Team Exercise #2
Services

Exercise: April 21, 2010
Report Due Date: April 28, 2010

1 Introduction

As you are aware, difficult economic times and an inability to secure additional capital has led to the bankruptcy of ACME Ltd., the leading supplier of rocket-propelled roller skates, quick drying glue, super-magnets, and anvils to the coyote community of the desert southwest. Their troubles are an opportunity for our company to expand; we now plan to expand and develop new offices in New Mexico. Our headquarters will be in Socorro (I-40 west then a left turn at Albuquerque) ; we will have an engineering office in Las Cruces to take advantage of the university there and sales offices in Roswell and Los Alamos.

Because of the difficulty in starting from scratch so far from home, we will form a strategic partnership with one other company. Remember though- they may be partners today, but they may become competitors tomorrow.

Your job is to develop the IT infrastructure for our New Mexico affiliates. Job requirements include:

1. We need a functioning web presence.
   (a) Remember though, that because we are new to the area, the web page must reflect well on us as a company- damage to the web site may irreparably harm our reputation in the area.
   (b) The region's web server will be housed in our headquarters in Socorro.
   (c) We need smaller, more specialized web pages for the engineering and sales offices.
   (d) Our local web team will need to be able to update the web page from various (unknown) remote sites, as well as from our Maryland offices.
2. To better serve the local coyote community, our engineering offices will need to design and test new products.
   (a) We will need to be able to securely share our designs with select area coyotes; should these designs be made public, trade secrets would be revealed.
   (b) Some of our designs need to also be shared with our partner company.
   (c) Appropriate design tools need to be installed.
3. Our sales offices will need to be able to share their insights from client meetings with the engineering group
   (a) We expect that files too large to be sent via email will need to move to and from the sales office sites.
   (b) The regular sales office staff are only familiar with Microsoft products, and insist that they have administrator rights on their machines.
4. We will need to provide the complete network infrastructure for the organization- including DNS and domain controllers.

You need to design the complete architecture, including an estimate of the number and types of machines that will be at each office. Usability of the system is of maximum importance- if we are unable to get our jobs done (design, engineering, sales) you will lose yours. Security breaches are unacceptable, and may cause us to join ACME on the scrapheap of companies that cannot make it in today's competitive economy. Particular attention needs to be paid to the prevention of industrial espionage.

1.1 About the exercise structure

On April 19, you will need to provide to the instructor (by email) two sets of documentation on your infrastructure. One will describe how your own (non-IT staff) employees will access and use the systems, and the second will describe how your partner will do the same. These will be passed to your fellow students, who will judge your systems on their usability.

The "documents" and "designs" described above are not terribly relevant to the exercise; certainly their content is not. However, appropriate samples need to be created in whatever format you feel fits the simulation. The same holds true of the web site- reasonable facsimiles of a real site need to be provided, but only so that the exercise has a whiff of realism, no more. You need to provide a list of the documents designs you have created, and who should be allowed to access them; this list also needs to be provided on April 19. Remember- not every employee should be allowed to access every document. Authorized users who cannot access their files or unauthorized used who can are to be avoided.

2 Before the exercise

As in previous exercises, a complete machine information sheet should be completed before the start of the exercise.

You will need to describe in detail the structure of your network and the rationales for the choices you made- and it is probably a good idea to do so before the exercise begins.

3 During the exercise

You will be provided with documented access to two other teams- either as a partner or as an employee. Verify that the instructions provided by the other team work, and make some judgment as to the usability of the solution provided.

Try to complete a machine information sheet for all of the machines from the team for which you do not have access credentials. In particular, for each of their machines, try to determine

- The IP address,
- The hosting team,
- The OS, and
- The types and versions of all available services.

Attempt to access your opponent's assets. Their leaked data are your bonus points; the more sensitive the data, the higher the score [No credit is given for access to data to which you are allowed access; for example defacing a web page to which you have authorized write access is valueless]. Access to an opponent's log server or other defensive systems will be granted additional style points.

During the exercise, you need to record the commands that you execute..

Try to cover your tracks as best as you can. The use of arbitrary third party tools may be allowed, at the discretion of the instructor, however all such tools must be approved prior to 4/19. All third party tools will be available for all members of the class.

The use of cunning and guile are encouraged.

4 After the Exercise

Your report will contain three components.

Design and Implementation: Describe the architectural decisions that you made. How did you set up your production systems? What defensive assets did you deploy (log servers)? How were they configured? Why did you make the decisions in this fashion?

Reconnaissance and Attack: For your partner team- were you able to access the data they claimed you should? Were their procedures to access the data reasonable? Were you able to gain unauthorized access to other data?

Similarly, for the team to which you have employee credentials- were you able to access the data they claimed you should? Were their procedures to access the data reasonable? Were you able to gain unauthorized access to other data?

Were you able to determine what services were running on your opponent's machines? Were you able to access any of their information?

Analysis: How well did your network hold up to actual use? Were your employees and partners able to access exactly the data that they should? Were there any security breaches? If so, explain in detail what happened and how.

Remember- as bad as a security breach might be- it is much worse if it occurs without your knowledge!

5 Grading

Your report will be graded out of 25 points. Points will be awarded for the following:

- 5 points for the overall written quality of your report.
- 5 points for the actions you took to prepare your network.
- 5 points for the reconnaissance and attack activities you took during the exercise
- 10 points for your analysis of what took place on your own network.

When teams design their networks, they should use a variety of systems with a variety of servers. Each member of the student team should set up at least one server and should demonstrate that they know how to set up all of the servers of the team.

Accurate record keeping is essential for each team. This includes accurate Machine Information Sheets, and complete Command Summary Forms. Failure to submit accurate records will result in SUBSTANTIAL GRADE PENALTIES- up to half of the final grade.

You have been warned.

The report of the responsibilities and activities of each team member will be used together with the report grade to assign the final grade for each student. If, in the judgment of the instructor different team members made substantially different contributions, then members of the team may be assigned different grades.

5.1 Extra Credit

Extra credit may be awarded to teams who go beyond the minimal requirements for the project:

- (+2 pts) Set up a functioning mail server for your team. To get full credit you must:
  - Provide email accounts and passwords to the instructor and to all students who ask.
  - You must provide instructions on your web page on how users of your email system are to configure their client.
  - Users must be able to successfully send email through your network.
- (+2 pts) Set up a functioning blog server for your team. To get full credit you must:
  - Configure the server appropriately for your network (including some basic content)
  - You must allow authorized users (only) to make a blog post and unauthenticated users to comment on them. Members of your corporate partner are to be considered authorized. Provide instructions to them on how they are to use the system in the documentation you provide on April 19.
  - The functioning system must be demonstrated to the instructor on the day of the exercise.
- (+1.5 pt) Set up a functioning wiki. To get full credit you must:
  - Configure the server appropriately for your network (including some basic content)
  - Exercise participants must be able to add and modify content on the wiki.
  - If authentication and/or authorization is required to add or modify content, then instructions must be ppro-vided.
  - The functioning system must be demonstrated to the instructor on the day of the exercise.

It should be noted that the requirements for full extra credit are necessary and not suffiicent. In particular, even if a team meets all of the requirements they may not receive the full credit because, for example, their write up of how the team set up and configured the additional component is deficient in some way, or because the additional service did not function completely as intended, or even because other teams were able to gain unauthorized access to one or more system components.