Performance:

P1 – DOS

P1.1 – TODO

P2.2 – Run brute force on Small (which returns a 10 KB file) with a very high number requests and then see the RTT of other requests. Test the RTT of three requests from a different source and take the average.

P2.3 – TODO

P2.4 – Limit the number of simultaneous transactions from a particular IP and port address

P2.5 - TODO

P2 – Large File Requests

P2.1 – TODO

P2.2 – Run brute force on Big (which returns a ten MB file) and Small (which returns 10 KB file). Check the average response time after running it for 60 seconds.

P2.3 – TODO

P2.4 – Prioritize the easier, faster files in order to improve average response times

P2.5 – TODO

Availability:

A1 – DOS

A1.1 – TODO

A2.2 – Run brute force on Small (which returns a 10 KB file) with a very high number requests and see if the system is still available for other users

A2.3 – TODO

A2.4 – Limit the number of simultaneous transactions from a particular IP address

A2.5 - TODO

A2 – Server Throttled to Death

A1.1 – TODO

A2.2 – Run brute force on Large (which returns a 10 MB file) with a high enough rate that it will entirely throttle the server. Determine the downtime.

A2.3 – TODO

A2.4 – Have the server automatically restart in order to minimize downtime.

A2.5 - TODO

Security:

S1 – DOS

S1.1 – TODO

S2.2 – Run brute force on Small (which returns a 10 KB file) with a very high number requests and see if the system is still available for other users

S2.3 – TODO

S2.4 – Limit the number of simultaneous transactions from a particular IP address

S2.5 - TODO

S2 – Data Source Integrity

S2.1 TODO

S2.2 Run important requests without any way of knowing originator

S2.3 There is no real quantitative metric for this one. It doesn’t have the information before and it will after.

S2.4 Create a logging system that logs requests in order to keep track of who is responsible for different requests.

S2.5 – TODO

Tactics

Limit open sockets for ip and port

Prioritize smaller files

Watchdog reset

File log