Lab - Pre-Engagement Scope and Planning

Addressing Table – Data Center

Servers	VLAN	IP Address	Subnets
Administration	2-5	172.24.1.0/24	(4) 255.255.255.192
Amazon Support	10 - 25	172.25.0.0/16	(11) 255.255.252.0
Operations	50 - 55	172.26.0.0/21	(5) 255.255.255.0
Logistics	80 – 85	172.27.0.0/21	(5) 255.255.255.0
Management	100 - 110	172.30.0.0/16	various as necessary

Addressing Table – LAN

Department	VLAN	IP Address	Subnet Mask
Administration	120	172.16.1.0	255.255.255.0
Finance	130	172.16.4.0	255.255.255.0
Information Technology	140	172.16.8.0	255.255.255.0
Warehouse	150	172.16.12.0	255.255.255.0
Customer Service	160	172.16.16.0	255.255.255.0
Shipping	170	172.16.20.0	255.255.255.0

Objectives

Obtaining agreement on the rules of engagement that apply to a penetration test or security audit is the first step in any engagement with a client. It is important to spend the time to ensure that both your firm and the client have a clear understanding of the terms and scope of the testing engagement.

- Create a penetration test scope and plan document that addresses the requirements for penetration testing services that were gathered from the client.
- Determine the rules of engagement elements.

Background / Scenario

Your company was contacted to perform a security audit for Nexus Plaza, an online retail enterprise. You have been assigned to assist the lead auditor in developing the scope of the testing engagement. Use the network diagram and the transcript of the interview with the enterprise CEO and IT director to fill out the Scope Worksheet.

Interview with CEO and IT Director

> **CEO**: Welcome to Nexus Plaza. We've invited you here to kick off our engagement and to discuss what we are expecting from this security audit. We are anxious to ensure that our security infrastructure meets or exceeds the necessary safeguards. I'll turn this over to our IT director to describe our network environment.
>
> **IT Director**: As you know, we are primarily an online retail enterprise. Our customer-facing ecommerce sites are hosted on Amazon, but all our communications, warehousing and shipping IT services are handled in-house. We operate a local datacenter in Houston which supports our manufacturing and warehousing facilities. There are currently 25 servers segregated into three clusters: administration, operations, and logistics. In addition, we operate a cluster that provides support for our Amazon storefront. Remote access to these systems is through SSL or IPsec VPN. We use two ISPs to connect us to the internet, but one is used primarily for communications with Amazon to support real-time orders, inventory, and customer contact.
>
> **CEO**: One of our competitors recently was hit with a ransomware attack that targeted their production inventory system. They lost a significant number of customer orders due to being unable to pick and ship inventory in a timely manner. We are concerned that our warehouse and shipping systems may have vulnerabilities that could shut us down similarly if a breach occurs. When you depend on fast delivery to customers, any delay is a disaster.
>
> **IT Director**: The systems that support our warehousing and shipping are located in two clusters in the datacenter: operations and logistics. Internal access to these systems is restricted to the warehouse administration staff, IT personnel, and inventory control clerks. Our inventory control system is supported by a Microsoft SQL Server database. As you can see on the diagram, the SQL database is housed on a separate SAN with connections to both the warehouse and production systems. Our business depends on our access to Amazon; therefore, no testing should encroach on the datacenter clusters that contain the Amazon storefront data and inventory. These are identified on the diagram.
>
> **CEO**: We want you to test the security controls to ensure that an attacker who successfully obtains access to an end-user account and computer within the warehouse cannot obtain administrator access to any of the servers or have access to the production inventory database. We also want to be sure that the software and operating systems are up-to-date and there are no known vulnerabilities present in our applications.
>
> **IT Director**: We will give you internal access through an isolated VLAN within the IT department from which to perform your testing. There is a firewall with integrated IDS separating the datacenter networks from the corporate LAN, including the IT department. Within the datacenter, each server has a local firewall enabled. Internal DNS is provided through Microsoft Active Directory services, and external DNS is a Linux server located in a separate DMZ. External

access to the operations and logistics clusters is limited to employees connecting through VPN. No HTTP access is permitted into these clusters. Servers in these two clusters do not have internet access, except to obtain automatic software updates.

CEO: Because the systems that we want you to test are production systems, we hope to limit the disruptions caused by the testing to the minimum. We will give you access to a development Microsoft SQL Server system that is configured identically to the production system with a mirror of the database.

IT Director: Yes, I want to reinforce the need to keep disruptions to a minimum. We will give you a timeslot during our normal scheduled maintenance window to perform load testing and denial-of-service attack simulations. Our scheduled maintenance window is between 2:00 am and 6:00 am Friday, Saturday, and Sunday. Other non-disruptive tests can be run during normal business hours.

CEO: We are limiting the number of IT personnel who are aware of the testing. Only the IT staff directly responsible for monitoring the operations and logistics systems will be notified of when the testing will occur. We will provide a list of warehouse and operations staff email addresses, since we are worried that most ransomware and data breaches start with a successful social engineering attack. End users will not be made aware that testing is occurring. It is our expectation that the engagement will begin two weeks from the signing of the contract and the NDA. We will expect the final report within 60 days.

Your primary contacts for this engagement are the IT director, the warehouse manager, and the operations manager. Schedule a weekly update report and teleconference to inform them of the testing progress and interim findings.

Instructions

Part 1: Determine the Scope of the Engagement

Step 1: Analyze the information obtained from the client.

a. Review the information obtained in the interview with the client CEO and IT Director.
b. Identify points that influence the scope of the project and the rules of engagement.

Step 2: Complete the Scope Worksheet.

Use the information you identified from the interview transcript to complete the Scope Worksheet.

Scope Worksheet

To determine the scope and rules of engagement for the penetration testing project, answer the questions based on the results of your interview analysis.

1. What are the client's biggest security concerns? (Examples include disclosure of sensitive information, interruption of production processing, embarrassment due to website defacement, etc.)

Answer Area

<!----><!---->

2. What specific server clusters, network address ranges, or applications should be tested?

Answer Area

<!----><!---->

3. What specific server clusters, network address ranges, or applications should explicitly NOT be tested?

Answer Area

<!----><!---->

4. Will the test be performed against a live production environment or a test environment?

Answer Area

<!----><!---->

5. Will the penetration test include internal network testing? If so, how will access be obtained?

Answer Area

<!----><!---->

6. Are client/end-user systems included in the scope? If so, how may clients will be leveraged?

Answer Area

<!----><!---->

Is social engineering permitted? If so, is it limited?

Answer Area

<!----><!---->

Are Denial of Service and other disruptive attacks allowed? If so, are there limits to when disruptive tests can be performed?

Answer Area

<!----><!---->

Are there devices in place that may impact the results of a penetration test? If so, what are they?

Answer Area

<!----><!---->

7. Is testing wireless access part of this engagement?

Answer Area

<!----><!---->

8. Are web services included in the scope of testing?

Answer Area

<!----><!---->

9. Are employees aware of the testing and the timeframe when it will occur?

Answer Area

<!----><!---->

10. Where is the client data center physically located?

Answer Area

<!----><!---->

Part 2: Determine the Rules of Engagement

Step 1: Review the information on the Scope Worksheet.

Using the interview transcript and the information from the Scope Worksheet to fill out the table of Rules of Engagement Elements.

Rules of Engagement Element	Value
Testing Timeline	Answer Area <!----><!---->
Location of Testing	Answer Area <!----><!---->
Time windows for testing (times of day)	Answer Area <!----><!---->

Rules of Engagement Element	Value
Preferred method of communications	Answer Area <!----><!---->
Security controls that could potentially detect or prevent testing	Answer Area <!----><!---->
Sensitive data handling	Answer Area <!----><!---->
IP addresses or networks from which testing will originate	Answer Area <!----><!---->
Types of allowed or disallowed tests	Answer Area <!----><!---->
Client contacts	Answer Area <!----><!---->