

Exploit:

<input type="checkbox"/>	Sev ▼	Score ▼	Name ▲
<input type="checkbox"/>	CRITICAL	10.0 *	NFS Exported Share Information Disclosure
<input type="checkbox"/>	CRITICAL	10.0 *	rexecd Service Detection
<input type="checkbox"/>	CRITICAL	10.0	Unix Operating System Unsupported Version Detection
<input type="checkbox"/>	CRITICAL	10.0 *	VNC Server 'password' Password
<input type="checkbox"/>	CRITICAL	9.8	Bind Shell Backdoor Detection
<input type="checkbox"/>	CRITICAL	9.8	Bind Shell Backdoor Detection

Let's address only the highlighted vulnerability

NFS Exported Share Information Disclosure

NFS Exported Share Information Disclosure

Language: English ▾

CRITICAL Nessus Plugin ID 11356

Information

Dependencies

Dependents

Changelog

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.

Solution

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

Plugin Details

Severity: Critical

ID: 11356

File Name: nfs_mount.nasl

Version: 1.21

Type: remote

Family: RPC

Published: 3/12/2003

Updated: 8/30/2023

Supported Sensors:
Nessus

To mitigate this vulnerability, we can apply the NFS jumbo patch (Patch-ID# 100173-13) obtained from the Sun Microsystems Website.

Following patch installation, execute fsirand across the entirety of your file system. The updated fsirand utility enhances security by rendering NFS filehandles less predictable, thereby thwarting unauthorized mounting and access attempts by remote system users.

rexecd Service Detection

rexecd Service Detection

Language: English

CRITICAL

Nessus Plugin ID 10203

Information

Dependencies

Dependents

Changelog

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.

Solution

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

Plugin Details

Severity: Critical

ID: 10203

File Name: rexecd.nasl

Version: 1.33

Type: remote

Family: Service detection

Published: 8/31/1999

Updated: 6/29/2023

Supported Sensors: Nessus

```
GNU nano 2.0.7      File: etc/inetd.conf      Modified

#<off># netbios-ssn    stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sb$
telnet                stream  tcp    nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp            stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sb$
tftp                  dgram   udp    wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tf$
shell                 stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs$
login                 stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl$
exec                  stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re$
ingreslock stream tcp nowait root /bin/bash bash -i

[ Read 8 lines ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text    ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^U Next Page  ^U UnCut Text ^T To Spell
```

```
GNU nano 2.0.7      File: etc/inetd.conf      Modified

#<off># netbios-ssn    stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sb$
telnet                stream  tcp    nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp            stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sb$
tftp                  dgram   udp    wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tf$
shell                 stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs$
login                 stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl$
#exec                 stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re$
ingreslock stream tcp nowait root /bin/bash bash -i

[ Read 8 lines ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text    ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^U Next Page  ^U UnCut Text ^T To Spell
```

Access the inetd.conf file situated in the /etc directory by utilizing the nano command. Begin from the start directory by executing the command `cd /`.

VNC Server 'password' Password

VNC Server 'password' Password

Language: English ▾

CRITICAL

Nessus Plugin ID 61708

Information

Dependencies

Dependents

Changelog

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.

Solution

Secure the VNC service with a strong password.

Plugin Details

Severity: Critical

ID: 61708

File Name:
vnc_password_password.nasl

Version: Revision: 1.2

Type: remote

Family: [Gain a shell remotely](#)

Published: 8/29/2012

Updated: 9/24/2015

Supported Sensors:
Nessus

To modify or update your VNC password, utilize the `vncpasswd` command. This command will prompt you twice to input your new password.

```
vncpasswd
```

Now set the new password and write it another time to verify than click enter.

Bind Shell Backdoor Detection

Bind Shell Backdoor Detection

Language: English ▼

CRITICAL

Nessus Plugin ID 51988

Information

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.

Solution

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

Plugin Details

Severity: Critical

ID: 51988

File Name:

```
wild_shell_backdoor.nas
|
```

Version: 1.10

Type: remote

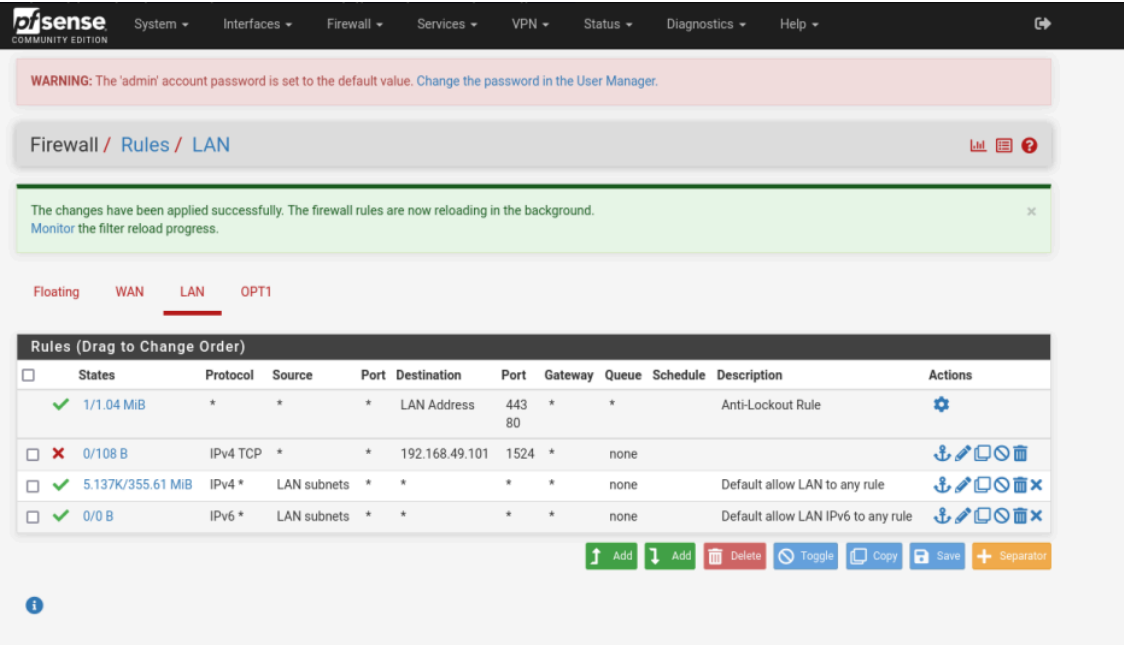
Family: Backdoors

Published: 2/15/2011

Updated: 4/11/2022

Configuration: Enable thorough checks

Supported Sensors:
Nessus



In this scenario, you need to block the port TCP 1524 in the firewall rule.

