**Collaborative learning forums**

The collaborative learning forums cover the following learning outcomes**:**

* Identify and analyse security risks and vulnerabilities in IT network systems and determine appropriate methodologies, tools and techniques to manage and/or solve them
* Design and critically appraise programs and systems to produce solutions that help manage and audit risk and security issues
* Gather and synthesise information from multiple sources (including internet security alerts & warning sites) to aid in the systematic analysis of security breaches & issues
* Articulate the legal, social, ethical and professional issues faced by information security professionals

**Discussion 1**

The initial post can be found in: <https://www.my>course.co.uk/mod/hsuforum/discuss.php?d=256232

**The response I received from : my peer** Arunanthy (2021) **:**

**“***Anum, thank you for highlighting an essential feature to prevent Denial Of Service (DoS) attack – firewall. Firewalls can be configured to allow the specific addresses to communicate with the network by whitelisting the particular IPs and network addresses. In addition, network administrators can use Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) solutions to monitor traffic and block known malicious and prohibited traffic (Canadian Centre for Cyber Security, 2020).*

*Also, network administrators can implement several monitoring tools to monitor unusual network movement. These monitoring tools can alert administrators when there is a significant increase in traffic relative to the company baseline or any suspicious traffic overloading a network.*

*Security training, including information related to various DoS attacks and details about services that can be utilised to identify the attacks effectively, is critical to address the risks associated with DoS attacks.*

*Reference:*

*Canadian Centre for Cyber Security. (2020) Protecting Your Organization Against Denial of Service Attacks (ITSAP.80.100). Available from: https://cyber.gc.ca/en/guidance/protecting-your-organization-against-denial-service-attacks-itsap80100 [Accessed 16 May 2021].”*

**The response I received from : my Tutor** Khan (2021) **:**

“Two security threats were discussed in this research paper, the first one being ‘Brute Force Attack” and the second one “Denial Of Service”. Glisson et al, 2015)

Hi Anum,

Glad that you brought up these two issues that are highlighted in the case study. I would be nice to have a bit more critical reflections on the other challenges and how they can be mitigated. Maybe you can mention a couple of more threats and ways to overcome those challenges.

Regards,

Nawaz”

The response I gave to a peer: (Nova, 2021)

*“I agree with your point about it is essential for smart hospitals to ensure that is protected from cyber threats.*

*As technology is increasing, Hospitals are using more and more technology which gives an advantage to cyber criminals.*

*Study shows that the healthcare department is incurring data breaches for the tenth year in a row. The healthcare department out of other departments such as energy, entertainment, industrial have achieved the highest cost of data breach; 7.13 million dollars. (Ibm.com, 2020)*

*Reference*

*Ibm.com. (2020). Cost of a Data Breach Study. [online] Available at: [Accessed 26 July 2021].”*

**The summary response can be found in:**

https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=267253

Discussion 2

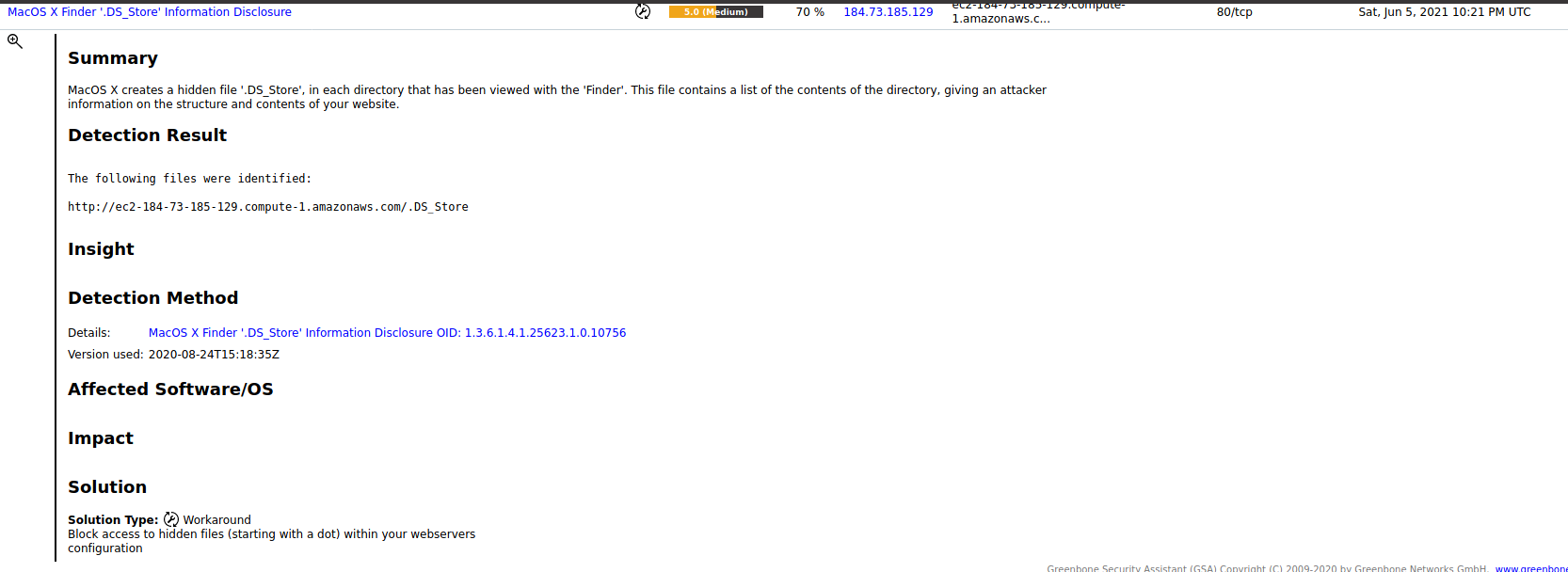
The initial Post can be found in: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=267231

**Summary:**

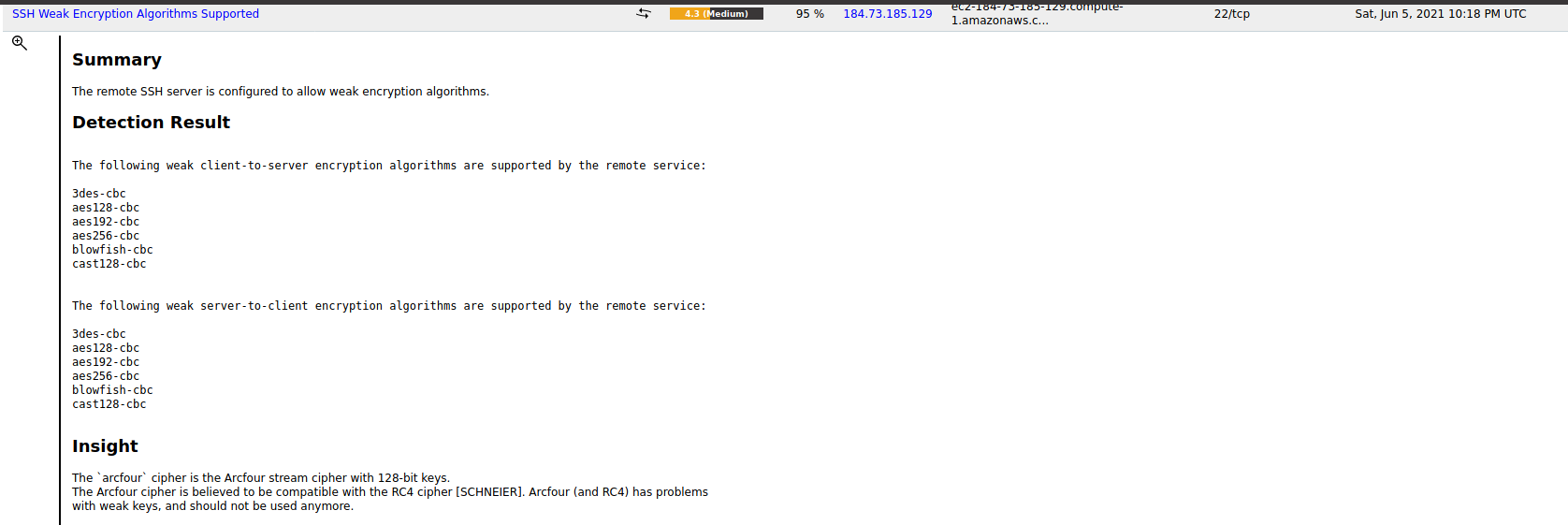
As a summary OpenVAS tool offers vulnerability scanning. I tested out the tool on the IP address 184.73.185.129.

The useful information found by carrying out this scan was that Port 22 (TCP) revealed an enabled SSH service and Port 80 (TCP) revealed vulnerability regarding access to hidden files/ folders.

The great feature about this tool is that it provides mitigation actions for the specific vulnerability:



As for the information disclosure vulnerability the solution for it was to block access to hidden files.





As for the weak encryption vulnerability, the mitigation action was to disable the weak encryption algorithms.

Overall, this specific vulnerability tool proved to generate fast results, it was easy to use as a beginner, and it was easy to repeat the scan if I wanted to. However, research suggests that vulnerability scanning tools can sometimes miss vulnerabilities. This becomes a huge advantage to hackers as they realise that the tool does not find all the vulnerabilities so they could use this to their advantage and exploit that specific vulnerability which was not found in the scan results (Fonseca et al., 2007).

On the other hand to tackle this issue we can use multiple scanning tools for example Nmap, Test SSL etc, as maybe one scanning tool will pick up a vulnerability which the other has not.

Reference

Fonseca, J., Vieira, M. and Madeira, H., 2007, December. Testing and comparing web vulnerability scanning tools for SQL injection and XSS attacks. In *13th Pacific Rim international symposium on dependable computing (PRDC 2007)* (pp. 365-372). IEEE.

**Discussion 3**

**The initial post can be found in**: <https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=267051>

**The response I received from** : my peer Murerwa (2021) **:**

*“Thank you Anum for detailing your case study.*

*Indeed PTSB failed to keep up with the GDPR regulations and violated article 5- Principles relating to processing of personal data. GDPR Articles as cited by Intersoft Consulting (N.D),  Article 5 explicitly states that personal data shall be:*

*"accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’)"*

*In this case they clearly failed to keep personal data up to date. They also failed to do diligence checks with regards to the lady's' address. It seem apparent that they linked the wrong address based on prior applications. On the new application the old address was not used. However, PTSB linked it mistakenly and ended up disclosing personal data to third parties. This is lack of diligence and integrity on the part of PTSB that can cost even their reputation and clientele.*

*References*

*Intersoft Consulting (N.D) Art 5 -Principles relating to processing of personal data. Available from:*[*https://gdpr-info.eu/art-5-gdpr/*](https://gdpr-info.eu/art-5-gdpr/)*”*

**The response I gave to a peer:** (Nova, 2021)

*“If I was information security manager, to prevent this issue from happening I would make sure that thorough training is provided to the company which details the GDPR issues. Also I would ensure that there are daily reviews to ensure all opt-out requests are completed correctly. “*

**The summary Post can be found in:**

https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=267254