SFU SIMON FRASER UNIVERSITY
ENGAGING THE WORLD

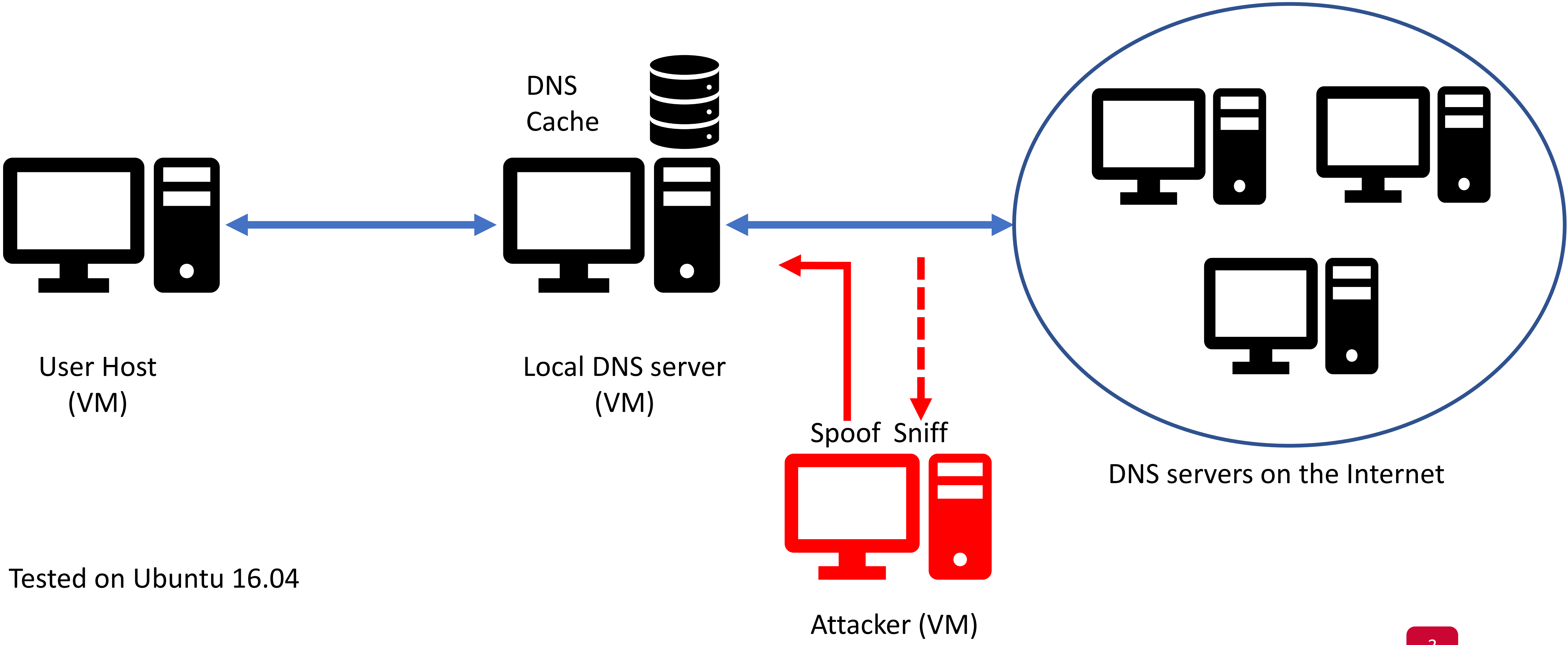
Cybersecurity Lab II

Lab 10

Three Tasks

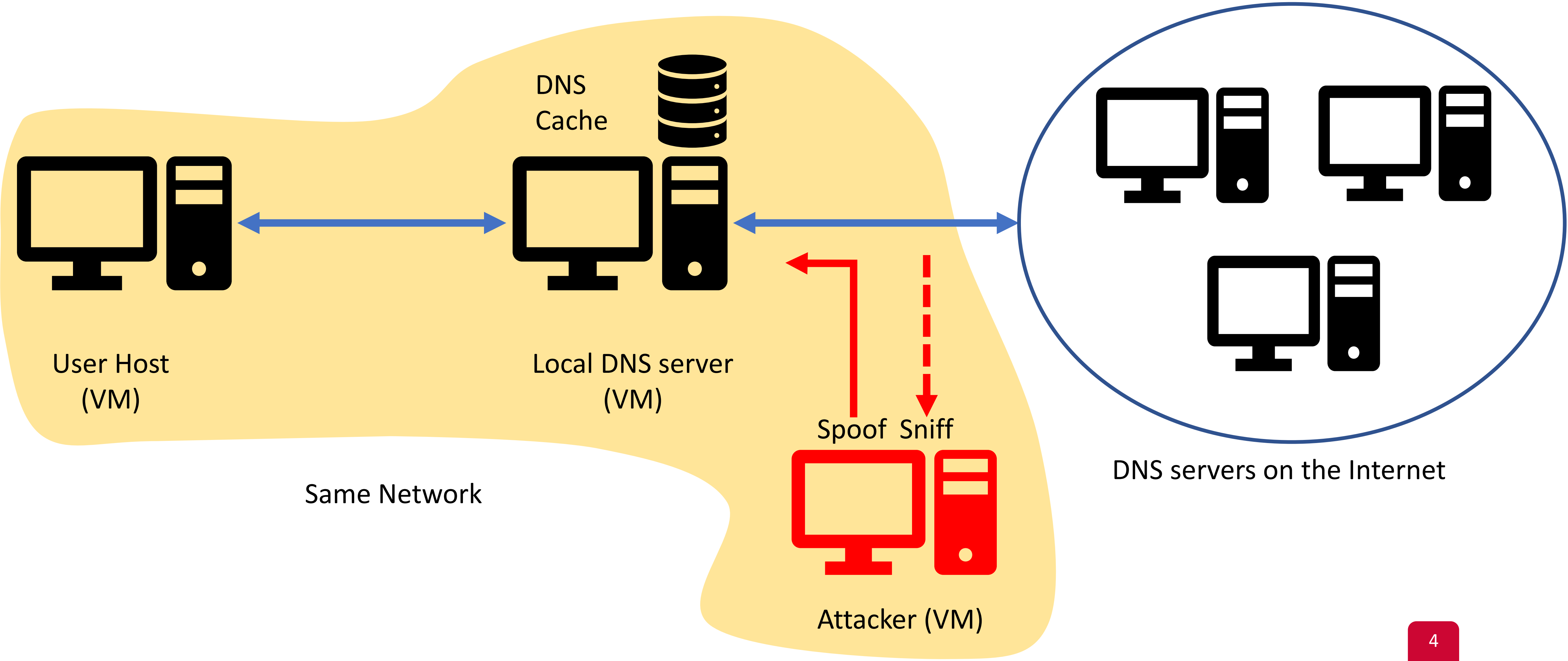
- Setup a local DNS server
- Cache Poisoning: Targeting a single hostname
- Cache Poisoning: Targeting a whole domain

Environment

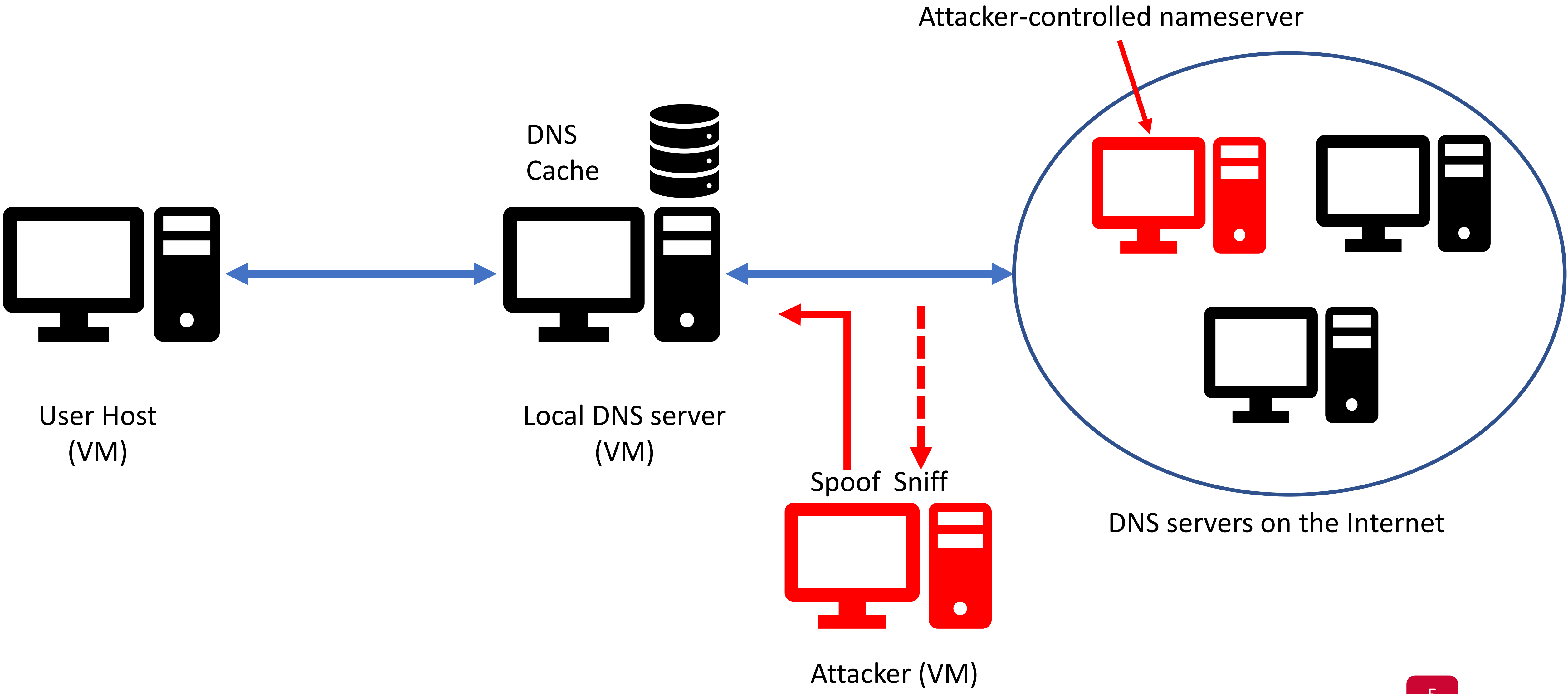


Tested on Ubuntu 16.04

Environment



Environment (Task 3)



Setup local DNS server

- BIND: Berkeley Internet Name Domain
  - A popular DNS server
- You need to:
  1. Install BIND
  2. Configure BIND
  3. Create a DNS zone for “example.com”

Setup local DNS server: Note on Configuration

- Main configuration file: `/etc/bind/named.conf`
- It includes other configuration files, such as:
  - `/etc/bind/named.conf.options`
  - `/etc/bind/named.conf.local`
  - …

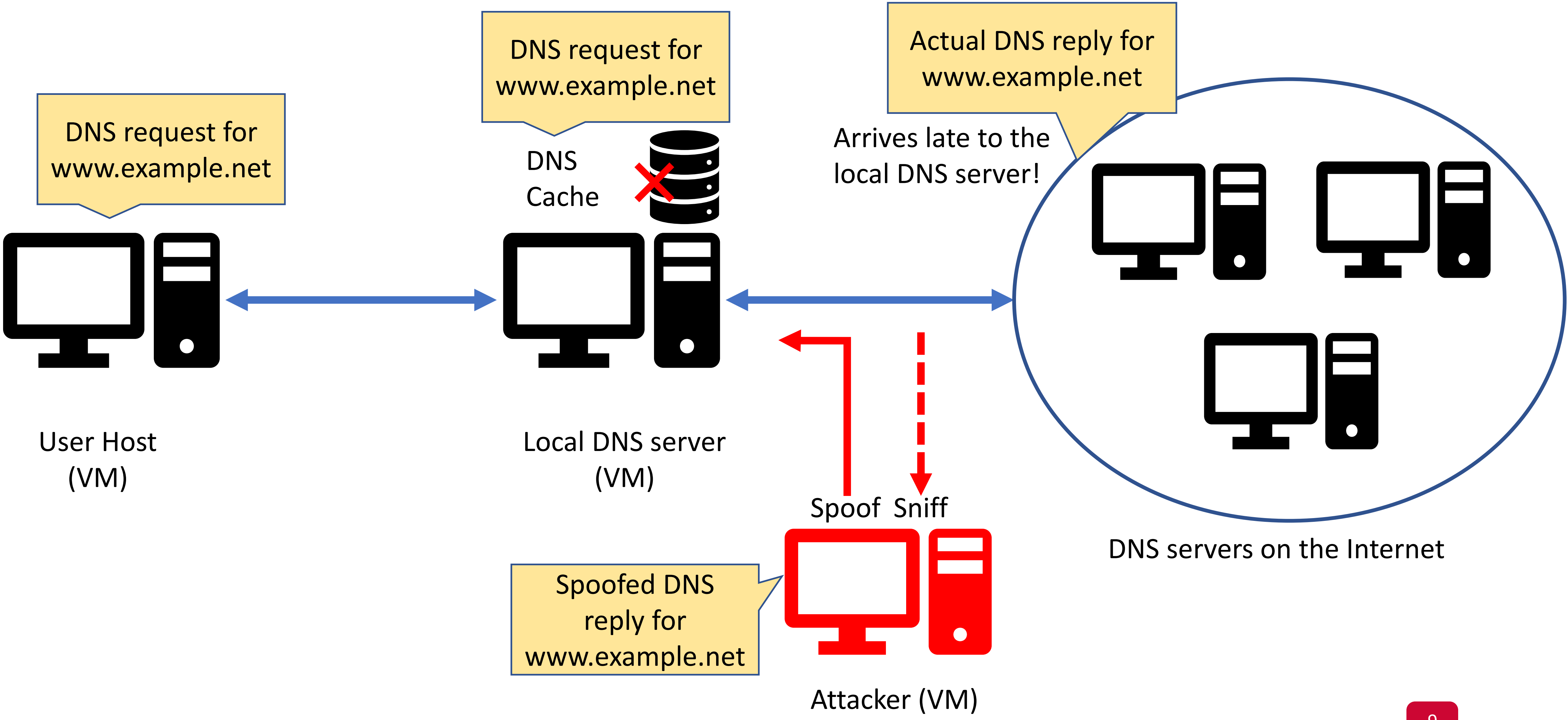
Setup local DNS server: Useful Commands

- Every time you configure BIND:
  - `sudo service bind9 restart`

- To flush the cache:
  - `sudo rndc flush`

- To write the cache content to dump file:
  - `sudo rndc dumpdb -cache`

Targeting a Single Hostname


DNS request for www.example.net
DNS request for www.example.net
DNS
Cache
Actual DNS reply for www.example.net
Arrives late to the local DNS server!
User Host (VM)
Local DNS server (VM)
Spoof
Sniff
DNS servers on the Internet
Spoofed DNS reply for www.example.net
Attacker (VM)

Targeting a Single Hostname

- You may use the “netwox 105” tool
- Sniff the network and send spoofed DNS replies:
  - Including the spoofed Answer Section
- Run the command for advanced usage:

```
$ netwox 105 --help2
```

Targeting the Whole Domain

- Targeting the domain: example.net
- More damaging as the attacker controls *any* hostname!
  - But requires an attacker-controlled nameserver!

- You need to spoof both the:
  - Answer Section
  - Authority Section
- You will use scapy to perform this task

Questions?