Team Exercise #3

Networks

Exercise: April 11, 2007

Report Due Date: April 18, 2007

You have decided to go into business for yourself, selling the latest techno-widgets.

- Please choose a company name. All of your machine names bust be clearly identified with your company name.

Because the business world is quite competitive, you have decided to form a strategic partnership with one other company.

- Please choose your company's strategic partner.
- Your partner will have access to some of your company's documents that are not open to the general public.

Your job us to begin developing your new company's IT infrastructure. Your business requirements are the following:

- We need a functioning web page.
    - The main web page must be accessible to everyone.
    - Because we prefer working at home to working in the office, we need the ability to update the web site from arbitrary machines.
- Our developers group 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.
    - The development machines will need access to a functioning compiler. They will also need access to a web server and a database server for testing purposes.
    - There are three developers in our group.
- Our product design group will be working closely with our partner company.
    - We need a way to securely share schematics with our partner company.
    - If these schematics become public however, our company will lose quite a bit of money.
    - We do not know the precise IP addresses of our partner company, though we are sure they will be on the subnet 10.0.1.0/24.
    - Once a product is sold to the public, we will need to provide product support information to the public. This will include various large downloadable files.
- We will need to create and manage two databases for the company.
    - *Database #1: Clients.*
        - The clients database will contain information about all of our clients, including:
            - Names

        - Addresses
        - Credit card numbers
    - Access to this database needs to be maximally protected.
    - Access to the database needs to be given to various automated scripts that will eventually run on our webserver. These scripts will allow users to enter and view their information, and later to place orders.
    - Our developers are creating automated administrative tools to let us work with the database. These scripts need complete access to the database, but will only be run from inside our network.
    - The database should be populated with a reasonable set of test data before the start of the exercise.
- *Database #2: Products:*
    - This database contains a list of all of our products, including
        - Name
        - Product code
        - List price
        - Manufacturing cost
    - This is data that we do not want made public. However, we will be sharing this information with our partner company. They will need access to this database.
    - Access to the database needs to be given to various automated scripts that will eventually run on our webserver. These scripts will allow users to enter and view their information, and later to place orders.
    - Our developers are creating automated administrative tools to let us work with the database. These scripts need complete access to the database, but will only be run from inside our network.
    - The database should be populated with a reasonable set of test data before the start of the exercise.
- We also need to set up and create an appropriate defensive infrastructure, including logging server(s), network monitoring (e.g. ntop, ethereal) and intrusion detection systems. Be prepared for all types of reconnaissance attacks, including SNMP walking.

Most of the machines in this corporate network can be re-used for subsequent projects. Be sure to save a snapshot of them ***before*** the exercise begins so that you do not have to re-build them from scratch later.

During the Exercise

Check all of the services offered by your partner company. Are they working? Carefully indicate which services are running correctly and which are not.

Try to complete a machine information sheet for all of the other machines in the room. In particular, for each active machine, try to determine

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

Attempt to access your opponents assets. Their leaked data are your bonus points; the more sensitive the data, the higher the score. Access to an opponents IDS or other defensive systems will be granted additional style points.

During the exercise, you need to complete your command summary sheets.

Try to cover your tracks as best as you can. The use of arbitrary third party tools is now allowed, however all such tools must be approved by the instructor no later than the class on Monday evening. All third party tools will be available for all members of the class.

The use of cunning and guile are encouraged.

After the Exercise

Based on your work, you will write a final report. This report should contain the results of your scans- including machine information sheets for all of the active guests in the room.

More importantly, the report try to ascertain who scanned and/or probed your network, and what they accomplished. If unauthorized users accessed your data, you need to determine how this was accomplished, and detail your findings.