CYBER DEFENSE COMPETITION

Competition Scenario

IOWA STATE UNIVERSITY, INFORMATION ASSURANCE CENTER
FALL 2007

You are an employee of Iowa State 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 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 now to establish a secure technological infrastructure needed for the station to operate. Currently the research team has set up a simple network, which works but lacks security. The research team will be maintaining two camps, each of which is of equal importance to the project. Camp 1 has already been set up by the research team which is already present making discoveries. You will not have access to Camp 1 until you arrive on December 1. Camp 2 will need to be set up remotely so it is ready to go live upon your arrival. For redundancy, each camp will have a different low-latency satellite internet connection provider (and thus different subnets). Each subnet 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, with both a public and password-protected portion so that status updates can be posted. 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.
>
> 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.
>
> 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 from both camps 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 both camps and offsite.
>
> A Wireless access point so that researchers can connect their personal laptops to your network. There is an outlying building that must be physically isolated from the rest of the camp due to the nature of the research being done there. There will be a kiosk machine in this building that is connected to Camp 1 wirelessly.

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.

Service Scanner: As your networks are physically separate, you might want to deploy an automated system to ensure all of your services are up and running.

Firewall(s): To protect your networks from attack, you might want to deploy one or more firewalls to restrict network traffic.

VPN: To securely interconnect your two camps

From time to time you will be host to a variety of other researchers and sponsors which Iowa State 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. If this is done, you will need to notify the Base Guest Director (Green Team leader) of the change and the new password. Note that these passwords must work for the web, mail, shell, and file servers. If the password is changed, you must be sure that it still works in all of these places.

Your team will be given eight machines – plus whatever has been set up at the second site. You cannot move machines between sites due to the logistics of taking them out in the Antarctic climate. Iowa State has mandated that you distribute services and resources as equally as possible between the camps so that the mission can continue if one camp should be disabled for any reason (loss of power, loss of network connectivity, snowstorm, et cetera). Therefore you must have redundant services at each camp.

You may use any software that is free of cost, site-licensed to Iowa State, or available to students of Iowa State. You may not use any software for which Iowa State does not have rights to use (this excludes software you or another individual own). 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, programming 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) by one week from this time. 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...