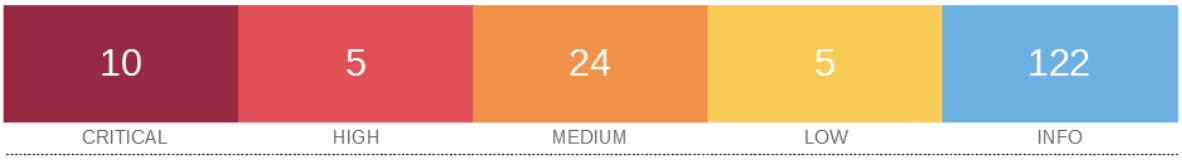
meta

Report generated by Nessus™ Thu, 24 Nov 2022 09:11:55 EST

192.168.50.111



Scan Information

Start time:	Thu Nov 24 08:45:17 2022
End time:	Thu Nov 24 09:11:55 2022

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.50.111
MAC Address:	08:00:27:78:DE:AF
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

VULNERABILITY

61708 - VNC Server 'password' 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.

SOLUTION

Secure the VNC service with a strong password.

RISK FACTOR

Critical

PLUGIN OUTPUT

tcp/5900/vnc

11356 - NFS Exported Share Information Disclosure

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.

SOLUTION

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

RISK FACTOR

Critical

PLUGIN OUTPUT

udp/2049/rpc-nfs

51988 - Bind Shell Backdoor Detection

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.

SOLUTION

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

RISK FACTOR

Critical

PLUGIN OUTPUT

tcp/1524/wild_shell