

HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

MODULE THỰC HÀNH
MÃ ĐỘC

BÀI THỰC HÀNH SỐ 01
Xây dựng môi trường phân tích mã độc

Người thực hiện bài thực hành:

TS Đặng Xuân Bảo

Hà Nội, 2020

MỤC LỤC

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH.....	3
CHUẨN BỊ BÀI THỰC HÀNH.....	4
XÂY DỰNG MÔI TRƯỜNG PHÂN TÍCH MÃ ĐỘC	5
1.1. Mô tả	5
1.2. Chuẩn bị	5
1.3. Mô hình cài đặt	5
1.4. Xây dựng môi trường phân tích.....	5
1.4.1. Cấu hình chung	5
1.4.2. Cấu hình môi trường mạng	7
A. Cài đặt máy ảo Kali Linux	7
B. Cài đặt máy Win2008	13
1.5. Cài đặt bộ công cụ phân tích mã độc	16
1.6. Cài đặt bộ mẫu mã độc.....	16

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH

Tên bài thực hành: Xây dựng môi trường phân tích mã độc

Học phần: Mã độc

Số lượng sinh viên cùng thực hiện:

Địa điểm thực hành: Phòng máy

Yêu cầu:

- Yêu cầu phần cứng:
 - + Máy tính với cấu hình tối thiểu: CPU 2.0 GHz, RAM 4GB, HDD 500GB
- Yêu cầu phần mềm trên máy:
 - + Hệ điều hành Windows 10
 - + VMware Workstation 15.0
- Công cụ thực hành:
 - + Windows 2008 Server: Win2008-Target.7z
 - + Kali Linux 32 bit VM PAE: Kali-Linux-2016.2-vm-i686.7z
 - + Các công cụ phân tích mã độc: IDA Pro, string, Process monitor, Process explorer, PEView, PEiD, Bintext, Dependency Walker...
- Yêu cầu kết nối mạng LAN: có
- Yêu cầu kết nối mạng Internet: có

CHUẨN BỊ BÀI THỰC HÀNH

Đối với giảng viên

Trước buổi học, giảng viên (người hướng dẫn thực hành) cần kiểm tra sự phù hợp của điều kiện thực tế của phòng thực hành với các yêu cầu của bài thực hành.

Ngoài ra không đòi hỏi gì thêm.

Đối với sinh viên

Trước khi bắt đầu thực hành, cần tạo các bản sao của máy ảo để sử dụng. Đồng thời xác định vị trí lưu trữ các công cụ đã chỉ ra trong phần yêu cầu.

XÂY DỰNG MÔI TRƯỜNG PHÂN TÍCH MÃ ĐỘC

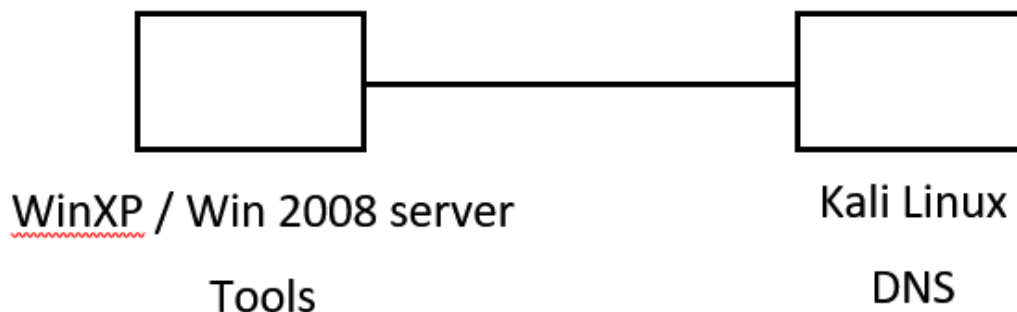
1.1. Mô tả

Ngày nay việc phân tích mã độc hầu như toàn bộ được thực hiện trên môi trường máy ảo. Bài thực hành hướng dẫn sinh viên xây dựng môi trường phân tích mã độc đơn giản.

1.2. Chuẩn bị

- 1 máy ảo Windows 2008 Server (Win2008-Target.7z)
- 1 máy ảo Kali Linux

1.3. Mô hình cài đặt



Hình 1. Mô hình môi trường phân tích mã độc

1.4. Xây dựng môi trường phân tích

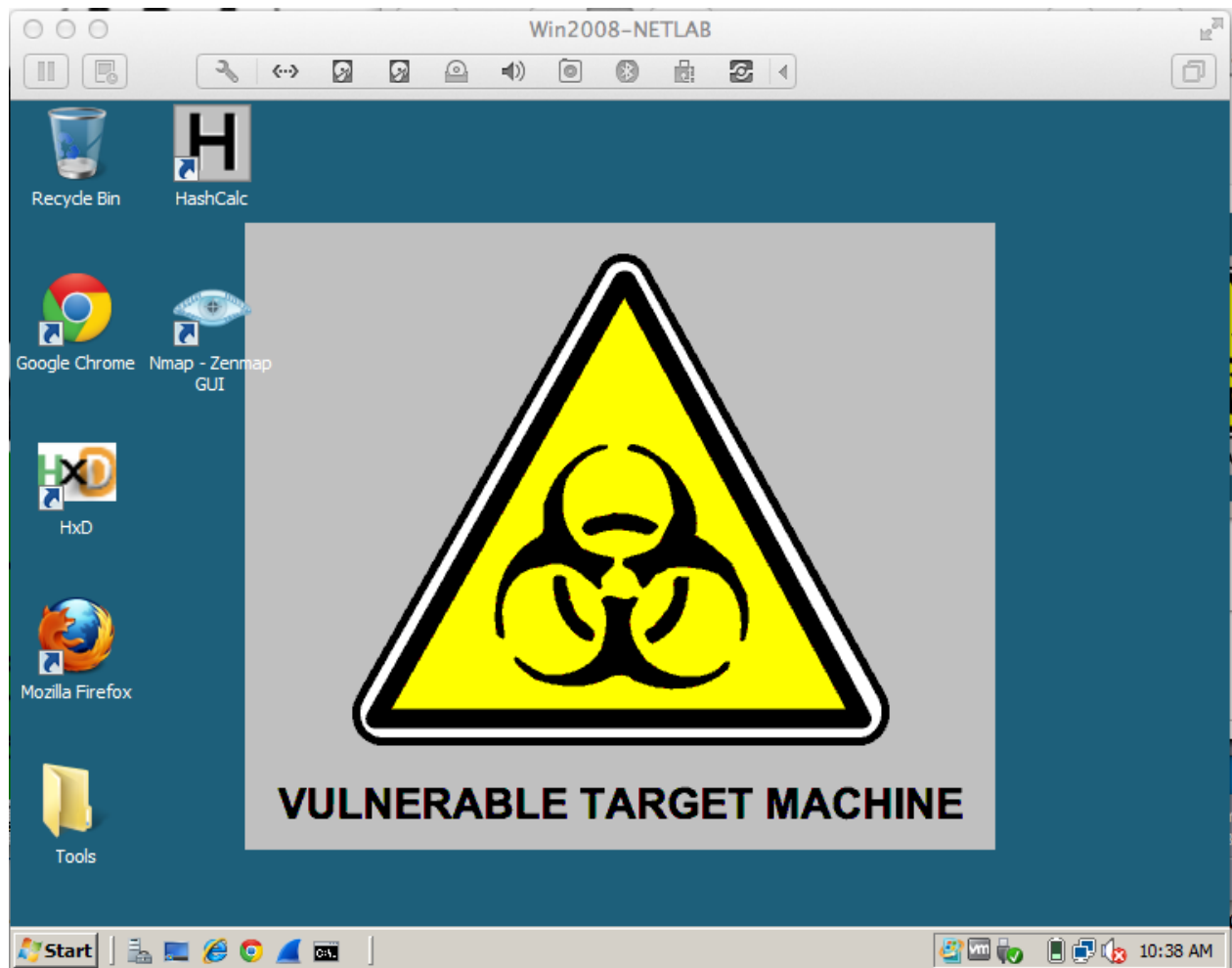
1.4.1. Cấu hình chung

Truy cập vào địa chỉ <https://samsclass.info/download-vms.htm> và tải 2 máy ảo cần thiết

- + Windows 2008 Server: Win2008-Target.7z
- + Kali Linux 32 bit VM PAE: Kali-Linux-2016.2-vm-i686.7z

Giải nén hai máy ảo. Để đăng nhập vào máy ảo Win2008-Target sử dụng tài khoản **Administrator** và mật khẩu **P@ssw0rd**.

Giao diện máy ảo Win2008-Target như sau



Hình 2. Giao diện máy ảo Win2008-Target

Đăng nhập vào Kali với tài khoản “**root**” và mật khẩu “**toor**”

Giao diện máy ảo Kali Linux như sau:

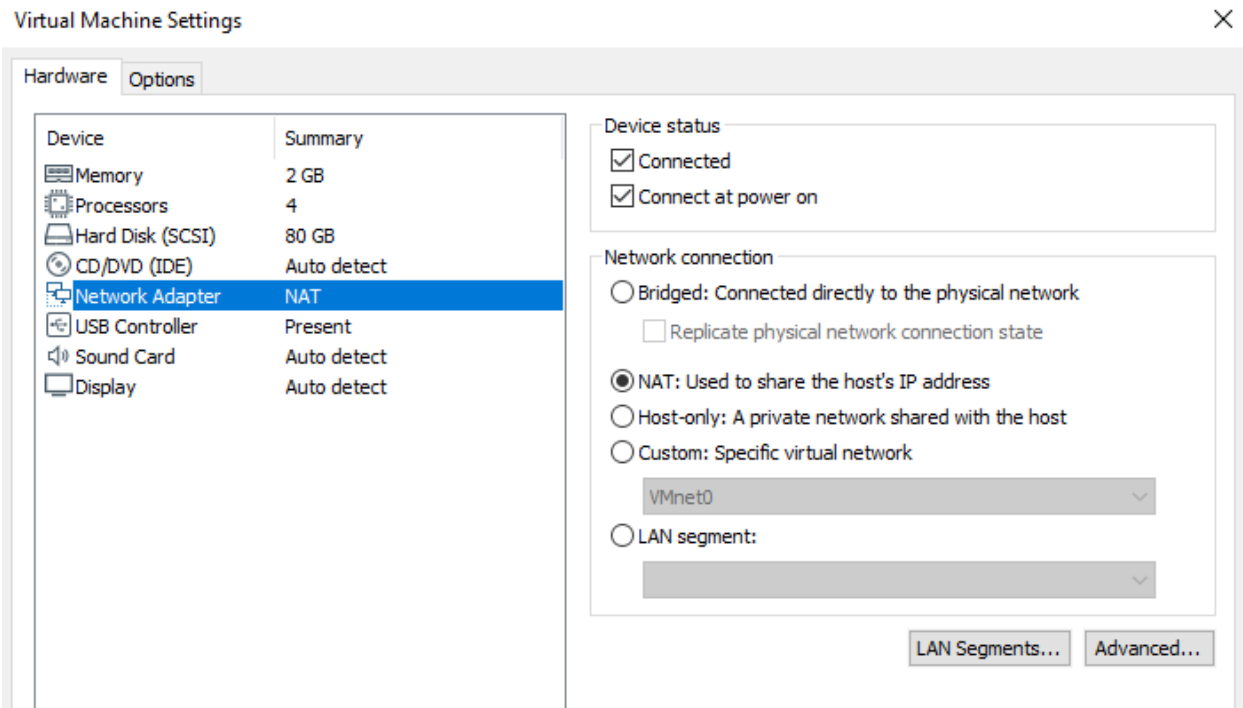


Hình 2. Giao diện máy ảo Kali Linux

1.4.2. Cấu hình môi trường mạng

A. Cài đặt máy ảo Kali Linux

Trong cửa sổ Vmware Player hiển thị màn hình Kali Linux, ở trên cùng bên trái, chọn Player, Manage, "Virtual Machine Settings". Trên cửa sổ "Virtual Machine Settings" cấu hình "Network Adapter" ở chế độ "NAT".



Mở cửa sổ Terminal. Trong cửa sổ Terminal, nhập lệnh **dhclient**
-v để nhận địa chỉ IP mới, rồi nhấn phím Enter

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# dhclient -v  
Internet Systems Consortium DHCP Client 4.4.1  
Copyright 2004-2018 Internet Systems Consortium.  
All rights reserved.  
For info, please visit https://www.isc.org/software/dhcp/  
  
Listening on LPF/eth0/00:0c:29:8b:36:49  
Sending on   LPF/eth0/00:0c:29:8b:36:49  
Sending on   Socket/fallback  
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 7  
DHCPOFFER of 192.168.235.131 from 192.168.235.254  
DHCPREQUEST for 192.168.235.131 on eth0 to 255.255.255.255 port 67  
DHCPACK of 192.168.235.131 from 192.168.235.254  
RTNETLINK answers: File exists  
bound to 192.168.235.131 -- renewal in 802 seconds.
```

Mở cửa sổ Terminal, nhập lệnh: **ifconfig**


```

root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.235.131 netmask 255.255.255.0 broadcast 192.168.235.255
    inet6 fe80::20c:29ff:fe8b:3649 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:8b:36:49 txqueuelen 1000 (Ethernet)
    RX packets 14796 bytes 21493403 (20.4 MiB)
    RX errors 97 dropped 0 overruns 0 frame 0
    TX packets 6354 bytes 353731 (345.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

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 24 bytes 1272 (1.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24 bytes 1272 (1.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Kiểm tra máy chủ Web server

Trên máy Linux, mở cửa sổ Terminal window, sử dụng lệnh: **lsof -i :80**

```

root@kali:~# lsof -i :80
COMMAND PID  USER  FD  TYPE DEVICE SIZE/OFF NODE NAME
http    2324  _apt   3u  IPv4  35656      0t0  TCP kali:36784->hebe.kali.org:http (
CLOSE_WAIT)
http    2325  _apt   3u  IPv4  31042      0t0  TCP kali:51664->linux.cs.nctu.edu.tw
:http (ESTABLISHED)
http    2327  _apt   3u  IPv4  32144      0t0  TCP kali:35206->219.216.128.25:http
(CLOSE_WAIT)
http    2328  _apt   3u  IPv4  29449      0t0  TCP kali:35024->104.18.102.100:http
(ESTABLISHED)
apache2 2387   root    4u  IPv6  31184      0t0  TCP *:http (LISTEN)
apache2 2388 www-data 4u  IPv6  31184      0t0  TCP *:http (LISTEN)
apache2 2389 www-data 4u  IPv6  31184      0t0  TCP *:http (LISTEN)
apache2 2390 www-data 4u  IPv6  31184      0t0  TCP *:http (LISTEN)
apache2 2391 www-data 4u  IPv6  31184      0t0  TCP *:http (LISTEN)
apache2 2392 www-data 4u  IPv6  31184      0t0  TCP *:http (LISTEN)
apache2 2393 www-data 4u  IPv6  31184      0t0  TCP *:http (LISTEN)

```

Lệnh này hiển thị các quy trình nghe trên cổng 80. Nếu bạn thấy các tiến trình apache2, như được hiển thị thì thực hiện lệnh “**service apache2 stop**” để dừng apache.

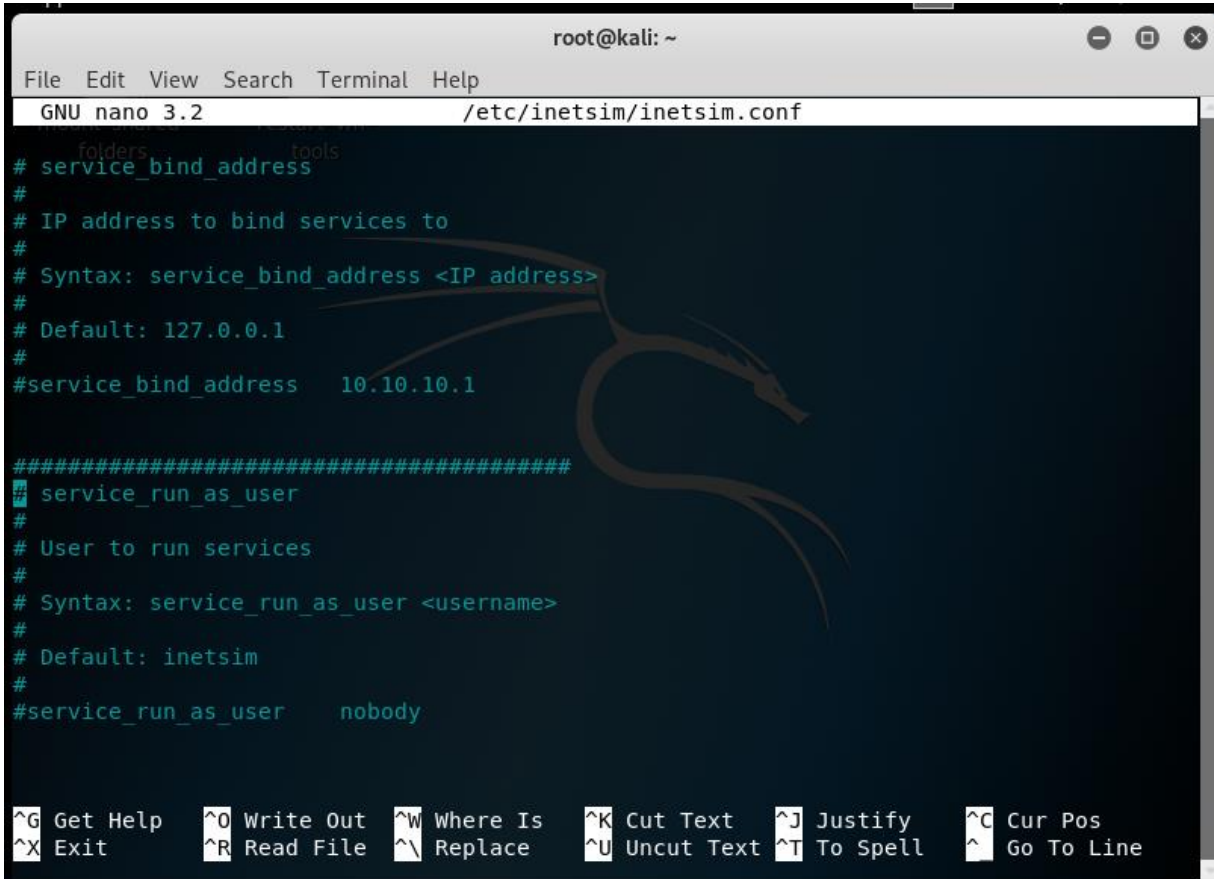
Cấu hình INetSim

INetSim đã có trong Kali Linux 2. Trên máy Linux của bạn, trong cửa sổ Terminal, thực hiện các lệnh sau:

cp /etc/inetsim/inetsim.conf /etc/inetsim/inetsim.conf.orig

nano /etc/inetsim/inetsim.conf

Cuộn xuống khoảng 3 màn hình. Tìm phần **service_bind_address** hiển thị bên dưới. Tất cả những dòng này là nhận xét vì chúng bắt đầu bằng ký tự #.



```
root@kali: ~
File Edit View Search Terminal Help
GNU nano 3.2 /etc/inetsim/inetsim.conf

# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
#service_bind_address 10.10.10.1

#####
# service_run_as_user
#
# User to run services
#
# Syntax: service_run_as_user <username>
#
# Default: inetsim
#
#service_run_as_user nobody

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell   ^_ Go To Line
```

Thay đổi dòng:

#service_bind_address 10.10.10.1 thành **service_bind_address 0.0.0.0**

như hình dưới đây. Điều này đặt INetSim lắng nghe trên tất cả các địa chỉ IP của Kali.

```
root@kali: ~
File Edit View Search Terminal Help
GNU nano 3.2 /etc/inetsim/inetsim.conf
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 0.0.0.0

#####
# service_run_as_user
#
# User to run services
#
# Syntax: service_run_as_user <username>
#
# Default: inetsim
```

Xóa # ở đầu dòng

Cuộn xuống một vài màn hình khác để tìm phần **dns_default_ip** được hiển thị bên dưới. Tìm dòng này: **#dns_default_ip 10.10.10.1**

Xóa # ở đầu dòng và thay thế địa chỉ IP bằng địa chỉ IP của máy Kali Linux của bạn, như được hiển thị bên dưới: **dns_default_ip 192.168.235.131**

```
root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~ x root@kali: ~ x + v
GNU nano 3.2 /etc/inetsim/inetsim.conf Modified

#
#dns_bind_port          53

#####
# dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
dns_default_ip          192.168.235.131

#####
# dns_default_hostname
#
# Default hostname to return with DNS replies
#

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text     ^J Justify     ^C Cur Pos
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line
```

Thay đổi địa chỉ IP mặc định "192.168.235.131".

Lưu tệp bằng Ctrl + X, Y, Enter.

Để bắt đầu INetSim, trong cửa sổ Terminal, thực hiện lệnh: **inetsim**

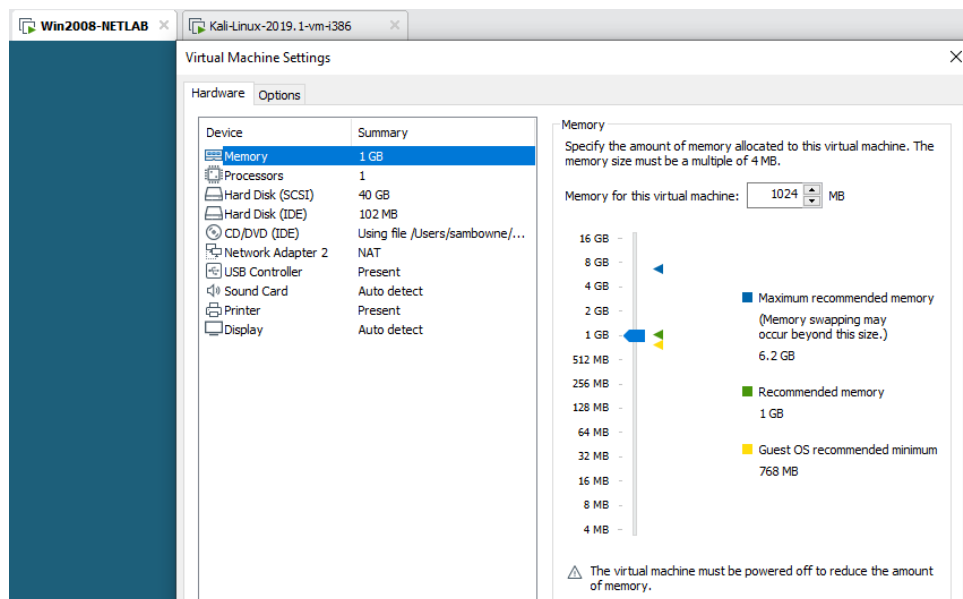

```
Applications ▾ Places ▾ Terminal ▾ Wed 08:32 1
root@kali: ~
File Edit View Search Terminal Tabs Help

root@kali: ~ x root@kali: ~ x + ▾

root@kali:~#
root@kali:~# inetsim
INetSim 1.2.7 (2017-10-22) by Matthias Eckert & Thomas Hungenberg
Main logfile '/var/log/inetsim/main.log' does not exist. Trying to create it...
Main logfile '/var/log/inetsim/main.log' successfully created.
Sub logfile '/var/log/inetsim/service.log' does not exist. Trying to create it...
Sub logfile '/var/log/inetsim/service.log' successfully created.
Debug logfile '/var/log/inetsim/debug.log' does not exist. Trying to create it...
Debug logfile '/var/log/inetsim/debug.log' successfully created.
Using log directory: /var/log/inetsim/
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 2506) ===
Session ID: 2506
Listening on: 0.0.0.0
Real Date/Time: 2020-02-26 08:31:37
Fake Date/Time: 2020-02-26 08:31:37 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 2510)
* ident_113_tcp - started (PID 2523)
* daytime_13_tcp - started (PID 2527)
* irc_6667_tcp - started (PID 2520)
* tftp_69_udp - started (PID 2519)
* dummy_1_udp - started (PID 2538)
```

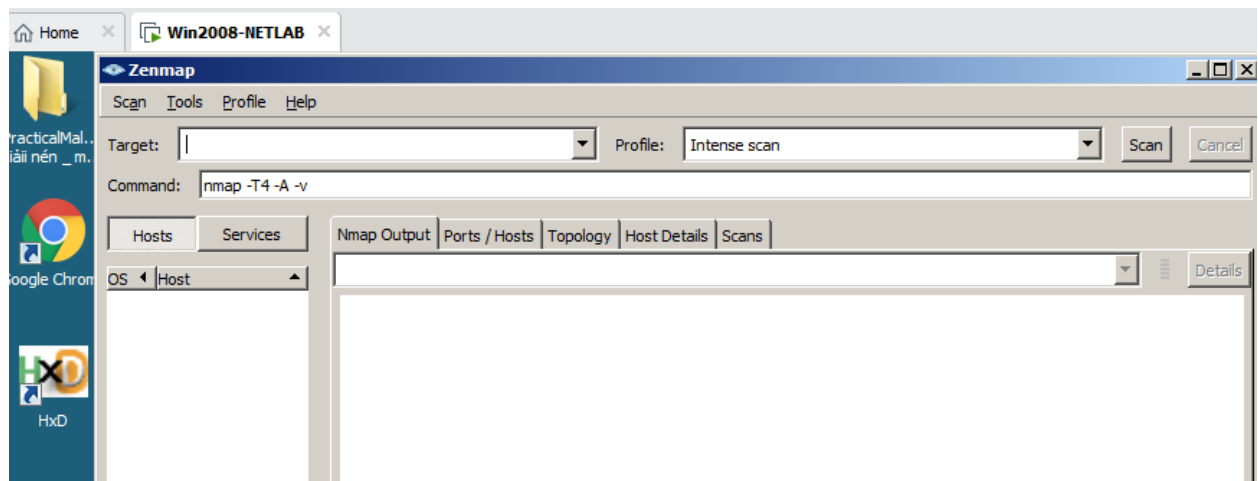
B. Cài đặt máy Win2008

Chỉnh card mạng về chế độ NAT



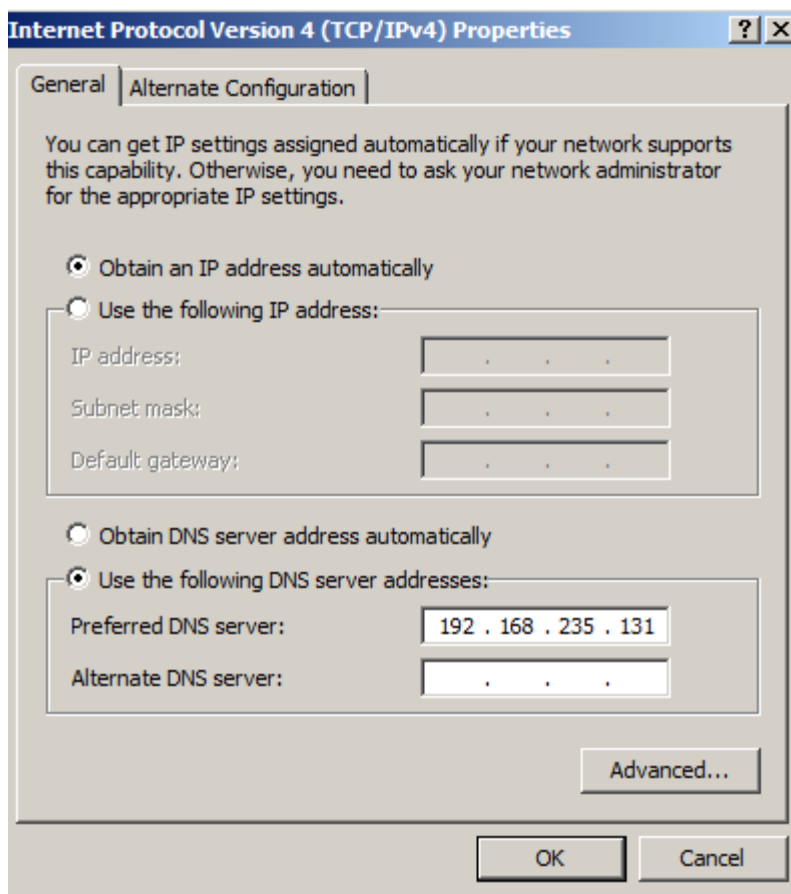
Cài đặt Nmap

Tải Nmap tại <http://nmap.org/> và cài đặt.



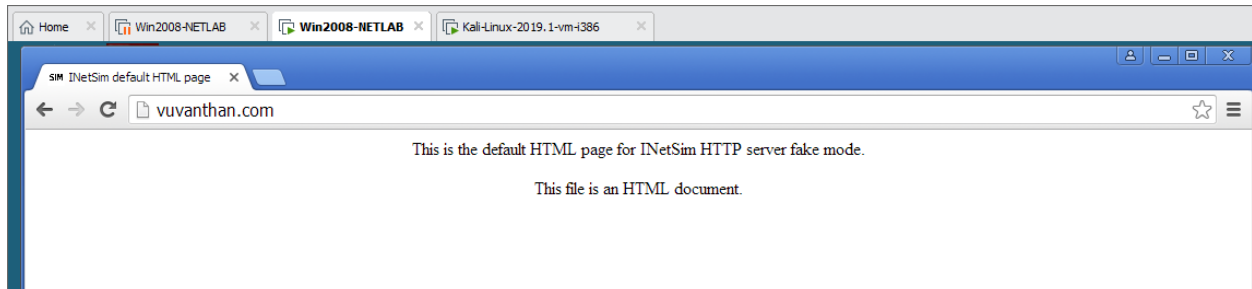
Cài đặt DNS Server

Sửa địa chỉ máy chủ DNS thành địa chỉ IP của máy Kali Linux.



Mở trình duyệt Web trên Windows VM và truy cập URL: <http://vuvanthan.com> (có thể là 1 URL bất kỳ)

Bạn thấy trang HTML mặc định của INetSim, như được hiển thị bên dưới:

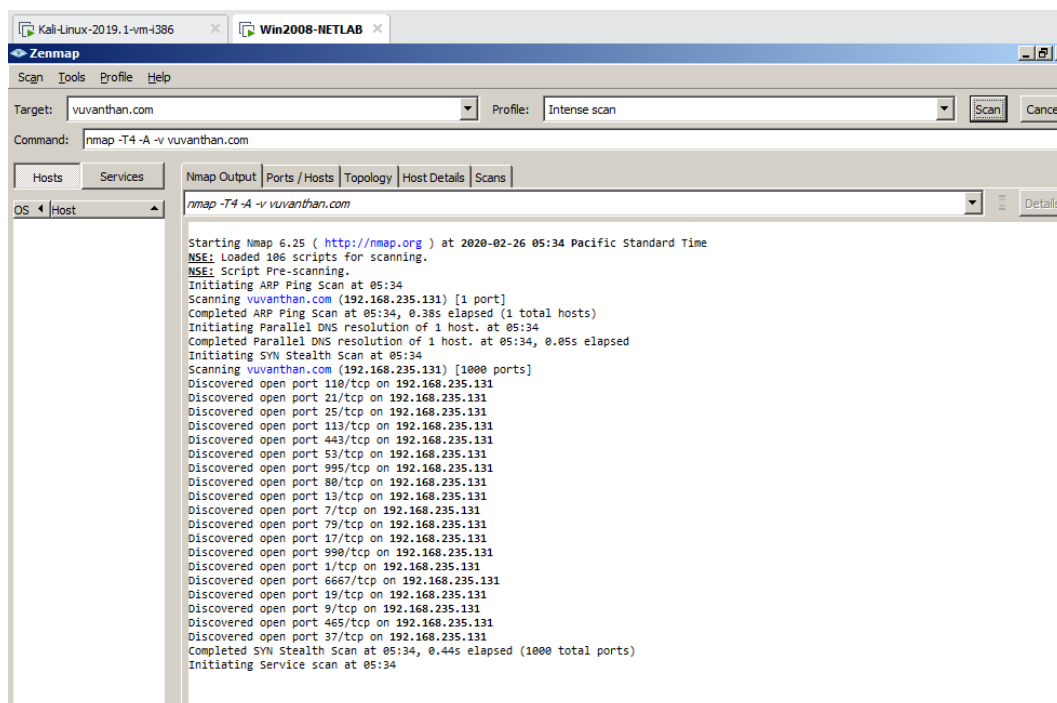


Trình duyệt Web cần hiển thị hai điều sau:

- Vuvanthan trong URL
- Thông báo "INetSim HTTP server"

Quét đường dẫn vuvanthan.com

Mở Nmap. Nhập **vuvanthan.com** sẽ thấy rất nhiều cổng mở như hình dưới đây.



1.5. Cài đặt bộ công cụ phân tích mã độc

Sinh viên tự cài đặt các công cụ phân tích tĩnh, phân tích động vào máy ảo Win2008:

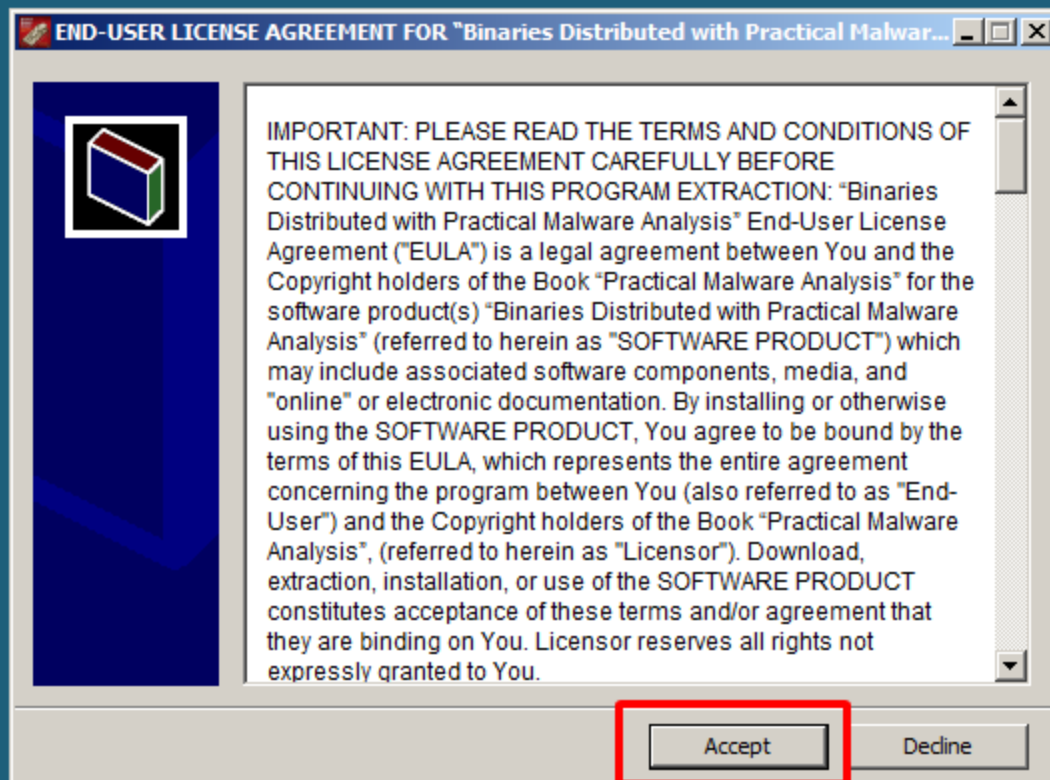
- + Peview
- + PEiD
- + Bintext
- + Dependency Walker
- + Process monitor
- + Process explorer
- + IDA Pro
- +

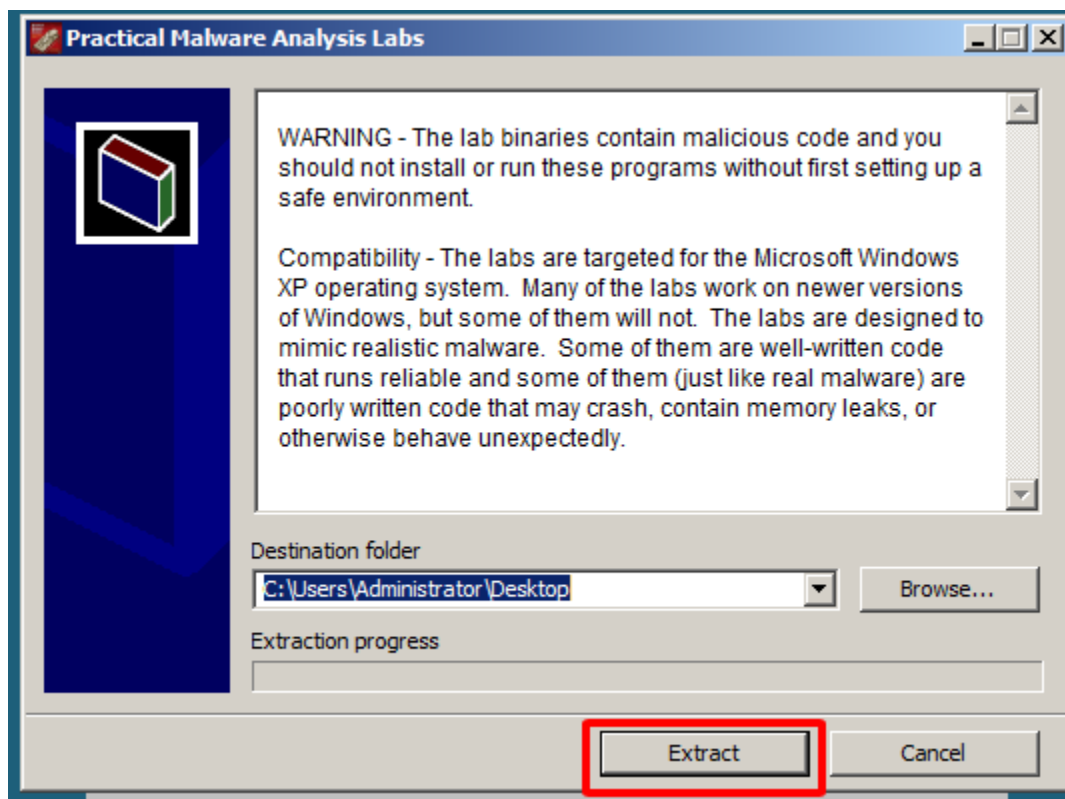
1.6. Cài đặt bộ mẫu mã độc

Tải các mẫu mã độc tại link:

<https://github.com/mikesiko/PracticalMalwareAnalysis-Labs>

Tải tệp 7-zip về **máy thật**, giải nén tệp bằng mật khẩu “malware”, được tệp EXE. **Copy tệp EXE vào máy Win2008**, **nhấp đúp** để thực hiện giải nén tiếp. Nhấp vào nút **Accept**. Nhấp vào nút **Extract**.





Kết quả ta thu được thư mục " Practical Malware Analysis Labs". Các mẫu mã độc có trong "Binarycollection ".



