3.1

Thursday, September 21, 2023 12:17 PM

DNS on port 53

DNSSEC packets > 512 bytes which is limit for UDP

uses TCP instead (53)

kerberos = TCP and UDP port 88

LDAP = UDP port 389

session initiation protocol SIP - establish, disestablish, and manage VOIP

- user discovery
- availability
- negotiate session params (audio/vid
- session management

SSL/TLS - encrypt tcp connections

SSL/TLS - encrypt tcp connection and HTTP

between app and transport layers

Stratum 1 servers obtain time from accurate clock like atomic clock

Stratum 2 from stratum 1

Stratum 3 from Stratum 2

cant go backwards

SFTP

ssh

TCP port 22

FTPS

TLS

TCP port 989 990

or FTP = port 20 ; 21

TFTP - trivial FTP

connectionless proto that uses

UDP 69

Explicit TLS FTPES - uses

AUTH TLS to upgrade

unsecure connection on port

21

protects auth creds

LDAPS = LDAP secure w/ TLS

fingerprinting - use port scanner tools to reveal presence of router and dynamic routing / manage protocols if it is running

route injection - traffic misdirected to monitoring port (sniffer), sent to blackhole (non-exist addr), or continuously looped

routers can block traffic

SFTP uses SSH, not TLS, so therefore not a tunnel

Transport mode = private net

Tunnel mode = VPN

AH - authentication header; does hash
plus

AH - authentication header; au
on whole packet + header plus
shared secret key
HMAC added as Integrity check value
ICV

integrity not confidentiality

Encapsulation security protocol ESP
encrypts payload
CI + authentication

Kerberos - secure authen + autho proto
for directory services

secure comms for dir services

SSO based on time-sensitive
ticket granting system

routing protocols such as Border
and

routing protocols such as
gateway protocol BGP and
Open Shortest path first OSPF

transmit new and updated routes
between routers/gateways for
fast comms

SSO provides enterprise access to
Sob services

SNMPv1 and v2c both use
community names sent over
plaintext

SNMPv3 uses encryption & auth

Management Information Base MIB
database that SNMP agent uses

tion RSS - feeds

Really simple syndication RSS - feeds
push updated articles or news
items to client/browser

Voice/video stream comms:

- SRTP encrypts actual data
  in calls
- SIP provides session management
- SIPS secure w/ TLS
- QoS info about connection
  like outages, dropped packets, ..

Unified communications UC
voice, message, whiteboards, data
share, email, video

VOIP ≠ video

Video teleconferencing VTC

voice + video

"cant be only audio"

Web conferencing

live meetings

SMTP - how mail is delivered from 1 system to another

Secure Internet Message Access protocol v4

IMAP4

dial-up access

client contacts server to download messages then disconnects

supports perm connections and multi-clients to same mailbox

Secure Post office protocol POP3

where mail stored

Secure Post office protocol

mailbox protocol where mail stored on server and downloaded to recipients email at their convenience

S/MIME - digital cert containing public key signed by CA

TLS 1.2 added TLS from 1.1

SSL 2.0 deprecated

SSL 3.0 less secure than all TLS