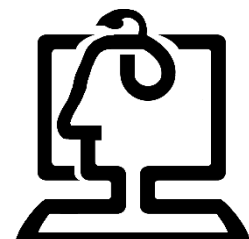




دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

فرم گزارش کار آزمایشگاه شبکه



دانشکده مهندسی کامپیوتر

نام و نام خانوادگی	حسین تاتار	شماره دانشجویی	40133014	نام و شماره آزمایش	-6 کار با کاربردهای Web، DNS، سوکت و پویش سرویس ها
هدف آزمایش	در این آزمایش قصد داریم با تعدادی از ابزارهای شبکه که به وسیله آن می توانیم در کاربرد های DNS، Web به عنوان سرویس گیرنده استفاده شوند، آشنا شویم.				
ابزارهای مورد نیاز	کامپیوتر شخصی با سیستم عامل ویندوز 7 یا بالاتر برای هرگروه برنامه Nmap نسخه 7.7 به بالا برنامه Wireshark نسخه 2.4 به بالا				
شرح آزمایش	<p>سوال 1: در قسمت Domain / IP Whois رفته و آدرس soft98.ir را وارد نمایید.</p> <p>الف) نام و اطلاعات فردی که دامنه به اسم ثبت شده است چیست؟</p> <p>جواب: در خروجی WHOIS مشاهده می شود که اطلاعات مالک دامنه مخفی (hidden) شده است. این معمولاً به این معناست که ثبت کننده از سرویس «حریم خصوصی دامنه» استفاده کرده است. بنابراین، اطلاعاتی مانند نام، ایمیل یا آدرس فرد/شرکت در اینجا قابل مشاهده نیست.</p> <p>ب) آدرس name server آن چیست؟</p> <p>جواب: بر اساس خروجی WHOIS، name server های دامنه soft98.ir عبارتند از:</p> <ul style="list-style-type: none"> ir1.hostdl.com ir2.hostdl.com 				

سوال 2: در وبسایت به قسمت DNS Report رفته و آدرس soft98.ir را وارد نمایید
الف) رکوردهای A، NS، MX را مشخص کنید. هر یک از این رکوردها چه چیزی را مشخص میکنند؟
جواب:

رکورد A (Address Record):

- آدرس IPv4 مربوط به دامنه را مشخص می کند.
- مقدار رکورد A برای www.soft98.ir دارای یک آدرس IP عمومی است، اگرچه مقدار دقیق IP ذکر نشده.

رکورد NS (Name Server Record):



- سرورهای DNS مسئول برای دامنه را مشخص می کند.
- مقدار رکوردها: ir1.hostdl.com - ir2.hostdl.com

رکورد MX (Mail Exchange Record):


- این رکورد مشخص می کند که سرورهای ایمیل دامنه کدامند. مقدار 0 نشان دهنده اولویت (Priority) است.
- مقدار رکوردها: 0 soft98.ir (با TTL=14400 ثانیه یا ۴ ساعت).


رکورد TXT (Text Record):


- اطلاعات متنی دلخواهی را که می تواند برای اهداف مختلفی استفاده شود، مشخص می کند.
- چون اطلاعات هویتی فرد مخفی است بنابراین این رکورد مشخص نیست.

STATUS	TEST CASE	INFORMATION
		Nameserver records returned by the parent servers are:
	NS records listed at parent servers	ir2.hostdl.com. [NO GLUE] [TTL=1440] ir1.hostdl.com. [NO GLUE] [TTL=1440] This information was kindly provided by d.nic.ir.
	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 retrieved from your local nameservers were:
	NS records at your local servers	ir1.hostdl.com. [NO GLUE] [TTL=86400] ir2.hostdl.com. [NO GLUE] [TTL=86400]

STATUS	TEST CASE	INFORMATION
		Your Mail eXchanger (MX) records are:
	MX Records	0 soft98.ir. [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.
---	----------------------------	--

ب) در قسمت DNS Report با وارد کردن دامنه ی دانشگاه (aut.ac.ir) mail server را مشخص کنید. آیا آدرس IP آن را میتوانید مشخص کنید؟

جواب: بر اساس گزارش DNS ارائه شده، رکوردهای MX (Mail Exchange) برای دامنه aut.ac.ir به صورت زیر هستند:

- mx01.aut.ac.ir با Reverse DNS معتبر: 17.90.211.185.in-addr.arpa
- mx02.aut.ac.ir با Reverse DNS معتبر: 18.90.211.185.in-addr.arpa

این رکوردها نشان می دهند که سرورهای ایمیل دانشگاه دو گانه (برای افزونگی) تنظیم شده اند.
با توجه به ساختار Reverse DNS در گزارش، می توان آدرس IP سرورهای ایمیل را استخراج کرد:

- رکورد A برای زیردامنه `www`
- مقدار رکورد: `www.aut.ac.ir. A 185.211.88.131` (با `TTL=3600` ثانیه).
- این رکورد آدرس IP وب سرور دانشگاه (`185.211.88.131`) را مشخص می کند.

MX records have reverse DNS entries

Good! All your MX IP addresses have reverse DNS entries. The reverse entries returned were:

17.90.211.185.in-addr.arpa <--> mx01.aut.ac.ir.

18.90.211.185.in-addr.arpa <--> mx02.aut.ac.ir.

WWW Record Tests

STATUS	TEST CASE	INFORMATION
	WWW record	<p>www.aut.ac.ir A records are:</p> <p>www.aut.ac.ir. A 185.211.88.131 [TTL=3600]</p>

سوال 3: در قسمت `Lookup IP Reverse` آدرس `farsnews.ir` را وارد کنید.

الف) چه وبسایت های دیگری بر روی همین سرور قرار دارند (آدرس IP آن ها را با آدرس IP سایت `farsnews.ir` مقایسه کنید)؟

جواب: بر اساس گزارش `Reverse IP Lookup` برای آدرس `45.157.244.26` مربوط به `farsnews.ir`، دامنه های زیر روی این IP میزبانی می شوند:

DOMAIN NAME	LAST RESOLVED	آدرس IP سرور
FARSNEWS.IR	2025-04-09	45.157.244.26
FARS.PRESS	2025-01-03	45.157.244.26

مقایسه آدرس IP ها:

- هر دو دامنه `farsnews.ir` و `fars.press` از یک سرور با IP ثابت (`45.157.244.26`) استفاده می کنند.
- این نشان می دهد که احتمالاً:
 - هر دو متعلق به یک سازمان هستند (مثلاً خبرگزاری فارس).
 - یا از خدمات میزبانی مشترک (`Shared Hosting`) استفاده می کنند.

Reverse IP Lookup

Find all domains hosted on a given IP address.

HTMLJSON

Reverse IP results for `farsnews.ir` (`45.157.244.26`)

There are 2 domains hosted on this server.
The complete listing of these is below:

DOMAIN NAME	LAST RESOLVED
fars.press	2025-01-03
farsnews.ir	2025-04-09

ب) به نظر شما سرور چگونه وب سرور درخواست شده را تشخیص می دهد ؟

آیا این روش نیز نوعی `Multiplexing` است؟

جواب:

- روش اصلی تشخیص دامنه Name-Based Virtual Hosting است که با استفاده از هدر Host کار می‌کند.
- هنگامی که درخواست به سرور می‌رسد، سرآیند Host آن بررسی می‌شود که حاوی نام دامنه است و از آن استفاده می‌کند تا درخواست را به root directory سایت مورد نظر هدایت کند.
- این روش شکلی از Multiplexing محسوب می‌شود، اما در لایه اپلیکیشن (نه لایه انتقال).

سوال 4: به وبسایت زیر بروید:

<https://simplifiedns.com/lookup-dg>

در این وبسایت آدرس aut.ac.ir وارد کرده و درخواست ها و پاسخ های دریافت شده را بررسی کنید.

جواب:

۱. مرحله اول: ارتباط با روت سرورها (Root Servers)
 - سیستم با j.root-servers.net آدرس 192.58.128.30 ارتباط برقرار می‌کند.
 - پاسخ دریافتی DNS: سرورهای مسئول دامنه‌های .ir. معرفی می‌شوند:
 - a.nic.ir (193.189.123.2)
 - b.nic.ir (193.189.122.83)
 - c.nic.ir (45.93.171.206)
 - d.nic.ir (194.225.70.83)
۲. مرحله دوم: ارتباط با سرورهای دامنه .ir
 - سیستم با a.nic.ir آدرس (193.189.123.2) ارتباط برقرار می‌کند.
 - پاسخ دریافتی DNS: سرورهای مسئول دامنه aut.ac.ir معرفی می‌شوند:
 - ns1.aut.ac.ir (185.211.89.14)
 - ns2.aut.ac.ir (185.211.90.9)
 - ns3.aut.ac.ir (185.211.88.6)
۳. مرحله سوم: ارتباط با سرورهای دامنه aut.ac.ir
 - سیستم با ns2.aut.ac.ir آدرس (185.211.90.9) ارتباط برقرار می‌کند.
 - پاسخ دریافتی: رکورد A دامنه aut.ac.ir ارائه می‌شود:
 - aut.ac.ir = 185.211.88.131

Trace DNS Delegation

Tracing DNS delegation for "aut.ac.ir":

Loading root server list (static data):

```
-> a.root-servers.net (198.41.0.4)
-> b.root-servers.net (192.228.79.201)
-> c.root-servers.net (192.33.4.12)
-> d.root-servers.net (128.8.10.90)
-> e.root-servers.net (192.203.230.10)
-> f.root-servers.net (192.5.5.241)
-> g.root-servers.net (192.112.36.4)
-> h.root-servers.net (128.63.2.53)
-> i.root-servers.net (192.36.148.17)
-> j.root-servers.net (192.58.128.30)
-> k.root-servers.net (193.0.14.129)
-> l.root-servers.net (199.7.83.42)
-> m.root-servers.net (202.12.27.33)
```

Sending request to "j.root-servers.net" (192.58.128.30)

Received referral response - DNS servers for ".ir":

```
-> a.nic.ir (193.189.123.2)
-> b.nic.ir (193.189.122.83)
-> c.nic.ir (45.93.171.206)
```

Sending request to "j.root-servers.net" (192.58.128.30)

Received referral response - DNS servers for "ir":

-> a.nic.ir (193.189.123.2)
-> b.nic.ir (193.189.122.83)
-> c.nic.ir (45.93.171.206)
-> d.nic.ir (194.225.70.83)

Sending request to "a.nic.ir" (193.189.123.2)

Received referral response - DNS servers for "aut.ac.ir":

-> ns3.aut.ac.ir (185.211.88.6)
-> ns2.aut.ac.ir (185.211.90.9)
-> ns1.aut.ac.ir (185.211.89.14)

Sending request to "ns2.aut.ac.ir" (185.211.90.9)

Received authoritative (AA) response:

-> Answer: A-record for aut.ac.ir = 185.211.88.131

سوال 5: مشاهده و تخصیص پورت های لایه انتقال با استفاده از ابزار Netsta:

الف) برای لیست کردن برنامه هایی که در حال حاضر پورت های لایه انتقال را بر روی سیستم باز کرده اند، از چه دستور خط فرمانی استفاده می شود؟

جواب: برای لیست کردن برنامه هایی که در حال استفاده از پورت های لایه انتقال (TCP/UDP) هستند، می توان از دستور زیر در خط فرمان استفاده کرد:

netstat -nob

این دستور لیستی از تمام برنامه هایی که پورت های لایه انتقال را باز کرده اند همراه با نام دقیق برنامه نمایش می دهد. البته، این دستور نیاز به اجرا با دسترسی Administrator دارد.

```
C:\Windows\System32>netstat -nob
```

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	127.0.0.1:12017	127.0.0.1:60425	ESTABLISHED	15344
[msedge.exe]				
TCP	127.0.0.1:20817	127.0.0.1:60425	ESTABLISHED	12660
[chrome.exe]				
TCP	127.0.0.1:60425	127.0.0.1:12017	ESTABLISHED	7216
[Explorer.EXE]				
TCP	127.0.0.1:60425	127.0.0.1:20817	ESTABLISHED	7216
[Explorer.EXE]				
TCP	172.24.24.177:11358	87.248.129.17:443	ESTABLISHED	1880
[Copilot.exe]				
TCP	172.24.24.177:11372	192.178.24.170:443	ESTABLISHED	12660
[chrome.exe]				
TCP	172.24.24.177:11373	192.178.24.170:443	ESTABLISHED	12660
[chrome.exe]				
TCP	172.24.24.177:11922	35.174.127.31:443	ESTABLISHED	12660
[chrome.exe]				
TCP	172.24.24.177:11938	142.251.168.188:443	ESTABLISHED	12660
[chrome.exe]				
TCP	172.24.24.177:24756	13.107.213.254:443	CLOSE_WAIT	1092
[SearchHost.exe]				
TCP	172.24.24.177:27544	40.99.26.210:443	TIME_WAIT	0
TCP	172.24.24.177:27550	87.248.129.16:443	LAST_ACK	1092

ب) دستوری را پیدا کنید که به وسیله آن تمام پورت های سیستم در هر وضعیت اتصالی همراه با مبدا و مقصد اتصال به صورت عددی لیست شوند.

جواب:

netstat -ano

توضیح سوئیچ های کلیدی:

عملکرد

سوئیچ

-A	نمایش تمام اتصالات فعال و پورت‌های LISTENING
-N	نمایش آدرس‌ها و پورت‌ها به صورت عددی (عدم resolve نام‌ها)
-O	نمایش PID (شناسه فرآیند) مرتبط با هر اتصال

```
C:\Users\hosse>netstat -ano

Active Connections

Proto Local Address Foreign Address State PID
TCP 0.0.0.0:21 0.0.0.0:0 LISTENING 4260
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 1484
TCP 0.0.0.0:443 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:902 0.0.0.0:0 LISTENING 4784
TCP 0.0.0.0:912 0.0.0.0:0 LISTENING 4784
TCP 0.0.0.0:2179 0.0.0.0:0 LISTENING 3104
TCP 0.0.0.0:5040 0.0.0.0:0 LISTENING 7348
TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING 1184
TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING 512
TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING 3080
TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING 3188
TCP 0.0.0.0:49668 0.0.0.0:0 LISTENING 3948
TCP 0.0.0.0:49670 0.0.0.0:0 LISTENING 1156
TCP 127.0.0.1:1001 0.0.0.0:0 LISTENING 4
TCP 127.0.0.1:33847 127.0.0.1:35643 ESTABLISHED 14008
TCP 127.0.0.1:35643 0.0.0.0:0 LISTENING 12224
TCP 127.0.0.1:35643 127.0.0.1:33847 ESTABLISHED 12224
TCP 127.0.0.1:35643 127.0.0.1:35744 ESTABLISHED 12224
TCP 127.0.0.1:35744 127.0.0.1:35643 ESTABLISHED 9664
TCP 172.17.224.1:139 0.0.0.0:0 LISTENING 4
TCP 172.23.185.190:139 0.0.0.0:0 LISTENING 4
TCP 172.23.185.190:4206 104.18.27.90:443 ESTABLISHED 14008
TCP 172.23.185.190:4207 104.18.21.157:443 ESTABLISHED 14008
TCP 172.23.185.190:4209 34.197.233.115:443 ESTABLISHED 14008
TCP 172.23.185.190:4210 142.250.184.234:443 ESTABLISHED 14008
TCP 172.23.185.190:4239 13.107.246.254:443 CLOSE_WAIT 3100
TCP 172.23.185.190:4249 47.246.50.182:443 ESTABLISHED 14008
TCP 172.23.185.190:4263 13.107.253.45:443 ESTABLISHED 10448
TCP 172.23.185.190:4264 2.19.198.33:443 ESTABLISHED 6020
TCP 172.23.185.190:4265 52.111.209.8:443 ESTABLISHED 2312
TCP 172.23.185.190:4266 185.200.232.11:443 ESTABLISHED 3100
TCP 172.23.185.190:4269 52.98.178.242:443 ESTABLISHED 3100
TCP 172.23.185.190:4270 52.98.178.242:443 ESTABLISHED 3100
```

سوال 6: کارکرد Web:

الف: دلیل وارد کردن دو enter پشت سر هم چیست؟

در پروتکل HTTP/1.1، دو Enter یا یک خط خالی \r\n\r\n به عنوان علامت پایان هدرهای درخواست استفاده می‌شود. این کار به سرور می‌گوید که:

- هدرهای HTTP شما تمام شده است مثل GET و Host.
- سرور می‌تواند پردازش درخواست را آغاز کند و پاسخ را ارسال نماید.

```
C:\Windows\System32>ncat -v aut.ac.ir 80
Ncat: Version 7.95 ( https://nmap.org/ncat )
Ncat: Connected to 172.30.31.6:80.
GET / HTTP/1.1

Host: aut.ac.ir
```

سوال 7: با فشردن CTRL+C ارتباط قبلی را خاتمه دهید و دستور زیر را وارد کنید:

ncat -v -l -p 16000 -e c:\Windows\System32\cmd.exe

این دستور یک سوکت TCP ایجاد میکند که بر روی پورت 16000 گوش فرا میدهد. این موضوع را با استفاده از netstat -abn مشاهده کنید.

الف: این پورت بر روی کدام آدرس IP bind شده است؟

جواب: آدرس IP ای که پورت 16000 روی آن bind شده است:

بر اساس خروجی netstat در تصویر، پورت 16000 روی تمام آدرس‌های IP محلی (هم IPv4 و هم IPv6) bind شده است:

- 0.0.0.0: IPv4 به معنای همه آدرس‌های IPv4 سیستم
- [::]: IPv6 به معنای همه آدرس‌های IPv6 سیستم

این یعنی سرور ncat روی تمام رابطهای شبکه (Network Interfaces) سیستم گوش می دهد و از هر آدرس IP محلی مثلاً 192.168.1.2 یا 127.0.0.1 قابل دسترسی خواهد بود.

```
C:\Windows\System32>ncat -v -l -p 16000 -e c:\Windows\System32\cmd.exe
Ncat: Version 7.95 ( https://nmap.org/ncat )
Ncat: Listening on [::]:16000
Ncat: Listening on 0.0.0.0:16000

C:\Users\hosse>netstat -ano | findstr :16000
TCP    0.0.0.0:16000      0.0.0.0:0          LISTENING        3444
TCP    [::]:16000        [::]:0             LISTENING        3444
```

سوال 8: آدرس IP سیستم دوست خود را یادداشت کنید، دستور زیر را اجرا کرده تا به پورت 16000 سیستم دوست خود متصل شوید:

ncat friend_ip 16000

برای اینکه مطمئن شوید، با استفاده از دستور ipconfig تایید کنید که در سیستم دوستان هستید. ارتباط را با دستور C+CTRL ارتباط قبلی را خاتمه دهید.

جواب: پس از اتصال، خط فرمان (cmd.exe) سیستم دوستان برای ما نمایش داده می شود (مانند تصویر اول)

C:\Users\PC>

```
C:\Users\hosse>ncat 192.168.169.190 16000
Microsoft Windows [Version 10.0.22631.5189]
(c) Microsoft Corporation. All rights reserved.

C:\Users\PC>ls
ls

C:\Users\PC>cd Downloads
cd Downloads

C:\Users\PC\Downloads>cd ..
cd ..

C:\Users\PC>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Unknown adapter Local Area Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Unknown adapter Local Area Connection 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::83ca:d1b5:2ccb:b259%4
    IPv4 Address. . . . . : 192.168.169.190
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.169.79
```

سوال 9:(امتیازی) با استفاده از دستور زیر میتوانید یک server web ساده ایجاد کنید . این سرور تنها فایل index.html را که به آن داده اید میزبانی میکند و به کاربر تحویل می دهد.

ncat -l -p 4444 < index.html

برای فایل index.html میتوانید از محتوای زیر استفاده کنید:

HTTP/1.1 200 OK

<html>

```
<head>
<title>HELLO!</title>
<body>Salam!</body>
</head>
</html>
```

الف) دقت کنید یک خط خالی بین http و <html> باید وجود داشته باشد. بنظر شما دلیل وجود خط اول در این فایل چیست؟ یک فایل دیگر بدون خط اول در این فایل بسازید و نتیجه را امتحان کنید.

جواب: این خط یک هدر HTTP استاندارد است که به مرورگر یا کلاینت اطلاع می‌دهد:

- پروتکل استفاده شده: HTTP/1.1

- وضعیت پاسخ 200 OK: یعنی درخواست موفق بوده است.

بدون این هدر، بسیاری از مرورگرها و ابزارهای HTTP ممکن است محتوای HTML را به درستی تفسیر نکنند. در مرورگر ادرس <http://localhost:4444> زده شده است و پاسخ فایل دیده میشود.

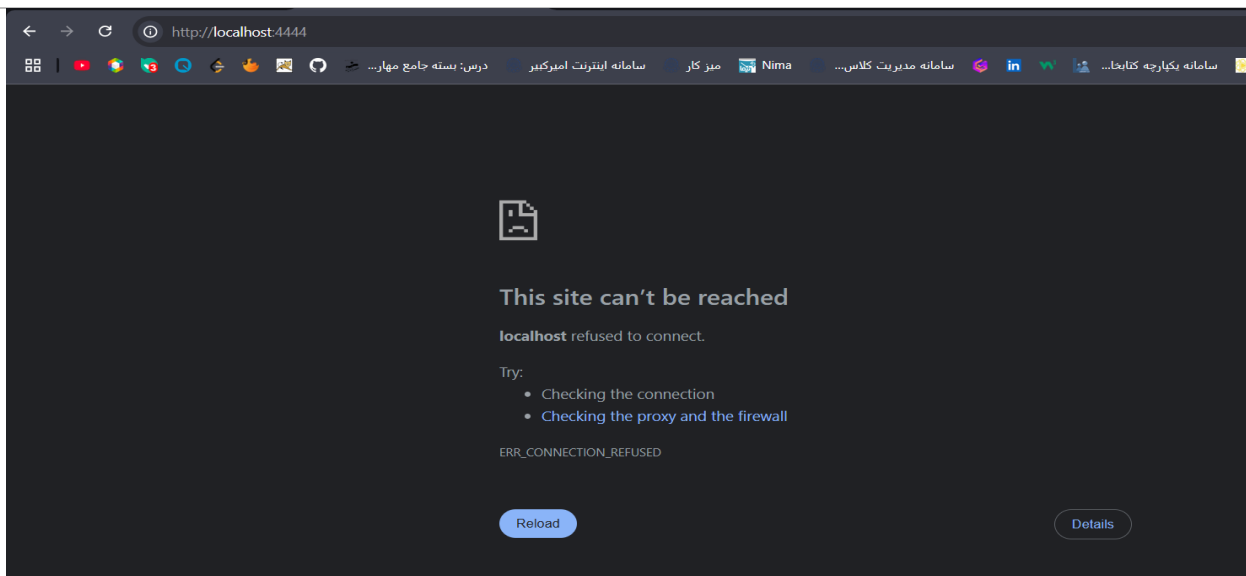
```
C:\Users\hosse\OneDrive\Desktop>ncat -l -p 4444 < index.html
GET / HTTP/1.1
Host: localhost:4444
Connection: keep-alive
sec-ch-ua: "Google Chrome";v="135", "Not-A.Brand";v="8", "Chromium";v="135"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9
```



Salam!

در اینجا ما امدیم و خط اول را حذف نمودیم، جواب ترمینال تغییری نکرد ولی صفحه دیگر در مرورگر نمایش داده نشد.

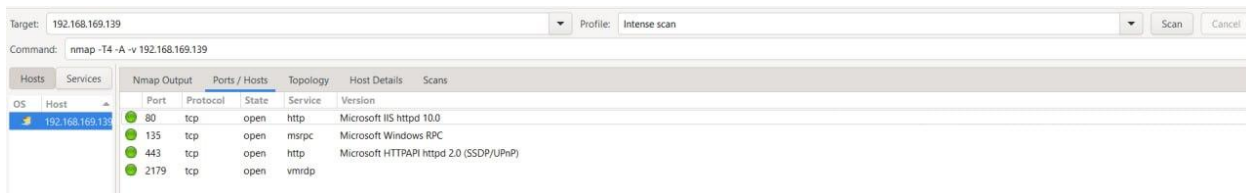
```
C:\Users\hosse\OneDrive\Desktop>ncat -l -p 4444 < index.html
GET / HTTP/1.1
Host: localhost:4444
Connection: keep-alive
sec-ch-ua: "Google Chrome";v="135", "Not-A.Brand";v="8", "Chromium";v="135"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9
```

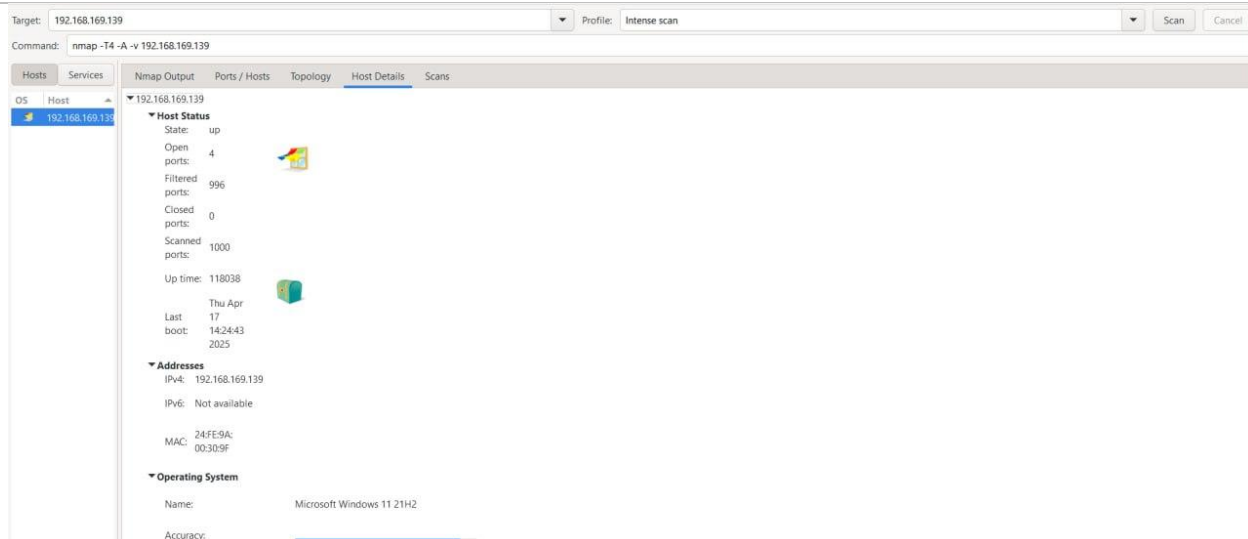



سوال 10: برنامه Zenmap را اجرا کرده و با استفاده از آن آدرس ip سیستم دوست خود را اسکن کنید.
الف) سیستم عامل دوست شما چیست؟
ب) چه پورت هایی روی سیستم دوست شما باز است؟
ج) سرویس هایی که از طریق این پورت ها ارائه میشود چیست؟
جواب:

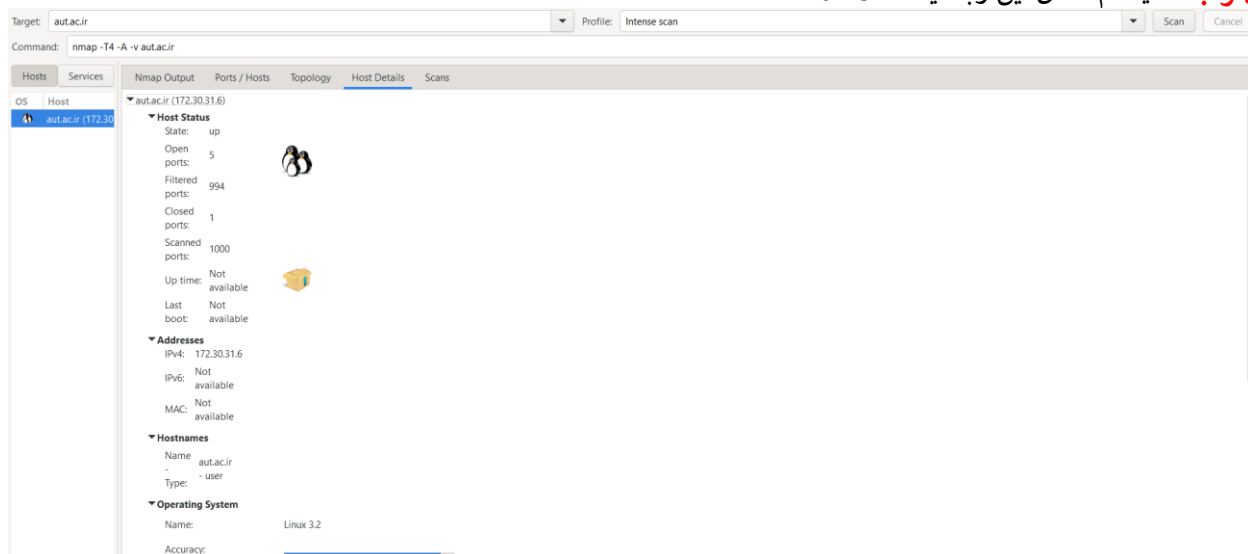
سیستم عامل شناسایی شده Microsoft Windows 11 Z1H2
توضیحات

پورت	سرویس	
90	HTTP	سرویس وب با سرور Microsoft IIS Httpd 10.0
135	MS-RPC	سرویس Microsoft Windows RPC امکان ارتباطات راه دور
419	HTTP	سرویس وب با سرور Microsoft HTTPAPI Httpd 2.0 احتمالاً برای SSDP/UPnP
2179	VRMDP	پروتکل Virtual Router Management Protocol مدیریت روتر مجازی





د) مراحل بالا را برای سایت aut.ac.ir انجام دهید. سیستم عامل این وبسایت چیست؟
جواب: سیستم عامل این وبسایت Linux 3.2 است.



ه) این بار آدرس asg.aut.ac.ir را پویش کنید. با انتخاب پروفایل Intense scan نتیجه چیست؟
جواب: اطلاعات کلی سیستم هدف:

- آدرس IP: 194.225.53.10
- نام دامنه: asg.aut.ac.ir
- سیستم عامل:

• شناسایی شده (Linux 3.10) Android 7.1.2

پورت‌های باز و سرویس‌های مرتبط:

بر اساس نتایج اسکن Nmap پروفایل: Intense Scan

پورت	پروتکل	وضعیت	سرویس	نسخه/توضیحات
22	TCP	open	ssh	Dropbear SSH (protocol 2.0)
25	TCP	open	smtp	(سرور ایمیل)
53	TCP	open	domain	(DNS)

200	TCP	open	?	code-KEQ (ناشناخته)
210	TCP	closed	ident	(غیرفعال)
3128	TCP	open	squid-http	پروکسی Squid (Squid)
4433	TCP	open	?	phairos (احتمالاً سرویس اختصاصی)
4444	TCP	open	?	tab524 (ناشناخته)
5060	TCP	open	sip	VoIP پروتکل
8000	TCP	open	?	optmessaging (پیام رسانی)

Target: asg.aut.ac.ir Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v asg.aut.ac.ir

Hosts Services

OS Host

asg.aut.ac.ir (194.225.33.10)

Host Status

State: up

Open ports: 9

Filtered ports: 990

Closed ports: 1

Scanned ports: 1000

Up time: Not available

Last boot: Not available

Addresses

IPv4: 194.225.33.10

IPv6: Not available

MAC: Not available

Hostnames

Name: asg.aut.ac.ir

Type: user

Operating System

Name: Android 7.1.2 (Linux 3.10)

Accuracy:

Target: asg.aut.ac.ir Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v asg.aut.ac.ir

Hosts Services

OS Host

asg.aut.ac.ir (194.225.33.10)

Port	Protocol	State	Service	Version
22	tcp	open	ssh	Linksys WRT45G modified dropbear sshd (protocol 2.0)
25	tcp	open	smtp	
53	tcp	open	domain	
113	tcp	closed	ident	
2000	tcp	open	cisco-sccp	
3128	tcp	open	squid-http	
4443	tcp	open	pharos	
4444	tcp	open	krb524	
5060	tcp	open	sip	
8090	tcp	open	opsmessaging	

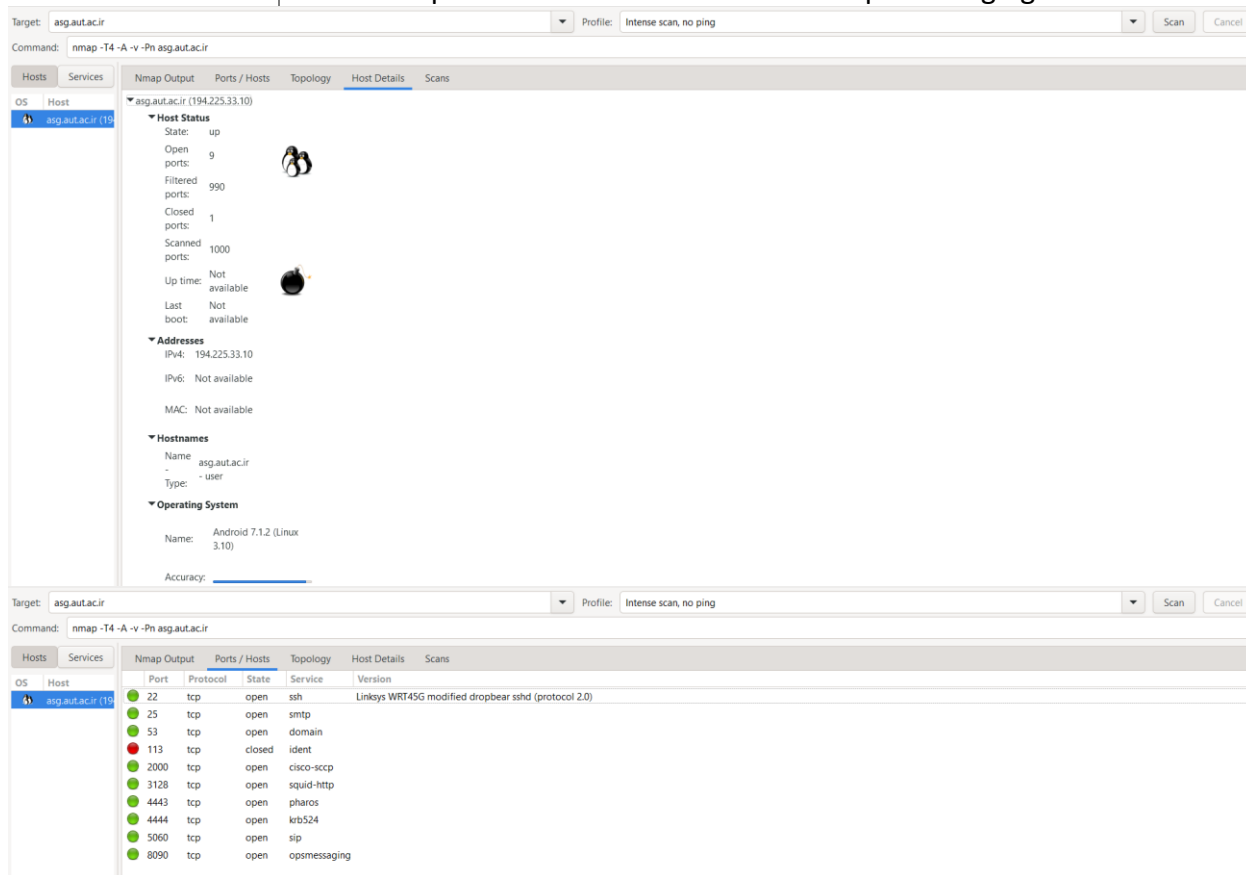
پروفایل Intense scan No ping را انتخاب کنید. نتیجه چیست؟

جواب: اطلاعات کلی سیستم هدف:

- آدرس IP: 194.225.33.10 و IPv6: 1942:23:33:10
 - نام دامنه asg.aut.ac.ir
 - سیستم عامل شناسایی شده: Android 7.1.2 (Linux 3.10)
- نتایج اسکن پورت‌ها:

پورت	پروتکل	وضعیت	سرویس	توضیحات
22	TCP	open	ssh	Dropbear SSH (protocol 2.0)
25	TCP	open	smtp	سرور ایمیل
53	TCP	open	domain	سرویس DNS
200	TCP	open	?	code-KEQ (ناشناخته)
210	TCP	closed	ident	غیرفعال
3128	TCP	open	squid-http	پروکسی Squid

4433	TCP	open	?	phairos (احتمالاً اختصاصی)
4444	TCP	open	?	tab524 (ناشناخته)
5060	TCP	open	sip	VoIP پروتکل
8000	TCP	open	?	optimessaging



آدرس asg.aut.ac.ir را Ping کنید. به نظر شما نتیجه اسکن به چه دلیلی تغییر کرده است؟

این ماشین چه نقشی در دانشگاه دارد؟

جواب: نتیجه پینگ و تغییرات در اسکن:

- پینگ asg.aut.ac.ir:

اگر پینگ پاسخ دهد (State: up) ، نشان دهنده فعال بودن میزبان است. اگر پاسخ ندهد، ممکن است به دلایل زیر باشد:

○ مسدودسازی ICMP توسط فایروال.

○ میزبان واقعاً خاموش باشد.

- تغییر نتایج اسکن:

○ در اسکن اول (Intense scan) ، ۹ پورت باز و ۹۹۰ پورت فیلتر شده گزارش شد.

○ در اسکن دوم (No ping) ، ممکن است تعداد پورت های فیلتر شده کمتر باشد، زیرا:

- اسکن بدون پینگ، پورت های فیلتر شده توسط فایروال را بهتر تشخیص می دهد.
- برخی سرویس ها (مثل SSH) ممکن است فقط به درخواست های خاص پاسخ دهند.

نقش این ماشین در دانشگاه:

با توجه به پورت های باز و سرویس ها، احتمالاً یکی از نقش های زیر را دارد:

الف) سرور پروکسی: (Squid)

- پورت ۳۱۲۸: سرویس squid-http نشان دهنده یک پروکسی وب است.

- ممکن است برای کش کردن ترافیک اینترنت دانشگاه استفاده شود.
- یا دسترسی به منابع خاص را مدیریت کند.
- ب) دستگاه شبکه مانند روتر/فایروال:
 - پورت‌های ناشناخته: (4444, 5000)
 - ممکن است مربوط به مدیریت تجهیزات شبکه (مثل روترهای سیسکو) باشد.
 - پورت 5060 (SIP)
 - برای سرویس‌های VoIP دانشگاه (تماس‌های داخلی).
- ج) سرور خدمات عمومی:
 - پورت ۲۲ (SSH): برای مدیریت از راه دور.
 - پورت ۲۵ (SMTP): احتمالاً بخشی از سرور ایمیل دانشگاه.

Target: asg.aut.ac.ir Profile: Ping scan Scan Cancel

Command: nmap -sn asg.aut.ac.ir

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

asg.aut.ac.ir (194.225.33.10)

▼ Host Status

State: up

Open ports: 9

Filtered ports: 0

Closed ports: 1

Scanned ports: 10

Up time: Not available

Last boot: Not available

▼ Addresses

IPv4: 194.225.33.10

IPv6: Not available

MAC: Not available

▼ Hostnames

Name: asg.aut.ac.ir

Type: user

▼ Operating System

Name: Android 7.1.2 (Linux 3.10)

Accuracy:

Target: asg.aut.ac.ir Profile: Ping scan Scan Cancel

Command: nmap -sn asg.aut.ac.ir

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

Port	Protocol	State	Service	Version
22	tcp	open	ssh	Linksys WRT45G modified dropbear sshd (protocol 2.0)
25	tcp	open	smtp	
53	tcp	open	domain	
113	tcp	closed	ident	
2000	tcp	open	cisco-scp	
3128	tcp	open	squid-http	
4443	tcp	open	pharos	
4444	tcp	open	krb524	
5060	tcp	open	sip	
8090	tcp	open	opsmessaging	