

Lab 1 - Introduction to the Attack Lab

CSE 4481 4.0 Computer Security Lab, Winter 2012

Due: Tuesday , Jan 17th, 2012, 11:59pm

Format: Individual

Learning Objective: To become familiar with the Attack Lab environment, practice configuring a small network, and perform some simple security related tasks.

1 Network Configuration

A small company has decided to deploy a new IT infrastructure. While there are plans to add several workstations in the future, the proposed infrastructure contains only the devices shown in Figure 1.

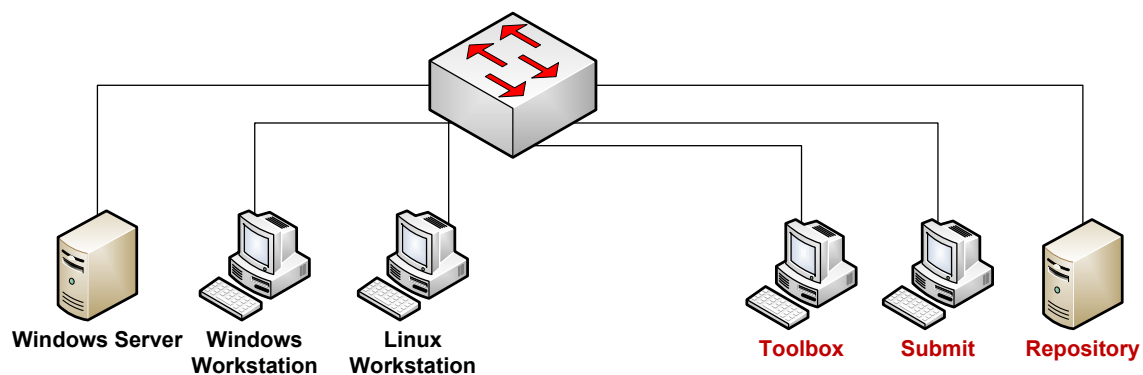


Figure 1: Network Configuration

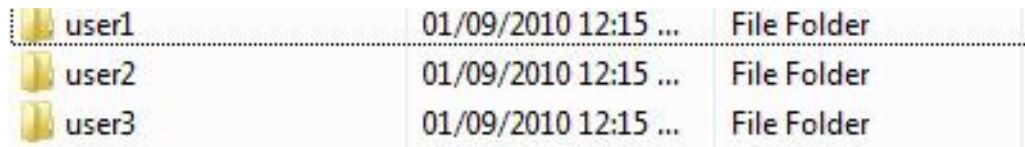
The company office will contain a Windows workstation, a Linux workstation, and a Windows 2003 server. The Windows 2003 server will be a domain controller.

Two users for the Windows workstation must be created in the domain controller. Also, three local users are required for the Linux workstation.

The IT department does not enforce any naming or IP convention. However, they do have the following policies:

1. There must be 50 reserved static IP addresses
2. Workstations are using dynamic IP addresses

3. The routing prefix of the network is $192.168.10x.0/24$ where x is your workgroup number (it will be provided by the instructor).
4. For each Windows user, there needs to be a shared directory whose name is the same as the user name. This shared directory is located on the domain controller in a directory called `public`. Users are allowed to read/write/delete files from their shared directory, as well as read files from other users' shared directories. The shared directories must be protected from being deleted by any non-admin user (advanced feature). An example is shown in Figure 2.



user1	01/09/2010 12:15 ...	File Folder
user2	01/09/2010 12:15 ...	File Folder
user3	01/09/2010 12:15 ...	File Folder

Figure 2: Sample content of the `public` directory

5. The `public` directory mounts automatically when a user logs in any workstation
6. Workstation users should be able to launch executable files in the `<userhome>/pbin` directory.

Your task is to configure and setup the IT infrastructure (the workstations and the server) according to the above specification. Your job is also to develop a suitable IP address schema.

What to do:

1. Design naming and IP schema
2. Configure the Windows 2003 server
3. Verify connectivity of all devices, i.e. every computer must be able to ping all others
4. Promote the Windows 2003 server into a domain controller
5. Verify DNS configuration (name resolving and reverse resolving)
6. Add the Windows workstation into the domain
7. Create the `public` directory on Windows 2003 server
8. Create users

9. Modify user profiles

- Configure auto-mount of the user's home directory
- Configure ability to launch programs from `<userhome>/pbin`
- Configure auto-mount of the `public` directory

10. Verify configuration correctness

The network diagram in Figure 1 contains three more machines: Submit, Repository and Tools. These machines are supplementary for the course. You need to perform the following two tasks: the Repository machine should have a static IP, and the Linux workstation and the Toolbox machine must be configured to download packages from the Repository.

Report: Provide answers to the following questions:

- How did you configure the various computers? Provide appropriate screenshots.
- What documentation did you use to help you with the setup? List the documents you used (with URLs if applicable) with short summaries for each document.
- How did you troubleshoot?
- How did you prove configuration correctness? Include screenshots with connectivity, DNS and pbin test.

2 Security Testing

Once the configuration of the infrastructure is completed, perform the following security tasks:

1. Once an attacker gains control of a machine, they commonly search for files that store passwords in clear text. Your task is to find all files in the Linux workstation that contain passwords by searching for the following keywords: `pass`, `password`, `passwd`. Identify the exact names of all such files. Open each discovered file using `less` to verify the existence of passwords.

Report: Include a list of all password containing files.

2. An attacker often needs to hide files in a compromised computer. For this task, identify two scenarios for the creation of hidden files in Windows OS.

Report: Describe the scenarios in your report

3. Assume that a user has the ability to modify any binary file in the system. Design an attack which gives a root shell to this user. To test your attack, you may use the root account in the Linux workstation to modify binary files.

Report: Describe the attack you designed

4. Assume that you found an application that provides read/write permissions to all users for a file in /tmp, e.g. /tmp/lab1 (without modifying the content of the file). Design an attack which gives root access to any user. Hint: A setuid application can modify the permissions of the /tmp/lab1 file regarding the file owner.

Report: Include the source code of the application (it should be only a few lines of code) and explain the attack

Helpful material

The course website contains several links to documents that should be helpful for this lab, such as protocols (DHCP, DNS and ICMP), and file permission schemas for Windows and Linux. Make sure to consult with them.

The following list of commands (some apply only to Linux) should also come in handy: `find`, `dig`, `nslookup`, `ping`, `ln`, `dcpromo`. Become familiar with them by studying the man pages.

What to Submit

Before the deadline, submit electronically the report you created. To submit, navigate to the directory that contains the report, and give a command like the following

```
submit 4481 lab1 lab1.pdf
```

where `lab1.pdf` is your report.

Also, drop off a hard copy of the report into the CSE 4481 assignment dropoff box located on the first floor of CSEB. The hard copy will be the one to be marked. The electronic copy will be used for record keeping.