



CHOICE EQUITY BROKING PVT. LTD

Hardening Policy

Version Control

Action	Date	Revision Details	Prepared / Amended By	Approved By	
Created On	17-Oct-16	1.0	Mahesh Tamhankar	Amit Jaokar	Inherited from Consolidated ISMS Policy
Reviewed On	21-Feb-17	1.1	Mahesh Tamhankar	Amit Jaokar	Inherited from Consolidated ISMS Policy
Reviewed On	13-Feb-18	1.2	Mahesh Tamhankar	Amit Jaokar	Inherited from Consolidated ISMS Policy
Reviewed On	20-Feb-18	1.3	Mahesh Tamhankar	Utpal Parekh	Inherited from Consolidated ISMS Policy
Reviewed On	10-Aug-19	1.4	Mahesh Tamhankar	Yogesh Jadhav	Inherited from Consolidated ISMS Policy
Reviewed On	11-Jan-20	1.4	Mahesh Tamhankar	Yogesh Jadhav	Inherited from Consolidated ISMS Policy
Reviewed On	14-July-21	1.6	Sunil Utekar	Yogesh Jadhav	Inherited from Consolidated ISMS Policy

Reviewed On	08-Jan-22	1.7	Sunil Utekar	Yogesh Jadhav	Inherited from Consolidated ISMS Policy
Reviewed On	09-Apr-23	2.0	Ashutosh Bhardwaj	Yogesh Jadhav	Inherited from Consolidated ISMS Policy
Reviewed On	31-Jan-24	2.1	Anil Ashok & Associates	Ashutosh Bhardwaj	Inherited from Consolidated ISMS Policy
Reviewed On	31-Mar-24	2.2	Abhishek Vinayak	Ashutosh Bhardwaj	Added Latest Hardening controls
Approved On	08-Jan-2025	2.3	Abhishek Vinayak	Yogesh Jadhav	Approval as per ISO requirement

TABLE OF CONTENTS

Contents

Version: 1.0	1
Document Classification: Internal	1
Confidentiality Agreement	3
Fortinet Firewall	3
1 Overview	3
2 Audience	3
3 Scope	3
4 Fortinet Compliance Checks	3
Switch	10
1 Overview	10
2 Audience	10
3 Scope	10
4 Switch Compliance Checks	10
Windows Server	12
1 Overview	12
2 Audience	12
3 Scope	12
4 Hardening Windows Server.	12
Ubuntu OS	16
1 Overview	16
2 Audience	16
3 Scope	16
4 Hardening Ubuntu Systems.	16

Confidentiality Agreement

This document is classified as Choice Equity Broking Private Limited(referred to as CEBPL throughout the document) Internal. No part of it may be reproduced or disclosed without the prior consent of CEBPL, to include duplication and/or storage of documents to an alternate location. Disclosure of this document is solely for review and approval as is required for CEBPL to meet pertinent regulatory requirements and corporate policy compliance. No part of this document shall be taken to create or modify any contractually binding obligations upon CEBPL.

Fortinet Firewall

1. Overview

This document provides prescriptive guidance for establishing a secure configuration posture for Fortinet Firewall OS v7.4.0 build2360.

2. Audience

This document is intended for the Firewall Administrator to implement secure solutions that incorporate Fortinet Firewall.

3. Scope

Revisions to this security baseline will be applicable to builds occurring after the revision date. No retroactive configurations are required as a result of revisions unless otherwise identified as necessary by Information Security Architecture.

4. Fortinet Compliance Checks

4.1 Install the FortiGate unit in a physically secure location

A good place to start with is physical security. Install your FortiGate in a secure location, such as a locked room or one with restricted access. A restricted location prevents unauthorized users from getting physical access to the device. If unauthorized users have physical access, they can disrupt your entire network by disconnecting your FortiGate (either by accident or on purpose). They could also connect a console cable and attempt to log into the CLI. Also, when a FortiGate unit reboots, a person with physical access can interrupt the boot process and install different firmware.

4.2 Register your product with Fortinet Support

You need to register your Fortinet product with Fortinet Support to receive customer services, such as firmware updates and customer support. You must also register your product for FortiGuard services, such as up-to-date antivirus and IPS signatures. To register your product the Fortinet Support website

4.3 Keep your FortiOS firmware up to date

Always keep FortiOS up to date. The most recent version is the most stable and has the most bugs fixed and vulnerabilities removed. Fortinet periodically updates the FortiGate firmware to include new features and resolve important issues.

After you register your FortiGate, you can receive notifications on FortiGate GUI about firmware updates. You can update the firmware directly from the GUI or by downloading firmware updates from the Fortinet Support website.

Before you install any new firmware, be sure to follow these steps:-

- Review the release notes for the latest firmware release.
- Review the Upgrade Path tool to determine the best path to take from your current version of FortiOS to the latest version.
- Back up the current configuration.

Only FortiGate administrators who have read and write privileges can upgrade the FortiOS firmware.

4.4 Disable administrative access to the external (Internet-facing) interface

When possible, don't allow administration access on the external (Internet-facing) interface. Unless and until it is required and approval is given.

To disable administrative access, go to Network > Interfaces, edit the external interface and disable HTTPS, PING, HTTP, SSH, and TELNET under Administrative Access.

From the CLI:

```
config system interface
edit <external-interface-name>
unset allowaccess
End
```

4.4 Allow only HTTPS access to the GUI and SSH access to the CLI

Use the following command to require TLS <LATEST_STABLE_TLS_VERSION> for HTTPS administrator access to the GUI:

```
config system global
set admin-https-ssl-versions tlsv(<LATEST_STABLE_TLS_VERSION>)
end
```

4.6 Re-direct HTTP GUI logins to HTTPS

Go to *System > Settings > Administrator Settings* and enable Redirect to HTTPS to make sure that all attempted

HTTP login connections are redirected to HTTPS.

From the CLI:

```
config system global
set admin-https-redirect enable
end
```

4.7 Change the HTTPS and SSH admin access ports to non-standard ports

Go to *System > Settings > Administrator Settings* and change the HTTPS and SSH ports.

You can change the default port configurations for HTTPS and SSH administrative access for added security. To

connect to a non-standard port, the new port number must be included in the collection request. For example:

If you change the HTTPS port to 7734, you would browse to `https://<ip-address>:7734`.

If you change the SSH port to 2344, you would connect to `ssh admin@<ip-address>:2344`

To change the HTTPS and SSH login ports from the CLI:

```
config system global
set admin-sport 7734
set admin-ssh-port 2344
end
```

If you change to the HTTPS or SSH port numbers, make sure your changes do not conflict with ports used for other services.

4.8 Maintain short login timeouts

Set the idle timeout to a short time to avoid the possibility of an administrator walking away from their management computer and leaving it exposed to unauthorized personnel.

To set the administrator idle timeout, go to *System > Settings* and enter the amount of time for the *Idle timeout*. A best practice is to keep the default time of 4 minutes. To set the administrator idle timeout from the CLI:

```
config system global
set admintimeout 10
end
```

You can use the following command to adjust the grace time permitted between making an SSH connection and authenticating. The range can be between 10 and 3600 seconds, the default is 120 seconds (minutes). By shortening this time, you can decrease the chances of someone attempting a brute force attack from being successful. For example, you could set the time to 30 seconds.

```
config system global
set admin-ssh-grace-time 30
end
```

4.9 Restrict logins from trusted hosts

Setting up trusted hosts for an administrator limits the addresses from where they can log into FortiOS. The trusted hosts configuration applies to most forms of administrative access including HTTPS, SSH, and SNMP. When you identify a trusted host for an administrator account, FortiOS accepts that administrator's login only from one of the trusted hosts. A login, even with proper credentials, from a non-trusted host is dropped.

To identify trusted hosts, go to *System > Administrators*, edit the administrator account, enable *Restrict login to trusted hosts*, and add up to ten trusted host IP addresses.

To add two trusted hosts from the CLI:

```
config system admin
edit <administrator-name>
set trustedhost1 172.24.176.23 244.244.244.244
set trustedhost2 172.24.177.0 244.244.244.0
end
```

Trusted host IP addresses can identify individual hosts or subnets. Just like firewall policies, FortiOS searches through the list of trusted hosts in order and acts on the first match it finds. When you configure trusted hosts, start by adding specific addresses at the top of the list. Follow with more general IP addresses. You don't have to add addresses to all of the trusted hosts as long as all specific addresses are above all of the 0.0.0.0 0.0.0.0 addresses.

4.10 Set up two-factor authentication for administrators

FortiOS supports FortiToken and FortiToken Mobile 2-factor authentication. FortiToken Mobile is available for iOS and Android devices from their respective application stores. Every registered FortiGate unit includes two trial tokens for free. You can purchase additional tokens from your reseller or from Fortinet. To assign a token to an administrator, go to *System > Administrators* and select *Enable Two-factor Authentication* for each administrator.

4.11 Create multiple administrator accounts

Rather than allowing all administrators to access FortiOS with the same administrator account, you can create accounts for each person or each role that requires administrative access. This configuration allows you to track the activities of each administrator or administrative role. If you want administrators

to have different functions you can add different administrator profiles. Go to *System > Admin Profiles* and select *Create New*.

4.12 Modify administrator account lockout duration and threshold values

By default, the FortiGate sets the number of passwords retries at three, allowing the administrator a maximum of three attempts to log into their account before locking the account for a set amount of time. Both the number of attempts (admin-lockout-threshold) and the wait time before the administrator can try to enter a password again (admin-lockout-duration) can be configured within the CLI.

To configure the lockout options:

```
config system global
set admin-lockout-threshold <failed_attempts>
set admin-lockout-duration <seconds>
end
```

The default value of admin-lockout-threshold is 3 and the range of values is between 1 and 10. The admin lockout-duration is set to 60 seconds by default and the range of values is between 1 and 2147483647 seconds. Keep in mind that the higher the lockout threshold, the higher the risk that someone may be able to break into the FortiGate.

Example

To set the admin-lockout-threshold to one attempt and the admin-lockout-duration to a five minute duration before the administrator can try to log in again, enter the commands:

```
config system global
set admin-lockout-threshold 1
set admin-lockout-duration 300
end
```

4.13 Rename the admin administrator account

You can improve security by renaming the admin account. To do this, create a new administrator account with the super_admin admin profile and log in as that administrator. Then go to *System > Administrators* and edit the admin administrator and change the *User Name*. Renaming the admin account makes it more difficult for an attacker to log into FortiOS.

4.14 Add administrator disclaimers

FortiOS can display a disclaimer before or after logging into the GUI or CLI (or both). In either case the administrator must read and accept the disclaimer before they can proceed. Use the following command to display a disclaimer before logging in:

```
config system global
set pre-login-banner enable
end
```

Use the following command to display a disclaimer after logging in:

```
config system global
set post-login-banner enable
end
```

You can customize the replacement messages for these disclaimers by going to *System > Replacement Messages*. Select *Extended View* to view and edit the *Administrator* replacement messages.

From the CLI:

```
config system replacemsg admin pre_admin-disclaimer-text
config system replacemsg admin post_admin-disclaimer-text
```

4.14 Turn on global strong encryption

Enter the following command to configure FortiOS to use only strong encryption and allow only strong ciphers (AES, 3DES) and digest (SHA1) for HTTPS, SSH, TLS, and SSL functions.

```
config system global
set strong-crypto enable
end
```

4.16 Disable static keys for TLS

You can use the following command to prevent all TLS sessions that are terminated by FortiGate from using static keys (AES128-SHA, AES246-SHA, AES128-SHA246, AES246-SHA246):

```
config system global
set ssl-static-key-ciphers disable
end
```

4.17 Require larger values for Diffie-Hellman exchanges

Larger Diffie-Hellman values result in stronger encryption. Use the following command to force Diffie-Hellman exchanges to use 8192 bit values (the highest configurable DH value).

```
config system global
set dh-params 8192
end
```

4.18 Disable auto USB installation

If USB installation is enabled, an attacker with physical access to a FortiGate could load a new configuration or firmware on the FortiGate using the USB port. You can disable USB installation by entering the following from the CLI:

```
config system auto-install
set auto-install-config disable
set auto-install-image disable
end
```

4.19 Set system time by synchronizing with an NTP server

For accurate time, use an NTP server to set system time. Synchronized time facilitates auditing and consistency between expiry dates used in expiration of certificates and security protocols. From the GUI go to *System > Settings > System Time* and select *Synchronize with NTP Server*. By default, this causes FortiOS to synchronize with Fortinet's FortiGuard secure NTP server. From the CLI you can use one or more different NTP servers:

```
config system ntp
set type custom
set ntpsync enable
config ntpserver
edit 1
set server <ntp-server-ip>
next
edit 2
set server <other-ntp-server-ip>
end
```

4.20 Enable password policies

Go to *System > Settings > Password Policy*, to create a password policy that all administrators must follow. Using the available options you can define the required length of the password, what it must contain (numbers, upper and lower case, and so on) and an expiry time. Use the password policy feature to make sure all administrators use secure passwords that meet your organization's requirements.

4.21 Configure auditing and logging

For optimum security go to *Log & Report > Log Settings* enable *Event Logging*. For best results send log messages to FortiAnalyzer or FortiCloud. From FortiAnalyzer or FortiCloud, you can view reports or system event log messages to look for system events that may indicate potential problems. You can also view system events by going to *FortiView > System Events*. Establish an auditing schedule to routinely inspect logs for signs of intrusion and probing.

4.22 Disable unused interfaces

To disable an interface from the GUI, go to *Network > Interfaces*. Edit the interface to be disabled and set *Interface State* to *Disabled*.

From the CLI, to disable the port21 interface:

```
config system interface
edit port21
set status down
end
```

4.23 Disable unused protocols on interfaces

You can use the config system interface command to disable unused protocols that attackers may attempt to use to gather information about a FortiGate unit. Many of these protocols are disabled by default. Using the config system interface command you can see the current configuration of each of these options for the selected interface and then choose to disable them if required.

```
config system interface
edit <interface-name>
set dhcp-relay-service disable
set pptp-client disable
set arpforward disable
set broadcast-forward disable
set l2forward disable
set icmp-redirect disable
set vlanforward disable
set stpforward disable
set ident-accept disable
set ipmac disable
set netbios-forward disable
set security-mode none
set device-identification disable
set lldp-transmission disable
end
```

Option Description

- dhcp-relay-service:- Disable the DHCP relay service.
- pptp-client:- Disable operating the interface as a PPTP client.
- arpforward:- Disable ARP forwarding.
- broadcast-forward:- Disable forwarding broadcast packets.
- l2forward:- Disable layer 2 forwarding.
- icmp-redirect:- Disable ICMP redirect.
- vlanforward:- Disable VLAN forwarding.
- stpforward:- Disable STP forwarding.
- ident-accept:- Disable authentication for this interface. The interface will not respond to a connection with an authentication prompt.
- ipmac:- Disable IP/MAC binding.
- netbios-forward:- Disable NETBIOS forwarding.
- security-mode:- Set to none to disable captive portal authentication. The interface will not respond to a connection with a captive portal.
- device-identification:- Disable device identification.

- Ildp-transmission:- Disable link layer discovery (LLDP).

Switch

1. Overview

This document provides prescriptive guidance for establishing a secure configuration posture for Switch

2. Audience

This document is intended for Network Administrator to implement secure solutions that incorporate on Switch.

3. Scope

Revisions to this security baseline will be applicable to builds occurring after the revision date. No retroactive configurations are required as a result of revisions unless otherwise identified as necessary by Information Security Architecture.

4. Switch Compliance Checks

The following list of security features lets you judge how secure the Switch

4.1 Default passwords

Change the default passwords on the device, all of them, not just the one on the account being used. A number of switches have multiple built in accounts, some of which are easily forgotten.

4.2 SNMP v3

If the device supports it, use it, otherwise use a nice long community string, just be aware that it will be compromised and at least read access to the device will be gained.

4.3 Logging and Monitoring

Use centralized logging of switch activities.

Regularly review logs to identify any anomalies or potential security breaches.

4.4 Management VLAN

Many switches support a management VLAN so configure it and then use ACL to control access to this VLAN.

4.5 Network Segmentation:

Set up VLANs to segregate your network segments, then use ACLs to control traffic flows between them

4.6 SSH /Telnet

Use SSH v2, disable telnet.

Use secure protocols like SSH (Secure Shell) or HTTPS for management access.

Implement strong, unique passwords for administrative accounts.

4.7 Web interface

If you need it use SSL, otherwise disable it

4.8 Update and Patch

Keep the switch firmware updated with the latest security patches and bug fixes provided by OEM.

Regularly check for and apply updates to ensure the system is protected against known vulnerabilities

4.9 Disable Unused Services and Ports

Turn off unnecessary services and ports to reduce the attack surface if possible.

Disable unused interfaces and services such as Telnet, SNMPv1/v2, or any other protocols not in use.

4.10 Physical Security

Secure the physical access to the switch to prevent unauthorized access or tampering.

4.11 Backup Configuration

Regularly backup switch configurations to ensure quick recovery in case of configuration errors or security incidents.

Windows Server

1. Overview

This document provides prescriptive guidance for establishing a secure configuration posture for Windows Server

2. Audience

This document is intended for the Windows Server Administrator to implement secure solutions that incorporate Windows Server.

3. Scope

Revisions to this security baseline will be applicable to builds occurring after the revision date. No retroactive configurations are required as a result of revisions unless otherwise identified as necessary by Information Security Architecture.

4. Hardening Windows Server

Hardening a Windows Server involves securing the system by implementing various measures to reduce its attack surface and enhance its resilience against potential threats. Here's a basic guideline for hardening steps:

1. Installation and Configuration:

- Install the latest version of Windows Server from a trusted source.
- During installation, configure roles and features only as necessary to minimize the attack surface.

2. Applying Updates:

- Regularly update the server with the latest patches and security updates from Microsoft.
- Enable automatic updates or establish a schedule for manual updates.

3. User Accounts and Permissions:

- Implement the principle of least privilege. Assign users only the permissions they need to perform their tasks.
- Disable or remove unnecessary default user accounts.
- Change default passwords and ensure strong password policies are enforced.

4. Firewall Configuration:

- Enable Windows Firewall and configure it to allow necessary traffic while blocking unnecessary ports and services.
- Use Group Policy or Windows Defender Firewall with Advanced Security to create specific rules.

5. Antivirus and Malware Protection:

- Install reputable antivirus software and keep it updated regularly.
- Schedule regular scans and configure real-time protection.

6. Remote Desktop Protocol (RDP) Security:

- Change the default RDP port from 3389 to a custom port to deter unauthorized access attempts.
- Implement Network Level Authentication (NLA) for RDP sessions.

7. Data Encryption:

- Use an encryption tool to encrypt sensitive data on the server's drives.
- Ensure that encryption keys are properly managed and stored securely.

8. Auditing and Logging:

- Enable Windows auditing to track and log security events and system activities.
- Configure log settings to store logs securely and regularly review them for suspicious activities.

9. Server Roles and Features:

- Disable or remove unnecessary server roles and features.
- Regularly review installed applications and services, removing or updating those not in use.

10. Backup and Recovery:

- Set up regular backups of critical data and system configurations.
- Test the backup and recovery process periodically to ensure its effectiveness.

11. Physical Security and Access Control:

- Ensure physical access to the server is restricted and monitored.
- Implement measures to protect against unauthorized access to server hardware.

12. Monitoring and Incident Response:

- Deploy intrusion detection systems or monitoring tools to detect and respond to security incidents promptly.
- Develop and regularly update an incident response plan.

Ubuntu OS

1. Overview

This document provides prescriptive guidance for establishing a secure configuration posture for systems with Ubuntu Os.

2. Audience

This document is intended for the Ubuntu System Administrator to implement secure solutions that incorporate Ubuntu Systems.

3. Scope

Revisions to this security baseline will be applicable to builds occurring after the revision date. No retroactive configurations are required as a result of revisions unless otherwise identified as necessary by Information Security Architecture.

4. Hardening Ubuntu Systems

Hardening a Ubuntu System involves securing the system by implementing various measures to reduce its attack surface and enhance its resilience against potential threats. Here's a basic guideline for hardening steps:

1. Change time zone

Control Statement

- It's important to ensure that you select a valid timezone identifier. You can refer to the IANA Time Zone database for a complete list of available time zones.

Risk/Impact

- Changing the time zone can affect the synchronization of time across various services and applications. It is important to ensure that services relying on accurate time information, such as databases, log files, and time-sensitive applications, are properly configured to handle the time zone change. In some cases, a system restart or service restart may be required for the changes to take effect.

2. Add below lines to ~/.bash_history

Control Statement

- The history size determines the number of commands that can be stored in the command history. By increasing the value of history size we can store a larger number of commands. Keep in mind that a larger history size may consume more system resources.

Risk/Impact

- By carefully managing the history size and considering the factors mentioned above, you can strike a balance between usability, security, and resource efficiency in your Ubuntu system.

3. Ensure that the sticky bit should be set on the below mentioned partitions.

Control Statement

- The sticky bit is typically used on directories to control file deletion within that directory by restricting deletion rights to the owner of the file and the directory's owner. The sticky bit does not have an effect on files.

Risk/Impact

- It helps prevent accidental or unauthorized deletion of files within shared directories. However, careful consideration should be given to the purpose and requirements of each directory to avoid unnecessary complications or hindered collaboration.

4. Edit the /etc/fstab file and add nodev, noexec and nosuid to the fourth field (mounting options).

Control Statement

- This file is a critical system configuration file that contains information about filesystems and devices mounted during system boot. It controls the automatic mounting of partitions, network shares, and other filesystems.

Risk/Impact

- It's important to exercise caution and have a thorough understanding of its syntax and the implications of the changes. Incorrect or improper modifications to this file can lead to system boot failures or cause file system errors.

5. Check status for services:

Control Statement

- This will provide detailed information about the service, including its current status, whether it is running or not, any error messages, and the last time it was started or stopped.

Risk/Impact

- The risk and impact of checking the status of services in Ubuntu are generally low. It provides valuable information for troubleshooting and monitoring purposes.

6. Unconfined daemon

Control Statement

- A process running without any confinement or security restrictions imposed by a mandatory access control framework such as AppArmor or SELinux. Controlling an unconfined daemon involves ensuring appropriate security measures are in place.

Risk/Impact

- It's crucial to properly assess the risks associated with unconfined daemons and take appropriate measures to confine and secure them within a mandatory access control framework.
- Confining daemons helps mitigate vulnerabilities, limit access, enforce security policies, and maintain compliance with security standards and regulatory requirements.

7. Network Configuration and Firewalls**Control Statement**

- It's important to follow best practices, such as configuring network interfaces correctly, implementing secure firewall rules, and regularly monitoring and reviewing network and firewall configurations to maintain a secure and well-managed network environment.

Risk/Impact

- By addressing risks and implementing proper security measures, organizations can strengthen their network defenses and mitigate potential impacts on network performance, security, and compliance.

8. IPv6 Networking Protocols**Control Statement**

- IPv6 is a networking protocol that supersedes IPv4. It has more routable addresses and has built in security

Risk/Impact

- It is recommended that systems not accept router advertisements as they could be tricked into routing traffic to compromised machines. Setting hard routes within the system (usually a single default route to a trusted router) protects the system from bad routes.

9. Ensure mounting of FAT filesystems is disabled**Control Statement**

- The FAT filesystem format is primarily used on older windows systems and portable USB drives or flash modules. It comes in three types FAT12, FAT16, and FAT32, all of which are supported by the vfat kernel module

Risk/Impact

- Removing support for unneeded file system types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

10. Logging and Auditing**Configure rsyslog****Control Statement**

- The rsyslog software is recommended as a replacement for the default syslogd daemon and provides improvements over syslogd, such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server.

Risk/Impact

- The security enhancements of rsyslog such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server) justify installing and configuring the package.

11. Configure System Accounting (Optional)**Control Statement**

- System auditing, through auditd, allows system administrators to monitor their systems such that they can detect unauthorized access or modification of data. By default, auditd will audit SELinux AVC denials, system logins, account modifications, and authentication events.
- Events will be logged to /var/log/audit/audit.log. The recording of these events will use a modest amount of disk space on a system. If significantly more events are captured, additional on system or off system storage may need to be allocated.

Risk/Impact

- It is important that an appropriate size is determined for log files so that they do not impact the system and audit data is not lost.

12. System Access, Authentication, and Authorization**Restrict access to Cron****Control Statement**

- The anacron daemon is used on systems that are not up 24x7. The anacron daemon will execute jobs that would have normally been run had the system not been down.

Risk/Impact

- Cron jobs may include critical security or administrative functions that need to run on a regular basis. Use this daemon on machines that are not up 24x7, or if there are jobs that need to be executed after the system has been brought back up after a maintenance window.

13. Configure SSH**Control Statement**

- SSH is a secure, encrypted replacement for common login services such as telnet, ftp, rlogin, rsh, and rcp.

Risk/Impact

- It is strongly recommended that sites abandon older clear-text login protocols and use SSH to prevent session hijacking and sniffing of sensitive data off the network.

14. Configure PAM**Control Statement**

- PAM (Pluggable Authentication Modules) is a service that implements modular Risk/Impact Authentication modules on UNIX systems. PAM is implemented as a set of shared objects that are loaded and executed when a program needs to authenticate a user.
- Files for PAM are typically located in the `/etc/pam.d` directory. PAM must be carefully configured to secure system authentication. While this section covers some of PAM, please consult other PAM resources to fully understand the configuration capabilities.

Risk/Impact

- The SHA-512 algorithm provides much stronger hashing than MD5, thus providing additional protection to the system by increasing the level of effort for an attacker to successfully determine passwords.

15. Restrict Access to the su Command**Control Statement**

- The su command allows a user to run a command or shell as another user. The program has been superseded by sudo, which allows for more granular control over privileged access. Normally, the su command can be executed by any user.
- By uncommenting the `pam_wheel.so` statement in `/etc/pam.d/su`, the su command will only allow users in the wheel group to execute su.

Risk/Impact

- Restricting the use of su, and using sudo in its place, provides system administrators better control of the escalation of user privileges to execute privileged commands. The sudo utility also provides a better logging and audit mechanism, as it can log each command executed via sudo, whereas su can only record that a user executed the su program.

16. User Accounts and Environment**Set Shadow Password Suite Parameters****Control Statement**

- While a majority of the password control parameters have been moved to PAM, some parameters are still available through the shadow password suite
- Any changes made to `/etc/login.defs` will only be applied if the `usermod` command is used.
- If userIDs are added a different way, use the `chage` command to effect changes to individual userIDs.

Risk/Impact

This may lead to increased chances of brute force attacks.

17. Disable System Accounts**Control Statement**

- There are a number of accounts provided with the ubuntu that are used to manage applications and are not intended to provide an interactive shell.

Risk/Impact

- It is important to make sure that accounts that are not being used by regular users are locked to prevent them from being used to provide an interactive shell.
- By default, Ubuntu sets the password field for these accounts to an invalid string, but it is also recommended that the shell field in the password file be set to /choice/nologin.
- This prevents the account from potentially being used to run any commands.

18. Set Default Group for root Account**Control Statement**

- The usermod command can be used to specify which group the root user belongs to. This affects permissions of files that are created by the root user.

Risk/Impact

- Using GID 0 for the root account helps prevent root-owned files from accidentally becoming accessible to non-privileged users.

19. Set Default umask for Users**Control Statement**

- The default umask determines the permissions of files created by users. The user creating the file has the discretion of making their files and directories readable by others via the chmod command. Users who wish to allow their files and directories to be readable by others by default may choose a different default umask by inserting the umask command into the standard shell configuration files (.profile, .cshrc, etc.) in their home directories.

Risk/Impact

- Setting a very secure default value for umask ensures that users make a conscious choice about their file permissions.
- A default umask setting of 077 causes files and directories created by users to not be readable by any other user on the system. A umask of 027 would make files and directories readable by users in the same Unix group, while a umask of 022 would make files readable by every user on the system.

20. Lock Inactive User Accounts**Control Statement**

- User accounts that have been inactive for over a given period of time can be automatically disabled. It is recommended that accounts that are inactive for 35 or more days be disabled.

Risk/Impact

- Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

21. Warning Banners**Set Warning Banner for Standard Login Services****Control Statement**

- The contents of the /etc/issue file are displayed prior to the login prompt on the system's console and serial devices, and also prior to logins via telnet. The contents of the /etc/motd file is generally displayed after all successful logins, no matter where the user is logging in from, but is thought to be less useful because it only provides notification to export HISTTIMEFORMAT="%F %T "the user after the machine has been accessed.

Risk/Impact

- Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Consult with your organization's legal counsel for the appropriate wording for your specific organization.

-

22. Remove OS Information from Login Warning Banners**Control Statement**

- Unix-based systems have typically displayed information about the OS release and patch level upon logging into the system. This information can be useful to developers who are developing software for a particular OS platform.
- If mingetty(8) supports the following options, they display operating system information: \m - machine architecture (uname -m)
\r - operating system release (uname -r)
\s - operating system name
\v - operating system version (uname -v)

Risk/Impact

- Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system.
- Authorized users can easily get this information by running the "uname -a" command once they have logged in.

23. System Maintenance**Control Statement**

- Ensure proper system maintenance practices are followed to optimize system performance, reliability, and security.
- Conducting regular monitoring and reviews, organizations can effectively maintain their systems, optimize performance, ensure data integrity, and mitigate security risks.

Risk/Impact

- Proper planning, risk assessment, and adherence to best practices can help mitigate these risks and minimize the potential impact of system maintenance.
- Regular backups, thorough testing, communication with stakeholders, and following established change management processes are essential to ensure smooth and secure maintenance activities.

24. Review User and Group Settings

Control Statement

- This section provides guidance on securing aspects of the users and groups.

Risk/Impact

- All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user.

25. Encryption

Restrict Cipher list

Control Statement

- Based on research conducted at various institutions, it was determined that the symmetric portion of the SSH Transport Protocol (as described in RFC 4253) has security weaknesses that allowed recovery of up to 32 bits of plaintext from a block of ciphertext that was encrypted with the Cipher Block Chaining (CBD) method.

Risk/Impact

- Data will be communicated in plain text and unauthorized users may try to perform MitM attacks.

26. Enable TLS 1.2 & Above protocol

Control Statement

- Strong protocol ensures the message communicated between client and server must be in an encrypted way so that data integrity will not be affected. In order to encrypt handshake data, strong protocol must be enabled on the system.

Risk/Impact

- Data will be communicated in plain text and unauthorized users may try to perform MitM attacks.

27. Disable weak encryption protocol

Control Statement

- Strong protocol provides that the message communicated between client and server must be in an encrypted way so that data integrity will not be affected. In order to encrypt handshake data, strong protocol must be enabled on the system.

Risk/Impact

- Data will be communicated in plain text and unauthorized users may try to perform MitM attacks.

28. Install RKhunter

Control Statement

- Rkhunter is a shell script which carries out various checks on the local system to try and detect known rootkits and malware. It also performs checks to see if commands have been modified, if the system startup files have been modified, and various checks on the network interfaces, including checks for listening applications.

Risk/Impact

- Rootkit scanner is scanning tool to ensure you for about 99.9%* you're clean of nasty tools.
- This tool scans for rootkits, backdoors and local exploits by running tests like:
 - Looks for default files used by rootkits
 - Wrong file permissions for binaries
 - Looks for suspected strings in LKM and KLD modules
 - Looks for hidden files

29. Ensure ptrace_scope is restricted (Automated)**Control Statement**

- The ptrace() system call provides a means by which one process (the "tracer") may observe and control the execution of another process (the "tracee"), and examine and change the tracee's memory and registers.

Risk/Impact

- If one application is compromised, it would be possible for an attacker to attach to other running processes (e.g. Bash, Firefox, SSH sessions, GPG agent, etc) to extract additional credentials and continue to expand the scope of their attack.

30. Ensure core dumps are restricted (Automated)

Control Statement

- A core dump is the memory of an executable program. It is generally used to determine why a program aborted. It can also be used to glean confidential information from a core file. The system provides the ability to set a soft limit for core dumps, but this can be overridden by the user.

Risk/Impact

- Setting a hard limit on core dumps prevents users from overriding the soft variable. If core dumps are required, consider setting limits for user groups. In addition, setting the `fs.suid_dumpable` variable to 0 will prevent setuid programs from dumping core.

