Project phase 4+ & report

WPI CS4516 Spring 2019 D term

Instructor: Lorenzo De Carli (ldecarli@wpi.edu)

ATTN: phase 4+ is only required for teams needing 1 BS/MS extra credit

The project report is required for **all teams**

Overall goals

- Phase 1: gateway creation
- Phase 2: traffic sniffing/logging
- Phase 3: offline traffic classification
- Phase 4: online traffic classification
- Phase 4+: firewalling based on classification
  - **Due on 4/29**

Expected result

- Blacklist remote IP addresses associated with two applications:
  - Fruit Ninja
  - Youtube
- Every time a flow is labeled as generated by one of the applications above, communication with the remote endpoints part of the flow must be permanently blocked

How to accomplish the result

- Use Linux's built-in firewall (iptables)
- As soon as a flow is labeled, issue an iptables command to block packets to/from the flow's remote endpoint
  - To clarify: "remote endpoint" means the IP with which the Android VM is communicating (not the IP of the VM itself)
- Additional requirement: do not break networking in the VM (must be careful not to blacklist the DNS server and the gateway VM)

How to interact with iptables

- Option 1: use shell commands (“os.system” in Python)
- Option 2: use an iptables Python wrapper (python-iptables)
- (Option 1 is the easiest and requires little or no dependencies to be installed)

Phase 4+ deliverable

- Upload a copy of the gateway VM with the following files in /home/tc:
  - A Python script named blockFlows. When executed, the script must print out a list of bursts, flows in every burst, and the label of each flow that originated a certain action (if any). Flows by the two applications to be blocked must be additionally labeled as “BLOCKED”:

```
➢ ./blockFlows
Burst 1:
<timestamp> <src addr> <dst addr> <src port> <dst port> <proto>\
<#packets sent> <#packets rcvd> <#bytes send> <#bytes rcvd> \
<label> BLOCKED
```

Phase 4+ grading

- We will execute all the actions described in Phase 3
- We will verify if:
  - Executing blacklisted actions results in iptables rules blocking the destination Ips
  - Executing non-blacklisted actions does not have any effect

Phase 4+ deliverable/2

- Upload a copy of the gateway VM with the following files in /home/tc:
  - A file named readme.txt describing:
    - Anything we need to know in order to run and grade your work
    - Anything else you want us to be aware of (limitations, problems, etc.)

Final project report

- This is required **for all teams**
- **Due on 4/29**
- Each team must deliver a 3 to 6 pages PDF file, single-spaced, 11-point font, 1-inch margins, containing a final project report

Final project report - content

- **Overview:** what the project consisted of and what you implemented
- **Phase details:** a section, clearly divided in 4 paragraphs (5 for teams implementing Phase 4+), describing the implementation of each phase:
  - Phase 1: how was the gateway configured?
  - Phase 2: how was traffic logging implemented?
  - Phase 3: which classification algorithm did you use? Which features? How many traces did you use for training and evaluation? Which accuracy did you obtain?
  - Phase 4: how was the classifier integrated into the traffic logger?
  - Phase 4+: how does the classifier interface to iptables?

Final project report – content/2

- **Lesson learned and limitations:** described anything that you tried during any of the phases that did not work. Also, describe limitations of your implementation and anything that did not perform according to your expectations.

Project report grading

- We will evaluate if :
  - Each section of the report contains answers to the questions listed in the previous slides
  - The report is well-written and clear

Good luck with the final part!