Name: Kenneth Kimathi Kinoti

Student ID: 671497

Instructor: Dr. Dennis Mugambi

Lab: 2.2.9 - Pre-Engagement Scope and Planning

Course: MIS 6130

Title: Information Systems Security, Control and Audit

Lab 2.2.9 - Pre-Engagement Scope and Planning

Based on the scenario and interview with Nexus Plaza's CEO and IT Director, here is a completed Scope Worksheet for the penetration testing engagement:

A **scope worksheet** is a planning document that outlines what is to be tested during a penetration test. It defines the boundaries of the test to ensure all stakeholders (client and tester) understand what systems, applications, and environments are in-scope or out-of-scope.

The **rules of engagement** are a set of guidelines and limitations that govern how the penetration testing will be conducted. It ensures that the test is conducted ethically, legally, and without causing harm to systems or business operations.

Scope Worksheet

1. What are the client's biggest security concerns?

Answer:

1. Unauthorized access to production inventory and warehouse/shipping systems
2. A ransomware attack similar to their competitor's breach
3. Attackers escalating privileges from an end-user account to an administrator
4. Presence of unpatched software and known vulnerabilities in applications
5. Disruption of critical business operations

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

Answer:

1. Operations and Logistics server clusters

2. Warehouse and Shipping systems
3. Development Microsoft SQL Server (mirrored from production)
4. Internal client systems used by warehouse and inventory control staff
5. Remote access services (VPN, IPsec/SSL) for internal access

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

Answer:

The administration and Amazon Support server clusters, and the LAN IP address ranges.

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

Answer:

Primarily a live production environment

However, the SQL Server testing will use a development environment with a mirrored production database

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

Answer:

Yes, internal network testing is included

Access will be provided through an isolated VLAN within the IT department

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

Answer:

Yes, end-user systems in the warehouse and shipping departments are included

The testing will simulate an attacker starting from a compromised warehouse user account and computer

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

Answer:

Yes, social engineering is allowed

Limited to a list of warehouse and operations staff email addresses provided by the client

End users will not be informed about the testing

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

Answer:

Yes, DoS and load testing are allowed

Only permitted during the scheduled maintenance window:

2:00 am – 6:00 am on Friday, Saturday, and Sunday

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

Answer:

Yes

Firewall with integrated IDS separating the datacenter and corporate LAN

Local firewalls on each server

VPN access restrictions

No HTTP access to the Operations and Logistics clusters

Servers in these clusters have no internet access, except for automatic updates

10. Is testing wireless access part of this engagement?

Answer:

No, wireless access testing was not discussed or scoped in the engagement

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

Answer:

No, web services (especially those hosted on Amazon) are explicitly out of scope

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

Answer:

Only specific IT personnel directly responsible for operations and logistics are aware

End users will not be informed

Testing is expected to begin two weeks from contract and NDA signing

13. Where is the client data center physically located?

Answer:

Houston, Texas

Rules of Engagement Elements

Element	Details
1. Testing Timeline	Testing will begin two weeks after contract and NDA signing, with the final report due within 60 days.
2. Location of Testing	On-site at Nexus Plaza's Houston datacenter, using an isolated VLAN within the IT Department (LAN – VLAN 140, IP: 172.16.8.0/24)
3. Time Windows for Testing	- Disruptive testing (e.g., DoS/load tests): 2:00 AM – 6:00 AM, Friday–Sunday (maintenance window) - Non-disruptive testing: during normal business hours
4. Preferred Method of Communications	Weekly teleconferences and update reports to the primary contacts: IT Director, Warehouse Manager, Operations Manager.
5. Security Controls That Could Detect or Prevent Testing	- Firewall with IDS between corporate LAN and datacenter - Local firewalls on each server - VPN access controls - No HTTP access to Operations/Logistics clusters
6. Sensitive Data Handling	- Use of development SQL Server with mirrored production data - Minimize disruption to production systems
7. IP Addresses from Which Testing Will Originate	From the IT VLAN on the LAN: 172.16.8.0/24 (VLAN 140)

8. Types of Allowed or **Disallowed Tests**	**Allowed:** - Internal network penetration - Privilege escalation from end-user systems - Social engineering (via provided emails) - Vulnerability assessments - Load/DoS testing (during window) **Disallowed:** - Testing Amazon storefront clusters - Unauthorized disruption outside maintenance window
9. Client Contacts	- IT Director - Warehouse Manager - Operations Manager