

CompTIA Security + 2.0 Technologies and Tools

Filename: comptia-seclussy0501-2-6-implement_secure_protocols

Title: Implement Secure Protocol

Subtitle: CompTIA Security+ (SY0-501)

2.6 Implement Secure Protocols

- Given a scenario, implement secure protocols
 - Protocols
 - DNSSEC
 - Show Windows Client NRPT/DNSSEC settings
 - S/MIME
 - SRTP
 - Securing RTP
 - Provides authentication and encryption
 - LDAPS
 - Show nmap port scan on DC 10.10.10.100
 - FTPS
 - SFTP
 - SNMPv3
 - SSL/TLS
 - mentioned below
 - HTTPS
 - Show Google Cert mention it's integrity and encryption usage
 - Secure POP/IMAP
 - SSH
 - Start Wireshark on Mac with *SSH* filter
 - Verify *sshd* is running on CentOS7 box
 - `systemctl -a | grep ssh`
 - `ip addr` note IP address
 - Connect to CentOS via Mac terminal
 - Verify in WireShark SSH stream
 - Use cases
 - Voice and video(*mentioned in SRTP*)
 - Time synchronization(**mention importance**)
 - Email and web(*mentioned in Secure POP/IMAP and S/MIME*)
 - File transfer (*mentioned in FTPS, SFTP*)
 - Directory services(*mentioned in LDAPS/LDAP*)
 - Remote access(*mentioned in SSH/Telnet*)
 - Domain name resolution(*mentioned in DNSEC*)
 - Routing and switching(**mention protection via above technologies**)
 - Network address allocation
 - Subscription services(**mention with HTTPS**)