Maxwell B. Antwi

Penetration Testing Scope and Plan

Hypothetical Scenario:

XYZ Logistics, a leading warehouse and shipping company, heavily relies on its production systems and Amazon integration for smooth operations. Due to increasing cybersecurity threats, the company seeks to assess its security posture and identify vulnerabilities that could disrupt its warehouse and logistics infrastructure. The primary concern is the potential for system shutdowns due to cyberattacks, as well as threats to their critical Amazon-dependent business model.

To address these risks, XYZ Logistics has engaged a security firm to conduct a comprehensive penetration test focusing on their operations and logistics servers, software, and Microsoft SQL Server applications. The security assessment will involve live production testing with controlled parameters, ensuring minimal disruption while identifying vulnerabilities. Internal network penetration testing limited social engineering, and scheduled denial-of-service testing are also included in the scope. This engagement will provide XYZ Logistics with an in-depth understanding of its security weaknesses and recommended mitigations to enhance overall cybersecurity resilience.

---

1. Objective: The goal of this penetration test is to identify vulnerabilities within the warehouse and shipping system that could lead to system shutdowns, as well as to ensure the security and availability of Amazon-related business operations.

2. Scope of Testing:

In-Scope Systems:

- Production systems, including warehouse and shipping infrastructure.
- Software and operating systems.
- Operation and logistics servers:
    - IP address range: 172.26.0.0/21
    - IP address range: 172.27.0.0/21
    - Microsoft SQL Server applications.

Out-of-Scope Systems:

- Datacenter server containing Amazon services:
    - IP address: 172.25.0.0/16
    - Subnet mask: 255.255.255.192
- HTTP access within operations and logistics clusters.
- Wireless network testing.
- Web services.
- Client/end-user systems.

3. Testing Environment:

- Majority of tests will be conducted in a live production environment.

- Intrusive SQL Server testing will be limited to the development environment, which mirrors production.

4. Internal Network Testing:

- Internal network testing will be conducted with access provided through an isolated VLAN within the IT department.

5. Social Engineering:

- Limited social engineering permitted on designated email addresses only.

6. Denial of Service (DoS) and Disruptive Testing:

- Allowed only between 2:00 AM and 6:00 AM on Friday, Saturday, and Sunday.

7. Security Devices Impacting Testing:

- Firewalls and Intrusion Detection Systems (IDS) in place.

8. Physical Location of Data Center:

- Houston Facility.

9. Rules of Engagement:

Testing Timeline:

- Start Date: Two weeks from authorization.

- Final Report: Within 60 days.

Testing Location:

- Houston Facility.

Time Window for Testing:

- Non-invasive testing during business hours.
- Invasive testing (e.g., DoS and load testing) only between 2 AM and 6 AM (Friday to Sunday).

Communication Method:

- Weekly status updates.
- Final comprehensive report.

Security Controls in Place:

- Firewalls and IDS systems.

Sensitive Data Handling:

- Compliance with a signed Non-Disclosure Agreement (NDA).

Testing Source Locations:

- Internal IT VLAN.

Allowed and Disallowed Tests:

- Allowed:
  - Operations and logistics server penetration testing.
  - SQL Server testing (limited to development environment).
  - Social engineering (limited to provided emails).
- Disallowed:

    - Testing on Amazon-related datacenter.
    - HTTP access testing in the operations/logistics clusters.
    - Wireless security testing.
    - Web services security testing.

Client Contacts:

- Warehouse Manager.
- IT Director.
- Operations Manager.