5.10.1

INTRUSION DETECTION

(Back Officer Friendly)

Objective

At the end of this lab students will be able to install and use BackOfficer Friendly to detect port scans, as well as connection attempts of servers via telnet, FTP, HTTP, and email. Students will also be able to detect intruders using Back Orifice.

Information for Laboratory

A. Students will use configure BackOfficer Friendly to monitor intrusion attempts.
B. Students will test BackOfficer Friendly by attempting to connect via telnet, FTP, and HTTP.
C. Students will see how BackOfficer Friendly responds to a port scanner.
D. Student will then observe BackOfficer Friendly behave as a Back Orifice server.

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

Estimated Completion Time

60 Minutes

Honeypots

A thief breaks into a home and discovers it is empty. The occupants are away, but there is a savor in the air produced by a meal in a crock-pot, and the contents of a bread machine. Surely he has time to take in a little flounder before taking his loot, unaware that a secret alarm has been tripped.

Another scenario might have the thief notice smudges on a painting frame. The safe behind it is an easy target, but the contents turn out to be worthless. Meanwhile, a secret camera has recorded the event.

Both of these examples illustrate the principle of a honeypot. Network resources are feigned in order to allure an intruder into thinking he is accessing them. While the intruder wastes time exploring insignificant resources, system administrators have time for detection.

Honeypots frequently are in the form of special programs that mimic resources, but not always. For example, an administrator can make a file directory structure that is not difficult for an intruder to access, and which appears to be sensitive data. Buried within the directory structure might be what appears to be a data file of users. While the intruder spends time exploring frivolous, fake resources, he is caught.

BackOfficer Friendly, distributed by Network Flight Recorder™, Inc., is an example of a honeypot mimicking server resources. It can detect hosts attempting to connect via telnet, FTP, HTTP, STMP, and POP3.

Backdoors

A backdoor is an insidious piece of software infecting a host that allows unauthorized access. It's as though the gardener has locked things up, but he has an extra key for the back door. Or perhaps a thief has possession of a special tool or system designed to defeat a certain type of security system.

Any software of this type is considered a virus. Back Orifice is one such tool developed by some nice people at Cult of the Dead Cow. Infected hosts act as a Back Orifice server. Back Orifice clients can gain complete access to the infected machine which can then be completely ruined.

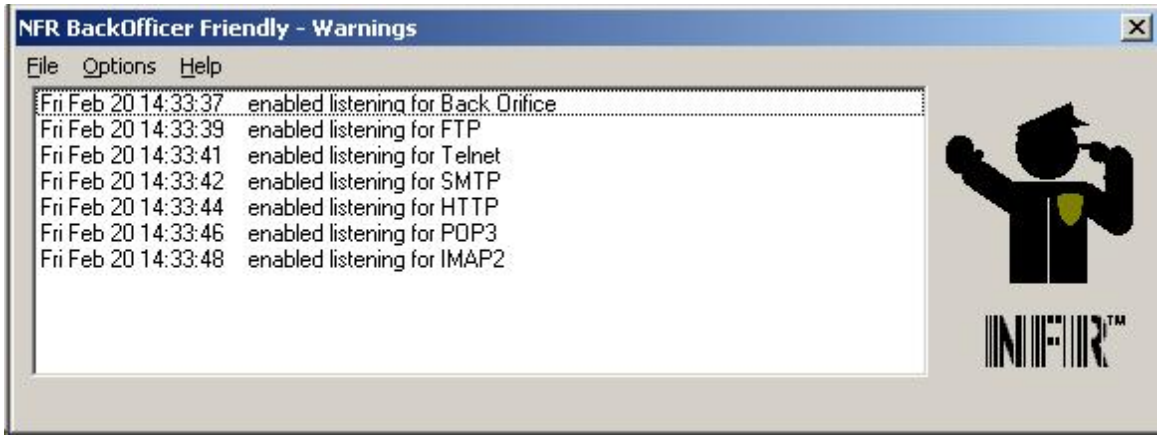
A honeypot can be used to mimic a backdoor virus. This is the case with BackOfficer Friendly, for which the original intent was to detect Back Orifice clients by posing as a Back Orifice server.

Using BackOfficer Friendly

BackOfficer Friendly can detect several different points of attempted entry. This lab is intended to demonstrate most of its capabilities using only two networked computers. Both computers will run BackOfficer Friendly while each attempts unauthorized access to the other. See the Appendix for information regarding installation files.

Step 1:

Execute Nfrbof.exe to initiate BackOfficer Friendly, hereafter BOF. Upon execution, BOF will simply appear on the task bar. Double click the task bar icon to bring up the BOF dialog box. Under the dropdown Options, activate all listen options and fake replies. You should see something like the following graphic:

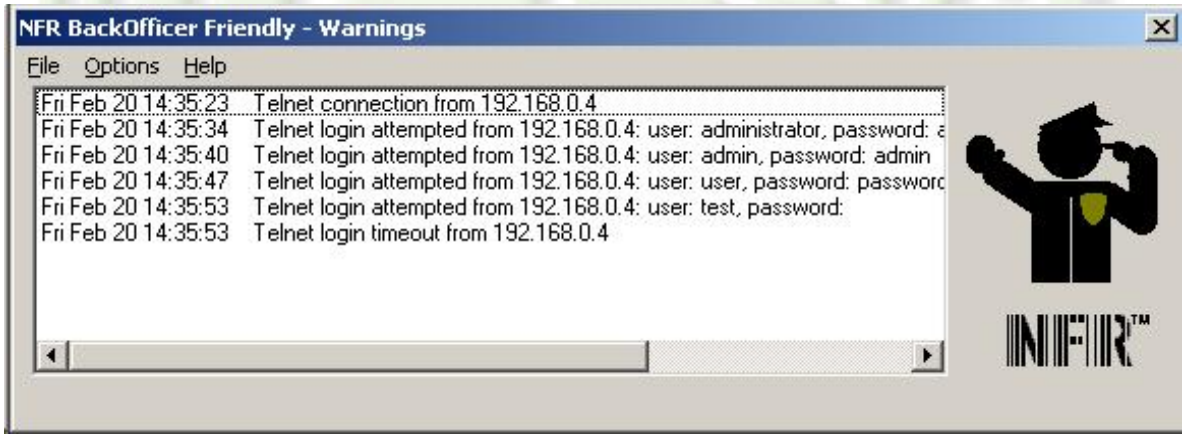


Step 2:

Now that the BOF honeypot is running, use File-Clear on the BOF menus so that any intrusion attempts are easily seen. Next try to telnet to your partner's honeypot. From a command window,

C:>telnet 192.168.0.2

where the IP address should be that of your partner running BOF. Note that BOF responds as if it supports telnet, requesting a login. Attempt to guess a login name and password. Meanwhile, back at the honeypot, BOF should look something like,



Note that BOF tells you the IP address of the intruder.

Step 3:

Clear the BOF dialog box as in the previous step. Taking the role of an intruder, execute a browser such as Internet Explorer. In the address box type the address of the BOF partner. You will probably see an authorization error. Next, type the following in the address:

FTP:\\192.168.0.2

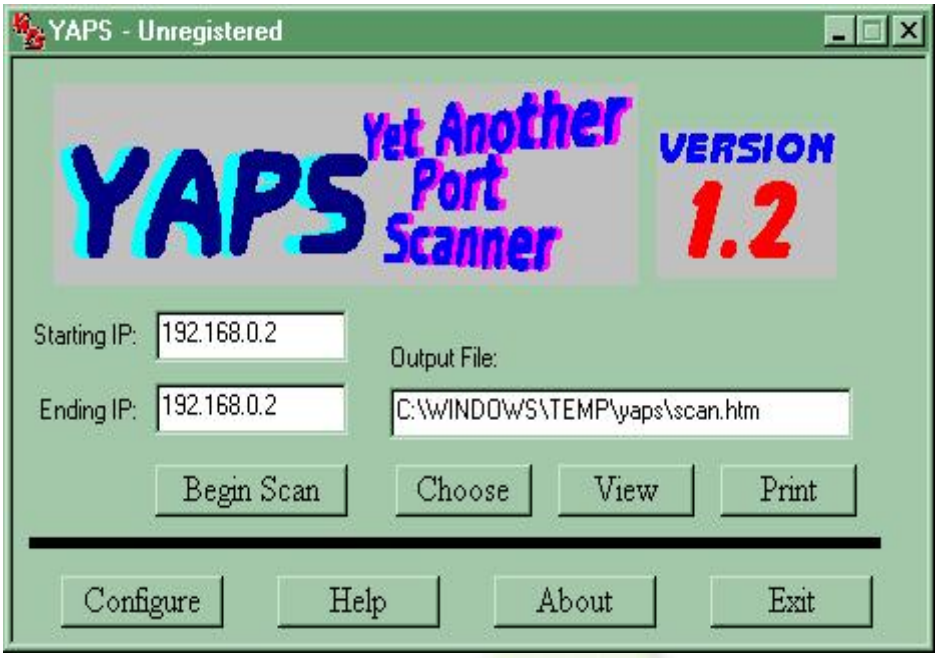
where the IP address should be that of the target BOF computer. This will probably generate an error at the intruder computer. Nevertheless, BOF will record the attempt, and of course the IP address of the source.

Step 4:

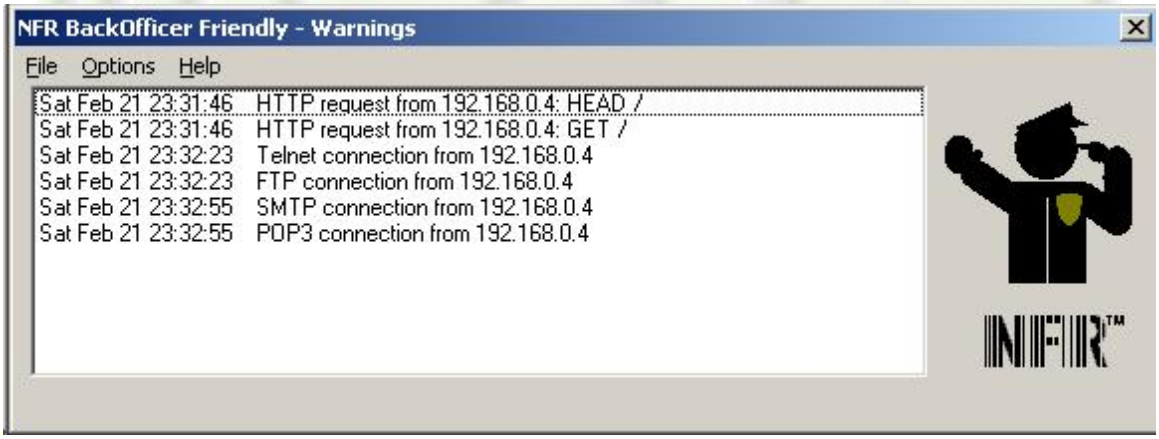
Some intruders may wish to invoke the use of a port scanner to try and see if any UDP/TCP ports are vulnerable. This is a little like a prowler checking around the neighborhood to see if all the doors are locked. There are many port scanners available, and if you have a favorite, by all means use it to scan the honeypot computer. It is best to clear the BOF dialog box prior to the scan. You may wish to restrict the port range to scan in order to save time, perhaps up to 255.

If a port scanner is unavailable, YAPS (Yet Another Port Scanner) may be used. See the Appendix for the location of install files.

To use YAPS, accept the default configuration, and simply insert the target BOF computer IP address for both starting and ending address. An optional output file may be specified, then simply Begin Scan. YAPS will look like,



BOF will respond to several of the scanned ports in accordance to how the options are set.



Step 5:

Unzip Back Orifice into a directory if you haven't already done so. Please keep in mind that a real Back Orifice server is not required for the lab. The file Boserve.exe should **not** be executed, and is best deleted. Virus protection should be disabled, as this will most likely prohibit the client as well. Recall that BOF acts as a Back Orifice server.

To initiate intrusions using Back Orifice, start a Back Office client by executing Boclient.exe which opens a command line window with prompt

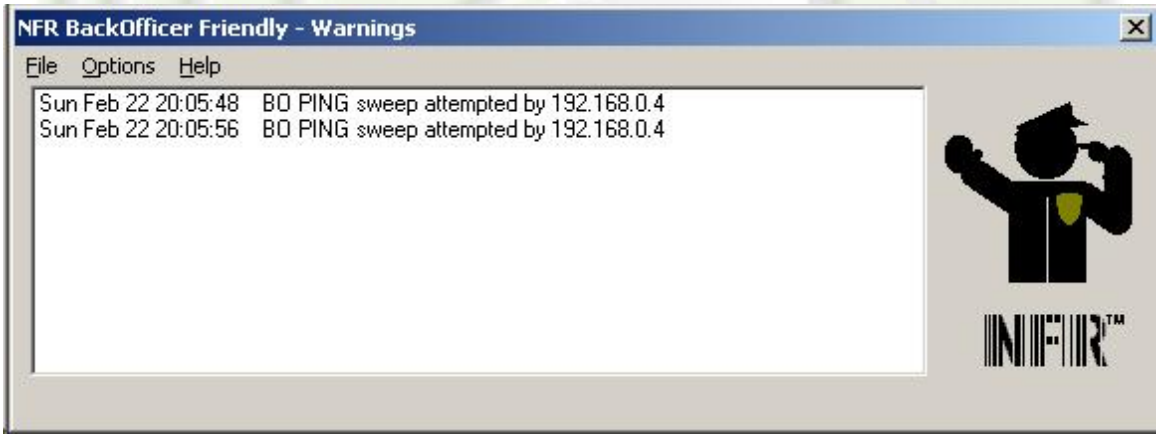
BO>

The default configuration of Back Orifice uses encrypted UDP packets at port 31337. Refer to the file Bo.txt for command details. You may wish to experiment with the GUI client as well by executing Bogui.exe.

Use Back Orifice to sweep your network.

BO>sweep 192.168.0.0

where the appropriate subnet should be used. Back Orifice will think it has discovered Back Orifice servers that have been infected by the Boserver.exe file. In our example host 192.168.0.2 looks infected. BOF will look something like,



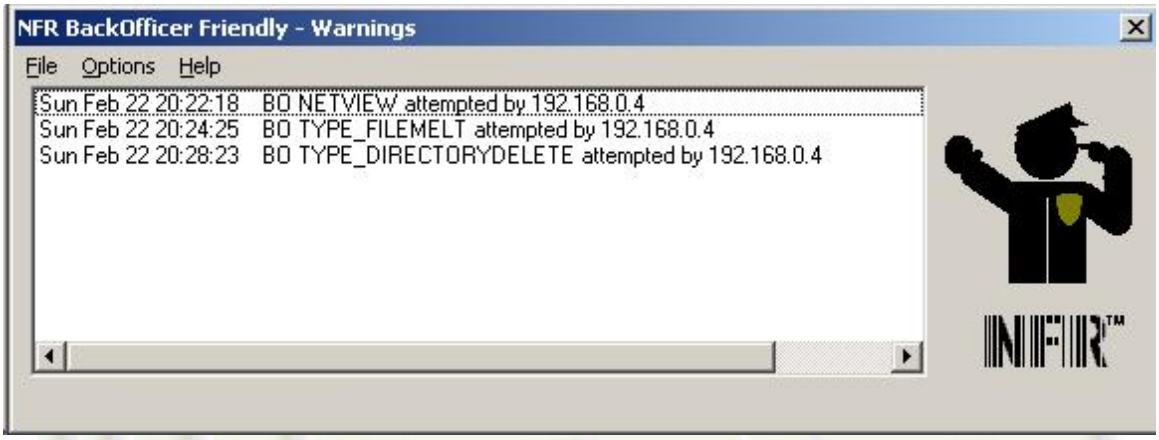
Now the intruder can go into high gear. Execute the following at the Back Orifice client:

BO>host 192.168.0.2

where the appropriate BOF IP address should be used.

BO:192.168.0.2>netview
BO:192.168.0.2>view c:\autoexec.bat
BO:192.168.0.2>rd c:\windows

At the BOF honeypot simulating the Back Orifice server,



Our Officer has recorded someone trying to delete the windows directory on the target machine, and if a real Back Orifice server virus was running, he would have been successful.

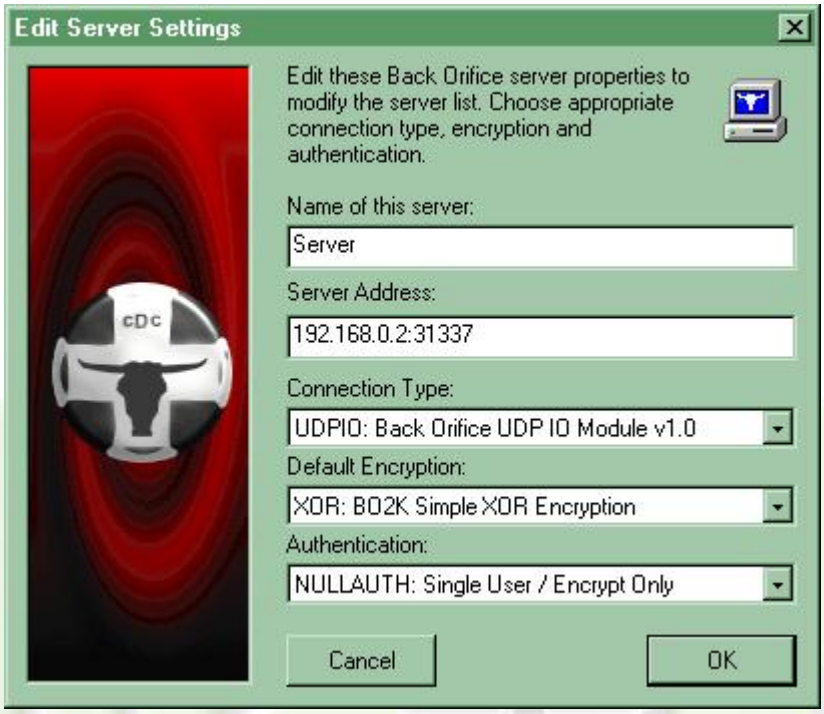
Instead, he gets the message,

------- Packet received from 192.168.0.2 port 31337 -------
thanks. We've logged your attempt to access our system. Now go play elsewhere.
------ End of Data -------
O:192.168.0.2>

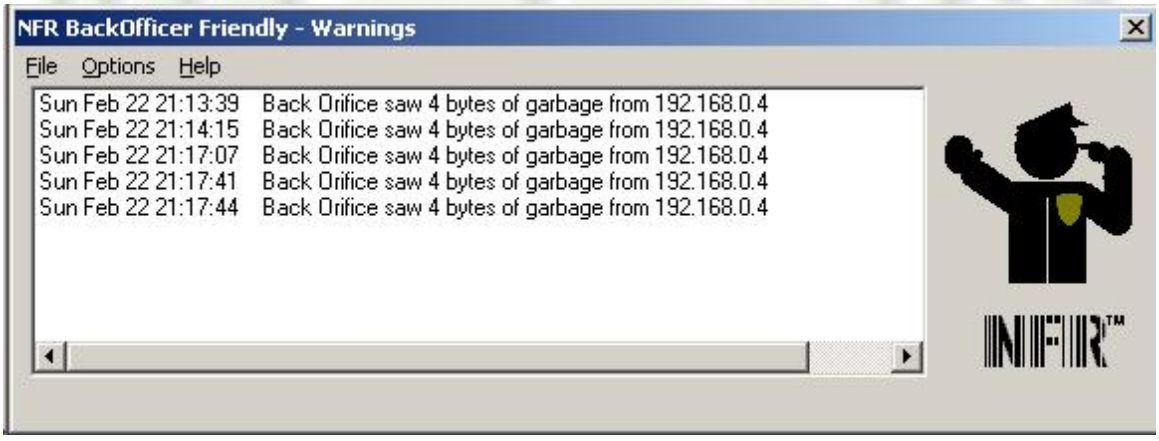
Step 6:

Network technology is very dynamic, and this is especially true of viruses and countermeasure software. The boys at Cult of the Dead Cow have continued to develop their "product". Back Orifice 2K is the latest stable release. Unzip Back Orifice 2K into a directory and execute the client bo2kgui.exe. The new client only comes in a GUI version. Be sure to consult the documentation at,

www.bo2k.com/documentation.html. Look at the tutorial first. Note that the server is not required to complete the lab. Let's see if the Back Orifice 2K client can find BOF mimicking the original Back Orifice configured using UDP:31337.



Now try to connect to the BOF honeypot with a few commands from the Back Orifice 2K client. BOF will look something like,



The Back Orifice 2K client behaves differently, and shows a failure to connect. Yet BOF still indicates an attempt from the source 192.168.0.4. NFR has not indicated that it intends further development towards mimicking a Back Orifice 2K server. Instead, emphasis is placed on its ability to detect other intrusions such as telnet, HTTP, FTP, POP3, and STMP.

Analysis

1) What limitations does BOF have regarding intrusions via Back Orifice 2K?
2) Would you recommend that NFR develop BOF to function as a Back Orifice 2K server?
3) What assumptions does BOF make regarding use of services inbound vs. outbound? Does BOF assume it is running on a secure host?
4) Delineate the different roles of virus protection software vs. honeypots for dealing with back door vulnerabilities.
5) Construct a rough network layout of your local place of business or school. Then consider how BackOfficer Friendly might be utilized in your network.

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

If You Want To Learn More

Explore the web site of NFR, www.nfr.com, to obtain articles and resources pertaining to network security.

Appendix

This lab was performed using BackOfficer Friendly version1.0.1.1, Back Orifice client version 1.20, Back Orifice 2K version 1.0, and YAPS version 1.2 on hosts running Windows XP.

Install files for BackOfficer Friendly can be found at, www.nfr.com under the dropdown Resource Center.

Install files for Back Orifice can be found at, www.cultdeadcow.com/tools/bo.html

Install files for Back Orifice 2K may be found at the same site by clicking on “other tools”.

YAPS may be downloaded from the following site: hale.tni.net/tedware/Yaps/Yaps.html