What is the OCSP used for?
As a faster method for certificate validity

What is a Data Recovery Agent?
An administrator who recovers data when keys go corrupt

Where does the DRA get the recovery keys?
They will get the private key from the key escrow

Why might a certificate use extended validation?
It proves that the certificate has a higher level of trust.

What is PGP?
Asymmetric encryption between two people

What do you need to set up PGP?
A key pair. Both people exchange public keys.

What is a trust model?
This is a bridge trust model in which two CAs send each other a certificate and trust each other. Known as cross certification.

Where is a web of trust used?
Used in PGP where the two parties trust each others' certificates

When you install a certificate, where is it added first?
It is added into the Trusted Root Certificate Authorities Store. It is then trusted by the computer.

What is the function of certificate chaining?
It shows trust, from the CA and the intermediary through to the certificate itself. It is normally comprised of three layers: the vendor, the CA, and the computer itself.

What does certificate pinning prevent?
It prevents CA compromise, certificate forgery, and M-I-M attacks

What is the purpose of certificate stapling?

It allows a web server to query an OCSP for faster lookup

What is the extension and PKCS of a private key?
.pfx extension, P12 format

How does a private key provide non-repudiation?
There is only one private key; therefore, if you digitally sign an email or document, they cannot deny it was not you.

How can a private key provide integrity?
If you digitally sign your email, it creates a hash value. It can then be checked using your Public Key to verify integrity.

What is the extension and PKCS of a public key?
.cer extension, P7B format

What certificate extension uses a BASE 64 format?
PEM - ASCII (Base 64 format)

What tool do you use to protect DNS traffic?
DNSSEC. It produces RRSIG records.

What is the first step in encryption?
Exchange keys

How many keys are there in asymmetric encryption?
It uses two keys: public and private

Which asymmetric technique creates a secure channel?
Diffie Hellman (he does not encrypt, he builds tunnels)

What is the purpose of using Diffie Hellman?
It is used in the IKE handshake setting up an IPSec channel used UDP Port 500. In-Band Key Exchange. Creating a secure channel before symmetric keys are exchanged.

What is ECC used for?
For encryption of mobile devices, as it is small and fast and uses a Diffie Hellman handshake.

On which cell phone would you never use ECC?
A military mobile phone. You would use AES-256.

What are the two functions of the private key?
The creation of a digital signature and the decryption of data.

Whose public key do you use to encrypt data?
You always give your public key away and use someone else's

If you are going to set up a server to accept SSH for remote access, which key do you install on the remote server?
The public key. Your private key is like your bank card; you can never send it anywhere. Please remember that a key pair also includes a private so both are never installed on a remote server

What does the command ssh-keys -t RSA produce?
It creates a key pair of RSA certificates

How many keys are there in symmetric encryption and what are they called?
Symmetric encryption uses one key, called the secret key.

Why is symmetric encryption used for encrypting large amounts of data?
It uses block cipher and has a smaller key. Where stream cipher is bit by bit encryption, block cipher is faster to pack and is therefore better for moving large amounts of data.

Name five symmetric encryption techniques
Blowfish 64 bit, Twofish 128 bit, DES 56 bit, 3 DES 168 bit, AES 128/192/256 bit

Which is faster, a twofish or blowfish?
Blowfish. Remember you can blow faster than you can pick up two fish.

Which encryption algorithm has the smaller key?
DES - it uses a 56 bit key in the CompTIA Security+ exam

Which is the strongest protocol for a L2TP/IPSec tunnel?
AES – goes up to 256 bit

What are the two portions of an IP Sec packet?
Authenticated Header (AH; uses SHA1/MD5), and Encapsulated Security Payload (holds the data that is encrypted by DES, 3 DES or AES).

Is hashing reversible?
No. It is a one-way function.

What is the main reason to use hashing?
Integrity of data

What is hashing?
Taking data and transforming it into a numerical value

How can you tell if your data has been tampered with?
Hash the data before and after. If the hash value is different, then the data has been tampered with.

Name two hashing techniques
MD5 128 bit. SHA1 160 bit.

What is HMAC used for?
Data integrity and data authentication.

What is a NAT used for?
Hiding the internal network securing internal routing

What is an IDS?
Intrusion Detection System. It detects changes to network traffic, using sensors and collectors. Think of it as being Sherlock Holmes.

What is an IPS?
Intrusion Prevention System. It protects against attack. Think of it as being your Intrusion Protection System: John Wick with a huge gun.

What device is known as inline?
The NIPS - all the traffic flows through it

Where can NIPS and NIDS operate?
They are both network-based as they start with a 'N'. They cannot be used on a host.

Where can HIDS and HIPS operate?
They are host-based as they start with a 'H'. They cannot operate on the network.

When would you use a HIPS?
To protect a guest virtual machine or a host desktop from attack

Where would you place a NIPS?
Behind the firewall as an additional layer of security

What are the limitations of a signature-based IDS/IPS?
They can only operate on a known database

What is the weakness of a signature-based NIPS/NIDS/HIDS/HIPS?
If the signature database is not updated, it cannot find new variants

What is the function of an anomaly-based IDS/IPS?
It has the signature database but can find new variants and add them to the database. Sometimes called heuristic.

What is an inline NIPS?
A NIPS where the traffic must go through it

What is a passive IDS?
The traffic does not go through it. This is normally your IDS that scans the network for attacks and new hosts.

What is the function of active monitoring?
It will alert you of any changes in real time

What is the function of passive monitoring?
It only listens

What is a SCADA network?
Supervisory Control and Data Acquisition (SCADA) is a network with a controller and many layers that monitors many layers of

industrial systems. An industrial plant that makes water, gas, oil, or nuclear material is one such example.

How can you stop unauthorised traffic to a SCADA network?
Use a firewall

What is an example of an additional layer of security for a SCADA network?
Installation of a Network Intrusion Prevention System (NIPS)

What is a Storage Area Network (SAN)?
It is a hardware solution that holds a large amount of fast disk storage

Who uses a SAN, and what for?
Cloud providers for storing virtual guests. Companies using virtualization for mail and SQL databases..

What is the purpose of an 802.1x switch?
An 802.1x switch is a managed switch that authenticates users and devices.

What is port security?
A security measure which limits the functionality of a switch by turning the port off

If someone connects a laptop to your network how would you prevent this?
Port Security

How would you prevent a rogue access point?
802.1x - it authenticates devices and would not let the rogue access point attach to your network

Why would you create a VLAN?
For network segmentation. Think of it as departmental isolation.

What is needed to send traffic to the correct VLAN?
A VLAN tag. Each VLAN has a different tag.

Why does a switch use a flood guard?

To prevent MAC flooding or a SYN flood attack on a switch

Why would you use a VPN?
To create a secure channel between you and your work

What is the most secure VPN tunnel?
L2TP/IPSec

What is a split tunnel?
This is where a secure remote connection is made to your company and the user then opens up an insecure connection.

Describe IPSec Tunnel Mode
It sets a VPN tunnel over the internet, where both the packer header (AH) and the data payload (ESP) are encrypted.

Describe IPSec transport mode
It is used internally from server-to-server or client-to-server. Only the data payload (ESP) is encrypted..

Describe the function of Internet Key Exchange (IKE)
It uses a Diffie Hellman handshake, creating a secure VPN session.

What is the purpose of a VPN Concentrator?
It is a device that creates a secure connection for the VPN tunnel.

Describe an ALWAYS ON VPN
It is used with a site-to-site VPN. The connection is always live.

When would you use a site-to-site VPN?
As a point-to-point connection, normally between two sites or a Head Office and a Branch Office

What is SRTP?
Secure Voice Traffic. SIP and RTP are also used for video-conferencing.

Describe Network Access Control (NAC)

It happens after a remote user authenticates themselves on a network. The health authority checks that the device being used is fully patched.

What does NAC do with non-compliant machines?
It puts them into a quarantine network where a remediation server gives updates to the host

What is a NAC Dissolvable Agent?
The agent is put on the host so it can be checked and removed after the audit

What is a NAC Permanent Agent?
The agent stays permanently on the host. This is the best method to ensure that the NAC is enforced.

What is a load balancer?
It is used to balance the load of a high volume of web traffic

What is affinity?
Affinity is where the load balancer sends the client to the same host each time

What is a proxy server?
It is a go-between through which the client requests a webpage. It changes the internal IP to an external IP.

In what direction does a proxy work?
Internal to external

What type of attack could someone use a proxy server for?
Man in the middle

What are the three main roles of a Proxy server?
URL filtering, content filtering, webpage caching.

What is a URL filter?
A filter that stops someone from going to a website by blocking a particular URL. Example: if we block www.nfl.com, nobody can visit the football site.

How would you complete a URL filter?
Add the URL to the Default Block Page

What is content filtering?
It blocks access to a website based on the content available on that site. An example would be a filter to prevent gambling.

What is the function of an active proxy?
It caches web pages in advance. You would set up a job to do this.

What is the function of a passive proxy?
It fetches and caches web pages when requested, if they are not already in the cache.

Why can't stock market data be actively cached?
The transactions refresh far too quickly

What is the function of a reverse proxy?
It authenticates incoming requests. The traffic flows external to internal.

What is another function of a reverse proxy server?
It decrypts incoming traffic. This can take a large amount of CPU.

How should your relationship with your Cloud Service Provider (CSP) be?
You should be able to trust them 100%

What is MaaS?
Monitoring-as-a-service. This is where the company monitoring your network and logs is cloud-based.