Hengyi Shi

CS528

Lab 2 Report

Machine set up table:

- Apollo IP :192.168.15.4 Port: 20000
- dns_usr :192.168.15.5 Port: 20001
- dns_attacker :192.168.15.6 port: 20002

Targeted domain name server for example.edu:

- Name-server 1 : 199.43.135.53

Lab Configuration:

I set the "dns_usr"'s default DNS server to be "Apollo" following the instruction since we need to verify the attack later. I also changed the source port number such that all DNS query requests would be sent via port 33333. This step is necessary otherwise the attack would have become harder since the DNS server choosing random ports in general. And I also disabled "dnssec" feature on "Apollo" based on lab instruction.

Attack Program:

The program "dns_attack.c" uses "gcc dns_attack.c -o dns_attack1" to compile and "sudo ./dns_attack 192.168.15.6 192.168.15.4" to run due to my machine set up. You can change the two IP parameter to any IP you want to satisfy the test environment.

The program I write is based on the provided code udp.c which was given on Piazza. I added a extra structure for authoritative section "NSRecord". I carefully construct UDP response and fill in data for each field. And use UDP destination port 33333. The transaction ID start from "3000" and I send 500 packets per domain name for attack. It will usually take 20-30 sec to make a successful attack. (See image below)

```
; authauthority
example.edu.        8185    NS  ns.dnslabattacker.net.
; additional
            86386   DS  44042 8 1 (
                    043A6301C88EB7D22305905C6B63331BD147
                    922A )
            86386   DS  44042 8 2 (
                    6F7520DCE4AB634085EF24C46D75343BF115
                    375B241C4BB8A8B5AF0C67964E13 )
```

The image above was taken from dump file shows the example.edu is successfully changed to ns.dnslabattacker.net

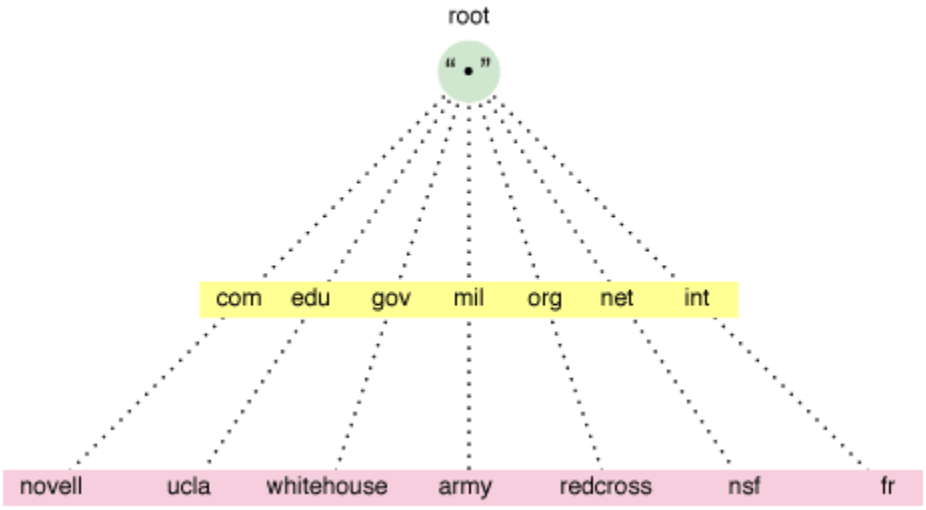
Verification:

As for verification, I simply followed lab instruction to make configuration changes. And here is the result snip.

```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57390
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; QUESTION SECTION:
;www.example.edu.               IN      A

;; ANSWER SECTION:
www.example.edu.        259200  IN      A       1.1.1.1

;; AUTHORITY SECTION:
example.edu.            135     IN      NS      ns.dnslabattacker.net.

;; ADDITIONAL SECTION:
ns.dnslabattacker.net.  604800  IN      A       192.168.15.6
ns.dnslabattacker.net.  604800  IN      AAAA    ::1

;; Query time: 9 msec
;; SERVER: 192.168.15.4#53(192.168.15.4)
;; WHEN: Fri Mar  1 11:51:08 2019
;; MSG SIZE  rcvd: 128
```

Question: Why is the IP address for ns.dnslabattacker.net mentioned in the additional records section of the spoofed DNS response not accepted by Apollo?

DNS hierarchy is a distributed tree structure. Each layer represents a different zone or domain. (See figure below)



In this lab, we are dealing with two zones: .edu and .net zone. As we successfully spoofed a response indicating the example.edu domain is ns.dnslabattacker.net, we only spoofed IP for example.edu. Since we didn't spoof to ns.dnslanattacker.net, as the result, what we added in the additional section that indicating the IP of ns.dnslabattacker.net is ignored as we are not given authority to specify the IP for that domain.