Installation, Configuration et Utilisation de Squid sur Ubuntu

Dans le cadre de ce projet, nous avons entrepris l'installation, la configuration et l'utilisation de Squid sur une machine U buntu. Squid est un serveur proxy open source qui offre diverses fonctionnalités telles que la mise en cache, le filtrage du conte n u web, et la gestion des accès au réseau. L'objectif principal de ce projet est de fournir un service de proxy fiable et sécurisé, capable de gérer l'historique de navigation des utilisateurs ainsi que de bloquer l'accès à des sites spécifiques.

Installation de Squid

Nous avons débuté par l'installation de Squid en utilisant le gestionnaire de paquets d'Ubuntu.

Configuration de Squid

Une fois l'installation terminée, nous avons procédé à la configuration de Squid. Le fichier de configuration principal de Sq uid se trouve dans `/etc/squid/squid.conf`. Voici quelques directives clés que nous avons ajustées dans ce fichier :

Port d'écoute: Nous avons spécifié le port sur lequel Squid écoutera les requêtes entrantes.

Politiques d'accès: Nous avons défini les politiques d'accès pour contrôler les autorisations des clients.

Filtrage du contenu: Nous avons configuré des listes de contrôle d'accès pour permettre ou bloquer l'accès à certains sites web.

Mise en cache: Nous avons configuré les paramètres de mise en cache pour améliorer les performances en stockant localement les données web fréquemment demandées.

Affichage de l'historique de Navigation

Pour suivre l'historique de navigation des clients, nous avons utilisé l'outil d'analyse de journal de Squid. Les journaux de Squid sont généralement situés dans /var/log/squid/access.log. Nous avons mis en place des scripts ou utilisé des outils d'analyse de journaux pour extraire et visualiser l'historique de navigation.

Blocage de Sites Sélectionnés

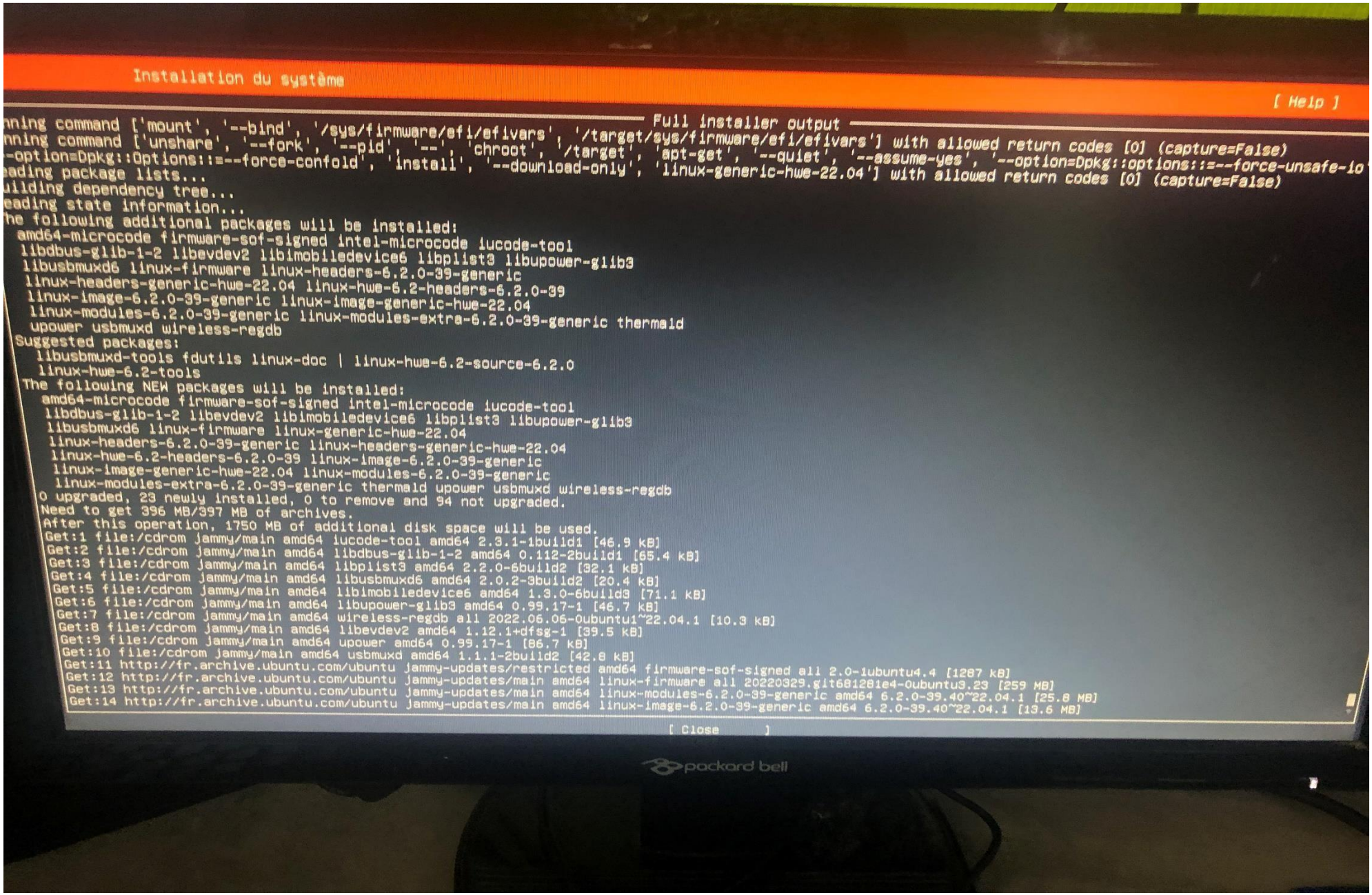
Pour bloquer l'accès à des sites spécifiques, nous avons utilisé les listes de contrôle d'accès (ACL) dans la configuration d e Squid. Nous avons défini des règles pour bloquer les requêtes provenant des clients vers les sites web indésirables. Cela peut être fait en spécifiant les adresses IP des sites à bloquer ou en utilisant des expressions régulières pour les URLs.

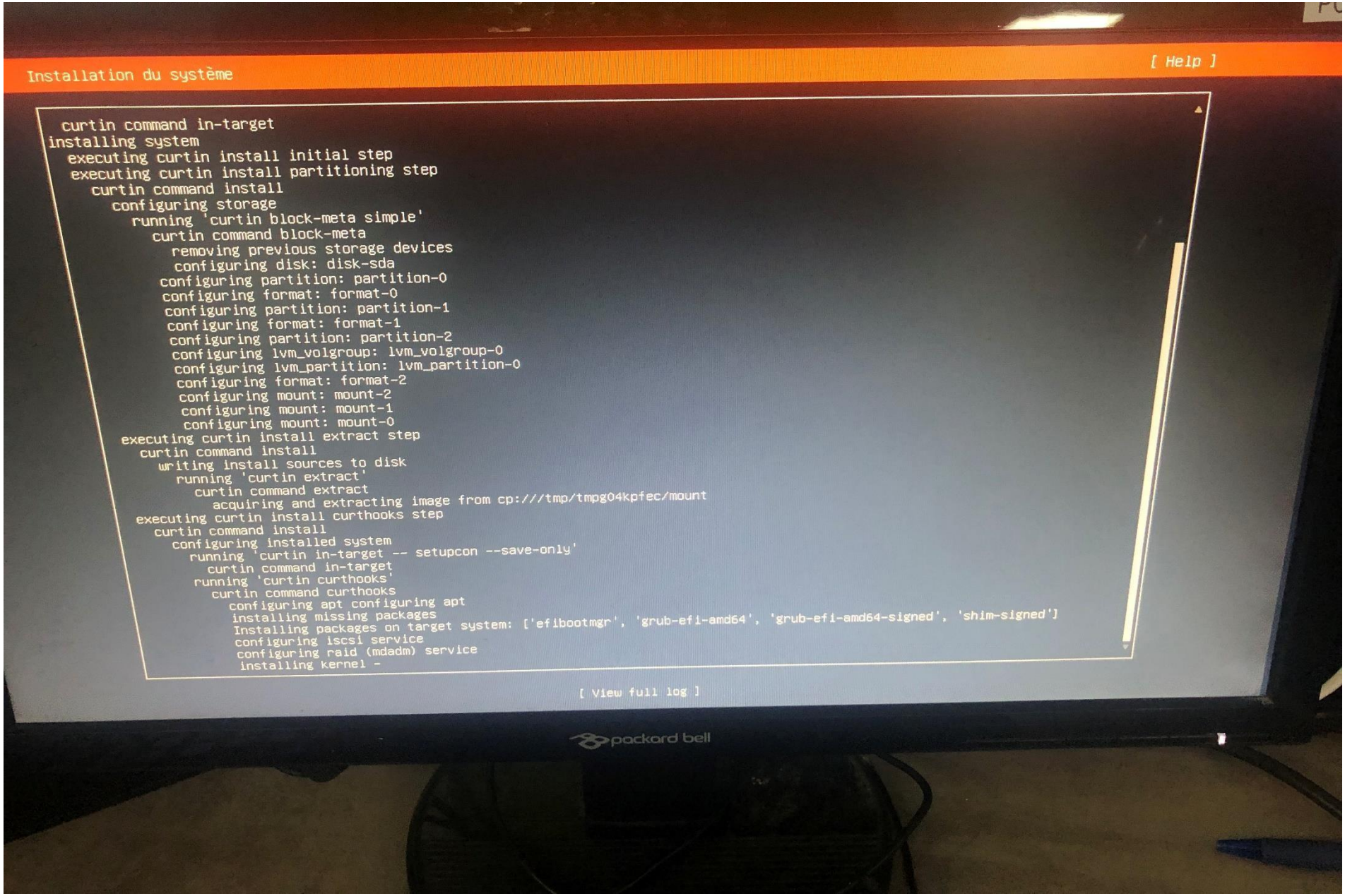
Ce projet nous a permis de mettre en place un serveur proxy fonctionnel en utilisant Squid sur Ubuntu. Nous avons appris à in staller, configurer et utiliser Squid pour fournir un accès contrôlé à internet, en suivant les étapes mentionnées ci -dessus. En outre, nous avons mis en place des fonctionnalités telles que la gestion de l'historique de navigation des clients et le blocage sélectif des sites web

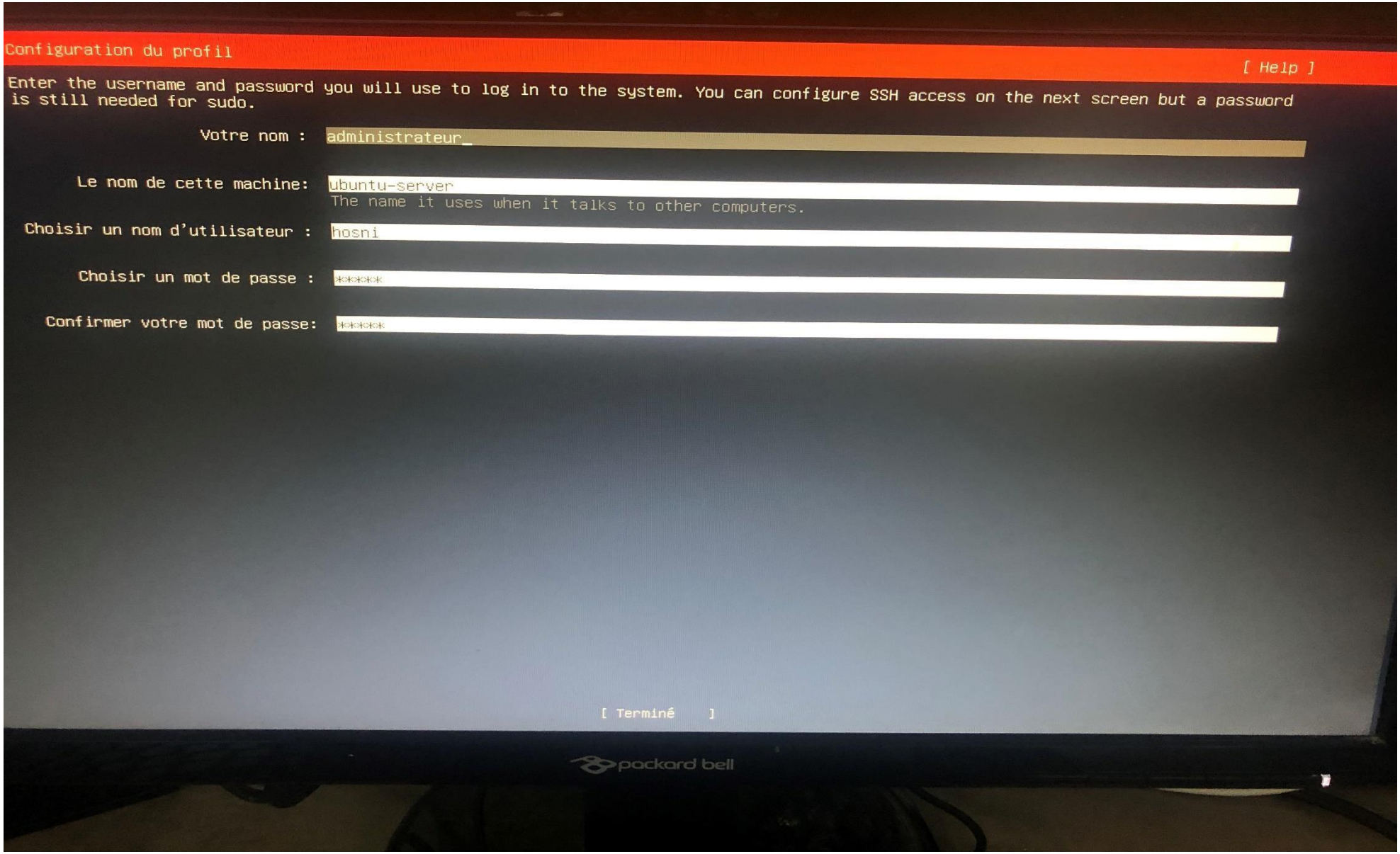
pour assurer la sécurité et la conformité aux politiques d'utilisation du réseau. Ce projet fournit une base solide pour la gestion des services proxy dans un environnement Ubuntu.

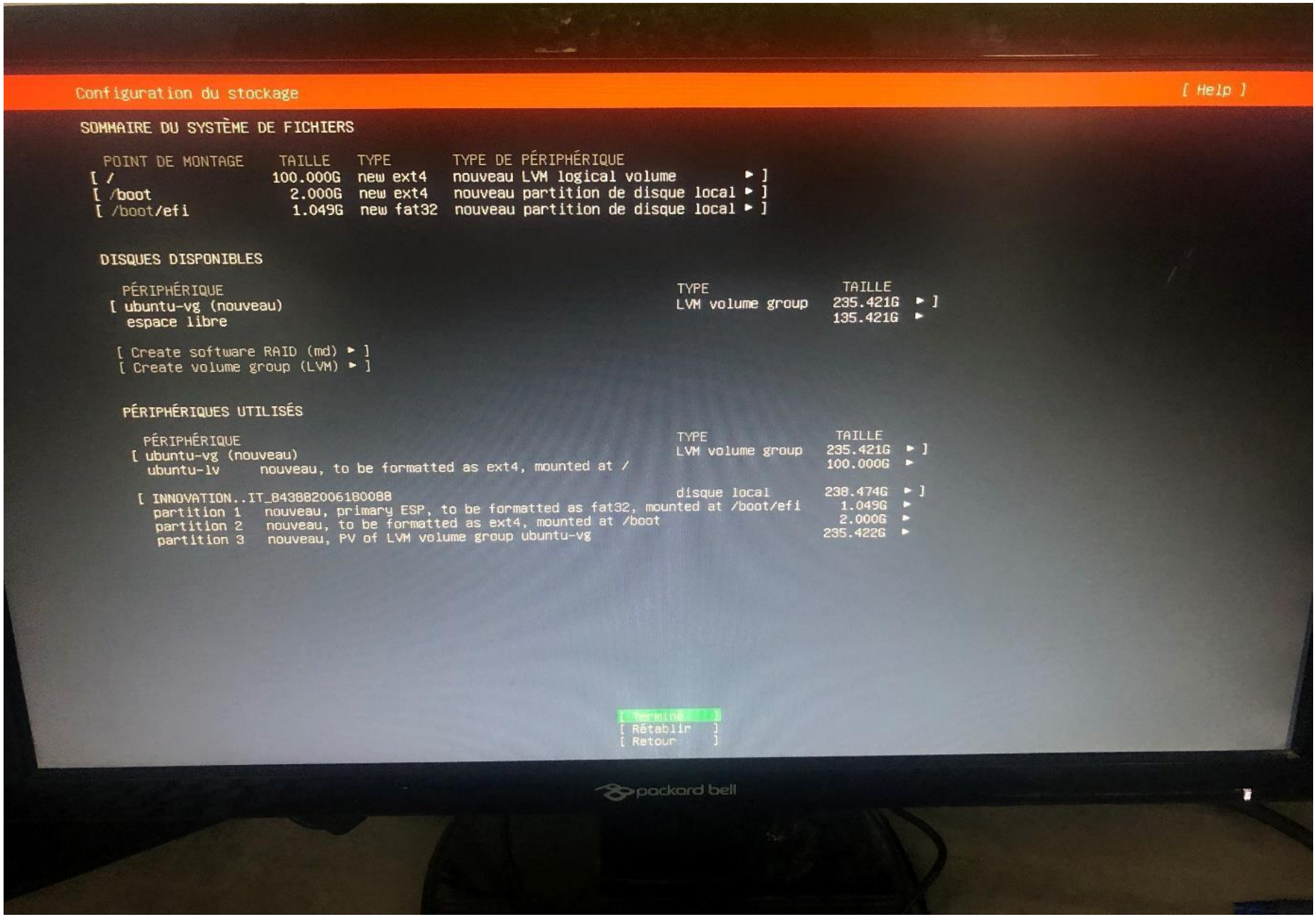

dresses
adresses
tions
2.168.2.2] PC1
2.168.2.4] PC3
2.168.2.6] PC5
92.168.2.3] PC2
92.168.2.5] PC4
92.168.2.8] PC7
92.168.2.9] PC8
192.168.2.7] PC6
192.168.2.10] PC9
192.168.2.14] PC13
[192.168.2.17] PC16
[192.168.2.18] ADMIN
[192.168.2.16] PC15
[192.168.2.12] PC11
[192.168.2.11] PC10
[192.168.2.30] 3020-WIN10
[192.168.2.15] PC14
[192.168.2.13] PC12
[192.168.2.65] Archer_C50
[192.168.2.253] ubuntu-server
Options d'étendue
Stratégies
tégies
res
192.168.2.38 31/12/2023 10:26:48 DHCP 34415d32f... Accès complet
192.168.2.39 31/12/2023 10:21:34 DHCP 5e37b2ee3... Accès complet
192.168.2.40 23/12/2023 08:56:50 DHCP 42abc0170... Accès complet
192.168.2.41 30/12/2023 16:46:43 DHCP c2cf8bf37... Accès complet
192.168.2.43 LAPTOP-OALLDLF8 23/12/2023 11:47:43 DHCP d8c0a63fe... Accès complet
192.168.2.44 31/12/2023 08:49:42 DHCP 9621db2b... Accès complet
192.168.2.45 31/12/2023 10:44:28 DHCP 34415d32e... Accès complet
192.168.2.46 31/12/2023 08:37:38 DHCP 3ecfdc403... Accès complet
192.168.2.47 AirdeBouchra2 23/12/2023 11:16:24 DHCP 50de06b9... Accès complet
192.168.2.48 23/12/2023 11:48:51 DHCP 0a4040639... Accès complet
192.168.2.49 30/12/2023 13:33:16 DHCP 34415da7... Accès complet
192.168.2.50 7G0325DPAJDAC5D 02/01/2024 10:53:04 DHCP 6c1c71f54... Accès complet
192.168.2.51 31/12/2023 09:00:56 DHCP 34415d32e... Accès complet
192.168.2.52 Galaxy-A22-5G 26/12/2023 09:18:02 DHCP 12578f829... Accès complet
192.168.2.53 21/01/2024 17:44:06 DHCP d037452a... Accès complet
192.168.2.54 26/12/2023 13:43:27 DHCP 7a043f9a6... Accès complet
192.168.2.56 31/12/2023 09:55:59 DHCP 34415d332... Accès complet
192.168.2.57 Galaxy-Note10-de-... 01/01/2024 10:09:09 DHCP a648999a9... Accès complet
192.168.2.58 S20-FE-de-No-name 27/12/2023 11:32:58 DHCP da5e5fcfd... Accès complet
192.168.2.60 27/12/2023 16:40:08 DHCP 00e04cc4d... Accès complet
192.168.2.61 01/01/2024 11:11:02 DHCP 720ae1db... Accès complet
192.168.2.62 01/01/2024 14:41:34 DHCP 2605f81ffd... Accès complet
192.168.2.63 LAPTOP-181ODS9D 01/01/2024 15:06:56 DHCP 5c3a45c31... Accès complet
192.168.2.64 DESKTOP-25TSCP7 02/01/2024 10:19:48 DHCP 30e171259... Accès complet
192.168.2.65 Archer_C50 Réservation (active) Aucun 3c846aa62... Accès complet
192.168.2.66 03/01/2024 11:03:13 DHCP 106530261... Accès complet
192.168.2.68 pc4nv.hanned.lan 22/01/2024 08:51:01 DHCP b083fe9b2... Accès complet
192.168.2.76 HCVR 02/01/2024 08:48:20 DHCP 4c11bf788... Accès complet
192.168.2.110 HCVR 22/01/2024 10:21:46 DHCP 14a78b662... Accès complet
192.168.2.124 4EMEA.hanned.lan 22/01/2024 11:18:23 DHCP 6451063e4... Accès complet
192.168.2.129 4eme.hanned.lan 22/01/2024 09:34:56 DHCP 989096c1a... Accès complet
192.168.2.131 31/12/2023 10:02:16 DHCP 08119657f... Accès complet
192.168.2.132 31/12/2023 09:08:15 DHCP a08869fc8... Accès complet
192.168.2.133 01/01/2024 13:59:27 DHCP ea7f71c68... Accès complet
192.168.2.137 6eB.hanned.lan 22/01/2024 11:17:54 DHCP b083fe7ec... Accès complet
192.168.2.138 5e.hanned.lan 22/01/2024 10:07:07 DHCP 64006a93b... Accès complet
192.168.2.156 Khoumba 27/12/2023 09:20:00 DHCP 202b20a19... Accès complet
192.168.2.159 4è.hanned.lan 22/01/2024 10:15:23 DHCP b083fe9e0... Accès complet
192.168.2.166 direction.hanned.lan 03/01/2024 10:17:11 DHCP b083fe9df... Accès complet
192.168.2.180 31/12/2023 09:11:52 DHCP ce6b35f8c... Accès complet
192.168.2.253 ubuntu-server Réservation (inactive) Aucun b6220feb0... Accès complet
N/D

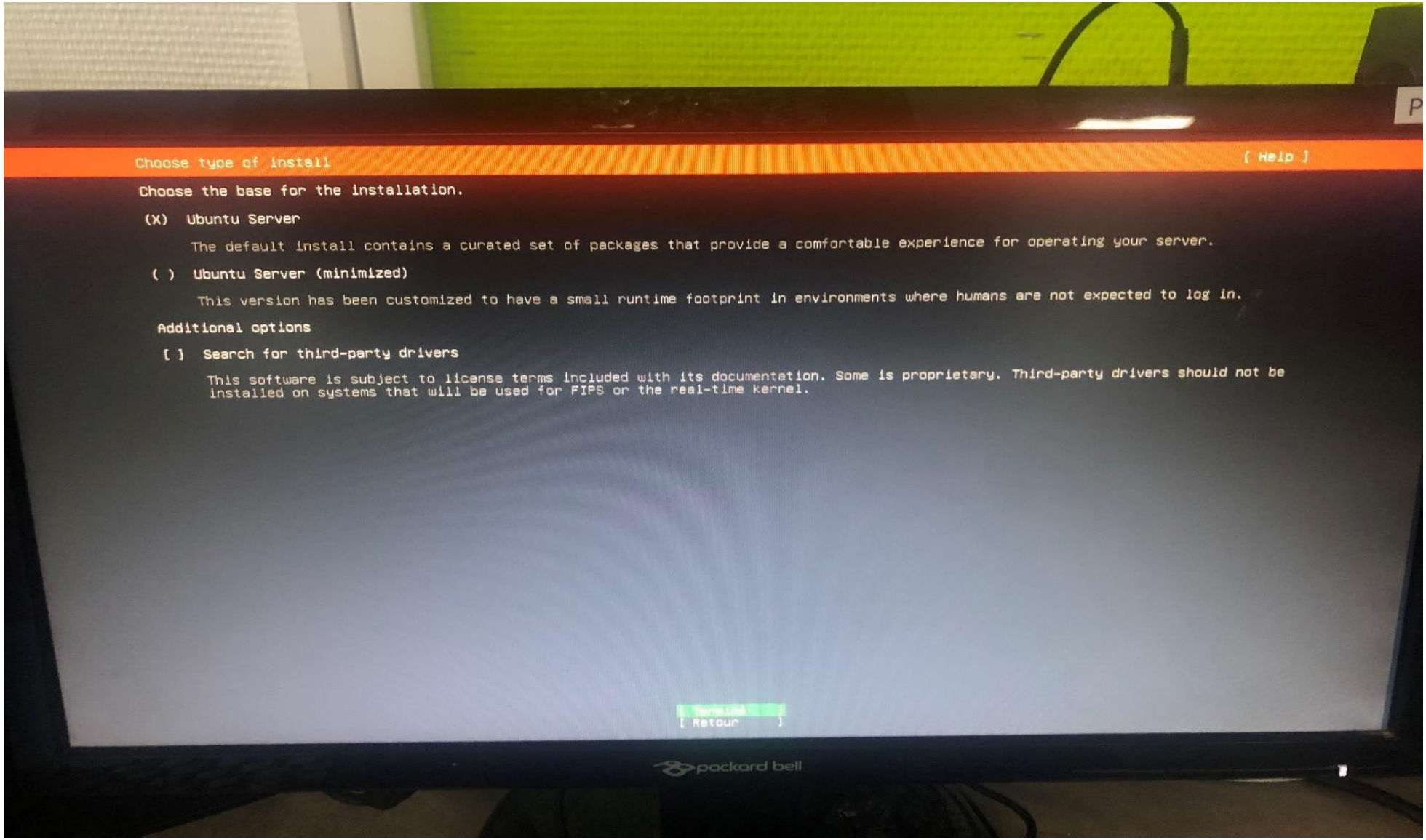
ProDesk
HEWLETT-PACKARD

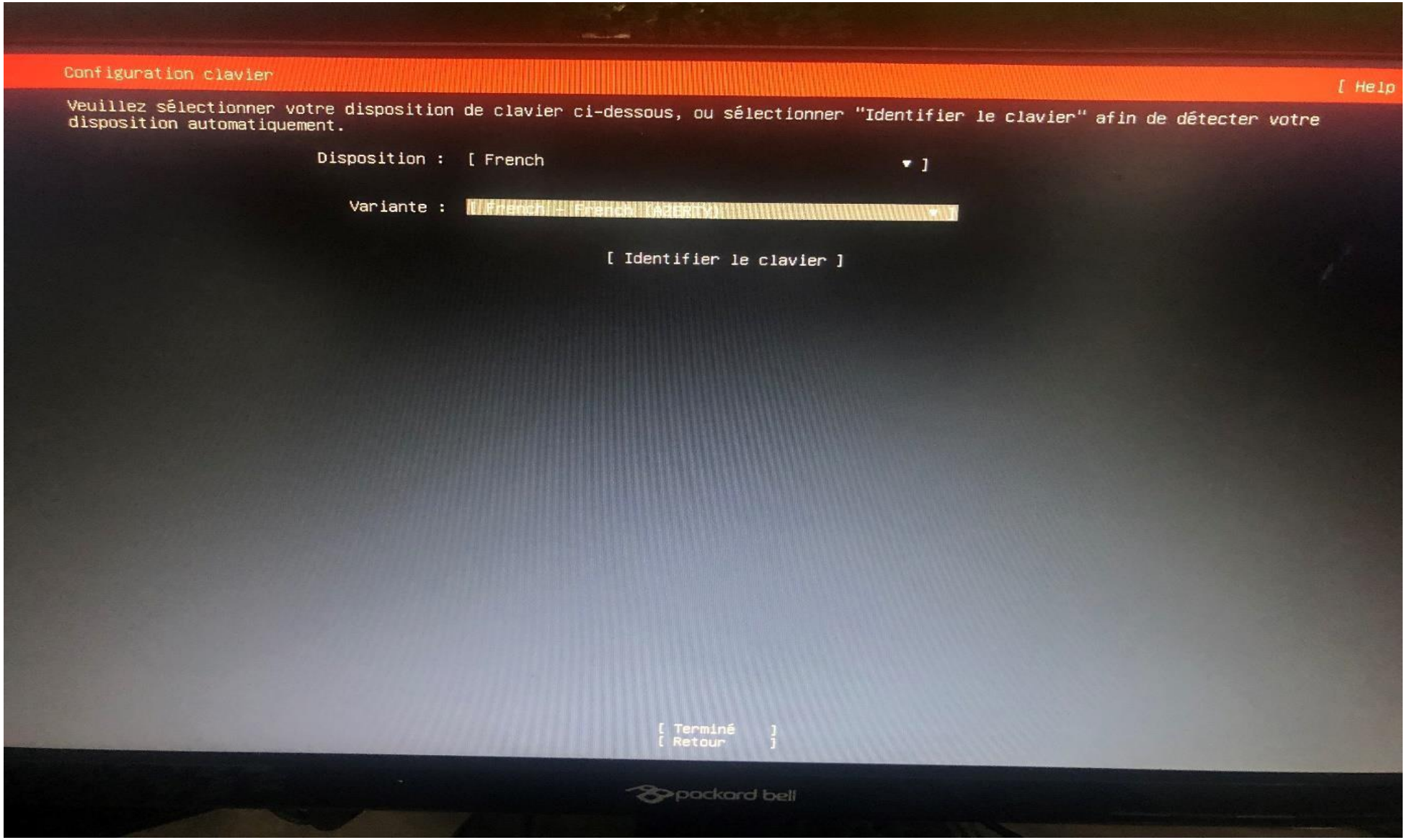

Installation du système
[Help]
Full installer output
nning command ['mount', '--bind', '/sys/firmware/efi/efivars', '/target/sys/firmware/efi/efivars'] with allowed return codes [0] (capture=False)
nning command ['unshare', '--fork', '--pid', '--', 'chroot', '/target', 'apt-get', '--quiet', '--assume-yes', '--option=Dpkg::options::=--force-unsafe-io'
-option=Dpkg::Options::=--force-confold', 'install', '--download-only', 'linux-generic-hwe-22.04'] with allowed return codes [0] (capture=False)
ading package lists...
uilding dependency tree...
eading state information...
he following additional packages will be installed:
amd64-microcode firmware-sof-signed intel-microcode iucode-tool
libdbus-glib-1-2 libevdev2 libimobiledevice6 libplist3 libupower-glib3
libusbmuxd6 linux-firmware linux-headers-6.2.0-39-generic
linux-headers-generic-hwe-22.04 linux-hwe-6.2-headers-6.2.0-39
linux-image-6.2.0-39-generic linux-image-generic-hwe-22.04
linux-modules-6.2.0-39-generic linux-modules-extra-6.2.0-39-generic thermald
upower usbmuxd wireless-regdb
Suggested packages:
libusbmuxd-tools fdutils linux-doc | linux-hwe-6.2-source-6.2.0
linux-hwe-6.2-tools
The following NEW packages will be installed:
amd64-microcode firmware-sof-signed intel-microcode iucode-tool
libdbus-glib-1-2 libevdev2 libimobiledevice6 libplist3 libupower-glib3
libusbmuxd6 linux-firmware linux-generic-hwe-22.04
linux-headers-6.2.0-39-generic linux-headers-generic-hwe-22.04
linux-hwe-6.2-headers-6.2.0-39 linux-image-6.2.0-39-generic
linux-image-generic-hwe-22.04 linux-modules-6.2.0-39-generic
linux-modules-extra-6.2.0-39-generic thermald upower usbmuxd wireless-regdb
0 upgraded, 23 newly installed, 0 to remove and 94 not upgraded.
Need to get 396 MB/397 MB of archives.
After this operation, 1750 MB of additional disk space will be used.
Get:1 file:/cdrom jammy/main amd64 iucode-tool amd64 2.3.1-1build1 [46.9 kB]
Get:2 file:/cdrom jammy/main amd64 libdbus-glib-1-2 amd64 0.112-2build1 [65.4 kB]
Get:3 file:/cdrom jammy/main amd64 libplist3 amd64 2.2.0-6build2 [32.1 kB]
Get:4 file:/cdrom jammy/main amd64 libusbmuxd6 amd64 2.0.2-3build2 [20.4 kB]
Get:5 file:/cdrom jammy/main amd64 libimobiledevice6 amd64 1.3.0-6build3 [71.1 kB]
Get:6 file:/cdrom jammy/main amd64 libupower-glib3 amd64 0.99.17-1 [46.7 kB]
Get:7 file:/cdrom jammy/main amd64 wireless-regdb all 2022.06.06-0ubuntu1~22.04.1 [10.3 kB]
Get:8 file:/cdrom jammy/main amd64 libevdev2 amd64 1.12.1+dfsg-1 [39.5 kB]
Get:9 file:/cdrom jammy/main amd64 upower amd64 0.99.17-1 [86.7 kB]
Get:10 file:/cdrom jammy/main amd64 usbmuxd amd64 1.1.1-2build2 [42.8 kB]
Get:11 http://fr.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 firmware-sof-signed all 2.0-1ubuntu4.4 [1287 kB]
Get:12 http://fr.archive.ubuntu.com/ubuntu jammy-updates/main amd64 linux-firmware all 20220329.git681281e4-0ubuntu3.23 [259 MB]
Get:13 http://fr.archive.ubuntu.com/ubuntu jammy-updates/main amd64 linux-modules-6.2.0-39-generic amd64 6.2.0-39.40~22.04.1 [25.8 MB]
Get:14 http://fr.archive.ubuntu.com/ubuntu jammy-updates/main amd64 linux-image-6.2.0-39-generic amd64 6.2.0-39.40~22.04.1 [13.6 MB]
[Close]
packard bell

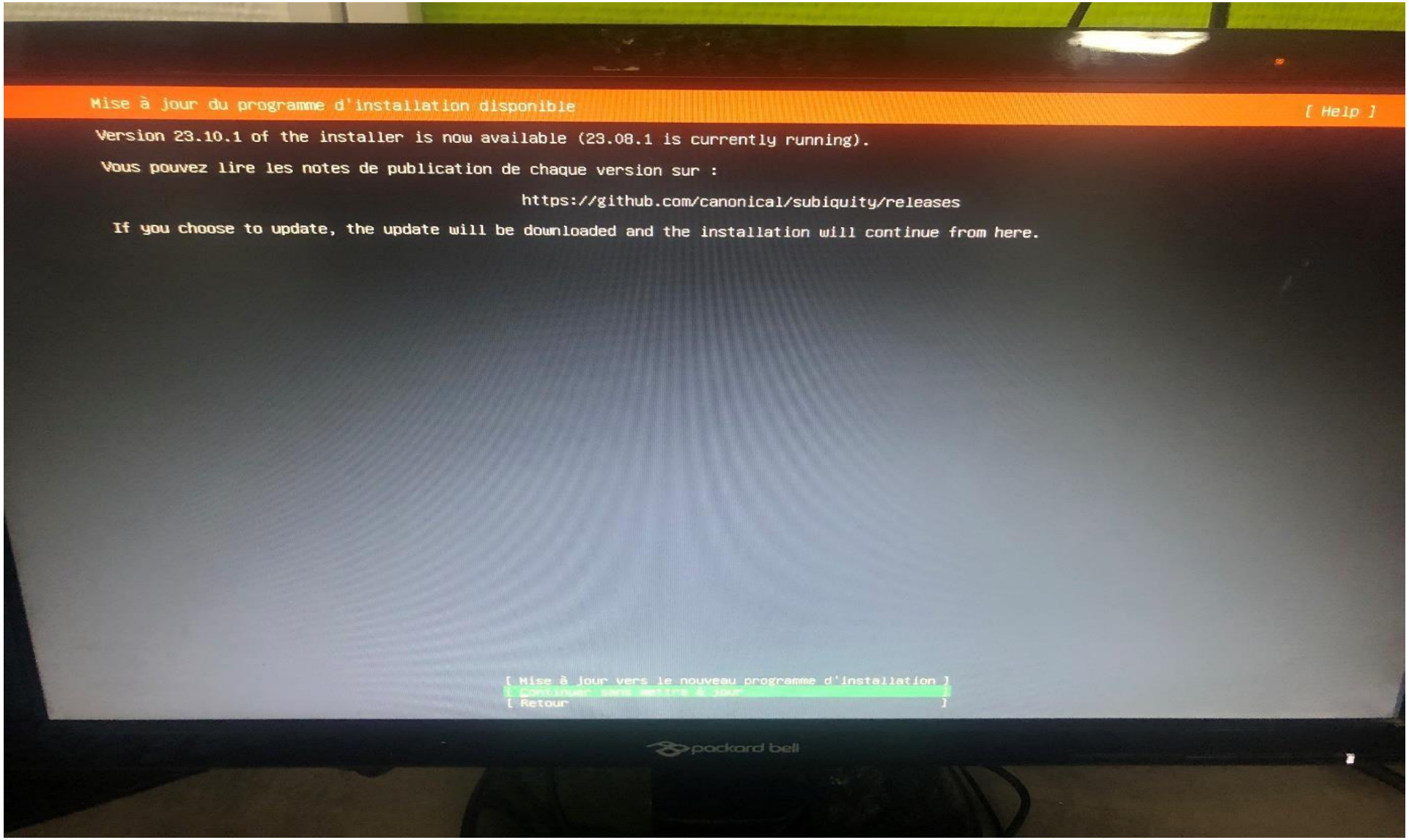

Installation du système
[Help]
curtin command in-target
installing system
executing curtin install initial step
executing curtin install partitioning step
curtin command install
configuring storage
running 'curtin block-meta simple'
curtin command block-meta
removing previous storage devices
configuring disk: disk-sda
configuring partition: partition-0
configuring format: format-0
configuring partition: partition-1
configuring format: format-1
configuring partition: partition-2
configuring lvm_volgroup: lvm_volgroup-0
configuring lvm_partition: lvm_partition-0
configuring format: format-2
configuring mount: mount-2
configuring mount: mount-1
configuring mount: mount-0
executing curtin install extract step
curtin command install
writing install sources to disk
running 'curtin extract'
curtin command extract
acquiring and extracting image from cp:///tmp/tmpg04kpfec/mount
executing curtin install curthooks step
curtin command install
configuring installed system
running 'curtin in-target -- setupcon --save-only'
curtin command in-target
running 'curtin curthooks'
curtin command curthooks
configuring apt configuring apt
installing missing packages
Installing packages on target system: ['efibootmgr', 'grub-efi-amd64', 'grub-efi-amd64-signed', 'shim-signed']
configuring iscsi service
configuring raid (mdadm) service
installing kernel -
[View full log]
packard bell

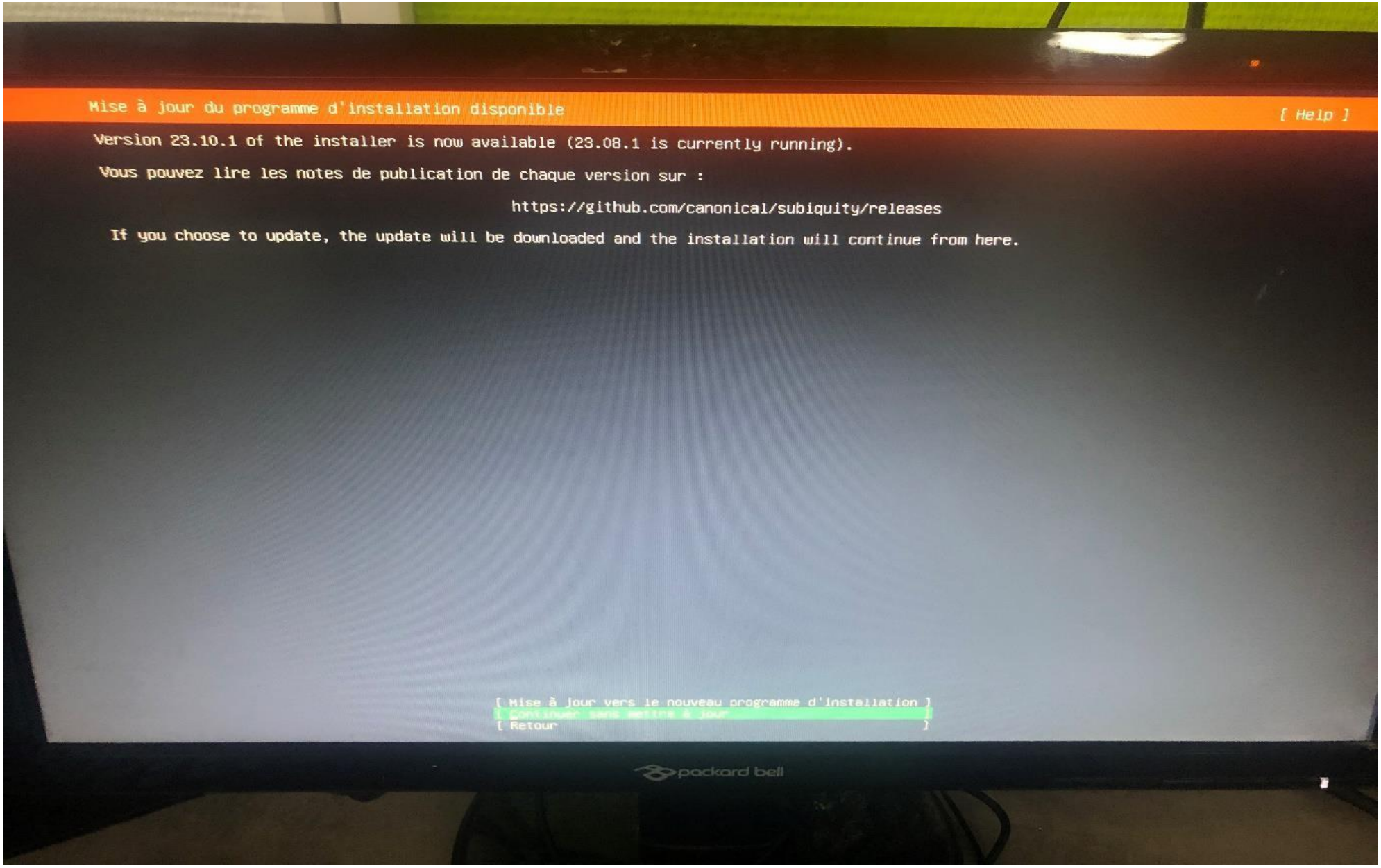

Configuration du profil
[Help]
Enter the username and password you will use to log in to the system. You can configure SSH access on the next screen but a password is still needed for sudo.
Votre nom : administrateur
Le nom de cette machine: ubuntu-server
The name it uses when it talks to other computers.
Choisir un nom d'utilisateur : hosni
Choisir un mot de passe : ******
Confirmer votre mot de passe: ******
[Terminé]
packard bell

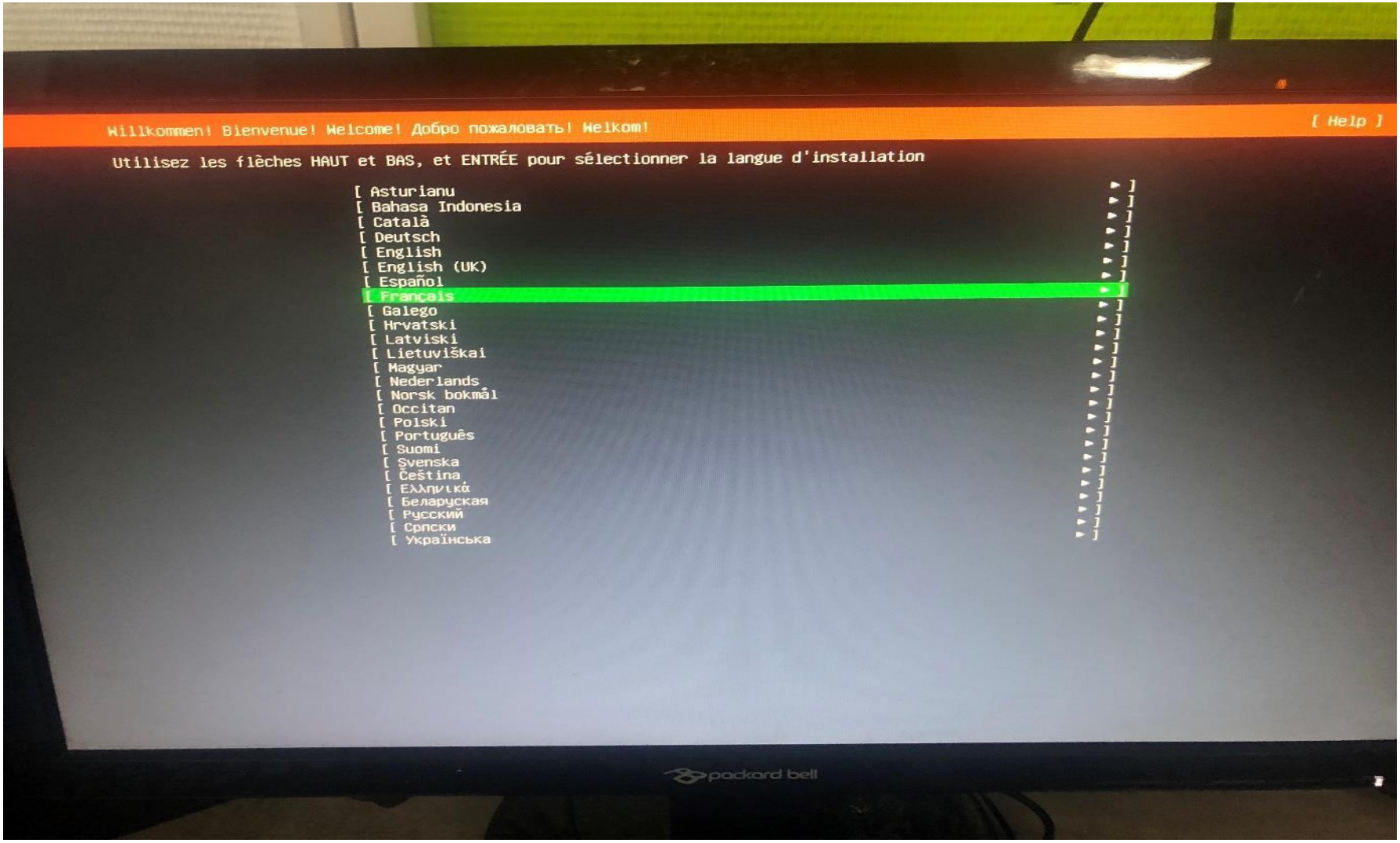

Configuration du stockage
[Help]
SOMMAIRE DU SYSTÈME DE FICHIERS
POINT DE MONTAGE TAILLE TYPE TYPE DE PÉRIPHÉRIQUE
[/ 100.000G new ext4 nouveau LVM logical volume ▸]
[/boot 2.000G new ext4 nouveau partition de disque local ▸]
[/boot/efi 1.049G new fat32 nouveau partition de disque local ▸]
DISQUES DISPONIBLES
PÉRIPHÉRIQUE TYPE TAILLE
[ubuntu-vg (nouveau) LVM volume group 235.421G ▸]
espace libre 135.421G ▸
[Create software RAID (md) ▸]
[Create volume group (LVM) ▸]
PÉRIPHÉRIQUES UTILISÉS
PÉRIPHÉRIQUE TYPE TAILLE
[ubuntu-vg (nouveau) LVM volume group 235.421G ▸]
ubuntu-lv nouveau, to be formatted as ext4, mounted at / 100.000G ▸
[INNOVATION..IT_843882006180088 disque local 238.474G ▸]
partition 1 nouveau, primary ESP, to be formatted as fat32, mounted at /boot/efi 1.049G ▸
partition 2 nouveau, to be formatted as ext4, mounted at /boot 2.000G ▸
partition 3 nouveau, PV of LVM volume group ubuntu-vg 235.422G ▸
[Terminé]
[Rétablir]
[Retour]
packard bell

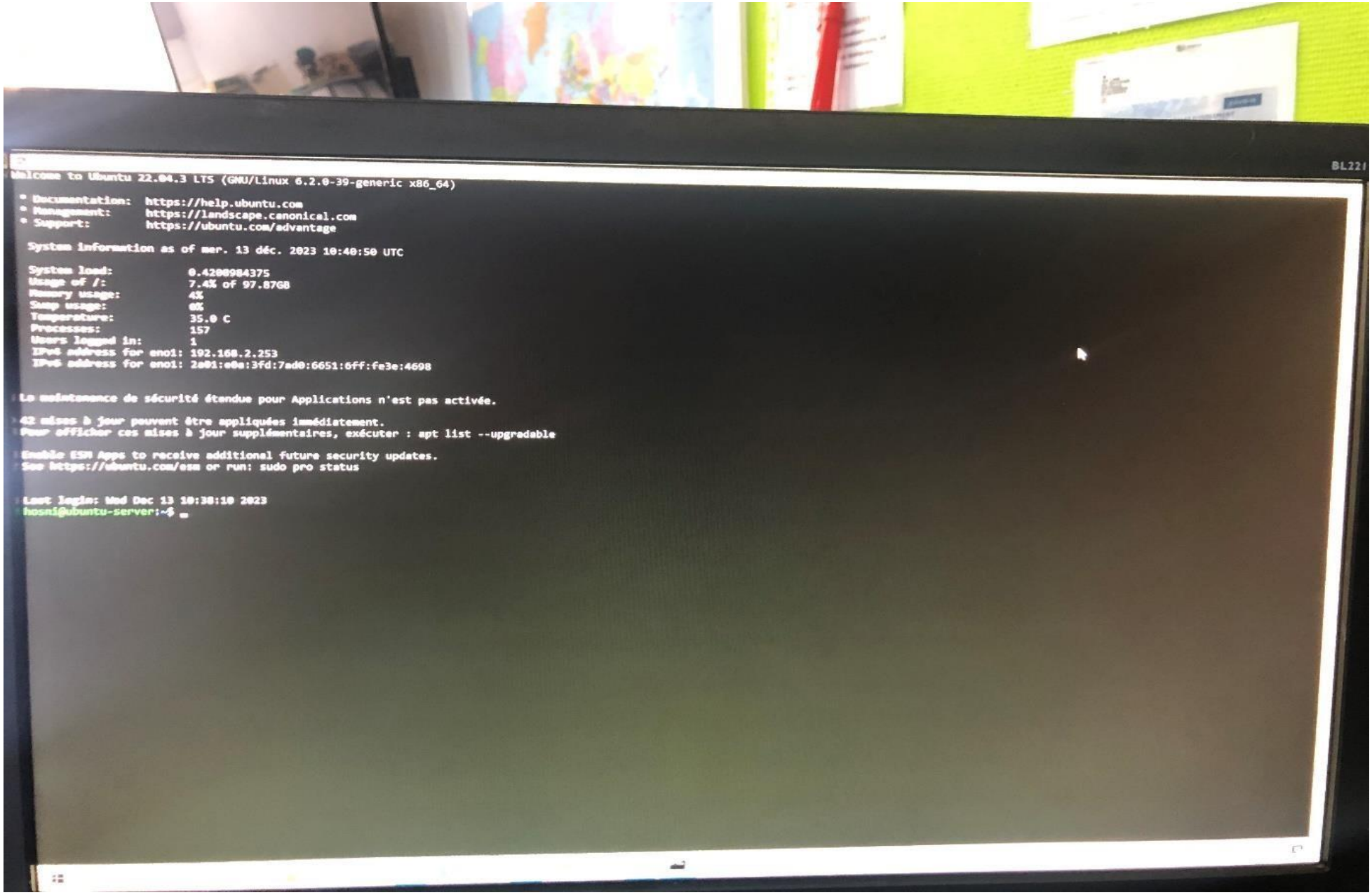

Choose type of install
[Help]
Choose the base for the installation.
(X) Ubuntu Server
The default install contains a curated set of packages that provide a comfortable experience for operating your server.
( ) Ubuntu Server (minimized)
This version has been customized to have a small runtime footprint in environments where humans are not expected to log in.
Additional options
[ ] Search for third-party drivers
This software is subject to license terms included with its documentation. Some is proprietary. Third-party drivers should not be installed on systems that will be used for FIPS or the real-time kernel.
[Retour]
packard bell

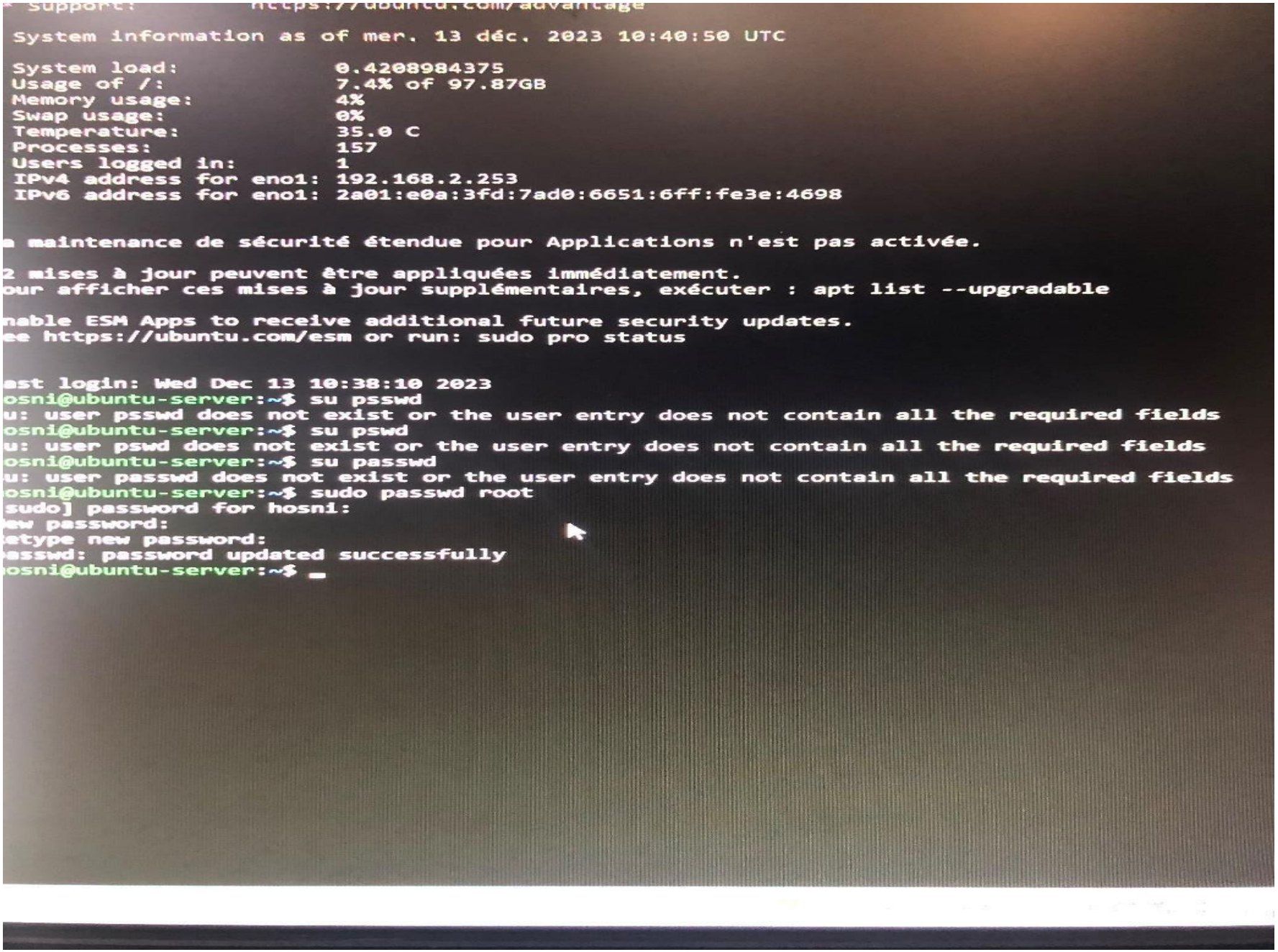

Configuration clavier
[Help
Veuillez sélectionner votre disposition de clavier ci-dessous, ou sélectionner "Identifier le clavier" afin de détecter votre disposition automatiquement.
Disposition : [French ▾]
Variante : [French - French (AZERTY) ▾]
[Identifier le clavier]
[Terminé]
[Retour]
packard bell

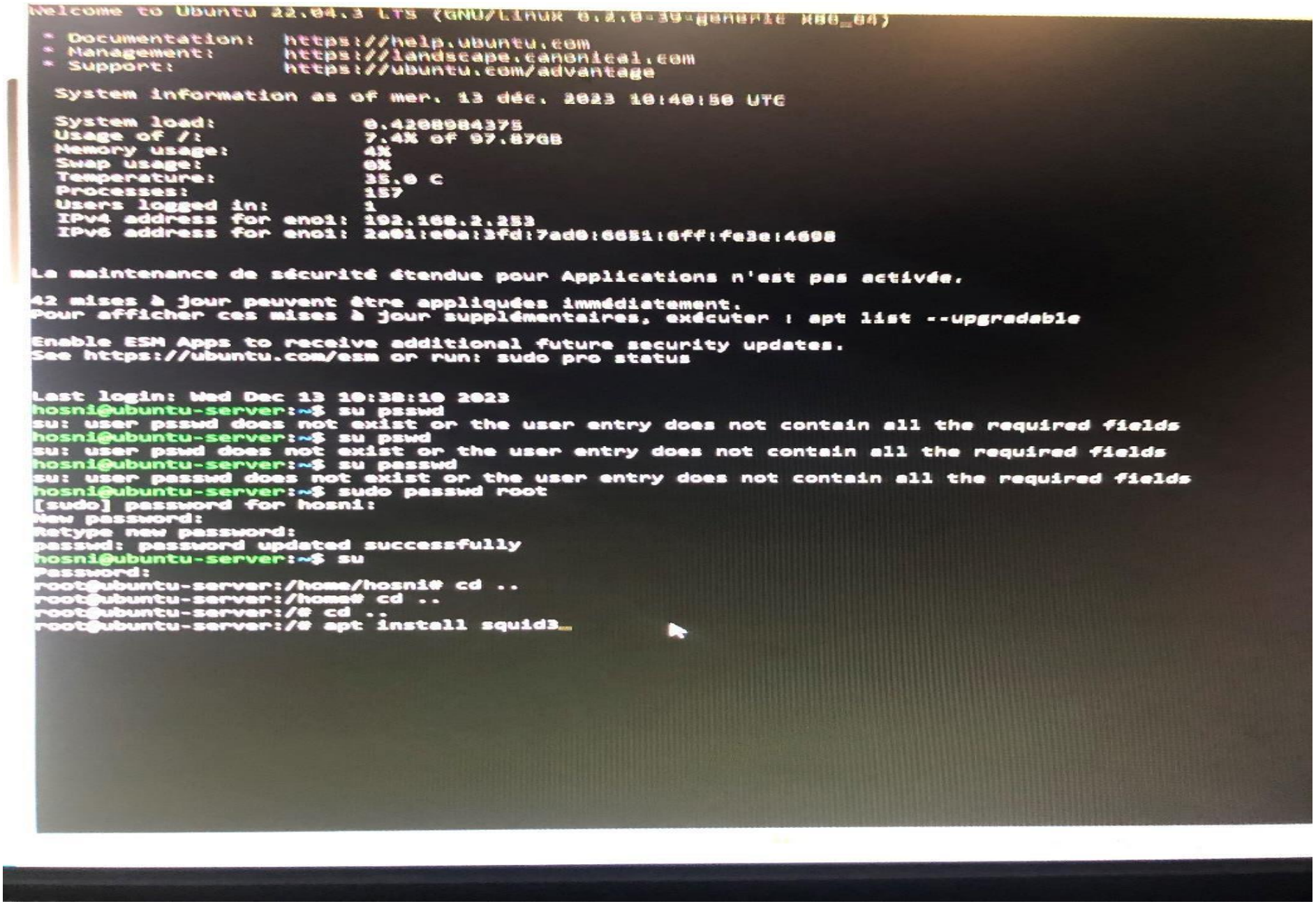

Mise à jour du programme d'installation disponible
[Help]
Version 23.10.1 of the installer is now available (23.08.1 is currently running).
Vous pouvez lire les notes de publication de chaque version sur :
https://github.com/canonical/subiquity/releases
If you choose to update, the update will be downloaded and the installation will continue from here.
[Mise à jour vers le nouveau programme d'installation]
[Continuer sans mettre à jour]
[Retour]
packard bell

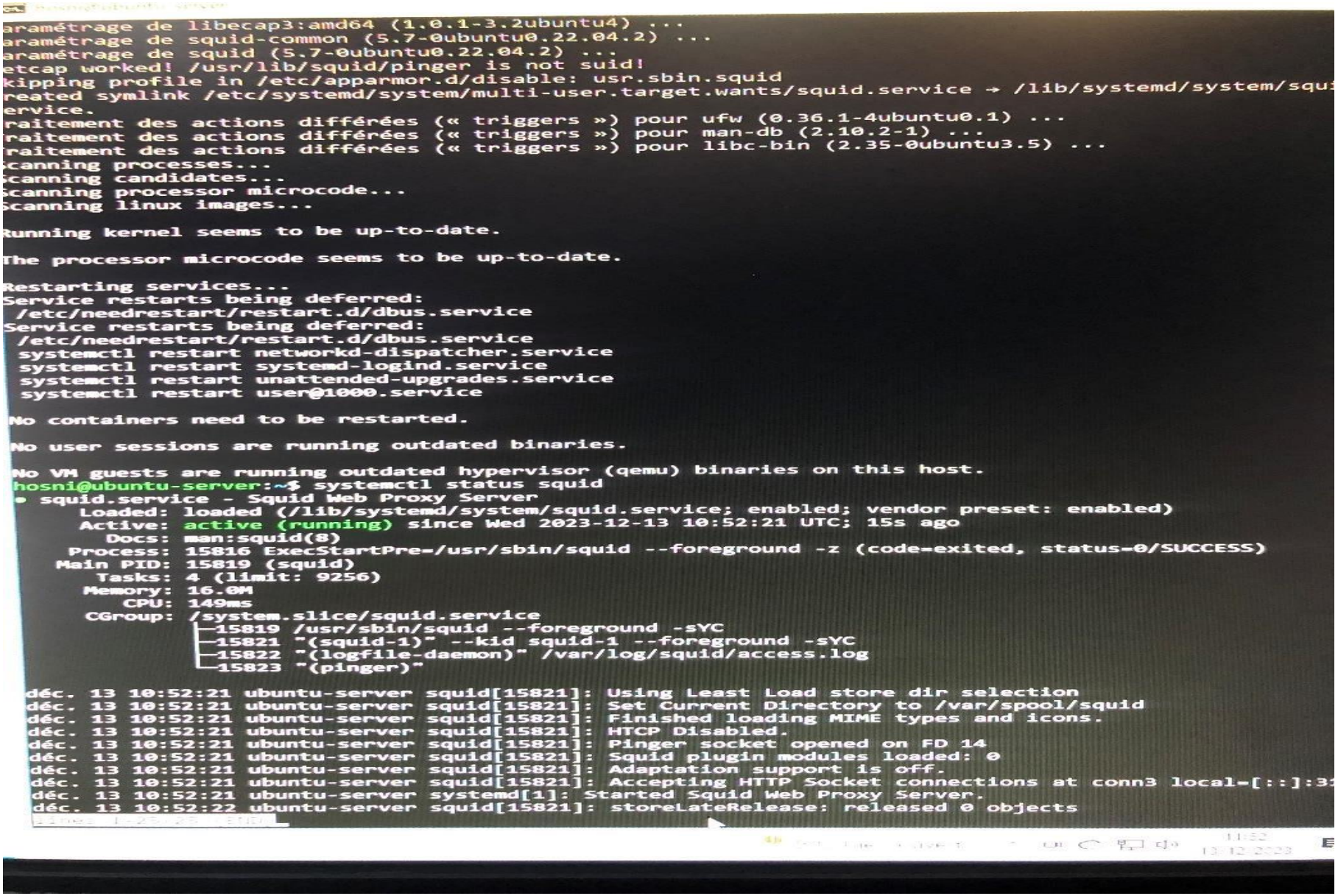

Mise à jour du programme d'installation disponible
[Help]
Version 23.10.1 of the installer is now available (23.08.1 is currently running).
Vous pouvez lire les notes de publication de chaque version sur :
https://github.com/canonical/subiquity/releases
If you choose to update, the update will be downloaded and the installation will continue from here.
[Mise à jour vers le nouveau programme d'installation]
[Continuer sans mettre à jour]
[Retour]
packard bell

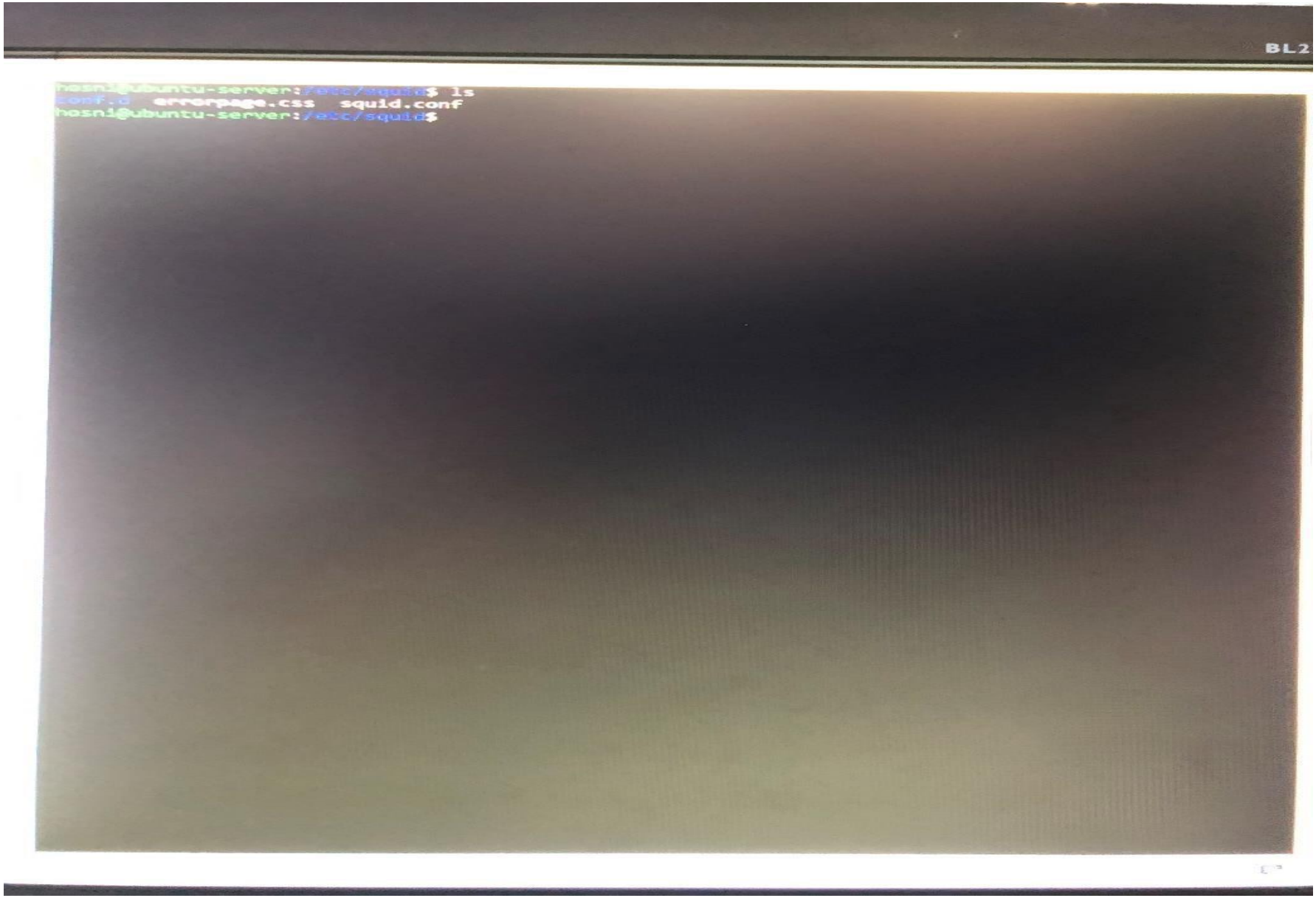

Willkommen! Bienvenue! Welcome! Добро пожаловать! Welkom!
[Help]
Utilisez les flèches HAUT et BAS, et ENTRÉE pour sélectionner la langue d'installation
[Asturianu
[Bahasa Indonesia
[Català
[Deutsch
[English
[English (UK)
[Español
[Français
[Galego
[Hrvatski
[Latviski
[Lietuviškai
[Magyar
[Nederlands
[Norsk bokmål
[Occitan
[Polski
[Português
[Suomi
[Svenska
[Čeština
[Ελληνικά
[Беларуская
[Русский
[Српски
[Українська
packard bell

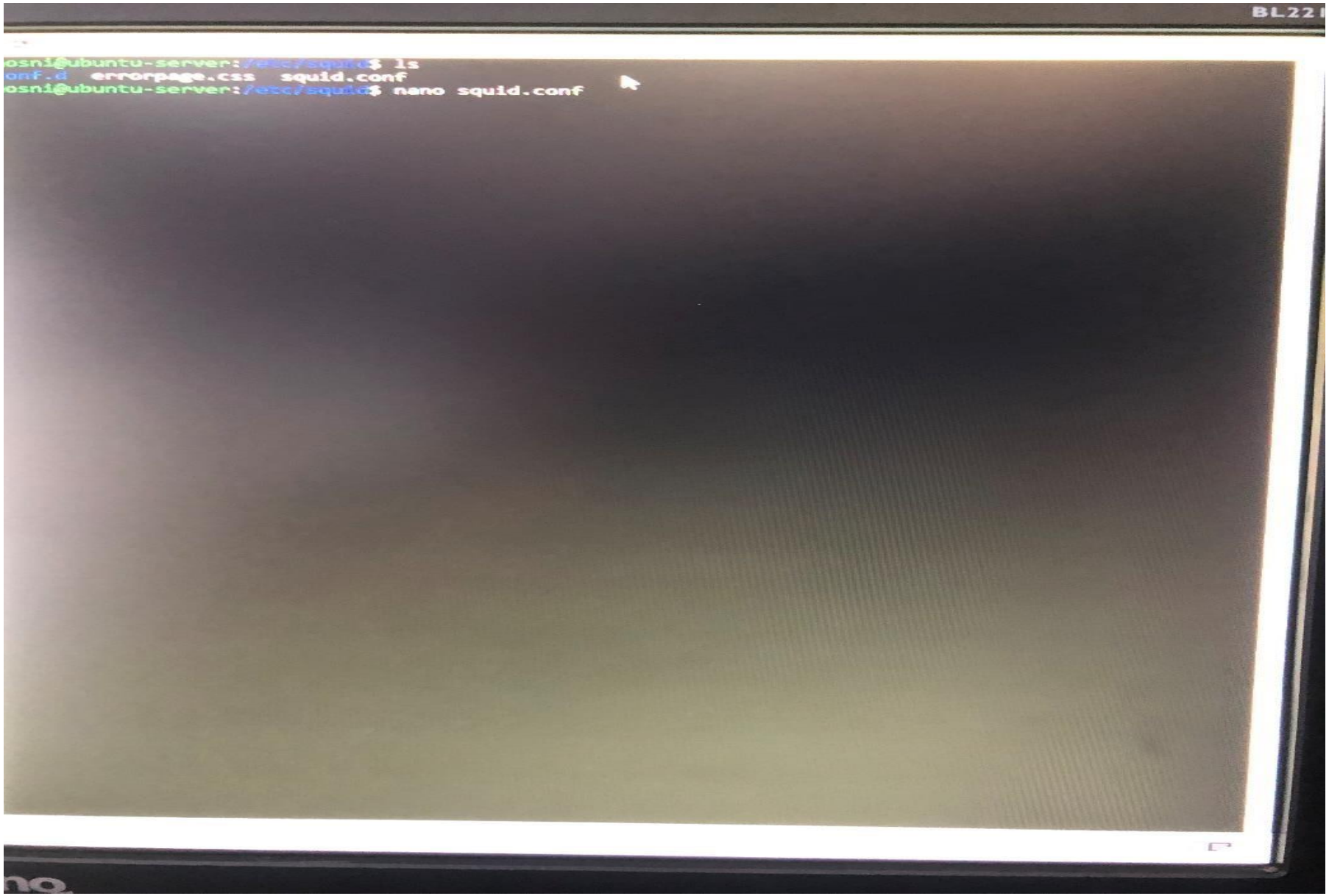

Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-39-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of mer. 13 déc. 2023 10:40:50 UTC
System load: 0.4208984375
Usage of /: 7.4% of 97.87GB
Memory usage: 4%
Swap usage: 0%
Temperature: 35.0 C
Processes: 157
Users logged in: 1
IPv4 address for eno1: 192.168.2.253
IPv6 address for eno1: 2a01:e0a:3fd:7ad0:6651:6ff:fe3e:4698
La maintenance de sécurité étendue pour Applications n'est pas activée.
42 mises à jour peuvent être appliquées immédiatement.
Pour afficher ces mises à jour supplémentaires, exécuter : apt list --upgradable
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
Last login: Wed Dec 13 10:38:10 2023
hosni@ubuntu-server:~$

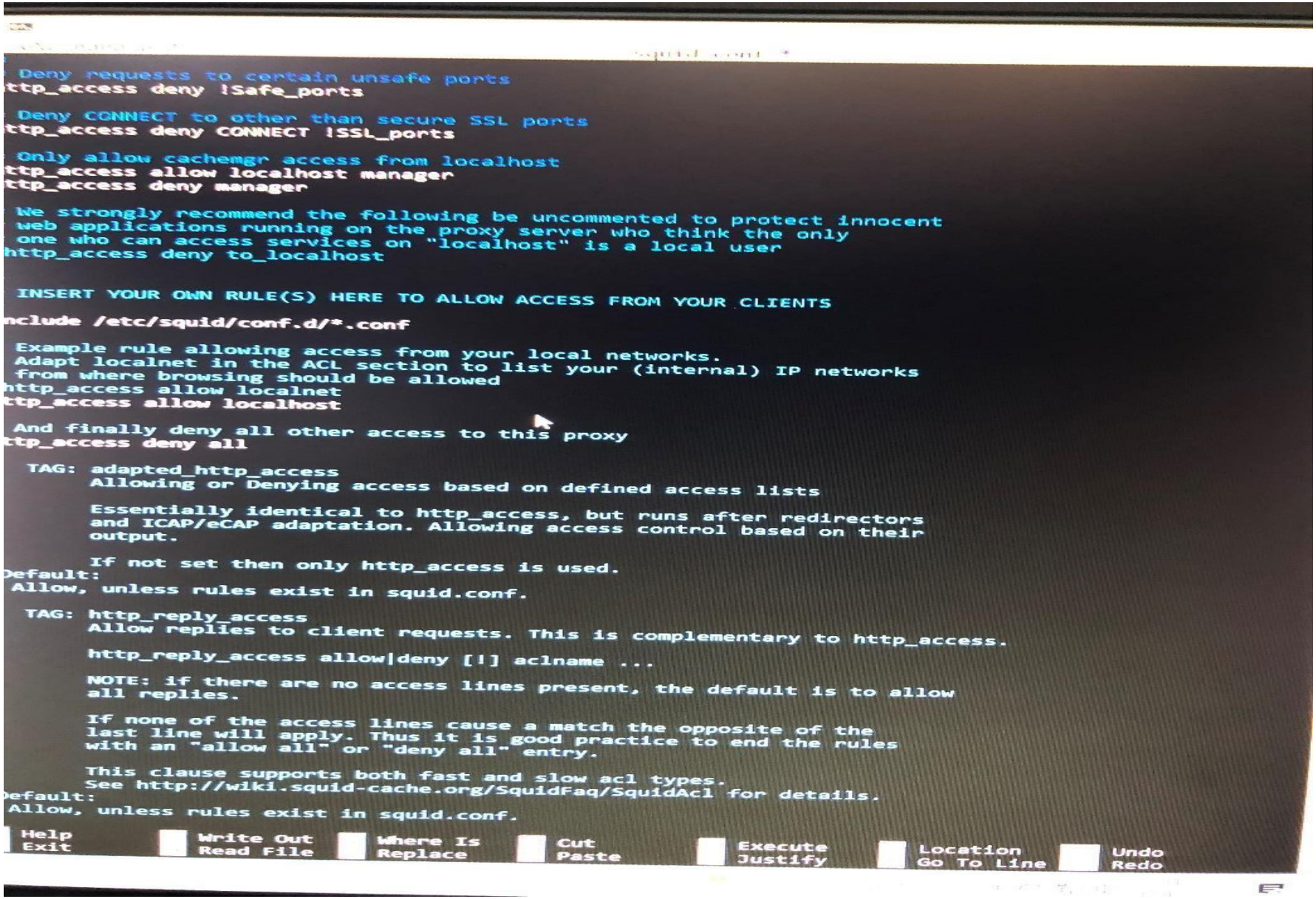

* Support: https://ubuntu.com/advantage
System information as of mer. 13 déc. 2023 10:40:50 UTC
System load: 0.4208984375
Usage of /: 7.4% of 97.87GB
Memory usage: 4%
Swap usage: 0%
Temperature: 35.0 C
Processes: 157
Users logged in: 1
IPv4 address for eno1: 192.168.2.253
IPv6 address for eno1: 2a01:e0a:3fd:7ad0:6651:6ff:fe3e:4698
maintenance de sécurité étendue pour Applications n'est pas activée.
2 mises à jour peuvent être appliquées immédiatement.
our afficher ces mises à jour supplémentaires, exécuter : apt list --upgradable
nable ESM Apps to receive additional future security updates.
ee https://ubuntu.com/esm or run: sudo pro status
ast login: Wed Dec 13 10:38:10 2023
osni@ubuntu-server:~$ su psswd
u: user psswd does not exist or the user entry does not contain all the required fields
osni@ubuntu-server:~$ su pswd
u: user pswd does not exist or the user entry does not contain all the required fields
osni@ubuntu-server:~$ su passwd
u: user passwd does not exist or the user entry does not contain all the required fields
osni@ubuntu-server:~$ sudo passwd root
sudo] password for hosni:
ew password:
etype new password:
asswd: password updated successfully
osni@ubuntu-server:~$

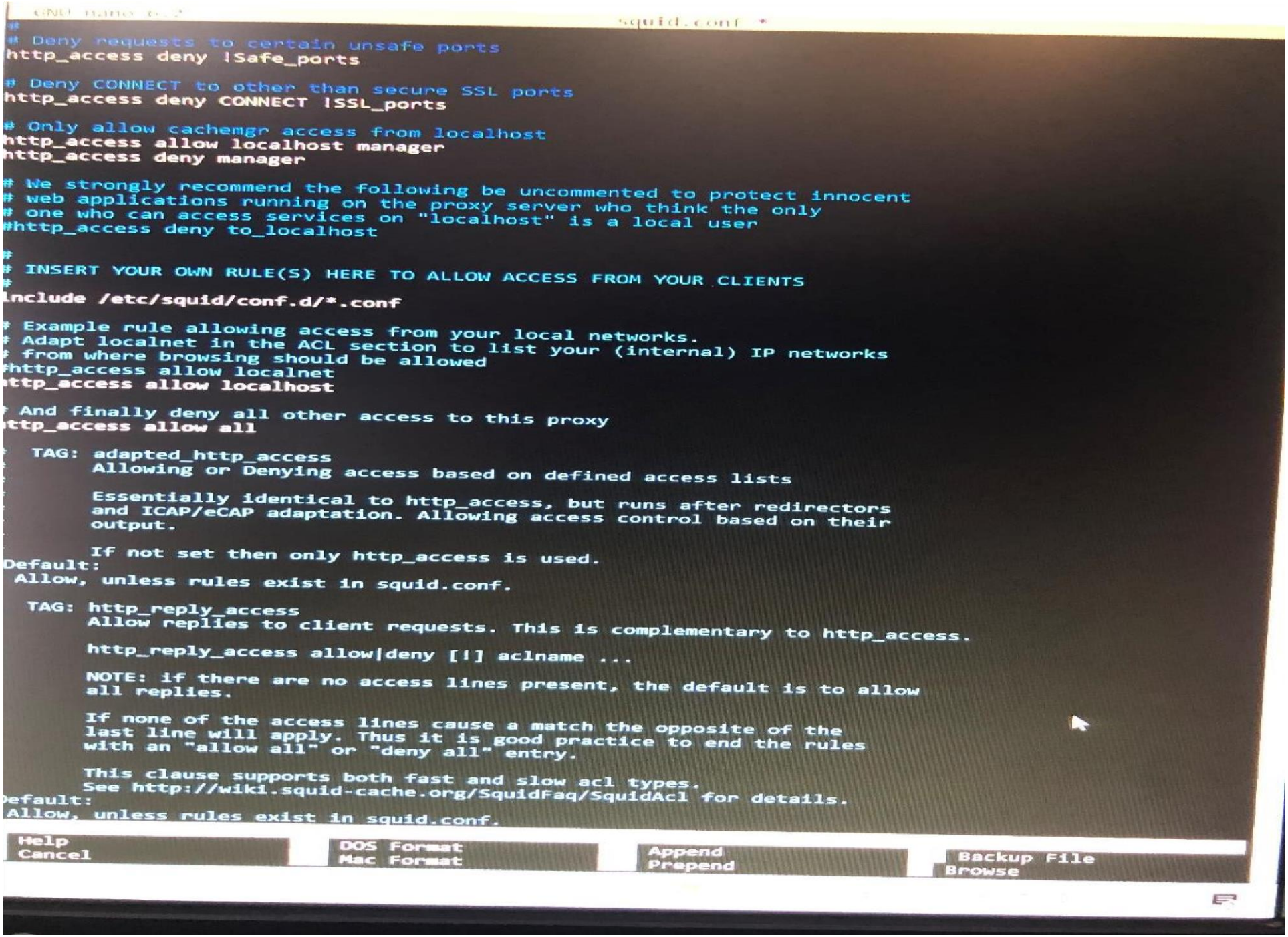

Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-39-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of mer. 13 déc. 2023 10:40:50 UTC
System load: 0.4208984375
Usage of /: 7.4% of 97.87GB
Memory usage: 4%
Swap usage: 0%
Temperature: 35.0 C
Processes: 157
Users logged in: 1
IPv4 address for eno1: 192.168.2.253
IPv6 address for eno1: 2a01:e0a:3fd:7ad0:6651:6ff:fe3e:4698
La maintenance de sécurité étendue pour Applications n'est pas activée.
42 mises à jour peuvent être appliquées immédiatement.
Pour afficher ces mises à jour supplémentaires, exécuter : apt list --upgradable
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
Last login: Wed Dec 13 10:38:10 2023
hosni@ubuntu-server:~$ su psswd
su: user psswd does not exist or the user entry does not contain all the required fields
hosni@ubuntu-server:~$ su pswd
su: user pswd does not exist or the user entry does not contain all the required fields
hosni@ubuntu-server:~$ su passwd
su: user passwd does not exist or the user entry does not contain all the required fields
hosni@ubuntu-server:~$ sudo passwd root
[sudo] password for hosni:
New password:
Retype new password:
passwd: password updated successfully
hosni@ubuntu-server:~$ su
Password:
root@ubuntu-server:/home/hosni# cd ..
root@ubuntu-server:/home# cd ..
root@ubuntu-server:/# cd ..
root@ubuntu-server:/# apt install squid3

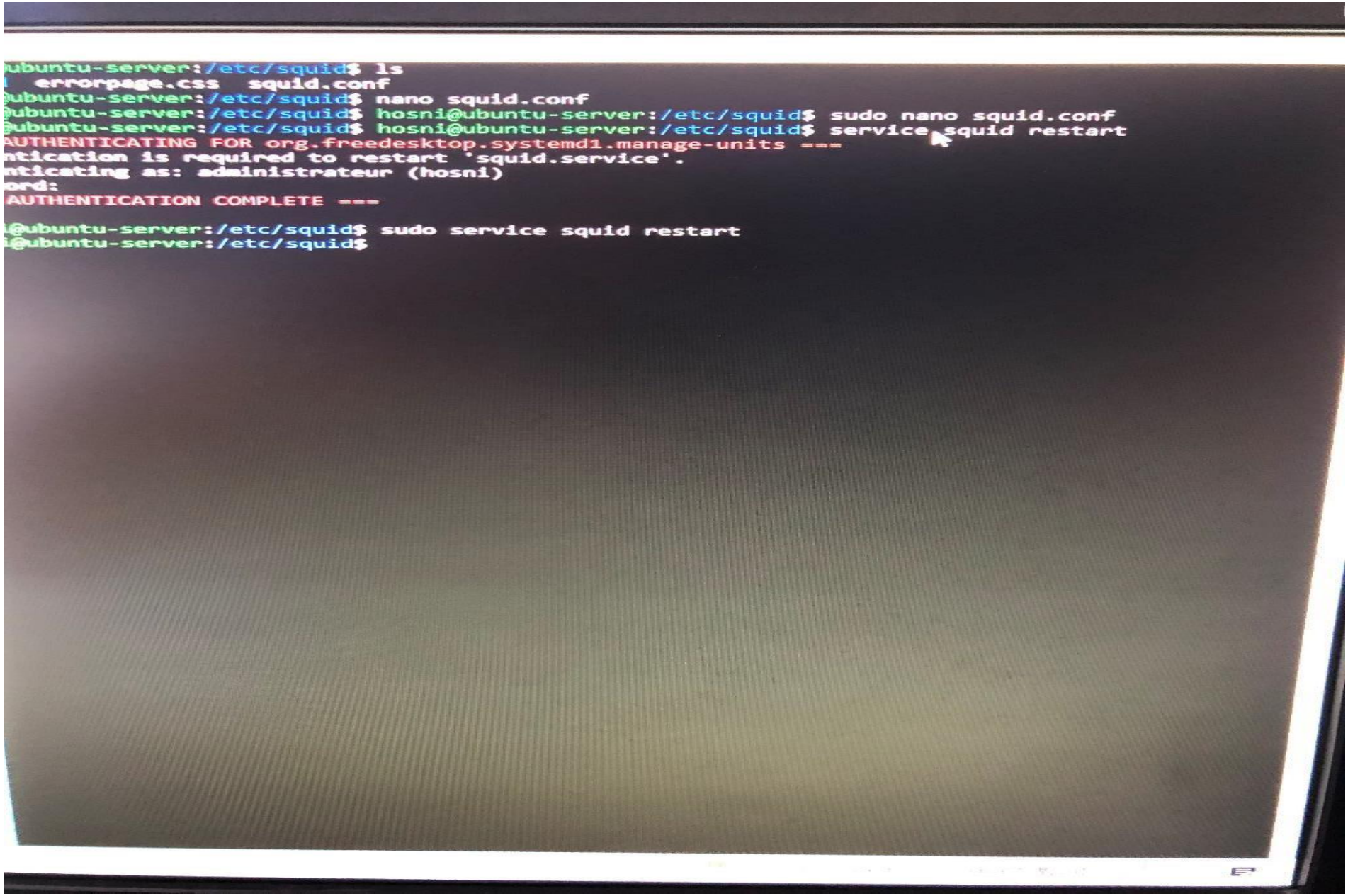

aramétrage de libecap3:amd64 (1.0.1-3.2ubuntu4) ...
aramétrage de squid-common (5.7-0ubuntu0.22.04.2) ...
aramétrage de squid (5.7-0ubuntu0.22.04.2) ...
etcap worked! /usr/lib/squid/pinger is not suid!
kipping profile in /etc/apparmor.d/disable: usr.sbin.squid
reated symlink /etc/systemd/system/multi-user.target.wants/squid.service → /lib/systemd/system/squi
ervice.
raitement des actions différées (« triggers ») pour ufw (0.36.1-4ubuntu0.1) ...
raitement des actions différées (« triggers ») pour man-db (2.10.2-1) ...
raitement des actions différées (« triggers ») pour libc-bin (2.35-0ubuntu3.5) ...
canning processes...
canning candidates...
canning processor microcode...
canning linux images...
unning kernel seems to be up-to-date.
The processor microcode seems to be up-to-date.
estarting services...
Service restarts being deferred:
/etc/needrestart/restart.d/dbus.service
Service restarts being deferred:
/etc/needrestart/restart.d/dbus.service
systemctl restart networkd-dispatcher.service
systemctl restart systemd-logind.service
systemctl restart unattended-upgrades.service
systemctl restart user@1000.service
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
hosni@ubuntu-server:~$ systemctl status squid
● squid.service - Squid Web Proxy Server
Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
Active: active (running) since Wed 2023-12-13 10:52:21 UTC; 15s ago
Docs: man:squid(8)
Process: 15816 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
Main PID: 15819 (squid)
Tasks: 4 (limit: 9256)
Memory: 16.0M
CPU: 149ms
CGroup: /system.slice/squid.service
├─15819 /usr/sbin/squid --foreground -sYC
├─15821 "(squid-1)" --kid squid-1 --foreground -sYC
├─15822 "(logfile-daemon)" /var/log/squid/access.log
└─15823 "(pinger)"
déc. 13 10:52:21 ubuntu-server squid[15821]: Using Least Load store dir selection
déc. 13 10:52:21 ubuntu-server squid[15821]: Set Current Directory to /var/spool/squid
déc. 13 10:52:21 ubuntu-server squid[15821]: Finished loading MIME types and icons.
déc. 13 10:52:21 ubuntu-server squid[15821]: HTCP Disabled.
déc. 13 10:52:21 ubuntu-server squid[15821]: Pinger socket opened on FD 14
déc. 13 10:52:21 ubuntu-server squid[15821]: Squid plugin modules loaded: 0
déc. 13 10:52:21 ubuntu-server squid[15821]: Adaptation support is off.
déc. 13 10:52:21 ubuntu-server squid[15821]: Accepting HTTP Socket connections at conn3 local=[::]:3
déc. 13 10:52:21 ubuntu-server systemd[1]: Started Squid Web Proxy Server.
déc. 13 10:52:22 ubuntu-server squid[15821]: storeLateRelease: released 0 objects

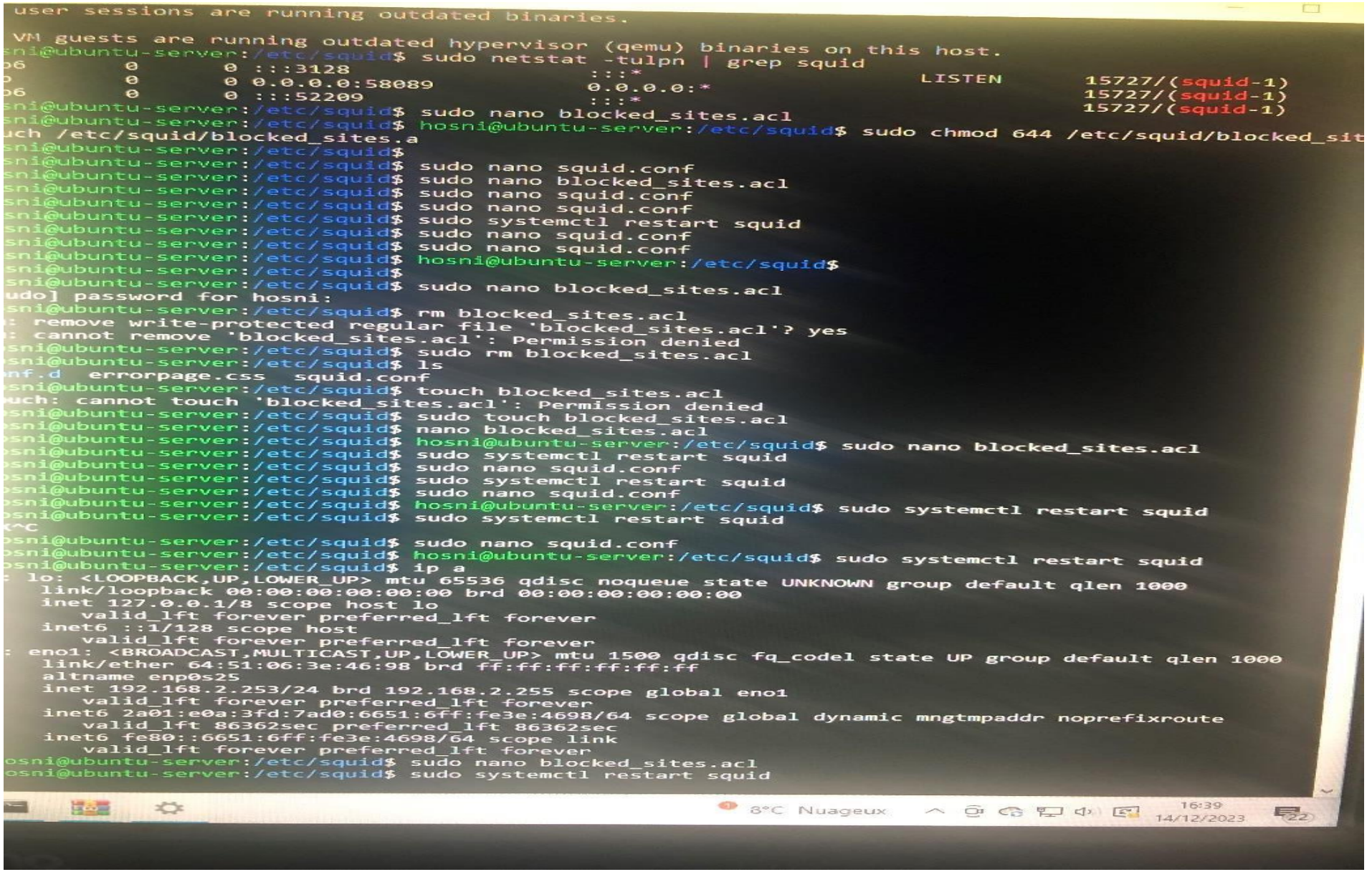

BL2
hosni@ubuntu-server:/etc/squid$ ls
conf.d errorpage.css squid.conf
hosni@ubuntu-server:/etc/squid$

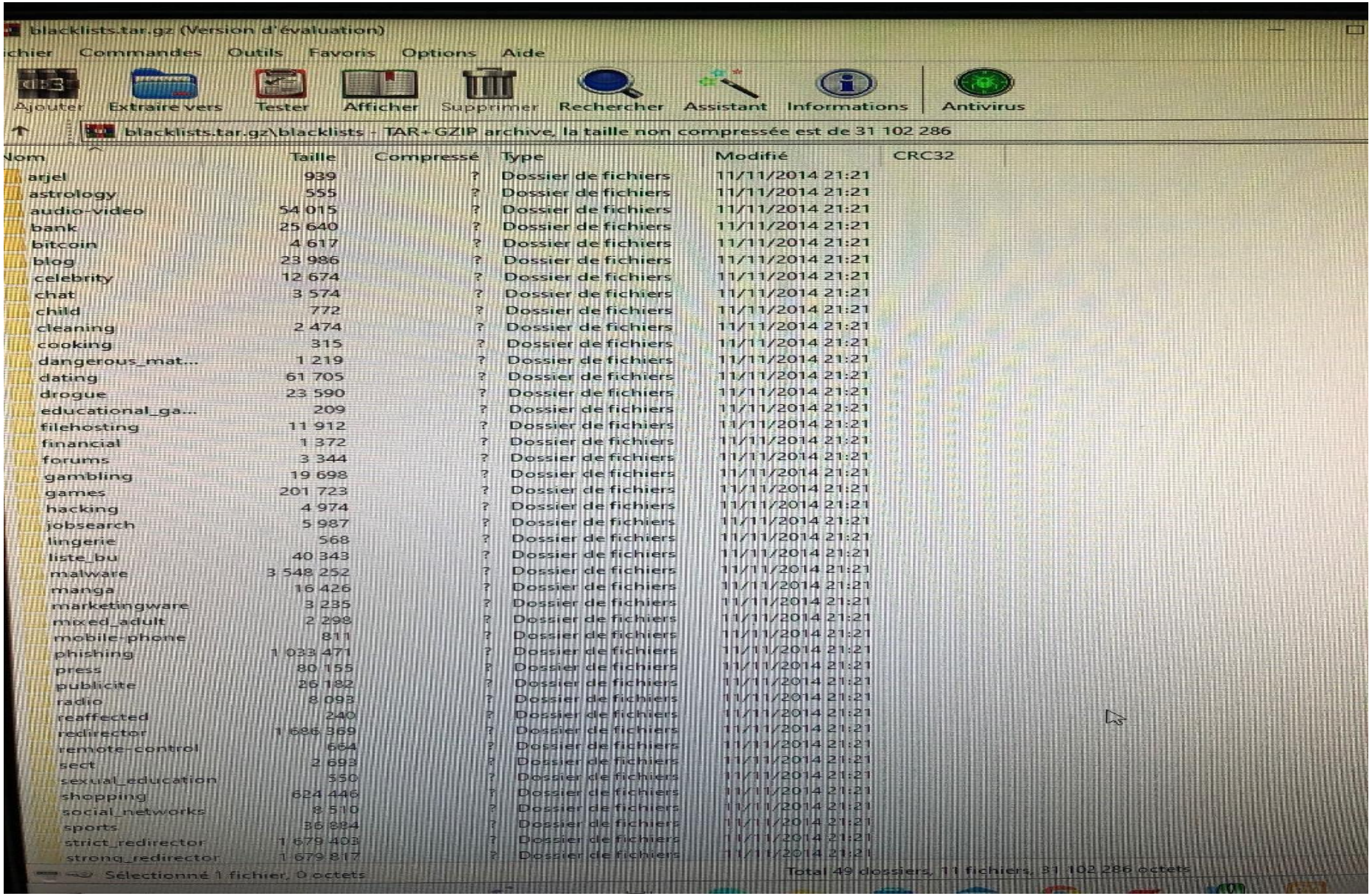

osni@ubuntu-server:/etc/squid$ ls
conf.d errorpage.css squid.conf
osni@ubuntu-server:/etc/squid$ nano squid.conf

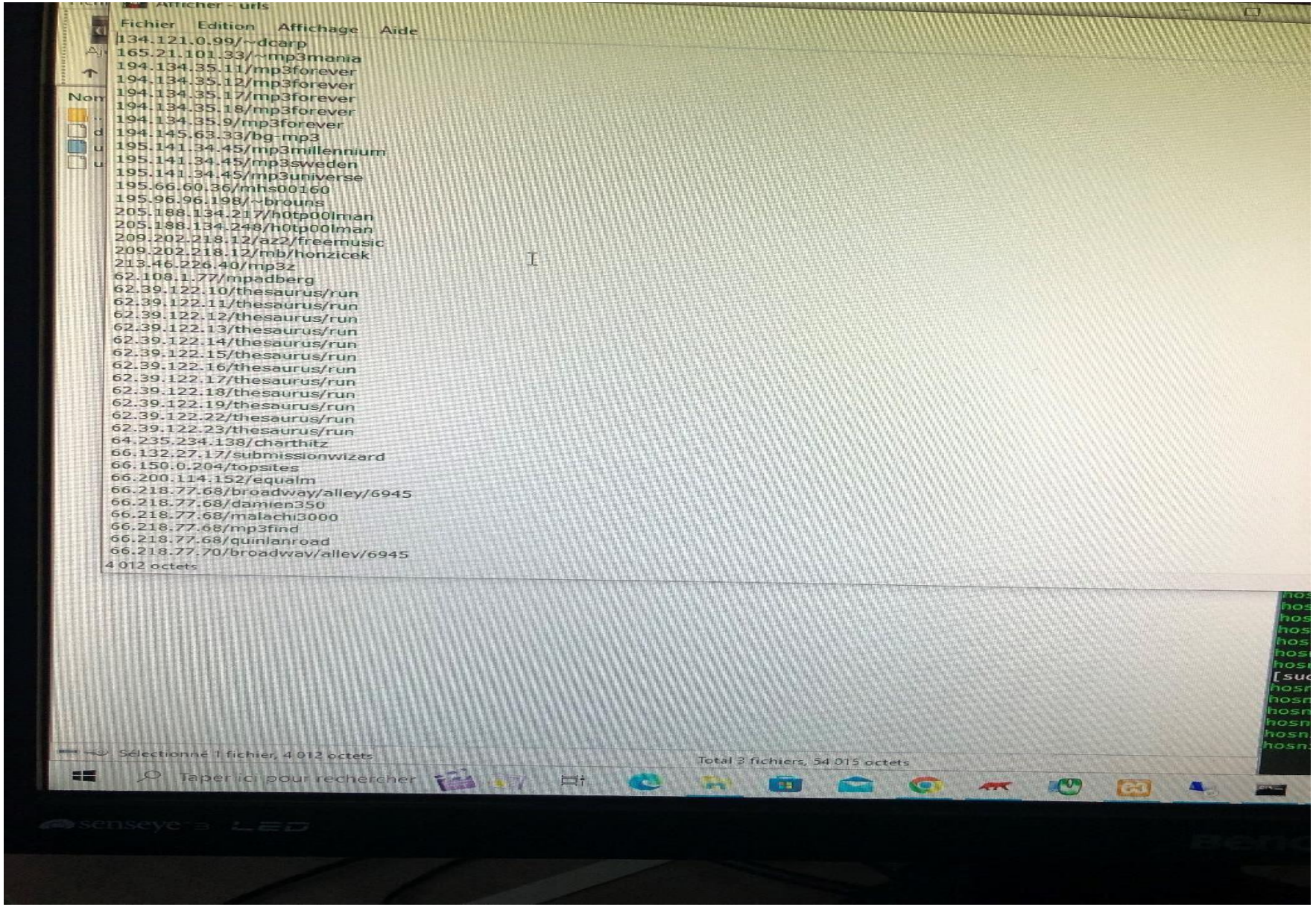

Deny requests to certain unsafe ports
ttp_access deny !Safe_ports
Deny CONNECT to other than secure SSL ports
ttp_access deny CONNECT !SSL_ports
Only allow cachemgr access from localhost
ttp_access allow localhost manager
ttp_access deny manager
We strongly recommend the following be uncommented to protect innocent
web applications running on the proxy server who think the only
one who can access services on "localhost" is a local user
http_access deny to_localhost
INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
nclude /etc/squid/conf.d/*.conf
Example rule allowing access from your local networks.
Adapt localnet in the ACL section to list your (internal) IP networks
from where browsing should be allowed
http_access allow localnet
ttp_access allow localhost
And finally deny all other access to this proxy
ttp_access deny all
TAG: adapted_http_access
Allowing or Denying access based on defined access lists
Essentially identical to http_access, but runs after redirectors
and ICAP/eCAP adaptation. Allowing access control based on their
output.
If not set then only http_access is used.
Default:
Allow, unless rules exist in squid.conf.
TAG: http_reply_access
Allow replies to client requests. This is complementary to http_access.
http_reply_access allow|deny [!] aclname ...
NOTE: if there are no access lines present, the default is to allow
all replies.
If none of the access lines cause a match the opposite of the
last line will apply. Thus it is good practice to end the rules
with an "allow all" or "deny all" entry.
This clause supports both fast and slow acl types.
See http://wiki.squid-cache.org/SquidFaq/SquidAcl for details.
Default:
Allow, unless rules exist in squid.conf.
Help
Write Out
Where Is
Cut
Execute
Location
Undo
Exit
Read File
Replace
Paste
Justify
Go To Line
Redo

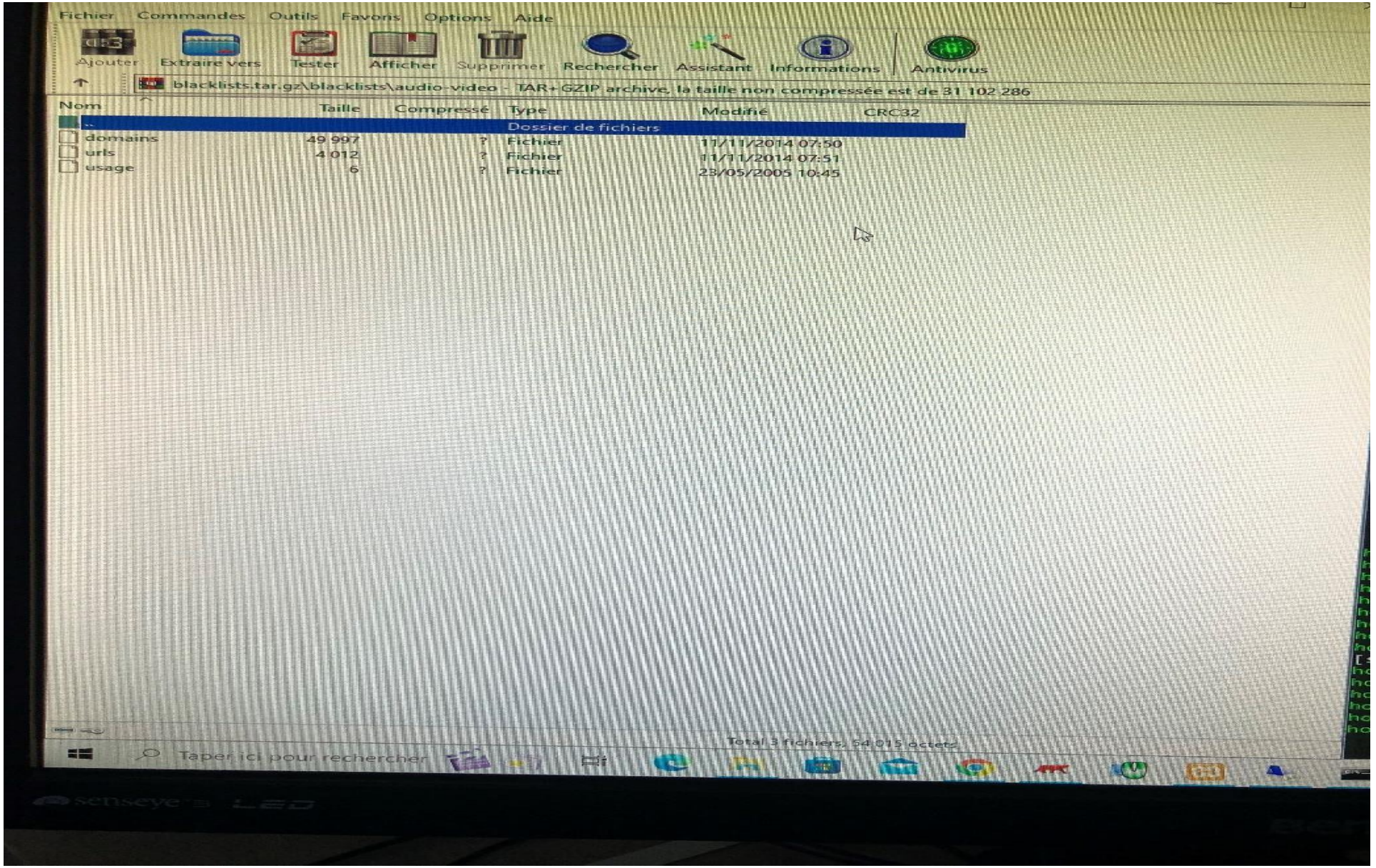

squid.conf *
Deny requests to certain unsafe ports
http_access deny !Safe_ports
Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports
Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager
We strongly recommend the following be uncommented to protect innocent
web applications running on the proxy server who think the only
one who can access services on "localhost" is a local user
#http_access deny to_localhost
#
INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
include /etc/squid/conf.d/*.conf
Example rule allowing access from your local networks.
Adapt localnet in the ACL section to list your (internal) IP networks
from where browsing should be allowed
#http_access allow localnet
http_access allow localhost
And finally deny all other access to this proxy
http_access allow all
TAG: adapted_http_access
Allowing or Denying access based on defined access lists
Essentially identical to http_access, but runs after redirectors
and ICAP/eCAP adaptation. Allowing access control based on their
output.
If not set then only http_access is used.
Default:
Allow, unless rules exist in squid.conf.
TAG: http_reply_access
Allow replies to client requests. This is complementary to http_access.
http_reply_access allow|deny [!] aclname ...
NOTE: if there are no access lines present, the default is to allow
all replies.
If none of the access lines cause a match the opposite of the
last line will apply. Thus it is good practice to end the rules
with an "allow all" or "deny all" entry.
This clause supports both fast and slow acl types.
See http://wiki.squid-cache.org/SquidFaq/SquidAcl for details.
Default:
Allow, unless rules exist in squid.conf.
Help
Cancel
DOS Format
Mac Format
Append
Prepend
Backup File
Browse

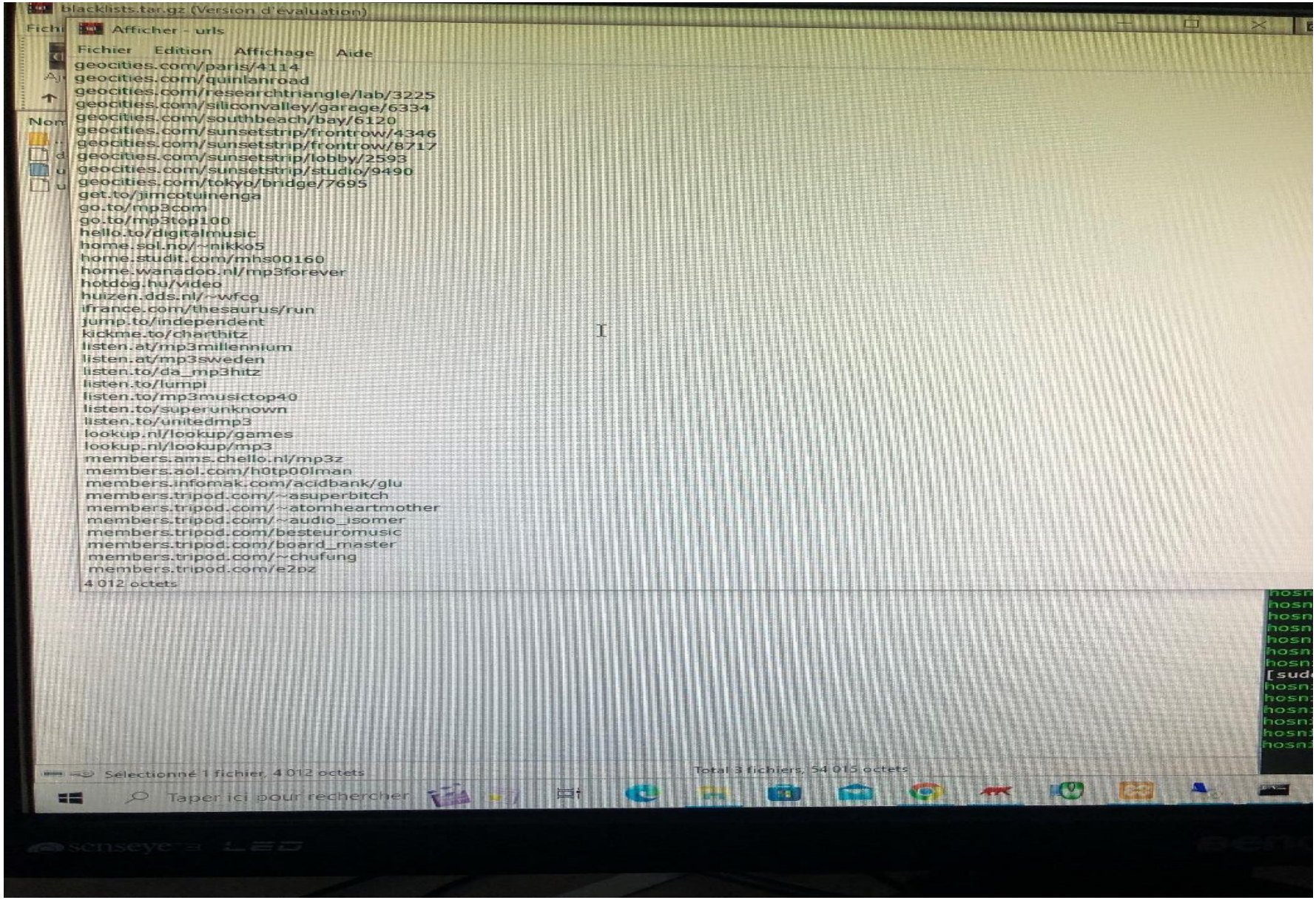

ubuntu-server:/etc/squid$ ls
errorpage.css squid.conf
ubuntu-server:/etc/squid$ nano squid.conf
ubuntu-server:/etc/squid$ hosni@ubuntu-server:/etc/squid$ sudo nano squid.conf
ubuntu-server:/etc/squid$ hosni@ubuntu-server:/etc/squid$ service squid restart
AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
ntication is required to restart 'squid.service'.
nticating as: administrateur (hosni)
ord:
AUTHENTICATION COMPLETE ===
i@ubuntu-server:/etc/squid$ sudo service squid restart
i@ubuntu-server:/etc/squid$

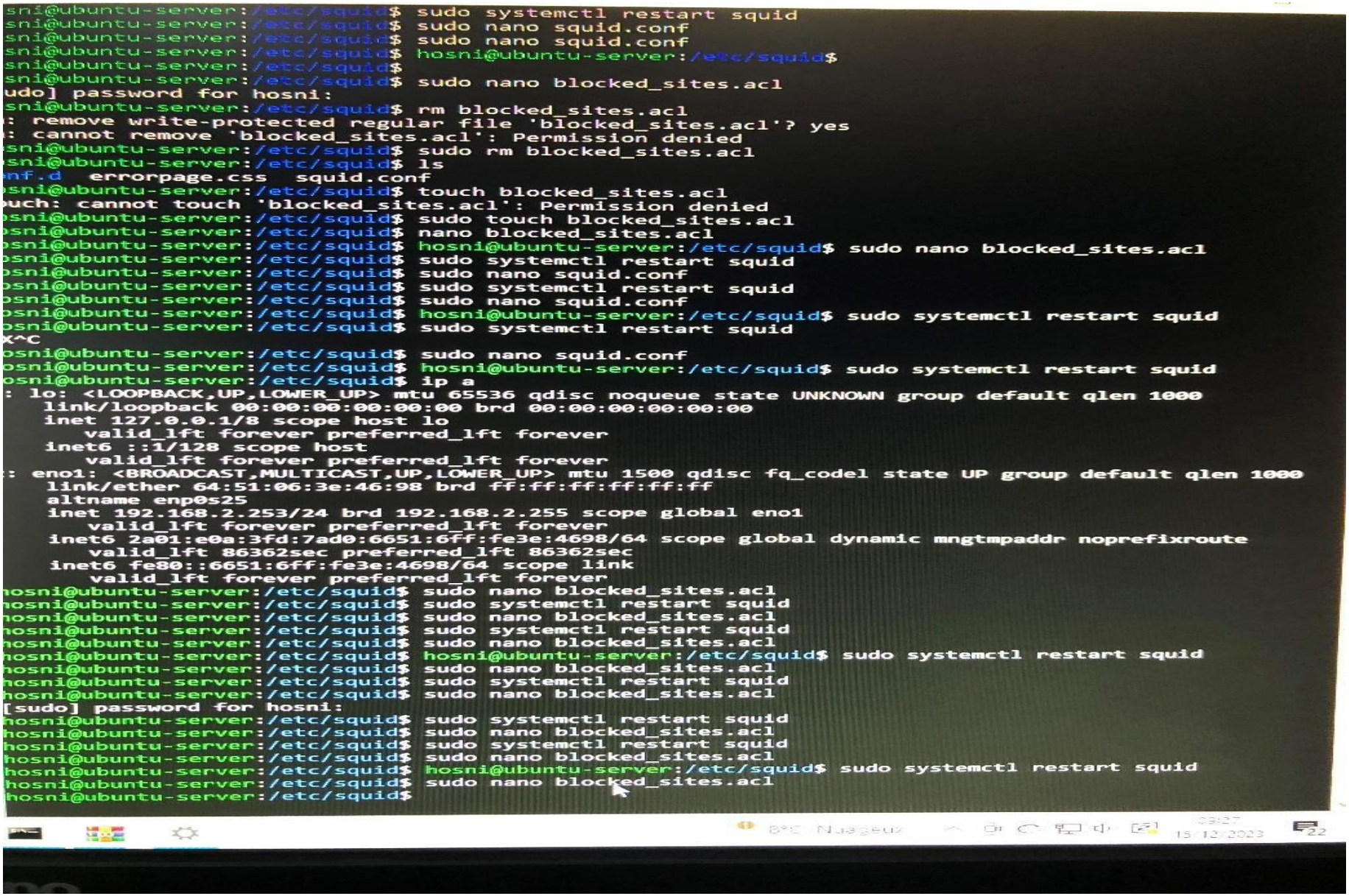

user sessions are running outdated binaries.
VM guests are running outdated hypervisor (qemu) binaries on this host.
sni@ubuntu-server:/etc/squid$ sudo netstat -tulpn | grep squid
p6 0 0 :::3128 :::* LISTEN 15727/(squid-1)
p 0 0 0.0.0.0:58089 0.0.0.0:* 15727/(squid-1)
p6 0 0 :::52209 :::* 15727/(squid-1)
sni@ubuntu-server:/etc/squid$ sudo nano blocked_sites.acl
sni@ubuntu-server:/etc/squid$ hosni@ubuntu-server:/etc/squid$ sudo chmod 644 /etc/squid/blocked_sit
uch /etc/squid/blocked_sites.a
sni@ubuntu-server:/etc/squid$
sni@ubuntu-server:/etc/squid$ sudo nano squid.conf
sni@ubuntu-server:/etc/squid$ sudo nano blocked_sites.acl
sni@ubuntu-server:/etc/squid$ sudo nano squid.conf
sni@ubuntu-server:/etc/squid$ sudo nano squid.conf
sni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
sni@ubuntu-server:/etc/squid$ sudo nano squid.conf
sni@ubuntu-server:/etc/squid$ sudo nano squid.conf
sni@ubuntu-server:/etc/squid$ hosni@ubuntu-server:/etc/squid$
sni@ubuntu-server:/etc/squid$
sni@ubuntu-server:/etc/squid$ sudo nano blocked_sites.acl
udo] password for hosni:
sni@ubuntu-server:/etc/squid$ rm blocked_sites.acl
: remove write-protected regular file 'blocked_sites.acl'? yes
: cannot remove 'blocked_sites.acl': Permission denied
sni@ubuntu-server:/etc/squid$ sudo rm blocked_sites.acl
sni@ubuntu-server:/etc/squid$ ls
nf.d errorpage.css squid.conf
sni@ubuntu-server:/etc/squid$ touch blocked_sites.acl
uch: cannot touch 'blocked_sites.acl': Permission denied
sni@ubuntu-server:/etc/squid$ sudo touch blocked_sites.acl
sni@ubuntu-server:/etc/squid$ nano blocked_sites.acl
sni@ubuntu-server:/etc/squid$ hosni@ubuntu-server:/etc/squid$ sudo nano blocked_sites.acl
sni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
sni@ubuntu-server:/etc/squid$ sudo nano squid.conf
sni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
sni@ubuntu-server:/etc/squid$ sudo nano squid.conf
sni@ubuntu-server:/etc/squid$ hosni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
sni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
^C
sni@ubuntu-server:/etc/squid$ sudo nano squid.conf
sni@ubuntu-server:/etc/squid$ hosni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
sni@ubuntu-server:/etc/squid$ ip a
lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 64:51:06:3e:46:98 brd ff:ff:ff:ff:ff:ff
altname enp0s25
inet 192.168.2.253/24 brd 192.168.2.255 scope global eno1
valid_lft forever preferred_lft forever
inet6 2a01:e0a:3fd:7ad0:6651:6ff:fe3e:4698/64 scope global dynamic mngtmpaddr noprefixroute
valid_lft 86362sec preferred_lft 86362sec
inet6 fe80::6651:6ff:fe3e:4698/64 scope link
valid_lft forever preferred_lft forever
osni@ubuntu-server:/etc/squid$ sudo nano blocked_sites.acl
osni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
8°C Nuageux
16:39
14/12/2023

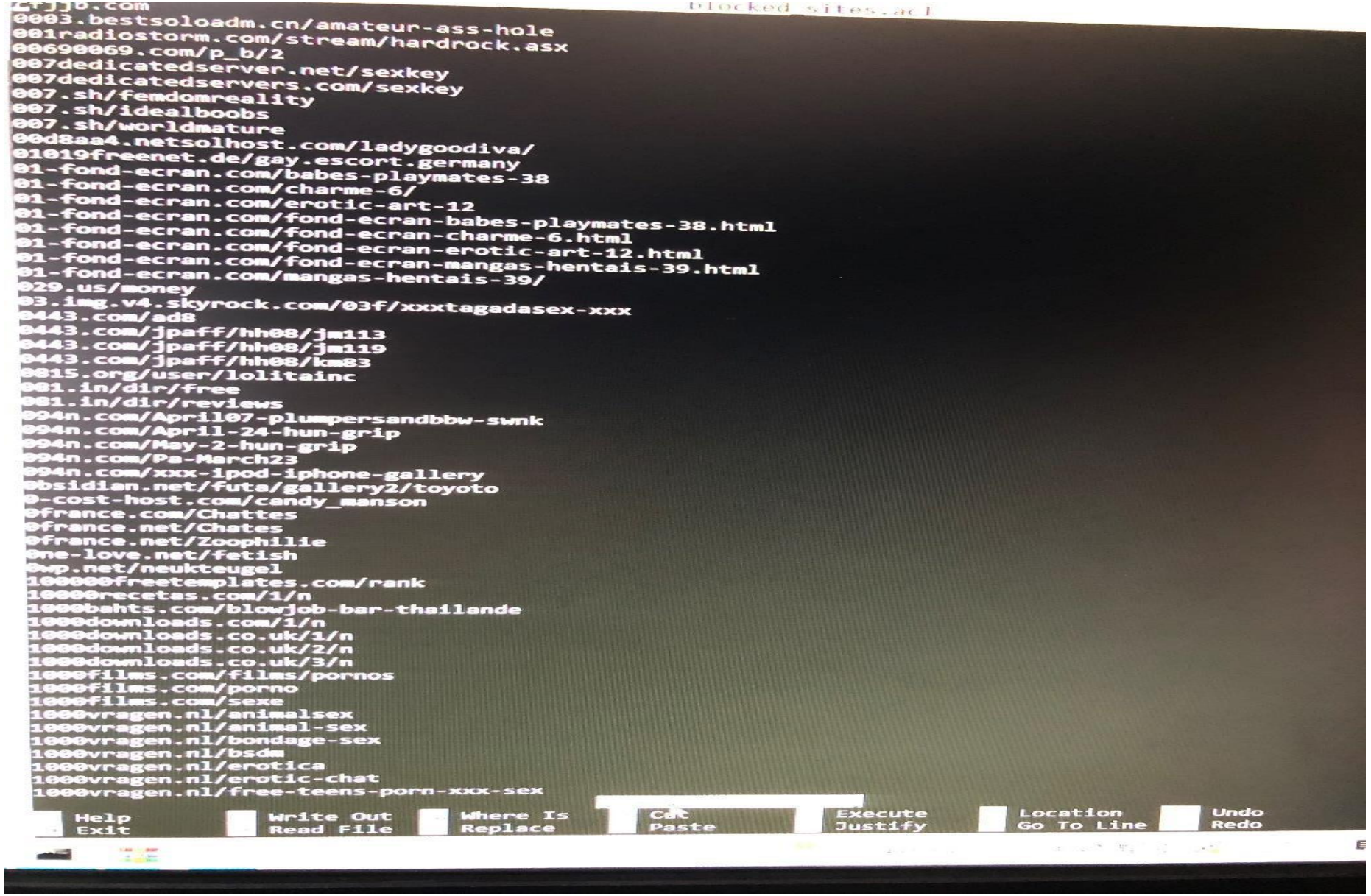

blacklists.tar.gz (Version d'évaluation)
Commandes Outils Favoris Options Aide
Ajouter Extraire vers Tester Afficher Supprimer Rechercher Assistant Informations Antivirus
blacklists.tar.gz\blacklists - TAR+GZIP archive, la taille non compressée est de 31 102 286
Nom Taille Compressé Type Modifié CRC32
arjel 939 ? Dossier de fichiers 11/11/2014 21:21
astrology 555 ? Dossier de fichiers 11/11/2014 21:21
audio-video 54 015 ? Dossier de fichiers 11/11/2014 21:21
bank 25 640 ? Dossier de fichiers 11/11/2014 21:21
bitcoin 4 617 ? Dossier de fichiers 11/11/2014 21:21
blog 23 986 ? Dossier de fichiers 11/11/2014 21:21
celebrity 12 674 ? Dossier de fichiers 11/11/2014 21:21
chat 3 574 ? Dossier de fichiers 11/11/2014 21:21
child 772 ? Dossier de fichiers 11/11/2014 21:21
cleaning 2 474 ? Dossier de fichiers 11/11/2014 21:21
cooking 315 ? Dossier de fichiers 11/11/2014 21:21
dangerous_mat... 1 219 ? Dossier de fichiers 11/11/2014 21:21
dating 61 705 ? Dossier de fichiers 11/11/2014 21:21
drogue 23 590 ? Dossier de fichiers 11/11/2014 21:21
educational_ga... 209 ? Dossier de fichiers 11/11/2014 21:21
filehosting 11 912 ? Dossier de fichiers 11/11/2014 21:21
financial 1 372 ? Dossier de fichiers 11/11/2014 21:21
forums 3 344 ? Dossier de fichiers 11/11/2014 21:21
gambling 19 698 ? Dossier de fichiers 11/11/2014 21:21
games 201 723 ? Dossier de fichiers 11/11/2014 21:21
hacking 4 974 ? Dossier de fichiers 11/11/2014 21:21
jobsearch 5 987 ? Dossier de fichiers 11/11/2014 21:21
lingerie 568 ? Dossier de fichiers 11/11/2014 21:21
liste_bu 40 343 ? Dossier de fichiers 11/11/2014 21:21
malware 3 548 252 ? Dossier de fichiers 11/11/2014 21:21
manga 16 426 ? Dossier de fichiers 11/11/2014 21:21
marketingware 3 235 ? Dossier de fichiers 11/11/2014 21:21
mixed_adult 2 298 ? Dossier de fichiers 11/11/2014 21:21
mobile-phone 811 ? Dossier de fichiers 11/11/2014 21:21
phishing 1 033 471 ? Dossier de fichiers 11/11/2014 21:21
press 80 155 ? Dossier de fichiers 11/11/2014 21:21
publicite 26 182 ? Dossier de fichiers 11/11/2014 21:21
radio 8 093 ? Dossier de fichiers 11/11/2014 21:21
reaffected 240 ? Dossier de fichiers 11/11/2014 21:21
redirector 1 686 369 ? Dossier de fichiers 11/11/2014 21:21
remote-control 664 ? Dossier de fichiers 11/11/2014 21:21
sect 2 693 ? Dossier de fichiers 11/11/2014 21:21
sexual_education 350 ? Dossier de fichiers 11/11/2014 21:21
shopping 624 446 ? Dossier de fichiers 11/11/2014 21:21
social_networks 8 510 ? Dossier de fichiers 11/11/2014 21:21
sports 36 884 ? Dossier de fichiers 11/11/2014 21:21
strict_redirector 1 679 403 ? Dossier de fichiers 11/11/2014 21:21
strong_redirector 1 679 817 ? Dossier de fichiers 11/11/2014 21:21
Sélectionné 1 fichier, 0 octets
Total 49 dossiers, 11 fichiers, 31 102 286 octets

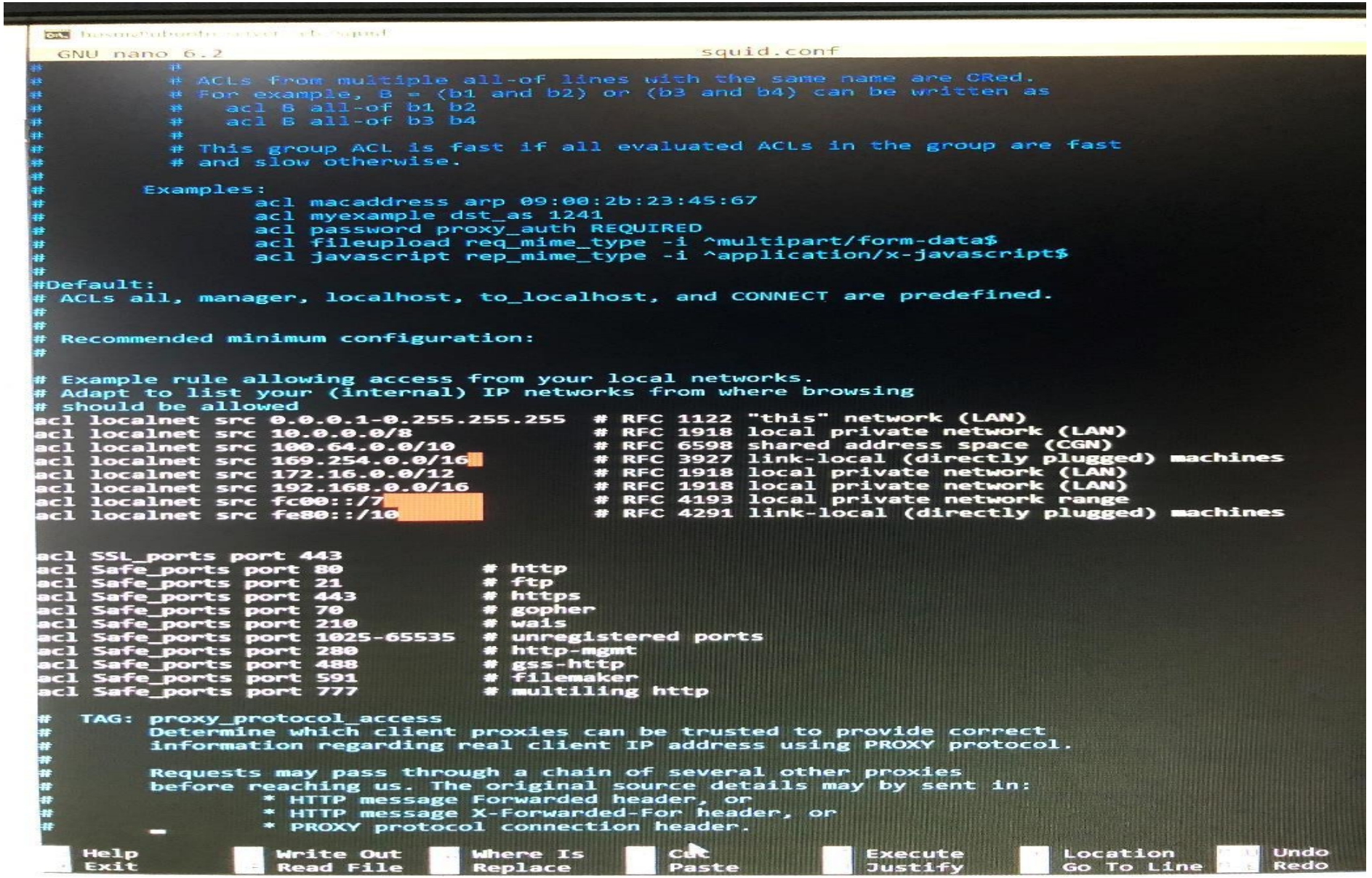

Afficher - urls
Fichier Edition Affichage Aide
134.121.0.99/~dcarp
165.21.101.33/~mp3mania
194.134.35.11/mp3forever
194.134.35.12/mp3forever
194.134.35.17/mp3forever
194.134.35.18/mp3forever
194.134.35.9/mp3forever
194.145.63.33/bg-mp3
195.141.34.45/mp3millennium
195.141.34.45/mp3sweden
195.141.34.45/mp3universe
195.66.60.36/mhs00160
195.96.96.198/~brouns
205.188.134.217/h0tp00lman
205.188.134.248/h0tp00lman
209.202.218.12/az2/freemusic
209.202.218.12/mb/honzicek
213.46.226.40/mp3z
62.108.1.77/mpadberg
62.39.122.10/thesaurus/run
62.39.122.11/thesaurus/run
62.39.122.12/thesaurus/run
62.39.122.13/thesaurus/run
62.39.122.14/thesaurus/run
62.39.122.15/thesaurus/run
62.39.122.16/thesaurus/run
62.39.122.17/thesaurus/run
62.39.122.18/thesaurus/run
62.39.122.19/thesaurus/run
62.39.122.22/thesaurus/run
62.39.122.23/thesaurus/run
64.235.234.138/charthitz
66.132.27.17/submissionwizard
66.150.0.204/topsites
66.200.114.152/equalm
66.218.77.68/broadway/alley/6945
66.218.77.68/damien350
66.218.77.68/malachi3000
66.218.77.68/mp3find
66.218.77.68/quinlanroad
66.218.77.70/broadway/alley/6945
4 012 octets
Sélectionné 1 fichier, 4 012 octets
Total 3 fichiers, 54 015 octets
Taper ici pour rechercher

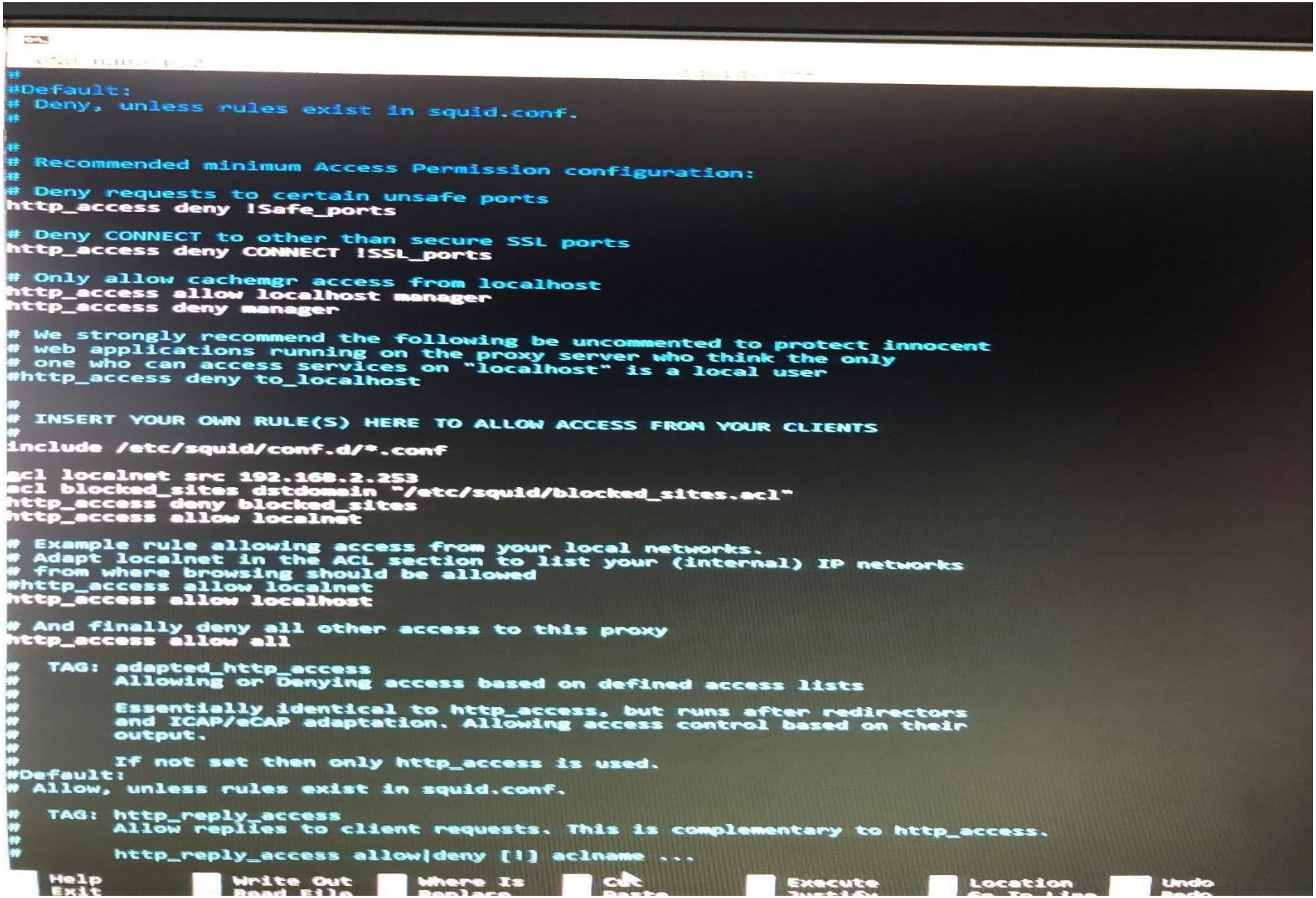

Fichier Commandes Outils Favoris Options Aide
Ajouter
Extraire vers
Tester
Afficher
Supprimer
Rechercher
Assistant
Informations
Antivirus
blacklists.tar.gz\blacklists\audio-video - TAR+GZIP archive, la taille non compressée est de 31 102 286
Nom Taille Compressé Type Modifié CRC32
.. Dossier de fichiers
domains 49 997 ? Fichier 11/11/2014 07:50
urls 4 012 ? Fichier 11/11/2014 07:51
usage 6 ? Fichier 23/05/2005 10:45
Total 3 fichiers, 54 015 octets
Taper ici pour rechercher

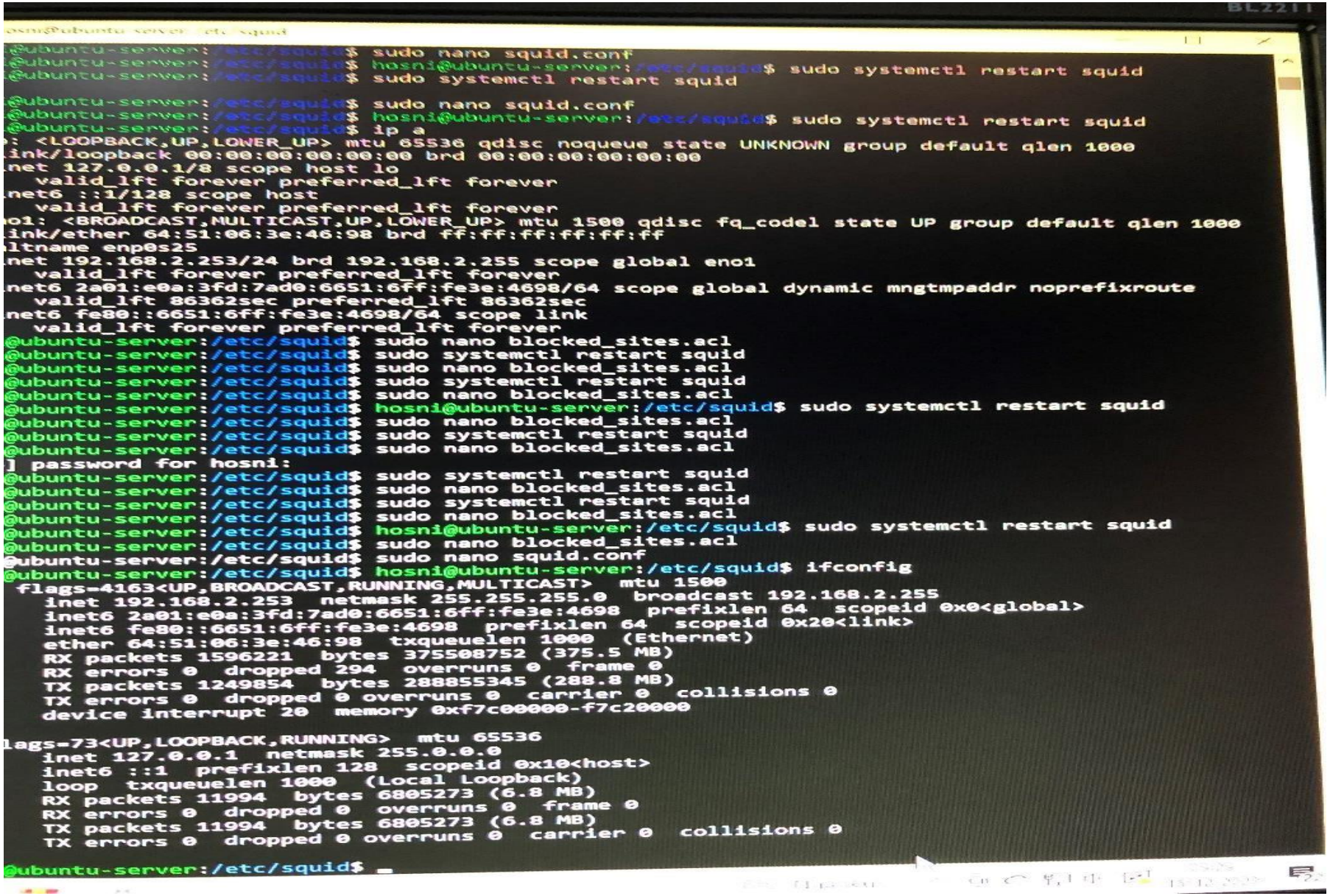

blacklists.tar.gz (Version d'évaluation)
Afficher - urls
Fichier Edition Affichage Aide
geocities.com/paris/4114
geocities.com/quinlanroad
geocities.com/researchtriangle/lab/3225
geocities.com/siliconvalley/garage/6334
geocities.com/southbeach/bay/6120
geocities.com/sunsetstrip/frontrow/4346
geocities.com/sunsetstrip/frontrow/8717
geocities.com/sunsetstrip/lobby/2593
geocities.com/sunsetstrip/studio/9490
geocities.com/tokyo/bridge/7695
get.to/jimcotuinenga
go.to/mp3com
go.to/mp3top100
hello.to/digitalmusic
home.sol.no/~nikko5
home.studit.com/mhs00160
home.wanadoo.nl/mp3forever
hotdog.hu/video
huizen.dds.nl/~wfcg
ifrance.com/thesaurus/run
jump.to/independent
kickme.to/charthitz
listen.at/mp3millennium
listen.at/mp3sweden
listen.to/da_mp3hitz
listen.to/lumpi
listen.to/mp3musictop40
listen.to/superunknown
listen.to/unitedmp3
lookup.nl/lookup/games
lookup.nl/lookup/mp3
members.ams.chello.nl/mp3z
members.aol.com/h0tp00lman
members.infomak.com/acidbank/glu
members.tripod.com/~asuperbitch
members.tripod.com/~atomheartmother
members.tripod.com/~audio_isomer
members.tripod.com/besteuromusic
members.tripod.com/board_master
members.tripod.com/~chufung
members.tripod.com/e2pz
4 012 octets
Sélectionné 1 fichier, 4 012 octets
Total 3 fichiers, 54 015 octets
Taper ici pour rechercher

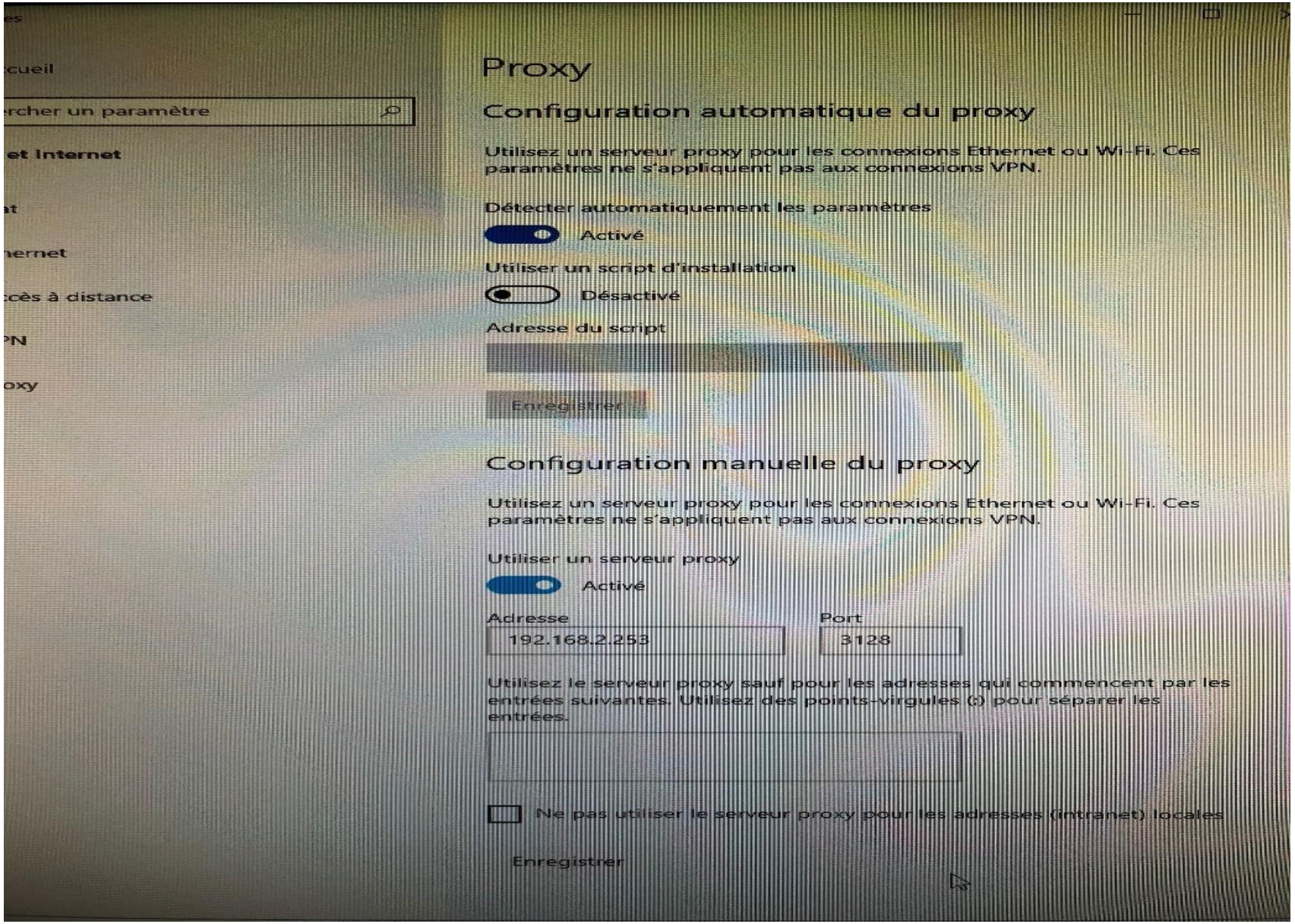

sni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
sni@ubuntu-server:/etc/squid$ sudo nano squid.conf
sni@ubuntu-server:/etc/squid$ sudo nano squid.conf
sni@ubuntu-server:/etc/squid$ hosni@ubuntu-server:/etc/squid$
sni@ubuntu-server:/etc/squid$
sni@ubuntu-server:/etc/squid$ sudo nano blocked_sites.acl
udo] password for hosni:
sni@ubuntu-server:/etc/squid$ rm blocked_sites.acl
: remove write-protected regular file 'blocked_sites.acl'? yes
: cannot remove 'blocked_sites.acl': Permission denied
sni@ubuntu-server:/etc/squid$ sudo rm blocked_sites.acl
sni@ubuntu-server:/etc/squid$ ls
nf.d errorpage.css squid.conf
sni@ubuntu-server:/etc/squid$ touch blocked_sites.acl
uch: cannot touch 'blocked_sites.acl': Permission denied
sni@ubuntu-server:/etc/squid$ sudo touch blocked_sites.acl
sni@ubuntu-server:/etc/squid$ nano blocked_sites.acl
sni@ubuntu-server:/etc/squid$ hosni@ubuntu-server:/etc/squid$ sudo nano blocked_sites.acl
sni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
sni@ubuntu-server:/etc/squid$ sudo nano squid.conf
sni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
sni@ubuntu-server:/etc/squid$ sudo nano squid.conf
sni@ubuntu-server:/etc/squid$ hosni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
sni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
X^C
sni@ubuntu-server:/etc/squid$ sudo nano squid.conf
sni@ubuntu-server:/etc/squid$ hosni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
sni@ubuntu-server:/etc/squid$ ip a
: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
: eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 64:51:06:3e:46:98 brd ff:ff:ff:ff:ff:ff
altname enp0s25
inet 192.168.2.253/24 brd 192.168.2.255 scope global eno1
valid_lft forever preferred_lft forever
inet6 2a01:e0a:3fd:7ad0:6651:6ff:fe3e:4698/64 scope global dynamic mngtmpaddr noprefixroute
valid_lft 86362sec preferred_lft 86362sec
inet6 fe80::6651:6ff:fe3e:4698/64 scope link
valid_lft forever preferred_lft forever
hosni@ubuntu-server:/etc/squid$ sudo nano blocked_sites.acl
hosni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
hosni@ubuntu-server:/etc/squid$ sudo nano blocked_sites.acl
hosni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
hosni@ubuntu-server:/etc/squid$ sudo nano blocked_sites.acl
hosni@ubuntu-server:/etc/squid$ hosni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
hosni@ubuntu-server:/etc/squid$ sudo nano blocked_sites.acl
hosni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
hosni@ubuntu-server:/etc/squid$ sudo nano blocked_sites.acl
[sudo] password for hosni:
hosni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
hosni@ubuntu-server:/etc/squid$ sudo nano blocked_sites.acl
hosni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
hosni@ubuntu-server:/etc/squid$ sudo nano blocked_sites.acl
hosni@ubuntu-server:/etc/squid$ hosni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
hosni@ubuntu-server:/etc/squid$ sudo nano blocked_sites.acl
hosni@ubuntu-server:/etc/squid$

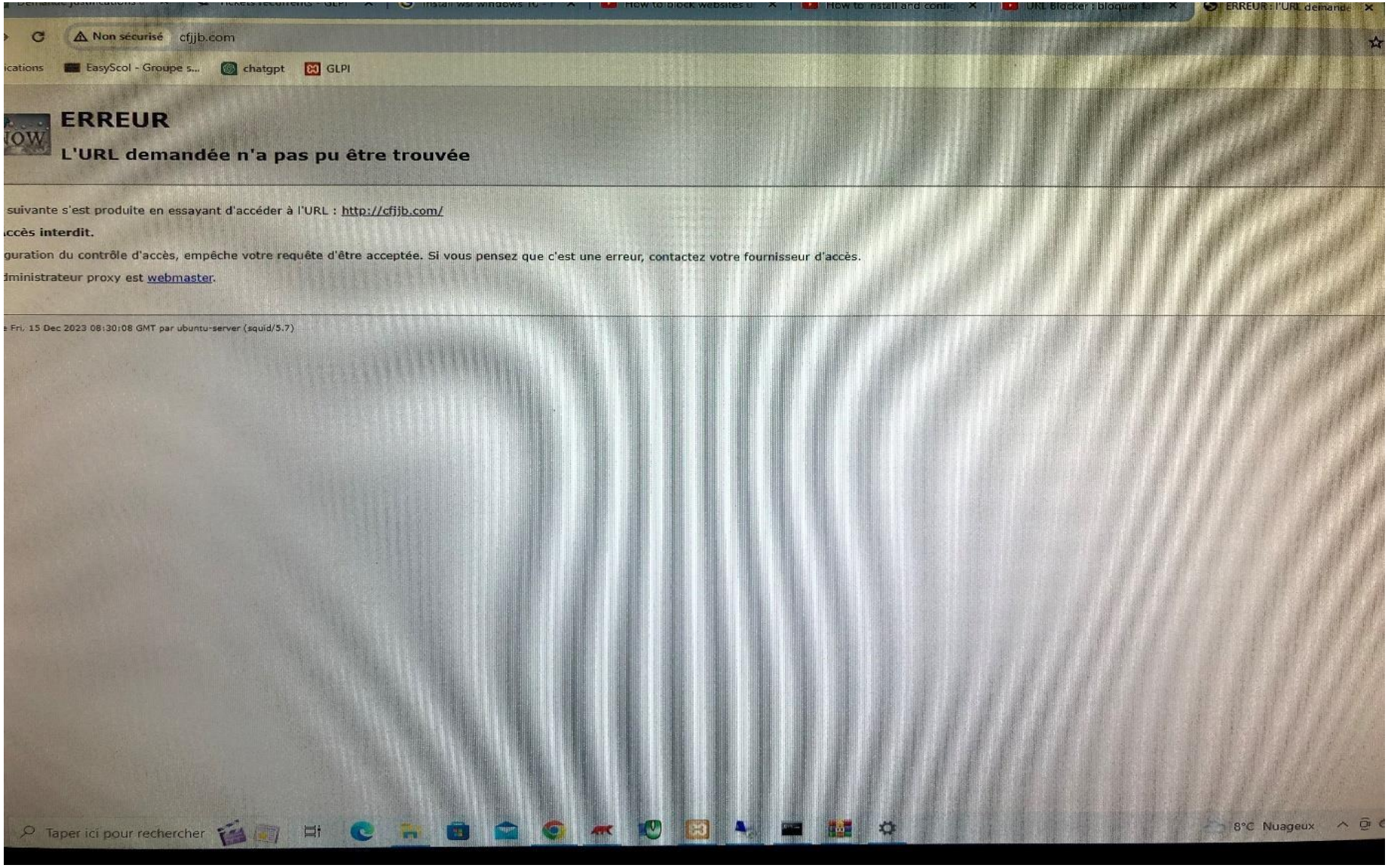

blocked_sites.acl
0003.bestsoloadm.cn/amateur-ass-hole
001radiostorm.com/stream/hardrock.asx
00690069.com/p_b/2
007dedicatedserver.net/sexkey
007dedicatedservers.com/sexkey
007.sh/femdomreality
007.sh/idealboobs
007.sh/worldmature
00d8aa4.netsolhost.com/ladygoodiva/
01019freenet.de/gay.escort.germany
01-fond-ecran.com/babes-playmates-38
01-fond-ecran.com/charme-6/
01-fond-ecran.com/erotic-art-12
01-fond-ecran.com/fond-ecran-babes-playmates-38.html
01-fond-ecran.com/fond-ecran-charme-6.html
01-fond-ecran.com/fond-ecran-erotic-art-12.html
01-fond-ecran.com/fond-ecran-mangas-hentais-39.html
01-fond-ecran.com/mangas-hentais-39/
029.us/money
03.img.v4.skyrock.com/03f/xxxtagadasex-xxx
0443.com/ad8
0443.com/jpaff/hh08/jm113
0443.com/jpaff/hh08/jm119
0443.com/jpaff/hh08/km83
0815.org/user/lolitainc
081.in/dir/free
081.in/dir/reviews
094n.com/April07-plumpersandbbw-swnk
094n.com/April-24-hun-grip
094n.com/May-2-hun-grip
094n.com/Pa-March23
094n.com/xxx-ipod-iphone-gallery
0bsidian.net/futa/gallery2/toyoto
0-cost-host.com/candy_manson
0france.com/Chattes
0france.net/Chates
0france.net/Zoophilie
0ne-love.net/fetish
0wp.net/neukteugel
100000freetemplates.com/rank
10000recetas.com/1/n
1000bahts.com/blowjob-bar-thailande
1000downloads.com/1/n
1000downloads.co.uk/1/n
1000downloads.co.uk/2/n
1000downloads.co.uk/3/n
1000films.com/films/pornos
1000films.com/porno
1000films.com/sexe
1000vragen.nl/animalsex
1000vragen.nl/animal-sex
1000vragen.nl/bondage-sex
1000vragen.nl/bsdm
1000vragen.nl/erotica
1000vragen.nl/erotic-chat
1000vragen.nl/free-teens-porn-xxx-sex
Help
Exit
Write Out
Read File
Where Is
Replace
Cut
Paste
Execute
Justify
Location
Go To Line
Undo
Redo


GNU nano 6.2
squid.conf
#
ACLs from multiple all-of lines with the same name are CRed.
For example, B = (b1 and b2) or (b3 and b4) can be written as
acl B all-of b1 b2
acl B all-of b3 b4
#
This group ACL is fast if all evaluated ACLs in the group are fast
and slow otherwise.
#
Examples:
acl macaddress arp 09:00:2b:23:45:67
acl myexample dst_as 1241
acl password proxy_auth REQUIRED
acl fileupload req_mime_type -i ^multipart/form-data$
acl javascript rep_mime_type -i ^application/x-javascript$
#
#Default:
ACLs all, manager, localhost, to_localhost, and CONNECT are predefined.
#
#
Recommended minimum configuration:
#
Example rule allowing access from your local networks.
Adapt to list your (internal) IP networks from where browsing
should be allowed
acl localnet src 0.0.0.1-0.255.255.255 # RFC 1122 "this" network (LAN)
acl localnet src 10.0.0.0/8   # RFC 1918 local private network (LAN)
acl localnet src 100.64.0.0/10   # RFC 6598 shared address space (CGN)
acl localnet src 169.254.0.0/16   # RFC 3927 link-local (directly plugged) machines
acl localnet src 172.16.0.0/12   # RFC 1918 local private network (LAN)
acl localnet src 192.168.0.0/16   # RFC 1918 local private network (LAN)
acl localnet src fc00::/7   # RFC 4193 local private network range
acl localnet src fe80::/10   # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80   # http
acl Safe_ports port 21   # ftp
acl Safe_ports port 443   # https
acl Safe_ports port 70   # gopher
acl Safe_ports port 210   # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280   # http-mgmt
acl Safe_ports port 488   # gss-http
acl Safe_ports port 591   # filemaker
acl Safe_ports port 777   # multiling http
TAG: proxy_protocol_access
Determine which client proxies can be trusted to provide correct
information regarding real client IP address using PROXY protocol.
#
Requests may pass through a chain of several other proxies
before reaching us. The original source details may by sent in:
* HTTP message Forwarded header, or
* HTTP message X-Forwarded-For header, or
* PROXY protocol connection header.
^G Help
^X Exit
^O Write Out
^R Read File
^W Where Is
^\ Replace
^K Cut
^U Paste
^T Execute
^J Justify
^C Location
M-G Go To Line
M-U Undo
M-E Redo

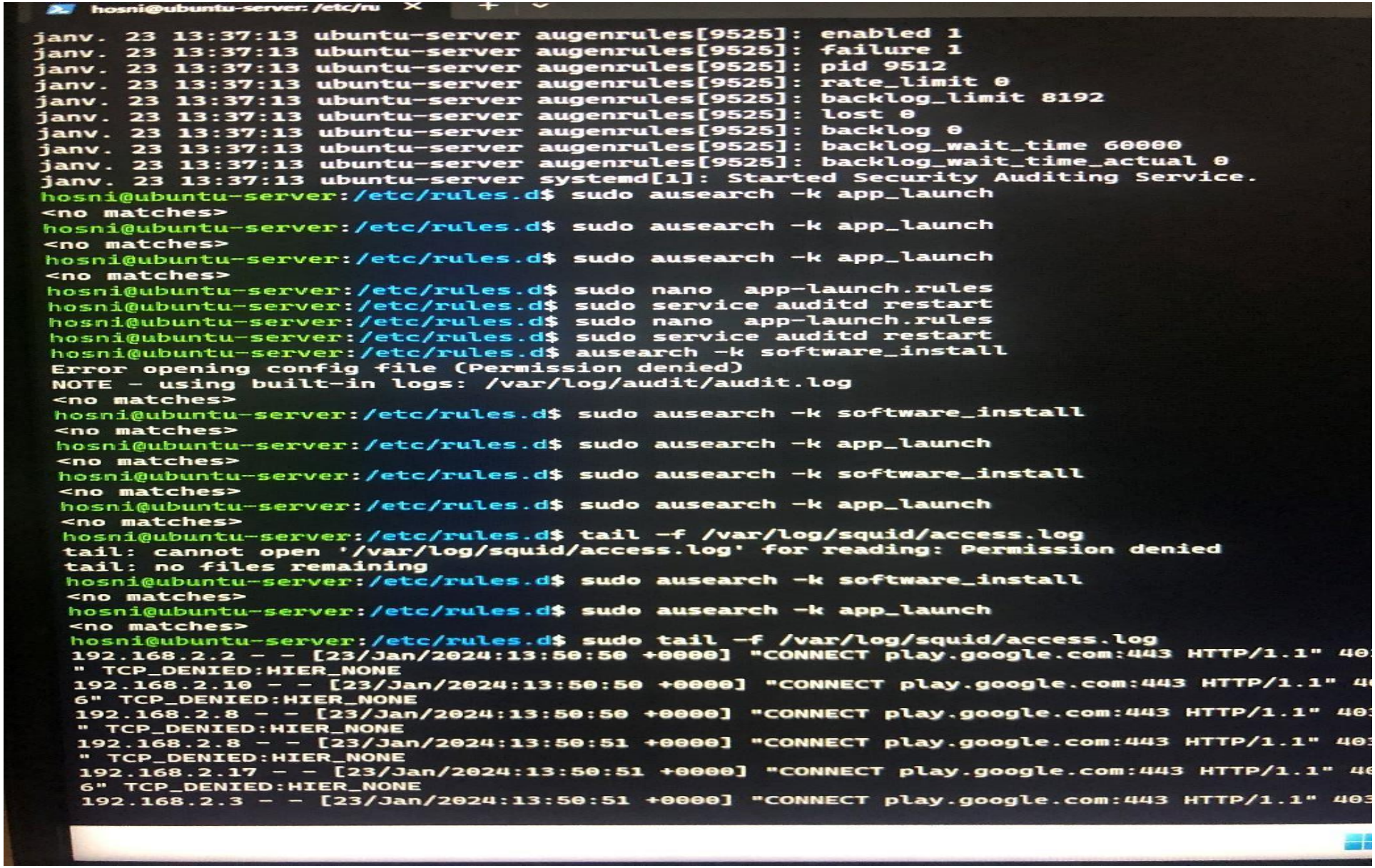

#
#Default:
Deny, unless rules exist in squid.conf.
#
#
Recommended minimum Access Permission configuration:
#
Deny requests to certain unsafe ports
http_access deny !Safe_ports
Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports
Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager
We strongly recommend the following be uncommented to protect innocent
web applications running on the proxy server who think the only
one who can access services on "localhost" is a local user
#http_access deny to_localhost
#
INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
include /etc/squid/conf.d/*.conf
acl localnet src 192.168.2.253
acl blocked_sites dstdomain "/etc/squid/blocked_sites.acl"
http_access deny blocked_sites
http_access allow localnet
Example rule allowing access from your local networks.
Adapt localnet in the ACL section to list your (internal) IP networks
from where browsing should be allowed
#http_access allow localnet
http_access allow localhost
And finally deny all other access to this proxy
http_access allow all
TAG: adapted_http_access
Allowing or Denying access based on defined access lists
#
Essentially identical to http_access, but runs after redirectors
and ICAP/eCAP adaptation. Allowing access control based on their
output.
#
If not set then only http_access is used.
#Default:
Allow, unless rules exist in squid.conf.
TAG: http_reply_access
Allow replies to client requests. This is complementary to http_access.
#
http_reply_access allow|deny [!] aclname ...
Help
Write Out
Where Is
Execute
Location
Undo


@ubuntu-server:/etc/squid$ sudo nano squid.conf
@ubuntu-server:/etc/squid$ hosni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
@ubuntu-server:/etc/squid$ sudo systemctl restart squid
@ubuntu-server:/etc/squid$ sudo nano squid.conf
@ubuntu-server:/etc/squid$ hosni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
@ubuntu-server:/etc/squid$ ip a
: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
o1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 64:51:06:3e:46:98 brd ff:ff:ff:ff:ff:ff
altname enp0s25
inet 192.168.2.253/24 brd 192.168.2.255 scope global eno1
valid_lft forever preferred_lft forever
inet6 2a01:e0a:3fd:7ad0:6651:6ff:fe3e:4698/64 scope global dynamic mngtmpaddr noprefixroute
valid_lft 86362sec preferred_lft 86362sec
inet6 fe80::6651:6ff:fe3e:4698/64 scope link
valid_lft forever preferred_lft forever
@ubuntu-server:/etc/squid$ sudo nano blocked_sites.acl
@ubuntu-server:/etc/squid$ sudo systemctl restart squid
@ubuntu-server:/etc/squid$ sudo nano blocked_sites.acl
@ubuntu-server:/etc/squid$ sudo systemctl restart squid
@ubuntu-server:/etc/squid$ sudo nano blocked_sites.acl
@ubuntu-server:/etc/squid$ hosni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
@ubuntu-server:/etc/squid$ sudo nano blocked_sites.acl
@ubuntu-server:/etc/squid$ sudo systemctl restart squid
@ubuntu-server:/etc/squid$ sudo nano blocked_sites.acl
] password for hosni:
@ubuntu-server:/etc/squid$ sudo systemctl restart squid
@ubuntu-server:/etc/squid$ sudo nano blocked_sites.acl
@ubuntu-server:/etc/squid$ sudo systemctl restart squid
@ubuntu-server:/etc/squid$ sudo nano blocked_sites.acl
@ubuntu-server:/etc/squid$ hosni@ubuntu-server:/etc/squid$ sudo systemctl restart squid
@ubuntu-server:/etc/squid$ sudo nano blocked_sites.acl
@ubuntu-server:/etc/squid$ sudo nano squid.conf
@ubuntu-server:/etc/squid$ hosni@ubuntu-server:/etc/squid$ ifconfig
flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.2.253 netmask 255.255.255.0 broadcast 192.168.2.255
inet6 2a01:e0a:3fd:7ad0:6651:6ff:fe3e:4698 prefixlen 64 scopeid 0x0<global>
inet6 fe80::6651:6ff:fe3e:4698 prefixlen 64 scopeid 0x20<link>
ether 64:51:06:3e:46:98 txqueuelen 1000 (Ethernet)
RX packets 1596221 bytes 375508752 (375.5 MB)
RX errors 0 dropped 294 overruns 0 frame 0
TX packets 1249854 bytes 288855345 (288.8 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device interrupt 20 memory 0xf7c00000-f7c20000
lags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 11994 bytes 6805273 (6.8 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 11994 bytes 6805273 (6.8 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
@ubuntu-server:/etc/squid$


Proxy
Configuration automatique du proxy
Utilisez un serveur proxy pour les connexions Ethernet ou Wi-Fi. Ces paramètres ne s'appliquent pas aux connexions VPN.
Détecter automatiquement les paramètres
Activé
Utiliser un script d'installation
Désactivé
Adresse du script
Enregistrer
Configuration manuelle du proxy
Utilisez un serveur proxy pour les connexions Ethernet ou Wi-Fi. Ces paramètres ne s'appliquent pas aux connexions VPN.
Utiliser un serveur proxy
Activé
Adresse
192.168.2.253
Port
3128
Utilisez le serveur proxy sauf pour les adresses qui commencent par les entrées suivantes. Utilisez des points-virgules (;) pour séparer les entrées.
Ne pas utiliser le serveur proxy pour les adresses (intranet) locales
Enregistrer


Non sécurisé
cfjjb.com
EasyScol - Groupe s...
chatgpt
GLPI
ERREUR
L'URL demandée n'a pas pu être trouvée
suivante s'est produite en essayant d'accéder à l'URL : http://cfjjb.com/
ccès interdit.
guration du contrôle d'accès, empêche votre requête d'être acceptée. Si vous pensez que c'est une erreur, contactez votre fournisseur d'accès.
dministrateur proxy est webmaster.
Fri, 15 Dec 2023 08:30:08 GMT par ubuntu-server (squid/5.7)
Taper ici pour rechercher
8°C Nuageux

```
 GNU nano 6.2                                                    squid.conf
http_access deny manager

# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

include /etc/squid/conf.d/*.conf
acl localnet src 192.168.2.253
acl blocked_sites dstdomain "/etc/squid/blocked_sites.acl"
acl bloque_porn url_regex -i porn
acl bloque_jeux url_regex -i jeu
acl bloque_game url_regex -i game
acl bloque_play url_regex -i play
acl bloque_viol url_regex -i viol
acl bloque_download url_regex -i download
acl bloque_telechargement url_regex -i telec
#acl bloque_xx url_regex -i x
http_access deny bloque_download
http_access deny bloque_play
http_access deny bloque_telechargement
http_access deny blocked_sites
http_access deny bloque_viol
http_access deny bloque_jeux
http_access deny bloque_game
http_access deny bloque_porn
#http_access deny bloque_xx


# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
#http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
http_access allow all

#  TAG: adapted_http_access
#       Allowing or Denying access based on defined access lists
#
#       Essentially identical to http_access, but runs after redirectors
#       and ICAP/eCAP adaptation. Allowing access control based on their
#       output.

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo         M-A Set Mark     M-] To Bracket   M-Q Previous     ^B Back          ^◂ Prev Word
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo         M-6 Copy         ^Q Where Was     M-W Next         ^F Forward       ^▸ Next Word
```


hosni@ubuntu-server: /etc/ru
janv. 23 13:37:13 ubuntu-server augenrules[9525]: enabled 1
janv. 23 13:37:13 ubuntu-server augenrules[9525]: failure 1
janv. 23 13:37:13 ubuntu-server augenrules[9525]: pid 9512
janv. 23 13:37:13 ubuntu-server augenrules[9525]: rate_limit 0
janv. 23 13:37:13 ubuntu-server augenrules[9525]: backlog_limit 8192
janv. 23 13:37:13 ubuntu-server augenrules[9525]: lost 0
janv. 23 13:37:13 ubuntu-server augenrules[9525]: backlog 0
janv. 23 13:37:13 ubuntu-server augenrules[9525]: backlog_wait_time 60000
janv. 23 13:37:13 ubuntu-server augenrules[9525]: backlog_wait_time_actual 0
janv. 23 13:37:13 ubuntu-server systemd[1]: Started Security Auditing Service.
hosni@ubuntu-server:/etc/rules.d$ sudo ausearch -k app_launch
<no matches>
hosni@ubuntu-server:/etc/rules.d$ sudo ausearch -k app_launch
<no matches>
hosni@ubuntu-server:/etc/rules.d$ sudo ausearch -k app_launch
<no matches>
hosni@ubuntu-server:/etc/rules.d$ sudo nano app-launch.rules
hosni@ubuntu-server:/etc/rules.d$ sudo service auditd restart
hosni@ubuntu-server:/etc/rules.d$ sudo nano app-launch.rules
hosni@ubuntu-server:/etc/rules.d$ sudo service auditd restart
hosni@ubuntu-server:/etc/rules.d$ ausearch -k software_install
Error opening config file (Permission denied)
NOTE - using built-in logs: /var/log/audit/audit.log
<no matches>
hosni@ubuntu-server:/etc/rules.d$ sudo ausearch -k software_install
<no matches>
hosni@ubuntu-server:/etc/rules.d$ sudo ausearch -k app_launch
<no matches>
hosni@ubuntu-server:/etc/rules.d$ sudo ausearch -k software_install
<no matches>
hosni@ubuntu-server:/etc/rules.d$ sudo ausearch -k app_launch
<no matches>
hosni@ubuntu-server:/etc/rules.d$ tail -f /var/log/squid/access.log
tail: cannot open '/var/log/squid/access.log' for reading: Permission denied
tail: no files remaining
hosni@ubuntu-server:/etc/rules.d$ sudo ausearch -k software_install
<no matches>
hosni@ubuntu-server:/etc/rules.d$ sudo ausearch -k app_launch
<no matches>
hosni@ubuntu-server:/etc/rules.d$ sudo tail -f /var/log/squid/access.log
192.168.2.2 - - [23/Jan/2024:13:50:50 +0000] "CONNECT play.google.com:443 HTTP/1.1" 40
" TCP_DENIED:HIER_NONE
192.168.2.10 - - [23/Jan/2024:13:50:50 +0000] "CONNECT play.google.com:443 HTTP/1.1" 4
6" TCP_DENIED:HIER_NONE
192.168.2.8 - - [23/Jan/2024:13:50:50 +0000] "CONNECT play.google.com:443 HTTP/1.1" 40
" TCP_DENIED:HIER_NONE
192.168.2.8 - - [23/Jan/2024:13:50:51 +0000] "CONNECT play.google.com:443 HTTP/1.1" 40
" TCP_DENIED:HIER_NONE
192.168.2.17 - - [23/Jan/2024:13:50:51 +0000] "CONNECT play.google.com:443 HTTP/1.1" 4
6" TCP_DENIED:HIER_NONE
192.168.2.3 - - [23/Jan/2024:13:50:51 +0000] "CONNECT play.google.com:443 HTTP/1.1" 403