

ECE6612 Network Security Class Competition Fall 2005

Abstract

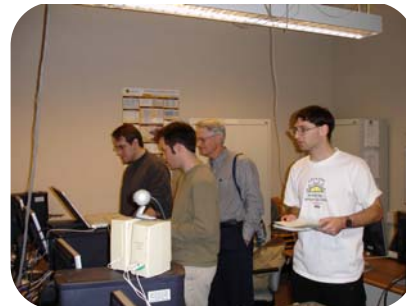
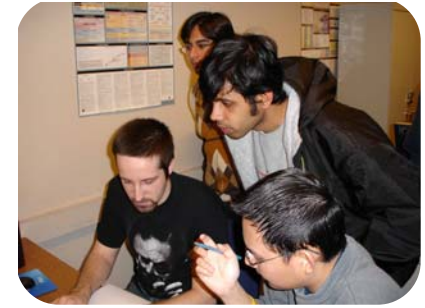
The purpose of this exercise was two fold: hardening a default installation of Redhat Linux and compromising other computers on the lab's network. Points were assigned according to the level of compromise teams were able to achieve on other computers.



Points

Points were assigned based upon level of compromise each team was able to accomplish. Points were awarded for:

- Mapping the network (2 pts. per IP address)
- Mapping services (20 pts. per box)
- OS detection (10 pts. per victim box)
- Gaining user access to victim box (30 pts.)
- Gaining user access to a team box (50 pts.)
- Gaining root access to a victim box and retrieving the shadow hash file (150 pts.)
- Gaining root access to a team box and retrieving the shadow hash file (250 pts.)
- Time bonus: Additional points were awarded if all of the above goals were accomplished between:
 - 0 to 5 minutes: 200 points
 - 5 to 10 minutes: 150 points
 - 10 to 15 minutes: 100 points
 - 15 to 20 minutes: 50 points
- Not having all services (ssh, telnet, smtp, www, mysql, samba) up: -150 points
- If another team compromised your team box: -300 pts



Rankings

Team	Points	Root
Bears	1698	5X
Jackals	1576	5X
Wolverine	968	3X
Gators	882	3X
Badgers	410	3X
Tigers	92	0X

