«بـــــــه نام خـــالق آرامـــش»

نام کتاب: مقدمات هک

نام نویسنده: ــــــــــــــــــ

تعداد صفحات: ۷۹ صفحه

تاریخ انتشار: ــــــــــــــــــ

کافئین بوکلی

CaffeineBookly.com

بخش یک

مقدمات هک

جلسه اول

ترمینولوژی (اصطلاح‌شناسی)

Hacker کیست ؟

هکر کسی است که با سیستم های کامپیوتری آشناست و می‌تواند با روش‌هایی خاص (بدون اجازه) وارد آنها شود... این انسان می‌تواند خوب یا بد باشد (در هر حال هکر است)

سوال: یک هکر از چه راهی وارد یک سیستم می‌شود؟

از راه شبکه (نه بابا !)

باید توجه کنید که هر سیستم کامپیوتری (به عبارت بهتر هر سیستم عامل) به هر حال محصول کار تعدادی انسان است و حتما دارای تعدادی bug (خطاهایی که بعد از ارائه محصول به بازار به تدریج کشف می‌شوند) خواهد بود. بعد از اینکه یک باگ مشخص شد، شرکت ها نرم‌افزارهایی را به‌سرعت (در عرض چند ساعت) ایجاد می‌کنند تا مشکل رفع شود این‌ها را patch می‌گویند. و بعد مدیران شبکه (Wbemasters) در عرض چند روز تا چند سال (آین آخری در مورد ایرانه) آنها را download کرده و مشکل را حل می‌کنند. در این فاصله هکرها دمار از روزگار این سایت‌ها در می‌اورند...

تعریف چند اصطلاح:

- Hacker واقعی = سامورایی : کسی که هدفش از نفوذ به سیستمها نشان دادن ضعف سیستمهای کامپیوتری است نه سوءاستفاده ...
- Wacker (واکر): کسی که هدفش از نفوذ به سیستمها، استفاده از اطلاعات آن سیستمهاست (جزو هکرهای کلاه سیاه)
- Cracker (کراکر): کسی که هدفش از نفوذ به سیستمها، خرابکاری و ایجاد اختلال در سیستمهای کامپیوتری است. (جرو هکرهای کلاه سیاه)
- Preaker : از قدیمي‌ترین هکرها هستند که برای کارشان نیاز (و دسترسی) به کامپیوتر نداشتند و کارشان نفوذ به خطوط تلفن برای تماس مجانی، استراق‌سمع و ... بود. این جزو آموزش من نیست چون کار خیلی بدیه (-;

زنگ تفریح

تقسیم بندی من برای هکرها:

۱- جوجه‌هکرها (احمق کوچولوها):

توانایی‌ها: بلدند از Sub 7 , ۱۸۷ استفاده کنند و فکر کنند دیگه همه‌چی رو یاد گرفته‌اند !

۲- خروس‌هکرها یا مرغ‌هکرها (احمق‌های بزرگتر):

توانایی‌ها: Mail Box را هم می‌توانند Bomb کنند ... ماشاءالله!

۳- هکرهای قابل‌احترام (مثل خود شما):

دارند یاد می‌گیرند و هنوز ۲،۳ سال کار دارند.

۴- هکرهای پیش‌کسوت:

دیگه آفتاب لبه بومه ... هکرهای قابل احترام را دوس دارند.

تقسیم‌بندی

انواع کامپیوترهای شبکه:

- کامپیوترهای Server : کامپیوترهایی که کارشان تامین اطلاعات در شبکه است، مثلاً کامپیوترهایی که سایت‌ها را نگه می‌دارند.
- کامپیوترهای Client : کامپیوترهایی که استفاده کننده هستند مثل همین کامپیوتر خودتان که دارید ازش کار می‌کشید.

انواع سیستم عامل‌هایی که Server ها از آن استفاده می‌کنند:

۱. سیستم‌های فعلی:
   - خانواده Unix (مثل FreeBSD, Linux, Sun Solaris)
   - خانواده Windows (مثل WinNT, Win2000)
   - OsMac
۲. سیستم‌های قدیمی:
   - ... , AIX, IRIS, DEC10, DEC20

سوال: کدام‌ها را باید یاد گرفت؟

Win2000, Unix(Linux) را باید یاد بگیرید. پیشنهاد من این است که Win2000و RedHat Linux را روی کامپیوتر خود همزمان داشته باشید.

برای شروع چه چیزی لازم است؟

۱- Win2000 , Linux را روی کامپیوتر خود نصب کرده و شروع به یادگیری کنید.

۲- شروع به یادگیری زبان C کنید.

۳- شروع به یادگیری TCP/IP کنید. (یک کتاب بخرید)

۴- مهمترین چیز علاقه به طی کردن یک را بسیییییار طووووولانی

تقسیم‌بندی انواع حملات

اولین نکته‌ای که لازم است بگویم اینه که وقت خود را برای هک کردن کامپیوترهای کلاینت هدر ندهید (اگرچه برای افراد مبتدی کار با نرم‌افزاری مثل Sub7 زیاد هم بد نیست ولی نباید زیاده روی کرد) علت هم اینه که هربار که به اینترنت وصل می‌شوند ip جدیدی به آنها اختصاص پیدا می‌کنه و زحماتتون هدر می‌ره (البته برای جلوگیری از این امر هم روشهایی هست که در آینده ایشاالله میگم).

حالا تقسیم‌بندی:

۱- حمله به روش (DoS) Denial of Service Attack

۲- حمله به روش Exploit

۳- حمله به روش Info Gathering (تلنت کردن یکی از مثالهای آن است که امروز آموختید)

۴- حمله به روش Disinformation

در مورد هرکدام به‌زودی توضیح می‌دم.

t Speak۱۳۳ چیست؟

گاهی هکرها در هنگام نوشتن به جای تعدادی از حروف انگلیسی معادل‌های قراردادی به کار می‌روند که لیست آنها را در زیر می‌بینید:

```
0  <= O
1 <= L; I
2  <= Z
3  <= E
4  <= A
5  <= S
6  <= G
```

```
7   <= T
8   <= B
|  <= L; I
@  <= at (duh)
$   <= S
)(   <= H
}{   <= H
/\/  <= N
\/\/ <= W
/\/\ <= M
|>   <= P; D
|<   <= K
ph   <= f
z   <= s
```

مثلا he Speaks می‌شود:

```
}{3 $|>34|< z
```

توصیه من اینه که از این معادل‌ها تا جایی که می‌تونید استفاده نکنید. فقط یاد بگیرید که کم نیارید.

ترسیم مسیر برای آینده

۱- اولین و مهمترین تصمیم انتخاب نوع کامپیوتری است که می‌خواهید هک کنید (کلاینت یا سرور)، زیرا روش‌هک کردن این دو بجز در مراحل ابتدایی کاملا متفاوت است.

۲- دومین گام انتخاب یک کامپیوتر مشخص (مثلا کامپیوتری که فلان سایت را نگه می‌دارد که مثالی برای کامپیوتر سرور است و یا کامپیوتر فلان شخصی که با او چت می‌کنید که مثالی برای کامپیوتر کلاینت است) و جمع‌آوری اطلاعات در مورد آن است. این جمع‌آوری اطلاعات از قربانی (Victim) را Footprinting گویند. اولین مشخصه‌ای که باید کشف شود، ip اوست. یکی دیگر از اطلاعات مهم که معمولا دنبالش هستیم، پیدا کردن نوع سیستم‌عامل و نیز برنامه‌هایی است که

کامپیوتر شخص از آنها بهره می‌برد. یکی از مهمترین (و گاه خطرناک‌ترین) کارها، تست‌کردن پورت‌های آن کامپیوتر برای دیدن اینکه کدام پورت‌ها باز و کدام‌ها بسته هستند.

۳- مرحله بعدی در واقع شروع تلاش برای نفوذ به سیستم است. این نفوذ سطوح مختلف دارد و بالاترین آن که در کامپیوترهای سرور روی می‌دهد، حالتی است که بتوان username و password مربوط به مدیر کامپیوتر (administrator) یا superuser را به‌دست آورده و از طریق این Shell Account به نهایت نفوذ دست یابیم ولی گاه به‌دلایل مختلف (مربوط به سطح علمی خود و ...) نمی‌توان به این سطح دست‌یافت اما به هر حال برای مرحله بعدی می‌تواند استفاده شود. این مرحله جایی است که هنر شما به عنوان یک هکر آغاز شده و نیز به پایان می‌رسد.

۴- این مرحله بعد از نفوذ روی می‌دهد که در آن به یک سطحی از کنترل سیستم رسیده‌اید. رفتار شما در این مرحله مشخص می‌کند که چه نوع هکر هستید(ساموراپی، واکر و یا کراکر) و اینکه آیا جنبه یاد گرفتن را داشته‌اید یا نه، همینجا مشخص خواهد شد.

۵- مرحله آخر پاک کردن ردپاست تا گیر نیفتیم (البته بعضی وقتها برای کلاس گذاشتن باید گیر بیفتیم، هه هه ...). بعضی از سیستم‌ها آمار login را نگه می‌دارند که در مورد آنها این مرحله بسیار مهم است.

خلاصه مطالب بالا به این صورت است:

Selection -> FootPrinting -> Penetration -> [Changings] -> Cleaning

جلسه دوم

IP

شماره ایست که به هر کامپیوتر متصل به اینترنت داده می‌شود تا بتوان به‌کمک آن شماره به آن کامپیوترها دسترسی داشت. این عدد برای کامپیوترهایی که حالت سرور دارند (مثلا سایت‌ها) و نیز کامپیوترهای کلاینتی که معمولا به روشی غیر از شماره‌گیری (Dial Up) به اینترنت وصل هستند، عددی ثابت و برای دیگران عددی متغیر است. مثلا هر بار که شما با شرکت ISP خود تماس گرفته و به اینترنت وصل می‌شوید، عددی جدید به شما نسبت داده می‌شود.

این عدد یک عدد ۳۲ بیتی (۴ بایتی) است و برای راحتی به‌صورت زیر نوشته می‌شود:

xxx.xxx.xxx.xxx که منظور از xxx عددی بین ۰ تا ۲۵۵ است (البته بعضی شماره‌ها قابل استفاده نیست که بعدا علت را توضیح خواهم داد). مثلا ممکن است آدرس شما به صورت ۱۹۵,۲۱۹,۱۷۶,۶۹ باشد. حتی اسم‌هایی مثل www.yahoo.com که برای اتصال استفاده می‌کنید، در نهایت باید به یک IP تبدیل شود، تا شما سایت یاهو را ببینید.

در IP معمولا xxx اولی معنای خاصی دارد، که بعدا توضیح می‌دهم... فقط این را بگویم که اگر به روش Dial Up به اینترنت وصل شوید، معمولا عددی که به عنوان xxx اول می‌گیرید، مابین ۱۹۲ تا ۲۲۳ خواهد بود.این توضیح برای تشخیص کامپیوترهای کلاینت از سرور (حداقل در ایران) بسیار می‌تواند مفید باشد.

بعد از اتصال به اینترنت برای به دست آوردن IP خود، از دستور IPCONFIG در command prompt استفاده کنید. (البته یک سری نکات فنی داریم که بعدا می‌گم)

Port

در ساده ترین تعریف، محلی است که داده‌ها وارد یا خارج می‌شوند. در مبحث هک معمولا با پورت‌های نرم‌افزاری سروکار داریم که به هر کدام عددی نسبت می‌دهیم. این اعداد بین ۱ و ۶۵۵۳۵ هستند. معمولا به یک سری از پورت‌ها کار خاصی را نسبت می‌دهند و بقیه به‌صورت پیش‌فرض برای استفاده شما هستند. پورت‌های که فعال هستند، هرکدام توسط یک نرم‌افزار خاص مدیریت می‌شوند. مثلا پورت ۲۵ برای ارسال Email است، بنابراین باید توسط یک نرم‌افزار این کار انجام شود و این نرم‌افزار بر روی پورت ۲۵ منتظر (فال‌گوش) می‌ماند. اینجا ممکن است

شخصی از فلان نرم‌افزار و دیگری از بهمان نرم‌افزار استفاده کند ولی به‌هر حال پورت ۲۵ همیشه برای ارسال Email است.

در پایین لیستی از مهمترین پورت‌ها و کاربردشان را می‌بینید:

Port Num	Service	Why it is phun!
7	echo	Host repearts what you type
9	discard	Dev/null
11	systat	Lots of info on users
13	daytime	Time and date at computers location
15	netstat	Tremendous info on networks
19	chargen	Pours out a stream of ASCII characters.
21	ftp	Transfers files
23	telnet	Where you log in.
25	smpt	Forge email
37	time	Time
39	rlp	Resource location
43	whois	Info on hosts and networks
53	domain	Nameserver
70	gopher	Out-of-date info hunter
79	finger	Lots of info on users
80	http	Web server
110	pop	Incoming email
119	nntp	Usenet news groups -- forge posts, cancels
443	shttp	Another web server
512	biff	Mail notification
513	rlogin	Remote login
	who	Remote who and uptime
514	shell	Remote command, no password used!
	syslog	Remote system logging

520	route	Routing information protocol

از میان این پورت‌ها شماره‌های ۷، ۱۵، ۲۱، ۲۳، ۲۵، ۷۹، ۸۰، ۱۱۰و ۱۱۹ فعلا برای ما مهم‌ترند و به‌تدریج با آنها آشنا خواهید شد.

جلسه سوم

RFC چیست؟

متون بسیار کامل ولی خشک و ثقیل که در مورد مفاهیم مختلف شبکه بحث می‌کنند. این فایل‌ها به صورت متنی و با پسوند txt هستند و به‌عنوان مرجع (برای مراجعه و نه مطالعه کامل) کاربرد دارند. این فایل‌ها یک‌بار منتشر شده و هرگز تغییر داده نمی‌شوند (حتی اگر حاوی اشتباه باشند.)

فایل‌های RFC از کجا قابل دسترسی هستند؟

RFCها از سایت‌های بسیاري قابل دسترس هستند ولی سایت مورد علاقه من برای RFCها، سایت زیر است:

```
http://www.ietf.org/rfc/xxxxxxx.txt
```

که به‌جای xxxxxxx نام rfc موردنظر را می‌نویسیم. مثلا برای دسترسی به rfc791 باید آدرس را به صورت زیر تایپ کنیم:

```
http://www.ietf.org/rfc/rfc791.txt
```

لیست مشهورترین RFCها

```
+General Information
RFC1360 IAB Official Protocol Standards
RFC1340 Assigned Numbers
RFC1208 Glossary of Networking Terms
RFC1180 TCP/IP Tutorial
RFC1178 Choosing a Name for Your Computer
RFC1175 FYI on Where to Start:
    A Bibliography of Inter-networking Information
RFC1173 Responsibilities of Host and Network Managers:
    A Summary of the Oral Tradition of the Internet
```

RFC1166 Internet Numbers

RFC1127 Perspective on the Host Requirements RFCs

RFC1123 Requirements for Internet Hosts—Application and Support

RFC1122 Requirements for Internet Hosts—Communication Layers

RFC1118 Hitchhiker"s Guide to the Internet

RFC1011 Official Internet Protocol

RFC1009 Requirements for Internet Gateways

RFC980 Protocol Document Order Information

+TCP and UDP

RFC1072 TCP Extensions for Long-Delay Paths

RFC896 Congestion Control in IP/TCP Internetworks

RFC879 TCP Maximum Segment Size and Related Topics

RFC813 Window and Acknowledgment Strategy in TCP

RFC793 Transmission Control Protocol

RFC768 User Datagram Protocol

+IP and ICMP

RFC1219 On the Assignment of Subnet Numbers

RFC1112 Host Extensions for IP Multicasting

RFC1088 Standard for the Transmission of IP Datagrams over NetBIOS Networks

RFC950 Internet Standard Subnetting Procedure

RFC932 Subnetwork Addressing Schema

RFC922 Broadcasting Internet Datagrams in the Presence of Subnets

RFC919 Broadcasting Internet Datagrams

RFC886 Proposed Standard for Message Header Munging

RFC815 IP Datagram Reassembly Algorithms

RFC814 Names, Addresses, Ports, and Routes

RFC792 Internet Control Message Protocol

RFC791 Internet Protocol

RFC781 Specification of the Internet Protocol (IP) Timestamp Option

+Lower Layers

RFC1236 IP to X.121 Address Mapping for DDN

RFC1220 Point-to-Point Protocol Extensions for Bridging

RFC1209 Transmission of IP Datagrams over the SMDS Service

RFC1201 Transmitting IP Traffic over ARCNET Networks

RFC1188 Proposed Standard for the Transmission of IP Datagrams over FDDI Networks

RFC1172 Point-to-Point Protocol Initial Configuration Options

RFC1171 Point-to-Point Protocol for the Transmission of Multiprotocol Datagrams over Point-to-Point Links

RFC1149 Standard for the Transmission of IP Datagrams on Avian Carriers

RFC1055 Nonstandard for Transmission of IP Datagrams over Serial Lines: SLIP

RFC1044 Internet Protocol on Network System"s HYPERchannel: Protocol Specification

RFC1042 Standard for the Transmission of IP Datagrams over IEEE 802 Networks

RFC1027 Using ARP to Implement Transparent Subnet Gateways

RFC903 Reverse Address Resolution Protocol

RFC895 Standard for the Transmission of IP Datagrams over Experimental Ethernet Networks

RFC894 Standard for the Transmission of IP Datagrams over Ethernet Networks

RFC893 Trailer Encapsulations

RFC877 Standard for the Transmission of IP Datagrams over Public Data Networks

+Bootstrapping

RFC1084 BOOTP Vendor Information Extensions

RFC951 Bootstrap Protocol

RFC906 Bootstrap Loading Using TFTP

+Domain Name System

RFC1101 DNS Encoding of Network Names and Other Types

RFC1035 Domain Names—Implementation and Specification

RFC1034 Domain Names—Concepts and Facilities

RFC1033 Domain Administrators Operations Guide

RFC1032 Domain Administrators Guide

RFC974 Mail Routing and the Domain System

RFC920 Domain Requirements

RFC799 Internet Name Domains

+File Transfer and File Access

RFC1094 NFS: Network File System Protocol Specification

RFC1068 Background File Transfer Program (BFTP)

RFC959 File Transfer Protocol

RFC949 FTP Unique-Named Store Command

RFC783 TFTP Protocol (Revision 2)

RFC775 Directory Oriented FTP Commands

+Mail

RFC1341 MIME (Multipurpose Internet Mail Extensions) Mechanisms for Specifying and Describing the Format of Internet Message

Bodies

RFC1143 Q Method of Implementing Telnet Option Negotiation

RFC1090 SMTP on X.25

RFC1056 PCMAIL: A Distributed Mail System for Personal Computers

RFC974 Mail Routing and the Domain System

RFC822 Standard for the Format of ARPA Internet Text Messages

RFC821 Simple Mail Transfer Protocol

+Routing Protocols

RFC1267 A Border Gateway Protocol 3 (BGP-3)

RFC1247 OSPF version 2

RFC1222 Advancing the NSFNET Routing Architecture

RFC1195 Use of OSI IS-IS for Routing in TCP/IP and Dual Environments

RFC1164 Application of the Border Gateway Protocol in the Internet

RFC1163 Border Gateway Protocol (BGP)

RFC1136 Administrative Domains and Routing Domains:

A Model for Routing in the Internet

RFC1074 NSFNET Backbone SPF-Based Interior Gateway Protocol

RFC1058 Routing Information Protocol

RFC911 EGP ateway under Berkeley UNIX 4.2

RFC904 Exterior Gateway Protocol Formal Specification

RFC888 STUB Exterior Gateway Protocol

RFC827 Exterior Gateway Protocol (EGP)

RFC823 DARPA Internet Gateway

+Routing Performance and Policy

RFC1254 Gateway Congestion Control Survey

RFC1246 Experience with the OSPF Protocol

RFC1245 OSPF Protocol Analysis

RFC1125 Policy Requirements for Inter-Administrative Domain Routing

RFC1124 Policy Issues in Interconnecting Networks

RFC1104 Models of Policy-Based Routing

RFC1102 Policy Routing in Internet Protocols

+Terminal Access

RFC1205 Telnet 5250 Interface

RFC1198 FYI on the X Window System

RFC1184 Telnet Linemode Option

RFC1091 Telnet Terminal-Type Option

RFC1080 Telnet Remote Flow Control Option

RFC1079 Telnet Terminal Speed Option

RFC1073 Telnet Window Size Option

RFC1053 Telnet X.3 PAD Option

RFC1043 Telnet Data Entry Terminal Option: DODIIS Implementation

RFC1041 Telnet 3270 Regime Option

RFC1013 X Window System Protocol, version 11: Alpha Update

RFC946 Telnet Terminal Location Number Option

RFC933 Output Marking Telnet Option

RFC885 Telnet End of Record Option

RFC861 Telnet Extended Options: List Option

RFC860 Telnet Timing Mark Option

RFC859 Telnet Status Option

RFC858 Telnet Suppress Go Ahead Option

RFC857 Telnet Echo Option

RFC856 Telnet Binary Transmission

RFC855 Telnet Option Specifications

RFC854 Telnet Protocol Specification

RFC779 Telnet Send-Location Option

RFC749 Telnet SUPDUP-Output Option

RFC736 Telnet SUPDUP Option

RFC732 Telnet Data Entry Terminal Option

RFC727 Telnet Logout Option

RFC726 Remote Controlled Transmission and Echoing Telnet Option

RFC698 Telnet Extended ASCII Option

+Other Applications

RFC1196 Finger User Information Protocol

RFC1179 Line Printer Daemon Protocol

RFC1129 Internet Time Synchronization: The Network Time Protocol

RFC1119 Network Time Protocol (version 2) Specification
and Implementation

RFC1057 RPC: Remote Procedure Call Protocol Specification: Version 2

RFC1014 XDR: External Data Representation Standard

RFC954 NICNAME/WHOIS

RFC868 Time Protocol

RFC867 Daytime Protocol

RFC866 Active Users

RFC865 Quote of the Day Protocol,

RFC864 Character Generator Protocol

RFC863 Discard Protocol

RFC862 Echo Protocol

Network Management

RFC1271 Remote Network Monitoring Management Information Base

RFC1253 OSPE version 2: Management Information Base

RFC1243 Appletalk Management Information Base

RFC1239 Reassignment of Experimental MIBs to Standard MIBs

RFC1238 CLNS MIB for Use with Connectionless Network Protocol (ISO 8473) and End System to Intermediate System (ISO 9542)

RFC1233 Definitions of Managed Objects for the DS3 Interface Type

RFC1232 Definitions of Managed Objects for the DS1 Interface Type

RFC1231 IEEE 802.5 Token Ring MIB

RFC1230 IEEE 802.4 Token Bus MIB

RFC1229 Extensions to the Generic-Interface MIB

RFC1228 SNMP-DPI: Simple Network Management Protocol Distributed Program Interface

RFC1227 SNMP MUX protocol and MIB

RFC1224 Techniques for Managing Asynchronously Generated Alerts

RFC1215 Convention for Defining Traps for Use with the SNMP

RFC1214 OSI Internet Management: Management Information Base

RFC1213 Management Information Base for Network Management of TCP/IP-based Internets: MiB-II

RFC1212 Concise MIB Definitions

RFC1187 Bulk Table Retrieval with the SNMP

RFC1157 Simple Network Management Protocol (SNMP)

RFC1156 Management Information Base for Network Management of TCP/IP-based Internets

RFC1155 Structure and Identification of Management Information for TCP/IP-Based Internets

RFC1147 FYI on a Network Management Tool Catalog: Tools for Monitoring and Debugging TCP/IP Internets and Interconnected Devices

RFC1089 SNMP over Ethernet

+Tunneling

RFC1241 Scheme for an Internet Encapsulation Protocol: Version 1

RFC1234 Tunneling IPX Traffic through IP Networks

RFC1088 Standard for the Transmission of IP Datagrams over NetBIOS Networks

RFC1002 Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Detailed Specifications

RFC1001 Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Concepts and Methods

+OSI

RFC1240 OSI Connectionless Transport Services on Top of UDP: Version 1

RFC1237 Guidelines for OSI NSAP Allocation in the Internet

RFC1169 Explaining the Role of GOSIP

+Security

RFC1244 Site Security Handbook

RFC1115 Privacy Enhancement for Internet Electronic Mail: Part III Algorithms, Modes, and Identifiers [Draft]

RFC1114 Privacy Enhancement for Internet Electronic Mail: Part II Certificate-Based Key Management [Draft]

RFC1113 Privacy Enhancement for Internet Electronic Mail: Part I— Message Encipherment and Authentication Procedures [Draft]

RFC1108 Security Options for the Internet Protocol

+Miscellaneous

RFC1251 Who"s Who in the Internet: Biographies of IAB, IESG, and IRSG Members

RFC1207 FYI on Questions and Answers: Answers to Commonly Asked "Experienced Internet User

RFC1206 FYI on Questions and Answers: Answers to Commonly Asked "New Internet User" Questions

جلسه چهارم

Command Prompt چیست؟

در بسیاری از درس‌های آینده از Command Prompt (خط فرمان) ویندوز استفاده خواهیم کرد. برای باز کردن آن یکی از روش‌های زیر را به کار برید:

۱- مسیر زیر را در ویندوز طی کنید:

```
Start > Programs > Accessories > Command Prompt
```

۲- در قسمت Run بنویسید: command یا cmd

پیدا کردن ip یک سایت با دانستن آدرس اینترنتی آن (پیدا کردن ip سرور)

برای این کار روشهای مختلفی هست:

۱- در Internet Explorer (IE) آدرس را تایپ کنید و Enter را فشار دهید. در قسمت پایین مرورگر یعنی Status Bar پس از چند لحظه برای مدت کوتاهی ip نمایش داده می‌شود و می‌توانید آنرا یادداشت کنید. اگر طول این مدت بسیار کوتاه است می‌توانید از صفحه عکس بگیرید (با دکمه Print Screen) و در یک نرم‌افزار گرافیکی بعد از باز کردن یک صفحه خالی به کمک Ctrl+V آنرا مشاهده کنید. [عجب راه احمقانه‌ای ;-)

اگر این کار را برای www.yahoo.com انجام دهیم:

که همان شماره ip برای www.yahoo.com است.

نکته بسیار مهم این است که به‌دلیل ضریب اشتباه بسیار بالای آن هیچ‌گاه از این روش استفاده نکنید. نتایج ممکن است کاملا اشتباه باشد که بعدا میگم چرا.

۲- دستور ping را در command prompt صادر کنید:

```
ping domain
```

در این حالت می‌توانم ip آن سایت را ملاحظه کنم. (البته کار اصلی ping یک چیز دیگست و میشه گفت داریم ازش سوءاستفاده می‌کنیم). مثلا برای پیدا کردن ip سازین می‌نویسم:

```
ping sazin.com
```

و جواب می‌شنوم:

```
Pinging sazin.com [63.148.227.65] with 32 bytes of data:

Reply from 63.148.227.65: bytes=32 time=821ms TTL=111
Reply from 63.148.227.65: bytes=32 time=821ms TTL=111
Reply from 63.148.227.65: bytes=32 time=822ms TTL=111
Reply from 63.148.227.65: bytes=32 time=811ms TTL=111

Ping statistics for 63.148.227.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 811ms, Maximum =  822ms, Average =  818ms
```

ملاحظه می‌فرمایید که ip سازین ٦٣,١٤٨,٢٢٧,٦٥ است.

اگر دستور ping را به‌جای sazin.com برای www.sazin.com صادر کنید، جواب همان است. البته برای سایت‌های بزرگ جواب‌های حاصل متفاوت خواهد بود.

۳- روش بعدی و کامل‌ترین روش whois کردن به بعضی سایت‌های خاص است. بعدا این را کامل‌تر توضیح می‌دم ولی فعلا روشش رو می‌گم. آدرس زیر را در مرورگر خود تایپ کنید:

```
http://www.samspade.org/t/ipwhois?a=xxxxxx
```

که به‌جای xxxxxx آدرس مورد نظر را تایپ کنید. مثلا برای sazin.com یکی از دو آدرس زیر را باید تایپ کرد:

```
http://www.samspade.org/t/ipwhois?a=sazin.com
```

http://www.samspade.org/t/ipwhois?a=www.sazin.com

چیزی که در صفحه ظاهر می‌شود به صورت زیر است:

```
whois -h magic 63.148.227.65
sazin.com resolves to 63.148.227.65

Trying whois -h whois.arin.net 63.148.227.65
Qwest Communications NET-QWEST-BLKS-2 (NET-63-144-0-0-1)
                                63.144.0.0 - 63.151.255.255
Neutron Digital Media Corp. QWST-63-148-224 (NET-63-148-224-0-1)
                                63.148.224.0 - 63.148.231.255

# ARIN Whois database, last updated 2002-09-04 19:05
# Enter ? for additional hints on searching ARIN"s Whois database.
```

که آدرس ip در سطر اول و دوم ذکر شده است.

اگر دو روش آخر را برای سایت بزرگ yahoo انجام دهیم، نتایج زیر را می‌بینیم:

<-- روش ping :

www.yahoo.com ====> ٦٤,٥٨,٧٦,٢٢٩

yahoo.com ====> ٦٦,٢١٨,٧١,١٩٨

<-- روش whois :

www.yahoo.com و... ====> ٦٦,٢١٨,٧١,٨٦

yahoo.com و ٦٤,٥٨,٧٩,٢٣٠ ====> ٦٦,٢١٨,٧١,١٩٨

نتایج حاصل گویای آن است که چرا بهتر است از whois استفاده کنیم.

تقسیم بندی آدرس‌های ip

آدرس‌های ip به ۵ کلاس تقسیم‌بندی می‌شوند که A تا E نام دارند ولی از این بین سه کلاس اول (یعنی C,B,A) کاربرد عملی دارند که آنها را شرح می‌دهیم:

۱- کلاس A: اگر ip را به‌صورت xxx.yyy.yyy.yyy در نظر بگیرید، این کلاس تمام ipهایی را شامل می‌شود که xxx بین ۱ تا ۱۲۶ است. این کلاس ویژه backbone های بزرگ اینترنتی است و در هنگام ثبت domain برای گرفتن ip از آنها استفاده می‌شود. بنابراین اکثر سایت‌ها چنین ipهایی دارند. این کلاس را /۸ هم می‌گویند.

۲- کلاس B: این کلاس تمام ipهایی را شامل می‌شود که xxx بین ۱۲۸ و ۱۹۱ است. این کلاس هم از جمله کلاس‌های پرکاربرد است. این کلاس را /۱٦ هم می‌گویند.

۳- کلاس C: این این کلاس تمام ipهای را شامل می‌شود که xxx بین ۱۹۲ و ۲۲۳ است. این کلاس معمولا به ISP هایی که خدمات dial-up ارائه می‌دهند، تعلق می‌گیرد (این جمله چندان مستند نیست.). بنابراین اگر به‌صورت dial-up به اینترنت متصل شوید، چنین ip می‌گیرید. این کلاس را /۲٤ هم می‌گویند.
سوالی که پیش می‌آید این است که xxx چرا نه در کلاس A و نه در B، عدد ۱۲۷ را شامل نمی‌شود؟ جواب این است که ۱۲۷ برای کامپیوتر خودمان رزرو شده است. مثلا ۱۲۷,۰,۰,۱ معمولا یعنی localhost یعنی خودمان.

به‌دست آوردن ip خودتان بعد از اتصال به اینترنت

برای این‌کار راههای متفاوتی وجود دارد:

۱- راحت‌ترین راه استفاده از دستور ipconfig است. من با تایپ کردن آن به نتایج زیر رسیدم:

```
Windows 2000 IP Configuration

PPP adapter neda:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 217.66.198.116
        Subnet Mask . . . . . . . . . . . : 255.255.255.255
        Default Gateway . . . . . . . . . : 217.66.198.116
```

که آدرس ip تان را می‌توانید در سطر Ip Address ببینید. (مسئله پروکسی را فعلا نادیده بگیرید)

۲- بعد از اتصال به اینترنت حداقل یک صفحه باز کنید و بعد دستور netstat -n را در command prompt تایپ کنید. من با تایپ این دستور به نتایج زیر رسیدم:

Active Connections

Proto	Local Address	Foreign Address	State
TCP	217.66.198.116:2469	64.58.76.177:80	ESTABLISHED
TCP	217.66.198.116:2471	66.163.175.130:80	ESTABLISHED
TCP	217.66.198.116:2473	212.73.194.143:80	ESTABLISHED
TCP	217.66.198.116:2474	212.73.194.143:80	ESTABLISHED
TCP	217.66.198.116:2476	212.73.194.136:80	SYN_SENT

ستونی که زیر عبارت Local Address قرار دارد، ip من در آن اتصال است. بنابراین ip من در آن اتصال ۲۱۷,٦٦,۱۹۸,۱۱٦ بوده است.

پیدا کردن ip طرف مقابل هنگام chat با yahoo messenger

نکته: این روش قدیمی شده، الان دیگه کار نمی‌کنه

می‌خواهیم درباره یک کلاینت مثلا کسی که مثل شما یک اتصال مثلا dial-up به اینترنت دارد و فرضا دارد با شما chat می‌کند، کسب اطلاعات کرد.

در این مورد هم اولین نکته‌ای که باید کشف شود، ip اوست. در این جلسه می‌خوام بهتون یاد بدم که وقتی با یه نفر از طریق yahoo messenger به صورت pm چت می‌کنید، چطوری می‌تونید ip اش رو پیدا کنید. البته باید توجه کرد که این روش گاهی کار نمی‌کند. نیز فرض می‌کنم که فقط با یک نفر دارید چت می‌کنید.

یکی از دستورهای زیر را تایپ می‌کنید:

netstat -n

netstat

دستور اولی برای پیدا کردن ip طرف مقابل است و دستور دوم گاه می‌تواند اسم کامپیوتر او را برای شما نشان دهد.

من دستور netstat -n را تایپ کردم و به نتایج زیر رسیدم:

Active Connections

```
Proto  Local Address          Foreign Address        State
TCP    195.219.176.126:1296   66.163.173.77:5050     ESTABLISHED
TCP    195.219.176.126:1341   66.218.75.149:80       LAST_ACK
TCP    195.219.176.126:1325   212.234.112.74:5101    SYN_SENT
```

اولین کاری که می‌کنید این است که سطری را پیدا می‌کنید که در Local Address یا Foreign Address آن، پورت ۵۱۰۱ داشته باشد. در این مثال سطر آخر، سطر مورد نظر ماست. زیرا در ستون Foreign Address از سطر آخر، پورت آن ۵۱۰۱ است. البته اگر در ستون Local Address هم بود، فرقی نمی‌کرد. وقتی آن سطر را پیدا کردید، ip طرف مقابل را از ستون Foreign Address از همان سطر پیدا می‌کنیم. در این مثال ip طرف مقابل ۲۱۲,۲۳٤,۱۱۲,۷٤ است.

اگر به‌جای netstat -n ، از netstat استفاده می‌کردم، به نتایج زیر می‌رسیدم:

```
Active Connections

Proto  Local Address          Foreign Address        State
TCP    artawill...:1296       cs55.msg.sc5.yahoo.com:5050  ESTABLISHED
TCP    artawill...:1298       dl3.yahoo.com:http           TIME_WAIT
TCP    artawill...:1325       Majid:5101                   SYN_SENT
```

ملاحظه می‌فرمایید که همه ip ها به معادل های اسمی تبدیل شده‌اند و در مورد همان سطر آخر به جای ip طرف مقابل اسم کامپیوتر فرد را می‌نویسد (البته در حالتی که طرف مقابل dial-up نباشد، قضیه فرق می‌کند.)

حالا فرض کنید که یک pm دیگر هم اضافه می‌شود. و دوباره دستور netstat -n را تایپ می‌کنم. حالا نتایج زیر را می‌بینم:

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    195.219.176.126:1296   66.163.173.77:5050     ESTABLISHED
  TCP    195.219.176.126:1344   64.58.77.197:80        ESTABLISHED
```

TCP	195.219.176.126:5101	212.234.112.74:3735	ESTABLISHED
TCP	195.219.176.126:5101	194.225.184.95:1460	ESTABLISHED

الان دوتا سطر دارم که دارای پورت ۵۱۰۱ باشد، و چون می‌دانم که ۲۱۲,۲۳۴,۱۱۲,۷۴ مربوط به نفر قبلی بود، پس ۱۹۴,۲۳۵,۱۸۴,۹۵ مربوط به pm دومی است.

جلسه پنجم

Whois چیست؟

تعریف کلی برای whois نمی‌توان ارائه داد ولی فعلا منظور ما از Whois همان کسب اطلاعات در مورد یک سایت است. (قبلا با نوع خاصی از whois برای تبدیل domain به ip آشنا شده‌اید).

کاری که امروز می‌خواهم انجام دهم کسب اطلاعات در مورد یک شماره ip و یا یک domain (مثلا irib.com) خاص است. برای کسب این اطلاعات باید به اینترنت وصل شده و به‌طریقی به یک سری سایت‌های خاص که وظیفه ثبت domain , ... را دارند متصل شده و اطلاعات را از آنها درخواست کنم. این سایت‌های خاص database (بانک‌های اطلاعاتی) ویژه این وظایف را دارند.

برای کسب این اطلاعات از سایت‌ها روش‌های زیر را می‌توان به‌کار برد:

۱- اگر از طریق سیستم عامل یونیکس یا لینوکس به اینترنت وصل شده‌اید، دستوری به اسم whois در آنها وجود دارد. و یا می‌توانید از نرم‌افزارهای خاصی که برای این سیستم‌عامل‌ها وجود دارد (مثل Xwhois) استفاده کنید. ولی فعلا بحث روی ویندوز است و این دستور در ویندوز وجود ندارد.

۲- برای whois کردن در ویندوز نرم‌افزارهای زیادی وجود دارد (که به زودی نوشتن یک whois متوسط را در زبان C یاد خواهم داد.) از مشهورترین این نرم‌افزارها Netscan tools و SamSpade است. ولی از اینها هم فعلا صرف نظر می‌کنم تا شما بیشتر با جزئیات این کار آشنا شوید.

۳- روشی که ما در این جلسه به کار می‌بریم، استفاده از سایت‌هایی است که این جستجو را برای ما انجام می‌دهند.

datebase های whois در چه سایت‌هایی وجود دارد؟

تعداد زیادی از سایت‌ها این داده‌ها را دارند که مشهورترین‌ها عبارتند از:

whois.internic.net (The InterNIC)
whois.onlinenic.com (The OnLineNIC)
whois.arin.net (American Registry for Internet Numbers)
whois.ripe.net (European IP Address Allocations)
whois.apnic.net (European IP Address Allocations)
whois.nic.mil (US Military)

whois.nic.gov (US Government)

اولین سایت مشهورترین سایت ثبت domain برای org , net , com است.

توجه کنید که امروزه سایت‌های مختلفی عمل ثبت domain را انجام می‌دهند و برای اینکه در مورد یک سایت خاص (که در واقع یک domain خاص دارد) اطلاعاتی کسب کنیم باید اطلاعات مربوطه را از آن سایتی بگیریم که ثبت domain را انجام داده است و چون این کار مشکلی است به جای استفاده از خود سایت‌های بالایی، از سایت‌هایی دیگر استفاده می‌کنیم که این کار را برای ما ساده‌تر می‌کنند (خود آن سایت‌ها در نهایت اطلاعاتشان را از سایت‌های اصلی می‌گیرند و فقط یک نقش واسط دارند... لازم به‌ذکر است که ایجاد چنین صفحات وبی زیاد هم مشکل نیست.). سایت مورد علاقه من برای کسب اطلاعات سایت زیر است:

http://www.samspade.org/t/whois?a=xxxxxxxxx

که بجای xxxxxxxxx آدرس سایت و یا ip آنرا می‌نویسیم و آدرس حاصله را در مرورگر خود می‌بینیم. مثلا اگر بخواهم در مورد سایت sazin.com اطلاعاتی به‌دست بیاورم، می‌نویسم:

http://www.samspade.org/t/whois?a=sazin.com

و اطلاعات زیر به دست می‌آید:

```
sazin.com is registered with BULKREGISTER.COM, INC. - redirecting
to whois.bulkregister.com

whois -h whois.bulkregister.com sazin.com
The data in Bulkregister.com"s WHOIS .....(deleted)

SazinNetWork
  2nd.Floor,Bldg#116,Mollasadra Ave.
  Tehran, TEH 14358
  IR

  Domain Name: SAZIN.COM

  Administrative Contact:
```

Mohammad Hajati mjhajati@hotmail.com

Sazin Rasaneh Co.

4th.Floor,Bldg.339,Mirdamad Ave.

Tehran, TEH 19696

IR

Phone: +98 21 8787064

Fax: +98 21 8789841

Technical Contact:

Mohammad Hajati mjhajati@hotmail.com

Sazin Rasaneh Co.

4th.Floor,Bldg.339,Mirdamad Ave.

Tehran, TEH 19696

IR

Phone: +98 21 8787064

Fax: +98 21 8789841

Record updated on 2002-03-02 05:47:36

Record created on 1999-05-10

Record expires on 2007-05-10

Database last updated on 2002-09-15 08:58:02 EST

Domain servers in listed order:

DNS.SAZIN.COM	80.78.134.221
S1.SAZIN.COM	63.148.227.63
S2.SAZIN.COM	63.148.227.64

ملاحظه می‌کنید که اطلاعات زیادی در مورد این سایت را به این طریق می‌توان به‌دست آورد. اطلاعاتی درمورد آدرس ISP ، شخصی که به‌عنوان Admin کار ثبت را انجام داده است و ... البته باز هم نمی‌توان در مورد صحت و سقم آن اظهارنظر قطعی داشت.

تعدادی از مهمترین اطلاعات را در قسمت DNS Servers یا Domain servers (که در این مثال در آخر قرار دارد) می‌بینید. بعدا در مورد این آدرس‌ها توضیح خواهم داد ولی فعلا می‌گم که به کمک همین چند آدرسی که در آخر به‌دست آوردیم به کمک دستوری به نام nslookup می‌توان اطلاعات با ارزش‌تری به‌دست آورد که به‌زودی یاد می‌گیرید.

ادامه بحث whois

قبلا در مورد ip whois و dns whois صحبت کردم. بحث dns whois (کسب اطلاعات در مورد یک domain خاص) رو ادامه می‌دم.

از سایت SamSpade استفاده کردم. اگر این whois رو تست کرده باشید، می‌دانید که برای یک سری از domain (دامنه) ها، جواب نمی‌دهد. مثال آن سایت‌هایی است که دارای دامنه جغرافیایی مثلا ایران هستند، در مورد دامنه‌های جغرافیایی ایران باید گفت که به ir. ختم می‌شوند (مثلا: neda.net.ir). مثال دیگری که در whois سایت SamSpade کار نمی‌کند، تعدادی از دامنه‌های com. , net. , org. هستند که در internic.net ثبت نشده‌اند، بلکه در domainpeople.com ثبت شده‌اند (مثلا sanjesh.org). چند سال پیش ثبت domain هایی که در گروه org, net, com بودند، مختص به internic.net بود ولی الان دیگر اینطور نیست.

کاری که شما باید برای whois کردن باید انجام دهید، توجه به نوع آن domain است که از نوع com است یا ir است یا biz است و ... بعد از آن از یکی از سایت‌های زیر استفاده کنید :

۱- internic.net:

برای com , net , org , edu عالی است. برای museum , int , info , coop , biz , arpa, aero هم می‌تواند استفاده شود.

صفحه وب مربوطه عبارت است از http://www.internic.net/whois.html یا می‌توانید مستقیما در مرورگر بنویسید:

whois_nic=xxxxxxxx&http://www.internic.net/cgi/whois?type=domain که به‌جای xxxxxxxx مثلا باید بنویسید: far30.com

۲- nic.ir :

برای ir استفاده می‌شود.

صفحه وب مربوطه عبارت است از http://whois.nic.ir/

۳- www.tv :

برای tv , biz , info , cc عالی است.

صفحه وب مربوطه عبارت است از http://www.tv/ یا می‌توانید مستقیما در مرورگر بنویسید:

tld=zzzz&http://www.tv/en-def-8e33e8cf5e3c/cgi-bin/whois.cgi?domain=yyyyyy

که اگر بخواهم مثلا hack.tv را whois کنم به جای yyyyy باید بنویسید hack و به جای zzzz باید بنویسید tv

۴- domainpeople.com :

برای biz , name , com , net , org , info عالی است.

صفحه وب مربوطه عبارت است از http://whois.domainpeople.com/

همانطور که ملاحظه می‌فرمایید، com , net , org در ۱ و ۴ مشترک است. علت آن است که بعضی‌ها در اولی و بعضی‌ها در چهارمی ثبت می‌شوند ولی برای whois کردن فرقی نمی‌کنه که شما از اولی استفاده کنید یا چهارمی چون همدیگر رو ساپورت می‌کنند.

چگونگی استفاده از nslookup

وقتی که DNS Server یک سایت را به‌دست آورده باشیم (از طریق whois)، به کمک دستور nslookup می‌توان اطلاعاتی اضافی در مورد آن سایت پیدا کرد. طریقه استفاده این دستور به صورت زیر است:

فرض کنید که من می‌خواهم از Domain Server سایت خودم (far30.com) اطلاعاتی به‌دست بیارم. اگر به این سایت whois کنم، می‌بینم که دوتا Name Server یا Server DNS دارد:

```
s1.sazin.com
s2.sazin.com
```

حالا دیگر آدرس DNS Server مربوط به com.far30 را دارم و می‌توانم شروع کنم:

۱- دستور nslookup را در prompt command نوشته و اجرا می‌کنم:

```
C:\>nslookup
```

و نتایج را می‌بینم:

```
*** Can"t find server name for address 192.168.20.3: Non-exi...
*** Can"t find server name for address 192.168.20.1: Non-exi...
*** Default servers are not available
Default Server:  UnKnown
Address:  192.168.20.3
 >
```

علامت > یعنی شما می‌توانید دستورات را تایپ کنید.

۲- در جلوی علامت < دستور زیر را تایپ می‌کنیم:

```
> server dns_server
```

که به جای dns_server باید آدرس DNS Server سایت موردنظر را بنویسم. پس برای سایت far30.com می‌شود:

```
> server s1.sazin.com
```

و جواب می‌شنوم:

```
Default Server:  s1.sazin.com
Address:  63.148.227.63
```

اگر در این مرحله پیغام خطا می‌گیرید، باید دوباره این دستور را تایپ کنید و نیز می‌توانید از DNS Server دومی که در whois برای far30.com به‌دست آوردیم ، استفاده کنیم.

۳- دستور زیر را تایپ کنید:

```
> set type=any
```

۴- حالا به کمک دستور زیر اطلاعات را به‌دست می‌آوریم:

```
> ls -d site_name.
```

که برای far30.com می‌شود:

```
>ls -d far30.com.
```

دقت کنید که بعد از اسم سایت یک نقطه (dot) گذاشته‌ام، شما هم بهتر است این طوری بنویسید. نتایج زیر حاصل می‌شود:

```
[s1.sazin.com]
 far30.com.                SOA    s1.sazin.com admin.sazin.com.
(2002070412 3600 600 86400 3600)
 far30.com.                A      63.148.227.65
 far30.com.                NS     s1.sazin.com
 far30.com.                NS     s2.sazin.com
 far30.com.                MX     10   mail.far30.com
 far30.com.                MX     15   far30.com
    CNAME  far30.com     ftp
 mail                      A      63.148.227.65
 www                       CNAME  far30.com
 far30.com.                SOA    s1.sazin.com admin.sazin.com.
(2002070412 3600 600 86400 3600)
>
```

بعدا در مورد کاربرد تک‌تک اینها صحبت خواهم کرد ولی بعضی از آنها همین‌طوری هم اطلاعات واضحی دارند.

۵- دستور exit را مقابل > تایپ کرده و از nslookup خارج می‌شویم.

شما برای تمرین همین کار را در مورد سایت neda.net.ir انجام دهید.

جلسه ششم

TCP و UDP چیست؟

مدل TCP/IP که برای ارتباط اینترنتی به‌کار می‌رود، می‌توان به لایه‌های مختلفی تقسیم‌بندی کرد که بعدا بیشتر توضیح می‌دم، اما یکی از این لایه‌ها، لایه ارتباط host2host است که خود شامل دو پروتکل است به نامهای TCP و UDP :

۱- TCP (Transmission Control Protocol) :

این پروتکل قوی‌تر و قابل اعتمادتر است و اصولا پروتکل مهمتری نسبت به UDP محسوب می‌شود. این پروتکل توانایی بازبینی بسته‌هاو کنترل خطا را هم دارد.

۲- (UDP) User Datagram Protocol) :

این پروتکل برای کاهش overflow طراحی شده است و در خیلی از موارد وابسته به TCP است.

نکته مهم این است که وقتی با یک پورت خاص روی یک کامپیوتر دیگر ارتباط برقرار می‌کنیم، این ارتباط می‌تواند از نوع TCP یا UDP باشد. بنابراین وقتی می‌خواهیم یک کامپیوتر خاصی را از نظر پورت‌ها بررسی کنیم، هردو باید بررسی شود.

تقسیم‌بندی پورت‌ها از روی شماره آنها

۱- پورت‌های ۰ تا ۱۰۲۳ :

مشهورترین پورت‌ها هستند و معمولا هرکدام برای یک سرویس خاص استفاده می‌شود. با تعدادی از این پورت‌ها در جلسات قبل آشنا شده‌اید.

۲- پورت‌های ۱۰۲٤ تا ٤۹۱٥۱ :

این سری از پورت‌ها مشخصا با هیچ‌یک از سرویس‌های اینترنتی مرتبط نیستند بلکه وقتی که با یک ابزار شبکه مانند مرورگر اینترنت(مثل Internet Explore یا Netscape Navigator)، نرم‌افزار ارسال و دریافت E-mail (مثل Outlook یا Edura)، نرم‌افزارهای FTP (مثل WS-FTP یا Cute-FTP) کار می‌کنید، یکی از این پورت‌ها به صورت random باز شده و یک ارتباط با سرور (با توجه به‌نوع سرویس اینترنتی که می‌دهد که یکی از پورت‌های ۰ تا ۱۰۲۳ است) برقرار شده و داده‌ها ارسال و دریافت می‌شوند. یعنی پورت شما یکی از پورت‌های این قسمت است و پورت سرور یکی از پورت‌های بالایی.این سری پورت‌ها را پورت‌های register شده هم می‌گویند.

۳- پورت‌های ٤٩١٥٢ تا ٦٥٥٣٥ :

این سری از پورت‌ها به‌ندرت استفاده می‌شوند. کاربرد اساسی آنها برای یک سری سرویس‌های خاص اینترنتی است و یا توسط trojanها (که برای Hack کردن کامپیوتر است) است. البته خیلی از trojanهای معروف از پورت‌های ردیف ۲ هم استفاده می‌کنند و این تقسیم‌بندی‌ها همیشه برقرار نیست و به‌همین علت است که گاهی پورت‌ها را به دودسته زیر ١٠٢٤ و بالای ١٠٢٤ تقسیم می‌کنند.

تکمیل لیست پورت‌ها

در جلسه دوم در مورد مهمترین پورت‌ها صحبت کردم. حالا یک لیست کامل‌تر را در این درس می‌گم. اگر می‌خواهید یک مرجع نسبتا کامل برای مراجعه داشته باشید، اینجا را کلیک کنید. دقت کنید درس امروز و نیز لینک بالا هیچ بحثی در مورد تروجان‌ها نمی‌کند زیرا تروجان‌های شناخته شده هم یک سری پورت پیش‌فرض دارند که در جای خود بحث خواهد شد.

Ports	TCP/UDP	Service or Application
7	tcp	echo
11	tcp	systat
19	tcp	chargen
21	tcp	ftp-data
22	tcp	ssh
23	tcp	telnet
25	tcp	smtp
42	tcp	nameserver
43	tcp	whois
49	udp	tacacs
53	udp	dns-lookup
53	tcp	dns-zone
66	tcp	oracle-sqlnet
69	udp	tftp
79	tcp	finger

80	tcp	http
81	tcp	alternative for http
88	tcp	kerberos or alternative for http
109	tcp	pop2
110	tcp	pop3
111	tcp	sunrpc
118	tcp	sqlserv
119	tcp	nntp
135	tcp	ntrpc-or-dec
139	tcp	netbios
143	tcp	imap
161	udp	snmp
162	udp	snmp-trap
179	tcp	bgp
256	tcp	snmp-checkpoint
389	tcp	ldap
396	tcp	netware-ip
407	tcp	timbuktu
443	tcp	https/ssl
445	tcp	ms-smb-alternate
445	udp	ms-smb-alternate
500	udp	ipsec-internet-key-exchange (ike)
513	tcp	rlogin
513	udp	rwho
514	tcp	rshell
514	udp	syslog
515	tcp	printer
515	udp	printer
520	udp	router

524	tcp	netware-ncp
799	tcp	remotely possible
1080	tcp	socks
1313	tcp	bmc-patrol-db
1352	tcp	notes
1433	tcp	ms-sql
1494	tcp	citrix
1498	tcp	sybase-sql-anywhere
1524	tcp	ingres-lock
1525	tcp	oracle-srv
1527	tcp	oracle-tli
1723	tcp	pptp
1745	tcp	winsock-proxy
2000	tcp	remotely-anywhere
2001	tcp	cisco-mgmt
2049	tcp	nfs
2301	tcp	compaq-web
2447	tcp	openview
2998	tcp	realsecure
3268	tcp	ms-active-dir-global-catalog
3268	udp	ms-active-dir-global-catalog
3300	tcp	bmc-patrol-agent
3306	tcp	mysql
3351	tcp	ssql
3389	tcp	ms-termserv
4001	tcp	cisco-mgmt
4045	tcp	nfs-lockd
5631	tcp	pcanywhere
5800	tcp	vnc

6000	tcp	xwindows
6001	tcp	cisco-mgmt
6549	tcp	apc
6667	tcp	irc
8000	tcp	web
8001	tcp	web
8002	tcp	web
8080	tcp	web
9001	tcp	cisco-xremote
12345	tcp	netbus
26000	tcp	quake
31337	udp	backorifice
32771	tcp	rpc-solaris
32780	udp	snmp-solaris
43188	tcp	reachout
65301	tcp	pcanywhere-def

چگونه به یک پورت Telnet کنیم؟

برای اینکه عملکرد یک پورت برای شما روشن شود، باید به آن پورت Telnet کنید. (البته معمولا تعدادی از پورت‌هایی را که ممکن است اطلاعاتی مهم را در اختیار هکرها قرار دهند مثل پورت ۷۹ معمولا بسته است و ارتباط با آنها شاید برقرار نشود.) برای telnet کردن در prompt command دستور زیر را تایپ کنید:

```
telnet hostname portnum
```

در این دستور به‌جای hostname شماره ip و یا نام سایت را وارد می‌کنید و به‌جای portnum شماره پورت و یا معادل آن از جدول. مثلا برای تلنت کردن به پورت ۱۳ که ساعت و تاریخ را به‌دست می‌دهد در کامپیوتری به اسم www.iums.ac.ir می‌نویسید:

```
telnet iums.ac.ir 13
telnet iums.ac.ir daytime
```

هر دو این دستورات معادل هم هستند.

تلنت کردن معمولا اولین کاری است که یک هکر برای هک کردن یک سایت انجام می‌دهد، زیرا بعضی از پورت‌ها در صورت بسته نبودن روی آن سرور، معمولا حاوی اطلاعات بسیار مهمی هستند.

همین الان شروع کنید و مثل یک هکر واقعی به کامپیوترهای مختلف و پورت‌های گوناگون تلنت کنید.

جلسه هفتم

انواع Scanning

دو نوع معمول Scanning وجود دارد:

۱- Port Scanning :

در این حالت ما IP یا IPهای مورد نظر را انتخاب کرده‌ایم و حالا می‌خواهیم بدانیم که کدام پورت‌ها روی آن کامپیوترها باز است.

۲- IP Scanning :

در این اسکنینگ می‌خواهیم بدانیم که از بین یک مجموعه ip ، کدام‌ها up و کدام‌ها down هستند. یعنی کدام ip ها الان قابل دسترسی هستند (یعنی به یه کامپیوتر در اینترنت نسبت داده شده است!) فرض کنید که شما یک سری IP مربوط به یک ISP خاص را دارید و می‌خواهید بدانید که در این لحظه کدام‌ها فعال (up) هستند تا فقط آنها را بررسی کنید و نه همه را. (این کار معمولا موقعی پیش می‌آید که قرار است کلاینت هک کنید و مهم نیست چه کسی باشد)

چگونه یک ارتباط TCP برقرار می‌شود که بگوییم فلان پورت باز است یا نه؟

برای اینکه تعیین کنیم که یک پورت روی یک سرور باز است یا نه، معمولا باید یک TCP connect scan انجام دهیم. اول این را بگم که Port Scanning انواع مختلف دارد که فعلا ما نوع TCP connect را مدنظر داریم. این نوع اسکن سه مرحله دارد که به آن TCP's 3-way handshakeمی‌گویند:

۱- اول کامپیوتر ما به سمت سرور یک SYN packet می‌فرستد که به معنی درخواست اتصال است.

۲- اگر سرور این درخواست را قبول کند، در مرحله دوم سرور به سمت ما یک SYN/ACK packet می‌فرستد.

۳- در مرحله آخر کامپیوتر ما یک ACK packet به سمت سرور می‌فرستد.

نوع دیگری از پورت اسکن TCP SYN scan نام دارد. با توجه به اینکه معمولا اگر پورت اسکن به روش بالا (TCP connect scan) انجام دهیم، معمولا در سرور این اتصال ذخیره خواهد شد و بعدا می‌تواند ما را ردیابی کنند، به جای آن می‌توان از TCP SYN scan استفاده کرد. در این نوع اسکن،

مراحل ۱ و ۲ از بالا انجام می‌شود ولی مرحله ۳ نه! اگر در مرحله ۲ به ما یک SYN/ACK برسد، آن پورت باز است و اگر یک RST/ACK برسد، یعنی بسته است.

انواع دیگری از پورت اسکنینگ هم وجود دارد مثل UDP scan, TCP Window scan, TCP ACK Scan scan, TCP Null, TCP Xmas Tree, TCP FIN

چگونه می‌توان عمل Port scanning را انجام داد؟

در تمام مطالبی که تا این مرحله گفته‌ام سعی کرده‌ام که فقط از ابزارهای موجود در ویندوز استفاده کنم و هیچ ابزار دیگری به‌کار نبرم، اما در مبحث پورت اسکنینگ چون هیچ ابزاری در ویندوز برای این کار نیست، به‌ناچار باید یک سری برنامه را از اینترنت داونلود کنید. (توجه داشته باشید که فعلا حرفی از لینوکس نزده‌ام و سعی می‌کنم فعلا هیچ بحثی را در مورد آن مطرح نکنم)

برای Scanning Port می‌توان از ابزارهای مختلفی استفاده کرد که اکثرا برای لینوکس طراحی شده‌اند، اما مهم‌ترین پورت اسکنرها برای ویندوز عبارتند از:

۱- نرم‌افزار NMapWin v1.3.0 :

نسخه گرافیکی و مخصوص ویندوز برای nmap است (nmap در لینوکس استفاده می‌شود). nmap از کامل‌ترین ابزارهایی است که هکرها استفاده می‌کنند که علاوه بر توانایی انواع پورت اسکنینگ‌ها، می‌تواند کارهای بسیاری چون تشخیص سیستم‌عامل سرور و ... را انجام دهد. این ابزار را بعدا توضیح خواهم داد ولی فعلا برای کار ما بیش از حد کامله ;-)

۲- NetScanTools Pro 2000 :

این هم از بهترین‌هاست ولی چون پولی است به جای داونلود باید در CD هایی که در بازار هست پیدایش کنید.

۳- WinScan :

برای اسکن کردن TCP (ونه UDP) می‌توانید از آن استفاده کنید. من زیاد ازش خوشم نیومد.

۴- ipEye v1.2 :

من در این درس از این نرم‌افزار استفاده خواهم کرد، برای داونلود آن می‌توانید به سایت http://www.ntsecurity.nu مراجعه کنید. لازم است بگویم که این نرم‌افزار فقط در ویندوز ۲۰۰۰ و xp کار می‌کند و نیز در یک بار اجرا فقط یک ip را می‌تواند تست کند. ضمنا فقط TCP را تست می‌کند.

چگونه از ipEye برای پورت اسکنینگ استفاده کنیم؟

با تایپ ipEye در command prompt این نتایج ظاهر می‌شود:

```
ipEye 1.2 - (c) 2000-2001, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
        - http://ntsecurity.nu/toolbox/ipeye/

Error: Too few parameters.

Usage:

 ipEye <target IP> <scantype> -p <port> [optional parameters]
 ipEye <target IP> <scantype> -p <from port> <to port>
[optional parameters]

 <scantype> is one of the following:
   -syn  = SYN scan
   -fin  = FIN scan
   -null = Null scan
   -xmas = Xmas scan>br>
   (note: FIN, Null and Xmas scans don"t work against Windows systems.

 [optional parameters] are selected from the following:
   -sip <source IP>  = source IP for the scan
   -sp <source port> = source port for the scan
   -d <delay in ms>  = delay between scanned ports in milliseconds
                       (default set to 750 ms)
```

فرض کنید که می‌خواهیم سایت سازین را از نظر پورت‌ها از پورت ۱ تا ۲۰۰ تست کنیم. اول باید ip آن را به دست بیاوریم که می‌شود، ٦٣,١٤٨,٢٢٧,٦٥ و حالا به کمک دستور زیر آن را بررسی می‌کنیم:

```
ipeye 63.148.227.65 -syn -p 1 200
```

دقت کنید که ۶۳,۱۴۸,۲۲۷,۶۵ عدد ip سازین، syn- یعنی SYN SCAN و p- 1 200 یعنی تست از پورت ۱ تا ۲۰۰ باشد. البته پارامترهای دیگری را هم می‌شود ست کرد که فعلا به درد ما نمی‌خورد. با اجرای این دستور به نتایج زیر می‌رسیم:

```
ipEye 1.2 - (c) 2000-2001, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
        - http://ntsecurity.nu/toolbox/ipeye/


1-20 [drop]
21 [open]
22 [closed or reject]
23-24 [drop]
25 [open]
26-52 [drop]
53 [open]
54-79 [drop]
80 [open]
81-109 [drop]
110 [open]
111-142 [drop]
143 [open]
144-200 [drop]
201-65535 [not scanned]
```

Closed یعنی کامپیوتر در آن طرف هست ولی به پورت گوش نمی‌دهد، Reject یعنی اینکه یک firewall هست که اجازه اتصال به آن پورت را نمی‌دهد، Drop یعنی اینکه یک firewall همه‌چیز را پس می‌زند و یا اصلا کامپیوتری اونور نیست، Open هم که یعنی باز.

در مورد سازین می‌بینید که از بین پورت‌های ۱ تا ۲۰۰ ، پورت‌های ۲۱، ۲۵، ۵۳، ۸۰، ۱۱۰، ۱۴۳ باز است و می‌توان به آنها telnet کرد. دقت کنید که تا تمام پورت‌هایی که مشخص شده، تست نشده است، هیچ نتیجه‌ای نشان داده نمی‌شود و یه‌کم صبر می‌خواد.

تعیین پورت‌های باز کامپیوتر خودتان

می‌خواهیم درباره کامپیوتر خودمان این اطلاعات را پیدا کنیم. برای این کار یکی از دستورات زیر را به کار می‌بریم:

```
netstat -an
netstat -a
```

فرق این دو دستور در این است که اولی پورت‌ها را به صورت عددی و دومی به صورت معادل اسمی آن پورت می‌نویسد. مثلا معادل اسمی پورت ۷ ، echo است.

مثلا اگه netstat -an را تایپ کنم، به اطلاعات زیر می‌رسم:

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:7	0.0.0.0:0	LISTENING
TCP	0.0.0.0:9	0.0.0.0:0	LISTENING
TCP	0.0.0.0:13	0.0.0.0:0	LISTENING
TCP	0.0.0.0:17	0.0.0.0:0	LISTENING
TCP	0.0.0.0:19	0.0.0.0:0	LISTENING
TCP	0.0.0.0:21	0.0.0.0:0	LISTENING
TCP	0.0.0.0:25	0.0.0.0:0	LISTENING
TCP	0.0.0.0:53	0.0.0.0:0	LISTENING
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:119	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:143	0.0.0.0:0	LISTENING
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:515	0.0.0.0:0	LISTENING
TCP	0.0.0.0:563	0.0.0.0:0	LISTENING

TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1026	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1033	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1037	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1040	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1041	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1043	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1755	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1801	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3372	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:6034	0.0.0.0:0	LISTENING
TCP	0.0.0.0:6666	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7007	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7778	0.0.0.0:0	LISTENING
TCP	0.0.0.0:8181	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1039	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1433	0.0.0.0:0	LISTENING
TCP	127.0.0.1:2103	0.0.0.0:0	LISTENING
TCP	127.0.0.1:2105	0.0.0.0:0	LISTENING
TCP	127.0.0.1:2107	0.0.0.0:0	LISTENING
UDP	0.0.0.0:7	*:*	
UDP	0.0.0.0:9	*:*	
UDP	0.0.0.0:13	*:*	
UDP	0.0.0.0:17	*:*	
UDP	0.0.0.0:19	*:*	
UDP	0.0.0.0:68	*:*	
UDP	0.0.0.0:135	*:*	
UDP	0.0.0.0:161	*:*	

```
UDP    0.0.0.0:445            *:*
UDP    0.0.0.0:1030           *:*
UDP    0.0.0.0:1036           *:*
UDP    0.0.0.0:1038           *:*
UDP    0.0.0.0:1042           *:*
UDP    0.0.0.0:1075           *:*
UDP    0.0.0.0:1434           *:*
UDP    0.0.0.0:1645           *:*
UDP    0.0.0.0:1646           *:*
UDP    0.0.0.0:1755           *:*
UDP    0.0.0.0:1812           *:*
UDP    0.0.0.0:1813           *:*
UDP    0.0.0.0:3456           *:*
UDP    0.0.0.0:3527           *:*
UDP    127.0.0.1:53           *:*
UDP    127.0.0.1:1028         *:*
UDP    127.0.0.1:1029         *:*
UDP    127.0.0.1:1035         *:*
UDP    127.0.0.1:1044         *:*
UDP    127.0.0.1:1045         *:*
UDP    127.0.0.1:1100         *:*
```

من دستور را موقعی اجرا کردم که به اینترنت متصل نبودم. اگر همین کار را در زمان اتصال به اینترنت انجام می‌دادم، یک سری سطرهای جدید هم اضافه می‌شد که مربوط به آن اتصال می‌شد. و نیز دقت کنید که من سویچ an- را استفاده کردم و پورت‌ها به صورت عددی نمایش داده شده است که همین الان - الساعه - براتون توضیح می‌دم:

اولین نکته‌ای که به نظر می‌رسد، نامی است که برای هر ستون نوشته شده است:

```
Proto  Local Address          Foreign Address        State
```

Proto : یعنی پروتکل، که می‌تواند TCP یا UDP باشد.

Local Address : نشان‌دهنده ip کامپیوتر خودمان و شماره پورت‌هاست. مثلا سطر اول می‌گوید که ip من ۰,۰,۰,۰ است (دقت کنید که من به اینترنت متصل نیستم) و اولین پورت باز (از نوع TCP با توجه به اول سطر) عدد ۷ است زیرا این به صورت ۰,۰,۰,۰:۷ نوشته شده است که قسمت قبل از کاراکتر : ، ip است و بعد از کاراکتر :، پورت است.

Address Foreign : چون در این مثال از سویچ a- یا an- استفاده کرده‌ایم، کاربردی ندارد. ولی بعدا خواهید دید که اگر از یک سویچ دیگر استفاده کنیم، می‌تواند مهم باشد.

State : وضعیت اتصال را نشان می‌دهد

حالا اگه پورت‌ها را یکی یکی بررسی کنید، می‌بینید که در پروتکل TCP ، پورت‌های ۷، ۹، ۱۳، ۱۷، ۱۹، ۳۱ و... باز است و در پروتکل UDP ، پورت‌های ۷، ۹، ۱۳، ۱۷، ۱۹، ۶۸ و ... باز است.

حالا ممکن است بپرسید که این اطلاعات به چه دردی می‌خورد؟

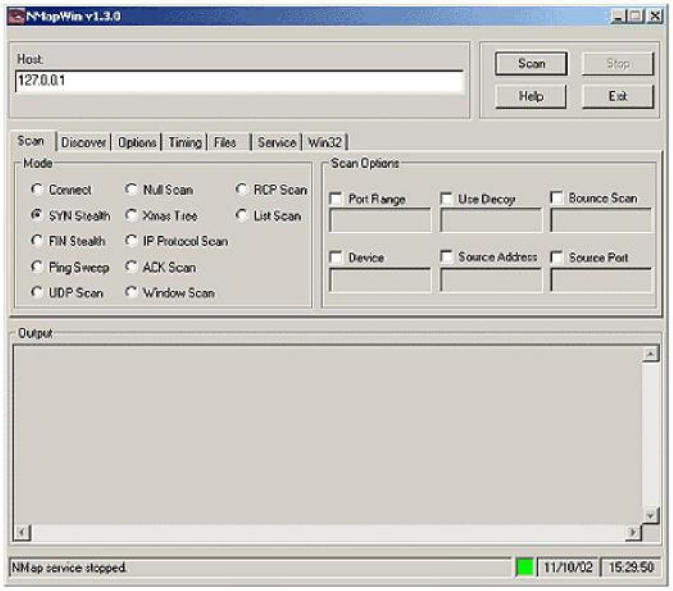
جواب این است که دانستن این اطلاعات برای محافظت از خودتان در برابر همکارانتان (هکرها) است. مثلا اگر یک تروجان روی کامپیوتر شما نصب شده باشد، با این دستور می‌توان آن را کشف کرد.

جلسه هشتم

معرفی nmap و NMapWin

اگر بخواهید مهم‌ترین ابزاری را که یک هکر برای footprinting استفاده می‌کند بدانید، آن نرم‌افزار nmap خواهد بود که برای سیستم‌های لینوکس و یونیکس طراحی شده است. برای هکرهای تازه‌کار که سیستم‌عامل ویندوز را به کار می‌برند، نسخه گرافیکی و تحت ویندوزی طراحی شده است که NMapWin نام دارد و همان امکانات را فراهم می‌آورد. بحث این جلسه درباره این نرم‌افزار است. برای داون‌لود این نرم‌افزار اینجا را کلیک کنید! اندازه برنامه ٦,١٨ مگابایت است و اگر اتصالتان dial-up است، کمی طول خواهد کشید. ضمنا توجه کنید که این برنامه مخصوص ویندوز ۲۰۰۰ و xp است.

این نرم‌افزار مجموعه ابزارهای footprinting مثل پورت اسکن، آی‌پی اسکن، تشخیص سیستم‌عامل کامپیوتر مورد نظر (OS detection) و ... را گرد هم آورده است. شکل ظاهری برنامه را در زیر می‌بینید:



بررسی ظاهر برنامه

شکل ظاهری برنامه چهار قسمت دارد:

۱- Network Section :

بالاترین قسمت پنجره برنامه است که محلی برای ورود ip یا ip ها دارد به نام Host. بعد از وارد کردن ip و تنظیم کردن پارامترها، دکمه Scan را کلیک می‌کنیم تا کار اسکن شروع شود.

اگر قرار باشد بیش از یک ip وارد شود، این کار را می‌توان به صورت‌های مختلف انجام داد. مثلا: ۱۹۲,۱۳۰.*.* یعنی تمام ip هایی که با ۱۹۲,۱۳۰ شروع می‌شوند ولی دو عدد بعدی هرچیزی می‌تواند باشد. و نوشتن به صورت ۱۹۲,۱۳۰,۱۲۰,۱۲-۱۵ یعنی عدد آخری می‌تواند از ۱۲ تا ۱۵ باشد.

۲- Option Folder :

این قسمت در واقع محل تنظیمات است و به کمک آن مشخص می‌کنیم که از برنامه می‌خواهیم که چه‌کاری انجام دهد که مفصلا در موردش صحبت خواهم کرد. در این قسمت، برگه‌هایی با نام‌های Scan , Discover , Option , ... وجود دارد.

۳- Log Output :

محل ظاهر شدن نتایج است. در حالتی که اسکن شروع نشده باشد، خالی است.

۴- bar Status :

پایین‌ترین بخش پنجره برنامه است و دو بخش مهم دارد:

قسمت سمت چپ نشان می‌دهد که اگر بخواهیم در nmap همین کار رو انجام بدیم، چه سویچ‌هایی را باید بکار بریم (دقت کنید که nmap برخلاف NMapWin گرافیکی نیست). هر تغییری که در قسمت Option Folder اعمال کنیم، در این قسمت تغییری را مشاهده می‌کنیم و توصیه می‌کنم که حتما به این قسمت توجه ویژه‌ای داشته باشید.

اما در سمت راست آن، یک مربع کوچک مشاهده می‌شود که می‌تواند به رنگ‌های سبز یا قرمز باشد. سبز یعنی اینکه برنامه آماده برای اجرای دستورات شماست و قرمز یعنی در حال انجام دستورات وارد شده است و فعلا دستور جدید نمی‌پذیرد.

شروع کار با NMapWin

فرض کنید که می‌خواهم سایت far30.com رو می‌خواهم مورد بررسی قرار دهم. برای اینکار ابتدا ip رو بدست آورده (۶۳,۱۴۸,۲۲۷,۶۵) و در قسمت Host تایپ می‌کنیم. حالا فعلا بدون اعمال تغییری در قسمت Option Folder ، دکمه Scan رو کلیک می‌کنیم. اسکن شروع می‌شود و بعد از چند دقیقه، نتایج زیر در قسمت Log Output ظاهر می‌شود:

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on  (63.148.227.65):
(The 1583 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
25/tcp     open        smtp
31/tcp     open        msg-auth
53/tcp     open        domain
80/tcp     open        http
110/tcp    open        pop-3
135/tcp    open        loc-srv
143/tcp    open        imap2
443/tcp    open        https
445/tcp    open        microsoft-ds
1025/tcp   open        NFS-or-IIS
1026/tcp   open        LSA-or-nterm
1050/tcp   open        java-or-OTGfileshare
1433/tcp   open        ms-sql-s
3372/tcp   open        msdtc
3389/tcp   open        ms-term-serv
6666/tcp   open        irc-serv
7007/tcp   open        afs3-bos
Remote operating system guess: Windows 2000/XP/ME
Nmap .... -- 1 IP address (1 host up) scanned in 156 seconds
```

در همین‌جا سه نوع اطلاعات قابل دسترسی است:

۱- لیست پورت‌های باز روی کامپیوتر سرور و کاربرد آن پورت‌ها

۲- تشخیص سیستم عامل که Windows 2000/XP/ME حدس زده شده است (سطر ماقبل آخر)

۳- و سطر آخر می‌گوید که این ip روشن (up) است.

بررسی برگه Scan از قسمت Folder Option

این برگه خود ۲ بخش دارد:

بخش Mode :

در درس‌های قبلی گفتم که اسکنینگ انواع مختلفی داره، و اینجا جایی است که نوع اسکنینگ رو مشخص می‌کنیم:

- Connect : اسکن از نوع TCP connect scan است که قبلا در درس هفتم درباره‌اش بحث کرده‌ام.
- SYN Stealth : در درس هفتم درباره این هم گفته‌ام. - پیش‌فرض هم همین است
- Null Scan , Xmas tree , FIN Stealth : برای سرورهای غیر از ویندوز کار می‌کنند.
- UDP Scan : برای اسکن کردن پورت‌های udp است.
- Ping Sweep : برای عمل ip scanning است که بدانیم که از بین یک سری ip کدام‌ها فعال هستند.
- List Scan : همان Ping Sweep است ولی به طوری که ip مان لو نرود.
- ACK Scan : معمولا برای تشخیص فایروال‌ها کاربرد دارد.
- Window Scan : همان ACK Scan است ولی کامل‌تر
- RCP Scan : جزو کامل‌ترین حالت‌های اسکنینگ است با اطلاعات فراوان.

بخش Scan Options :

این قسمت شش گزینه دارد که فقط یکی‌شان به درد می‌خوره:

- Port Range : مشخص می‌کند که چه پورت‌هایی باید اسکن شود: اگر خالی بماند، یعنی همه پورت‌ها ، اگر یک عدد نوشته شود یعنی فقط آن پورت و اگر به‌صورت n-m نوشته شود (که n و m عدد هستند) یعنی از پورت n تا پورت m اسکن شود.

بررسی برگه Discover از قسمت Option Folder

این برگه دارای چهار گزینه است:

- TCP Ping : برای بررسی فعال بودن کامپیوتر مورد نظر می‌تواند به‌کار رود.
- ICMP Ping : پینگ فقط از نوع ICMP باشد.
- TCP+ICMP : برای بررسی فایروال‌ها مناسب است (پیش‌فرض)
- Don"t Ping : پینگ نکند.

بررسی برگه Options از قسمت Option Folder

این برگه خود ۲ بخش دارد:

بخش Options :

Fragmentation : اگر بخواهیم در اسکنینگ‌هایی از نوع Null, Xmas, FIN, SYN تا حدودی تغییرات اعمال کنیم تا حداقل خطر را برای ما داشته باشند، می‌توان این گزینه را انتخاب کرد. ولی باید توجه داشت که گاهی با انتخاب این گزینه اسکنینگ موفقیت آمیز نخواهد بود.

Idented Info Get : اگر بخواهیم اسکنینگ از نوع connect صورت دهیم، با انتخاب این گزینه گاه اطلاعات ذی‌قیمتی برای ما به ارمغان می‌آورد.

Resolve All : در حالت پیش‌فرض، این نرم‌افزار روی ip هایی که up هستند، عمل Reverse Whois را انجام می‌دهد (یعنی از روی ip، به دنبال اسم DNS مربوطه می‌گردد). اگر Resolve All را انتخاب کرده باشیم، روی همه ip ها، چه up و چه down عمل Reverse Whois انجام خواهد شد.

Don"t Resolve : هرگز Reverse Whois نخواهد کرد.

OS Detection : از جمله مهم‌ترین گزینه‌های این نرم‌افزار است که اگر انتخاب‌شده باشد، برنامه سعی می‌کند که سیستم‌عامل کامپیوتر مقابل را حدس بزند.

Random Host : به صورت تصادفی ip هایی را تست می‌کند، و هرگز هم به پایان نمی‌رسد.

بخش Debug :

Debug : اگر مارک شده باشد، نتایج دیباگ مرحله به مرحله در خروجی نشان داده می‌شود.

Verbose : اگر انتخاب‌شده باشد، پیشرفت کار را نشان می‌دهد.

Very Verbose : پیشرفت کار را با نهایت جزئیات نشان می‌دهد.

بررسی برگه Timing از قسمت Folder Option

این برگه خود ۲ بخش دارد:

بخش Throttle :

در این بخش هرچه گزینه‌های بالاتر را انتخاب کنید، کار کندتر و دقیق‌تر است و احتمال detection (لو رفتن) شما کمتر است و هرچه پایین تر برعکس. به نظر می‌رسد، Normal بهترین انتخاب باشد.

بخش Timeouts :

Host Timeout : حداکثر زمانی را مشخص می‌کند که برای یک ip می‌تواند صرف شود.

Max RTT : حداکثر زمانی را مشخص می‌کند که برای یک probe می‌تواند صرف شود. پیش‌فرض، ۹۰۰۰ است (یعنی ۹ ثانیه)

Min RTT : برای هر probe حداقل به این اندازه صبر می‌کند.

Initial RTT : این گزینه خصوصا در ip هایی که فایروال دارند، مفید است.

Parallelism : اگر در مورد acw_spscan دقت کرده باشید، این برنامه هر بار فقط یک پورت را پروب می‌کند و نه بیشتر (به همین خاطر است که اول اسم آن simple دارد). ولی محصولات واقعی باید همزمان تعدادی پورت را تست کنند. در این قسمت می‌توان حداکثر تعداد پورت‌هایی که می‌تواند همزمان پروب شوند را مشخص می‌کنیم.

Scan Delay : بین هر اسکن، حداقل به این میزان صبر می‌کند.

بررسی برگه Files از قسمت Folder Option

این برگه خود ۲ بخش دارد:

بخش Input :

برای اینکه روند کارها را سریع‌تر کنیم، می‌توان از این بخش استفاده کرد. در این حالت ورودی از یک فایل خوانده می‌شود.

بخش Output :

این قسمت برای آن است که نتایج را در یک فایل ذخیره کنیم. این فایل می‌تواند به‌صورت Normal (متنی معمولی)، Grep (که الان دیگه به‌کار نمیره)، XML و یا All (هر سه مورد) باشد.

بررسی برگه Service از قسمت Option Folder

فرض کنید می‌خواهید اول هر هفته فلان ip رو تست کنید و کارهایی از این‌دست... این برگه برای همین‌جور کارهاست (میشه گفت یک نوع اتوماسیون)

بررسی برگه Win32 از قسمت Folder Option

این برگه دو بخش دارد به نام‌های Commands , Options که فقط Options رو بررسی می‌کنم:

No Pcap : وقتی که NMapWin را نصب می‌کنیم، Pcap هم نصب می‌شود (که فقط روی سیستم‌های ویندوز ۲۰۰۰ و xp می‌تواند نصب شود) و کارها را برعهده می‌گیرد. اگر بخواهیم که از آن استفاده نشود و به‌جای آن از Raw Socket استفاده شود، این گزینه را مارک می‌کنیم.

No IP HLP Api : مثل بالایی فقط اینکه بین ارسال هر پکت، ۱۵ ثانیه منتظر می‌ماند.

No Raw Sockets : با انتخاب آن Raw Socket به‌کار نمی‌رود.

Force Raw Socket : باعث می‌شود که فقط Socket Raw به‌کار رود.

Win Trace : برای سیستم‌های Win32 کمی اطلاعات بیشتری به‌دست می‌دهد.

استفاده از NMapWin برای تعیین نوع سیستم عامل

اگر مهم‌ترین کاربردهای nmap را بخواهیم بدانیم، یکی port scanning و دیگری OS detection (تشخیص سیستم‌عامل مقابل) است که ویژگی دوم به قدری مهم است که گاه nmap را با همین ویژگی می‌شناسند. برای اینکه نوع سیستم‌عامل را تعیین کنیم، باید در برگه Options از NMapWin، گزینه OS detection انتخاب شده باشد.

حالا چند مثال را بررسی می‌کنیم (شما خودتان این ip ها و ip های دیگر را تست و تمرین کنید) :

۱۹٤,۲۲٥,۱۸٤,۱٥

guess Remote operating system: Windows 2000 server SP2

۱۹٥,۲۱۹,۱۷٦,٥

operating system guess Remote: ۲,٥,۲۰ - Linux Kernel 2.4.0

۲۰٦,۱۰٤,۲۳۸,۲۰۸

Remote operating system guess: Linux 2.1.19 - 2.2.20

۲۱۷,٦٦,۱۹۹,٦

system guess Remote operating): ۱۲,۲-۱۲,۱,٥ Cisco router running IOS)٦a)

٦۳,۱٤۸,۲۲۷,٦٥

Remote operating system guess: Windows 2000/XP/ME

۱۹٤,۲۲٥,۱۸٤,۲

If you know what OS is running on it, see) for host No exact OS matches (http://www.insecure.org/cgi-bin/nmap-submit.cgi).

در این مورد می‌بینید که nmap موفق به تعیین نوع سیستم‌عامل نشده است. ممکن است دلیلش این باشد که ip در آن لحظه up نبوده است.

نکته‌ای که باید در نظر داشت این است که گاه باید از یک سری اطلاعات فنی هم استفاده کرد تا به جواب قطعی رسید :

- مثلا ip ماقبل آخر که نتیجه آن به صورت Windows 2000/XP/ME ظاهر شده است، متعلق به sazin.com است که چون یک سایت است و باید در یک سرور باشد و هیچ سروری نمی‌تواند ME یا XP باشد، پس سیستم‌عامل آن Win 2000 خواهد بود.

- یا یک حالت دیگر موردی است که ببینید صفحات یک وب سایت با asp یا asp.net درست شده است (مثلا اسم صفحه به صورت zzzzzz.asp یا zzzzzz.aspx باشد، که نمونه آن سایت far30.com است که اسم همین صفحه default.asp است). در این حالت سرور آن حتما سروری از محصولات مایکروسافت است مثل Win NT و یا Win 2000 و نمی‌تواند Linux یا Unix یا Sun Solaris و... باشد.

چگونه از nmap استفاده کنیم؟

قبلا با نرم‌افزار NMapWin آشنا شدید که نسخه گرافیکی nmap برای ویندوز بود. nmap در واقع نرم‌افزار اصلی است که هم برای یونیکس (لینوکس) و هم برای ویندوز نسخه‌هایی را دارد. nmap برخلاف NMapWin، حالت خط فرمانی (command prompt) دارد. در این قسمت می‌خواهیم با nmap مخصوص ویندوز آشنا شویم. برای داون‌لود این نرم‌افزار اینجا را کلیک کنید. (اگر قبلا NMapWin را نصب نکرده‌اید، باید از یک نسخه دیگر از nmap که اصطلاحا nmap installer نام دارد، استفاده کنید. این نسخه nmap را می‌توانید از اینجا داون‌لود کنید.)

همان‌طور که می‌دانید، در نرم‌افزارهای خط فرمانی، باید از پارامترها استفاده کنیم. با توجه به اینکه پارامترهای nmap بسیار زیاد و یادگیری آنها مشکل است، ما برای پیدا کردن پارامترهای درست برای یک عمل خاص (که معمولا scanning ip یا port scanning است) از NMapWin استفاده می‌کنیم. به این ترتیب که در NMapWin تنظیمات را انجام می‌دهیم و بعد در پایین پنجره آن مشاهده می‌کنید که در قسمت :CMD لیست پارامترها را به دست می‌آوریم. این مراحل را با دو مثال شرح می‌دهم:

۱- می‌خواهیم برای پورت‌های ۱ تا ۲۰۰ در کامپیوتری که ip آن ٦٣,١٤٨,٢٢٧,٦٥ است، یک پورت اسکنینگ انجام دهیم. برای این‌کار در NMapWin، برگه Scan را درحالت SYN Stealth تنظیم می‌کنیم و Port Range را می‌نویسیم: ۱-۲۰۰ و بعد برگه Discover باید در حالت TCP+ICMP باشد و اگر بخواهیم نوع سیستم‌عامل را هم مشخص کنیم، در برگه Options، گزینه OS detection را در حالت انتخاب شده قرار می‌دهیم. ip را هم در بالای پنجره، ٦٣,١٤٨,٢٢٧,٦٥ می‌نویسیم. حالا آماده اسکن هستیم ولی ما می‌خواهیم این کار را با nmap انجام دهیم، پس فقط باید قسمت CMD را از پایین پنجره ببینید، ملاحظه می‌کنید که نوشته شده:

```
CMD: -sS -PT -PI  -p 1-200 -O -T 3 63.148.227.65
```

با حذف کلمه :CMD به عبارت زیر می‌رسیم:

```
-sS -PT -PI  -p 1-200 -O -T 3 63.148.227.65
```

اینها پارامترهایی است که باید در nmap استفاده کنید. به این صورت که می‌نویسید:

```
nmap -sS -PT -PI  -p 1-200 -O -T 3 63.148.227.65
```

و بعد از اجرای دستور و صبر کردن برای چند دقیقه، نتایج را می‌بینیم.

بعد از مدتی که با nmap کار کنید، این پارامترها را می‌آموزید و دیگه نیازی به NMapWin نخواهید داشت. مثلا همین O- یعنی OS detection، و p 1-۲۰۰ یعنی پورت‌های ۱ تا ۲۰۰ می‌باشد. بعدها خودتان می‌بینید که کار کردن با nmap بسیار دلچسب‌تر از NMapWin است.

۲- می‌خواهیم یک ip scanning انجام دهیم برای ۱۹۵,۲۱۹,۱۷۶,۰ تا ۱۹۵,۲۱۹,۱۷۶,۱۰ . برای اینکار در NMapWin، در برگه Mode، گزینه Ping Sweep را انتخاب می‌کنیم. در برگه Discovery، گزینه ICMP Ping را انتخاب کرده و در برگه Options، گزینه OS detection را در حالت انتخاب نشده قرار می‌دهیم. برای نوشتن ip ملاحظه می‌فرمایید که ۱۹۵,۲۱۹,۱۷۶ در هر دو مشترک است، پس می‌نویسیم: ۱۹۵,۲۱۹,۱۷۶,۰-۱۰ .حالا می‌بینیم که پارامترها به صورت زیر است:

```
-sP -PI -T 3 195.219.176.0-10
```

پس ما می‌نویسیم:

```
nmap -sP -PI -T 3 195.219.176.0-10
```

جلسه نهم

IP Scanning

IP Scanning به روش‌های مختلف می‌تواند صورت بگیرد:

۱- در ساده‌ترین نوع آن، یک پکت از نوع ICMP ECHO به یک ip خاص می‌فرستیم و اگر یک ICMP ECHO REPLAY به سمت ما برگشت، در این صورت آن ip به‌اصطلاح up است. برای این‌کار می‌توان از ابزارهای زیر استفاده کرد:

الف) استفاده از ping موجود در سیستم‌عامل‌های ویندوز و یونیکس (لینوکس). به صورت زیر:

```
ping xxx.xxx.xxx.xxx
```

مثلا برای ۶۳,۱۴۸,۲۲۷,۶۵ می‌نویسیم:

```
ping 63.148.227.65
```

اگر در ویندوز این دستور را تایپ کنید و به جواب زیر برسید، یعنی آن ip فعال است:

```
Reply from 63.148.227.65: bytes=32 time=1402ms TTL=105
Reply from 63.148.227.65: bytes=32 time=941ms TTL=105
Reply from 63.148.227.65: bytes=32 time=1402ms TTL=105
Reply from 63.148.227.65: bytes=32 time=941ms TTL=105
```

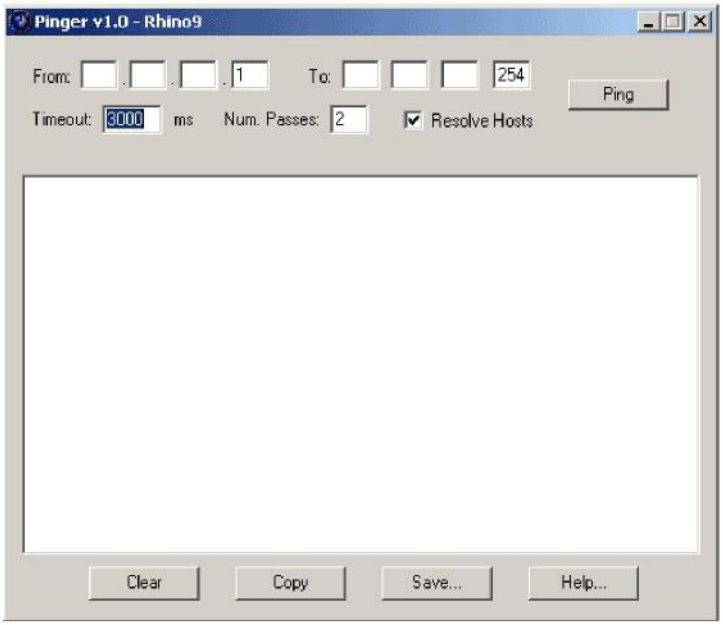
و اگه به پیغام زیر رسیدید، یعنی فعال نیست:

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

همان طور که می‌بینید با این دستور در یک لحظه فقط می‌شود، یک ip را تست کرد و این کار ما را کند می‌کند.

ب) در سیستم‌عامل لینوکس می‌شود از gping استفاده کرد که یک مجموعه ip را به سرعت تست کرد.

ج) در سیستم عامل ویندوز می‌شود از Pinger استفاده کرد. برای داونلود این نرم‌افزار اینجا را کلیک کنید. Pinger یک نرم‌افزار گرافیکی است و کار ping کردن به یک مجموعه ip را ساده می‌کند.



در قسمت From و To مشخص می‌کنیم که از کدام ip تا کدام ip را می‌خواهیم ping کنیم. با فشار دکمه Ping لیست ip هایی که up هستند، نمایش داده می‌شود. فرض کنید که ip فعلی شما ۱۹۵,۲۱۹,۱۷۶,۸۸ باشد و بخواهیم بدانیم در کلاس C مربوط به ما چه ip های دیگری up هستند. در این حالت باید ۱۹۵,۲۱۹,۱۷۶,۱ تا ۱۹۵,۲۱۹,۱۷۶,۲۵٤ را ping کنیم.

د) حالا می‌خواهیم همین کار را با NMapWin انجام دهیم. برای اینکار باید در برگه Scan، قسمت Mode را در حالت Ping Sweep قرار دهید. برگه Discover باید درحالت ICMP Ping باشد و در قسمت Options باید گزینه Detection OS را از حالت انتخاب شده خارج کنید. بعد باید لیست ip

ها را تنظیم کنیم، برای اینکار باید در قسمت Host ، لیست ip ها را وارد می‌کنیم. مثلا اگر بخواهیم ۱۹۵,۲۱۹,۱۷٦,۱ تا ۱۹۵,۲۱۹,۱۷٦,۲٥٤ را تست کنیم باید بنویسیم: ۱۹۵,۲۱۹,۱۷٦,۰/۲٤ که این ۲٤/ یعنی کلاس C که از ۱ تا ۲٥٥ است. و بعد دکمه Scan را فشار دهیم.

```
Host  (195.219.176.0) seems to be a subnet broadcast address ...
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Host  (195.219.176.1) appears to be up.
Host  (195.219.176.3) appears to be up.
Host  (195.219.176.5) appears to be up.
Host  (195.219.176.7) appears to be up.
Host  (195.219.176.9) appears to be up.
Host  (195.219.176.11) appears to be up.
Host  (195.219.176.12) appears to be up.
Host  (195.219.176.13) appears to be up.
Host  (195.219.176.14) appears to be up.
Host H-GVSVY95KXINRJ (195.219.176.15) appears to be up.
Host  (195.219.176.16) appears to be up.
Host  (195.219.176.17) appears to be up.
Host  (195.219.176.18) appears to be up.
Host  (195.219.176.19) appears to be up.
Host KERYASBA (195.219.176.20) appears to be up.
Host MARYAM (195.219.176.22) appears to be up.
Host  (195.219.176.23) appears to be up.
Host  (195.219.176.24) appears to be up.
Host FFX-L2XA0ZM87Q3 (195.219.176.25) appears to be up.
Host  (195.219.176.26) appears to be up.
Host  (195.219.176.27) appears to be up.
Host  (195.219.176.28) appears to be up.
,...
```

ملاحظه می‌فرمایید که در بعضی موارد اسم کامپیوتر مربوط به ip هم ذکر شده است.

۲- در تمام روش‌های بالا، از پکت‌های ICMP برای پینگ استفاده کردیم. در بعضی کامپیوترها ممکن است پکت‌های ICMP توسط فایروال یا روتر بلاک شوند. در این حالت باید از پورت اسکنینگ برای IP اسکنینگ استفاده کرد! برای این‌کار می‌توان از ابزارهای زیر استفاده کرد:

الف) در سیستم عامل یونیکس (لینوکس) می‌توان از ابزارهایی مثل hping و icmpenum و ... استفاده کرد. که فعلا بحث ما نیستند.

ب) در سیستم‌عامل ویندوز، بازهم از NMapWin استفاده می‌کنیم. ولی طوری Port Scanning می‌کنیم که نیاز ما را برای IP Scanning جواب دهد. این‌کار توسط یک سری پورت‌های عمومی صورت می‌گیرد که در اکثر کامپیوترها باز هستند مثل ۸۰ ، ۳۵ و...
برای این‌کار در برگه Scan ، قسمت Mode را در حالت Connect تنظیم می‌کنیم و در قسمت Scan Options ، گزینه Port Range را مثلا برای عدد ۸۰ تنظیم می‌کنیم. Discover را در حالت TCP Ping قرار می‌دهیم. و در برگه Option ، گزینه OS Detection را از حالت انتخاب شده خارج می‌کنیم. لیست ip ها را ست کرده و اسکن را شروع می‌کنیم.

جلسه دهم

ping چیست؟

ping دستوری است که مشخص می‌کند که آیا یک کامپیوتر خاص که ما ip یا domain آن را می‌دانیم، روشن و فعال (Active) هست یا نه. و اینکه اگر فعال باشد مدت زمان رسیدن بسته‌های tcp/ip از آن کامپیوتر به کامپیوتر ما چقدر است.

کاربرد این دستور به صورت زیر است:

```
ping ip-or-domain
```

که به جای ip-or-domain باید شماره ip و یا domain آن(اگر داشته باشد) را می‌گذاریم.

مثلا ping sazin.com را در command prompt تایپ کردم و به نتایج زیر رسیدم:

```
Pinging sazin.com [63.148.227.65] with 32 bytes of data:
 Reply from 63.148.227.65: bytes=32 time=1402ms TTL=105
Reply from 63.148.227.65: bytes=32 time=941ms TTL=105
Reply from 63.148.227.65: bytes=32 time=981ms TTL=105
Reply from 63.148.227.65: bytes=32 time=851ms TTL=105

Ping statistics for 63.148.227.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 851ms, Maximum =  1402ms, Average =  1043ms
```

این نتایج نشان می‌دهد که sazin.com فعال است.

حالا به کامپیوتری با ip شماره ٦٣,١٤٨,٢٢٧,٦٥ (که همان sazin.com است)، ping می‌کنم. نتایج همان است فقط با تغییراتی در سطر اول. (البته time که معنای مدت زمان رسیدن پکت را می‌دهد، با توجه به ترافیک شبکه، کم و زیاد خواهد شد). برای ping کردن به این ip ، دستور ping ٦٣,١٤٨,٢٢٧,٦٥ را صادر می‌کنم :

```
Pinging 63.148.227.65 with 32 bytes of data:
```

```
Reply from 63.148.227.65: bytes=32 time=861ms TTL=105
Reply from 63.148.227.65: bytes=32 time=852ms TTL=105
Reply from 63.148.227.65: bytes=32 time=851ms TTL=105
Reply from 63.148.227.65: bytes=32 time=881ms TTL=105

Ping statistics for 63.148.227.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 851ms, Maximum =  881ms, Average =  861ms
```

فرض کنید که به یک ip که فعال نیست، ping کنیم:

```
Pinging 217.66.196.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 217.66.196.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

که نشان می‌دهد که آن ip در آن لحظه فعال نیست.

البته تمام مطالبی که در بالا ذکر شد، در حالتی است که مستقیما به اینترنت وصل شده‌اید و یا اگر از طریق شبکه محلی به اینترنت وصل هستید، شبکه شما به درستی پیکربندی شده باشد. اصولا ping یکی از بهترین دستورات برای پیدا کردن ایراد در شبکه است.

tracert چیست؟

tracert (در یونیکس می‌شود traceroute) ابزاری است که نشان می‌دهد که یک packet اطلاعاتی از کامپیوتر شما چه مسیری را طی می‌کند و از چه کامپیوترهایی می‌گذرد تا به یک

مقصد خاص برسد. مقصد را ما مشخص می‌کنیم و معمولا همان کامپیوتری است که داریم footprinting می‌کنیم.

کاربرد این دستور به صورت زیر است:

```
tracert ip-or-domain
```

مثلا می‌خواهم ببینم که از چه کامپیوترهایی باید رد شویم تا به sazin.com برسیم. برای اینکار می‌توان از یکی از دستورهای زیر استفاده کرد:

```
tracert sazin.com
tracert 63.148.227.65
```

به نتیجه زیر رسیدم:

```
Tracing route to sazin.com [63.148.227.65]
over a maximum of 30 hops:

  1   160 ms   160 ms   160 ms  217.218.84.3
  2   381 ms   691 ms  1772 ms  217.218.84.5
  3     *        *     2324 ms  217.218.77.1
  4   201 ms  1101 ms   180 ms  217.218.0.252
  5   341 ms   220 ms   180 ms  217.218.0.2
  6  1993 ms   180 ms   181 ms  217.218.158.41
  7   180 ms   160 ms   160 ms  195.146.63.101
  8  2824 ms     *        *     195.146.32.134
  9  1472 ms  1463 ms   871 ms  195.146.33.73
 10   791 ms   841 ms   811 ms  if-1....eglobe.net [207.45.218.161]
 11  1692 ms     *     2654 ms  if-4-....eglobe.net [207.45.222.77]
 12  1282 ms   891 ms  1052 ms  if-1-....globe.net [207.45.220.245]
 13   902 ms   931 ms   881 ms  if-15.....globe.net [66.110.8.134]
 14   931 ms   861 ms   871 ms  if-8-....leglobe.net [64.86.83.174]
 15   901 ms   841 ms   852 ms  if-5-.....globe.net [207.45.223.62]
```

```
16   841 ms   862 ms   851 ms  pos6-.....vel3.net [209.0.227.33]
17   841 ms   842 ms   941 ms  so-4-1.....vel3.net [209.247.10.205]
18   882 ms   931 ms   851 ms  so-0-1....vel3.net [209.247.11.197]
19   871 ms   891 ms   951 ms  gige9....vel3.net [209.247.11.210]
20  1011 ms   851 ms   902 ms  unknown.Level3.net [63.208.0.94]
21   852 ms     *      882 ms  64.156.25.74
22   961 ms   942 ms   841 ms  63.148.227.65

Trace complete.
```

این نتایج نشان می‌دهد که باید از ۲۲ کامپیوتر بگذرم تا به sazin.com برسم. این اطلاعات همان‌طور که بعدا خواهید دید، حاوی اطلاعات زیادی برای پیدا کردن فایروال‌ها و ... است. (بعضی سطرها رو کوتاه کردم و به‌جاش .... گذاشتم)

tracert دارای تعدادی switch است که دوتاش رو توضیح می‌دم:

-d <==

با استفاده از این سویچ در نتایج حاصله فقط ip ها نمایش داده می‌شود.

مثلا می‌نویسیم: tracert sazin.com -d

h *-max-hops* <==

حداکثر تعداد گام‌ها را تعیین می‌کند. حالت پیش‌فرض ۳۰ است.

مثلا می‌نویسیم: tracert sazin.com -h ۵۰

از این دستور بعدا بسیار استفاده خواهیم کرد.

ادامه بحث telnet

telnet هم جزو مواردی است که در footprinting مورد استفاده قرار می‌گیرد. کاربرد آن در حالتیست که بخواهیم بدانیم که روی فلان پورت چه برنامه‌ای فال‌گوش‌ه و version آن چنده. به این صورت که به یک پورت خاص (که می‌دانیم روی آن سرور باز است) تلنت می‌کنیم و بعد می‌بینیم که نتایجی ظاهر می‌شود که نشان‌دهنده اطلاعاتی است که به‌کار می‌رود. گاهی با مکثی طولانی مواجه می‌شویم و هیچ چیزی نمایش داده نمی‌شود، در این حالت یکی دوبار ,

Ctrl+D , Ctrl+C , Ctrl+break , Ctrl+Z را می‌زنیم و خارج می‌شویم. در مثال پایین جمع‌بندی مواردی که تا حالا از footprinting گفته‌ام را می‌آورم.

جمع‌بندی مطالب گفته شده و بررسی یک سایت

فرض کنید می‌خواهیم در مورد www.iums.ac.ir اطلاعاتی کسب کنیم :

◊ اول به سایت پینگ می‌کنم و ip آن را به‌دست می‌آورم: ۱۹٤,۲۲٥,۱۸٤,۱٥

◊ به کمک ip که به‌دست آوردیم، به کمک یک پورت اسکنر پورت‌ها را بررسی می‌کنیم و می‌بینیم که پورت‌هایی مثل ۲۱، ۲٥، ٤۳، ٥۳، ۸۰، ۱۱۰، ۱۱۹، ۱۳۹، ۱٤۳ و ... باز است.

◊ چون domain به ir ختم می‌شود، برای whois کردن از whois.nic.ir استفاده می‌کنم و Name Server آن را به دست می‌آورم که ۱۹٤,۲۲٥,۱۸٤,۲۰ است.

◊ به کمک این Name Server ، یک nslookup می‌کنم و به نتایج زیر می‌رسم:

```
iums.ac.ir.              SOA    sina.i.....0 345600)
iums.ac.ir.              NS     sina.iums.ac.ir
iums.ac.ir.              NS     ns1.nic.ir
iums.ac.ir.              MX     10   sina.iums.ac.ir
smtp.iums.ac.ir.          A      195.146.34.181
sina.iums.ac.ir.      HINFO  Sun-SuperSPARC5/75  UNIX-Solaris-2.6
sina.iums.ac.ir.          MX     10   sina.iums.ac.ir
sina.iums.ac.ir.          A      194.225.184.20
sina.iums.ac.ir.          A      195.146.34.181
sun.iums.ac.ir.           CNAME  sina.iums.ac.ir
cisco.iums.ac.ir.         CNAME  router.iums.ac.ir
webmail.iums.ac.ir.        A      195.146.34.181
linux.iums.ac.ir.         A      194.225.184.19
linux.iums.ac.ir.     HINFO  Intel-Xeon/800  RedHat-Linux-7.2
mta.iums.ac.ir.           A      195.146.34.181
pop3.iums.ac.ir.          CNAME  sina.iums.ac.ir
localhost.iums.ac.ir.     A      127.0.0.1
proxy.iums.ac.ir.         CNAME  arvand.iums.ac.ir
```

```
www.iums.ac.ir.          A     195.146.34.180
atrak.iums.ac.ir.        A     194.225.184.14
ns1.iums.ac.ir.          CNAME sina.iums.ac.ir
arvand.iums.ac.ir.       A     194.225.184.13
router.iums.ac.ir.       A     194.225.184.1
router.iums.ac.ir.   HINFO Cisco3640/Access-Server IOS-IP-12.0
iums.ac.ir.              SOA   sina.iu.....3456000 345600)
```

تک تک سطرهای این نتایج کاربرد دارد که خواهیم رسید. الان فقط در مورد HIFNO صحبت می‌کنم که برای مشخص تر بودن در بالا به صورت کمی فرورفته‌تر نوشتم. مثلا:

```
sina.iums.ac.ir.     HINFO Sun-SuperSPARC5/75 UNIX-Solaris-2.6
```

HIFNO برای تعیین نوع کامپیوتر و سیستم‌عامل سرور اهمیت دارد. در این سطر مشخص است که sina.iums.ac.ir از Sun-SuperSPARC5/75 UNIX-Solaris-2.6 استفاده می‌کند.

◊ چون پورت‌های باز را هم توسط پورت اسکنر به دست آورده‌ام به آنها تلنت می‌کنم با دستور:

portnum **telnet www.iums.ac.ir**

نتایج حاصل از بعضی را می‌بینید:

: ۲۵

..master.iums.ac.ir Microsoft ESMTP MAIL Service, Version: 5.0.2195.4905 ready at ۲۲۰

پس پورت ۲۵ (smtp) در آن کامپیوتر از Microsoft ESMTP MAIL Service, Version: 5.0.2195.4905 استفاده می‌کند.

: ۱۱۰

+OK Microsoft Exchange 2000 POP3 server version 6.0.5762.3 (master.iums.ac.ir) ready.

پس پورت ۱۱۰ (pop3) در آن کامپیوتر از Microsoft Exchange 2000 POP3 server version ٦,٠,٥٧٦٢,٣ استفاده می‌کند.

: ۱۱۹

NNTP Service 5.00.0984 Version: 5.0.2195.2966 Posting Allowed

و ...

جلسه یازدهم

Social Engineering چیست؟

Social Engineering یا مهندسی اجتماعی، تکنیکی است که بر گول زدن مردم استوار است. در این تکنیک شما با انسان‌ها سر و کار دارید و نه با کامپیوترها. حال اگه یک user رو مثلا گول بزنید، می‌توانید اطلاعات او را مثل پسورد و ... را بدست بیاورید که نمونه‌ای است از Client Hacking و اگه Administer یک سایت را گول بزنید و سایت را هک کنید، نمونه‌ای است از Server Hacking.
پس با مهندسی اجتماعی هم می‌شود کلاینت هک کرد و هم سرور. البته چون کلاینت‌ها معمولا user های کم‌سوادتری (از نظر دانش هک) دارند، هک کردن آنها بسیار آسان‌تر است.
این نکته را هم باید بگم که روش Social Engineering معمولا در مراحل اولیه هک استفاده می‌شود و بعد از آن باید مسیر را عوض کنید و از اطلاعات فنی‌تان برای ادامه کار بهره ببرید.

مثال‌هایی از مهندسی اجتماعی

در اینجا می‌خواهم تعدادی از تکنیک‌های Social Endineering را براتون بگم. البته توجه کنید که اگرچه این روش‌ها اطلاعات فنی زیادی نمی‌خواد ولی معمولا نتایج خوبی داره. و نیز بگم که این روش‌ها خیلی گسترده است و هر بار به شکلی بروز می‌کند. اما نکته مشترکی که من در همه‌شان دیدم اینه که همیشه از شما می‌خواهند که پسوردتان را یک جایی وارد کنید و این دقیقا محلی است که فرق شما رو با یک user معمولی نشون میده. زیرا نباید گول بخورید (-;

۱- تلفن زدن :

یکی از روش‌های مهندسی اجتماعی است. هکر اطلاعاتي از افراد یک شرکت جمع‌آوری می‌کند و بعد با شرکت تماس گرفته و مثلا از فلان فرد می‌خواهد که پسورد را عوض کند. پیشرفته‌ترین متدهای این نوع هک توسط مشهورترین (و یکی از بهترین) هکرهای تاریخ، Mitnick Kevin اجرا شده است.

۲- مخ زدن برای ارسال فایل:

مثلا با یک نفر چت می‌کنید و می‌گید که بیا عکس منو ببین! و به جای ارسال یک فایل تصویری، یک فایل اجرایی مثلا تروجان براش می‌فرستید. تا این مرحله کار شما به عنوان مهندسی اجتماعی است ولی مابقی (مثلا استفاده از تروجان فرستاده شده) دیگه Social engineering نیست.

۳- برای ما E-mail بزنید و ما پسورد E-mail کسی که شما می‌خواهید را براتون پیدا می‌کنیم:

ممکنه در اینترنت به این نوع پیغام‌ها برخورد کرده‌اید که مثلا می‌گوید:

" به ما ایمیل بزنید، در سطر اول E-mail کسی که می‌خواهید ما براتون هک کنیم رو بنویسید، در سطر دوم E-mail خودتون رو، سطر آخر هم پسورد E-mail خودتون رو. ما پسورد E-mail ی که در سطر اول مشخص کردید براتون می‌فرستیم. "

ممکنه عجیب به نظر برسه ولی خیلی‌ها به همین راحتی هک می‌شوند. این دیگه از اون بهترینا‌ش، چون یک تیره و سه نشون. ۳ تا آدرس E-mail برای فرستادن تبلیغات و نیز پسورد E-mail خودتون.

۴- فایل ضمیمه (attached) به E-mail را باز کنید:

مثلا اینکه می‌گوید در این E-mail عکس من attach شده است باز کنید و ببینید. درحالی که فایل attach شده فایل تصویری نیست، بلکه یک فایل آلوده است.

۵- ساختن یک صفحه شبیه به سایت‌های مشهور و درخواست login :

مثلا ساختن یک صفحه شبیه به یاهو برای login درحالی‌که این صفحه برای دزدیدن id و password شماست.

۶- و ...

جلسه دوازدهم

شروع کار با نرم‌افزار netcat

اگر یادتون باشه در درس ۸ مهم‌ترین ابزاری که یک هکر برای footprinting استفاده می‌کنه را nmap معرفی کردم. حالا می‌خوام مهمترین نرم‌افزاری که یک هکر در کل زندگی‌اش !! استفاده می‌کنه رو معرفی کنم. این نرم‌افزار netcat نام دارد که به‌طور خلاصه nc نامیده میشه (این nc با اون nc که تو DOS بود فرق می‌کنه). nc بقدری نرم‌افزار مهمی است که حتی یک سری لقب هم دارد. اگر جایی "Pocket Knife of network utilities" یا "Knife TCP/IP Swiss Army" شنیدید، بدونین که منظورشان همین nc است(این نرم‌افزار را به چاقوی جیبی تشبیه می‌کنند). من فعلا نمی‌خوام یه معرفی کامل از اون بکنم فقط می‌گم که علاوه بر قابلیت‌های عمومی مثل Scanning ها، چیزی که اون رو خیلی معروف کرده یکی عملکرد مشابه ولی بهتر از telnet و دیگری کاربرد اون به‌عنوان هم کلاینت و هم سرور (یه چیزی تو مایه‌های تروجان) است.

این نرم‌افزار اولین بار برای سیستم‌عامل‌های یونیکس نوشته شد ولی نسخه مخصوص ویندوز هم داره که برای داون‌لود اون اینجا را کلیک کنید. این نسخه فقط در ویندوزهای NT (مثل Windows2000، Windows XP) کار می‌کنه.

برای به دست آوردن لیست پارامتر های اون می‌نویسیم:

```
nc -help
```

و جواب می‌شنویم:

```
[v1.10 NT]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
        -d              detach from console, stealth mode

        -e prog         inbound program to exec [dangerous!!]
        -g gateway      source-routing hop point[s], up to 8
        -G num          source-routing pointer: 4, 8, 12, ...
        -h              this cruft
```

```
        -i secs         delay interval for lines sent, ports scanned
        -l              listen mode, for inbound connects
        -L              listen harder, re-listen on socket close
        -n              numeric-only IP addresses, no DNS
        -o file         hex dump of traffic
        -p port         local port number
        -r              randomize local and remote ports
        -s addr         local source address
        -t              answer TELNET negotiation
        -u              UDP mode
        -v              verbose [use twice to be more verbose]
        -w secs         timeout for connects and final net reads
        -z              zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]
```

تا همینجا بماند تا بعدا تک تک پارامترها رو توضیح می‌دم.

استفاده از nc برای port scanning

برای پورت اسکنینگ قبلا از NMapWin و nmap استفاده کردیم. اما این کار را با nc هم می‌توان انجام داد (اگرچه من بازهم برای پورت اسکنینگ همان nmap رو توصیه می‌کنم.) برای port scanning با nc باید بنویسید:

```
nc -v -z host  pornum
```

به‌جای host باید ip (ip ها) یا نام آن (مثلا اسم سایت) را بنویسیم. و به‌جای portnum ، شماره پورت (یا پورت‌ها) را می‌نویسیم. v- یعنی verbose یعنی نتایج با جزئیات نمایش داده شود. z- وقتی استفاده می‌شود که از nc برای scanning استفاده می‌کنیم.

فرض کنید می‌خواهیم ip ی به شماره ۲۱۷,٦٦,۱۹۵,۱۸۱ را برای پورت‌های ۱ تا ۲۰۰ چک کنم، می‌نویسم:

```
nc -v -z 217.66.195.181 1-200
```

و جواب می‌شنوم:

```
artawill-1dedm4 [217.66.195.181] 143 (imap) open
artawill-1dedm4 [217.66.195.181] 139 (netbios-ssn) open
artawill-1dedm4 [217.66.195.181] 135 (epmap) open
artawill-1dedm4 [217.66.195.181] 119 (nntp) open
artawill-1dedm4 [217.66.195.181] 80 (http) open
artawill-1dedm4 [217.66.195.181] 53 (domain) open
artawill-1dedm4 [217.66.195.181] 25 (smtp) open
artawill-1dedm4 [217.66.195.181] 21 (ftp) open
artawill-1dedm4 [217.66.195.181] 19 (chargen) open
artawill-1dedm4 [217.66.195.181] 17 (qotd) open
artawill-1dedm4 [217.66.195.181] 13 (daytime) open
artawill-1dedm4 [217.66.195.181] 9 (discard) open
artawill-1dedm4 [217.66.195.181] 7 (echo) open
```

می‌بینید که پورت‌ها از آخر به اول لیست شده‌اند. و نیز اینکه این نرم‌افزار هم می‌تواند سرویس‌های احتمالی مربوط به هر پورت باز را هم لیست کند.

اگر می‌خواستم یک سری پورت را که به صورت پشت‌سرهم نیستند، بررسی کنم، باید پورت ها را یکی پس از دیگری با فاصله از هم جدا کنید. مثلا برای بررسی پورت‌های ۲۵، ۸۰ و ۱۱۰ را چک کنم، می‌نویسم:

```
nc -v -z 217.66.195.181 25 80 110
```

در درس‌های بعدی با کاربردهای بیشتری از nc آشنا خواهیم شد.

بخش دوم

کار با پورت‌ها

جلسه سیزدهم

شروع کار با پورت‌ها

الان به جایی رسیده‌ایم که می‌توانیم بحث پورت‌ها را شروع کنیم. اولین نکته‌ای که باید بگم این است که ابزاری که به کمک آن با پورت‌ها صحبت می‌کنیم در همه پورت‌ها یکی است ولی هر پورتی زبان مخصوص خود دارد (درست مثل زبان‌های مختلف در جهان که همشون از طریق زبان و دهان ادا می‌شن ولی هر کدام روش خاصی برای ارتباط برقرار کردن دارند). پس ما برای کار با پورت‌ها باید زبان هرکدام را یاد بگیریم.

بحث بعدی این است که وقتی می‌گیم یه پورت بازه باید توجه کنید که برنامه‌ای روی آن کامپیوتر نصب شده و اون پورت را باز کرده است (پورت‌ها خود به خود باز نمی‌شوند). یک سری پورت‌ها توسط خود سیستم‌عامل باز می‌شوند (یعنی به محض نصب سیستم‌عامل که خودش هم درواقع یه نرم‌افزاره) و نیازی نیست که برنامه دیگری برایش نصب کنیم. در مقابل، بعضی پورت‌های دیگر توسط برنامه‌های جانبی باز می‌شوند.

به عنوان مثال وقتی می‌گم که پورت ۲۵ روی یک ip باز است، این معنی را دارد که برنامه‌ای روی اون کامپیوتر خاص وجود دارد که پورت ۲۵ را باز کرده و من وقتی از طریق کامپیوتر خودم با آن پورت کار می‌کنم در واقع دارم با آن برنامه خاص (که اون پورت را باز کرده) صحبت می‌کنم.

حالا یه سوال پیش می‌آد که چرا اصلا یه نرم‌افزار باید پورت باز کنه و اینکه کدام نرم‌افزارها باید پورت باز کنند؟

جواب این است که هر برنامه‌ای که بخواهد از طریق شبکه (یعنی از راه دور اصطلاحا remote) قابل دسترس باشه باید یه پورت باز کنه. پس یک برنامه‌ای که نیازی به برقراری ارتباط شبکه‌ای ندارد (مثلا یه نرم‌افزار گرافیکی) نباید و نشاید که پورت باز کند.

باید ببینیم که از طریق چه برنامه‌ای می‌توان با پورت‌ها صحبت کرد (البته با هر کدام به روش خودشان) ؟

برای این‌کار از دو نرم‌افزار به نام‌های telnet و nc استفاده می‌کنیم. telnet که در خود سیستم‌عامل وجود دارد و nc را هم که جلسه قبل داون‌لود کردیم.

حالا چگونه از این دو نرم‌افزارها می‌توان استفاده کنیم؟

۱- استفاده از telnet :

اگر بخواهیم با ip ای به شماره ۱۹٤,۲۲٥,۱۸٤,۱۳ از طریق پورت ۲۵ صحبت کنیم باید بنویسیم:

```
telnet 194.225.184.13 25
```

و بعد اینکه ارتباط برقرار شد باید شروع کنیم و از طریق زبان پورت ۲۵ با آن صحبت کنیم.

۲- استفاده از nc :

اگر بخواهیم همان کار را با netcat انجام دهیم، باید بنویسیم:

```
nc -v 194.225.184.13 25
```

و بعد از برقراری ارتباط شروع به صحبت کنیم.

با پورت ۱۳ صحبت کنیم

نام دیگر اون daytime است و کارش هم اینه که زمان و تاریخ رو در اون کامپیوتر به ما می‌ده. این پورت اصولا خیلی سر راسته. فقط کافیه که بهش وصل شیم تا اطلاعاتشون بیرون بریزه. البته این پورت رو خیلی از کامپیوترها بسته است. (یادتون باشه که وقتی می‌توان با یه پورت کار کرد که باز باشد).

حالا می‌خوایم با پورت ۱۳ از ip شماره ۱۹٤,۲۲٥,۱۸٤,۱۳ صحبت کنم. یکی از این دو دستور را می‌نویسم:

```
telnet 194.225.184.13 13
nc -v 194.225.184.13 13
```

البته در آن دستورات به جای عدد ۱۳ می‌توان معادلش را نوشت که daytime است.

و جواب می‌شنوم:

```
11:35:33 AM 10/5/2002
```

بله، با این پورت ارتباط برقرار کردیم و اطلاعاتش رو دریافت کردیم. این اطلاعات معمولا به درد این می‌خورد که مکان جغرافیایی اون کامپیوتر را حدس بزنیم (البته اگر زمان اون کامپیوتر صحیح باشد). به عنوان مثال این کامپیوتر خاص در ایران است چون ساعتش همزمان با ایران است.

با پورت ۷ صحبت کنیم

اسم این پورت echo است. من این پورت رو پورت میمون می‌گم چون هرچی که شما براش بنویسید را تقلید می‌کنه و همان‌ها را براتون پس می‌فرستد. مثلا من به پورت ۷ کامپیوتری با ip شماره ۱۹٤,۲۲٥,۱۸٤,۱۳ تلنت یا nc می‌کنم.

```
telnet 194.225.184.13 7
nc -v 194.225.184.13 7
```

بعد از برقراری ارتباط، هر چی من بنویسم، اون برام پس می‌فرسته. مثلا اگه تایپ کنم Ali1000 و Enter بزنیم، جواب می‌شنوم، Ali1000 ... خودتون امتحان کنید تا ببینید. برای تمام شدن کار باید دکمه Ctrl+C را فشار دهیم تا این میمون بازی تموم بشه.

پس کار کردن با این پورت هم زیاد سخت نیست

جلسه چهاردهم

پورت ۷۹ چیست؟

پورت ۷۹ را پورت finger مي‌گویند. کاربرد این پورت به اوایل ایجاد اینترنت برمي‌گرده و کاربردش مخصوص سیستم‌عامل یونیکس بوده‌است (الان هم تقریبا فقط در خانواده سیستم‌های یونیکس این پورت قابل استفاده است).

وقتي این پورت روی سیستم‌عامل یونیکس باز باشه، مي‌شه با یک request ساده فهمید که از بین کساني که در آن سیستم account دارند، کدام‌ها on هستند (یعني کدام‌ها به سیستم login شده‌اند). برنامه‌اي که پورت ۷۹ رو در یک سیستم باز مي‌کنه، finger server مي‌گن و چون مختص سیستم‌عامل یونیکس است، مي‌تونین از عبارت Finger Deamon استفاده کنین. حالا که پورت ۷۹ روي سیستم باز شد، شما مي‌تونین با اون ارتباط برقرار کنین.

با پورت ۷۹ صحبت کنیم

همان‌طور که مي‌دانید، براي صحبت کردن با پورت‌ها از دو برنامه telnet و nc میشه استفاده کرد. در مورد پورت ۷۹ یه نرم‌افزار دیگر به نام finger در تمام سیستم‌عامل‌های یونیکس و برخي سیستم‌عامل‌هاي ویندوز وجود دارد که علاوه بر دو برنامه قبلي، اونم مي‌شه به کار برد.

فرض کنید که مي‌خوام با پورت ۷۹ در کامپیوتری به اسم router2.iums.ac.ir ارتباط برقرا کنم. برای این کار یکي از سه دستور زیر را استفاده مي‌کنم:

```
telnet router2.iums.ac.ir 79
nc -v router2.iums.ac.ir 79
finger .@router2.iums.ac.ir
```

دقت کنید که در دو دستور اول شماره پورت مشخص شده ولي دستور آخري نه، چون دستور finger فقط براي همین‌کار استفاده مي‌شه و نمي‌توان باهاش با پورت دیگه‌ای ارتباط برقرار کرد.

ضمنا به ساختار دستور آخر توجه کنید. بعد از اجرای دستور، جواب مي‌شنوم:

```
  Line      User     Host(s)              Idle Location
 33 tty 33  whgh     Async interface       0
 34 tty 34  najahan  Async interface       0
 35 tty 35  sadf     Async interface       0
```

```
 36 tty 36  abokho    Async interface        0
 38 tty 38  whgh      Async interface        0
 39 tty 39  bzamani   Async interface        0
 40 tty 40  saeedmah  Async interface        0
 41 tty 41  mfaizi    Async interface        0
 42 tty 42  gourabi   Async interface        0
 43 tty 43  farhadz   Async interface        0
 44 tty 44  arbks     Async interface        0
 45 tty 45  mhalavi   Async interface        0
 46 tty 46  farhood   Async interface        0
 47 tty 47  staavoni  Async interface        0
 48 tty 48  whgh      Async interface        0
* 66 vty 0            idle                  0 217.218.84.58

  Interface  User      Mode                 Idle Peer Address
```

نكته مهم اين است كه اطلاعاتي كه به كمک پورت ۷۹ به دست مي‌آد، خيلي بستگي به سروري داره كه اين اطلاعات رو مي‌فرسته. بعضي از سيستم‌ها علاوه بر نام افراد (username) كه در اين مثال ديده مي‌شه، نام و نام خانوادگي افراد، ساعت و محل login كردن و ... را نمايش مي‌دهند. اما چيزي كه هميشه وجود دارد و مشترک است، username هاست كه از نقطه نظر يک هكر بسيار ارزشمند است. در اين مثال ما اكانت‌هايي به اسم whgh،najahan و ... در اين سرور وجود دارد و افراد مربوطه در حال حاضر login كرده‌اند. اگر اكانتي موجود باشد ولي فرد مورد نظر در حال حاضر از آن اكانت وارد نشده باشد، نمايش داده نمي‌شود. اين ليست فقط براي اكانت‌های فعال است. پس نتايجي كه شما در ارتباط با اين سرور كسب مي‌كنيد، با نتايجي كه من نوشتم متفاوت خواهد بود.

اين اطلاعات به چه دردي مي‌خورد؟

اول اينو بگم كه finger كردن، جزئي از مراحل Enumeration است (البته در حالت كاربرد legal يا قانوني). منظور از عبارت Enumeration يا به طور خلاصه Enum، پيدا كردن ليست كاربران است.

- فرض کنید مي‌خواهید یک لیست از پسوردها را تست کنید تا اینکه یکي شانسي درست در بیاد (درست مثل دزدها که یه سري کلید را تست مي‌کنن که یکي به قفل بخوره و باز کنه!) حالا سوال اینه که این پسوردها رو برای چه username ي تست مي‌کنید؟ جواب، username هایي است که با Enumeration به دست اومده است. پس اول با Enumeration یه لیست پیدا مي‌کنید و بعد تعداد زیادی پسورد رو روش تست مي‌کنید (روش این کارو بعدا مي‌گم).
- کاربرد بعدی finger در رابطه با یک سري اکانت‌هاي خاص است. من همیشه وقتي به یک اکانت به اسم guest برخورد مي‌کنم، همیشه پسوردهای guest یا libguest یا myguest و ... رو تست مي‌کنم که گاهي جواب میده. همین‌طور در مورد اکانتي به اسم demo پسورد demo را تست مي‌کنم و ... معمولا موسسات بزرگ پر است از این username هاي عمومي که حدس زدن پسورد مربوطه کار مشکلي نیست.
- گفتم که بعضي سرورهاي finger نام و نام‌خانوادگي افراد را هم برایمان مي‌فرستند. چون بعضي از افراد متاسفانه یا خوشبختانه از این اطلاعات براي پسوردشون استفاده مي‌کنند، مي‌تونه مفید باشه.
- یک کاربرد دیگه و البته بسیار مهم موقعي است که مثلا مي‌خواهید یک سري پسورد رو روي یک اکانت خاص تست کنید. من همیشه اول یک finger مي‌کنم که مطمئن بشم که فرد در حال حاضر login نکرده باشد و بعد این کار رو شروع مي‌کنم (یعني انقدر صبر مي‌کنم که دیگه آن اسم خاص در finger نمایش داده نشه یعني طرف مقابل logout کرده باشد!)
- بازم یه کاربردهاي مهم دیگه هست که الان بهتون نمي‌گم تا تو خماریش بمونین ! شوخي کردم، وقتي بحث پورت‌ها تموم شد و رسیدیم به کاربردهاي غیر معمول این پورت‌ها، براتون حتما مي‌گم.

جلسه پانزدهم

پورت ۸۰ چیست؟

پورت ۸۰ یکی از مهم‌ترین پورت‌هاست. دنیای وب (صفحات اینترنتی) بر اساس همین پورت کار می‌کنه. توضیح اینکه وقتی به یه سایت وصل می‌شیم و صفحه وب را درخواست می‌کنیم، در واقع مرورگر اینترنتی به پورت ۸۰ اون کامپیوتر وصل می‌شه و اطلاعات رو می‌گیره (البته بعد از گرفتن اطلاعات اون رو تفسیر می‌کنه و به صورت یه صفحه نشون می‌ده - دقت کنید که اطلاعات در واقع به صورت یک سری تگ HTML است).

با پورت ۸۰ صحبت کنیم

حالا ما می‌خواهیم با پورت ۸۰ یک کامپیوتر صحبت کنیم ولی به کمک telnet و nc.

اول باید یه connection (اتصال) با پورت ۸۰ برقرار کنیم (مثلا برای سایت hotmail.com باید بنویسم):

```
telnet www.hotmail.com 80
nc -v www.hotmail.com 80
```

پس اول باید یکی از دستورات بالا را استفاده کنیم. من همیشه توصیه‌ام استفاده از nc بوده و خواهد بود.

حالا باید شروع به صحبت با پورت ۸۰ کنیم. من فعلا دو تا جمله براتون می‌گم و بقیه‌اش بمونه واسه بعد. دقت کنید که موقع کار با پورت ۸۰ با تلنت (نه nc) دستوراتی که ما می‌نویسیم، نمایش داده نمی‌شود ولی کار می‌کنه.

۱- اولین جمله اینه: **GET / HTTP/1.0** و بعدش دوتا Enter

به فاصله‌ها دقت کنید. دو طرف / ی که بعد از GET است، فاصله وجود دارد. این جمله به پورت ۸۰ می‌گه که هرچی در header داره، نشون بده. و جواب می‌شنوم:

```
HTTP/1.0 302 Moved Temporarily
Server: Microsoft-IIS/5.0
Date: Thu, 05 Dec 2002 12:02:51 GMT
Location: http://lc2.law5.hotmail.passport.com/cgi-bin/login
X-Cache: MISS from cache5.neda.net.ir
```