|  |
| --- |
| **Network Vulnerable Testing.**  Group 6th - Computer Networking Project  **Group Members:**  4518 – Vedanshu Kocharekar  4519 – Prathamesh Kulkarni  4520 – Ritik Lohiya  4545 – Ved Gandhi |

## **What Is A Network Vulnerability Testing?**

A network vulnerability assessment is a network security practice that helps organizations to identify, quantify and prioritize the risks and vulnerabilities in their network infrastructure. It also helps your dev teams to fix those vulnerabilities.

In other words, network vulnerability assessment is all about knowing your weaknesses before someone else does.

## 

## There are many factors to consider when conducting a network vulnerability assessment, but some of the most important aspects include:

## Identifying all network systems and devices in your network infrastructure

## Determining how these systems and devices are interconnected

## Analyzing system configurations and installed software for known vulnerabilities

## Scanning for open ports and services that could be exploited

## Testing for weak passwords or other authentication issues

**Why is Network Vulnerability Assessment Necessary?**

As we’ve already discussed, network security breaches are becoming increasingly common and costly. And to prevent such breaches, it is necessary to know the potential security vulnerabilities in the network infrastructure.

Conducting a network vulnerability assessment helps organizations to detect any kind of weaknesses in their system before attackers do. It also provides detailed information on how to fix those vulnerabilities with priority.

Not only that but network vulnerability assessment is also required by many compliance standards such as PCI-DSS, HIPAA, SOX, ISO, etc.

**Most Common Network Vulnerabilities**

**Unpatched software and operating systems**

Unpatched software and operating systems are one of the most common causes of network vulnerabilities. Hackers can exploit these vulnerabilities in the network to further gain access to sensitive data or launch attacks on other organizations using the infected network devices (botnet).

**Weak passwords**

Weak passwords are another major cause of network vulnerabilities. Hackers can use brute force attacks to guess weak passwords and gain access to sensitive data.

**Open ports and services**

Open ports and services are also a critical element to look at when you’re planning to secure your network. An attacker can bypass your security controls via open ports and can further harm your network systems by gaining access to it.

**Insecure Wireless Networks**

One of the most common types of vulnerabilities is an unsecured wireless network. Hackers can easily exploit these networks to gain access to sensitive data or launch attacks on other systems.

**Lack of encryption**

Another common vulnerability is a lack of encryption. This leaves any data vulnerable to interception by hackers.

## **Best Practices to Prevent Network Compromise or Data Breach**

Now that we’ve discussed some of the most common network vulnerabilities, let’s take a look at some best practices to prevent them.

**1. Patch systems and software regularly**

One of the best ways to prevent network vulnerabilities is to patch or update systems and software on a regular basis. The updated software and systems will help reduce vulnerability exploitation risks as well as prevent you from attacks that could be performed on vulnerable/older versions of systems or software.

### **2. Use strong passwords**

Another important practice is to use strong passwords for your network access control and admin areas in your networking devices. Strong passwords such as passphrases are difficult to guess and they can easily prevent any unauthorized access using any automated tools such as brute-forcing.

### **3. Use two-factor (2FA) authentication for access**

Enabling two-factor authentication for yourself and your team members can be very effective to improve the security posture of your organization. The 2FA requires users to provide two forms of identification, such as a password and a fingerprint or an access card before they can gain access to sensitive data.

### **4. Encrypt your data**

Enabling encryption for your data at rest and in transition is another best practice for preventing network and data breaches. The encryption allows organizations to transform their readable data into an encrypted data format. This can stop hacking attacks because the data is now encrypted.

### **5. Implement user access control to secure sensitive data**

Implementation of proper user authentication and giving user-level or admin-level privileges to only authorized and trusted users can secure the sensitive data of your and your customers from falling into the hands of hackers. For example, only allowing administrators to access certain areas of the network.

### 

### **6. Monitor network activity**

There are dedicated companies in the cybersecurity industry that only offer network monitoring solutions. And by knowing this you can guess how important it is to regularly monitor your network in real-time. Network monitoring is as important as any other network security control. It allows an organization to see any unauthorized intrusion and incoming or outgoing network attack traffic. This helps to take immediate actions to remedy or prevent the intrusion.

### **7. Use network security solutions**

There are many different network security solutions available that can help to protect against attacks. These solutions can include firewalls, intrusion detection systems, antivirus software, zero-trust network security, DDoS mitigation solutions, etc.

### **8. Perform regular VAPT for your network devices**

Performing periodic vulnerability assessments and [pentest](https://www.getastra.com/blog/security-audit/penetration-testing/) for your organizations’ network assets can assist with recognizing any security weakness in the network that could be taken advantage of by hackers. These tests can likewise assist with the decision of implementing network security practices to patch security weaknesses before these are exploited in the wild by hackers.

One of the best tools for checking network vulnerability is nmap

**Nmap** (**Network Mapper**) is a [network scanner](https://en.wikipedia.org/wiki/Network_scanner) created by [Gordon Lyon](https://en.wikipedia.org/wiki/Gordon_Lyon) (also known by his [pseudonym](https://en.wikipedia.org/wiki/Pseudonym) *Fyodor Vaskovich*) Nmap is used to discover [hosts](https://en.wikipedia.org/wiki/Host_(network)) and [services](https://en.wikipedia.org/wiki/Web_service) on a [computer network](https://en.wikipedia.org/wiki/Computer_network) by sending [packets](https://en.wikipedia.org/wiki/Network_packet) and analyzing the responses .Nmap provides a number of features for probing computer networks, including host discovery and service and [operating system](https://en.wikipedia.org/wiki/Operating_system) detection.

Features of Nmap:-

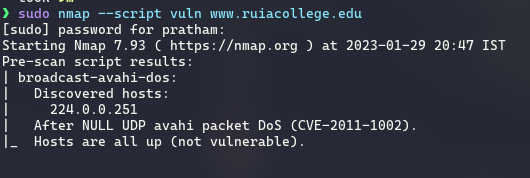
* Host discovery – Identifying hosts on a network. For example, listing the hosts that respond to [TCP](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) and/or [ICMP](https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol) requests or have a particular port open.
* [Port scanning](https://en.wikipedia.org/wiki/Port_scanner) – Enumerating the open [ports](https://en.wikipedia.org/wiki/TCP_and_UDP_port) on target hosts.
* Version detection – Interrogating network services on remote devices to determine application name and version number.
* [TCP/IP stack fingerprinting](https://en.wikipedia.org/wiki/TCP/IP_stack_fingerprinting) – Determining the [operating system](https://en.wikipedia.org/wiki/Operating_system) and hardware characteristics of network devices based on observations of network activity of said devices.
* Scriptable interaction with the target – using Nmap Scripting Engine (NSE) and [Lua](https://en.wikipedia.org/wiki/Lua_(programming_language)) programming language.

Uses of Nmap:-

* Auditing the security of a device or [firewall](https://en.wikipedia.org/wiki/Firewall_(computing)) by identifying the network connections which can be made to, or through it.
* Identifying open ports on a target host in preparation for auditing.
* Network inventory, [network mapping](https://en.wikipedia.org/wiki/Network_mapping), maintenance and asset management.
* Auditing the security of a network by identifying new servers.
* Generating traffic to hosts on a network, response analysis and response time measurement.
* Finding and [exploiting](https://en.wikipedia.org/wiki/Exploit_(computer_security)) vulnerabilities in a network.
* [DNS](https://en.wikipedia.org/wiki/Domain_Name_System) queries and [subdomain](https://en.wikipedia.org/wiki/Subdomain) search

The vuln script is used to scan for the vulnerability

As you see the below site has no vulnerability



This network has some vulnerabilities

