

«به نام ایزد یکتا»



گزارش آزمایش چهارم درس شبکه‌های کامپیوتر

استاد: مهندس مشایخ

تهیه کننده: بردیا اردکانیان

۹۸۳۱۰۷۲

سوال (1)

نام و آدرس را در این قسمت مشاهده می‌کنیم

```
domain: soft98.ir
ascii: soft98.ir
remarks: (Domain Holder) alireza bagheri
remarks: (Domain Holder Address) Shariati-Khiaban Mirzapour-Mehr 3 Gharbi-Pelak 20, Tehran, Tehran, IR
holder-c: ab590-irnic
admin-c: ab590-irnic
```

سوال (2)

این سایت دو نیم سرور دارد






```
nserver: ir1.hostdl.com
nserver: ir2.hostdl.com
```

سوال (3)


رکوردها را به ترتیب توضیح می‌دهیم:

رکورد NS: این رکوردها مشخص می‌کنند که در ادامه‌ی فرآیند ترجمه نام دامنه به آدرس ای پی باید به کدام name server های معتبر درخواست بفرستیم.

Parent Nameserver Tests




Status	Test Case	Information
	NS records listed at parent servers	Nameserver records returned by the parent servers are: ir1.hostdl.com. [NO GLUE] [TTL=1440] ir2.hostdl.com. [NO GLUE] [TTL=1440] This information was kindly provided by a.nic.ir.
	Domain listed at parent servers	Good! The parent servers have information on your domain. Some other domains (like .co.us) do not have a DNS zone at the parent servers.
	NS records listed at parent servers	Good! The parent servers have your NS records listed. If they didn't, people wouldn't be able to find your domain!
	Parent servers return glue	OK. The TLD of your domain (ir) differs from that of your nameservers (com). As such, the parent servers are not required to send glue.
	A record for each NS at parent	OK. The parent servers don't need to have A records for your nameservers since the TLD of your domain (ir) differs from that of your nameservers (com).

Local Nameserver Tests

Status	Test Case	Information
	NS records at your local servers	NS records retrieved from your local nameservers were: ir1.hostdl.com. [NO GLUE] [TTL=86400] ir2.hostdl.com. [NO GLUE] [TTL=86400]
		Oops! Your local nameservers don't return IP addresses (glue) along with your NS records! This isn't a fatal error but means an extra

رکورد A: اين رکورد مخفف Address شامل ادرس ای پی درخواستی است.











WWW Record Tests

Status	Test Case	Information
	WWW record	www.soft98.ir A records are: www.soft98.ir. CNAME soft98.ir. [TTL=14400] soft98.ir. A 79.127.127.35 [TTL=14400]
	WWW A record has public IP	Good! The IP address(es) of the A records returned for your WWW record have public IP addresses.
	WWW CNAME lookup	Good! You have a CNAME entry for your WWW record which also returns the associated A record! This saves an extra lookup which would delay loading times for your site.

رکورد TXT: مخفف text است. رکوردي است که در آن اطلاعات اضافي ميشود که توسط domain در رکوردهای DNS مربوط به آن گذاشته می شود و می تواند شامل یک سری دستورالعملها برای انسان ها یا ماشین ها باشد یا برای شناسایی قابل اطمینان بودن منبع ایمیل مورد استفاده قرار گیرد. که البته در این پویش چنین رکوردي یافت نشد.



رکورد MX: استفاده از این رکورد برای مشخص کردن serve mail ایست که مسئول دریافت ایمیل های این دامنه می باشد.

Mail eXchanger (MX) Tests

Status	Test Case	Information
	MX Records	Your Mail eXchanger (MX) records are: 0 soft98.ir. [TTL=14400]
	All nameservers have same MX records	Good! All of your nameservers have the same MX records.
	All MX records contain valid hostnames	Good! All of your MX entries have valid hostnames (e.g. are not IP's or invalid domain names).
	All MX records use public IP addresses	Good! All of your MX entries have public IP addresses.
	MX record is not a CNAME/alias	Good! When querying for your MX records we did not receive a CNAME record as a result.
	MX A records are not CNAME's	Good! No CNAME records are present for your MX A records.
	Number of MX records	Oops! You only have one MX record! In the event that this mail server is down, you could potentially lose mail! It is recommended to have two or more MX records (and hence mail servers) if you want uninterrupted mail functionality.
	Duplicate MX A records	Good! No two MX records resolve to the same IP address.
	Differing MX A records	Good! You have no different IP's for your MX A records than the DNS server that is authoritative for that hostname.
	MX records have reverse DNS entries	Good! All your MX IP addresses have reverse DNS entries. The reverse entries returned were: 35.127.127.79.in-addr.arpa <--> hosted-by.hostdl.com.asiatech.ir.

سوال 4

برای این کار باید رکوردهای MX را بررسی کنیم که در تصویر زیر می‌بینیم. آدرس server mail دانشگاه عبارت است از asg.aut.ac.ir و آدرس ای پی آن هم 185.211.88.20 می‌باشد.

Status	Test Case	Information
	MX Records	Your Mail eXchanger (MX) records are: 5 asg.aut.ac.ir. [TTL=3600]
	MX records have reverse DNS entries	Good! All your MX IP addresses have reverse DNS entries. The reverse entries returned were: 20.88.211.185.in-addr.arpa <--> asg525.aut.ac.ir.

سوال 5

بخشی از نتایج در تصویر قابل مشاهده است

*نام چند مورد از وبسایت‌های دیگر در زیر قابل مشاهده است. و آدرس IP چند مورد نیز مشخص شده که همه با هم برابر و برابر Cert.it IP Addr. است.

به این پدیده hosting virtual می‌گویند. دستهبندی‌های آن میتواند بر حسب IP، نام و یا پورت باشد. که در آن چند آدرس دامنه توسط یک سرور همدل می‌شوند.

Reverse IP results for cert.ir (185.143.233.41, 185.143.234.41)

=====

Domain	Last Resolved Date
7peykar.ir	2021-06-22
92762.ir	2021-06-22
aadak.ir	2021-06-21
abrmarketing.net	2021-06-22
aghlovahy.com	2021-06-22
agoracomplex.com	2021-06-22
axhome.ir	2021-06-22
bankbattery.co	2021-06-22
bemanbespar.ir	2021-06-16
bimehnama.com	2021-06-22
binazirshop.com	2021-06-22
bizilyapp.com	2021-06-22
bodyspinners.com	2021-06-22
bornosmode.com	2021-06-22
brifenews.ir	2021-06-09

[185.143.234.41]

[185.143.234.41]

سوال (6)

اتفاقي شبيه به multiplexing در اينجا رخ مي دهد multiplexing. در حقيقت در لايه انتقال است ولي اينجا بايد در لايه کاربرد انجام شود. هر بسته با توجه به هدر http آن به دامنه مربوطه تحويل داده مي شود.

سوال (7)

```
-p proto    Shows connections for the protocol specified by proto; proto
            may be any of: TCP, UDP, TCPv6, or UDPv6.  If used with the -s
            option to display per-protocol statistics, proto may be any of:
            IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
-q          Displays all connections, listening ports, and bound
            nonlistening TCP ports. Bound nonlistening ports may or may not
            be associated with an active connection.
```

با استفاده از دستور netstat ؟ مي توانيم دستورات netstat را مشاهده كنيم.

براي مشاهده كردن پورت هاي اختصاص داده شده به پروتكل tcp و udp به ترتيب netstat -p tcp و netstat -p udp را وارد مي كنيم. دستور netstat -q نيز تمامي پورت هاي tcp را اعم از وضعيت ليست مي كند.

سوال (8)

دستور netstat -a تمامي پورتهاي فعال و ارتباطات باز را نمايش مي دهد و netstat -n آنها را به صورت عددي نمايش مي دهد.

C:\Users\ASUS>netstat -n				C:\Users\ASUS>netstat -a			
Active Connections				Active Connections			
Proto	Local Address	Foreign Address	State	Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:1939	127.0.0.1:1940	ESTABLISHED	TCP	0.0.0.0:135	DESKTOP-TDV08C4:0	LISTENING
TCP	127.0.0.1:1940	127.0.0.1:1939	ESTABLISHED	TCP	0.0.0.0:445	DESKTOP-TDV08C4:0	LISTENING
TCP	127.0.0.1:1963	127.0.0.1:1964	ESTABLISHED	TCP	0.0.0.0:1309	DESKTOP-TDV08C4:0	LISTENING
TCP	127.0.0.1:1964	127.0.0.1:1963	ESTABLISHED	TCP	0.0.0.0:1536	DESKTOP-TDV08C4:0	LISTENING
TCP	127.0.0.1:1970	127.0.0.1:1971	ESTABLISHED	TCP	0.0.0.0:1537	DESKTOP-TDV08C4:0	LISTENING
TCP	127.0.0.1:1971	127.0.0.1:1970	ESTABLISHED	TCP	0.0.0.0:1538	DESKTOP-TDV08C4:0	LISTENING
TCP	127.0.0.1:1982	127.0.0.1:1983	ESTABLISHED	TCP	0.0.0.0:1539	DESKTOP-TDV08C4:0	LISTENING
TCP	127.0.0.1:1983	127.0.0.1:1982	ESTABLISHED	TCP	0.0.0.0:1541	DESKTOP-TDV08C4:0	LISTENING
TCP	127.0.0.1:1986	127.0.0.1:1987	ESTABLISHED	TCP	0.0.0.0:1542	DESKTOP-TDV08C4:0	LISTENING
TCP	127.0.0.1:1987	127.0.0.1:1986	ESTABLISHED	TCP	0.0.0.0:5040	DESKTOP-TDV08C4:0	LISTENING
TCP	127.0.0.1:1991	127.0.0.1:1992	ESTABLISHED	TCP	0.0.0.0:13337	DESKTOP-TDV08C4:0	LISTENING
TCP	127.0.0.1:1992	127.0.0.1:1991	ESTABLISHED	TCP	127.0.0.1:1001	DESKTOP-TDV08C4:0	LISTENING
TCP	127.0.0.1:2264	127.0.0.1:2265	ESTABLISHED	TCP	127.0.0.1:1540	DESKTOP-TDV08C4:0	LISTENING
TCP	127.0.0.1:2265	127.0.0.1:2264	ESTABLISHED	TCP	127.0.0.1:1543	DESKTOP-TDV08C4:0	LISTENING
TCP	127.0.0.1:2299	127.0.0.1:2300	ESTABLISHED	TCP	127.0.0.1:1939	pingplotter:1940	ESTABLISHED
				TCP	127.0.0.1:1940	pingplotter:1939	ESTABLISHED
				TCP	127.0.0.1:1963	pingplotter:1964	ESTABLISHED

سوال 9

چون قالب درخواستهای HTTP به این صورت است که در انتهای هر خط `/r/n` قرار دارد که معنی آن استفاده از یک `enter` است. و در انتهای درخواست `http` نیز باید با استفاده از یک `enter` پیام را به پایان برسانیم. (قالب این دستورات در ادامه نشان داده شده است)

```
GET /index.html HTTP/1.1\r\n
```

```
Host: [host-name]\r\n
```

```
...
```

```
\r\n
```

سوال 10

پاسخ درخواست به صورت زیر است و با ارور 301 مواجه می‌شویم که به معنی `moved permanently` است و با بررسی این پاسخ مشخص است که آدرس جدیدی که دامنه به آن منتقل شده است <https://aut.ac.ir:443> می‌باشد.

```
C:\Users\ASUS>ncat -C aut.ac.ir 80
GET / HTTP/1.1
Host: aut.ac.ir

HTTP/1.1 301 Moved Permanently
Date: Wed, 23 Jun 2021 17:36:36 GMT
Server: Apache
Location: https://aut.ac.ir:443/
Content-Length: 230
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://aut.ac.ir:443/">here</a>.</p>
</body></html>
```


امكان استفاده از 80 aut.ac.ir -v ncat نمي توان استفاده كرد.

ip.addr == 185.211.88.131						
No.	Time	Source	Destination	Protocol	Length	Info
373	11.346117	192.168.1.103	185.211.88.131	TCP	66	14913 → 80 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
374	11.346428	192.168.1.103	185.211.88.131	TCP	66	1027 → 80 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
375	11.377200	185.211.88.131	192.168.1.103	TCP	62	80 → 14913 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1390 SACK_PERM=1
376	11.377262	192.168.1.103	185.211.88.131	TCP	54	14913 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
377	11.377624	192.168.1.103	185.211.88.131	HTTP	668	GET / HTTP/1.1
378	11.378506	185.211.88.131	192.168.1.103	TCP	62	80 → 1027 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1390 SACK_PERM=1
379	11.378568	192.168.1.103	185.211.88.131	TCP	54	1027 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
380	11.420135	185.211.88.131	192.168.1.103	TCP	60	80 → 14913 [ACK] Seq=1 Ack=615 Win=30086 Len=0
381	11.421719	185.211.88.131	192.168.1.103	HTTP	528	HTTP/1.1 301 Moved Permanently (text/html)
382	11.423898	192.168.1.103	185.211.88.131	TCP	66	32164 → 443 [SYN] Seq=0 Win=17520 Len=0 MSS=1460 WS=256 SACK_PERM=1
383	11.454012	185.211.88.131	192.168.1.103	TCP	62	443 → 32164 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1390 SACK_PERM=1
384	11.454172	192.168.1.103	185.211.88.131	TCP	54	32164 → 443 [ACK] Seq=1 Ack=1 Win=17520 Len=0
385	11.454770	192.168.1.103	185.211.88.131	TLSv1.2	571	Client Hello
386	11.462327	192.168.1.103	185.211.88.131	TCP	54	14913 → 80 [ACK] Seq=615 Ack=475 Win=17046 Len=0
387	11.495781	185.211.88.131	192.168.1.103	TCP	60	443 → 32164 [ACK] Seq=1 Ack=518 Win=30016 Len=0
391	11.509858	185.211.88.131	192.168.1.103	TLSv1.2	1444	Server Hello
392	11.511241	185.211.88.131	192.168.1.103	TCP	622	[TCP Previous segment not captured] 443 → 32164 [PSH, ACK] Seq=2781 Ack=518
393	11.511331	192.168.1.103	185.211.88.131	TCP	66	32164 → 443 [ACK] Seq=518 Ack=1391 Win=17520 Len=0 SLE=2781 SRE=3349
394	11.514258	185.211.88.131	192.168.1.103	TCP	1444	[TCP Out-Of-Order] 443 → 32164 [ACK] Seq=1391 Ack=518 Win=30016 Len=1390
395	11.514370	192.168.1.103	185.211.88.131	TCP	54	32164 → 443 [ACK] Seq=518 Ack=3349 Win=17520 Len=0
396	11.530274	192.168.1.103	185.211.88.131	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
397	11.530776	192.168.1.103	185.211.88.131	TLSv1.2	886	Application Data
399	11.565680	185.211.88.131	192.168.1.103	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
400	11.606770	192.168.1.103	185.211.88.131	TCP	54	32164 → 443 [ACK] Seq=1476 Ack=3400 Win=17469 Len=0
401	11.617279	185.211.88.131	192.168.1.103	TCP	60	443 → 32164 [ACK] Seq=3400 Ack=1476 Win=31616 Len=0
402	11.827471	185.211.88.131	192.168.1.103	TLSv1.2	364	[TCP Previous segment not captured], Ignored Unknown Record
403	11.827562	192.168.1.103	185.211.88.131	TCP	66	[TCP Dup ACK 400#1] 32164 → 443 [ACK] Seq=1476 Ack=3400 Win=17469 Len=0 SLE
404	11.830165	185.211.88.131	192.168.1.103	TCP	1444	[TCP Out-Of-Order] 443 → 32164 [ACK] Seq=3400 Ack=1476 Win=31616 Len=1390
405	11.830289	192.168.1.103	185.211.88.131	TCP	54	32164 → 443 [ACK] Seq=1476 Ack=5100 Win=17520 Len=0
406	11.834968	185.211.88.131	192.168.1.103	TLSv1.2	1444	[TCP Previous segment not captured], Ignored Unknown Record
> Frame 381: 528 bytes on wire (4224 bits), 528 bytes captured (4224 bits) on interface \Device\NPF_{06D8CCB2-7CC6-46ED-9FEA-E154E3CDD55D}, id 0 > Ethernet II, Src: Tp-LinkT_f2:55:60 (18:a6:f7:f2:55:60), Dst: AzureWav_1e:36:59 (80:c5:f2:1e:36:59) > Internet Protocol Version 4, Src: 185.211.88.131, Dst: 192.168.1.103 > Transmission Control Protocol, Src Port: 80, Dst Port: 14913, Seq: 1, Ack: 615, Len: 474 Source Port: 80 Destination Port: 14913 [Stream index: 41] [TCP Segment Len: 474] Sequence Number: 1 (relative sequence number)						

تصديق حرف بالا

سوال 11

مقادير keep-alive در ورژن HTTP 1.1 به صورت ديڤالت براي يك اتصال persistent تنظيم مي شود. ما هم چون مقدارش را نفرستاديم به صورت persistent مي باشد.

سوال 12

با ورود اين دستور، هرگاه به پورت 16000 درخواستي فرستاده شود، cmd اجرا خواهد شد. آدرس IP بايد شده 0.0.0.0 است.

```
C:\Users\ASUS>ncat -v -l -p 16000 -e c:\Windows\System32\cmd.exe
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::16000
Ncat: Listening on 0.0.0.0:16000
```

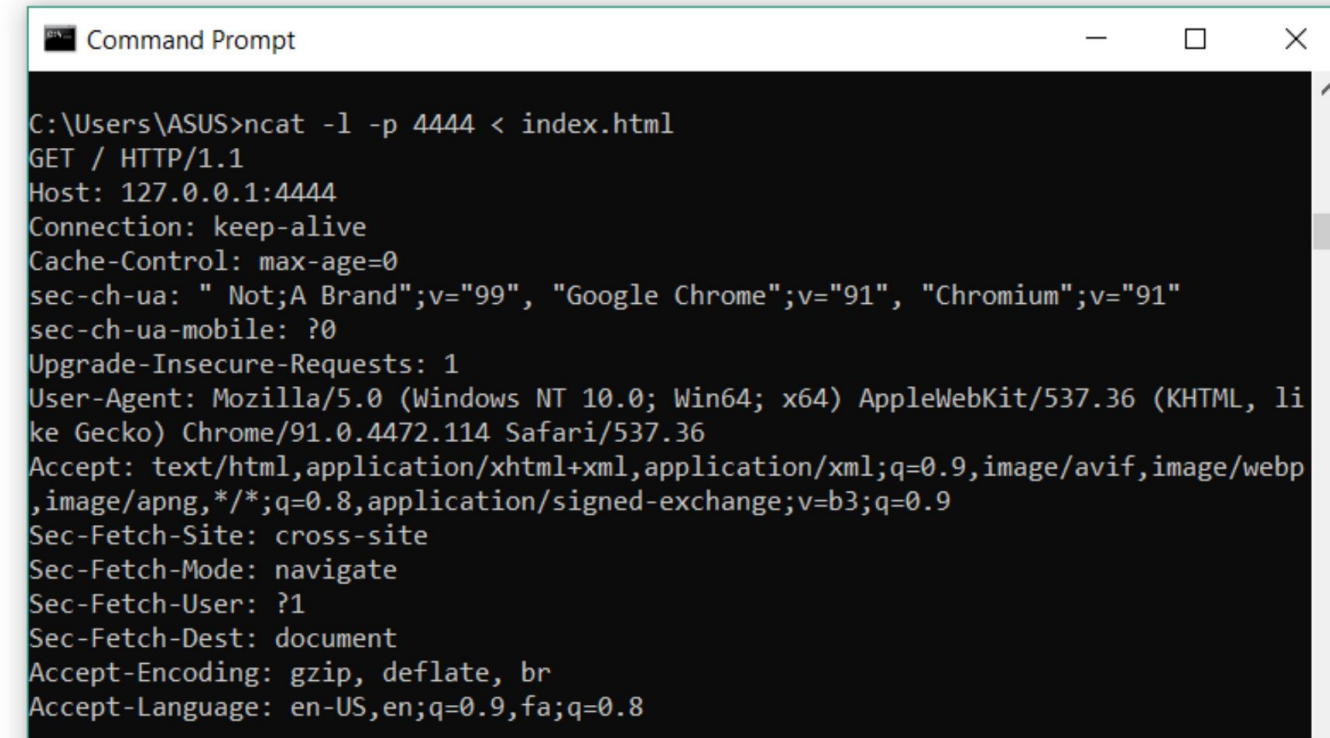
دستور netstat -abn :

```
Can not obtain ownership information
TCP    [::]:16000      [::]:0          LISTENING
```

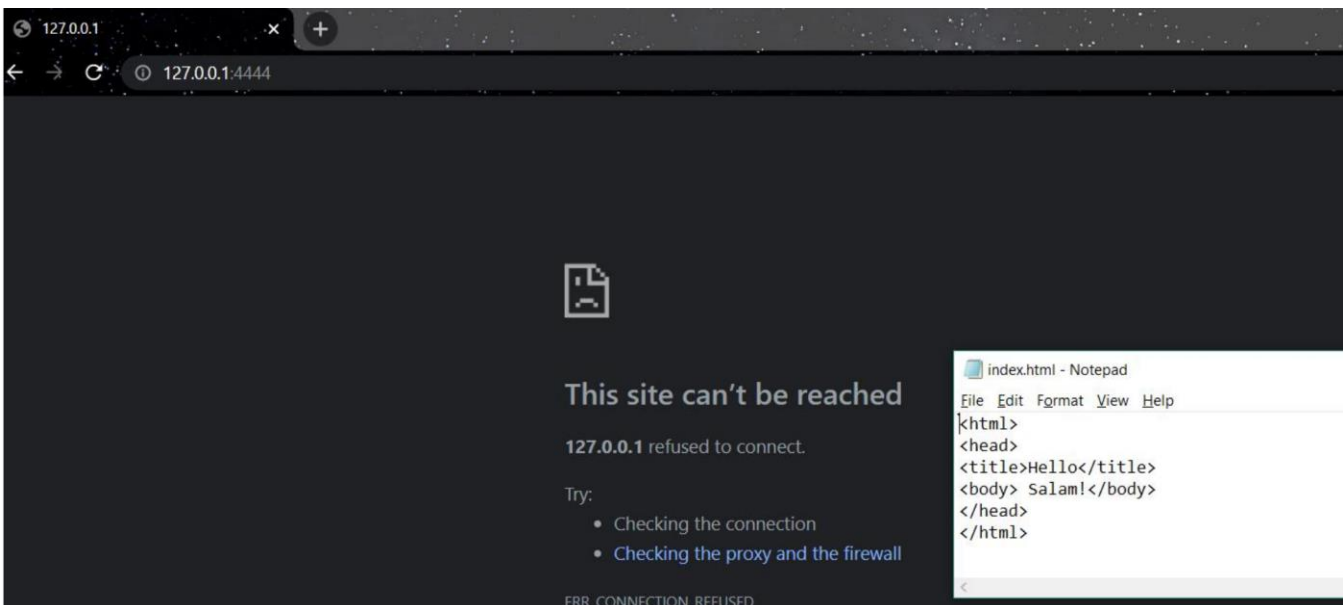
سوال 13



Salam!



بعد:



دليل وجود خط اول آن است كه بعد از اينكه درخواست http براي اين سرور ارسال شد، اين سرور در پاسخي كه براي كالينت ارسال مي كند ابتدا در يك خط status به درخواست http پاسخ مي دهد كه وجود اين خط در پاسخهاي http الزامي است در حالي كه هدرهاي بعد از آن اختياري هستند و در انتهاي خطوط مربوط به هدر يك enter اضافي مي گذاريم كه اتمام هدر http را نشان مي دهد و در سوال 9 نيز به آن اشاره كرديم كه اين enter نهايي هم اجباري است و در نهايت data مورد درخواست کاربر كه يك فايل html است را قرار مي دهيم.

سوال 14

اطلاعات سيستم عامل سرور:

Device type: WAP|phone
Running: Linux 2.4.X|2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:sonyericsson:u8i_vivaz
OS details: Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone

سوال 15

پورت هاي باز سرور:

Hosts	Services	Nmap Output	Ports / Hosts	Topology	Host Details	Scans
Service		Hostname	Port	Protocol	State	Version
tcpwrapped		aut.ac.ir (185.211.88.131)	443	tcp	open	
		aut.ac.ir (185.211.88.131)	80	tcp	open	

سوال 16

سرويس tcpwrapperd در اين پورت ارايه مي شود. پورت 443 نيز بزي secure shell SSL مي باشد.