Claudio De cicco
25/11/2022

Report iniziale VA

Metasploitable basic scan

Report generated by Nessus™ Thu, 24 Nov 2022 07:48:33 EST

Nessus Essentials

192.168.1.102

13	6	26	5	132
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.1.102
MAC Address:	08:00:27:F0:63:36
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

1- 61708 - VNC Server 'password' Password

Synopsis:

A VNC server running on the remote host is secured with a weak password.

Description:

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Risk Factor:

Critical

Plugin Output:

tcp/5900/vnc

Solution:

Secure the VNC service with a strong password.

2- 10203 - rexecd Service Detection

Synopsis:

The rexecd service is running on the remote host.

Description:

The rexecd service is running on the remote host. This service is design to allow users of a network to execute commands remotely. However, rexecd does not provide any good means of authentication, so it may be abused by an attacker to scan a third-party host.

Risk Factor:

Critical

Plugin Output:

tcp/512/rexecd

Solution:

Comment out the 'exec' line in /etc/inetd.conf and restart the inetd process

3- 11356 NFS Exported Share Information Disclosure

Synopsis:

It is possible to access NFS shares on the remote host.

Description:

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Risk Factor:

Critical

Plugin Output:

udp/2049/rpc-nfs

Solution:

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

4- 51988 Bind Shell Backdoor Detection

Synopsis:

The remote host may have been compromised.

Description:

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Risk Factor:

Critical

Plugin Output:

tcp/1524/wild_shell

Solution:

Verify if the remote host has been compromised, and reinstall the system if necessary.