Nova's Calculated, Comprehensive Sorcery Guide

Users:

```
# remove users besides root that are UID 0
# audit sudo/wheel group
# remove Unauthorized users

# Run below script

getent passwd {1000..2000} | cut -d: -f1 > user.txt
while read u; do
      echo '$u:<password>' | chpasswd
     chage -d 0 -m 7 -M 90 -I 30 -W 14
done<user.txt

# Run below commands
passwd -l bin
passwd root
```

Account Policies:

In /etc/login.defs
PASS_MAX_DAYS 90
PASS_MIN_DAYS 7
PASS_WARN_AGE 14
ENCRYPT_METHOD SHA512 # Change to YESCRYPT for U22 and F36

Configure the PAM policies:

In common-auth:

```
Ubuntu 20 and earlier:
auth  required                        pam_faildelay.so delay=4000000
auth  required                        pam_tally2.so deny=3 onerr=fail audit
no_log_info even_deny_root

Ubuntu 22 and after:
auth    required              pam_faillock.so preauth audit silent deny=3
unlock_time=600 fail_interval=900 even_deny_root
auth  required                pam_faildelay.so delay=4000000
auth  [success=1 default=ignore]    pam_unix.so
```

```
auth    [default=die]              pam_faillock.so  authfail audit deny=3
unlock_time=600 fail_interval=900 even_deny_root
auth    sufficient                 pam_faillock.so  authsucc audit deny=3
unlock_time=600 fail_interval=900 even_deny_root
```

In common-password

```
password    requisite   pam_pwquality.so retry=3 difok=8 minlen=15
dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1 minclass=4 maxrepeat=3
maxclassrepeat=5 gecoscheck=1 dictcheck=1 usercheck=1 usersubstr=3
enforcing=1 enforce_for_root

password    requisite   pam_pwhistory.so remember=5 use_authtok retry=3
authtok_type=secure enforce_for_root

password    [success=1 default=ignore]    pam_unix.so obscure use_authtok
try_first_pass yescrypt shadow rounds=65536
```

> Check gdm-password and sssd-shadowutils for differences from the default

Local Policies

```
# sysctl.conf

https://raw.githubusercontent.com/konstruktoid/hardening/master/misc/sysctl
.conf

And add kernel.unprivileged_userns_clone=0
```

Misc:

```
echo >/etc/securetty

AllowRoot=false and DisallowTCP=true in /etc/gdm3/custom.conf

lightdm --show-config # show current lightdm confs

# Lightdm configs to add or change
greeter-hide-users=true
greeter-show-manual-login=true
greeter-show-remote-login=false
allow-guest=false
xserver-allow-tcp=false
```

```
# Add GRUB bootloader password and remove any weird boot parameters like
noexec=off

/etc/host.conf
nospoof on

# Check /etc/sudoers, /etc/sudoers.d/* for any “bad” lines. You can also
check /etc/polkit-1/ too.
```

Packages & Service auditing

```
# Show manually installed packages and remove games, hacking tools, and
extraneous services:

apt-mark showmanual


# Misc.
   -  Enable and start apparmor
   -  Enable and start rsyslog
   -  Enable and start systemd-journald
   -  $ apt purge rsync # unless this removes mysql

# Check snaps
$ snap list
```

Permissions

```
# 0600 /boot/grub/grub.cfg
# 0600 /etc/shadow
# 0644 /etc/passwd
# 0644 /etc/group
# 0644 /path/to/service/configuration/file
# 0755 /path/to/file/share
# Make sure /var/lib/mysql is not world readable
# Remove SUID/SGID permissions from binaries that are not supposed to have
it
# SSH host keys are not world readable




/etc/fstab
```

```
none     /tmp     tmpfs     rw,noexec,nosuid,nodev     0     0
proc  /proc       proc  defaults,hidepid=2      0     0 # might be
hidepid=invisible for versions >18

$ mount -o rw,noexec,nodev,nosuid /tmp
$ mount -o remount,rw,hidepid=invisible /proc
```

Application Security

```
   -  Firefox, just do the settings
   -  Thunderbird, just do the settings
   -  Apache2
         -  ServerSignature Off
         -  ServerTokens Prod
         -  TraceEnable Off
         -  FileETag None
         -  LogLevel warn
   -  PHP
         -  file_uploads = Off
         -  expose_php = Off
         -  display_errors = Off
         -  allow_url_fopen = Off
         -  session.use_strict_mode = 1
         -  Disable_functions = <use this>
   -  Samba
         -  min protocol = SMB3_00
         -  max protocol = SMB3_00
         -  protocol = SMB3_00
         -  client min protocol = SMB3_00
         -  client max protocol = SMB3_00
         -  server min protocol = SMB3_00
         -  server max protocol = SMB3_00
         -  restrict anonymous = 2
         -  null passwords = no
         -  encrypt passwords = yes
         -  client ntlmv2 auth = no
         -  ntlm auth = no
   -  MySQL
         -  bind-address=127.0.0.1
         -  # remove any skip-grant-tables
         -  symbolic-links=0
         -  local-infile=0
         -  user=mysql
         -  # Uncomment all SSL lines
   -  SSH
         -  PermitRootLogin no
```

```
        -  PermitEmptyPasswords no
        -  X11Forwarding no
        -  PermitUserEnvironment no
   -  Nginx
        -  server_tokens off;
        -  add_header X-XSS-Protection "1; mode=block";
        -  add_header Content-Security-Policy "default-src 'self' http:
           https: data: blob: 'unsafe-inline'" always;
   -  VSFTPD
        -  write_enable=NO/YES
        -  pasv_promiscuous=NO
        -  port_promiscuous=NO
        -  chroot_local_user=NO/YES
   -  Proftpd
        -  ServerIdent                    off
        -  # Remove /etc/proftpd/conf.d/anonymous.conf
        -  User                      proftpd
        -  TLSengine                 on
   -  PureFTPD
        -  echo "2" > /etc/pure-ftpd/conf/TLS
        -  echo "no" > /etc/pure-ftpd/conf/AnonymousOnly
        -  echo "yes" > /etc/pure-ftpd/conf/NoAnonymous
   -  Postgres
        -  SSL enabled
        -  Reject all non-local connection requests without SSL
        -  require authentication for all connections
        -  configured to log connections
        -  Do not map any user to the postgres account
   -  OpenVPN
        -  Configure to run as NOT root
        -  Enable logging
   -  Squid
        -  Disable Via headers
        -  Disable X-Forwarded-For headers
        -  Disable SNMP
```

Backdoors/Malware/Prohibited files

```
$ find / -iname “*.mp3” # do this for .csv, .zip, .tar.gz, .gz, .tgz

# also look for hidden files

# If there is a webroot, search for phpinfo() files and webshells

Common backdoors:
/var/spool/cron/crontabs/*
Malicious systemd services
```