**CSCI 3250**

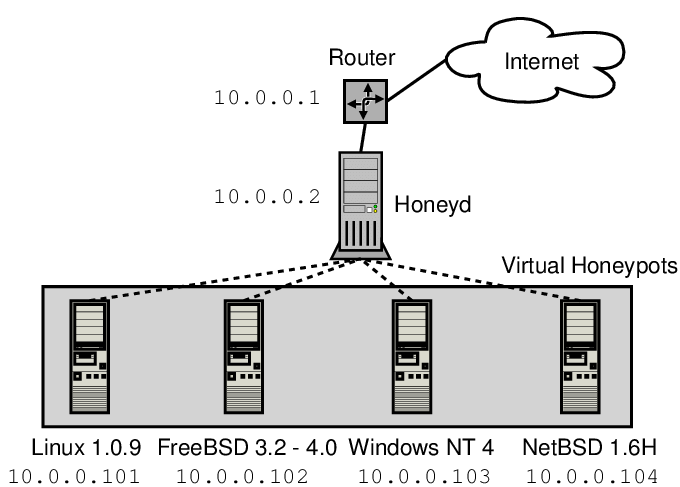
**Group Assignment 36**

**Honeypot**

**Member Present: Sylas Sun, Eros Hernandez**

For this assignment explain features of your assigned topic in a reader-friendly manner. Use bulleted text for each feature item.

Group 2: Virtual Honeypots

1. Definition:  
   A virtual honeypot is a simulated IT system or network designed to attract and deceive malicious actors, allowing organizations to study their techniques and intentions without exposing real assets to risk. The concept ‘virtual’ means it refers to simulation achieved via software-based technology rather than utilizing physical hardware to actually build one.
2. Methods:  
   Some tools that are used for virtual honeypot is Honeyd, Allows the user to create a virtual Honeypot which can emulate service attacks. Kippo is a tool that records the action of the attacker like brute force. Honeydrive is a tool that makes it easy for the user to deploy a Honeypot environment.   
   
3. Behavior:  
   Like how other honeypot techniques function, the goal of virtual honeypot is the same: lore out the attacker, distract them from critical assets, and examine the record/trace of intruder using computer forensic in order to learn their techniques and intention without actually exposing core assets to the risk or taking any damage from the attack.
4. Vulnerability:   
   Honeypot vulnerabilities can occur if it’s misconfigured. Attackers who are experienced can recognize patterns that honeypots use: This is the vulnerability existing in all honeypot techniques-- if the hackers are able to identify the target being a honeypot, it instantly loses all its meaning and nothing will work.
5. Potential user/environment application:  
   Due to the complexity of setting up a virtual honeypot (it can be more difficult sometime due to the fact that it does not have a corresponding physical hardware), this type of technique usually being used by:  
    1. Cyber defense research & training institutions

2. Intrusion detection & prevention in technical advanced company  
 3. Deploy as deception and misdirection in critical infrastructures  
