ECE-GY 9383 Network Security LAB 4 - Breaking HTTPS Lab
Credit to: Prof. Danny Y. Huang, Vaibhav Jain

What to Return: A PDF file that contains answers to all the questions below.

In this lab, you will be asked to intercept HTTPS traffic using an L2TP IPSEC tunnel along with MITMproxy. Most of the lab steps are recorded in video as complementary materials in the course Brightspace site.

Task 1. Set up a VPN server.

Steps

1. On your computer's browser, go to "https://api.ipify.org".
2. Get a Ubuntu 20 virtual machine on Digital Ocean (or other similar cloud providers). From now onwards, we shall call this virtual machine the Cloud VM.
3. Set up an L2TP with IPSEC VPN server on the Cloud VM by following these instructions.
4. Connect your computer (or your Kali Linux virtual machine) to the VPN server. If you're running Kali, you may not be able to see the L2TP option under VPN; in this case, run "`sudo apt update; sudo apt install network-manager-l2tp-gnome`" in the terminal to install L2TP support.
5. On your computer's browser, go to "https://api.ipify.org".

Questions

1. What is the IP address shown in Step 1 above?
2. What is the IP address of your Digital Ocean instance (from Step 2 above)?
3. Include a screenshot that shows you've set up the L2TP VPN server correctly in Step 3.
4. What is the IP address shown in Step 5?
5. Please explain why the IP address in Step 5 is different from the IP address in Step 1.

Task 2. Experiment with certificates.

Do the following steps on your computer (or on a Kali Linux VM). Feel free to use a browser of your choice.

Steps

1. Visit https://self-signed.badssl.com/
2. Visit https://expired.badssl.com/

3. Visit https://revoked.badssl.com/

For each of the steps above, answer the following two questions:

Questions

1. What is your observation in visiting the site? Include a screenshot of your browser.
2. Explain the observation. Provide relevant information from the certificate as a part of your explanation.

Task 3. Set up MITMproxy.

Steps

1. On the Cloud VM, set up MITMproxy per these instructions.
2. Configure the appropriate iptable rules so that network traffic from the VPN server is forwarded to the MITMproxy. Remember to turn on IP forwarding and also replace “eth0” with the appropriate L2TP interface (such as “ppp0”) when you configure the IP table rules.
3. Do not install the MITMproxy certificate authority yet.
4. Make sure to keep the L2TP tunnel running (which you established in Task 1).
5. On the Cloud VM, run MITMproxy on the co\mmand line: “`./mitmproxy --mode transparent --showhost`”. Press “F” to follow new flows.
6. On your computer (or Kali Linux VM), open http://neverssl.com/ in the browser.
7. On your computer (or Kali Linux VM), open https://www.nytimes.com/ in the browser.
8. Install the MITMproxy certificate authority on your computer (or Kali Linux) by following the “Quick Setup” section.
9. On your computer (or Kali Linux VM), open http://neverssl.com/ in the browser.
10. On your computer (or Kali Linux VM), open https://www.nytimes.com/ in the browser.
11. Visit https://self-signed.badssl.com/
12. Visit https://expired.badssl.com/
13. Visit https://revoked.badssl.com/

Questions

1. For Step 6 in this task, what do you see in the browser and on MITMproxy? Please include the relevant screenshots and explain your observations.
2. For Step 7 in this task, what do you see in the browser and on MITMproxy? Please include the relevant screenshots and explain your observations.

3. Once you complete Step 8, show a screenshot of the MITMproxy certificate in the root store.
4. For Step 9, what do you see in the browser and on MITMproxy? Please include the relevant screenshots and explain your observations.
5. For Step 10, what do you see in the browser and on MITMproxy? Please include the relevant screenshots and explain your observations.
6. Briefly explain how MITMproxy allows you to intercept TLS traffic in Steps 9 and 10.
7. For Step 11, what do you observe and why? Please include any relevant screenshots.
8. For Step 12, what do you observe and why? Please include any relevant screenshots.
9. For Step 13, what do you observe and why? Please include any relevant screenshots.