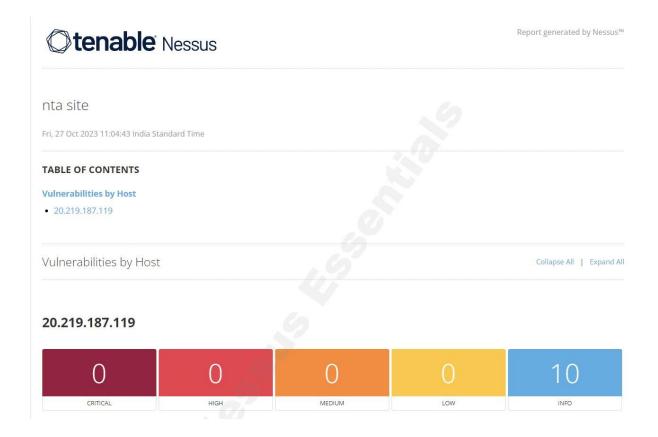
# MAIN WEBSITE NESSUS SCANNING



# **VULNERABILITIES FOUND:**

## Synopsis

It was possible to enumerate CPE names that matched on the remote system.

#### 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.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

#### See Also

http://cpe.mitre.org/ https://nvd.nist.gov/products/cpe

#### Solution

n/a

#### **Risk Factor**

None

## **Plugin Information**

Published: 2010/04/21, Modified: 2023/07/27

## **Plugin Output**

tcp/0

The remote operating system matched the following CPE :

cpe:/o:microsoft:windows -> Microsoft Windows

## 54615 - Device Type

17

## Synopsis

It is possible to guess the remote 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).

## Solution

n/a

# Risk Factor

None

## Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

## **Plugin Output**

tcp/0

Remote device type : general-purpose Confidence level : 70

## Synopsis

A web server is running on the remote host.

## Description

This plugin attempts to determine the type and the version of the remote web server.

## Solution

n/a

## Risk Factor

None

## References

XREF

IAVT:0001-T-0931

## Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

## Plugin Output

tcp/80/www

The remote web server type is : Microsoft-HTTPAPI/2.0

#### 24260 - HyperText Transfer Protocol (HTTP) Information

## Synopsis

Some information about the remote HTTP configuration can be extracted.

# Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

## Solution

n/a

## Risk Factor

None

## **Plugin Information**

Published: 2007/01/30, Modified: 2019/11/22

# Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1

SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Fri, 27 Oct 2023 05:28:27 GMT
```

11219 - Nessus SYN scanner

## Synopsis

It is possible to determine which TCP ports are open.

## 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.

#### Solution

Protect your target with an IP filter.

## **Risk Factor**

None

## Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

# Plugin Output

tcp/80/www

Port 80/tcp was found to be open

11219 - Nessus SYN scanner

300

## **Synopsis**

It is possible to determine which TCP ports are open.

## 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.

# Solution

Protect your target with an IP filter.

## Risk Factor

None

## Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

## **Plugin Output**

tcp/443

Port 443/tcp was found to be open

19506 - Nessus Scan Information

#### Synopsis

This plugin displays information about the Nessus scan.

#### 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.

#### Solution

n/a

#### Risk Factor

None

#### **Plugin Information**

Published: 2005/08/26, Modified: 2023/07/31

## **Plugin Output**