

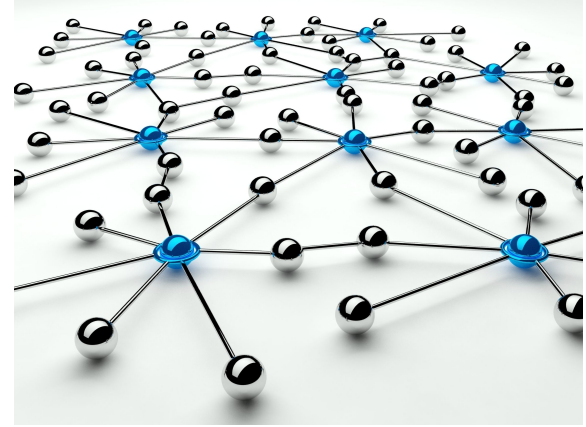
# True stories on the analysis of network activity using Python

Dmitry Alimov

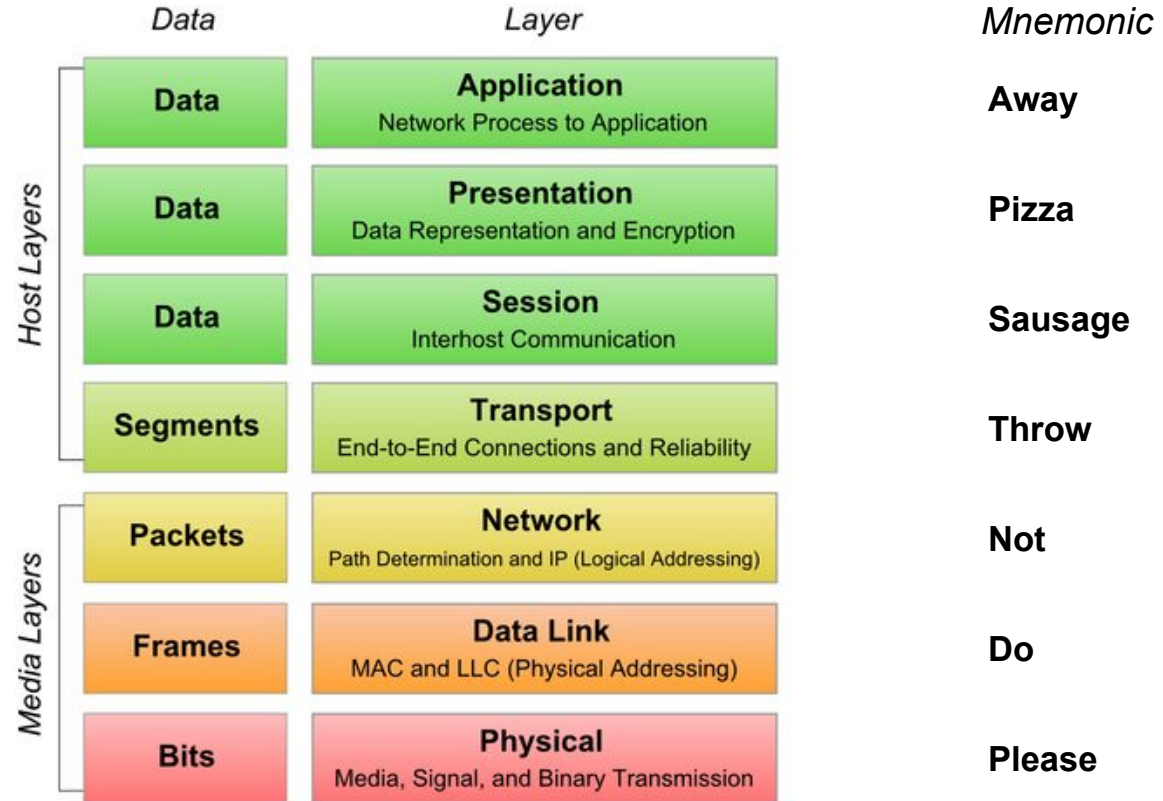
2018

# Outline

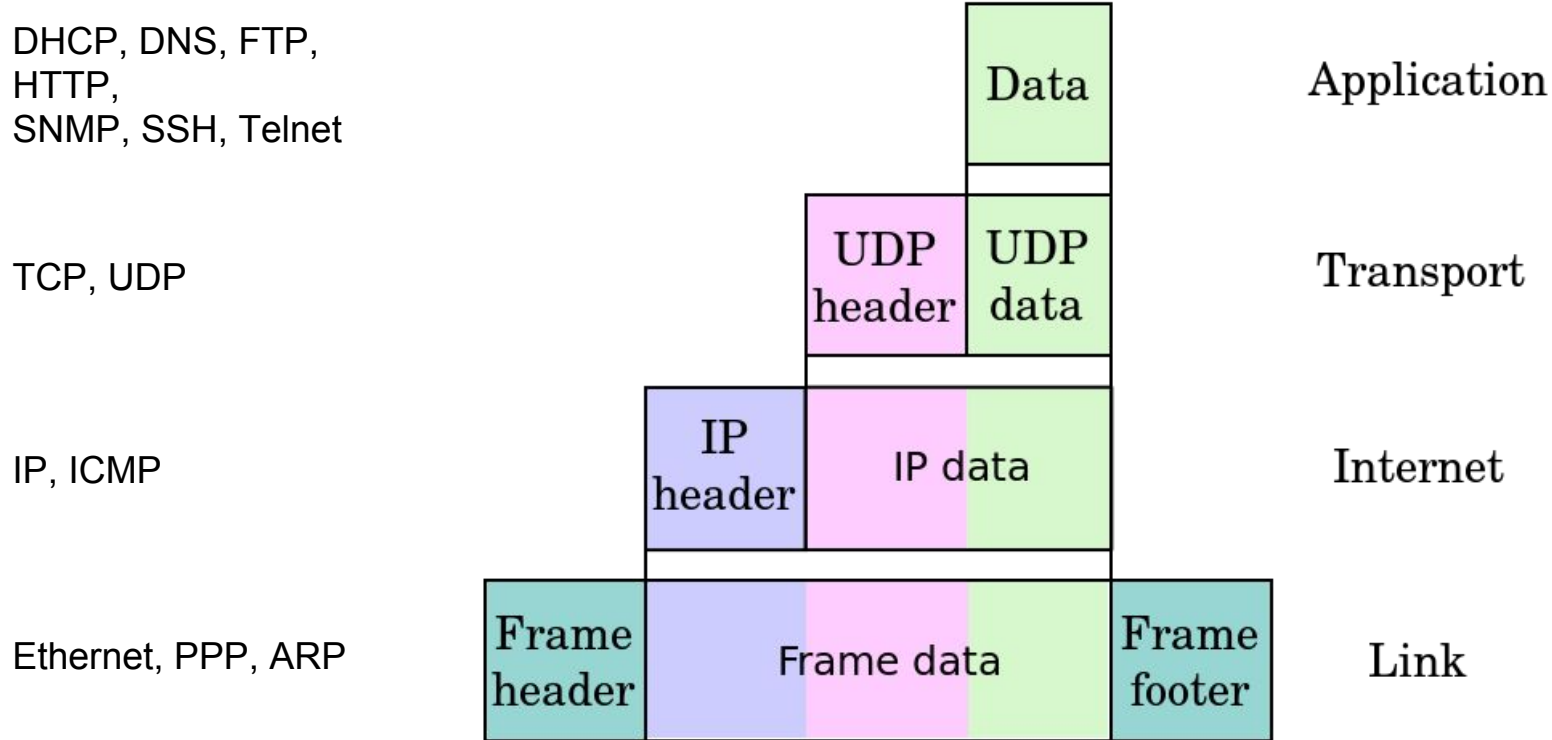
1. Theory
2. Network packets analysis
3. IPv4/IPv6 network filters (iptables)  
Network packets crafting
4. Open ports



# OSI model



# Internet protocol suite (TCP/IP) model



# Network packets analysis

# Network activity

- Requests
- Used hosts
- Lost packets
- Statistics



# Tools

- wireshark
- tcpdump
- scapy



# Wireshark

No.	Time	Source	Destination	Protocol	Length	Leftover Capture Data	Info
1	0.000000	2001:618:400::519...	2001:618:1:8000::5	TCP	80		35995 → 80 [SYN] Seq=0 Win=5680 Len=0 MSS=...
2	0.031862	2001:618:1:8000::5	2001:618:400::519...	TCP	80		80 → 35995 [SYN, ACK] Seq=0 Ack=1 Win=5734...
3	0.031917	2001:618:400::519...	2001:618:1:8000::5	TCP	72		35995 → 80 [ACK] Seq=1 Ack=1 Win=5680 Len=...
4	0.032259	2001:618:400::519...	2001:618:1:8000::5	HTTP	420		GET / HTTP/1.1
5	0.084015	2001:618:1:8000::5	2001:618:400::519...	TCP	1480		[TCP segment of a reassembled PDU]
6	0.084078	2001:618:400::519...	2001:618:1:8000::5	TCP	72		35995 → 80 [ACK] Seq=349 Ack=1409 Win=8496...
7	0.087901	2001:618:1:8000::5	2001:618:400::519...	HTTP	955		HTTP/1.1 200 OK (text/html)
8	0.087961	2001:618:400::519...	2001:618:1:8000::5	TCP	72		35995 → 80 [ACK] Seq=349 Ack=2292 Win=1131...
9	1.175970	2001:618:400::519...	2001:618:1:8000::5	TCP	80		35997 → 80 [SYN] Seq=0 Win=5680 Len=0 MSS=...
10	1.206866	2001:618:1:8000::5	2001:618:400::519...	TCP	80		80 → 35997 [SYN, ACK] Seq=0 Ack=1 Win=5734...

▶ Frame 6: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)

Raw packet data

▶ Internet Protocol Version 6, Src: 2001:618:400::5199:cc70, Dst: 2001:618:1:8000::5

▼ Transmission Control Protocol, Src Port: 35995, Dst Port: 80, Seq: 349, Ack: 1409, Len: 0

Source Port: 35995

Destination Port: 80

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 349 (relative sequence number)

Acknowledgment number: 1409 (relative ack number)

Header Length: 32 bytes

▶ Flags: 0x010 (ACK)

Window size value: 2124

[Calculated window size: 8496]

[Window size scaling factor: 4]

Checksum: 0xc1b2 [unverified]

```

0000  60 00 00 00 00 20 06 40  20 01 06 18 04 00 00 00  ....@.....
0010  00 00 00 00 00 51 99 cc 70  20 01 06 18 00 01 80 00  ....Q..p....
0020  00 00 00 00 00 00 00 05  8c 9b 00 50 6a e7 08 93  ......Pj...
0030  b8 ef 1c c3 80 10 08 4c  c1 b2 00 00 01 01 08 0a  ....L.....
0040  00 dd 1a 8d 9c 0c 30 ed  ....0.

```



# tcpdump

Tool for dumping the traffic on a network



```
/mnt/nfs/tcpdump -i eth1 -w ./tcpdump.pcap 'ip and not (src 192.168.17.1 or dst  
192.168.17.1) and not broadcast and not multicast and host not 10.12.1.100' &
```

N.B. filters!

Examples:

```
# show traffic to 10.12.1.2 that is not ICMP:
```

```
tcpdump dst 10.12.1.2 and src net and not icmp
```

```
# show SYNACK packets:
```

```
tcpdump 'tcp[13]=18'
```

# tcpdump output

Convert pcap to txt:

```
tcpdump -ttttnnr tcpdump.pcap > tcpdump.pcap.txt
```

```
2017-09-04 11:42:20.475594 IP 127.255.90.99.67 > 127.255.90.99.68: BOOTP/DHCP, Reply, length 357
E.....@.[Z.....C.D.m.....&.....N.c.L.....
.....
.....c.Sc5..6.Dr$.3.....:.....;..
...V.....~.....lab.com.....}{..&.#.!.....v..1.....lab.com..
```

```
2017-09-04 11:42:22.322596 IP 127.255.90.18.46800 > 127.255.90.214.51001: Flags [S], seq
3059494393, win 14600, options [mss 1460,sackOK,TS val 4294828083 ecr 0,nop,wscale 7], length 0
```

```
2017-09-04 11:42:22.755378 IP 127.255.90.18.45832 > 192.0.1.207.8081: Flags [P.], seq 1:79, ack 1,
win 115, length 78
E..v0.@@.....r.....e.....P..s....GET /hdr.dat HTTP/1.1
Host: 192.0.1.207:8081
Connection: close
```

# Test report

total DNS sessions: 17

domain name	bad responses
host1-lab.com.	2
host2-lab.com.	2
host3-lab.com.	2

TCP sessions stats:

destination ip:port	times connected total (good / bad)	total length
192.0.114.207:8081	21 (4 good / 17 bad)	8808
127.255.90.214:51001	16 (0 good / 16 bad)	0
192.0.105.184:443	2 (2 good / 0 bad)	11866
192.0.112.19:8080	2 (1 good / 1 bad)	408
192.0.80.137:42272	1 (0 good / 1 bad)	3057
192.0.80.137:41012	1 (1 good / 0 bad)	3505

UDP sessions stats:

destination ip:port	quantity	total length
192.0.80.137:48723	1	8
192.0.80.137:40030	1	8
192.0.80.137:59320	1	8

# PCAP analysis with Scapy

```
from scapy.all import *

packets = rdpcap('tcpdump.pcap')

for packet in packets:
    if TCP in packet:
        if Raw in packet:
            print('from {} to {}'.format(packet[IP].src, packet[IP].dst))
            print('payload:')
            print('{}'.format(packet[Raw].load))
```

```
> from 127.255.210.110 to 192.0.140.246
> payload:
> GET /configs/main.cfg HTTP/1.1
> Host: 192.0.140.246
> Accept: */*
```

# IPv4/IPv6 packets filtering

# IPv4/IPv6 network filters (iptables)

iptables/ip6tables — administration tool for IPv4/IPv6 packet filtering and NAT

## **Task:**

Test IPv4/IPv6 network filters

E.g. ICMP, IPv6-ICMP, TCP (SSH), UDP (SNMP, DHCP, DHCPv6)

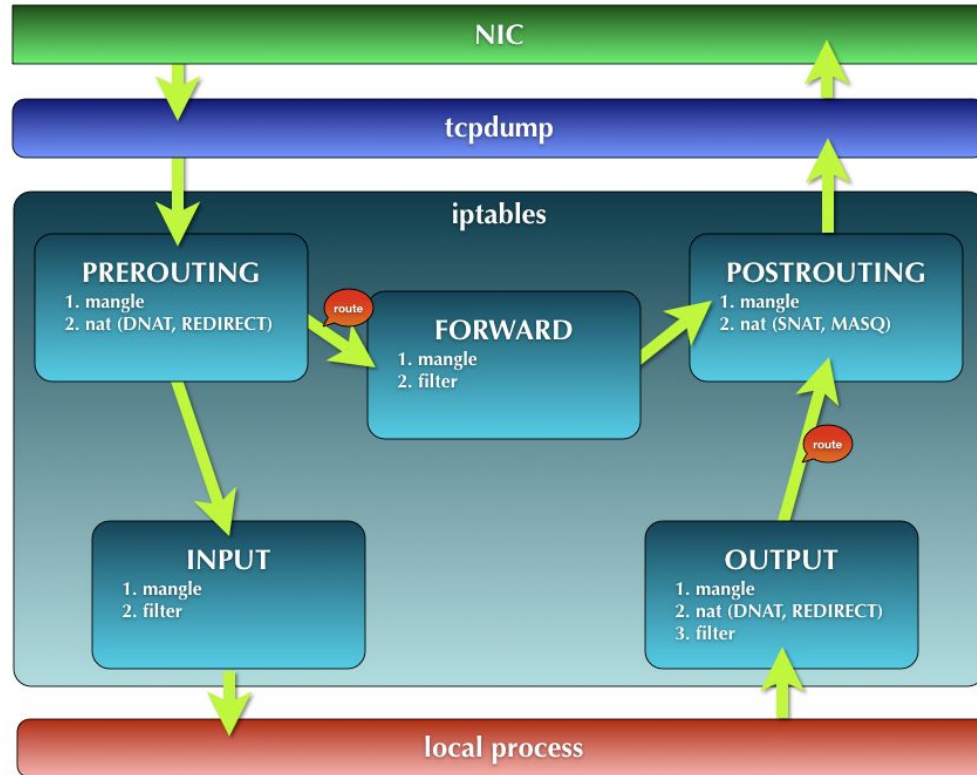
## **Possible solutions:**

tcpdump

iptables/ip6tables



# IPv4/IPv6 network filters (iptables)



# /sbin/ip6tables -x -v -n -L

Chain INPUT (policy DROP 6737 packets, 1273025 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination	
2	120	DROP	tcp		*	*	::/0	::/0	tcp dpt:22 /* Drop SSH */
1	48	DROP	udp		*	*	::/0	::/0	udp dpt:161 /* Drop SNMP */
2	160	DROP	icmpv6		*	*	::/0	::/0	ipv6-icmp type 137 /* Drop ICMP Redirect Message */
2	208	ACCEPT	all		*	*	::/0	::/0	state ESTABLISHED,RELATED
2	208	ACCEPT	all		lo	*	:::1	:::1	
1	48	ACCEPT	icmpv6		*	*	::/0	::/0	ipv6-icmp type 128 /* Echo Request */
5342	405940	ACCEPT	icmpv6		*	*	fe80::/10	::/0	ipv6-icmp type 130 /* Multicast Listener Query */
3	216	ACCEPT	icmpv6		*	*	fe80::/10	::/0	ipv6-icmp type 131 /* Multicast Listener Report */
1	72	ACCEPT	icmpv6		*	*	fe80::/10	::/0	ipv6-icmp type 132 /* Multicast Listener Done */
14	1000	ACCEPT	icmpv6		*	*	::/0	::/0	ipv6-icmp type 135 /* Neighbor Discovery (ND) Solicitation */
1377	99088	ACCEPT	icmpv6		*	*	::/0	::/0	ipv6-icmp type 136 /* Neighbor Discovery (ND) Advertisement */
1	48	ACCEPT	icmpv6		*	*	::/0	::/0	ipv6-icmp type 141 /* Inverse Neighbor Discovery Solicitation */
1	48	ACCEPT	icmpv6		*	*	::/0	::/0	ipv6-icmp type 142 /* Inverse Neighbor Discovery Advertisement */
1	57	ACCEPT	icmpv6		*	*	::/0	::/0	ipv6-icmp type 148 /* Secure ND Certificate Path Solicitation */
1	57	ACCEPT	icmpv6		*	*	::/0	::/0	ipv6-icmp type 149 /* Secure ND Certificate Path Advertisement */
1	48	ACCEPT	udp		*	*	::/0	::/0	udp spt:547 dpt:546 /* Accept DHCPv6 */

Chain OUTPUT (policy ACCEPT 5419 packets, 419928 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination
------	-------	--------	------	-----	----	-----	--------	-------------



# /sbin/ip6tables -x -v -n -L

Chain INPUT (policy DROP 6737 packets, 1273025 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination	
2	120	DROP	tcp		*	*	::/0	::/0	tcp dpt:22 /* Drop SSH */
1	48	DROP	udp		*	*	::/0	::/0	udp dpt:161 /* Drop SNMP */
2	160	DROP	icmpv6		*	*	::/0	::/0	ipv6-icmp type 137 /* Drop ICMP Redirect Message */
2	208	ACCEPT	all		*	*	::/0	::/0	state ESTABLISHED,RELATED
2	208	ACCEPT	all		lo	*	:::1	:::1	
1	48	ACCEPT	icmpv6		*	*	::/0	::/0	ipv6-icmp type 128 /* Echo Request */
5342	405940	ACCEPT	icmpv6		*	*	fe80::/10	::/0	ipv6-icmp type 130 /* Multicast Listener Query */
3	216	ACCEPT	icmpv6		*	*	fe80::/10	::/0	ipv6-icmp type 131 /* Multicast Listener Report */
1	72	ACCEPT	icmpv6		*	*	fe80::/10	::/0	ipv6-icmp type 132 /* Multicast Listener Done */
14	1000	ACCEPT	icmpv6		*	*	::/0	::/0	ipv6-icmp type 135 /* Neighbor Discovery (ND) Solicitation */
1377	99088	ACCEPT	icmpv6		*	*	::/0	::/0	ipv6-icmp type 136 /* Neighbor Discovery (ND) Advertisement */
1	48	ACCEPT	icmpv6		*	*	::/0	::/0	ipv6-icmp type 141 /* Inverse Neighbor Discovery Solicitation */
1	48	ACCEPT	icmpv6		*	*	::/0	::/0	ipv6-icmp type 142 /* Inverse Neighbor Discovery Advertisement */
1	57	ACCEPT	icmpv6		*	*	::/0	::/0	ipv6-icmp type 148 /* Secure ND Certificate Path Solicitation */
1	57	ACCEPT	icmpv6		*	*	::/0	::/0	ipv6-icmp type 149 /* Secure ND Certificate Path Advertisement */
1	48	ACCEPT	udp		*	*	::/0	::/0	udp spt:547 dpt:546 /* Accept DHCPv6 */

Chain OUTPUT (policy ACCEPT 5419 packets, 419928 bytes)

pkts	bytes	target	prot	opt	in	out	source	destination
------	-------	--------	------	-----	----	-----	--------	-------------

# Network packets crafting

socket for TCP, UDP (e.g. SNMP, DHCP) -> user permissions

```
socket(AF_INET / AF_INET6, SOCK_STREAM)
```

```
socket(AF_INET / AF_INET6, SOCK_DGRAM)
```

raw sockets -> root permissions

Python + Scapy



# Examples

```
from scapy.all import *
```

```
def test_tcp_dpt_22(self):  
    # Check SSH  
    ipv6 = IPv6(dst=self.ipv6)  
    payload = ipv6 / TCP(dport=22)  
    # Send packets at layer 3 and return only the first answer  
    sr1(payload, timeout=2)
```

Begin emission:

..Finished to send 1 packets.

# Examples

```
from scapy.all import *
```

```
def test_udp_dpt_161(self):
```

```
    # Check SNMP
```

```
    ipv6 = IPv6(dst=self.ipv6)
```

```
    payload = ipv6 / UDP(dport=161)
```

```
    # Send packets at layer 3 and return only the first answer
```

```
    sr1(payload, timeout=2)
```

# Examples

```
from scapy.all import *

def test_ipv6_icmptype_128(self):
    # Check ICMPv6 Echo Request
    payload = ICMPv6EchoRequest(type=128)
    ipv6 = IPv6(dst=self.ipv6)
    sr1(ipv6 / payload, timeout=2)
```

# Examples

```
from scapy.all import *

def test_ipv6_icmptype_130(self):
    # add RouterAlert option
    hbh = IPv6ExtHdrHopByHop(options=[RouterAlert(value=0)])
    multicast = 'ff02::1'
    ipv6 = IPv6(dst=multicast)
    payload = ICMPv6MLQuery(type=130)
    sr1(ipv6 / hbh / payload, timeout=2)
```

# Scapy “/layers/inet6.py”

```
#138: Do Me - RFC 2894 - Seems painful
```

```
...
```

```
#143: Do Me - RFC 3810
```

```
...
```

```
#148: Do Me - SEND related - RFC 3971
```

```
#149: Do Me - SEND related - RFC 3971
```

} not implemented :(

```
...
```

```
# tous les messages MLD sont emis avec une adresse source lien-locale
```

```
# -> Y veiller dans le post_build si aucune n'est specifiee
```

```
# La valeur de Hop-Limit doit etre de 1
```

```
...
```

# Examples

```
from scapy.all import *

def test_ipv6_icmptype_148(self):
    # make ICMPv6 type 148 from ICMPv6Unknown
    payload = ICMPv6Unknown(type=148, msgbody='test_type_148')
    ipv6 = IPv6(dst=self.ipv6)
    sr1(ipv6 / payload, timeout=2)
```



# PCAP packets replay with Scapy

```
from scapy.all import *

packets = rdpcap("tcpdump.pcap")

new_mac = 'DE:EE:11:33:33:77'
new_src = '123.34.45.56'

for packet in packets:
    packet[Ether].src = new_mac
    packet[IP].src = new_src
    send(packet)
```

# Open ports

# Nmap

```
$ nmap -p- 192.168.1.93
Starting Nmap 7.01 ( https://nmap.org ) at 2017-12-15 11:29 MSK
Nmap scan report for 192.168.1.93
Host is up (0.038s latency).
Not shown: 65524 closed ports
PORT      STATE      SERVICE
22/tcp    open       ssh
23/tcp    open       telnet
111/tcp   open       rpcbind
135/tcp   filtered  msrpc
136/tcp   filtered  profile
137/tcp   filtered  netbios-ns
138/tcp   filtered  netbios-dgm
139/tcp   filtered  netbios-ssn
445/tcp   filtered  microsoft-ds
593/tcp   filtered  http-rpc-epmap
9555/tcp  open       unknown
12345/tcp open       unknown
```

# Netstat

netstat -an

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	User	Inode	PID/Program name
tcp	0	0	0.0.0.0:873	0.0.0.0:*	LISTEN	0	50500	2805/rsync
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	0	37787	2605/sshd
tcp	0	0	127.0.0.1:631	0.0.0.0:*	LISTEN	0	41189	2429/cupsd
tcp6	0	0	:::25	:::*	LISTEN	0	50340	-
udp	0	0	0.0.0.0:68	0.0.0.0:*		0	33595	2584/dhclient

# Ports monitor

No netstat? No problem

/proc/net/udp\*, /proc/net/tcp\*, lsof

```
cat /proc/net/tcp
```

sl	local_address	rem_address	st	tx_queue	rx_queue	tr	tm->when	retrnsmt	uid	timeout	inode
0:	00000000:0369	00000000:0000	0A	00000000:00000000	00:00000000	00000000	0	0	0	50500	1 00000000 100 0 0 10 0
1:	00000000:0016	00000000:0000	0A	00000000:00000000	00:00000000	00000000	0	0	0	37787	1 00000000 100 0 0 10 0
2:	0100007F:0277	00000000:0000	0A	00000000:00000000	00:00000000	00000000	0	0	0	41189	1 00000000 100 0 0 10 0

```
sudo lsof -i
```

COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME
cupsd	2429	root	9u	IPv4	41189	0t0	TCP	localhost:ipp (LISTEN)
sshd	2605	root	3u	IPv4	37787	0t0	TCP	*:ssh (LISTEN)
rsync	2805	root	4u	IPv4	50500	0t0	TCP	*:rsync (LISTEN)

```
states = {
    0x01: TCP_ESTABLISHED,
    0x0A: TCP_LISTEN,
    ...
}
```

# Ports monitor

```
import paramiko

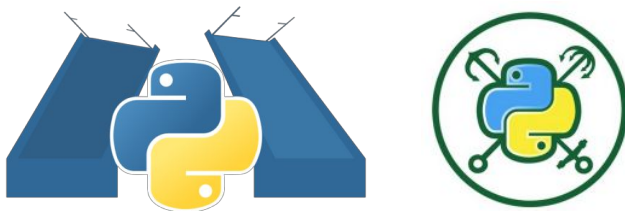
def send_command(ip, command, login, password, port=22, timeout=30):
    ssh = paramiko.SSHClient()
    ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())
    ssh.connect(ip, port=port, timeout=timeout, username=login, password=password)
    _, stdout, _ = ssh.exec_command(command)
    stdout_data = stdout.read()
    ssh.close()
    return stdout_data

def main():
    ...
    output = send_command(ip, 'cd /proc/net/; cat tcp udp tcp6 udp6')
    ...
    lsof_data = get_lsof(ip)
    tables = map_sockets_procs(lsof_data)
    print(tables)
```

# Ports monitor

proto	reqcv-q	send-q	local ip:port	foreign ip:port	state	pid	process
tcp	0	0	127.0.0.1:37610	0.0.0.0:0	LISTEN	1071	/bin/app
tcp	0	0	127.0.0.1:37610	127.0.0.1:30642	ESTABLISHED	1046	/usr/bin/manager
tcp	0	0	127.0.0.1:40642	127.0.0.1:37610	ESTABLISHED	1070	/default/applauncher
udp	0	0	0.0.0.0:40019	0.0.0.0:0		1407	/bin/busybox
udp	0	0	0.0.0.0:40022	0.0.0.0:0		1407	/bin/busybox
udp	0	0	192.168.13.23:28881	0.0.0.0:0		???	???
udp	0	0	192.168.13.23:28899	0.0.0.0:0		???	???
tcp6	0	0	:::31275	:::0	LISTEN	1271	/bin/app
tcp6	0	0	:::61246	:::0	LISTEN	1270	/default/applauncher
tcp6	0	0	:::41226	:::0	LISTEN	1246	/usr/bin/manager
tcp6	0	0	:::31286	:::0	LISTEN	1287	/usr/bin/hstool
udp6	0	0	:::51244	:::0		1270	/default/applauncher
udp6	0	0	:::51238	:::0		1270	/default/applauncher
tcp6	0	0	:::22	:::0	LISTEN	2605	/sbin/dropbear
tcp6	0	0	0.0.0.0:23	0.0.0.0:0	LISTEN	2789	/bin/busybox
tcp	0	0	0.0.0.0:111	0.0.0.0:0	LISTEN	767	/bin/portmap
tcp	0	0	0.0.0.0:873	0.0.0.0:0	LISTEN	2805	/bin/rsync

# Questions?



<https://t.me/spbpython>

[https://t.me/piterpy\\_meetup](https://t.me/piterpy_meetup)



# Bonus slides

# lsof - list open files

```
$ sudo lsof -n
```

COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME
init	1	root	cwd	DIR	0,70	176	258	/
init	1	root	rtd	DIR	0,70	176	258	/
init	1	root	txt	REG	0,70	163096	215892	/sbin/init
init	1	root	mem	REG	0,42		215892	/sbin/init (path dev=0,70)
....								
init	1	root	2u	CHR	1,3	0t0	6	/dev/null
init	1	root	3r	FIFO	0,10	0t0	34066	pipe
init	1	root	4w	FIFO	0,10	0t0	34066	pipe
init	1	root	5r	0000	0,11	0	7041	anon_inode
init	1	root	7u	unix	0x0000000000000000	0t0	34067	socket
init	1	root	8u	unix	0x0000000000000000	0t0	34270	socket
init	1	root	11w	REG	0,70	95	4137723	/var/log/upstart/acpid.log.1
...								
sshd	2963	root	3u	IPv4	93504	0t0		TCP *:ssh (LISTEN)
...								
lsof	9128	d	7w	FIFO	0,10	0t0	173854523	pipe

# List open files

No lsof? No problem :)

```
# ls -l /proc/2963/exe
lrwxrwxrwx 1 root root 0 Dec 18 15:52 /proc/2963/exe -> /usr/sbin/sshd
```

```
# ls -l /proc/2963/fd/
total 0
dr-x----- 2 root root  0 Dec 18 15:52 .
dr-xr-xr-x  9 root root  0 Dec 12 17:55 ..
lrwx----- 1 root root 64 Dec 18 15:54 0 -> /dev/null
lrwx----- 1 root root 64 Dec 18 15:54 1 -> /dev/null
lrwx----- 1 root root 64 Dec 18 15:54 2 -> socket:[93504]
```

```
# cat /proc/net/tcp
sl  local_address rem_address  st tx_queue rx_queue tr tm->when retrnsmt uid  timeout inode
0: 00000000:0369 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0      0 72565 1 0 100 0 0 10 0
1: 00000000:0016 00000000:0000 0A 00000000:00000000 00:00000000 00000000 0      0 93504 1 0 100 0 0 10 0
...
```

# Images references

<https://github.com/spbpython/spb-pig-logo>

<https://www.meetup.com/PiterPy-Meetup/>

<http://www.i3intl.com/infrastructure/network-services/>

<http://ciscoccnaselfstudy.blogspot.ru/2015/10/osi-model-layers-and-its-functions-on.html>

[https://commons.wikimedia.org/wiki/File:UDP\\_encapsulation.svg](https://commons.wikimedia.org/wiki/File:UDP_encapsulation.svg)

<http://cje-rdp.org/atelier-methodes-dynamiques-de-recherche-demploi/>

<http://www.freeperformancesoftware.com/product/159/>

<https://www.brandsoftheworld.com/logo/wireshark>

<http://benrenaut.com/?filter=design>

<https://www.python.org/community/logos/>

<http://www.emoji.com/view/emoji/1853/smileys-people/thinking-face>

<http://d.hatena.ne.jp/hirose31/20090401/1238585753>

<https://thumbs.dreamstime.com/t/toegang-verleende-ontkende-zegel-44982540.jpg>