به دلیل اینکه وبسایت دانشگاه به طور خودکار کاربر را از http به https ریدایرکت میکند، از وبسایت http://pwnable.kr استفاده خواهم کرد

باز کردن سایت

1- پروتکل های TCP, DNS, TLSv1.2, QUIC, HTTP, ARP

2- حدود 0.4 ثانیه

No.	Time	Source	Destination	Protocol	Length	Time	Info
8	0.060894	192.168.1.101	128.61.240.205	HTTP	632		GET / HTTP/1.1
16	0.475981	128.61.240.205	192.168.1.101	HTTP	524		HTTP/1.1 200 OK (text/html)

3- به 192.168.1.1 ، این آدرس متعلق به dns سرور شبکه است، به این دلیل که اولین مرحله باز کردن سایت، پیدا کردن آدرس آن است

پروتکل HTTP

1- هر دو نسخه 1.1 را استفاده میکنند، این دو نسخه تفاوت های زیادی دارند که به چند مورد اشاره میکنم: Proxy support, Persistent connection, OPTIONS method

منظور از persistent connection این است که برای هر بار ارسال یک بسته، نیاز به باز کردن یک کانکشن جدید نیست.

2- `Accept-Language: en-US,en;q=0.9\r\n`

3- `Src: 192.168.1.101, Dst: 128.61.240.205`

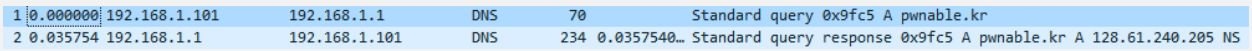
کامپیوتر: 192.168.1.101 سرور: 128.61.240.205

4- TCP

5-
```
Transmission Control Protocol, Src Port: 15160, Dst Port: 80,
```
مبدا: 15160 مقصد: 80

6-
```
HTTP/1.1 200 OK  (text/html)
```
کد 200 نشان دهنده موفقیت آمیز بودن درخواست است

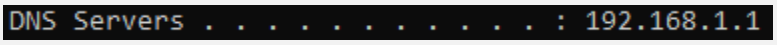
ردیابی DNS



1- آدرس فرستنده درخواست 192.168.1.101 است، آدرس فرستنده پاسخ ها 192.168.1.1 است
از پروتکل UDP استفاده شده است

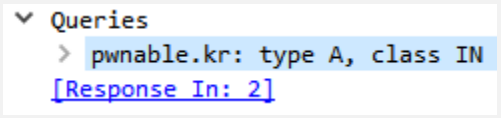
2- پورت 53 که مربوط به DNS Service است

3- به آدرس 192.168.1.1 فرستاده شده است



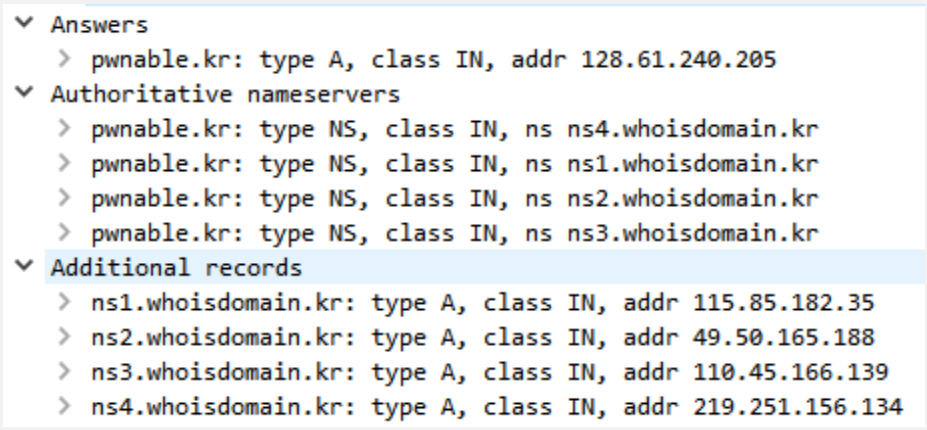
بله یکسان هستند

4-

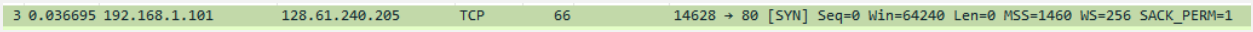


از نوع A است، حاوی جواب نیست

-5



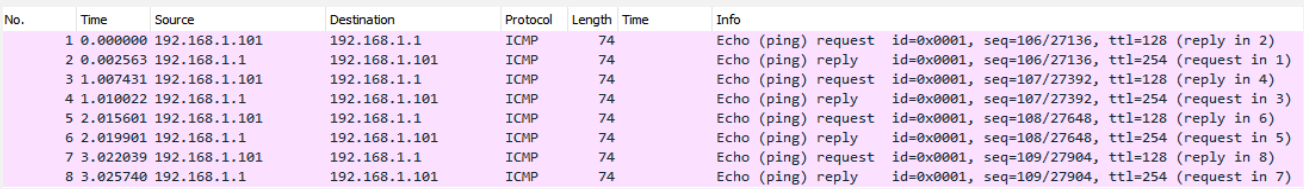
-6



بله، آدرس 128.61.240.205 مطابقت دارد

-7

ردیابی بسته های ICMP



No.	Time	Source	Destination	Protocol	Length	Time	Info
1	0.000000	192.168.1.101	192.168.1.1	ICMP	74		Echo (ping) request id=0x0001, seq=106/27136, ttl=128 (reply in 2)
2	0.002563	192.168.1.1	192.168.1.101	ICMP	74		Echo (ping) reply id=0x0001, seq=106/27136, ttl=254 (request in 1)
3	1.007431	192.168.1.101	192.168.1.1	ICMP	74		Echo (ping) request id=0x0001, seq=107/27392, ttl=128 (reply in 4)
4	1.010022	192.168.1.1	192.168.1.101	ICMP	74		Echo (ping) reply id=0x0001, seq=107/27392, ttl=254 (request in 3)
5	2.015601	192.168.1.101	192.168.1.1	ICMP	74		Echo (ping) request id=0x0001, seq=108/27648, ttl=128 (reply in 6)
6	2.019901	192.168.1.1	192.168.1.101	ICMP	74		Echo (ping) reply id=0x0001, seq=108/27648, ttl=254 (request in 5)
7	3.022039	192.168.1.101	192.168.1.1	ICMP	74		Echo (ping) request id=0x0001, seq=109/27904, ttl=128 (reply in 8)
8	3.025740	192.168.1.1	192.168.1.101	ICMP	74		Echo (ping) reply id=0x0001, seq=109/27904, ttl=254 (request in 7)

پروتکل ICMP فعال شده است