**Malicious Code Protection (NIST SI-3)**

1. ClamAV shall be deployed on database server (next section) to detect and eradicate malicious code.
2. ClamAV shall be updated whenever new releases are available.
3. ClamAV shall be configured to:
4. Perform daily scans of the server and real-time scans of files from external sources as the files are downloaded, opened, or executed
5. Block and quarantine malicious code and sends alert to administrator in response to malicious code detection
6. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

**ClamAV Installation and Configuration (NIST SI-3)**

Implement the following steps on a terminal console for the desired database server:

1. sudo apt-get update
2. sudo apt-get -y install clamav-daemon
3. sudo systemctl enable clamav-daemon
4. sudo systemctl start clamav-daemon
5. $ tail /var/log/clamav/clamav.log

Response:   
Sun Jun 28 19:08:32 2020 -> Portable Executable support enabled.  
Sun Jun 28 19:08:32 2020 -> ELF support enabled.  
Sun Jun 28 19:08:32 2020 -> Mail files support enabled.  
Sun Jun 28 19:08:32 2020 -> OLE2 support enabled.  
Sun Jun 28 19:08:32 2020 -> PDF support enabled.  
Sun Jun 28 19:08:32 2020 -> SWF support enabled.  
Sun Jun 28 19:08:32 2020 -> HTML support enabled.  
Sun Jun 28 19:08:32 2020 -> XMLDOCS support enabled.  
Sun Jun 28 19:08:32 2020 -> HWP3 support enabled.  
Sun Jun 28 19:08:32 2020 -> Self checking every 3600 seconds.

1. Run a scan:

sudo clamdscan –fdpass

Response:

/home/testuser: OK

----------- SCAN SUMMARY -----------

Infected files: 0

Time: 0.015 sec (0 m 0 s)

1. Test by downloading a virus file:

wget www.eicar.org/download/eicar.com

1. Rescan:

sudo clamdscan –fdpass

Response:

/home/ubuntu/eicar.com: Win.Test.EICAR\_HDB-1 FOUND

----------- SCAN SUMMARY -----------

Infected files: 1

Time: 0.005 sec (0 m 0 s)

1. sudo mkdir /root/quarantine
2. Exclude certain directories from being scanned (all one line):

sudo printf "ExcludePath ^/proc\nExcludePath ^/sys\nExcludePath ^/run\nExcludePath ^/dev\nExcludePath ^/snap\nExcludePath ^/var/lib/lxcfs/cgroup\nExcludePath ^/root/quarantine\n" | sudo tee -a /etc/clamav/clamd.conf

1. Restart clamav-daemon:

sudo systemctl restart clamav-daemon

1. sudo su –
2. Execute clamdscan every night at 1:00 am (this is one continuous line):

echo "0 1 \* \* \* root /usr/bin/clamdscan --fdpass --log=/var/log/clamav/clamdscan.log --move=/root/quarantine /" | tee /etc/cron.d/clamdscan

1. Exit (from sudo su - )
2. Test full system scan (with quarantine file movement):

sudo /usr/bin/clamdscan --fdpass --log=/var/log/clamav/clamdscan.log --move=/root/quarantine /

Results:

--------------------------------------

/snap: Excluded

/run: Excluded

/dev: Excluded

/proc: Excluded

/sys: Excluded

/var/lib/lxcfs/cgroup: Excluded

WARNING: /var/lib/lxd/unix.socket: Not supported file type

/home/ubuntu/eicar.com: Win.Test.EICAR\_HDB-1 FOUND

/home/ubuntu/eicar.com: moved to ‘/root/quarantine/eicar.com’

/root/quarantine: Excluded

----------- SCAN SUMMARY -----------

Infected files: 1

Total errors: 1

Time: 235.497 sec (3 m 55 s)

1. Begin to enable real-time scanning:

sudo printf "OnAccessIncludePath /home\nOnAccessIncludePath /var/www\nOnAccessExcludeUname clamav\nOnAccessExcludeRootUID true" | sudo tee -a /etc/clamav/clamd.conf

1. Create a systemd file for clamonacc:

[Unit]  
Description=ClamAV On Access Scanner  
Requires=clamav-daemon.service  
After=clamav-daemon.service syslog.target network.target  
  
[Service]  
Type=simple  
User=root  
ExecStartPre=/bin/bash -c "while [ ! -S /var/run/clamav/clamd.ctl ]; do sleep 1; done"  
ExecStart=/usr/bin/clamonacc -F --config-file=/etc/clamav/clamd.conf --log=/var/log/clamav/clamonacc.log --move=/root/quarantine  
  
[Install]  
WantedBy=multi-user.target

1. Enable and start the clamonacc daemon:

sudo systemctl enable clamonacc  
sudo systemctl start clamonacc

1. Download a virus file to see if it’s automatically detected and quarantined:

wget [www.eicar.org/download/eicar.com](http://www.eicar.org/download/eicar.com)

1. See if the file was moved:

ls -l

Result:

Total: 0

1. Check the quarantine folder:

sudo ls /root/quarantine

Result:

eicar.com

1. Check the logs:

sudo tail /var/log/clamav/clamonacc.log

Result:  
--------------------------------------  
ClamInotif: watching '/home' (and all sub-directories)  
ClamInotif: watching '/var/www' (and all sub-directories)  
/home/testuser/eicar.com: Win.Test.EICAR\_HDB-1 FOUND  
/home/testuser/eicar.com: moved to '/root/quarantine/eicar.com'