DNS Sinkholes: Defense and Offense

Purpose

- The purpose of this lab is to gain a better understanding of how DNS works. Students will also discover how it can be used differently than the primary intended use for defensive and offensive purposes.

Learning Outcomes

- Demonstrate a deep understanding of network protocols through critical analysis to better provision and secure network services (**DNS**)
- Utilize appropriate resources to internalize and articulate network architectures, emerging technologies, and network mechanisms and apply this knowledge to address current network and security challenges. (**DNS Sinkhole**)

Expected Time

- 3-6 Hours over 16 days (see learning suite for exact due date)

Instructions

1. Before beginning the lab work it is recommended that you do a quick study of what a DNS sinkhole is and how it works. There are some recommended resources at the end of the lab instructions.
2. Setting up the virtual environment
    a. Download and install VMware.
    b. Download the latest Ubuntu Desktop iso
        i. https://ubuntu.com/download/desktop
    c. Create 3 new VMs
        i. You will only need to run two of these at a time, this is something to consider when allocating hardware resources to the VMs.
        ii. User: This will act as an end user device
        iii. PiHole: This is where we will install PiHole
        iv. Sinkhole: This is where we will create a DNS sinkhole manually
        v. Install Ubuntu on each VM.
    d. Set a static IP address on the PiHole and Sinkhole VMs.

e. Make sure that “User” can ping PiHole and Sinkhole.
    i. If they can’t you may need to do some research about the network options in VMware.

3. PiHole
    a. Follow the Getting Started instructions on the PiHole documentation
        i. https://docs.pi-hole.net/main/
        ii. Complete the PreReq and Installation sections on the PiHole VM.
        iii. Since we have not enabled the firewall on our PiHole VM you can skip the section about adding allow rules.
        iv. During the installation you will be given an admin password, make sure to save this before continuing.
    b. On the User VM find a website that has ads. Take a screenshot and include it in your writeup.
    c. Now set the DNS server on the User VM to the IP address of the PiHole VM.
    d. Refresh the same site, you should no longer see the ads. Include a screenshot in your writeup.
        i. If it doesn’t work here are some things to try
            1. Another site, it is possible the domain for the ad is not included in any of the PiHole lists
            2. In your browser disable DNS over HTTPS
            3. On the User VM run sudo resolvevtl flush-caches
4. Exploring PiHole
    a. Log into the web interface for PiHole
        i. http://IP Address:80/admin
    b. Explore the available options
    c. Figure out how to block YouTube. Include a screenshot of YouTube not working on the User VM.
    d. For 2 additional options, answer the following questions:
        i. What was the option/feature?
        ii. How/when would it be useful?
5. DNS Sinkhole
    a. For this section you will need to research the exact commands and code to use.
    b. Power off the PiHole VM and start the Sinkhole VM
    c. Install bind9
    d. Configure a forwarder so that requests are sent to 8.8.8.8.
    e. Block https://www.linux.org/
        i. Define a custom zone. Include a screenshot in your writeup.

        ii. Create a custom entry file. Include a screenshot in your writeup.
        iii. Point to an incorrect IP address so the User VM is unable to access linux.org
    f. Visit Linux.org on the User VM to be sure that it is working
        i. You may need to change the DNS server back to auto or 8.8.8.8
    g. Set the DNS server on the User VM to the IP address of the Sinkhole VM.
    h. Now confirm that linux.org is unreachable. Include a screenshot in your writeup.
    i. Now find a website with ads. Find the domain that the ads come from. Use the method you used to block linux.org to block the ads on the site. Include a screenshot of the site with ads, and the site without ads.
        i. You have now manually replicated the primary functionality of PiHole
6. Questions
    a. Compare and contrast PiHole vs manually setting up a DNS Sinkhole. Some things to consider are the pros and cons as well as different use cases.
    b. Aside from ad-blocking what is one defensive use case for DNS sinkholes?
    c. How might a DNS Sinkhole be used offensively? Describe the scenario and effects.

Deliverables

- Screenshot of a site with and without ads using PiHole (2 screenshots)
- Screenshot of YouTube not working on the User VM using bind9
- Screenshot of your bind9 custom zone for linux.org
- Screenshot of your custom entry file for linux.org
- Screenshot of linux.org not working using bind9
- Screenshot of a site with and without ads using bind9 (2 screenshots)
- 3 questions

Resources

- https://en.wikipedia.org/wiki/DNS_sinkhole

- https://docs.paloaltonetworks.com/advanced-threat-prevention/administration/configure-threat-prevention/use-dns-queries-to-identify-infected-hosts-on-the-network/how-dns-sinkholing-works
- https://ubuntu.com/download/desktop
- https://docs.pi-hole.net/main/
- https://www.isc.org/bind/
- https://ubuntu.com/server/docs/how-to/networking/install-dns/
- https://bind9.readthedocs.io/en/latest/reference.html
- If you try to block an ad or site and it doesn't work after correct configuration try:
    - Another site, it is possible the domain for the ad is not included in any of the PiHole lists (if you are in the Bind9 section, add the domain yourself)
    - In your browser disable DNS over HTTPS
    - On the User VM run sudo resolvevtl flush-caches

Rubric

- Screenshot of a site with and without ads using PiHole (2 screenshots) +2
- Screenshot of YouTube not working on the User VM using bind9 +2
- Screenshot of your bind9 custom zone for linux.org +3
- Screenshot of your custom entry file for linux.org +3
- Screenshot of linux.org not working using bind9 +2
- Screenshot of a site with and without ads using bind9 (2 screenshots) +2
- 3 questions
    a. Compare and contrast PiHole vs manually setting up a DNS Sinkhole. Some things to consider are the pros and cons as well as different use cases. +2
    b. Aside from ad-blocking what is one defensive use case for DNS sinkholes? +2
    c. How might a DNS Sinkhole be used offensively? Describe the scenario and effects. +2