Emma Stensland

Reese Pearsall

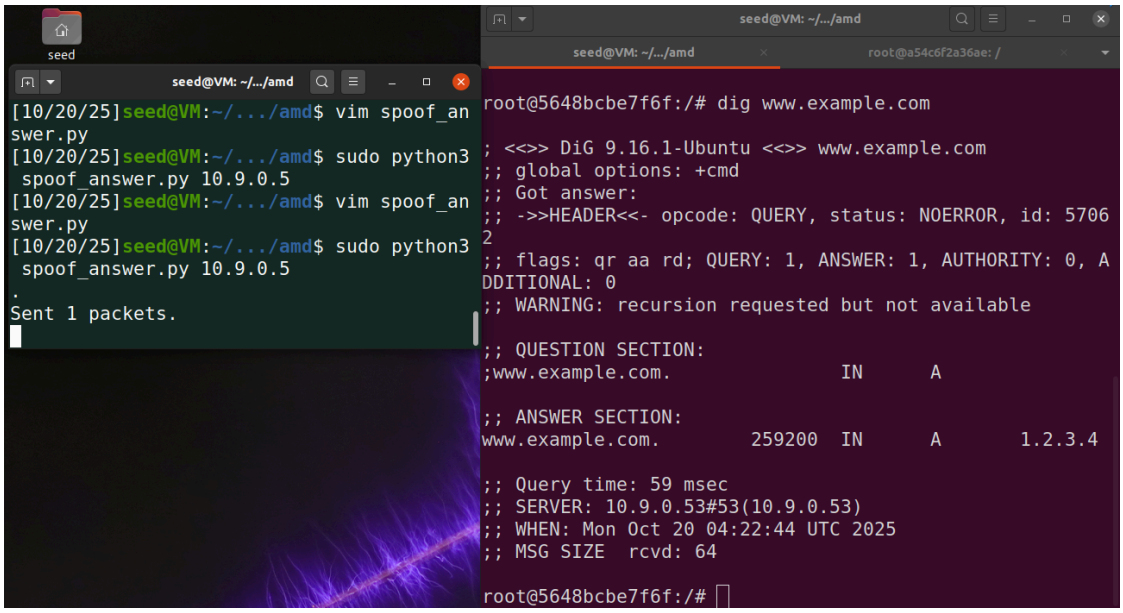
CSCI 476

October 26, 2025

Seedlabs: Local DNS Cache Poisoning

Task 1: Spoofing DNS Responses to the user

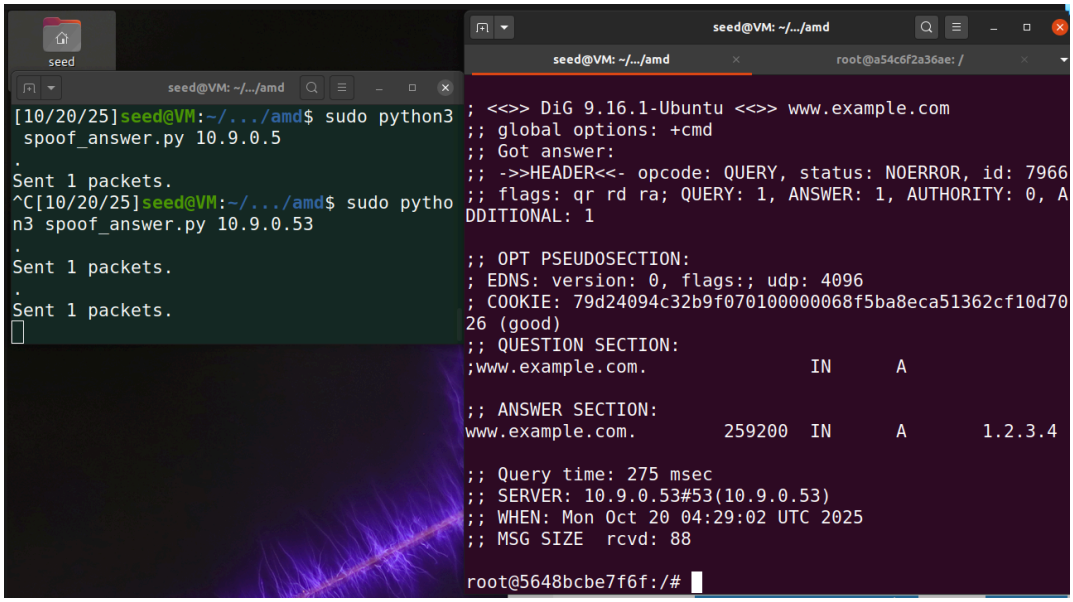
Python code sniffed on the network where DNS requests and responses were happening, and spoofed a DNS packet with the attacker's desired IP.

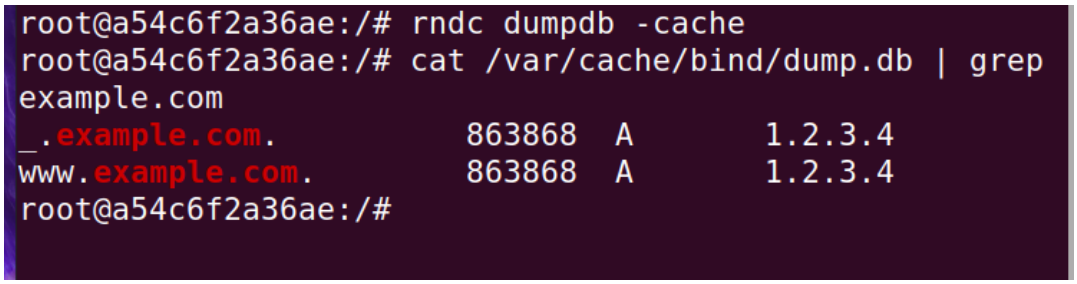


Observations: The attack was sucessful, and the the victim will go to the malicious IP address instead of the actual IP address.

Task 2: Spoofing DNS Responses to the Local DNS Server

Python code sniffed on the network where DNS requests and responses were happening, and spoofed a DNS packet from the Global DNS server to the Local DNS server.

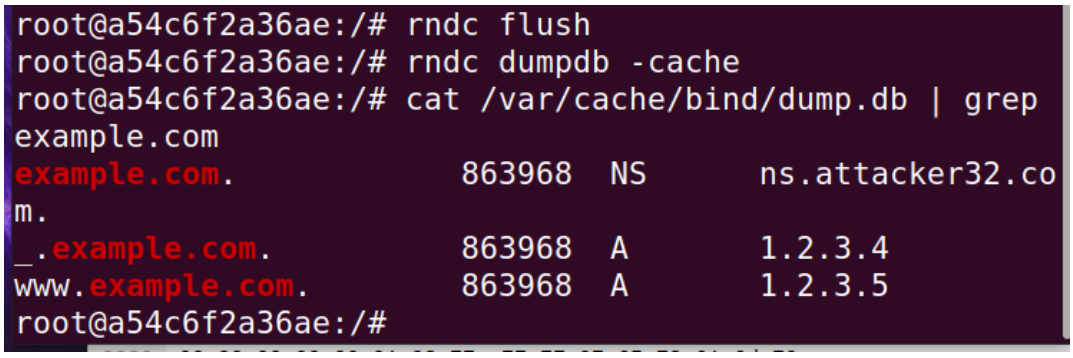




Observations: The attack was successful, and now the DNS server cached the attacker's website, so each time the victim tries to access the website it goes to the attacker's IP.

Task 3: Spoofing NS Records

A packet was spoofed via the python code with a section added with the authority being the attacker's NS.



Observations: The attack was sucessful, and the NS for any example.com was set to the attacker's.

Task 4: Experimenting with /etc/hosts

The file /etc/hosts was updated so have the Local DNS set an IP for a website.

```
# For Shellshock Lab
10.9.0.80       www.seedlab-shellshock.com

# Temp For DNS Lab
9.9.9.9 www.csci476.com
[10/20/25]seed@VM:~/.../amd$ dig www.csci476.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.csci476.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31319
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.csci476.com.               IN      A

;; ANSWER SECTION:
www.csci476.com.        0       IN      A       9.9.9.9

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Oct 20 00:44:15 EDT 2025
;; MSG SIZE  rcvd: 60

[10/20/25]seed@VM:~/.../amd$
```

Observations: /etc/hosts was successful in making the website resolve to the selected IP.