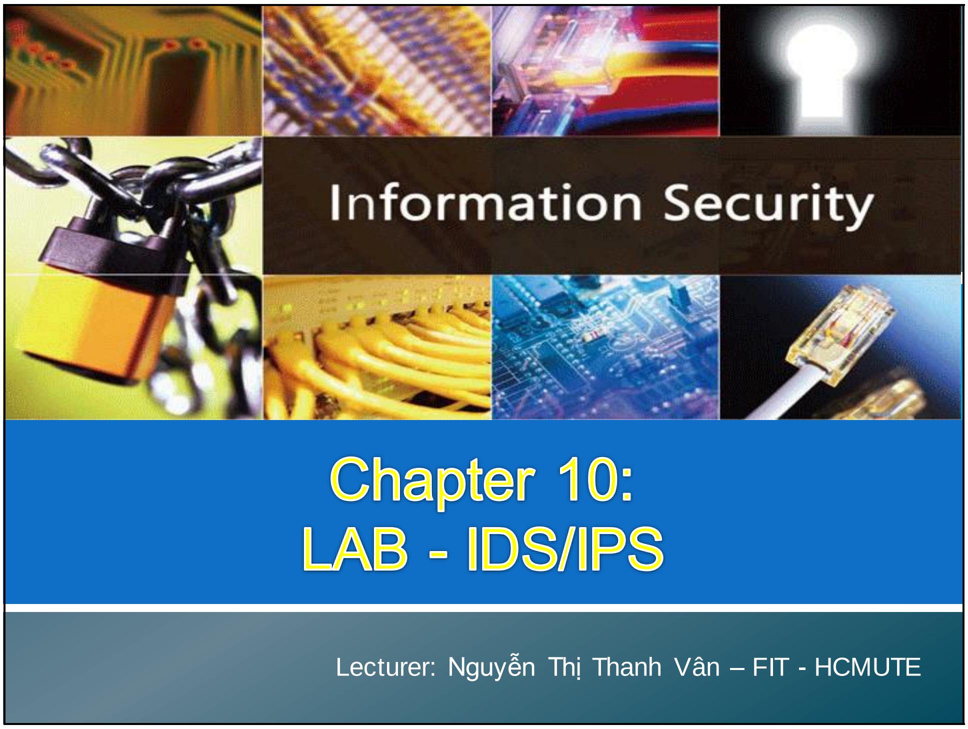
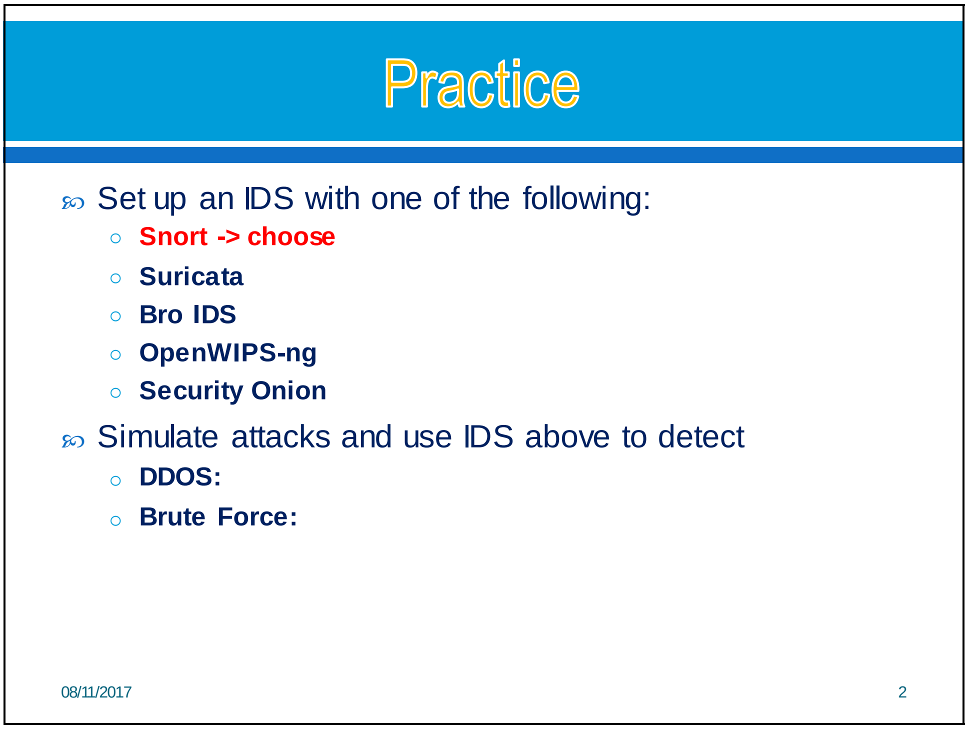


Information Security

Chapter 10:
LAB - IDS/IPS

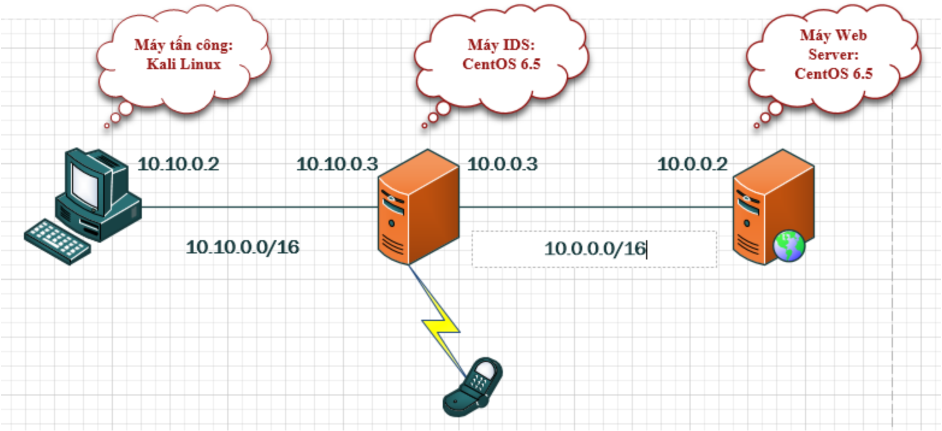
Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE



Practice

- Set up an IDS with one of the following:
  - **Snort -> choose**
  - **Suricata**
  - **Bro IDS**
  - **OpenWIPS-ng**
  - **Security Onion**
- Simulate attacks and use IDS above to detect
  - **DDOS:**
  - **Brute Force:**

IDS

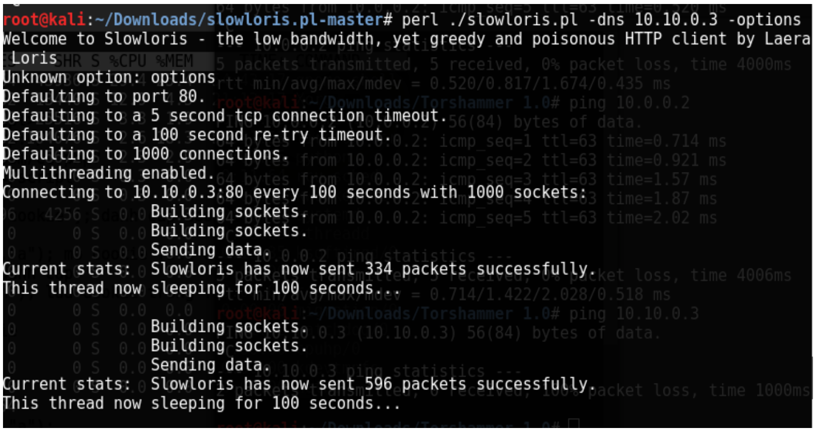


Process

- Set up IDS with Snort
  - Download and install Snort
  - Database: MySQL – install, create, GRANT….
  - Graphic Interface for Snort:
    - Web server, PHP
    - pear
    - **ADODB:** ***http://nchc.dl.sourceforge.net/sourceforge/adodb/***
    - **BASE:** ***http://nchc.dl.sourceforge.net/sourceforge/secureideas/base-1.4.2.tar.gz***
- Set up attacker machine (DOS, Brute Force)
  - **DDOS:** slowloris.pl – download and install - run
  - **Brute Force:** xHydra (Kali Linux) - run

DoS, ex

Attack:



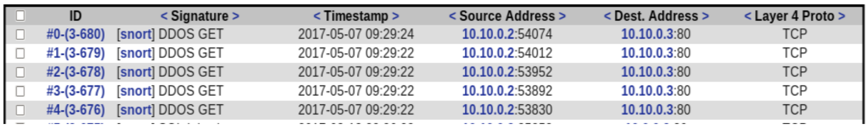
```
root@kali:~/Downloads/slowloris.pl-master# perl ./slowloris.pl -dns 10.10.0.3 -options
Welcome to Slowloris - the low bandwidth, yet greedy and poisonous HTTP client by Laera
 Loris
Unknown option: options
Defaulting to port 80.
Defaulting to a 5 second tcp connection timeout.
Defaulting to a 100 second re-try timeout.
Defaulting to 1000 connections.
Multithreading enabled.
Connecting to 10.10.0.3:80 every 100 seconds with 1000 sockets:
                Building sockets.
                Building sockets.
                Sending data.
Current stats:  Slowloris has now sent 334 packets successfully.
This thread now sleeping for 100 seconds...

                Building sockets.
                Building sockets.
                Sending data.
Current stats:  Slowloris has now sent 596 packets successfully.
This thread now sleeping for 100 seconds...
```

- Rule:

alert tcp any -> $HOME_NET 80 (msg:"DDOS GET";content:"GET / HTTP"; flow:to_server, established; threshold: type threshold, track by_src, count 30, seconds 30; sid:1000004;)

DoS, ex

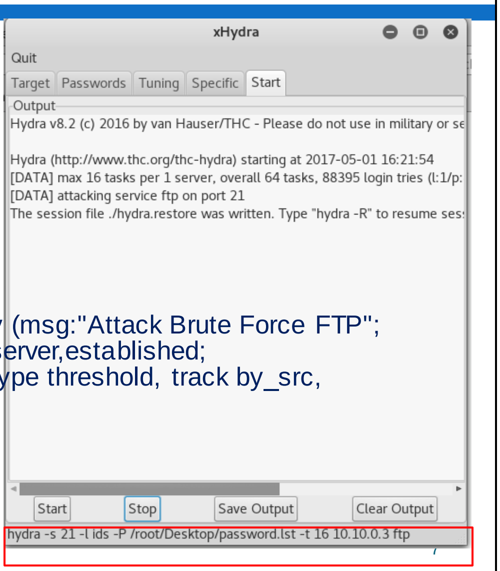
- Result:



□	ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
□	#0-(3-680)	[snort] DDOS GET	2017-05-07 09:29:24	10.10.0.2:54074	10.10.0.3:80	TCP
□	#1-(3-679)	[snort] DDOS GET	2017-05-07 09:29:22	10.10.0.2:54012	10.10.0.3:80	TCP
□	#2-(3-678)	[snort] DDOS GET	2017-05-07 09:29:22	10.10.0.2:53952	10.10.0.3:80	TCP
□	#3-(3-677)	[snort] DDOS GET	2017-05-07 09:29:22	10.10.0.2:53892	10.10.0.3:80	TCP
□	#4-(3-676)	[snort] DDOS GET	2017-05-07 09:29:22	10.10.0.2:53830	10.10.0.3:80	TCP

Brute force, ex

- Attack:



```
Hydra v8.2 (c) 2016 by van Hauser/THC - Please do not use in military or se

Hydra (http://www.thc.org/thc-hydra) starting at 2017-05-01 16:21:54
[DATA] max 16 tasks per 1 server, overall 64 tasks, 88395 login tries (l:1/p:
[DATA] attacking service ftp on port 21
The session file ./hydra.restore was written. Type "hydra -R" to resume ses:
```

```
hydra -s 21 -l ids -P /root/Desktop/password.lst -t 16 10.10.0.3 ftp
```

- Rule:

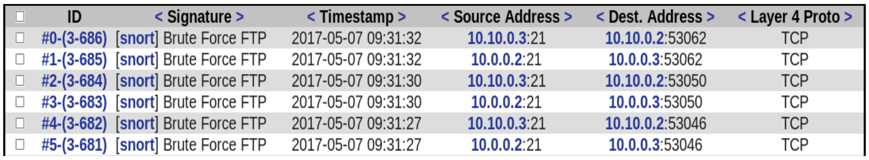
alert tcp any 21 -> $HOME_NET any (msg:"Attack Brute Force FTP"; content:"Login incorrect"; flow:from_server,established; classtype:bad-unknown; threshold: type threshold, track by_src, count 10, seconds 2; sid: 1000009;)

08/11/2017

7

Brute force, ex

- Result



□	ID	< Signature >	< Timestamp >	< Source Address >	< Dest. Address >	< Layer 4 Proto >
□	#0-(3-686)	[snort] Brute Force FTP	2017-05-07 09:31:32	10.10.0.3:21	10.10.0.2:53062	TCP
□	#1-(3-685)	[snort] Brute Force FTP	2017-05-07 09:31:32	10.0.0.2:21	10.0.0.3:53062	TCP
□	#2-(3-684)	[snort] Brute Force FTP	2017-05-07 09:31:30	10.10.0.3:21	10.10.0.2:53050	TCP
□	#3-(3-683)	[snort] Brute Force FTP	2017-05-07 09:31:30	10.0.0.2:21	10.0.0.3:53050	TCP
□	#4-(3-682)	[snort] Brute Force FTP	2017-05-07 09:31:27	10.10.0.3:21	10.10.0.2:53046	TCP
□	#5-(3-681)	[snort] Brute Force FTP	2017-05-07 09:31:27	10.0.0.2:21	10.0.0.3:53046	TCP

08/11/2017

8