Tue Jun 4 10:11:02 2024

Vulnerability Scan

Report

prepared by
Dabbaghi walid

Overview

1 Executive Summary

Vulnerability scans were conducted on selected servers, networks, websites, and applications. This report contains the discovered potential risks from these scans. Risks have been classified into categories according to the level of threat and degree of potential harm they may pose.

1.1 Total Risks

Below is the total number of risks found by severity. High risks are the most severe and should be evaluated first. An accepted risk is one which has been manually reviewed and classified as acceptable to not fix at this time, such as afalse positive or an intentional part of the system's architecture.

High: 0 Medium: 9 Low: 14 Accepted: 0

1.2 Report Coverage

This report includes findings for 1 target that were scanned. Each target is a single URL, IP address, or fully qualified domain name (FQDN).

Vulnerability Categories

Number of ports: 23

Open TCP Ports

2 Risks By Target

This section contains the vulnerability findings for each target that was scanned. Prioritize the most vulnerable assets first.

2.1 Targets Summary

The total number of risks found for each target, by severity.

Target

Adresse: 192.168.58.131, Nom d'hôte: N/A

High: 0 Medium: 9 Low: 14 Accepted: 0

2.2 Target Breakdowns

The risks discovered for each target.

Target

Adresse: 192.168.58.131, Nom d'hôte: N/A

Total Risks:

High: 0 Medium: 9 Low: 14 Accepted: 0

Open Ports

Open tcp Port: 21

Open tcp Port: 22

Open tcp Port: 23

Open tcp Port: 25

Open tcp Port: 53

Open tcp Port: 80

Open tcp Port: 111

Open tcp Port: 139

Open tcp Port: 445

Open tcp Port: 512

Open tcp Port: 513

Open tcp Port: 514

Open tcp Port: 1099

Open tcp Port: 1524

Open tcp Port: 2049

Open tcp Port: 2121

Open tcp Port: 3306

Open tcp Port: 5432

Open tcp Port: 5900

Open tcp Port: 6000

Open tcp Port: 6667

Open tcp Port: 8009

Open tcp Port: 8180

3 Open TCP Ports

The NMAP TCP port scan discovers open TCP ports with a complete scan of ports 0 to 65535.

3.1 Total Risks

Total number of risks found by severity.

High: 0 Medium: 9 Low: 14 Accepted: 0

3.2 Risks Breakdown

Summary list of all detected risks.

Open Ports(Title):

Open tcp Port: 21

Open tcp Port: 22

Open tcp Port: 23

Open tcp Port: 25

Open tcp Port: 53

Open tcp Port: 80

Open tcp Port: 111

Open tcp Port: 139

Open tcp Port: 445

Open tcp Port: 512

Open tcp Port: 513

Open tcp Port: 514

Open tcp Port: 1099

Open tcp Port: 1524

Open tcp Port: 2049

Open tcp Port: 2121

Open tcp Port: 3306

Open tcp Port: 5432

Open tcp Port: 5900

Open tcp Port: 6000

Open tcp Port: 6667

Open tcp Port: 8009

Open tcp Port: 8180

3.3 Full Risk Details

Detailed information about each risk found by the scan.

Open Port: Medium Ports: 21, 22, 23, 25, 139, 445, 1099, 1524, 5432 meduim

Description

An open port may be an expected configuration. For example, web servers use port 80 to serve websites over http and port 443 to serve websites over https. For a list of commonly used ports see https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers. An unexpected open port could give unintended access to applications, data, and private networks. Open ports can also be dangerous when expected services are out of date and exploited through security vulnerabilities.

Vulnerable Target

Adresse: 192.168.58.131, Nom d'hôte: N/A

Open Port: Low Ports: 53, 80, 111, 512, 513, 514, 2049, 2121, 3306, 5900, 6000, 6667, 8009, 8180 Low

Description

An open port may be an expected configuration. For example, web servers use port 80 to serve websites over http and port 443 to serve websites over https. For a list of commonly used ports see https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers.
An unexpected open port could give unintended access to applications, data, and private networks. Open ports can also be dangerous when expected services are out of date and exploited through security vulnerabilities.

Vulnerable Target

Adresse: 192.168.58.131, Nom d'hôte: N/A

4 Glossary

Accepted Risk

An accepted risk is one which has been manually reviewed and classified as acceptable to not fix at this time, such as a false positive or an intentional part of the system's architecture.

Fully Qualified Domain Name (FQDN)

A fully qualified domain name is a complete domain name for a specific website or service on the internet. This includes not only the website or service name, but also the top-level domain name, such as .com, .org, .net, etc. For example, 'www.example.com' is an FQDN.

Open TCP Ports

The NMAP TCP port scan discovers open TCP ports with a complete scan of ports 0 to 65535.

Risk

A risk is a finding from a vulnerability scan. Each risk is a potential security issue that needs review. Risks are assigned a threat level which represents the potential severity.

Target

A target represents target is a single URL, IP address, or fully qualified domain name (FQDN) that was scanned.

Threat Level

The threat level represents the estimated potential severity of a particular risk. Threat level is divided into 4 categories: High, Medium, Low and Accepted.

Threat Level

The threat level represents the estimated potential severity of a particular risk. Threat level is divided into 4 categories:High, Medium, Low and Accepted.

CVSS Score

The CVSS 3.0 score is a global standard for evaluating vulnerabilities with a 0 to 10 scale. CVSS maps to threat levels: 0.1 - 4.9 = Low, 5 - 8.5 = Medium, 8.6 - 10 = High