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

### ۱-۲- 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) پروتكل هاى DNS ،UDP ،TCP ،HTTP را توضيح دهيد.

ب) ابزار netstat و کاربرد آن را توضیح دهید.

ج) كاربر دستور ncat چيست؟ و تفاوت ارتباط persistent و non-persistent را توضيح دهيد.

# ۳-۲- 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

## ۴-۲- شرح آزمایش

## ۲-۴-۱ کارکرد DNS

در ابتدا با ابزارهای برخط کار کرد DNS آشنا می شویم. یکی از این ابزارها، وب سایت DNS 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.

Tools API Research I	Data		
Reverse IP Lookup	Reverse Whois Lookup Find domain names owned by an individual or company.	IP History Show historical IP addresses for a domain.	
nino an area nosteo on a given serven	rind contain names owned by an individual or company.	Show risconder an appreciate for a company	
Domain / IP	Registrant Name or Email Address	Domain (e.g. domain.com)	
00	GO	GO	
ONS Report revides a complete report on your DNS settings.	Reverse MX Lookup [NEW] Find all sites that use a given mail server.	Reverse NS Lookup Find all ares that use a given nameserver.	
Inmain (a.g. domain com)	Mail server (a.g. mail gongle rom)	Rameserver (e.g. nst example rom)	
60	GO	GO	
IP Location Finder Find the peographic location of an IP Address-	Chinese Firewall Test Checks whether a site is accessible from China.  DNS Propagation Check Check whether recent DNS changes have		
	URL / Domain	Diomain (e.g. domain.com)	
GO	GO	GO	
Is My Site Down There whather a site is actually down or not.	Iran Firewall Test Charle whether a site is arrassible in Iran.  Domain / IP Whois Loding information on a Domain or ID address.		
	Landa va	2 3 32	
Demain (e.g. demain.eem) GO	Site URL / Demain	coff98 ir GO	
Get HTTP Headers New the HTTP headers returned by a demain.	DNS Record Lookup View all DNS records for a specified demain-	Port Scanner Check if common ports are open on a serven	
		2	
GO CO	Demain (e.g. demain.com)	Demein / IP	
Fraceroute	Spam Database Lookup	Reverse DNS Lookup	
Demain / IP	IP GO	In GO	
60	100	100	
ASN Lookup nokup leformation on an ASN.	Ping Text the latency of a remote system from ViewDNS.	DNSSEC Test Test if any domain name is configured for DNSSEC.	
Autonomous System Number (a.g. 2456)	Comain / 10	Stemain (e.g. demain.com)	
URL / String Decode Convert a URL with 1988 values to a readable format.	Abuse Contact Lookup Find the abuse contact address for a domain name.	MAC Address Lookup Determine the manufecturer of a network device.	
URL / String	Demain	MAC Address (e.g. 00-22-15-11-22-22)	
GO	GO	GO	
Free Email Lookup Determine if a domain provides free email addresses.			
Domain (e.g. gmail com)			
GO			

شكل(۱)وب سايت 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 TXT 'A 'NS 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؟

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

الف) چه وبسایت های دیگری بر روی همین سرور قـرار دارنـد (آدرس IP آن هـا را بـا آدرس IP مقاسه 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 بررسے کنید.

### ۲-۴-۲ مشاهده و تخصیص پورت های لایه انتقال با استفاده از ابزار Netstat

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	ννν:8580	TIME_WAIT
TCP	127.0.0.1:6179	ννν:8580	TIME WAIT
TCP	127.0.0.1:6180	ννν: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	ννν:8580	TIME_WAIT
TCP	127.0.0.1:6192	www:8580	TIME_WAIT
101	127.0.0.1.0172	www-0300	TITE_WHIT

شکل(۲) نمونه ای از خروجی دستور netstat

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 نامه دیگری قبل از آن ها، به آن پورت خاص گوش بدهد برنامه جدید قادر به گوش دادن به آن پورت هایی 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 بـر 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.

### ۳-۴-۲ کار کرد 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 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) دليل وارد كردن دو enter پشت سر هم چيست؟

ب) پیامی که در پاسخ تقاضای شما داده می شود چیست؟ صفحه ی اصلی در کجا قرار دارد؟ ادعای خود را 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 بـر روی پـورت ۱۶۰۰۰ گـوش فـرا میدهـد، ایـن موضوع را با استفاده از netstat -abn مشاهده کنید.

الف) این پورت بر روی کدام آدرس bind ، IP 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.

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

 $e^{-}$  برای اینکه مطمئن شوید، با استفاده از دستور ipconfig تایید کنید که در سیستم دوستتان هستید. ارتباط را با دستور  $e^{+}$  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 بسازید و نتیجه را امتحان کنید.

# ۲-۴-۲- 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 ایزار Zenmap نام دارد.

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

الف) سيستم عامل دوست شما چيست؟

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 براى سايت aut.ac.ir انجام دهيد. سيستم عامل اين وبسايت چيست؟

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