NIDS using SNORT - Part 2: Writing Cutom Rules

Objectives

- Writing Custom snort rules

Prerequisites

- Wireshark or tcpdump for network traffic analysis (optional)

Activity 1: Detecting TELNET logging attempts

1. Open `hydra_telnet.pcap` using wireshark

2. Use snort with the following rule:

```
alert tcp any any <> any 23 (flags:S; msg:"Telnet Login";sid:9000005;rev:1;)
```

- **Questions:**
  - How many rules are there?
  - Which are the IP addresses of the hosts involved
  - Which are the TCP ports they are using

Activity 2: Detecting File Types, Emails Content & Attachements

- Use the following rules on pcap files (`with_*.pcap`)

```
alert tcp any any -> any any (content:"GIF89a"; msg:"GIF";sid:10000)
alert tcp any any -> any any (content:"%PDF"; msg:"PDF";sid:10001)
alert tcp any any -> any any (content:"|89 50 4E 47|";
msg:"PNG";sid:10002)
alert tcp any any -> any any (content:"|50 4B 03 04|";
msg:"ZIP";sid:10003)
alert tcp any any -> any any (content:"|FF D8|"; msg:"JPEG";sid:10004)
alert tcp any any -> any any (content:"|49 44 33|"; msg:"MP3";sid:10005)
alert tcp any any -> any any (content:"|52 61 72 21 1A 07 00|";
msg:"RAR";sid:10010)
alert tcp any any -> any any (content:"|D0 CF 11 E0 A1 B1 1A E1|";
msg:"Office 2010";sid:10011)
```

- Use the following rules on `email_cc2.pcap` from lab 2

```
alert tcp any any <> any any (pcre:"/5\d{3}(\s|-)?\d{4}(\s|-)?\d{4}(\s|-
)?\d{4}/"; msg:"MasterCard number detected in clear
```

```
text";content:"number";nocase;sid:9000003;rev:1;)

alert tcp any any <> any any (pcre:"/3\d{3}(\s|-)?\d{6}(\s|-)?\d{5}/"; msg:"American
Express number detected in clear text";content:"number";nocase;sid:9000004;rev:1;)

alert tcp any any <> any any (pcre:"/4\d{3}(\s|-)?\d{4}(\s|-)?\d{4}(\s|-)?\d{4}/";
msg:"Visa number detected in clear text";content:"number";nocase;sid:9000005;rev:1;)
```

- **Questions:**
- For each file related pcaps (`with_*.pcap`), How many file type has been detected ?
- For cc2 captures, how many alerts are there ?