CYBER DEFENSE COMPETITION

Competition Scenario

IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER
Spring 2008

You are an employee of your local University supporting a research team being deployed to Antarctica that is on the verge of making a ground-breaking discovery regarding the magnitude and effects of global warming. The research for this project is being kept as secret as possible, as its leakage could enable competitors (other Universities) to make the discovery first, or motivate others to sabotage the team and its resources to keep them from making the discovery. For this reason, your team's top two priorities are: availability of the systems and security of the data.

Your team is being deployed ahead of the research team to establish a secure technological infrastructure needed for the station to operate. You will not have physical access to your station until you arrive on February 22. The station will need to be set up remotely so it is ready to go live upon your arrival. You will have a low-latency satellite internet connection provider, which will contain a class C IP range block (4 of the addresses will be reserved).

The station requires the following services:

A web server at www.stationN.iastate.edu, where **N** is your team's assigned number. The website itself will be given to you for you to inspect and load on your webserver.

An email server at mail.stationN.iastate.edu with IMAP and SMTP access. The web server will need to have a webmail interface added to it so that users can access their mail without a mail client.

A name server at ns1.stationN.iastate.edu (and possibly a second at ns2.stationN.iastate.edu) to resolve stationN.iastate.edu host names for the outside world. The Station Commander (White Team) will need the IP of this machine as early as possible. Please point your DNS to to resolve all unknown addresses to 199.100.16.100.

A password-protected file server for storage of data, reports, and personal files. Users should be allowed at least 10GB of storage on this server. Users should also be able to access this from off-site (i.e., back at Iowa State) via FTP and internally via Windows file sharing (ftp.stationN.iastate.edu).

A password-protected Unix programming environment at shell.stationN.iastate.edu which can compile FORTRAN90, C, and Java programs. This machine must be accessible via Telnet and SSH from offsite. This machine will be preloaded by the research team and given to you to integrate into the network once you reach camp. To avoid stepping on any toes, you need to keep the machine intact (hardware and software-wise), but it would be wise to inspect it for security vulnerabilities.

There will be a kiosk machine in the building which must be able to access all of the above systems. This will be attached via a wired connection to your network. Please provide documentation to be placed at the Kiosk for researchers. This documentation should include instructions detailing how to change your password and how to log onto a variety of services.

You might also want to consider these services (but they aren't required):

> Intrusion Detection System: Due to the controversial nature of the research team's work, you must assume that your networks will be attacked to attempt to steal information or sabotage ongoing work. Therefore, it might be wise to deploy a system to watch for intrusions so you can report them and respond appropriately. Remember that attacks can also come from the inside.
>
> Firewall(s): To protect your networks from attack, you might want to deploy one or more firewalls to restrict network traffic.

From time to time you will be host to a variety of other researchers and sponsors which your University has given the okay to access your networks, in addition to the dedicated research team. You will be given a list of authorized users and their passwords. You may not change these passwords, but you may encourage the users to change their passwords if you feel it is necessary. Note that these passwords must work for the web, mail, shell, and file servers. If the password is changed, you must provide directions to be sure that it still works in all of these places.

You may use any software that is free of cost, site-licensed to Iowa State, or available to students. You may not use any software for which Iowa State does not have rights to use (this excludes software you or another individual have created yourselves). You may not add hardware of your own to the network, but you may request additional hardware from the Station Commander (White Team). Additionally, one of: file server, web server,DNS server or mail server must be run on an Operating System from the list of legacy operating systems (see the rules document). However, you may patch these systems as you see fit. You must also have at least one Unix machine (i.e., BSD, Linux, Mac) and one Windows machine.

You will be given remote access one month ahead of your arrival. You will need to provide detailed network documentation to the Station Commander (White Team Leader) the time you show up for the competition. This should include network diagrams, lists of which services are running on which operating systems (and versions), IP addresses, and any other information you feel helps demonstrate the competency and preparedness of your team.

It is expected that all services be operational by the time you arrive. If news of their arrival and what their research may discover is leaked to the press, their first night at camp could be an exciting one for you...