LUMBERJACK

Presented by

Alejandra Reinares, Álvaro Sáenz-Torre, Marino Oliveros, Joan Bayona and Luis Domene

INDEX

Why Lumberjack?

```
stlog                wtmp
ightdm               wtmp.1
nbs                  Xorg.0.log
eech-dispatcher      Xorg.0.log.old
slog
uth.log
uthority=local): Registered Authentication Agent for unix-session
ome/polkit-gnome-authentication-agent-1], object path /org/gnome/

ogind[589]: Removed session c1.
pam_unix(systemd-user:session): session closed for user lightdm
kr-pam: unlocked login keyring
): pam_unix(cron:session): session opened for user root by (uid=0)
): pam_unix(cron:session): session closed for user root
kr-pam: unlocked login keyring
paolo : TTY=pts/5 ; PWD=/home/paolo ; USER=root ; COMMAND=/usr/bin

_unix(sudo:session): session opened for user root by paolo(uid=0)
_unix(sudo:session): session closed for user root

ager[584]: <info>  (wlp12s0): supplicant interface state: 4-way ha

Terminal[1356]: Gtk-Message: GtkDial
```

Scope: A web app

01 DETECTION OF SUSPICIOUS LOG AND REASONS

02 REAL TIME

03 RETRAINING

04 OPEN-SOURCE

Scope

Our team believes in being open-source, so all of the software we create/use will be open source.

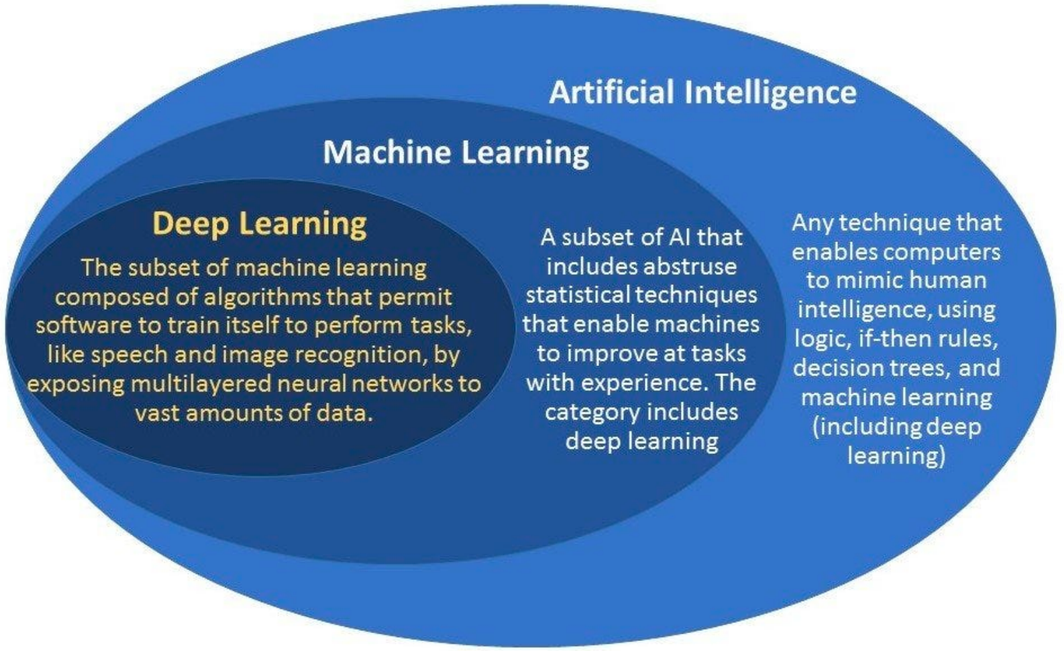
QUALITY AND RESOURCES

Flask

web development,
one drop at a time

QUALITY AND RESOURCES

real time



Prototype


Log Analysis in Real Time
LOG REGISTER
ANALYZER

LOG REGISTER

IP: 10.10.34.257
Score: 0.83 Veredict: Suspicious

IP: 212.23.65.89
Score: 0.18 Veredict: Normal Activity

IP: 27.23.156.234
Score: 0.42 Veredict: Normal Activity

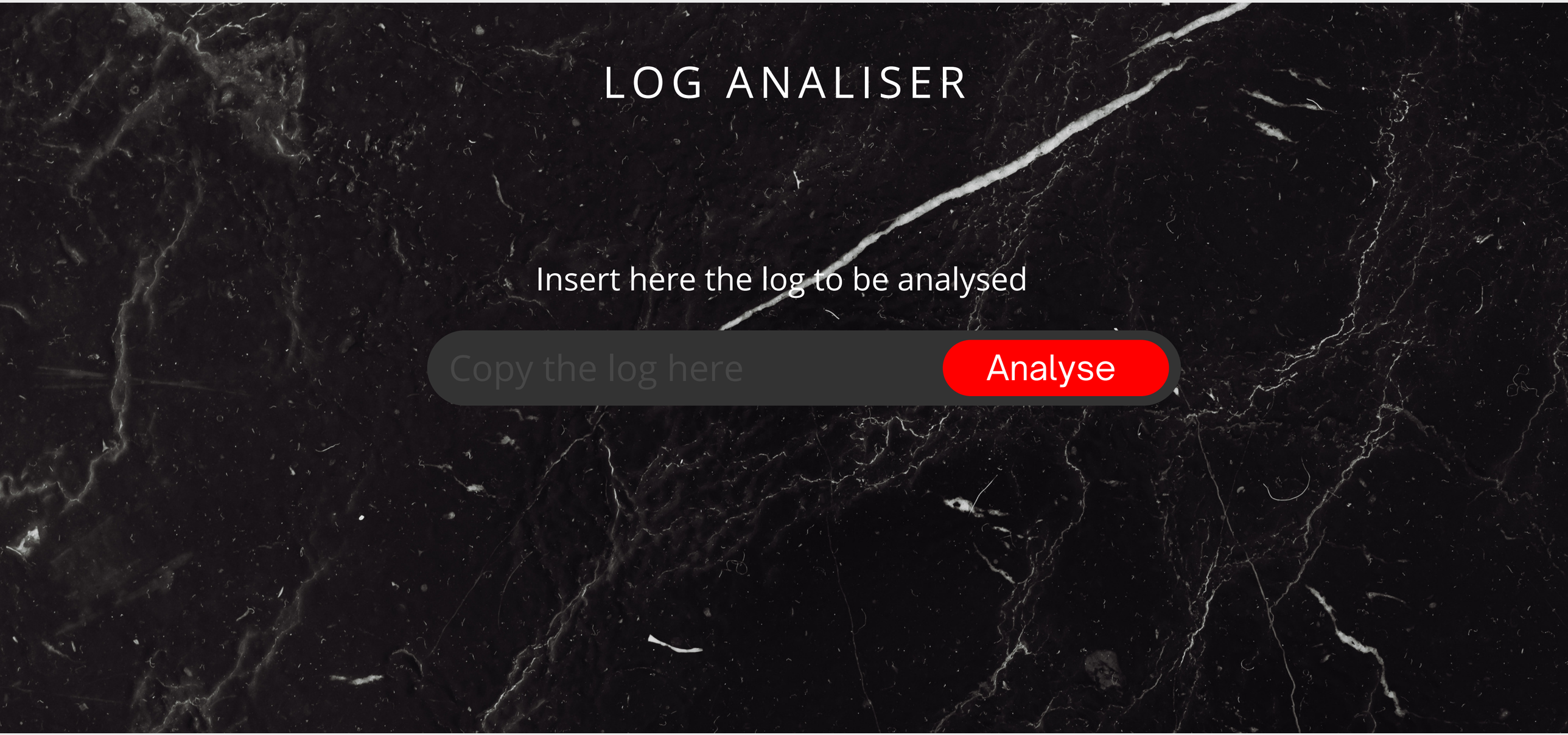
IP: 12.32.45.89
Score: 0.79 Veredict: Suspicious

IP: 13.65.89.123
Score: 0.02 Veredict: Normal Activity

IP: 17.82.78.167
Score: 0.24 Veredict: Normal Activity

IP: 13.67.176.98
Score: 0.16 Veredict: Normal Activity

Extract csv with malicious logs


LOG ANALISER
Insert here the log to be analysed
Copy the log here
Analyse

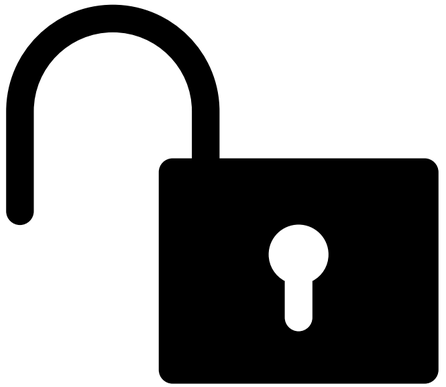
LOG ANALISER

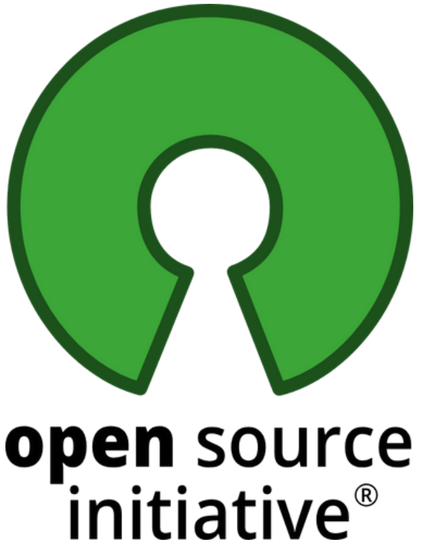
78%

IP ADRESS LOCATED IN BHUTAN

RISKS

CONCLUSIONS





THANKS FOR YOUR ATTENTION