# Final Exercise
# Let's go Shopping!

Exercise: May 16 & 18, 2011
Report Due Date: Monday May 23, 2011 at 5:15

## 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 & advertising 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 and avertising offices will need to design and test new products.
   (a) The engineering team has a staff of 20. [You do not need twenty computers, but rather a few (identical) computers with 20 accounts.]
   (b) 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.
   (c) Some of our designs need to also be shared with our partner company.
   (d) Appropriate design tools need to be installed.
   (e) The engineering group also needs to create a number of applications.
      - They will need secure remote access, and the ability to compile and test code. We do not know what machines they will be using when the access our development machines.
      - They will also need access to a web server and a database server for testing purposes that matches our e-commerce site for testing.
3. We need to set up a functioning e-commerce site ; we will use Zen Cart as the underlying base platform.
   (a) The e-commerce site can be housed in one of our offices or at another site, at your discretion.
   (b) To improve our supply chain management, we will allow specific partner companies limited access to the data in our e-commerce site databases.
      - Our partner companies need read access to our customer list, our product list, and our manufacturer list.
      - They are not to have access to any other data; in particular they are explicitly not to have access to our order data.

- Our partner companies will need to have this access to this data from a variety of hosts and locations. I have been told that allowing access from arbitrary locations poses a security risk- please explain how you mitigated this risk, either through appropriate security or by developing an application that controls access. Regardless of the approach, this level of access is key to our company's success, and so failure here is not optional.

4. Our sales offices will need to be able to share their insights from client meetings with the engineering group
   (a) Each sales offices has a staff of 30, and members of one sales office often are temporarily assigned to another sales office.
   (b) We expect that files too large to be sent via email will need to move to and from the sales office sites.
   (c) The regular sales office staff are only familiar with Microsoft products, and insist that they have administrator rights on their machines.
   (d) Each member of the sales office team needs read access to all of the data in our e-commerce site.
   (e) Each sales office needs an internal file server.
   (f) Complete instructions on how to access the e-commerce data must be present on the internal file server. Each member of the sales office team has created a text file on the file share that contains the information that they use to access the database.

5. Our headquarters staff has fifteen people- One VP, a manager for each sales group, a manager for the enginnering group, and IT group manager, five administrators, and a staff of five IT experts.
   - The managers need to have access to both the headquarters computers as well as the computers in their respective offices.

6. We will need to provide the complete network infrastructure for the organization- including DNS and domain controllers.

7. The team needs to provide a complete and appropriate defensive infrastructure- firewalls, logging, and intrusion detection.

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 Sunday May 15, 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; it should include all accounts and password save those for the IT staff and system administrators. 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.

**FAILURE TO PROVIDE THIS DOCUMENTATION ON TIME WILL RESULT IN A LOSS OF 10% OF THE TEAM'S FINAL GRADE.**

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. 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. The Zen Cart web site does not need to be customized beyond the default install, but it should contain a reasonable amount of "dummy" data, especially old customers and old orders.

## 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.

Do some shopping at the e-commerce sites of the other teams. Order yourself something nice.

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. It is imperative that you record your own locations whenever you access a remote system, as this will be used to both check the results of your attack as well ad the reactions of the defense.

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 5/16. 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? How appropriate was your defensive infrastructure design? How was it all configured? Why did you make the decisions in this fashion?

Be sure to describe (briefly) each computer you set up, including its role, name(s), IP(s) and configuration. The student(s) who set up that machine should also be named.

**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.

You should summarize the entire situation, then drill down into the details on each machine.

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