ipt_geofence

github.com/ntop/ipt_geofence

Francesco Lorenzoni

f.lorenzoni4@studenti.unipi.it

frenzis01

Yuri Caprini

y.caprini@studenti.unipi.it

yuricaprini

Salvatore Guastella

s.guastella2@studenti.unipi.it

salvogs

Topics

- What is ipt_geofence?
- Main Features
- Configuration and Execution
- Architecture
- Performance Evaluation
- Future improvements

What is ipt_geofence?

- A tool that allows you to protect your host or network by blocking incoming/outcoming connections from/to unwanted countries or continents (**geofencing**).
- Not only *"geo"*: can also be configured to block connections from/to specified unwanted hosts (**blacklisting**) or from/to hosts connecting on specified port ranges (**honeypot**)
- More on that later...

Main Features

Geofencing

Based on **.mmdb database** (maxmind/dbip)
to determine country of an host

You can:

- Choose default policy to **PASS** or **DROP** packets
- Specify **countries** to be *blacklisted* or *whitelisted*
- Filter packets with specific tcp/udp ports

Blacklisting

Load potentially malicious hosts **blacklists** from the internet

ipt_geofence automatically **reloads** live-updated blacklists without rebooting the app

Honeypot

Make ipt_geofence act like a **honeypot** by specifying port ranges

- 15 minutes ban for hosts that send pkts on the given ports
- Periodic banned hosts **harvesting** (and upper bound) to avoid flooding

Configuration

```
{
    "queue_id": 0,
    "markers": {
        "pass": 1000,
        "drop": 2000
    },
    "default_policy": "DROP",
    "policy": {
        "drop": {
            "countries_whitelist": ["IT", "DE", "CH", "NL"],
            "continents_whitelist": ["NA"]
        },
        "pass": {
            "countries_blacklist": ["RU", "BY"],
            "continents_blacklist": []
        }
    },
    "monitored_ports": {
        "tcp": [22, 80, 443],
        "udp": [],
        "ignored_ports": [123],
        "honeypot_ports": ["51000-56000","50000-56100", "51000-52000",10,20,30]
    },
    "blacklists": [
        "https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/dshield_7d.netset",
        "https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/alienvault_reputation.ipset",
        "https://feodotracker.abuse.ch/downloads/ipblocklist_recommended.txt",
        "https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt",
        "https://feodotracker.abuse.ch/downloads/ipblocklist.txt",
        "https://sslbl.abuse.ch/blacklist/sslipblacklist.txt"
    ]
}
```

Usage

1) Configure the firewall

```
./ipt_config_utils/single_iface.sh
```

2) Edit `config.json` to suit your needs

3) Run the program

```
./ipt_geofence -m database.mmdb -c config.json
```

Execution

```
sudo ./ipt_geofence -v -m dbip-country-lite-2022-05.mmdb -c sample_config.json
19/Jun/2022 20:00:55 [GeoIP.cpp:37] Successfully loaded dbip-country-lite-2022-05.mmdb
19/Jun/2022 20:00:55 [Configuration.cpp:80] Markers are set to: pass 1000, drop 2000
19/Jun/2022 20:00:55 [Configuration.cpp:87] Default policy: DROP
19/Jun/2022 20:00:55 [Configuration.cpp:101] Adding TCP/22
19/Jun/2022 20:00:55 [Configuration.cpp:101] Adding TCP/80
19/Jun/2022 20:00:55 [Configuration.cpp:101] Adding TCP/443
19/Jun/2022 20:00:55 [Configuration.cpp:121] Ignoring TCP/UDP port 123
19/Jun/2022 20:00:55 [Configuration.cpp:275] Protecting range [51000-56000]
19/Jun/2022 20:00:55 [Configuration.cpp:241] Merging ranges [50000-56100] and [51000-56000] into [50000-56100]
19/Jun/2022 20:00:55 [Configuration.cpp:275] Protecting range [50000-56100]
19/Jun/2022 20:00:55 [Configuration.cpp:241] Merging ranges [51000-52000] and [50000-56100] into [50000-56100]
19/Jun/2022 20:00:55 [Configuration.cpp:149] Protecting port 10
19/Jun/2022 20:00:55 [Configuration.cpp:149] Protecting port 20
19/Jun/2022 20:00:55 [Configuration.cpp:149] Protecting port 30
19/Jun/2022 20:00:55 [Configuration.cpp:159] All UDP ports will be monitored
19/Jun/2022 20:00:55 [Configuration.cpp:176] Adding IT to countries_whitelist
19/Jun/2022 20:00:55 [Configuration.cpp:176] Adding DE to countries_whitelist
19/Jun/2022 20:00:55 [Configuration.cpp:176] Adding CH to countries_whitelist
19/Jun/2022 20:00:55 [Configuration.cpp:176] Adding NL to countries_whitelist
19/Jun/2022 20:00:55 [Configuration.cpp:176] Adding NA to continents_whitelist
19/Jun/2022 20:00:55 [Blacklists.cpp:210] Downloading https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/dshield_7d.netset...
19/Jun/2022 20:00:55 [Blacklists.cpp:210] Downloading https://raw.githubusercontent.com/firehol/blocklist-ipsets/master/alienvault_reputation.ipset...
19/Jun/2022 20:00:56 [Blacklists.cpp:210] Downloading https://feodotracker.abuse.ch/downloads/ipblocklist_recommended.txt...
19/Jun/2022 20:00:56 [Blacklists.cpp:210] Downloading https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt...
19/Jun/2022 20:00:57 [Blacklists.cpp:210] Downloading https://feodotracker.abuse.ch/downloads/ipblocklist.txt...
19/Jun/2022 20:00:58 [Blacklists.cpp:210] Downloading https://sslbl.abuse.ch/blacklist/sslipblacklist.txt...
19/Jun/2022 20:00:58 [NwInterface.cpp:56] Successfully connected to NF_QUEUE 0
19/Jun/2022 20:00:58 [NwInterface.cpp:492] Starting reload configuration loop
19/Jun/2022 20:00:58 [NwInterface.cpp:316] {"dst":{"host":"192.168.0.185","port":48930},"proto":"TCP","src":{"continent":"EU","country":"IT","host":"146.75.54.49","port":443},"verdict":"pass"}
19/Jun/2022 20:01:00 [NwInterface.cpp:416] Ignoring TCP ports 0/0
19/Jun/2022 20:01:00 [NwInterface.cpp:416] Ignoring TCP ports 0/0
19/Jun/2022 20:01:02 [NwInterface.cpp:316] {"dst":{"continent":"EU","country":"NL","host":"52.108.56.19","port":443},"proto":"TCP","src":{"host":"192.168.0.185","port":35640},"verdict":"pass"}
19/Jun/2022 20:01:02 [NwInterface.cpp:318] WARNING: {"dst":{"continent":"EU","country":"GB","host":"149.154.165.120","port":443},"proto":"TCP","src":{"host":"192.168.0.185","port":
36748},"verdict":"drop"}
19/Jun/2022 20:01:03 [NwInterface.cpp:316] {"dst":{"continent":"NA","country":"US","host":"149.154.175.55","port":443},"proto":"TCP","src":{"host":"192.168.0.185","port":41150},"verdict":"pass"}
19/Jun/2022 20:01:03 [NwInterface.cpp:318] WARNING: {"dst":{"host":"192.168.0.185","port":58934},"proto":"TCP","src":{"continent":"EU","country":"IE","host":"52.108.196.24","port":
443},"verdict":"drop"}
19/Jun/2022 20:01:03 [NwInterface.cpp:318] WARNING: {"dst":{"continent":"EU","country":"IE","host":"52.108.196.24","port":443},"proto":"TCP","src":{"host":"192.168.0.185","port":
58934},"verdict":"drop"}
19/Jun/2022 20:01:04 [NwInterface.cpp:318] WARNING: {"dst":{"continent":"EU","country":"GB","host":"149.154.167.91","port":443},"proto":"TCP","src":{"host":"192.168.0.185","port":
54744},"verdict":"drop"}
19/Jun/2022 20:01:06 [NwInterface.cpp:416] Ignoring TCP ports 0/0
19/Jun/2022 20:01:06 [NwInterface.cpp:316] {"dst":{"host":"224.0.0.251","port":5353},"proto":"UDP","src":{"host":"192.168.0.168","port":5353},"verdict":"pass"}
19/Jun/2022 20:01:06 [NwInterface.cpp:316] {"dst":{"host":"ff02::fb","port":5353},"proto":"UDP","src":{"host":"fe80::4051:e0bc:e099:de6d","port":5353},"verdict":"pass"}
19/Jun/2022 20:01:06 [NwInterface.cpp:316] {"dst":{"host":"192.168.0.185","port":43620},"proto":"TCP","src":{"continent":"NA","country":"US","host":"34.120.52.64","port":443},"verdict":"pass"}
19/Jun/2022 20:01:06 [NwInterface.cpp:316] {"dst":{"continent":"NA","country":"US","host":"34.120.52.64","port":443},"proto":"TCP","src":{"host":"192.168.0.185","port":43620},"verdict":"pass"}
19/Jun/2022 20:01:08 [NwInterface.cpp:318] WARNING: {"dst":{"continent":"EU","country":"GB","host":"149.154.167.91","port":443},"proto":"TCP","src":{"host":"192.168.0.185","port":
54746},"verdict":"drop"}
19/Jun/2022 20:01:08 [NwInterface.cpp:318] WARNING: {"dst":{"continent":"EU","country":"GB","host":"149.154.167.91","port":80},"proto":"TCP","src":{"host":"192.168.0.185","port":
54000},"verdict":"drop"}
19/Jun/2022 20:01:09 [NwInterface.cpp:318] WARNING: {"dst":{"continent":"EU","country":"GB","host":"149.154.167.91","port":443},"proto":"TCP","src":{"host":"192.168.0.185","port":
```

Execution

PASS

{"dst":{"host":"192.168.0.185","port":45070},
"proto":"TCP",
"src":{"continent":"EU","country":"IT","host":"146.75.54.49","port":443},
"verdict":"pass"}

DROP

WARNING: {"dst":{"continent":"EU","country":"ES","host":"142.250.184.67","port":443},
"proto":"TCP",
"src":{"host":"192.168.0.185","port":36896},
"verdict":"drop"}

BLACKLIST

WARNING:
{"dst":{"host":"192.168.0.185","port":50740},
"proto":"TCP",
"src":{"blacklisted":true,"host":"149.154.167.91","port":443},
"verdict":"drop"}

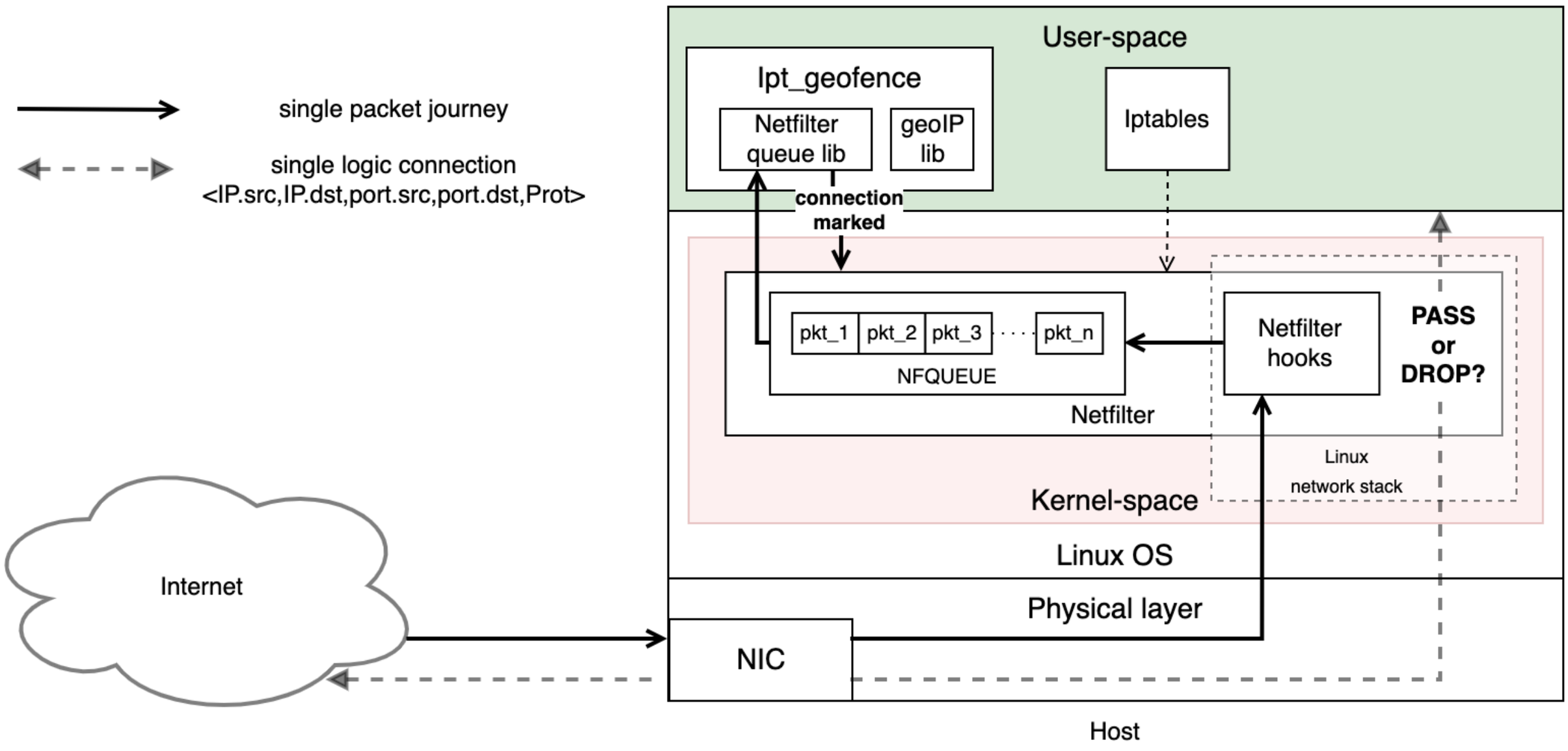
HONEYPOT

WARNING: Banning host 149.154.167.91 || Protected port 50726

Architecture

- Packets coming from network interfaces or user space are pushed in a queue.
- ipt_geofence pops a packet from the queue, analyzes it (IP and Transport layer) and marks its related connection with a value.
- All packets belonging to a marked connection are automatically *dropped* or *passed* depending on the mark value.
- Note: only **one** packet per connection needs to be analyzed!

Architecture



Performance Evaluation

~0.025 ms

Processing time per **unmarked** connection

i7-8750H (Q2'18)

Depends on the HW → i5-4210U(Q2'14) ~6 times slower

How much is 0.025ms?

DNS ping

```
C:\Users\pc>ping 8.8.8.8

Esecuzione di Ping 8.8.8.8 con 32 byte di dati:
Risposta da 8.8.8.8: byte=32 durata=25ms TTL=117
Risposta da 8.8.8.8: byte=32 durata=25ms TTL=117
Risposta da 8.8.8.8: byte=32 durata=23ms TTL=117
Risposta da 8.8.8.8: byte=32 durata=23ms TTL=117

Statistiche Ping per 8.8.8.8:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 23ms, Massimo =  25ms, Medio =  24ms

C:\Users\pc>ping 1.1.1.1

Esecuzione di Ping 1.1.1.1 con 32 byte di dati:
Risposta da 1.1.1.1: byte=32 durata=14ms TTL=59
Risposta da 1.1.1.1: byte=32 durata=14ms TTL=59
Risposta da 1.1.1.1: byte=32 durata=14ms TTL=59
Risposta da 1.1.1.1: byte=32 durata=15ms TTL=59

Statistiche Ping per 1.1.1.1:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 14ms, Massimo =  15ms, Medio =  14ms
```

0.12% delay
on a ~20ms DNS ping

Internet services *latency*
is much more relevant,
even for basic ones

Web page request

Wireshark · Conversations · wlp3s0

Ethernet · 1 | IPv4 · 2 | IPv6 | TCP · 1 | UDP · 2

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
francis-TP500LN.station	one.one.one.one	4	384	2	170	2	214	0.206056	0.0557	24 k	
francis-TP500LN.station	www.google.com	46	23 k	24	2.475	22	21 k	0.262326	0.3556	55 k	

```
francis@2086|0:curl_test$ curl -w "@fmt" -o /dev/null -s "https://www.google.com/"

        time_total:  0.377186s
```

2x0.025ms → **0.013%** delay

Google search

Wireshark · Conversations · wlp3s0

Ethernet · 1 | IPv4 · 2 | IPv6 | TCP · 1 | UDP · 2

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
francis-TP500LN.station	one.one.one.one	4	384	2	170	2	214	0.206056	0.0557	24 k	
francis-TP500LN.station	www.google.com	46	23 k	24	2.475	22	21 k	0.262326	0.3556	55 k	

```
francis@2079|0:curl_test$ curl -w "@fmt" -o /dev/null -s "https://www.google.com/search?channel=fs&client
=ubuntu&q=average+google+search+response+time"

        time_total:  1.474833s
```

2x0.025ms → **0.0033%** delay

Performance degradation?

Processing time is **not** affected by the number of *new* connections per second, but NFQUEUE is.

If NFQUEUE cannot mitigate a traffic spike, packets will be dropped

Performance degradation over ~**60K *new*** connections per **second**... Pretty *unlikely* scenario

Common scenario

53.72% of global traffic → video streaming (Sandvine)

«How many ~~packets~~ ***connections*** are established while watching a movie?»

Most likely much less than **60K** (per *second*)

Performance Evaluation

Further information in our report

ipt_geofence - Performance Evaluation

Francesco Lorenzoni, Yuri Caprini, Salvatore Guastella

June 16, 2022

Contents

1 Architectural overview **3**

2 Worst-case scenario **4**

3 Measuring T_e **5**
3.1 Measurement Methods 7

4 Test bed and results **7**

5 Observations **9**
5.1 Older hardware 9
5.2 About method 1 9

6 Conclusions **10**

Future Improvements

- JSON Logging on disk
- Exponential honeypot ban
- More structured testing
- Avoid dropping packets when *nfqueue* is full
- ASN filtering
- Integration with **ntopng** alerts through Syslog Log Ingestion

Conclusions

- ipt_geofence offers fast basic, yet efficient, filtering
- netfilter/iptables → Linux only 
- Open source
- You are welcome to contribute!

https://github.com/ntop/ipt_geofence 

Thank you

Francesco Lorenzoni

f.lorenzoni4@studenti.unipi.it

frenzis01

Yuri Caprini

y.caprini@studenti.unipi.it

yuricaprini

Salvatore Guastella

s.guastella2@studenti.unipi.it

salvogs