

Network Security

- DNS Cache Poisoning -

GROUP 14

Bruno Boscia

Davide Todeschi

Giacomo Filippetto

Lab outline

- **Objective**
- **Environment setup**
- **Step 1:** remote attack (with DoS)
- **Step 2:** defense strategy through port and transaction ID randomization
- **Step 3:** attacker has access to the DNS's network (or eventually has performed a MITM Attack)

Objective

The objective is to show:

- How to poison a record in a recursive DNS's cache
- How defense strategies can prevent a DNS cache poisoning attack

Environment setup

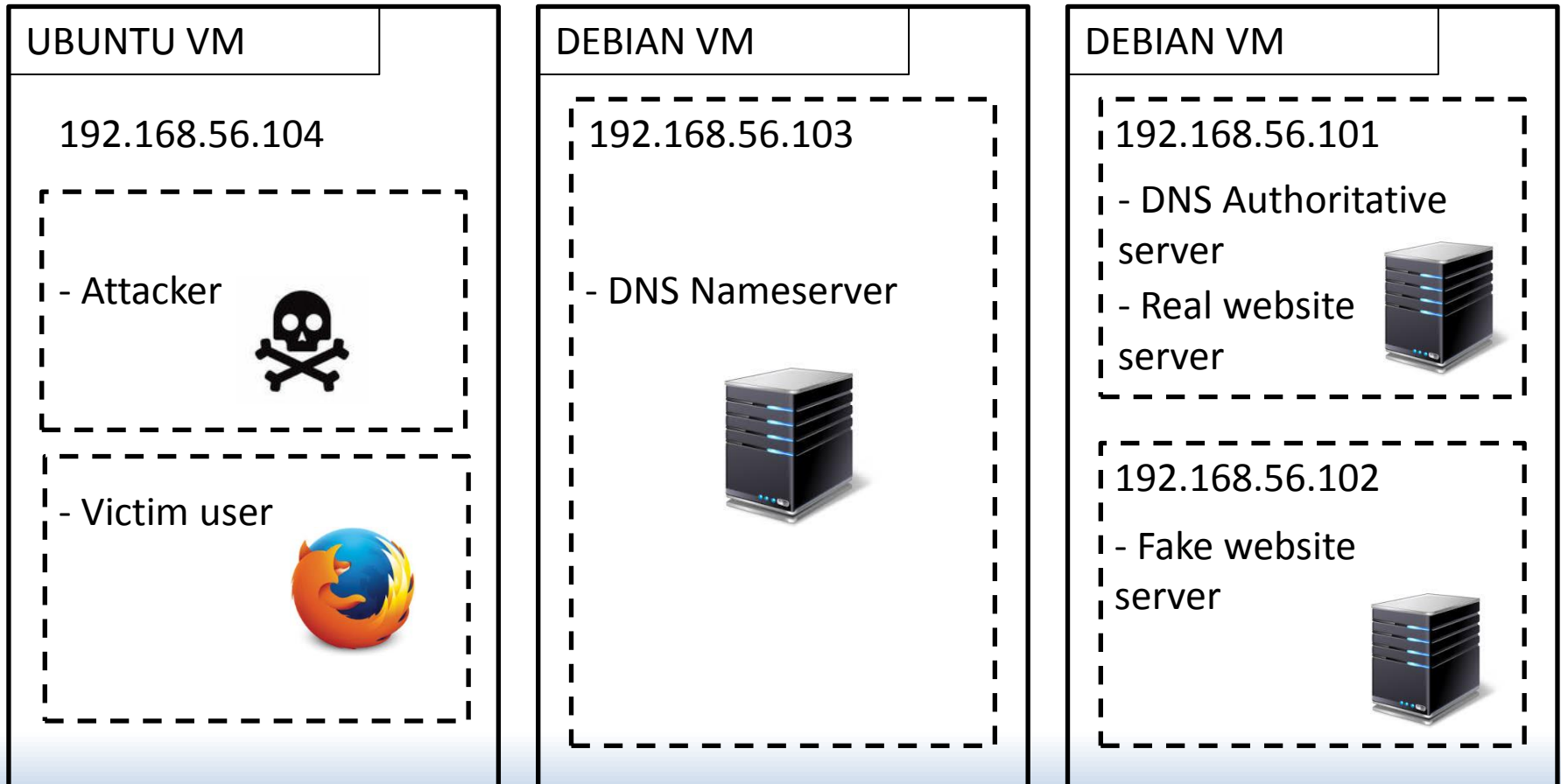
- Start **all** the virtual machines
- The following username and password are valid on each Virtual Machine

username : **user**

password : **netsec**

- Enter the “super user” mode in the server machines typing “su” and entering the password
- Let’s start!

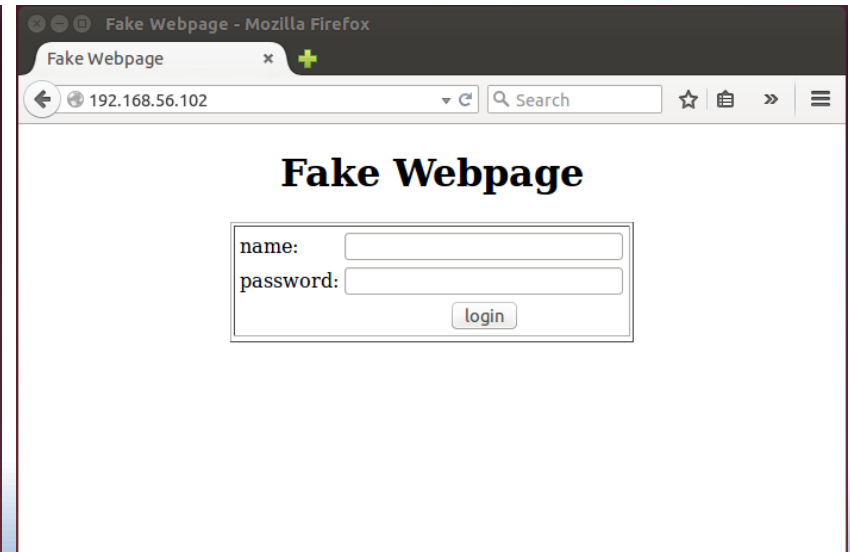
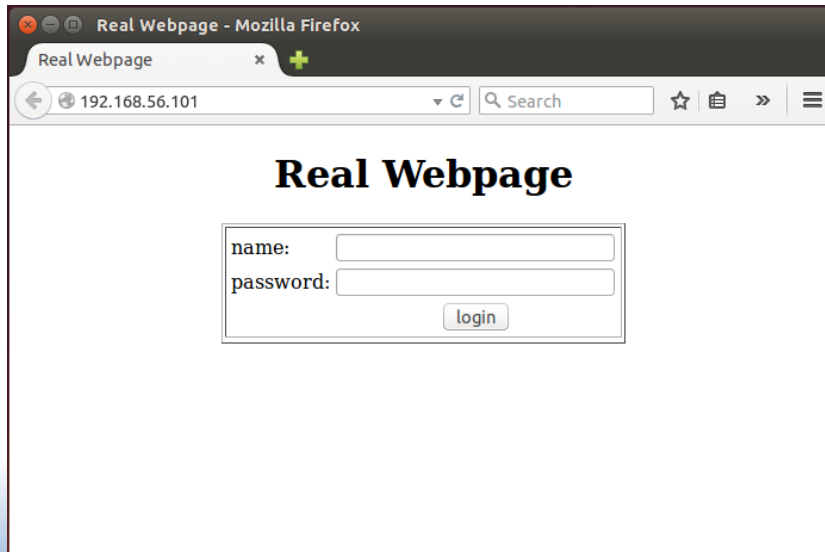
Environment setup



Environment setup

On the Ubuntu machine, verify you can reach the two Web Servers:

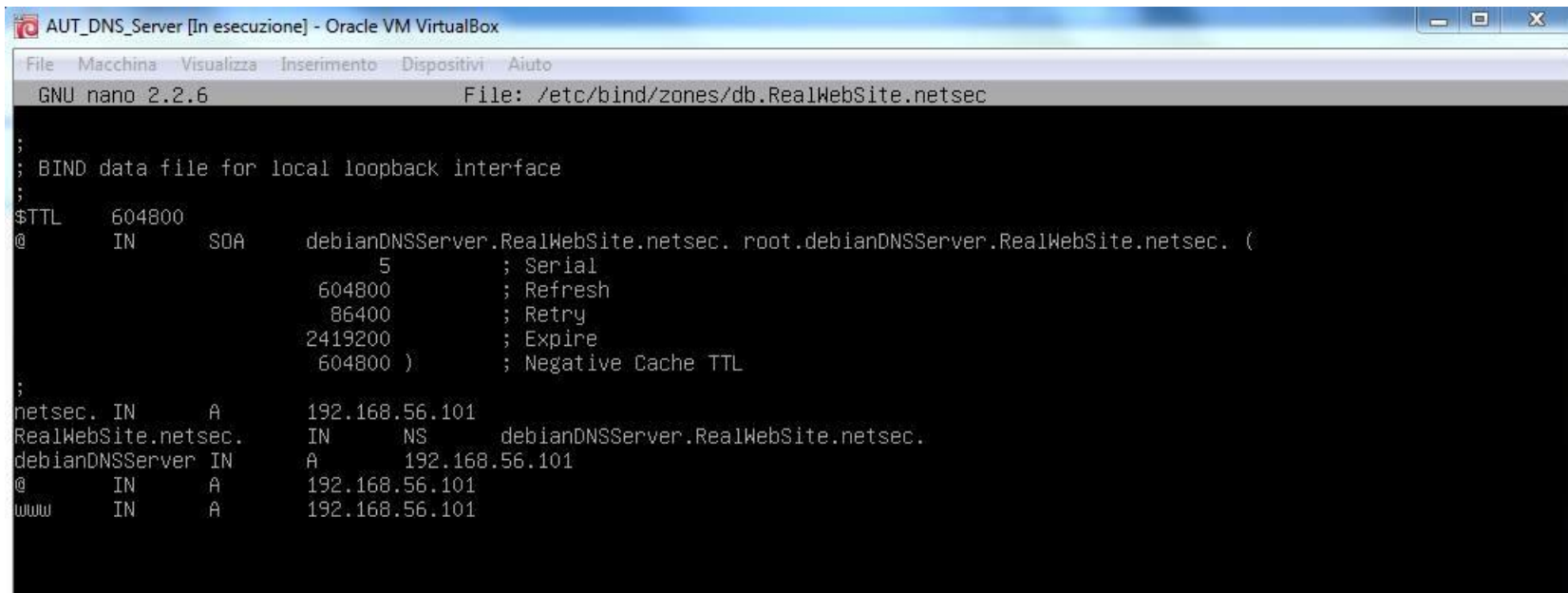
- 192.168.56.101 'Real Website'
- 192.168.56.102 'Fake Website'



Environment setup

On the AUT_DNS_Server machine type:

> nano /etc/bind/zones/db.RealWebSite.netsec

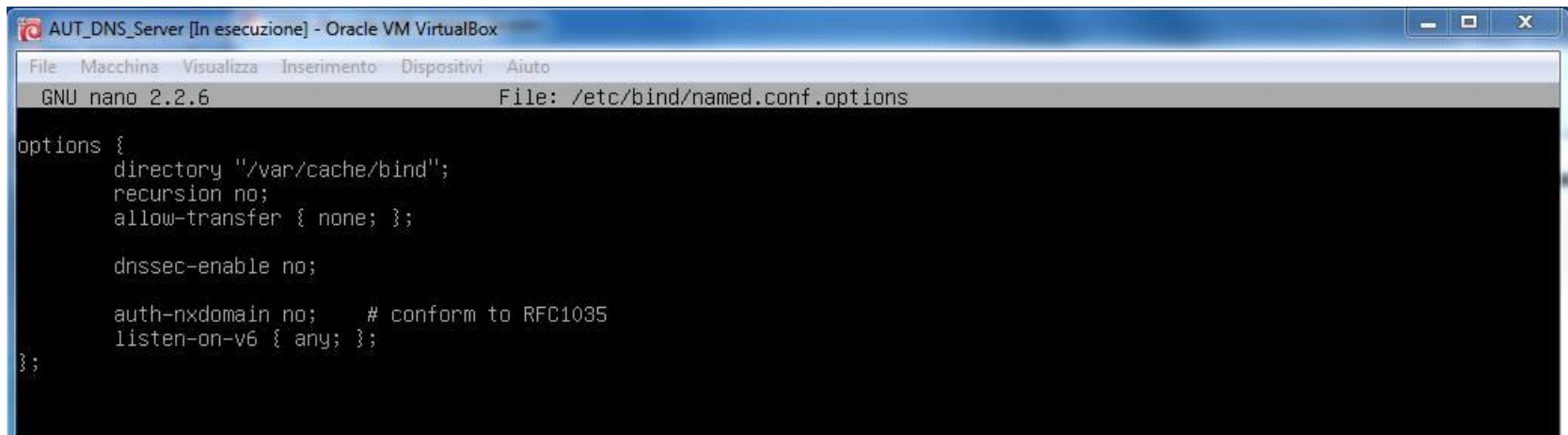


```
AUT_DNS_Server [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.2.6      File: /etc/bind/zones/db.RealWebSite.netsec
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      debianDNSServer.RealWebSite.netsec. root.debianDNSServer.RealWebSite.netsec. (
; Serial
          5          ; Refresh
          604800     ; Retry
          86400     ; Expire
 2419200  ; Negative Cache TTL
          604800 )
;
netsec.   IN      A          192.168.56.101
RealWebSite.netsec. IN  NS      debianDNSServer.RealWebSite.netsec.
debianDNSServer IN  A          192.168.56.101
@         IN      A          192.168.56.101
www      IN      A          192.168.56.101
```

Environment setup

On the AUT_DNS_Server machine type:

> nano /etc/bind/named.conf.options



The screenshot shows a terminal window titled "AUT_DNS_Server [In esecuzione] - Oracle VM VirtualBox". The window contains the output of the nano text editor editing the file "/etc/bind/named.conf.options". The content of the file is as follows:

```
options {
    directory "/var/cache/bind";
    recursion no;
    allow-transfer { none; };

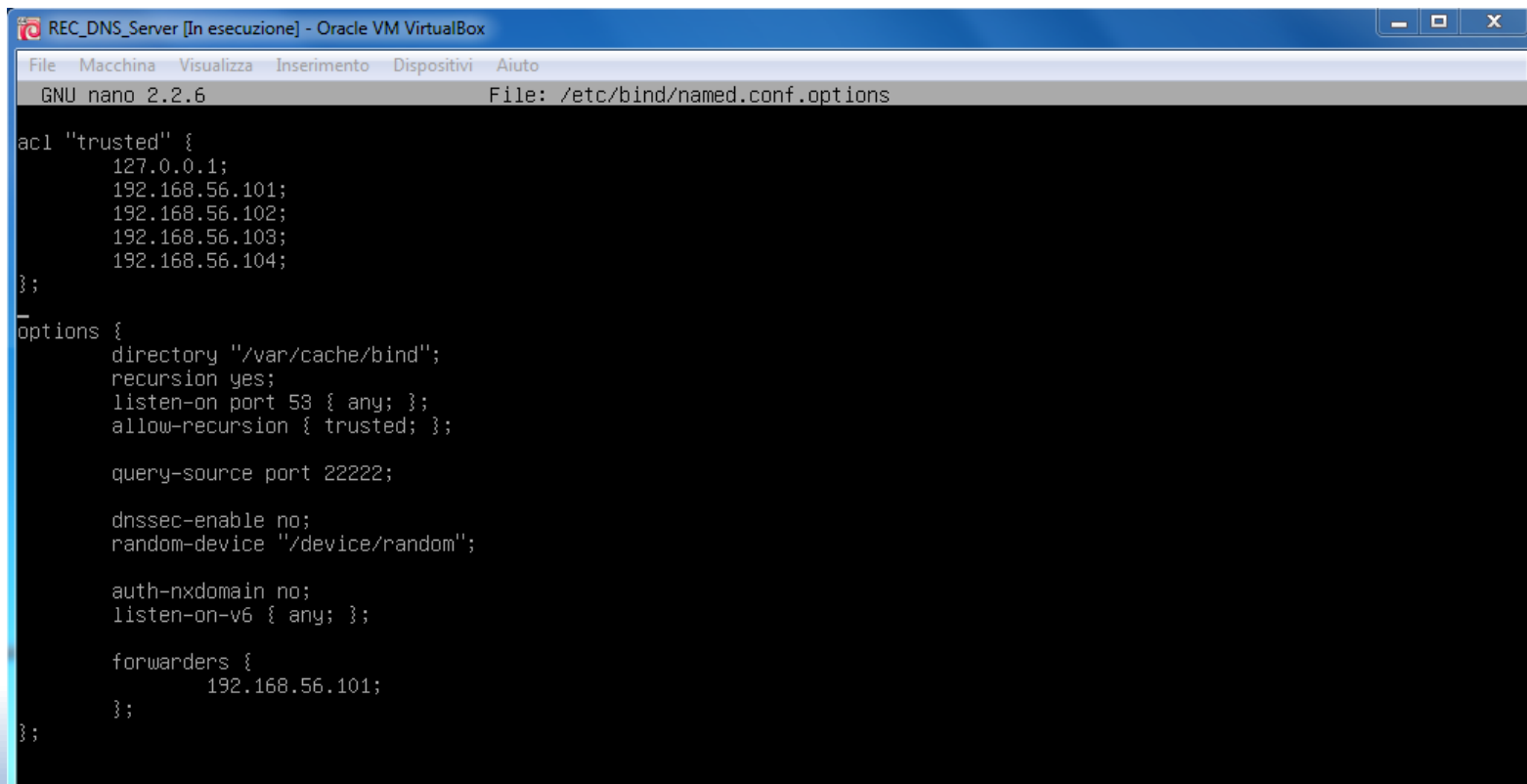
    dnssec-enable no;

    auth-nxdomain no;    # conform to RFC1035
    listen-on-v6 { any; };
};
```


Environment setup

On the REC_DNS_Server machine type:

> nano /etc/bind/named.conf.options



```
REC_DNS_Server [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.2.6                               File: /etc/bind/named.conf.options

acl "trusted" {
    127.0.0.1;
    192.168.56.101;
    192.168.56.102;
    192.168.56.103;
    192.168.56.104;
};

options {
    directory "/var/cache/bind";
    recursion yes;
    listen-on port 53 { any; };
    allow-recursion { trusted; };

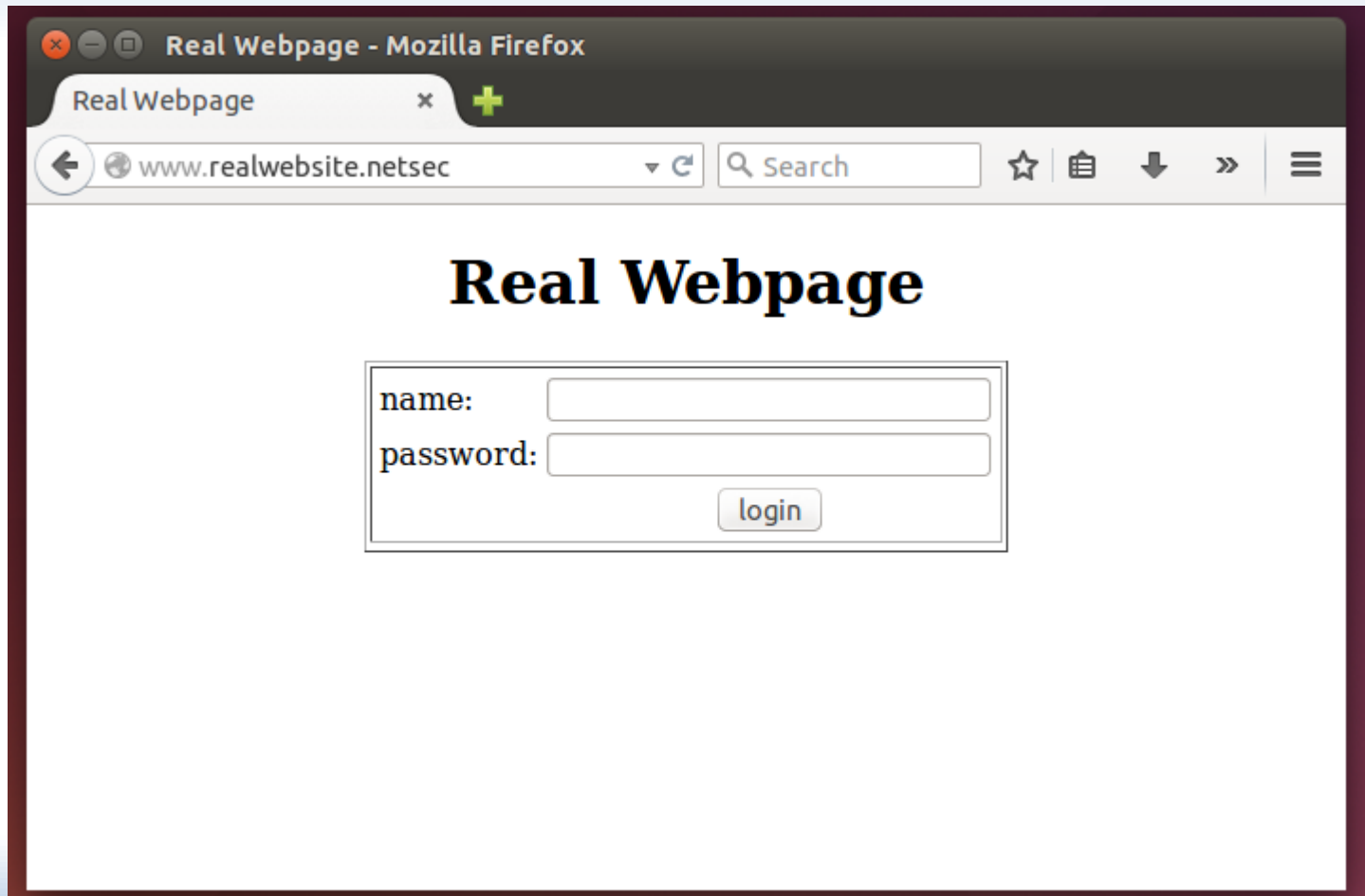
    query-source port 22222;

    dnssec-enable no;
    random-device "/dev/random";

    auth-nxdomain no;
    listen-on-v6 { any; };

    forwarders {
        192.168.56.101;
    };
};
```

Environment setup



About the DNS Cache

on the REC_DNS_Server:

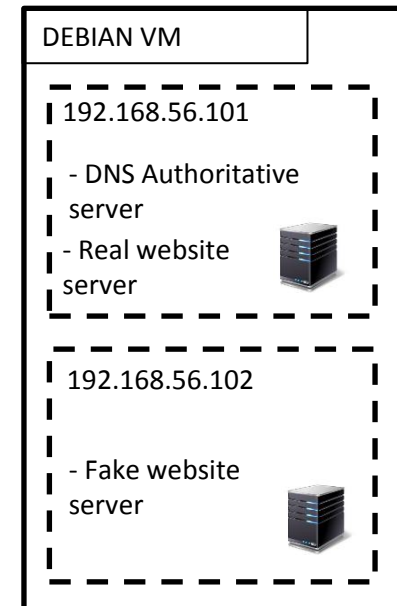
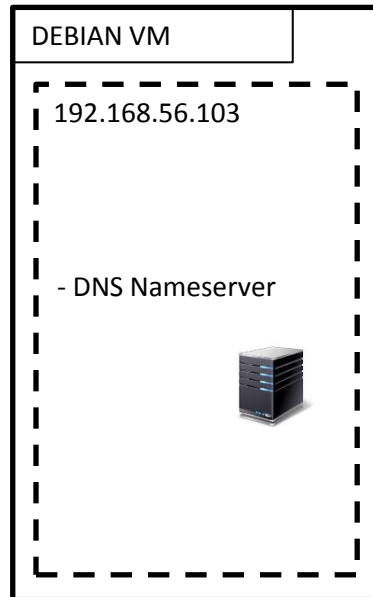
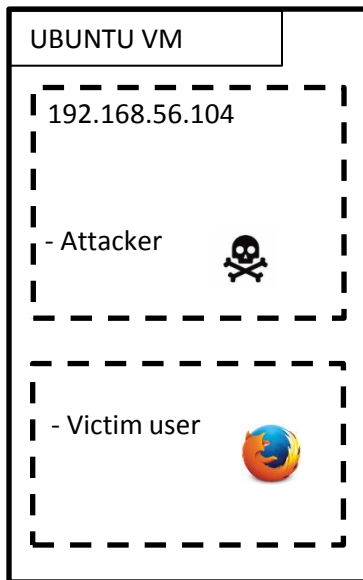
- In order to visualize the actual cache,
 - > `rndc dumpdb -cache`
 - > `nano /var/cache/bind/named_dump.db`
- In order to flush the cache:
 - > `rndc flush`

Step 1 - Attack

Birthday Attack:

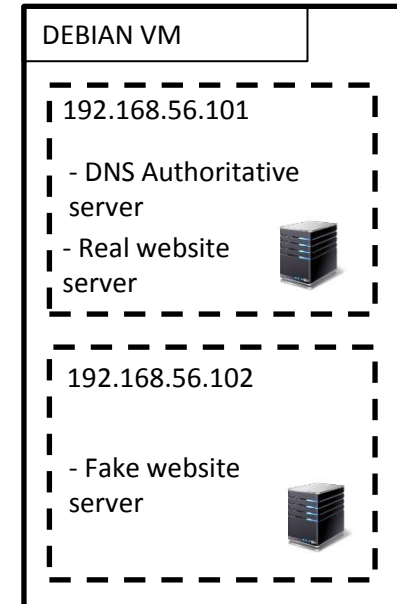
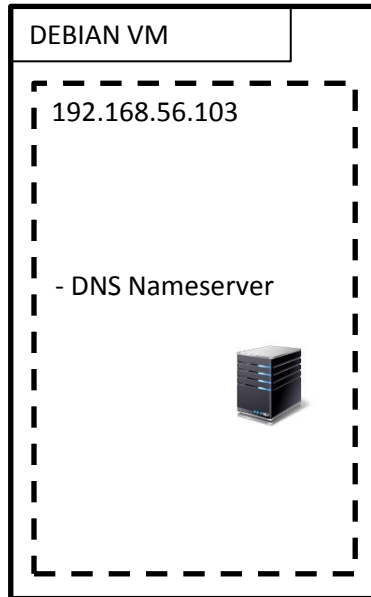
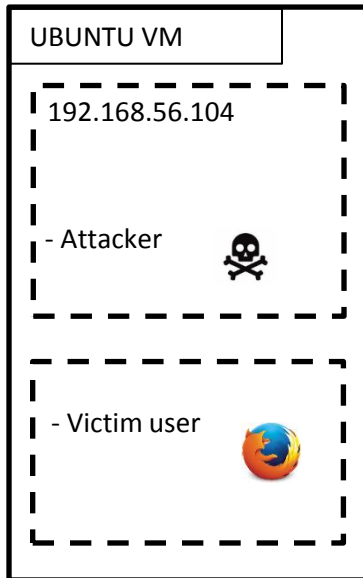
- Continuously generate DNS requests and DNS answers with random Transaction IDs
- The attack exploits the mathematics behind the 'birthday paradox'

Step 1 - Attack



Step 1 - Attack

DNS REQUEST
www.realwebsite.netsec



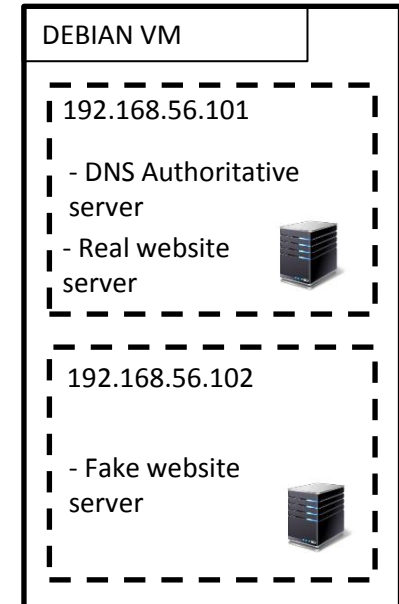
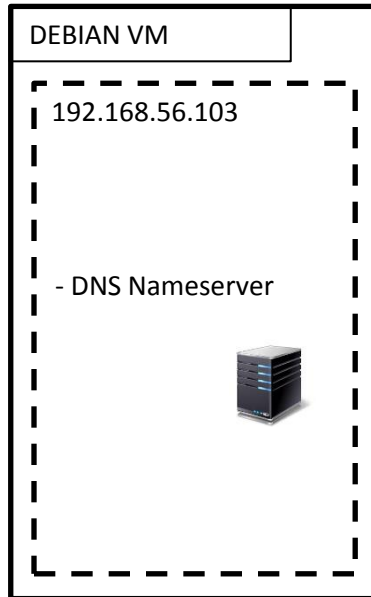
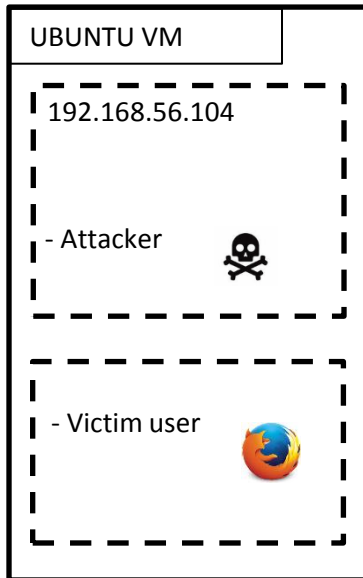
Step 1 - Attack

DNS REQUEST
www.realwebsite.netsec

DNS REQUEST
www.realwebsite.netsec

N

N



Step 1 - Attack

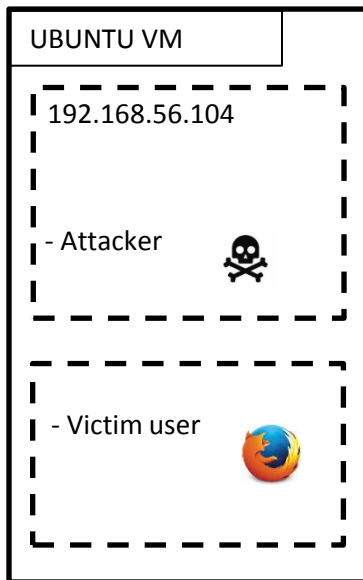
DNS REQUEST
www.realwebsite.netsec

DNS REQUEST
www.realwebsite.netsec

N

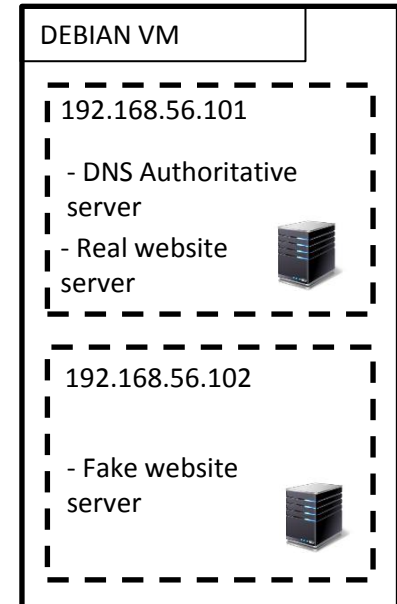
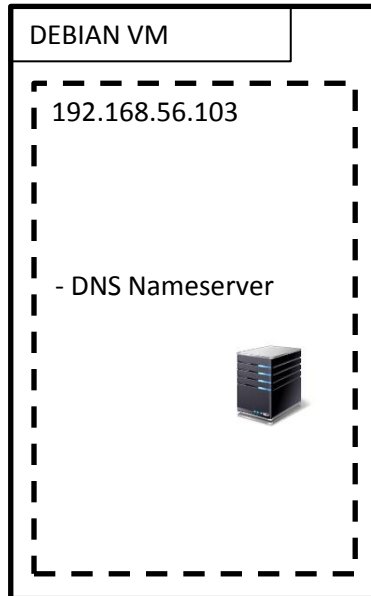
N

Denial Of Service Attack

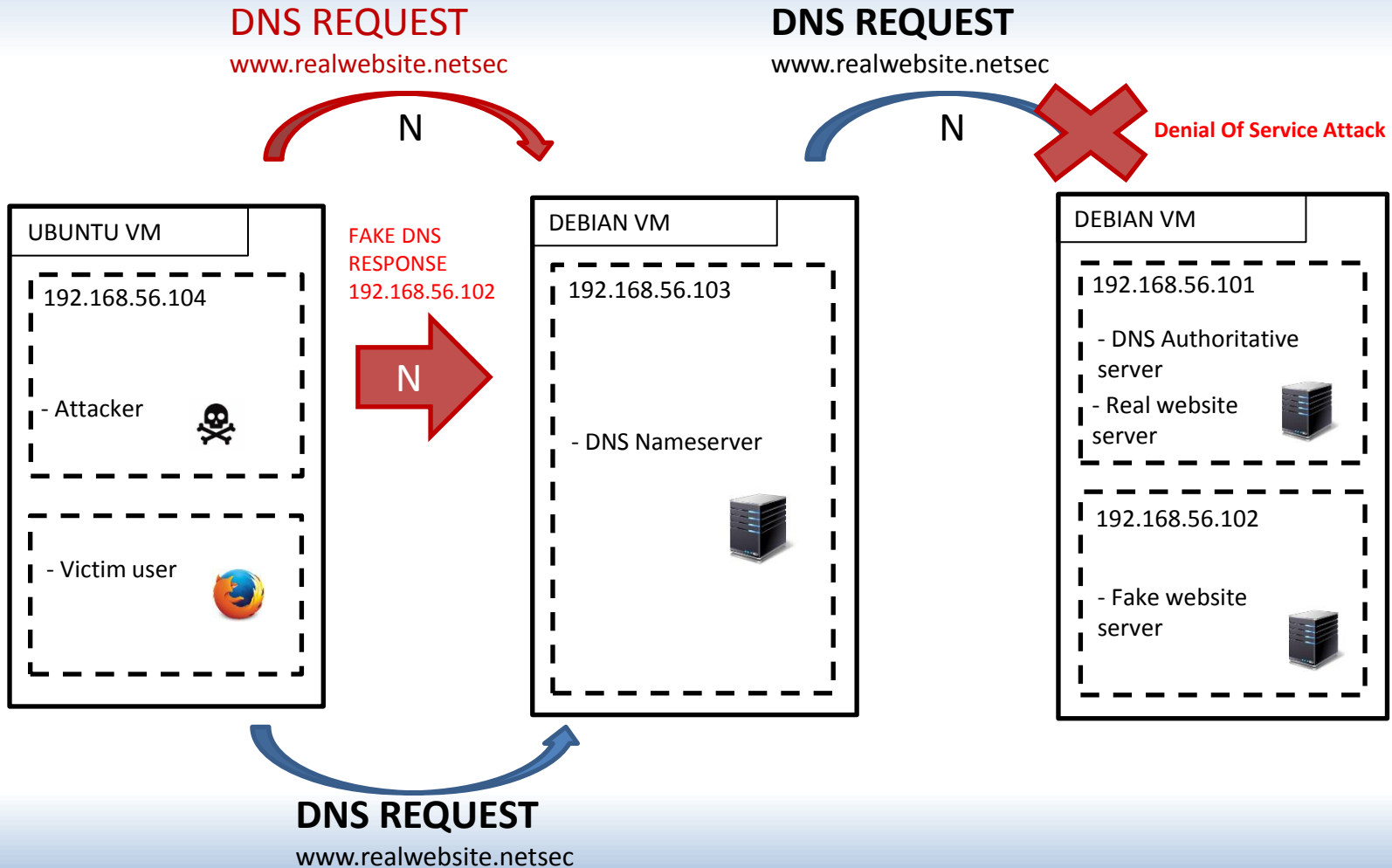


FAKE DNS
RESPONSE
192.168.56.102

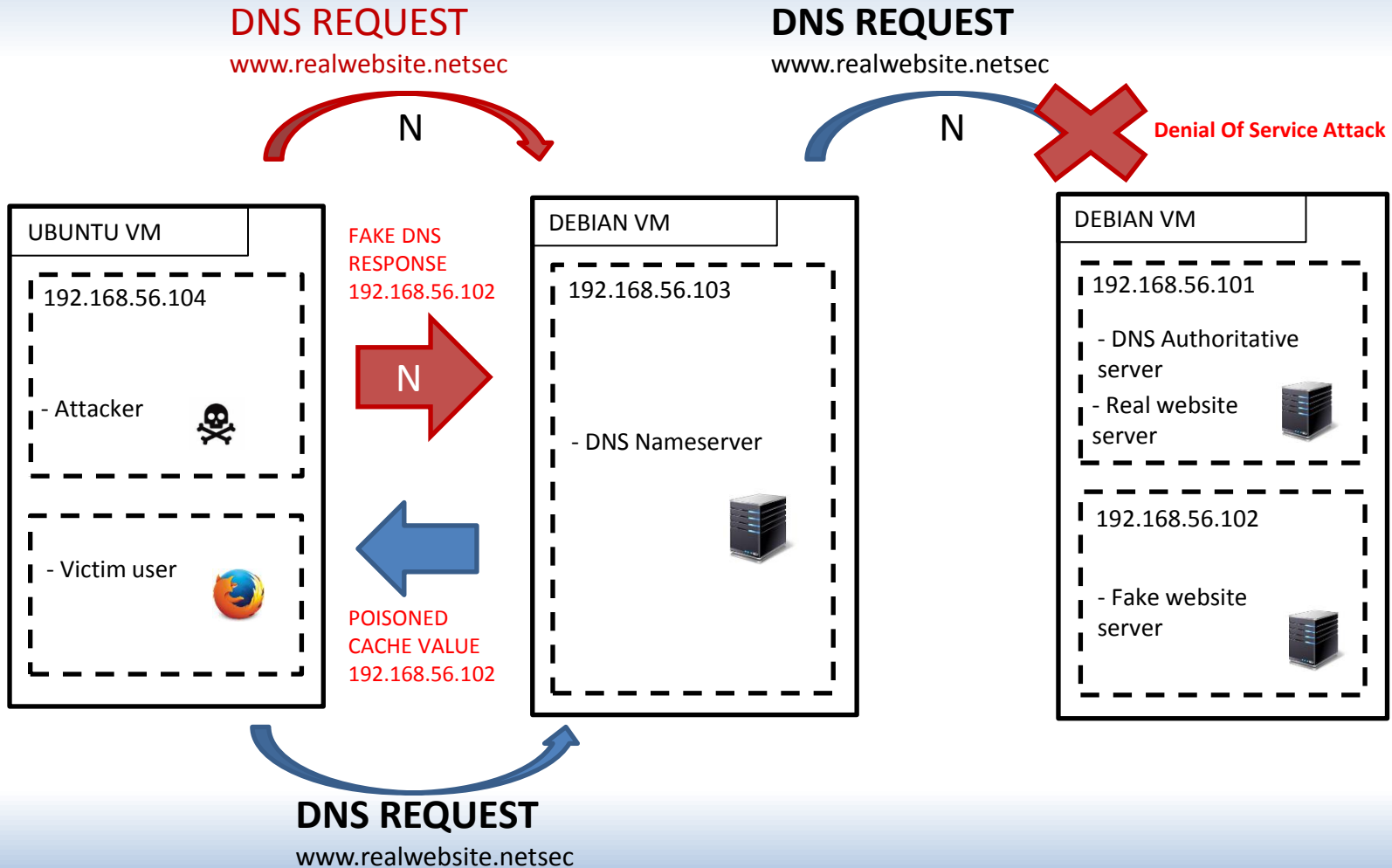
N



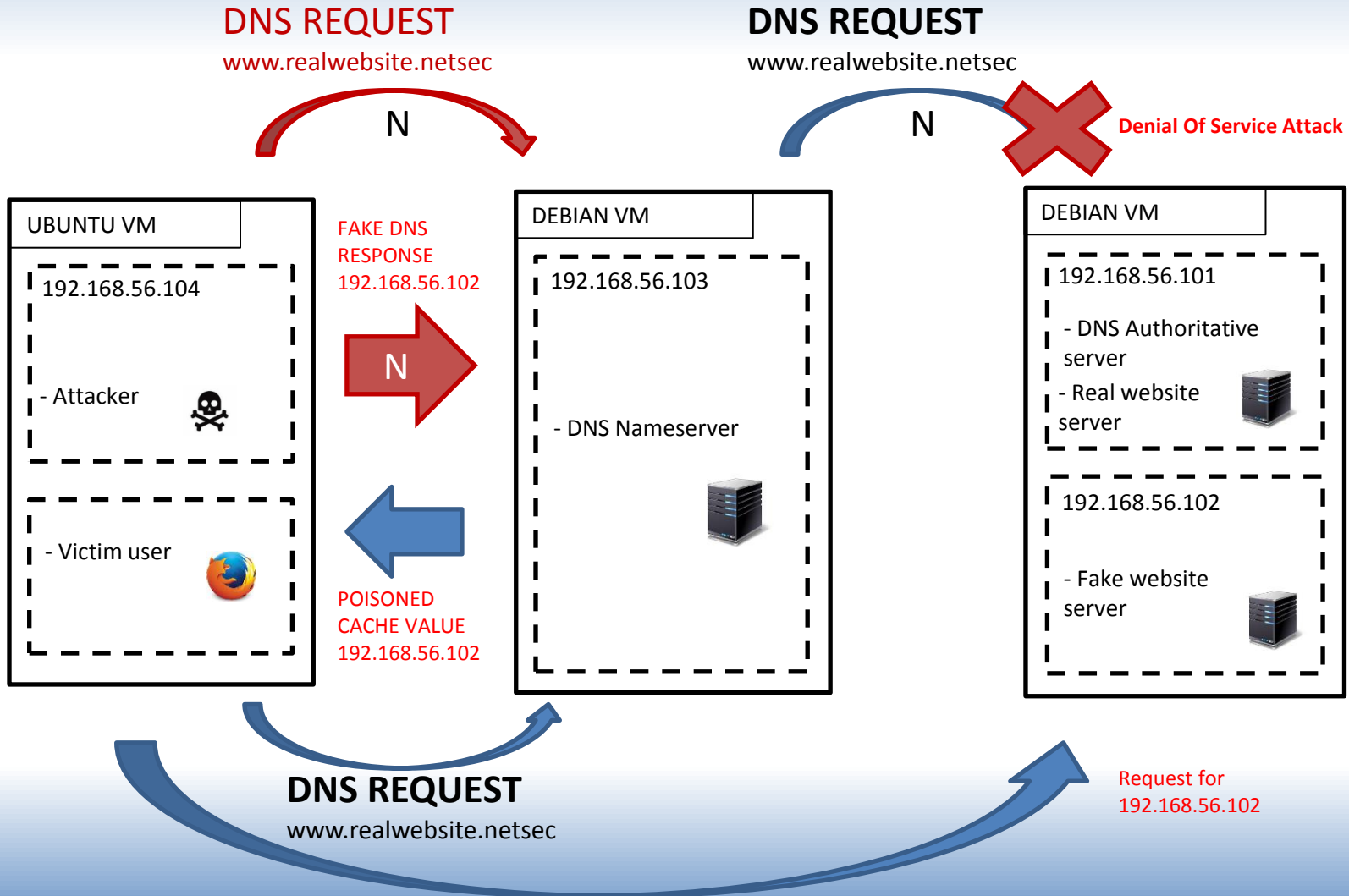
Step 1 - Attack



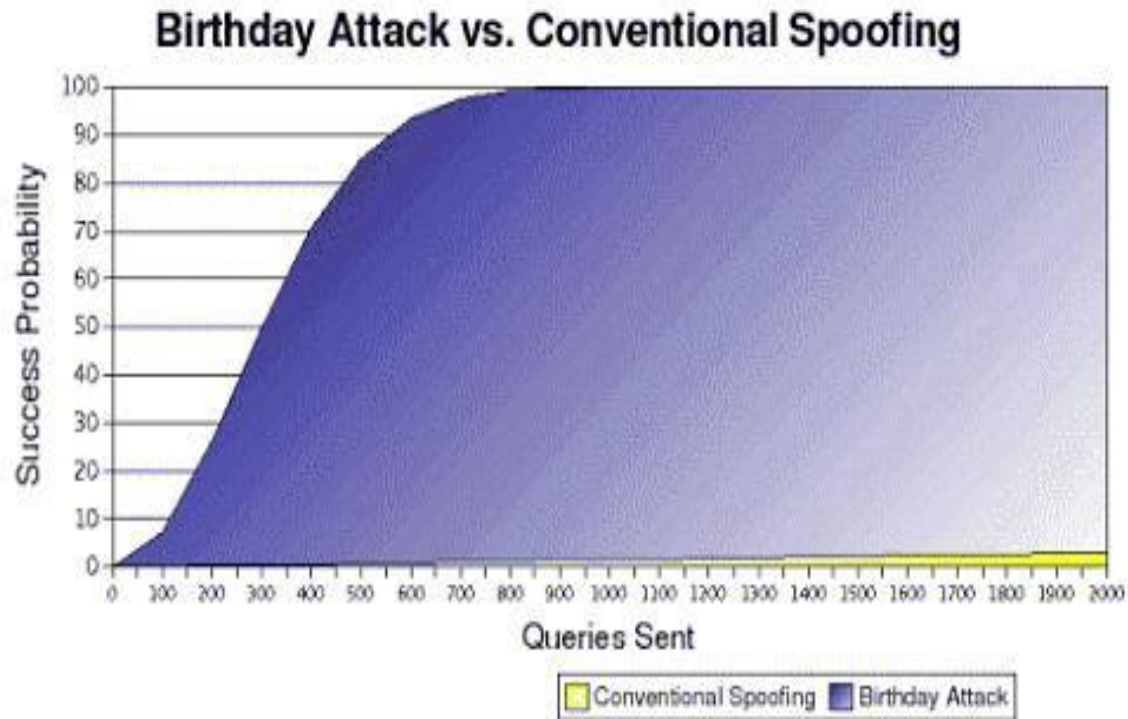
Step 1 - Attack



Step 1 - Attack



Step 1 - Attack



Step 1 - Attack

Now we have to perform a DoS attack,
but for this time we will cheat a bit...

Firewall

Block a specific IP address:

```
> iptables -A INPUT -s 192.168.56.103 -j DROP
```

Remove the block on that address:

```
> iptables -D INPUT -s 192.168.56.103 -j DROP
```

Show actual rules:

```
> iptables -L
```

Firewall

Now, if you send a ping from the REC_DNS_Server to the AUT_DNS_Server, you should receive no answer...

On the REC_DNS_Server type:

```
> ping 192.168.56.101
```

And check that nothing is displayed after the following

```
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
```

Step 1 - Attack

Birthday Attack:

Open the Ubuntu Console and run the following script:

```
> gedit /home/user/Desktop/birthday_attack.py
```


Step 1 - Attack

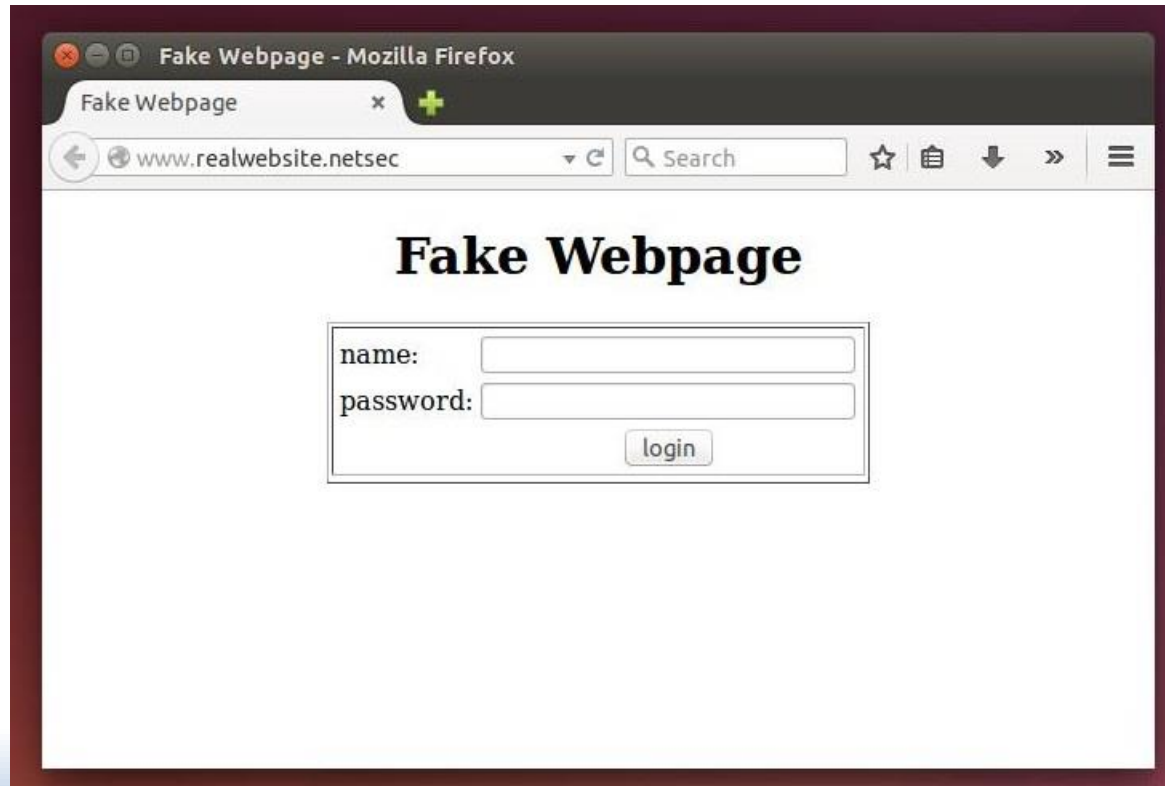
Birthday Attack:

Open the Ubuntu Console and run the following script:

```
> sudo python /home/user/Desktop/birthday_attack.py
```

Step 1 - Attack

If it works, you should see something like this...



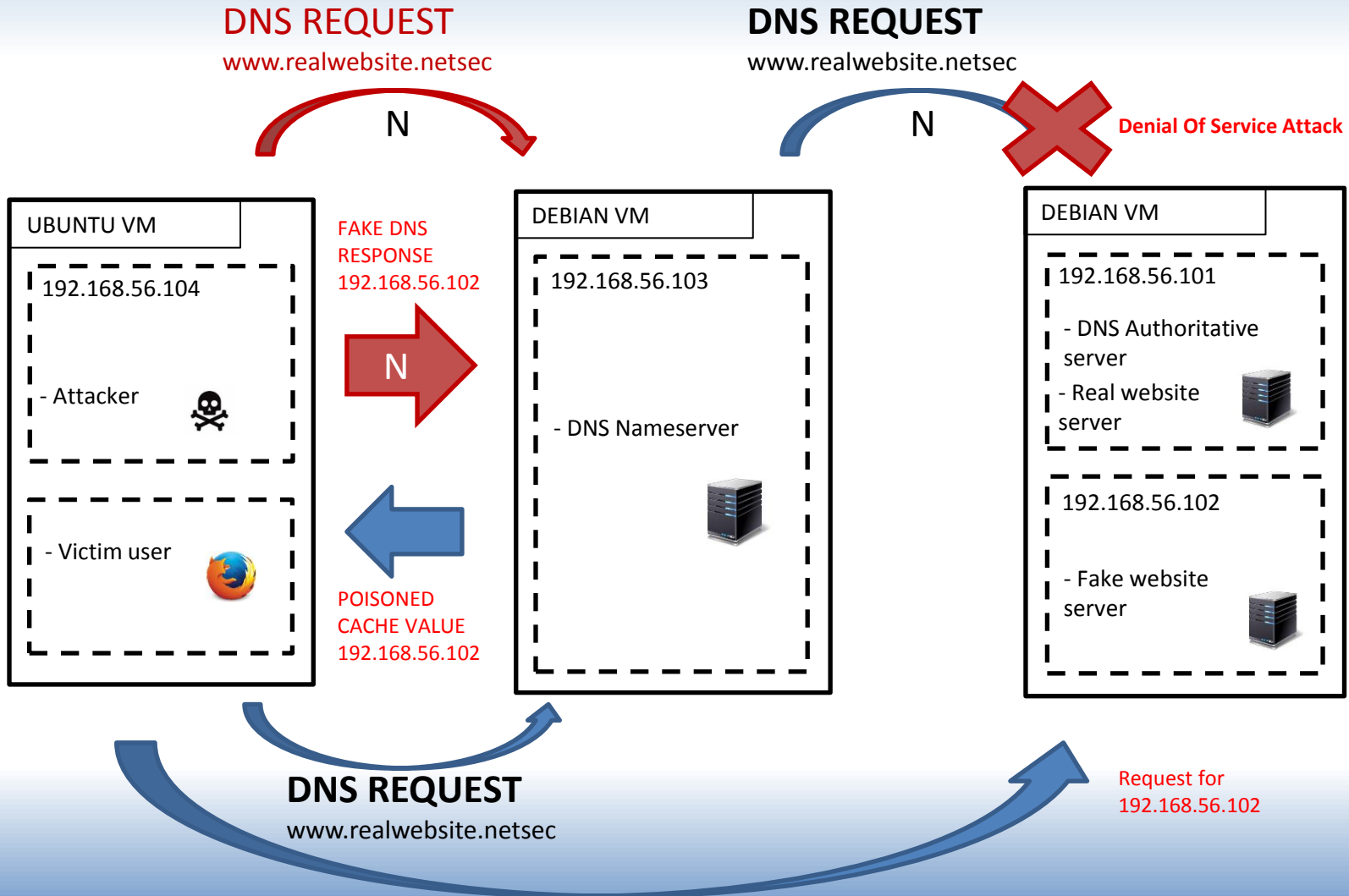
Step 1 - Attack

...well, actually... it doesn't...

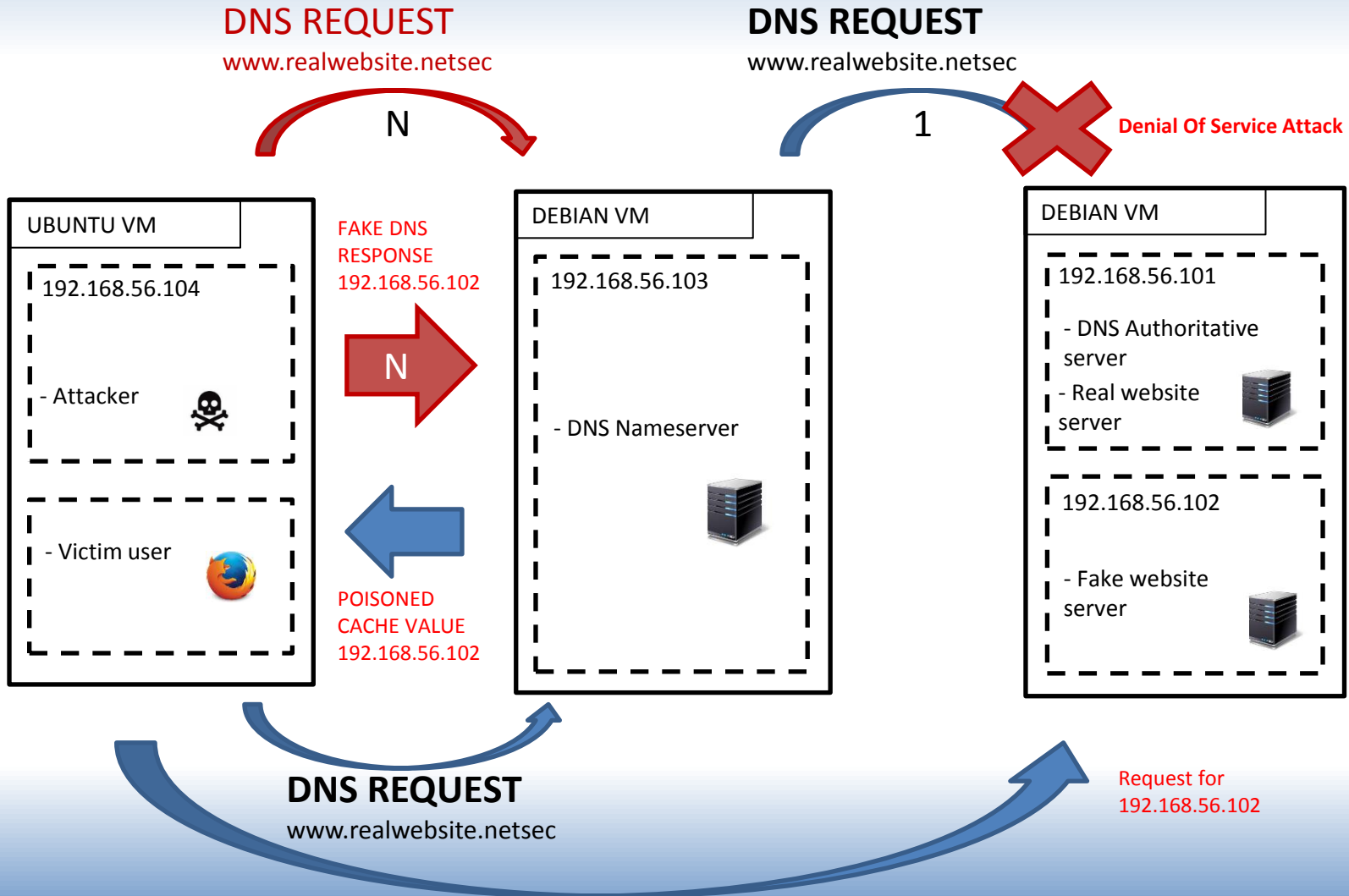
Step 2 - Defense

- The previous attack exploit a vulnerability that used to be present in bind4, but we are using bind9 instead...
- The birthday attack has become useless since even if the DNS recursive receives more than one request, it forwards only one of them, which times out after few seconds.
- However, with a fast enough algorithm, this defense could be broken.

Step 2 – Defense



Step 2 – Defense



Step 2 - Defense

- A system's defense can easily be hardened by introducing Port randomization.
- On the REC_DNS_Server type:
 - > nano /etc/bind/named.conf.options
- Then, remove or comment 'query-source port 22222;' and check that random-device is set to "/device/random";

Step 2 - Defense

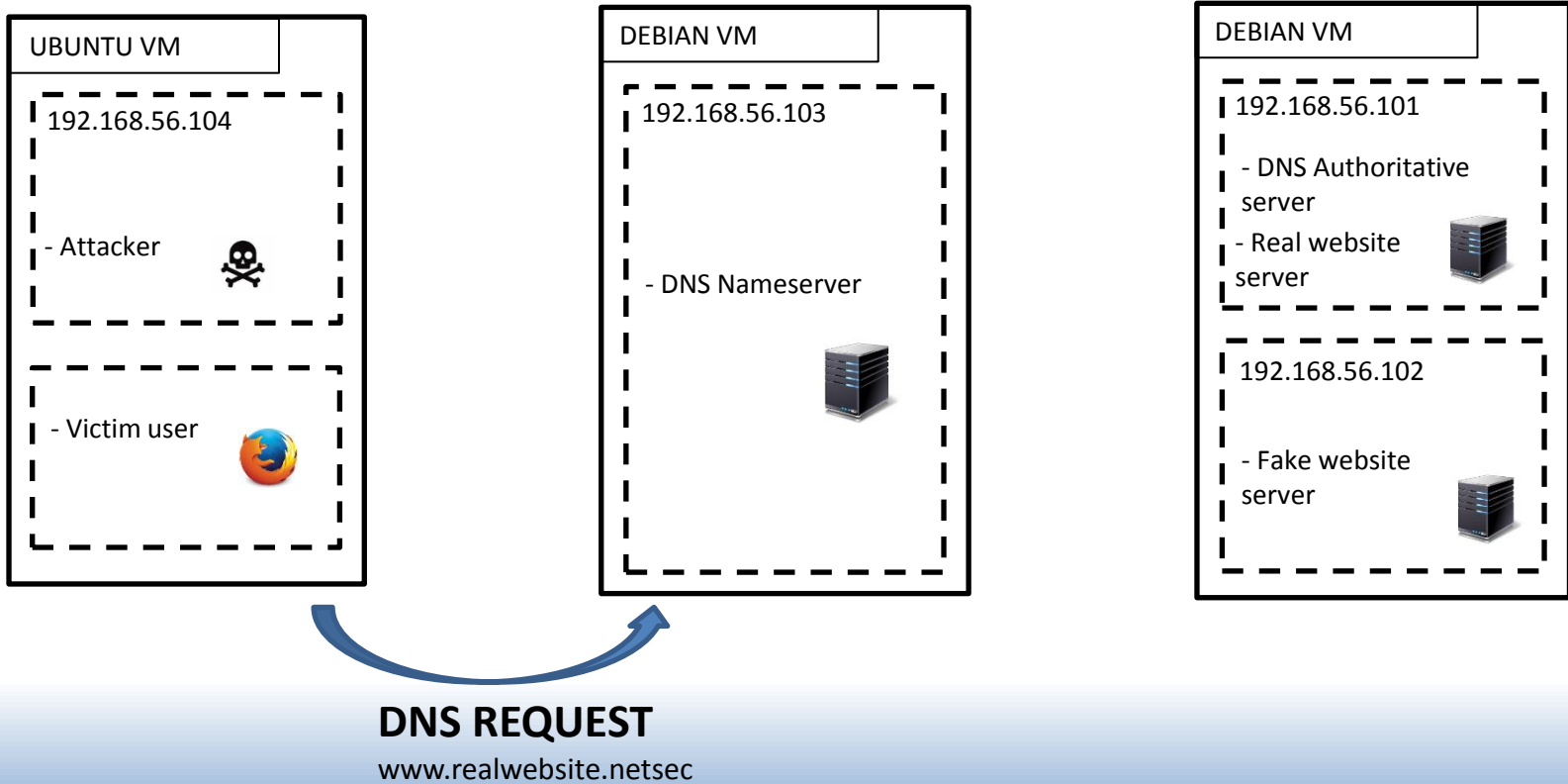
- Reproducing such an attack would be much harder, if not impossible, even with a very powerful algorithm.

Step 3 - Attack

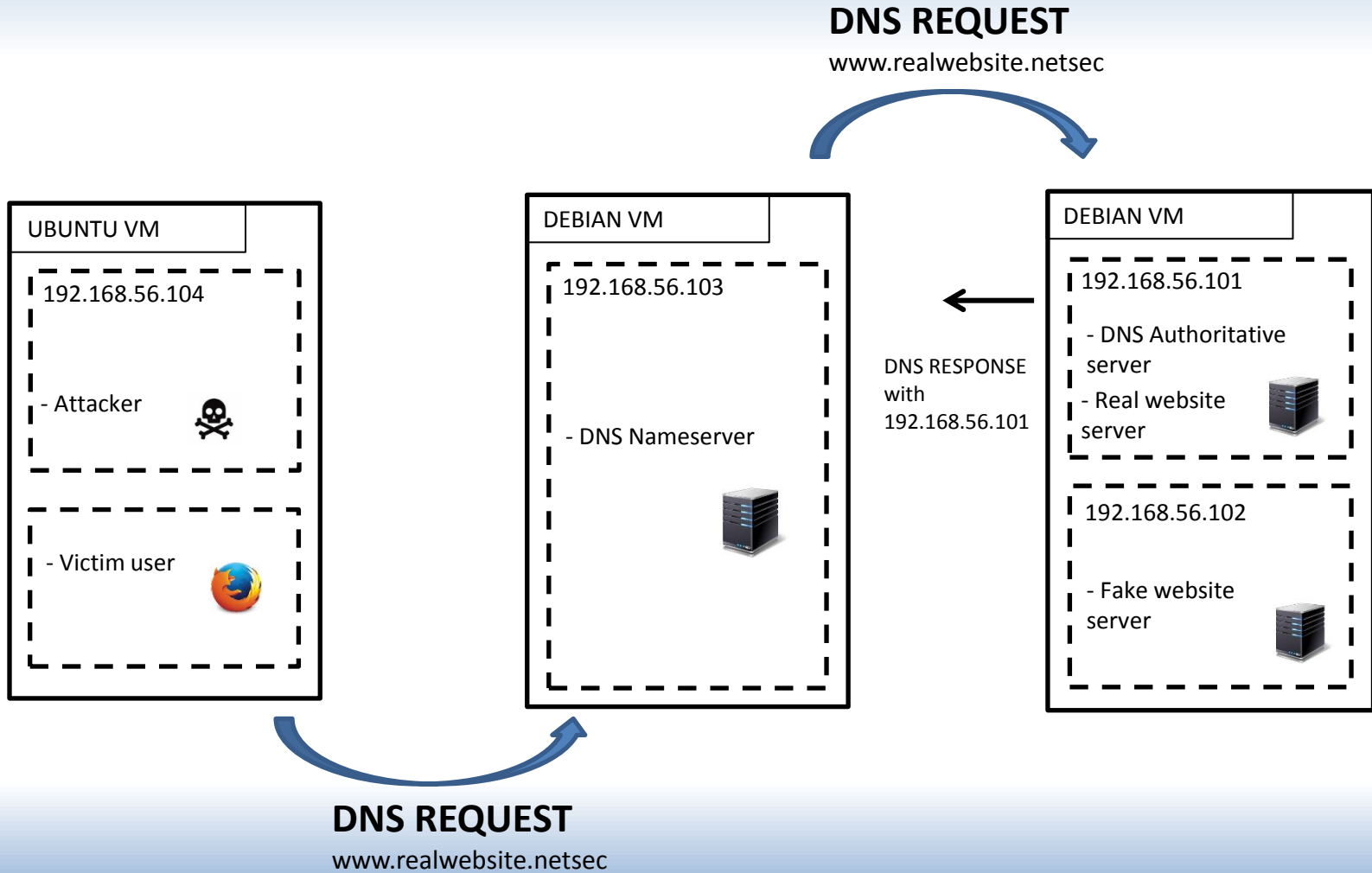
Packet Sniffing

In the case the attacker has access to the DNS's physical network (or he has performed a Man In The Middle attack), he could be able to sniff the packets, answering to the DNS Queries while acting like the Authoritative DNS.

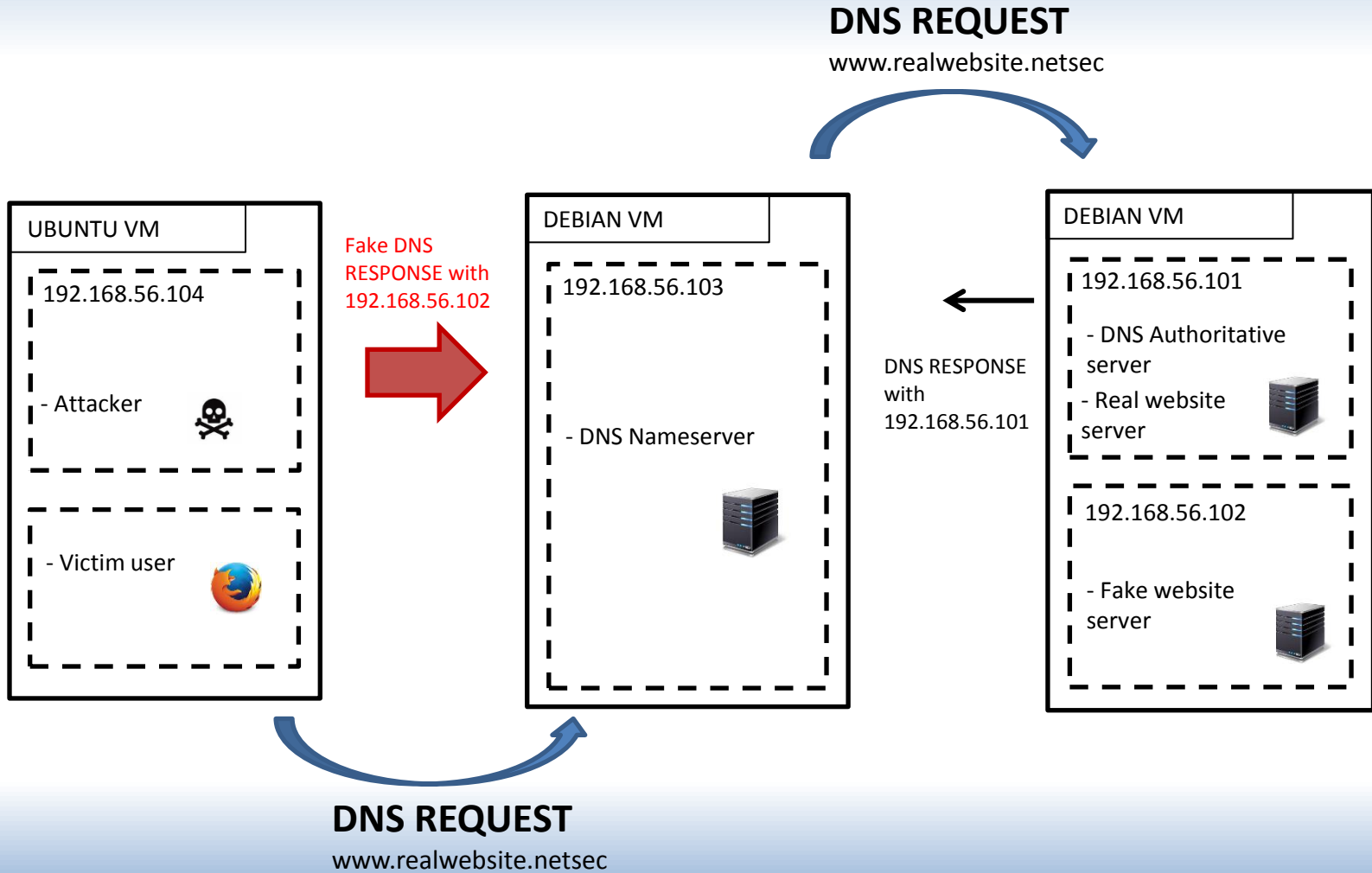
Step 3 - Attack



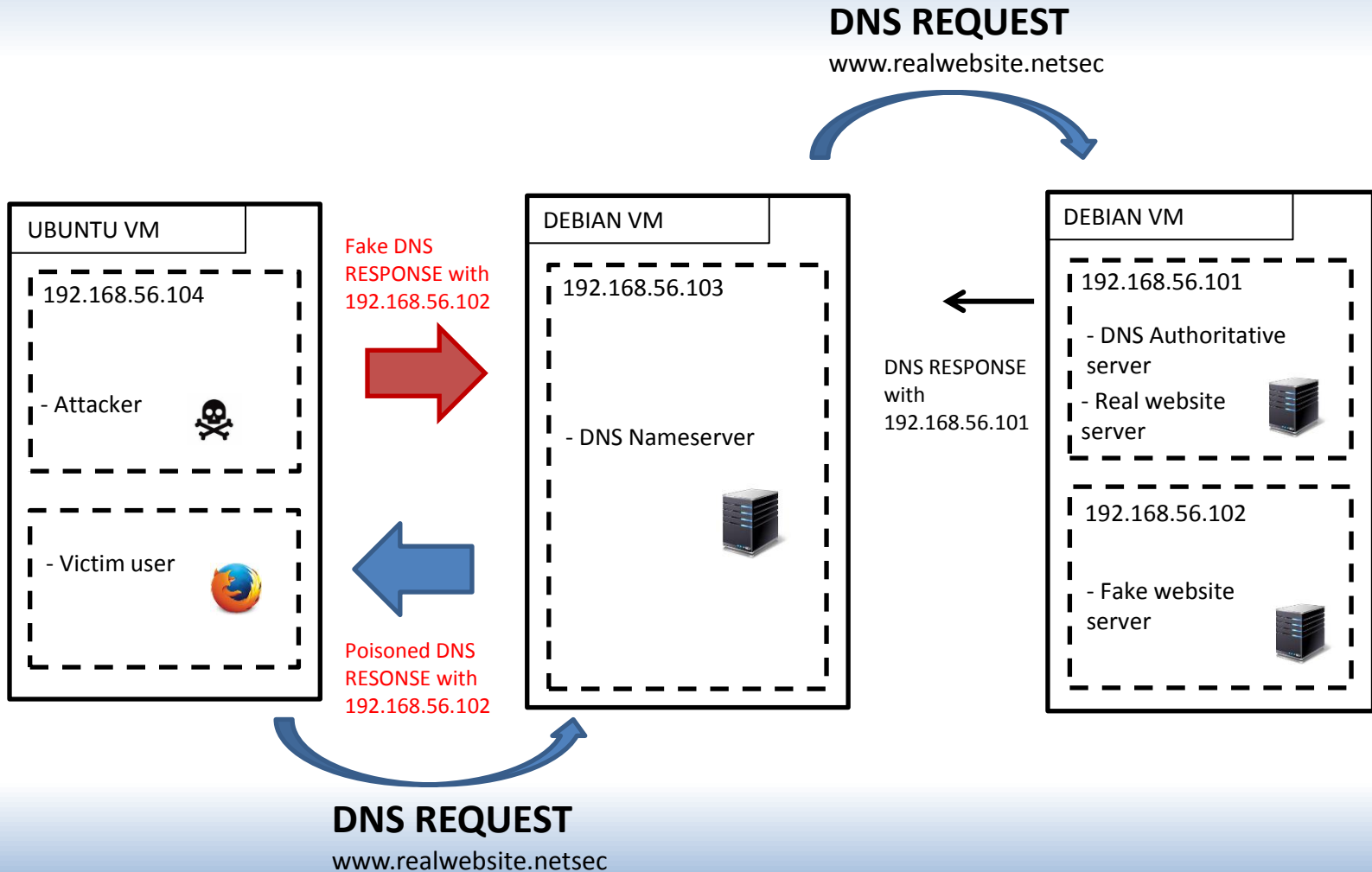
Step 3 - Attack



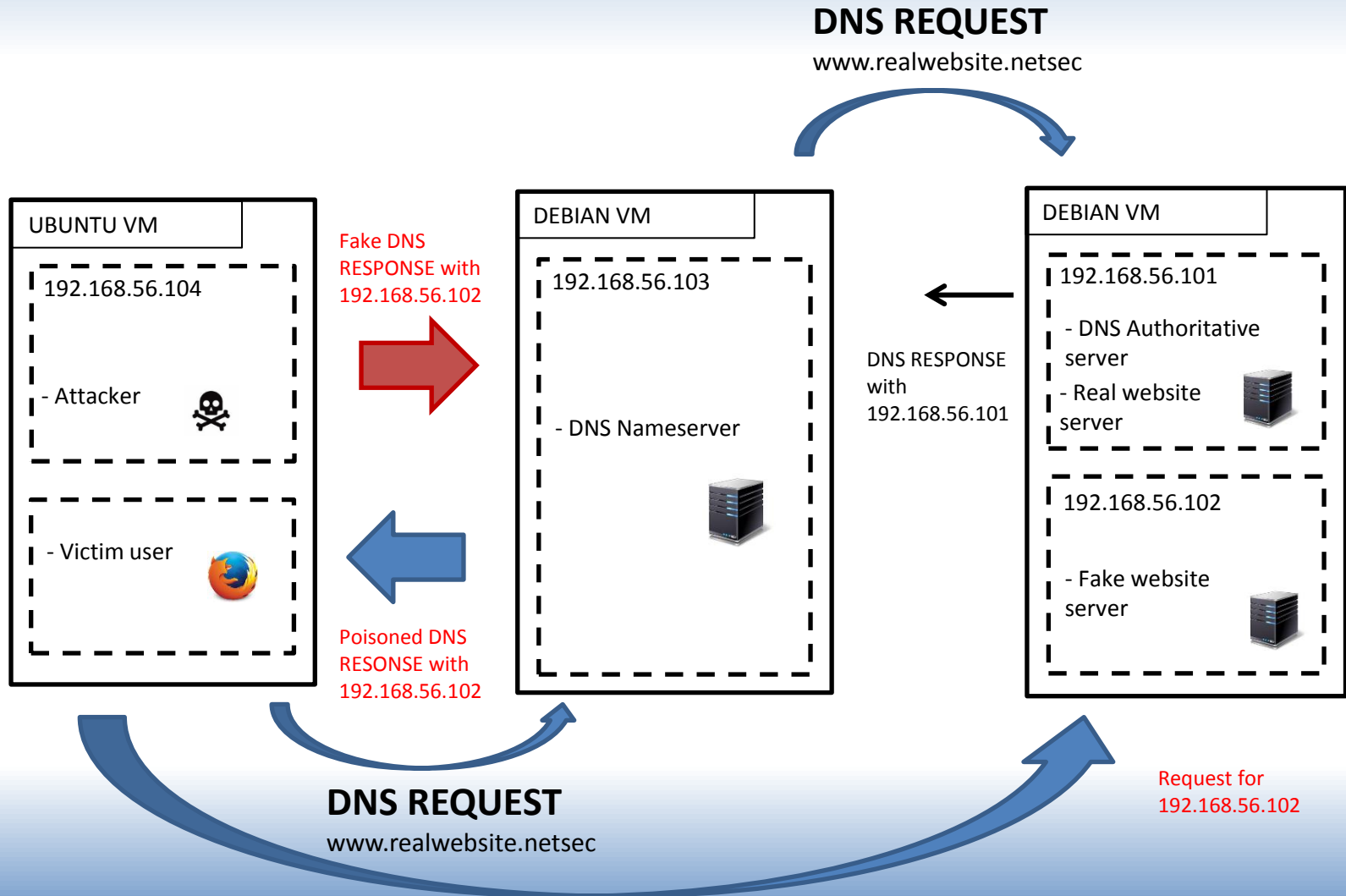
Step 3 - Attack



Step 3 - Attack



Step 3 - Attack



Step 3 - Attack

On the Ubuntu machine, open 2 terminals.

- In the first one, type

 - > `sudo python /home/user/Desktop/sniffing_attack.py`

- In the second one, type

 - > `ping www.realwebsite.netsec`

If the attack went well, when you open the browser and look for 'www.realwebsite.netsec' you should be redirected to the fake website.