HTTP
Hypertext Transfer Protocol, text/graphics
Client/Server application, Request/Response
TCP/80, URI (Uniform Resource ID)
clear-text passwords
```
ip http authentication [en|loc|tac]
ip http access-class ACL
ip http port PORT
```
HTT PS
security enhancement, certificate-based (SSL)
TCP/443, authentication/encryption serv-cli
trusted CA, X.509, public key certificate
```
ip http secure-server
ip http secure-port
```
SMTP
Simple Mail Transfer Protocol
email handling (sending), TCP/25
Mail client → MUA - Mail User Agent
Mail server → MTA - Mail Transfer Agent
SMTP handles the envelope only, not the body
Sec - username/password
optional - STARTTLS, SSL
messages
HELO - initiates the connection
MAIL - initiates the mail transaction
RCPT - set of recipients
SEND - sending the mail
DATA - data of the email
ESMTP - Enhanced SMTP
DHCP
Dynamic Host Configuration Protocol
dynamic IP assignment, client/server
DHCP operation
DHCPDISCOVER (C→broadcast)
DHCPOFFER (S→C)
DHCPREQUEST (C→S)
DHCPACK (S→C)
UDP/67 DHCPS, UDP/68 DHCPC
lease-time, various DHCP options
DHCP Relay (helper)
DHCP snooping, interface rate-limit
DNS
Domain Name System, TCP.UDP/53
TCP - DNS Zone transfer
UDP - DNS lookups
hierarchical, name-to-IP, namespace (name, IP)
name servers - root, then lower
caching, recursive (non-authoritative)
record types
SOA - Start of Authority
NS - Nameserver
A - Address
CNAME - Canonical Name
MX - Mail Exchange
PTR - Pointer
AAAA - IPv6 Address
FTP
File Transfer Protocol, TCP/20,21
clear-text auth, TCP21 open, TCP20 data
active vs. passive mode
listing function, anonymous access
Simple FTP - between FTP and TFTP (RFC913)
TFTP
Trivial File Transfer Protocol
easy, no auth, no listing, UDP/69
NTP
Network Time Protocol, TCP.UDP/123
Client/server, PtP, bcast/mcast
```
ntp authenticate
 ntp trusted-key X
```
NTP stratum, then +1, ntp auth
IOS Config
```
 ntp master
 ntp peer X.X.X.X key XYZ
 ntp authentication-key X md5 XYZ
```
SNMP
Simple Network Management Protocol, UDP/161
three versions
v1 - community, poor securitz
v2c - comm-based, user-based, interoper w/ v1
v3 - complex security - user/group, encr, auth
MIB - Mngmt Information Base - set of objects
community, RO/RW, access-class, SNMP view
SNMP notifications/traps
Syslog
message or event logging, server/client
UDP/514, TCP/6514
facility
local0-local7, kern, user ...
severity level
0 - emergency
1 - alert
2 - critical
3 - error
4 - warning
5 - notice
6 - informational
7 - debug
no auth, no encr, simple protocol
Netlogon
MS Windows server process
authenticate the user in domain
using SMB (Server Message Block prot)
NetBIOS
Network Basic I/O System
API, related to L5 OSI, UDP/137-138,TCP/139
Name Service
using 16B name
Add Name, Delete Name, Find Name
Datagram Distribution Service
control for connectionless sessions
Send [Bcast] Data, Receive [Bcast] Data
Session Service
Complete session control
Call, Listen, Hangup, Send, Receive
WINS - NetBIOS Name Server
Serve Message Block (SMB)
also known as CIFS (Common INET FS)
L7 OSI, sharing the data, TCP/445
SMB 2.0 - Vista, less chattiness,symlinks
SMB 2.1 - Win 7
SMB 3.0 - Win 8, multi connects per session
Samba - unix equivalent for FS
RPC
Remote Procedure Call
Client/Server, base for NFS
JSON, JAVA-RMI, Python Spyne
client calls server and execute the command
RDP
Remote Desktop Protocol
Microsoft, TCP/3389, client/server
graphical remote access, RC4 encryption
support of TLS, FreeRDP/XRDP
VNC
Virtual Network Computing
GNU GPL, TCP/5900, client/server
using RFB - remote framebuffer
encrypted password, encryption key
PCoIP
PC over IP, Teradici remote graphic
thin-client provisioning
VMWare and AWS support
lossy and highly compression
OWASP
Open-WEB App Security Project
US non-profit org
makes software security documented