Deficiency Analysis of the Defense Information Systems Agency Security Technical Implementation Guide for Redhat Enterprise Linux 7

by
Jeremy Filizetti

May 10, 2020

Table of Contents

Figures and Tables

Abstract

The Department of Defense spends countless hours into security configuration, assessment, and documentation. These security configurations are often derived from Security Technical Implementation Guides (STIGs) that are published for various hardware and software. One of the most time consuming and problematic STIGs is related to operating systems for the Redhat Enterprise Linux system that is created by the Defense Information Systems Agency. This STIG is of vast complexity due to the complex nature of the operating system. As a result, there is often outdated information incorporated into this document. In addition, many changes recommended in this STIG have far reaching effects on performance and usability.

In this report many deficiencies with the current DISA RHEL 7 STIG are investigated and approximately 40% of them require additional consideration.

Introduction

Cyber security is the fastest growing focus area of information technology systems in the Department of Defense. The goal of security is to provide Confidentiality, Integrity, and Availability also known in the security community as the CIA triad. To achieves these goals operating systems must continually be evaluated as new features are integrated to ensure that the security is not compromised. In addition, security often creates hurdles for usability and performance and therefore most operating systems are not shipped in a "secure by default" configuration. To mitigate this problem the DoD creates Security Technical Implementation Guides with coordination from operating system vendors to provide a security posture they consider to be secure. In this report I plan to evaluate the STIG for the Redhat Enterprise Linux (RHEL) 7 operating system to determine areas that have failed to properly account for usability, performance, Denial of Service (DoS), and other issues. This is report is based off of the latest STIG published by the Defense Information Systems Agency Version 2 release 7 dated April 24, 2020 referenced as [1].

This report is targeted at technical evaluators and decision makers to bring attention to the numerous issues created by the process of implementing security guidance without full understanding of the impacts. It is often joked that the only secure system is the one that isn't plugged in. We must strive to provide effective use of tax payer dollars by squeezing all the performance we can get out of hardware and without hindering our operations and maintenance staff with burdensome requirements that affect their ability to do their jobs. I this assessment I will evaluate the following areas as it applies to the DISA STIG for RHEL 7 [1]:

- Outdated Items
- Performance Impacts
- Potential DoS
- Usability Impacts
- Other Issues

There are several areas in this report where small excerpts of source code are provided from the RHEL/Centos 7.8 packages. These are included to provide assistance to technical staff who would like to validate the details in this report. Each inclusion of source code will have several surrounding lines to provide context, the line numbers, and source file identified. Also, every item detailed in this report also details the STIG ID numbers from [1] at the end of the section. This is to provide clarity and also assistance to any further review necessary

Data Section

Outdated Items

Password Outdated Items

The current release for the RHEL 7 STIG [1] was released on April 24, 2020. Despite this recent release it is still out of date with the guidance from the National Institute of Standards and Technology (NIST) Special Publication 800-63 Digital Identity Guidelines [2]. There are several criteria that have been outdated with the latest recommendations and are detailed below. These guidelines apply to human passwords and not stored machine level passwords.

Password Expiration No Longer Recommended

According to [3] users tended to choose weaker passwords when they know password changes were imminent in the near future. The password changes often used “common transformations such as increasing a number in the password” [3]. The result is that security is not increased by these changes. While recommendations for temporal password expirations are no longer recommended event-based expirations still remain in place. Event-based password expirations are the result of some sort of breach of the password database.

Affected STIG IDs: RHEL-07-010230, RHEL-07-010240, RHEL-07-010250, RHEL-07-010260

Password Composition Rules No Longer Recommended

The current requirements in [1] specify the following password composition rules:

- At least one each of class (uppercase letters, lowercase letters, numbers, and symbols)
- No more than 3 repeating characters
- No more than 4 repeating characters in the same class

All these requirements have been removed as of [2]. The reasoning is again based on human factors. Users tended to use predictable methods of fulfilling these requirements which minimized any security gain. Another determined weakness of the old scheme is that these rules encouraged people to use the same password across multiple systems. This is particularly damaging for DoD users where accounts can exist on multiple networks. These multiple networks are very common in DoD environments where users may have an account on unclassified, secret, and top-secret systems.

Affected STIG IDs:
RHEL-07-010120, RHEL-07-010130, RHEL-07-010140, RHEL-07-010150, RHEL-07-010160, RHEL-07-010170, RHEL-07-010180, RHEL-07-010190, RHEL-07-010280

Additional Password Restrictions

The new mechanism of preventing weak passwords is to utilize a blacklist of common passwords. A specific list of potential candidates is included below from [2]:

- Passwords obtained from previous breach corpuses
- Dictionary words
- Repetitive or sequential characters (e.g. ‘aaaaaa’, ‘1234abcd’).
- Context-specific words, such as the name of the service, the username, and derivatives thereof

Password databases are included with the cracklib package that comes with the operating system. Any of these databases of blacklisted passwords can be added to the pam_pwquality module.

Password Based Key Derivation Functions (PBKDFs)

The updated recommendation for memorized secret verifiers should use time and memory hard key derivation functions. The only NIST evaluated algorithm that supports this requirement is Balloon [3]. This particular rule only affects one item in [1] related to PBKDFs which is for the grub2 boot loaded. Unfortunately, there is no support in grub2 for the Balloon algorithm. Given the lack of a current technical implementation this item should be prioritized to develop a solution.

Mount Options for /dev/shm

The temporary file system used for shared-memory applications is setup by the system init process, systemd. Several STID IDs require this file system to be mounted with the nodev and nosuid options. However, these options are already defined in the source code for systemd used by the operating system. The specific lines are highlighted below:

Note: Some white-space has been trimmed from the following source code for readability.

Source file: systemd-219/src/core/mount-setup.c

```
 76 static const MountPoint mount_table[] = {
 77 { "sysfs", "/sys", "sysfs", NULL, MS_NOSUID|MS_NOEXEC|MS_NODEV,
 78   NULL,   MNT_FATAL|MNT_IN_CONTAINER },
 79 { "proc", "/proc", "proc", NULL,  MS_NOSUID|MS_NOEXEC|MS_NODEV,
 80   NULL,          MNT_FATAL|MNT_IN_CONTAINER },
 81 { "devtmpfs","/dev", "devtmpfs", "mode=755", MS_NOSUID|MS_STRICTATIME,
 82   NULL,          MNT_FATAL|MNT_IN_CONTAINER },
 83 { "securityfs", "/sys/kernel/security", "securityfs", NULL, MS_NOSUID|MS_NOEXEC|MS_NODEV,
 84   NULL,          MNT_NONE                   },
 85 #ifdef HAVE_SMACK
 86 { "smackfs", "/sys/fs/smackfs", "smackfs", "smackfsdef=*", MS_NOSUID|MS_NOEXEC|MS_NODEV,
 87   mac_smack_use, MNT_FATAL                  },
 88 { "tmpfs", "/dev/shm", "tmpfs","mode=1777,smackfsroot=*", MS_NOSUID|MS_NODEV|MS_STRICTATIME,
 89   mac_smack_use, MNT_FATAL                  },
 90 #endif
 91 { "tmpfs", "/dev/shm", "tmpfs","mode=1777", MS_NOSUID|MS_NODEV|MS_STRICTATIME,
```

Affected STIG IDs: RHEL-07-021022, RHEL-07-021023

Disable Promiscuous Mode

The current recommendation to disable promiscuous mode is unnecessary as enabling it through the init scripts has been deprecated in RHEL 7 as detailed in [4].

Affected STIG ID: RHEL-07-040670

Performance Impacts

Auditing Performance

Auditing accounts for 71 of the 248 STIG items in [1]. Given the large footprint there should be some significant research into the impact of auditing on performance. However, there is minimal information to document the impact but the most comprehensive appears to be [5] from 2015 and [6] from 2018. [5] discussed the impact of audit overhead based on the frequency of audit events per second and is captured in Figure 1. [6] details the overhead of common programs and breaks down the performance by area of the audit system. Figure 2 details their findings

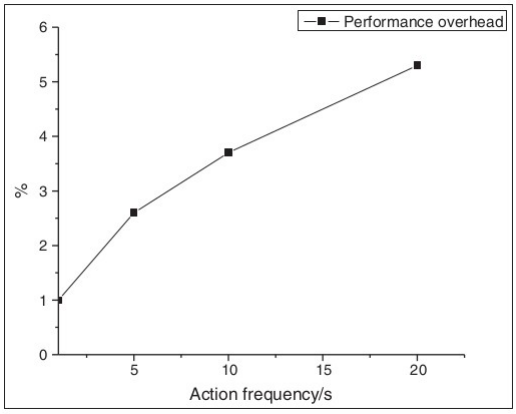

Figure 1 Audit Performance Overhead Source: [5]

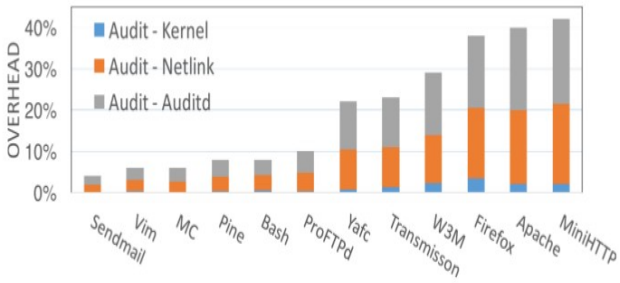

Figure 2 Audit Overhead by Program Source: [6]

It is clear from both figures that auditing can add unacceptable overhead. In Figure 2 the overhead added by the kernel is minimal but the Netlink socket used to flush data to the audit daemon, and the audit daemon overhead itself is significant for various programs. Especially affected are programs like Firefox and Apache that generate many audit records. Further analysis should be conducted to determine how auditing performance affects scalability of a single system.

Affected STIG IDs:
RHEL-07-030000, RHEL-07-030010, RHEL-07-030300, RHEL-07-030310, RHEL-07-030320, RHEL-07-030330, RHEL-07-030340, RHEL-07-030350, RHEL-07-030360, RHEL-07-030370, RHEL-07-030380, RHEL-07-030390, RHEL-07-030400, RHEL-07-030410, RHEL-07-030420, RHEL-07-030430, RHEL-07-030440, RHEL-07-030450, RHEL-07-030460, RHEL-07-030470, RHEL-07-030480, RHEL-07-030490, RHEL-07-030500, RHEL-07-030510,

RHEL-07-030520, RHEL-07-030530, RHEL-07-030540, RHEL-07-030550, RHEL-07-030560, RHEL-07-030570, RHEL-07-030580, RHEL-07-030590, RHEL-07-030610, RHEL-07-030620, RHEL-07-030630, RHEL-07-030640, RHEL-07-030650, RHEL-07-030660, RHEL-07-030670, RHEL-07-030680, RHEL-07-030690, RHEL-07-030700, RHEL-07-030710, RHEL-07-030720, RHEL-07-030740, RHEL-07-030750, RHEL-07-030760, RHEL-07-030770, RHEL-07-030780, RHEL-07-030800, RHEL-07-030810, RHEL-07-030820, RHEL-07-030830, RHEL-07-030840, RHEL-07-030870, RHEL-07-030880, RHEL-07-030890, RHEL-07-030900, RHEL-07-030910, RHEL-07-030920, RHEL-07-030321, RHEL-07-030871, RHEL-07-030872, RHEL-07-030873, RHEL-07-030874, RHEL-07-030819, RHEL-07-030821, RHEL-07-030200, RHEL-07-030201, RHEL-07-030210, RHEL-07-030211

Firewall Performance

The firewall functionality of RHEL is implemented using iptables. There have been numerous performance issues identified in iptables and so careful attention must be paid to the number of rules used. However, [1] requires “that the firewall must be configured to “system access control program must be configured to grant or deny system access to specific hosts and services”. As hardware continues to grow in capability it can support more and more services. As the number of services supported from a single machine grows so will the to enforce these requirements. Figure 3 shows the impact on throughput as the number of rules increase while Figure 4 details the impact on throughput of supporting more ports. The purple line in these graphs represent iptables used by RHEL 7.

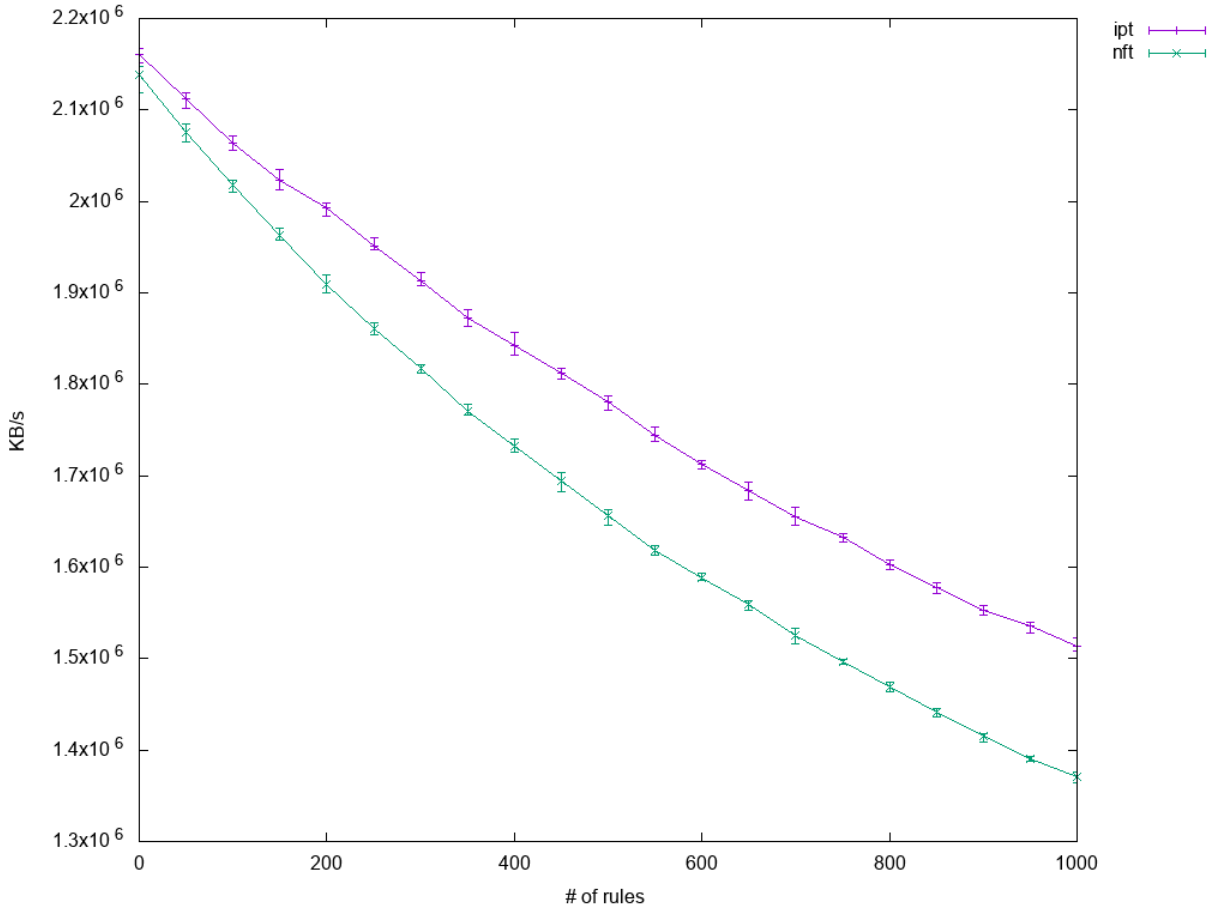

Figure 3: iptables performance impact of rules Source: [8]

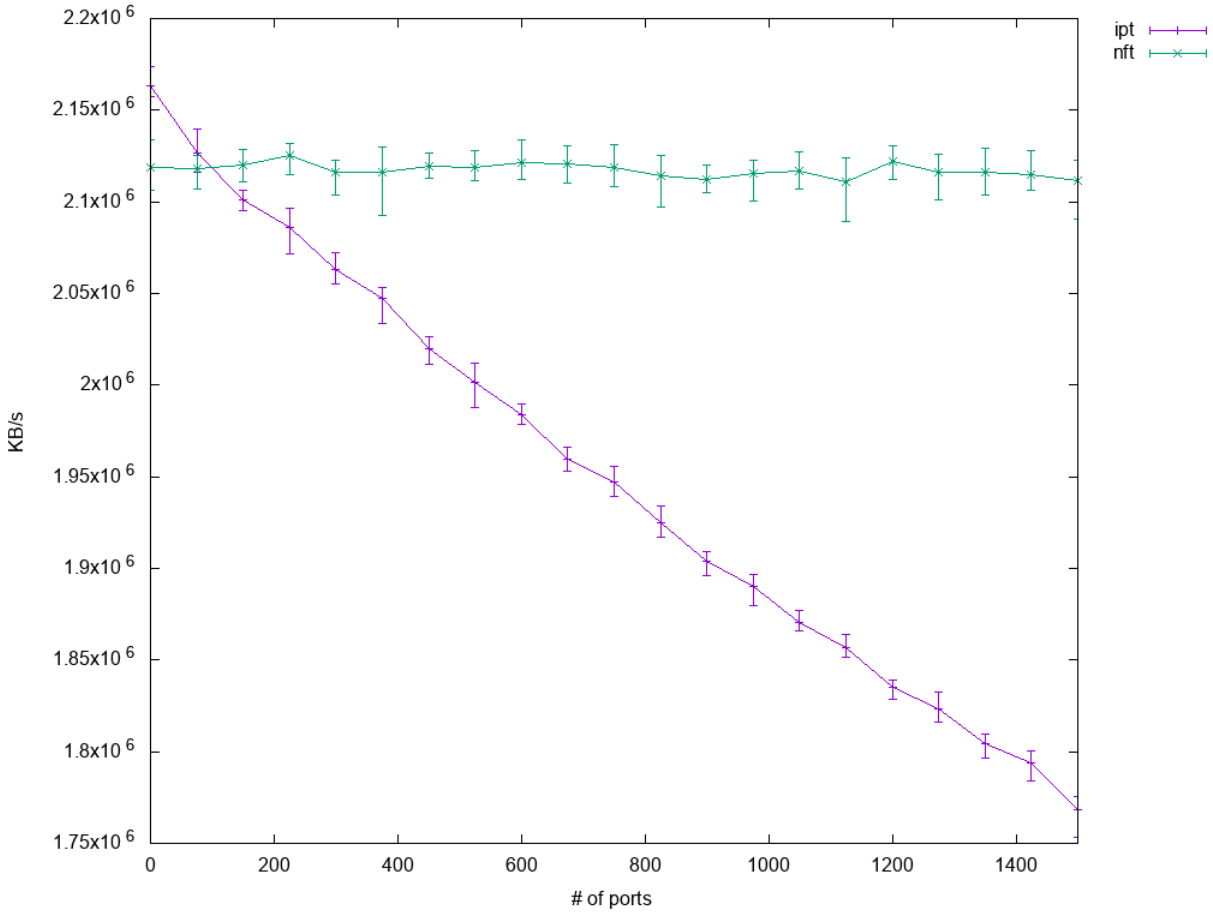

Figure 4 iptables performance impact with increasing ports Source [8]

Affected STIG ID: RHEL-07-040100, RHEL-07-040520, RHEL-07-040810

Potential Denial of Service (DoS) Changes

There are several recommendations from [1] that open possible avenues of DoS.

Login DoS

[1] requires that accounts be locked out for a minimum of 15 minutes after three unsuccessful logon attempts within a 15-minute timeframe. Given the weakened security posture from using outdated password guidelines may be some justification for this rule but this setting opens user accounts to a simple DoS. Furthermore, this rule ultimately compromises availability of the CIA triad. The PCI-DSS standard [7] requires a user id to be locked out after no more than 6 attempts. The PCI-DSS standard seems more reasonable of a balance between confidentiality and availability.

Another rule from [1] requires the root (superuser) account to also be locked out for 15 minutes after three unsuccessful logon attempts within a 15-minute time frame. This policy creates the possibility of a DoS to all system users with no ability to resolve it from within since only a superuser can unlock accounts.

Rather than lockout the root account, the pam_securetty module can be used to limit access to a console through out-of-band access using a Backplane Management Console (BMC) or Integrated Lights Out (ILO). With this additional security measure, the root account could be exempted from account lock out while still preserving security.

Affected STIG ID: RHEL-07-010320, RHEL-07-010330, RHEL-07-010430, RHEL-07-040670

System DoS

There are several requirements in [1] that require home directories, /var, and /tmp file systems to all exist on separation partitions. The justification for this requirement is that it could protect the system if the partition "became full or failed". The failure of the /var or /tmp file systems would prevent many system level daemons from functioning properly. Failures in /home would only cause user access DoS. However, these fail to account for the impact to system performance as a disk is partitioned up. On Solid State Devices (SSDs) there is no significant impact, but when utilizing Hard Disk Drives (HDDs) the impact can be dramatic. HDDs only support approximately 100-150 Input Output Operations (IOPs) per second where SSDs tend to support around 4000+ IOPS. When disks are partitioned many data transfers that could have been merged into a single IOP can no longer be merged due to their non-contiguous nature. The result is that a system disk can become saturated causing multiple second delays in responsiveness. Therefore, this recommendation should be considered only when the partitions are on SSDs or separate HDDs.

Affected STIG ID: RHEL-07-021310, RHEL-07-021320, RHEL-07-021340

Other Items

There are several rules from [1] that are inaccurate in their justification and therefore should be corrected or removed.

Removing System Accounts

[1] states that "If the accounts on the system do not match the provided documentation, or accounts that do not support an authorized system function are present, this is a finding". The recommendation is to remove several system accounts. However, these accounts come suitably protected by providing an unusable login shell and having a locked password. Therefore, there is no risk of unauthorized use of these accounts. In addition, these conflict with vendor guidance in [5] that states:

> It is recommended to keep UIDs/GIDs of the system service accounts as default. The UIDs/GIDs of some system service accounts are hard-coded in the application itself, changing the uids/gids may potentially break the functionality of an application.

These accounts exist for compliance with the Linux Standard Base [9].

Affected STIG ID: RHEL-07-020270

Interactive Users Must Have Home Directory in /etc/passwd

The discussion in [1] states that “This could create a Denial of Service because the user would not be able to access their logon configuration files, and it may give them visibility to system files they normally would not be able to access”. The first part of the statement is true but there is no risk of visibility into system files they would not normally have. This is because the Linux Discretionary Access Control (DAC) is still in use. As can be seen below from the login source code that if changing directory to the user’s home directory fails then the “/” directory is used:

util-linux-2.23.2/login-utils/login.c

```
1330        /* wait until here to change directory! */
1331        if (chdir(pwd->pw_dir) < 0) {
1332                warn(_("%s: change directory failed"), pwd->pw_dir);
1333
1334                if (!getlogindefs_bool("DEFAULT_HOME", 1))
1335                        exit(0);
1336                if (chdir("/"))
1337                        exit(EXIT_FAILURE);
1338                pwd->pw_dir = "/";
1339                printf(_("Logging in with home = \"/\".\n"));
1340        }
```

Also, relevant is the DEFAULT_HOME attribute can be set to “no” in the /etc/login.defs file to prevent login in the event that the user’s home directory is inaccessible.

Affected STIG ID: RHEL-07-020620

Usability Items

Impact on Usability

Security must be a balance between the impact on performance and usability. Different groups have different numbers of personnel to be able to operate and maintain their systems and so a discussion is necessary about the STIG rules that impact efficient system administration. Efficient administration is the ability for a small number of administrators to operate and maintain a large number of systems. The following items detail various STIG rules and their impact on efficient administration.

Delay between failed login attempts

[1] requires the addition of a 4 second delay be added to the Pluggable Authentication Modules (PAM) configuration for pam_faillock. This restriction however, ignores the fact that configuration provided by the vendor already provides a two second delay on failure on local password failures through the pam_unix module. The following source code section captures the respective section for pam_unix and highlights the fail delay setting.

Linux-PAM-1.1.8/modules/pam_unix/support.c

```
721 int _unix_verify_password(pam_handle_t * pamh, const char *name
722                           ,const char *p, unsigned int ctrl)
723 {
724         struct passwd *pwd = NULL;
725         char *salt = NULL;
726         char *data_name;
727         int retval;
728
729
730         D(("called"));
731
732 #ifdef HAVE_PAM_FAIL_DELAY
733         if (off(UNIX_NODELAY, ctrl)) {
734                 D(("setting delay"));
735                 (void) pam_fail_delay(pamh, 2000000);   /* 2 sec delay for on failure */
```

This setting combined with the idle connection closing only creates a nuisance for users and administrators logging into the system and has a negligible impact on security. To capture the additional security, see the following two approximate equations where the values are represented by the following:

900 is the number of seconds an account is locked after 3 failures

3 failures before an account is locked

1000 attempts to guess the password

6 is the number of seconds with the pam_faildelay requirement

2 is the number of seconds removing the pam_faildelay requirement

$time\,no\,fail\,delay = ¿$

$time\,with\,fail\,delay = ¿$

The addition of the failure delay is clearly insubstantial and therefore should be removed from the requirements.

Affected STIG ID: RHEL-07-010430

Remote privileged user access without password prompts

There are number of tools developed by High Performance Computing (HPC) administrators to effectively administer a large number of systems efficiently. These tools are often developed based on the need to administer thousands of systems by a small administration team. Two of the most common of these tools are Parallel Distributed Shell (pdsh) and Clustered Shell (clush). These tools work by opening secure shell connections to each server and running a command across hundreds of thousands of servers in just seconds. In order to make administrative changes efficiently administrators must be able to login as root (the superuser) or have the ability to run commands with superuser privileges using su or sudo. [1] requires that both remote root logins be disabled and su/sudo be disabled without a password. Preventing direct access to the root account is a considered a good security practice. This prevents users from logging in directly as a

user other than their own and preserving non-repudiation. However, additional security restrictions can be added to restrict su/sudo to only users of a specific group. Using these productions allow privileged escalation while maintaining non-repudiation and increased security. To make these changes the su command can be restricted to the wheel group by adding highlighted line to /etc/pam.d/su.

```
#%PAM-1.0
auth            sufficient      pam_rootok.so
auth            required        pam_wheel.so use_uid group=wheel
auth            substack        system-auth
auth            include         postlogin
account         sufficient      pam_succeed_if.so uid = 0 use_uid quiet
account         include         system-auth
password        include         system-auth
session         include         system-auth
session         include         postlogin
session         optional        pam_xauth.so
```

Restricting sudo access to the wheel group can be done by adding the following to the /etc/sudoers file.

```
%wheel        ALL=(ALL)       NOPASSWD: ALL
```

Affected STIG ID: RHEL-07-010340, RHEL-07-010350

Conclusion

Summary of findings

There are many issues identified in this report which should cause alterations of the DISA RHEL 7 STIG. To highlight the percentages of issues we have discussed here the following chart shows the percentage of those issues based on the 248 Rules in [1]. It is clear here that much consideration needs to be addressed to ensure that the Confidentiality, Integrity, and Availability are evaluated in a balanced manner. It appears as though the Availability portion of the three is not adequately being considered in many of the STIG rules identified here. Figure 5 captures the percentage of issues and acceptable rules identified in [1].

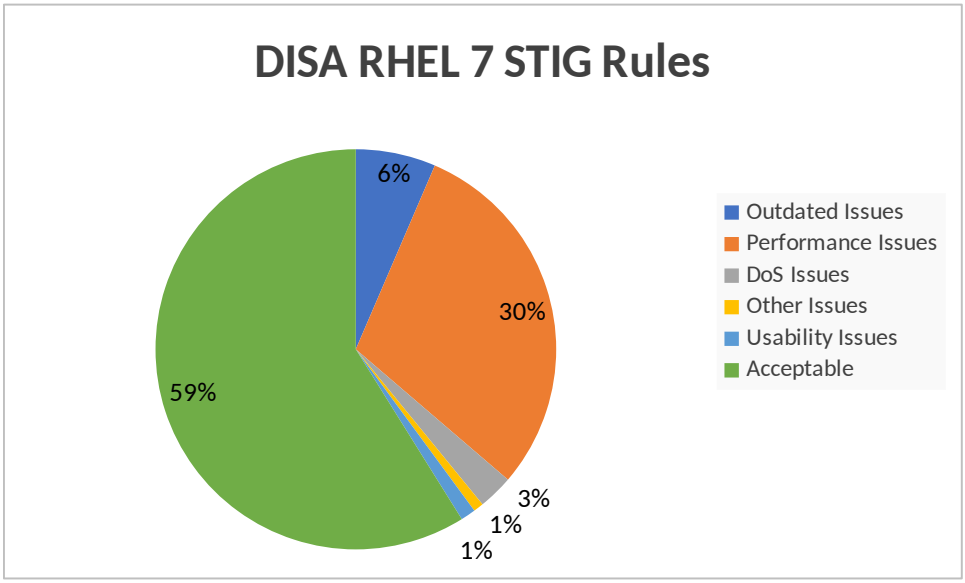

Figure 5 DISA RHEL 7 STIG Rules Breakdown

Recommendations

Based on the findings from source code reviews, updated guidance, and the various performance issues the following actions are recommended for updating the DISA RHEL 7 STIG:

1. Update all outdated password rules
2. Develop a memory and time hard PBKDF implementation (Balloon) for the GRUB2 bootloader
3. Develop a tool to monitor performance impacts of compliant auditing
4. Develop a tool to monitor performance impacts of compliant firewall rules
5. Utilize provided information for DoS issues to fix STIG rules
6. Remove the password fail delay requirement
7. Allow documented exceptions for privileged escalation without password for admin groups utilizing the documented security enhancements here

Acronyms

BMC	Backplane Management Console
CIA	Confidentiality, Integrity, Availability
DAC	Discretionary Access Control
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoS	Denial of Service
GID	Group ID
GRUB	GRand Unified Bootloader
HDD	Hard Disk Drive
HPC	High Performance Computing
ILO	Integrated Lights Management
IOPs	Input Output Operations
NIST	National Institute of Standards and Technology
PAM	Pluggable Authentication Module
PBKDF	Password Based Key Derivation Function
PCI-DSS	Payment Card Industry Data Security Standard
RHEL	Redhat Enterprise Linux
SSD	Solid State Disk
SSH	Secure Shell
STIG	System Technical Implementation Guide
UID	User ID

References

[1] *Red Hat Enterprise Linux 7 Security Technical Implementation Guide*, Version 2 Release 7, 2020.

[2] *Digital Identity Guidelines*, NIST SP 800-63, 2017.

[3] NIST SP 800-63 Digital Identity Guidelines-FAQ, *pages.nist.gov*. [Online]. Available: https://pages.nist.gov/800-63-FAQ/. [Accessed: 26-Apr-2020].

[4] "How do you set an interface to permanent promiscuous mode in RHEL 7?," *Red Hat Customer Portal*, 18-Mar-2019. [Online]. Available: https://access.redhat.com/solutions/3525641. [Accessed: 09-May-2020].

[5] H. Chen, Y. Xiao, L. Zeng, "Auditing overhead, auditing adaptation, and benchmark evaluation in Linux," *Security and Communication Networks 2015*, pp. 3523-2534, June 2015.

[6] S. Ma, J. Zhai, Y. Kwon, K. H. Lee, X. Zhang, G. Ciocarlie, A. Gehani, V. Yegneswaran, D. Xu, and S. Jha, "Kernel-supported cost-effective audit logging for causality tracking," in *Proc. 2018 USENIX Annual Technical Conference (ATC)*, Boston, MA, Jul. 2018

[7] "Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards," *PCI Security Standards Council*. [Online]. Available: https://www.pcisecuritystandards.org/document_library. [Accessed: 09-May-2020].

[8] P. Sutter, "Benchmarking nftables," *Red Hat Developer*, 18-Oct-2018. [Online]. Available: https://developers.redhat.com/blog/2017/04/11/benchmarking-nftables/. [Accessed: 08-May-2020].

[9] "Is it safe to remove/change system user account on Red Hat Enterprise Linux ?," *Red Hat Customer Portal*, 22-Oct-2019. [Online]. Available: https://access.redhat.com/solutions/31669. [Accessed: 09-May-2020].

[10] *Users and Groups*, Linux Standard Base Core Specification 5.0, 2015.