Grading Sheet for CEG 4420

Root Kits

Weight 5% Instructor: Prabhaker Mateti

Student	LoginID	Bonus	Points

Item description	Max	Points
Full Name, email address, WSU UID, Gandalf ID shown	05	
M1: Build / Install two rootkit detection packages D1, D2 on M1 (Knoppix or Kali/BackTrack)	2*5	
M2: Boot into Knoppix or Kali. Console login as root. Create a new user named "intruder". Remain logged in as root through out this Lab.	10	
Ssh to M2 as user "intruder". (i) Dowload+build a rootkit R, (ii) corrupt M2 with a rootkit R. If necessary, become root (well known for Knoppix, and trivial in Kali). Make further use of the machine M2. Be creative.	10	
Describe the activity of user intruder you (as root) were able to observe with standard Linux utilities, both before and after R was installed.	10	
Download from M1 the rootkit detection packages D1 and D2. What does D1 detect? What does D2 detect?	2*5	
Suppose you are the attacker. What changes would you make to M2 so that these rootkit detection tools become ineffective if they were downloaded and built on M2 instead of M1?	10	
Write a shell-script and a report on how you would clean M2 up.	10	
Make this lab "real": Discuss the elimination of the role of M1, and the "help" of root in building/installing R. Assume that the "intruder" is a legitimate but ordinary user (whose password was compromised).	10	
Overall quality (your explanations in addition to cut-n-paste's) of the Lab Report	15	
Total	100	