Lab 7: Snort

1 Details

Aim: To provide a foundation in understanding of Snort.

To start this, open up the following page:

https://asecuritysite.com/forensics/snort2

2 Activities

L1.1 To detect an FTP connection to the server, we can detect the connection to a destination port of 21:

```
# Signature Detection
alert tcp any any -> any 21 ( msg:"FTP";sid:10000)
```

We can then use a PCAP file of "FTP".

How many rules are there?

Which are the IP addresses of the hosts involved:

Which are the TCP ports they are using:

L1.2 We can improve the rules with by detecting a SYN connection and a bad login (530):

```
alert tcp any any -> any 21 (flags:S;msg:"FTP
    Connection";sid:9000005;rev:1;)
alert tcp any 21 -> any any (msg:"FTP Bad login"; content:"530 User ";
    nocase; flow:from_server,established; sid:491; rev:5;)
```

If we select the "FTP" trace, we get:

How many rules are there?

Which are the IP addresses of the hosts involved:

Which are the TCP ports they are using:

L1.3 Now let's detect a TELNET connection:

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

Next select the "Hydra Telnet" trace, we get:

How many rules are there?

Which are the IP addresses of the hosts involved:

Which are the TCP ports they are using:

L1.4 We can now detect file types. We can create some rules to detect various file types:

```
# Signature Detection
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 49 46 46|";
     msg:"AVI";sid:10006)
alert tcp any any -> any any (content:"|46 57 53|"; msg:"Flash
     SWF";sid:10007)
alert tcp any any -> any any (content:"|46 4C 56|"; msg:"Flash
     Video";sid:10008)
alert tcp any any -> any any (content:"|1F 8B 08|"; msg:"GZip";sid:10009)
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)
```

If we use "email_with_gif", we will get:

How many GIF files are there?

L1.5 We can detect credit card details with:

```
# Detecting credit card details
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;)
```

If we select "Email with credit card details", determine the following:

How many GIF files are there?

What are the IP addresses involved?