University
Carlos III of Madrid

Distributed Systems Security

Denial of Service (DoS) Detection

IT Security Group

Guillermo Suárez de Tangil
(guillermo.suarez.tangil@uc3m.es)

Remembering module 1…

- Firewall configuration
  - All users should have granted access to Fakebook
  - The machine should have granted access to security updates
  - Any other access should’ve not be granted
  - Remote access and PING should be logged
  - Remote connections only from a specific IP address
- SSH
  - Remote administration (SSH)
- File-system Permissions
  - New web administrator user

Today

- Denial of Service Attack
  - We will see how to detect a DoS…
- Snort
  - … by means of **Snort**,
  - an Intrusion Detection System (IDS)

Denial of Service Detection

- Attempt to make a computer resource unavailable
- Prevent an internet site or service from functioning efficiently or at all, temporarily or indefinitely:
  - Web servers
  - Gateways such as credit card payments
  - Root name server
- Techniques:
  - Saturation
  - Malformed packets
- Techniques:
  - Http Flood, ICMP Flood, SYN Flood, etc.

Prevention and Response

- How to detect DoS?
  - Blocking malicious packets
    - *Ping of the dead*
  - Blocking saturation
    - Counting number of connections per second from the same source IP
- Yes! But what about…?
  - Low-rate Denial-of-Service attacks
  - Permanent denial-of-service attacks

Prevention and Response

- Effective prevention and response:
  - Firewalls
    - Deny some protocols
  - Switches and routers
    - Rate limiting capability
  - **Intrusion Detection and Prevention Systems**

Intrusion Detection Systems (IDS)*

- Network and computer intrusions presents behavioral patterns
- Intrusion Detections
  - Methods and techniques used to detect suspicious activities
  - Matching of data with a set of known rules
  - Generate alerts and logs suspicious activities
- Classification
  - Network IDS (NIDS)
    - Sniffs network traffic
  - Host IDS (HIDS)
    - Monitors computers

Intrusion Detection Systems (IDS)

- Pattern
  - Signatures revealing malicious activities
  - In network packets:
    - Patterns can be related to any of the attributes of the packet
- Alerts
  - Anomalous activity is notified to the user and/or admin
  - Stored in a log file or a data base
- False Alert
  - Generated by non-malicious activity
- Sensor
  - Machine in which the IDS is running

Snort

- NIDS tool
- Anomaly-based inspection
  - Packet headers
- Misuse detection (pattern)
  - Packet content
- Open source multiplatform
- Rule files grouped into categories: **/etc/snort/rules**
- Configuration file: **/etc/snort/snort.conf**

Snort Components

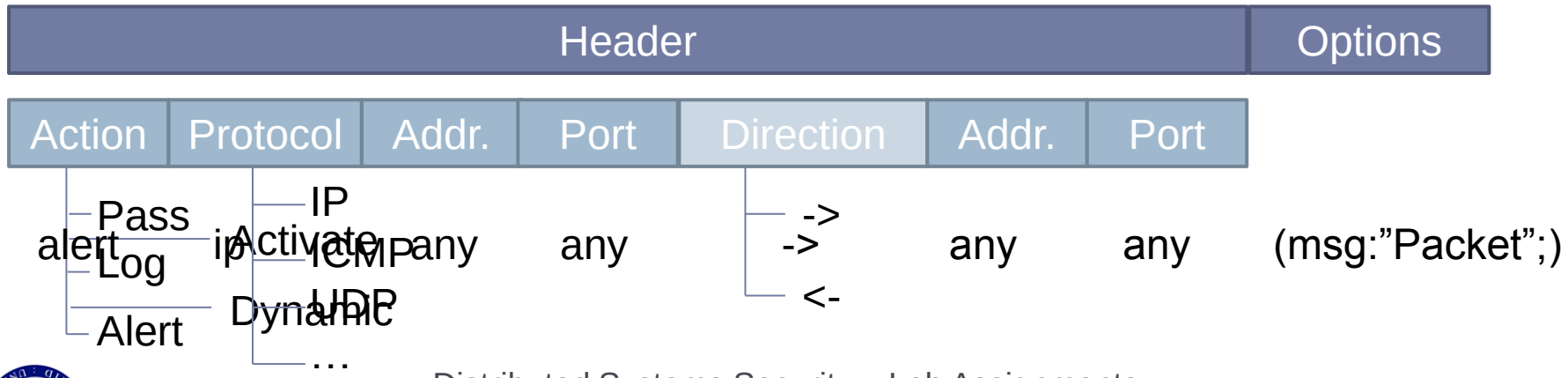
- Packet decoder
  - Sniffs packets and decode them
- Preprocessor
  - Run before the detection engine is called, but after the packet has been decoded
  - The packet can be modified or analyzed in an out-of-band manner
- Detector engine
  - Pattern matching according to pre-configured rules
- Alert system
  - **/var/log/snort**
- Output modules
  - Plug-ins -> Logs and alarms

Snort commands

- Verification
  - ./snort –dvi eth0
- Start and stop
  - /etc/init.d/snortd start/stop
  - ./snort –A full snort.conf
- Help
  - ./snort -?
- Alerts
  - tail -f /var/log/snort/alerts

Snort Rules

- Rules
  - Header
    - **Matching** conditions
    - Post-condition **actions**
  - Options
    - Alert message
    - Additional criterions



Snort Rule Options

- Options
  - msg: message
  - dsize: size of the payload
  - content: content of the payload (most used)
  - classtype: keyword is used to categorize a rule
  - **sid: snort id**
- Example
  - alert tcp any any -> 192.168.1.0/24 21 (content: "USER root"; nocase; msg: "FTP root user access attempt";)

Snort Rule Options

- **flags**:
  - F - FIN (LSB inTCP Flags byte)
  - S - SYN
  - R - RST
  - P - PSH
  - A - ACK
  - U - URG

- **Logic operators**
  - * - ANY flag
  - ! - NOT flag

Example

- alert any any -> 192.168.1.0/24 any (flags: SF; msg: "Possible SYN FIN scan";)

Preparing the environment

- DoS:
  - Small test:
    - **HttpFloodDoS.java**
  - Optionally:
    - http://www.joedog.org/index/siege-home
- Installing snort
  - Execute **cleanUbuntu.sh**
  - Execute **sudo –i**
  - Execute **installSnort.sh**
  - Configure:
    - Configuring snort Interface(s): eth2
    - Address range for the local network: 192.168.0.0/16

DoS Detection in Fakebook

- Task:

> Provide the server with an Intrusion Detection System (IDS) so that the system's administrator will be alerted whenever a machine is performing a large number of connections to Fakebook.

- Documentation:
  - http://www.snort.org/assets/166/snort_manual.pdf
- Tips
  - Detection filters (3.7.10):
    - You can use detection filters to specify a threshold that must be exceeded before a rule generates an event.
  - Event filters (2.4.2)
    - You can use event filters to reduce the number of logged events for noisy rules. This can be tuned to significantly reduce false alarms

University
Carlos III of Madrid

Distributed Systems Security

Lets work!

Guillermo Suárez de Tangil
(guillermo.suarez.tangil@uc3m.es)