Grading Sheet for

CEG 4420/6420: Host Computer Security

Sniffing and Probing

Weight 5%

Student	LoginID	Bonus	Points

Item description	MaxPts	Points
Acceptable Lab Report structure	10	
Setup a network of P0 to P3. Configure P1 and P2 as routers under BackTrack. Boot P0 into Windows, P3 into Knoppix.	10	
Setup and start ssh, http, nfs, samba services, one each on the four machines.	10	
Sniff (on P1, e.g.) using sniffit; include 5 selected packets	5	
Sniff (on P1, e.g.) using a sniffer other than sniffit; include 5 selected packets	5	
the six capabilities exercised/determined.	10	
Choose, build and install from http://packetstormsecurity.org/ an anti-sniffer.	10	
Evaluate how effective the anti-sniffer is.	10	
Descriptions of Windows/BackTrack/Knoppix services modified/misconfigured	5	
Install a firewall on Windows P0. Configure the firewall carefully. Describe the configuration.	5	
Start `nmap` on P1. Probe all ports on P0, P2, and P3. Record, and annotate later, the firewall + nmap output.	10	
Analysis of discoveries made by `nmap`	10	
Bonus Points: Capture relevant packets and explain how nmap identified the OS of P0, P2, and P3	10 B	
Total	100	