CS 528. Network Security Lab2

Zhanfu Yang

yang1676@purdue.edu

Content

UDP 1:

The IP address and names of each machine:

(1) **DNS Server: 192.168.15.6**
(2) **User: 192.168.15.7**
(3) **Attacker: 192.168.15.8**

Attacker:

Run:

bash run.sh

Server:

bash check.sh

// sudo rndc dumpdb -cache
// cat /var/cache/bind/dump.db | grep "attacker" | head

Result:

```
[[02/28/2019 17:55] cs528user@cs528vm:~$ bash check.sh
[[02/28/2019 18:07] cs528user@cs528vm:~$ bash check.sh
[[02/28/2019 18:07] cs528user@cs528vm:~$ bash check.sh
[[02/28/2019 18:07] cs528user@cs528vm:~$ bash check.sh
[[02/28/2019 18:07] cs528user@cs528vm:~$ bash check.sh
[[02/28/2019 18:07] cs528user@cs528vm:~$ bash check.sh
[[02/28/2019 18:07] cs528user@cs528vm:~$ bash check.sh
[[02/28/2019 18:07] cs528user@cs528vm:~$ bash check.sh
[[02/28/2019 18:07] cs528user@cs528vm:~$ bash check.sh
[[02/28/2019 18:07] cs528user@cs528vm:~$ bash check.sh
[[02/28/2019 18:07] cs528user@cs528vm:~$ bash check.sh
[[02/28/2019 18:10] cs528user@cs528vm:~$ bash check.sh
 example.edu.            172574  NS      ns.dnslabattacker.net.
[[02/28/2019 18:10] cs528user@cs528vm:~$ bash check.sh
 example.edu.            172571  NS      ns.dnslabattacker.net.
[[02/28/2019 18:10] cs528user@cs528vm:~$ bash check.sh
 example.edu.            172569  NS      ns.dnslabattacker.net.
[[02/28/2019 18:10] cs528user@cs528vm:~$ bash check.sh
 example.edu.            172565  NS      ns.dnslabattacker.net.
[[02/28/2019 18:10] cs528user@cs528vm:~$ bash check.sh
 example.edu.            172563  NS      ns.dnslabattacker.net.
[[02/28/2019 18:11] cs528user@cs528vm:~$ bash check.sh
 example.edu.            172561  NS      ns.dnslabattacker.net.
[[02/28/2019 18:11] cs528user@cs528vm:~$ bash check.sh
 example.edu.            172559  NS      ns.dnslabattacker.net.
 [02/28/2019 18:11] cs528user@cs528vm:~$
```

Figure. 1. Attack UDP

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?

Answer:

As figure 2. DNS uses a hierarchy to manage its distributed database system. The DNS tree has a single domain at the top of the structure called the root domain. Each children layer of the tree represents a different domain. As per DNS's specifications, only a special entity(s) may assume administrative role for different zones.

When we send spoofed packets to Apollo, the domain "ns.dnslabattacker.net" is the authoritative name server for the "example.edu".

Because we can spoof the IP of the actual name server of "example.edu" , which can be considered to have administrative rights to specify values of the "example.edu" domain, Apollo accepts response and updates it.

As we are not able to spoof "ns.dnslabattacker.net", the information mentioned in additional section which shows IP address of the "ns.dnslabattacker.net" is ignored. We are not given the authority to specify the IP for that domain.

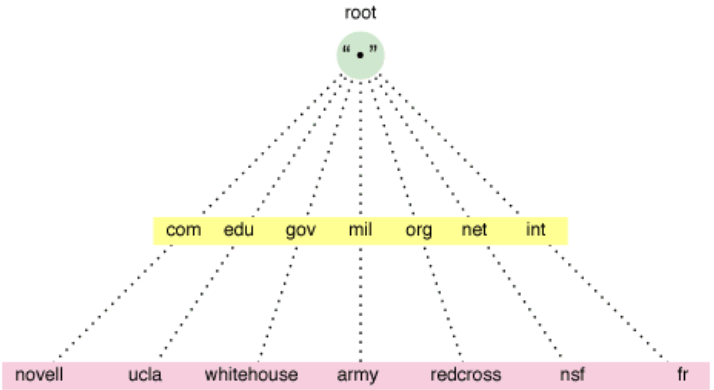

Figure. 2. DNS structure.

UDP 2:

```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4967
;; 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.            172700  IN      NS      ns.dnslabattacker.net.

;; ADDITIONAL SECTION:
ns.dnslabattacker.net.  604800  IN      A       192.168.15.8
ns.dnslabattacker.net.  604800  IN      AAAA    ::1

;; Query time: 13 msec
;; SERVER: 192.168.15.6#53(192.168.15.6)
;; WHEN: Thu Feb 28 19:47:13 2019
;; MSG SIZE  rcvd: 128

[02/28/2019 19:47] cs528user@cs528vm:~$ dig NS www.example.edu
```

Figure. 3. Dig result