Chameleon Security

NESSUS VULNERABILITY ASSESSMENT REPORT

Vulnerability Assessment

https://react-test-6najyje5cq-uc.a.run.app/

Brock Alexiadis

TABLE OF CONTENTS

Introduction:

Background

Nessus is an effective tool for evaluating the security of networks and computer systems. It functions similarly to a digital security guard, looking for any vulnerabilities that hackers might use to exploit the system. Nessus has gained a lot of traction among security professionals who wish to ensure that their systems are safe from online threats. This report outlines our findings from using Nessus to scan the Chameleon website for vulnerabilities. It will point out any vulnerabilities in the system and offer recommendations for strengthening its security.

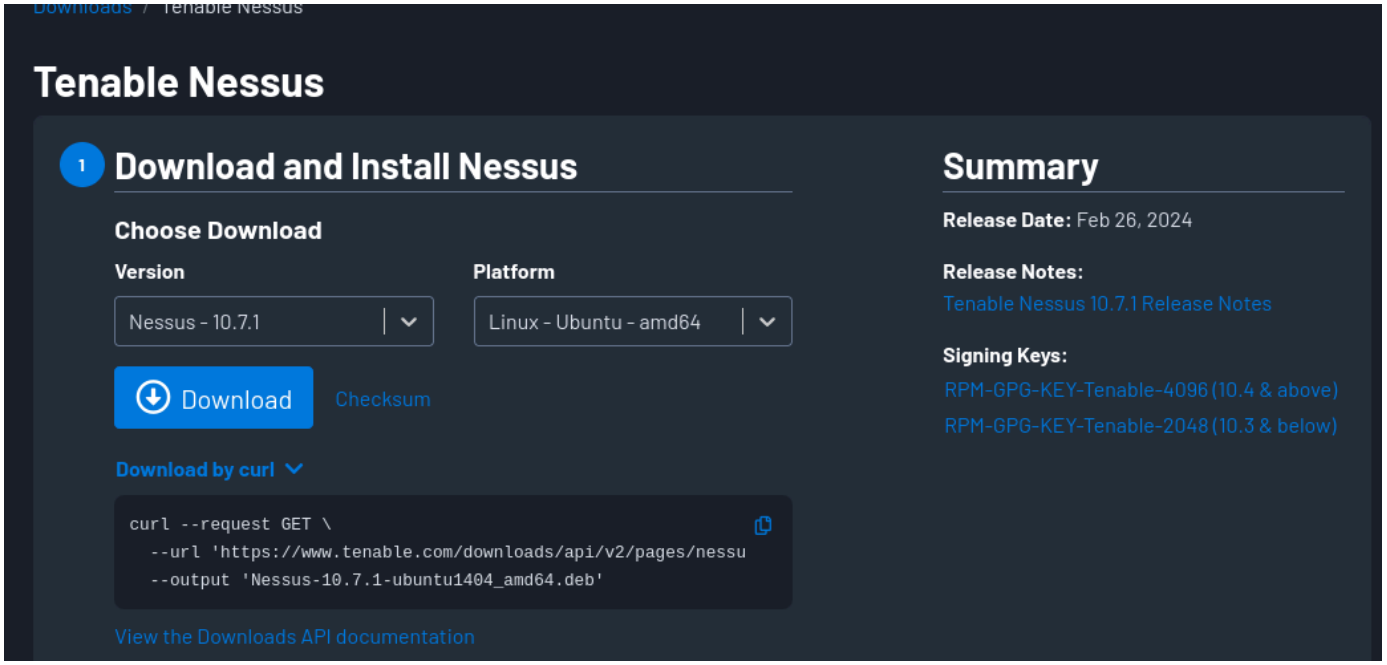
Objectives

Identifying any potential flaws or vulnerabilities in the target system or network infrastructure is the first goal of this vulnerability assessment using Nessus. The second goal is to offer practical advice and suggestions for improving overall security posture and mitigating these vulnerabilities. Through a methodical process of searching for established weaknesses and evaluating the results, the evaluation seeks to empower interested parties to make knowledgeable choices about risk reduction tactics and resource distribution to protect against possible online attacks.

Methodology

Downloading Nessus

before we can conduct the scan, we must first download and set up the tools we are going to use. to download nessus we go to their website (link) and download the linux version as we are using kali linux.



we are installing by curl so copy the curl command and run it into a kali command prompt

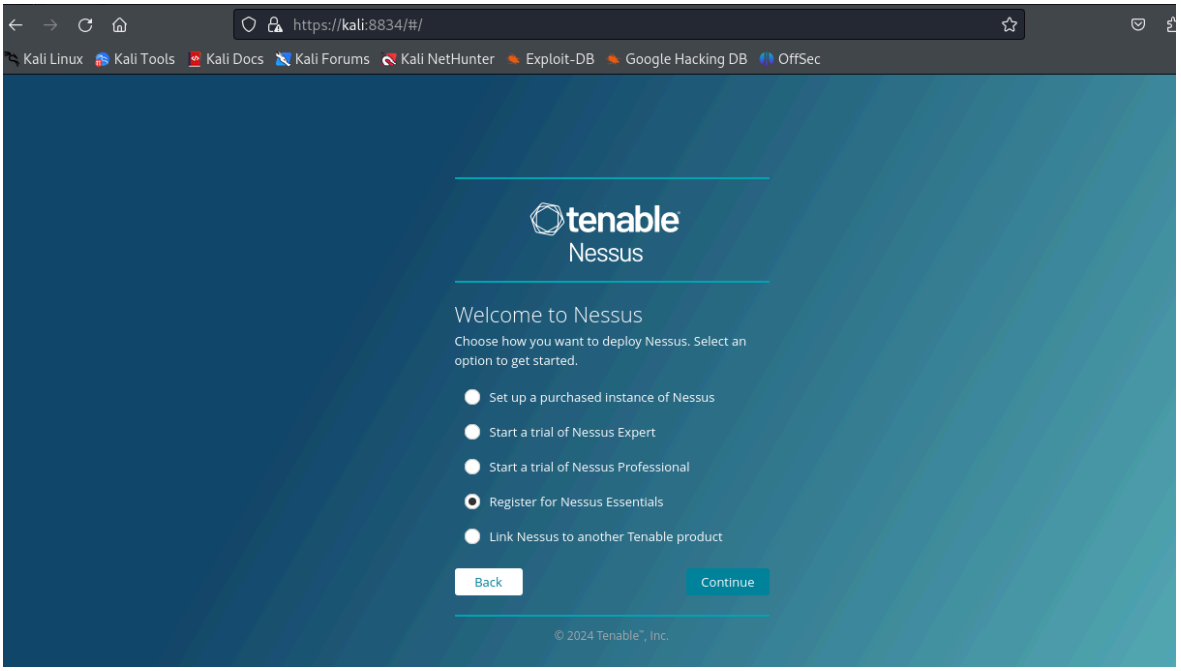
```
┌──(kali㉿kali)-[~]
└─$ curl --request GET \
  --url 'https://www.tenable.com/downloads/api/v2/pages/nessus/files/Nessus-10.7.1-ubuntu1404_amd64.deb' \
  --output 'Nessus-10.7.1-ubuntu1404_amd64.deb'
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
100 2989k    0 2989k    0     0  3217k      0 --:--:-- --:--:-- --:--:-- 3217
100 8028k    0 8028k    0     0  4164k      0 --:--:--  0:00:01 --:--:-- 4164
100 12.7M    0 12.7M    0     0  4463k      0 --:--:--  0:00:02 --:--:-- 4464
100 17.6M    0 17.6M    0     0  4610k      0 --:--:--  0:00:03 --:--:-- 4610
100 22.6M    0 22.6M    0     0  4697k      0 --:--:--  0:00:04 --:--:-- 4697
100 27.5M    0 27.5M    0     0  4754k      0 --:--:--  0:00:05 --:--:-- 5040
100 32.4M    0 32.4M    0     0  4792k      0 --:--:--  0:00:06 --:--:-- 5034
100 37.3M    0 37.3M    0     0  4822k      0 --:--:--  0:00:07 --:--:-- 5031
100 42.1M    0 42.1M    0     0  4833k      0 --:--:--  0:00:08 --:--:-- 5008
100 47.0M    0 47.0M    0     0  4855k      0 --:--:--  0:00:09 --:--:-- 5012
100 50.8M    0 50.8M    0     0  4766k      0 --:--:--  0:00:10 --:--:-- 4781
100 55.7M    0 55.7M    0     0  4790k      0 --:--:--  0:00:11 --:--:-- 4786
100 60.5M    0 60.5M    0     0  4788k      0 --:--:--  0:00:12 --:--:-- 4734
100 65.5M    0 65.5M    0     0  4819k      0 --:--:--  0:00:13 --:--:-- 4795
100 65.5M    0 65.5M    0     0  4819k      0 --:--:--  0:00:13 --:--:-- 4730
k
```

now run the command ‘dpkg -i Nessus-10.7.1-ubuntu1404_amd64.deb’ to complete the installation.

NOTE: running this command requires root privilege so use ‘sudo’ if needed

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# dpkg -i Nessus-10.7.1-ubuntu1404_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 404653 files and directories currently installed.)
Preparing to unpack Nessus-10.7.1-ubuntu1404_amd64.deb ...
Unpacking nessus (10.7.1) ...
Setting up nessus (10.7.1) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
```

start nessus using the command ‘/bin/systemctl start nessusd.service’ and go to the website ‘https://kali:8834/’ to register your nessus



we are registering for nessus essentials it will ask for you to create an account and email you an activation code once you enter the code the initial set up is complete

now nessus is installed on our kali machine and we can begin the vulnerability scan

Scanning New Chameleon MOP Website With Nessus

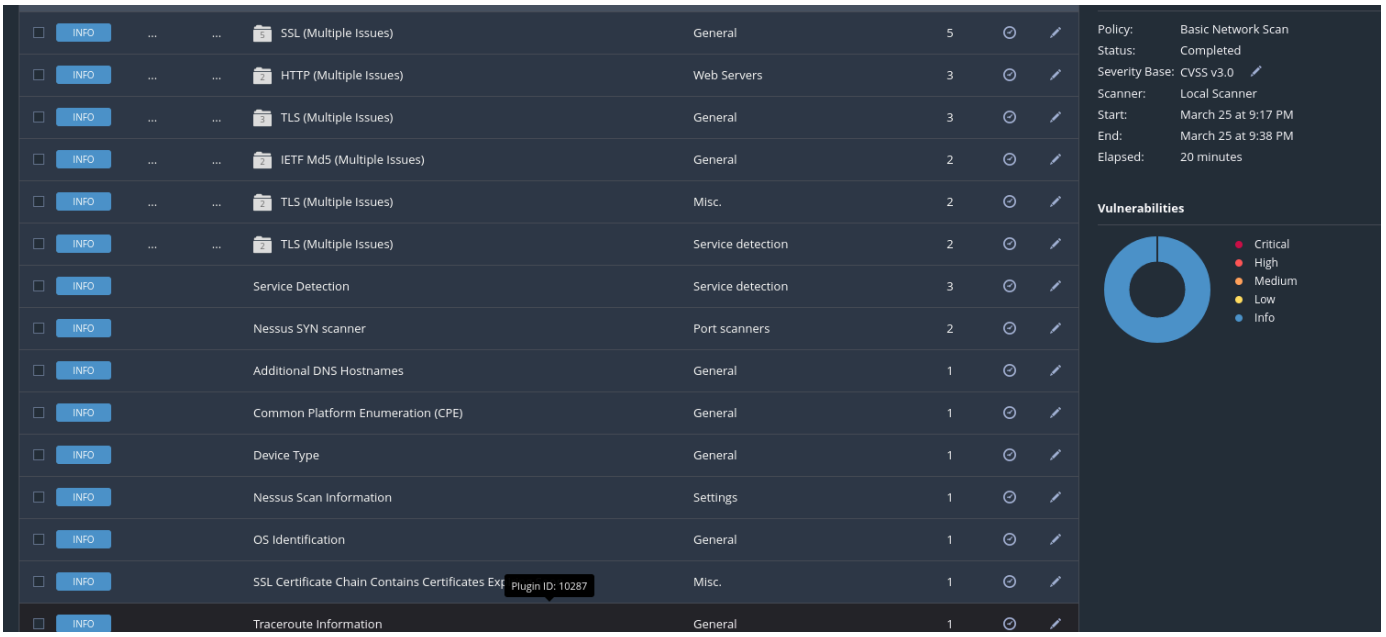
Overview

First we need to find the ip address of our scan target(the new MOP website). we can simply do this by pinging the url in the command prompt. The ip is found to be 216.239.36.53

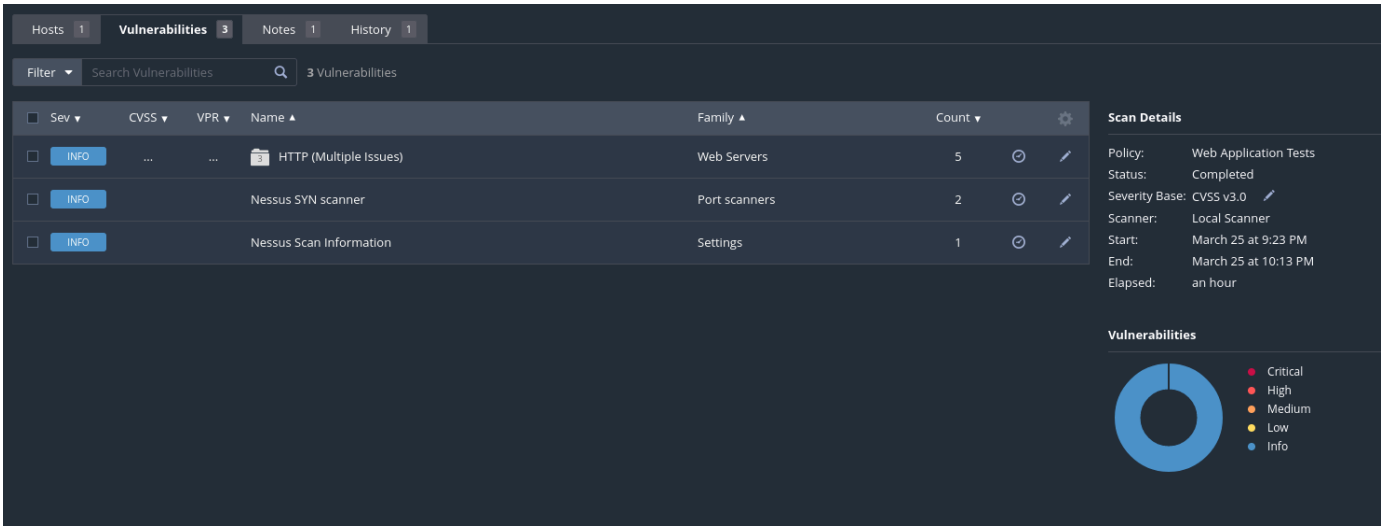
We can now use this ip to scan the MOP website. for this report we will be doing 2 scans, a basic network scan, and a web application scan

setting up the scans is very easy you simply click new scan, select the type of scan ou want and enter the target ip, and wait for the scan to complete

Basic Network Scan



Web Application Scan



Findings:

As can be seen in both screenshots there are actually no vulnerabilities in categories from low to critical, only in info. What this means is that through various probes on the MOP site, an attacker may pick up information that could help them with future attacks. i will list some of the examples below and their risk factor as well as solutions if any:

Device Type

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Risk Factor

None

Nessus Scan Information

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.

- The type of scanner (Nessus or Nessus Home).

- The version of the Nessus Engine.

- The port scanner(s) used.

- The port range scanned.

- The ping round trip time

- Whether credentialed or third-party patch management checks are possible.

- Whether the display of superseded patches is enabled

- The date of the scan.

- The duration of the scan.

- The number of hosts scanned in parallel.

- The number of checks done in parallel.

Risk Factor

None

Nessus SYN Scanner

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Risk Factor

None

Solution

Protect your target with an IP filter.

Common Platform Enumeration (CPE)

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Risk Factor

None

Service Detection

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Risk Factor

None

OS Identification

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Risk Factor

None

SSL Certificate Chain Contains Certificates Expiring Soon

Description

The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.

Solution

Renew any soon to expire SSL certificates.

Traceroute Information

Description

Makes a traceroute to the remote host.

Risk Factor

None

Recommendations:

because the issues found aren't actually vulnerabilities it is just general information that can be found about the website and servers there isn't many solutions. The only actual solutions are to renew SSL certificates and protect the site with an IP filter.

Conclusion:

An extensive summary of the environment's security posture was obtained from the Nessus scan that was carried out on 26/03/2024. The scan results show that the infrastructure is strong and well-maintained overall, with no significant weaknesses found. Most of the issues that were found were small ones, like alerts about SSL certificates expiring and informative discoveries about different kinds of systems and their configurations.

Despite the fact that the assessment did not reveal any security vulnerabilities, network security must be maintained by being proactive and watchful. In order to reduce potential risks and guarantee the systems' continuous availability and integrity, regular monitoring, patch management, and adherence to security best practices are essential.