**Lab 7 - Password Cracking and Network Poisoning**

**Objectives**

* Crack Windows passwords using weak NTLM hashing.
* Crack Website passwords that use basic authenticaiton.
* Poison a network via ARP poisoning.

**Pre-Lab:** For this lab, you'll need your Windows XP , Windows 7, and Kali VM.

1. **Password Cracking on a Windows XP system**

* On your Kali VM, ensure the webserver is running and available by typing: service apache2 restart
* Enter the Kali account password when prompted, and then browse to http://localhost to confirm you can access the website.
* Inside of your Windows XP VM, download the 0phcrack utility and the tables from your Kali VM's website by browsing to http://[Kali IP address] (ophcrack directory). Once downloaded, unzip all files including the table zips. To run Ophcrack, browse into the ophcrack directory/x86/ and doubleclick the ophcrack.exe file. After ensuring Ophcrack loads, create a local Windows user with the password of “Password1234” (Go to Start-> Control Panel -> user accounts).
* Inside of Ophcrack, select "Load" then "Local SAM with samdump2". This will load in the local SAM file of the workstation you are currently on.
* It is also possible to use a password hash which you took off of another machine. This could be used in cases where you grabbed the SAM by booting off of a disk to avoid administrator login privileges.
* Next Go to the "Tables" icon and ensure that XP free small is enabled (there is a green dot by it). If it is not then hit the Install icon and browse to the location of the unzipped tables file you downloaded.
* Go back to the Main screen and look at the users passwords that you are trying to crack. Ophcrack will attempt to crack all of the passwords on this list.
* Press the "Crack" button

A screenshot of a computer

Description automatically generated

Ans: After creating the user testing, we run ophcrack to find the password for the newly created user. It was found to be Password1234 as shown in the screenshot.

2**. Password Cracking a website**

* For this portion of the lab, we're going to attack a website running within your Kali VM.
* In Kali open up firefox and go to the site http://localhost/protected/. If the web browser prompts about a problem with the certificate click “Continue”.
* Notice that this site is protected by a password. Hydracrack is able to crack this password protected website. Leave this prompt up until we are able to break the password later. (In this case we know the username was "test". Let’s assume we got this by knowing the username assignment policy, by shoulder surfing (looking over someone’s shoulder when they are typing in the username and password) or some other means.
* Download the darkc0de.lst wordlist from your Kali Webserver by navigating to http://localhost/lab-files/wordlists. Save the file in a directory of your choosing, such as Desktop or Downloads.
* View the dictionary file by entering the command "cat /[directory path]/darkc0de.lst". This will display the words in the dictionary list.
* From the terminal, run the following command which will launch an attack against the web server to brute force the password:

**hydra -l test -P /[directory path]/darkc0de.lst [Kali IP address] http-get -m /protected**

* The options used are as follows:
  + -l : login name to crack
  + -P: this point to a list of words to try.
  + http-get : use the protocol of http
  + -m : uri to crack based on the ip/domain address provided in brackets []
* Run this utility and wait for it to return the password.
* The password is intentionally set to something that is early on the password list. This was by design to lower the amount of waiting time. Previous semesters, students have reported this finishing within 12 hours, so I would recommend letting this run overnight.

A screenshot of a computer

Description automatically generated

After running hydra, we found the username and password of the website login as follows:

Login: test password: password

OPTIONAL

1. Sniffing/Poisoning the Network

* Power on your Windows 7, webserver, and Kali VMs, and take note of your IP addresses and your router IP.
* Within Kali, Open a terminal and change directory to /usr/share/ettercap
* Open the file etter.filter in an editor of your choice. If you are new to linux file editing, you may want to try leafpad by using the following command: leafpad etter.filter
* Edit the if statement to say the following: (NOTE that copying and pasting may introduce issues, however you only need to edit three areas, the first line and the "replace" line Also, the {IP of webserver VM} is to include the actual IP of your webserver.)
  + if (ip.proto == TCP && search(DATA.data, "www.bankofamerica.com") ){
  + log(DATA.data, "/tmp/mispelled\_ettercap.log");
  + replace("www.bankofamerica.com", "{IP of webserver VM}/logon");
  + msg("Correctly substituted and logged.\n");
  + }
* Save your new file. At the command prompt, run the following to "compile" the new rule.
* etterfilter etter.filter -o etter.filter.boa

A screenshot of a computer

Description automatically generated

* Open Ettercap in GUI mode using the following command:
* ettercap -G
* From the menu, select Sniff, and Unified Sniffing. Select your interface (should be eth0)
* From the Hosts menu, select Hosts List, and then select Scan for hosts. This should return your Windows 7 VM's IP, and the router for your subnet.
* Highlight your Windows 7 VM and select "Add to Target 1". Highlight your Router and select "Add to Target 2"
* From the Mitm menu, select "ARP Poisoning" and check the "Sniff remote connections" option.
* From the Filers menu, select "Load a Filter" and then select the etter.filter.boa file we created earlier.
* On your Windows 7 VM, browse to www.bankofamerica.com You may receive a Certificate Warning message, if so, select proceed anyway.
* The result should be that the browser was redirected to a pretty basic login page that is hosted off of the webserver VM.

A screenshot of a computer

Description automatically generated

* Optionally, you can use the "Bettercap" container in Kali by running:

**docker run -it --privileged --net=host bettercap/bettercap**

* For more information on "Bettercap", check out the website https://www.bettercap.org

2. Using Cain/Abel to perform network poisoning

* Use a Windows VM (XP or 7) for all of the following steps.
* Load Cain on the VM. If it is not installed, download it from http://www.oxid.it/cain.html
* Click on the Sniffer Tab, and then click on Configure to select your network adapter.
* Enable Sniffing by clicking the second icon from the left (looks like a network card)
* Right Click in the empty table space and choose “Scan MAC addresses” in order to populate “victims” on the network
* Click the APR tab
* Click on the + sign in the toolbar to add a new ARP poison routing entry.
* Choose the gateway for the network on the left side, on the right side select which victims you want to poison.
* Once selected, click on the 3rd icon from the left (looks like a biohazard symbol) to begin poisoning. If any of the “Victim” systems you selected above are performing any tasks on the network, Cain will show them in the appropriate categories under the “Passwords” tab.
* Now click on the APR-DNS heading in the left side listings under APR, and click on the + sign
* Enter the address you want to spoof, such as facebook.com and the corresponding spoofed information. Click on resolve to bring up the dialog box to enter the named URL to resolve to IP, such as myspace.com
* Now re-toggle the “Poison” icon to restart poisoning with your spoofed DNS entry. Have your victim try accessing your spoofed URL.

A screenshot of a computer

Description automatically generated