|  |  |  |
| --- | --- | --- |
| Qualification Code: | ICT60515 | |
| Qualification Title: | Advanced Diploma of Computer Systems Technology | |
| Unit Code/s: | ICTNWK509 | |
| Unit Title/s: | Design and implement a security perimeter for ICT networks | |
| Student Id | Cal14385330 | |
| Student Name | Benjamen Calleja | **Signature** |
| Assessment Due Date: |  | |
| Assessment Name: | Assessment Item 2 Test | |
| Teacher’s name: | Murad Quazi | |
| Teacher’s email: | mquazi@kangan.edu.au | |

|  |
| --- |
| 1. Task Instructions |

This test is close book and it requires students to work by themselves and address all requirements as per Assessment item Description. Students are required to accomplish their task professionally and in time.

|  |
| --- |
| 1. Submission instructions |

All items submitted must be clearly marked with the following details:

• Your full name

• Your student number

• Your class group

• The date

This cover sheet must accompany all items submitted.

Student’s Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Marking Criteria

|  |  |
| --- | --- |
| **Grade** |  |
| NP | * Assessment aims have not been met |
| CA | * All requirements mentioned in assessment item description are correctly addressed. * Students answered at-least 8 questions correctly. * Comparison is done wherever required * OHS Risks are identified and documented * OHS Risk control measure are taken if required * Contents are comprehensive, accurate and professionally presented |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Comments: |  | | | |
| Teachers Signature: | |  | Date: |  |

# Assessment Item Description

**Students are required to answer 10 questions, allocated time for this assessment item is 90 mins.**

This test requires students to work by themselves and accomplish their task professionally and in time. This assessment item is closed book and student need to finish their assessment in front of teacher.

**All students are required to submit their test in written document. They can choose any 10 questions out of following questions**

1. Students are required to Identify, list and discuss threats to enterprise security and what sort of security measures we must take to protect our enterprise.  
   **Phishing. Phishing emails are a common way hackers gain access/information to your enterprise systems or trick business leaders into wiring money  
     
   CEO spoofing. IS similar concept to phishing, but with a twist it tricks users via an email, instead of a link. It can occur like this: Using social media, a cybercriminal can see when a CEO is at a conference. Then he or she can send an email that appears to be from the CEO to the CFO saying to transfer money.  
     
   Insider threats. These are a major cybersecurity concern for enterprises that are often overlooked. One way to protect against this is to revoke employee credentials when someone leaves the company.  
     
   Internet of things vulnerabilities. Without a strong website security, hackers can often gain access to utilities such as water towers and wind turbines. Often times web cameras are often found in stores and companies unsecured and criminals can easily gain access and move the cameras around**
2. Describe the differences between local and centralized authentication.  
   **Local authentication uses face identification, or fingerprint API to authenticate the user with a face or fingerprint scan.**  
     
     
   **Centralized Authentication.  
   With centralized authentication the authentication process is different. Typically, typically centralization authentication solutions completely offload user management from an application. They provide powerful APIs or query languages to connect the user system to one or many applications.**
3. What are the general steps a firewall uses to authenticate users?  
   **A firewall user is a network user who must provide a username and password for authentication when initiating a connection across the firewall. After you define firewall users, you can create a policy that requires the users to authenticate themselves through one of the**
4. What is a disadvantage of centralized authentication?  
   **A disadvantage of a centralized authentication is it is a single point of failure. SPOFs are undesirable in any system with a goal of high availability or reliability, be it a business practice, software application, or other industrial system.**
5. Compare TACACS+ and RADIUS with regard to strength of security  
   **Terminal access controller access control system is a protocol set created and intended for controlling access to Unix terminals TACACS+ is mainly used for Device Administration AAA, it is possible to use it for some types of network access AAA.  
     
   Remote Access Dial-in User Service is an IETF standard for AAA RADIUS is most likely being used between the wireless device and the AAA server**
6. What are some of the advanced security functions provided by modern firewalls?

**Some of the advance functions with modern day firewalls are.  
Multi-functional traditional firewalls provide basic packet filtering, network and port address translations, state-full inspections and can even support virtual private networks, however they are only limited to the data link later and transport layer.  
  
Application awareness. Traditional firewalls typically block common application ports or service on a network to control application access and monitor specific threats. However, with network connectivity becoming more complex. or service on a network to control application access and monitor specific threats. However with network connectivity becoming more complex.  
  
Streamlines infrastructure. Traditional firewalls require a separate security appliance for every new threat, which leads to additional cost and efforts for maintaining and updating each of those devices.  
  
Threat protection. Unlike traditional firewalls, NGFWs include antivirus and malware protection that’s continuously upgrade automatically whenever new threats are discovered. The NGFW device also minimizes the avenues of attack  
  
Network speed. Though many vendors of traditional firewalls claim to offer a specific throughput 9 usually a gigabyte) from every port.**

1. Describe stateless packet-filtering firewalls.  
   **A stateless firewall watch network traffic and restrict/block packets based on source and destination address or other static values. A stateless firewall used simple rule sets that do not account for the possibility that a packet might be received by the firewall.**
2. What is a MAC layer firewall?  
   **A MAC layer firewall is designed to operate at the media access control layer (Layer 2). It is also able to consider specific host’s computer’s identity for its filtering decisions. The mac address of a specific hosts computer is linked to a ACL that identifies specific types of packets that can be sent to each host.**
3. Describe each generation of firewalls.  
   **Packet filtering firewalls  
   This is the original type of firewall, it operates inline junction points where’re a device such as a router or a switch do their work. However this firewall doesn’t route packets but instead compares each packet received to a set of established IP address.  
     
   Circuit level gateways  
   Using another relatively quick way to identify malicious content, these devices monitor The TCP handshakes across the network as they are established between the local and remote hosts to determine whether the session being initiated is legitimated.  
     
   Stateful inspection firewalls  
   State aware devices not only examine each packet but also keep track of whether or not that packet is part of an established TCP session, this offers more security that either packet filtering or circuit monitoring alone.  
     
   Application level gateways.  
   This kind of device, technically a proxy, and sometimes referred to as proxy firewall, combines some of the attributes of packet filtering firewalls with those of circuit-level gateways. They filter packets not only according to the service of which they are intended.  
     
   Next Generation Firewalls.  
   A next gen firewall is a deep packet inspection firewall that moves beyond port protocol inspection and blocking to add application level inspection. The benefits of next gen firewalls are that they are able to block malware from entering a network, something that traditional firewalls would never be able to achieve. They are also better equipped to address advanced persistent threats.**
4. Describe the differences between software and hardware firewalls.  
   **A hardware firewall is a unit that is connected between the network and the device for connecting the internet. A software firewall is a program that is installed on the computer with the help of an internet connection.**What is IP forwarding? **Ip routing is a process used to determine which path a packet can be sent. The process uses routing information to make decisions and is designed to send a packet over multiple networks.**
5. What are VPN endpoints?  
   **VPN endpoints are where the vpn terminate, Instead of your vpn client passing through a router and terminating on your pc, the connection goes from vpn endpoint to vpn endpoint device. This will allow you to tunnel between 2 separate networks that are behind the router.**
6. Describe the drawbacks of VPNs.  
   **Some drawbacks of using VPNS are**

**>Using a VPN might be illegal in your country**

**Some countries that don’t allow their citizens to use any type of vpn service for example its is banned in Belarus IRAQ North Korea Turkmenistan  
  
>It Might Be Difficult To Set Up For Business Users**

**For individual users, VPN might be easy to set up since you just need to download your VPN apps or software and install it on your device. However, for business users, the case might not be like that. For business users, VPN is much more complicated to set up, especially if you need to set up the private network on your business premise. It will add more complexity to your overall network connection, and it will affect each device that you use on your business. While many VPN companies can simplify that for you, you might still need a dedicated network management team to oversee the private connection network on your business.  
  
> It Might Add More Cost To Your Network Connection  
By default, the virtual private network is a premium private connection service that you need to pay separately from your regular network connection or ISP. Also, if you want to use a VPN router, you have to purchase additional router hardware to be able to be used alongside your VPN connection. Thus, it might not come to you free of charge. Sure, there are many free private connections that you can use, but they are generally not reliable and they have lots of limitations. So, another disadvantage of private connection is that it can be very costly for you in the long term.**