

1. از طریق دستور $A - nmap iut.ac.ir$ سایت اول را چک کردم:

```
mohammad@mohammad-K556UQ: ~$ nmap iut.ac.ir -A
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-10 17:03 +0430
Nmap scan report for iut.ac.ir (176.101.52.155)
Host is up (0.058s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
|_ http-server-header: ASPA-WAF
|_ http-title: Did not follow redirect to https://iut.ac.ir/
443/tcp    open  ssl/http nginx (reverse proxy)
|_ http-generator: Drupal 8 (https://www.drupal.org)
|_ http-server-header: ASPA-WAF
|_ http-title: \x08\xAF\x08\xA7\x09\x08\x04\x0A\xAF\x08\xA7\x09\x87 \x08\xB5\x09\x08\x09\x08\xA4\x08\xB8 \x08\xA7\x08\xB5\x09\x81\x09\x08\xA7\x09\x86 | \x0A\x08\x09\x87\x09\x84\x08\xB3\x08\xA4\x09\x88
\x09\x86 \x08\xAF\x08\xA7\x09\x86...
ssl-cert: Subject: commonName=iut.ac.ir/countryName=IR
Subject Alternative Name: DNS:*.iut.ac.ir, DNS:iut.ac.ir
Not valid before: 2020-03-01T04:29:53
Not valid after: 2022-03-01T04:29:53
_tls-date: TLS randomness does not represent time
tls-alpn:
|_ http/1.1
|_ http/1.1
|_ http/1.1
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 68.88 seconds
```

از طریق دستور $A - nmap mit.edu$ سایت دوم را چک کردم:

```
mohammad@mohammad-K556UQ: ~$ nmap mit.edu -A
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-10 17:07 +0430
Nmap scan report for mit.edu (104.05.40.223)
Host is up (0.14s latency).
Other addresses for mit.edu (not scanned): 2a02:26f0:3400:189::255e 2a02:26f0:3400:19b::255e
DNS record for 104.05.40.223: a104-05-40-223.deploy.static.akamaitechnologies.com
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
|_ http-title: Did not follow redirect to http://web.mit.edu/
443/tcp    open  ssl/http AkamaiGhost (Akamai's HTTP Acceleration/Mirror service)
|_ http-title: Did not follow redirect to https://web.mit.edu/
ssl-cert: Subject: commonName=web.mit.edu/organizationName=Massachusetts Institute of Technology/stateOrProvinceName=Massachusetts/countryName=US
Subject Alternative Name: DNS:web.mit.edu, DNS:mit.mit.edu, DNS:glving.mit.edu, DNS:news.mit.edu, DNS:emergency-dev.mit.edu, DNS:www.mit, DNS:events-static.mit.edu, DNS:emergency.mit.edu, DNS:www-mit.mit.edu,
DNS:www-mit.edu, DNS:img.mit.edu, DNS:www-cert.mit.edu, DNS:swartz-report.mit.edu, DNS:www.mit.edu, DNS:swartz-documents.mit.edu, DNS:web-forms.mit.edu, DNS:w.mit.edu, DNS:alum.mit.edu, DNS:alum-dev.mit.edu, DN
S:www-web.mit.edu, DNS:newsoffice.mit.edu, DNS:web.mit, DNS:web-cert.mit.edu, DNS:mit.edu, DNS:www-newsoffice.mit.edu, DNS:w3.mit.edu, DNS:betterworld.mit.edu, DNS:emergency.mit.net
Not valid before: 2019-07-01T00:00:00
Not valid after: 2020-09-29T12:00:00
_tls-date: TLS randomness does not represent time
tls-alpn:
|_ http/1.1
|_ http/1.1
|_ http/1.0
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.91 seconds
```

2. از سایت iut اطلاعات بیشتر بدست آمد.

شاید دلیل اینکه از سایت iut اطلاعات بیشتری را کسب میکنیم این باشد که دانشگاه از سیستم های این سورس برای پیاده سازی ساختار خود استفاده کرده اما در mit تمام این ها به شرکت های بیرونی سپرده شده.

3. سیستم هایی که ipv6 را پشتیبانی میکنند لازم است که ipv4 را هم پشتیبانی کنند در نتیجه ممکن است در نتیجه این حالت مشکلاتی برای ids/ips ایجاد شود که ممکن است بدلیل فضای گسترده ipv6 یا ساختار مازولار ipv6 ایجاد شود همچنین در حالت کلی وقتی کانکشن ایجاد شود سیستم حمله کننده پس از دریافت بسته syn ack اگر بسته drop را ارسال کند از کانکشن خارج شده و ids ips هم لاگ نمیکند.

4. معمولاً بسته های udp مربوط به dns از فایروال به راحتی عبور میکنند. میتوان از این ضعف برای دور زدن فایروال استفاده کرد. در این حالت میتوان با قرار دادن اطلاعات در dns request ارسال را به dns server فرستاد و ان هم درخواست ما را به سرور مورد نظر ارسال میکند.