Scanning Activity

1. **How many hops from your machine to your assigned website?**

Fisher (2023) defines a hop as the number of routers a packet goes through from its source to its destination. Each router a packet passes through increases the hop count, which can potentially slow down the network. To improve network performance, it's essential to minimise the hop count. However, a lower hop count doesn't always translate to faster connection speed, as other factors like network congestion and bandwidth limitations can also affect performance. With the advent of edge computing, the significance of hop count has been reduced. To determine the number of hops from my computer to a website, I have used the tracert command on Command Prompt in Windows. Regarding pamperedpets.org.uk, my computer took around ten hops to reach the link: pamperedpets.org.uk.

```
C:\Users\hcham>tracert pamperedpets.org.uk

Tracing route to pamperedpets.org.uk [68.66.247.187]
over a maximum of 30 hops:

  1     1 ms     1 ms    <1 ms  SkyRouter.Home [192.168.0.1]
  2     3 ms     3 ms     3 ms  2.127.238.242
  3     9 ms     9 ms     8 ms  02780f25.bb.sky.com [2.120.15.37]
  4     9 ms     9 ms     8 ms  02780d4d.bb.sky.com [2.120.13.77]
  5     *        *        *     Request timed out.
  6    15 ms    15 ms    15 ms  adm-bb2-link.ip.twelve99.net [62.115.137.235]
  7    15 ms    15 ms    15 ms  adm-b10-link.ip.twelve99.net [62.115.120.229]
  8    15 ms    15 ms    15 ms  a2hosting-ic-370345.ip.twelve99-cust.net [62.115.145.217]
  9    14 ms    14 ms    14 ms  69.48.138.11
 10    31 ms    19 ms    13 ms  68.66.247.187.static.a2webhosting.com [68.66.247.187]

Trace complete.
```

2. **Which step causes the biggest delay in the route? What is the average duration of that delay?**

Network delays and variations are crucial performance metrics for many wide-area network applications. Understanding the causes and effects of network delays is critical to achieving better network performance guarantees. Factors contributing to

significant changes in network performance include network topology changes and traffic fluctuations. Predicting the impact of these factors on network performance can enable valuable applications such as proactive mitigation against performance degradation and performance-sensitive route selections (Pucha et al. 2007).

Hart (2021) states that network delays can arise due to various factors such as distance, intermediate stations, data loss or corruption, and delays at transmission nodes. The time a packet travels from one end of a communication link to another is known as latency, which comprises propagation, transmission, queuing, and processing delays. It can use the ping command to assess delays and determine the route taken by the data packet. Although queuing and processing delays are typically addressed in data communication implementations, this may lead to additional transmission delays.

According to Frontier (2022), latency is the delay between a sender and receiver or between a user's action and the corresponding response. A low-latency network is ideal as it ensures a good connection even when large amounts of data are being sent. Although the internet speed should move at the speed of light, factors like refraction and distance may cause latency to increase. Different types of connections have other latency times, with fibre having a typical latency of 10-12ms, DSL with 11-40ms, Cable with 13-27ms, and Satellite with 594-612ms. It requires a suitable bandwidth, good throughput, and low latency to ensure good network performance. For instance, latency issues in a network can arise due to DNS server errors, poorly optimised website databases, insufficient memory, poor transmission mediums, multiple routers, wireless disturbances, and heavy online application traffic.

The network delay duration can vary depending on the type of network. For instance, in fiber optic networks, the delay is caused by the time it takes for light to travel through the fiber. The quality of fiber optic cables can reduce latency. In Voice over Internet Protocol (VoIP) networks, latency occurs due to the delay in voice packet transmission. Conversely, operational latency is the total time each operation takes (IR Team, N.D.).

There is a 15 ms delay at the fifth hop in the tracer route to pamperedpets.org.uk.

3. What are the main nameservers for the website?

Every internet-connected device has a unique set of four numbers known as an IP address. To access a website, the domain name must be matched to the IP address of the web server. This is where nameservers come in – they are machines that perform this task. To create a website, we need to set up nameserver addresses so that your domain name points to the server that hosts your website (Domain, N.D.).

```
C:\Users\hcham>whois.exe pamperedpets.org.uk

Whois v1.21 - Domain information lookup
Copyright (C) 2005-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to UK.whois-servers.net...

    Domain name:
        pamperedpets.org.uk

    Data validation:
        Nominet was able to match the registrant's name and address against a 3rd party data source on 25-Apr-2022

    Registrar:
        eNom LLC [Tag = ENOM]
        URL: https://www.enom.com

    Relevant dates:
        Registered on: 25-Apr-2022
        Expiry date:   25-Apr-2024
        Last updated:  14-Apr-2023

    Registration status:
        Registered until expiry date.

    Name servers:
        ns1.a2hosting.com
        ns2.a2hosting.com
        ns3.a2hosting.com
        ns4.a2hosting.com

    WHOIS lookup made at 23:00:56 23-Nov-2023
```

The main names for the website pamperedpets.org.uk are:

Name servers:
    ns1.a2hosting.com
    ns2.a2hosting.com
    ns3.a2hosting.com
    ns4.a2hosting.com

4. Who is the registered contact?

```
C:\Users\hcham>whois.exe pamperedpets.org.uk

Whois v1.21 - Domain information lookup
Copyright (C) 2005-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to UK.whois-servers.net...


    Domain name:
        pamperedpets.org.uk

    Data validation:
        Nominet was able to match the registrant's name and address against a 3rd party data source on 25-Apr-2022

    Registrar:
        eNom LLC [Tag = ENOM]
        URL: https://www.enom.com

    Relevant dates:
        Registered on: 25-Apr-2022
        Expiry date:   25-Apr-2024
        Last updated:  14-Apr-2023

    Registration status:
        Registered until expiry date.

    Name servers:
        ns1.a2hosting.com
        ns2.a2hosting.com
        ns3.a2hosting.com
        ns4.a2hosting.com

    WHOIS lookup made at 23:00:56 23-Nov-2023

--
This WHOIS information is provided for free by Nominet UK the central registry
for .uk domain names. This information and the .uk WHOIS are:

    Copyright Nominet UK 1996 - 2023.

You may not access the .uk WHOIS or use any data from it except as permitted
by the terms of use available in full at https://www.nominet.uk/whoisterms,
which includes restrictions on: (A) use of the data for advertising, or its
repackaging, recompilation, redistribution or reuse (B) obscuring, removing
or hiding any or all of this notice and (C) exceeding query rate or volume
limits. The data is provided on an 'as-is' basis and may lag behind the
register. Access may be withdrawn or restricted at any time.

Connecting to ame:...
No such host is known.
```

The registered contact is Enom (https://www.enom.com).

5. What is the MX record for the website?

```
C:\Users\hcham>nslookup -q=MX pamperedpets.org.uk
Server:   UnKnown
Address:  fd6b:5466:cfcf:0:6ea0:b4ff:fecf:6dc8

Non-authoritative answer:
pamperedpets.org.uk      MX preference = 0, mail exchanger = mail.pamperedpets.org.uk
```

The MX for the website pamperedpets.org.uk is

6. Where is the website hosted?

The website is hosted in A2 Hosting (www.a2webhosting.com)

Reflection

Looking back at the first three units of my studies, I realised that delving deeper into the content of cybersecurity vulnerabilities was daunting. The biggest challenge I faced was discovering ways to penetrate various websites. However, it was a valuable learning experience that has given me a greater appreciation for the importance of cybersecurity measures in today's digital age.

I conducted extensive research to tackle the challenges and carefully evaluated the data from various literary sources. My top priority was ensuring that all the information I gathered was accurate and reliable. I also shared my previous works with my tutor, who gave me valuable insights and suggestions. Such feedback helped me address my issues and overcome any obstacles during the research process. By incorporating these ideas, I created a more detailed and comprehensive work that met all the requirements and exceeded my initial expectations, which I will share on my ePortfolio.

After conducting an in-depth analysis, I identified several trustworthy sources of information that are highly relevant to my assignment. Specifically, I gathered valuable insights on cybersecurity vulnerabilities, website audits, and application audits.

I successfully addressed all the research questions I plan to share in my ePortfolio. I used a reliable and comprehensive methodology to conduct the study, ensuring the information I obtained was accurate and relevant. Furthermore, I critically analysed the research results to understand the findings and their implications better.

I am confident that the information I have gathered will be instrumental in achieving my objectives and delivering a high-quality Vulnerability Audit.

References:

- Fisher, T. (2023). *What Are Hops & Hop Counts?* [online] Lifewire. Available at: https://www.lifewire.com/what-are-hops-hop-counts-2625905.
- Pucha, H., Zhang, Y., Z. Morley Mao & Y. Charlie Hu (2007). Understanding network delay changes caused by routing events. *Performance evaluation review*, 35(1), pp.73–84. doi:https://doi.org/10.1145/1269899.1254891.
- Hart, G.V.D. (2021). *Networking delays: A Hands-on experience.* [online] Ubble. Available at: https://www.ubble.ai/networking-delays-a-hands-on-experience/ [Accessed 23 Nov. 2023].
- Frontier (2022). *What is network latency and how do I fix latency issues?* Available at: https://frontier.com/resources/what-is-network-latency.
- IR Team (N.D.). *Network Latency - Common Causes and Best Solutions | IR.* [online] www.ir.com. Available at: https://www.ir.com/guides/what-is-network-latency.
- Domain (N.D.). *What is a Nameserver | Domain.com.* [online] Available at: https://www.domain.com/help/article/what-is-a-nameserver [Accessed 23 Nov. 2023].