Infosec 1 **Network Security: Configurations + CTF** **Nov. 12, 2014**

Firewall/NIDS Configurations

- Packet filter only

Benefits	Drawbacks

- Dual-homed gateway (______________________________)

Benefits	Drawbacks

- Screened Subnet (_______________)

Benefits	Drawbacks

Placement of NIDS Sensors (use DMZ diagram)

Location	Benefits	Drawbacks
1.		
2.		
3.		
4.		

CTF Overview

Network Diagram

Services

Flags

CTF Project: The CTF include four parts

Pre-CTF (30% of your grade):

- Learn some Web security basics
- Practice basic skills on hackthissite.com

First week:

- Get into teams, find out about your technical strengths.
- Each person focuses on a different service, one person on system security and logs
- Understand the services on your image and how the flag server can plant and check for flags.

First week and on your own:

- Examine your image for vulnerabilities that can be exploited to get flags.
- Modify vulnerable software to prevent other teams from getting your flags.

CTF! During lab, Dec. 1-4 (participation is 10% of your grade):

- Keep your services running so that the flag server scores you as being available.
- Watch for attacks from other teams. Hint: you can learn from them!
- Get flags from other teams and submit them for points.
- Stay within the spirit and letter of the rules or you will lose points.
- Grab screen shots and keep notes of key moments, prepare your report

Report (one per team, broken out by person):

- 1-2 pages (more with screen shots and/or code)
- What you contributed, focused on
- Key details of any exploit/vuln.

Report Grading: 50% of CTF grade

- Graded on Technical Skills Demonstrated: 90%, Report formatting and quality: 10%
- Grade is 80% individual and 20% team average.

Team Presentations: During our Final on Dec. 10, 2:00-4:30 PM. 10% of CTF grade

- Graded on Findings/Technical Skills: 30%, Slides/Preparation: 40%, Clarity: 30%
- Show your team’s best stuff overall, not one thing from everybody.