INFORMATION SECURITY FUNDAMENTALS

Purpose

- Understand IDS, IPS
- Understand differences between IDS, IPS and firewall
- Understand Snort rules and commands
- Ability to write a Snort rules
- Ability to operate Snort basically

Class Activities

1. Activity 1 (individual)
    - Estimated Duration: 20 mins

Students research on Firewall, IDS and IPS and try to answer following questions:

- What is IDS?
- What is IPS?
- Indicate differences between IDS and IPS
- Indicate differences between Firewall and IDS

2. Activity 2 (individual)
    - Estimated Duration: 20 mins

Students research on Snort and try to answer following questions:

- What is Snort?
- 3 working modes of Snort: sniffer mode, logging mode and IDS mode.
- Snort rule syntax?
- Meaning of the following snort rules:

```
alert tcp 127.0.0.1 any -> any any (msg:"access eBay";content:"eBay.com";
alert tcp 127.0.0.1 any -> any any (msg:"Access to
Youtube";content:"www.youtube.com"; sid:1000001;) log icmp any any ->
any any (msg: " PING PING PING";sid:10000007;) log !192.168.1.0/24 any
<> 192.168.1.0/24 23
```

`alert` - generates an alert using the selected alert method, and then log

the packet `log` - logs the packet `pass` - drops (ignore) the packet

3. Activity 3 (individual): Snort Installation

- Estimated Duration: 40 mins

Students install and configure Snort, following instructions at Snort Installation Guide, available at FIT portal.

4. Activitiy 4 (group): Snort Testing

- Estimated Duration: 40 mins

a. Test Snort

- Validate Snort configuration

```
C:\Snort\bin>snort  -i 1 -l  C:\Snort\log  -c  C:\Snort\etc\snort.conf  -T
```

-T = Test and report on the current snort configure

- Test alerts mode of Snort

```
C:\Snort\bin>snort  -i 1 -l  C:\Snort\log  -c  C:\Snort\etc\snort.conf  -A full
```

Where -A = set alert mode: fast ,full,console,test or none

b. Detect ICMP/WEB traffic

- Add the following rules to rules\local.rules to detect ICMP packets:

  ```
  alert icmp any any -> any any (msg: “ PING PING PING";sid:10000007;)
  ```

- Run logging mode

```
C:\Snort\bin>snort  -i 1-l  C:\Snort\log  -c  C:\Snort\etc\snort.conf  -K ascii
```

- Ask your friends to ping your PC and check it out in log file.

More details at: Snort Installation Guide, available at FIT portal.

References http://badshah-tech.blogspot.com/2012/08/install-and-configure-snort-ids-on.html