Hongqi Guo

HW3

CptS 427/527 Assignment #3 – Covert Channel

1. **How does your covert channel work? [Include its type (e.g., timing or shared resource) and bandwidth.]**
   shared resource

2. **Is your covert channel noisy or noiseless?**
   Noisy

3. **Instructions for implementing your proof of concept.**
   My design concept is that the attacker needs to use an external device (USB flash drive) for pre-installed control software (Remote Administration Tool (RAT)). Now the attacker can remotely control the opponent's computer.
   This creates a channel, which is secret because the user does not know that the remote-control software is installed on their computer.

4. **How could a defender detect your covert channel?**
   The disadvantage of remote-control software is that the attacker cannot occupy the defender's computer for a long time, which will greatly increase the possibility of detection by the defender.
   Second, the remote-control software needs to be running on the back end, and some firewalls or software and the like will raise a warning.

5. **How could you modify your covert channel to avoid this detection?**
   The transmission method I can think of is to construct a tunnel through the SSH protocol to achieve data encryption transmission.
   Given that the attacker has implemented remote control of the system, but the attacker cannot use it for long, this can be very easy to detect.
   Firstly, the attacker needs to modify the SSH address of the other host, so that the listening port can be bound to any IP address. then attacker can use the SSH service to link to the other's host. Here we use AUTOSSH. The SSH backlink will result in timeout closure. If the channel from the outer network to the inner network is closed, for this we need AutoSSH to provide a stable ssh reverse proxy tunnel. Once the channel is established, an attacker can use this SSH tunnel to gain access to the other host.

6. **A time log of your activities for this assignment (e.g., research, implementation, documentation, etc.)**

Attacker computer output interface:

```
[root@localhost ~]# lsof -i:4010
COMMAND   PID    USER   FD   TYPE             DEVICE SIZE/OFF NODE NAME
ssh      6710 lixl    5u  IPv6 0x15699cecfe8a4995      0t0  TCP
localhost:altserviceboot (LISTEN)
autossh 46984 lixl    3u  IPv4 0x15699cece41d5e95      0t0  TCP
localhost:altserviceboot (LISTEN)
```

As shown in the output above, the attacker has successfully established the interface. Due to limited technology, AUTOSSH can only be used on Linux systems, and my computer can only support one virtual machine. Ideally, there will be two SSH links on the defender's computer that have the same command. One of these is the attacker's interface.

Conclusion:

All in all, there are several ways in which covert channels can be used. I cannot perfectly display a good covert passageway because of my limited abilities. This does not affect my interest in computer security. Through learning this course in this semester, I have learned a lot about network security and information security.

This will provide a good foundation for my further study in the future.