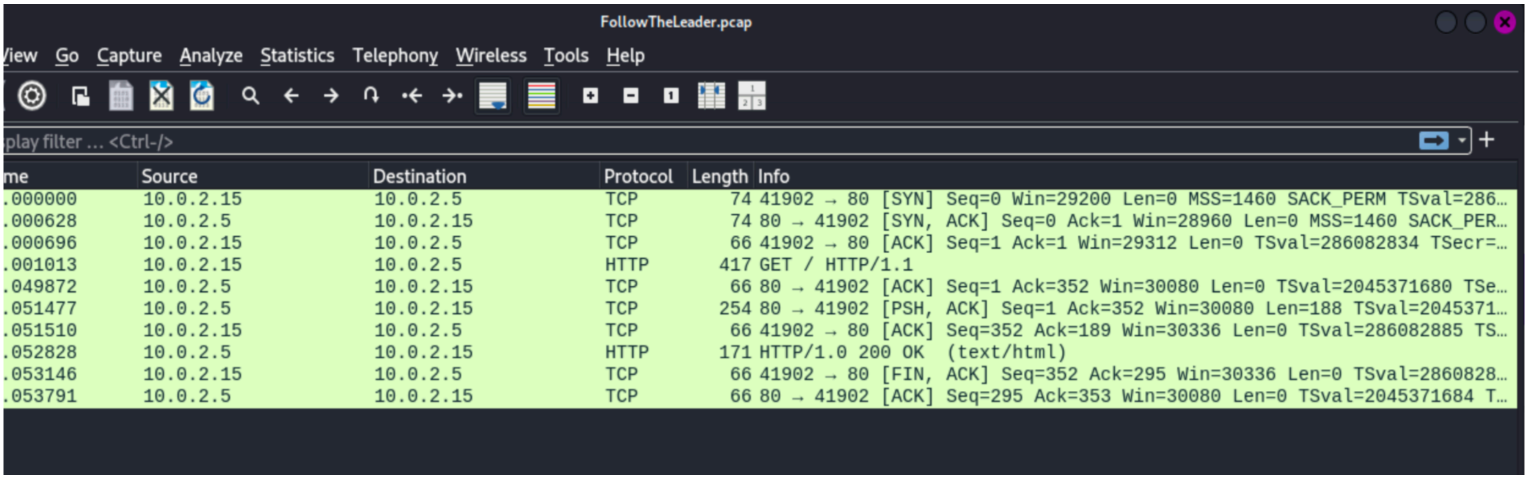
Workshop on Sniffing and Spoofing

23bcs048
G V Prajwal

Sniffing Tools

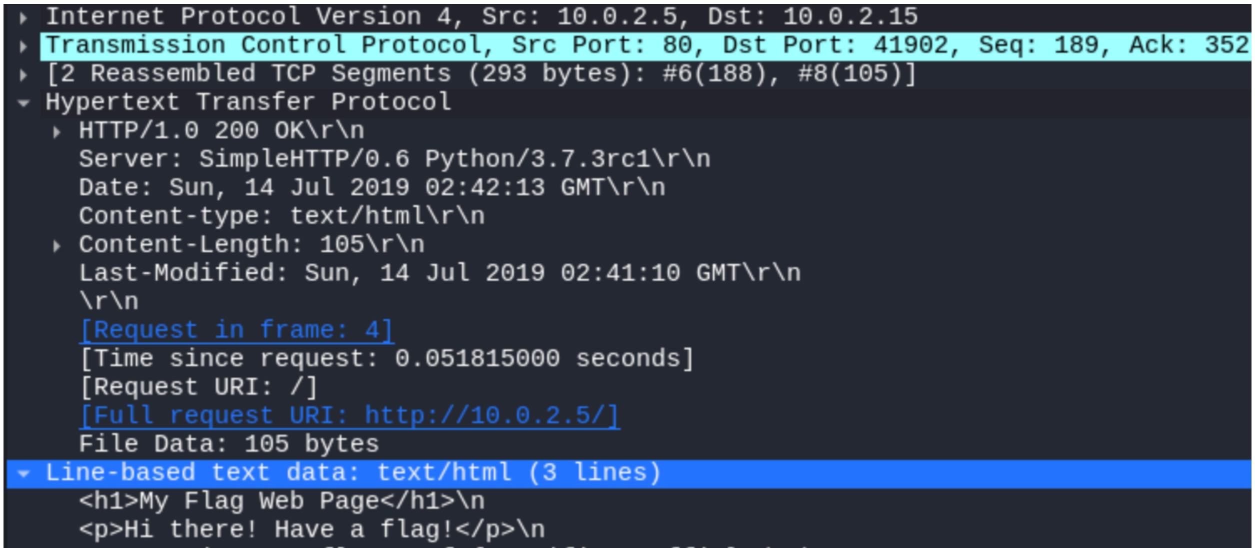
Wireshark

Today I'll be using wireshark to solve the challenge on this link:
https://ctfacademy.github.io/network/challenge1/index.htm


FollowTheLeader.pcap
iew Go Capture Analyze Statistics Telephony Wireless Tools Help
play filter … <Ctrl-/>

```
me        Source       Destination   Protocol Length Info
.000000   10.0.2.15    10.0.2.5      TCP        74 41902 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=286…
.000628   10.0.2.5     10.0.2.15     TCP        74 80 → 41902 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PER…
.000696   10.0.2.15    10.0.2.5      TCP        66 41902 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=286082834 TSecr=…
.001013   10.0.2.15    10.0.2.5      HTTP      417 GET / HTTP/1.1
.049872   10.0.2.5     10.0.2.15     TCP        66 80 → 41902 [ACK] Seq=1 Ack=352 Win=30080 Len=0 TSval=2045371680 TSe…
.051477   10.0.2.5     10.0.2.15     TCP       254 80 → 41902 [PSH, ACK] Seq=1 Ack=352 Win=30080 Len=188 TSval=2045371…
.051510   10.0.2.15    10.0.2.5      TCP        66 41902 → 80 [ACK] Seq=352 Ack=189 Win=30336 Len=0 TSval=286082885 TS…
.052828   10.0.2.5     10.0.2.15     HTTP      171 HTTP/1.0 200 OK  (text/html)
.053146   10.0.2.15    10.0.2.5      TCP        66 41902 → 80 [FIN, ACK] Seq=352 Ack=295 Win=30336 Len=0 TSval=2860828…
.053791   10.0.2.5     10.0.2.15     TCP        66 80 → 41902 [ACK] Seq=295 Ack=353 Win=30080 Len=0 TSval=2045371684 T…
```

As seen in the picture above there are two HTTP protocols and one of them is sending a text/html. On inspecting that packet, we get:



```
▸ Internet Protocol Version 4, Src: 10.0.2.5, Dst: 10.0.2.15
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 41902, Seq: 189, Ack: 352
▸ [2 Reassembled TCP Segments (293 bytes): #6(188), #8(105)]
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.0 200 OK\r\n
    Server: SimpleHTTP/0.6 Python/3.7.3rc1\r\n
    Date: Sun, 14 Jul 2019 02:42:13 GMT\r\n
    Content-type: text/html\r\n
  ▸ Content-Length: 105\r\n
    Last-Modified: Sun, 14 Jul 2019 02:41:10 GMT\r\n
    \r\n
    [Request in frame: 4]
    [Time since request: 0.051815000 seconds]
    [Request URI: /]
    [Full request URI: http://10.0.2.5/]
    File Data: 105 bytes
▾ Line-based text data: text/html (3 lines)
    <h1>My Flag Web Page</h1>\n
    <p>Hi there! Have a flag!</p>\n
```

Spoofing Tools

How Spoofing Works

1. **Reconnaissance:** Gathering information about the target.
2. **Impersonation:** Falsified data is created.
3. **Deception:** The data is sent to trick the victim.
4. **Exploitation:** Attacker gains access or data from the victim.

Ettercap

Ettercap can be used to find the IP and MAC addresses of all the hosts in the network then choosing any two communicating systems and setting them as target 1 and target 2.
Target 1 is the host you want to impersonate and target 2 is the one which is sending it.
Then, you can also perform ARP poisoning and other attacks to manipulate the packets and forward them.
We can simulate this by setting some sort of communication (like TCP using nc or netcat) and spoof the packets transferred between them.