities, which have been documented as leading to successfully compromising the assets or services.

Note: *The points detailed above are not exhaustive and are merely provided for context and visualization of what may occur during this phase.*

Attack Simulation & Exploitation (Automated & Manual)

Execute attack path to compromise
- Command & Control activities *(optional – dictated by SoW/objectives)*
- Exfiltration activities *(optional – dictated by SoW/objectives)*

During the targeted attack simulation and exploitation phase of testing, the test team will work towards proving or disproving their ability to interact in an unintended manner and/or to compromise the target environment/application/asset(s) using the enumerated data collected, in conjunction with any vulnerabilities that were mapped earlier in the Vulnerability Mapping and Data Analysis phase.

This will ultimately unfold in such a manner, where the test team will emulate the actions of a malicious individual/threat actor or group; however, a distinct and noticeable difference in general penetration testing engagements, is that they are time-boxed and executed in a controlled manner. This will minimize disruption to client service level agreements, impact to the network and to the services or assets they are targeting; however, a legitimate threat actor, depending on skill/technical ability may not care of the resulting impact of such activities, nor are they limited by time.

Example Attack Scenario: NTLM Relay Attack (High-level overview)

The test team has identified and confirmed the presence of server message block (SMB) traffic, and that Link-Local Multicast Name Resolution (LLMNR), along with NetBIOS Name Resolution (NBT-NS), is enabled.

- Using the tool, CrackMapExec, the consultant generated a relay list of SMB hosts that do not enforce signing, which will serve as relay targets.
- Responder used to carry out a poisoning attack against LLMNR, NBT-NS, and mDNS traffic, along with capturing authentication hashes.
- NTLMrelayX is then used to relay those authentication hashes to the list of relay targets.

A successful relay can result in the following:

- Command execution
- Establish additional footholds
- Persistence
- Interactive shells on the exploited server
- Lateral/vertical movement
- Establish additional footholds
- Persistence
- Dumping Hashes
- Offline cracking

Command & Control activities (optional – dictated by SoW/objectives)

Where a foothold has been successfully gained, a malicious individual or hacking group will often attempt to take their attacks further by escalating access privileges of any compromised users and/or accounts. This may require a command and control (C2) element but can be done without. Often, Lares consultants will perform additional enumeration without using C2 communications and operate from compromised endpoints or using legitimate user access.

The test team's next steps would be to emulate the same approach and install some form of C2; this can be as simple as a reverse connection to using more complex frameworks alongside multiple connectivity methods to ensure redundancy.

Ultimately, the goal is to gain administrative/complete control of the compromised target. This may include but is not limited to, such assets as:

- A domain controller(s)
- Active Directory
- Critical system(s) containing sensitive data
- Network devices i.e. switches, routers, firewalls (if or where applicable)
- Application Servers
- Cloud environments

Exfiltration activities (optional – dictated by SoW/objectives)

Data exfiltration and proof-of-concepts are typically the final active stages of any penetration testing engagement. Data exfiltration is not conducted on every engagement. It is generally agreed in advance as an engagement deliverable, or more commonly reserved for scenario-driven, offensive or bespoke object-orientated testing (commonly referred to as “red or purple team” type engagements).

It is worth noting that depending on the data “in play”, various legal considerations may need to be assessed and understood before any actual execution of data exfiltration. For instance, European/UK clients and their associated data may be governed by legislation such as the General Data Protection Regulation (GDPR) and/or the UK’s Data Protection Act.

In general, data can be categorized as **non-sensitive** or **sensitive**.

- **Non-sensitive PII** is information that can be transmitted in an unencrypted form without harming the individual. Non-sensitive PII can be easily gathered from public records, phone books, corporate directories, and websites.
- **Sensitive PII** is information that, when disclosed, could harm the individual whose privacy has been breached. Sensitive PII should therefore be encrypted in transit and when data is at rest. Such information includes biometric information, medical information, personally identifiable financial information (PIFI) and unique identifiers such as passport or Social Security numbers.

So, it is highly recommended, that before any data exfiltration the test team understand the type of data they will be interacting, along with any regulatory/legal requirements.

Finally, it is essential to realise that, as general penetration tests are carried out within the context of a timeboxed and controlled manner, attacks such as Denial-of-Service (DoS) attacks are often avoided, along with exploits/exploitation, which may be unreliable or are known to work in such a way that they cause damage or disruption.

Where there is a requirement/deliverable for this type of specific testing, where possible, testing should be carried out in a simulated and representative test environment rather than against the real/live asset(s) itself; this is particularly beneficial where sensitive or high use production environments are being tested.

Analysis & Reporting

A good friend and colleague of mine comments regularly that:

> ...we get paid to write reports, the hacking is free!

and this is definitely true!

The main deliverable of any penetration test is a formal penetration/engagement test report. This should be compiled by the test team and overseen by a senior/lead tester for each engagement. The final report will be ultimately sent directly to the customer and/or

related in house security/technical teams *(where agreed in advance).*

Ultimately, the analysis and reporting of the engagement should include:

- Any security issues uncovered.
- The test team assesses the level of risk that each vulnerability exposes to the organisation or system.
- A method of resolving each issue found.
- We will use our consultants' professional opinion on the accuracy of your organisation's security posture based on the evidence from the penetration testing.
- Advice on how to improve your vulnerability assessment and management process.

As such, a typical penetration testing engagement report, at a minimum, should have the following sections:

- Executive Summary
- Technical Summary
- Engagement Overview
- Engagement Phases and Detailed Findings
- Supplemental Data
- Appendices

Client Debrief

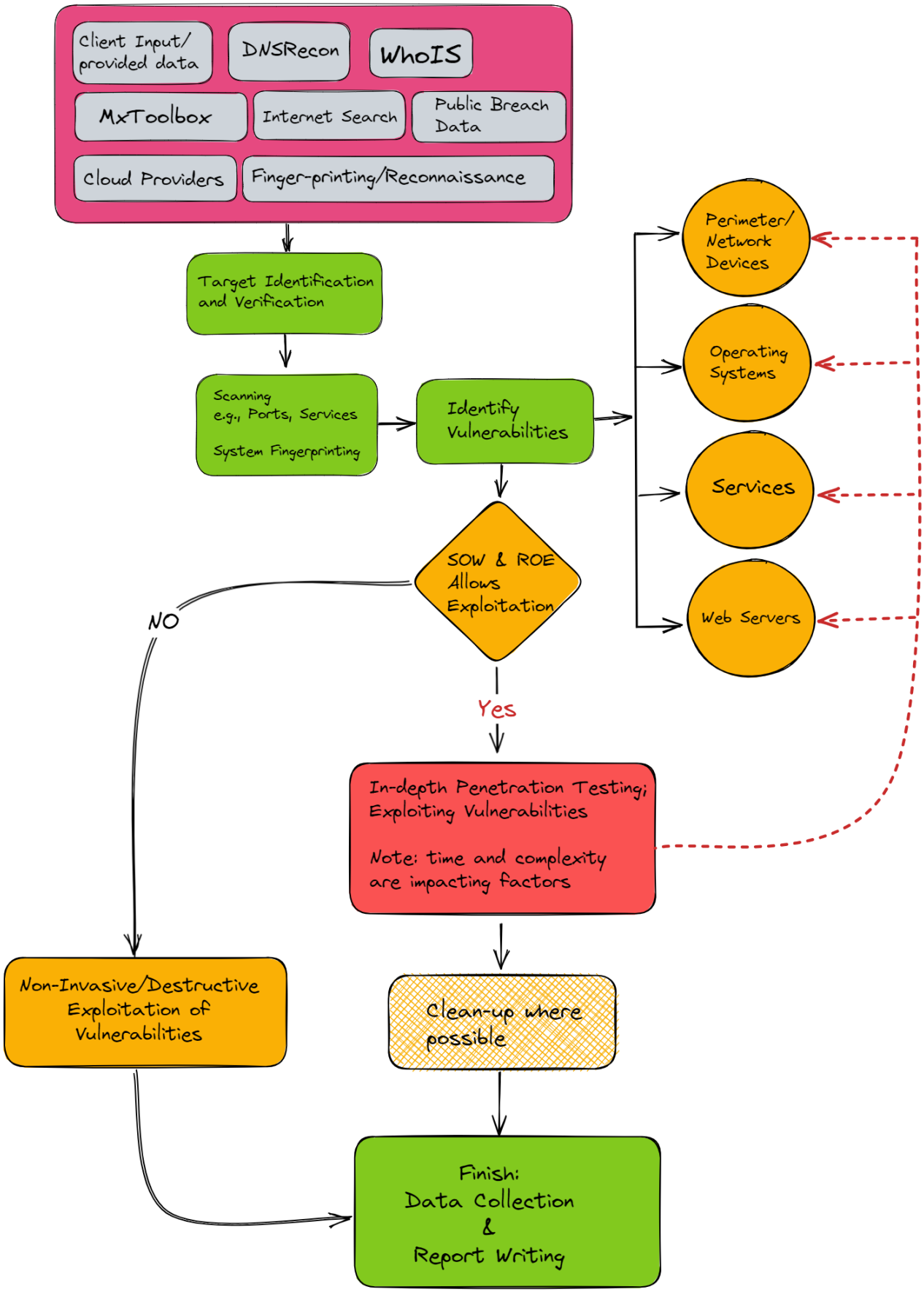
A penetration testing debriefing session should be arranged(where applicable per assessment type) after a suitable/pre-agreed timeframe, after which the client's in-house technical and security teams have had ample time to read, understand, and formulate the basis of any engagement questions and remediation approach.

This serves as a crucial step in the overall assessment process, providing an opportunity for the test team to communicate their findings comprehensively and for the client to gain deeper insights into the security posture of their systems.

Practical Execution of the Methodology: External Penetration Test

In reality, an actual practical example of the execution of a penetration test, for example, an external penetration test, might look like this, as depicted in the image below.

Note: this is a high-level representation of the execution of the methodology.



Practical Example of Executing a Penetration Testing Methodology

Using our previously defined methodology, let's break down the example in the image above.

- **Planning & Reconnaissance**
  Activities are conducted against a number of services/ resources, as annotated within the pink box.
- **Discovery & Enumeration**
  - Target identification/verification
  - Port scanning
  - Banner grabbing
  - Manual interaction
  - Vulnerability assessment
- **Attack Simulation & Exploitation**
  Test team reference the SOW & engagement deliverables:
  - **If allowed:** further targeted activities can be focused on perimeter/network devices, Operating Systems, Servers, Web Servers and Services, with the view to identify vulnerabilities leading to viable attack paths and exploitation.
  - **If not allowed:** Conduct a vulnerability assessment *(see note below)*, with follow-up non-invasive manual verification, along with documenting any the likely outcome/risk.

Note: a vulnerability assessment is not the same as an actual penetration test; these two terms are used interchangeably regularly. A key point to note is that a vulnerability assessment generally focuses on the identification of as many vulnerabilities within the allotted period as possible, whereas an 'actual' penetration test will not only identify vulnerabilities, it will also focus on active exploitation of these vulnerabilities, to fully understand their actual security risk and impact.

Let's recap...

In summary, we've discussed/walked through the execution of the scope-of-work (SOW) and the actual phases of a penetration test, what they look like in general, the types of actions that could be taken throughout that process, reporting and what that should look like, along with the view of a practical representation of what this looks like in 'real life', using an external penetration test as our reference point.

If you are ever in doubt or unsure about your penetration testing needs, seeking assistance from a dedicated organisation that provides such services regularly and has a proven track record and reputation is the first step to maturing your security posture, awareness, and understanding of penetration testing.

Over time, you will become more informed and able to take more ownership of this process.

From here, the following steps involve: Given that we carried out the scope of work and our testing activities following our methodology, we now need to compile the engagement report, deliver it to our client, and follow this up with a debrief call/session. This will be covered in part 4 of the 'Pentesting 101' series.

How can we help?

Here at Lares, we help empower organizations to maximize their security Potential.

Lares is a security consulting firm that helps companies secure electronic, physical, intellectual, and financial assets through a unique blend of assessment, testing, and coaching.

If you would like any further information, you can get in touch here or head over to the Lares.com website for more information about how we can help.