Linux Hardening

Tuvshinbayar Davaa

#> whoami

- Үндэсний Дата Төв УТҮГ -т систем хөгжүүлэлт хариуцсан менежер

- MNCERT CC -д сайн дурын ажилтан

- Харуул Занги тэмцээний зохион байгуулалтад сүүлийн 3 жил оролцож байна.

- RHCE, RHCI

#> ls /mnsec/slide/content/

- Introduction
- Pluggable Authentication Module
- sudo
- setuid, setgid, acl, selinux
- auditd
- sshd
- iptables, firewalld
- OpenSCAP
- Заавар, зөвлөгөө

#> man hardening

- Муу залуусыг ичээх зорилготой
- Үйлдлийн систем + Програм хангамж + Хандалт, удирдлага
- Audit > Harden > Repeat

#> systemctl disable hardening

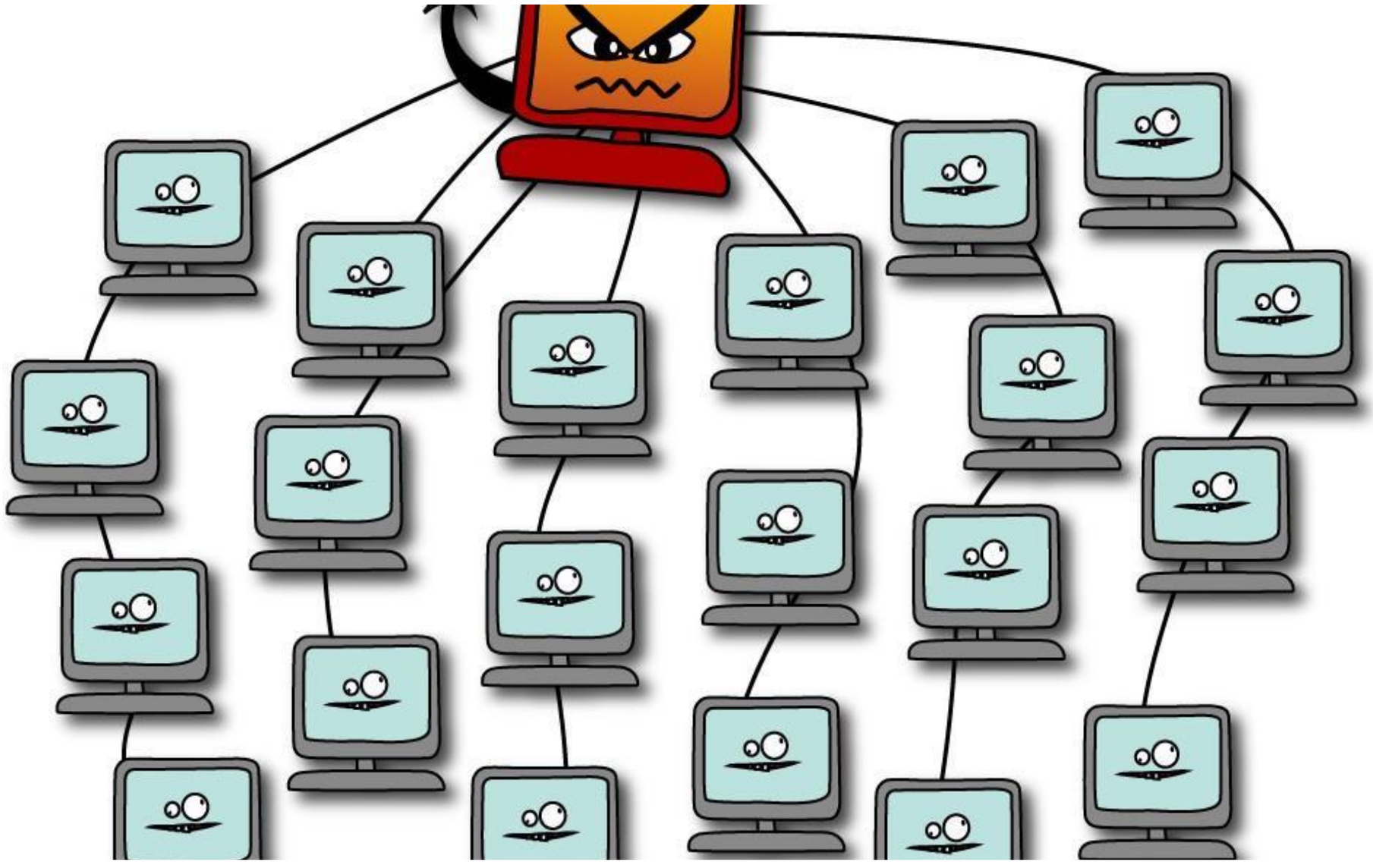
Хэрвээ системийн аюулгүй байдлыг орхигдуулвал юу болох вэ?

#> systemctl disable hardening

Хэрвээ системийн аюулгүй байдлыг орхигдуулвал юу болох вэ?

#> systemctl disable hardening

Хэрвээ системийн аюулгүй байдлыг орхигдуулвал юу болох вэ?



#> man hardening

- Програм хангамж, сервисийн тохиргоо
- VCS мэдээллээ ил болгох: .git, Example: unaa.mn, mongolduu.com
- Service info; Example: phpinfo, debug mode
- Minimal package installation - VestaCP
- chmod -R 777 /var/www/uploads/

#> echo “Service information disclosures”

```
~ » curl -i http://caak.mn
HTTP/1.1 301 Moved Permanently
Server: nginx/1.11.8
Date: Fri, 05 Oct 2018 01:07:29 GMT
Content-Type: text/html
Content-Length: 185
Connection: keep-alive
Location: https://www.caak.mn/
```

Nginx » Nginx » 1.11.8 : Security Vulnerabilities

Cpe Name:*cpe:/a:nginx:nginx:1.11.8*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.
1	CVE-2017-7529	190		Overflow +Info	2017-07-13	2018-01-04	5.0	None	Remote	Low	Not required	Partial	None

Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially craft request.

Total number of vulnerabilities : **1** Page : 1 (This Page)

#> echo “PAM - Pluggable Authentication Mechanism”

PAM - directives:

- auth - системийн хэрэглэгчийн таних
- account - хэрэглэгчийн үйлдлийг тодорхойлох
- session - тухайн session -ний эцэс болон төгсгөлд хийгдэх үйлдлийг тодорхойлох
- password - Нууц үг солихтой холбоотой үйлдлийг журамлах

#> echo “PAM - Pluggable Authentication Mechanism”

PAM - controls:

- required - fails after the stack is processed
- requisite - fails immediately
- sufficient - if succeeds (with no prior failures), stack succeeds
- optional - only matters if it is the only module in the stack

#> echo “PAM - Pluggable Authentication Mechanism”

```
[root@jail ~]# cat /etc/pam.d/system-auth
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        required      pam_faildelay.so delay=2000000
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     required      pam_permit.so

password    requisite     pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional      pam_systemd.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
```

#> echo “PAM - Pluggable Authentication Mechanism”

SSH bruteforce хийхээс хамгаалах

```
[root@jail ~]# cat > /etc/pam.d/sshd
#%PAM-1.0
auth            required        pam_abl.so config=/etc/security/pam_abl.conf
auth            include         system-login
account         include         system-login
password        include         system-login
session         include         system-login
```

2FA authentication

https://github.com/google/google-authenticator-libpam

Smartcard Authentication

/etc/pam.d/smartcard-auth

Log everything

session required pam_tty_audit.so enable=*

type=TTY msg=audit(11/30/2011 15:38:39.178:12763684) : tty pid=32377 uid=root

auid=matthew major=136 minor=2 comm=bash data=<up>,<ret>

#> echo “PAM - Pluggable Authentication Mechanism”

PAM can be malicious

- Log’s user password
- Set password backdoor
- Lock out users

#> man sudo

- Тухайн хэрэглэгчийн эрхээр админ түвшний үйлдлийг хийж гүйцэтгэх

- /etc/sudoers

- /usr/sbin/visudo

```
Oct  4 14:55:08 jail su: pam_tty_audit(su-l:session): changed status from 0 to 1
Oct  4 14:55:14 jail sudo: lkhagva : TTY=pts/0 ; PWD=/home/lkhagva ; USER=root ; COMMAND=/sbin/ip route show
```

#> echo “Access Control”

- UGO + RWX
- Set GID
- Set UID
- Sticky bit
- ACL
- SELinux or AppArmor

#> echo “Access Control”

```
[root@jail ~]# ls -lah /etc/
total 1.1M
drwxr-xr-x. 75 root root 8.0K Oct  4 14:01 .
dr-xr-xr-x. 17 root root  224 Sep 16 09:40 ..
-rw-------.  1 root root    0 Sep 16 09:37 .pwd.lock
-rw-r--r--.  1 root root  163 Sep 16 09:37 .updated
-rw-r--r--.  1 root root 5.0K Apr 11 04:20 DIR_COLORS
-rw-r--r--.  1 root root 5.6K Apr 11 04:20 DIR_COLORS.256color
-rw-r--r--.  1 root root 4.6K Apr 11 04:20 DIR_COLORS.lightbgcolor
-rw-r--r--.  1 root root   94 Mar 25  2017 GREP_COLORS
-rw-r--r--.  1 root root  842 Nov  6  2016 GeoIP.conf
-rw-r--r--.  1 root root  858 Nov  6  2016 GeoIP.conf.default
drwxr-xr-x.  7 root root  134 Apr 13 20:48 NetworkManager
drwxr-xr-x.  5 root root   57 Sep 16 09:37 X11
-rw-r--r--.  1 root root   16 Sep 16 09:40 adjtime
-rw-r--r--.  1 root root 1.5K Jun  7  2013 aliases
-rw-r--r--.  1 root root  12K Sep 16 09:43 aliases.db
```

#> echo “Access Control”

Set UID - Ийм флаг зоогдсон бол тухайн файл нь execute хийх үед ажиллаж буй процессийн эзэмшигчээр бус зөвхөн тухайн файлын эзэмшигчийн эрхээр ажиллана гэсэн үг.

- chmod u+s test

```
[root@jail ~]# ls -lah /bin/passwd
-rwsr-xr-x. 1 root root 28K Jun 10  2014 /bin/passwd
```

#> echo “Access Control”

Set GID - Ийм флаг зоогдсон хавтасд шинэ файл үүсэхдээ тухайн хэрэглэгчийн group биш тухайн хавтас харъяалагдах group -д оногдоно гэсэн үг.

- chmod g+s test

#> echo “Access Control”

Sticky Bit - Тухайн файлын эзэн нь зөвхөн өөрөө нэр өөрчлөх, устгах эрхтэй

- chmod o+s test

```
[root@jail ~]# ls -ld /tmp
drwxrwxrwt. 7 root root 105 Oct  4 14:53 /tmp
```

#> man setfacl

ACL - Flexible access control mechanism

- getfacl
- setfacl

Supported file systems: NFSv4, EXT3, EXT4, ZFS, HFS +

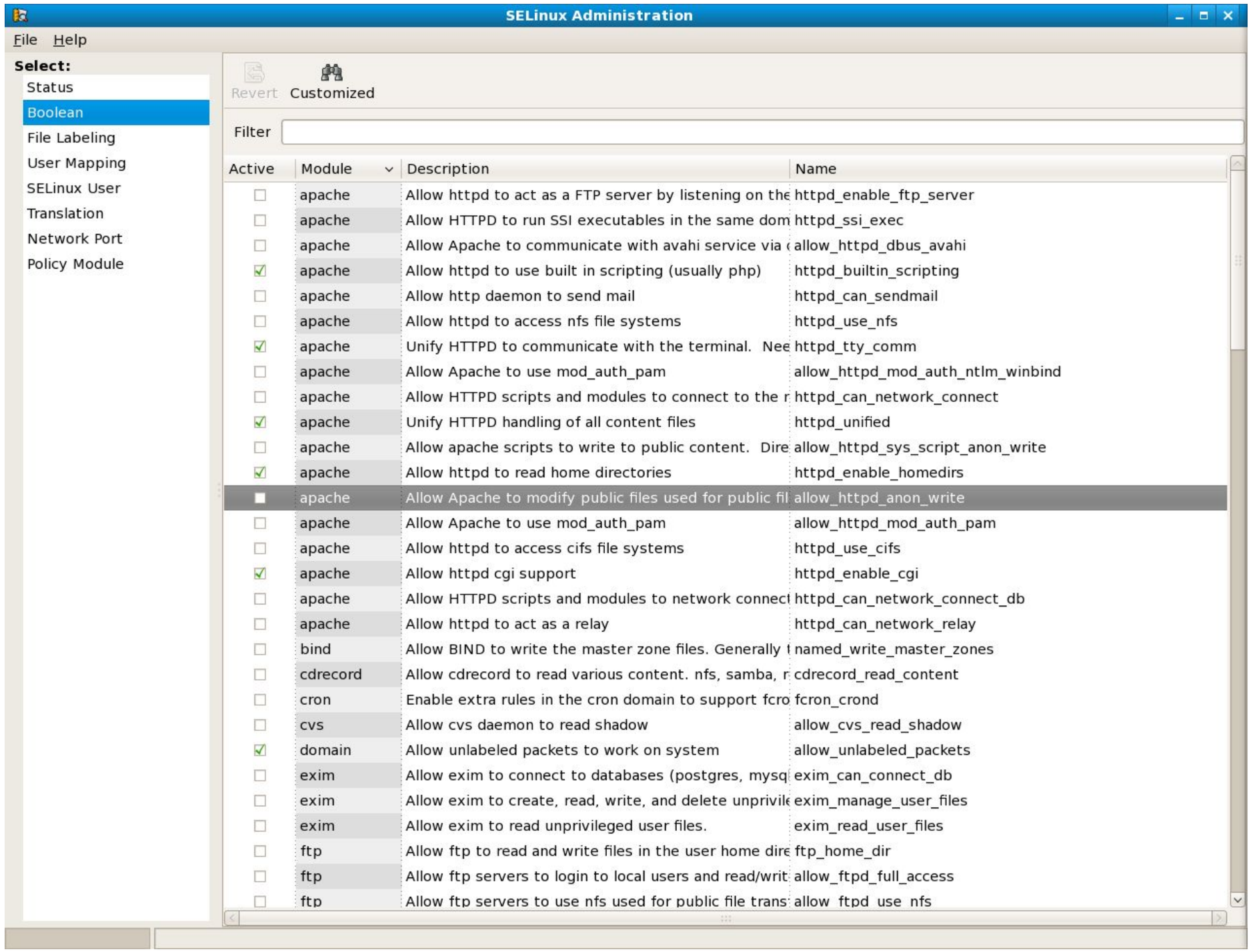
```
[root@jail ~]# setfacl -m u:lkhagva:rw prison_break.docker
[root@jail ~]# getfacl prison_break.docker
# file: prison_break.docker
# owner: root
# group: root
user::rw-
user:lkhagva:rw-
group::---
mask::rw-
other::---
```

#> man selinux

SELinux - Security-Enhanced Linux

- journald
- /var/log/audit/audit.log
- /var/log/messages
- /etc/selinux/config
- getenforce
- setenforce 1
- chcon
- ls -lZ ./

#> man selinux


SELinux Administration
File Help
Select:
Status
Boolean
File Labeling
User Mapping
SELinux User
Translation
Network Port
Policy Module
Revert
Customized
Filter
Active
Module
Description
Name
apache Allow httpd to act as a FTP server by listening on the httpd_enable_ftp_server
apache Allow HTTPD to run SSI executables in the same dom httpd_ssi_exec
apache Allow Apache to communicate with avahi service via allow_httpd_dbus_avahi
apache Allow httpd to use built in scripting (usually php) httpd_builtin_scripting
apache Allow http daemon to send mail httpd_can_sendmail
apache Allow httpd to access nfs file systems httpd_use_nfs
apache Unify HTTPD to communicate with the terminal. Nee httpd_tty_comm
apache Allow Apache to use mod_auth_pam allow_httpd_mod_auth_ntlm_winbind
apache Allow HTTPD scripts and modules to connect to the r httpd_can_network_connect
apache Unify HTTPD handling of all content files httpd_unified
apache Allow apache scripts to write to public content. Dire allow_httpd_sys_script_anon_write
apache Allow httpd to read home directories httpd_enable_homedirs
apache Allow Apache to modify public files used for public fil allow_httpd_anon_write
apache Allow Apache to use mod_auth_pam allow_httpd_mod_auth_pam
apache Allow httpd to access cifs file systems httpd_use_cifs
apache Allow httpd cgi support httpd_enable_cgi
apache Allow HTTPD scripts and modules to network connect httpd_can_network_connect_db
apache Allow httpd to act as a relay httpd_can_network_relay
bind Allow BIND to write the master zone files. Generally t named_write_master_zones
cdrecord Allow cdrecord to read various content. nfs, samba, r cdrecord_read_content
cron Enable extra rules in the cron domain to support fcro fcron_crond
cvs Allow cvs daemon to read shadow allow_cvs_read_shadow
domain Allow unlabeled packets to work on system allow_unlabeled_packets
exim Allow exim to connect to databases (postgres, mysq exim_can_connect_db
exim Allow exim to create, read, write, and delete unprivile exim_manage_user_files
exim Allow exim to read unprivileged user files. exim_read_user_files
ftp Allow ftp to read and write files in the user home dire ftp_home_dir
ftp Allow ftp servers to login to local users and read/writ allow_ftpd_full_access
ftp Allow ftp servers to use nfs used for public file trans allow_ftpd_use_nfs

#> man chroot

- Change root
- OS level isolation
- chroot is not enough
- Docker, LXC, FreeBSD jails

#> auditd

- ausearch
- aureport
- ausearch -m USER_LOGIN -sv no
- ausearch -ui bat
- ausearch -p 2317

#> sshd

- Passwordless login
- Permit root login disable
- Hosts.allow

#> echo “Iptables & firewalld”

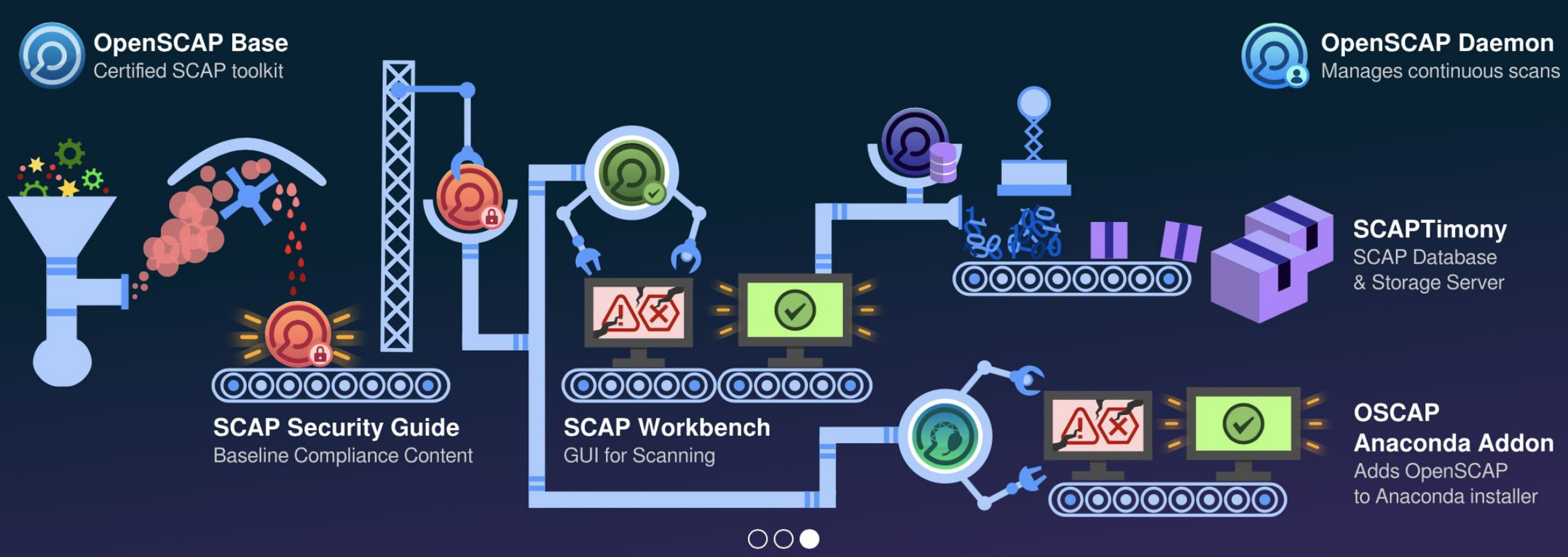
- !systemctl disable firewalld
- Iptables vs firewalld

#> echo “Kernel flags”

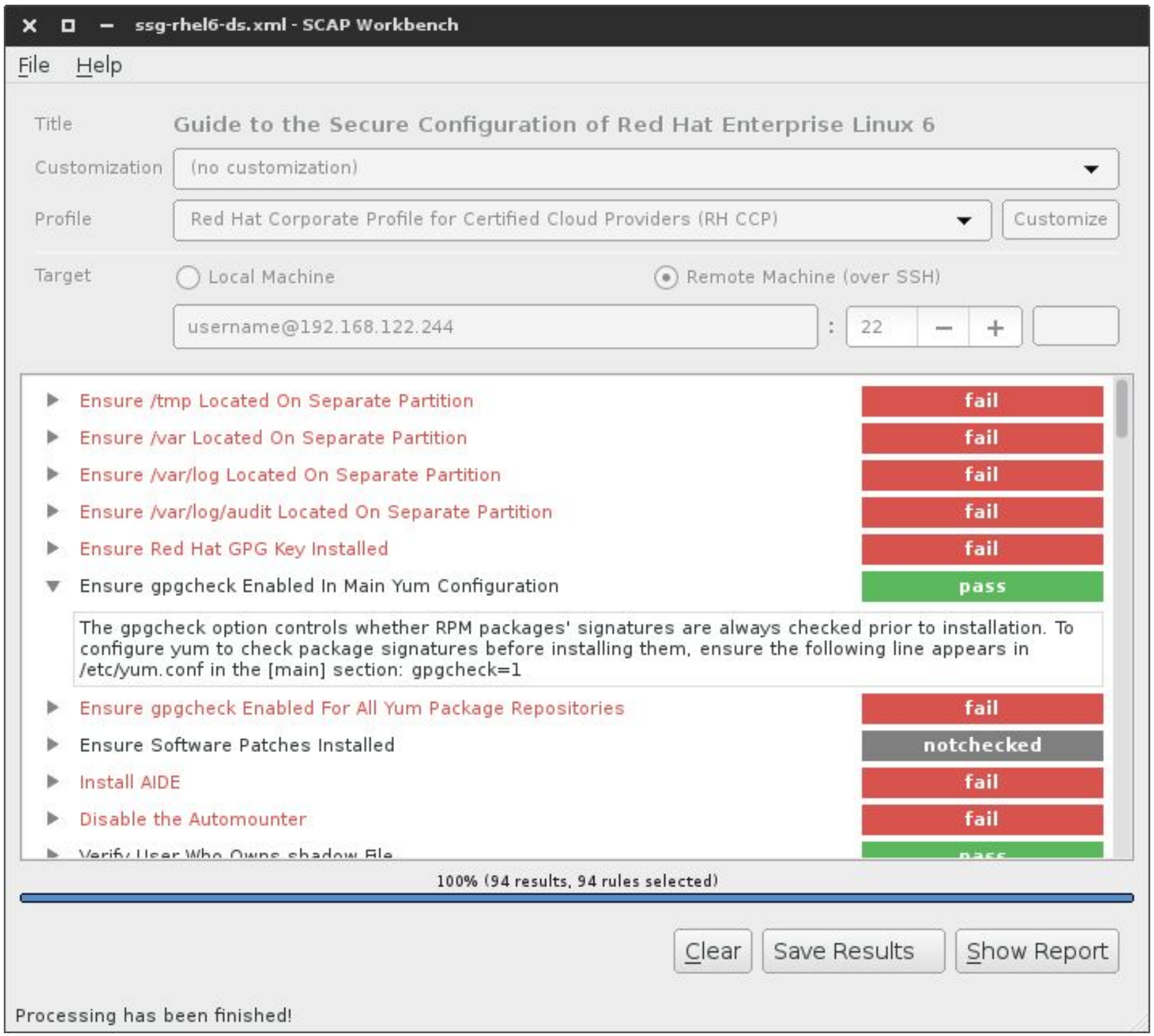
- /etc/security/limits.conf

#> whois open-scap.org

- Automated tool
- Security Compliance
- Vulnerability assessment



#> whois open-scap.org



#> *echo* “Заавар, зөвлөгөө”

- Hide service infos
- Grant mandatory access controls
- Do not turn off the firewall even if the server is behind the firewall
- SELinux, turn off and on
- Minimal packages
- Services
- Configuration
- Securing linux in scalable environment