آموزش Hack

جلسه دوم

IP چیست؟

شماره‌ایست که به هر کامپیوتر متصل به اینترنت داده می‌شود تا بتوان به‌کمک آن‌شماره به آن کامپیوترها دسترسی‌داشت. این‌عدد برای کامپیوترهایی که حالت Server دارند (مثلاً سایت‌ها) و نیز کامپیوترهای Client که معمولاً به‌روشی غیر از شماره‌گیری (DialUp) به اینترنت متصل می‌شوند، عددی ثابت و برای دیگر کاربران، عددی متغیر است. مثلاً هربار که شما با شرکت ISP خود تماس‌گرفته و به اینترنت وصل می‌شوید، عددی جدید ازبین آدرس‌های خالی و اختصاص‌نیافته، به شما نسبت‌داده می‌شود.

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

xxx.xxx.xxx.xxx که منظور از xxx عددی بین صفر تا ۲۵۵ است (اینقدر فکر بد نکنید!!!). البته بعضی شماره‌ها قابل‌استفاده نیست که علت آنرا بعداً توضیح خواهم‌داد). مثلاً ممکن‌است آدرس شما به‌صورت ۱۹۵,۲۱۹,۱۷۶,۶۹ باشد. حتی اسم‌هایی مثل www.yahoo.com که برای اتصال، مورداستفاده قرار می‌دهید، درنهایت باید به یک IP تبدیل‌شود (که همان آدرس کامپیوتری است که اطلاعات وب‌سایت Yahoo! برروی آن قراردارد)، تا شما بتوانید سایت Yahoo! را مشاهده‌کنید.

در IP معمولاً xxx اولی، معنای خاصی دارد (این را هم بعداً توضیح می‌دهم). فقط این‌را بگویم که اگر به‌روش DialUp به اینترنت وصل‌شوید، معمولاً عددی که به‌عنوان xxx اول می‌گیرید، مابین ۱۹۲ تا ۲۲۳ خواهد بود. این نکته برای تشخیص کامپیوترهای Client از Server (حداقل در ایران) می‌تواند بسیار مفید باشد.

بعد از اتصال به اینترنت، برای به‌دست‌آوردن IP خود، از دستور IPCONFIG در Command Prompt استفاده‌کنید (اطلاعات فنی توضیحات این دستور را نیز بعداً توضیح می‌دهم). فقط دقت کنید که درقسمت PPP Adapter...، در بخش IP Address، آدرس IP شما نوشته شده‌است.

Port چیست؟

طبق ساده‌ترین تعریف، محلی است که داده‌ها وارد یا خارج می‌شوند. در مبحث Hack، معمولاً با پورت‌های نرم‌افزاری سروکار داریم که به هرکدام، عددی نسبت می‌دهیم. این اعداد مابین ۱ و ۶۵۵۳۵ هستند. معمولاً به یک‌سری از پورت‌های مشخص، کارهای خاصی را نسبت می‌دهند و بقیه، برای استفاده کاربران، آزاد است. پورت‌های فعال، توسط یک نرم‌افزار خاص مدیریت می‌شوند. مثلاً پورت ۲۵ برای ارسال E-Mail است، بنابراین باید توسط یک نرم‌افزار مخصوص این‌کار، مدیریت‌شود و این نرم‌افزار، برروی پورت ۲۵ منتظر (فال‌گوش) می‌ماند. دراینجا ممکن‌است افراد مختلف، از نرم‌افزارهای مختلفی استفاده‌کنند ولی درهرحال، پورت ۲۵ همیشه برای ارسال E-Mail است و همه نرم‌افزارها از همین پورت برای ارسال E-Mail استفاده می‌کنند.

در ادامه، لیستی از مهم‌ترین پورت‌ها و کاربردشان را می‌بینید. به این جدول، دقت‌کرده و پورت‌های را که احساس می‌کنید بیشتر موردنیاز شماست، حفظ‌کنید. البته اگر بتوانید همه را حفظ‌کنید که نور علی نور است!

شماره پورت	نام سرویس موردنظر	برای چه‌کاری خوب است؟
۷	echo	کامپیوتر میزبان هرچه تایپ‌کنید، تکرار می‌کند.
۹	discard	دستوری که درحال ارسال آن هستید را لغو می‌کند.
۱۱	systat	اطلاعات زیادی درباره کاربران دراختیار قرار می‌دهد.
۱۳	daytime	می‌توانید بفهمید که در محل کامپیوتر مقصد، ساعت و تاریخ جاری، چیست؟
۱۵	netstat	اطلاعات فوق‌العاده درباره شبکه‌ها
۱۹	chargen	یک رشته از کارکترهای ASCII را استخراج می‌کند.
۲۱	ftp	برای انتقال فایل به‌کار می‌رود.
۲۳	telnet	توسط آن، می‌توانید وارد سیستم‌شوید.
۲۵	smtp	برای ارسال و دریافت E-Mail به‌کار می‌رود.
۳۷	time	ساعت جاری سیستم را تعیین می‌کند.
۳۹	rlp	محل قرارگیری منابع را مشخص می‌کند.
۴۳	whois	اطلاعاتی درباره میزبان‌ها و شبکه‌ها ارائه می‌دهد.
۵۳	domain	نام‌های متناظر با IPها را مشخص می‌کند.
۷۰	gopher	یک شکارچی اطلاعات که از رده خارج‌شده‌است.
۷۹	finger	اطلاعات زیادی درباره کاربران دراختیار قرار می‌دهد.
۸۰	http	Server وب که درابتدای هر آدرس اینترنتی مشاهده می‌کنید.
۱۱۰	pop	E-Mail ورودی
۱۱۹	nntp	شبکه‌های گروه‌های خبری، ارسال و لغو پیام‌ها
۴۴۳	shttp	مشابه http با این تفاوت که امکانات امنیتی نیز در آن گنجانده شده‌است.
۵۱۲	biff	هشدار دریافت E-Mail
۵۱۳	rlogin	ورود به سیستم از راه دور
	who	تشخیص کاربر فعال و زمان فعالیت در سیستم ازراه دور
۵۱۴	shell	صدور و اجرای دستور از راه دور (بدون نیاز به رمز عبور!)
	syslog	دسترسی به گزارشات (Log) سیستم ازراه دور
۵۲۰	route	پروتکل اطلاعات مسیریابی

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

RFC چیست؟

متون بسیار کامل ولی خشک و ثقیل که درمورد مفاهیم مختلف شبکه بحث می‌کنند. این فایل‌ها به‌صورت متنی و با پسوند txt هستند و به‌عنوان مرجع (برای مراجعه و نه مطالعه کامل!) کاربرد دارند. این فایل‌ها یک‌بار منتشرشده و هرگز تغییرداده نمی‌شوند (حتی اگر حاوی اشتباهات متعدد باشند!).

فایل‌های RFC از کجا قابل‌دسترسی هستند؟

RFCها از سایت‌های بسیاری قابل‌دسترسی هستند ولی سایت موردعلاقه من برای RFCها، سایت زیر است:

http://www.ietf.org/rfc/xxxxxxxx.txt

که به‌جای xxxxxxxx نام RFC موردنظر را می‌نویسیم. مثلاً برای دسترسی به rfc791 باید آدرس را به‌صورت زیر تایپ‌کنیم:

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 12

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

RFC9l9 Broadcasting Internet Datagrams

RFC886 Proposed Standard for Message Header Mugging

RFC815 IP Datagram Reassembly Algorithms

RFC814 Names, Addresses, Ports, and Routes 13

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 HYPER channel: 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 14

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 15 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 gateway 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 16

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 17

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 18

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 19

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 20

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