CS 482: Selected Topics in Information Security
Spring 2005 – Section 1

Module 2 – Assignment 1

Introduction

Information from insecure.org/nmap/nmap_doc.html about ftp bounce attack:
FTP bounce attack: is an interesting "feature" of the ftp protocol (RFC 959) is support for "proxy" ftp connections. A user should be able to connect from team1server.com to the FTP team2server-PI (protocol interpreter) of team2server.com to establish the control communication connection. A user should then be able to request that the team2server-PI initiate an active server-DTP (data transfer process) to send a file ANYWHERE on the internet! Presumably to a User-DTP, although the RFC specifically states that asking one server to send a file to another is OK. Now this may have worked well in 1985 when the RFC was just written. Unfortunately, in this technologically advance age we do not want attackers hijacking our ftp servers and requesting that data be sent out to arbitrary points on the internet. As *Hobbit* wrote back in 1995, this protocol flaw "can be used to post virtually untraceable mail and news, hammer on servers at various sites, fill up disks, try to hop firewalls, and generally be annoying and hard to track down at the same time." What we will exploit this for is to scan TCP ports from a "proxy" ftp server. Thus you could connect to an ftp server behind a firewall, and then scan ports that are more likely to be blocked. If the ftp server allows reading from and writing to a directory (such as /incoming), you can send arbitrary data to ports that you do find open.

For port scanning, our technique is to use the PORT command to declare that our passive "User-DTP" is listening on the target box at a certain port number. Then we try to LIST the current directory, and the result is sent over the Server-DTP channel. If our target host is listening on the specified port, the transfer will be successful (generating a 150 and a 226 response). Otherwise we will get "425 Can't build data connection: Connection refused."

Advantages/Disadvantages of Technique

+ Can issue another PORT command to try the next port on the target host of the previous port is closed.
+ The requests are harder to trace, potential to bypass firewalls.
- The process is slow
- Some FTP servers have disabled the proxy "feature"

Assignment

Phase 1:

1. Create a 1 page document with information on the exact syntax of the ftp bounce attack
2. Create a 1 to 2 page document on how to enable and disable the proxy server on a Linux machine. You may also want to find out how to do this on a Windows machine.

Phase 2:

1. Use NMAP to scan your team's network.
2. Create an FTP server with anonymous login on the Linux-WEB Virtual Machine.
3. Using the technique of the ftp bounce attack, open an ftp connection from one of the external machines to the Linux-WEB and attempt to connect to two open port on the WinXP-[A1, A2, B1, B2] machine.
4. Using the same technique attempt to connect to two closed port on the same WinXP machine.
5. Disable the proxy server and perform step 3 and 4.

Deliverable:

1. A document detailing the result of the NMAP scan of your team's network.
2. A document with the result of the connection attempts to the two open and closed ports on the WinXP machine when the proxy server is enable and when it is disable.