What type of attack is an interception attack in which the data is forwarded at a later date? What authentication protocol can prevent this?
Replay attack. This can be prevented by using Kerberos.

What type of attack is an amplification attack in which a directed IP broadcast is sent to the border router and the victim gets the resultant reply? How can this be prevented?
A Smurf Attack sends a directed IP broadcast to a border router with the victim getting the replies; each packet produces four replies. This can be prevented by disabling IP broadcast on the border router.

What type of attack is an on-path attack in which the data is replayed immediately?
A Man-In-The-Middle attack is an interception attack in which the data is replayed immediately. An example is a POODLE attack.

What type of attack is it when someone pretends to be from the helpdesk and calls you to reset your password?
A Social Engineering impersonation attack is where the attacker pretends to work on the help desk.

What type of virus attack cannot be detected by anti-virus software, NIDS, NIPS, or a SIEM system? How can you detect it?
A Zero-Day virus has no updates until 2-3 days after discovery. The only way to detect it is by comparing the original baseline with the current baseline.

What type of attack is it when the HR Manager sends you an email demanding that you complete a form that has your personal details?
A Social Engineering authority attack sends you an email to obtain your details. It could come from the CEO or the HR Manager.

What type of attack is an email attack that is sent to the high-level executives in your company?
Spear Phishing is an attack sent to high-level executives (plural). If it is singular, it is called a whaling attack.

What is a Pass-the-Hash attack? Name two ways to stop it.
A Pass-the-Hash attack is launched on a server that uses NTLM as the authentication protocol. It can be stopped either by installing Kerberos or by disabling NTLM.

What type of attack is it if a fireman arrives and you let him into the server room?
A Social Engineering urgency is when you let the fireman into the server room. It is urgent because the receptionist is worried that the room will burn down.

What type of attack uses interference as its attack vector?
Jamming is an interference attack wherein the wireless communication is interrupted.

What authentication model uses tokens?
OAuth 2.0

What authentication model uses tickets?
Kerberos

What authentication model is short-lived?
TOTP 30 - 60 seconds

What authentication model uses cookies?
Federated Services

What authentication model prevents replay attacks?
Kerberos. It uses USN and time stamps

What authentication model uses extended attributes?
Federated Services

What authentication model is third party to third party?
Federated Services

What authentication model reduces the number of times you need to authenticate within a system?
Single sign-on

What authentication protocol supports OpenID Connect?
OAuth

What authentication model prevents a hash attack?

Kerberos

What authentication model do IaaS, PaaS and SaaS use?
Cloud uses Federation Services and could use SAML tokens

When a user’s certificate becomes corrupt, what support person will help them get their data back, what key will they need, and where will they obtain that key?
The Data Recovery Agent (DRA) will obtain a copy of your Private Key from the Key Escrow to decrypt your data

What do the CRL and OCSP have in common, and how do they differ?
Both the CRL and the OCSP can tell you if your certificate is valid. You would use an OCSP only when the CRL is running slowly.

What is the file extension and format of a Private Key?
The Private Key has an extension of .pfx and is a P12 format

What is the file extension and format of a Public Key?
The Public Key has a file extension of .cer and is a P7B format

Which key can be protected by a password?
When you export a Private Key, you can create a password for it.

If you have encrypted data with an old CAC card and need to recover the old data, how can you achieve that?
You need to obtain a copy of your old Private Key to decrypt the old data

What is the difference between certificate stapling and certificate pinning?
Certificate Stapling is when a web server bypasses the CRL and goes to the OCSP for faster certificate validation. Certificate Pinning prevents CA Compromise and Fraud.

When either a client computer or a web server gets a certificate trust error, what are the first two things that you need to test?
When a device has a certificate trust error, you must ensure that the certificate has not expired and has been added to the Trusted Root Certificate Authorities store. The certificate will be cached locally.

If the certificate on your laptop is working prior to loaning the laptop to a colleague but displays a certificate trust error upon its return, what could have been done to cause this?
If your colleague has deleted the local certificate cache on the laptop, the certificate will no longer be trusted.

When designing your Certificate Authority, what is the first thing that you need to decide?
When designing your Certificate Authority (CA), you need to decide whether you are going to use Public or Private Certificates even if your CA is going to be used locally.

What is the fastest tool to determine if a certificate is valid?
OCSP; it is much faster than legacy CRL

How many keys are there in symmetric encryption, and what are they called?
One Key, called either the private or shared key

Which key would you use to encrypt data in a PKI environment?
The public key of the recipient (the person receiving the encrypted data)

How many keys are there in asymmetric encryption, and what are they called?
There are two keys the public and private. The private key is always retained.

Name the ephemeral keys.
Diffie Hellman (DHE) and Elliptic Curve Cryptography (ECDHE). These are one-time use keys.

Which key provides non-repudiation?
Private key, as you digitally sign an email (for example). There should only be one private key.

Which encryption type is used for small mobile devices?
Elliptic Curve Cryptography (ECC). AES-256 is used for military phones,

How can you check if a certificate is valid, even without the internet?
CRL - this is the default, even if you have no internet it can

be internal. OCSP is used when the CRL is going slowly, or if you want a much faster option.

What is certificate stapling?
Where the web server bypasses the CRL and goes to the OCSP for faster validation

What file extension and PKCS is a private key?
.pfx (file extension). P12 (PKCS format).

What is a CSR?
It is a new certificate request.

What is the file extension and format of a public key?
.cer (file extension). P7B (PKCS format).

When a laptop is taken from a suspect, what is taken from the laptop to be given to the forensic investigator?
The forensic team will capture a system image.

Why would a forensic investigator use the following command? dd if = /dev/sda of = /dev/sdb
To copy the entire hard disk. They are going to copy the first SCSI disk (sda) to the second SCSI disk (sdb).

What is chain of custody?
Recording all stages wherein evidence is collected and names of those who have handled it until it goes to court

What would happen if you put evidence in a suitcase, locked it, and put it in the checked luggage on a flight?
You would have broken the chain of custody

What should you do with evidence if it is collected from different countries at the same time for a multinational criminal investigation?
Record the time offset, with the local regional time

What is time normalization?
Taking the regional times of the data collected, using a time zone such as GMT, and converting the time offset to GMT. This would give a true picture of the sequence of events.

What precautions should you take before investigating forensic data?
 Hash the data. You would also hash the data afterwards to prove to the court that the evidence was not tampered with.

What clause should you ensure is added to any contract with a cloud provider so you can collect evidence?
 A 'right to audit' clause

What is Legal Hold?
 Preventing someone who is under investigation from deleting the evidence--for example, placing legal hold on a mailbox. This would put the emails in a purges folder and prevent deletion.

What is the first stage of investigating a web-based attack?
 Capturing the network traffic

When would you stop an attack and not collect the volatile evidence?
 The exception to collecting the volatile evidence first would be when you have a dynamic or rapidly spreading virus. In exceptional cases, you may need to contain it through isolation as you would not be able to control it.

Name two hashing algorithms
 SHA1 160 bit and MD5 128 bit

If my server has NTLM authentication, what is it vulnerable to?
 Pass-the-Hash attack

What are Rainbow Tables?
 Pre-computed lists of passwords with corresponding hashes

What is the purpose of hashing a document?
 For data integrity

What can I do to prevent a pass-the-hash attack? Name two ways in order of priority.
 Enable Kerberos or Disable NTLM. (Enabling Kerberos is higher priority.)

What type of website attack uses the phrase 1=1?
SQL Injection

What type of website attack uses the tool strcpy?
Buffer Overflow

What type of website attack uses netcat, telnet, curl, nmap or Dimitri?
Banner Grabbing

What is the best way to stop a SQL injection attack?
Stored Procedure

What would be the second choice to stop a SQL injection attack?
Input Validation

What is the first stage my forensics team should take when they discover a website attack in progress?
Capture the network traffic to identify the cause

What is a website attack that can use HTML tags or JavaScript?
Cross Site Scripting (XSS)

What would you use to control the data being put into a web request form?
Input Validation

What could you use to find the patch level version of your web server?
Banner Grabbing

What is Risk Control Self-Assessment?
A bottom-up approach. Employees fill in a survey.

What is inherent risk?
Raw risk

What is residual risk?
The small amount of risk left over after mitigation

What is control risk?
Checking the risk after implementation to ensure it is valid

What is GDPR?
An EU law ensuring data privacy user rights

What is Sarbanes-Oxley (SOX)?
A US law on financial transactions

What is HIPAA?
US law protecting medical information

What is PCI DSS
Regulations on card payments

What is the RPO?
The amount of time you can be without your data, i.e. acceptable downtime. After this point the company operations would be adversely affected.

What is the RTO?
The time when you are back to an operational state

What is measured by the MTTR?
Time to repair an item

What is measured by the MTBF?
The reliability of a system

What is a tabletop exercise?
A paper-based hypothetical exercise

What is a site risk?
Construction site risks and hazards, e.g. spillage of chemicals. You need a health and safety certificate.

What is a hacktivist?
A politically motivated hacker with a social conscience

What is a script kiddie?
Someone with low technical skills. They purchase a program from the Dark Web. Their motivation is fame and notoriety.

What is a direct access attack?
An attack where someone gains physical access to a company

What is a supply chain risk?
A risk from third-party maintenance or supplier or sub-contractor. The target computer could get a virus from the HVAC maintenance personnel.

What is the risk from removable media?
Purchasing unlicensed products or obtaining free products that could contain a virus

What is OSINT?
Open source intelligence, freely available

What is closed/proprietary intelligence?
A higher level of intelligence purchased from a commercial company that specialises in obtaining this information

What are Public/Private Information Sharing Centers?
Where the government and the private sector share threat information

Why would commercial companies trawl the Dark Web?
To identify people who sell illegal products

How can people that sell on the Dark Web avoid detection?
Use the Onion Router (TOR). It has many layers to help avoid detection.

What is STIX?
Structured Threat Information Exchange. From MITRE.

What is TAXII?
Trusted Automated Exchange of Indicator Information

Why do STIX and TAXII work together?

To distribute Counter Threat Intelligence (CTI) over HTTP

What is AIS?
Where the US Federal Government shares information about cyber attacks. Can participate in STIX and TAXII.

What is predictive analysis?
Filtering huge data volumes using machine learning

What is the following image an example of? <img src="https://secplusprod.wpengine.com/wp-content/uploads/2021/10/flashcard_image_1.png" />
A Threat Map

What is the following image an example of? <img src="https://secplusprod.wpengine.com/wp-content/uploads/2021/10/flashcard_image_2.png" />
A Risk Matrix or Heat Map. More severe risks are in red; they have a larger number.