Table of Contents

Secure RHEL 7

```
#Change umask
sed -i 's/022/027/g' /etc/profile
sed -i 's/002/027/g' /etc/profile

#Blacklist modules
echo "blacklist firewire-core" > /etc/modprobe.d/blacklist-firewire.conf

#Remove postfix
rpm -e postfix

#Secure SSH
sed -i "s/#AllowTcpForwarding yes/AllowTcpForwarding no/g"
/etc/ssh/sshd_config
sed -i "s/#ClientAliveCountMax 3/ClientAliveCountMax 2/g"
/etc/ssh/sshd_config
sed -i "s/#Compression delayed/Compression no/g" /etc/ssh/sshd_config
sed -i "s/#MaxAuthTries 6/MaxAuthTries 3/g" /etc/ssh/sshd_config
sed -i "s/#PermitRootLogin yes/PermitRootLogin no/g" /etc/ssh/sshd_config
sed -i "s/#AllowAgentForwarding yes/AllowAgentForwarding no/g"
/etc/ssh/sshd_config
sed -i "s/#AllowAgentForwarding yes/AllowAgentForwarding no/g"
/etc/ssh/sshd_config
sed -i "s/UseDNS yes/UseDNS no/g" /etc/ssh/sshd_config
sed -i "s/#Banner none/Banner \/etc\/issue.net/g" /etc/ssh/sshd_config
sed -i "s/#Protocol 2/Protocol 2/g" /etc/ssh/sshd_config
sed -i "s/#IgnoreRhosts yes/IgnoreRhosts yes/g" /etc/ssh/sshd_config
sed -i "s/#HostbasedAuthentication no/HostbasedAuthentication no/g"
/etc/ssh/sshd_config
sed -i "s/#PermitEmptyPasswords no/PermitEmptyPasswords no/g"
/etc/ssh/sshd_config
sed -i "s/#PermitUserEnvironment no/PermitUserEnvironment no/g"
/etc/ssh/sshd_config
sed -i "s/#LogLevel INFO/LogLevel INFO/g" /etc/ssh/sshd_config
echo "MACs hmac-sha1-etm@openssh.com,umac-64-etm@openssh.com,umac-128-
etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-
etm@openssh.com,hmac-ripemd160-etm@openssh.com,hmac-
sha1,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-
sha2-512,hmac-ripemd160" >> /etc/ssh/sshd_config
echo "Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-
gcm@openssh.com,aes256-gcm@openssh.com,chacha20-poly1305@openssh.com" >>
/etc/ssh/sshd_config
systemctl restart sshd

#Set banner
echo "  ____ ____  __  __" > /etc/issue
echo "  ____ ____  __  __" > /etc/issue.net
echo " / ___| __ )|  \/  |" >> /etc/issue
echo " / ___| __ )|  \/  |" >> /etc/issue.net
```

```
echo "| |  _|  _ \| |\/| | Este equipo esta  restringido para  el uso" >>
/etc/issue
echo "| |  _|  _ \| |\/| | Este equipo esta  restringido para  el uso" >>
/etc/issue.net
echo "| |_| | |_) | |  | | exclusivo del personal autorizado por GBM." >>
/etc/issue
echo "| |_| | |_) | |  | | exclusivo del personal autorizado por GBM." >>
/etc/issue.net
echo " \____|____/|_|  |_|" >> /etc/issue
echo " \____|____/|_|  |_|" >> /etc/issue.net

#Secure kernel parameters
echo "net.ipv4.tcp_timestamps = 0" >> /etc/sysctl.conf
echo "kernel.dmesg_restrict = 1" >> /etc/sysctl.conf
echo "kernel.kptr_restrict =  2" >> /etc/sysctl.conf
echo "kernel.sysrq = 0" >> /etc/sysctl.conf
echo "net.ipv4.conf.all.accept_redirects = 0" >> /etc/sysctl.conf
echo "net.ipv4.conf.all.log_martians = 1" >> /etc/sysctl.conf
echo "net.ipv4.conf.all.send_redirects = 0" >> /etc/sysctl.conf
echo "net.ipv4.conf.default.send_redirects = 0" >> /etc/sysctl.conf
echo "net.ipv4.conf.default.accept_redirects = 0" >> /etc/sysctl.conf
echo "net.ipv4.conf.default.log_martians = 1" >> /etc/sysctl.conf
echo "net.ipv6.conf.all.accept_redirects = 0" >> /etc/sysctl.conf
echo "net.ipv6.conf.default.accept_redirects = 0" >> /etc/sysctl.conf
echo "net.ipv6.conf.all.accept_ra = 0" >> /etc/sysctl.conf
echo "net.ipv6.conf.default.accept_ra = 0" >> /etc/sysctl.conf
echo "net.ipv4.conf.all.secure_redirects = 0" >> /etc/sysctl.conf
echo "net.ipv4.conf.default.secure_redirects = 0" >> /etc/sysctl.conf
sysctl -p

#Secure RPC
echo "rpcbind: 192.168.122.14" >> /etc/hosts.allow
echo "rpcbind: ALL" >> /etc/hosts.deny

#Secure /dev/shm
echo "tmpfs                   /dev/shm                tmpfs
defaults,nodev,nosuid,noexec 0 0" >> /etc/fstab

#Secure cron
chmod 600 /etc/crontab /etc/cron.hourly /etc/cron.daily /etc/cron.weekly
/etc/cron.monthly
chmod 700 /etc/cron.d

#Secure rsyslog.conf
chmod 600 /etc/rsyslog.conf
```

Tools

- https://cisofy.com/lynis/
- http://rkhunter.sourceforge.net/

- https://github.com/XalfiE/Nix-Auditor