Mini Project Progress Review #1

Project Title	: MOOC on IDS using Snort	
Project ID	: MP1702	
Project Guide	: Prof H.B Prasad	
Project Team	: R Siva Girish	PES1201700159
	Gaurav C.G	PES1201700989

Project Abstract and Scope

- MOOC for intrusion Detection with Snort.
- Aim to help beginners learn Snort freely and elegantly by providing them with the right resources.
- Step by step analysis of concepts explained.
- By the end of the mooc every beginner should be able to write their very own snort rules.
- Learners should be able to recognize attacks and prevent them using Snort.
- Snort is an open source software and highly used by industry professionals.

Further Literature Survey

- **Papers/References Studied**
  - Snort Manual(Version Specific)
  - Snort2.1 Intrusion Detection by Jay and Caswell
  - Advanced Intrusion Detection using Snort, Apache, MySql, PHP and ACID
  - Managing Security with Snort and IDS tools
  - Comprehensive Guide on Snort (Part-1) - Hacking Articles

User Characteristics

- Most of our customer base will be involving beginners who have no prior knowledge about Intrusion Detection Systems.
- The MOOC would necessarily be covering all prerequisites as well as in depth explanation of concepts covered.

Dependencies / Assumptions / Risks

- Usually performing intrusion detection on any network is computationally very expensive.Hence IDS is installed on a dedicated host.
- For testing purposes systems must be capable of running preferably 2 virtual machines at the same time.(Both Kali Linux and Ubuntu seed labs).
- Risks include the complexity of the attack being detected.The more complex the attack the more harder it is to monitor packets and automatically flag the operation as an attack.

Technologies Used

- ❖ Snort is an open source network intrusion detection and prevention system.
    - ➢ An IDS is a tool that monitors network traffic as well as analyses network packets from the log files of routers, firewalls and servers.
- ❖ We will be using a packet generator to generate packets of data(maybe nping/Scapy - TBD)
- ❖ Use of Kali Linux for better understanding of attacks.
- ❖ Use of seed ubuntu(lite version of ubuntu) as a defending machine.

Thank You