Amazon Inspector - Assessment Report

Findings Report

Report generated on 2024-06-03 at 17:03:33 UTC

Assessment Template: Assessment Template 2024

Assessment Run start: 2024-06-03 at 16:41:40 UTC
Assessment Run end: 2024-06-03 at 16:59:49 UTC

Section 1: Executive Summary

This is an Inspector assessment report for an assessment started on 2024-06-03 16:41:40 UTC for assessment template 'Assessment Template 2024'. The assessment target included 1 instances, and was tested against 4 Rules Packages.

The assessment target is defined using the following EC2 tags

Key	Value

The following Rules Packages were assessed. A total of 103 findings were created, with the following distribution by severity:

Rules Package	High	Medium	Low	Informational
CIS Operating System Security Configuration Benchmarks-1.0	90	0	0	8
Common Vulnerabilities and Exposures-1.1	0	0	0	0
Network Reachability-1.1	0	0	0	4
Security Best Practices-1.0	0	1	0	0

Section 2: What is Tested

This section details the Rules Packages included in this assessment run, and the EC2 instances included in the assessment target.

2.1: Rules Packages - Count: 4

2.1.1: CIS Operating System Security Configuration Benchmarks-1.0

Description: The CIS Security Benchmarks program provides well-defined, un-biased and consensus-based industry best practices to help organizations assess and improve their security.

The rules in this package help establish a secure configuration posture for the following operating systems:

- Amazon Linux 2 (CIS Benchmark for Amazon Linux 2 Benchmark v1.0.0 Level 1)
- Amazon Linux 2 (CIS Benchmark for Amazon Linux 2 Benchmark v1.0.0 Level 2)
- Ubuntu Linux 18.04 LTS (CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 1 Server)
- Ubuntu Linux 18.04 LTS (CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 2 Server)
- Ubuntu Linux 18.04 LTS (CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 1 Workstation)
- Ubuntu Linux 18.04 LTS (CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 2 Workstation)
- Amazon Linux version 2015.03 (CIS benchmark v1.1.0)
- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Domain Controller)
- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Member Server Profile)

- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows Server 2012 R2, v2.2.0, Level 1 Member Server Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows Server 2012 R2, v2.2.0, Level 1 Domain Controller Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows Server 2012 non-R2, v2.0.0, Level 1 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows Server 2012 non-R2, v2.0.0, Level 1 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows Server 2016 RTM (Release 1607), v1.1.0, Level 1 Member Server Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows Server 2016 RTM (Release 1607), v1.1.0, Level 2 Member Server Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows Server 2016 RTM (Release 1607), v1.1.0, Level 1 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows Server 2016 RTM (Release 1607), v1.1.0, Level 2 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows Server 2016 RTM (Release 1607), v1.1.0, Next Generation Windows Security Profile)
- Amazon Linux (CIS Benchmark for Amazon Linux Benchmark v2.1.0 Level 1)
- Amazon Linux (CIS Benchmark for Amazon Linux Benchmark v2.1.0 Level 2)
- CentOS Linux 7 (CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 1 Server)
- CentOS Linux 7 (CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 2 Server)
- CentOS Linux 7 (CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 1 Workstation)
- CentOS Linux 7 (CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 2 Workstation)
- Red Hat Enterprise Linux 7 (CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 1 Server)
- Red Hat Enterprise Linux 7 (CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 2 Server)
- Red Hat Enterprise Linux 7 (CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 1 Workstation)
- Red Hat Enterprise Linux 7 (CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 2 Workstation)

- Ubuntu Linux 16.04 LTS (CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 1 Server)
- Ubuntu Linux 16.04 LTS (CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 2 Server)
- Ubuntu Linux 16.04 LTS (CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 1 Workstation)
- Ubuntu Linux 16.04 LTS (CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 2 Workstation)
- CentOS Linux 6 (CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2, Level 1 Server)
- CentOS Linux 6 (CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2, Level 2 Server)
- CentOS Linux 6 (CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2, Level 1 Workstation)
- CentOS Linux 6 (CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2, Level 2 Workstation)
- Red Hat Enterprise Linux 6 (CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2, Level 1 Server)
- Red Hat Enterprise Linux 6 (CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2, Level 2 Server)
- Red Hat Enterprise Linux 6 (CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2, Level 1 Workstation)
- Red Hat Enterprise Linux 6 (CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 2 Workstation)
- Ubuntu Linux 14.04 LTS (CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0, Level 1 Server)
- Ubuntu Linux 14.04 LTS (CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0, Level 2 Server)
- Ubuntu Linux 14.04 LTS (CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0, Level 1 Workstation)
- Ubuntu Linux 14.04 LTS (CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0, Level 2 Workstation)

If a particular CIS benchmark appears in a finding produced by an Amazon Inspector assessment run, you can download a detailed PDF description of the benchmark from https://benchmarks.cisecurity.org/ (free registration

required). The benchmark document provides detailed information about this CIS benchmark, its severity, and how to mitigate it.
Provider: Amazon Web Services, Inc.
Version: 1.0

2.1.2: Common Vulnerabilities and Exposures-1.1

Description: The rules in this package help verify whether the EC2 instances in your application are exposed to Common Vulnerabilities and Exposures (CVEs). Attacks can exploit unpatched vulnerabilities to compromise the confidentiality, integrity, or availability of your service or data. The CVE system provides a reference for publicly known information security vulnerabilities and exposures. For more information, see https://cve.mitre.org/. If a particular CVE appears in one of the produced Findings at the end of a completed Inspector assessment, you can search https://cve.mitre.org/ using the CVE's ID (for example, "CVE-2009-0021") to find detailed information about this CVE, its severity, and how to mitigate it.
Provider: Amazon Web Services, Inc.
Version: 1.1

2.1.3: Network Reachability-1.1

Description: These rules analyze the reachability of your instances over the network. Attacks can exploit your instances over the network by accessing services that are listening on open ports. These rules evaluate the security your host configuration in AWS to determine if it allows access to ports and services over the network. For reachable ports and services, the Amazon Inspector findings identify where they can be reached from, and provide guidance on how to restrict access to these ports.
Provider: Amazon Web Services, Inc.
Version: 1.1

2.1.4: Security Best Practices-1.0

Description: The rules in this package help determine whether your systems are configured securely.
Provider: Amazon Web Services, Inc.

Version: 1.0

2.2: Assessment Target - Assessment Template 2024

2.2.1: EC2 Tags:

The following EC2 tags (Key/Value pairs) were used to define this assessment target.

Key	Value

2.2.2: Instances - Count 1

Instance ID
i-098025956ed3541cf

Section 3: Findings Summary

This section lists the rules that generated findings, the severity of the finding, and the number of instances affected. More details about the findings can be found in the "Findings Details" section. Rules that passed on all target instances available during the assessment run are listed in the "Passed Rules" section.

3.1: Findings table - CIS Operating System Security Configuration Benchmarks-1.0

3.1.1 Level 1

Rule	Severity	Failed
1.1.2 Ensure /tmp is configured	High	1
1.1.17 Ensure noexec option set on /dev/shm partition	High	1
1.1.1.1 Ensure mounting of cramfs filesystems is disabled	High	1
1.1.1.2 Ensure mounting of hfs filesystems is disabled	High	1
1.1.1.3 Ensure mounting of hfsplus filesystems is disabled	High	1
1.1.1.4 Ensure mounting of squashfs filesystems is disabled	High	1
1.1.1.5 Ensure mounting of udf filesystems is disabled	High	1
1.3.1 Ensure AIDE is installed	High	1
1.3.2 Ensure filesystem integrity is regularly checked	High	1
1.5.1 Ensure core dumps are restricted	High	1
1.5.2 Ensure address space layout randomization (ASLR) is enabled	High	1
1.7.1.1 Ensure message of the day is configured properly	High	1
1.7.1.2 Ensure local login warning banner is configured properly	Informational	1
1.7.1.3 Ensure remote login warning banner is configured properly	Informational	1
2.1.1.3 Ensure chrony is configured	High	1
3.1.1 Ensure IP forwarding is disabled	High	1
3.1.2 Ensure packet redirect sending is disabled	High	1
3.2.1 Ensure source routed packets are not accepted	High	1
3.2.2 Ensure ICMP redirects are not accepted	High	1
3.2.3 Ensure secure ICMP redirects are not accepted	High	1
3.2.4 Ensure suspicious packets are logged	High	1
3.2.5 Ensure broadcast ICMP requests are ignored	High	1

3.2.6 Ensure bogus ICMP responses are ignored	High	1
3.2.7 Ensure Reverse Path Filtering is enabled	High	1
3.2.8 Ensure TCP SYN Cookies is enabled	High	1
3.2.9 Ensure IPv6 router advertisements are not accepted	High	1
3.3.3 Ensure /etc/hosts.deny is configured	Informational	1
3.4.1 Ensure DCCP is disabled	Informational	1
3.4.2 Ensure SCTP is disabled	Informational	1
3.4.3 Ensure RDS is disabled	Informational	1
3.4.4 Ensure TIPC is disabled	Informational	1
3.5.1.1 Ensure default deny firewall policy	High	1
3.5.1.2 Ensure loopback traffic is configured	High	1
3.5.1.4 Ensure firewall rules exist for all open ports	High	1
3.5.2.1 Ensure IPv6 default deny firewall policy	High	1
3.5.2.2 Ensure IPv6 loopback traffic is configured	High	1
4.2.4 Ensure permissions on all logfiles are configured	High	1
4.2.1.3 Ensure rsyslog default file permissions configured	High	1
4.2.1.4 Ensure rsyslog is configured to send logs to a remote log host	High	1
5.6 Ensure access to the su command is restricted	High	1
5.1.2 Ensure permissions on /etc/crontab are configured	High	1
5.1.3 Ensure permissions on /etc/cron.hourly are configured	High	1
5.1.4 Ensure permissions on /etc/cron.daily are configured	High	1
5.1.5 Ensure permissions on /etc/cron.weekly are configured	High	1
5.1.6 Ensure permissions on /etc/cron.monthly are configured	High	1
5.1.7 Ensure permissions on /etc/cron.d are configured	High	1
5.1.8 Ensure at/cron is restricted to authorized users	High	1
5.2.4 Ensure SSH Protocol is set to 2	High	1
5.2.5 Ensure SSH LogLevel is appropriate	High	1
5.2.7 Ensure SSH MaxAuthTries is set to 4 or less	High	1
5.2.8 Ensure SSH IgnoreRhosts is enabled	High	1
5.2.9 Ensure SSH HostbasedAuthentication is disabled	High	1
5.2.10 Ensure SSH root login is disabled	High	1
5.2.11 Ensure SSH PermitEmptyPasswords is disabled	High	1
5.2.12 Ensure SSH PermitUserEnvironment is disabled	High	1
5.2.13 Ensure only strong ciphers are used	High	1
5.2.14 Ensure only strong MAC algorithms are used	High	1
5.2.15 Ensure that strong Key Exchange algorithms are used	High	1
5.2.16 Ensure SSH Idle Timeout Interval is configured	High	1
5.2.17 Ensure SSH LoginGraceTime is set to one minute or less	High	1
5.2.18 Ensure SSH access is limited	High	1

5.2.19 Ensure SSH warning banner is configured	High	1
5.3.1 Ensure password creation requirements are configured	High	1
5.3.2 Ensure lockout for failed password attempts is configured	High	1
5.3.3 Ensure password reuse is limited	High	1
5.4.4 Ensure default user umask is 027 or more restrictive	High	1
5.4.1.1 Ensure password expiration is 365 days or less	High	1
5.4.1.2 Ensure minimum days between password changes is 7 or more	High	1
5.4.1.4 Ensure inactive password lock is 30 days or less	High	1

3.1.2 Level 2

Rule	Severity	Failed
1.1.2 Ensure /tmp is configured	High	1
1.1.6 Ensure separate partition exists for /var	High	1
1.1.7 Ensure separate partition exists for /var/tmp	High	1
1.1.11 Ensure separate partition exists for /var/log	High	1
1.1.12 Ensure separate partition exists for /var/log/audit	High	1
1.1.13 Ensure separate partition exists for /home	High	1
1.1.17 Ensure noexec option set on /dev/shm partition	High	1
1.1.1.1 Ensure mounting of cramfs filesystems is disabled	High	1
1.1.1.2 Ensure mounting of hfs filesystems is disabled	High	1
1.1.1.3 Ensure mounting of hfsplus filesystems is disabled	High	1
1.1.1.4 Ensure mounting of squashfs filesystems is disabled	High	1
1.1.1.5 Ensure mounting of udf filesystems is disabled	High	1
1.3.1 Ensure AIDE is installed	High	1
1.3.2 Ensure filesystem integrity is regularly checked	High	1
1.5.1 Ensure core dumps are restricted	High	1
1.5.2 Ensure address space layout randomization (ASLR) is enabled	High	1
1.6.1.2 Ensure the SELinux state is enforcing	High	1
1.6.1.3 Ensure SELinux policy is configured	High	1
1.6.1.6 Ensure no unconfined daemons exist	High	1
1.7.1.1 Ensure message of the day is configured properly	High	1
1.7.1.2 Ensure local login warning banner is configured properly	Informational	1
1.7.1.3 Ensure remote login warning banner is configured properly	Informational	1
2.1.1.3 Ensure chrony is configured	High	1
3.6 Disable IPv6	Informational	1
3.1.1 Ensure IP forwarding is disabled	High	1
3.1.2 Ensure packet redirect sending is disabled	High	1
3.2.1 Ensure source routed packets are not accepted	High	1

3.2.2 Ensure ICMP redirects are not accepted	High	1
3.2.3 Ensure secure ICMP redirects are not accepted	High	1
3.2.4 Ensure suspicious packets are logged	High	1
3.2.5 Ensure broadcast ICMP requests are ignored	High	1
3.2.6 Ensure bogus ICMP responses are ignored	High	1
3.2.7 Ensure Reverse Path Filtering is enabled	High	1
3.2.8 Ensure TCP SYN Cookies is enabled	High	1
3.2.9 Ensure IPv6 router advertisements are not accepted	High	1
3.3.3 Ensure /etc/hosts.deny is configured	Informational	1
3.4.1 Ensure DCCP is disabled	Informational	1
3.4.2 Ensure SCTP is disabled	Informational	1
3.4.3 Ensure RDS is disabled	Informational	1
3.4.4 Ensure TIPC is disabled	Informational	1
3.5.1.1 Ensure default deny firewall policy	High	1
3.5.1.2 Ensure loopback traffic is configured	High	1
3.5.1.4 Ensure firewall rules exist for all open ports	High	1
3.5.2.1 Ensure IPv6 default deny firewall policy	High	1
3.5.2.2 Ensure IPv6 loopback traffic is configured	High	1
4.1.3 Ensure auditing for processes that start prior to auditd is enabled	High	1
4.1.4 Ensure events that modify date and time information are collected	High	1
4.1.5 Ensure events that modify user/group information are collected	High	1
4.1.6 Ensure events that modify the system's network environment are collected	High	1
4.1.7 Ensure events that modify the system's Mandatory Access Controls are collected	High	1
4.1.8 Ensure login and logout events are collected	High	1
4.1.9 Ensure session initiation information is collected	High	1
4.1.10 Ensure discretionary access control permission modification events are collected	High	1
4.1.11 Ensure unsuccessful unauthorized file access attempts are collected	High	1
4.1.12 Ensure use of privileged commands is collected	High	1
4.1.13 Ensure successful file system mounts are collected	High	1
4.1.14 Ensure file deletion events by users are collected	High	1
4.1.15 Ensure changes to system administration scope (sudoers) is collected	High	1
4.1.16 Ensure system administrator actions (sudolog) are collected	High	1
4.1.17 Ensure kernel module loading and unloading is collected	High	1
4.1.18 Ensure the audit configuration is immutable	High	1
4.1.1.2 Ensure system is disabled when audit logs are full	High	1

4.1.1.3 Ensure audit logs are not automatically deleted	High	1
4.2.4 Ensure permissions on all logfiles are configured	High	1
4.2.1.3 Ensure rsyslog default file permissions configured	High	1
4.2.1.4 Ensure rsyslog is configured to send logs to a remote log host	High	1
5.6 Ensure access to the su command is restricted	High	1
5.1.2 Ensure permissions on /etc/crontab are configured	High	1
5.1.3 Ensure permissions on /etc/cron.hourly are configured	High	1
5.1.4 Ensure permissions on /etc/cron.daily are configured	High	1
5.1.5 Ensure permissions on /etc/cron.weekly are configured	High	1
5.1.6 Ensure permissions on /etc/cron.monthly are configured	High	1
5.1.7 Ensure permissions on /etc/cron.d are configured	High	1
5.1.8 Ensure at/cron is restricted to authorized users	High	1
5.2.4 Ensure SSH Protocol is set to 2	High	1
5.2.5 Ensure SSH LogLevel is appropriate	High	1
5.2.6 Ensure SSH X11 forwarding is disabled	High	1
5.2.7 Ensure SSH MaxAuthTries is set to 4 or less	High	1
5.2.8 Ensure SSH IgnoreRhosts is enabled	High	1
5.2.9 Ensure SSH HostbasedAuthentication is disabled	High	1
5.2.10 Ensure SSH root login is disabled	High	1
5.2.11 Ensure SSH PermitEmptyPasswords is disabled	High	1
5.2.12 Ensure SSH PermitUserEnvironment is disabled	High	1
5.2.13 Ensure only strong ciphers are used	High	1
5.2.14 Ensure only strong MAC algorithms are used	High	1
5.2.15 Ensure that strong Key Exchange algorithms are used	High	1
5.2.16 Ensure SSH Idle Timeout Interval is configured	High	1
5.2.17 Ensure SSH LoginGraceTime is set to one minute or less	High	1
5.2.18 Ensure SSH access is limited	High	1
5.2.19 Ensure SSH warning banner is configured	High	1
5.3.1 Ensure password creation requirements are configured	High	1
5.3.2 Ensure lockout for failed password attempts is configured	High	1
5.3.3 Ensure password reuse is limited	High	1
5.4.4 Ensure default user umask is 027 or more restrictive	High	1
5.4.5 Ensure default user shell timeout is 900 seconds or less	High	1
5.4.1.1 Ensure password expiration is 365 days or less	High	1
5.4.1.2 Ensure minimum days between password changes is 7 or more	High	1
5.4.1.4 Ensure inactive password lock is 30 days or less	High	1

3.2: Findings table - Common Vulnerabilities and Exposures-1.1

No findings were generated for this rules package.

3.3: Findings table - Network Reachability-1.1

Rule	Severity	Failed
TCP port 20 (FTP) is reachable from the internet with no listener on instance	Informational	1
TCP port 21 (FTP) is reachable from the internet with no listener on instance	Informational	1
TCP port 22 (SSH) is reachable from the internet with active listener on instance	Informational	1
TCP port 23 (Telnet) is reachable from the internet with no listener on instance	Informational	1

3.4: Findings table - Security Best Practices-1.0

Rule	Severity	Failed
Disable root login over SSH	Medium	1

Section 4: Findings Details

This section details the findings generated in this assessment run, and the instances that generated the finding. If an instance is not listed here, that means it was checked and passed.

4.1: Findings details - CIS Operating System Security Configuration Benchmarks-1.0

4.1.1 Level 1

1.1.2 Ensure /tmp is configured

Severity
High

Description
Description The /tmp directory is a world-writable directory used for temporary storage by all users and some applications. Rationale Making /tmp its own file system allows an administrator to set the noexec option on the mount, making /tmp useless for an attacker to install executable code. It would also prevent an attacker from establishing a hardlink to a system setuid program and wait for it to be updated. Once the program was updated, the hardlink would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw. This can be accomplished by either mounting tmpfs to /tmp, or creating a separate partition for /tmp.

Recommendation
Configure /etc/fstab as appropriate. example:tmpfs /tmp tmpfs defaults,rw,nosuid,nodev ,noexec,relatime 0 0 or Run the following commands to enable systemd /tmp mounting: systemctl unmask tmp.mountsystemctl enable tmp.mount Edit /etc/systemd/system/ local-fs.target.wants/tmp.mount to configure the /tmp mount: [Mount]What=tmpfsWhe re=/tmpType=tmpfsOptions=mode=1777,strictatime,noexec,nodev,nosuid Impact: Since the /tmp directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to a separate partition.Running out of /tmp space is a

problem regardless of what kind of filesystem lies under it, but in a default installation a disk-based /tmp will essentially have the whole disk available, as it only creates a single / partition. On the other hand, a RAM-based /tmp as with tmpfs will almost certainly be much smaller, which can lead to applications filling up the filesystem much more easily./tmp utalizing tmpfs can be resized using the size={size} parameter on the Options line on the tmp.mount file

Failed Instances
i-098025956ed3541cf

1.1.17 Ensure noexec option set on /dev/shm partition

Severity
High

Description
Description The noexec mount option specifies that the filesystem cannot contain executable binaries. Rationale Setting this option on a file system prevents users from executing programs from shared memory. This deters users from introducing potentially malicious software on the system.

Recommendation
Edit the /etc/fstab file and add noexec to the fourth field (mounting options) for the /dev/shm partition. See the fstab(5) manual page for more information. Run the following command to remount /dev/shm : # mount -o remount,noexec /dev/shm

Failed Instances
i-098025956ed3541cf

1.1.1.1 Ensure mounting of cramfs filesystems is disabled

Severity
High

Description
Description The cramfs filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems. A cramfs image can be used without having to first decompress the image. Rationale Removing support for unneeded filesystem types reduces the local attack surface of the server. If this filesystem type is not needed, disable it.

Recommendation
Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/cramfs.conf and add the following line: install cramfs /bin/true Run the following command to unload the cramfs module: # rmmod cramfs

Failed Instances
i-098025956ed3541cf

1.1.1.2 Ensure mounting of hfs filesystems is disabled

Severity
High

Description
Description The hfs filesystem type is a hierarchical filesystem that allows you to mount Mac OS filesystems. Rationale Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Recommendation
Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/hfs.conf and add the following line: install hfs /bin/true Run the following command to unload the hfs module: # rmmod hfs

Failed Instances
i-098025956ed3541cf

1.1.1.3 Ensure mounting of hfsplus filesystems is disabled

Severity
High

Description
Description The hfsplus filesystem type is a hierarchical filesystem designed to replace hfs that allows you to mount Mac OS filesystems. Rationale Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Recommendation

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/hfsplus.conf and add the following line: install hfsplus /bin/true Run the following command to unload the hfsplus module: # rmmod hfsplus

Failed Instances
i-098025956ed3541cf

1.1.1.4 Ensure mounting of squashfs filesystems is disabled

Severity
High

Description
Description The squashfs filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems (similar to cramfs). A squashfs image can be used without having to first decompress the image. Rationale Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Recommendation
Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/squashfs.conf and add the following line: install squashfs /bin/true Run the following command to unload the squashfs module: # rmmod squashfs

Failed Instances
i-098025956ed3541cf

1.1.1.5 Ensure mounting of udf filesystems is disabled

Severity
High

Description
Description The udf filesystem type is the universal disk format used to implement ISO/IEC 13346 and ECMA-167 specifications. This is an open vendor filesystem type for data storage on a broad range of media. This filesystem type is necessary to support writing DVDs and newer optical disc formats. Rationale Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Recommendation
Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/udf.conf and add the following line: install udf /bin/true Run the following command to unload the udf module: # rmmod udf

Failed Instances
i-098025956ed3541cf

1.3.1 Ensure AIDE is installed

Severity
High

Description
Description AIDE takes a snapshot of filesystem state including modification times, permissions, and file hashes which can then be used to compare against the current state of the filesystem to detect modifications to the system. Rationale By monitoring the filesystem state compromised files can be detected to prevent or limit the exposure of accidental or malicious misconfigurations or modified binaries.

Recommendation
Run the following command to install aide : # yum install aide Configure AIDE as appropriate for your environment. Consult the AIDE documentation for options. Initialize AIDE: # aide --init# mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz

Failed Instances
i-098025956ed3541cf

1.3.2 Ensure filesystem integrity is regularly checked

Severity
High

Description
Description Periodic checking of the filesystem integrity is needed to detect changes to the filesystem. Rationale Periodic file checking allows the system administrator to determine on a regular basis if critical files have been changed in an unauthorized fashion.

Recommendation

Run the following command: # crontab -u root -e Add the following line to the crontab: 0 5 * * * /usr/sbin/aide --check

Failed Instances
i-098025956ed3541cf

1.5.1 Ensure core dumps are restricted

Severity
High

Description
Description 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. Rationale 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 (see limits.conf(5)). In addition, setting the fs.suid_dumpable variable to 0 will prevent setuid programs from dumping core.

Recommendation
Add the following line to /etc/security/limits.conf or a /etc/security/limits.d/* file: * hard core 0 Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file: fs.suid_dumpable = 0 Run the following command to set the active kernel parameter: # sysctl -w fs.suid_dumpable=0

Failed Instances
i-098025956ed3541cf

1.5.2 Ensure address space layout randomization (ASLR) is enabled

Severity
High

Description
Description Address space layout randomization (ASLR) is an exploit mitigation technique which randomly arranges the address space of key data areas of a process. Rationale Randomly placing virtual memory regions will make it difficult to write memory page exploits as the memory placement will be consistently shifting.

Recommendation
Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file: kernel.randomize_va_space = 2 Run the following command to set the active kernel parameter: # sysctl -w kernel.randomize_va_space=2

Failed Instances
i-098025956ed3541cf

1.7.1.1 Ensure message of the day is configured properly

Severity
High

Description
Description The contents of the /etc/motd file are displayed to users after login and function as a message of the day for authenticated users. Unix-based systems have typically displayed information about the OS release and patch level upon logging in to 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 \r - operating system release \s - operating system name \v - operating system version Rationale 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. 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.

Recommendation
Edit the /etc/motd file with the appropriate contents according to your site policy, remove any instances of \m , \r , \s ,\v. , or references to the OS platform

Failed Instances
i-098025956ed3541cf

1.7.1.2 Ensure local login warning banner is configured properly

Severity
Informational

Description

Description The contents of the /etc/issue file are displayed to users prior to login for local terminals. Unix-based systems have typically displayed information about the OS release and patch level upon logging in to 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 \r - operating system release \s - operating system name \v - operating system version Rationale 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. 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.

Recommendation

Edit the /etc/issue file with the appropriate contents according to your site policy, remove any instances of \m , \r , \s , \v or references to the OS platform: # echo "Authorized uses only. All activity may be monitored and reported." > /etc/issue

Failed Instances

i-098025956ed3541cf

1.7.1.3 Ensure remote login warning banner is configured properly

Severity

Informational

Description

Description The contents of the /etc/issue.net file are displayed to users prior to login for remote connections from configured services. Unix-based systems have typically displayed information about the OS release and patch level upon logging in to 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 \r - operating system release \s - operating system name \v - operating system version Rationale 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. 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.

Recommendation
Edit the /etc/issue.net file with the appropriate contents according to your site policy, remove any instances of \m , \r , \s , or \v , or references to the OS platform: # echo "Authorized uses only. All activity may be monitored and reported." > /etc/issue.net

Failed Instances
i-098025956ed3541cf

2.1.1.3 Ensure chrony is configured

Severity
High

Description
Description chrony is a daemon which implements the Network Time Protocol (NTP) is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate. More information on chrony can be found at http://chrony.tuxfamily.org/. chrony can be configured to be a client and/or a server. Rationale If chrony is in use on the system proper configuration is vital to ensuring time synchronization is working properly. This recommendation only applies if chrony is in use on the system.

Recommendation
Add or edit server or pool lines to /etc/chrony.conf as appropriate: server <remote-server> Add or edit the OPTIONS in /etc/sysconfig/chronyd to include '-u chrony': OPTIONS="-u chrony"

Failed Instances
i-098025956ed3541cf

3.1.1 Ensure IP forwarding is disabled

Severity
High

Description

Description The net.ipv4.ip_forward and net.ipv6.conf.all.forwarding flags are used to tell the system whether it can forward packets or not. Rationale Setting the flags to 0 ensures that a system with multiple interfaces (for example, a hard proxy), will never be able to forward packets, and therefore, never serve as a router.

Recommendation
Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.ip_forward = 0net.ipv6.conf.all.forwarding = 0 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.ip_forward=0# sysctl -w net.ipv6.conf.all.forwarding=0# sysctl -w net.ipv4.route.flush=1# sysctl -w net.ipv6.route.flush=1

Failed Instances
i-098025956ed3541cf

3.1.2 Ensure packet redirect sending is disabled

Severity
High

Description
Description ICMP Redirects are used to send routing information to other hosts. As a host itself does not act as a router (in a host only configuration), there is no need to send redirects. Rationale An attacker could use a compromised host to send invalid ICMP redirects to other router devices in an attempt to corrupt routing and have users access a system set up by the attacker as opposed to a valid system.

Recommendation
Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.conf.all.send_redirects = 0net.ipv4.conf.default.send_redirects = 0 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.conf.all.send_redirects=0# sysctl -w net.ipv4.conf.default.send_redirects=0# sysctl -w net.ipv4.route.flush=1

Failed Instances
i-098025956ed3541cf

3.2.1 Ensure source routed packets are not accepted

Severity

High

Description
Description In networking, source routing allows a sender to partially or fully specify the route packets take through a network. In contrast, non-source routed packets travel a path determined by routers in the network. In some cases, systems may not be routable or reachable from some locations (e.g. private addresses vs. Internet routable), and so source routed packets would need to be used. Rationale Setting net.ipv4.conf.all.accept_source_route, net.ipv4.conf.default.accept_source_route, net.ipv6.conf.all.accept_source_route and net.ipv6.conf.default.accept_source_route to 0 disables the system from accepting source routed packets. Assume this system was capable of routing packets to Internet routable addresses on one interface and private addresses on another interface. Assume that the private addresses were not routable to the Internet routable addresses and vice versa. Under normal routing circumstances, an attacker from the Internet routable addresses could not use the system as a way to reach the private address systems. If, however, source routed packets were allowed, they could be used to gain access to the private address systems as the route could be specified, rather than rely on routing protocols that did not allow this routing.

Recommendation
Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.conf.all.accept_source_route = 0net.ipv4.conf.default.accept_source_route = 0net.ipv6.conf.all.accept_source_route = 0net.ipv6.conf.default.accept_source_route = 0 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.conf.all.accept_source_route=0# sysctl -w net.ipv4.conf.default.accept_source_route=0# sysctl -w net.ipv6.conf.all.accept_source_route=0# sysctl -w net.ipv6.conf.default.accept_source_route=0# sysctl -w net.ipv4.route.flush=1# sysctl -w net.ipv6.route.flush=1

Failed Instances
i-098025956ed3541cf

3.2.2 Ensure ICMP redirects are not accepted

Severity
High

Description
Description ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of

allowing an outside routing device to update your system routing tables. By setting net.ipv4.conf.all.accept_redirects and net.ipv6.conf.all.accept_redirects to 0, the system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables. Rationale Attackers could use bogus ICMP redirect messages to maliciously alter the system routing tables and get them to send packets to incorrect networks and allow your system packets to be captured.

Recommendation
Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.conf.all.accept_redirects = 0net.ipv4.conf.default.accept_redirects = 0net.ipv6.conf.all.accept_redirects = 0net.ipv6.conf.default.accept_redirects = 0 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.conf.all.accept_redirects=0# sysctl -w net.ipv4.conf.default.accept_redirects=0# sysctl -w net.ipv6.conf.all.accept_redirects=0# sysctl -w net.ipv6.conf.default.accept_redirects=0# sysctl -w net.ipv4.route.flush=1# sysctl -w net.ipv6.route.flush=1

Failed Instances
i-098025956ed3541cf

3.2.3 Ensure secure ICMP redirects are not accepted

Severity
High

Description
Description Secure ICMP redirects are the same as ICMP redirects, except they come from gateways listed on the default gateway list. It is assumed that these gateways are known to your system, and that they are likely to be secure. Rationale It is still possible for even known gateways to be compromised. Setting net.ipv4.conf.all.secure_redirects to 0 protects the system from routing table updates by possibly compromised known gateways.

Recommendation
Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.conf.all.secure_redirects = 0net.ipv4.conf.default.secure_redirects = 0 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.conf.all.secure_redirects=0# sysctl -w net.ipv4.conf.default.secure_redirects=0# sysctl -w net.ipv4.route.flush=1

Failed Instances
i-098025956ed3541cf

3.2.4 Ensure suspicious packets are logged

Severity
High

Description
Description When enabled, this feature logs packets with un-routable source addresses to the kernel log. Rationale Enabling this feature and logging these packets allows an administrator to investigate the possibility that an attacker is sending spoofed packets to their system.

Recommendation
Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.conf.all.log_martians = 1net.ipv4.conf.default.log_martians = 1 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.con f.all.log_martians=1# sysctl -w net.ipv4.conf.default.log_martians=1# sysctl -w net.ipv4.route.flush=1

Failed Instances
i-098025956ed3541cf

3.2.5 Ensure broadcast ICMP requests are ignored

Severity
High

Description
Description Setting net.ipv4.icmp_echo_ignore_broadcasts to 1 will cause the system to ignore all ICMP echo and timestamp requests to broadcast and multicast addresses. Rationale Accepting ICMP echo and timestamp requests with broadcast or multicast destinations for your network could be used to trick your host into starting (or participating) in a Smurf attack. A Smurf attack relies on an attacker sending large amounts of ICMP broadcast messages with a spoofed source address. All hosts receiving this message and responding would send echo-reply messages back to the spoofed address, which is probably not routable. If many hosts respond to the packets, the amount of traffic on the network could be significantly multiplied.

Recommendation
Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4 .icmp_echo_ignore_broadcasts = 1 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1# sysctl -w net.ipv4.route.flush=1

Failed Instances
i-098025956ed3541cf

3.2.6 Ensure bogus ICMP responses are ignored

Severity
High

Description
Description Setting icmp_ignore_bogus_error_responses to 1 prevents the kernel from logging bogus responses (RFC-1122 non-compliant) from broadcast reframes, keeping file systems from filling up with useless log messages. Rationale Some routers (and some attackers) will send responses that violate RFC-1122 and attempt to fill up a log file system with many useless error messages.

Recommendation
Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.icmp_ig nore_bogus_error_responses = 1 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1# sysctl -w net.ipv4.route.flush=1

Failed Instances
i-098025956ed3541cf

3.2.7 Ensure Reverse Path Filtering is enabled

Severity
High

Description
Description Setting net.ipv4.conf.all.rp_filterand net.ipv4.conf.default.rp_filter to 1 forces the Linux kernel to utilize reverse path filtering on a received packet to determine if the packet was valid. Essentially, with reverse path filtering, if the return packet does not go out the same interface that the corresponding source packet came from, the

packet is dropped (and logged if log_martians is set). Rationale Setting these flags is a good way to deter attackers from sending your system bogus packets that cannot be responded to. One instance where this feature breaks down is if asymmetrical routing is employed. This would occur when using dynamic routing protocols (bgp, ospf, etc) on your system. If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

Recommendation
Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.conf.all.rp_filter = 1net.ipv4.conf.default.rp_filter = 1 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.conf.all.rp_filter=1# sysctl -w net.ipv4.conf.default.rp_filter=1# sysctl -w net.ipv4.route.flush=1

Failed Instances
i-098025956ed3541cf

3.2.8 Ensure TCP SYN Cookies is enabled

Severity
High

Description
Description When tcp_syncookies is set, the kernel will handle TCP SYN packets normally until the half-open connection queue is full, at which time, the SYN cookie functionality kicks in. SYN cookies work by not using the SYN queue at all. Instead, the kernel simply replies to the SYN with a SYN|ACK, but will include a specially crafted TCP sequence number that encodes the source and destination IP address and port number and the time the packet was sent. A legitimate connection would send the ACK packet of the three way handshake with the specially crafted sequence number. This allows the system to verify that it has received a valid response to a SYN cookie and allow the connection, even though there is no corresponding SYN in the queue. Rationale Attackers use SYN flood attacks to perform a denial of service attacked on a system by sending many SYN packets without completing the three way handshake. This will quickly use up slots in the kernel's half-open connection queue and prevent legitimate connections from succeeding. SYN cookies allow the system to keep accepting valid connections, even if under a denial of service attack.

Recommendation

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.tcp_syncookies = 1 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.tcp_syncookies=1# sysctl -w net.ipv4.route.flush=1

Failed Instances
i-098025956ed3541cf

3.2.9 Ensure IPv6 router advertisements are not accepted

Severity
High

Description
Description This setting disables the system's ability to accept IPv6 router advertisements. Rationale 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.

Recommendation
Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv6.conf.all.accept_ra = 0net.ipv6.conf.default.accept_ra = 0 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv6.conf.all.accept_ra=0# sysctl -w net.ipv6.conf.default.accept_ra=0# sysctl -w net.ipv6.route.flush=1

Failed Instances
i-098025956ed3541cf

3.3.3 Ensure /etc/hosts.deny is configured

Severity
Informational

Description
Description The /etc/hosts.deny file specifies which IP addresses are not permitted to connect to the host. It is intended to be used in conjunction with the /etc/hosts.allow file. Rationale The /etc/hosts.deny file serves as a failsafe so that any host not specified in /etc/hosts.allow is denied access to the system.

Recommendation
Run the following command to create /etc/hosts.deny : # echo "ALL: ALL" >> /etc/hosts.deny

Failed Instances
i-098025956ed3541cf

3.4.1 Ensure DCCP is disabled

Severity
Informational

Description
Description The Datagram Congestion Control Protocol (DCCP) is a transport layer protocol that supports streaming media and telephony. DCCP provides a way to gain access to congestion control, without having to do it at the application layer, but does not provide in-sequence delivery. Rationale If the protocol is not required, it is recommended that the drivers not be installed to reduce the potential attack surface.

Recommendation
Edit or create the file /etc/modprobe.d/CIS.conf and add the following line: install dccp /bin/true

Failed Instances
i-098025956ed3541cf

3.4.2 Ensure SCTP is disabled

Severity
Informational

Description
Description The Stream Control Transmission Protocol (SCTP) is a transport layer protocol used to support message oriented communication, with several streams of messages in one connection. It serves a similar function as TCP and UDP, incorporating features of both. It is message-oriented like UDP, and ensures reliable in-sequence transport of messages with congestion control like TCP. Rationale If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Recommendation
Edit or create the file /etc/modprobe.d/CIS.conf and add the following line: install sctp /bin/true

Failed Instances
i-098025956ed3541cf

3.4.3 Ensure RDS is disabled

Severity
Informational

Description
Description The Reliable Datagram Sockets (RDS) protocol is a transport layer protocol designed to provide low-latency, high-bandwidth communications between cluster nodes. It was developed by the Oracle Corporation. Rationale If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Recommendation
Edit or create the file /etc/modprobe.d/CIS.conf and add the following line: install rds /bin/true

Failed Instances
i-098025956ed3541cf

3.4.4 Ensure TIPC is disabled

Severity
Informational

Description
Description The Transparent Inter-Process Communication (TIPC) protocol is designed to provide communication between cluster nodes. Rationale If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Recommendation
Edit or create the file /etc/modprobe.d/CIS.conf and add the following line: install tipc /bin/true

Failed Instances
i-098025956ed3541cf

3.5.1.1 Ensure default deny firewall policy

Severity
High

Description
Description A default deny all policy on connections ensures that any unconfigured network usage will be rejected. Rationale With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Recommendation
Run the following commands to implement a default DROP policy: # iptables -P INPUT DROP# iptables -P OUTPUT DROP# iptables -P FORWARD DROP

Failed Instances
i-098025956ed3541cf

3.5.1.2 Ensure loopback traffic is configured

Severity
High

Description
Description Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8). Rationale Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Recommendation
Run the following commands to implement the loopback rules: # iptables -A INPUT -i lo -j ACCEPT# iptables -A OUTPUT -o lo -j ACCEPT# iptables -A INPUT -s 127.0.0.0/8 -j DROP

Failed Instances

i-098025956ed3541cf

3.5.1.4 Ensure firewall rules exist for all open ports

Severity
High

Description
Description Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic. Rationale Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

Recommendation
For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections: # iptables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j ACCEPT

Failed Instances
i-098025956ed3541cf

3.5.2.1 Ensure IPv6 default deny firewall policy

Severity
High

Description
Description A default deny all policy on connections ensures that any unconfigured network usage will be rejected. Rationale With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Recommendation
Run the following commands to implement a default DROP policy: # ip6tables -P INPUT DROP# ip6tables -P OUTPUT DROP# ip6tables -P FORWARD DROP

Failed Instances
i-098025956ed3541cf

3.5.2.2 Ensure IPv6 loopback traffic is configured

Severity
High

Description
Description Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (::1). Rationale Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (::1) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Recommendation
Run the following commands to implement the loopback rules: # ip6tables -A INPUT -i lo -j ACCEPT# ip6tables -A OUTPUT -o lo -j ACCEPT# ip6tables -A INPUT -s ::1 -j DROP

Failed Instances
i-098025956ed3541cf

4.2.4 Ensure permissions on all logfiles are configured

Severity
High

Description
Description Log files stored in /var/log/ contain logged information from many services on the system, or on log hosts others as well. Rationale It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

Recommendation
Run the following command to set permissions on all existing log files: # find -L /var/log -type f -exec chmod g-wx,o-rwx {} +

Failed Instances
i-098025956ed3541cf

4.2.1.3 Ensure rsyslog default file permissions configured

Severity
High

Description
Description rsyslog will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files. Rationale It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

Recommendation
Edit the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files and set $FileCreateMode to 0640 or more restrictive: $FileCreateMode 0640

Failed Instances
i-098025956ed3541cf

4.2.1.4 Ensure rsyslog is configured to send logs to a remote log host

Severity
High

Description
Description The rsyslog utility supports the ability to send logs it gathers to a remote log host running syslogd(8) or to receive messages from remote hosts, reducing administrative overhead. Rationale Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system

Recommendation
Edit the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files and add the following line (where loghost.example.com is the name of your central log host). *.* @@loghost.example.com Run the following command to reload the rsyslogd configuration: # pkill -HUP rsyslogd

Failed Instances
i-098025956ed3541cf

5.6 Ensure access to the su command is restricted

Severity
High

Description

Description 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 . Rationale 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.

Recommendation
Add the following line to the /etc/pam.d/su file: auth required pam_wheel.so use_uid Create a comma separated list of users in the wheel statement in the /etc/group file: wheel:x:10:root,<user list>

Failed Instances
i-098025956ed3541cf

5.1.2 Ensure permissions on /etc/crontab are configured

Severity
High

Description
Description The /etc/crontab file is used by cron to control its own jobs. The commands in this item make sure that root is the user and group owner of the file and that only the owner can access the file. Rationale This file contains information on what system jobs are run by cron. Write access to these files could provide unprivileged users with the ability to elevate their privileges. Read access to these files could provide users with the ability to gain insight on system jobs that run on the system and could provide them a way to gain unauthorized privileged access.

Recommendation
Run the following commands to set ownership and permissions on /etc/crontab : # chown root:root /etc/crontab# chmod og-rwx /etc/crontab

Failed Instances
i-098025956ed3541cf

5.1.3 Ensure permissions on /etc/cron.hourly are configured

Severity
High

Description
Description This directory contains system cron jobs that need to run on an hourly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. Rationale Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Recommendation
Run the following commands to set ownership and permissions on /etc/cron.hourly : # chown root:root /etc/cron.hourly# chmod og-rwx /etc/cron.hourly

Failed Instances
i-098025956ed3541cf

5.1.4 Ensure permissions on /etc/cron.daily are configured

Severity
High

Description
Description The /etc/cron.daily directory contains system cron jobs that need to run on a daily basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. Rationale Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Recommendation
Run the following commands to set ownership and permissions on /etc/cron.daily : # chown root:root /etc/cron.daily# chmod og-rwx /etc/cron.daily

Failed Instances
i-098025956ed3541cf

5.1.5 Ensure permissions on /etc/cron.weekly are configured

Severity
High

Description
Description The /etc/cron.weekly directory contains system cron jobs that need to run on a weekly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. Rationale Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Recommendation
Run the following commands to set ownership and permissions on /etc/cron.weekly : # chown root:root /etc/cron.weekly# chmod og-rwx /etc/cron.weekly

Failed Instances
i-098025956ed3541cf

5.1.6 Ensure permissions on /etc/cron.monthly are configured

Severity
High

Description
Description The /etc/cron.monthly directory contains system cron jobs that need to run on a monthly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. Rationale Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an

unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Recommendation
Run the following commands to set ownership and permissions on /etc/cron.monthly : # chown root:root /etc/cron.monthly# chmod og-rwx /etc/cron.monthly

Failed Instances
i-098025956ed3541cf

5.1.7 Ensure permissions on /etc/cron.d are configured

Severity
High

Description
Description The /etc/cron.d directory contains system cron jobs that need to run in a similar manner to the hourly, daily weekly and monthly jobs from /etc/crontab , but require more granular control as to when they run. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. Rationale Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Recommendation
Run the following commands to set ownership and permissions on /etc/cron.d : # chown root:root /etc/cron.d# chmod og-rwx /etc/cron.d

Failed Instances
i-098025956ed3541cf

5.1.8 Ensure at/cron is restricted to authorized users

Severity
High

Description

Description Configure /etc/cron.allow and /etc/at.allow to allow specific users to use these services. If /etc/cron.allow or /etc/at.allow do not exist, then /etc/at.deny and /etc/cron.deny are checked. Any user not specifically defined in those files is allowed to use at and cron. By removing the files, only users in /etc/cron.allow and /etc/at.allow are allowed to use at and cron. Note that even though a given user is not listed in cron.allow , cron jobs can still be run as that user. The cron.allow file only controls administrative access to the crontab command for scheduling and modifying cron jobs. Rationale On many systems, only the system administrator is authorized to schedule cron jobs. Using the cron.allow file to control who can run cron jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

Recommendation
Run the following commands to remove /etc/cron.deny and /etc/at.deny and create and set permissions and ownership for /etc/cron.allow and /etc/at.allow : # rm /etc/cron.deny# rm /etc/at.deny# touch /etc/cron.allow# touch /etc/at.allow# chmod og-rwx /etc/cron.allow# chmod og-rwx /etc/at.allow# chown root:root /etc/cron.allow# chown root:root /etc/at.allow

Failed Instances
i-098025956ed3541cf

5.2.4 Ensure SSH Protocol is set to 2

Severity
High

Description
Description SSH supports two different and incompatible protocols: SSH1 and SSH2. SSH1 was the original protocol and was subject to security issues. SSH2 is more advanced and secure. Rationale SSH v1 suffers from insecurities that do not affect SSH v2.

Recommendation
Edit the /etc/ssh/sshd_config file to set the parameter as follows: Protocol 2

Failed Instances
i-098025956ed3541cf

5.2.5 Ensure SSH LogLevel is appropriate

Severity
High

Description
Description INFO level is the basic level that only records login activity of SSH users. In many situations, such as Incident Response, it is important to determine when a particular user was active on a system. The logout record can eliminate those users who disconnected, which helps narrow the field. VERBOSE level specifies that login and logout activity as well as the key fingerprint for any SSH key used for login will be logged. This information is important for SSH key management, especially in legacy environments. Rationale SSH provides several logging levels with varying amounts of verbosity. DEBUG is specifically not recommended other than strictly for debugging SSH communications since it provides so much data that it is difficult to identify important security information.

Recommendation
Edit the /etc/ssh/sshd_config file to set the parameter as follows: LogLevel VERBOSE or LogLevel INFO

Failed Instances
i-098025956ed3541cf

5.2.7 Ensure SSH MaxAuthTries is set to 4 or less

Severity
High

Description
Description The MaxAuthTries parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the syslog file detailing the login failure. Rationale Setting the MaxAuthTries parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. While the recommended setting is 4, set the number based on site policy.

Recommendation
Edit the /etc/ssh/sshd_config file to set the parameter as follows: MaxAuthTries 4

Failed Instances
i-098025956ed3541cf

5.2.8 Ensure SSH IgnoreRhosts is enabled

Severity
High

Description
Description The IgnoreRhosts parameter specifies that .rhosts and .shosts files will not be used in RhostsRSAAuthentication or HostbasedAuthentication . Rationale Setting this parameter forces users to enter a password when authenticating with ssh.

Recommendation
Edit the /etc/ssh/sshd_config file to set the parameter as follows: IgnoreRhosts yes

Failed Instances
i-098025956ed3541cf

5.2.9 Ensure SSH HostbasedAuthentication is disabled

Severity
High

Description
Description The HostbasedAuthentication parameter specifies if authentication is allowed through trusted hosts via the user of .rhosts , or /etc/hosts.equiv , along with successful public key client host authentication. This option only applies to SSH Protocol Version 2. Rationale Even though the .rhosts files are ineffective if support is disabled in /etc/pam.conf , disabling the ability to use .rhosts files in SSH provides an additional layer of protection .

Recommendation
Edit the /etc/ssh/sshd_config file to set the parameter as follows: HostbasedAuthentication no

Failed Instances
i-098025956ed3541cf

5.2.10 Ensure SSH root login is disabled

Severity
High

Description
Description The PermitRootLogin parameter specifies if the root user can log in using ssh(1). The default is no. Rationale Disallowing root logins over SSH requires system admins to authenticate using their own individual account, then escalating to root via sudo or su . This in turn limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident

Recommendation
Edit the /etc/ssh/sshd_config file to set the parameter as follows: PermitRootLogin no

Failed Instances
i-098025956ed3541cf

5.2.11 Ensure SSH PermitEmptyPasswords is disabled

Severity
High

Description
Description The PermitEmptyPasswords parameter specifies if the SSH server allows login to accounts with empty password strings. Rationale Disallowing remote shell access to accounts that have an empty password reduces the probability of unauthorized access to the system

Recommendation
Edit the /etc/ssh/sshd_config file to set the parameter as follows: PermitEmptyPasswords no

Failed Instances
i-098025956ed3541cf

5.2.12 Ensure SSH PermitUserEnvironment is disabled

Severity
High

Description

Description The PermitUserEnvironment option allows users to present environment options to the ssh daemon. Rationale Permitting users the ability to set environment variables through the SSH daemon could potentially allow users to bypass security controls (e.g. setting an execution path that has ssh executing trojan'd programs)

Recommendation
Edit the /etc/ssh/sshd_config file to set the parameter as follows:
PermitUserEnvironment no

Failed Instances
i-098025956ed3541cf

5.2.13 Ensure only strong ciphers are used

Severity
High

Description
Description This variable limits the ciphers that SSH can use during communication. Rationale Weak ciphers that are used for authentication to the cryptographic module cannot be relied upon to provide confidentiality or integrity, and system data may be compromised The DES, Triple DES, and Blowfish ciphers, as used in SSH, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, aka a "Sweet32" attack The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah" issue The passwords used during an SSH session encrypted with RC4 can be recovered by an attacker who is able to capture and replay the session Error handling in the SSH protocol; Client and Server, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors The mm_newkeys_from_blob function in monitor_wrap.c, when an AES-GCM cipher is used, does not properly initialize memory for a MAC context data structure, which allows remote authenticated users to bypass intended ForceCommand and login-shell restrictions via packet data that provides a crafted callback address

Recommendation
Edit the /etc/ssh/sshd_config file add/modify the Ciphers line to contain a comma separated list of the site approved ciphers Example: Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr

Failed Instances
i-098025956ed3541cf

5.2.14 Ensure only strong MAC algorithms are used

Severity
High

Description
Description This variable limits the types of MAC algorithms that SSH can use during communication. Rationale MD5 and 96-bit MAC algorithms are considered weak and have been shown to increase exploitability in SSH downgrade attacks. Weak algorithms continue to have a great deal of attention as a weak spot that can be exploited with expanded computing power. An attacker that breaks the algorithm could take advantage of a MiTM position to decrypt the SSH tunnel and capture credentials and information

Recommendation
Edit the /etc/ssh/sshd_config file and add/modify the MACs line to contain a comma separated list of the site approved MACs Example: MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512,hmac-sha2-256

Failed Instances
i-098025956ed3541cf

5.2.15 Ensure that strong Key Exchange algorithms are used

Severity
High

Description
Description Key exchange is any method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm. If the sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received Rationale Key exchange

methods that are considered weak should be removed. A key exchange method may be weak because too few bits are used, or the hashing algorithm is considered too weak. Using weak algorithms could expose connections to man-in-the-middle attacks

Recommendation
Edit the /etc/ssh/sshd_config file add/modify the KexAlgorithms line to contain a comma separated list of the site approved key exchange algorithms Example: KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256

Failed Instances
i-098025956ed3541cf

5.2.16 Ensure SSH Idle Timeout Interval is configured

Severity
High

Description
Description The two options ClientAliveInterval and ClientAliveCountMax control the timeout of ssh sessions. When the ClientAliveInterval variable is set, ssh sessions that have no activity for the specified length of time are terminated. When the ClientAliveCountMax variable is set, sshd will send client alive messages at every ClientAliveInterval interval. When the number of consecutive client alive messages are sent with no response from the client, the ssh session is terminated. For example, if the ClientAliveInterval is set to 15 seconds and the ClientAliveCountMax is set to 3, the client ssh session will be terminated after 45 seconds of idle time. Rationale Having no timeout value associated with a connection could allow an unauthorized user access to another user's ssh session (e.g. user walks away from their computer and doesn't lock the screen). Setting a timeout value at least reduces the risk of this happening.. While the recommended setting is 300 seconds (5 minutes), set this timeout value based on site policy. The recommended setting for ClientAliveCountMax is 0. In this case, the client session will be terminated after 5 minutes of idle time and no keepalive messages will be sent.

Recommendation

Edit the /etc/ssh/sshd_config file to set the parameters according to site policy: ClientAliveInterval 300ClientAliveCountMax 0

Failed Instances
i-098025956ed3541cf

5.2.17 Ensure SSH LoginGraceTime is set to one minute or less

Severity
High

Description
Description The LoginGraceTime parameter specifies the time allowed for successful authentication to the SSH server. The longer the Grace period is the more open unauthenticated connections can exist. Like other session controls in this session the Grace Period should be limited to appropriate organizational limits to ensure the service is available for needed access. Rationale Setting the LoginGraceTime parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. It will also limit the number of concurrent unauthenticated connections While the recommended setting is 60 seconds (1 Minute), set the number based on site policy.

Recommendation
Edit the /etc/ssh/sshd_config file to set the parameter as follows: LoginGraceTime 60

Failed Instances
i-098025956ed3541cf

5.2.18 Ensure SSH access is limited

Severity
High

Description
Description There are several options available to limit which users and group can access the system via SSH. It is recommended that at least one of the following options be leveraged: AllowUsers The AllowUsers variable gives the system administrator the option of allowing specific users to ssh into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of

user@host. AllowGroups The AllowGroups variable gives the system administrator the option of allowing specific groups of users to ssh into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable. DenyUsers The DenyUsers variable gives the system administrator the option of denying specific users to ssh into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of user@host. DenyGroups The DenyGroups variable gives the system administrator the option of denying specific groups of users to ssh into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable. Rationale Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.

Recommendation
Edit the /etc/ssh/sshd_config file to set one or more of the parameter as follows: AllowUsers <userlist>AllowGroups <grouplist>DenyUsers <userlist>DenyGroups <grouplist>

Failed Instances
i-098025956ed3541cf

5.2.19 Ensure SSH warning banner is configured

Severity
High

Description
Description The Banner parameter specifies a file whose contents must be sent to the remote user before authentication is permitted. By default, no banner is displayed. Rationale Banners are used to warn connecting users of the particular site's policy regarding connection. Presenting a warning message prior to the normal user login may assist the prosecution of trespassers on the computer system.

Recommendation
Edit the /etc/ssh/sshd_config file to set the parameter as follows: Banner /etc/issue.net

Failed Instances
i-098025956ed3541cf

5.3.1 Ensure password creation requirements are configured

Severity
High

Description
Description The pam_pwquality.so module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more. The following are definitions of the pam_pwquality .so options. try_first_pass - retrieve the password from a previous stacked PAM module. If not available, then prompt the user for a password.retry=3 - Allow 3 tries before sending back a failure. The following options are set in the /etc/security/pwquality.conf file: minlen = 14 - password must be 14 characters or moredcredit = -1 - provide at least one digitucredit = -1 - provide at least one uppercase characterocredit = -1 - provide at least one special characterlcredit = -1 - provide at least one lowercase character The settings shown above are one possible policy. Alter these values to conform to your own organization's password policies. Rationale Strong passwords protect systems from being hacked through brute force methods.

Recommendation
Edit the /etc/pam.d/password-auth and /etc/pam.d/system-auth files to include the appropriate options for pam_pwquality.so and to conform to site policy: password requisite pam_pwquality.so try_first_pass retry=3 Edit /etc/security/pwquality.conf to add or update the following settings to conform to site policy: minlen = 14dcredit = -1ucredit = -1ocredit = -1lcredit = -1

Failed Instances
i-098025956ed3541cf

5.3.2 Ensure lockout for failed password attempts is configured

Severity
High

Description
Description Lock out users after n unsuccessful consecutive login attempts. The first sets of changes are made to the PAM configuration files. The second set of changes are applied to the program specific PAM configuration file. The second set of changes must

be applied to each program that will lock out users. Check the documentation for each secondary program for instructions on how to configure them to work with PAM. Set the lockout number to the policy in effect at your site. Rationale Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Recommendation
Edit the /etc/pam.d/password-auth and /etc/pam.d/system-auth files and add the following pam_faillock.so lines surrounding a pam_unix.so line modify the pam_unix.so is [success=1 default=bad] as listed in both: auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900auth [success=1 default=bad] pam_unix.soauth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900

Failed Instances
i-098025956ed3541cf

5.3.3 Ensure password reuse is limited

Severity
High

Description
Description The /etc/security/opasswd file stores the users' old passwords and can be checked to ensure that users are not recycling recent passwords. Rationale Forcing users not to reuse their past 5 passwords make it less likely that an attacker will be able to guess the password. Note that these change only apply to accounts configured on the local system.

Recommendation
Edit the /etc/pam.d/password-auth and /etc/pam.d/system-auth files to include the remember option and conform to site policy as shown: password sufficient pam_unix.so remember=5 or password required pam_pwhistory.so remember=5

Failed Instances
i-098025956ed3541cf

5.4.4 Ensure default user umask is 027 or more restrictive

Severity
High

Description
Description 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 , .bashrc , etc.) in their home directories. Rationale 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.

Recommendation
Edit the /etc/bashrc, /etc/profile and /etc/profile.d/*.sh files (and the appropriate files for any other shell supported on your system) and add or edit any umask parameters as follows: umask 027

Failed Instances
i-098025956ed3541cf

5.4.1.1 Ensure password expiration is 365 days or less

Severity
High

Description
Description The PASS_MAX_DAYS parameter in /etc/login.defs allows an administrator to force passwords to expire once they reach a defined age. It is recommended that the PASS_MAX_DAYS parameter be set to less than or equal to 365 days. Rationale The window of opportunity for an attacker to leverage compromised credentials or successfully compromise credentials via an online brute force attack is limited by the age of the password. Therefore, reducing the maximum age of a password also reduces an attacker's window of opportunity.

Recommendation

Set the PASS_MAX_DAYS parameter to conform to site policy in /etc/login.defs : PASS_MAX_DAYS 90 Modify user parameters for all users with a password set to match: # chage --maxdays 90 <user>

Failed Instances
i-098025956ed3541cf

5.4.1.2 Ensure minimum days between password changes is 7 or more

Severity
High

Description
Description The PASS_MIN_DAYS parameter in /etc/login.defs allows an administrator to prevent users from changing their password until a minimum number of days have passed since the last time the user changed their password. It is recommended that PASS_MIN_DAYS parameter be set to 7 or more days. Rationale By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

Recommendation
Set the PASS_MIN_DAYS parameter to 7 in /etc/login.defs : PASS_MIN_DAYS 7 Modify user parameters for all users with a password set to match: # chage --mindays 7 <user>

Failed Instances
i-098025956ed3541cf

5.4.1.4 Ensure inactive password lock is 30 days or less

Severity
High

Description
Description 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 30 days after password expiration be disabled. Rationale Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

Recommendation
Run the following command to set the default password inactivity period to 30 days: # useradd -D -f 30 Modify user parameters for all users with a password set to match: # chage --inactive 30 <user>

Failed Instances
i-098025956ed3541cf

4.1.2 Level 2

1.1.2 Ensure /tmp is configured

Severity
High

Description
Description The /tmp directory is a world-writable directory used for temporary storage by all users and some applications. Rationale Making /tmp its own file system allows an administrator to set the noexec option on the mount, making /tmp useless for an attacker to install executable code. It would also prevent an attacker from establishing a hardlink to a system setuid program and wait for it to be updated. Once the program was updated, the hardlink would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw. This can be accomplished by either mounting tmpfs to /tmp, or creating a separate partition for /tmp.

Recommendation
Configure /etc/fstab as appropriate. example:tmpfs /tmp tmpfs defaults,rw,nosuid,nodev ,noexec,relatime 0 0 or Run the following commands to enable systemd /tmp mounting: systemctl unmask tmp.mountsystemctl enable tmp.mount Edit /etc/systemd/system/ local-fs.target.wants/tmp.mount to configure the /tmp mount: [Mount]What=tmpfsWhe re=/tmpType=tmpfsOptions=mode=1777,strictatime,noexec,nodev,nosuid Impact: Since the /tmp directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to a separate partition.Running out of /tmp space is a problem regardless of what kind of filesystem lies under it, but in a default installation a disk-based /tmp will essentially have the whole disk available, as it only creates a single / partition. On the other hand, a RAM-based /tmp as with tmpfs will almost certainly be much smaller, which can lead to applications filling up the filesystem much

more easily./tmp utalizing tmpfs can be resized using the size={size} parameter on the Options line on the tmp.mount file

Failed Instances
i-098025956ed3541cf

1.1.6 Ensure separate partition exists for /var

Severity
High

Description
Description The /var directory is used by daemons and other system services to temporarily store dynamic data. Some directories created by these processes may be world-writable. Rationale Since the /var directory may contain world-writable files and directories, there is a risk of resource exhaustion if it is not bound to a separate partition.

Recommendation
For new installations, during installation create a custom partition setup and specify a separate partition for /var . For systems that were previously installed, create a new partition and configure /etc/fstab as appropriate. Impact: Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

Failed Instances
i-098025956ed3541cf

1.1.7 Ensure separate partition exists for /var/tmp

Severity
High

Description
Description The /var/tmp directory is a world-writable directory used for temporary storage by all users and some applications. Rationale Since the /var/tmp directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to a separate partition. In addition, making /var/tmp its own file system allows an administrator to set the noexec option on the mount, making /var/tmp useless for an

attacker to install executable code. It would also prevent an attacker from establishing a hardlink to a system setuid program and wait for it to be updated. Once the program was updated, the hardlink would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.

Recommendation
For new installations, during installation create a custom partition setup and specify a separate partition for /var/tmp For systems that were previously installed, create a new partition and configure /etc/fstab as appropriate. Impact: Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

Failed Instances
i-098025956ed3541cf

1.1.11 Ensure separate partition exists for /var/log

Severity
High

Description
Description The /var/log directory is used by system services to store log data . Rationale There are two important reasons to ensure that system logs are stored on a separate partition: protection against resource exhaustion (since logs can grow quite large) and protection of audit data.

Recommendation
For new installations, during installation create a custom partition setup and specify a separate partition for /var/log . For systems that were previously installed, create a new partition and configure /etc/fstab as appropriate. Impact: Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

Failed Instances

i-098025956ed3541cf

1.1.12 Ensure separate partition exists for /var/log/audit

Severity
High

Description
Description The auditing daemon, auditd , stores log data in the /var/log/audit directory. Rationale There are two important reasons to ensure that data gathered by auditd is stored on a separate partition: protection against resource exhaustion (since the audit.log file can grow quite large) and protection of audit data. The audit daemon calculates how much free space is left and performs actions based on the results. If other processes (such as syslog) consume space in the same partition as auditd , it may not perform as desired.

Recommendation
For new installations, during installation create a custom partition setup and specify a separate partition for /var/log/audit . For systems that were previously installed, create a new partition and configure /etc/fstab as appropriate. Impact: Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

Failed Instances
i-098025956ed3541cf

1.1.13 Ensure separate partition exists for /home

Severity
High

Description
Description The /home directory is used to support disk storage needs of local users. Rationale If the system is intended to support local users, create a separate partition for the /home directory to protect against resource exhaustion and restrict the type of files that can be stored under /home .

Recommendation

For new installations, during installation create a custom partition setup and specify a separate partition for /home . For systems that were previously installed, create a new partition and configure /etc/fstab as appropriate. Impact: Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

Failed Instances
i-098025956ed3541cf

1.1.17 Ensure noexec option set on /dev/shm partition

Severity
High

Description
Description The noexec mount option specifies that the filesystem cannot contain executable binaries. Rationale Setting this option on a file system prevents users from executing programs from shared memory. This deters users from introducing potentially malicious software on the system.

Recommendation
Edit the /etc/fstab file and add noexec to the fourth field (mounting options) for the /dev/shm partition. See the fstab(5) manual page for more information. Run the following command to remount /dev/shm : # mount -o remount,noexec /dev/shm

Failed Instances
i-098025956ed3541cf

1.1.1.1 Ensure mounting of cramfs filesystems is disabled

Severity
High

Description
Description The cramfs filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems. A cramfs image can be used without having to first decompress the image. Rationale Removing support for unneeded filesystem

types reduces the local attack surface of the server. If this filesystem type is not needed, disable it.

Recommendation
Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/cramfs.conf and add the following line: install cramfs /bin/true Run the following command to unload the cramfs module: # rmmod cramfs

Failed Instances
i-098025956ed3541cf

1.1.1.2 Ensure mounting of hfs filesystems is disabled

Severity
High

Description
Description The hfs filesystem type is a hierarchical filesystem that allows you to mount Mac OS filesystems. Rationale Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Recommendation
Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/hfs.conf and add the following line: install hfs /bin/true Run the following command to unload the hfs module: # rmmod hfs

Failed Instances
i-098025956ed3541cf

1.1.1.3 Ensure mounting of hfsplus filesystems is disabled

Severity
High

Description
Description The hfsplus filesystem type is a hierarchical filesystem designed to replace hfs that allows you to mount Mac OS filesystems. Rationale Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Recommendation
Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/hfsplus.conf and add the following line: install hfsplus /bin/true Run the following command to unload the hfsplus module: # rmmod hfsplus

Failed Instances
i-098025956ed3541cf

1.1.1.4 Ensure mounting of squashfs filesystems is disabled

Severity
High

Description
Description The squashfs filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems (similar to cramfs). A squashfs image can be used without having to first decompress the image. Rationale Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Recommendation
Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/squashfs.conf and add the following line: install squashfs /bin/true Run the following command to unload the squashfs module: # rmmod squashfs

Failed Instances
i-098025956ed3541cf

1.1.1.5 Ensure mounting of udf filesystems is disabled

Severity
High

Description
Description The udf filesystem type is the universal disk format used to implement ISO/IEC 13346 and ECMA-167 specifications. This is an open vendor filesystem type for data storage on a broad range of media. This filesystem type is necessary to support writing DVDs and newer optical disc formats. Rationale Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Recommendation
Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/udf.conf and add the following line: install udf /bin/true Run the following command to unload the udf module: # rmmod udf

Failed Instances
i-098025956ed3541cf

1.3.1 Ensure AIDE is installed

Severity
High

Description
Description AIDE takes a snapshot of filesystem state including modification times, permissions, and file hashes which can then be used to compare against the current state of the filesystem to detect modifications to the system. Rationale By monitoring the filesystem state compromised files can be detected to prevent or limit the exposure of accidental or malicious misconfigurations or modified binaries.

Recommendation
Run the following command to install aide : # yum install aide Configure AIDE as appropriate for your environment. Consult the AIDE documentation for options. Initialize AIDE: # aide --init# mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz

Failed Instances
i-098025956ed3541cf

1.3.2 Ensure filesystem integrity is regularly checked

Severity
High

Description
Description Periodic checking of the filesystem integrity is needed to detect changes to the filesystem. Rationale Periodic file checking allows the system administrator to determine on a regular basis if critical files have been changed in an unauthorized fashion.

Recommendation

Run the following command: # crontab -u root -e Add the following line to the crontab: 0 5 * * * /usr/sbin/aide --check

Failed Instances
i-098025956ed3541cf

1.5.1 Ensure core dumps are restricted

Severity
High

Description
Description 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. Rationale 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 (see limits.conf(5)). In addition, setting the fs.suid_dumpable variable to 0 will prevent setuid programs from dumping core.

Recommendation
Add the following line to /etc/security/limits.conf or a /etc/security/limits.d/* file: * hard core 0 Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file: fs.suid_dumpable = 0 Run the following command to set the active kernel parameter: # sysctl -w fs.suid_dumpable=0

Failed Instances
i-098025956ed3541cf

1.5.2 Ensure address space layout randomization (ASLR) is enabled

Severity
High

Description
Description Address space layout randomization (ASLR) is an exploit mitigation technique which randomly arranges the address space of key data areas of a process. Rationale Randomly placing virtual memory regions will make it difficult to write memory page exploits as the memory placement will be consistently shifting.

Recommendation
Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file: kernel.randomize_va_space = 2 Run the following command to set the active kernel parameter: # sysctl -w kernel.randomize_va_space=2

Failed Instances
i-098025956ed3541cf

1.6.1.2 Ensure the SELinux state is enforcing

Severity
High

Description
Description Set SELinux to enable when the system is booted. Rationale SELinux must be enabled at boot time in to ensure that the controls it provides are in effect at all times.

Recommendation
Edit the /etc/selinux/config file to set the SELINUX parameter: SELINUX=enforcing

Failed Instances
i-098025956ed3541cf

1.6.1.3 Ensure SELinux policy is configured

Severity
High

Description
Description Configure SELinux to meet or exceed the default targeted policy, which constrains daemons and system software only. Rationale Security configuration requirements vary from site to site. Some sites may mandate a policy that is stricter than the default policy, which is perfectly acceptable. This item is intended to ensure that at least the default recommendations are met.

Recommendation
Edit the /etc/selinux/config file to set the SELINUXTYPE parameter: SELINUXTYPE=targeted

Failed Instances
i-098025956ed3541cf

1.6.1.6 Ensure no unconfined daemons exist

Severity
High

Description
Description Daemons that are not defined in SELinux policy will inherit the security context of their parent process. Rationale Since daemons are launched and descend from the init process, they will inherit the security context label initrc_t . This could cause the unintended consequence of giving the process more permission than it requires.

Recommendation
Investigate any unconfined daemons found during the audit action. They may need to have an existing security context assigned to them or a policy built for them.

Failed Instances
i-098025956ed3541cf

1.7.1.1 Ensure message of the day is configured properly

Severity
High

Description
Description The contents of the /etc/motd file are displayed to users after login and function as a message of the day for authenticated users. Unix-based systems have typically displayed information about the OS release and patch level upon logging in to 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 \r - operating system release \s - operating system name \v - operating system version Rationale 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. 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.

Recommendation

Edit the /etc/motd file with the appropriate contents according to your site policy, remove any instances of \m , \r , \s ,\v. , or references to the OS platform

Failed Instances
i-098025956ed3541cf

1.7.1.2 Ensure local login warning banner is configured properly

Severity
Informational

Description
Description The contents of the /etc/issue file are displayed to users prior to login for local terminals. Unix-based systems have typically displayed information about the OS release and patch level upon logging in to 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 \r - operating system release \s - operating system name \v - operating system version Rationale 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. 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.

Recommendation
Edit the /etc/issue file with the appropriate contents according to your site policy, remove any instances of \m , \r , \s , \v or references to the OS platform: # echo "Authorized uses only. All activity may be monitored and reported." > /etc/issue

Failed Instances
i-098025956ed3541cf

1.7.1.3 Ensure remote login warning banner is configured properly

Severity
Informational

Description

Description The contents of the /etc/issue.net file are displayed to users prior to login for remote connections from configured services. Unix-based systems have typically displayed information about the OS release and patch level upon logging in to 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 \r - operating system release \s - operating system name \v - operating system version Rationale 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. 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.

Recommendation
Edit the /etc/issue.net file with the appropriate contents according to your site policy, remove any instances of \m , \r , \s , or \v , or references to the OS platform: # echo "Authorized uses only. All activity may be monitored and reported." > /etc/issue.net

Failed Instances
i-098025956ed3541cf

2.1.1.3 Ensure chrony is configured

Severity
High

Description
Description chrony is a daemon which implements the Network Time Protocol (NTP) is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate. More information on chrony can be found at http://chrony.tuxfamily.org/. chrony can be configured to be a client and/or a server. Rationale If chrony is in use on the system proper configuration is vital to ensuring time synchronization is working properly. This recommendation only applies if chrony is in use on the system.

Recommendation

Add or edit server or pool lines to /etc/chrony.conf as appropriate: server <remote-server> Add or edit the OPTIONS in /etc/sysconfig/chronyd to include '-u chrony': OPTIONS="-u chrony"

Failed Instances
i-098025956ed3541cf

3.6 Disable IPv6

Severity
Informational

Description
Description Although IPv6 has many advantages over IPv4, not all organizations have IPv6 or dual stack configurations implemented. Rationale If IPv6 or dual stack is not to be used, it is recommended that IPv6 be disabled to reduce the attack surface of the system.

Recommendation
Edit /etc/default/grub and remove add ipv6.disable=1 to the GRUB_CMDLINE_LINUX parameters: GRUB_CMDLINE_LINUX="ipv6.disable=1" Run the following command to update the grub2 configuration: # grub2-mkconfig -o /boot/grub2/grub.cfg

Failed Instances
i-098025956ed3541cf

3.1.1 Ensure IP forwarding is disabled

Severity
High

Description
Description The net.ipv4.ip_forward and net.ipv6.conf.all.forwarding flags are used to tell the system whether it can forward packets or not. Rationale Setting the flags to 0 ensures that a system with multiple interfaces (for example, a hard proxy), will never be able to forward packets, and therefore, never serve as a router.

Recommendation

Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.ip_forward = 0net.ipv6.conf.all.forwarding = 0 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.ip_forward=0# sysctl -w net.ipv6.conf.all.forwarding=0# sysctl -w net.ipv4.route.flush=1# sysctl -w net.ipv6.route.flush=1

Failed Instances
i-098025956ed3541cf

3.1.2 Ensure packet redirect sending is disabled

Severity
High

Description
Description ICMP Redirects are used to send routing information to other hosts. As a host itself does not act as a router (in a host only configuration), there is no need to send redirects. Rationale An attacker could use a compromised host to send invalid ICMP redirects to other router devices in an attempt to corrupt routing and have users access a system set up by the attacker as opposed to a valid system.

Recommendation
Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.conf.all.send_redirects = 0net.ipv4.conf.default.send_redirects = 0 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.conf.all.send_redirects=0# sysctl -w net.ipv4.conf.default.send_redirects=0# sysctl -w net.ipv4.route.flush=1

Failed Instances
i-098025956ed3541cf

3.2.1 Ensure source routed packets are not accepted

Severity
High

Description
Description In networking, source routing allows a sender to partially or fully specify the route packets take through a network. In contrast, non-source routed packets travel a path determined by routers in the network. In some cases, systems may not be routable

or reachable from some locations (e.g. private addresses vs. Internet routable), and so source routed packets would need to be used. Rationale Setting net.ipv4.conf.all.accept_source_route, net.ipv4.conf.default.accept_source_route, net.ipv6.conf.all.accept_source_route and net.ipv6.conf.default.accept_source_route to 0 disables the system from accepting source routed packets. Assume this system was capable of routing packets to Internet routable addresses on one interface and private addresses on another interface. Assume that the private addresses were not routable to the Internet routable addresses and vice versa. Under normal routing circumstances, an attacker from the Internet routable addresses could not use the system as a way to reach the private address systems. If, however, source routed packets were allowed, they could be used to gain access to the private address systems as the route could be specified, rather than rely on routing protocols that did not allow this routing.

Recommendation
Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.conf.all.accept_source_route = 0net.ipv4.conf.default.accept_source_route = 0net.ipv6.conf.all.accept_source_route = 0net.ipv6.conf.default.accept_source_route = 0 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.conf.all.accept_source_route=0# sysctl -w net.ipv4.conf.default.accept_source_route=0# sysctl -w net.ipv6.conf.all.accept_source_route=0# sysctl -w net.ipv6.conf.default.accept_source_route=0# sysctl -w net.ipv4.route.flush=1# sysctl -w net.ipv6.route.flush=1

Failed Instances
i-098025956ed3541cf

3.2.2 Ensure ICMP redirects are not accepted

Severity
High

Description
Description ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables. By setting net.ipv4.conf.all.accept_redirects and net.ipv6.conf.all.accept_redirects to 0, the system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables. Rationale Attackers could use bogus ICMP redirect messages to maliciously alter the system routing tables and get them to send packets to incorrect networks and allow your system packets to be captured.

Recommendation
Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.con f.all.accept_redirects = 0net.ipv4.conf.default.accept_redirects = 0net.ipv6.conf.a ll.accept_redirects = 0net.ipv6.conf.default.accept_redirects = 0 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.conf.all.accept_red irects=0# sysctl -w net.ipv4.conf.default.accept_redirects=0# sysctl -w net.ipv6.con f.all.accept_redirects=0# sysctl -w net.ipv6.conf.default.accept_redirects=0# sysctl -w net.ipv4.route.flush=1# sysctl -w net.ipv6.route.flush=1

Failed Instances
i-098025956ed3541cf

3.2.3 Ensure secure ICMP redirects are not accepted

Severity
High

Description
Description Secure ICMP redirects are the same as ICMP redirects, except they come from gateways listed on the default gateway list. It is assumed that these gateways are known to your system, and that they are likely to be secure. Rationale It is still possible for even known gateways to be compromised. Setting net.ipv4.conf.all.secure_redirec ts to 0 protects the system from routing table updates by possibly compromised known gateways.

Recommendation
Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4 .conf.all.secure_redirects = 0net.ipv4.conf.default.secure_redirects = 0 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.conf.al l.secure_redirects=0# sysctl -w net.ipv4.conf.default.secure_redirects=0# sysctl -w net.ipv4.route.flush=1

Failed Instances
i-098025956ed3541cf

3.2.4 Ensure suspicious packets are logged

Severity
High

Description
Description When enabled, this feature logs packets with un-routable source addresses to the kernel log. Rationale Enabling this feature and logging these packets allows an administrator to investigate the possibility that an attacker is sending spoofed packets to their system.

Recommendation
Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.conf.all.log_martians = 1net.ipv4.conf.default.log_martians = 1 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.con f.all.log_martians=1# sysctl -w net.ipv4.conf.default.log_martians=1# sysctl -w net.ipv4.route.flush=1

Failed Instances
i-098025956ed3541cf

3.2.5 Ensure broadcast ICMP requests are ignored

Severity
High

Description
Description Setting net.ipv4.icmp_echo_ignore_broadcasts to 1 will cause the system to ignore all ICMP echo and timestamp requests to broadcast and multicast addresses. Rationale Accepting ICMP echo and timestamp requests with broadcast or multicast destinations for your network could be used to trick your host into starting (or participating) in a Smurf attack. A Smurf attack relies on an attacker sending large amounts of ICMP broadcast messages with a spoofed source address. All hosts receiving this message and responding would send echo-reply messages back to the spoofed address, which is probably not routable. If many hosts respond to the packets, the amount of traffic on the network could be significantly multiplied.

Recommendation
Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4 .icmp_echo_ignore_broadcasts = 1 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1# sysctl -w net.ipv4.route.flush=1

Failed Instances

i-098025956ed3541cf

3.2.6 Ensure bogus ICMP responses are ignored

Severity
High

Description
Description Setting icmp_ignore_bogus_error_responses to 1 prevents the kernel from logging bogus responses (RFC-1122 non-compliant) from broadcast reframes, keeping file systems from filling up with useless log messages. Rationale Some routers (and some attackers) will send responses that violate RFC-1122 and attempt to fill up a log file system with many useless error messages.

Recommendation
Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.icmp_ignore_bogus_error_responses = 1 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1# sysctl -w net.ipv4.route.flush=1

Failed Instances
i-098025956ed3541cf

3.2.7 Ensure Reverse Path Filtering is enabled

Severity
High

Description
Description Setting net.ipv4.conf.all.rp_filterand net.ipv4.conf.default.rp_filter to 1 forces the Linux kernel to utilize reverse path filtering on a received packet to determine if the packet was valid. Essentially, with reverse path filtering, if the return packet does not go out the same interface that the corresponding source packet came from, the packet is dropped (and logged if log_martians is set). Rationale Setting these flags is a good way to deter attackers from sending your system bogus packets that cannot be responded to. One instance where this feature breaks down is if asymmetrical routing is employed. This would occur when using dynamic routing protocols (bgp, ospf, etc) on your system. If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

Recommendation
Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.conf.all.rp_filter = 1net.ipv4.conf.default.rp_filter = 1 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.conf.all.rp_filter=1# sysctl -w net.ipv4.conf.default.rp_filter=1# sysctl -w net.ipv4.route.flush=1

Failed Instances
i-098025956ed3541cf

3.2.8 Ensure TCP SYN Cookies is enabled

Severity
High

Description
Description When tcp_syncookies is set, the kernel will handle TCP SYN packets normally until the half-open connection queue is full, at which time, the SYN cookie functionality kicks in. SYN cookies work by not using the SYN queue at all. Instead, the kernel simply replies to the SYN with a SYN|ACK, but will include a specially crafted TCP sequence number that encodes the source and destination IP address and port number and the time the packet was sent. A legitimate connection would send the ACK packet of the three way handshake with the specially crafted sequence number. This allows the system to verify that it has received a valid response to a SYN cookie and allow the connection, even though there is no corresponding SYN in the queue. Rationale Attackers use SYN flood attacks to perform a denial of service attacked on a system by sending many SYN packets without completing the three way handshake. This will quickly use up slots in the kernel's half-open connection queue and prevent legitimate connections from succeeding. SYN cookies allow the system to keep accepting valid connections, even if under a denial of service attack.

Recommendation
Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.tcp_syncookies = 1 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.tcp_syncookies=1# sysctl -w net.ipv4.route.flush=1

Failed Instances
i-098025956ed3541cf

3.2.9 Ensure IPv6 router advertisements are not accepted

Severity
High

Description
Description This setting disables the system's ability to accept IPv6 router advertisements. Rationale 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.

Recommendation
Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv6.conf.all.accept_ra = 0net.ipv6.conf.default.accept_ra = 0 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv6.conf.all.accept_ra=0# sysctl -w net.ipv6.conf.default.accept_ra=0# sysctl -w net.ipv6.route.flush=1

Failed Instances
i-098025956ed3541cf

3.3.3 Ensure /etc/hosts.deny is configured

Severity
Informational

Description
Description The /etc/hosts.deny file specifies which IP addresses are not permitted to connect to the host. It is intended to be used in conjunction with the /etc/hosts.allow file. Rationale The /etc/hosts.deny file serves as a failsafe so that any host not specified in /etc/hosts.allow is denied access to the system.

Recommendation
Run the following command to create /etc/hosts.deny : # echo "ALL: ALL" >> /etc/hosts.deny

Failed Instances
i-098025956ed3541cf

3.4.1 Ensure DCCP is disabled

Severity
Informational

Description
Description The Datagram Congestion Control Protocol (DCCP) is a transport layer protocol that supports streaming media and telephony. DCCP provides a way to gain access to congestion control, without having to do it at the application layer, but does not provide in-sequence delivery. Rationale If the protocol is not required, it is recommended that the drivers not be installed to reduce the potential attack surface.

Recommendation
Edit or create the file /etc/modprobe.d/CIS.conf and add the following line: install dccp /bin/true

Failed Instances
i-098025956ed3541cf

3.4.2 Ensure SCTP is disabled

Severity
Informational

Description
Description The Stream Control Transmission Protocol (SCTP) is a transport layer protocol used to support message oriented communication, with several streams of messages in one connection. It serves a similar function as TCP and UDP, incorporating features of both. It is message-oriented like UDP, and ensures reliable in-sequence transport of messages with congestion control like TCP. Rationale If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Recommendation
Edit or create the file /etc/modprobe.d/CIS.conf and add the following line: install sctp /bin/true

Failed Instances
i-098025956ed3541cf

3.4.3 Ensure RDS is disabled

Severity
Informational

Description
Description The Reliable Datagram Sockets (RDS) protocol is a transport layer protocol designed to provide low-latency, high-bandwidth communications between cluster nodes. It was developed by the Oracle Corporation. Rationale If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Recommendation
Edit or create the file /etc/modprobe.d/CIS.conf and add the following line: install rds /bin/true

Failed Instances
i-098025956ed3541cf

3.4.4 Ensure TIPC is disabled

Severity
Informational

Description
Description The Transparent Inter-Process Communication (TIPC) protocol is designed to provide communication between cluster nodes. Rationale If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Recommendation
Edit or create the file /etc/modprobe.d/CIS.conf and add the following line: install tipc /bin/true

Failed Instances
i-098025956ed3541cf

3.5.1.1 Ensure default deny firewall policy

Severity
High

Description

Description A default deny all policy on connections ensures that any unconfigured network usage will be rejected. Rationale With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Recommendation
Run the following commands to implement a default DROP policy: # iptables -P INPUT DROP# iptables -P OUTPUT DROP# iptables -P FORWARD DROP

Failed Instances
i-098025956ed3541cf

3.5.1.2 Ensure loopback traffic is configured

Severity
High

Description
Description Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8). Rationale Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Recommendation
Run the following commands to implement the loopback rules: # iptables -A INPUT -i lo -j ACCEPT# iptables -A OUTPUT -o lo -j ACCEPT# iptables -A INPUT -s 127.0.0.0/8 -j DROP

Failed Instances
i-098025956ed3541cf

3.5.1.4 Ensure firewall rules exist for all open ports

Severity
High

Description

Description Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic. Rationale Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

Recommendation
For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections: # iptables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j ACCEPT

Failed Instances
i-098025956ed3541cf

3.5.2.1 Ensure IPv6 default deny firewall policy

Severity
High

Description
Description A default deny all policy on connections ensures that any unconfigured network usage will be rejected. Rationale With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Recommendation
Run the following commands to implement a default DROP policy: # ip6tables -P INPUT DROP# ip6tables -P OUTPUT DROP# ip6tables -P FORWARD DROP

Failed Instances
i-098025956ed3541cf

3.5.2.2 Ensure IPv6 loopback traffic is configured

Severity
High

Description
Description Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (::1). Rationale Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (::1) traffic

should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Recommendation
Run the following commands to implement the loopback rules: # ip6tables -A INPUT -i lo -j ACCEPT# ip6tables -A OUTPUT -o lo -j ACCEPT# ip6tables -A INPUT -s ::1 -j DROP

Failed Instances
i-098025956ed3541cf

4.1.3 Ensure auditing for processes that start prior to auditd is enabled

Severity
High

Description
Description Configure grub so that processes that are capable of being audited can be audited even if they start up prior to auditd startup. Rationale Audit events need to be captured on processes that start up prior to auditd, so that potential malicious activity cannot go undetected.

Recommendation
Edit /etc/default/grub and add audit=1 to GRUB_CMDLINE_LINUX: GRUB_CMDLINE_LINUX="audit=1" Run the following command to update the grub2 configuration: # grub2-mkconfig -o /boot/grub2/grub.cfg

Failed Instances
i-098025956ed3541cf

4.1.4 Ensure events that modify date and time information are collected

Severity
High

Description
Description Capture events where the system date and/or time has been modified. The parameters in this section are set to determine if the adjtimex (tune kernel clock), settimeofday (Set time, using timeval and timezone structures) stime (using seconds since 1/1/1970) or clock_settime (allows for the setting of several internal clocks and

timers) system calls have been executed and always write an audit record to the /var/log/audit.log file upon exit, tagging the records with the identifier "time-change" Rationale Unexpected changes in system date and/or time could be a sign of malicious activity on the system.

Recommendation
For 32 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change-a always,exit -F arch=b32 -S clock_settime -k time-change-w /etc/localtime -p wa -k time-change For 64 bit systems add the following lines to the /etc/audit/audit.rules file: -a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change-a always,exit -F arch=b64 -S clock_settime -k time-change-a always,exit -F arch=b32 -S clock_settime -k time-change-w /etc/localtime -p wa -k time-change

Failed Instances
i-098025956ed3541cf

4.1.5 Ensure events that modify user/group information are collected

Severity
High

Description
Description Record events affecting the group , passwd (user IDs), shadow and gshadow (passwords) or /etc/security/opasswd (old passwords, based on remember parameter in the PAM configuration) files. The parameters in this section will watch the files to see if they have been opened for write or have had attribute changes (e.g. permissions) and tag them with the identifier "identity" in the audit log file. Rationale Unexpected changes to these files could be an indication that the system has been compromised and that an unauthorized user is attempting to hide their activities or compromise additional accounts.

Recommendation
Add the following lines to the /etc/audit/rules.d/audit.rules file: -w /etc/group -p wa -k identity-w /etc/passwd -p wa -k identity-w /etc/gshadow -p wa -k identity-w /etc/shadow -p wa -k identity-w /etc/security/opasswd -p wa -k identity

Failed Instances

i-098025956ed3541cf

4.1.6 Ensure events that modify the system's network environment are collected

Severity
High

Description
Description Record changes to network environment files or system calls. The below parameters monitor the sethostname (set the systems host name) or setdomainname (set the systems domainname) system calls, and write an audit event on system call exit. The other parameters monitor the /etc/issue and /etc/issue.net files (messages displayed pre-login), /etc/hosts (file containing host names and associated IP addresses), /etc/sysconfig/network file and /etc/sysconfig/network-scripts/ directory (containing network interface scripts and configurations). Rationale Monitoring sethostname and setdomainname will identify potential unauthorized changes to host and domainname of a system. The changing of these names could potentially break security parameters that are set based on those names. The /etc/hosts file is monitored for changes in the file that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring /etc/issue and /etc/issue.net is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring /etc/sysconfig/network and /etc/sysconfig/network-scripts/ is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised. All audit records will be tagged with the identifier "system-locale."

Recommendation
For 32 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale-w /etc/issue -p wa -k system-locale-w /etc/issue.net -p wa -k system-locale-w /etc/hosts -p wa -k system-locale-w /etc/sysconfig/network -p wa -k system-locale-w /etc/sysconfig/network-scripts/ -p wa -k system-locale For 64 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale -a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale-w /etc/issue -p wa -k system-locale-w /etc/issue.net -p wa -k system-locale-w /etc/hosts -p wa -k system-locale-w /etc/sysconfig/network -p wa -k system-locale-w /etc/sysconfig/network-scripts/ -p wa -k system-locale

Failed Instances
i-098025956ed3541cf

4.1.7 Ensure events that modify the system's Mandatory Access Controls are collected

Severity
High

Description
Description Monitor SELinux mandatory access controls. The parameters below monitor any write access (potential additional, deletion or modification of files in the directory) or attribute changes to the /etc/selinux or directory. Rationale Changes to files in these directories could indicate that an unauthorized user is attempting to modify access controls and change security contexts, leading to a compromise of the system.

Recommendation
Add the following lines to the /etc/audit/rules.d/audit.rules file: -w /etc/selinux/ -p wa -k MAC-policy-w /usr/share/selinux/ -p wa -k MAC-policy

Failed Instances
i-098025956ed3541cf

4.1.8 Ensure login and logout events are collected

Severity
High

Description
Description Monitor login and logout events. The parameters below track changes to files associated with login/logout events. The file /var/log/lastlog maintain records of the last time a user successfully logged in. The /var/run/failock directory maintains records of login failures via the pam_faillock module. Rationale Monitoring login/ logout events could provide a system administrator with information associated with brute force attacks against user logins.

Recommendation
Add the following lines to the /etc/audit/rules.d/audit.rules file: -w /var/log/lastlog -p wa -k logins-w /var/run/faillock/ -p wa -k logins

Failed Instances

i-098025956ed3541cf

4.1.9 Ensure session initiation information is collected

Severity
High

Description
Description Monitor session initiation events. The parameters in this section track changes to the files associated with session events. The file /var/run/utmp file tracks all currently logged in users. All audit records will be tagged with the identifier "session." The /var/log/wtmp file tracks logins, logouts, shutdown, and reboot events. The file /var/log/btmp keeps track of failed login attempts and can be read by entering the command /usr/bin/last -f /var/log/btmp . All audit records will be tagged with the identifier "logins." Rationale Monitoring these files for changes could alert a system administrator to logins occurring at unusual hours, which could indicate intruder activity (i.e. a user logging in at a time when they do not normally log in).

Recommendation
Add the following lines to the /etc/audit/rules.d/audit.rules file: -w /var/run/utmp -p wa -k session-w /var/log/wtmp -p wa -k logins-w /var/log/btmp -p wa -k logins

Failed Instances
i-098025956ed3541cf

4.1.10 Ensure discretionary access control permission modification events are collected

Severity
High

Description
Description Monitor changes to file permissions, attributes, ownership and group. The parameters in this section track changes for system calls that affect file permissions and attributes. The chmod , fchmod and fchmodat system calls affect the permissions associated with a file. The chown , fchown , fchownat and lchown system calls affect owner and group attributes on a file. The setxattr , lsetxattr , fsetxattr (set extended file attributes) and removexattr , lremovexattr , fremovexattr (remove extended file attributes) control extended file attributes. In all cases, an audit record will only be written for non-system user ids (auid >= 1000) and will ignore Daemon events (auid

= 4294967295). All audit records will be tagged with the identifier "perm_mod." Rationale Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

Recommendation
For 32 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod For 64 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

Failed Instances
i-098025956ed3541cf

4.1.11 Ensure unsuccessful unauthorized file access attempts are collected

Severity
High

Description
Description Monitor for unsuccessful attempts to access files. The parameters below are associated with system calls that control creation (creat), opening (open , openat) and truncation (truncate , ftruncate) of files. An audit log record will only be written if the user is a non-privileged user (auid > = 1000), is not a Daemon event (auid=4294967295) and if the system call returned EACCES (permission denied to the file) or EPERM (some other permanent error associated with the specific system call). All audit records will be tagged with the identifier "access." Rationale Failed attempts

to open, create or truncate files could be an indication that an individual or process is trying to gain unauthorized access to the system.

Recommendation
For 32 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access For 64 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access

Failed Instances
i-098025956ed3541cf

4.1.12 Ensure use of privileged commands is collected

Severity
High

Description
Description Monitor privileged programs (those that have the setuid and/or setgid bit set on execution) to determine if unprivileged users are running these commands. Rationale Execution of privileged commands by non-privileged users could be an indication of someone trying to gain unauthorized access to the system.

Recommendation
To remediate this issue, the system administrator will have to execute a find command to locate all the privileged programs and then add an audit line for each one of them. The audit parameters associated with this are as follows: -F path=" $1 " - will populate each file name found through the find command and processed by awk. -F perm=x - will write an audit record if the file is executed. -F auid>=1000 - will write a record if the user executing the command is not a privileged user. -F auid!= 4294967295 - will ignore Daemon events All audit records should be tagged with the identifier

"privileged". Run the following command replacing <partition> with a list of partitions where programs can be executed from on your system: # find <partition> -xdev \(-perm -4000 -o -perm -2000 \) -type f | awk '{print \"-a always,exit -F path=" $1 " -F perm=x -F auid>=1000 -F auid!=4294967295 \-k privileged" }' Add all resulting lines to the /etc/audit/rules.d/audit.rules file.

Failed Instances
i-098025956ed3541cf

4.1.13 Ensure successful file system mounts are collected

Severity
High

Description
Description Monitor the use of the mount system call. The mount (and umount) system call controls the mounting and unmounting of file systems. The parameters below configure the system to create an audit record when the mount system call is used by a non-privileged user Rationale It is highly unusual for a non privileged user to mount file systems to the system. While tracking mount commands gives the system administrator evidence that external media may have been mounted (based on a review of the source of the mount and confirming it's an external media type), it does not conclusively indicate that data was exported to the media. System administrators who wish to determine if data were exported, would also have to track successful open , creat and truncate system calls requiring write access to a file under the mount point of the external media file system. This could give a fair indication that a write occurred. The only way to truly prove it, would be to track successful writes to the external media. Tracking write system calls could quickly fill up the audit log and is not recommended. Recommendations on configuration options to track data export to media is beyond the scope of this document.

Recommendation
For 32 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts For 64 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts

Failed Instances

i-098025956ed3541cf

4.1.14 Ensure file deletion events by users are collected

Severity
High

Description
Description Monitor the use of system calls associated with the deletion or renaming of files and file attributes. This configuration statement sets up monitoring for the unlink (remove a file), unlinkat (remove a file attribute), rename (rename a file) and renameat (rename a file attribute) system calls and tags them with the identifier "delete". Rationale Monitoring these calls from non-privileged users could provide a system administrator with evidence that inappropriate removal of files and file attributes associated with protected files is occurring. While this audit option will look at all events, system administrators will want to look for specific privileged files that are being deleted or altered.

Recommendation
For 32 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete For 64 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete

Failed Instances
i-098025956ed3541cf

4.1.15 Ensure changes to system administration scope (sudoers) is collected

Severity
High

Description
Description Monitor scope changes for system administrations. If the system has been properly configured to force system administrators to log in as themselves first and then use the sudo command to execute privileged commands, it is possible to monitor

changes in scope. The file /etc/sudoers will be written to when the file or its attributes have changed. The audit records will be tagged with the identifier "scope." Rationale Changes in the /etc/sudoers file can indicate that an unauthorized change has been made to scope of system administrator activity.

Recommendation
Add the following line to the /etc/audit/rules.d/audit.rules file: -w /etc/sudoers -p wa -k scope-w /etc/sudoers.d/ -p wa -k scope

Failed Instances
i-098025956ed3541cf

4.1.16 Ensure system administrator actions (sudolog) are collected

Severity
High

Description
Description Monitor the sudo log file. If the system has been properly configured to disable the use of the su command and force all administrators to have to log in first and then use sudo to execute privileged commands, then all administrator commands will be logged to /var/log/sudo.log . Any time a command is executed, an audit event will be triggered as the /var/log/sudo.log file will be opened for write and the executed administration command will be written to the log. Rationale Changes in /var/log/ sudo.log indicate that an administrator has executed a command or the log file itself has been tampered with. Administrators will want to correlate the events written to the audit trail with the records written to /var/log/sudo.log to verify if unauthorized commands have been executed.

Recommendation
Add the following lines to the /etc/audit/rules.d/audit.rules file: -w /var/log/sudo.log -p wa -k actions

Failed Instances
i-098025956ed3541cf

4.1.17 Ensure kernel module loading and unloading is collected

Severity
High

Description
Description Monitor the loading and unloading of kernel modules. The programs insmod (install a kernel module), rmmod (remove a kernel module), and modprobe (a more sophisticated program to load and unload modules, as well as some other features) control loading and unloading of modules. The init_module (load a module) and delete_module (delete a module) system calls control loading and unloading of modules. Any execution of the loading and unloading module programs and system calls will trigger an audit record with an identifier of "modules". Rationale Monitoring the use of insmod , rmmod and modprobe could provide system administrators with evidence that an unauthorized user loaded or unloaded a kernel module, possibly compromising the security of the system. Monitoring of the init_module and delete_module system calls would reflect an unauthorized user attempting to use a different program to load and unload modules.

Recommendation
For 32 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -w /sbin/insmod -p x -k modules-w /sbin/rmmod -p x -k modules-w /sbin/modprobe -p x -k modules-a always,exit -F arch=b32 -S init_module -S delete_module -k modules For 64 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -w /sbin/insmod -p x -k modules-w /sbin/rmmod -p x -k modules-w /sbin/modprobe -p x -k modules-a always,exit -F arch=b64 -S init_module -S delete_module -k modules

Failed Instances
i-098025956ed3541cf

4.1.18 Ensure the audit configuration is immutable

Severity
High

Description
Description Set system audit so that audit rules cannot be modified with auditctl . Setting the flag "-e 2" forces audit to be put in immutable mode. Audit changes can only be made on system reboot. Rationale In immutable mode, unauthorized users cannot execute changes to the audit system to potentially hide malicious activity and then put the audit rules back. Users would most likely notice a system reboot and that could alert administrators of an attempt to make unauthorized audit changes.

Recommendation

Add the following line to the end of the /etc/audit/rules.d/audit.rules file. -e 2

Failed Instances
i-098025956ed3541cf

4.1.1.2 Ensure system is disabled when audit logs are full

Severity
High

Description
Description The auditd daemon can be configured to halt the system when the audit logs are full. Rationale In high security contexts, the risk of detecting unauthorized access or nonrepudiation exceeds the benefit of the system's availability.

Recommendation
Set the following parameters in /etc/audit/auditd.conf: space_left_action = emailaction_mail_acct = rootadmin_space_left_action = halt

Failed Instances
i-098025956ed3541cf

4.1.1.3 Ensure audit logs are not automatically deleted

Severity
High

Description
Description The max_log_file_action setting determines how to handle the audit log file reaching the max file size. A value of keep_logs will rotate the logs but never delete old logs. Rationale In high security contexts, the benefits of maintaining a long audit history exceed the cost of storing the audit history.

Recommendation
Set the following parameter in /etc/audit/auditd.conf: max_log_file_action = keep_logs

Failed Instances
i-098025956ed3541cf

4.2.4 Ensure permissions on all logfiles are configured

Severity
High

Description
Description Log files stored in /var/log/ contain logged information from many services on the system, or on log hosts others as well. Rationale It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

Recommendation
Run the following command to set permissions on all existing log files: # find -L /var/log -type f -exec chmod g-wx,o-rwx {} +

Failed Instances
i-098025956ed3541cf

4.2.1.3 Ensure rsyslog default file permissions configured

Severity
High

Description
Description rsyslog will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files. Rationale It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

Recommendation
Edit the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files and set $FileCreateMode to 0640 or more restrictive: $FileCreateMode 0640

Failed Instances
i-098025956ed3541cf

4.2.1.4 Ensure rsyslog is configured to send logs to a remote log host

Severity
High

Description
Description The rsyslog utility supports the ability to send logs it gathers to a remote log host running syslogd(8) or to receive messages from remote hosts, reducing

administrative overhead. Rationale Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system

Recommendation
Edit the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files and add the following line (where loghost.example.com is the name of your central log host). *.* @@loghost.example.com Run the following command to reload the rsyslogd configuration: # pkill -HUP rsyslogd

Failed Instances
i-098025956ed3541cf

5.6 Ensure access to the su command is restricted

Severity
High

Description
Description 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 . Rationale 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.

Recommendation
Add the following line to the /etc/pam.d/su file: auth required pam_wheel.so use_uid Create a comma separated list of users in the wheel statement in the /etc/group file: wheel:x:10:root,<user list>

Failed Instances
i-098025956ed3541cf

5.1.2 Ensure permissions on /etc/crontab are configured

Severity

High

Description
Description The /etc/crontab file is used by cron to control its own jobs. The commands in this item make sure that root is the user and group owner of the file and that only the owner can access the file. Rationale This file contains information on what system jobs are run by cron. Write access to these files could provide unprivileged users with the ability to elevate their privileges. Read access to these files could provide users with the ability to gain insight on system jobs that run on the system and could provide them a way to gain unauthorized privileged access.

Recommendation
Run the following commands to set ownership and permissions on /etc/crontab : # chown root:root /etc/crontab# chmod og-rwx /etc/crontab

Failed Instances
i-098025956ed3541cf

5.1.3 Ensure permissions on /etc/cron.hourly are configured

Severity
High

Description
Description This directory contains system cron jobs that need to run on an hourly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. Rationale Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Recommendation
Run the following commands to set ownership and permissions on /etc/cron.hourly : # chown root:root /etc/cron.hourly# chmod og-rwx /etc/cron.hourly

Failed Instances
i-098025956ed3541cf

5.1.4 Ensure permissions on /etc/cron.daily are configured

Severity
High

Description
Description The /etc/cron.daily directory contains system cron jobs that need to run on a daily basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. Rationale Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Recommendation
Run the following commands to set ownership and permissions on /etc/cron.daily : # chown root:root /etc/cron.daily# chmod og-rwx /etc/cron.daily

Failed Instances
i-098025956ed3541cf

5.1.5 Ensure permissions on /etc/cron.weekly are configured

Severity
High

Description
Description The /etc/cron.weekly directory contains system cron jobs that need to run on a weekly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. Rationale Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Recommendation

Run the following commands to set ownership and permissions on /etc/cron.weekly : # chown root:root /etc/cron.weekly# chmod og-rwx /etc/cron.weekly

Failed Instances
i-098025956ed3541cf

5.1.6 Ensure permissions on /etc/cron.monthly are configured

Severity
High

Description
Description The /etc/cron.monthly directory contains system cron jobs that need to run on a monthly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. Rationale Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Recommendation
Run the following commands to set ownership and permissions on /etc/cron.monthly : # chown root:root /etc/cron.monthly# chmod og-rwx /etc/cron.monthly

Failed Instances
i-098025956ed3541cf

5.1.7 Ensure permissions on /etc/cron.d are configured

Severity
High

Description
Description The /etc/cron.d directory contains system cron jobs that need to run in a similar manner to the hourly, daily weekly and monthly jobs from /etc/crontab , but require more granular control as to when they run. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user

and group root, preventing regular users from accessing this directory. Rationale Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Recommendation
Run the following commands to set ownership and permissions on /etc/cron.d : # chown root:root /etc/cron.d# chmod og-rwx /etc/cron.d

Failed Instances
i-098025956ed3541cf

5.1.8 Ensure at/cron is restricted to authorized users

Severity
High

Description
Description Configure /etc/cron.allow and /etc/at.allow to allow specific users to use these services. If /etc/cron.allow or /etc/at.allow do not exist, then /etc/at.deny and /etc/cron.deny are checked. Any user not specifically defined in those files is allowed to use at and cron. By removing the files, only users in /etc/cron.allow and /etc/at.allow are allowed to use at and cron. Note that even though a given user is not listed in cron.allow , cron jobs can still be run as that user. The cron.allow file only controls administrative access to the crontab command for scheduling and modifying cron jobs. Rationale On many systems, only the system administrator is authorized to schedule cron jobs. Using the cron.allow file to control who can run cron jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

Recommendation
Run the following commands to remove /etc/cron.deny and /etc/at.deny and create and set permissions and ownership for /etc/cron.allow and /etc/at.allow : # rm /etc/cron.deny# rm /etc/at.deny# touch /etc/cron.allow# touch /etc/at.allow# chmod og-rwx /etc/cron.allow# chmod og-rwx /etc/at.allow# chown root:root /etc/cron.allow# chown root:root /etc/at.allow

Failed Instances

i-098025956ed3541cf

5.2.4 Ensure SSH Protocol is set to 2

Severity
High

Description
Description SSH supports two different and incompatible protocols: SSH1 and SSH2. SSH1 was the original protocol and was subject to security issues. SSH2 is more advanced and secure. Rationale SSH v1 suffers from insecurities that do not affect SSH v2.

Recommendation
Edit the /etc/ssh/sshd_config file to set the parameter as follows: Protocol 2

Failed Instances
i-098025956ed3541cf

5.2.5 Ensure SSH LogLevel is appropriate

Severity
High

Description
Description INFO level is the basic level that only records login activity of SSH users. In many situations, such as Incident Response, it is important to determine when a particular user was active on a system. The logout record can eliminate those users who disconnected, which helps narrow the field. VERBOSE level specifies that login and logout activity as well as the key fingerprint for any SSH key used for login will be logged. This information is important for SSH key management, especially in legacy environments. Rationale SSH provides several logging levels with varying amounts of verbosity. DEBUG is specifically not recommended other than strictly for debugging SSH communications since it provides so much data that it is difficult to identify important security information.

Recommendation
Edit the /etc/ssh/sshd_config file to set the parameter as follows: LogLevel VERBOSE or LogLevel INFO

Failed Instances
i-098025956ed3541cf

5.2.6 Ensure SSH X11 forwarding is disabled

Severity
High

Description
Description The X11Forwarding parameter provides the ability to tunnel X11 traffic through the connection to enable remote graphic connections. Rationale Disable X11 forwarding unless there is an operational requirement to use X11 applications directly. There is a small risk that the remote X11 servers of users who are logged in via SSH with X11 forwarding could be compromised by other users on the X11 server. Note that even if X11 forwarding is disabled, users can always install their own forwarders.

Recommendation
Edit the /etc/ssh/sshd_config file to set the parameter as follows: X11Forwarding no

Failed Instances
i-098025956ed3541cf

5.2.7 Ensure SSH MaxAuthTries is set to 4 or less

Severity
High

Description
Description The MaxAuthTries parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the syslog file detailing the login failure. Rationale Setting the MaxAuthTries parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. While the recommended setting is 4, set the number based on site policy.

Recommendation
Edit the /etc/ssh/sshd_config file to set the parameter as follows: MaxAuthTries 4

Failed Instances
i-098025956ed3541cf

5.2.8 Ensure SSH IgnoreRhosts is enabled

Severity
High

Description
Description The IgnoreRhosts parameter specifies that .rhosts and .shosts files will not be used in RhostsRSAAuthentication or HostbasedAuthentication . Rationale Setting this parameter forces users to enter a password when authenticating with ssh.

Recommendation
Edit the /etc/ssh/sshd_config file to set the parameter as follows: IgnoreRhosts yes

Failed Instances
i-098025956ed3541cf

5.2.9 Ensure SSH HostbasedAuthentication is disabled

Severity
High

Description
Description The HostbasedAuthentication parameter specifies if authentication is allowed through trusted hosts via the user of .rhosts , or /etc/hosts.equiv , along with successful public key client host authentication. This option only applies to SSH Protocol Version 2. Rationale Even though the .rhosts files are ineffective if support is disabled in /etc/pam.conf , disabling the ability to use .rhosts files in SSH provides an additional layer of protection .

Recommendation
Edit the /etc/ssh/sshd_config file to set the parameter as follows: HostbasedAuthentication no

Failed Instances
i-098025956ed3541cf

5.2.10 Ensure SSH root login is disabled

Severity
High

Description
Description The PermitRootLogin parameter specifies if the root user can log in using ssh(1). The default is no. Rationale Disallowing root logins over SSH requires system admins to authenticate using their own individual account, then escalating to root via sudo or su . This in turn limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident

Recommendation
Edit the /etc/ssh/sshd_config file to set the parameter as follows: PermitRootLogin no

Failed Instances
i-098025956ed3541cf

5.2.11 Ensure SSH PermitEmptyPasswords is disabled

Severity
High

Description
Description The PermitEmptyPasswords parameter specifies if the SSH server allows login to accounts with empty password strings. Rationale Disallowing remote shell access to accounts that have an empty password reduces the probability of unauthorized access to the system

Recommendation
Edit the /etc/ssh/sshd_config file to set the parameter as follows: PermitEmptyPasswords no

Failed Instances
i-098025956ed3541cf

5.2.12 Ensure SSH PermitUserEnvironment is disabled

Severity
High

Description
Description The PermitUserEnvironment option allows users to present environment options to the ssh daemon. Rationale Permitting users the ability to set environment

variables through the SSH daemon could potentially allow users to bypass security controls (e.g. setting an execution path that has ssh executing trojan'd programs)

Recommendation
Edit the /etc/ssh/sshd_config file to set the parameter as follows:
PermitUserEnvironment no

Failed Instances
i-098025956ed3541cf

5.2.13 Ensure only strong ciphers are used

Severity
High

Description
Description This variable limits the ciphers that SSH can use during communication. Rationale Weak ciphers that are used for authentication to the cryptographic module cannot be relied upon to provide confidentiality or integrity, and system data may be compromised The DES, Triple DES, and Blowfish ciphers, as used in SSH, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, aka a "Sweet32" attack The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah" issue The passwords used during an SSH session encrypted with RC4 can be recovered by an attacker who is able to capture and replay the session Error handling in the SSH protocol; Client and Server, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors The mm_newkeys_from_blob function in monitor_wrap.c, when an AES-GCM cipher is used, does not properly initialize memory for a MAC context data structure, which allows remote authenticated users to bypass intended ForceCommand and login-shell restrictions via packet data that provides a crafted callback address

Recommendation

Edit the /etc/ssh/sshd_config file add/modify the Ciphers line to contain a comma separated list of the site approved ciphers Example: Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr

Failed Instances
i-098025956ed3541cf

5.2.14 Ensure only strong MAC algorithms are used

Severity
High

Description
Description This variable limits the types of MAC algorithms that SSH can use during communication. Rationale MD5 and 96-bit MAC algorithms are considered weak and have been shown to increase exploitability in SSH downgrade attacks. Weak algorithms continue to have a great deal of attention as a weak spot that can be exploited with expanded computing power. An attacker that breaks the algorithm could take advantage of a MiTM position to decrypt the SSH tunnel and capture credentials and information

Recommendation
Edit the /etc/ssh/sshd_config file and add/modify the MACs line to contain a comma separated list of the site approved MACs Example: MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512,hmac-sha2-256

Failed Instances
i-098025956ed3541cf

5.2.15 Ensure that strong Key Exchange algorithms are used

Severity
High

Description
Description Key exchange is any method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm. If the sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received Rationale Key exchange methods that are considered weak should be removed. A key exchange method may be

weak because too few bits are used, or the hashing algorithm is considered too weak. Using weak algorithms could expose connections to man-in-the-middle attacks

Recommendation
Edit the /etc/ssh/sshd_config file add/modify the KexAlgorithms line to contain a comma separated list of the site approved key exchange algorithms Example: KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256

Failed Instances
i-098025956ed3541cf

5.2.16 Ensure SSH Idle Timeout Interval is configured

Severity
High

Description
Description The two options ClientAliveInterval and ClientAliveCountMax control the timeout of ssh sessions. When the ClientAliveInterval variable is set, ssh sessions that have no activity for the specified length of time are terminated. When the ClientAliveCountMax variable is set, sshd will send client alive messages at every ClientAliveInterval interval. When the number of consecutive client alive messages are sent with no response from the client, the ssh session is terminated. For example, if the ClientAliveInterval is set to 15 seconds and the ClientAliveCountMax is set to 3, the client ssh session will be terminated after 45 seconds of idle time. Rationale Having no timeout value associated with a connection could allow an unauthorized user access to another user's ssh session (e.g. user walks away from their computer and doesn't lock the screen). Setting a timeout value at least reduces the risk of this happening.. While the recommended setting is 300 seconds (5 minutes), set this timeout value based on site policy. The recommended setting for ClientAliveCountMax is 0. In this case, the client session will be terminated after 5 minutes of idle time and no keepalive messages will be sent.

Recommendation
Edit the /etc/ssh/sshd_config file to set the parameters according to site policy: ClientAliveInterval 300ClientAliveCountMax 0

Failed Instances
i-098025956ed3541cf

5.2.17 Ensure SSH LoginGraceTime is set to one minute or less

Severity
High

Description
Description The LoginGraceTime parameter specifies the time allowed for successful authentication to the SSH server. The longer the Grace period is the more open unauthenticated connections can exist. Like other session controls in this session the Grace Period should be limited to appropriate organizational limits to ensure the service is available for needed access. Rationale Setting the LoginGraceTime parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. It will also limit the number of concurrent unauthenticated connections While the recommended setting is 60 seconds (1 Minute), set the number based on site policy.

Recommendation
Edit the /etc/ssh/sshd_config file to set the parameter as follows: LoginGraceTime 60

Failed Instances
i-098025956ed3541cf

5.2.18 Ensure SSH access is limited

Severity
High

Description
Description There are several options available to limit which users and group can access the system via SSH. It is recommended that at least one of the following options be leveraged: AllowUsers The AllowUsers variable gives the system administrator the option of allowing specific users to ssh into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of user@host. AllowGroups The AllowGroups variable gives the system administrator the option of allowing specific groups of users to ssh into the system. The list consists

of space separated group names. Numeric group IDs are not recognized with this variable. DenyUsers The DenyUsers variable gives the system administrator the option of denying specific users to ssh into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of user@host. DenyGroups The DenyGroups variable gives the system administrator the option of denying specific groups of users to ssh into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable. Rationale Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.

Recommendation
Edit the /etc/ssh/sshd_config file to set one or more of the parameter as follows: AllowUsers <userlist>AllowGroups <grouplist>DenyUsers <userlist>DenyGroups <grouplist>

Failed Instances
i-098025956ed3541cf

5.2.19 Ensure SSH warning banner is configured

Severity
High

Description
Description The Banner parameter specifies a file whose contents must be sent to the remote user before authentication is permitted. By default, no banner is displayed. Rationale Banners are used to warn connecting users of the particular site's policy regarding connection. Presenting a warning message prior to the normal user login may assist the prosecution of trespassers on the computer system.

Recommendation
Edit the /etc/ssh/sshd_config file to set the parameter as follows: Banner /etc/issue.net

Failed Instances
i-098025956ed3541cf

5.3.1 Ensure password creation requirements are configured

Severity
High

Description
Description The pam_pwquality.so module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more. The following are definitions of the pam_pwquality .so options. try_first_pass - retrieve the password from a previous stacked PAM module. If not available, then prompt the user for a password.retry=3 - Allow 3 tries before sending back a failure. The following options are set in the /etc/security/pwquality.conf file: minlen = 14 - password must be 14 characters or moredcredit = -1 - provide at least one digitucredit = -1 - provide at least one uppercase characterocredit = -1 - provide at least one special characterlcredit = -1 - provide at least one lowercase character The settings shown above are one possible policy. Alter these values to conform to your own organization's password policies. Rationale Strong passwords protect systems from being hacked through brute force methods.

Recommendation
Edit the /etc/pam.d/password-auth and /etc/pam.d/system-auth files to include the appropriate options for pam_pwquality.so and to conform to site policy: password requisite pam_pwquality.so try_first_pass retry=3 Edit /etc/security/pwquality.conf to add or update the following settings to conform to site policy: minlen = 14dcredit = -1ucredit = -1ocredit = -1lcredit = -1

Failed Instances
i-098025956ed3541cf

5.3.2 Ensure lockout for failed password attempts is configured

Severity
High

Description
Description Lock out users after n unsuccessful consecutive login attempts. The first sets of changes are made to the PAM configuration files. The second set of changes are applied to the program specific PAM configuration file. The second set of changes must be applied to each program that will lock out users. Check the documentation for each secondary program for instructions on how to configure them to work with PAM. Set

the lockout number to the policy in effect at your site. Rationale Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Recommendation
Edit the /etc/pam.d/password-auth and /etc/pam.d/system-auth files and add the following pam_faillock.so lines surrounding a pam_unix.so line modify the pam_unix.so is [success=1 default=bad] as listed in both: auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900auth [success=1 default=bad] pam_unix.soauth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900

Failed Instances
i-098025956ed3541cf

5.3.3 Ensure password reuse is limited

Severity
High

Description
Description The /etc/security/opasswd file stores the users' old passwords and can be checked to ensure that users are not recycling recent passwords. Rationale Forcing users not to reuse their past 5 passwords make it less likely that an attacker will be able to guess the password. Note that these change only apply to accounts configured on the local system.

Recommendation
Edit the /etc/pam.d/password-auth and /etc/pam.d/system-auth files to include the remember option and conform to site policy as shown: password sufficient pam_unix.so remember=5 or password required pam_pwhistory.so remember=5

Failed Instances
i-098025956ed3541cf

5.4.4 Ensure default user umask is 027 or more restrictive

Severity
High

Description

Description 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 , .bashrc , etc.) in their home directories. Rationale 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.

Recommendation

Edit the /etc/bashrc, /etc/profile and /etc/profile.d/*.sh files (and the appropriate files for any other shell supported on your system) and add or edit any umask parameters as follows: umask 027

Failed Instances

i-098025956ed3541cf

5.4.5 Ensure default user shell timeout is 900 seconds or less

Severity

High

Description

Description The default TMOUT determines the shell timeout for users. The TMOUT value is measured in seconds. Rationale Having no timeout value associated with a shell could allow an unauthorized user access to another user's shell session (e.g. user walks away from their computer and doesn't lock the screen). Setting a timeout value at least reduces the risk of this happening.

Recommendation

Edit the /etc/bashrc and /etc/profile files (and the appropriate files for any other shell supported on your system) and add or edit any umask parameters as follows: TMOUT=600

Failed Instances

i-098025956ed3541cf

5.4.1.1 Ensure password expiration is 365 days or less

Severity
High

Description
Description The PASS_MAX_DAYS parameter in /etc/login.defs allows an administrator to force passwords to expire once they reach a defined age. It is recommended that the PASS_MAX_DAYS parameter be set to less than or equal to 365 days. Rationale The window of opportunity for an attacker to leverage compromised credentials or successfully compromise credentials via an online brute force attack is limited by the age of the password. Therefore, reducing the maximum age of a password also reduces an attacker's window of opportunity.

Recommendation
Set the PASS_MAX_DAYS parameter to conform to site policy in /etc/login.defs : PASS_MAX_DAYS 90 Modify user parameters for all users with a password set to match: # chage --maxdays 90 <user>

Failed Instances
i-098025956ed3541cf

5.4.1.2 Ensure minimum days between password changes is 7 or more

Severity
High

Description
Description The PASS_MIN_DAYS parameter in /etc/login.defs allows an administrator to prevent users from changing their password until a minimum number of days have passed since the last time the user changed their password. It is recommended that PASS_MIN_DAYS parameter be set to 7 or more days. Rationale By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

Recommendation

Set the PASS_MIN_DAYS parameter to 7 in /etc/login.defs : PASS_MIN_DAYS 7 Modify user parameters for all users with a password set to match: # chage --mindays 7 <user>

Failed Instances
i-098025956ed3541cf

5.4.1.4 Ensure inactive password lock is 30 days or less

Severity
High

Description
Description 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 30 days after password expiration be disabled. Rationale Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

Recommendation
Run the following command to set the default password inactivity period to 30 days: # useradd -D -f 30 Modify user parameters for all users with a password set to match: # chage --inactive 30 <user>

Failed Instances
i-098025956ed3541cf

4.2: Findings details - Common Vulnerabilities and Exposures-1.1

No findings were generated for this rules package.

4.3: Findings details - Network Reachability-1.1

TCP port 20 (FTP) is reachable from the internet with no listener on instance

Severity
Informational

Description
On this instance, recognized port(s) are reachable from the internet with no process listening on the port.

Recommendation
You can edit the Security Group sg-03c0fe3e924055723 to remove access from the internet on port 20

Failed Instances
i-098025956ed3541cf

TCP port 21 (FTP) is reachable from the internet with no listener on instance

Severity
Informational

Description
On this instance, recognized port(s) are reachable from the internet with no process listening on the port.

Recommendation
You can edit the Security Group sg-03c0fe3e924055723 to remove access from the internet on port 21

Failed Instances
i-098025956ed3541cf

TCP port 22 (SSH) is reachable from the internet with active listener on instance

Severity
Informational

Description
A recognized port is reachable from the internet with a service listening

Recommendation
You can edit the Security Group sg-03c0fe3e924055723 to remove access from the internet on port 22

Failed Instances
i-098025956ed3541cf

TCP port 23 (Telnet) is reachable from the internet with no listener on instance

Severity
Informational

Description
On this instance, recognized port(s) are reachable from the internet with no process listening on the port.

Recommendation
You can edit the Security Group sg-03c0fe3e924055723 to remove access from the internet on port 23

Failed Instances
i-098025956ed3541cf

4.4: Findings details - Security Best Practices-1.0

Disable root login over SSH

Severity
Medium

Description
This rule helps determine whether the SSH daemon is configured to permit logging in to your EC2 instance as root.

Recommendation
To reduce the likelihood of a successful brute-force attack, we recommend that you configure your EC2 instance to prevent root account logins over SSH. To disable SSH root account logins, set PermitRootLogin to 'no' in /etc/ssh/sshd_config and restart sshd. When logged in as a non-root user, you can use sudo to escalate privileges when necessary. If you want to allow public key authentication with a command associated with the key, you can set PermitRootLogin to 'forced-commands-only'.

Failed Instances
i-098025956ed3541cf