# Advanced Security Lab4

One type of attack that can be mounted against a system is the NTP amplification which is a type of DDoS attack. This attack the attacker exploits the public Network Time Protocol servers to overwhelm the user under attack UDP traffic. The most basic version of this attack is the attacker repeatedly sends the “get monlist” to the NTP server while spoofing the requesting servers IP address to the victim’s server. The NTP server will send back a list of spoofed IP addresses. This response is considerably larger than the request and this will amplify the amount of traffic. This will inhibit the server from getting legitimate requests.

Another form of attack is replay attack. Replay attack occurs when an attacker records protocol packets and repays them without amendment. This form of attack only occurs when the time of the message was change this will get the system out of sync. This will cause a massive influx of security issues as everything in the system uses the clocks.

Rogue Master Attack occurs when an attacker tries to lead other network nodes to identify it as master by manipulating the BMC algorithm. The rouge master attack does not falsify the identity of the node but can manipulate the mater election process with malicious control packets.

Packet interception and removal is another form of attack. This attack occurs when protocol packets are intercept and removed by an MITM attacker and the destination node is prevented from receiving some or all the effect packets.