



# Fiche de manuel du logiciel IDS GORAD

- Utilité : Multi-usage (administration des systèmes, hacking éthique, surveillance de votre ordinateur)
- But : Contrôler les machines cibles par des commandes | attaques (bouger les souris, ouvrir des sites, BSOD (écran bleu de la mort))

Architecture du logiciel :

- le logiciel tourne sur l'architecture client / serveur

Serveur IDS GORAD

| Agent

- LAN (réseau local - par adresse ip ex:192.168.43.212)
- WAN (réseaux internet par passerelle comme pagekite ou serveo)

Comment l'installer ?

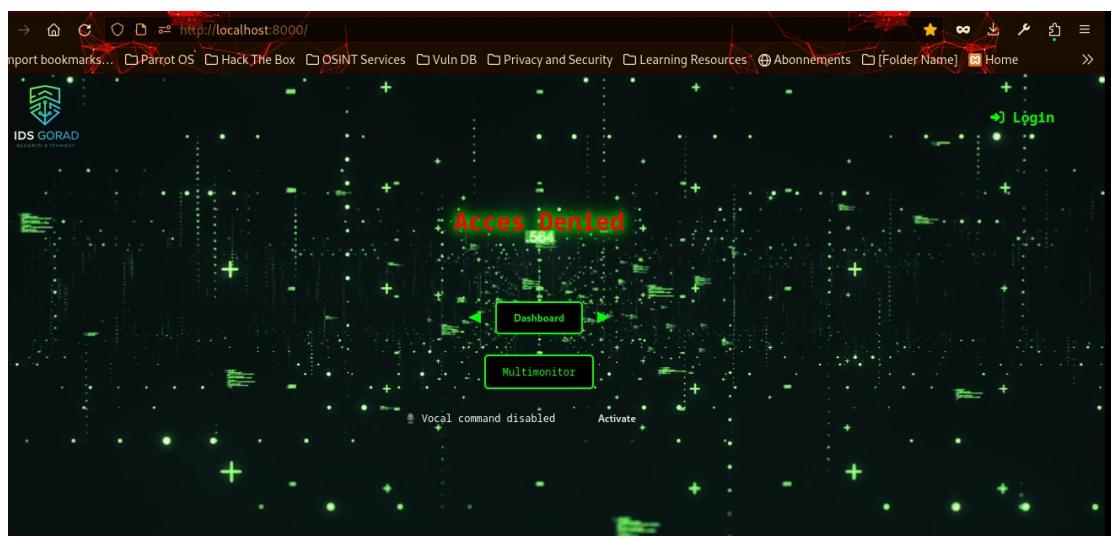
étape 1 : Obtenir le fichier GORAD-PACKAGE.deb

étape 2 : ouvrir un terminal en mode superutilisateur par la commande «**sudo su**»

étape 3 : naviger vers le répertoire où GORAD-PACKAGE se place

étape 4 : Lancer la commande **dpkg -i GORAD-PACKAGE.deb** **NB:** Vous devez avoir de la connexion internet pendant l'installation pour installer toutes les dépendances

étape 5: Ouvrir le navigateur et entrez localhost:8000 ensuite l application se lance et demande de s'authentifier en entrant le nom utilisateur : hacker et mot de passe hacker.



Le logiciel possède 2 modes différents :

- Monitor: surveillance de votre ordinateur --pas besoin de connecter sur un réseau {localhost:8000}
- Multimonitor: pour le mode hacker --doit être connecté sur un réseau {votre-adresse-ip:8000} -- continuer la lecture...

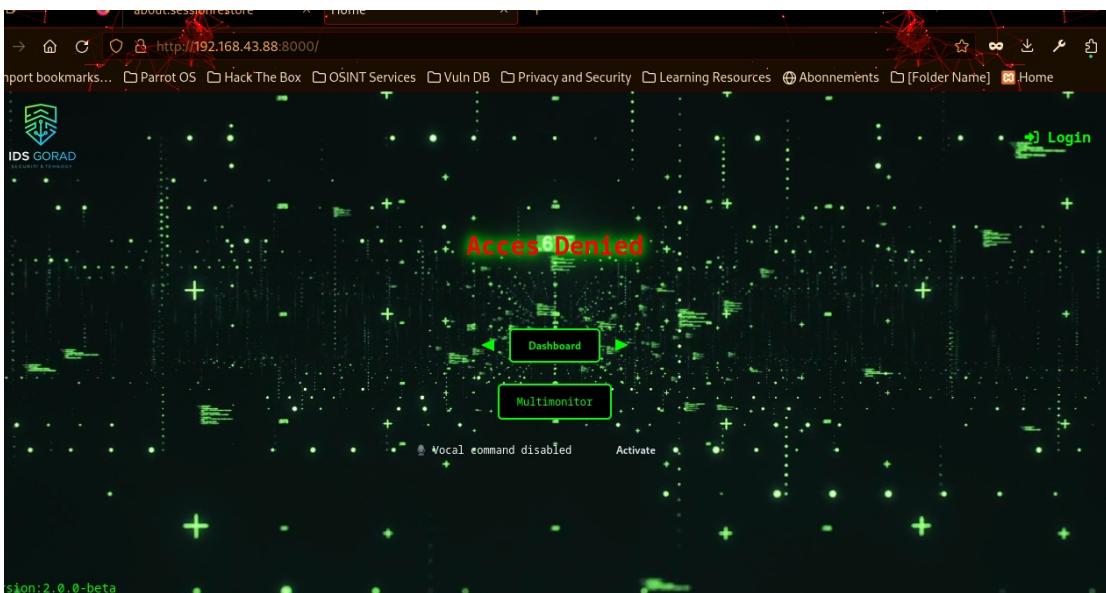
### MODE HACKER:

- Pour surveiller les ordinateurs on a besoin de configurer l'application appelés **agent** (Inclus dans le logiciel)
- Tous d'abord notre ordinateur doit être connecté sur un réseau | ensuite nous devons savoir notre adresse IP en ouvrant une commande et en tapant la commande **ip a** | ou **ifconfig** si en mode super utilisateur

```
[cybergorad@parrot]~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group 0
    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 noprefixroute
            valid_lft forever preferred_lft forever
2: enp4s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel group 2
    link/ether b4:b5:2f:90:0f:9e brd ff:ff:ff:ff:ff:ff
3: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group 3
    link/ether b4:b6:76:32:37:0f brd ff:ff:ff:ff:ff:ff
        altname wlp3s0
        inet 192.168.43.88/24 brd 192.168.43.255 scope global dynamic noprefixroute
            valid_lft 3589sec preferred_lft 3589sec
        inet6 fe80::423c:10eb:967a:3846/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
[cybergorad@parrot]~$
```

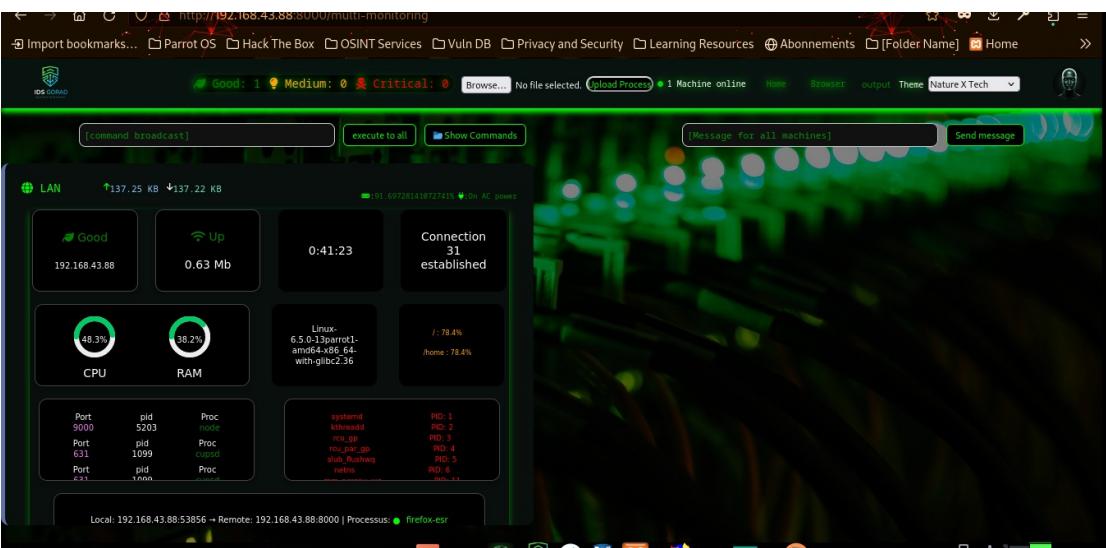
dans cette image l'adresse IP est 192.168.43.88

- Ensuite ouvrant un navigateur et entrant «**votre-adresse-ip:8000**»



**NB:**cette fois on n'est plus sur localhost:8000 mais dans notre ip connecté sur le réseau

- Ensuite Ouvrir un nouveau terminal en mode administrateur et entrant la commande '**systemctl restart multi-gorad**' **IMPORTANT**
  - Ensuite configurer l'application agent en extensions python agent.py  
Voir la section adresse ip et en modifiant sur l'address ip sur votre ordinateur .
  - Lancer l'agent (soit en entrant un terminal et entrant la commande **python3 agent.py** ou en créant un package en utilisant l'outils **pyinstaller**)
  - Les agent connecté s'affiche sur le tableau de bord



<https://ids-gorad-web.onrender.com>

ET C'EST LA QUE ON PEUT CONTROLER LES ORDINATEUR A DISTANCE GRACE AU COMMANDE QUE NOUS TAPONS SUR LA SECTION COMMANDE.