2.2.10 Lab - Create a Pentesting Agreement.

Any business agreement between two organizations must be formalized in a legally binding contract. They need to agree on the conditions of the agreement, the processes that will be used, and the definition of the deliverables. The project timeline needs to be agreed on as do the costs and payment schedule.

Lab - Create a Pentesting Agreement

Answers In Red

Objectives

In this lab, you will create your own pentesting agreement.

- Complete a simple pentesting agreement.

Background / Scenario

A penetration testing agreement is a legally-binding contract between the client or customer, and the penetration tester. The agreement defines all the terms and conditions required for the penetration testing exercise. The agreement will include elements that are mutually agreed upon by both parties. It may contain things, such as the date for the commencement of pentesting, the scope of work, the service-level agreement, the potential pentesting completion date, etc. Also included in the contract will be other terms and conditions as well as pricing details.

Imagine that you are hired by a company to perform pentesting. You will need to draft a pentesting agreement between your company and the client. In a real-world situation, you would likely consult with an attorney who is specialized in such contracts because understanding them and what information they contain is very important.

Instructions

Part 1: Complete a Simple Pentesting Agreement

Step 1: Research pentesting agreements and contracts.

a. Using your favorite search engine, conduct a search for pentesting contracts, statements of work, and agreements.
b. Find several pentesting agreement examples and review the information contained in each section.

Step 2: Develop the pentesting agreement.

Using the information that you gathered from your research in step 1, create your own penetration testing agreement for your company. At a minimum, the agreement should include the sections listed below.

a. Parties to the agreement

Service Provider (Penetration Tester):
Protego Security Solutions (PSS)
Headquarters: San Francisco, California, USA
Branch Offices: London, UK and Singapore
Phone: (415) 555-0199
Email: contact@protegosecurity.com
Website: www.protegosecurity.com

Client (Recipient of Services):
Pixel Paradise
Headquarters: San Francisco, California, USA
Phone: (415) 555-0142
Email: admin@pixelparadise.games
Website: www.pixelparadise.games

b. Scope of work

The Penetration Tester (Protego Security Solutions) agrees to:

- Conduct a comprehensive black-box penetration test on Pixel Paradise's network infrastructure, web applications, and internal systems.
- Perform social engineering simulations to evaluate employee security awareness.
- Deliver a detailed vulnerability assessment report and risk mitigation recommendations upon completion.
- Operate within agreed-upon timeframes and legal constraints.
- Maintain strict confidentiality of any sensitive information discovered during the testing process.
- Adhere to all industry standards and certifications, including ISO 27001 and CREST guidelines.

The Client (Pixel Paradise) agrees to:

- Provide timely access to relevant systems, applications, and personnel as needed.
- Clearly define in-scope and out-of-scope assets prior to commencement.
- Ensure internal teams are informed of testing to avoid false alarms or operational disruptions.
- Pay all agreed fees within the billing terms defined below.
- Cooperate with Protego for the duration of the engagement.

c. Timeframe

The testing engagement will begin on August 5, 2025, and conclude by August 19, 2025**.**
The final report will be delivered no later than August 23, 2025**.**

d. Fees, billing, and payment details

Total Fee for Services: $25,000 USD

- Billing Schedule:
  - 50% ($12,500) due upfront upon signing of agreement
  - 50% ($12,500) due upon final report delivery
- Payment Method: Bank transfer or corporate credit card
- Any materials or tools required for testing will be provided by Protego Security Solutions.
- Additional services beyond the defined scope will require a new agreement or amendment.

e. Termination of contract

Either party may terminate this agreement prior to completion under the following conditions:

- Breach of Contract: If either party fails to fulfill obligations after written notice.
- Mutual Agreement**:** Both parties agree to terminate the engagement in writing.
- Unforeseen Legal or Security Circumstances: Any incident that renders testing illegal or unethical.

Upon termination, all pending dues must be cleared within 15 business days.

Step 3: Bonus – Additional Agreement Sections

In addition to the sections, you completed above, list and define some other clauses that are typically found in a penetration testing agreement.

1. Confidentiality Clause
All findings, reports, and client data are confidential. Protego will not disclose any information to third parties without written consent from Pixel Paradise.

2. Liability and Indemnity
Protego shall not be liable for any incidental or consequential damages resulting from testing. Both parties agree to hold each other harmless for claims arising from negligence or willful misconduct.

3. Non-Disclosure Agreement (NDA)
A separate NDA may be executed to cover sensitive project information and internal communications.