Bachelor's thesis

Degree programme in Information Technology

2018

Kaisa Henttunen

AUTOMATED HARDENING AND TESTING CENTOS LINUX 7

Security profiling with the USGCB baseline

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Degree programme in Information Technology

2018 | 41 number of pages, 71 number of pages in appendices

Kaisa Henttunen

AUTOMATED HARDENING AND TESTING CENTOS LINUX 7

Security profiling with the USGCB baseline

Operating system hardening for a Linux operating system can be automated and needs to be performed in high security environments. Automated hardening is needed in virtual environments with lots of instances. Also, for identical system environments deployment automation is essential.

Automatic system hardening is a well-established administration procedure. The purpose of this work was to combine several tools and guides in one text and to obtain a low-level guide for a secure virtual environment.

In this Bachelor's Thesis work, theory of Linux operating system hardening was studied and a study on automated installation of hardened Linux operating systems, according to the USGCB security standard, was performed. Also, the security standard, SCAP content via XCCDF checklist was studied and a new independent rule was created for system hardening.

The produced environment consists of a hardened virtualization host and three hardened guest virtual machines. The system environment was designed in parts with VMware Workstation and implemented on DELL server hardware, where the study and analysis of the automated hardening were performed.

A quantitative results of the hardening are discussed and the created and tested checklists presented. The results indicate that a sufficiently good security state can be obtained with the used tools and with only a little manual configuration.

KEYWORDS:

kickstart, centos, hardening, kvm, openscap, usgcb

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Degree programme in Information Technology

2018 | 41 sivua, 71 liitesivua

Kaisa Henttunen

AUTOMATISOITU CENTOS LINUX KOVENNUS

USGCB standardin mukainen tietoturvaprofilointi

Linux -käyttöjärjestelmäkoventaminen, eli tietoturvakäytännön mukainen konfigurointi, voidaan automatisoida CentOS käyttöjärjestelmälle. Kovennettu käyttöjärjestelmä on yleinen vaatimus korkean turvallisuuden ympäristöissä. Automatisoidusti suoritettu kovennus on tarpeen esimerkiksi virtuaaliympäristöissä missä on paljon virtuaalikoneita, tai jos tietyllä tavalla kovennettu virtuaalikone täytyy asentaa useaan eri paikkaan.

Automaattinen käyttöjärjestelmäkoventaminen on tietoturva-ammattilaisten hyvin tuntema toimenpide. Tämän työn tarkoituksena on, uuden kovennustavan keksimisen sijaan, tutkia ja tuottaa dokumentti usean vapaan lähdekoodin kovennusohjelmiston käytöstä kovennetun virtuaaliympäristön tuottamisesta.

Tässä työssä on tutustuttu käyttöjärjestelmäkoventamisen teoriaan ja tutkittu automatisoitua USGCB tietoturvastandardin mukaista Linux -käyttöjärjestelmäkoventamista. Tässä työssä on myös tutkittu tietoturvastandardi SCAP:in mukaisen itsenäisen kovennussännön tuottamista.

Tuotettu ympäristö koostuu kovennetusta virtuaalialustasta sekä kolmesta virtuaalikoneesta. Virtuaalikoneet on rakennettu sekä testattu VMware Workstation -virtuaalikonneessa ja varsinaista tutkimusta varten asennettu DELL PowerEdge palvelimelle.

Tutkimuksen tuloksena esitetään analyysi käytetyn OpenSCAP ohjelmiston tulosten perusteella. Analyysin perusteella esitetään CentOS käyttöjärjestelmän automaattisen koventamisen tuottavan riittävän hyvän tietoturvatason. Prosessi vaati vähäistä manuaalista konfigurointia asennuksen jälkeen.

ASIASANAT:

kickstart, centos, käyttöjärjestelmäkovennus, kvm, openscap, usgcb

CONTENT

APPENDICES

FIGURES

TABLES

LIST OF ABBREVIATIONS

ALSR	Address Space Layout Randomization
API	Application Programming Interface
CCE	Common Configuration Enumeration
CIS	Center for Internet Security
CVE	Common Vulnerabilities and Exposures
DISA	Defense Systems Information Agency
DoD	U.S. Department of Defense
GUI	Graphical User Interface
HTML	Hypertext Markup Language
HTTPS	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I/O	Input / Output
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
KVM	Kernel-based Virtual Machine
MAC	Mandatory Access Control
MITRE	Massachusetts Institute of Technology Research and Engineering
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
OVAL	Open Vulnerability and Assessment Language

PKI	Public Key Infrastructure
QEMU	Quick Emulator
RAM	Random Access Memory
SCAP	Security Content Automation Protocol
SHA	Secure Hash Algorithm
SOC	Security Operations Center
SSG	SCAP Security Guide
SSH	Secure Shell
SSL	Secure Sockets Layer
STIG	Security Technical Information Guides
TLS	Transfer Layer Security
UDP	User Datagram Protocol
USGCB	United States Government Configuration Baseline
VMM	Virtual Machine Monitor
XCCDF	The Extensible Configuration Checklist Description Format
XML	Extensible Markup Language

1 INTRODUCTION

Operating system security hardening consists of technically configuring an operating system in such a way that security aspects are taken into account.

It is essential for all the computer environments that host services to the internet. Also, in high security environments, such as campuses, hospitals, enterprise class businesses or in military environments, all systems need to be hardened and good security measures maintained throughout the lifetime of the system. For this need standardized security benchmarks, that offer technical security measures and guidance, were developed. This thesis discusses applying such measures in an automated fashion for a particular operating system, namely Centos Linux 7.

This work concentrates fully on operating system level hardening. No other end point security measures or systems are discussed, such as malware detection, or authentication. A secure system will always require layers of security of which the lowest level that all the other security layers rely upon is the secure operating system. A standardized security benchmark was used as the basis of the security policy. Also creating and testing new security rules was studied.

There exists a lot of information and guides, used by the professionals, about operating system hardening in the internet, see (Red Hat Manual, 2018) (Waltermire;Quinn;Booth;Scarfone;& Prisaca, 2018) (Sumit, 2006) for references. Nonetheless, for setting up such a system, with example commands and files that describe in detail both the automated installation and security auditing, such a guide was not available at the time of writing. This work, therefore, provides a hands-on guide on how to produce a hardened virtual environment and how to deploy hardened CentOS systems automatically.

All the used software, except the VMware Workstation are open source and readily available in the internet. CentOS 7 was chosen as the main operating system, because it uses the Anaconda installer that enables the automatic installation. The other workhorse in this work was the open source security compliance solution, OpenSCAP (OpenSCAP Team, 2018). It was used as both the hardening and testing tool and as the tool to measure the applicability of the configuration for hardened virtual environment building.

The auditing procedure with OpenSCAP often involves several iterations of checking the system against the security policy and fixing the found vulnerabilities with built in remediation scripts. When run regularly from a script the used automated checking can be also used to keep the system at the chosen security policy and also to inform the administrator of any failed check items. Continuous administration and users' actions will not be discussed in detail in this work.

The purpose of this work was to study the hardening automation of the target system and to build and test systems so that a security policy compliance would be obtained with minimal manual configuration.

The system environment was designed in parts with VMware Workstation and implemented on DELL server hardware, where the tests and analysis of the automated hardening were performed.

In this work only, the Kernel-based Virtual Machine (KVM) virtualization host configurations and files are referenced inline or in the Appendix as an example. The virtual guest system configurations and results were very similar and can be constructed from the referenced basing on the description in the Section 5.3.

In this work, **bold** is used for software and file names. *Italics* is used for highlighting the virtualization host and guest attributes, such as the *Host policy*, or to emphasize special concepts. In the code sections, commands starting with the # -command prompt are run as the root user.

The references in this work are mainly internet hyper-links. There may be many reasons, why officially printed document is not produced, one of the main reasons being the constantly updated nature of the referenced material. For example, the open source documentation is nowadays very rarely printed into books or published in journal articles because of the constantly changing content and the critical relation to the software and hardware the information lives on. The open source references are many times not owned by single authors, but the information is produced by an ever-changing community of people. The documentation that is maintained by the open source communities, that are often spread across many continents, is typically produced only as web pages that could be described as live documents.

By no means, books on several of the studied subjects can be found, but these are not written by the authors of the software and are not as authoritative as the community documentation that provides the most up-to-date information. %The project documentation is after all the documentation that is referenced as the project origin in the published guide books also.

Another invaluable source of information with Linux operating system software are the manual pages, generally referred to as **man**, that provide for each software version the most original and up to date information on the correct usage. All the Linux commands (referred to in this work with **bold** characters) can be referenced in a suitable Linux system with the **man** tool. Also, some Business or governmental White Papers that might not have an ISBN reference or publication classification are referenced here with a web reference.

For these reasons web content is referred if scientific or official publications of the contents are lacking.

The thesis is structured as follows. In Section 2 the theory of operating system hardening is introduced with concrete examples of technical implementation. The security standards are, also, introduced to give context to the later implemented security policy. In Section 3 concepts of Linux virtualization are visited as applicable to this work. Also, the used operating systems and the used OpenSCAP tools are briefly described. Section 4 presents the hardening automation concept for CentOS and how to implement it. In Section 5 the install process is described in detail with the used files and commands and in Section 6 the analysis on the produced systems are reported. Finally, in Conclusions 7 the hardening automaton benefits and drawbacks are discussed based on the test system.

2 HARDENING THEORY

Hardening is the art of enhancing security of your network infrastructure and operating systems to maintain and improve the effective security configuration settings. By hardening the operating systems, the attack surface is decreased by removing vulnerable services, upgrading software as well as implementing security practices into the operating system e.g. by monitoring users' password strength and logins.

The depth of hardening depends on the organization policies and on the skills of the administrator. The commonly used methodology is to use predefined checklists, that are run periodically to maintain the chosen security policy. These checklists can be run via auditing tools such as OpenSCAP, that can utilize standardized file formats specially crafted for security auditing.

These standardized protocols, file formats and specification languages include The Security Content Automation Protocol (SCAP), Open Vulnerability and Assessment Language (OVAL) definitions and The Extensible Configuration Checklist Description Format (XCCDF) benchmarks. SCAP validated products meet National Voluntary Laboratory Accreditation Program (NVLAP) laboratory and National Institute of Standards and Technology, NIST IR 7511, requirements (NIST, 2018).

There exists several standardized government level security protocols and practices, such as the USGCB (NIST USGCB, 2018), DISA/STIG (IASE STIGs, 2018), NIST SP 800-53 (NIST Special Publication, 2013) and the CIS Benchmark (CIS Benchmark, 2018)[1] that provide a set of security measures for several operating systems. These practices provide guidance in several levels of concreteness, ranging from high level guidance to detailed technical checklists like the National Checklist Program NIST SP 800-70 (NIST Special Publication, 2018) and Center of Internet Security (CIS) Benchmarks.

The USGCB profile offers prescriptive guidance and can be used in technical hardening via SCAP. CIS Benchmarks also provide a prescriptive basis for operating system hardening for many use cases. The DISA STIG baseline for CentOS Linux 7 and MITRE

[1] United States Government Configuration Baseline (USGCB), Defence Suystems Information Agency (DISA), Security Technical Information Guides (STIG), National Institute of Standards and Technology (NIST)

CCE's together provide the security settings for US Department of Defense (DoD) systems.

These international standard organizations and government organizations, update their guidelines and add new entries to the checklists periodically which can be downloaded and directly used in the OpenSCAP testing automation.

The SCAP security protocol, utilized in this work, is one of the industry standards. The NIST Information Technology Laboratory (ITL) validated SCAP specifications are derived from SCAP community ideas and keep constantly changing as the security landscape evolves. The community consists of partnership public/private parties from industry, research and educational institutions, and U.S. government parties that are working in standardization of technical security operations.

The SCAP protocol (Waltermire;Quinn;Booth;Scarfone;& Prisaca, 2018) utilizes, not one, but multiple standards and specifications that are used together in automatic security testing. Within SCAP, the OVAL and XCCDF languages are used, also command line scripts (with Bash, Python, Perl and Ruby) with the Script Check Engine (SCE) can be utilized to easily deliver an interoperable state for the system security.

Also, software vulnerabilities can be mitigated with OVAL definitions using the same tool OpenSCAP. For vulnerability specification and software exploits MITRE CVE database[2] (MITRE Corporation, 2018) provides the industry standard reference. The CVE database is updated as new vulnerabilities are found. This work does not treat software vulnerabilities (Redwood, 2015),(Simons, 2005) but concentrates only on the operating system vulnerabilities (Niu;Mo;Zhang;& Lv, 2014) and hardening.

Hardening controls and mechanisms include: *administrative control* protocols and policies (government regulations, organization security policies) that lead to automated *hardening scripts* (kickstart CentOS install automation, OpenSCAP), *access control* tools (SELinux, AppArmor), implemented *network controls* (firewalls, iptables), *process and memory group* (cgroups) and *monitoring* (SCAP, IDS, IPS) utilization.

The hardening in this work concentrates on CentOS operating system automated hardening with Anaconda kickstart system installer and the OpenSCAP tool that allows to change the system configuration of required security controls at install time. Kickstart

[2] Massachusetts Instituite of Technology Research and Engineering (MITRE), Common Vulnerabilities and Exposures (CVE)

is an automated network installation system for Red Hat, Fedora and CentOS Linux distributions. This system is discussed in Section 4.

The automated hardening was done by accessing files from external server, named **node.intra**, that contains all the needed operating system and configuration files.

2.1 Hardening tiers and policies

Operating system hardening consists of different tiers of security operations ensuring the appropriate system configuration, service software, firmware and applications are actively updated. The organizations risk management and security policy should embrace all the information and physical security aspects, asset management, human resources and communications up to compliance, business continuity and incident management. This work deals only with one part of information systems' management particularly on the lowest level, or lowest tier as is called in this thesis, namely the operating system security.

On the *first tier*, the secure operating system configuration also can be divided in to several hardening levels. In this work the hardened systems consist of the hypervisor and virtual guest systems for which the partitioning, kernel, and operating system services and applications should be configured according to a security baseline (for example according to the USGCB security standard).

In the *second tier* the software is promptly updated and upgraded according to the available vendor patches or reconfigured to avoid the reported Common Vulnerabilities and Exposures (CVE). The security policy can also be maintained in this tier with compliance tools such as **oscap**.

The *third tier* builds upon active security monitoring continuously performed by the system administrators based on e.g. logs and monitoring tools.

The operating system level hardening can be automatically performed already at the installation phase via the Anaconda Kickstart installation method created by Red Hat. This work studies the hardening of CentOS Linux 7 operating systems with Anaconda Kickstart and OpenSCAP tool.

Only a minimal installation with minimal amount of services was chosen for the systems in accordance with general security requirements (see section 2.2). The *KVM host* only

includes the virtualization environment and security services to comply with the chosen security *Host policy*. In the *Guest* virtual machines, some services are hosted such as IDS, messaging services or web services, each in their own virtual servers.

The tailored checklists for the *Host policy* and *guest policies* were crafted from the OpenSCAP USGCB security policy with the **oscap-workbench** program and saved to the installation server for the automatic installation. The security policy in this work was chosen to comply only to the most critical steps of a secure system according to the author and should not be used as is without carefully assessing the necessary measures of security for each system individually.

Separate checklists were made for all target systems: The CentOS 7 *KVM Host* and the CentOS *Guests*, but only the *Host* files will be available in the Appendices. With the automatic kickstart installation, available for the Red Hat derived operating systems, the installed system is guaranteed to comply the chosen security policy from the first boot when implemented as is done in this work.

2.2 Hardening technical requirements for CentOS Linux

As general ideas for operating system hardening the access privileges of users and applications need to be carefully minimized, authentication and logging need to be considered to suit each use case. Also, some security measures, like secure partitioning, need to be considered already at the operating system installation. The technical procedures that can be taken to harden the system are called a security policy in the context of this work.

The security policy is basically a set of technical requirements, that can be described as a checklist of system configuration rules. The CIS Benchmark checklist or USGCB standard requirements provide a basis for such policies. These general rule sets need to be customized for particular environments to contain only the relevant rules before implementation. In the full checklist there exists several even contradictory items allowing implementation of the operating system based benchmark to different system environments. The security requirements are defined by the OpenSCAP USGCB XCCDF and datastream (DS) files, described in more detail in Section 3.3, and are referenced in this work as the *KVM Host policy*.

This section describes a list of general technical hardening procedures and security requirements for the kernel to be considered when designing a hardened Linux operating system environment and is meant as a mere guide for creating an adjusted security policy.

- The BIOS password needs to be set (not used in this work).
- The disks are partitioned so that the **/boot,** root **/, /swap, /tmp, /var/log**, **/var/log/audit** and **/var/lib/libvirt** (in the case of KVM) -partitions are created separate and on Logical Volume Management (LVM). Make separate logging partitions although logging is to be configured and handled in the hardened system by separate logging server after the install.
- The **swap, root** and **/var/log/audit** partitions are encrypted with LUKS.
- Root login is disabled.
- All unnecessary listening daemons are disabled, such as **cupsd.**
- Should SSH be allowed on the virtualisation host, it should be only allowed with cryptographic keys.
- A strong password policy is enforced.
- NTP should be configured.
- Any necessary authentication protocols should be hardened.
- An Intrusion Detection System (IDS) or an Intrusion Protection System (IPS) is deployed. In this work, SELKS Linux, was used.
- Frequent updating of the operating system and applications is enforced.
- Logging is performed outside the system and is encrypted with TLS/SSL certificates or via **kerberos**, that also provides non-repudiation.
- Network is isolated such that the virtualization host management interface is separate from the guests traffic interface.
- Only the network ports needed for the system management and a separate service port are allowed and managed.
- Test and review the enforced firewall rules regularly. For firewalling, **/etc/sysconfig/iptables** was used in this work.
- IP forwarding is disabled in the kernel.
- Ipv6 protocol is turned off at the kernel level if not specifically needed and carefully firewalled in the system.
- Any unnecessary kernel modules system such as **bluetooth** or appletalk are disabled.

- Mandatory Access Control is deployed at the kernel level. Here SELinux was utilised.
- Deploy Address Space Layout Randomisation (ASLR) that can prevent certain types of buffer overflow attacks. This is not included in the USGCB profile.
- CVE kernel vulnerabilities and exploits for guest to host escalation are taken care of by frequent patching.

Kernel hardening can be further enhanced by providing a custom kernel, but this requires extra manual work each time new kernel is required by the operating system upgrade. The level of kernel hardening in this work was utilized via disabling unwanted kernel modules and by using SELinux a linux security module (Wright;Cowan;Smalley;Morris;& Kroah-Hartman, 2002) (Chen, 2009). Security-Enhanced Linux (SELinux), is a Mandatory Access Control (MAC) system for the Linux kernel. It provides via sVirt the wanted resource isolation for the KVM host. SELinux provides for the KVM host in addition to the user isolation also process confinement.

As the compromise of the host would compromise all the guest operating systems too, host security is of crucial importance. Network security is a vast field of it's own and is not described in depth in this work. The produced system would benefit from a coherent network security plan, but due to the test nature of the rehearsal, is omitted. Only local firewalls, composed of direct **iptables** rules, provide network security in this work. In a production environment it is vital to consider the secure network configuration, that correctly takes into account the needed services and protocols and bans everything else.

2.3 An example of technical hardening

From the technical point of view the Linux operating system hardening procedures mainly include software installation, removal and configuration via the configuration files. To keep the security content portable the security benchmarks refers, if possible, to the Common Configuration Enumeration list, CCEs currently maintained by NIST (NIST NVD, 2018), that provides unique standardized identifiers to system security configuration issues.

Code snippet 1 Security policy rule examples, presents an example of some security post install hardening procedures that can be identified with the CCE enumeration. In this example the specific CCE security policy requirements are fulfilled by forcing the

removal of certain vulnerable services or applications (marked in the Code Snippet with a minus (-) before the service) or by changing the system configuration (here **/etc/fstab**).

```
  # CCE-14495-6 (row 222)
  -sendmail
  # CCE-4464-4 (row 219)
  -dhcp
  # CCE-14881-7 (row 240)
  -vsftpd
  # CCE-4514-6 (row 241)
  -httpd
  -gnome-user-share
  # CCE-14825-4 (row 178)
  -isdn4k-utils
  # CCE-17504-2 (row 255)
  -irda-utils
  # CCE-18200-6 (row 253)
  -talk

  # CCE-14584-7 (Row 25)
  grep " \/var\/tmp " ${FSTAB} >/dev/null
  if [ $? -eq 1 ]; then
    echo -e
"/tmp\t\t/var/tmp\t\t\text3\tdefaults,bind,nodev,noexec,nosuid\t0
0" >> ${FSTAB}
  fi
```

Code snippet 1 Security policy rule examples

The first tier hardening operations were enforced, in this work, via the automated kickstart installer, discussed in the Section 4.1. The involved kickstart file and the provided OpenSCAP security content implement the chosen security policy via technical rules like the ones presented in the Code snippet 1.

3 VIRTUALIZATION, PLATFORMS AND TOOLS

3.1 Virtualization

The concept of separating user privileges and system processes has for long been a necessary part of system testing and administration.

The earliest UNIX concept, **chroot**, has been used since 1979 for dependency control, recovery bootstrapping and privilege separation, that effectively allows for system sandboxing and offers many desired security features. The chroot operation changes the root directory for all children process to a designated file tree and, therefore confines the operating environment to a subset of system files and folders. This kind of a procedure have also coined the names jail and container that are currently used for modern privilege separation when enforced with e.g. root user constraints, network and kernel namespace separation.

Virtualisation refers to fully software based operating environments. ``The primary goal of virtualization is to decouple the software from the available hardware resources in order to allocate them optimally to each system in isolation.'' (Ritzau & Warnke, 2010) Virtual machines are full operating systems that do not run directly on hardware. Different types of virtualisation techniques exist, of which only KVM, a Type 1 Hypervisor (or Virtual Machine Monitor, VMM), is introduced in this work. VMware Workstation was also used in this work for testing purposes, but is not discussed here. Templates with a specific version of an operating system define virtual machines that can be saved as a snapshot state of that particular environment. Later these snapshots can be restored independently. In a virtualisation environment the *host* machine that provides the I/O resources (CentOS Linux 7 in this case) is installed on the physical hardware and offers hardware virtualisation for other operating systems with KVM and the Quick Emulator (QEMU). The complete isolated *guest* operating systems can be installed ``on top of'' the host operating system using hardware emulation provided by the hypervisor and is, therefore, called a virtual machine. In this kind of a system the guest systems are effectively separated from each other and userspace isolation and process control is better than in one system with multiple users. The virtualisation adds security to the

system by separating also the network services from each other. It is not recommended for security reasons to operate several services on one machine. If one machine gets compromised, the other services are unaffected because these reside on isolated virtualised systems (Wang, 2012).

Virtualisation has become an extremely important part of almost all networked business from software development to cloud based IaaS services, which emphasises the significance of security in all digital services and infrastructures. The advantages of virtualisation in addition to the ones mentioned include better hardware utilisation and availability, because the virtual machines can be copied to another hypervisor, or consolidated.

Network is the avenue the virtual guest's systems and applications are accessed, so securely configuring the network interfaces is of utmost importance in the hardening process. The management interface of the hypervisor must be separate from all other networking and must be encrypted with SSH or TLS/SSL.

As virtualisation has gained a massive foothold of the digital services, the attacks and their counter measures are currently highly sophisticated and will keep evolving. Keeping the systems updated necessarily requires a high level of automation. This work concentrates on the hardening automation with standard tools and policies. In all virtualised environments some kernel operations necessarily remain shared, which leaves attack surface for the hostile party. Also because of the massive concentration of information and services, hypervisors are an attractive target for attacks. Virtualisation is not, however, a magick bullet in security. The entire solution stack needs to be secured. Sometimes this might be difficult because of complexity in system resources like memory that can be spread across and dependent on also other machines.

For example, one attack vector for KVM, involves taking advantage on how the modern microprocessor designs have implemented speculative execution of instructions (Red Hat, 2018). As a result of this, an unprivileged user could use the flaws to read privileged memory by conducting targeted cache side-channel attacks utilising hardware implementation weaknesses. These type of attacks include for example timing information, power consumption and electromagnetic leaks. Mitigating the guest-to-host escalation attack is not an important subject in this work, but none the less an important aspect to be taken care of when planning a production environment.

KVM and libvirt

The open source Kernel-based Virtual Machine (KVM) was chosen as the virtualisation hypervisor for this work. KVM is a Linux kernel module that changes the processor instruction execution states, called protection ring states, to a new set of states, thus dividing the virtual operating system as a separate operating environments. These ring states, or hierarchical protection domains, dictate the privilege level of the executed machine code. For example a software running on ring 3 cannot access the hardware directly, because this requires ring 1 privilege. In KVM a different set of ring states are created for each virtual machine so that they cannot access other virtual operating systems.

The kernel module **kvm.ko**, turns the Linux operating system into a Type 1 bare-metal hypervisor. KVM is a virtualization solution for Linux x86 architecture containing virtualization extensions for Intel VT and AMD-V. It consists of a loadable kernel modules that provide the full virtualization infrastructure. On KVM, multiple virtual guest machines can run Linux and Windows images with virtualized hardware such as a network cards, disks and graphics adapters. (Ivanov, 2017) (Chirammal;Mukhedkar;& Vettathu, 2016)

KVM is a fork of QEMU (Ritzau & Warnke, 2010) and uses QEMU emulation for some tasks with a division of work that provides the most efficient result. QEMU is a portable processor emulator that provides hardware emulation of any operating system on top of any QEMU supported architectures. There are multiple layers of security in the QEMU driver. Also SELinux protection with **svirt** for QEMU virtual machines protects the host operating system from compromised hosts.

The **libvirt** KVM/QEMU driver is a virtualization Application Programming Interface (API) to manage virtualization platforms like the QEMU emulator and KVM. Pure KVM or QEMU can be run from the command line, but **libvirt** can be used to program a Graphical User Interface (GUI) application for virtual machine management. Readily available in the CentOS libvirt installation, the **virt-manager**, using **libvirt**, is used for virtual machine management in this work.

On kernel hardening

KVM uses **libvirt** as the virtualisation Application Programming Interface (API) and **svirt** integrates to **libvirt** for providing a MAC framework (discussed in 2.2) for the virtual guests. A part of the USGCB kernel hardening is choosing the SELinux *Host policy* for the KVM host. This is done by setting the libvirt SELinux booleans. This was, however, not done in this work and the default SELinux booleans were used instead.

One of the points in kernel level hardening is mitigating the attacks that could allow malicious user to escalate from the *Guest* to the *Host*, or laterally, from a *Guest* to another *Guest* (Szefer;Keller;Lee;& Rexford, 2011). Expecially memory sharing can be an issue, even with the Address Space Layout Randomization (Jang;Lee;& Kim, 2016).

The IPV6 protocol and IP packet forwarding was chosen to be disabled in this work, as part of kernel level hardening, to decrease the attack surface.

Custom kernel could also be provided with stripped down set of kernel modules to further diminish the kernel attack surface (Anil & Robby, 2014). This procedure could strip down unwanted services that could be used in an attack (e.g. with a rootkit). This measure was not taken in this work, but instead the default kernel provided by the CentOS 7 Everything was used.

3.2 The studied operating systems and hardware

VMware Workstation was used for setting up the automated installation infrastructure and security testing and also to host the distribuiton server via bridged network connection.

Two hardware servers were utilized in the process, namely DELL PowerEdge R310 and PowerEdge R420xr. The first server failed to boot the automated Anaconda installation and was not tested any further. The server RAID for R420xr was configured with 2 1TB ssd disks as mirroring (RAID 0) for redundancy and initialized at the DELL RAID Configuration Utility.

CentOS Linux 7

Community ENTerprise Operating System (CentOS) Linux is a community maintained, stable open source operating system built with changes from the Red Hat Enterprise Linux Source Code (CentOS Project, 2018). While being a community project, CentOS Linux does not inherit Red Hat Enterprise Linux certifications or evaluations.

CentOS 7 was used as the operating system, in this work, for the virtualization host system and for the Instant Messenger guest server.

SELKS

The SELKS (Stamus Networks, 2018) operating system is designed specially for network security management and provides a prebuilt complete IDS/IPS ecosystem with it's own graphic manager. SELKS is an entirely open source, Debian based, system with **S**uricata IDS/IPS and network security monitoring engine (Suricata); **E**lasticsearch RESTful search engine (Elasticsearch); **L**ogstash (Elastic Logstash); **K**ibana analytics dashboard for Elasticsearch (Elastic Kibana); **S**cirius (Stamus Networks Scirius) and Evebox (Evebox, 2018).

3.3 OpenSCAP and XCCDF checklists

OpenSCAP is a security compliance tool that can check security configuration settings or examine signs of a compromise by comparing existing operating system settings to chosen security policies (OpenSCAP Team, 2018). OpenSCAP, and its Authenticated Configuration Scanne, has been validated by nist currently for the Red Hat Enterprise Linux 5.9 Desktop. These certifications do not, however, apply to CentOS whose products are build from the Red Hat source code as it is released (with only modifying trademarks).

The SCAP content is readily available via the **scap-security-guide** -package in the CentOS repository. The **scap-security-guide** (SSG) is an open-source project that creates security policies for various platforms and delivers these in standardised description XML format. The security policies contained in the SSG strictly implements the industry standardised requirements, for example the USGCB standard. In the context

of SSG the XCCDF format describes the used checklist, CCE's point to the identified security settings, and the OVAL file provides the XML content that describes the desired tests assessing the CCE configuration settings (NIST NVD, 2018).

OpenSCAP -tool, that can scan, validate, and edit standardized security content, is used in this work to implement the major part of the operating system hardening via a tailored XCCDF file basing on the USGCB security policy.

The **oscap** -tool, from the CentOS package **openscap-scanner**, can be run on the command line to perform the XCCDF checklist evaluation and system remediation based on the evaluation results. It can also evaluate OVAL CVE vulnerabilities and exploits, and to write both XML and HTML -format reports based on these evaluations. The system remediation enforces a security policy checklist on the running operating system and will try to fix the failed items with built-in scripts. This option is very useful also when installing a fresh system that needs to be compliant with a particular security policy (e.g. a USGCB compliant CentOS Linux 7 system).

As a Linux commandline program **oscap** returns always a definite exit status and is, therefore, well suited for versatile administration use and automated administration. In a production environment the **oscap-ssh** tool should be considered, for remote scans to avoid having the XCCDF policy files locally on the target machines.

Customizing and tailoring the XCCDF security policies

XCCDF is a specification language, developed by NIST, for security information interchange, document creation and situational tailoring and compliance testing that allow unified distribution of good security practices. The XCCDF documents are expressed in XML and must, therefore, conform to the XML Schema. An XCCDF document represents a structured collection of rules, referred as a checklist, that is designed for automated compliance testing and scoring.

By using the **OpenSCAP Workbench** -tool, new policy rule sets can be *customized* from the full SCAP content (e.g. a DS file from the SSG) by cherry picking the desired rules. The customized XCCDF -file contains only the changed options as a separate difference file to the original datastream. The original DS file is always fully referenced and, therefore, replacable. When a new SSG DS file is released by SCAP the customized difference file still applies to the updated datastream without any modification.

As the customized files, crafted for examle with the **Workbench** -tool, offer a flexible setup for choosing a security policy from a standardised security content the individual rules are impossible to be modified or entirely new rules to be created with this tool. As we are dealing with open-source software. It is also possible to download the source code of the **scap-security-guide** and to modify it, but this is not trivial if one doesn't fully understand the protocol inner workings. Modifying the SCAP content (e.g. the SSG DS **ssg-centos7-ds.xml**) to contain *tailored* rules that do not exist in the standardised specification is very challenging without a special tool designed for this purposeand is not considered in this work.

At the time of writing, there only exists one outdated tool meant for exactly this, namely the eSCAPe, Enhanced SCAP Editor (G2, 2018). This tool can be used to create or tailor OVAL files. This tool currently can also modify, but not create XCCDF files for the SCAP 1.3 content. It allows security analysts to create SCAP content without requiring in-depth knowledge of the underlying protocol and to maintain the XML Schema format. To note, the new rules are not best suited for operating system rule creation, because the OVAL procedures only include a few operations namely: environment variable, filehash check, family state, ldap or sql -type.

In this work the eSCAPe -tool was utilized for creating a new rule for **iptables** with the filehash SHA1 check. The SSG DS file for CentOS 7 does not have any rules for the **iptables** firewall (some rules for Red Hat 6 (rhel6) exists, via systemd but currently in rhel7 **iptables** is not operated via **systemctl**). The created rule compares the SHA1 hash of the original file **/etc/sysconfig/iptables**, copied to the system from the node.intra server at the installation time, to the one in the running system. This file should be kept immutable to be in accordance with the *Host security policy*. This check is performed daily by **cron** and a failure in the check indicates that the firewall is tampered with and the **iptables** file is replaced with the original one (note that the **cron** script is not available in the Appendices). If the server needs to be modified such that new ports need to be opened also the firewall hash needs to be modified in the **iptables-oval.xml** file. The **iptables** hash check rule file for **oscap** is attached in the Appendix 3. The referenced OVAL file contains the checksum of the correct *KVM host* iptables rules.

A rule for checking that the iptables module **ip_tables** is loaded and a script to load it in the case the check fails would also be needed, but is outside the scope of this work. Creating such rule was not possible with the eSCAPe tool and would require several

hand written rules and configuration scripts in accordance with XML Schema and XCCDF and OVAL specifications.

The eSCAPe User's Guide, provided by the eSCAPe package explains clearly how to first create a valid OVAL rule specification and then how to create the XCCDF file from this specification. Once the new rules are implemented, the new file should be validated with the SCAP Content Validation Tool or with eSCAPe that can only validate up to XCCDF version 5.10. Note, that while the outdated eSCAPe tool can perform valid XCCDF rule implementation, it cannot validate the current SCAP 1.3 content.

4 HARDENING AUTOMATION

The crafted *Host policy* was fully implemented in a kickstart install file, **kvmhost-ks.cfg**, that dictates the CentOS installer behavior and can utilize the **oscap** tool with the **--remediate** option for system configuration. This way the system will be in the desired state from the first boot on and very few system configuration procedures are needed after the installation. Remediation scripts can also be generated offline with **oscap xccdf generate fix** -command. Auto-remediation should, however, be used with care. For a large set of systems it is recommended to use a configuration management systems like Ansible or Puppet.

Installing the full configured system via Anaconda kickstart takes only a few minutes and is an ideal way to spawn Red Hat compatible virtual machines.

4.1 The automated Anaconda kickstart installation

CentOS implements the Anaconda installer (Red Hat, 2018) that is written in Python and C and supports a wide range of hardware platforms. The installer automatically detects all the resources of the system prior to installation and requires user input for installation options.

With Anaconda the installation can also be automated with a configuration text file, the kickstart file **ks.cfg**, that will provide the installation parameters to the installer. The automatic installation saves time and minimizes the administrator supervision. The kickstart file describes the installed system configuration. For example the chosen language, keymap, partitioning and the installed base system packages are given to the Anaconda installer as parameters.

In this work the kickstart file was fully constructed from an **Anaconda-ks.cfg** file provided by a fresh CentOS install to comply with the *Host policy* requirements.

The customized files were served for the Anaconda installer from the **node.intra** server in the same network and the automated kickstart installation was started from the CentOS installer's grub boot splash screen by hand. The used kickstart configuration for the *KVM host* is presented as **kvmhost-ks.cfg**, available in the Appendix 1.

4.2 Implementing the USGCB hardening via OpenSCAP

USGCB security baseline was chosen to be the basis of hardening. The CentOS 7 checklist was further modified according to the *Host policy*, partly described in the Section 2.2 and for which the implementation details are available in the Appendices 3 and 4.

With the chosen kickstart install parameters, a part of the USGCB based custom *Host policy* requirements can be already fulfilled. The rest of the policy implementation is done with the **oscap** tool.

The customized USGCB profile checklists **xccdf.xml**, that were run as post install procedures during the kickstart installations, were specially crafted to fulfil the chosen CentOS hardening requirements described as the *Host policy* and *Guest policies* in this work. The *Host policy* checklist file is presented for reference in the Appendix 2 and can be most conveniently viewed with the **OpenSCAP Workbench** program. Note, that viewing the content also requires the datastream file (e.g. **ssg-centos7-ds.xml** provided by the **scap-security-guide** package) to provide the full SCAP content.

The checklist was based on the full 357 item USGCB policy and was produced with the **Workbench** -tool prior to the installation. 151 items from the USGCB checklist were chosen to form the *Host security policy.*

The *Host policy* checklist, **kvmhost-xccdf.xml**, is implemented as part of the *KVM host* kickstart installation with remediation scripts of the oscap commandline tool. The test and remediation results are saved as a HTML file to the **/root** directory of the newly created machine.

5 THE INSTALLATION PHASE

For the work two DELL PowerEdge hardware servers were used as the hypervisor hardware. CentOS Linux 7 was chosen as the operating system for the KVM virtualisation host. Several iterations of virtual machines on VMware Workstation was needed to obtain the wanted state of the virtual *KVM Host* and *Guests* that were installed on the DELL PowerEdge R420xr server hardware. As a result of the automated installation a hardened CentOS Linux 7 *KVM Host* with 2 *Guest* virtual servers were produced. As virtual guests to the KVM virtual host an CentOS based Instant Messenger server and an SELKS IDS/IPS server were set up. Some system services needed to be configured after the installation was finished because of failures in the kickstart installation or in **oscap --remediation**.

First a distribution and repository server, **node.intra**, needed to be set up to provide the resources for the constructed environment. The network topology is shown in the Figure 1.

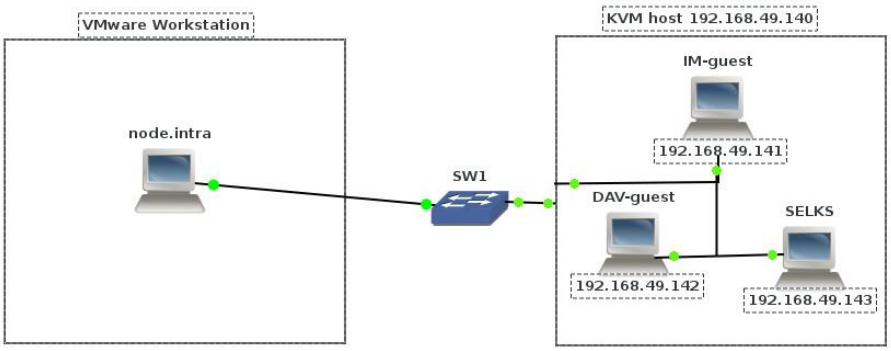


Figure 1. The network topology

5.1 Setting up the **node.intra** distribution server

A distribution server was set up in the VMware Workstation as a CentOS 7 minimal install web server with bridged interface and an **IP 192.168.49.200**.

For the automation a **node.intra** server containing a NTP server and an Apache web server with a CentOS mirror and the customised files first needed to be set up. The required files include the **kickstart-ks.cfg**, the oscap USGCB security policy in files **ssg-centos7-ds.xcml** and **kvmhost-xccdf.xml**, the **iptables** firewall policy and the testing scripts , and the cron script **oscap-recurrent.sh** for monitoring the systems' state. The server contained also the full vanilla CentOS Linux 7 Everything ISO content as a repository proxy and the SELKS iso image.

The served, and **apache** owned, files should have only read permissions at the HTTP-server. Furthermore, in a production environment, HTTPS protocol should only be used.

A Network Time Protocol (NTP) server is needed in a secured network for example for log synchronisation. In this environment the **node.intra** server also acts as the NTP server although in a production environment, it should be a separate server that also encrypts the NTP traffic with PKI.

No logging server was actually implemented for this environment although it is referred to later in this work.

```
# chown root:apache /var/www/html/kickstart-ks.cfg
# chmod 640 /var/www/html/kickstart-ks.cfg
```

The CentOS 7 mirror was produced by copying the mounted iso image fully to a folder in the webroot and metadata for the repository was produced by the **createrepo** -command.

```
# createrepo /var/www/html/Centos/7
```

For the NTP server, the **node.intra** needs to be in contact with some NTP pool server in the internet before installing any of the test systems.

```
# systemctl enable ntpd.service
# ntpdate node.intra

# echo '30 * * * * root /usr/sbin/ntpd -q -u ntp:ntp' >
/etc/cron.d/ntpd
```

The default CentOS installation includes a firewall service **firewalld**, that can be modified to enable traffic to and from the Apache web server and NTP server:

```
# firewall-cmd --zone=public --add-service=http --permanent
```

```
# firewall-cmd --zone=public --add-service=ntp --permanent
```

Lastly the web server and the **ntpd** needed to be started with

```
# service httpd start
# service ntpd start
```

5.2 Installing the *KVM host* with kickstart

The kickstart installation was tested before the deployment to the hardware in VMware Workstation to make sure the modified install parameters and scripts were functional. The partitioning, encryption, initial passwords, networking, needed software packages and post installation procedures were checked in particular to produce the wanted result.

KVM was successfully installed on the DELL PowerEdge R420xr server hardware with the kickstart file served from **node.intra** by running the Anaconda installer from a USB via BIOS (UEFI option not booting from the local network did not work). With older hardware, namely PowerEdge R310, where only the UEFI installer was detected, a critical bug (Red Hat, 2018) (Red Hat, 2018) in the UEFI installer's dracut initramfs -tool prohibited the automated kickstart installation.

The kickstart configuration forced, for example, the following constraints on passwords, partitioning and packages. A strict password policy was chosen to require at least 15 characters, to have at least one digit, one upper case, one lowercase and one special character, not to have more than two consecutive repeating characters and to choose characters from at least three character categories. Also the password should be changed every 30 days.

The partitioning required separate partitions to **root, /boot, /swap, /tmp, /var/log, /var/log/audit** and **/var/lib/libvirt** as in Section 2.2 and also disk encryption. A secure password policy would require for the CentOS Linux 7 **escrowcert** usage for the partition encryption key, in a production environment. For this test system, however, passwords were given in plain text in the kickstart file. Also note that HTTP rather than HTTPS was used in the **node.intra** communication in this work. For a production environment install, Registration Authority server would need to be set up for TLS/SSL and **escrowcert**.

For minimising the attack surface in the *KVM host* a minimal install with graphical interface was the preferred choice, so the following package groups (in quotes) and packages were chosen to achieve this: **``Minimal'', ``Core'' ``X Window System''** and the software packages: **gnome-classic-session, gnome-terminal, control-center** and **liberation-mono-fonts**. Also the virtualisation environment was installed with: **``Virtualization Client'', ``Virtualization Tools'', ``Virtualization Platform''**. The OpenSCAP is installed with **openscap-scanner** and **scap-security-guide**. Other software that was required included **git, wget** and **ntp**. The full list of the installed packages can be seen in the **kvmhost-ks.cfg** file. The *Host policy* also enforces requirements for some services and removes or forces installation of some packages.

The CentOS default firewall **firewalld** will be disabled in these systems and instead a custom **iptables** rule set is run on the systems. In the iptables rules only the ports required by the services, for the particular *Guest* server, are allowed to be open.

The iptables rules were successfully forced into action, but only after all the *Guest* systems had been installed so that the installation can proceed till the end normally. The KVM host iptables drops all traffic but the out going UDP logging messages in the management interface after deployment. The *KVM host* will be operated in this set up only via console connection.

The automated installation with oscap remediation, run as a post install script in the kickstart file, takes about five minutes in total with 6 cores and 4096 MB of RAM. The procedure does not need any other intervening from the administrator than describing the installation source for the installer boot manager. The kickstart file is given as a boot command, by pressing **ESC** at the CentOS installer splash screen and then typing the command to the **boot>** prompt.

```
  boot> linux ks=http://192.168.49.200/kvmhost-ks.cfg
ip=192.168.49.140 netmask=255.255.255.0 gateway=192.168.49.200
```

The newly created *KVM host* is forced to obtain the **IP 192.168.49.140** to be able to connect to **node.intra**.

Logging should be performed via the *KVM Host* management network interface in this setup by using a remote logging server at **node.intra**. For secure log message transfer TLS certificates should be used. Instead in this work, the log messages are sent as UDP packets and outgoing connection for this on the management interface **ens33** (**ens33**

was the default interfacename produced in the kickstart installation, and is defined to be the management interface) is opened in the firewall, included in the Appendix 5.

5.3 Installing the *KVM guests*

Three *Guest systems* were installed on the *KVM Virtualization Host*. A CentOS 7 Instant Messenger server that contains **openfire** instant messenger and a version management server with **webdav** and **apache**. The third system was a Debian based SELKS IDS/IPS server, for which the automated installation was not an option.

The headless *Instant Messenger guest* server install was performed as a kickstart installation with **oscap --remediation** as in the *KVM host* installation. The kickstart file **IM-ks.cfg** was modified along the needs of the KVM guest server with **sshd, mailx, iptables** and **openfire** with its dependencies. Also, the XCCDF **IM-xccdf.xml** file was customized for the **openssh-server**, SMTPS and **openfire** rules (the SMTPS port 25 needs to be opened for sending the auditing reports via **mailx**).

Also a kickstart file, XCCDF content and firewall rules were created for a headless *WebDAV server Guest* for version management. The XCCDF and firewall rules only differ from the *IM Guest* with the installed services and opened ports.

The SELKS IDS/IPS virtual machine was installed with the **virt-manager** GUI by starting the debian installer directly from an ISO file. In the debian installer the encrypted LVM partitioning scheme was chosen with separate **/home, /var** and **/tmp** partitions. The fresh SELKS installation had no firewall rules implemented and the default passwords needed to be changed. Security auditing script that utilizes **oscap** in the *Guest* servers is presented in the Section 6.3.

6 OPENSCAP TESTS AND THE HARDENING RESULTS

All the systems were checked after the installation and needed some post installation configuration. Also, the **oscap** test was run again to see any difference in the reports provided by the kickstart installation. The test results are presented in this chapter. The iptables rules that were made and validated with **eSCAPe** could also be successfully implemented and run after the firewall was in place.

After the first boot, the installation oscap report, **oscap_usgcb_install_report.html**, was readily available showing as overall pass score 91.46% with only 3 failed items for the *KVM host*. The virtual *Guests* performed similarily, because the added services did not raise failures nor errors (the base system for all minimal CentOS installs was the same and the XCCDF checklists very similar).

The CentOS Linux 7 minimal installation with only the ``**Core''** system packages arrives at a good security state with the chosen automatic hardening. Here the automatic installaton already includes the chosen USGCB based security policy implemented by the kickstart file **kvmhost-ks.cfg** and the customized security policy **kvmhost-xccdf.xml**.

6.1 Test summary and analysis of the hardened systems

The remediation report produced by the kickstart installation reveal a few rules that have failed or produced errors. With the kickstart file, the **oscap --remediate**, run at the **%post** phase, produced a report of the checked rules with the result: 135 passed, 3 failed, 10 errors and 3 notchecked. The overall score according to **urn:xccdf:scoring:default** - scoring system amounts to 91.46%.

Some errors disappeared when running the oscap --remediate again right after the first boot producing the **oscap_usgcb_remediation_report.html** report that will be analysed here. This report scores higher, with a result 95.42%, and the error producing items and severities are listed in the Tables 1 and 2.

Table 1 Reported remediation errors

141	passed
3	failed
4	error
3	notchecked

Table 2 Severity of the failed rules

#	SEVERITY	RULES
2	medium	IPV6 loading, audit rule
1	high	bootloader password

Table 3 Reasons why the rules failed

ITEM	**FAILING REASONS** (if applicable)
notchecked:	
Yum updates could not be produced	The local repository is not configured
Disable Bluetooth and WiFi in BIOS	"No candidate or applicable check found"
Disable IPV6	"No candidate or applicable check found"
errors:	
/etc/pam.d/system-auth contains retry=5	Was fixed, but showed an error
PAM faillock deny root	Was fixed, but showed an error
NTP enable	"no rpm GPG key installed"
Specify NTP server	failed to verify the local server
fails:	
GRUB2 bootloader password not set up correctly	Cannot fix automatically
IPV& automatic loading	
audit rule usergroup_modification_password	

The Table 3 shows the reason of failure for the analysed rules. Three of the rules were not checked bacause the available remediation scripts did not apply to CentOS 7. The produced info states: No candidate or applicable check found. This happened for Yum updates, disabling Bluetooth and WiFi in the BIOS and when Disabling IPV6 via **/etc/sysconfig/network**.

The produced errors were tried to be remediated by the **oscap** tool but some checks failed. The STDERR messages claim missing remote resources, which seems unreasonable. These errors were related to the PAM password policies, namely: *Set Password retry Prompts Permitted per-Session and Configure the root Account for Failed Password Attempts*. The NTP errors were due to not having valid GPG keys in place for the CentOS package manager **yum**.

The bootloader password needed to be configured manually, as guided by the report: ``To prevent hard-coded passwords, automatic remediation of this control is not available.'' Furthermore, disabling IPV6 and one audit rule, **audit_rules_usergroup_modification_passwd** failed with no reported reason.

These errors and failures occurred for the *KVM Host* and the virtual *Guests* and all the failures did not vanish with consecutive runs of **oscap**. This might indicate that the installed version of **scap-security-guide** had some bugs. The error hunting was not pursued from here on because of the test nature of this environment. The few issues were manually configured and fully compliant systems were produced.

The SELKS operating system has been pre-hardened to operate as a network sniffer only so the installation ISO file should produce a safe system after the basic configuring tasks discussed in the next section. No SCAP content testing could be performed on this system because the OpenSCAP tool is broken for the Debian distribution version 8 at the time of writing. It is stated in the project web pages: ``By now, a Debian host can't check its own policy compliance because Debian CPE are defined for oldstable and older, and the scap-security-guide packages only exists in unstable and testing. Here, we use a policy server based on unstable. Support for new stable (9.0) is not yet merged in upstream'' (Debian, 2018). Also the datastream file **ssg-debian8-ds.xml** compiled from the **scap-security-guide** found in github failed to load in the **OpenSCAP Workbench**.

6.2 Post installation procedures

There were some correcting procedures and system configuration to take care of after the automated install to acquire the policy compliant state.

The CentOS package manager needs to be set up to use the **node.intra** repository if needed. The **yum** package manager is not functional and packages via **yum** cannot be

installed if either an internet connection is established or the local repository is set up in the installed machine.

The failed configurations, revealed by the **oscap** report that was studied in Section 6.1, were fixed manually according to the available information in the report and in the SCAP content. The SCAP USGCB content could be viewed with the **Workbench** tool.

According to the *KVM Host policy* two interfaces, one for the host management and the other for the guest external traffic, were required. Only one network interface **ens33** could, however, be produced with the kickstart script in these tests. The other external network interface **ens34** needed, therefore, to be set up by hand after the installation had finished.

The iptables rules were also set up by hand in order not to intervene with the automatic installation or post installation. The iptables tailored rule was run successfully after the iptables firewall implementation with the **oscap** tool from the command line.

The SELKS system user credentials need to be hardened and firewall implemented after the installation.

6.3 On second tier security practices

As a second tier security practice, it is convenient to regularly scan the system. The systems can be regularly audited with the security policy by running **oscap xccdf eval --remediate** via the cron service. In this work a maintenance script, to automatically monitor the state of the *Guest servers* with **oscap**, was produced.

A script, **oscap-recurrent.sh**, was copied to the *Guest* systems in the kickstart installation for cron execution to maintain the system in the preferred state. The script is available as the Appendix 6 and is not referred to in the presented *KVM host* configuration files. The script sends out a report in case of a failure via mail, therefore a mail server would also be required in the virtual environment. Opening a mail service in the *KVM host* itself was not desirable and, therefore, scanning the host is desirable to be performed via SSH protocol e.g. with the **oscap-ssh** tool.

The script was provided to the **cron** service in the kickstart installation to maintain the chosen security policy. The **/etc/crontab** rule reads:

```
30 3 * * * root /root/oscap-recurrent.sh
```

For the monitoring a virtual mail server should also be set up to connect outside the *KVM host* for reporting. Currently in the script **root@node.intra** is set as the report reciever. The sent fail-report can be read from the received email file with the **munpack** program.

Systems with SCAP content checking can also be remotely scanned with **oscap-ssh** or with a systems management tool **Spacewalk** (Red Hat, 2018), that can also perform scheduled scans.

7 DISCUSSION AND CONCLUSIONS

In this work it was shown that a sufficiently secure Linux operating system can be obtained with automated installation scripts and open source auditing tools. An automatically hardened CentOS operating system configuration was built successfully. The main tools to obtain the secure environment were the Anaconda kickstart installer with CentOS Linux 7 and the OpenSCAP auditing tool. USGCB SCAP content via XCCDF checklists was used in this work for the hardening benchmark and a completely new rule to the XCCDF content was successfully created with eSCAPe and tested with the OpenSCAP.

Operating system hardening is not studied a lot because it already belongs to the realm of well known administration tasks. The study in this work is still interesting, because there does not exist many publications on hardening procedures and none that describes a deployment of a USGCB hardened environment with the configuration commands and configuration files included. All the information currently lies in separate sources and the referenced example files are not often very detailed. This text can be used as a reference for setting up a full hardened virtualization environment that complies to a particular security policy.

The fully automated secure operating system implementation was the main goal of this study, however, a few configuration tasks were left to be performed manually after the first boot. The OpenSCAP auditing tool was used for implementing the security policy by large. The tool was also used measure the applicability of the configuration for hardened virtual environment building. Some rules in the OpenSCAP tests failed and these also needed to be fixed by hand. Of special interest was also the question of tailoring new XCCDF rules by fully creating a new individual security checklist item from scratch. This could be performed with the eSCAPe tool that was not maintained at the time of writing, but nonetheless could produce an implementable new rule. Using eSCAPe has it's limitations also in the rule creation, but was well suited for the studied setting.

The studied test system environment consists of a Type 1 Kernel-based Virtual Machine, KVM, hypervisor and 3 virtual guest systems. Additionally in the test network there is a separate HTTP server that servers the installation files and the CentOS repository. All services are configured through non-encrypted channels in this work for convenience. All services should in production environments be configured to use TLS for all inter service communication.

A minimal CentOS Linux 7 installation was chosen for the *KVM host* system. In the virtual environment three *virtual guest machines*, two headless Centos linux 7 servers and a Debian OS based SELKS IDS/IPS server, were installed and tested. Unfortunately, the SSG for Debian was not available through the repositories and compiling it from the source code produced a datastream file that was not recognised by the **Workbench** -tool. Therefore, the SELKS installation failed to be confronted with the chosen security policy.

The newly installed CentOS system, using the policy compliant kickstart installation with OpenSCAP, obtained a rather high security score after the first boot already. According to the **urn:xccdf:scoring:default** scoring system built within the oscap -tool, the score was already 95.82\% after the first test on the fresh system and before any manual configuration. Also the produced errors were partly due to the lack of internet connection or missing repository configuration, so the result can be considered to be very good. This result gives also a very good impression of the usability of the secured Anaconda kickstart installation on CentOS 7 with OpenSCAP.

The test system configuration can be modified to implement a relatively small secured environment with all the relevant changes in each configuration file. Also, the security policy needs to be profiled for each use case. For further development, this environment requires also kernel hardening, full network configuration and configuration for all the needed services, like a logging server.

.

REFERENCES

Anil, K.;& Robby, Z. (2014). A tale of two kernels: Towards ending kernel hardening wars with split kernel. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (ss. 1366-1377). ACM.

CentOS Project. (15. January 2018). *The CentOS Project*. Retrieved from https://www.centos.org/

Chen, H. (2009). *Analysis of access control policies in operating systems.* Indiana: Purdue University, West Lafayette.

Chirammal, H. D.;Mukhedkar, P.;& Vettathu, A. (2016). *Mastering KVM Virtualization.* Packt Publisihing.

CIS Benchmark. (5. May 2018). *Report CIS CentOS Linux 7 Benchmark v.2.2.0 12-27-2017.* Retrieved from https://www.newnettechnologies.com/cis-benchmark.html

Debian. (9. May 2018). *Using SCAP tools for Security check and remediation*. Retrieved from https://wiki.debian.org/UsingSCAP

Elastic Kibana. (5. May 2018). *Your Window into*. Retrieved from https://www.elastic.co/products/kibana

Elastic Logstash. (5. May 2018). *Centralize, Transform & Stash Your Data*. Retrieved from https://www.elastic.co/products/logstash

Elasticsearch. (5. May 2018). *The Heart of the Elastic Stack*. Retrieved from https://www.elastic.co/products/elasticsearch

Evebox. (5. May 2018). *Evebox The Inbox for your Suricata Events*. Retrieved from https://evebox.org/

G2. (28. April 2018). *eSCAPe Content Editor*. Retrieved from https://www.g2-inc.com/escape-content-editor

IASE STIGs. (1. May 2018). *Security Technical Implementation Guides (STIGs)*. Retrieved from https://iase.disa.mil/stigs/Pages/index.aspx

Ivanov, K. (2017). *KVM Virtualization Cookbook: Learn how to use KVM effectively in production.* Birmingham: Packt Publishing Limited.

Jang, Y.;Lee, S.;& Kim, T. (2016). Breaking Kernel Address Space Layout Randomization with Intel TSX. *Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS).* Vienna, Austria.

Mann, S.;& Mitchell, E. (2001). Linux System Security: An Administrator's Guide to Open Source Security Tools. *The EDP Audit, Control, and Security Newsletter,Volume 28, Issue 8*, 1-3.

MITRE Corporation. (5. May 2018). *Common Vulnerabilities and Exposures*. Retrieved from https://cve.mitre.org/

NIST. (1. May 2018). *Security Content Automation Protocol Validation Program*. Retrieved from https://scap.nist.gov/validation/.

NIST NVD. (9. May 2018). *Common Configuration Enumeration (CCE) Details*. Retrieved from https://nvd.nist.gov/config/cce/index

NIST Special Publication. (April 2013). *NIST Special Publication 800-53, Revision 4.* Retrieved from http://dx.doi.org/10.6028/NIST.SP.800-

NIST Special Publication. (23. April 2018). *National Institute of Standards and Technology Special Publication 800-70 (February 2018) Revision 4, 52 pages; CODEN: NSPUE2.* Retrieved from https://doi.org/10.6028/NIST.SP.800

NIST USGCB. (1. May 2018). *United States Government Configuration Baseline*. Retrieved from https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline

Niu, S.;Mo, J.;Zhang, Z.;& Lv, Z. (2014). Overview of Linux Vulnerabilities. *Conference: 2nd International Conference on Soft Computing in Information.*

OpenSCAP Team. (1. May 2018). *OpenSCAP*. Retrieved from https://www.open-scap.org/.

Red Hat. (28. April 2018). *Introduction to Anaconda*. Retrieved from http://anaconda-installer.readthedocs.io/en/latest/intro.html

Red Hat. (28. April 2018). *Kernel Side-Channel Attacks - CVE-2017-5754 CVE-2017-5753 CVE-2017-5715*. Retrieved from https://access.redhat.com/security/vulnerabilities/speculativeexecution

Red Hat. (9. May 2018). *RHEL 7 prints "dracut-initqueue timeout - starting timeout scripts" messages in loop while booting*. Retrieved from https://access.redhat.com/solutions/2515741

Red Hat. (5. May 2018). *Spacewalk Free & Open Source Systems Management.* Retrieved from https://spacewalkproject.github.io/

Red Hat. (9. May 2018). *Why does system shows dracut warning dracut-initqueue timeout starting timeout scripts even during successful boot?* Retrieved from https://access.redhat.com/solutions/3047351

Red Hat Manual. (28. April 2018). *Installing Red Hat Enterprise Linux 7.5 on all architectures, Chapter 26. Kickstart Installations*. Retrieved from https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/installation_guide/chap-kickstart-installations.

Redwood, W. O. (2015). *Cyber Physical System Vulnerability.* Tallahassee, Florida: Florida State University.

Ritzau, T.;& Warnke, R. (2010). *qemu-kvm & libvirt, 4th edition; ISBN 978-3-8370-0876-0 .* Norderstedt: Books on Demand GmbH.

Simons, W. R. (2005). *The challenges of network security remediation at a regional university.* Tennessee: East Tennessee State University, ProQuest Dissertations Publishing.

Stamus Networks. (20. January 2018). *Stamus and Open Source*. Retrieved from https://www.stamus-networks.com/open-source/

Stamus Networks Scirius. (5. May 2018). *StamusNetworks/scirius*. Retrieved from https://github.com/StamusNetworks/scirius

Sumit, D. (2006). Securing and Hardening Red Hat Linux. *Information Systems Security, Issue 1*.

Suricata. (5. May 2018). *Suricata Open Source IDS / IPS / NSM engine*. Retrieved from https://suricata-ids.org/

Szefer, J.;Keller, E.;Lee, R. B.;& Rexford, J. (2011). Eliminating the Hypervisor Attack Surface. *CCS '11 Proceedings of the 18th ACM conference on Computer and communications security* (ss. 401-412). Chicago: ACM, NY, USA.

Waltermire, D.;Quinn, S.;Booth, H.;Scarfone, K.;& Prisaca, D. (February 2018). *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3; SP 800-126 Rev.3; Organizations: NIST, Scarfone Cybersecurity, G2.* Retrieved from https://csrc.nist.gov/publications/detail/sp/800-126/rev-3/final.

Wang, Z. (2012). *Securing Virtualization: Techniques and Applications.* Raleigh, North Carolina: North Carolina State University.

Wright, C.;Cowan, C.;Smalley, S.;Morris, J.;& Kroah-Hartman, G. (2002). Linux security modules: general security support for the linux kernel. *Proceedings of the 11th USENIX Security Symposium.* San Francisco: The USENIX Association.

A1 The KVM kickstart file

Kickstart install configuration file kvmhost-ks.cfg.

```
####
#MIT License
#
#Copyright (c) 2018 Kaisa Henttunen
#
#Permission is hereby granted, free of charge, to any person obtaining
#a copy of this software and associated documentation files (the
#"Software"), to deal in the Software without restriction, including
#without limitation the rights to use, copy, modify, merge, publish,
#distribute, sublicense, and/or sell copies of the Software, and to
#permit persons to whom the Software is furnished to do so, subject to
#the following conditions:
#
#The above copyright notice and this permission notice shall be
#included in all copies or substantial portions of the Software.
#
#THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
#EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
#MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
#NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS
#BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN
#ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN
#CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
#SOFTWARE.
####
#
#version=DEVEL
# System authorization information
auth --enableshadow --passalgo=sha512
# Use CDROM installation media
install
#cdrom
url --url="http://192.168.49.200/isoC7/"
# Not graphical install
text
# Run the Setup Agent on first boot
firstboot --enable
ignoredisk --only-use=sda
# Keyboard layouts
keyboard --vckeymap=fi --xlayouts='fi'
# System language
lang en_US.UTF-8

# Network information
#mgmt int:
network  --bootproto=static --ip=192.168.49.140 --
netmask=255.255.255.0 gateway=192.168.49.200 --noipv6
#guest int:
#network  --bootproto=dhcp --device=ens34 --noipv6
network  --hostname=hostess.localdomain
```

```
selinux --enforcing
# Root password
rootpw --lock
# System services at KVM host
services --disabled="chronyd,sshd,dhcpd,cupsd,firewalld"
services --enabled="auditd"
# System timezone
timezone Europe/Helsinki --isUtc --nontp
user --groups=wheel --name=admin --
password=$6$VBP379Q3$0CgyV7DSslllZ/IyV2vre5aX46nU.msa/wGPXFknf9.cTb
1ESCiLU50ErRggA4B29NZed2OWUCwuSvjjzfZA7. --iscrypted --
gecos="admin"

# System bootloader configuration
zerombr
bootloader --append=" crashkernel=auto" --location=mbr --boot-
drive=sda
bootloader --iscrypted --
password=grub.pbkdf2.sha512.10000.C68F6E4D2135869C48B7413662791E2BC
41AAB9BE3A82C59F541E3BE4F9E372A710B57363798C85CCFCB03AF67B623748E3A
CA220719E1B973F147BC2A336169.0EDC267DEFF0E18DC12F11870C7D66AB3EA766
3C9EB2DBA4E7E8427DDF3EA58922C2C7C96FC0F036B7AF0B52ED0828EAE021EF260
C782D46A5B555065B24FA34
# Partition clearing information
#clearpart --all --initlabel --drives=sda
clearpart --none --initlabel
part /boot --asprimary --ondisk=sda --fstype=ext4 --size=200
part pv.01 --asprimary --ondisk=sda --size=25000
volgroup vg_sys pv.01
# in production environment CHANGE ALL encryption passwords to --
escrowcert certificates like:
# logvol swap --name=lv_swap --vgname=vg_sys --size=1024 --
encrypted --escrowcert=RAserver.localdomain
logvol swap --name=lv_swap --vgname=vg_sys --size=1024 --encrypted
--passphrase=swapPASS1234567
logvol /tmp --fstype=ext4 --name=lv_tmp --vgname=vg_sys --size=512
--fsoptions="nodev,noexec,nosuid"
logvol /var/log --fstype=ext4 --name=lv_varlog --vgname=vg_sys --
size=5000 --fsoptions="nodev,noexec,nosuid"
logvol /var/log/audit --fstype=ext4 --name=lv_auditlog --
vgname=vg_sys --size=5000 --fsoptions="nodev,noexec,nosuid" --
encrypted --passphrase=auditlogPW12345
logvol / --fstype=ext4 --name=lv_root --vgname=vg_sys --size=10000
--encrypted --passphrase=rootPASS1234567
part pv.02 --asprimary --ondisk=sda --grow
volgroup vg_guests pv.02
logvol /var/lib/libvirt --fstype=ext4 --name=lv_guests --
vgname=vg_guests --size=30000 --grow

repo --name="CentOS 7" --
baseurl="http://192.168.49.200/isoC7/Packages"
%packages
@^minimal
@core
@virtualization-hypervisor
@virtualization-client
```

```
@virtualization-platform
@virtualization-tools
@hardware-monitoring
@x11
gnome-classic-session
gnome-terminal
control-center
liberation-mono-fonts
# gpgcheck disabled because local repository at node.intra is used
in this work
#gpgcheck
git
wget
ntp
screen
openscap
openscap-scanner
scap-security-guide
aide
# tripwire is in EPEL repository
#tripwire
rsyslog
# syslog-ng is in EPEL repository
#syslog-ng
#-rsyslog
-xinetd
-telnet-server
-telnet
-rsh-server
-rsh
-rexec
-tftp-server
-openssh-server
-cupsd
-dhcpd
-postfix
-sendmail
-dovecot
-openldap-server
-nfs-utils
-bind
-vsftpd
-httpd
-quagga
-samba
-squid
-net-snmp
-firewalld

%end

%addon com_redhat_kdump --enable --reserve-mb='auto'

%end

#%Anaconda
```

```
#pwpolicy root --minlen=15 --minquality=50 --strict --nochanges --
notempty
#pwpolicy user --minlen=15 --minquality=50 --strict --nochanges --
notempty
## pwpolicy luks --minlen=6 --minquality=1 --notstrict --nochanges
--notempty
#%end

%post --log /root/oscap.log
echo "192.168.49.200 node.intra node" >> /etc/hosts
systemctl enable ntpd.service
ntpdate node.intra
echo "server node.intra" >> /etc/ntp.conf
echo '30 * * * * root /usr/sbin/ntpd -q -u ntp:ntp' >
/etc/cron.d/ntpd

cd /root
#wget http://node.intra/iptabX/kvmfirewall
#chmod 700 kvmfirewall
## The  downloaded firewall is run only after the installetion has
been verified, because it will cut all traffic

wget -x http://node.intra/xccdf/ssg-centos7-ds.xml
wget -x http://node.intra/xccdf/kvmhost-xccdf.xml
oscap xccdf eval --remediate --profile
xccdf_ointra.node_profile_ospp-rhel7_kvmhost --report
/root/oscap_usgcb_install_report.html
/root/node.intra/xccdf/kvmhost-xccdf.xml
%end
```

A2 Customized XCCDF rules

A customized ruleset, the *Host policy*(kvmhost-xccdf.xml), from the USGCB datastream.

```
<?xml version="1.0" encoding="UTF-8"?>
<xccdf:Tailoring xmlns:xccdf="http://checklists.nist.gov/xccdf/1.2"
id="xccdf_scap-workbench_tailoring_default">
  <xccdf:benchmark href="/usr/share/xml/scap/ssg/content/ssg-
centos7-ds.xml"/>
  <xccdf:version time="2018-02-06T15:02:51">1</xccdf:version>
  <xccdf:Profile id="xccdf_ointra.node_profile_ospp-rhel7_kvmhost">
    <xccdf:title xmlns:xhtml="http://www.w3.org/1999/xhtml"
xml:lang="en-US" override="true">United States Government
Configuration Baseline (USGCB / STIG) - DRAFT
[CUSTOMIZED]</xccdf:title>
    <xccdf:description xmlns:xhtml="http://www.w3.org/1999/xhtml"
xml:lang="en-US" override="true">This profile is developed in
partnership with the
U.S. National Institute of Standards and Technology (NIST), U.S.
Department of
Defense, the National Security Agency, and Red Hat. The USGCB is
intended
to be the core set of security related configuration settings by
which all
federal agencies should comply.

This baseline implements configuration requirements from the
following documents:

- Committee on National Securiy Systems Instruction No. 1253 (CNSSI
1253)
- NIST Controlled Unclassified Information (NIST 800-171)
- NIST 800-53 control selections for MODERATE impact systems (NIST
800-53)
- U.S. Government Configuration Baseline (USGCB)
- NIAP Protection Profile for General Purpose Operating Systems
v4.0 (OSPP v4.0)
- DISA Operating System Security Requirements Guide (OS SRG)

For any differing configuration requirements, e.g. password
lengths, the stricter
security setting was chosen. Security Requirement Traceability
Guides (RTMs) and
sample System Security Configuration Guides are provided via the
scap-security-guide-docs package.

This profile reflects U.S. Government consensus content and is
developed through
the OpenSCAP/SCAP Security Guide initiative, championed by the
National
Security Agency. Except for differences in formatting to
accommodate
```

```
publishing processes, this profile mirrors OpenSCAP/SCAP Security
Guide
content as minor divergences, such as bugfixes, work through
the consensus process.
</xccdf:description>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_remediation_functions"
selected="false"/>
    <xccdf:select idref="xccdf_org.ssgproject.content_group_intro"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_general-principles"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_principle-encrypt-
transmitted-data" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_principle-minimize-
software" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_principle-separate-
servers" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_principle-use-security-
tools" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_principle-least-
privilege" selected="false"/>
    <xccdf:select idref="xccdf_org.ssgproject.content_group_how-to-
use" selected="false"/>
    <xccdf:select idref="xccdf_org.ssgproject.content_group_intro-
read-sections-completely" selected="false"/>
    <xccdf:select idref="xccdf_org.ssgproject.content_group_intro-
test-non-production" selected="false"/>
    <xccdf:select idref="xccdf_org.ssgproject.content_group_intro-
root-shell-assumed" selected="false"/>
    <xccdf:select idref="xccdf_org.ssgproject.content_group_intro-
formatting-conventions" selected="false"/>
    <xccdf:select idref="xccdf_org.ssgproject.content_group_intro-
reboot-required" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_mcafee_security_software"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_mcafee_hbss_software"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_permissions_within_import
ant_dirs" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_daemon_umask"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_root_paths"
selected="false"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_network_ipv6_limit_reques
ts" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_network_ssl"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_log_rotation"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_configure_logwatch_on_log
server" selected="false"/>
    <xccdf:select idref="xccdf_org.ssgproject.content_group_docker"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_sshd_strengthen_firewall"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_xwindows"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_disabling_xwindows"
selected="false"/>
    <xccdf:select idref="xccdf_org.ssgproject.content_group_avahi"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_disable_avahi_group"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_avahi_configuration"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_configure_printing"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_disabling_dhcp_server"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_dhcp_server_configuration
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_dhcp_server_minimize_serv
ed_info" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_disabling_dhcp_client"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_dhcp_client_configuration
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_dhcp_client_restrict_opti
ons" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_postfix_client"
selected="false"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_postfix_harden_os"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_postfix_configure_ssl_cer
ts" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_postfix_install_ssl_cert"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_postfix_server_configurat
ion" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_postfix_server_denial_of_
service" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_postfix_server_mail_relay
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_postfix_server_mail_relay
_set_trusted_networks" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_postfix_server_mail_smtpd
_relay_restrictions" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_postfix_server_mail_smtpd
_recipient_restrictions" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_postfix_server_mail_relay
_smtp_auth_for_untrusted_networks" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_postfix_server_mail_relay
_require_tls_for_smtp_auth" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_ldap_server_config_certif
icate_files" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_nfs_configuring_all_machi
nes" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_nfs_client_or_server_not_
both" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_nfs_configure_fixed_ports
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_configure_exports_restric
tively" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_use_acl_enforce_auth_rest
rictions" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_export_filesystems_read_o
nly" selected="false"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_dns_server_isolation"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_dns_server_dedicated"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_dns_server_chroot"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_dns_server_protection"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_dns_server_separate_inter
nal_external" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_dns_server_partition_with
_views" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_disabling_vsftpd"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_ftp_use_vsftpd"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_ftp_configure_vsftpd"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_ftp_restrict_users"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_ftp_limit_users"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_ftp_configure_firewall"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_installing_httpd"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_httpd_minimal_modules_ins
talled" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_securing_httpd"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_httpd_restrict_info_leaka
ge" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_httpd_minimize_loadable_m
odules" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_httpd_core_modules"
selected="false"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_httpd_basic_authenticatio
n" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_httpd_optional_components
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_httpd_minimize_config_fil
es_included" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_httpd_directory_restricti
ons" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_httpd_modules_improve_sec
urity" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_httpd_deploy_mod_ssl"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_httpd_deploy_mod_security
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_httpd_use_dos_protection_
modules" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_httpd_configure_php_secur
ely" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_httpd_configure_os_protec
t_web_server" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_httpd_restrict_file_dir_a
ccess" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_httpd_configure_firewalld
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_httpd_chroot"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_configure_dovecot"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_dovecot_support_necessary
_protocols" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_dovecot_enabling_ssl"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_dovecot_allow_imap_access
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_configuring_samba"
selected="false"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_smb_restrict_file_sharing
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_smb_disable_printing"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_snmp_configure_server"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_c2s_support"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_encrypt_partitions"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_ensure_gpgcheck_globally_a
ctivated" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_clean_components_post_upda
ting" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_ensure_gpgcheck_local_pack
ages" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_ensure_gpgcheck_repo_metad
ata" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_disable_prelink"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_aide_build_database"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_aide_scan_notification"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_aide_verify_acls"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_aide_verify_ext_attributes
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_aide_use_fips_hashes"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_rpm_verify_permissions"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_rpm_verify_hashes"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_install_hids"
selected="false"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_install_antivirus"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_dracut-
fips_installed" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_grub2_enable_fips_mode"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_installed_OS_is_certified"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_enable_dconf_user_profile"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_gnome_gdm_disable_automati
c_login" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_gnome_gdm_disable_guest_lo
gin" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_dconf_gnome_disable_user_l
ist" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_dconf_gnome_disable_restar
t_shutdown" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_dconf_gnome_enable_smartca
rd_auth" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_dconf_gnome_login_retries"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_dconf_gnome_screensaver_id
le_delay" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_dconf_gnome_screensaver_id
le_activation_enabled" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_dconf_gnome_screensaver_lo
ck_enabled" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_dconf_gnome_screensaver_lo
ck_delay" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_dconf_gnome_screensaver_mo
de_blank" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_dconf_gnome_screensaver_us
er_info" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_dconf_gnome_session_user_l
ocks" selected="false"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_dconf_gnome_disable_ctrlal
tdel_reboot" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_dconf_gnome_disable_user_a
dmin" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_dconf_gnome_disable_geoloc
ation" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_dconf_gnome_disable_wifi_c
reate" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_dconf_gnome_disable_wifi_n
otification" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_dconf_gnome_remote_access_
credential_prompt" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_dconf_gnome_remote_access_
encryption" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_dconf_gnome_disable_automo
unt" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_dconf_gnome_disable_thumbn
ailers" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_bootloader_nousb_argument"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_service_autofs_disabled"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_kernel_module_cramfs_disab
led" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_kernel_module_freevxfs_dis
abled" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_kernel_module_jffs2_disabl
ed" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_kernel_module_hfs_disabled
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_kernel_module_hfsplus_disa
bled" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_kernel_module_squashfs_dis
abled" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_no_files_unowned_by_user"
selected="false"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_file_permissions_ungroupow
ned" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_dir_perms_world_writable_s
ystem_owned" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_fs_suid_dumpable"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_kernel_exec_shield"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_install_PAE_kernel_on_x86-
32" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_kernel_dmesg_restri
ct" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_selinux_confinement_of_dae
mons" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_selinux_all_devicefiles_la
beled" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_abrt_anon_write"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_abrt_handle_event"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_abrt_upload_watch_a
non_write" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_auditadm_exec_conte
nt" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_cron_can_relabel"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_cron_system_cronjob
_use_shares" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_cron_userdomain_tra
nsition" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_daemons_dump_core"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_daemons_use_tcp_wra
pper" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_daemons_use_tty"
selected="false"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_deny_execmem"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_deny_ptrace"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_domain_fd_use"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_domain_kernel_load_
modules" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_fips_mode"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_gpg_web_anon_write"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_guest_exec_content"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_kerberos_enabled"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_logadm_exec_content
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_logging_syslogd_can
_sendmail" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_logging_syslogd_use
_tty" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_login_console_enabl
ed" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_mmap_low_allowed"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_mock_enable_homedir
s" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_mount_anyfile"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_polyinstantiation_e
nabled" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_secadm_exec_content
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_secure_mode_insmod"
selected="false"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_secure_mode"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_secure_mode_policyl
oad" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_selinuxuser_direct_
dri_enabled" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_selinuxuser_exechea
p" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_selinuxuser_execmod
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_selinuxuser_execsta
ck" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_selinuxuser_mysql_c
onnect_enabled" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_selinuxuser_ping"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_selinuxuser_postgre
sql_connect_enabled" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_selinuxuser_rw_noex
attrfile" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_selinuxuser_share_m
usic" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_selinuxuser_tcp_ser
ver" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_selinuxuser_udp_ser
ver" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_selinuxuser_use_ssh
_chroot" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_ssh_chroot_rw_homed
irs" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_ssh_keysign"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_ssh_sysadm_login"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_staff_exec_content"
selected="false"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_sysadm_exec_content
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_unconfined_login"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_use_ecryptfs_home_d
irs" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_user_exec_content"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_xdm_bind_vnc_tcp_po
rt" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_xdm_exec_bootloader
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_xdm_sysadm_login"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_xdm_write_home"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_xguest_connect_netw
ork" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_xguest_exec_content
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_xguest_mount_media"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_xguest_use_bluetoot
h" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_xserver_clients_wri
te_xshm" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_xserver_execmem"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sebool_xserver_object_mana
ger" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_gid_passwd_group_same"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_maximum_age_login
_defs" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_password_warn_age
_login_defs" selected="false"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_account_disable_post_pw_ex
piration" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_display_login_attempts"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_password_pam_maxc
lassrepeat" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_password_pam_dcre
dit" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_password_pam_ucre
dit" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_password_pam_lcre
dit" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_password_pam_difo
k" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_password_pam_minc
lass" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_passwords_pam_fai
llock_deny" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_passwords_pam_fai
llock_interval" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_set_password_hashing_algor
ithm_systemauth" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_set_password_hashing_algor
ithm_libuserconf" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_tmout"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_max_concurrent_lo
gin_sessions" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_umask_etc_login_d
efs" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_file_permissions_grub2_cfg
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_service_debug-
shell_disabled" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_disable_interactive_boot"
selected="false"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_screen_installed"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_banner_etc_issue"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_dconf_gnome_banner_enabled
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_dconf_gnome_login_banner_t
ext" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_network_sniffer_disabled"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_conf_defau
lt_send_redirects" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_conf_all_a
ccept_source_route" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_conf_all_a
ccept_redirects" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_conf_all_s
ecure_redirects" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_conf_defau
lt_log_martians" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_conf_defau
lt_accept_source_route" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_conf_defau
lt_accept_redirects" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_conf_defau
lt_secure_redirects" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_tcp_syncoo
kies" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_conf_all_r
p_filter" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_conf_defau
lt_rp_filter" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_network_ipv6_disable_rpc"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_net_ipv6_conf_all_a
ccept_source_route" selected="false"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_net_ipv6_conf_all_a
ccept_ra" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_net_ipv6_conf_defau
lt_accept_ra" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_net_ipv6_conf_all_a
ccept_redirects" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_net_ipv6_conf_defau
lt_accept_redirects" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_net_ipv6_conf_defau
lt_accept_source_route" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_net_ipv6_conf_all_f
orwarding" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_network_ipv6_privacy_exten
sions" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_service_firewalld_enabled"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_set_firewalld_default_zone
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_rsyslog_cron_logging"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_rsyslog_nolisten"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_bootloader_audit_argument"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_auditd_data_retention_num_
logs" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_auditd_data_retention_max_
log_file" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_auditd_data_retention_max_
log_file_action" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_auditd_data_retention_spac
e_left_action" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_auditd_data_retention_admi
n_space_left_action" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_auditd_data_retention_acti
on_mail_acct" selected="false"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_auditd_data_retention_flus
h" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_auditd_audispd_syslog_plug
in_activated" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_system_shutdow
n" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_usergroup_modi
fication_group" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_usergroup_modi
fication_gshadow" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_usergroup_modi
fication_shadow" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_usergroup_modi
fication_opasswd" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_login_events_f
aillock" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_session_events
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_unsuccessful_f
ile_modification_creat" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_unsuccessful_f
ile_modification_open" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_unsuccessful_f
ile_modification_openat" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_unsuccessful_f
ile_modification_open_by_handle_at" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_unsuccessful_f
ile_modification_truncate" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_unsuccessful_f
ile_modification_ftruncate" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_execution_chco
n" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_execution_rest
orecon" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_privileged_com
mands" selected="false"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_privileged_com
mands_unix_chkpwd" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_privileged_com
mands_gpasswd" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_privileged_com
mands_chage" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_privileged_com
mands_userhelper" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_privileged_com
mands_postdrop" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_privileged_com
mands_postqueue" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_privileged_com
mands_ssh_keysign" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_privileged_com
mands_pt_chown" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_privileged_com
mands_pam_timestamp_check" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_file_deletion_
events" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_file_deletion_
events_rmdir" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_file_deletion_
events_unlink" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_file_deletion_
events_unlinkat" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_file_deletion_
events_rename" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_file_deletion_
events_renameat" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_kernel_module_
loading_init" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_kernel_module_
loading_delete" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_service_xinetd_disabled"
selected="false"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_service_telnet_disabled"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_rsh_removed"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_service_rlogin_disabled"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_no_rsh_trust_files"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_ypserv_removed"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_service_ypbind_disabled"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_ypbind_removed"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_talk-
server_removed" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_talk_removed"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_service_kdump_disabled"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_service_sshd_enabled"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_file_permissions_sshd_pub_
key" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_file_permissions_sshd_priv
ate_key" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sshd_allow_only_protocol2"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sshd_disable_gssapi_auth"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sshd_enable_strictmodes"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sshd_use_priv_separation"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sshd_disable_compression"
selected="false"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sshd_set_keepalive"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sshd_disable_rhosts"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sshd_disable_user_known_ho
sts" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sshd_disable_rhosts_rsa"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_disable_host_auth"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sshd_enable_x11_forwarding
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sshd_disable_root_login"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sshd_disable_empty_passwor
ds" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sshd_enable_warning_banner
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sshd_do_not_permit_user_en
v" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sshd_use_approved_ciphers"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sshd_use_approved_macs"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sssd_memcache_timeout"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sssd_offline_cred_expirati
on" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sssd_ssh_known_hosts_timeo
ut" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_chronyd_or_ntpd_specify_mu
ltiple_servers" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_ldap_client_start_tls"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_mount_option_nodev_remote_
filesystems" selected="false"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_mount_option_nosuid_remote
_filesystems" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_mount_option_krb_sec_remot
e_filesystems" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_use_kerberos_security_all_
exports" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_service_zebra_disabled"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_partition_for_tmp"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_partition_for_var_log"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_partition_for_var_log_audi
t" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_ensure_redhat_gpgkey_insta
lled" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_ensure_gpgcheck_never_disa
bled" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_security_patches_up_to_dat
e" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_aide_installed"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_aide_periodic_cron_checkin
g" selected="true"/>
    <xccdf:select idref="xccdf_org.ssgproject.content_group_sudo"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sudo_remove_nopasswd"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sudo_remove_no_authenticat
e" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_mount_option_tmp_nosuid"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_mount_option_tmp_noexec"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_mount_option_tmp_nodev"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_mount_option_nosuid_remova
ble_partitions" selected="true"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_mount_option_noexec_remova
ble_partitions" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_mount_option_nodev_removab
le_partitions" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_mount_option_nodev_nonroot
_local_partitions" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_mount_option_var_tmp_bind"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_kernel_module_usb-
storage_disabled" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_permissions_important_acc
ount_files" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_userowner_shadow_file"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_groupowner_shadow_file"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_file_permissions_etc_shado
w" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_file_owner_etc_group"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_file_groupowner_etc_group"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_file_permissions_etc_group
" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_file_owner_etc_gshadow"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_file_groupowner_etc_gshado
w" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_file_permissions_etc_gshad
ow" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_file_owner_etc_passwd"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_file_groupowner_etc_passwd
" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_file_permissions_etc_passw
d" selected="true"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_file_permissions_unauthori
zed_sgid" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_file_permissions_unauthori
zed_suid" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_kernel_randomize_va
_space" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_enable_selinux_bootloader"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_no_direct_root_logins"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_securetty_root_login_conso
le_only" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_restrict_serial_port_login
s" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_no_shelllogin_for_systemac
counts" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_no_uid_except_zer
o" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_no_empty_passwords"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_password_all_shad
owed" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_password_minlen_l
ogin_defs" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_minimum_age_login
_defs" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_passwords_pam_fai
llock_unlock_time" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_passwords_pam_fai
llock_deny_root" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_password_pam_unix
_remember" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_set_password_hashing_algor
ithm_logindefs" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_logon_fail_delay"
selected="true"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_file_user_owner_grub2_cfg"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_file_group_owner_grub2_cfg
" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_bootloader_password"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_bootloader_uefi_password"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_smartcard_auth"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_require_singleuser_auth"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_disable_ctrlaltdel_reboot"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_network_disable_unused_in
terfaces" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_conf_all_s
end_redirects" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_ip_forward
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_conf_all_l
og_martians" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_icmp_echo_
ignore_broadcasts" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_icmp_ignor
e_bogus_error_responses" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_wireless_disable_in_bios"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_wireless_disable_interface
s" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_service_bluetooth_disabled
" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_kernel_module_bluetooth_di
sabled" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sysctl_kernel_ipv6_disable
" selected="true"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_network_ipv6_disable_inter
faces" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_kernel_module_dccp_disable
d" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_kernel_module_sctp_disable
d" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_libreswan_approved_tunnels
" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_rsyslog_files_ownership"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_rsyslog_files_groupownersh
ip" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_rsyslog_files_permissions"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_rsyslog_remote_loghost"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_time_adjtimex"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_time_settimeof
day" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_time_stime"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_time_clock_set
time" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_time_watch_loc
altime" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_dac_modificati
on_chmod" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_dac_modificati
on_chown" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_dac_modificati
on_fchmod" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_dac_modificati
on_fchmodat" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_dac_modificati
on_fchown" selected="true"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_dac_modificati
on_fchownat" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_dac_modificati
on_fremovexattr" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_dac_modificati
on_fsetxattr" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_dac_modificati
on_lchown" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_dac_modificati
on_lremovexattr" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_dac_modificati
on_lsetxattr" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_dac_modificati
on_removexattr" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_dac_modificati
on_setxattr" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_login_events_t
allylog" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_login_events_l
astlog" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_unsuccessful_f
ile_modification" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_execution_sema
nage" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_execution_sets
ebool" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_privileged_com
mands_passwd" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_privileged_com
mands_su" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_privileged_com
mands_sudo" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_privileged_com
mands_sudoedit" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_privileged_com
mands_newgrp" selected="true"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_privileged_com
mands_chsh" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_privileged_com
mands_umount" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_privileged_com
mands_crontab" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_kernel_module_
loading_insmod" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_kernel_module_
loading_rmmod" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_kernel_module_
loading_modprobe" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_immutable"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_usergroup_modi
fication_passwd" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_networkconfig_
modification" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_file_ownership_var_log_aud
it" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_file_permissions_var_log_a
udit" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_mac_modificati
on" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_media_export"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_audit_rules_sysadmin_actio
ns" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_service_auditd_enabled"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_xinetd_removed"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_telnet-
server_removed" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_telnet_removed"
selected="true"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_rsh-
server_removed" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_service_rexec_disabled"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_service_rsh_disabled"
selected="true"/>
    <xccdf:select idref="xccdf_org.ssgproject.content_group_tftp"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_tftp-
server_removed" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_file_owner_cron_allow"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_file_groupowner_cron_allow
" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_service_crond_enabled"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sshd_disable_kerb_auth"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_sshd_set_idle_timeout"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_service_sshd_disabled"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_printing"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_service_cups_disabled"
selected="true"/>
    <xccdf:select idref="xccdf_org.ssgproject.content_group_dhcp"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_dhcp_removed"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_service_chronyd_or_ntpd_en
abled" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_chronyd_or_ntpd_specify_re
mote_server" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_ntp_set_maxpoll"
selected="true"/>
    <xccdf:select idref="xccdf_org.ssgproject.content_group_mail"
selected="true"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_sendmail_removed"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_postfix_network_listening_
disabled" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_openldap_server"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_openldap-
servers_removed" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_openldap_client"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_disabling_nfs"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_disabling_nfs_services"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_service_nfslock_disabled"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_service_rpcgssd_disabled"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_service_rpcbind_disabled"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_service_rpcidmapd_disabled
" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_disabling_nfsd"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_mounting_remote_filesyste
ms" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_nfs_configuring_servers"
selected="false"/>
    <xccdf:select idref="xccdf_org.ssgproject.content_group_dns"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_disabling_dns_server"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_service_named_disabled"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_bind_removed"
selected="true"/>
    <xccdf:select idref="xccdf_org.ssgproject.content_group_ftp"
selected="true"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_vsftpd_removed"
selected="true"/>
    <xccdf:select idref="xccdf_org.ssgproject.content_group_http"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_disabling_httpd"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_httpd_removed"
selected="true"/>
    <xccdf:select idref="xccdf_org.ssgproject.content_group_imap"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_disabling_dovecot"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_dovecot_removed"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_quagga_removed"
selected="true"/>
    <xccdf:select idref="xccdf_org.ssgproject.content_group_smb"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_disabling_samba"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_samba_removed"
selected="true"/>
    <xccdf:select idref="xccdf_org.ssgproject.content_group_proxy"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_disabling_squid"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_squid_removed"
selected="true"/>
    <xccdf:select idref="xccdf_org.ssgproject.content_group_snmp"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_disabling_snmp_service"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_package_net-snmp_removed"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_selinux-booleans"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_password_quality_pwqualit
y" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_password_pam_retr
y" selected="true"/>
```

```
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_password_pam_maxr
epeat" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_password_pam_minl
en" selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_accounts_password_pam_ocre
dit" selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_selinux_state"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_root_logins"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_accounts-restrictions"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_accounts-pam"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_accounts-session"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_accounts-physical"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_console_screen_locking"
selected="false"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_selinux"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_rule_selinux_policytype"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_bootloader"
selected="true"/>
    <xccdf:select
idref="xccdf_org.ssgproject.content_group_screen_locking"
selected="false"/>
    <xccdf:set-value
idref="xccdf_org.ssgproject.content_value_var_accounts_maximum_age_
login_defs">64</xccdf:set-value>
    <xccdf:set-value
idref="xccdf_org.ssgproject.content_value_var_accounts_minimum_age_
login_defs">1</xccdf:set-value>
    <xccdf:set-value
idref="xccdf_org.ssgproject.content_value_var_password_pam_retry">5
</xccdf:set-value>
    <xccdf:set-value
idref="xccdf_org.ssgproject.content_value_var_password_pam_maxrepea
t">2</xccdf:set-value>
```

```
    <xccdf:set-value
idref="xccdf_org.ssgproject.content_value_var_password_pam_ocredit"
>-1</xccdf:set-value>
    <xccdf:set-value
idref="xccdf_org.ssgproject.content_value_sysctl_net_ipv4_conf_all_
log_martians_value">1</xccdf:set-value>
    <xccdf:set-value
idref="xccdf_org.ssgproject.content_value_var_accounts_password_min
len_login_defs">15</xccdf:set-value>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_login_banner_text"
selector="usgcb_default"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_inactivity_timeout_value"
selector="15_minutes"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_password_pam_minlen"
selector="15"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_password_pam_ocredit"
selector="1"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_password_pam_dcredit"
selector="1"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_password_pam_ucredit"
selector="1"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_password_pam_lcredit"
selector="1"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_sshd_idle_timeout_value"
selector="10_minutes"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_accounts_fail_delay"
selector="4"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_accounts_passwords_pa
m_faillock_deny" selector="3"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_accounts_passwords_pa
m_faillock_fail_interval" selector="900"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_accounts_passwords_pa
m_faillock_unlock_time" selector="never"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_password_pam_retry"
selector="3"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_sshd_listening_port"
selector="default"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_sysctl_net_ipv4_conf_all_
accept_redirects_value" selector="disabled"/>
```

```
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_sysctl_net_ipv4_conf_defa
ult_accept_redirects_value" selector="disabled"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_sysctl_net_ipv4_conf_defa
ult_accept_source_route_value" selector="disabled"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_sysctl_net_ipv4_icmp_echo
_ignore_broadcasts_value" selector="enabled"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_sysctl_net_ipv4_tcp_synco
okies_value" selector="enabled"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_auditd_action_mail_ac
ct" selector="root"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_auditd_admin_space_le
ft_action" selector="single"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_auditd_flush"
selector="data"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_auditd_max_log_file_a
ction" selector="rotate"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_auditd_max_log_file"
selector="6"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_auditd_num_logs"
selector="5"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_auditd_space_left_act
ion" selector="email"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_multiple_time_servers
" selector="rhel"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_accounts_user_umask"
selector="077"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_selinux_policy_name"
selector="targeted"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_selinux_state"
selector="enforcing"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_account_disable_post_
pw_expiration" selector="35"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_accounts_max_concurre
nt_login_sessions" selector="10"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_accounts_maximum_age_
login_defs" selector="60"/>
```

```
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_accounts_minimum_age_
login_defs" selector="7"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_accounts_password_min
len_login_defs" selector="6"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_accounts_password_war
n_age_login_defs" selector="7"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_accounts_tmout"
selector="10_min"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_password_pam_difok"
selector="8"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_password_pam_maxclass
repeat" selector="4"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_password_pam_maxrepea
t" selector="2"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_password_pam_minclass
" selector="4"/>
    <xccdf:refine-value
idref="xccdf_org.ssgproject.content_value_var_password_pam_unix_rem
ember" selector="5"/>
  </xccdf:Profile>
</xccdf:Tailoring>
```

A3 The tailored XCCDF rule

The XML files for the SCAP XCCDF rule (test-iptables-hash-xccdf.xml) and the OVAL information file (test-iptables-hash-cpe-oval.xml) produced by eSCAPe for the iptables ingrity checking.

```
<?xml version="1.0" encoding="UTF-8"?>
<Benchmark xmlns="http://checklists.nist.gov/xccdf/1.1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:cdf="http://checklists.nist.gov/xccdf/1.1"
xmlns:cpe="http://cpe.mitre.org/dictionary/2.0"
xmlns:cpelang="http://cpe.mitre.org/language/2.0"
xmlns:dc="http://purl.org/dc/elements/1.1/"
xmlns:xhtml="http://www.w3.org/1999/xhtml"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
id="test_iptables_hash_cpe_oval_xml_benchmark" resolved="0"
xml:lang="en-US"
xsi:schemaLocation="http://purl.org/dc/elements/1.1/
simpledc20021212.xsd http://www.w3.org/2000/09/xmldsig# xmldsig-
core-schema.xsd http://cpe.mitre.org/dictionary/2.0 cpe-
dictionary_2.0.xsd http://checklists.nist.gov/xccdf/1.1 xccdf-
1.1.4.xsd http://cpe.mitre.org/language/2.0 cpe-language_2.0.xsd">
  <status date="2018-04-05">draft</status>
  <description>File content for OVAL file test-iptables-hash-cpe-
oval.xml built on 2018-03-28T01:00:56</description>
  <version>v0.0</version>
  <Profile id="iptables_hashcheck">
    <title>iptables_hashcheck</title>
    <select idref="xccdf_oval_ointra_node_def_1_rule"
selected="true" />
  </Profile>
  <Group id="network">
    <Rule id="xccdf_oval_ointra_node_def_1_rule">
      <title>iptables module loaded</title>
      <description>Check that the ip_tables -module is currently
loaded.</description>
      <check system="http://oval.mitre.org/XMLSchema/oval-
definitions-5">
        <check-content-ref href="test-iptables-hash-cpe-oval.xml"
name="oval:ointra.node:def:1" />
      </check>
    </Rule>
  </Group>
</Benchmark>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<oval_definitions xmlns="http://oval.mitre.org/XMLSchema/oval-
definitions-5" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-
```

```
5" xmlns:oval-def="http://oval.mitre.org/XMLSchema/oval-
definitions-5" xmlns:independent-
def="http://oval.mitre.org/XMLSchema/oval-definitions-
5#independent"
xsi:schemaLocation="http://oval.mitre.org/XMLSchema/oval-
definitions-5 oval-definitions-schema.xsd
http://oval.mitre.org/XMLSchema/oval-common-5 oval-common-
schema.xsd http://oval.mitre.org/XMLSchema/oval-definitions-
5#independent independent-definitions-schema.xsd">
  <generator>
    <oval:product_name>Enhanced SCAP Content Editor
(eSCAPe)</oval:product_name>
    <oval:product_version>1.2.2</oval:product_version>
    <oval:schema_version>5.10</oval:schema_version>
    <oval:timestamp>2018-03-28T01:00:56</oval:timestamp>
  </generator>
  <!--generated.oval.base.identifier=ointra.node-->
  <definitions>
    <definition id="oval:ointra.node:def:1" version="1"
class="compliance">
      <metadata>
        <title>iptables module loaded</title>
        <affected family="unix">
          <platform>centos</platform>
        </affected>
        <reference source="CCE" ref_id="TBD" />
        <description>Check that the ip_tables -module is currently
loaded.</description>
      </metadata>
      <criteria operator="OR" negate="false" comment="">
        <criterion comment="File hash test for
/etc/sysconfig/iptables" test_ref="oval:ointra.node:tst:1"
negate="false" />
      </criteria>
    </definition>
  </definitions>
  <tests>
    <filehash_test xmlns="http://oval.mitre.org/XMLSchema/oval-
definitions-5#independent" id="oval:ointra.node:tst:1" version="1"
check="all" comment="File hash test for /etc/sysconfig/iptables"
check_existence="only_one_exists">
      <object object_ref="oval:ointra.node:obj:1" />
      <state state_ref="oval:ointra.node:ste:1" />
    </filehash_test>
  </tests>
  <objects>
    <filehash_object xmlns="http://oval.mitre.org/XMLSchema/oval-
definitions-5#independent" id="oval:ointra.node:obj:1" version="1"
comment="File hash for the iptables firewall rules
/etc/sysconfig/iptables">
      <path datatype="string"
operation="equals">/etc/sysconfig</path>
      <filename datatype="string"
operation="equals">iptables</filename>
    </filehash_object>
  </objects>
```

```
  <states>
    <filehash_state xmlns="http://oval.mitre.org/XMLSchema/oval-
definitions-5#independent" id="oval:ointra.node:ste:1" version="1"
comment="File hash stse for /etc/sysconfig/iptables">
      <sha1 datatype="string" operation="equals" entity_check="all"
var_check="all">ee91ff6f4555eacc03417917e3418865517fe2e7</sha1>
    </filehash_state>
  </states>
</oval_definitions>
```

A4 The OpenSCAP remediation report

The original **oscap –remediate** -report is produced in HTML format, but could not be viewed as a HTML file inside this document. Instead, the file is included inline below. (**oscap_usgcb_remediate_report.html**)

GUIDE TO THE SECURE CONFIGURATION OF CENTOS LINUX 7

This guide presents a catalog of security-relevant configuration settings for CentOS Linux 7. It is a rendering of content structured in the eXtensible Configuration Checklist Description Format

(XCCDF) in order to support security automation. The SCAP content is is available in the scap-security-guide package which is developed at https://www.open-scap.org/security-policies /scap-security-guide (https://www.open-scap.org/security-policies/scap-security-guide).

Providing system administrators with such guidance informs them how to securely configure systems under their control in a variety of network roles. Policy makers and baseline creators can use this catalog of settings, with its associated references to higher-level security control catalogs, in order to assist them in security baseline creation. This guide is a *catalog, not a checklist,* and satisfaction of every item is not likely to be possible or sensible in many operational scenarios. However, the XCCDF format enables granular selection and adjustment of settings, and their association with OVAL and OCIL content provides an automated checking capability.

Transformations of this document, and its associated automated checking content, are capable of providing baselines that meet a diverse set of policy objectives. Some example XCCDF *Profiles*, which are selections of items that form checklists and can be used as baselines, are available with this guide. They can be processed, in an automated fashion, with tools that support the Security Content Automation Protocol (SCAP). The DISA STIG for CentOS Linux 7, which provides required settings for US Department of Defense systems, is one example of a baseline created from this guidance.

This benchmark is a direct port of a *SCAP Security Guide* benchmark developed for *CentOS Linux*. It has been modified through an automated process to remove specific dependencies on *CentOS Linux* and to function with *CentOS*. The result is a generally useful *SCAP Security Guide* benchmark with the following caveats:

- *CentOS* is not an exact copy of *CentOS Linux*. There may be configuration differences that produce false positives and/or false negatives. If this occurs please file a bug report. *CentOS* has its own build system, compiler options, patchsets, and is a community supported, non-commercial operating system. *CentOS* does not inherit certifications or evaluations from *CentOS Linux*. As such, some configuration rules (such as those requiring *FIPS 140-2* encryption) will continue to fail on *CentOS*.

Members of the *CentOS* community are invited to participate in OpenSCAP (http://openscap.org) and SCAP Security Guide (https://github.com/OpenSCAP/scap-security-guide) development. Bug reports and patches can be sent to GitHub: https://github.com/OpenSCAP /scap-security-guide (https://github.com/OpenSCAP/scap-security-guide). The mailing list is at https://fedorahosted.org/mailman/listinfo/scap-security-guide (https://fedorahosted.org/mailman /listinfo/scap-security-guide).

Do not attempt to implement any of the settings in this guide without first testing them in a non-operational environment. The creators of this guidance assume no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic.

EVALUATION CHARACTERISTICS

Target machine	hostess.localdomain
Benchmark URL	/usr/share/xml/scap/ssg/content/ssg-centos7-ds.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_RHEL-7
Profile ID	xccdf_ointra.node_profile_ospp-rhel7_kvmhost
Started at	2018-04-04T17:54:55
Finished at	2018-04-04T17:55:12
Performed by	admin

CPE Platforms

- cpe:/o:centos:centos:7
- cpe:/o:redhat:enterprise_linux:7
- cpe:/o:redhat:enterprise_linux:7::client
- cpe:/o:redhat:enterprise_linux:7::computenode

Addresses

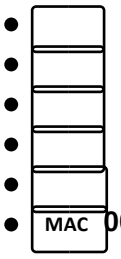
IPv4 127.0.0.1

IPv4 192.168.236.224

IPv6 0:0:0:0:0:0:0:1

IPv6 fe80:0:0:0:20c:29ff:fe5d:c478

MAC 00:00:00:00:00:00



- **00:0C:29:5D:C4:78**

COMPLIANCE AND SCORING

The target system did not satisfy the conditions of 3 rules! Furthermore, the results of 4 rules were inconclusive. Please review rule results and consider applying remediation.

Rule results

141 passed 3 7

Severity of failed rules

2 medium 1 high

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	95.419441	100.000000	95.42%

RULE OVERVIEW

Title	Severity	Result
Guide to the Secure Configuration of CentOS Linux 7 3x fail 4x error 3x notchecked		
Remediation functions used by the SCAP Security Guide Project		
Introduction		
System Settings 3x fail 2x error 3x notchecked		
Installing and Maintaining Software 1x notchecked		
Disk Partitioning		
Ensure /tmp Located On Separate Partition	low	**pass**
Ensure /var/log Located On Separate Partition	low	**pass**
Ensure /var/log/audit Located On Separate Partition	low	**pass**
Updating Software 1x notchecked		
Ensure Red Hat GPG Key Installed	high	**pass**
Ensure gpgcheck Enabled For All Yum Package Repositories	high	**pass**
System and Software Integrity		

Title	Severity	Result
Software Integrity Checking		

Verify Integrity with AIDE		
Verify Integrity with RPM		
Endpoint Protection Software		
McAfee Endpoint Security Software		
McAfee Host-Based Intrusion Detection Software (HBSS)		
Federal Information Processing Standard (FIPS)		
Operating System Vendor Support and Certification		
GNOME Desktop Environment		
Sudo		
Ensure Users Re-Authenticate for Privilege Escalation - sudo NOPASSWD	medium	**pass**
Ensure Users Re-Authenticate for Privilege Escalation - sudo !authenticate	medium	**pass**
File Permissions and Masks		
Restrict Partition Mount Options		
Add nodev Option to Removable Media Partitions	low	**pass**
Add noexec Option to Removable Media Partitions	low	**pass**
Add nosuid Option to Removable Media Partitions	low	**pass**
Add nodev Option to /tmp	low	**pass**

Add noexec Option to /tmp	low	**pass**
Add nosuid Option to /tmp	low	**pass**
Bind Mount /var/tmp To /tmp	low	**pass**

Title	**Severity**	**Result**
Restrict Dynamic Mounting and Unmounting of Filesystems		
Disable Modprobe Loading of USB Storage Driver	medium	**pass**
Verify Permissions on Important Files and Directories		
Verify Permissions on Files with Local Account Information and Credentials		
Verify User Who Owns shadow File	medium	**pass**
Verify Group Who Owns shadow File	medium	**pass**
Verify Permissions on shadow File	medium	**pass**
Verify User Who Owns group File	medium	**pass**
Verify Group Who Owns group File	medium	**pass**
Verify Permissions on group File	medium	**pass**
Verify User Who Owns gshadow File	medium	**pass**
Verify Group Who Owns gshadow File	medium	**pass**
Verify Permissions on gshadow File	medium	**pass**
Verify User Who Owns passwd File	medium	**pass**

Verify Group Who Owns passwd File	medium	**pass**
Verify Permissions on passwd File	medium	**pass**
Verify File Permissions Within Some Important Directories		
Ensure All SGID Executables Are Authorized	low	**pass**
Ensure All SUID Executables Are Authorized	low	**pass**
Restrict Programs from Dangerous Execution Patterns		
Daemon Umask		
Disable Core Dumps		

Title	**Severity**	**Result**
Enable ExecShield		
Enable Randomized Layout of Virtual Address Space	medium	**pass**
Enable Execute Disable (XD) or No Execute (NX) Support on x86 Systems		
SELinux		
SELinux - Booleans		
Ensure SELinux Not Disabled in /etc/default/grub	medium	**pass**
Ensure SELinux State is Enforcing	high	**pass**
Configure SELinux Policy	high	**pass**

Account and Access Control 1x fail 2x error		
Protect Accounts by Restricting Password-Based Login		
Restrict Root Logins		
Direct root Logins Not Allowed	medium	**pass**
Restrict Virtual Console Root Logins	medium	**pass**
Restrict Serial Port Root Logins	low	**pass**
Ensure that System Accounts Do Not Run a Shell Upon Login	medium	**pass**
Verify Only Root Has UID 0	high	**pass**
Verify Proper Storage and Existence of Password Hashes		
Prevent Log In to Accounts With Empty Password	high	**pass**
Verify All Account Password Hashes are Shadowed	medium	**pass**
Set Password Expiration Parameters		
Set Password Minimum Length in login.defs	medium	**pass**

Title	**Severity**	**Result**
Set Password Minimum Age	medium	**pass**
Set Account Expiration Parameters		

Protect Accounts by Configuring PAM 2x error		
Set Password Quality Requirements 1x error		
Set Password Quality Requirements with pam_pwquality 1x error		
Set Password Retry Prompts Permitted Per-Session	low	**error**
Set Password Maximum Consecutive Repeating Characters	medium	**pass**
Set Password Minimum Length	medium	**pass**
Set Lockouts for Failed Password Attempts 1x error		
Set Lockout Time For Failed Password Attempts	medium	**pass**
Configure the root Account for Failed Password Attempts	medium	**error**
Limit Password Reuse	medium	**pass**
Set Password Hashing Algorithm		
Set Password Hashing Algorithm in /etc/login.defs	medium	**pass**
Secure Session Configuration Files for Login Accounts		
Ensure that No Dangerous Directories Exist in Root's Path		
Ensure that Users Have Sensible Umask Values		

Ensure the Logon Failure Delay is Set Correctly in login.defs	low	**pass**
Protect Physical Console Access 1x fail		
Set Boot Loader Password 1x fail		

Title	Severity	Result
Verify /boot/grub2/grub.cfg User Ownership	medium	pass
Verify /boot/grub2/grub.cfg Group Ownership	medium	pass
Set Boot Loader Password	high	fail
Set the UEFI Boot Loader Password	medium	pass
Configure Screen Locking		
Configure Console Screen Locking		
Install the screen Package	medium	pass
Hardware Tokens for Authentication		
Require Authentication for Single User Mode	medium	pass
Disable Ctrl-Alt-Del Reboot Activation	high	pass
Warning Banners for System Accesses		
Network Configuration and Firewalls	**1x fail 2x notchecked**	
Disable Unused Interfaces		
Kernel Parameters Which Affect Networking		
Network Parameters for Hosts Only		
Disable Kernel Parameter for Sending ICMP Redirects for All Interfaces	medium	pass
Network Related Kernel Runtime Parameters for Hosts and Routers		
Configure Kernel Parameter to Log Martian Packets	low	pass
Configure Kernel Parameter to Ignore ICMP Broadcast Echo Requests	medium	pass
Configure Kernel Parameter to Ignore Bogus ICMP Error Responses	low	pass

Title	Severity	Result
Wireless Networking 1x notchecked		
Disable Wireless Through Software Configuration 1x notchecked		
Deactivate Wireless Network Interfaces	low	**pass**
Disable Bluetooth Service	medium	**pass**
Disable Bluetooth Kernel Modules	medium	**pass**
IPv6 1x fail 1x notchecked		
Disable Support for IPv6 Unless Needed 1x fail 1x notchecked		
Disable IPv6 Networking Support Automatic Loading	medium	**fail**
Disable Support for RPC IPv6	low	**pass**
Configure IPv6 Settings if Necessary		
firewalld		
Transport Layer Security Support		
Uncommon Network Protocols		
Disable DCCP Support	medium	**pass**
Disable SCTP Support	medium	**pass**
IPSec Support		
Configure Syslog		

Ensure Proper Configuration of Log Files		
Ensure Log Files Are Owned By Appropriate User	medium	**pass**
Ensure Log Files Are Owned By Appropriate Group	medium	**pass**
Ensure System Log Files Have Correct Permissions	medium	**pass**
Rsyslog Logs Sent To Remote Host		

Title	**Severity**	**Result**
Ensure Logs Sent To Remote Host	low	**pass**
Configure rsyslogd to Accept Remote Messages If Acting as a Log Server		
Ensure All Logs are Rotated by logrotate		
Configure Logwatch on the Central Log Server		
System Accounting with auditd **1x fail**		
Configure auditd Data Retention		
Configure auditd Rules for Comprehensive Auditing **1x fail**		
Records Events that Modify Date and Time Information		
Record attempts to alter time through adjtimex	low	**pass**
Record attempts to alter time through settimeofday	low	**pass**

Record Attempts to Alter Time Through stime	low	**pass**
Record Attempts to Alter Time Through clock_settime	low	**pass**
Record Attempts to Alter the localtime File	low	**pass**
Record Events that Modify the System's Discretionary Access Controls		
Record Events that Modify the System's Discretionary Access Controls - chmod	low	**pass**
Record Events that Modify the System's Discretionary Access Controls - chown	low	**pass**
Record Events that Modify the System's Discretionary Access Controls - fchmod	low	**pass**
Record Events that Modify the System's Discretionary Access Controls - fchmodat	low	**pass**
Record Events that Modify the System's Discretionary Access Controls - fchown	low	**pass**

Title	**Severity**	**Result**
Record Events that Modify the System's Discretionary Access Controls - fchownat	low	**pass**
Record Events that Modify the System's Discretionary Access Controls fremovexattr	medium	**pass**
Record Events that Modify the System's Discretionary Access Controls - fsetxattr	low	**pass**

Record Events that Modify the System's Discretionary Access Controls - lchown	low	**pass**
Record Events that Modify the System's Discretionary Access Controls lremovexattr	medium	**pass**
Record Events that Modify the System's Discretionary Access Controls - lsetxattr	low	**pass**
Record Events that Modify the System's Discretionary Access Controls - removexattr	medium	**pass**
Record Events that Modify the System's Discretionary Access Controls - setxattr	low	**pass**
Record Attempts to Alter Logon and Logout Events		
Record Attempts to Alter Logon and Logout Events - tallylog	medium	**pass**
Record Attempts to Alter Logon and Logout Events - lastlog	medium	**pass**
Record Unauthorized Access Attempts Events to Files (unsuccessful)		
Ensure auditd Collects Unauthorized Access Attempts to Files (unsuccessful)	medium	**pass**
Record Execution Attempts to Run SELinux Privileged Commands		
Record Any Attempts to Run semanage	medium	**pass**
Record Any Attempts to Run setsebool	medium	**pass**
Record Information on the Use of Privileged Commands		

Title	Severity	Result
Ensure auditd Collects Information on the Use of Privileged Commands - passwd	medium	**pass**
Ensure auditd Collects Information on the Use of Privileged Commands - su	medium	**pass**
Ensure auditd Collects Information on the Use of Privileged Commands - sudo	medium	**pass**
Ensure auditd Collects Information on the Use of Privileged Commands - sudoedit	medium	**pass**
Ensure auditd Collects Information on the Use of Privileged Commands - newgrp	medium	**pass**
Ensure auditd Collects Information on the Use of Privileged Commands - chsh	medium	**pass**
Ensure auditd Collects Information on the Use of Privileged Commands - umount	medium	**pass**
Ensure auditd Collects Information on the Use of Privileged Commands - crontab	medium	**pass**
Record File Deletion Events by User		
Record Information on Kernel Modules Loading and Unloading		
Ensure auditd Collects Information on Kernel Module Loading and Unloading insmod	medium	**pass**
Ensure auditd Collects Information on Kernel Module Loading and Unloading rmmod	medium	**pass**

Ensure auditd Collects Information on Kernel Module Loading and Unloading modprobe	medium	**pass**
Record Events that Modify User/Group Information - passwd	medium	**fail**
Record Events that Modify the System's Network Environment	low	**pass**

Title	**Severity**	**Result**
System Audit Logs Must Have Mode 0640 or Less Permissive	medium	**pass**
System Audit Logs Must Be Owned By Root	medium	**pass**
Record Events that Modify the System's Mandatory Access Controls	low	**pass**
Ensure auditd Collects Information on Exporting to Media (successful)	medium	**pass**
Ensure auditd Collects System Administrator Actions	low	**pass**
Make the auditd Configuration Immutable	medium	**pass**
Enable auditd Service	high	**pass**
Services 2x error		
Obsolete Services		
Xinetd		
Uninstall xinetd Package	low	**pass**

Telnet		
Uninstall telnet-server Package	high	**pass**
Remove telnet Clients	low	**pass**
Rlogin, Rsh, and Rexec		
Uninstall rsh-server Package	high	**pass**
Disable rexec Service	high	**pass**
Disable rsh Service	high	**pass**
NIS		
TFTP Server		
Uninstall tftp-server Package	high	**pass**
Chat/Messaging Services		

Title	**Severity**	**Result**
Base Services		
Cron and At Daemons		
Restrict at and cron to Authorized Users if Necessary		
Verify User Who Owns /etc/cron.allow file	medium	**pass**
Verify Group Who Owns /etc/cron.allow file	medium	**pass**
Enable cron Service	medium	**pass**

Docker Service		
SSH Server		
Configure OpenSSH Server if Necessary		
Strengthen Firewall Configuration if Possible		
Allow Only SSH Protocol 2	high	**pass**
Disable Kerberos Authentication	medium	**pass**
Set SSH Idle Timeout Interval	low	**pass**
Disable SSH Server If Possible (Unusual)	low	**pass**
System Security Services Daemon		
X Window System		
Disable X Windows		
Disable X Windows Startup By Setting Default Target	medium	**pass**
Avahi Server		
Print Support		
Configure the CUPS Service if Necessary		
Disable the CUPS Service	low	**pass**
DHCP		
Disable DHCP Server		

Title	Severity	Result
Uninstall DHCP Server Package	medium	**pass**
Disable DHCP Server		
Disable DHCP Client		
Configure DHCP Client if Necessary		
Network Time Protocol 2x error		
Enable the NTP Daemon	medium	**error**
Specify a Remote NTP Server	medium	**error**
Mail Server Software		
Configure SMTP For Mail Clients		
Configure Operating System to Protect Mail Server		
Uninstall Sendmail Package	medium	**pass**
LDAP		
Configure OpenLDAP Clients		
Configure OpenLDAP Server		
Install and Protect LDAP Certificate Files		
Uninstall openldap-servers Package	low	**pass**
NFS and RPC		
Disable All NFS Services if Possible		

Disable Services Used Only by NFS		
Disable Network File System Lock Service (nfslock)	low	**pass**
Disable Secure RPC Client Service (rpcgssd)	low	**pass**
Disable rpcbind Service	low	**pass**

Title	**Severity**	**Result**
Disable RPC ID Mapping Service (rpcidmapd)	low	**pass**
Configure All Systems which Use NFS		
Configure NFS Clients		
Disable NFS Server Daemons		
Disable Network File System (nfs)	low	**pass**
Mount Remote Filesystems with Restrictive Options		
Configure NFS Servers		
DNS Server		
Disable DNS Server		
Uninstall bind Package	low	**pass**
Isolate DNS from Other Services		
Protect DNS Data from Tampering or Attack		
FTP Server		
Disable vsftpd if Possible		
Uninstall vsftpd Package	high	**pass**

Use vsftpd to Provide FTP Service if Necessary		
Use vsftpd to Provide FTP Service if Necessary		
Web Server		
IMAP and POP3 Server		
Disable Dovecot		
Uninstall dovecot Package	low	**pass**
Configure Dovecot if Necessary		
Network Routing		
Disable Quagga if Possible		
Title	**Severity**	**Result**
Uninstall quagga Package	medium	**pass**
Samba(SMB) Microsoft Windows File Sharing Server		
Disable Samba if Possible		
Uninstall Samba Package	low	**pass**
Configure Samba if Necessary		
Proxy Server		
Disable Squid if Possible		
Uninstall squid Package	low	**pass**
SNMP Server		
Disable SNMP Server if Possible		
Uninstall net-snmp Package	low	**pass**
Configure SNMP Server if Necessary		
Documentation to Support C2S/CIS Mapping		

Generated using OpenSCAP (http://open-scap.org) 1.2.14

A5 KVM iptables firewall

An **iptables** configuration script (**kvmfirewall**) that, when run, produces the requested firewall.

```
#! /bin/sh
#
# Flush all rules
iptables -F
iptables -X

# Set default chain policies
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT

# Accept on localhost
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
iptables -A OUTPUT -o ens33 -p udp -j ACCEPT

# Accept NTP server to be polled
#iptables -A INPUT -i ens33 -p udp --dport 123 -j ACCEPT
#iptables -A OUTPUT -o ens33 -p udp --sport 123 -j ACCEPT

# Save the rules
/sbin/service iptables save
```

A6 Cron script for the regular security checks

A script (**oscap-recurrent.sh**) that is run by the **Cron** service. It will audit the system with **oscap** and mail a remote system administrator (currently **root@node.intra**) if any failures occur.

```
#! /bin/sh
####
#MIT License
#
#Copyright (c) 2018 Kaisa Henttunen
#
#Permission is hereby granted, free of charge, to any person obtaining
#a copy of this software and associated documentation files (the
#"Software"), to deal in the Software without restriction, including
#without limitation the rights to use, copy, modify, merge, publish,
#distribute, sublicense, and/or sell copies of the Software, and to
#permit persons to whom the Software is furnished to do so, subject to
#the following conditions:
#
#The above copyright notice and this permission notice shall be
#included in all copies or substantial portions of the Software.
#
#THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
#EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
#MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
#NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS
#BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN
#ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN
#CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
#SOFTWARE.
####
#
##
# This script mails the failed oscap remediation script to the
#local domain administrator root@node.intra
# You can recover the inline html from the message with "munpack
#email.txt", found in th CentOS package mpack
##
HOSTNAME=$(hostname)
DATE=$(date +%F)
FILE=/root/oscap-$HOSTNAME-report-$DATE.html
/usr/bin/oscap xccdf eval --remediate --profile
xccdf_ointra.node_profile_ospp-rhel7_kvmhost --report $FILE
/root/node.intra/xccdf/tailoring-xccdf.xml
grep -q rule-result-fail $FILE
if [ $? -eq 0 ]
then
          uuencode $FILE $FILE | mail -s "oscap Fail from
$HOSTNAME" -a $FILE root@intra.node

          echo "The daily oscap --remediate report failed at
$HOSTNAME. The report is attached." | mail -s "oscap Fail from
$HOSTNAME" -a $FILE root@intra.node
```

```
          uuencode $FILE $FILE |  mail -s "oscap report $DATE"
kaisa@$HOSTNAME
else
          exit 0
fi

exit 0
```