# 信息安全原理 HW4

姓名: 王晨雨

学号: 3200102324

## 实验过程:

1. 清除浏览器缓存:

○ 设置



Q 在设置中搜索

2. 重启网卡服务

C:\Windows\System32>net start npf 请求的服务已经启动。 请键入 NET HELPMSG 2182 以获得更多的帮助。

## 3. 获取目标网站服务器

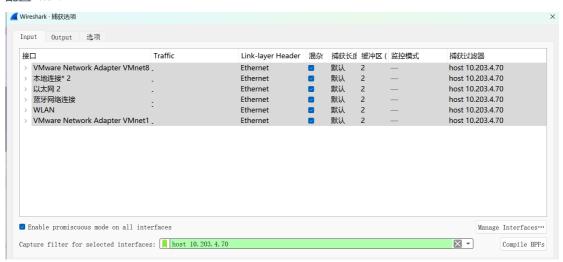
```
C:\Windows\System32>ping www.zju.edu.cn

正在 Ping www.zju.edu.cn [10.203.4.70] 具有 32 字节的数据:
来自 10.203.4.70 的回复:字节=32 时间=22ms TTL=59
来自 10.203.4.70 的回复:字节=32 时间=14ms TTL=59
来自 10.203.4.70 的回复:字节=32 时间=16ms TTL=59
来自 10.203.4.70 的回复:字节=32 时间=16ms TTL=59

10.203.4.70 的 Ping 统计信息:
数据包:已发送 = 4,已接收 = 4,丢失 = 0(0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 14ms,最长 = 22ms,平均 = 17ms
```

#### 4. 配置wireshark

#### 配置filter:



## 5. 开始抓包:

	Time	Source	Destination	Protocol	Length Info
	1 0.000000	10.162.86.163	10.203.4.70	TCP	74 3928 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25
	2 0.001954	10.162.86.163	10.203.4.70	TCP	74 3929 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25
	3 0.009724	10.203.4.70	10.162.86.163	TCP	74 443 → 3928 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS
	4 0.009726	10.203.4.70	10.162.86.163	TCP	74 443 → 3929 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS
	5 0.010312	10.162.86.163	10.203.4.70	TCP	66 3928 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=2
	6 0.010429	10.162.86.163	10.203.4.70	TCP	66 3929 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=2
	7 0.011068	10.162.86.163	10.203.4.70	TLSv1.2	586 Client Hello
	8 0.011734	10.162.86.163	10.203.4.70	TLSv1.2	586 Client Hello
	9 0.017931	10.203.4.70	10.162.86.163	TCP	66 443 → 3928 [ACK] Seq=1 Ack=521 Win=64640 Len=0 TSval=
	10 0.017933	10.203.4.70	10.162.86.163	TCP	66 443 → 3929 [ACK] Seq=1 Ack=521 Win=64640 Len=0 TSval:
	11 0.022366	10.203.4.70	10.162.86.163	TLSv1.2	1514 Server Hello
	12 0.022384	10.203.4.70	10.162.86.163	TCP	1514 443 → 3929 [ACK] Seq=1449 Ack=521 Win=64640 Len=1448
	13 0.022386	10.203.4.70	10.162.86.163	TLSv1.2	504 Certificate, Server Key Exchange, Server Hello Done
	14 0.022387	10.203.4.70	10.162.86.163	TLSv1.2	1514 Server Hello
	15 0.022389	10.203.4.70	10.162.86.163	TCP	1514 443 → 3928 [ACK] Seq=1449 Ack=521 Win=64640 Len=1448
	16 0.022390	10.203.4.70	10.162.86.163	TLSv1.2	504 Certificate, Server Key Exchange, Server Hello Done
	17 0.022770	10.162.86.163	10.203.4.70	TCP	66 3929 → 443 [ACK] Seq=521 Ack=3335 Win=131584 Len=0 T
	18 0.022918	10.162.86.163	10.203.4.70	TCP	66 3928 → 443 [ACK] Seq=521 Ack=3335 Win=131584 Len=0 TS
_	40 0 004447	10 100 00 100	40 202 4 70	T1 C. 4 3	ACO CISTAL NOT CONTRACT CONTRACT OF THE CONTRA
+h	ennet II Snc:	NewH3CTe h0:e8:02 (7	4.32.20.b0.68.02) D	st. IntelCon	65:e9:ba (c8:b2:9b:65:e9:ba)
	lernet 11, 51 c.	Newnocre_09.e0.02 (7	4.30.20.09.60.02), 0	sc. intercor_	05.69.00 (08.02.90.05.69.00)
20	-0 h2 0h CE -0	) ha 74 3a 20 b9 e8	02 00 00 45 00	e··t: ····F	
00 10		00 3b 06 cf 66 0a		·е··т: ·····ь ··@·;· ·f···F·	
20		68 cb b1 df da 26		P·h·· ··&T·Y·	
30		00 02 04 05 b4 04			
40		ee 01 03 03 07		)D	

# 6. 分析抓包结果:

1. TCP三次握手协议:

本机向目标服务器发送同步请求,将Flags字段的Sym设置为Set

```
Protocol Length Info
                                                                                                               74 3928 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25
74 3929 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25
                             10.162.86.163
                                                             10.203.4.70
     2 0.001954
                             10.162.86.163
                                                              10.203.4.70
                                                                                              TCP
                                                                                                               74 443 → 3928 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MS
                                                                                                              74 443 → 3929 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS 66 3928 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=2 66 3929 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=2
     4 0.009726
                             10.203.4.70
                                                             10.162.86.163
     6 0.010429
                             10.162.86.163
                                                             10.203.4.70
                                                                                             TCP
 Acknowledgment Number: 0
 Acknowledgment number (raw): 0
1010 .... = Header Length: 40 bytes (10) Flags: 0x002 (SYN)
    000. ... = Reserved: Not set
...0 ... = Nonce: Not set
...0 ... = Congestion Window Reduced (CWR): Not set
     .... .0. .... = ECN-Echo: Not set .... .0. .... = Urgent: Not set
    .... 0 .... = Acknowledgment: Not set .... 0... = Push: Not set
    .... .0.. = Reset: Not set
.... .1. = Syn: Set
```

# 目标服务器向本机回复一个ACK包,其中Syn和Acknowledgment都为Set

```
th Info
74 3928 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25
74 3929 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25
74 443 → 3928 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MS5
74 443 → 3929 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MS5
     1 0.000000
                             10.162.86.163
                                                              10.203.4.70
     2 0.001954
                             10.162.86.163
                                                              10.203.4.70
    3 0.009724
4 0.009726
                            10.203.4.70
10.203.4.70
                                                             10.162.86.163
10.162.86.163
                                                                                             TCP
                                                                                             TCP
                                                                                                              66 3928 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=2
66 3929 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=2
    5 0.010312
                            10.162.86.163
                                                             10.203.4.70
                                                                                              TCP
                             10.162.86.163
                                                             10.203.4.70
 Acknowledgment Number: 1
                                           (relative ack number)
Acknowledgment number: 1 (relative ac
Acknowledgment number (raw): 3572974186
1010 .... = Header Length: 40 bytes (10)
.... .0.. ... = ECN-Echo: Not set .... .0. ... = Urgent: Not set
    .... = Acknowledgment: Set
    .... 0... = Push: Not set
   .... .0.. = Reset: Not set
```

# 最后,本机向目标服务器发送一个ACK包,Flag和ACknowledgment设置为Set。成功连接。

```
74 3929 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=2!
                         10.162.86.163
                                                     10.203.4.70
    2 0.001954
                                                     10.162.86.163
10.162.86.163
                                                                                                74 443 → 3928 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MS:
74 443 → 3929 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MS:
   3 0.009724
                         10.203.4.70
                                                                                 TCP
   4 0.009726
                        10.203.4.70
                                                                                 TCP
                                                                                                66 3928 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=2
66 3929 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=2
   5 0.010312
                         10.162.86.163
                                                     10,203,4,70
                         10.162.86.163
                                                                                 ТСР
Acknowledgment Number: 1
                                     (relative ack number)
Acknowledgment Number: 1 (relative a Acknowledgment number (raw): 1333608940 1000 .... = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
   000. .... = Reserved: Not set ...0 .... = Nonce: Not set
  .... 0... = Push: Not set
.... 0... = Reset: Not set
    .... .... ..0. = Syn: Not set
```

#### 2. HTTP请求

## GET 请求

vo.	Time	Source	Destination	Protocol	Length Info				
	54 2.920826	10.162.86.163	10.203.4.70	TCP	66 3943 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=27				
	55 2.955722	10.162.86.163	10.203.4.70	TCP	74 3944 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=25€				
	56 2.962799	10.162.86.163	10.203.4.70	TCP	1514 3943 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=1448 TSva]				
	57 2.962829	10.162.86.163	10.203.4.70	TCP	1514 3943 → 80 [ACK] Seq=1449 Ack=1 Win=131584 Len=1448 TS				
-	58 2.962839	10.162.86.163	10.203.4.70	HTTP	460 GET /593/list.htm HTTP/1.1				
	59 2.971384	10.203.4.70	10.162.86.163	TCP	74 80 → 3944 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=				
	60 2.971588	10.162.86.163	10.203.4.70	TCP	66 3944 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=27				
	61 2.972837	10.203.4.70	10.162.86.163	TCP	66 80 → 3943 [ACK] Seq=1 Ack=1449 Win=64128 Len=0 TSval=				
	62 2.972838	10.203.4.70	10.162.86.163	TCP	66 80 → 3943 [ACK] Sea=1 Ack=2897 Win=63488 Len=0 TSval=				
<pre>&gt; [Timestamps] TCP payload (394 bytes) TCP segment data (394 bytes) &gt; [3 Reassembled TCP Segments (3290 bytes): #56(1448), #57(1448), #58(394)]</pre>									
H	ypertext Transfer								
GET /593/list.htm HTTP/1.1\r\n  Host: www.zju.edu.cn\r\n									
Connection: keep-alive\n									
	Upgrade-Insecure-Requests: 1\r\n								
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36\r\ Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex									

#### 目标服务器返回ACK:

```
460 GET /593/list.htm HTTP/1.1
       58 2.962839
                                     10.162.86.163
                                                                          10.203.4.70
                                                                                                               HTTP
                                                                                                                               460 GET /593/list.htm HTTP/1.1
74 80 → 3944 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=
66 3944 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=2
66 80 → 3943 [ACK] Seq=1 Ack=1449 Win=64128 Len=0 TSval=
66 80 → 3943 [ACK] Seq=1 Ack=2897 Win=63488 Len=0 TSval=
66 80 → 3943 [ACK] Seq=1 Ack=2897 Win=61428 Len=0 TSval=
478 HTTP/1.1 301 Moved Permanently (text/html)
1514 3928 → 443 [ACK] Seq=8160 Ack=17294 Win=131072 Len=14
       59 2.971384
                                     10.203.4.70
                                                                          10.162.86.163
                                                                                                               TCP
                                      10.162.86.163
       60 2.971588
61 2.972837
                                                                           10.203.4.70
                                                                                                                TCP
                                      10.203.4.70
                                                                           10.162.86.163
                                                                                                                ТСР
                                                                                                                TCP
       62 2.972838
                                     10.203.4.70
                                                                           10.162.86.163
       63 2.972838
64 2.972839
                                     10.203.4.70
10.203.4.70
                                                                          10.162.86.163
10.162.86.163
                                                                                                               TCP
HTTP
       65 2,982076
                                     10,162,86,163
                                                                          10,203,4,70
                                                                                                                TCP
Ethernet II, Src: NewH3CTe_b9:e8:02 (74:3a:20:b9:e8:02), Dst: IntelCor_65:e9:ba (c8:b2:9b:65:e9:ba)
Internet Protocol Version 4, Src: 10.203.4.70, Dst: 10.162.86.163

Transmission Control Protocol, Src Port: 80, Dst Port: 3944, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
Destination Port: 3944
     [Stream index: 3]
     [TCP Segment Len: 0]
     Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 3417432026
    [Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)
```

## 3. 断开TCP

	220 5.829149	10.162.86.163	10.203.4.70	TCP	66 3945 → 443 [FIN, ACK] Seq=4391 Ack=3661 Win=131584 L€
	221 5.829234	10.162.86.163	10.203.4.70	TCP	66 3928 → 443 [FIN, ACK] Seq=23428 Ack=35633 Win=131584
	222 5.829321	10.162.86.163	10.203.4.70	TCP	66 3948 → 443 [FIN, ACK] Seq=4391 Ack=3661 Win=131584 L€
	223 5.829406	10.162.86.163	10.203.4.70	TCP	66 3947 → 443 [FIN, ACK] Seq=4391 Ack=3661 Win=131584 L€
	224 5.829502	10.162.86.163	10.203.4.70	TCP	66 3929 → 443 [FIN, ACK] Seq=15890 Ack=17625 Win=131584
	225 5.829599	10.162.86.163	10.203.4.70	TCP	66 3946 → 443 [FIN, ACK] Seq=11925 Ack=4368 Win=130816 I
- [	226 5.838871	10.203.4.70	10.162.86.163	TCP	66 80 → 3944 [FIN. ACK] Sea=1 Ack=2 Win=65280 Len=0 TSva

- Frame 225: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{3049F57B-A74C-4A2B-8ADE-72A352AA7574},
- Ethernet II, Src: IntelCor\_65:e9:ba (c8:b2:9b:65:e9:ba), Dst: NewH3CTe\_b9:e8:02 (74:3a:20:b9:e8:02)
  Internet Protocol Version 4, Src: 10.162.86.163, Dst: 10.203.4.70
  Transmission Control Protocol, Src Port: 3946, Dst Port: 443, Seq: 11925, Ack: 4368, Len: 0