**SELinux (Security Enhanced Linux)**

Working in a few different ways:

1. MLS (Multi-Layers Security) –
2. Targeted – I am in a very specific way looking on the process and asking which process can access to which file (example: if HTTPD don’t have the permissions to go to /etc/passwd and Apache have so there is no entry)
3. Minimal – opposite from targeted

Can work in a 3 working level:

1. *setenforce [1]* = Enforcing
2. *setenforce [0]* = Permissive
3. vi /etc/sysconfig/selinux - Disabled

*getenforce =* show you which mode now

To configure disabled, we need to configure /etc/sysconfig/selinux

/etc/selinux/config – the file that show the SELinux configuration file

If we want to see the SELinux preferences, we need to enter *ls –Z* **: only the 3rd level is important!**

**If there is https\_sys\_content – there is an access from outside (httpd/apache)**

**If there is user\_tmp\_t – there is no access from outside**

*chcon –* change file follow another file *(*example*: chcon –v –reference=/var/www/html/file\_1 /var/www/html/file\_2 –* file 2 is getting permissions like file\_1)

*restorecon –* take policy follow existing SELinux policy on a file *(*example*: restorecon –RFvv /var/www/html/file\_3 )*

*semanage fcontext –* i can configure policy to specific path

(example: semanage fcontext –a –t httpd\_sys\_content\_t "/folder(/.\*)?" - change the policy and every file that created will have the 3rd field permissions context as we ask him to )

\*semanage היא פקודה קבוע בשונה מ2 הפקודות הקודמות

\*if we want to enforce existing files so we need to do the command *restorecon reset*

*Setmanage Boolean* – I can configure values to the Booleans that create SELinux policies

*getseboole –a | grep ftp* – show Booleans configurations for ftp

*setsebool ftp\_home\_dir=1* – change off to on

*semanage Boolean –l | grep ftp* – show me the details of each Boolean

if there is a problem with SELinux logs (/var/log/messages) and the syntax is a bit mess I need to install "setroubleshoot server" and it will help me to organize the syntax in the log file