Security checks

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.

Tuesday, 28-05-2024, 4:03 pm

Ensure 'Audit Other Logon/Logoff Events' is Set to 'Success and Failure'

Description:

- reports related to logon/logoff-related events
- It covers events such as:
  - Remote Desktop Services session disconnects and reconnects.
  - Using “RunAs” to run processes under a different account.
  - Locking and unlocking a workstation.
- Set of Events like:
  - 4649: A replay attack was detected.
  - 4778: A session was reconnected to a Window Station.
  - 4779: A session was disconnected from a Window Station.
  - 4800: The workstation was locked.
  - 4801: The workstation was unlocked.
  - 4802: The screen saver was invoked.
  - 4803: The screen saver was dismissed.

    - 5378: The requested credentials delegation was disallowed by policy.
    - 5632: A request was made to authenticate to a wireless network.
    - 5633: A request was made to authenticate to a wired network.
- Auditing these events may be useful when investigating a security incident.

Impact: security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur.

Solution:

configuration via GP, The recommended state for this setting is: Success and Failure.

`Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Other Logon/Logoff Events`

Default value: No Auditing.

Ensure 'Audit Policy Change' is Set to 'Success'

Description:

These events include changes to the system's audit policy settings.

Track modifications to audit settings, which can impact the security posture of your system.

The list of specific events audited under "Audit Policy Change":

- User right assignment changes.
- Trust relationship creation/removal.
- Audit policy modifications.
- IPSec policy agent events.
- Kerberos policy changes.
- Encrypted Data Recovery policy changes.
- System access grants/removals.
- Per-user auditing policy settings.
- Collision detection in namespace elements.
- Trusted forest information updates.

Impact:

Without proper auditing, security incidents might go undetected, or there may not be enough evidence for forensic analysis.

Solution:

- To configure this via Group Policy (GP):
    - Navigate to: `Computer Configuration → Policies → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Audit Policies → Policy Change → Audit Audit Policy Change`.
    - Set the value to "Success."
    - The default value is "No Auditing."

Ensure 'Audit Security System Extension' is Set to 'Success'

Description:

- When enabled, it audits and records specific system events related to the **loading of various extension code components by the security subsystem**.
- These extension code components include:
  - **Authentication packages**: Used for user authentication during logon.

  - Notification packages: Responsible for handling notifications related to security events.
  - Security packages: Used for secure communication and authentication (e.g., Kerberos and NTLM).

- Events Audited Under "Audit Security System Extension":
  - The following events are audited:
    - 4610: An authentication package has been loaded by the Local Security Authority.
    - 4611: A trusted logon process has been registered with the Local Security Authority.
    - 4614: A notification package has been loaded by the Security Account Manager.
    - 4622: A security package has been loaded by the Local Security Authority.
    - 4697: A service was installed in the system.

Impact:

If you ignore this recommendation:

- Security incidents may not be adequately detected.
- Forensic analysis after incidents could be challenging due to insufficient data.

Solution:

- To configure this via Group Policy (GP):
  - Navigate to: `Computer Configuration → Policies → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Audit Policies → System → Audit Security System Extension`.
  - Set the value to "Success".
  - The default value is "No Auditing".

Ensure 'Audit Security Group Management' is Set to 'Success'

Description:

- Security groups are a fundamental concept in Active Directory (AD) and other directory services.
- They serve as containers for grouping users, computers, and other objects based on common security requirements.
- Security groups simplify access control by allowing you to assign permissions to a group rather than individual users or devices.
- This audit policy setting tracks events related to security group management.
- It records actions such as creating, changing, or deleting security groups, as well as adding or removing members from these groups.
- Enabling this setting allows administrators to monitor events and detect unauthorized or accidental changes to security group accounts.

Events Audited Under "Audit Security Group Management":

```
- The following events are audited:
    - **4727**: A security-enabled global group was created.
    - **4728**: A member was added to a security-enabled global group.
    - **4729**: A member was removed from a security-enabled global group.
    - **4730**: A security-enabled global group was deleted.
    - **4731**: A security-enabled local group was created.
    - **4732**: A member was added to a security-enabled local group.
    - **4733**: A member was removed from a security-enabled local group.
    - **4734**: A security-enabled local group was deleted.
    - **4735**: A security-enabled local group was changed.
    - **4737**: A security-enabled global group was changed.
    - **4754**: A security-enabled universal group was created.
    - **4755**: A security-enabled universal group was changed.
    - **4756**: A member was added to a security-enabled universal group.
    - **4757**: A member was removed from a security-enabled universal group.
    - **4758**: A security-enabled universal group was deleted.
    - **4764**: A group's type was changed.
```

Impact:

If you ignore this recommendation:

- Security incidents may not be adequately detected.
- Forensic analysis after incidents could be challenging due to insufficient data.

Solution:

- To configure this via Group Policy (GP):
  - Navigate to: `Computer Configuration → Policies → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Audit Policies → Account Management → Audit Security Group Management`.
  - Set the value to **"Success"**.
  - The default value is **"No Auditing"**.

Ensure 'System: Specify the Maximum Log File Size (KB)' is Set to 'Enabled: 32,768 or Greater'

Description:

- This recommendation pertains to the configuration of the maximum size for log files in kilobytes (KB).
- Specifically, it focuses on the event logs generated by the Windows operating system.

Impact:

- If logs are not recorded or if they fill up too quickly, it becomes difficult to determine the root cause of system problems or unauthorized activities by malicious users.
- Event logs may not capture critical information due to limited space.
- Forensic analysis after security incidents could be compromised.

Solution:

- To configure this via Group Policy (GP):
  - Navigate to: `Computer Configuration → Policies → Administrative Templates → Windows Components → Event Log Service → Setup → Specify the maximum log file size (KB)`.
  - Set the value to **"Enabled: 32,768 or greater"**.
  - The default value is **"Disabled"** (which corresponds to a default log size of 20,480 KB).
  - Adjust the log size based on your system's requirements.
