MODULE-2

NETWORK SECURITY

Vulnerability Audit and Assessment - Baseline Analysis and Plan

MS-CYBERSECURITY | AMIT PAHUJA

Contents

Why Vulnerability Assessment?

Information about potential security flaws in a company's infrastructure can be gleaned from a vulnerability assessment. In addition, it offers guidance on how to weigh the dangers posed by those flaws.

The purpose of this exercise is to locate the potential entry points into a computer system that an adversary could use for malicious purposes.

(Vulnerability Assessment, N.D)

Scope of the vulnerability assessment

- Scope of the testing must involve:
    - All applicable Risk Owners - describes any particular concerns that may have an impact on testing, such as the necessity for out-of-hours testing, any vital systems requiring special handling, etc.
    - Educated technical personnel of the target system (System owner(s)) - Outlines the technical boundaries of the organization's IT estate.
    - Representation from the penetration testing team — Identifies the comprehensive testing that will provide a comprehensive view of the vulnerability state.
- Plan of action:
    - The output of scoping must be a document containing the following information:
        - Technical boundaries of the test
        - Types of tests
        - Timeframe and amount of effort – typically expressed in terms of resource days
        - Testing plan must satisfy Any compliance criteria requirements
        - Any Reporting requirements, such as CVSS scores inclusion
        - Any time limits on testing or reporting
- Changing Scope
    - The testing team may discover extraneous systems or components that aren't technically part of the system scope under test but could nevertheless compromise its safety if tested
- Reporting – Following should be included in the Test report:
    - All Security issues
    - Risk Level against each vulnerability
    - Method of resolving each issue
    - Opinion on the accuracy of the organization’s vulnerability assessment
    - Suggestions / advice on how to improve the internal vulnerability assessment process

- Common Vulnerability Scoring System (CVSS), that identifies the severity of the vulnerability, must be included when rating vulnerabilities.
    - Reports are required to state the risk level as HIGH, MEDIUM, LOW or INFORMATIONAL

(Penetration Testing, 2022)

Potential security challenges - generic & business specific

Here is the list of potential security vulnerabilities/concerns including, but not limited to, OWASP Top10:

- Financial Fraud
    - Fake Return and Refund
- Phishing
- DoS/DDoS
- Man-In-The-Middle (MITM)
- Broken Access Control
- Cryptographic failures
- Injections
- Insecure design
- Security misconfigurations
- Vulnerable and outdated components
- Identification and authentication failures
- Software and data integrity failures
- Security logging and monitoring failures
- Server-side request forgery (SSRF)
- Exploitation of known vulnerabilities – e.g. XSS

(OWASP TOP 10, N.D)

Security Assessment Methodology and list of Tools

Four distinct steps are used as part of the best practice assessment methodology:

1. **Reconnaissance**- To identify hosts, networks and users of interest
    a. Open Sources (Web Search Engines. **WHOIS databases** and DNS servers) can be used to map the target environment
    b. Useful pieces of information can be gathered – Public network blocks and internal IP addresses which can be used during vulnerability

scanning & penetration testing phases to identify exploitable vulnerabilities in the target.

c. Extracting User Details (Usernames, Email Addresses and phone numbers) through further reconnaissance

2. **Vulnerability Scanning** – To identify potentially exploitable stuff
    a. Network Scanning
        i. Once IP blocks of interest are identified during reconnaissance, bulk scanning is performed to identify accessible network services which can be exploited later for specific goals (Information Leak, Remote code execution or DoS)
        ii. Scanning Tools like **Qualys Guard, NESSUS, RAPID7 Nexpose and NMAP** scans the network for known vulnerabilities. NMAP to perform host discovery and port scans. Nessus/Qualys to perform bulk scanning
    b. Web App Scanning
        i. OWASP top 10 defines the list of common web vulnerabilities. Tools that can reliably test for such flaws include **Burp Suite, IBM Security AppScan, HP WebInspect, and Acunetix**.

3. **Investigation of Vulnerabilities** – For further identification / probing
    a. To effectively report vulnerabilities, one should know both the private and public domains
    b. Public Vulnerability sources
        i. NIST
        ii. The HackerOne Internet Bug Bounty
        iii. Offensive-Security Exploit Database
        iv. SecurityFocus
    c. Private Vulnerability sources
        i. Exodus Intelligence, Netragard, ReVuln etc. are the organizations known to provide details of unpatched bugs

4. **Vulnerabilities Exploitation** –
    a. Vulnerabilities found in exposed logic can be exploited for specific goals – Remote code execution, privileged network access, obtain sensitive information etc.
    b. Popular Exploitation frameworks are as follows:
        i. Rapid7 Metasploit
        ii. CORE Impact
        iii. Immunity CANVAS

Kali Linux is a penetration testing distribution that can be run easily within a virtualized environment and contains a lot of utilities including **Metasploit, NMAP, BurpSuite and Nikto.**

(Network Security Assessment, Chris McNab)

Most devices take around 30-40mins for scanning but can slow down to hours if the device being scanned is busy or the network is congested. If scanning can occur within a specific time window (like after business hours), scan strategy needs to be adjusted – (a) Add additional scanners (b) Set active scans to rollover.

REFERENCES

1. Vulnerability Assessment [N.D.]
   https://csrc.nist.gov/glossary/term/vulnerability_assessment

2. Penetration Testing [2022]
   https://www.ncsc.gov.uk/pdfs/guidance/penetration-testing.pdf

3. OWASP TOP 10 [N.D.]
   https://owasp.org/www-project-top-ten/

4. Network Security Assessment, Chris McNab
   https://essexonline.vitalsource.com/reader/books/9781491911051/epubcfi/6/40[%3Bvnd.vst.idref%3Dchapter-idm139659169389808]!/4/2/2[assessing_data_stores]/2/3:15[ta%20%2CSto