۲-کار با کاربردهای DNS، Web، سوکت و پویش سرویس ها

۲-۱- هدف آزمایش

در این آزمایش قصد داریم با تعدادی از ابزارهای شبکه که بهوسیله آن می توانیم در کاربرد های DNS،Web به عنوان سرویس گیرنده استفاده شوند، آشنا شویم.

۲-۲- فعالیت های قبل از آزمایش

الف) پروتکل های HTTP، TCP، UDP، DNS را توضیح دهید.

ب) ابزار netstat و کاربرد آن را توضیح دهید.

ج) کاربر دستور ncat چیست؟ و تفاوت ارتباط persistent وnon-persistent را توضیح دهید.

۲-۳- قطعات و ابزارهای موردنیاز

ابزارهای موردنیاز برای انجام این آزمایش ها عبارتند از:

- کامپیوتر شخصی با سیستم عامل ویندوز ۷ یا بالاتر برای هرگروه
- برنامه Nmap نسخه ۷.۷ به بالا
- برنامه Wireshark نسخه ۲.۴ به بالا

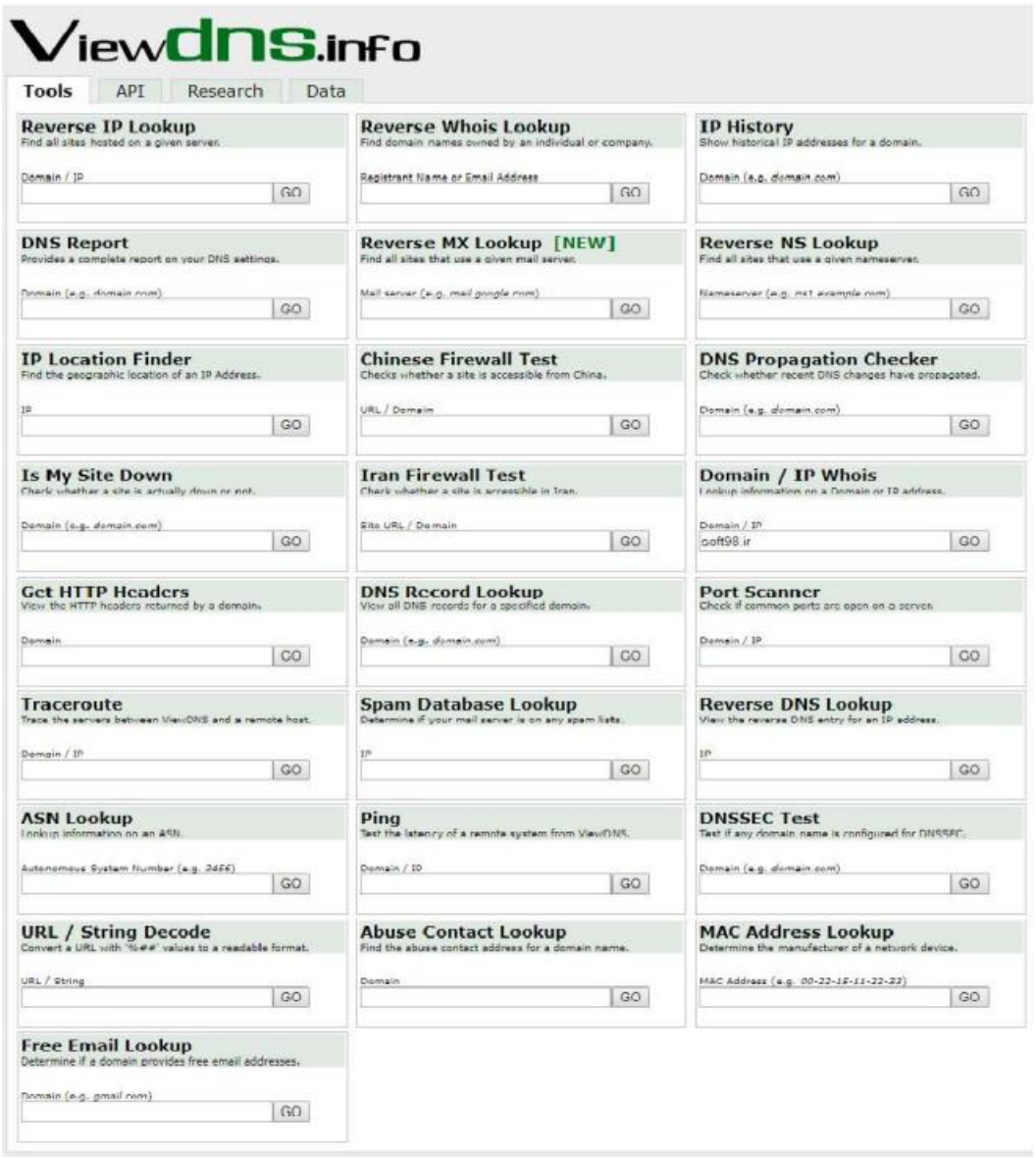
۲-۴- شرح آزمایش

۲-۴-۱- کارکرد DNS

در ابتدا با ابزارهای برخط کارکرد DNS آشنا می شویم. یکی از این ابزارها، وب سایت ViewDNS است. در گام اول با آدرس زیر وارد این وب سایت شوید:

http://viewdns.info/

صفحه اول این وب سایت در شکل زیر(۱) نمایش داده شده است.



شکل(۱)وب سایت ViewDNS

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

الف) نام و اطلاعات فردی که دامنه به اسم ثبت شده است چیست؟

ب) آدرس name server آن چیست؟

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

الف) رکوردهای NS، A، TXT و MX را مشخص کنید. هر یک از این رکوردها چه چیزی را مشخص می‌کنند؟

ب) 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 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 IPسایت farsnews.ir مقایسه کنید)؟

ب) 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://simpledns.com/lookup-dg

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

۲-۴-۲- مشاهده و تخصیص پورت های لایه انتقال با استفاده از ابزارNetstat

با استفاده از ابزار netstat میتوان وضعیت پورت های لایه انتقال سیستم را مشاهده کرد. به صورت دقیق تر میتوان مشاهده نمود که چه سوکت هایی در سیستم وجود دارند و وضعیت آن ها چیست. نمونه ای از خروجی این دستور در شکل (۲) مشاهده می شود.

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) نمونه ای از خروجی دستورnetstat

بسیاری از مواقع، برنامه هایی نیاز به گوش دادن به یک پورت خاص در سیستم هستند. حال اگر برنامه دیگری قبل از آن ها، 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 می توانید مشاهده کنید چه پورت هایی توسط چه برنامه هایی استفاده می شود.

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

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.

۲-۴-۳- کارکردWeb

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 TCPبا 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

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

ب) پیامی که در پاسخ تقاضای شما داده می شود چیست؟ صفحه ی اصلی در کجا قرار دارد؟ ادعای خود را با استفاده از تقاضا به همین صفحه در مرورگر و ضبط پیام ها با استفاده از wireshark اثبات کنید.

ج) آیا این ارتباط persistent است؟

۳- با فشردن C+CTRL 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 ۱۶۰۰۰ گوش فرا میدهد، این موضوع را با استفاده از netstat -abn مشاهده کنید.

الف) این پورت بر روی کدام آدرسIP ، 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 می شوند و خروجی دستورات از طریق ارتباط برقرار شده منتقل خواهد شد.

۵- آدرس IP سیستم دوست خود را یادداشت کنید، دستور زیر را اجرا کرده تا به پورت ۱۶۰۰۰ سیستم دوست خود متصل شوید:

ncat friend_ip 16000

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

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

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>

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.

۲-۴-۴- پویش سرویس ها

برنامه ی NMAP به منظور پویش شبکه و سرویس های سیستم های انتهایی مورداستفاده قرار میگیرد. با استفاده از این برنامه میتوانید تشخیص دهید بر روی هر سیستم چه سرویس هایی قرار دارد و آیا آن سرویس ها 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 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؟

د) مراحل بالا را برای سایت aut.ac.ir انجام دهید. سیستم عامل این وبسایت چیست؟

ه) این بار آدرس asg.aut.ac.ir را پویش کنید. با انتخـاب پروفایـل Intense scan ، نتیجه چیست؟ پروفایل No ping, Intense scan را انتخاب کنیـد. نتیجـه چیسـت؟ آدرس asg.aut.ac.ir را Ping کنید. به نظر شما نتیجه اسکن به چه دلیلی تغییر کرده است؟ ایـن ماشین چه نقشی در دانشگاه دارد؟