CREST

Common Ports

Port	Service
7	ECHO
9	Discard
13	Daytime
17	QotD (Quote of the Day)
19	Chargen
20	FTP (data)
21	FTP (control)
22	SSH
23	Telnet
43	Whois
49	TACACS+
53	DNS
67	DHCP
68	DHCP
69	TFTP
70	Gopher
79	Finger
80	HTTP
88	Kerberos

Port	Service
110	POP3
111	Sun RPC Endpoint Managr
112	VRRR
119	NNTP (network news protocol)
123	NTP
135	DCE/RPC
137	NetBIOS (datagram)
138	NetBIOS (session)
143	IMAP
161	SNMP
179	BGP
194	IRC
389	LDAP
443	HTTPS
445	SMB/Samba
465	SMTP over SSL/TLS
500	ISAKMP (VPN)
512	rexec
513	rlogin
514	syslog
514	rsh
515	LPD (Line Printer Daemon)

Port	Service
520	RIP
523	DB2
546	DHCPv6 (client)
547	DHCPv6 Server
548	AFP (Apple Filing Protocol)
554	RTSP (Real Time Streaming Protocol)
631	IPP (Internet Printing Protocol)
636	LDAP over SSL
860	iSCSI
989	FTPS (FTP over SSL) data
990	FTPS (FTP over SSL) control
995	POP3 over SSL
1194	OpenVPN
1433	MSSQL
1521	Oracle DB
1702	L2TP (VPN)
1723	PPTP (VPN)
1812	RADIUS (Authentication)
1813	RADIUS (Accounting)
1900	SSDP (UPnP Discovery)
2049	NFS
3306	MySQL

Port	Service
3389	RDP
3478	STUN
5432	Postgres SQL
5900	VNC
6000	X11
6667	IRC
6789	DB2
8080	HTTP Altenative

TTL

The operating system sets the initial TTL value or application creating the IP packet. Here are some common default TTL values:

Operating System	TTL Value
Linux/MAC OS, Android, Juniper	64
Windows 95, 98, NT	32
Windows	128
Cisco Routers	254
DNS	Depends on resolver (can range from 128 to 86400)

rlogin

- Opens ports between 512-514

Service	Port	Protocol
rcp	514	TCP
rexec	512	TCP
rlogin	513	TCP
rsh	514	TCP
rstat		UDP
ruptime	513	UDP
rwho	513	

Please note

- rlogin doesn't return any message when connection is successful
- rlogin and rsh use `/etc/hosts.equiv` and `$HOME/.rhosts`
- rlogin uses `rlogind`; rsh uses `rshd` as a daemon

hosts.equiv and .rhosts format

```
host1
host2 user_v
-host3
+@group1 -user_c
-@group2
```

> The traffic transmitted is unencrypted. The login process is without a password. This is blocked on modern systems

> The traffic can be intercepted and spoofed.

Command Examples

POP

POP protocol is session based.

> Changes occur only after you type QUIT.

```
USER [username] # type the username
PASS [password] # type the password
QUIT # log out

STAT # Total number of messages and total size
LIST # List all messages - indexed list
RETR [message index] # retrieve the message with the index id
DELE [message index] # Delete specified message
TOP [message index] [num lines] # return headers and top X lines of a message
UIDL [message index] # return unique ID
NOOP # Do nothing (no operation)
RSET # Undelete the messages if any marked for deletion
```

SMTP

```
HELO[FQDN] # establish connection
MAIL FROM # specify email address of the sender
RCPT TO # specify email address of the recipient
DATA # present content of the message (body text, attachments) you must send a . (full stop)
on a new line to complete the command
RSET # aborts current transacitons
VRFY # check if user or mailbox exists on the server
NOOP # Do nothing (no operation)
```

```
QUIT # Exit
```

SNMP

Some of the utilities used for SNMP protocol

- snpget
- snmpwalk
- snmpbulkget
- snmpbulkwalk

SIP

```
INVITE # invite a user to a call
ACK # acknowledgment is used to facilitate reliable message exchange for INVITEs.
BYE # Terminates a connection#
CANCEL # Terminates a request, or search for a user.
OPTIONS # solicits information about a server’s capabilities
REGISTER # registers a user’s current location
INFO # used for mid-session signalling
```

Telnet

```
-d #debug
-a #automatic login
-n tracefile # opens tracefile
-l user #specify user
-e escape char # specify escape char
-E # no character is recognised as escape character
```

```
-x # activate encryption

#Modes
character # Disables LINEMODE
line # enables LINEMODE
send abort # abort process
environ define variable value # assign a value to a variable
```

ICMP Responses

The below is not an extensive list. The rest of the responses are either deprecated or experimental

Type	Value
0	Echo reply
3	Destination Unreachable
5	Redirect
8	Echo
9	Router Advertisement
10	Router Solicitation
11	Time Exceeded
12	Parameter Problem
13	Timestamp
14	Timestamp Reply
40	Photuris
42	Extended Echo Requests
43	Extended Echo Reply

Misc

Encryption/Hashing

Block Ciphers

- ECB - Electronic Code Block
- CBC - Cipher Block Chaining
- OFB - Output Feedback
- CTR - Counter

Common Encryption algorithms

Name	Bits	Key length
DES	64	56
3DES	168	112
IDEA	128	
RC4	128	40
RC5	2048	0
AES	256	
RSA	2048	

Linux Password Hashes

- 1 - MD5
- 2ay - Blowfish
- 5 - SHA256
- 6 - SHA512

DNS

Record Type	Data
A	IPv4
AAAA	IPv6
CNAME	canonical name
ANAME	
SOA	Start of Authority
NS	Name Server
MX	Mail Exchange
TXT	Text record for various (SPF, DMARC, etc)
PTR	Pointer record

> Zone transfers happen over TCP 53. DNS queries over 53