Term Project – Report 1

Yansong Li
B00755354

Project mode: Blue and Red team defense and attack Game

Blue team: Target network with services in GNS3
Red team: Kali VM

Experiment time: Nov 29th to Dec 10th

1) Nov 29th to Dec 3rd: Red team attack blue team with no security set-up on blue team.
2) Dec 6th to Dec 10th: Red team attack blue team with as secure as possible set-up on blue team.

Environments:
Blue team:

1) Service: **Web service** in a small enterprise.
2) Generation of normal traffic:
   a) Automatic traffic generation using Ostinato.
   b) Manual traffic generation with web browsing using Firefox browser.
3) Defense tools:
   a) Access Control List on Cisco router to filter network traffic.
   b) Snort (Intrusion Detection System) associated with FRR router for detecting probes and attacks.
   c) PFsense/OPNSense Firewall.

Red team:

1) Penetration tools:
   a) Nmap for scanning blue team.
   b) Nessus for vulnerability assessment of the blue team.
   c) Metasploit for exploiting the vulnerabilities of the blue team found in scanning.
   d) Deny-of-Service attack for flooding the blue team with traffic.