

University of Wales

Trinity Saint David

Antoci Bianca

1817784

MODULE CODE/ COD Y MODIWL: ACCC5003

NETWORK OPERATING SYSTEMS AND SECURITY

Security Policy and Management

Observational Tasks

Table of Contents

Observational Tasks 1	2
Observational Tasks 2	6
Observational Tasks 3	7
Observational Tasks 4	9
Observational Tasks 5	11
References	13

Observational Tasks 1

A).

“Benefits of using Type 2 Hypervisor Virtualisation software.” [11]

This type of hypervisor is known to run on a conventional OS. They abstract the guest OSs from the host OS. It is also called a hosted hypervisor.

Benefits

- It provides an emulator environment in order to run another OS.
- The operating system entirely takes care of all the hardware components.
- Installation is quite easier as compared to type 1 hypervisor [1].

Strengths and weaknesses of the VirtualBox.

Strengths

- VirtualBox offers a good testing platform where you can test upgrades, server deployment rollouts, client environments etc.
- It has the ability to host a wide variety of platforms i.e. windows, Linux, Solaris etc.
- It offers a great temporary and cheap failover solution.
- In terms of cost, VirtualBox is absolutely free.
- It has a user-friendly interface.
- It has no effect on the host machine
- It supports the latest hardware version.

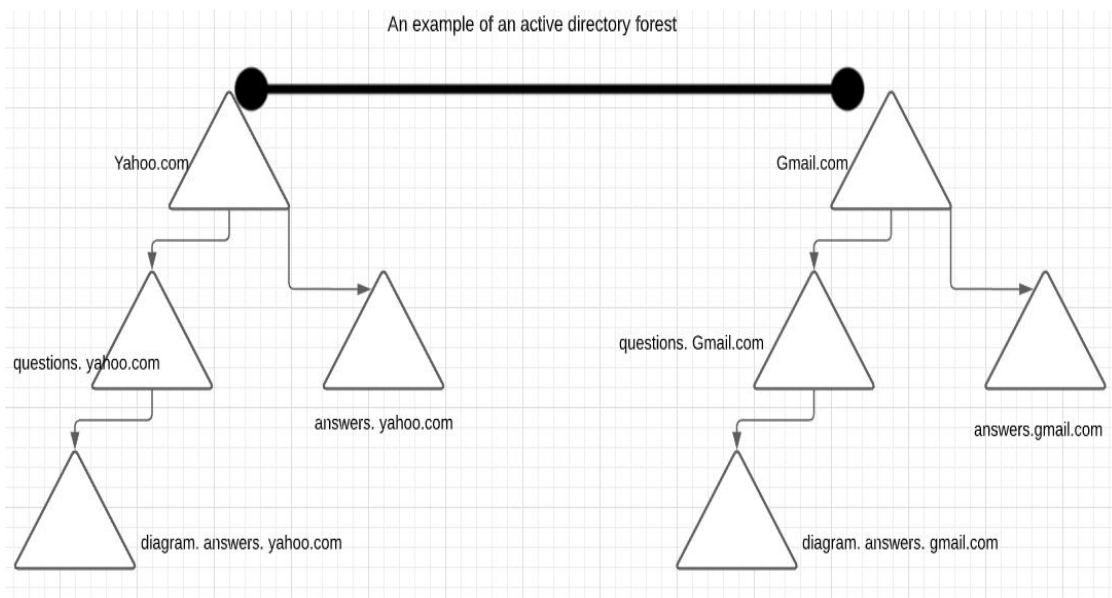
Weaknesses

- It is dependent on the host machine
- Virtual machines running on the virtual box are less efficient as compared to when running on the real machine [2].

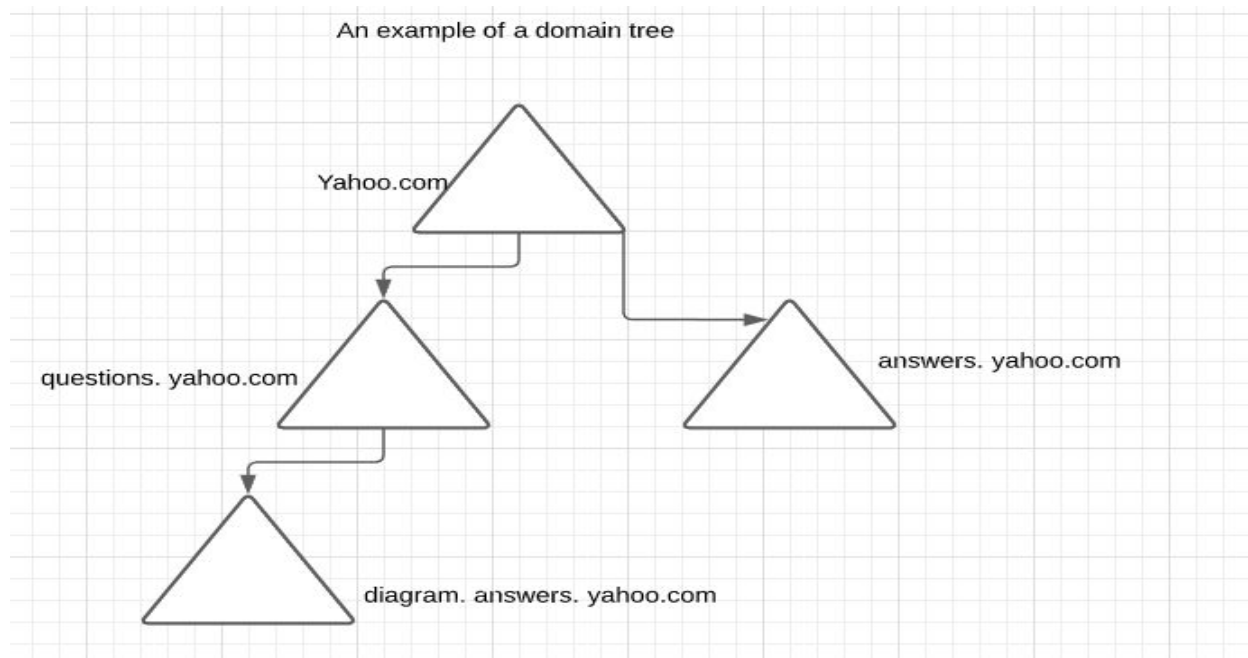
B).

“The significance of the following terms, Active Directory Forests, Trees, Parent and Child Domains.” [11]

- Active directory forests: AD forest is the uppermost level of organization within the AD. The main role of AD forests is to separate active directory trees with specific data and give the right to the user to interact with the data. A forest is basically a set of trees in an active directory.



- Trees- These are hierarchical arrangements of one or more domains that share contiguous namespace. Objects that are in different domains communicate with each other using trusts. If both domains communicate to each other, it is referred to as two-way trust and if only one domain is communicating, it's a one-way trust.



- Parent domain-it is a domain whose DNS forms the basis of subdomains referred to as child domains. It is definitely a top-level domain. Child domain- it is simply a subdomain in the active directory. Child domains are used by organizations to separate departments.

C).

“Main roles and responsibilities of an Active Directory Domain Controller.”

[11]

- It organizes all the domain's data in a logical data store
- It provides authentication of users and provides responses to queries concerning network objects.
- It makes the changes to directory information.
- It Stores and manages directory data.

Actions taken in the event a Domain Controller becomes unavailable.

- ❖ This can be solved by adding or changing the registry entry.
- ❖ Fix any existing DNS errors.
- ❖ Ensure that the time is correctly synchronized between domain controllers
- ❖ Reset the account password, then obtain a new Kerberos ticket.

Observational Tasks 2

A).

“Minimum password complexity requirements:” [11]

- ❖ The password must be at least 8 characters long. In which, it must comprise uppercase and lowercase letters and special characters.
- ❖ Passwords may not contain the user's account name or the entire full name since both checks are not case sensitive.
- ❖ Authentication or password hints should be avoided at all costs.
- ❖ Regular checks on known bad passwords to mitigate risks.
- ❖ Implementation of throttling to reduce the issue of failed authentication attempts [3].

B).

“Advantages and disadvantages of using Groups in Active Directory Advantages.” [11]

- ✓ There is a centralized location for all configurations needed.
- ✓ There is also increased productivity since users are not restricted to one single work computer [4] .
- ✓ All configurations settings are automatically hence saving on time and costs.
- ✓ There is an increase in security.

Disadvantages

- ✓ It can be expensive.
- ✓ High maintenance costs.

- ✓ Prone to attacks

Observational Tasks 3

A).

“Two different types of permissions in use within windows network environments.” [11]

Permission is a method in which users are given access rights to specific user accounts. It basically means controlling access to some network resources.

Types of permissions:

- a) NTFS permissions-they are applied to every file stored on a volume that is formatted using the NTFS file system. Permissions are inherited from the root folder to the files. These permissions are always available on every registry, file or folder. They are known to offer good control to resources in our systems [5].
- b) Share permissions-These type of permissions are only applicable to shared folders. They apply to a folder particularly shared and its contents.

B).

“Benefits of the NTFS File system in comparison with other network operating system’s file systems.” [11]

- ❖ NTFS file system provides security to files as compared to FAT 32.
- ❖ It is compatible with several operating systems.
- ❖ NTFS allows you to optimize your hard drive especially during partitioning [6].
- ❖ It also increases memory capacity.

- ❖ NTFS also allows quick access to external devices e.g. USB drives etc.
- ❖ It is also easier to configure.

C).

“Benefits of using groups in an Active Directory domain.” [11]

- ❖ They grant access to data by assigning permissions.
- ❖ With the use of groups, the active directory is well maintained.
- ❖ Security is enhanced.
- ❖ All configurations are done at a central point.

D).

“Benefits of using Group Policy and Organizational Units to manage a domain’s resources.” [11]

Group policy:

- ✓ Allows you to manage computers centrally.
- ✓ They grant access to data.

Organizational units:

- ✓ Are used to organize and manage objects in the active directory efficiently.
- ✓ They are also used to delegate administrative control.
- ✓ They deploy the settings of the group policy object.

Observational Tasks 4

A).

“Advantages of using the DHCP service in network infrastructures.” [11]

- DHCP as a service assigns an IP number automatically to the computer that requests it. The following are some of the advantages of using DHCP service;
- DHCP reduces the time that is needed to configure and/or reconfigure computers in a network.
- Since it assigns IP addresses automatically, configuration errors are avoided. It prevents the issue of address conflicts that occur when the same IP address is assigned to two computers mistakenly.
- DHCP eases data transmission from different devices [7].

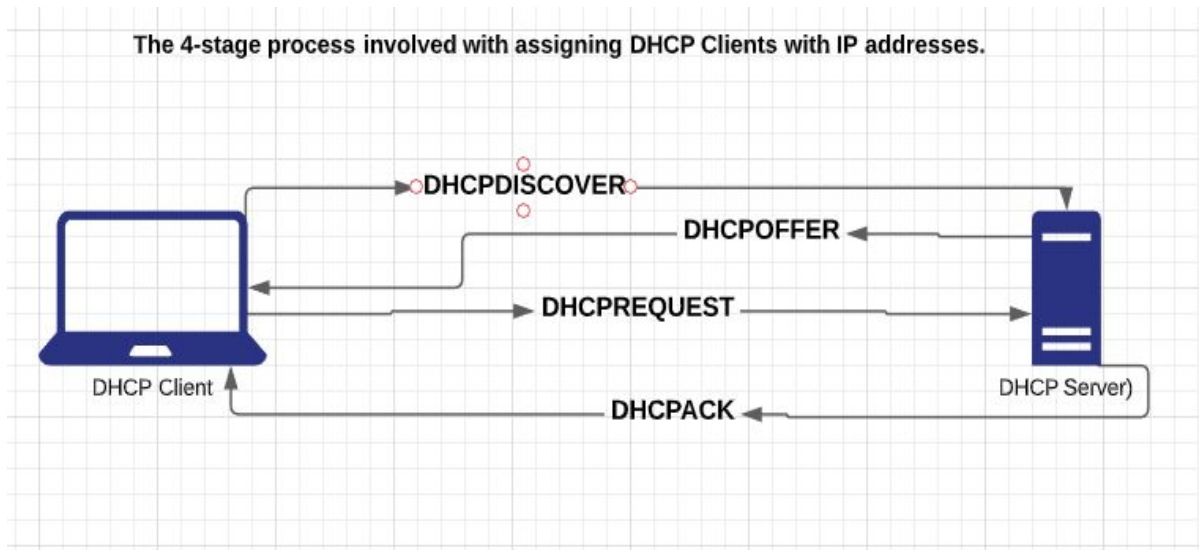
B).

“The 4-stage process involved assigning DHCP Clients with IP addresses.” [11]

In this scenario, a client requests an IP address, and the DHCP server serves the request. This is the procedure:

- i. DHCPDISCOVER**-A new client when connected to a network broadcasts the DHCPDISCOVER message to the network. The DHCP server on the other end will return a DHCPOFFER message to the client that requested it.

- ii. **DHCPOFFER**-the client will receive several DHCPOFFER messages from multiple servers but it will choose a specific message.
- iii. **DHCPREQUEST**-This message is basically sent as a response to the DHCPOFFER showing that the client has recognized the configuration of the network that was sent in the DHCPOFFER message.
- iv. **DHCPACK**-This is the message sent by the DHCP server due to DHCPREQUEST that was sent by the client. This is the last process. It is an acknowledgement by the DHCP server.



C).

“Potential threats/dangers that could occur when using a DHCP service.” [11]

- DHCP starvation attack- This is a case where an intruder exhausts the space available for addresses to the DHCP servers [8].
- Sniffing and reconnaissance attacks.
- Denial of service attacks.

Observational Tasks 5

A).

“How the Recursive Query and Iterative Query Processes resolve DNS Client Requests.” [11]

In recursive query, the DNS client necessitates the DNS server to give a response to a client with the resource requested or if not, returns an error message. If the DNS server is not in a position to give a requested resource, it will forward the query to other DNS servers until an answer is given or definitely the query fails.

Iterative query is where the DNS client permits the DNS server to give the best answer based on the zone data. In a scenario where an answer to your query is not available, it will absolutely give a referral to another DNS server which might have an answer.

B).

“The significance of root hints and how it resolves names that are not managed.” [11]

Root hints are defined as DNS data that are stored in a DNS server. Root hints are known to:

- Prepare servers that are authoritative for non-root zones in order to learn authoritative servers managing domains that are at a higher level or in other subtrees.

- Root hints can also be used by the DNS service in locating other DNS servers which are very authoritative for the root of the domain namespace tree [9].

C).

“How the Domain Name System breaks up FQDN into Host and Domain Namespace.” [11]

- i. The exact FQDN for this host is **subcontA.nwtraders.msft**
- ii. The host will be **subcontA** and the domain namespace is **nwtraders**

D).

“How DNS Zones are used in DNS.” [11]

DNS zones are used to host the DNS records for a specific domain. They are portions of the DNS system. Therefore, if you want to make changes to the DNS records of a particular domain, you need to first edit the DNS zone file. DNS zones therefore provide an easier method of putting together domain data from several domains for storage [10].

For easy management and convenience, it is good to keep all the records of a particular domain in the same DNS zone.

References

- [1] Bari, M. F., Boutaba, R., Esteves, R., Granville, L. Z., Podlesny, M., Rabbani, M. G., ... & Zhani, M. F. (2012). Data center network virtualization: A survey. *IEEE Communications Surveys & Tutorials*, 15(2), 909-928.
- [2] Eder, M. (2016). Hypervisor-vs. container-based virtualization. *Future Internet (FI) and Innovative Internet Technologies and Mobile Communications (IITM)*, 1.
- [3] Desmond, B., Richards, J., Allen, R., & Lowe-Norris, A. G. (2019). *Active Directory: Designing, Deploying, and Running Active Directory*. " O'Reilly Media, Inc."
- [4] Blezard, D. J., & Marceau, J. (2016, November). One user, one password: Integrating Unix accounts and active directory. In *Proceedings of the 30th annual ACM SIGUCCS conference on User services* (pp. 5-8).
- [5] Parkinson, S., & Crampton, A. (2016). Identification of irregularities and allocation suggestion of relative file system permissions. *Journal of information security and applications*, 30, 27-39.
- [6] Vangoor, B. K. R., Tarasov, V., & Zadok, E. (2017). To {FUSE} or Not to {FUSE}: Performance of User-Space File Systems. In *15th {USENIX} Conference on File and Storage Technologies ({FAST} 17)* (pp. 59-72).

- [7] Gedia, D., & Perigo, L. (2018). A Centralized Network Management Application for Academia and Small Business Networks. In *Information Technology in Industry Journal* (Vol. 6, No. 3, pp. 1-10). ITII.
- [8] Lin, C., Su, T., & Wang, Z. (2018, October). Summary of high-availability DHCP service solutions. In *2011 4th IEEE International Conference on Broadband Network and Multimedia Technology* (pp. 12-17). IEEE.
- [9] Allman, M. (2019, November). On Eliminating Root Name Servers from the DNS. In *Proceedings of the 18th ACM Workshop on Hot Topics in Networks* (pp. 1-8).
- [10] Krzywonos, T., Hyatt, R. N., Brown, P., Dehterov, D., & Meyer, S. P. (2019). *U.S. Patent No. 10,250,555*. Washington, DC: U.S. Patent and Trademark Office.
- [11] University of Wales, Trinity Saint David, "Network Operating System and Security(ACCC5003_LON)"[Online].
Available:<https://moodle.uwtsd.ac.uk/course/view.php?id=3760>