2018

Covert Communication Application

FINAL PROJECT – REPORT

DANNY LIEU

Table of Contents

Design 2

Detection & Recommendation 2

Design

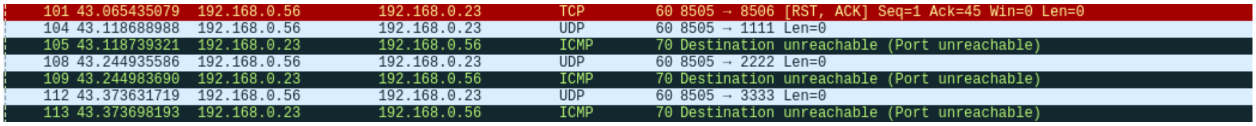
In this project, the backdoor will constantly sniff packets at the same level as the card level. That means it will receive the packet regardless any firewall rule is in place. To detect if the packet is meant to the backdoor, the payload of the packet has to have the password. Otherwise, the packet will be discarded. The command will be extracted from the payload and the backdoor will execute it accordingly. Depending on the type of commands, an appropriate response will be sent to the attacker. The attacker also has the ability of getting a specific file through command. The backdoor also allows to watch for a specific directory or a file for events and it will be sent to the attacker. Keylogger is one of the feature of the backdoor when the keystrokes will be sent if the buffer is full.

Detection & Recommendation

Backdoor is really hard to detect, and it requires patience from the network administrator. The hardest for the hacker to do is how to put the backdoor on the compromised machine. Knowing that, there are many ways to prevent backdoor implant:

- Be aware of any malicious content that you see when using the Internet
- Be very careful when clicking any links that you receive
- Use complicated password on your system

For this project, the port knocking is using UDP packet and Wireshark will capture all packets.



```
101 43.065435079  192.168.0.56      192.168.0.23      TCP       60 8505 → 8506 [RST, ACK] Seq=1 Ack=45 Win=0 Len=0
104 43.118688988  192.168.0.56      192.168.0.23      UDP       60 8505 → 1111 Len=0
105 43.118739321  192.168.0.23      192.168.0.56      ICMP      70 Destination unreachable (Port unreachable)
108 43.244935586  192.168.0.56      192.168.0.23      UDP       60 8505 → 2222 Len=0
109 43.244983690  192.168.0.23      192.168.0.56      ICMP      70 Destination unreachable (Port unreachable)
112 43.373631719  192.168.0.56      192.168.0.23      UDP       60 8505 → 3333 Len=0
113 43.373698193  192.168.0.23      192.168.0.56      ICMP      70 Destination unreachable (Port unreachable)
```

As we can see, all comeback packets have the message “Destination unreachable”. This will happen multiple times because the backdoor will send a lot of files back to the attacker. The administrator can look at Wireshark capture to detect such malicious activities.