UTSA
The University of Texas at San Antonio™

Cyber Warriors: A Comprehensive Introduction to Cybersecurity Tools and Techniques

Lab 7 – Web and Internet Security

Lab Description and Instructions

We learn how to carry out attacks on common Internet applications/services using a popular tool known as *hydra*. Specifically, we will use hydra to crack an (easy) SSH password of a user on the local VM. To better understand we will first create a new user using the following interactive command in the Terminal (skip this step if you have already done it during Lab 3, and simply use one of the users from Lab 3):

`sudo adduser username` (replace username with a unique name)

We will use a well-known dictionary (wordlist) for this attack. Kali ships with this wordlist which is located at /usr/share/wordlists/rockyou.txt.gz in a compressed format. We first extract this rockyou.txt file into the home directory (/home/student/) as follows:

```
cp /usr/share/wordlists/rockyou.txt.gz ~
gzip -dk rockyou.txt.gz
```

Next, we will use hydra to try and crack the password of the new user as follows:

`hydra -l username -P ~/rockyou.txt 192.168.13.150 -t 4 ssh` (Replace username with target user's username, and replace 192.168.13.150 with your targets server's IP address)

Homework:

Try all the above steps in your VM.