## **1. Does the Report Meet NCSC Requirements?**

The report does a **good job of identifying vulnerabilities**, giving a snapshot of the current security status across the network. It includes an executive summary, detailed lists of vulnerabilities, and clear recommendations for fixing them. This makes it very useful as a **starting point** for improving security.

However, it **doesn’t fully meet the NCSC requirement** for creating a proper baseline that can be used as a reference for future penetration tests. While the report highlights problems and their severity, it’s missing a few key things that would make it a complete baseline:

* There’s **no clear definition of acceptable risk levels** or timelines for fixing issues.
* It doesn’t link findings to **compliance standards** like Cyber Essentials, ISO 27001, or NIST, which are important for aligning with best practices.
* It lacks **trend data or historical comparisons**, so it’s hard to track progress over time.

**What I would change:**

1. **Set clear metrics** – for example:
   * The percentage of systems that should be fully patched.
   * Targets for how quickly vulnerabilities should be fixed based on severity.
2. **Add a risk matrix** to show which systems are most critical and the potential business impact if they are compromised.
3. **Include compliance mapping** so findings directly connect to regulatory requirements.
4. Provide **visual dashboards or trend charts** to make progress easier to track and communicate.

These changes would make the report more than just a list of issues — it would become a **living baseline** that teams can use to measure improvement over time.

## **2. Two Best Lessons or Examples**

**a. Clear and Actionable Security Policies**  
One of the strongest parts of the report is its focus on **password and account management best practices**.  
It gives straightforward recommendations like:

* Enforcing password history.
* Setting minimum and maximum password ages.
* Lockout policies to prevent brute force attacks

Sample-Vulnerability-Assessment…

.

These are simple steps, but they have a **big impact** on reducing risk and align perfectly with NCSC’s advice.

**b. Prioritized Remediation Strategy**  
Another highlight is how the report shows that **fixing just 9 hosts** would resolve **20% of all vulnerabilities**

Sample-Vulnerability-Assessment…

.

This kind of prioritization helps teams focus on **quick wins** first, rather than getting overwhelmed by the sheer volume of issues. It’s practical and helps organizations make immediate progress.

## **3. Two Things That Could Be Improved**

**a. Too Much Technical Detail Without Context**  
While it’s great to see thoroughness, the report is packed with very detailed information like dozens of specific patch numbers and updates (e.g., KB IDs).

* For technical teams, this is helpful.
* But for managers or executives, it’s **overwhelming** and hard to see the bigger picture.

**Improvement:**  
Group findings by business impact or system type, and move highly technical details to an appendix.

**b. Lack of Visual Summaries**  
The report is almost entirely text and tables.  
Adding **charts, graphs, or heatmaps** would make it much easier for stakeholders to:

* See which areas are most vulnerable.
* Track progress over time.
* Understand the urgency of different issues.

Visuals make it far easier to communicate with non-technical audiences.

## **4. Reflection**

**Challenges I Faced:**  
The biggest challenge was working through the **large amount of technical detail** in the report. With so many vulnerabilities and patches listed, it was easy to get lost and lose sight of the main issues.

**How I Overcame Them:**  
I started by focusing on the **executive summary and methodology** to get a high-level understanding first.  
Once I had a clear picture of the overall situation, I dug into the detailed sections to connect the dots.  
This top-down approach helped me make sense of the report without getting overwhelmed.

**Impact on My Final Report:**  
This experience taught me how important it is to **balance detail with clarity**.  
In my own reporting, I will:

* Provide clear, visual summaries for managers and decision-makers.
* Include technical details in appendices for IT teams.
* Define **baseline metrics** so future scans can easily be compared to today’s results.

This way, the final report will be both **actionable and easy to understand**.

## **Summary Table**

|  |  |
| --- | --- |
| **Question** | **Humanized Answer** |
| Does it meet NCSC baseline requirements? | **Partially.** It’s a strong starting point but needs baseline metrics, compliance links, and trend tracking to fully meet NCSC standards. |
| Best lessons/examples | 1. Practical password and account security policies. 2. Smart prioritization showing how fixing 9 hosts solves 20% of issues. |
| Could be improved | 1. Reduce overwhelming technical detail for non-technical readers. 2. Add visual charts and summaries. |
| Reflection – main challenge | Processing too much technical data at once. |
| Reflection – solution | Started with the high-level summary, then worked into the details. |
| Reflection – impact on final report | Include visuals, clear summaries, and defined metrics to make the report actionable and easy to track. |

## **References**

* PurpleSec Vulnerability Assessment Report

Sample-Vulnerability-Assessment…

* NCSC Cyber Essentials: https://www.ncsc.gov.uk/cyberessentials
* NIST Cybersecurity Framework: <https://www.nist.gov/cyberframework>