What are two ways to complete network segmentation or separation?

VLAN and a screened subnet (DMZ)

What type of device could suffer an arp attack?

A switch, because it works with MAC addresses

Which two devices use ACL?

Firewall and router

What device sits in the DMZ, authenticates incoming users, and decrypts incoming traffic?

Reverse Proxy

If you have a high volume of web traffic, what device could you install to manage the traffic?

A Load Balancer

Why might your VLAN traffic not arrive?

The VLAN is not tagged

How can you prevent DNS poisoning and what records are created?

DNSSEC and it creates RRSIG records

What device joins multiple networks together?

A router

What is the boundary layer that sits between the LAN and WAN called?

DMZ or screened subnet. It is a boundary layer and could be used for network segmentation.

What device would you use to manage large volumes of DDoS traffic?

A firewall. It will prevent access.

If an attacker is gathering information from a company's website and their Facebook page, what type of reconnaissance is this?

This is known as passive reconnaissance as the attacker is only gathering information

What is more likely to cause damage to a system – an intrusive scan or a credentialed scan?

An intrusive scan can cause damage to the system whereas a credentialed scan can audit files and find missing patches, certificates, or account information.

What type of penetration test is carried out where no information is provided prior to arriving on their site, and just before starting the test, the IT Manager provides a network diagram?

This is known as Gray Box testing

What is the first stage in Black Box penetration testing?

The first stage of Black Box testing is to search for a weakness to carry out the initial exploitation of a system - most likely a vulnerability scan

An attacker accesses a network via a vulnerable host with missing patches, then moves laterally to attack the database server. What is this commonly known as?

Pivoting is a technique in which you will first attack a vulnerable host and from there attack a secondary critical host. In a virtual environment, it is called VM Escape.

Why would someone carrying out White Box penetration testing use a technique known as fuzzing? Who else would use fuzzing?

Both Black Box and White Box pen testers will use fuzzing, where random information is inserted into an application to see if it will crash or generate an error.

What type of scan is the least intrusive and what does it look for?

The least intrusive scan is a vulnerability scan which involves looking for missing updates or patches.

The company SIEM system has detected an attack on a file server but a manual inspection of the file server finds nothing. What is this called and what could have caused the fault within the SIEM system?

This is known as a false positive and could have happened because the SIEM system was using the wrong input filter, was not being properly tuned, or had scanned the wrong host.

What type of attack is it when an attacker finds the username of a person on their computer screen and then rings the help desk to reset the password?

Active reconnaissance is where someone actively tries to use information to gain access to your system. It could also be accessing the run command or going to the registry.

How can you prevent buffer overflow, integer overflow, and SQL injection attacks?

Input validation can prevent all three of these attacks as it controls input to an application or database. A stored procedure is another prevention method that will prevent a SQL injection attack. This should be the first choice for a database.

What type of pen tester will have access to source code?

White Box

Which threat actor is socially or politically motivated?

Hacktivist

Which threat actor wants your trade secrets?

Competitor - they will also try to interfere with your production system

Which threat actor would buy a program from the Dark Web?

Script Kiddie

Which threat actor is a Foreign Government?

State actor – they are sophisticated, well-organized and well-funded

Which threat actor never goes away?

Advanced Persistent Threat (APT). They are also sophisticated, well-organized and well-funded, and have been in business for a long time.

Which threat actor would threaten or blackmail you?

Organized Crime. They may threaten to publish damaging information about you on social media.

Which threat actor seeks fame and notoriety and would like to appear on the news?

Script Kiddie

Which threat actor is the hardest to detect?

Malicious Insider

Which does a Hacktivist do?

Attend political events - they are politically motivated

Which threat actor does not have a high skill level?

Script Kiddie

What is the machine that hosts 100 virtual machines called?

Host

What are containers in a virtualization environment?

Isolated guest virtual machine

What is VM Escape?

A hacker attacks the host or guest from a guest virtual machine

What is the purpose of a snapshot?

Gives you the ability to roll back a virtual machine to previous settings.

What word refers to isolating a guest, then adding an application for testing, patching, or quarantine?

Sandboxing. Linux: chroot jail.

What does a VM Host need? Name three things.

RAM, CPU cores, and a fast disk

What is a safe virtual environment for contractors called?

VDI

What would allow you to roll back to an old operating system or configuration?

Snapshot

What is the first stage when dealing with a potential virus attack?

Running a scan to confirm that there is a virus

Which virus self-propagates?

A worm

What type of attack changes its hash value as it replicates?

A polymorphic virus replicates and mutates as it moves from host to host, changing the hash.

What type of virus piggybacks on top of a program?

Fileless malware

What type of virus attack cannot be detected other than by using baselines?

Zero-day viruses cannot be detected using baselines

What type of virus attack uses a script that can run at a later date when a disgruntled employee has left an organization?

A logic bomb is a virus that can be triggered by an event, in this case a time and date. Logic bombs can use task schedulers, .bat, and .cmd files.

What type of virus attack uses pop-ups?

Adware uses pop-ups

What type of virus attack still exists even when you have completely reinstalled the operating system twice?

A rootkit virus sits underneath the operating system; therefore, it keeps coming back

What type of virus attack demands money? Name two of them.

Ransomware and crypto-malware both demand money

How can you investigate potentially dangerous malware?

Test it in a virtual machine sandbox or a cuckoo sandbox

What type of wireless authentication can be vulnerable to a brute force attack?

Wi-Fi Protected Setup (WPS) accesses the wireless network by pushing a button. On the setup phase, you need to insert a password and push the button to gain access.

What type of wireless attack is bluejacking?

Bluejacking is a type of attack in which an attacker sends unsolicited messages through a Bluetooth device.

You have rolled out 10 Wireless Access Points (WAP) across a company, but they cannot all connect to the wireless network. What should you have done before implementing the roll out?

A site survey should have been carried out prior to installing a wireless network as many factors can interfere with the communication

How can you circumvent a Captive Portal at an airport?

You could spoof a MAC address to bypass a Captive Portal

What is a wireless payment type commonly used on mobile telephones?

Near Field Communication (NFC) is a wireless payment type that is commonly used

What do you need to install on a wireless device that is going to use EAP-TLS for authentication?

EAP-TLS requires a valid certificate to be installed on the endpoint

What is the most secure wireless encryption standard and what encryption protocol does it use? Address both WPA2 and WPA3.

WPA2 - CCMP (128 bit AES). WPA3 -GCMP (256 bit AES).

How can you prevent someone from deploying a Rogue Access Point onto your network?

By using a 802.1x managed switch where each device in authenticated prior to joining your network

If you renewed your CAC card a month ago, how can you recover the old data?

You would need to obtain the old private certificate from the key escrow.

How can a hotel roll out their wireless network so that the guests connecting to it do not have to use a password to connect? They are not bothered about security.

The hotel should use Open System Authentication as this option requires no authentication. However, it is prone to attacks as anyone can access the network.

What WPA3 wireless prevents IV attacks?

Protected Management Frames (PMF)

What is CURL?

Command Line tool for Banner Grabbing and Transferring Data

What is the function of theHARVESTER?

It collects email addresses

What is the function of Sn1per?

Used by pen testers and bug bounty hunters. It can be used to search for vulnerabilities and open ports and it has DNS and nmap capabilities.

What type of tool is Scanless?

Anonymous Port Scanner

What is the function of DNSenum?

It fetches company DNS information (A Records, MX Records, NS Records). From this you can tell the company size.

What type of tool is Nessus?

Remote scanning tool that can identify vulnerabilities that hackers can exploit

What is the function of Cuckoo?

It creates a sandbox for analyzing malware.

What is a Replay Attack?

On-Path attack where the data is replayed at a later date

What is an On-Path attack?

It is an interception attack; examples include Man-in-the-Middle or Replay attacks

How can a Replay Attack be prevented?

With Kerberos authentication, which uses USN and time stamps

What is a Smurf Attack?

It is an amplification attack in which directed IP Broadcasts are sent to a border router, and the victim receives the ICMP replies.

What type of attack is it if you see the command strcpy?

Buffer Overflow; you are copying strings of data

What type of attack is it if you see the phrase 1=1?

SQL Injection

What type of attack is an apostrophe in a data field?

SQL Injection

What is a Man-in-the-Middle attack?

An On-Path attack where the data is replayed immediately

What type of attack is an integer overflow?

An attack in which a number larger than the expected was input into a numerical cell.

What is input validation and what attack type does it prevent?

Accepting data in a particular format. It prevents Buffer Overflow, Integer Overflow and SQL Injection attacks

What type of attacks use HTML tags and JavaScript?

Cross Site Scripting (XSS)

How can I tell if a script is JavaScript?

Uses the word ‘var’ or has a .js file extension

What is a stored procedure and what type of attack does it prevent?

Writing a SQL statement into a sealed script; this prevents a SQL Injection attack

What type of attack is it if you let a fake fireman into the server room?

Social Engineering Urgency. You are led to believe that if you don’t let him in then the building could burn down.

What type of attack is it if the board members are sent an email asking for their bank details?

Spear Phishing (sent to a group of users)

What type of attack is it if you get a false email from HR telling you to fill in a form?

Social Engineering Authority. It could appear to come from the CEO or HR department.

What type of attack redirects you from a legitimate website to a fraudulent website?

Pharming or DNS Poisoning

What type of attack is a Man in the Browser (MITB)

On-Path

If you steal someone else's cookie, what type of attack is this?

Session replay, sometimes know as session hijacking

Why would you use a honeypot?

To see how an attacker is carrying out an attack so that you can mitigate it

Why would you shred or burn your personal documents? What type of attack are you preventing?

To prevent identity theft or fraud. You are preventing dumpster diving.

What type of attack would use a trusted website as its attack vector?

Watering Hole attack

What type of web-based attack could result in a financial transaction being made when you click on an icon?

Cross Site Request Forgery (CSRF)

What type of attack would find vulnerabilities on a computer and tell you to upgrade to a full product to remove them?

A subtle form of ransomware in which you are parting with your money

Which part of the PKI environment issues certificates to users?

Intermediary, sometimes known as the subordinate

Who processes certificate requests before they go to the CA?

Registrar

Where is the certificate serial number located?

OID. On the X509 itself.

Who holds the private keys for third parties?

Key Escrow

Where does the key escrow store private keys?

In the Hardware Security Module

What do you need to do to renew a certificate?

Create a CSR Certificate Signing Request

What is the CSR process?

It is a New Certificate Request. Generate 2 Keys. Send the Public Key to the CA. Get back a file (X509).

What tells you if your certificate is valid?

CRL - this is the default, even if you have no internet

Under what circumstances would you never use the CRL for certificate validity?

When the CRL is slow, or you need a fastest method of certificate validity. You will then choose the OCSP