ICTNWK511 Manage Network Security

Marking Guide

ICTNWK511 Manage Network Security			Created	9/5/2016
Marking Guide				
© Prime Learning Pty Ltd	Version #:	1	Last Modified Date:	9/5/2016

ASSESSMENT SUMMARY	
Assessment 1	Define a process for designing security
Assessment 2	Identify threats to network security
Assessment 3	Analyse security risks

Assessment 4	Create a security design
Assessment 5	Design and implement responses to security incidents
Assessment 6	Knowledge Questions

Assessor Instructions:

When adhering to the Principles of Assessment, the RTO should ensure that the principle of "Fairness" is applied appropriately. This requires the assessor to take into account any special needs a candidate with a documented disability may have.

If a candidate has identified and supplied evidence of a disability of any kind, the Assessor should take this into account and consider applying Reasonable Adjustment to assessment items, where required.

What is Reasonable Adjustment?

Definition

'Reasonable adjustment', as defined through the Disability Discrimination Act 1992, relates to a measure or action taken by an education provider to assist a learner with a disability (Disability Standards for Education, 2005).

When can Reasonable Adjustment be applied?

An Assessor should consider the learner's needs in the assessment process and make reasonable adjustments to accommodate the learner (*such as providing oral rather than written assessment*). However, don't compromise the rigour of the assessment process (*e.g. if there is a requirement to complete documentation in a unit of competency, oral assessment will not be appropriate*). "***Users' Guide to the Standards for Registered Training Organisations (RTOs) 2015"***

Why make a reasonable adjustment?

We make reasonable adjustments in VET to make sure that learners with a disability have:

- the same learning opportunities as learners without a disability
- the same opportunity to perform and complete assessments as those without a disability.

Reasonable adjustment applied to participation in teaching, learning and assessment activities can include:

- customising resources and activities within the training package or accredited course
- modifying the presentation medium
- learner support
- use of assistive / adaptive technologies
- making information accessible both prior to enrolment and during the course
- monitoring the adjustments to ensure learner needs continue to be met.

"Reasonable Adjustment in teaching, learning and assessment for learners with a disability A Guide for VET Practitioners November 2010"

Process for applying reasonable adjust assessment

1. Download the Content Assessment Tracker (C.A.T) from SMART to see how each assessment task is mapped and ensure that all mapped assessment components will be sufficiently addressed through the alternative assessment. To determine this, you must ensure that ALL critical aspects of evidence, range statements, skills and knowledge requirements (performance evidence/knowledge requirements) being assessed through the task are sufficiently assessed.
2. Review the alternative assessment and compare as above in accordance with "Rules of Evidence" requirements. Please refer to the NVR Standards for Registered Training Organisations. You must approve of any changes to the original assessment and give guidance to the student. Again, the onus is on you to ensure the assessment meets the unit requirements.
3. If you are unsure, please contact compliance who will audit the alternative assessment against rules of evidence to ensure sufficiency, validity, reliability and currency of the evidence.
4. Any adjustments from the original assessment, set out in the Student Assessment Guide MUST be documented under "Reasonable adjustment" in the Trainer Assessment Pack and also documented in the student notes in SMART so that anyone reviewing the student's work can clearly track changes made to the assessment.

Extract from Trainer Assessment Pack

REASONABLE ADJUSTMENT required to assessment (If 'yes' record details)
☐Yes
☐No

You may also find it necessary to clarify a student's assessment response/reply if you judge the initial response to be insufficient, incorrect or incomplete by asking additional questions.

In the Trainer Assessment Pack, you are to include a short note explaining how you clarified the assessment response and detail the students reply. This is important as it supports how you were able to determine the assessment judgement applied to the task or question.

Assessment Details

Evocca College is committed to assessment that incorporates a feedback process and is based on the criteria outlined in the Standards for Registered Training Organisations 2015 Standard 1 (Clauses 1.8-1.12), Conduct effective assessment:

- **Fair —** fairness requires that the assessor fully informs the student about the assessment process and includes an opportunity for the student being assessed to challenge the result of the assessment and to be reassessed if necessary.
- **Flexible** — the assessment should reflect the student's needs; provide for recognition of competencies no matter how, where or when they have been acquired, and draw on a range of assessment methods appropriate to the context, competency and the individual.
- **Reliable** — refers to the degree to which evidence presented for assessment is consistently interpreted, resulting in consistent assessment outcomes.
- **Valid** — ensuring that the assessment process is sound. Validity requires that assessment must cover the broad range of skills and knowledge that are essential to competent performance.

The provision of a comprehensive assessment tool will ensure that the following rules of evidence are met and that each student's assessment is:

- **Authentic** - assessor must be assured that the evidence presented for assessment is the student's own work.
- **Valid** - The assessor is assured that the learner has the skills, knowledge and attributes as described in the module or the unit of competency and associated assessment requirements
- **Current** - The assessor is assured that the assessment evidence demonstrates current competency. This requires the assessment evidence to be from the present or the very recent past.
- **Sufficient** - The assessor is assured that the quality, quantity and relevance of the assessment evidence enables a judgement to be made of a learner's competency.

For the learner to be assessed as competent you must ensure the learner demonstrates their:

- Ability to perform relevant tasks in a variety of workplace situations, or accurately simulated workplace situations.
- Understanding of what they are doing, and why, when performing tasks.
- Ability to integrate performance with understanding, to show they are able to adapt to different contexts and environments.

The learner must:

- Be assessed against all of the tasks identified in the elements of the unit or module.
- Demonstrate they are capable of performing these tasks to an acceptable level.

Remember to assess the Foundation Skills embedded in these tasks.

Please be aware that students are asked for their feedback on all assessment tools, as part of Evocca's continuous improvement. They are asked to email their feedback to *resource.development@evocca.edu.au*

Assessment 1 Define a process for designing security

Assessor Instructions

This assessment has been designed to allow students to demonstrate their ability to determine project requirements.

Students are required to read and respond to the scenario below. Any incorrect or incomplete responses must be returned to the student with feedback to allow them to resubmit. If the student requires additional training or guidance on the topic, you will need to negotiate time to assist them.

You must assess the student on their ability to:

1. Define planning phase for network security design
2. Define building phase for network security design
3. Define managing phase for network security design

You are also required to assess the employability skills embedded in this task including:

Writing	Uses factual information and industry related terminology to develop organisational plans, security policies and document security breaches
Oral Comm.	Uses active listening, observational and questioning techniques in order to identify different perspectives and confirm and clarify understanding
Numeracy	Calculates equipment costs in order to assess their business related value
Get the Work Done	Demonstrates a sophisticated understanding of principles, concepts, language and practices associated with the digital world and uses these to troubleshoot and reduce risks Uses digital tools to access and organise complex data and analyse multiple sources of information for strategic purposes Is acutely aware of the importance of understanding, monitoring and controlling access to digitally stored and transmitted information Uses a combination of formal and logical planning processes and an increasingly intuitive understanding of context to plan control methods for managing system security Makes a range of critical decisions in relatively complex situations, taking a range of constraints into account Recognises and addresses complex problems, including systems processes and rapid deployment of solutions to problems involving failure and security incidents

Record all assessment judgements in the Tutor Assessment Pack.

Benchmark answers are provided below each question in red.

Task 1: Define planning phase for network security design

Explain and describe the significance of the planning phase when dealing with network security.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:
The student will answer something similar to the following: Planning of any sort is critical for any project to be considered successful, in regards to network security even more so. The planning phase refers to the ability to estimate where there are potential breaches in an existing network or where they might exist in a brand new network. The more effort that is put into planning, the higher the chance that the network will be secure. Though, as with anything technological, the system of protection needs to be maintained and updated on a regular basis. Planning should cover the following main areas: - Encryption policy - Password policy - Email and communications - Identity - Anti-virus - Acceptable use policy - Remote access Learning Guide: 1.1 Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.
Tutor Use Only **Successful ☐ Unsuccessful ☐ Date:** Click here to enter a date. **Tutor Feedback:** Click here to enter text.

Task 2: Define building phase for network security design

Describe the building phase of network security, ensure that your description covers both physical and logical dimensions of a network. Provide examples of logical and physical security elements that could be implemented in a network.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:
The student will supply something similar to the following: The building phase can also be referred to as the implementation phase, the specific section of the timeline where the planned out security elements are put into operation. The implementation of the building phase can be broken down into two main sections: - Physical - Logical Physical security of network is based upon the ability to actually access the physical components of a network. This includes, but is not limited to, the server room, patch panels, switches, routers, desktop machines and any mobile device that might be attached to the network. It covers wired and wireless device access. An example of physical security, is a locked door scenario to a server room, the room requires key-card access and even then, each implemented device in the network is locked inside server racks which require key access. Logical security of a network is the implementation of software solutions to prevent damage to the information that is stored within a network. This is where aspects such as group policy objects, anti-virus, intrusion detection systems and firewalls come into play. Learning Guide: 1.2 Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.
Tutor Use Only **Successful** ☐ **Unsuccessful** ☐ **Date:** Click here to enter a date. **Tutor Feedback:** Click here to enter text.

Task 3: Define managing phase for network security design

Describe the managing phase, and explain the significance of this phase in any implemented project.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:
The student will answer something similar to: The managing phase is implemented after the building phase, this particular phase of a project is when monitoring and upgrading of the original design is implemented. Monitoring is when the areas in which the security is implemented, be it logical or physical, are constantly reviewed to determine if there have been attacks made to the system, if the current system handles the attacks and examination of areas that need improving based upon the data collected from any network attacks. If the attack was physical, then a stronger physical security could be implemented, such as surveillance cameras, stronger locks and bio-metric passwords to name a few items. Logical attacks will leave details in log files, which will allow the areas which need securing to be focused on and improved. This could be aspects of closing of ports using a firewall, implementation of Intrusion detection systems and so forth. The management phase is critical in any implemented project as this is where the strength of the security plan is monitored and its value determined. Learning Guide: 1.3 Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.
Tutor Use Only **Successful** ☐ **Unsuccessful** ☐ **Date:** Click here to enter a date. **Tutor Feedback:** Click here to enter text.

Assessment 2 Identify threats to network security

Assessor Instructions

This assessment has been designed to allow students to demonstrate their ability to determine project requirements.

Students are required to read and respond to the scenario below. Any incorrect or incomplete responses must be returned to the student with feedback to allow them to resubmit. If the student requires additional training or guidance on the topic, you will need to negotiate time to assist them.

You must assess the student on their ability to:

1. Determine why attacks occur
2. Determine who the attack may come from
3. Analyse common types of network vulnerabilities
4. Determine how attacks occur
5. Design a threat model to categorise treats

You are also required to assess the employability skills embedded in this task including:

Writing	Uses factual information and industry related terminology to develop organisational plans, security policies and document security breaches
Oral Comm.	Uses active listening, observational and questioning techniques in order to identify different perspectives and confirm and clarify understanding
Numeracy	Calculates equipment costs in order to assess their business related value
Get the Work Done	Demonstrates a sophisticated understanding of principles, concepts, language and practices associated with the digital world and uses these to troubleshoot and reduce risks Uses digital tools to access and organise complex data and analyse multiple sources of information for strategic purposes Is acutely aware of the importance of understanding, monitoring and controlling access to digitally stored and transmitted information Uses a combination of formal and logical planning processes and an increasingly intuitive understanding of context to plan control methods for managing system security Makes a range of critical decisions in relatively complex situations, taking a range of constraints into account Recognises and addresses complex problems, including systems processes and rapid deployment of solutions to problems involving failure and security incidents

Record all assessment judgements in the Tutor Assessment Pack.

Benchmark answers are provided below each question in red.

Task 1: Determine why attacks occur

Describe and supply an example of an environment where an attack would occur. In addition, describe why your example environment would be attacked and include the attacker's motivation.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:
The student will answer something similar to the following: Network attacks occur due to a multitude of different reasons, below is a list of malicious activities: - Theft of hardware and software - Ability to corrupt data and services - Modification of data - Stealing data, this data could be for financial gain or industrial espionage - Utilising resources, such as creating zombie bots The attacks can occur potentially due to the following reasons: - Political motivation - Industrial Espionage - Criminal activities - Seeking of Fame - Greed - Terrorism - Racism The student example is subjective to the student, but it should be a combination of the above lists, for example: The attacker's motivation is greed and as such, they are attacking corporation X to steal specific data. Learning Guide: 2.1 Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.
Tutor Use Only **Successful** ☐ **Unsuccessful** ☐ **Date:** Click here to enter a date. **Tutor Feedback:** Click here to enter text.

Task 2: Determine who the attack may come from

You've been hired by a local company that has multiple systems, they believe that the Debian1 server has had information maliciously modified. They have asked you to locate where the breach to the network came from. Examine the following diagram (Figure 1 Network Map), hexdump and auth.log images to determine the path that the attacker took to manipulate information on debiansrv1.

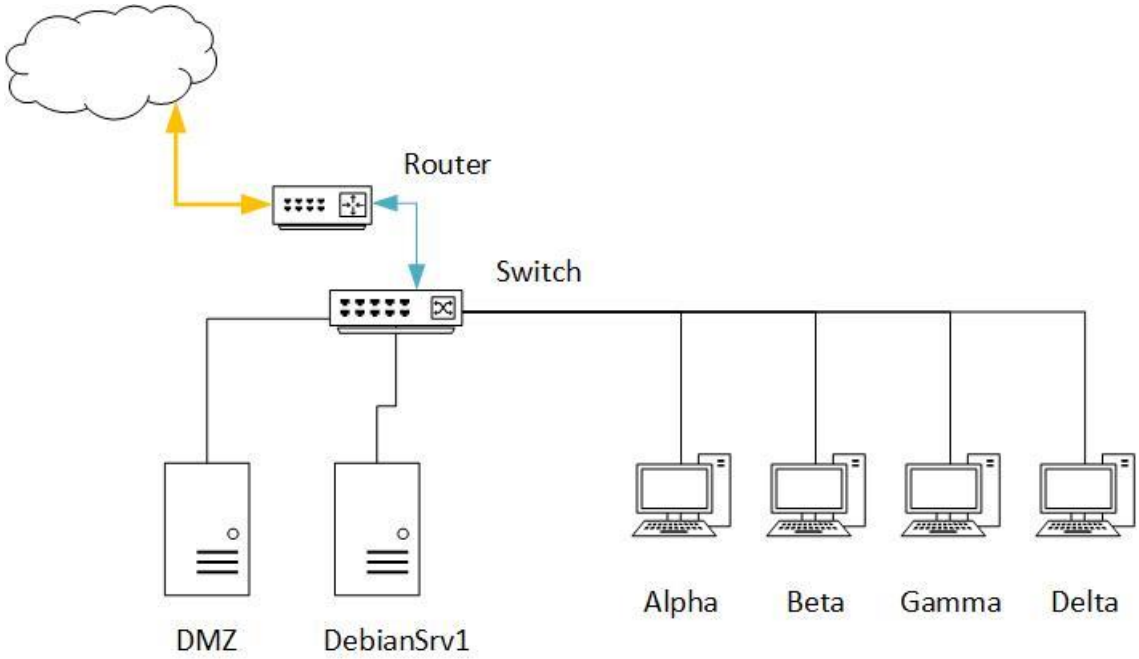


Figure 1 Network Map

```
May 12 11:23:37 Gamma su[1176]: pam_unix(su:session): session opened for user root by gamma(uid=1001)
May 12 11:24:10 Gamma sshd[1179]: Accepted password for gamma from 192.168.0.106 port 40935 ssh2
May 12 11:24:10 Gamma sshd[1179]: pam_unix(sshd:session): session opened for user gamma by (uid=0)
May 12 11:24:10 Gamma systemd-logind[475]: New session 2 of user gamma.
May 12 11:25:06 Gamma su[1194]: Successful su for root by gamma
May 12 11:25:06 Gamma su[1194]: + /dev/pts/2 gamma:root
May 12 11:25:06 Gamma su[1194]: pam_unix(su:session): session opened for user root by gamma(uid=1001)
May 12 11:36:34 Gamma su[1176]: pam_unix(su:session): session closed for user root
May 12 11:39:14 Gamma su[1312]: Successful su for root by gamma
May 12 11:39:14 Gamma su[1312]: + /dev/pts/1 gamma:root
May 12 11:39:14 Gamma su[1312]: pam_unix(su:session): session opened for user root by gamma(uid=1001)
May 12 11:43:03 Gamma sshd[1181]: Received disconnect from 192.168.0.106: 11: disconnected by user
May 12 11:43:03 Gamma sshd[1179]: pam_unix(sshd:session): session closed for user gamma
May 12 11:43:03 Gamma su[1194]: pam_unix(su:session): session closed for user root
May 12 11:53:54 Gamma sshd[1355]: Accepted password for gamma from 192.168.0.106 port 44608 ssh2
May 12 11:53:54 Gamma sshd[1355]: pam_unix(sshd:session): session opened for user gamma by (uid=0)
May 12 11:53:54 Gamma systemd-logind[475]: New session 3 of user gamma.
root@Gamma:/home/gamma#
```

Figure 2 Gamma Auth.log

```
May 12 11:43:03 dmz polkitd(authority=local): Unregistered Authentication Agent for unix-session:1 (system bus
ticationAgent, locale en_AU.UTF-8)
May 12 11:43:03 dmz kdm: :0[751]: pam_unix(kdm:session): session closed for user web
May 12 11:43:04 dmz sshd[473]: Received signal 15; terminating.
May 12 11:43:45 dmz sshd[472]: Server listening on 0.0.0.0 port 22.
May 12 11:43:45 dmz sshd[472]: Server listening on :: port 22.
May 12 11:43:45 dmz systemd-logind[474]: New seat seat0.
May 12 11:43:45 dmz systemd-logind[474]: Watching system buttons on /dev/input/event2 (Power Button)
May 12 11:43:45 dmz systemd-logind[474]: Watching system buttons on /dev/input/event3 (AT Translated Set 2 keyb
May 12 11:49:30 dmz kdm: :0[752]: pam_unix(kdm:session): session opened for user web by (uid=0)
May 12 11:49:30 dmz systemd-logind[474]: New session 1 of user web.
May 12 11:49:30 dmz systemd: pam_unix(systemd-user:session): session opened for user web by (uid=0)
May 12 11:49:53 dmz polkitd(authority=local): Registered Authentication Agent for unix-session:1 (system bus na
ication-agent-1], object path /org/kde/PolicyKit1/AuthenticationAgent, locale en_AU.UTF-8)
May 12 11:50:01 dmz su[1053]: Successful su for root by web
May 12 11:50:01 dmz su[1053]: + /dev/pts/0 web:root
May 12 11:50:01 dmz su[1053]: pam_unix(su:session): session opened for user root by web(uid=1000)
May 12 11:54:17 dmz sshd[1059]: Invalid user hank from 192.168.0.107
May 12 11:54:17 dmz sshd[1059]: input_userauth_request: invalid user hank [preauth]
May 12 11:54:20 dmz sshd[1059]: pam_unix(sshd:auth): check pass; user unknown
May 12 11:54:20 dmz sshd[1059]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruse
May 12 11:54:22 dmz sshd[1059]: Failed password for invalid user hank from 192.168.0.107 port 56433 ssh2
May 12 11:54:30 dmz sshd[1059]: pam_unix(sshd:auth): check pass; user unknown
May 12 11:54:32 dmz sshd[1059]: Failed password for invalid user hank from 192.168.0.107 port 56433 ssh2
May 12 11:54:59 dmz sshd[1059]: Failed password for invalid user hank from 192.168.0.107 port 56433 ssh2
May 12 11:54:59 dmz sshd[1059]: Connection closed by 192.168.0.107 [preauth]
May 12 11:54:59 dmz sshd[1059]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=1
root@dmz:/home/web#
```

Figure 3 DMZ Auth.log

```
May 12 11:51:04 debiansrv1 su[971]: Successful su for root by scott
May 12 11:51:04 debiansrv1 su[971]: + /dev/pts/0 scott:root
May 12 11:51:04 debiansrv1 su[971]: pam_unix(su:session): session opened for user root by scott(uid=1000)
May 12 11:52:06 debiansrv1 su[971]: pam_unix(su:session): session closed for user root
May 12 11:52:06 debiansrv1 polkitd(authority=local): Unregistered Authentication Agent for unix-session:1 (syste
h /org/kde/PolicyKit1/AuthenticationAgent, locale en_AU.UTF-8)
May 12 11:52:06 debiansrv1 kdm: :0[686]: pam_unix(kdm:session): session closed for user scott
May 12 11:52:07 debiansrv1 sshd[390]: Received signal 15; terminating.
May 12 11:52:37 debiansrv1 sshd[474]: Server listening on 0.0.0.0 port 22.
May 12 11:52:37 debiansrv1 sshd[474]: Server listening on :: port 22.
May 12 11:52:37 debiansrv1 systemd-logind[477]: New seat seat0.
May 12 11:52:37 debiansrv1 systemd-logind[477]: Watching system buttons on /dev/input/event2 (Power Button)
May 12 11:52:37 debiansrv1 systemd-logind[477]: Watching system buttons on /dev/input/event3 (AT Translated Set
May 12 11:52:48 debiansrv1 kdm: :0[755]: pam_unix(kdm:session): session opened for user scott by (uid=0)
May 12 11:52:48 debiansrv1 systemd-logind[477]: New session 1 of user scott.
May 12 11:52:48 debiansrv1 systemd: pam_unix(systemd-user:session): session opened for user scott by (uid=0)
May 12 11:53:01 debiansrv1 polkitd(authority=local): Registered Authentication Agent for unix-session:1 (system
4/libexec/polkit-kde-authentication-agent-1], object path /org/kde/PolicyKit1/AuthenticationAgent, locale en_AU
May 12 11:53:07 debiansrv1 su[1042]: Successful su for root by scott
May 12 11:53:07 debiansrv1 su[1042]: + /dev/pts/0 scott:root
May 12 11:53:07 debiansrv1 su[1042]: pam_unix(su:session): session opened for user root by scott(uid=1000)
May 12 11:55:20 debiansrv1 sshd[1057]: Accepted password for hank from 192.168.0.107 port 55260 ssh2
May 12 11:55:20 debiansrv1 sshd[1057]: pam_unix(sshd:session): session opened for user hank by (uid=0)
May 12 11:55:20 debiansrv1 systemd-logind[477]: New session 2 of user hank.
May 12 11:55:20 debiansrv1 systemd: pam_unix(systemd-user:session): session opened for user hank by (uid=0)
root@debiansrv1:/#
```

Figure 4 Debiansrv1 Auth.log

hexdump.txt

```
05/11-16:42:59.473423 223.28.32.189:1045 -> 192.168.0.106:53
UDP TTL:40 TOS:0x0 ID:18856
Len: 52
95 6A 01 00 00 01 00 00 00 00 00 00 03 31 30 37  .j...........107
02 37 31 02 38 30 03 32 31 36 07 69 6E 2D 61 64  .71.80.216.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

05/11-16:42:59.474405 192.168.0.106:1028 -> 128.8.10.90:53
UDP TTL:64 TOS:0x0 ID:18861
Len: 52
5C 21 01 00 00 01 00 00 00 00 00 00 03 31 30 37  \!...........107
02 37 31 02 38 30 03 32 31 36 07 69 6E 2D 61 64  .71.80.216.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

05/11-16:42:59.574808 128.8.10.90:53 -> 192.168.0.106:1028
UDP TTL:48 TOS:0x0 ID:5077
Len: 135
5C 21 81 00 00 01 00 00 00 02 00 00 03 31 30 37  \!...........107
02 37 31 02 38 30 03 32 31 36 07 69 6E 2D 61 64  .71.80.216.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01 02 37 31 02  dr.arpa......71.
38 30 03 32 31 36 07 49 4E 2D 41 44 44 52 04 61  80.216.IN-ADDR.a
72 70 61 00 00 02 00 01 00 07 E9 00 00 12 03 4E  rpa............N
53 30 08 45 4E 54 45 52 41 43 54 03 43 4F 4D 00  S0.ENTERACT.COM.
C0 2C 00 02 00 01 00 07 E9 00 00 13 07 42 49 46  .,...........BIF
52 4F 53 54 08 53 45 41 53 54 52 4F 4D C0 5B     ROST.SEASTROM.[

05/11-16:42:59.576169 192.168.0.106:1028 -> 198.32.64.12:53
UDP TTL:64 TOS:0x0 ID:18862
Len: 46
87 2A 00 00 00 01 00 00 00 00 00 00 07 42 49 46  .*...........BIF
52 4F 53 54 08 53 45 41 53 54 52 4F 4D 03 43 4F  ROST.SEASTROM.CO
4D 00 00 01 00 01                                M.....
```

Figure 5 Hexdump

Describe the method of entry and path that was used by the attacker, justify every choice and demonstrate the timeline. In addition, modify the network map to show the method of attack.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:
The student will examine the hexdump and locate the originating IP address of the attack. The attack entered via the DMZ through the DNS port the day before, this is determined by the date stamp on the hex dump. 05/11-16 (May 11th) The attack originated from IP: 223.28.32.189 On the May 12th; the attacker entered through the DMZ DMZ: 192.168.0.106 They then tested the hank account on the client Gamma, which failed. This is seen in the DMZ auth.log image

They successfully accessed the client Gamma, using the gamma user account and went to super user.

Gamma: 192.168.0.107

This is seen in the gamma auth.log file

Examining the debianSrv1 auth.log file

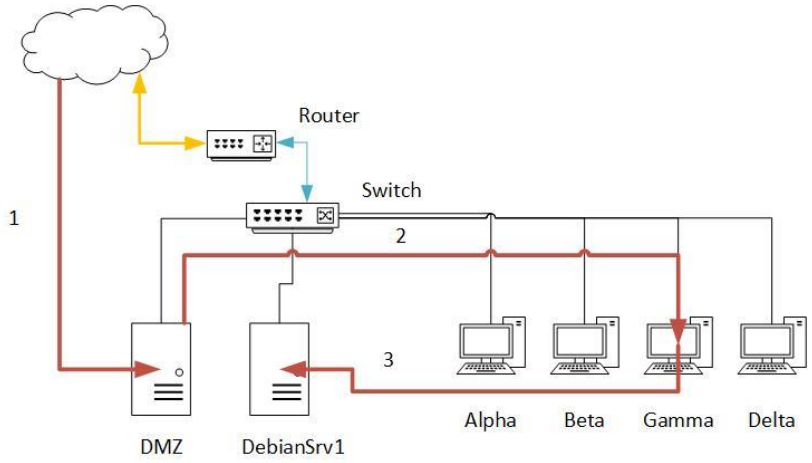
Debiansrv1: 192.168.0.103

The user hank has successfully made a connection and then been promoted to superuser.

The method for discovering this attack will start and run in the following order:

- Examine Debiansrv1 auth.log file and note the connections and actions.
- Grab the auth.log file from the Gamma client, as it was used to connect to the debiansrv1
- Examine the gamma auth.log file, note connections and actions
- Grab the auth.log file from the DMZ as it was used to connect to Gamma
- Examination of the Hexdump, shows in the first line the external IP of the attacker who linked to the DMZ.

The student should also supply a modified network map to look like:



1. Connection from External to DMZ
2. Connection from DMZ to Gamma
3. Connection from Gamma to DebianSrv1

Learning Guide: 2.2

Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.

Tutor Use Only

Successful ☐ **Unsuccessful** ☐ **Date:** Click here to enter a date.

Tutor Feedback:

Click here to enter text.

Task 3: Analyse common types of network vulnerabilities

List at least 5 of the most common vulnerabilities that can occur on a network and describe how each item on your list can be used to effect a network.

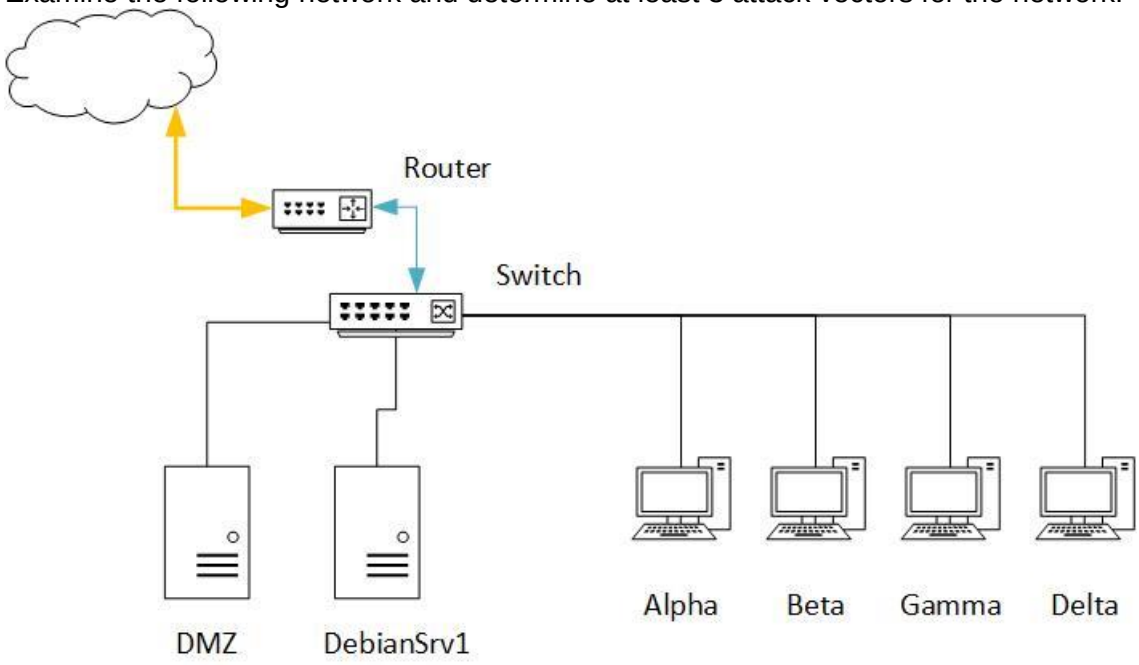
You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:
The student will answer with something similar to the following list: - Email: Ability to get malicious code inside the system where an authenticated user can run the code. - Websites: Ability to allow authenticated users to infect previously secured systems - USB drives: portable device that can contain malicious code - Laptops: Mobile devices, that have the ability to run a full suite of attack software to break or enter a network. - USB Devices: Like a USB drive, a usb device can have internal memory that could be used to store malicious code - Social Engineering: Employees being fooled to supply access, very similar to internal connections. - Internal connections: Employees can grant access to non-secured people who are dressed to look the part. - Mobile devices: can be used to locate access points such as wireless access points, and run specific software designed to damage a network. - Wireless Access points: Easily discovered access to a network, to enable additional attacks - Weak passwords: Easily guessed passwords, can allow for an authenticated user to login - Missing patches on Servers: This is where security patches are not applied to publicly discovered flaws and a hacker can locate the entry point to the network. - Misconfigured firewalls: Opened holes in the firewall to allow attacks access to the system - DOS/DDOS: Denial of Service/Distributed DOS, this is where a network's access to the net is removed, due to it being overwhelmed by constant machine requests and hence using all of a particular resource. And so forth, the student might add additional information, determine to the best of your industry knowledge if they answer correctly. Learning Guide: 2.3 Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.
Tutor Use Only **Successful** ☐ **Unsuccessful** ☐ **Date:** Click here to enter a date.

Tutor Feedback:
Click here to enter text.

Task 4: Determine how attacks occur

Examine the following network and determine at least 3 attack vectors for the network:



Describe, in details how the attacks would occur.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:

The student's answer will be subjective.

They have the possible attack vectors of:

- Email: Ability to get malicious code inside the system where an authenticated user can run the code.
- Websites: Ability to allow authenticated users to infect previously secured systems
- USB drives: portable device that can contain malicious code
- Laptops: Mobile devices, that have the ability to run a full suite of attack software to break or enter a network.
- USB Devices: Like a USB drive, a usb device can have internal memory that could be used to store malicious code
- Social Engineering: Employees being fooled to supply access, very similar to internal connections.
- Internal connections: Employees can grant access to non-secured people who are dressed to look the part.

- Mobile devices: can be used to locate access points such as wireless access points, and run specific software designed to damage a network.
- Wireless Access points: Easily discovered access to a network, to enable additional attacks
- Weak passwords: Easily guessed passwords, can allow for an authenticated user to login
- Missing patches on Servers: This is where security patches are not applied to publicly discovered flaws and a hacker can locate the entry point to the network.
- Misconfigured firewalls: Opened holes in the firewall to allow attacks access to the system
- DOS/DDOS: Denial of Service/Distributed DOS, this is where a network's access to the net is removed, due to it being overwhelmed by constant machine requests and hence using all of a particular resource.

The above list is a starting point for the student, they should select 3 potential vectors and then describe how the attack would happen.

For example, it could be a case of using a usb drive to install malicious code to open up administrative access on the network. In this manner, they would need to have physical access to the network.

Learning Guide: 2.4

Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.

Tutor Use Only

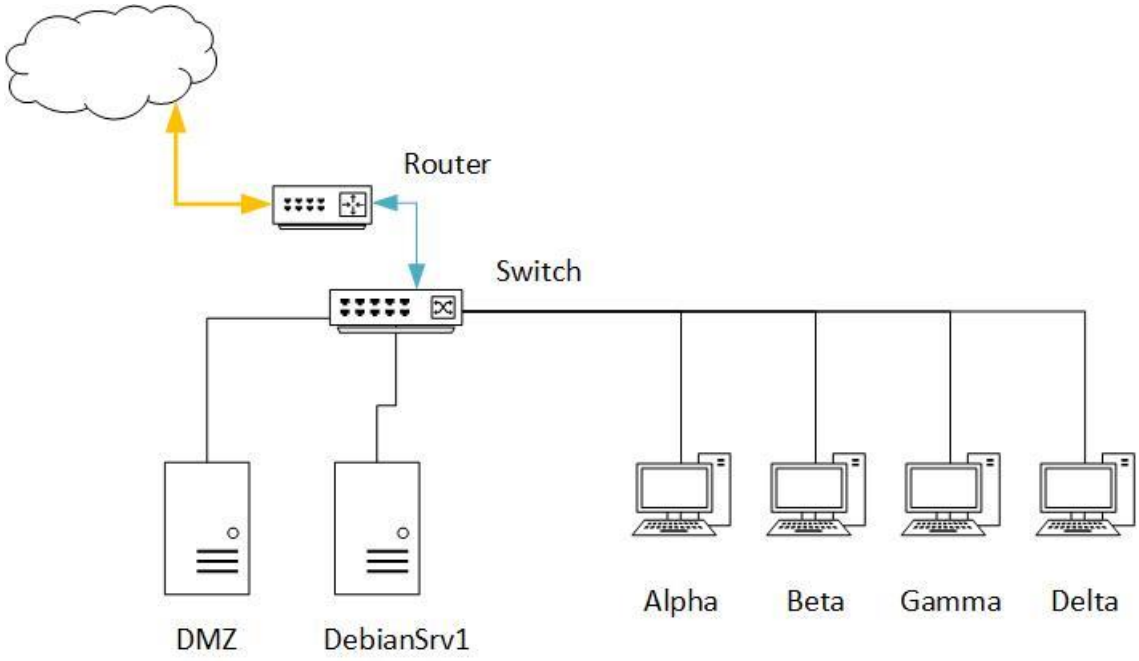
Successful ☐ **Unsuccessful** ☐ **Date:** Click here to enter a date.

Tutor Feedback:

Click here to enter text.

Task 5: Design a threat model to categorise threats

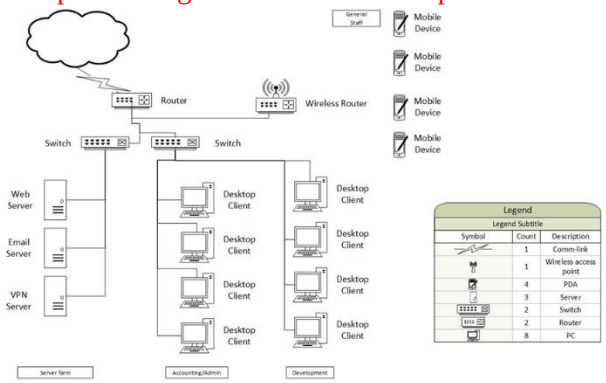
Generate a generic threat model to account for network security. List out categories for threats based on the following network map and supply examples for each category:



You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:

The student will answer with something similar:
 	
Threat model stages:
- Identify and document assets
  o For example, you could indicate there was a server, it's primary role is web development, connected internally, external access not allowed, the following Groups in Active Directory have access to it: Administrators, Web Developers; System; Test Viewers.
- Create an overview of the network
  o For Example, A description or legend on a network map will assist with this particular answer.
- Identify and document attack vectors



    - For Example
      attack vectors of:
        - Internet
        - Wireless Router
        - Physical access
- Identify threats
    - For Example; Wireless Router. Threats are internet based, primary threat is the ability to broadcast its existence as a network and enable connections. Once connections are established, the connected user has access to the network.
- Document and categorise threats
    - For Example; if you have identified the following threats:
        - Virus's
        - Malware
        - DDOS (Distributed Denial of Service)
        - USB Infection
    - You could break them into threat categories
        - High Threat: DDOS
        - Medium Threat: Virus, Malware
        - Low Threat: USB Infection
    - This categorisation allows for an easy way to understand the severity to the company due to the security threat that has occurred.
- Document potential solutions
    - For Example; Based off a virus threat, you would write up the following solutions
        - The machine that is infected gets removed from the network
        - The network is scanned
        - All anti-virus software is updated and system re-scanned
        - The infected machine is examined, log files to determine entry vector of virus
        - Machine gets cleaned
        - Machine returned to network
        - Education of end user
- Monitor security
    - For example: Monitoring Network logs, local machine logs and network logs
- Re-evaluate security
    - Set an end time frame for the current threat model, just to ensure that the content will be kept current with how fast technology changes.

Threats will be categorised in relevance to external and internal based upon the threats the student has recognised for the network.

Learning Guide: 2.5

Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.

Tutor Use Only

Successful ☐ Unsuccessful ☐ Date: Click here to enter a date.

Tutor Feedback:

Click here to enter text.

Assessment 3 Analyse security risks

Assessor Instructions

This assessment has been designed to allow students to demonstrate their ability to determine project requirements.

Students are required to read and respond to the scenario below. Any incorrect or incomplete responses must be returned to the student with feedback to allow them to resubmit. If the student requires additional training or guidance on the topic, you will need to negotiate time to assist them.

You must assess the student on their ability to:

1. Determine elements of risk management
2. Determine assets that require protection
3. Categorise assets and calculate their value to the organisation
4. Create a risk management plan

You are also required to assess the employability skills embedded in this task including:

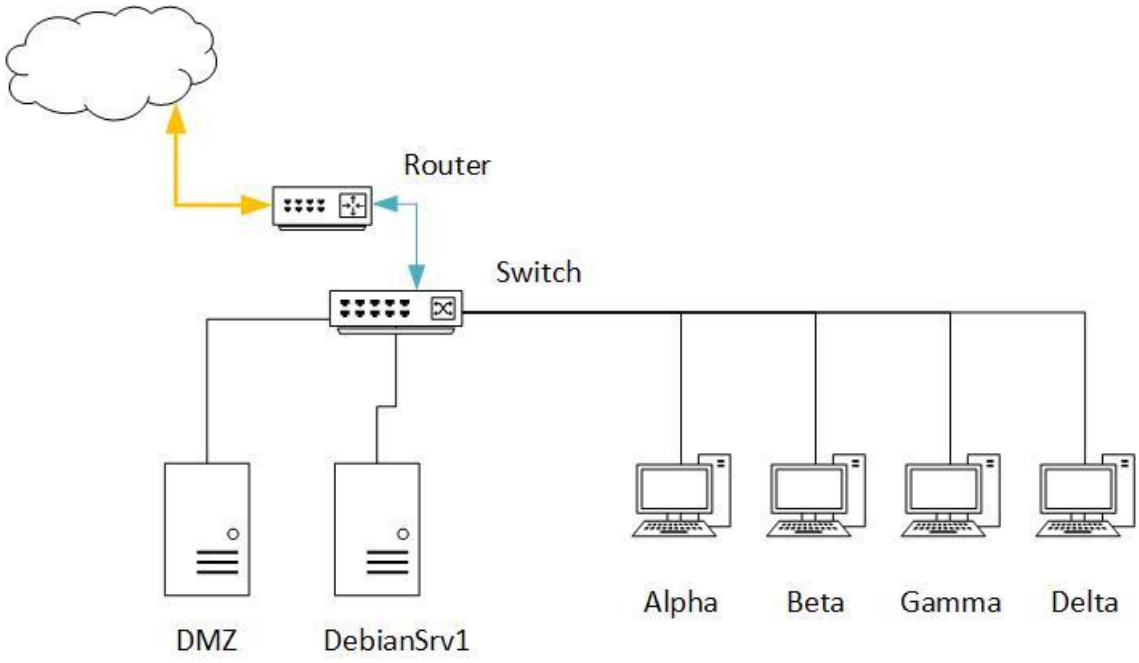
Writing	Uses factual information and industry related terminology to develop organisational plans, security policies and document security breaches
Oral Comm.	Uses active listening, observational and questioning techniques in order to identify different perspectives and confirm and clarify understanding
Numeracy	Calculates equipment costs in order to assess their business related value
Get the Work Done	Demonstrates a sophisticated understanding of principles, concepts, language and practices associated with the digital world and uses these to troubleshoot and reduce risks Uses digital tools to access and organise complex data and analyse multiple sources of information for strategic purposes Is acutely aware of the importance of understanding, monitoring and controlling access to digitally stored and transmitted information Uses a combination of formal and logical planning processes and an increasingly intuitive understanding of context to plan control methods for managing system security Makes a range of critical decisions in relatively complex situations, taking a range of constraints into account Recognises and addresses complex problems, including systems processes and rapid deployment of solutions to problems involving failure and security incidents

Record all assessment judgements in the Tutor Assessment Pack.

Benchmark answers are provided below each question in red.

Task 1: Determine elements of risk management

In the following network, the client stores business critical information on the Debiansrv1 system. They have a website on the DMZ server, which access the company's database stored on Debisnsrv1.



Determine the elements of risk for the network.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:

The student will answer similar to the following:
 	
In the network scenario provided, there are multiple locations in where the network is at risk. There are a few primary points that can cause issues these are:
- Scenario specific
  o Router configuration
  o DMZ configuration
  o DMZ server
  o Internal access to the machines.
- General Risks
  o Social engineering
  o Viruses, worms, and Trojan horses
  o Denial of service attack tools
  o Packet replaying
  o Packet modification
  o IP spoofing
  o Password cracking

There is a high chance the student will focus on the attack of this network based off Assessment 2, task 2. Ensure that they supply an answer that covers more than that particular incident with this network.

Learning Guide: 3.1

Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.

Tutor Use Only
Successful ☐ Unsuccessful ☐ Date: Click here to enter a date.
Tutor Feedback:
Click here to enter text.

Task 2: Determine assets that require protection

Generate a list and describe the assets that are critical for the network displayed in Assessment 3, task 1.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:

The primary assets are:

- DMZ server
  - Supports the company's website and provides an entry point to the company's data
- DebianSrv1 server
  - Holds the raw data and user details for the company.

Learning Guide: 3.2

Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.

Tutor Use Only
Successful ☐ Unsuccessful ☐ Date: Click here to enter a date.
Tutor Feedback:
Click here to enter text.

Task 3: Categorise assets and calculate their value to the organisation

Based off the information from Assessment 3, task 1 & 2, generate a table of hardware assets and values to the company.

Use the following information to calculate all values:

Item	Price	Amount
Server	$2350	2
Desktop	$1200	4
Router	$300	1
Switch	$300	1
Website (Generated daily income)	$500	
Employee	$20/hour	40Hrs/week 4 employees

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:

Item Values:

Item	Price	Amount	Total
Server	$2350	2	$4700
Desktop	$1200	4	$4800
Router	$300	1	$300
Switch	$300	1	$300
			$10,100

NB: Website and Employees, though assets are not included as hardware.

Learning Guide: 3.3

Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.

Tutor Use Only
Successful ☐ Unsuccessful ☐ Date: Click here to enter a date.
Tutor Feedback:
Click here to enter text.

Task 4: Create a risk management plan

Based off the information garnered in Assessment 3, task 1,2 and 3 create a risk management plan for the company.

Use the template: Risk Management Plan - Template.docx

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:
Confirm that the student has filled out all aspects of the template, ensure that the information makes sense and qualifies as a valid plan for the supplied network. Learning Guide: 3.4 Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.

Tutor Use Only
Successful ☐ Unsuccessful ☐ Date: Click here to enter a date.
Tutor Feedback:
Click here to enter text.

Assessment 4 Create a security design

Assessor Instructions

This assessment has been designed to allow students to demonstrate their ability to determine project requirements.

Students are required to read and respond to the scenario below. Any incorrect or incomplete responses must be returned to the student with feedback to allow them to resubmit. If the student requires additional training or guidance on the topic, you will need to negotiate time to assist them.

You must assess the student on their ability to:

1. Determine attacker scenarios and threats
2. Design security measures for network components
3. Obtain feedback and adjust if required
4. Develop security policies

You are also required to assess the employability skills embedded in this task including:

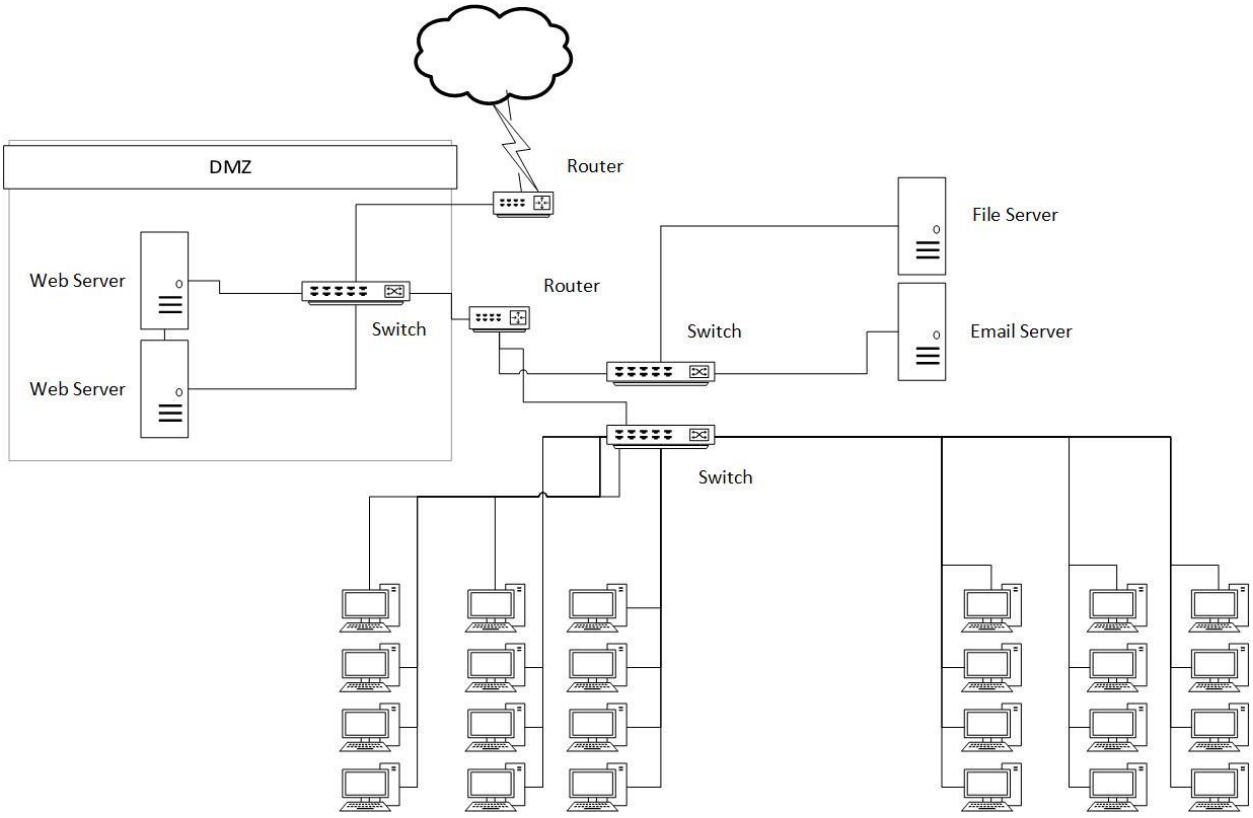
Writing	Uses factual information and industry related terminology to develop organisational plans, security policies and document security breaches
Oral Comm.	Uses active listening, observational and questioning techniques in order to identify different perspectives and confirm and clarify understanding
Numeracy	Calculates equipment costs in order to assess their business related value
Get the Work Done	Demonstrates a sophisticated understanding of principles, concepts, language and practices associated with the digital world and uses these to troubleshoot and reduce risks Uses digital tools to access and organise complex data and analyse multiple sources of information for strategic purposes Is acutely aware of the importance of understanding, monitoring and controlling access to digitally stored and transmitted information Uses a combination of formal and logical planning processes and an increasingly intuitive understanding of context to plan control methods for managing system security Makes a range of critical decisions in relatively complex situations, taking a range of constraints into account Recognises and addresses complex problems, including systems processes and rapid deployment of solutions to problems involving failure and security incidents

Record all assessment judgements in the Tutor Assessment Pack.

Benchmark answers are provided below each question in red.

Task 1: Determine attacker scenarios and threats

Based off the following network design, generate a list (at least 3) of potential attacker scenarios and threats.



The client is a small educational institute which stores results for their students on the file server. The webserver links to the file server to allow for authentication to check email and shared storage.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:
The students answer will be subjective based upon the knowledge they have garnered so far. In general, there could be attacks from: - Email - Web - Physical devices such as usb, Disc - Virus - Social Engineering - Unpatched systems The student will potentially add and make a more definite list, use your knowledge to confirm their answers. The scenarios should be a bit more in-depth, for example:

Scenario 1: A hacker has discovered a vulnerability in the router, this has allowed them to get into the system and attack the web servers in the DMZ. Primary issue of this is the ability to re-write the websites as they have gained access to the system.

Scenario 2: Infected USB, an employee introduces into the network an infected usb drive. The infection occurred as they were using the usb drive in non-corporate machines with minimal anti-virus/malware software.

Learning Guide: 4.1

Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.

Tutor Use Only

Successful ☐ Unsuccessful ☐ Date: Click here to enter a date.

Tutor Feedback:

Click here to enter text.

Task 2: Design security measures for network components

Based off the network shown in Assessment 4, task 1. Design measures to prevent all five of the scenarios that you created.

Provide your answer like:

Scenario X: <This is the scenario from Task 1>

Scenario X Solution: <Provide your solution>

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:

This is subjective to the previous answers that the student supplied.

Each scenario that the student has created will require a counter measure, and this can be based upon anything.

The scenarios should be a bit more in-depth, for example:

Scenario 1: A hacker has discovered a vulnerability in the router, this has allowed them to get into the system and attack the web servers in the DMZ. Primary issue of this is the ability to re-write the websites as they have gained access to the system.

Scenario 1 Solution: Monitor and patch routers, switches and servers. Ensure logging is occurring on all DMZ devices and core infrastructure.

Scenario 2: Infected USB, an employee introduces into the network an infected usb drive. The infection occurred as they were using the usb drive in non-corporate machines with minimal anti-virus/malware software.

Scenario 2 Solution: Ensure up to date anti-virus/malware on the corporate system. Education to employees in regards to using usb devices from corporate to home life.

Learning Guide: 4.2

Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.

Tutor Use Only

Successful ☐ Unsuccessful ☐ Date: Click here to enter a date.

Tutor Feedback:

Click here to enter text.

Task 3: Obtain feedback and adjust if required

Communicate (face to face, phone or skype) with the tutor in regards to the security measures you have designed in Assessment 4, task 2.

Discuss each scenario and solution, re-evaluate your solutions based on tutor feedback.

Generate a checklist of items that were discussed, and submit to the tutor.

You must answer the question in your own words for your knowledge to be considered satisfactory.

For this Task, you must play the part of Security Design expert. During this meeting you the Assessor must complete the Conversation Checklist Assess 4 – Task 3 (Assessor Use Only).docx.

This is required to ensure that the Foundation Skills and Performance Criteria associated with the task, are checked off as completed and satisfactory, during the candidate's conversation with the Assessor.

Answer:

The student will contact you via face to face, phone or skype.

This is subjective to the student.

Use the conversation checklist document to assist with evaluating the student's response.

During discussion ensure that the student understands the concepts of what they are discussing, if they haven't thought of the following mention these items to them:

- Group policy for Windows Servers
- Physical security: key card access, biometric security and so forth

- Distributed patch server software, ie Windows Server Update Services (WSUS)

Feel free to add additional security items if they are relevant to the scenarios presented.

The student will submit their own checklist showing that they have recorded the communication.

Learning Guide: 4.3

Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.

Tutor Use Only

Successful ☐ Unsuccessful ☐ Date: Click here to enter a date.

Tutor Feedback:

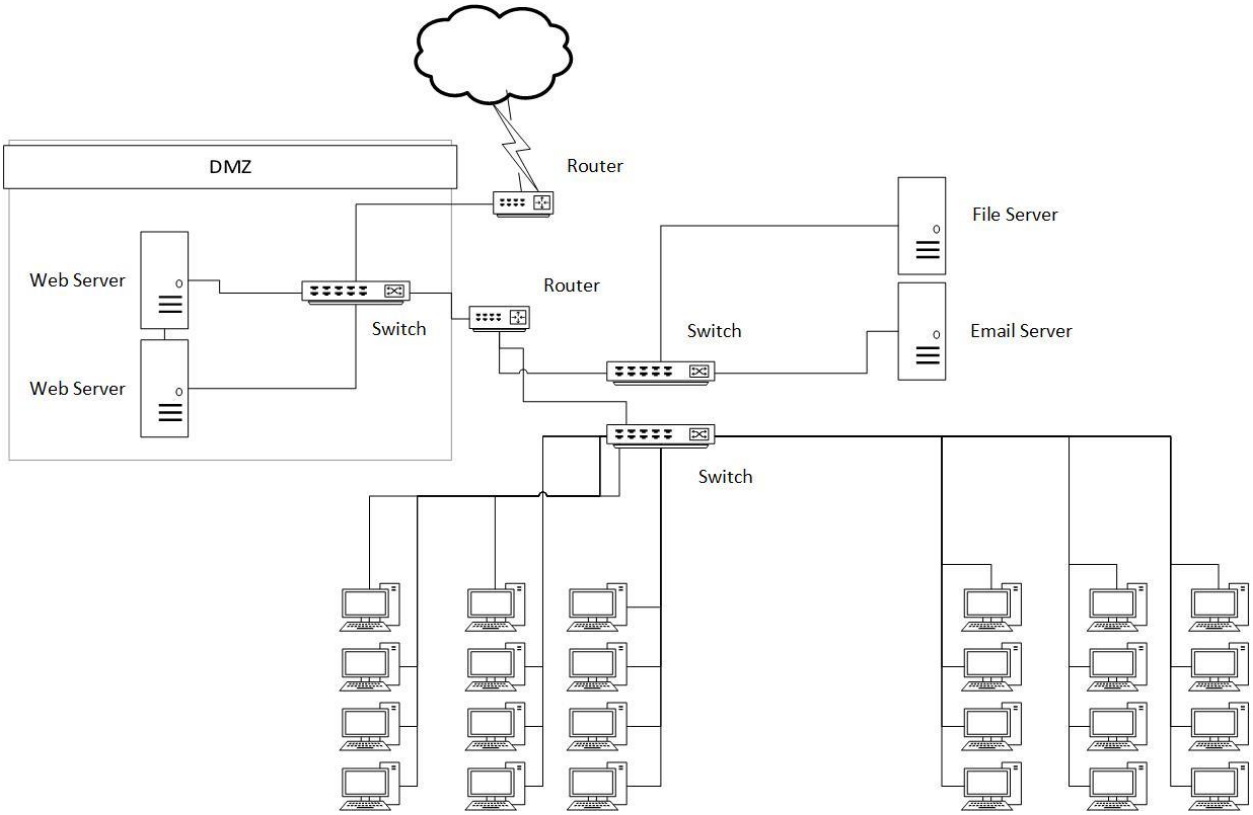
Click here to enter text.

Task 4: Develop security policies

Develop and document security polices for:

- Routers and switches
- Remote access

Base the design of the security polices off the following network:



Use the following document structure:

- Overview
- Purpose
- Scope
- Policy
- Policy Compliance
- Related Standards, Policies and processes
- Revision History

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:
Each policy should have the following headers: - Overview - Purpose - Scope - Policy - Policy Compliance - Related Standards, Policies and processes - Revision History Ensure each policy focuses on the areas they are supposed to. Review Examples: - Remote_access_policy-Assessor_Only.docx - Router and Switch security policy Assessor Only.docx Learning Guide: 4.4 Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.
Tutor Use Only **Successful ☐ Unsuccessful ☐ Date:** Click here to enter a date. **Tutor Feedback:** Click here to enter text.

Assessment 5 Design and implement responses to security incidents

Assessor Instructions

This assessment has been designed to allow students to demonstrate their ability to determine project requirements.

Students are required to read and respond to the scenario below. Any incorrect or incomplete responses must be returned to the student with feedback to allow them to resubmit. If the student requires additional training or guidance on the topic, you will need to negotiate time to assist them.

You must assess the student on their ability to:

1. Design auditing and incident response procedure
2. Document security incidents
3. Implement configurations aligned with incident response procedure design
4. Test and sign off

You are also required to assess the employability skills embedded in this task including:

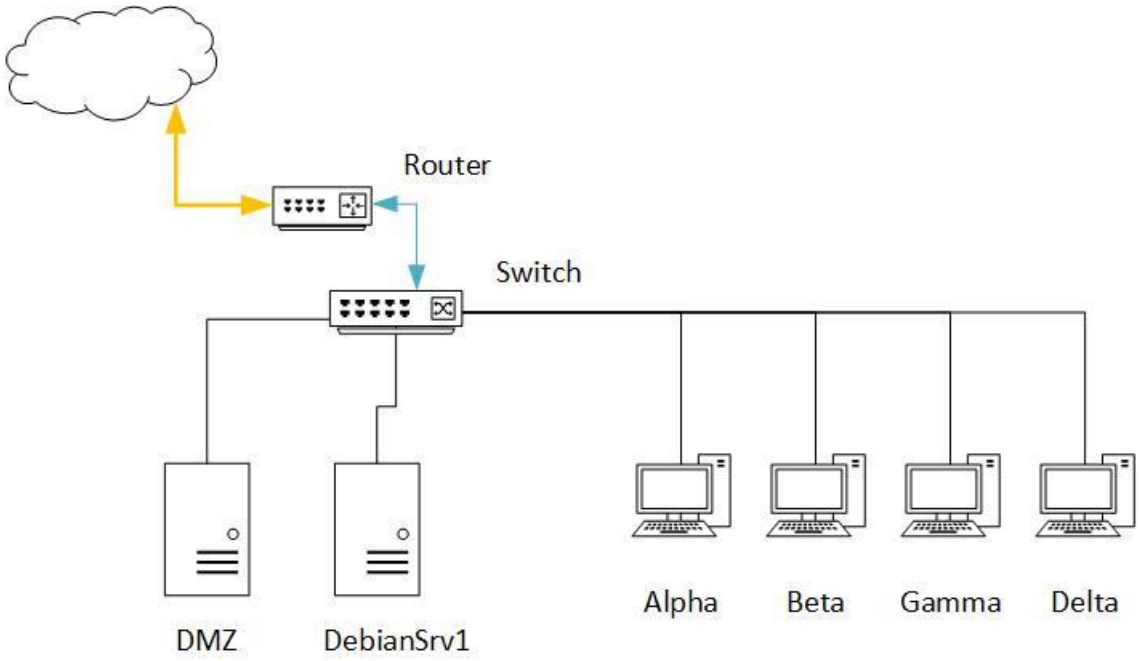
Writing	Uses factual information and industry related terminology to develop organisational plans, security policies and document security breaches
Oral Comm.	Uses active listening, observational and questioning techniques in order to identify different perspectives and confirm and clarify understanding
Numeracy	Calculates equipment costs in order to assess their business related value
Get the Work Done	Demonstrates a sophisticated understanding of principles, concepts, language and practices associated with the digital world and uses these to troubleshoot and reduce risks Uses digital tools to access and organise complex data and analyse multiple sources of information for strategic purposes Is acutely aware of the importance of understanding, monitoring and controlling access to digitally stored and transmitted information Uses a combination of formal and logical planning processes and an increasingly intuitive understanding of context to plan control methods for managing system security Makes a range of critical decisions in relatively complex situations, taking a range of constraints into account Recognises and addresses complex problems, including systems processes and rapid deployment of solutions to problems involving failure and security incidents

Record all assessment judgements in the Tutor Assessment Pack.

Benchmark answers are provided below each question in red.

Task 1: Design auditing and incident response procedure

Based off the following network:



Design an auditing and incident response procedure document.

Treat this as two separate documents:

- Auditing document; include a legend with any headings as needed.
- Incident response document.

Provide a completed version of both incident response and auditing document with the templates you create.

Using the templates, you created. Create an audit document by researching the web to locate specifications of a single desktop machine from any vendor.

Then, create an incident report for the desktop machine listed in your audit document. You will need to determine an incident of your choice and document as your incident response.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:
The audit document should have the following layout: - Hardware; break down to: cpu, ram, hdd, gpu - Software; break down to: Operating system, standard applications, anti-virus, specialised applications - Currency of Software: Are there patches or updates that need to be applied, when was the last time the application was patched - Revision history: when was the last audit performed

The incident response document should have the following headings:

- Recognize and respond to an incident;
- Assess the situation quickly and effectively;
- Notify the appropriate individuals and organizations about the incident;
- Organize the company's response activities, including activating a command centre;
- Escalate the company's response efforts based on the severity of the incident; and
- Support the business recovery efforts being made in the aftermath of the incident.

Ensure that the completed version that the student creates, works and makes sense. Use the completed form to determine the validity of the template they create.

Ensure that the template they supply for the incdent response form, is not a copy/paste from the SLG.

Learning Guide: 5.1

Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.

Tutor Use Only

Successful ☐ Unsuccessful ☐ Date: Click here to enter a date.

Tutor Feedback:

Click here to enter text.

Task 2: Document security incidents

Based off the network from Assessment 5, task 1. Document the following incidents using your templates:

- Virus infection on Beta and Gamma
- Hard drive failure on DebianSrv1.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:

The students answer will be similar to the following:

Virus Infection

- System wide update and sweep for the virus
- Infected machines removed from the network
- Appropriate people notified
- Log files examined to determine infection
- Infected machines cleaned and tested
- Machines returned to production

- Monitoring of the network increased for 7-day duration

HDD Failure

- Machine removed from network
- Replacement part purchased and installed
- Restoration of Operating system and files form backup solution
- Examination of log files to determine point of failure, if possible.
- Monitoring process continued on server for 7-day period

Learning Guide: 5.2

Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.

Tutor Use Only

Successful ☐ Unsuccessful ☐ Date: Click here to enter a date.

Tutor Feedback:

Click here to enter text.

Task 3: Implement configurations aligned with incident response procedure design

Based off the network from Assessment 5, task 1. Document one of the following incidents using your templates:

- Virus scan or HDD repair.

Virus Scan Instructions: To simulate the virus infection, instigate an update of your machines virus protection and scan the machine. Supply screen shots of update and finished scanning.

HDD Repair Instructions: To simulate replacement hard drive, submit screen shots of running and a completed chkdsk to fix the hard drive and a text file containing the output of the scan.

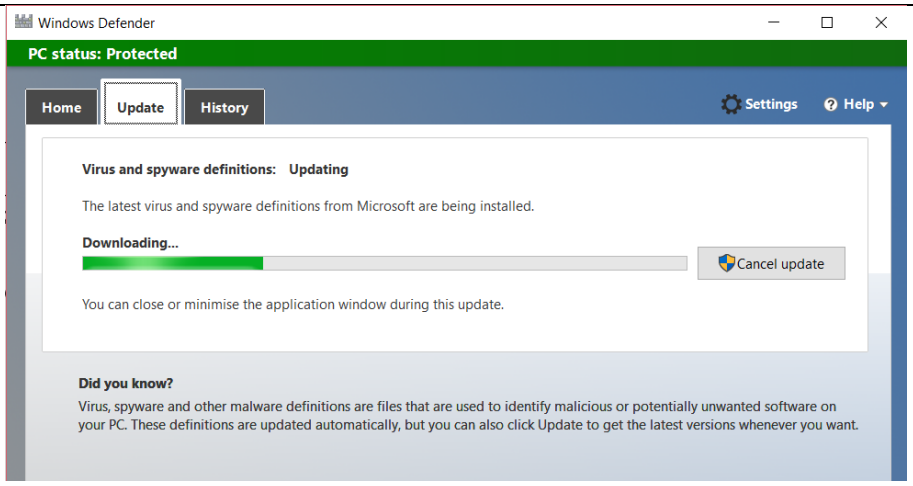
Submission: Submit a document describing the steps undertaken and screenshots of the activity occurring.

You must answer the question in your own words for your knowledge to be considered satisfactory.

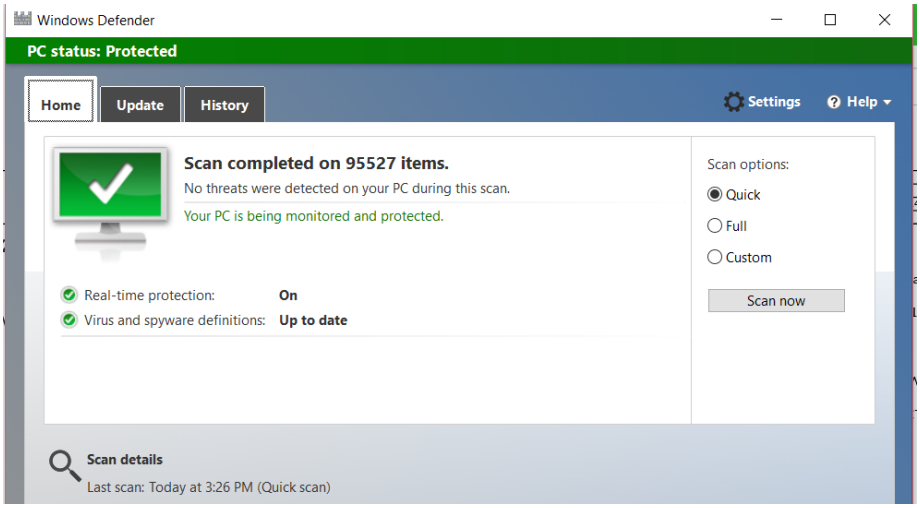
Answer:

Virus Scan:

- Update

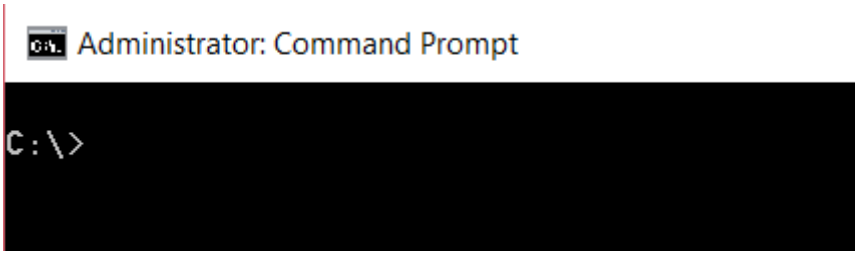


- Completed Scan

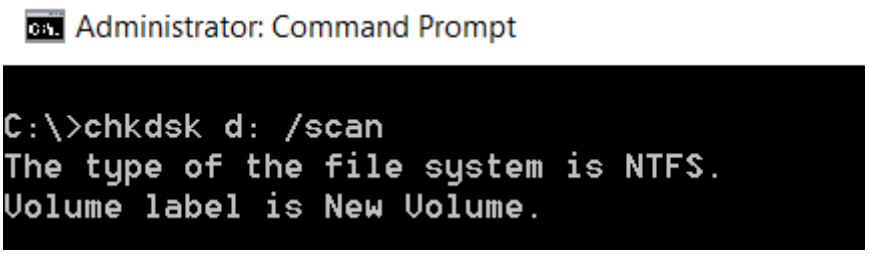


HDD Repair

- Elevated dos box



- Chkdsk command



- Log of the scan

The type of the file system is NTFS.

Volume label is New Volume.

Stage 1: Examining basic file system structure ...

Progress: 0 of 256 done; Stage: 0%; Total: 28%; ETA: 0:00:02
Progress: 256 of 256 done; Stage: 100%; Total: 34%; ETA: 0:00:02 .
256 file records processed.
File verification completed.

Progress: 0 of 0 done; Stage: 99%; Total: 71%; ETA: 0:00:02 .. 0 large file records processed.

Progress: 0 of 0 done; Stage: 99%; Total: 71%; ETA: 0:00:02 ... 0 bad file records processed.

Stage 2: Examining file name linkage ...

Progress: 276 of 276 done; Stage: 100%; Total: 86%; ETA: 0:00:01

276 index entries processed.
Index verification completed.

Progress: 0 of 0 done; Stage: 99%; Total: 86%; ETA: 0:00:01 . 0 unindexed files scanned.
Progress: 0 of 0 done; Stage: 99%; Total: 86%; ETA: 0:00:01 .. 0 unindexed files recovered to lost and found.
Stage 3: Examining security descriptors ...

Security descriptor verification completed.

Progress: 0 of 0 done; Stage: 100%; Total: 99%; ETA: 0:00:00 ...
10 data files processed.

Windows has scanned the file system and found no problems.

No further action is required.

30904319 KB total disk space.

63552 KB in 7 files.

8 KB in 12 indexes.

0 KB in bad sectors.

43839 KB in use by the system.

42224 KB occupied by the log file.

30796920 KB available on disk.

4096 bytes in each allocation unit.

7726079 total allocation units on disk.

7699230 allocation units available on disk.

- The above is the output from the chkdsk command
- Command used was chkdsk d: /scan > t.txt

Learning Guide: 5.3

Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.

Tutor Use Only

Successful ☐ **Unsuccessful** ☐ **Date:** Click here to enter a date.

Tutor Feedback:

Click here to enter text.

Task 4: Test and sign off

Create a sign off template that can be used to indicate work that has been completed. Ensure that there are locations on the document for yourself and the client to sign off on the work that has been achieved.

With this template document, add a completed document where you write up the work you have done in the previous assessment (Assessment 5, Task 3).

Submit both template and completed sign off sheet.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:
The student will produce two documents: - Template for a sign off sheet - Completed sign off sheet based on the previous task's result Use your industry knowledge to ensure that the document is of a high standard. Learning Guide: 5.4 Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.
Tutor Use Only **Successful** ☐ **Unsuccessful** ☐ **Date:** Click here to enter a date. **Tutor Feedback:** Click here to enter text.

Assessment 6 Knowledge Questions

Assessor Instructions

This assessment has been designed to allow students to demonstrate their ability to determine project requirements.

Students are required to read and respond to the scenario below. Any incorrect or incomplete responses must be returned to the student with feedback to allow them to resubmit. If the student requires additional training or guidance on the topic, you will need to negotiate time to assist them.

You must assess the student on their ability to:

1. recognise and describe common ICT networks and their configuration
2. identify and describe network attacks, vulnerabilities and related weaknesses of installed infrastructure, including: security technologies
3. identify and describe network attacks, vulnerabilities and related weaknesses of installed infrastructure, including: emerging security issues
4. identify and describe network security measures, including: auditing and penetration testing techniques
5. identify and describe network security measures, including: logging analysis techniques
6. identify and describe network security measures, including: organisational network infrastructure
7. identify and describe network security measures, including: capabilities of software and hardware solutions
8. identify and describe network security measures, including: general features of emerging security policies, with depth in security procedures
9. identify and describe network security measures, including: network management and security process controls
10. explain network security implementation risk management plans and procedures, including: network security planning
11. explain network security implementation risk management plans and procedures, including: implementation
12. explain network security implementation risk management plans and procedures, including: cost analysis and budgeting.

You are also required to assess the employability skills embedded in this task including:

Writing	Uses factual information and industry related terminology to develop organisational plans, security policies and document security breaches
Oral Comm.	Uses active listening, observational and questioning techniques in order to identify different perspectives and confirm and clarify understanding
Numeracy	Calculates equipment costs in order to assess their business related value

Get the Work Done	Demonstrates a sophisticated understanding of principles, concepts, language and practices associated with the digital world and uses these to troubleshoot and reduce risks Uses digital tools to access and organise complex data and analyse multiple sources of information for strategic purposes Is acutely aware of the importance of understanding, monitoring and controlling access to digitally stored and transmitted information Uses a combination of formal and logical planning processes and an increasingly intuitive understanding of context to plan control methods for managing system security Makes a range of critical decisions in relatively complex situations, taking a range of constraints into account Recognises and addresses complex problems, including systems processes and rapid deployment of solutions to problems involving failure and security incidents

Record all assessment judgements in the Tutor Assessment Pack.

Benchmark answers are provided below each question in red.

Task 1: Recognise and describe common ICT networks and their configuration

Describe and define a generalised network, name the topology and secure communications link of the network design.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:
The student will answer similar to the following: Topology: Star topology Network: VPN or VLAN, VPN secure encrypted tunnel between locations. VLAN segmentation to create secure internal connections. Learning Guide: 6.1 Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.
Tutor Use Only **Successful** ☐ **Unsuccessful** ☐ **Date:** Click here to enter a date. **Tutor Feedback:** Click here to enter text.

Task 2: Identify and describe network attacks, vulnerabilities and related weaknesses of installed infrastructure, including: security technologies

Identify and describe a physical and logical security technology.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:
The student will answer similar to: Physical: • Biometric Authentication: This technology involves the use of a physical attribute of the user to provide authentication. This can be done as fingerprint, voice, or iris scanning. Some examples are Windows hello in windows 10, this has the ability to use iris scan on the phone, facial recognition on a desktop and fingerprint via a fingerprint reader. Logical: • Mobile Application Wrappers: This technology allows for an enterprise to add security and management features to an application. This allows for security to be applied to applications on devices that do not fall under a company's security policy, such as Bring Your Own Device (BYOD) scenarios. • Multi-factor Authentication: Also referred to as two factor authentication. This is where the user requires multiple methods of authentication to ensure that they validate the security level of the users, this is can be done as username/password and a code that is sent to either email or phone. Learning Guide: 6.2 Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.
Tutor Use Only **Successful** ☐ **Unsuccessful** ☐ **Date:** Click here to enter a date. **Tutor Feedback:** Click here to enter text.

Task 3: Identify and describe network attacks, vulnerabilities and related weaknesses of installed infrastructure, including: emerging security issues

Describe ransomware and list 3 of the top ransomware infections.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:

The student will answer similar to this:

Ransomware: This is where malicious software can gain access to a computer/network and it does one of two things, the first one is that it encrypts the data on the machine and the machine can be unlocked if the owner of the machine pays a certain amount of money or, the second is that the machine has an unlockable lock screen so the user can't get to the operating system.

The student can select any of the following:

- Ransom:HTML/Tescrypt.E
- Ransom:HTML/Tescrypt.D
- Ransom:HTML/Locky.A
- Ransom:Win32/Locky
- Ransom:HTML/Crowti.A
- Ransom:HTML/Exxroute.A
- Ransom:Win32/Cerber.A
- Ransom:JS/FakeBsod.A
- Ransom:HTML/Cerber.A
- Ransom:JS/Brolo.C

Learning Guide: 6.3

Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.

Tutor Use Only

Successful ☐ **Unsuccessful** ☐ **Date:** Click here to enter a date.

Tutor Feedback:

Click here to enter text.

Task 4: Identify and describe network security measures, including: auditing and penetration testing techniques

Describe the value of auditing and penetration techniques for a generic network.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:

The student will answer similar to the following:

Penetration Testing

Penetration testing is a technique where a computer system is attacked to determine if there are any weaknesses or vulnerabilities that can be located to compromise the system. In general, a penetration test identifies and prioritises security risks, these risks can be located in the networks endpoints and applications. By implementing penetration testing, weaknesses in a network can be located and removed without any actual data loss for the client.

Auditing:

Auditing is key to ensuring that you know what all elements exist within a network, auditing covers the physical components and examination of network traffic. This recording of all elements allows for new elements to be easily discovered, these elements being unknown network traffic, a machine cpu suddenly maxing out for no apparent reason is indicative of that machine being infected. As you can tell, auditing is a way of ensuring that the unknown traffic or unknown system utilisation gets noticed, once noticed, then the machines in question can start to be examined to see if the traffic is just unique for that particular time frame or something more sinister in design.

Learning Guide: 6.4

Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.

Tutor Use Only

Successful ☐ **Unsuccessful** ☐ **Date:** Click here to enter a date.

Tutor Feedback:

Click here to enter text.

Task 5: Identify and describe network security measures, including: logging analysis techniques

Describe how you would perform logging analysis on a linux system that has been compromised.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:

The response from the student should cover the filtering/pattern mining technique described in the slg, ensure that they note which file to examine, auth.log, and the keywords they would remove to enable an easier time to examine the log file.

Keywords are:

- Invalid user
- Failed password for invalid user
- Authentication failure
- User unknown
- Check pass; user unknown
- Failed password for root from
- Failed password for
- Session closed for user
- Session opened for user root
- POSSIBLE BREAK-IN ATTEMPT

Ensure that the description they provide is viable for a real world scenario.

Learning Guide: 6.5

Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.

Tutor Use Only
Successful ☐ Unsuccessful ☐ Date: Click here to enter a date.
Tutor Feedback:
Click here to enter text.

Task 6: Identify and describe network security measures, including: organisational network infrastructure

Describe three areas in which attacks can occur, and how they can be minimised.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:

The student will answer will contain something similar to:

3 areas of threats

- Deliberate
- Environmental
- Accidental

With their definitions coming from:

Environmental threats are capable of eliminating entire physical networks and data, as such, the primary method of ensuring that information is kept secure during such an event is to ensure that the information of a company is stored safely away from a single point of impact. This can be as simple as having rotating tape backups that are removed on a daily basis and stored in a different part of the city, or to a more common variation nowadays is the implementation of cloud based backups of data. The distributed method of cloud based storage is perfect for ensuring that data will not get lost or destroyed in a singular event.

Accidental threats are human error. This is always bound to happen within an organisation and the larger the organisation, the more likely it will occur. The best way to ensure that the effects of this are minimised is to enable specific methodologies of data recovery. A very simple way of ensuring that end user's data is kept safe, is to have the end user save their data into a remote folder on the server. I.e. in this manner, with GPOs, it is possible to map the end users folder structure to the server, so, instead of the user have having a file structure for the documents folder like c:/users/%name%/documents the documents folder would be mapped to \\serverName\%user%\documents. The server would have versioning control, so that if the end user accidently re-wrote a particular file, it would be possible to go back a version to recover missing data. And, the server would be maintaining backups to a tape and synchronisation to a company cloud solution, such as Onedrive or Dropbox.

Deliberate threats are the main reason as to why security of networks becomes paramount. Simple steps can be done to prevent all but the most determined attack. These steps are:

- Education; educating an employee on how to safely use email and websites, i.e. don't click on a link you don't know or wasn't sent by a trusted source. Do not install applications unless authorised, social engineering works in the following manner, always get a manager to assist when allowing access to the network for an unknown person.
- Anti-virus/Anti-malware; These systems should be implemented and updated on all machines. Monitoring of this type of software is also important, as most enterprise variations allow for a centralised management suite, so if a single machine didn't receive the latest updated software, this updated could be pushed to the client.
- Group Policy Objects (GPOs); From a server point of view, restricting what can be occurring on a desktop machine can be critical in ensuring that an end user won't be able to accidently infect a machine by installing random software is important. Also locking down aspects of what the user can and cannot do, will ensure that uniformed end users won't make system causing mistakes.
- Access levels; these levels can be implemented using GPOs. Once implemented, you will be able to have areas of a network that a user won't be able to access. For example, if the client is a car yard, the mechanic who requires only email and access to specialised software, doesn't need access to accounting files and as such, using a GPO, this type of security can be implemented.
- Physical Security; This is where servers, switches, routers and other network components are locked away in secure areas to ensure that no one can just access them. Locked doors, lockable cabinets are all good ways of implementing this.
- Logical Security; This is where network components can be configured to only allow known machines, switches and routers can be locked down to mac addresses. So no one can just plug a machine into the network and get access. VLANs would be implemented to segment the network ensuring that a shared resource such as internet connection can exist, but machines that belong in accounting or finances in general can't be seen by a client accessing the wireless network.

Learning Guide: 6.6

Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.

Tutor Use Only

Successful ☐ **Unsuccessful** ☐ **Date:** Click here to enter a date.

Tutor Feedback:

Click here to enter text.

Task 7: Identify and describe network security measures, including: capabilities of software and hardware solutions

Describe firewall technologies in both hardware and software solutions.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:
The student's answer will contain something like: Hardware Firewall - Speed; a hardware firewall is designed to be fast and as such it can handle multiple traffic requests at any one point in time. - Security; Being designed for a singular action, a hardware firewall is locked up and the underlying operating system will have limited vulnerabilities to be exploited. - Interaction; Once the hardware firewall is configured and set up in the network, it is an isolated element. This isolation means that it does its task and doesn't interfere or manipulate any other aspect on the network. Software Firewall - Ease of use; software firewalls are normally configured with user friendly gui's that allow the end user to quickly and easily configure the firewall. - Flexible; With the advanced interface, software gui's have the ability to be extremely flexible in what they block and how they achieve certain tasks. - Control; combined with ease of use and flexibility, the software firewall allows the end user to configure and control the firewall settings extremely well. Learning Guide: 6.7 Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.
Tutor Use Only **Successful ☐ Unsuccessful ☐ Date:** Click here to enter a date. **Tutor Feedback:** Click here to enter text.

Task 8: Identify and describe network security measures, including: general features of emerging security policies, with depth in security procedures

Describe the structure of an emerging security policy and the layers of an in-depth security procedure.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:
The student will supply an answer similar to: Security Policy layout - Overview - Purpose - Scope - Policy - Policy Compliance - Related Standards, Policies and processes - Revision History Layers of security - Router - Hardware firewall - Switch - Software firewall, anti-virus, anti-malware - Group Policy Objects - Critical data Learning Guide: 6.8 Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.
Tutor Use Only **Successful** ☐ **Unsuccessful** ☐ **Date:** Click here to enter a date. **Tutor Feedback:** Click here to enter text.

Task 9: Identify and describe network security measures, including: network management and security process controls

Describe 3 areas in which security process controls can be implemented in network management.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:
The student will select and describe 3 elements from the following. Some areas in which security polices can be implemented are: - Physical computer security o Computers are kept secure, this can be done in a multitude of ways, locked rooms, attached to desks, monitored security cameras. Key card access to labs or office equipment. - Network security o Network security is where there is hardware designed to keep out intruders, such as firewalls, intrusion detection systems (IDS), vpn, vlan, anti-virus, anti-malware, group policy objects (GPOs), username/password combinations, file security and so forth. - Data security o Securing data is achieved by implementing secure and authenticated file systems, having software protect the data, ensuring that backups both onsite and offsite are taking place. Enabling authentication of users and folders, implementing version control for critical documents. - Contingency and disaster recovery plans and tests o These policies are planned responses to potential identified threats to a network. So, what happens during a fire/flood/earthquake/building disaster? Where is the data stored? How do you recover this information, what's the timeline on getting the business back on its feet? The creation of these plans and policies are designed to get a business back on its feet after a disaster. - Computer security and awareness training o Education of users is critical as attacks of a social engineering nature can be removed through the proper education and identification of what and how these types of attacks can occur. This training will also limit the amount of potential virus and malware infections that can occur due to users not blindly installing applications. - Security management and coordination policies o Policies of a security nature and coordination allow for a business to enhance the general security of a network. These policies inform and control the response to any particular incident. - Compliance of software o By ensuring the compliance of software as a policy this enables systems to be updated through network management to ensure that any vulnerabilities that are discovered are dealt with in a timely manner. An aspect of this is also ensuring that all systems in place in a network are the same, for example, if a company is using Office 365 as its default implementation of an office suite then word's default saved document is a docx, having a small part of the company implementing word 97 .doc documents shouldn't occur as the company on a whole is using the current standard. By ensuring compliance, this mismatch of file formats would not occur. Learning Guide: 6.9

Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.

Tutor Use Only
Successful ☐ Unsuccessful ☐ Date: Click here to enter a date.
Tutor Feedback:
Click here to enter text.

Task 10: Explain network security implementation risk management plans and procedures, including: network security planning

Describe 3 components of where a network security plan is vital, list and explain in your own words.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:

The student will answer something similar to the following, they may add additional research notes, ensure that the response they give is of industry standard.

- Security risks
  - A listing of potential risks that can occur. Physical and logical.
- Security strategies
  - Mitigation planning of the risks that were identified.
- Public access strategies
  - Determination of if the network infrastructure is to be shared with the public in anyway, an example of this is free wifi for clients that are waiting on a service the organisation is supplying.
- Authentication policies
  - What levels of authentication exist, password/username policies, does remote access into the network exist?
- Information security strategies
  - How is data secured? Is it encrypted? Does email and web traffic require encryption or special authentication policies applied to it?
- Administration policies
  - Monitoring of the network, ability to detect and resolve suspicious activity. A chain of command, so to speak, of where breaches and intrusion to the network are brought up.

Learning Guide: 6.10

Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.

Tutor Use Only
Successful ☐ Unsuccessful ☐ Date: Click here to enter a date.
Tutor Feedback:
Click here to enter text.

Task 11: Explain network security implementation risk management plans and procedures, including: implementation

Describe the implementation process of minimising the risk of ransomware in a network. Discuss which areas are to be examined and how you would implement preventative measures.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:

The student should answer something similar to:

Mitigating ransomware can be done by the following implementations:

- Software solutions
  - Operating Systems
  - Anti-virus / Anti-malware
  - Application patches
- Hardware solutions
  - Firewall
  - IDS
- Monitoring
  - Log files for network traffic
  - Log files for authorisation attempts

The student should describe how you would implement / stay current with general security practices to prevent infection from ransomware.

Learning Guide: 6.11

Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.

Tutor Use Only
Successful ☐ Unsuccessful ☐ Date: Click here to enter a date.
Tutor Feedback:
Click here to enter text.

Task 12: Explain network security implementation risk management plans and procedures, including: cost analysis and budgeting.

Generate a balance sheet for a client based off the following information:

Budget: $55,000/year

Requirements: 4 x Servers ($3,000), 20 x Desktop ($1,200), Software – Desktop ($600 per machine), Software – Server ($1,000 per machine), Hardware firewall ($900), IDS ($1500), installation cost ($4,000), training ($1,000).

Describe potential solutions for the network to achieve everything in the above list.

You must answer the question in your own words for your knowledge to be considered satisfactory.

Answer:

The student will supply an answer similar to:

Item	Element Cost	Amount of Items	Cost	Overall
Server	**3000**	**4**	**12000**	
Desktop	**1200**	**20**	**24000**	
Software – Desktop	**600**	**20**	**12000**	
Software – Server	**1000**	**4**	**4000**	
Firewall – Hardware	**900**	**1**	**900**	
IDS	**1500**	**1**	**1500**	
Installation	**4000**	**1**	**4000**	
training	**1000**	**1**	**1000**	
				59400

The student will then need to justify what they can do to acquire the additional funds to meet the final price, as this is subjective, the student could potential say they pull from the next year's budget, change software, modify hardware, converge Servers remove IDS or the HW firewall.

Learning Guide: 6.12

Note for Tutor: Answers may differ from those supplied in the SLG and benchmark. Use your professional judgement to assess if the student's responses satisfactorily meet the knowledge requirements.

Tutor Use Only

Successful ☐ **Unsuccessful** ☐ **Date:** Click here to enter a date.

Tutor Feedback:
Click here to enter text.