

PraticaS5L3

Impostazioni Nessus

PraticaS5L3Nessus / Configuration

[← Back to Scan Report](#)

Settings

Credentials

Plugins

BASIC

• General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

Description

Folder

Targets

Upload Targets

PraticaS5L3Nessus

04-12-2024

Metasploitable

192.168.1.218

Add File

PraticaS5L3Nessus / Configuration

[← Back to Scan Report](#)

Settings

Credentials

Plugins

BASIC

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Scan Type

General Settings:

Port Scanner Settings:

Ping hosts using:

Port scan (common ports)

Always test the local Nessus host

Use fast network discovery

Scan common ports

Use netstat if credentials are provided

Use SYN scanner if necessary

TCP

ARP


ICMP (2 retries)

PraticaS5L3Nessus / Configuration

[← Back to Scan Report](#)

Settings

Credentials

Plugins 

BASIC



DISCOVERY



ASSESSMENT



REPORT



ADVANCED



Scan Type

Default



General Settings:

Avoid potential false alarms

Disable CGI scanning

Web Applications:


Disable web application scanning

PraticaS5L3Nessus / Configuration

[← Back to Scan Report](#)

Settings

Credentials

Plugins 

BASIC



DISCOVERY



ASSESSMENT



REPORT



ADVANCED



General

Scan Type

Custom



Choose your own advanced settings.

Performance Options

☐ Slow down the scan when network congestion is detected

When enabled, Nessus detects when it is sending too many packets and the network pipe is approaching capacity. If network congestion is detected, Nessus throttles the scan to accommodate and alleviate the congestion. Once the congestion has subsided, Nessus automatically attempts to use the available space within the network pipe again.

Network timeout (in seconds)

5

Specifies the time that Nessus waits for a response from a host unless otherwise specified within a plugin. If you are scanning over a slow connection, you may want to set this to a higher number of seconds.

Max simultaneous checks per host

5

Specifies the maximum number of checks a Nessus scanner will perform against a single host at one time.

Max simultaneous hosts per scan

60

Specifies the maximum number of hosts that a Nessus scanner will scan at the same time.

La scansione ha rilevato varie vulnerabilità.

Ne ho analizzate tre critiche

1) Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Porta: 22

La vulnerabilità è grave perché mette a rischio la sicurezza delle comunicazioni SSH, le chiavi utilizzate per garantire la sicurezza delle connessioni potrebbero essere facilmente indovinate da un attaccante, quindi è necessario sostituirle e aggiornare il software per evitare che il sistema venga compromesso.

2) Bind Shell Backdoor Detection

Porta: 1524

Il sistema remoto ha una shell che sta ascoltando sulla porta 1524 e non richiede alcuna autenticazione per accedervi. Questo significa che chiunque riesca a connettersi a quella porta può inviare comandi direttamente al sistema, ottenendo il pieno controllo e la possibilità di eseguire comandi come amministratore.

3) Apache Tomcat AJP Connector Request Injection (Ghostcat)

Porta: 8009

La vulnerabilità Ghostcat (CVE-2020-1745) permette a un attaccante di leggere file importanti su un server Apache Tomcat vulnerabile, e in alcuni casi, di eseguire comandi dannosi. Per proteggere il sistema, è necessario aggiornare Tomcat e sistemare le impostazioni del server in modo che nessuno non autorizzato possa accedervi.