FPT University

Lab 8-10:
Configuring a Malware Lab
Manipulating HTTP/HTTPS with Burp Suite
Using Deep Freeze to Preserve Physical Systems

Because teaching teaches
teachers to teach

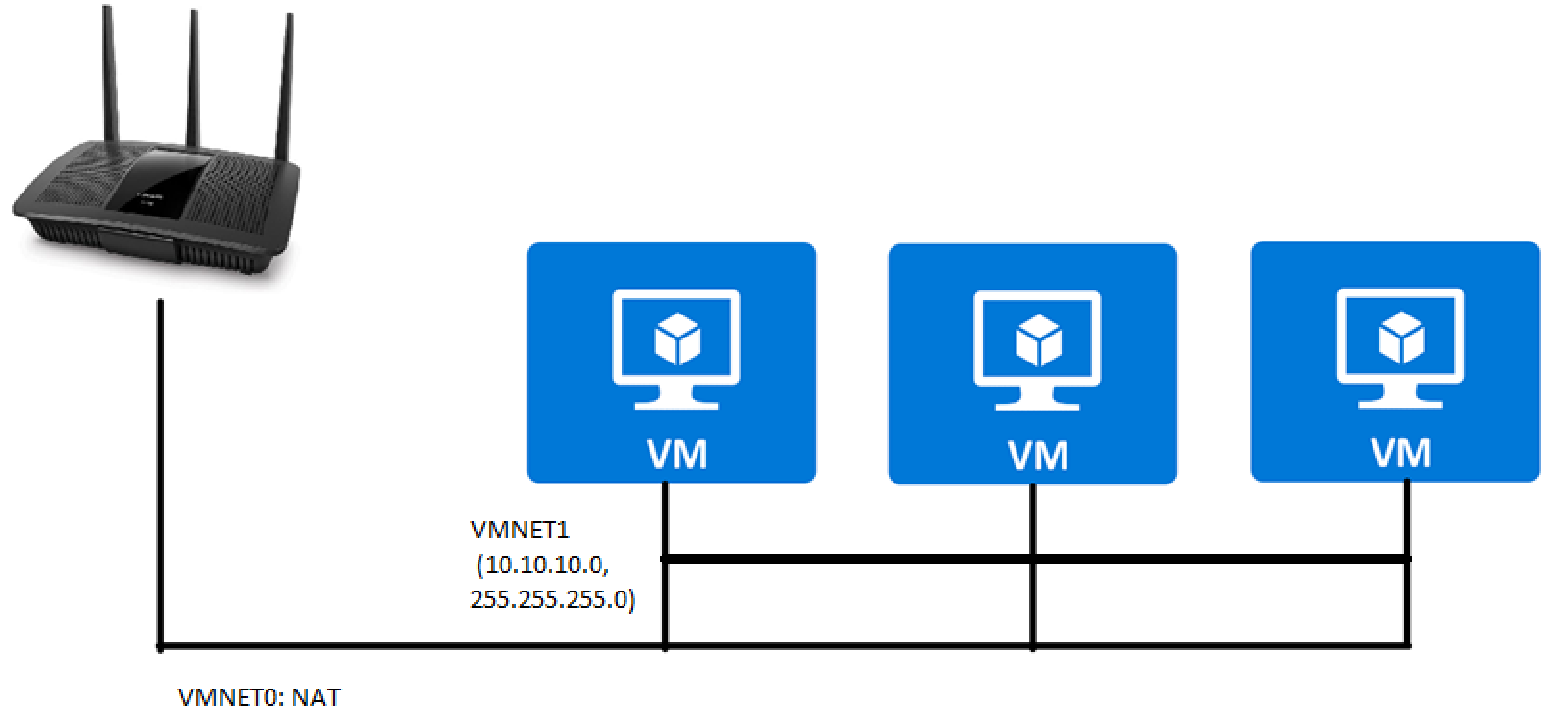
VMWARE WorkStation

- VMWARE is not freely available open source software
- 6 network modes are available
  - Not attached, NAT, Bridged Adapter, Internal Network, Host-only Adapter, Generic Driver

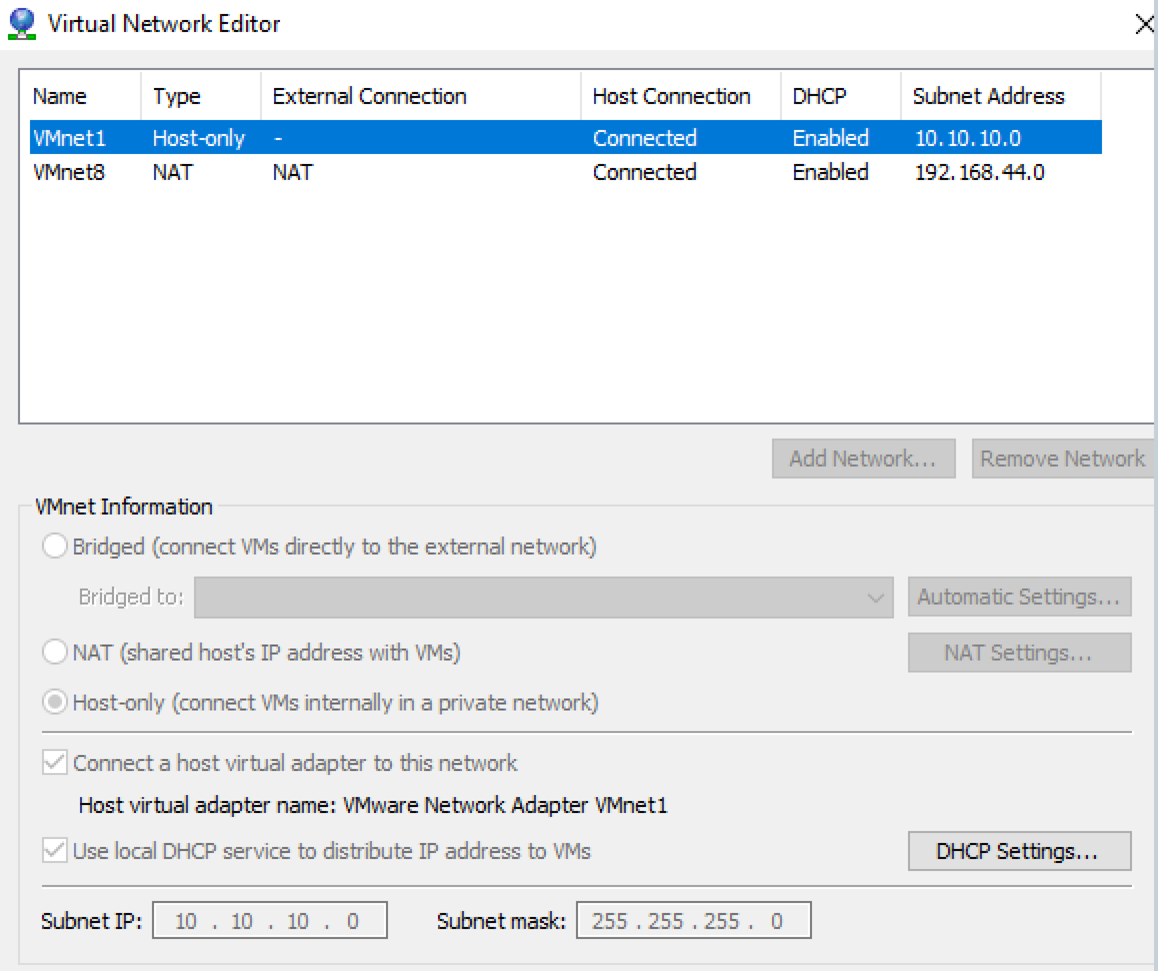
all Ubuntu on VMWARE WorkStation

- http://linuxscoop.com/video/how-to-install-ubuntu-16-04-lts-in-vmware

Configurations of 3 vmnets on vmware workstation



Configurations of NETWORK on vmware workstation



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet1	Host-only	-	Connected	Enabled	10.10.10.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.44.0

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to:

○ NAT (shared host's IP address with VMs)

● Host-only (connect VMs internally in a private network)

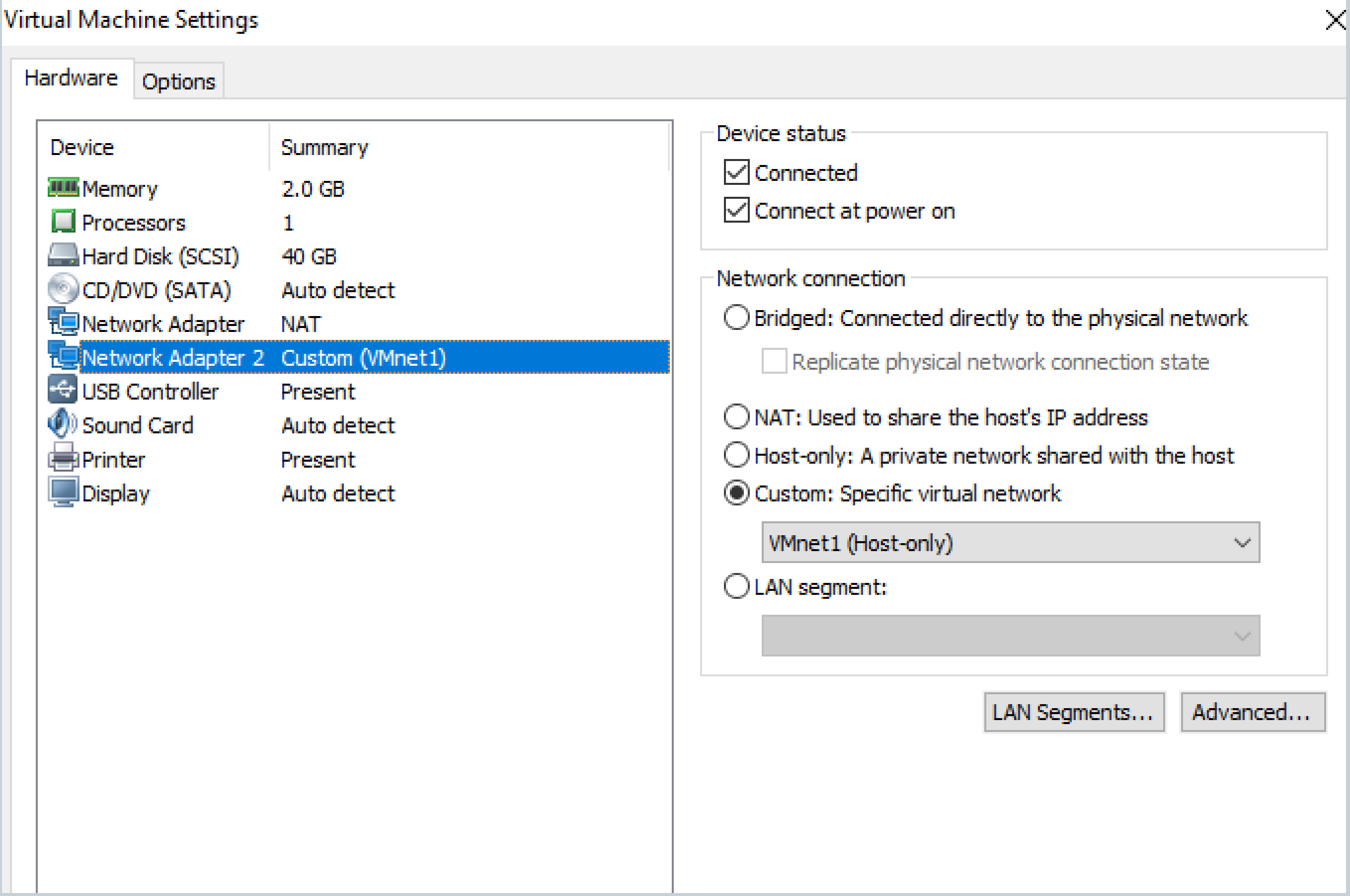
☑ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet1

☑ Use local DHCP service to distribute IP address to VMs

Subnet IP: 10 . 10 . 10 . 0   Subnet mask: 255 . 255 . 255 . 0

Configurations of NETWORK on vmware workstation



Virtual Machine Settings

Device	Summary
Memory	2.0 GB
Processors	1
Hard Disk (SCSI)	40 GB
CD/DVD (SATA)	Auto detect
Network Adapter	NAT
Network Adapter 2	Custom (VMnet1)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

○ NAT: Used to share the host's IP address

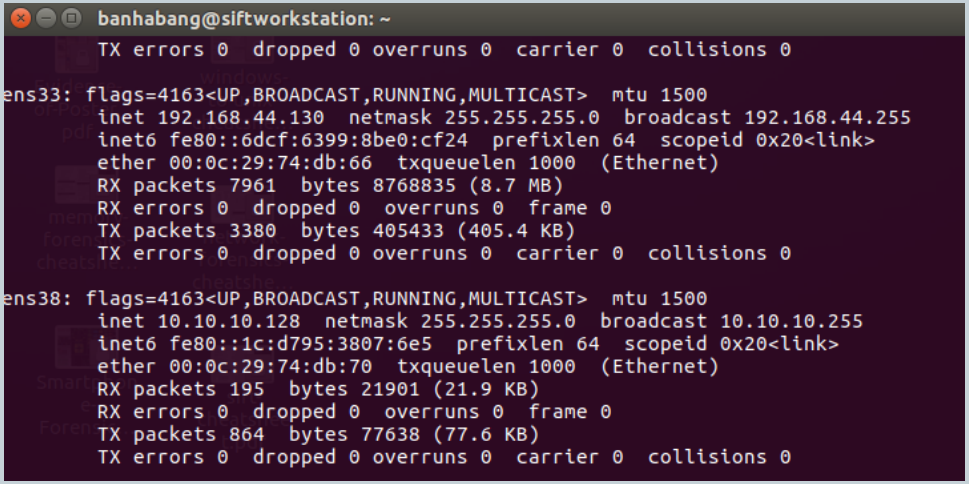
○ Host-only: A private network shared with the host

● Custom: Specific virtual network

VMnet1 (Host-only)

○ LAN segment:

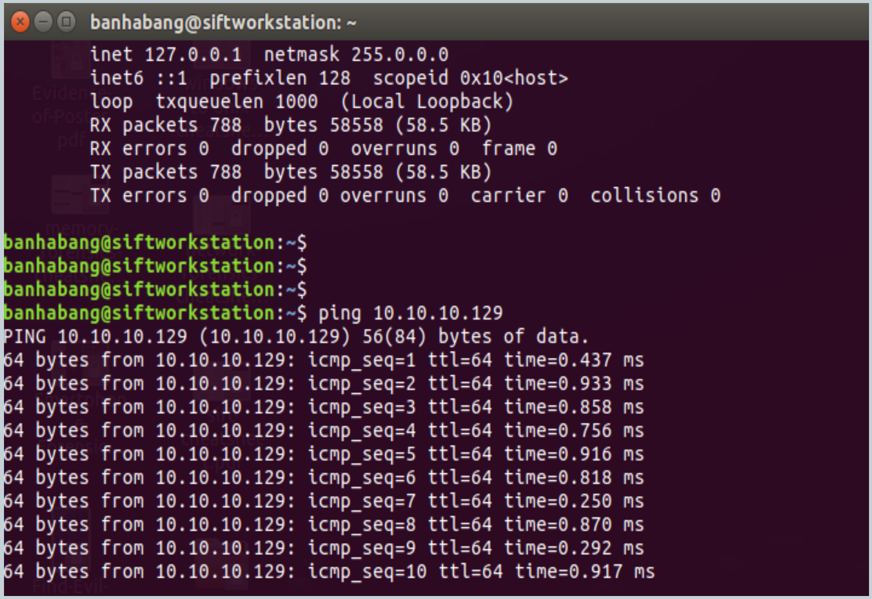
Configurations of NETWORK on vmware workstation



```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.44.130  netmask 255.255.255.0  broadcast 192.168.44.255
        inet6 fe80::6dcf:6399:8be0:cf24  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:74:db:66  txqueuelen 1000  (Ethernet)
        RX packets 7961  bytes 8768835 (8.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3380  bytes 405433 (405.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens38: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.128  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 fe80::1c:d795:3807:6e5  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:74:db:70  txqueuelen 1000  (Ethernet)
        RX packets 195  bytes 21901 (21.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 864  bytes 77638 (77.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

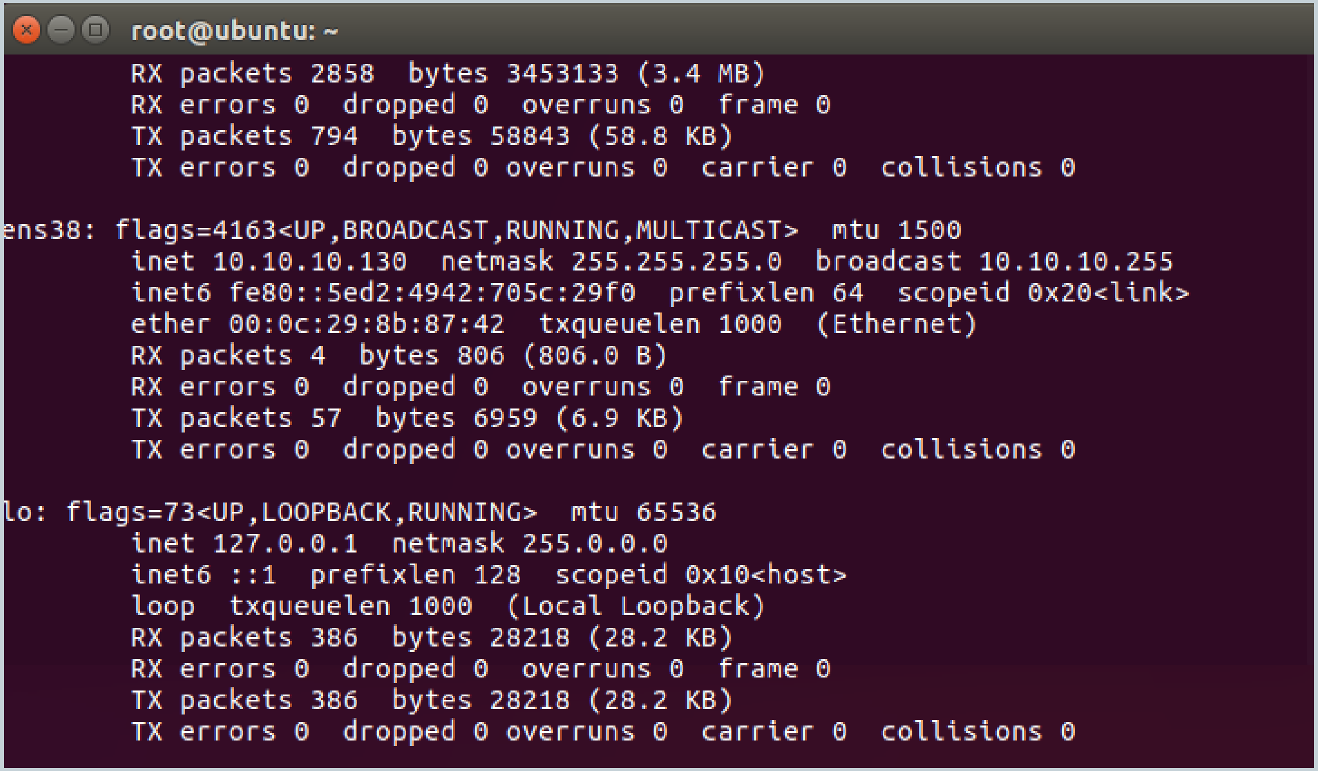


```
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 788  bytes 58558 (58.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 788  bytes 58558 (58.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

banhabang@siftworkstation:~$
banhabang@siftworkstation:~$
banhabang@siftworkstation:~$
banhabang@siftworkstation:~$ ping 10.10.10.129
PING 10.10.10.129 (10.10.10.129) 56(84) bytes of data.
64 bytes from 10.10.10.129: icmp_seq=1 ttl=64 time=0.437 ms
64 bytes from 10.10.10.129: icmp_seq=2 ttl=64 time=0.933 ms
64 bytes from 10.10.10.129: icmp_seq=3 ttl=64 time=0.858 ms
64 bytes from 10.10.10.129: icmp_seq=4 ttl=64 time=0.756 ms
64 bytes from 10.10.10.129: icmp_seq=5 ttl=64 time=0.916 ms
64 bytes from 10.10.10.129: icmp_seq=6 ttl=64 time=0.818 ms
64 bytes from 10.10.10.129: icmp_seq=7 ttl=64 time=0.250 ms
64 bytes from 10.10.10.129: icmp_seq=8 ttl=64 time=0.870 ms
64 bytes from 10.10.10.129: icmp_seq=9 ttl=64 time=0.292 ms
64 bytes from 10.10.10.129: icmp_seq=10 ttl=64 time=0.917 ms
```

VM1

Configurations of NETWORK on vmware workstation



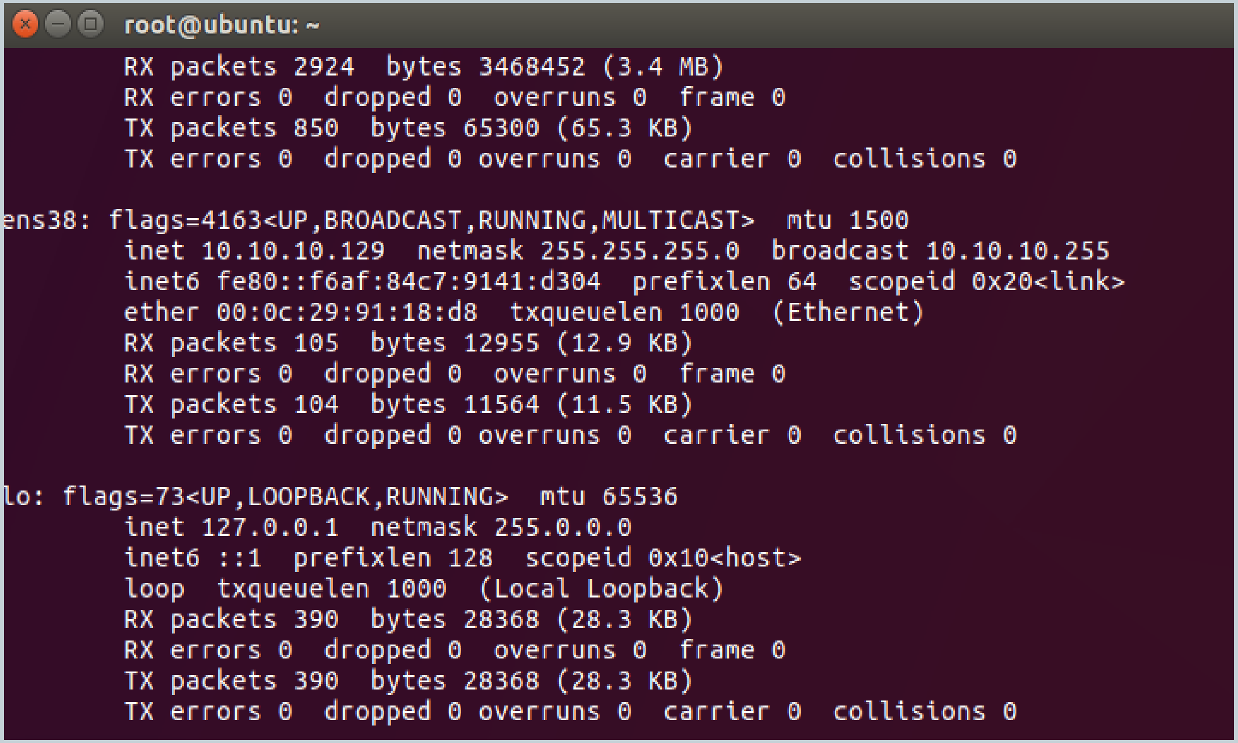
```
        RX packets 2858  bytes 3453133 (3.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 794  bytes 58843 (58.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens38: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.130  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 fe80::5ed2:4942:705c:29f0  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:8b:87:42  txqueuelen 1000  (Ethernet)
        RX packets 4  bytes 806 (806.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 57  bytes 6959 (6.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 386  bytes 28218 (28.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 386  bytes 28218 (28.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

VM2

Configurations of NETWORK on vmware workstation



```
        RX packets 2924  bytes 3468452 (3.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 850  bytes 65300 (65.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens38: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.129  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 fe80::f6af:84c7:9141:d304  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:91:18:d8  txqueuelen 1000  (Ethernet)
        RX packets 105  bytes 12955 (12.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 104  bytes 11564 (11.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 390  bytes 28368 (28.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 390  bytes 28368 (28.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

VM3

Install WireShark

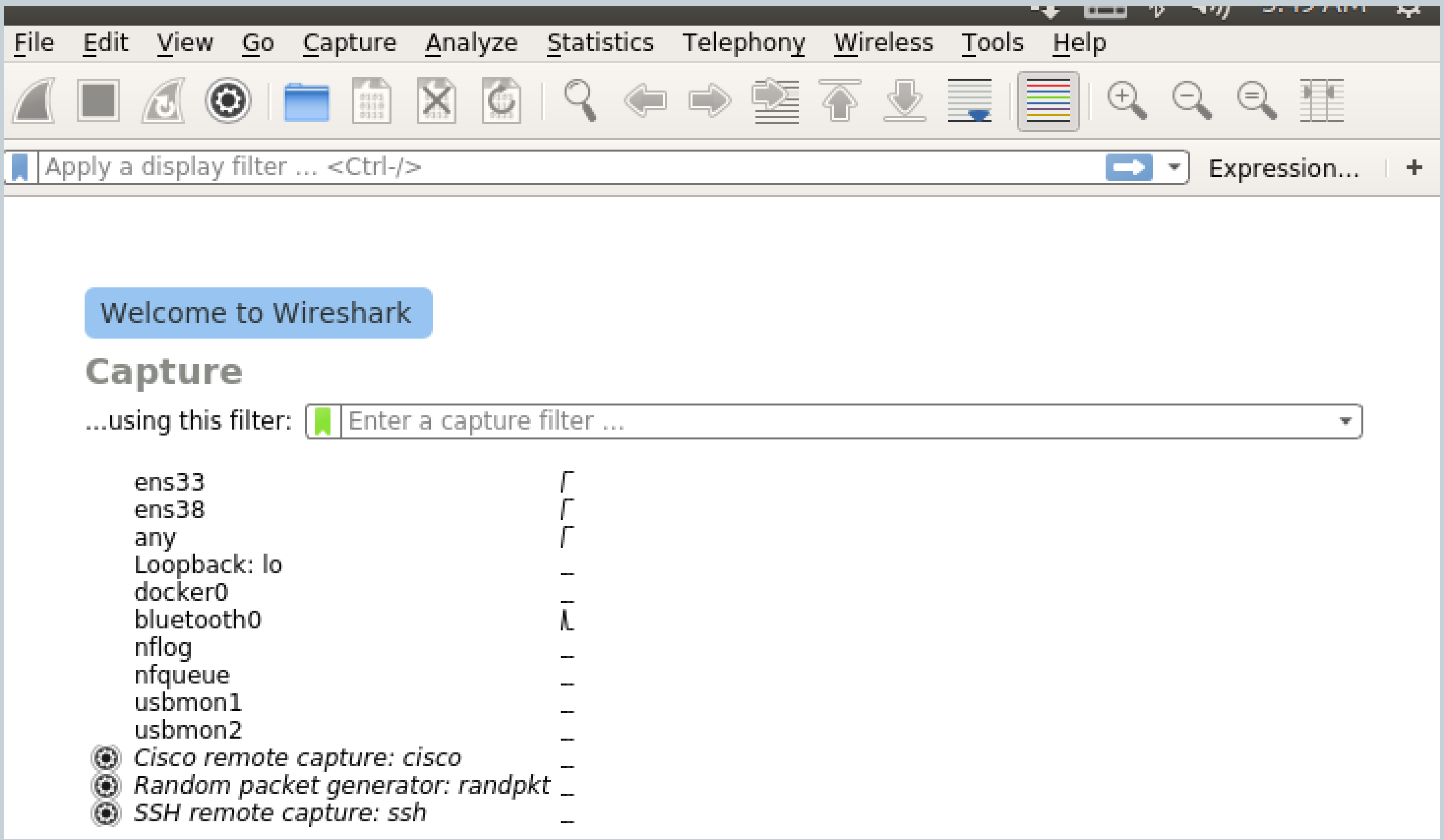
- Install:

  Comd: apt-get install wireshark

  apt-get install tshark

- Run: sudo wireshark

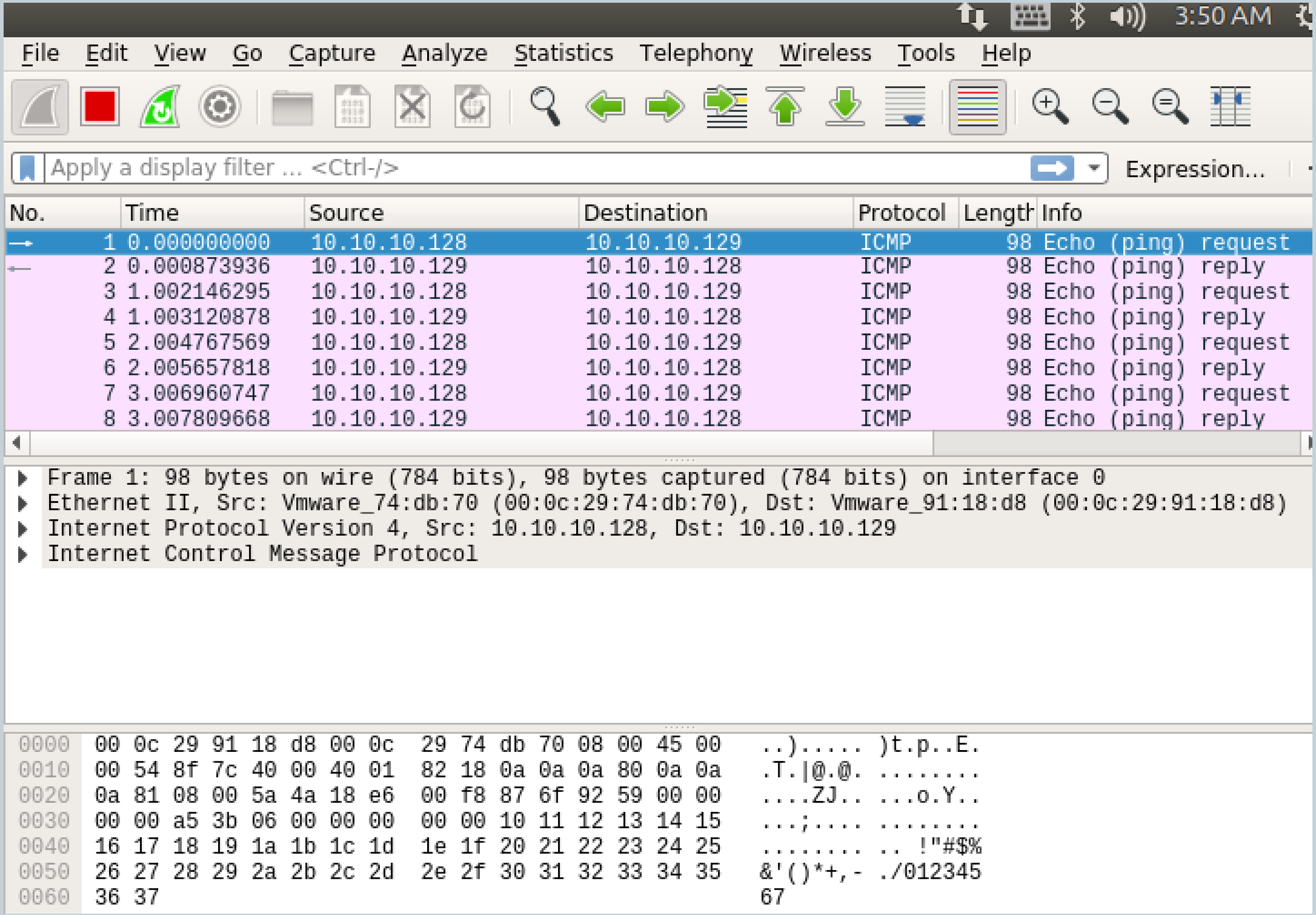
WIRESHARK



ens33
ens38
any
Loopback: lo
docker0
bluetooth0
nflog
nfqueue
usbmon1
usbmon2
Cisco remote capture: cisco
Random packet generator: randpkt
SSH remote capture: ssh

VM2

CAPTURE PACKET BY WIRESHARK


3:50 AM
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.     Time          Source          Destination     Protocol  Length Info
      1 0.000000000   10.10.10.128    10.10.10.129    ICMP          98 Echo (ping) request
      2 0.000873936   10.10.10.129    10.10.10.128    ICMP          98 Echo (ping) reply
      3 1.002146295   10.10.10.128    10.10.10.129    ICMP          98 Echo (ping) request
      4 1.003120878   10.10.10.129    10.10.10.128    ICMP          98 Echo (ping) reply
      5 2.004767569   10.10.10.128    10.10.10.129    ICMP          98 Echo (ping) request
      6 2.005657818   10.10.10.129    10.10.10.128    ICMP          98 Echo (ping) reply
      7 3.006960747   10.10.10.128    10.10.10.129    ICMP          98 Echo (ping) request
      8 3.007809668   10.10.10.129    10.10.10.128    ICMP          98 Echo (ping) reply
```

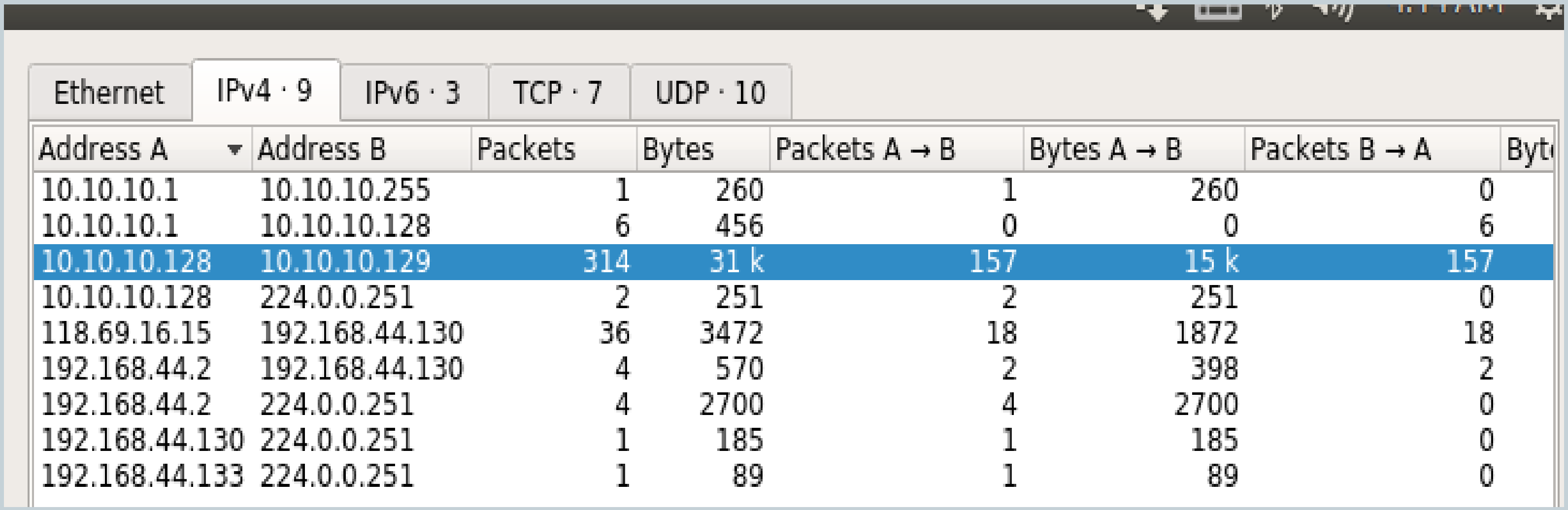
```
▶ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▶ Ethernet II, Src: Vmware_74:db:70 (00:0c:29:74:db:70), Dst: Vmware_91:18:d8 (00:0c:29:91:18:d8)
▶ Internet Protocol Version 4, Src: 10.10.10.128, Dst: 10.10.10.129
▶ Internet Control Message Protocol
```

```
0000  00 0c 29 91 18 d8 00 0c  29 74 db 70 08 00 45 00   ..)..... )t.p..E.
0010  00 54 8f 7c 40 00 40 01  82 18 0a 0a 0a 80 0a 0a   .T.|@.@. ........
0020  0a 81 08 00 5a 4a 18 e6  00 f8 87 6f 92 59 00 00   ....ZJ.. ...o.Y..
0030  00 00 a5 3b 06 00 00 00  00 00 10 11 12 13 14 15   ...;.... ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

Is there any malware involved?

- There is no simple way to figure out if there is a malware infection, by looking at capture files, as there are tons of different malware types out there and they all behave differently.
- There are some indicators, like a lot of connections or a lot of traffic form a single client (Statistics -> Conversations), "strange" DNS queries, etc.

Is there any malware involved?



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Byt
10.10.10.1	10.10.10.255	1	260	1	260	0	
10.10.10.1	10.10.10.128	6	456	0	0	6	
10.10.10.128	10.10.10.129	314	31 k	157	15 k	157	
10.10.10.128	224.0.0.251	2	251	2	251	0	
118.69.16.15	192.168.44.130	36	3472	18	1872	18	
192.168.44.2	192.168.44.130	4	570	2	398	2	
192.168.44.2	224.0.0.251	4	2700	4	2700	0	
192.168.44.130	224.0.0.251	1	185	1	185	0	
192.168.44.133	224.0.0.251	1	89	1	89	0	

Install InetSim

- Install:

```
apt-get install libnet-server-perl
apt-get install libnet-dns-perl
apt-get install libipc-shareable-perl
apt-get install libdigest-sha-perl
apt-get install libio-socket-ssl-perl
apt-get install iptables-dev
```

Dowload the INetSim from here

Install it by running the following command:

```
dpkg -i inetsim_1.2.4-1_all.deb
```

Install InetSim

- Configurtion in conf/inetsim.conf:
  - service_bind_address your IP ADDRESS
  - redirect_enabled yes
  - redirect_exclude_port tcp:22
- **sudo ./inetsim**

Install Burp Suite

- Install:
  - Install openjdk-9-jdk

    ```
    sudo apt-get install openjdk-9-jdk
    ```

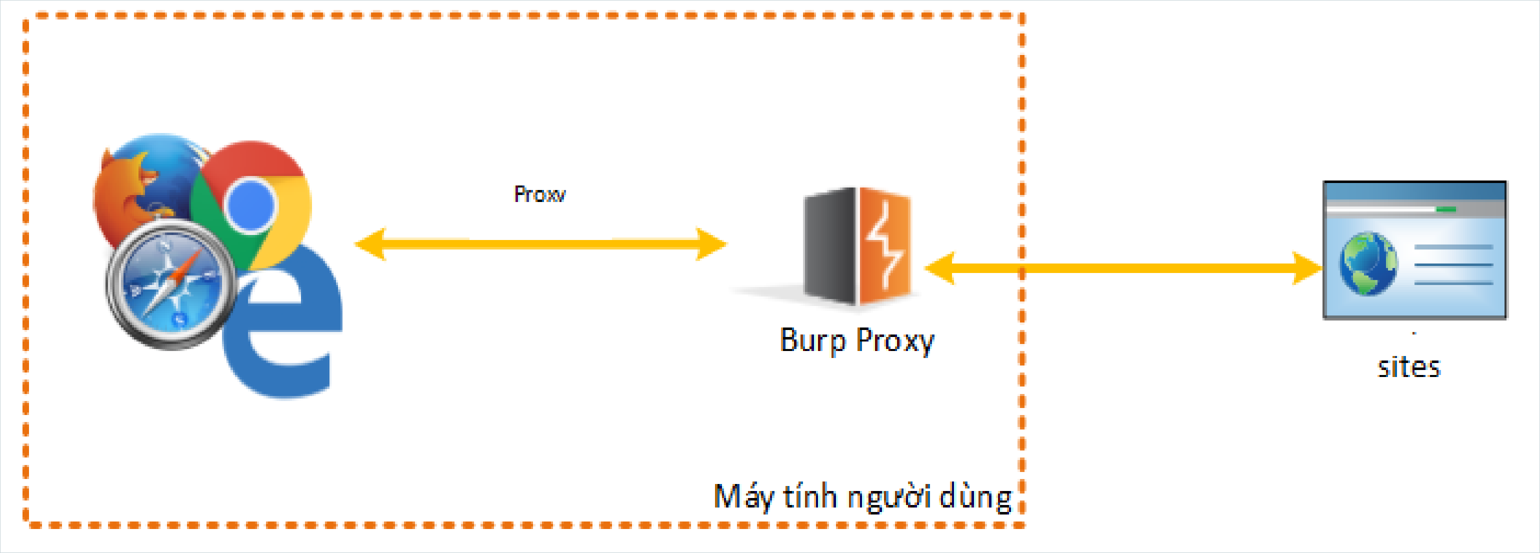
  - Download Burp Suite

    https://portswigger.net/burp/releases/download?product=free&version=1.7.26&type=linux

  - Install

    ```
    sh burpsuite_free_linux_v1_7_26.sh
    ```

Burp Suite



Features of Burp Suite

- Intercept browser traffic using man-in-the-middle proxy
- Automate custom attacks using Burp Intruder
- Clear and detailed presentation of vulnerabilities

Using Burp Suite

- Checking your Browser Proxy Configuration

  https://support.portswigger.net/customer/portal/articles/1783055-configuring-your-browser-to-work-with-burp

- Installing Burp's CA Certificate in your browser

  https://support.portswigger.net/customer/portal/articles/1783071-Installing_Browser%20Configuration%20Check.html

Workshop 1

- https://www.sans.org/reading-room/whitepapers/detection/identify-malicious-http-requests-34067
- Identifying Bruteforce:
  - Using hydra to Bruteforce
  - Using wireshark

Workshop 2

- http://honeynet.org/node/504
- Questions:
  - Which systems (i.e. IP addresses) are involved?
  - What can you find out about the attacking host (e.g., where is it located)?
  - How many TCP sessions are contained in the dump file?
  - How long did it take to perform the attack?

Workshop 2

- http://honeynet.org/node/504
- Questions:
  - Which systems (i.e. IP addresses) are involved?
  - What can you find out about the attacking host (e.g., where is it located)?
  - How many TCP sessions are contained in the dump file?
  - How long did it take to perform the attack?

Workshop 2

- Questions:
  - Which operating system was targeted by the attack? And which service? Which vulnerability?
  - Can you sketch an overview of the general actions performed by the attacker?
  - What specific vulnerability was attacked?
  - Do you think this is a manual or an automated attack? Why?

Install Deep Freeze

- Download trial version on http://www.faronics.com/en-uk/
- Install it.
- How to use it http://www.faronics.com/assets/DFS_Manual.pdf

Pros and Cons for Malware Analysis

- Download malware https://github.com/mikesiko/PracticalMalwareAnalysis-Labs
- Execute malware or browse malicious websites
- Simply reboot the machine to find that deleted files have returned and all changes have been reverted.

Understand more about Deep Unfreezer

- Download on http://usuarios.arnet.com.ar/fliamarconato/pages/edeepunfreezer.html
- How to prevent Deep Unfreezer

Q & A