15-04-2024

Index

Zeroconf Networking Should Be Disabled.

Description
Devices may automatically assign themselves an IP address and engage in IP communication without a statically-assigned address or even a DHCP server.

Zeroconf address assignment commonly occurs when the system is configured to use DHCP but fails to receive an address assignment from the DHCP server.

impact
Which could lead to unintended network connectivity.

Solution
To disable Zeroconf automatic route assignment in the *169.245.0.0* subnet, add or correct the following line in /etc/sysconfig/network

```
NOZEROCONF=yes
```

To disable in windows

```
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters /v IPAutoconfigurationEnabled /t REG_DWORD /d "00000000" /f
```

The Portmap Service Should Be Disabled.

- The Portmapper service runs on both **TCP** and **UDP port 111**.
- It manages the **port mappings**
- Portmapper keeps track of the mappings, making it easier for you to access services from outside your network.

Ensure Rsync Service is not Enabled

Description
rsync - This is a command-line utility used for synchronizing files and directories between systems over network.

Impact
It can be a security risk as it uses un-encrypted protocols (TCP port 873) for communication. Does not automatically encrypt the sensitive information during transit.

Solution
Disable rsync by using the below command

```
# systemctl --now disable rsync
```

/etc/passwd - File Permissions Should Be Set to 0600

Description

`/etc/passwd` is a file which contains the backup user account information. The `/etc/passwd` file keeps track of all users on the system.

`/etc/passwd` is a plain text-based database that contains information for all user accounts on the system. It is owned by root and has 644 permissions . The file can only be modified by root or users with sudo privileges and readable by all system users.

Modifying the `/etc/passwd` file by hand should be avoided unless you know what you are doing. Always use a command that is designed for the purpose. For example, to modify a user account, use the `usermod` command, and to add a new user account use the `useradd` command.

The Portmap Service Should Be Disabled.

Disable the portmapper services (bobcares.com)

The Sendmail Package Should Be Uninstalled.

Sendmail is a mail transfer agent (MTA), which is a software that transports email messages from one computer to another using SMTP, the standard protocol for sending emails.

Sendmail has had several vulnerabilities over the years.

SMTP Smuggling - CVE-2023-51765
MIME Message Denial of Service - CVE-2014-3956
X.509 Certificate Handling - CVE-2009-4565
Heap-Based Buffer Overflow - CVE-2009-1490

Tuesday, 14-05-2024, 5:40 am

Enable 'Scan Removable Drives' by Setting DisableRemovableDriveScanning (REG_DWORD) to 0

Description:

- REG_DWORD: This indicates the data type of a value stored in the Windows Registry.
- Setting this value to 0 enables scanning of removable drives.

Impact:

Solution:

Ensure 'Microsoft Network Server: Digitally Sign Communications (if Client agrees)' is Set to 'Enabled'

Description:

- configuration of Windows Firewall on a domain-joined machine.
- Determines whether locally created firewall rules on the machine can be applied alongside the rules defined by the domain policy (group policy).

- This is the recommended setting, allowing administrators on the machine to create additional firewall rules if needed.

Impact:

- Local administrators won't be able to create or manage firewall rules specific to that machine.

Solution:

Ensure 'Microsoft Network Server: Digitally Sign Communications (if Client agrees)' is Set to 'Enabled'

Description: SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

- negotiate SMB packet signing with clients that request it.

Impact: If no signing request comes from the client, a connection will be allowed without a signature if the Microsoft network server: Digitally sign communications (always) setting is not enabled.

Solution:

/etc/shadow- File Permissions Should Be Set to 0400

A critical system file in Linux that stores user account information, including encrypted passwords.
It contains details such as the username, password hash, and account expiration information.