

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

مبدأ: 15160 مقصد: 80

6- HTTP/1.1 200 OK (text/html)

کد 200 نشان دهنده موفقیت آمیز بودن درخواست است

## ردیابی DNS

1	0.000000	192.168.1.101	192.168.1.1	DNS	70	Standard query 0x9fc5 A pwnable.kr
2	0.035754	192.168.1.1	192.168.1.101	DNS	234	0.0357540... Standard query response 0x9fc5 A pwnable.kr A 128.61.240.205 NS

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

DNS Servers . . . . . : 192.168.1.1

بله یکسان هستند

4-

```
▼ Queries
> pwnable.kr: type A, class IN
[Response In: 2]
```

از نوع A است، حاوی جواب نیست

-5

```

Answers
  > pwnable.kr: type A, class IN, addr 128.61.240.205
Authoritative nameservers
  > pwnable.kr: type NS, class IN, ns ns4.whoisdomain.kr
  > pwnable.kr: type NS, class IN, ns ns1.whoisdomain.kr
  > pwnable.kr: type NS, class IN, ns ns2.whoisdomain.kr
  > pwnable.kr: type NS, class IN, ns ns3.whoisdomain.kr
Additional records
  > ns1.whoisdomain.kr: type A, class IN, addr 115.85.182.35
  > ns2.whoisdomain.kr: type A, class IN, addr 49.50.165.188
  > ns3.whoisdomain.kr: type A, class IN, addr 110.45.166.139
  > ns4.whoisdomain.kr: type A, class IN, addr 219.251.156.134

```

-6

```

3 0.036695 192.168.1.101 128.61.240.205 TCP 66 14628 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

```

بله، آدرس 128.61.240.205 مطابقت دارد

-7

```

1 0.000000 192.168.1.101 192.168.1.1 DNS 70 Standard query 0x9fc5 A pwnable.kr
2 0.035754 192.168.1.1 192.168.1.101 DNS 234 0.0357540.. Standard query response 0x9fc5 A pwnable.kr A 128.61.240.205 NS ns4.whoisdomain.kr NS ns1.whoisdomain.kr
16 1.332842 192.168.1.101 192.168.1.1 DNS 80 Standard query 0x93f6 A fonts.googleapis.com
17 1.362674 192.168.1.101 192.168.1.101 DNS 263 0.0306320.. Standard query response 0x93f6 A fonts.googleapis.com A 142.250.187.170 NS ns4.google.com NS ns1.google.co
18 1.369225 192.168.1.101 192.168.1.1 DNS 77 Standard query 0x7584 A fonts.gstatic.com
19 1.400000 192.168.1.101 192.168.1.101 DNS 289 0.0307750.. Standard query response 0x7584 A fonts.gstatic.com CNAME gstaticadssl.l.google.com A 172.217.169.99 NS ns1
21 1.407459 192.168.1.101 192.168.1.1 DNS 75 Standard query 0x874a A www.youtube.com
22 1.419389 192.168.1.101 192.168.1.1 DNS 71 Standard query 0xd852 A ctftime.org
23 1.421791 192.168.1.101 192.168.1.1 DNS 76 Standard query 0x4c8e A en.wikipedia.org
24 1.421997 192.168.1.101 192.168.1.1 DNS 71 Standard query 0xb8b4 A legitbs.net
26 1.448741 192.168.1.1 192.168.1.101 DNS 346 0.0412820.. Standard query response 0x874a A www.youtube.com A 10.10.34.35 NS ns1.google.com NS ns4.google.com NS ns2.
27 1.453750 192.168.1.1 192.168.1.101 DNS 223 0.0319590.. Standard query response 0x4c8e A en.wikipedia.org CNAME dyna.wikimedia.org A 91.198.174.192 NS ns1.wikimec
32 1.471635 192.168.1.101 192.168.1.1 DNS 72 Standard query 0x2ae7 A codegate.org
33 1.536300 192.168.1.1 192.168.1.101 DNS 158 0.1169110.. Standard query response 0xd852 A ctftime.org A 188.114.97.7 A 188.114.96.7 NS june.ns.cloudflare.com NS rj
34 1.538129 192.168.1.1 192.168.1.101 DNS 190 0.1161320.. Standard query response 0xb8b4 A legitbs.net A 185.199.111.153 A 185.199.108.153 A 185.199.109.153 A 185.1
35 1.539710 192.168.1.101 192.168.1.1 DNS 83 Standard query 0xb8df A ghostintheshellcode.com
36 1.540936 192.168.1.101 192.168.1.1 DNS 68 Standard query 0x873b A gts3.org
42 1.569566 192.168.1.1 192.168.1.101 DNS 163 0.0298560.. Standard query response 0xb8df A ghostintheshellcode.com A 69.163.155.47 NS ns3.dreamhost.com NS ns1.dream
43 1.571471 192.168.1.101 192.168.1.1 DNS 76 Standard query 0xc835 A io.netgarage.org
45 1.602546 192.168.1.1 192.168.1.101 DNS 141 0.0310750.. Standard query response 0xc835 A io.netgarage.org A 138.201.80.190 NS ns5.kasserver.com NS ns6.kasserver.c
46 1.604521 192.168.1.101 192.168.1.1 DNS 72 Standard query 0xbfc7 A w3challs.com
47 1.651529 192.168.1.1 192.168.1.101 DNS 285 0.1105930.. Standard query response 0x073b A gts3.org A 128.61.240.25 NS ns-1531.awsdns-63.org NS ns-1983.awsdns-55.cc
51 1.728387 192.168.1.1 192.168.1.101 DNS 134 0.1238660.. Standard query response 0x6fc7 A w3challs.com A 51.15.18.162 NS dns15.ovh.net NS ns15.ovh.net
52 1.859616 192.168.1.1 192.168.1.101 DNS 171 0.3879810.. Standard query response 0x2ae7 A codegate.org A 1.234.47.104 NS ns1.kshosting.co.kr NS ns2.kshosting.co.kr

```

## 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