Packet Inspection for Malware Detection

Ashrafur Rahman
ashraf882@gmail.com

January 16, 2019

Introduction

The Packet Capture library (pcap) provides a high level interface to packet capture systems. All packets on the network, even those destined for other hosts, are accessible through this mechanism. For this project, I used *libpcap* implementation of library.

Iptables

Iptables is an extremely flexible firewall utility built for Linux operating systems. By default the accept rule for iptables should be like the following output, if not, please change accordingly to match this code listing.

```
#!/bin/bash
iptables --policy INPUT ACCEPT
iptables --policy OUTPUT ACCEPT
iptables --policy FORWARD ACCEPT
```

Compilation

The code file is a source code written in C language and named as *cap.c*. To compile this file in unix environment, please write the following command in terminal emulator. We should include `sudo` command to avoid any permission related error.

```
sudo gcc ./cap.c -o cap -lpcap
```

This will generate an output file named *cap*. We will execute this file from terminal environment.

Parameters

To run this file, we need to define some parameter in the following format:

```
sudo ./cap "options" i search
```

Here different parameter represents:

`options:` for incomming packet types

```
      Expression              Description
      ----------             -----------
      ip                      Capture all IP packets
      tcp                     Capture only TCP packets
      tcp port 80             Capture only TCP packets with a port equal to 80
      ip host 10.1.2.3        Capture all IP packets to or from host 10.1.2.3
      src www.example.com     Capture all IP packets from source www.example.com
```

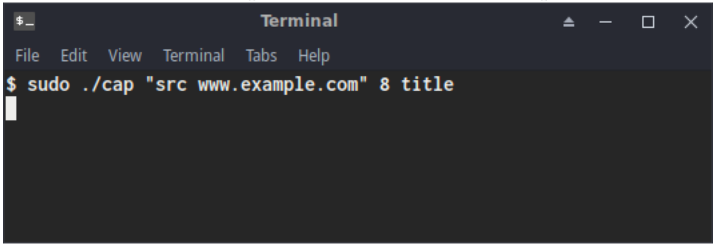
`i:` counter for packet scanning
`search:` search string for packet

Exection

If we execute this program with the following parameter, this program will scan 8 packets and scan for the term “title” in these packets.

```
sudo ./cap "src www.example.com" 8 title
```

It will wait for the packet from *www.example.com* address.

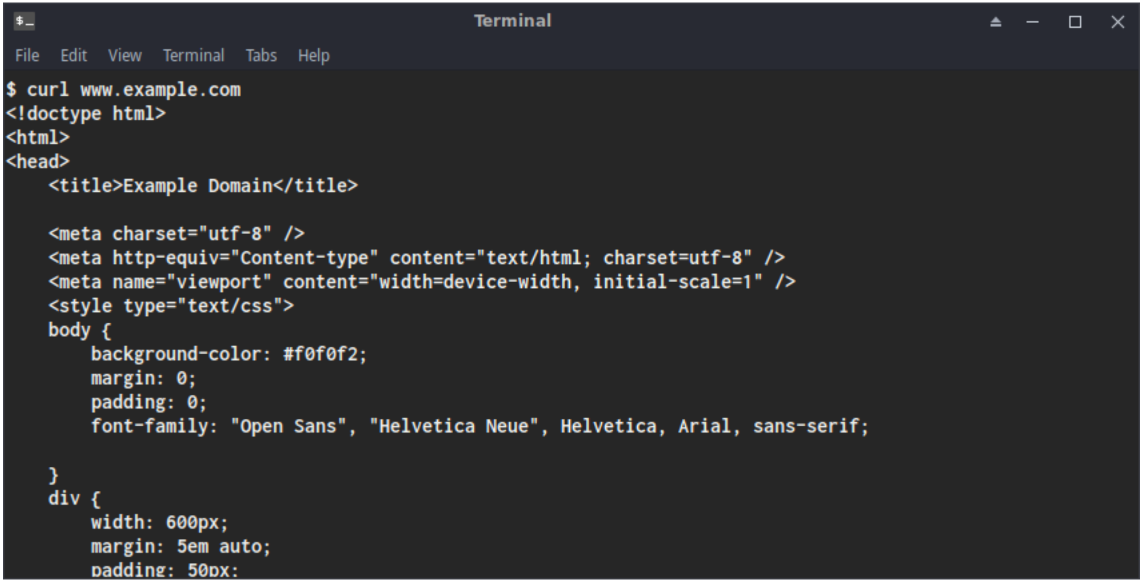


```
$ sudo ./cap "src www.example.com" 8 title
```

Now if we fetch data from *www.example.com* with the following command in another terminal:

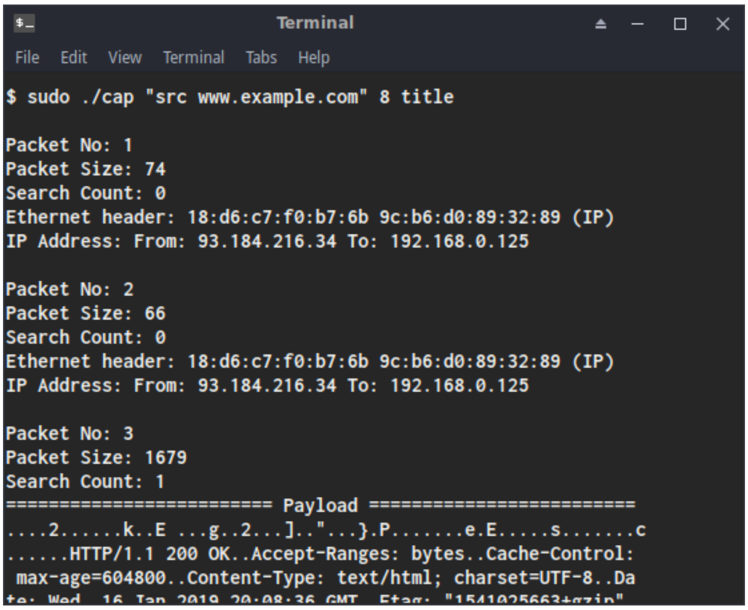
```
curl www.example.com
```

We will get some http data as follows:



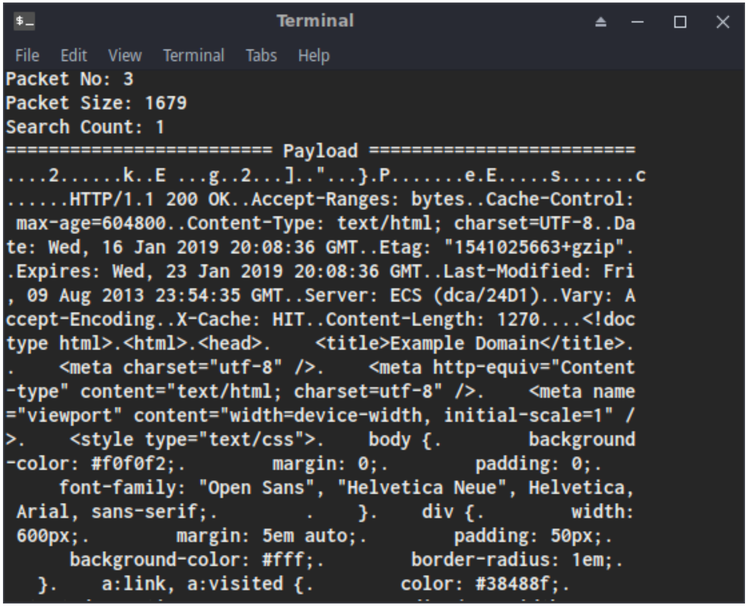
```
$ curl www.example.com
<!doctype html>
<html>
<head>
    <title>Example Domain</title>

    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
    body {
        background-color: #f0f0f2;
        margin: 0;
        padding: 0;
        font-family: "Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;

    }
    div {
        width: 600px;
        margin: 5em auto;
        padding: 50px;
```

Then the running program in other window will capture these packets and analyze them for the search string:



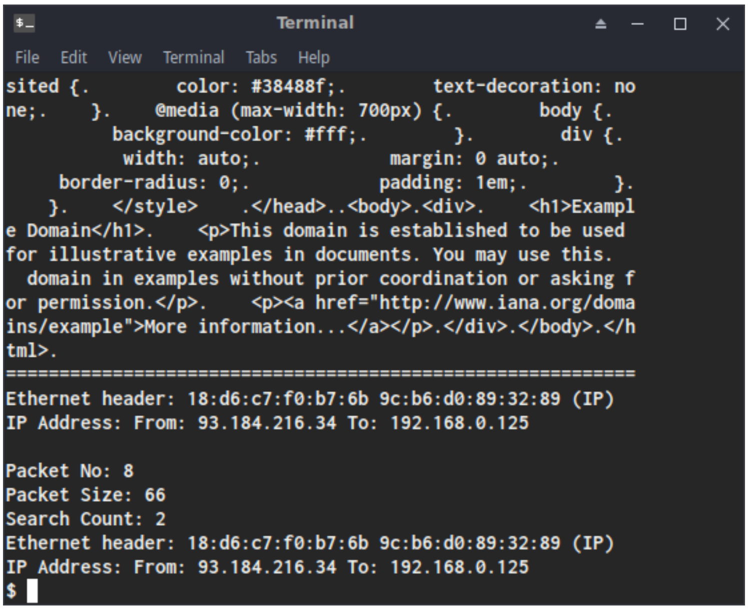
```
$ sudo ./cap "src www.example.com" 8 title

Packet No: 1
Packet Size: 74
Search Count: 0
Ethernet header: 18:d6:c7:f0:b7:6b 9c:b6:d0:89:32:89 (IP)
IP Address: From: 93.184.216.34 To: 192.168.0.125

Packet No: 2
Packet Size: 66
Search Count: 0
Ethernet header: 18:d6:c7:f0:b7:6b 9c:b6:d0:89:32:89 (IP)
IP Address: From: 93.184.216.34 To: 192.168.0.125

Packet No: 3
Packet Size: 1679
Search Count: 1
========================= Payload =========================
....2......k..E ...g..2...].."...}.P.......e.E.....s.......c
......HTTP/1.1 200 OK..Accept-Ranges: bytes..Cache-Control:
 max-age=604800..Content-Type: text/html; charset=UTF-8..Da
te: Wed, 16 Jan 2019 20:08:36 GMT..Etag: "1541025663+gzip"
```

From figure, we can see, it identified the search string at packet number 3 and after identifying, it prints the whole payload and increases the *Search Count* to 1:



```
Packet No: 3
Packet Size: 1679
Search Count: 1
========================= Payload =========================
....2......k..E ...g..2...]..."...}.P.......e.E.....s.......c
......HTTP/1.1 200 OK..Accept-Ranges: bytes..Cache-Control:
 max-age=604800..Content-Type: text/html; charset=UTF-8..Da
te: Wed, 16 Jan 2019 20:08:36 GMT..Etag: "1541025663+gzip".
.Expires: Wed, 23 Jan 2019 20:08:36 GMT..Last-Modified: Fri
, 09 Aug 2013 23:54:35 GMT..Server: ECS (dca/24D1)..Vary: A
ccept-Encoding..X-Cache: HIT..Content-Length: 1270....<!doc
type html>.<html>.<head>.    <title>Example Domain</title>.
.    <meta charset="utf-8" />.    <meta http-equiv="Content
-type" content="text/html; charset=utf-8" />.    <meta name
="viewport" content="width=device-width, initial-scale=1" /
>.    <style type="text/css">.    body {.        background
-color: #f0f0f2;.        margin: 0;.        padding: 0;.
     font-family: "Open Sans", "Helvetica Neue", Helvetica,
 Arial, sans-serif;.        .    }.    div {.        width:
 600px;.        margin: 5em auto;.        padding: 50px;.
      background-color: #fff;.        border-radius: 1em;.
   }.    a:link, a:visited {.        color: #38488f;.
```

After scanning total number of packets, it will display the total *Search Count* for the matching string.



```
sited {.        color: #38488f;.        text-decoration: no
ne;.    }.    @media (max-width: 700px) {.        body {.
          background-color: #fff;.        }.        div {.
           width: auto;.            margin: 0 auto;.
     border-radius: 0;.            padding: 1em;.        }.
    }.    </style>    .</head>..<body>.<div>.    <h1>Exampl
e Domain</h1>.    <p>This domain is established to be used
for illustrative examples in documents. You may use this.
  domain in examples without prior coordination or asking f
or permission.</p>.    <p><a href="http://www.iana.org/doma
ins/example">More information...</a></p>.</div>.</body>.</h
tml>.
===========================================================
Ethernet header: 18:d6:c7:f0:b7:6b 9c:b6:d0:89:32:89 (IP)
IP Address: From: 93.184.216.34 To: 192.168.0.125

Packet No: 8
Packet Size: 66
Search Count: 2
Ethernet header: 18:d6:c7:f0:b7:6b 9c:b6:d0:89:32:89 (IP)
IP Address: From: 93.184.216.34 To: 192.168.0.125
$ 
```

Repository

Github repository for the source code, compiled program and documentation;

https://github.com/code4ash/Packet-Inspection