



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/

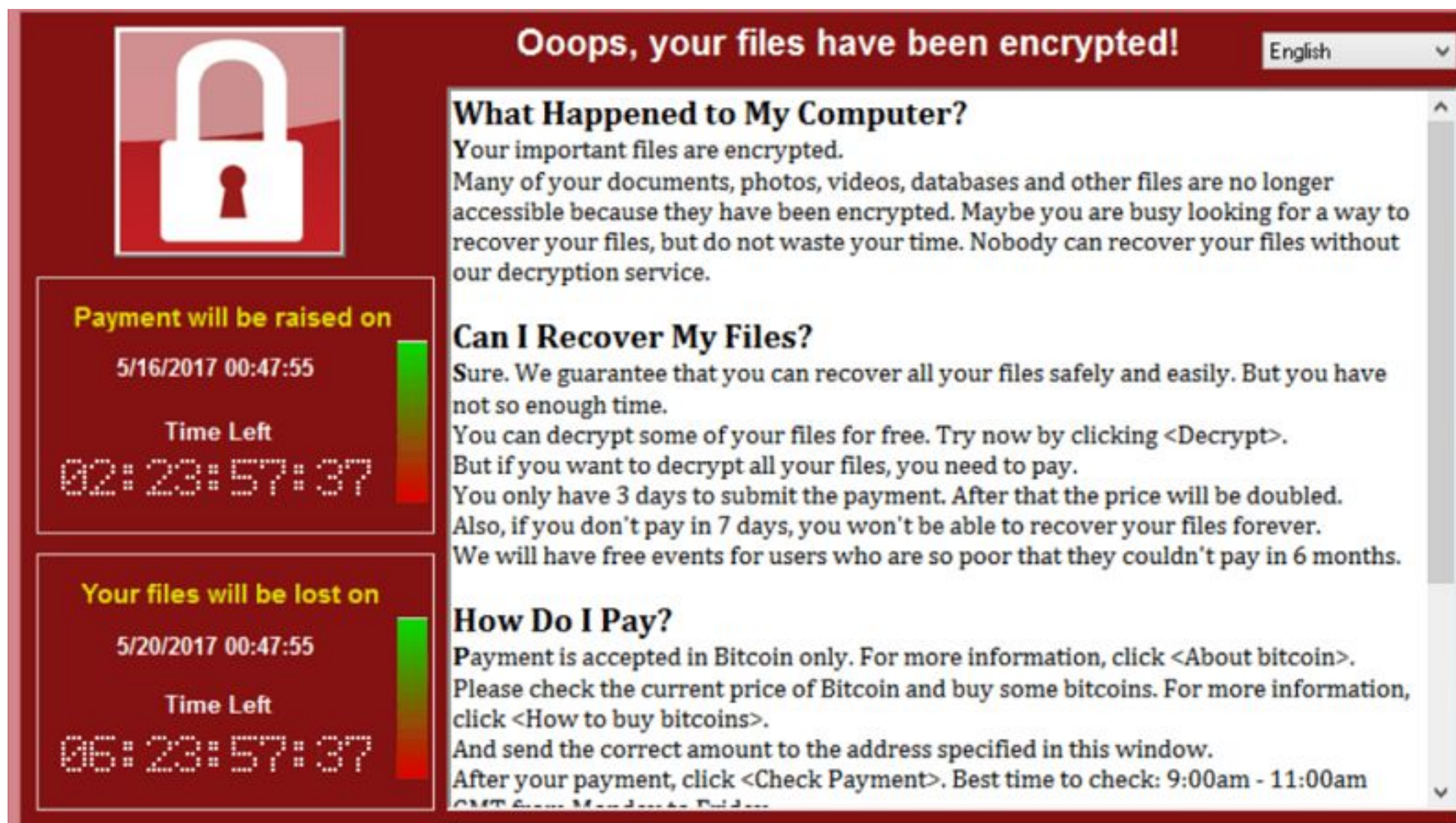
- Introduction
- Pluggable Authentication Module
- sudo
- setuid, setgid, acl, selinux
- auditd
- sshd
- iptables, firewalld
- OpenSCAP
- Заавар, зөвлөгөө

#> *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?



The screenshot shows a ransomware message window with a dark red background. At the top left is a white padlock icon. The title bar reads "Oops, your files have been encrypted!" and includes a language dropdown set to "English". The main text is as follows:

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am CMT from Mondays to Friday

On the left side, there are two red boxes with white text and a green-to-red progress bar:

- Payment will be raised on**
5/16/2017 00:47:55
Time Left
02:23:57:37
- Your files will be lost on**
5/20/2017 00:47:55
Time Left
06:23:57:37

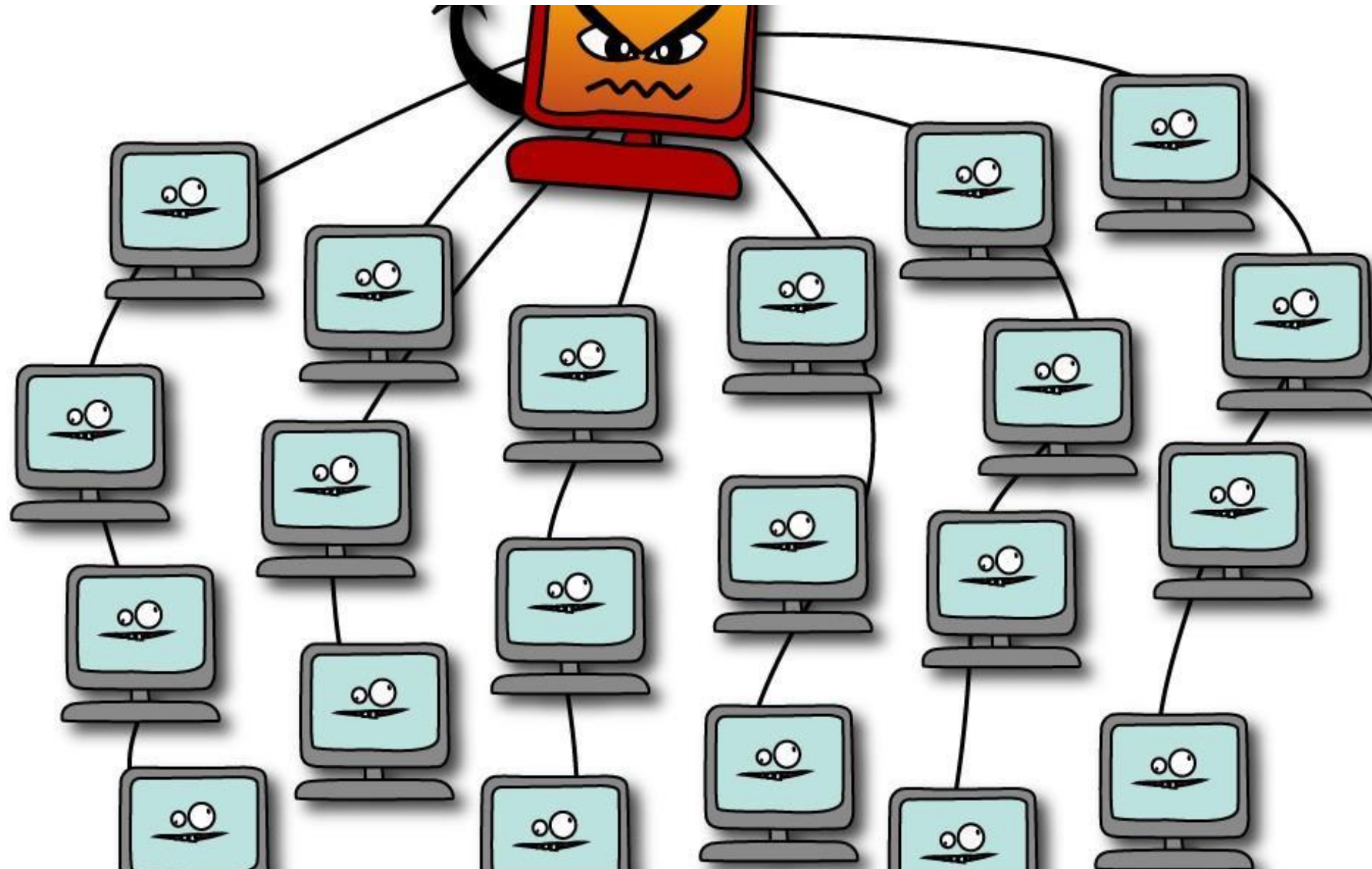
#> *systemctl disable hardening*

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 crafted 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
```

```
audit=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 +

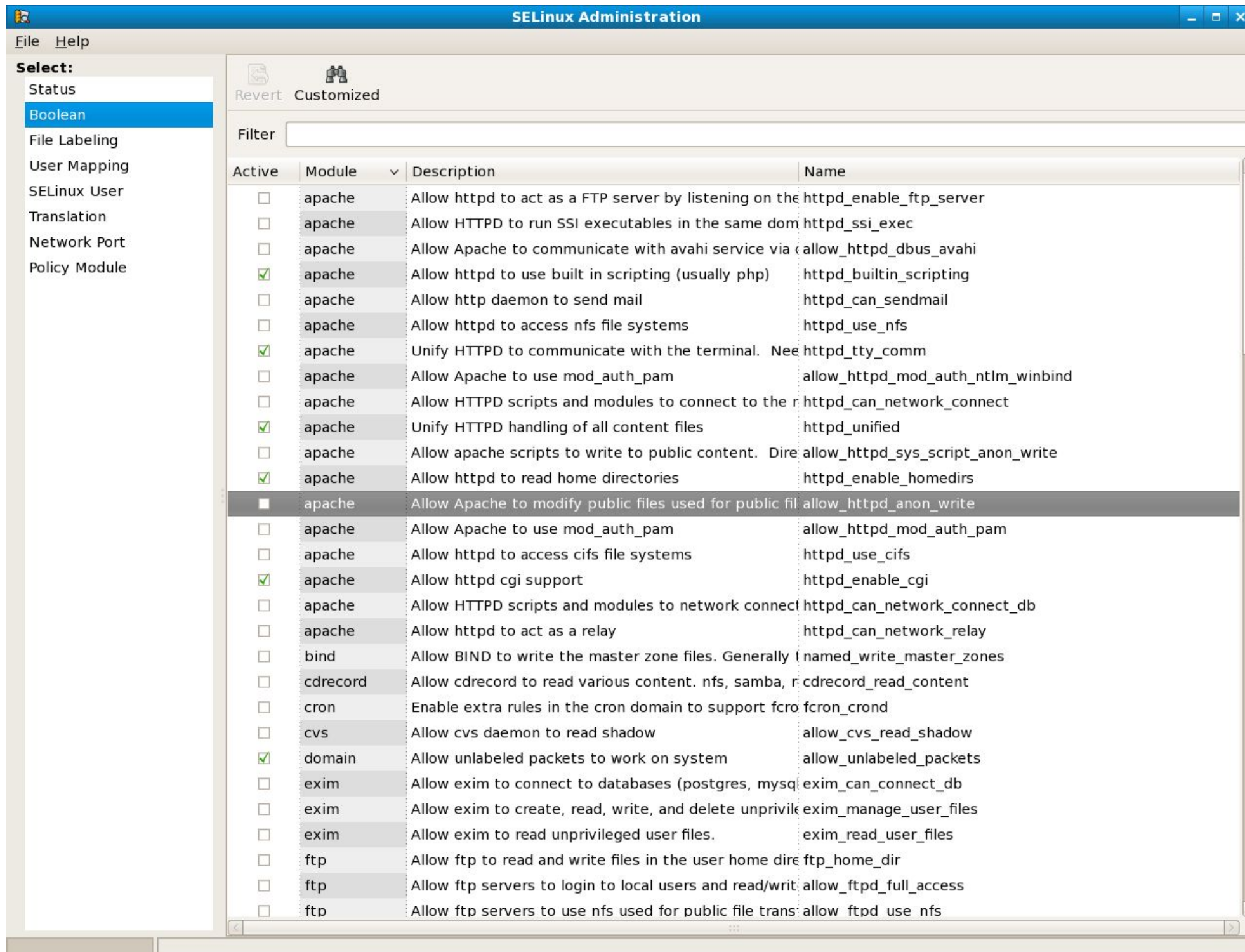
```
[root@jail ~]# setfacl -m u:lkhagva:rw prison_break.docker
[root@jail ~]# getfacl prison_break.docker
# file: prison_break.docker
# owner: root
# group: root
user::rw-
user:lkhagva:rw-
group:---
mask::rw-
other:---
```

#> 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*



The screenshot shows the SELinux Administration window. On the left, a sidebar lists various SELinux components, with 'Boolean' selected. The main area displays a table of SELinux booleans, including their status, module, description, and name. The 'allow_httpd_anon_write' boolean is highlighted.

Active	Module	Description	Name
<input type="checkbox"/>	apache	Allow httpd to act as a FTP server by listening on the	httpd_enable_ftp_server
<input type="checkbox"/>	apache	Allow HTTPD to run SSI executables in the same dom	httpd_ssi_exec
<input type="checkbox"/>	apache	Allow Apache to communicate with avahi service via	allow_httpd_dbus_avahi
<input checked="" type="checkbox"/>	apache	Allow httpd to use built in scripting (usually php)	httpd_builtin_scripting
<input type="checkbox"/>	apache	Allow http daemon to send mail	httpd_can_sendmail
<input type="checkbox"/>	apache	Allow httpd to access nfs file systems	httpd_use_nfs
<input checked="" type="checkbox"/>	apache	Unify HTTPD to communicate with the terminal. Need	httpd_tty_comm
<input type="checkbox"/>	apache	Allow Apache to use mod_auth_pam	allow_httpd_mod_auth_ntlm_winbind
<input type="checkbox"/>	apache	Allow HTTPD scripts and modules to connect to the r	httpd_can_network_connect
<input checked="" type="checkbox"/>	apache	Unify HTTPD handling of all content files	httpd_unified
<input type="checkbox"/>	apache	Allow apache scripts to write to public content. Dire	allow_httpd_sys_script_anon_write
<input checked="" type="checkbox"/>	apache	Allow httpd to read home directories	httpd_enable_homedirs
<input checked="" type="checkbox"/>	apache	Allow Apache to modify public files used for public fil	allow_httpd_anon_write
<input type="checkbox"/>	apache	Allow Apache to use mod_auth_pam	allow_httpd_mod_auth_pam
<input type="checkbox"/>	apache	Allow httpd to access cifs file systems	httpd_use_cifs
<input checked="" type="checkbox"/>	apache	Allow httpd cgi support	httpd_enable_cgi
<input type="checkbox"/>	apache	Allow HTTPD scripts and modules to network connect	httpd_can_network_connect_db
<input type="checkbox"/>	apache	Allow httpd to act as a relay	httpd_can_network_relay
<input type="checkbox"/>	bind	Allow BIND to write the master zone files. Generally t	named_write_master_zones
<input type="checkbox"/>	cdrecord	Allow cdrecord to read various content. nfs, samba, r	cdrecord_read_content
<input type="checkbox"/>	cron	Enable extra rules in the cron domain to support fcro	fcron_crond
<input type="checkbox"/>	cvs	Allow cvs daemon to read shadow	allow_cvs_read_shadow
<input checked="" type="checkbox"/>	domain	Allow unlabeled packets to work on system	allow_unlabeled_packets
<input type="checkbox"/>	exim	Allow exim to connect to databases (postgres, mysql	exim_can_connect_db
<input type="checkbox"/>	exim	Allow exim to create, read, write, and delete unprivik	exim_manage_user_files
<input type="checkbox"/>	exim	Allow exim to read unprivileged user files.	exim_read_user_files
<input type="checkbox"/>	ftp	Allow ftp to read and write files in the user home dire	ftp_home_dir
<input type="checkbox"/>	ftp	Allow ftp servers to login to local users and read/writ	allow_ftp_full_access
<input type="checkbox"/>	ftp	Allow ftp servers to use nfs used for public file trans	allow_ftp_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”

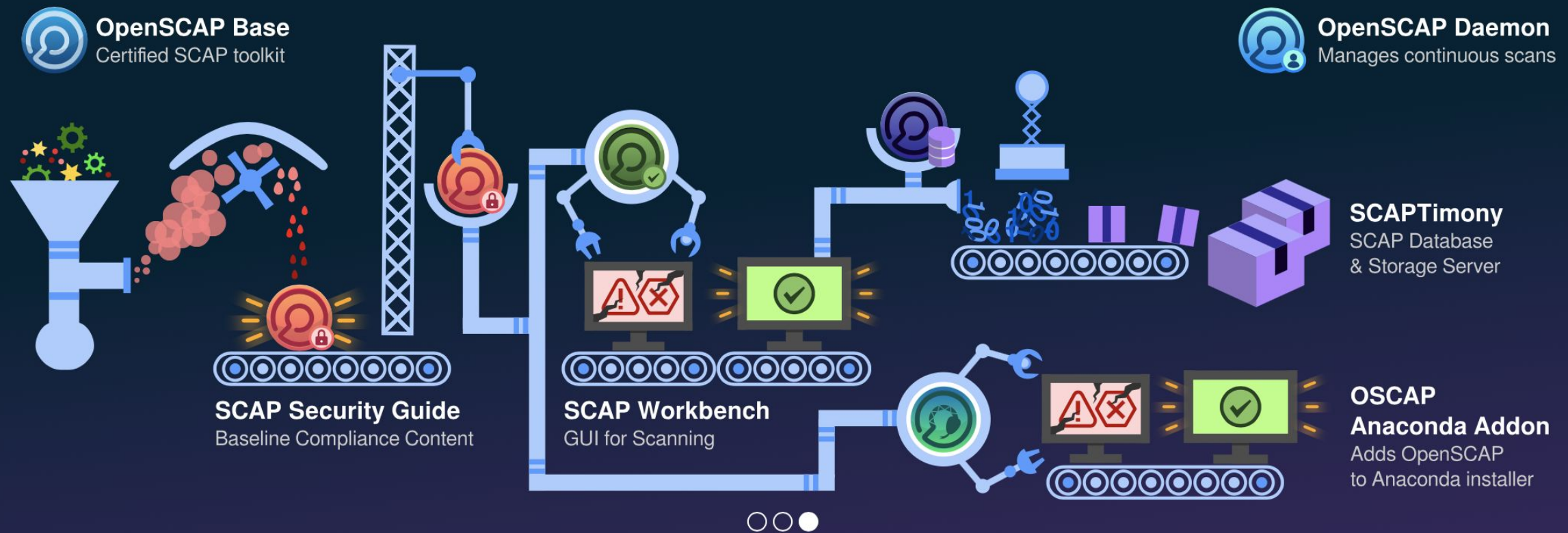
- !systemctl disable firewalld
- Iptables vs firewalld

#> echo “Kernel flags”

- /etc/security/limits.conf

#> *whois* open-scap.org

- Automated tool
- Security Compliance
- Vulnerability assessment



#> *whois* open-scap.org

The screenshot shows the SCAP Workbench interface for a security scan. The window title is "ssg-rhel6-ds.xml - SCAP Workbench". The main configuration area includes:

- Title:** Guide to the Secure Configuration of Red Hat Enterprise Linux 6
- Customization:** (no customization)
- Profile:** Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)
- Target:** Remote Machine (over SSH) with host "username@192.168.122.244" and port "22".

The scan results are displayed in a list of rules with corresponding status bars:

Rule Name	Status
Ensure /tmp Located On Separate Partition	fail
Ensure /var Located On Separate Partition	fail
Ensure /var/log Located On Separate Partition	fail
Ensure /var/log/audit Located On Separate Partition	fail
Ensure Red Hat GPG Key Installed	fail
Ensure gpgcheck Enabled In Main Yum Configuration	pass
The gpgcheck option controls whether RPM packages' signatures are always checked prior to installation. To configure yum to check package signatures before installing them, ensure the following line appears in /etc/yum.conf in the [main] section: gpgcheck=1	
Ensure gpgcheck Enabled For All Yum Package Repositories	fail
Ensure Software Patches Installed	notchecked
Install AIDE	fail
Disable the Automounter	fail
Verify User Who Owns shadow File	pass

At the bottom, a progress bar shows "100% (94 results, 94 rules selected)". Below the progress bar are buttons for "Clear", "Save Results", and "Show Report". A status message at the very bottom reads "Processing has been finished!"

#> **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