**Network Vulnerability Assessment**

# Introduction

## Purpose

The Vulnerability Assessment & Penetration Testing Audit provides inputs to the stakeholders to assess the issues/ bottlenecks, if any, in terms of existing weaknesses and loopholes. The tests were carried out assuming the identity of an attacker or a user with malicious intent. At the same time due care was taken not to harm the device.

The purpose of the Vulnerability Assessment & Penetration Testing Audit is to determine the security vulnerabilities in the Desktops and Firewall running on the Network specified in the scope. The tests were carried out assuming the identity of an Internal Threats or internal users with malicious intent. At the same time due care was taken not to harm the Desktops and Firewall.

## Scope of Work for VAPT

| **S. No.** | **Review Area** | **Scope Area** | **Scope Item** |
| --- | --- | --- | --- |
| 1 | **Technical Review – Internal IT Infrastructure Security Audit (VA)** | Security Architecture Review of Metasploitable Infrastructure, Vulnerability Assessment of Servers, Network Devices and user systems | * Network and Security Architecture Review * Vulnerability Assessment including configuration review of Critical Systems, Servers and Network devices. |
| 2 | **Technical Review - Network PT** | Penetration Testing to test the security robustness of Metasploitable Perimeter devices and resources accessible from Public Network | * Penetration Testing of No. of Public IP’s provided |

## Vulnerability Rating Classification

The significant issues are given in this section, the Executive summary. These list the security flaws that are of major concern. Vulnerabilities have been given a Severity rating of High, Medium or Low based on the risk they may pose. The basis of giving the severity rating is as described below:

**Individual Vulnerability Rating** –Individual vulnerability rating is based on the following;

|  |  |
| --- | --- |
| **Risk Level** | **Description** |
| **High** | **High Risk** vulnerability can be exploited by a malicious user to get full administrative access to the application or its primary operating system. |
| **Medium** | **Medium Risk** vulnerability discloses the information about the Systems and network components and its underlying communications which can be exploited by an attacker in conjunction with another vulnerability to gain administrative access to the application or to the primary operating system. |
| **Low** | **Low Risk** vulnerability can result in inventory of vital information held by or about the systems and network components or its primary operating system. |
| **Improvement Opportunity** | Suggested improvements which are not non-compliances but would help in further enhancements. |

### Methodology

Vulnerability/Security Assessment follows the concept of assessing the security of Metasploitable from an internal hacker's perspective. However, Vulnerability/Security Assessment involves more than finding out the weaknesses of internal network. The security holes discovered during the audit are documented; discovered vulnerabilities are prioritized according to risk, and recommendations given for fixing the vulnerabilities.

This exercise was carried out from inside the network, and focused on the following:

* Configurations of Router and Servers.
* Identify system-level vulnerabilities such as file permissions, account properties, registry settings, etc.
* OS patch level update.
* Antivirus Software configuration and Updating Schedule

The methodology adopted for Vulnerability Assessment consisted of two phases;

* Network-based testing
* Detailed manual compliance testing

Define

**Select the Server and Network devices of Network to be tested**

* Number of IP’s to be tested
* Testing Strategy

Conduct Evaluation

**Conduct Vulnerability Assessment as per below mentioned (Section 3.1.2.1) Guidelines**

* Scan Private IPs addresses of using automated vulnerability scanning tool
* Manually check servers Network devices configuration for policy
* compliance

Analysis

**Classify vulnerabilities according to the Risk Level**

* Analyze findings
* Analyze the threat due to the vulnerability and give the risk rating
* Classify vulnerabilities according to the Risk Level

Summary Conclusion

**Conclusion**

* Summarize Conclusion

Recommend

**Prepare Report**

* Prepare detailed Technical findings Report
* Suggest general recommendations to plug the vulnerability

Plan

**Foot Printing / Gather information of servers and network devices**

* Identify Private IPs to be tested
* Identify the location from where Vulnerability Assessment to be conduct

k

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S. No** | **Vulnerability** | **Severity** | **Vulnerable Hosts** | **Vulnerability Implication/Threat** | **Recommendation** |
| 1 | Administrator Account was not rename/disabled. | **Medium** | 192.168.40.131 | Malicious or unauthorized users can try to break the password using automated tools for default windows accounts. | Rename or disabled the default Administrator account as this default account are known to everyone. |
| 2 | Digitally sign communication (always) is set to 'Disable' all the system. | **Medium** | Signing is not required on the remote SMB server. An unauthenticated remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server. | Enforce message signing in the host's configuration. On windows, this is found in the policy setting Microsoft network server: Digitally sign communication (always). |
| 3 | Some servers having shares with the effective share permission as “Every – Full Control”. | **Low** | Malicious or unauthorized users can alter or misuse the valuable data or information. | Data should be share with minimum permission to only authorized users. Data folders should also have NTFS permissions applied to secure data from unauthorized local users. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **S. No** | **Vulnerability** | **Severity** | **Ports** | **Vulnerable Hosts** | **Vulnerability Implication/Threat** | **Recommendation** |
| 4 | The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. | **High** | 443 | 192.168.40.131 | These versions of SSL are affected by several cryptographic flaws. | Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead. |
| 5 | The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm | **High** | 443 | An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service. | Contact the Certificate Authority to have the SSL certificate reissued. |
| 6 | The remote host supports the use of SSL ciphers that offer medium strength encryption. | **High** | 443 | The remote host supports the use of SSL ciphers that offer medium strength encryption. Tool regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. | Reconfigure the affected application if possible to avoid use of medium strength ciphers. |
| 7 | The remote host is running a Telnet server over an unencrypted channel. | **Medium** | 23 | Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server. | Disable the Telnet service and use SSH instead. |
| 8 | The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. | **Medium** | 5057 | This may allow an attacker to recover the plaintext message from the ciphertext. | Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0. |