

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.

```
[10/20/25]seed@VM:~/.../amd$ vim spoof_answer.py
[10/20/25]seed@VM:~/.../amd$ sudo python3 spoof_answer.py 10.9.0.5
[10/20/25]seed@VM:~/.../amd$ vim spoof_answer.py
[10/20/25]seed@VM:~/.../amd$ sudo python3 spoof_answer.py 10.9.0.5
.
Sent 1 packets.

root@5648bcbe7f6f:/# dig www.example.com

; <>> DiG 9.16.1-Ubuntu <>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 5706
2
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available
;;
;; QUESTION SECTION:
;www.example.com.           IN      A
;;
;; ANSWER SECTION:
www.example.com.      259200  IN      A      1.2.3.4
;;
;; Query time: 59 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Oct 20 04:22:44 UTC 2025
;; MSG SIZE  rcvd: 64

root@5648bcbe7f6f:/#
```

Observations: The attack was successful, and 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.

The screenshot shows two terminal windows. The left window, titled 'seed@VM: ~.../amd', runs the command `sudo python3 spoof_answer.py 10.9.0.5`. It outputs: 'Sent 1 packets.' followed by a carriage return. The right window, titled 'seed@VM: ~.../amd' and 'root@a54c6f2a36ae:/', shows the result of a `DIG` query to `www.example.com`. The output includes the question section, the answer section (IP 1.2.3.4), and the header information.

```
[10/20/25]seed@VM:~/.../amd$ sudo python3
spoof_answer.py 10.9.0.5
.
Sent 1 packets.
^C[10/20/25]seed@VM:~/.../amd$ sudo python3
spoof_answer.py 10.9.0.53
.
Sent 1 packets.
.
Sent 1 packets.
[10/20/25]seed@VM:~/.../amd$ dig www.example.com
; <>> DiG 9.16.1-Ubuntu <>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7966
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 79d24094c32b9f070100000068f5ba8eca51362cf10d70
26 (good)
;; QUESTION SECTION:
;www.example.com. IN A
;; ANSWER SECTION:
www.example.com. 259200 IN A 1.2.3.4
;; Query time: 275 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Oct 20 04:29:02 UTC 2025
;; MSG SIZE rcvd: 88
root@5648bcbe7f6f:/#
```

```
root@a54c6f2a36ae:/# rndc dumpdb -cache
root@a54c6f2a36ae:/# cat /var/cache/bind/dump.db | grep
example.com
_.example.com.          863868  A      1.2.3.4
www.example.com.        863868  A      1.2.3.4
root@a54c6f2a36ae:/#
```

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.

```
root@a54c6f2a36ae:/# rndc flush
root@a54c6f2a36ae:/# rndc dumpdb -cache
root@a54c6f2a36ae:/# cat /var/cache/bind/dump.db | grep
example.com
example.com.          863968  NS    ns.attacker32.co
m.
_.example.com.        863968  A      1.2.3.4
www.example.com.      863968  A      1.2.3.5
root@a54c6f2a36ae:/#
```

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.