Capstone Project Guidelines

Updated Dec 01, 2023

Introduction

The capstone project is a “structured walkthrough” penetration test of a fictional company, Artemis, Incorporated (“Artemis”). A structured walkthrough is an organized procedure for a group of peers to review and discuss the technical aspects of various IT, IT Security, and IT Audit work products. The major objectives of a structured walkthrough are to find errors and to improve the quality of the product or service to be delivered.

This document provides a comprehensive overview of the project and the expected deliverables.

Overview

You work for a firm specializing in cybersecurity consulting, namely penetration tests, vulnerability assessments, and regulatory compliance. Artemis has hired your firm to perform an external penetration test. In preparation for this engagement, you must lead your team of new pen-testers in a structured walkthrough of the entire test so that:

a) Everyone on the team knows what to do.
b) The amount of time allotted for the actual test is utilized as efficiently as possible.
c) The client’s expectations are met or exceeded.

To accomplish this task, you must perform the following **five phases**:

1. Perform simulated reconnaissance of the client.
2. Simulate target identification and scans against the external network.
3. Simulate the identification of vulnerabilities.
4. Based on the above, assess the threats and make recommendations.
5. Create two mock reports for the client: An **Executive Summary** for the client's senior management, and a **Detailed Technical Report** for the client's IT staff.

This project is an excellent addition to your portfolio, as it demonstrates your understanding of critical security issues and your skills in identifying and analyzing threats and vulnerabilities. The project also allows you to speak knowledgeably about the entire process of performing a pen test, using your project as a reference point.

Each phase will include its own deliverable(s). A full description of what is required can be found under each phase.

Directions

When planning penetration tests, consulting firms always sit down with the client's key stakeholders to confirm scope and approach, identify the client's concerns, and set expectations regarding the outcome. To this end, you have been provided with an overview of the client and an overview of the client's IT environment. This information is critical because all risks must be evaluated within their context. The example below illustrates this concept:

Technically Accurate – Artemis' web application does not restrict or filter user uploads by file type. This is a vulnerability that could allow threat actors to connect remotely, execute arbitrary code, and then elevate their privileges within the application.

With context – Artemis' RFQ/RFP web application does not restrict or filter user uploads by file type. This is a vulnerability that could allow threat actors to connect remotely, execute arbitrary code, and then elevate their privileges within the application. In this instance, the threat actors would be able to view or download sensitive information regarding bids and even gain admin rights within the application.

As you can see, the second description indicates the technical aspects and the business impact as well.

The next two sections, **client overview** and **technology overview**, provide the context you will need to help you with the five phases of your capstone project.

Client Overview

ARTEMIS GAS, INC. (“Artemis”), based in Paris, France, is present in 40 countries with approximately 30,000 employees and serves more than 1.7 million customers and patients. Oxygen, nitrogen, and hydrogen have been at the core of its activities since its creation in 1922. They own and operate over 1,000 miles of industrial gas pipelines in the U.S., supplying mainly oxygen, nitrogen, hydrogen, and syngas in large quantities from multiple production sources to major customers in the chemicals, petrochemicals, refining, and steel industries. Their pipeline operations and industrial gas production facilities are closely monitored 24/7 within their leading-edge operations control center located in Houston, TX. Their operations control group monitors over 49,000 data points and assists with product supply and coordination. They are constantly optimizing their supply network to provide high reliability and energy efficiencies, allowing Artemis to adjust supply needs more quickly and effectively, thus enabling growth to their customers.

Artemis has grown quickly over the past few years, and the need to “make things work” has outpaced the need to “make things work securely.” Some security solutions are fairly mature and effective; some are less so. Among the company’s concerns are:

- Some older network hardware that is being phased out is unsupported and may have unpatched vulnerabilities.
- Some newer network hardware may not have been configured properly.
- Some business units do not always follow company policy regarding storing data in the cloud, creating websites, or conducting file transfers.
- Some IT admins like to do their own thing because “that’s the way they’ve always done it.” This could be exposing the network to unknown risks.

Technology Overview

Artemis utilizes a mix of security vendors and technologies. The firewall landscape consists of Cisco, Fortinet, and Palo Alto. They use F5 (Big IP) for load balancing, and for secure remote application access, they use Zscaler. Roughly half of their servers and applications are in the cloud (Amazon Web Services), and the rest are on-premise (on-prem). These on-prem assets are spread out among four major data centers located in Houston, Paris, Cairo, and Singapore.

The network is currently transitioning to SD-WAN, so there are still several MPLS links, especially at the smaller, more remote locations. The old Cisco equipment is being phased out in favor of Fortigate devices from Fortinet. Additionally, since the Fortigates can also act as firewalls, the company is considering eliminating the rest of its Cisco gear to cut costs. They are unable to supply a current network diagram. The ones they have are severely out of date and would not be of any use to you.

Internally, Artemis utilizes a Single Sign-On (SSO) solution that leverages Microsoft Active Directory to authenticate users to other applications, namely SAP. SAP is the company's primary ERP system and runs on servers running Linux and Oracle 12c. Messaging is a mix of Exchange Online (via the Office 365 cloud tenant) and on-prem Microsoft Exchange servers. The only other applications of note are the PARS system and the APOLLO system.

PARS allows engineers to submit technical information regarding potential patents. If the submission passes legal and technical review, it is forwarded to the Intellectual Property group for submission to either the US Patent Office, the National Institute of Industrial Property INPI) in France, or both. APOLLO is the repository for trade secrets, primarily around manufacturing processes.

Project Guidelines

This next section will provide you with the goals, procedures, deliverables, and time estimates expected for each phase of the project. Read each of these sections carefully before proceeding to begin on phase 1.

Phase 1. Perform Reconnaissance

Goal: Build as robust a profile on the target (Artemis) as possible. The profile should include the target's technology stack, email addresses, phone numbers, resumes, and so on.

Procedure: Detail the activities you plan to use to obtain as much publicly available information as you can.

Deliverable: Provide a minimum two-page description of all the tools and methods you will use to accomplish this task. Deliverable should cover at least 15 tools/resources.

Time estimate: 2 hours

Phase 2. Identify Targets and Run Scans

Goal: Identify the tools and techniques to be used to perform host discovery and enumeration.

Procedure: List out the tools you plan on using to perform network scans, the purpose for using them, and how you will use them. For example:

1. ***Tool:*** Nmap.
   Purpose: Obtain information on hosts and the services and operating systems they are running.

   Commands: *‹List commands to be used for identifying live hosts, banner grabbing, OS fingerprinting, open ports, etc.›*

Deliverable: Provide a minimum 2-page description of the tools you plan on using for the network scans, your reasoning for selecting them, and how they will be used. Be sure to include any challenges and potential drawbacks or limitations. Deliverable should cover at least 5 tools/resources.

Course content reference: There are two labs, ***Reconnaissance from the WAN*** and ***Scanning the Network on the LAN*****,** that may help you with this step.

NOTE: Kali is **not** a tool; it is a Linux distribution or *collection* of tools, so do not include it in your list.

Time estimate**:** 4 hours

Phase 3. Identify Vulnerabilities

Goal**:** Identify the tools and techniques to be used to scan for vulnerabilities.

Procedure: List out the tools you plan on using to perform vulnerability scanning and how you will use them. Include both Tenable Nessus and OpenVAS. Remember to include tools designed to look for vulnerabilities within specific technologies or platforms, such as Cisco devices, remote access services, and web applications (e.g., Burp Suite). Follow the same documentation procedure you performed in the previous step. Include screenshots of such tools showing configuration options and settings. Finally, list the pros and cons of each tool.

Deliverable: Provide a minimum 2-page description of the tools you plan on using for the vulnerability scans, how you will use them, screenshots of the tools with configuration options and settings, and the pros and cons of each tool. Deliverable should cover at least 5 tools.

Time estimate: 2 hours

Phase 4. Threat Assessment

Goal: Create a hypothetical threat assessment based on vulnerabilities you expect to find when you perform your actual scans against the client's network.

Procedure: Assume the scenarios below are what you are most likely to encounter when you begin your actual work.

Scenario 1: Unpatched RDP is exposed to the internet

Scenario 2: Web application is vulnerable to SQL Injection

Scenario 3: Default password on Cisco admin portal

Scenario 4: Apache web server vulnerable to CVE-2019-0211

Scenario 5: Web server is exposing sensitive data

Scenario 6: Web application has broken access control

Scenario 7: Oracle WebLogic Server vulnerable to CVE-2020-14882

Scenario 8: Misconfigured cloud storage (*AWS security group misconfiguration,* ***lack of access restrictions)***

Scenario 9: Microsoft Exchange Server vulnerable to CVE-2021-26855

Deliverable: Provide a spreadsheet or document showing the following items. Make sure you factor in the appropriate context. For example, if you think you might be able to penetrate the APOLLO system, evaluate those risks according to that system's sensitivity and criticality.

- Description of the vulnerability
- Operating systems/versions affected
- Risks of attempting to exploit (e.g., might crash the host or lock out an account)

- Risk (what could you or a threat actor do upon successful exploitation)?
    - Identify as many attack vectors as you can. Examples: launch an attack on internal systems, obtain password hashes, crack passwords, access other systems, move laterally, and so on).
    - Identify potential blocking mechanisms such as AV software or IDS/IPS, and how you might try to bypass them.
    - Document how you plan on cracking passwords. This will depend on the source system's course, but you should be ready for whatever you run into. Include online tools as well.
- Remediation action

Course content reference: You may need to refer back to the unit on **Application Security** to analyze the vulnerabilities and assess what threat they pose to Artemis. Remember: The threat depends on the likelihood and impact of the vulnerabilities being exploited and requires a review and knowledge of the current threats.

Include all the information and risk ratings to determine the threat profile for Artemis.

Time estimate: 6 hours

Phase 5: Reporting

Goal: Create two mock reports for the client: An **Executive Summary** for the client's senior management, and a **Detailed Technical Report** for the client's IT staff and submit them to your boss (in this case, your mentor).

Procedure: Create the two reports below:

- The **Detailed Technical Report** should contain the scope and approach, reconnaissance activities, vulnerabilities, and an analysis of the threats that Artemis faces based on the current threat environment. Use this resource as your guide and template for creating the Detailed Technical Report:

The report should include the following sections:

A. Cover page
B. Table of Contents
C. Scope of Work
D. Project Objectives
E. Assumptions
F. Timeline
G. Summary of Findings
H. Recommendations

***Target report length*: We expect the average report to have a minimum of 10 pages.

- **The Executive Summary.** The executive summary serves as a high-level view of the business risk in plain English. The purpose is to be concise and clear. Executives don't need (or want) to understand the technology. It is imperative that business leaders grasp what's at stake to make informed decisions for their companies, and the executive summary is essential to delivering that understanding. Visual communication can be tremendously helpful here. Try to use visuals like graphs and charts in communicating the summary data. The de facto approach is to use colors to denote risk severity, specifically, red, yellow, and green. If there are four categories, then add orange.

  Target report length: No more than 2 pages! Check out this example executive summary for some more guidance on what this final deliverable should look like.

***Time estimate*: 4 hour