Executive Summary:

- Who contracted and what they wanted to be accomplished
- The gameplan going in and what focuses there were at the beginning
- EX: What particular aspect was put on extra emphasis. Emphasis on gaining access? Emphasis on finding as many workable exploits as possible?
- What was the type of access that you started with? Could anyone with access to internet do this? Did you have to be on site to gain access?
- Was this an overt test or covert?

Summary of results:

- What was discovered from reconnaissance? How many IP's were there to break into to? What did it tell you about the IP's? Were there any blatantly obvious vulnerable OS's?
- Which IP's were you able to gain access to? Briefly explain what the vulnerability was and what you got from exploiting it? Did you brute force it?

Attack Narrative:

- Introduce in depth, step-by-step how you gained access to each system. Were there any similarities between different systems?
- Which ports were vulnerable, what were they running, what version?

Conclusion:

- Describe what vulnerabilities led to the gaining of access
- Restate the goals of the pen test
- Were those goals met?
- Explain how everything connected

Recommendations:

- What were the vulnerabilities?
- What were the exploits used?
- How could they be fixed?
- If passwords were reused for anything then they could only use each password once