Peer review Group 1 by Group 8

Summary

This report is about DDoS attacks on gaming servers. The problem owner was found after analyzing their dataset, which was all about DDoS attacks on servers. By investigating the attacked ports, this group was able to choose a problem owner. The chosen problem owner is the gaming community and the report describes which strategies this problem owner can utilize in order to minimize the effect of DDoS attacks on their servers. Risk accepting and avoidance are quickly dropped, the other strategies (mitigation and transfer) are further analyzed. In the next chapter, the other actors in the field are discussed. The only other actor was the internet service provider, which has more options to block DDoS attacks. At last, the ROSI is calculated for implementing a DDoS protection service and the conclusion is: gaming service providers enjoy mitigation techniques. Afterwards, a one sentence reflection on the usability of the data is given.

Strengths

- Inventive way to choose a problem owner after analyzing your dataset. This makes the choice for your problem owner very clear.
- Interesting port research
- Normalizing your data by dividing attack length between port is a good solution to normalize your data
- Good and understandable written

Major issues

- Your references are below standard. There are way too much statements missing relevant references. Some examples:
    - "Although roughly 4.3 billion addresses are possible, roughly 0.5 billion are set aside for internal use and other purposes, leaving us with only 3.8 billion usable addresses." → no source or explanation
    - "For some vulnerabilities there is virtually no cost" → which vulnarabilities?
    - Further investigation reveals that also port numbers over 65 thousand have been used, possible because the attacker was only interested in bandwidth, and not valid responses. → On what is this based? Pure guessing?
    - Every number in your ROSI calculation is based on nothing, not even a small comparison. In this way, your calculations can not be replicated by other in order to check whether you did a good or a bad job in calculating ROSI.
- The problem owner is wrong. Your problem owner is a gaming company, not the gaming community. The community involves companies, players, press etc.
- Accepting the risk is dropped down too quick. As a gaming company, some amount of DDoS attacks have to be accepted. One can never block it all. The way you drop this strategy in just own sentence is too short and needs more explanation.

Minor issues

- No page numbering, table numbering sometimes missing, no chapter numbering.
- "And now we see that only 0.03% of 'the internet' has fallen victim to a DDoS attack" → what is "the internet"? And why did you write it down like this?
- Finally, for the data regarding domain names, all attacks on more than 10 domains at the same time have not been taken into account due to performance considerations. → What kind of performance considerations? Which performance?
- Strange thing about the ports. Since the memory space for port addresses is 16 bit long, only 65.536 ports can be accessed, but this group mentioned more ports and did no research in finding out why.
- In your actor analysis, some other actors are missing, like the gamers (the users). There are way more actors in the field than just the gaming companies and the service providers.
- At the end of your ROSI calculation, the results aren't presented in an organized way. Just make a simple table and it will be more clear to the reader what you've just calculated.

Small errors

- The dollar sign should be on the other side of the number. So not 8$, but $8.