**NETWORK SECURITY   
Project 4**

DNS Packet Injection

*Submitted to: Submitted by:*

*Michalis Polychronakis Mahima Parashar (111463071)*

Design:

1. The DNS detect captures the packets from a network interface in promiscuous mode and injects the forged responses to selected DNS A request with the goal to poison the resolver’s cache.
2. The file dnsinject.c contains three functions described as follows:

* main(): This function is the starting point of dnsinject.c file, which captures the packet received from the interface.
* readFile(): This file reads the hostname file.
* packetHandler(): It is a callback function of the dnsinject that is activated whenever it receives a packet. This function checks if the incoming packet is a UDP packet with destination port as 53 and is type A. Finally, it injects a response to a query before the actual response.

1. The file dnsdetect.py majorly contains two functions described as follows:

* main(): It is the starting point of dnsdetect.py file, which parses the command line arguments and captures packets which in turn are given to the dns\_detect() function.
* dns\_detect(): This function detects DNS poising attack attemps like those generated by dnsinject. It is based on identifying duplicate responses towards the same destination that contain different answers for the same A request.

Files

1. MakeFile
2. hostnames.txt
3. dnsinject.c
4. dnsdetect.py
5. tracefile

Execution Steps:

1. make
2. For dnsinject:

gcc dnsinject.c -o dnsinject -lpcap -lnet -lresolv

1. For client:

sudo python dnsdetect.py [-i interface][-r test\_trace]

False Positives

The two legitimate consecutive responses with different IP addresses for the same hostname has been ignored because they will have the same TTL.

Working Examples:

1. For dnsdetect:

sudo python dnsdetect.py -r test\_trace

Password:

Sniffing from the tracefile

[20171209-05:54:08.013033] DNS poisoning attempt detected

TXID 9035 Request URL paypal.com

Answer1 [64.4.250.33]

Answer2 [10.6.7.8]

[20171209-05:54:08.018391] DNS poisoning attempt detected

TXID 6309 Request URL www.paypal.com

Answer1 [127.0.0.1]

Answer2 [geo.paypal.com.akadns.net.]

1. For dnsinject:

Command in one terminal:

sudo ./dnsinject -h hostnames.txt

Password:

Device: en0

en0

Second terminal:

dig @77.88.8.8 yahoo.com

; <<>> DiG 9.9.7-P3 <<>> @77.88.8.8 yahoo.com

; (1 server found)

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19372

;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:

;yahoo.com. IN A

;; ANSWER SECTION:

yahoo.com. 4 IN A 172.24.30.131

;; Query time: 70 msec

;; SERVER: 77.88.8.8#53(77.88.8.8)

;; WHEN: Sat Dec 09 05:58:35 EST 2017

;; MSG SIZE  rcvd: 43

Working Environment:

OS Version: Mac OS Sierra

Language: for dnsdetect-python(2.7)

for dnsinject – c

References:

* <https://stackoverflow.com/questions/2283494/get-ip-address-of-an-interface-on-linux>
* <http://libnet.sourceforge.net/libnet.html>
* <https://scapy.readthedocs.io/en/latest/>
* <https://linux.die.net/man/3/dn_expand>