IA5150
Take Home Lab 1

Online Brute Force Attack

This week's lecture discussed different attack methods targeting the application layer. One of those attacks covered is the online brute force attack. As discussed in the Verizon data breach report, weak passwords are one of the most common security vulnerabilities.

In this lab you will perform an online brute force attack against a web target. You will harvest potential usernames and use a common password list to gain access to a password-protected site.

You will need to read the documentation on each tool before executing any command. It is generally good practice to understand the tool in depth before using it.

WARNING: DO NOT TARGET ANY HOST OTHER THAN THOSE IDENTIFIED IN THE LAB. USING THE TOOLS DISCUSSED IN THIS LAB WITHOUT CONSENT OF THE TARGET CAN BE ILLEGAL AND WILL RESULT IN A FAILING GADE IN THE COURSE AND POSSIBLE REMOVAL FROM NORTHEASTERN.

1. To perform this lab, you should use the VMWare Kali Linux image you downloaded in task 2.

   Make sure you have VMWare tools installed in your Kali VM. Without VMWare tools you will run into a number of issues (low resolution, network connection issues, restricted mouse movement).

   Check to see if VMWare tools are running : http://serverfault.com/questions/147169/how-can-i-check-if-vmware-tools-is-running-on-my-guest-ubuntu-server

If they are not - download Kali Linux VMWare image and start fresh. This will save you hours of debugging in this task and others. See task 2 in blackboard.

Do not proceed to any other debugging until you have VMWare tools running.

2. You will start by creating a potential username list from the target organization. You will then use this information in subsequent steps.

Start by reading documentation on the tool "theHarvester". This tool is used to gather information about a target during the reconnaissance phase. Read and understand the differences between an Active and a Passive scan with this tool.

https://code.google.com/p/theharvester/

3. Using the ***theharvester*** tool in Kali Linux perform **'google'** data source scan on the domain "***ccs.neu.edu***". You should then take the list of email addresses returned and copy it to a file and save it as "user.txt"

before moving on verify that you have at least 50 email addresses in the user.txt file

if theharvester returns 0 results, it is most likely that google is blocking your searches because it believes you are a bot. See blackboard for debugging options

4. I have set up a number of virtual machines for use in the lab. Each student will be assigned a system. Please see blackboard for your assigned system

Before proceeding check to see your Kali VM can access the IP address of the lab system. In Kali, start a browser and go to IP address of the lab system you are assigned. You should be prompted for a username and password. This host has HTTP basic authentication enabled for all URLs. If

you do not see this, debug the network connectivity issues in your VM before proceeding.

5. Start a terminal in Kali. Download a password list from github. For this lab we will be using the 10k most common passwords. Save the password list to the working directory

wget https://raw.github.com/Hood3dRob1n/addicted2hash/master/dict/10k_most_common.txt

6. Read online documentation on **hydra** and understand each of the command line options. As discussed in the course you should understand the tool before using it

   Hydra doc: http://www.aldeid.com/wiki/Thc-hydra
   & https://github.com/vanhauser-thc/thc-hydra

   There are other tutorials available by searching google for thc hydra.

7. Use Kali Linux to perform the following online brute force attack

   Tool: hydra
   Userlist: 100+ ccs email addresses
   Passwords: 10k common dictionary file
   Target: Your Lab IP posted in Blackboard
   CLI Options: read online docs. (hint: make sure to include –f)

   Be sure to point hydra ONLY at your specific target VM IP. Each VM can have different user accounts and you will be graded on the information recovered from your VM.

   You should be able to brute force **one** user account with the 10k password list and the information returned from the harvester.

   Debugging:
   If hydra stops running because of connection timeouts, wait for 4-5 minutes (time for open TCP sessions to timeout) and try again with a lower thread count (example 5). If you see connection timeouts with 5, wait 3-4 min and try with 1.

If you see timeouts with 1 thread there most likely is something at issue in your VM or network. A single thread count simulates a browser hitting the site this should be functional on any network. Verify VMWare tools are installed and switch to wired port. and/or bridged mode. Once 1 thread is functional move to 2, 3,4,5. Don't go above 5.

I have tested this on a 768k DSL link (which is rather slow) it is functional at 5 threads with VMware tools installed. You should consider a faster link however if you have access to one.

This should take a number of hours. Login to the website using the brute forced account information. You should see a page welcoming you to the `secured area`.

8. Record screenshot of hydra output screen displaying the found username and password. Also include your Public IP (not RFC 1918) address and the time when the account was found. This allows me to quickly cross-reference your submission in access_logs.

9. Read the Secure Area Welcome page for hints on how to access next secure area. After you find the next secure area, follow the instructions to start the next brute force.

   Remember the word list in this step is 184k long, you can estimate your time remaining by [STATUS] messages while hydra is running.

10. After you have found the second username & password, record screenshot of hydra-gtk (or hydra-cli) output screen displaying the username, password, and public IP for this step.

Bonus (30%):
See web page on Step 10 for Bonus option. After you perform the bonus and decrypt the message, submit a screenshot how you did this, and your public IP.