CS393/682 - Network Security - Lab Assignment 6
War Games

Summary:
In this Lab you will use all that was learned throughout the semester to protect machines assigned to you and to attack machines of other groups. In fact, you will function as Red Team as well as Blue Team and you’re free to figure out the logistics of your group.

Pre-Lab:
You have until Friday 2nd, May 2003 17:00HRS EST to secure your machines. The Game starts at 17:01 and lasts until Thursday 8th, May 2003 17:00HRS. You are not responsible for attacks after that deadline. In fact, no team will get points for attacks performed after the deadline.

Rules of Engagement:

1. By Friday 17:00hrs EST you each team MUST have the following services running on their machines
   a. telnet, ssh: there must be a normal user called “tiger” with password “trigger” on your machines AND there must be a guest user with password guest.
   b. A web server. You can put your teams, name whatever on the web site.
   c. An FTP server, with anonymous ftp enabled.
   d. You must run a mail transfer agent, like Sendmail on standard SMTP port.
   e. Needless to say these service must be accessible from anywhere in ASSET

2. By Friday 17:00hrs all teams MUST email your root password to Kulesh (kulesh@isis.poly.edu) with the team name and IP address of corresponding machines.
3. Do not attack any machines until you get an email from Kulesh on Friday. Team found guilty will be penalized.
4. Once you get the “go a head” you are free to use any means necessary to compromise the machines of other teams and protect your machines from being compromised.
5. NO Network Flooding tools are to be used as means to compromise or bring down a system. Team found guilty of using any network flooding tool will be penalized heavily. (Note this doesn’t rule out other denial of service mechanisms, for example Land Attack.)
6. All teams MUST run the required services at all times. Graders will be scanning the network very often and teams found not running any service will be penalized. Also teams that find missing services can report their discovery to Kulesh.
7. When you compromise a machine, take a screenshot of the following items:
   a. Output from ifconfig
   b. Output of date
   c. /etc/passwd AND /etc/shadow (if you want to prove root compromise)
Reports:
Your reports are due on May 11th at 17:00hrs, no late handins and no electronic handins. Include the following in detail in your report:

1. What did you do to secure your machines?
2. How did you find the vulnerability, how it was exploited? and include appropriate screenshots.

10.1.x.x