Practical 2—drag and drop—certificates—answers Put the correct answer against each item	
The CA used for b2b	Public CA
A certificate used on multiple servers with one domain	Wildcard
Private key file extension	`.pfx`
Is my certificate valid?	CRL
First part of encryption	Exchange keys
Public key file format	`.cer`
A certificate used on servers in multiple domains	SAN
Who signs the X509 certificates	CA
Create new keys	CSR
CRL going slow, implement what?	OCSP
Private key format	P12
Prevent CA compromise	Pinning
X509 serial number	OID
Stores private keys	Key escrow
PKI to PKI trust	Bridge Trust Model
PEM	Base 64 format
Creates a secure tunnel	Diffie—Hellman
Stores the keys for the key escrow	HSM
Public key file format	P7B
They build the CA and/or intermediary	Architect
Web server bypassing CRL to go to OCSP	Stapling
Where is the X509 issuance policy held?	Certificate Template
What uses a web of trust?	PGP
The smaller the key...	The faster but less secure the encryption

Practical 3—drag and drop—ports/protocols—answers Put the correct answer against each item	
Lightweight Directory Access Protocol (LDAP)	389
Domain Naming System (DNS)	53
Remote Desktop Protocol (**RDP**)	3389
Simple network management protocol	UDP 161
Secure copy protocol	22
Lightweight Directory Access Protocol Secure (LDAPS)	636
File transfer protocol—passive	21
FTPS	989/990
Simple network management protocol— secure	UDP 162
Secure shell	22
Telnet	23
IMAP 4	142
POP 3 secure	995
Simple Mail Transfer Protocol (SMTP)	smtp 25
SIP	sip 5061
Worm	5000
IMAP 4 secure	993
Virus	1900
Ransomware	445
NETBIOS	137-139
TLS	443
HTTP	80
POP 3	110
HTTPS	443

Practical 4—drag and drop—authentication factors—answers Put the correct answer against each item	
Somewhere you are	London
Third-party to third-party authentication	Federation services
SAML—XML-based authentication	Federation services
Something you are	Palm reader
Something you are	Retina
Something you are	Iris
Something you know	Password
Something you know	PIN
Something you know	Birth Date
Something you do	Swipe
Something you do	Natural signature
Something you do	Gait
Prevents replay attacks	Kerberos
Wireless router password	PSK
Wireless—no password	WPS
Something you have	Token
Something you have	Smart Card

Practical 5—drag and drop—general—answers Put the correct answer against each item	
Captures the command on a network	Protocol analyzer
Where you keep a safe	Office
Authentication—provides most errors	Passwords
Web server information	Banner grabbing
Identity type of computer in a report	Standard naming convention
Prevent SQL injection	Input validation
Prevent SQL injection	Stored procedure
RAID 0—minimum disks	2
Where you keep keys	Office
Configures multiple settings on computers	Group policy
RAID 6— parity	Double
Policy used for BYOD commencing	Onboarding
Kerberos authentication	SSO
Prevent laptops from being stolen	Cable locks
Authentication for an office	Proximity card
RAID 5—minimum disks	3
Encrypts large amounts of data	Symmetric encryption
RAID 5—parity	Single
Finds a mobile device	Geolocation
A person leaves—what do you do with the account?	Disable account, reset password
Prevents a device from being stolen from a ship	RFID
Makes mobile devices secure	Strong passwords
RAID 1—number of disks	2
Prevents tablets being stolen	Cable locks
Makes mobile devices secure	Screen locks
RAID 6—minimum disks	4

Linux information

Although Linux is not mentioned in the exam syllabus, the Security+ exam is vendor neutral and the following commands may help you determine what is being asked:

- **Admin accounts**: Root top level
- `sudo`: Admin
- `su`: Lower admin
- `Kill` : Stops applications
- `Ls` : List
- `Grep` : Search
- `Pwd` : Parent Working Directory
- `Chmod` : Changes permissions
- `Mkdir`: Make directory
- `SetFACL` : Used to set permissions on a given file
- `Ifconfig`: Equivalent of `ipconfig`
- `IpTables`: Firewall rules
- `Chroot`: Change root directory
- **Root directories**: `/bin`, `/boot`, `/dev`, `/etc`, `/home`, `/mnt`, `/sbin`, and `/usr`