Lab 9: Adversary Role

Aim:

To provide a foundation in taking an adversary role.

Time to complete: Up to 30 minutes.

Activities:

- **Complete Lab 9**: Adversary Role
- **Complete Test 9**.

Leaning Activities:

At the end of these activities, you should understand:

- How to implement some adversary roles.

Reflective statements (end-of-exercise):

You should reflect on these questions:

- How might an intruder scan a network for hosts but remain undetected?

- How might you stop a continual testing of user accounts and passwords?

Lab 9: Pen Testing (Adversary)

1 Details

Aim: To provide a foundation in a Pen Testing using an adversary role.

2 Activities (Adversary)

L1.1 Download the Hydra tool and extract to your c:\ drive:

http://asecuritysite.com/hydra.zip

Perform the following test on the Windows 2003 virtual image.

L1.2 Open up a command line window, and go into the hydra folder (using cd hydra). Next you need to edit the user.txt and pass.txt files. For **user.txt** put in some sample user names (including one that you know will exist on the server you will test. Next put some passwords in the pass.txt (including one which matches the known user name).

L1.3 Next run Wireshark, and then scan your Windows 2003 host from your Windows hosts using:

Hydra –L user.txt –P pass.txt [Windows 2003] ftp

Did it manage to find a user name and password:

If so, which did it find:

What can you observe from the network traffic:

Can you determine from the network traffic where Hydra actually managed to login:

L1.4 Repeat the previous exercise for your Ubuntu host but this time do it for **telnet**:

Did it manage to find a user name and password:

If so, which did it find:

What can you observe from the network traffic:

Can you determine from the network traffic where Hydra actually managed to login: