

۲- کار با کاربردهای Web، DNS، سوکت و پویش سرویس‌ها

۲-۱- هدف آزمایش

در این آزمایش قصد داریم با تعدادی از ابزارهای شبکه که به وسیله آن‌ها می‌توانیم در کاربردهای Web و DNS به عنوان سرویس گیرنده استفاده شوند، آشنا شویم.

۲-۲- فعالیت‌های قبل از آزمایش

پروتکل‌های HTTP، TCP، UDP و DNS را یکبار مرور کنید.

۲-۳- قطعات و ابزارهای موردنیاز

ابزارهای موردنیاز برای انجام این آزمایش عبارت‌اند از:

- کامپیوتر شخصی با سیستم عامل ویندوز 7 یا بالاتر برای هر گروه
- برنامه Nmap نسخه ۷.۷ به بالا
- برنامه Wireshark نسخه ۲.۴ به بالا

۲-۴- شرح آزمایش

۲-۴-۱- کارکرد DNS

در ابتدا با ابزارهای برخط^{۲۵} کارکرد DNS آشنا می‌شویم. یکی از این ابزارها، وبسایت ViewDNS است. در گام اول با آدرس زیر وارد این وبسایت شوید:

<http://viewdns.info/>

صفحه اول این وبسایت در شکل (۲-۲۴) نمایش داده شده است.

²⁵ Online

The screenshot displays the ViewDNS.info website interface. At the top, the logo 'Viewdns.info' is visible, with 'View' in black and 'dns.info' in green. Below the logo is a navigation bar with tabs for 'Tools', 'API', 'Research', and 'Data'. The main content area is a grid of 24 tool cards, each with a title, a brief description, an input field, and a 'GO' button. The tools include: Reverse IP Lookup, Reverse Whois Lookup, IP History, DNS Report, Reverse MX Lookup [NEW], Reverse NS Lookup, IP Location Finder, Chinese Firewall Test, DNS Propagation Checker, Is My Site Down, Iran Firewall Test, Domain / IP Whois, Get HTTP Headers, DNS Record Lookup, Port Scanner, Traceroute, Spam Database Lookup, Reverse DNS Lookup, ASN Lookup, Ping, DNSSEC Test, URL / String Decode, Abuse Contact Lookup, MAC Address Lookup, and Free Email Lookup. Each tool card has a light green header and a white body.

شکل (۲۴-۲) وبسایت Viewdns

۱. در قسمت Domain / IP Whois رفته و آدرس soft98.ir را وارد نمایید.

سوال ۱: نام و اطلاعات فردی که دامنه به اسم ثبت شده است چیست؟

سوال ۲: آدرس name server آن چیست؟

۲. در وبسایت به قسمت DNS Report رفته و آدرس soft98.ir را وارد نمایید.

سوال ۳: رکوردهای NS، A، TXT و MX را مشخص کنید. هر یک از این رکوردها چه

چیزی را مشخص می‌کنند؟

سوال ۴: در قسمت DNS Report با وارد کردن دامنه‌ی دانشگاه (aut.ac.ir)، mail server

دانشگاه را مشخص کنید. آیا آدرس IP آن را می‌توانید مشخص کنید؟

۳. در قسمت Reverse IP Lookup آدرس farsnews.com را وارد کنید.

سوال ۵: چه وبسایت‌های دیگری بر روی همین سرور قرار دارند (آدرس IP آن‌ها را با آدرس IP سایت farsnews.com مقایسه کنید)؟

سوال ۶: به نظر شما سرور چگونه وب سرور درخواست شده را تشخیص می‌دهد؟ آیا این روش نیز نوعی Multiplexing است؟

۴. به وبسایت زیر بروید:

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

۵. در این وبسایت آدرس aut.ac.ir وارد کرده و درخواست‌ها و پاسخ‌های دریافت شده را بررسی کنید.

۲-۴-۲- مشاهده و تخصیص پورت‌های لایه انتقال با استفاده از ابزار Netstat

با استفاده از ابزار netstat می‌توان وضعیت پورت‌های لایه انتقال سیستم را مشاهده کرد. به صورت دقیق‌تر می‌توان مشاهده نمود که چه سوکت‌هایی در سیستم وجود دارند و وضعیت آن‌ها چیست. نمونه‌ای از خروجی این دستور در شکل (۲-۲۵) مشاهده می‌شود.

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:1395	www:1396	ESTABLISHED
TCP	127.0.0.1:1396	www:1395	ESTABLISHED
TCP	127.0.0.1:2681	www:19872	ESTABLISHED
TCP	127.0.0.1:6070	www:8580	CLOSE_WAIT
TCP	127.0.0.1:6128	www:8580	TIME_WAIT
TCP	127.0.0.1:6129	www:8580	TIME_WAIT
TCP	127.0.0.1:6130	www:8580	TIME_WAIT
TCP	127.0.0.1:6131	www:8580	TIME_WAIT
TCP	127.0.0.1:6133	www:8580	TIME_WAIT
TCP	127.0.0.1:6144	www:8580	TIME_WAIT
TCP	127.0.0.1:6148	www:8580	TIME_WAIT
TCP	127.0.0.1:6150	www:8580	TIME_WAIT
TCP	127.0.0.1:6155	www:8580	TIME_WAIT
TCP	127.0.0.1:6162	www:8580	TIME_WAIT
TCP	127.0.0.1:6164	www:8580	TIME_WAIT
TCP	127.0.0.1:6165	www:8580	TIME_WAIT
TCP	127.0.0.1:6166	www:8580	TIME_WAIT
TCP	127.0.0.1:6167	www:8580	TIME_WAIT
TCP	127.0.0.1:6169	www:8580	TIME_WAIT
TCP	127.0.0.1:6170	www:8580	TIME_WAIT
TCP	127.0.0.1:6171	www:8580	TIME_WAIT
TCP	127.0.0.1:6172	www:8580	TIME_WAIT
TCP	127.0.0.1:6174	www:8580	TIME_WAIT
TCP	127.0.0.1:6176	www:8580	TIME_WAIT
TCP	127.0.0.1:6177	www:8580	TIME_WAIT
TCP	127.0.0.1:6179	www:8580	TIME_WAIT
TCP	127.0.0.1:6180	www:8580	TIME_WAIT
TCP	127.0.0.1:6182	www:8580	TIME_WAIT
TCP	127.0.0.1:6187	www:8580	TIME_WAIT
TCP	127.0.0.1:6188	www:8580	TIME_WAIT
TCP	127.0.0.1:6190	www:8580	TIME_WAIT
TCP	127.0.0.1:6191	www:8580	TIME_WAIT
TCP	127.0.0.1:6192	www:8580	TIME_WAIT

شکل (۲-۲۵) نمونه‌ای از خروجی دستور netstat

بسیاری از مواقع، برنامه‌هایی نیاز به گوش دادن به یک پورت خاص در سیستم هستند. حال اگر برنامه دیگری قبل از آن‌ها، به آن پورت خاص گوش بدهد برنامه جدید قادر به گوش دادن به آن

پورت نخواهد بود. در این حالت با استفاده از این دستور می‌توانید مشاهده کنید چه پورت‌هایی توسط چه برنامه‌هایی استفاده می‌شود.

سوال ۷: برای لیست کردن برنامه‌هایی که در حال حاضر پورت‌های لایه انتقال را بر روی سیستم باز کرده‌اند، از چه دستور خط فرمانی استفاده می‌شود؟

سوال ۸: دستوری را پیدا کنید که به وسیله آن تمام پورت‌های سیستم در هر وضعیت اتصالی همراه با مبدا و مقصد اتصال به صورت عددی لیست شوند.

۳-۴-۲- کارکرد Web

۱. در این بخش می‌خواهیم با استفاده از ابزار ncat و پروتکل HTTP یک ارتباط با وب سرور دانشگاه ایجاد کنیم. CMD را باز کرده و با استفاده از دستور زیر ابتدا یک ارتباط TCP با aut.ac.ir روی پورت ۸۰ ایجاد کنید.

```
ncat -v aut.ac.ir 80
```

۲. در ادامه پیام HTTP مربوط به دریافت آدرس / را مطابق دستورات زیر وارد کنید. پس از فشردن دکمه enter در خط دوم یکبار دیگر enter را وارد کنید.

```
GET / HTTP/1.1
```

```
Host: aut.ac.ir
```

سوال ۹: دلیل وارد کردن دو enter پشت سر هم چیست؟

سوال ۱۰: پیامی که در پاسخ تقاضای شما داده می‌شود چیست؟ صفحه‌ی اصلی در کجا قرار دارد؟ ادعای خود را با استفاده از تقاضا به همین صفحه در مرورگر و ضبط پیام‌ها با استفاده از wireshark اثبات کنید.

سوال ۱۱: آیا این ارتباط persistent است؟

۳. 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
```

۴. 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.

سوال ۱۲: این پورت بر روی کدام آدرس IP، bind شده است؟ بعد از برقراری ارتباط با این سوکت، برنامه CMD نیز اجرا می‌شود. در ادامه دستوراتی که فرستنده ارسال کند به این برنامه داده می‌شوند و خروجی دستورات از طریق ارتباط برقرار شده منتقل خواهد شد.

۵. آدرس آی‌پی سیستم دوست خود را یادداشت کنید، دستور زیر را اجرا کرده تا به پورت 16000 سیستم دوست خود متصل شوید:

```
ncat friend_ip 16000
```

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

۷. با استفاده از دستور زیر می‌توانید یک web server ساده ایجاد کنید. این سرور تنها فایل index.html را که به آن داده‌اید می‌زبانی می‌کند و به کاربر تحویل می‌دهد.

```
ncat -l -p 4444 < index.html
```

۸. 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>
```

سوال ۱۳: دقت کنید یک خط خالی بین HTTP و <html> باید وجود داشته باشد. به نظر شما دلیل وجود خط اول در این فایل چیست؟ یک فایل دیگر بدون خط اول این فایل بسازید و نتیجه را امتحان کنید.

۴-۴-۲- پویش سرویس‌ها

برنامه‌ی NMAP به منظور پویش شبکه و سرویس‌های سیستم‌های انتهایی مورد استفاده قرار می‌گیرد. با استفاده از این برنامه می‌توانید تشخیص دهید بر روی هر سیستم چه سرویس‌هایی قرار دارد و آیا آن سرویس‌ها در دسترس هستند و یا خیر. رابط کاربری گرافیکی این ابزار Zenmap نام دارد.

۱. برنامه Zenmap را اجرا کرده و با استفاده از آن آدرس آی پی سیستم دوست خود را اسکن کنید.

سوال ۱۴: سیستم‌عامل دوست شما چیست؟

سوال ۱۵: چه پورت‌هایی روی سیستم دوست شما باز است؟

سوال ۱۶: سرویس‌هایی که از طریق این پورت‌ها ارائه می‌شود چیست؟

سوال ۱۷: مراحل بالا را برای سایت aut.ac.ir انجام دهید. سیستم‌عامل این وبسایت چیست؟

سوال ۱۸: این بار آدرس asg.aut.ac.ir را پویش کنید. با انتخاب پروفایل Intense scan، نتیجه چیست؟ پروفایل Intense scan, No ping را انتخاب کنید. نتیجه چیست؟ 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؟