Lab 7 - DNS

Goal

Examine DNS query and response traffic
Configure a DNS server(s)

Resources

Each student has been issued a **single** static address in 132.235.160.192/26 network. Gateway follows class convention.
XXX = Your personal 132.235.160.192/26 IP address. Same IP as your DNS server.

Each student has a student number. It's the last octet of your student VM's IP address.
Y = Student Number

At the Linux command line there are two likely editors available, nano or vim. We will use nano in the instructions for a more universal appeal, but vim is also can acceptable option in you are familiar with the operational workflow of that application.

GNS3 Configuration

1. Build **Secure Net** using Cloud, VyOS and Ubutu-GUI objects. See network diagram.

2. Connect VyOS-1 eth0 to Cloud 1 ens160. Config VyOS-1 eth0 to get address via DHCP. Remove 132.235.9.75 and 132.235.200.41 as DNS, set DNS server to 132.235.160.10

3. Setup a caching DNS server on VyOS-1:

```
set service dns forwarding system
set service dns forwarding listen-on eth1
```

4. Config a VyOS-1 NAT and DHCP server/service on the eth1 interface, using the IP on VyOS eth1 as the DNS server in the DHCP configuration (i.e. do not use 132.235.9.75 and 132.235.200.41 as the DNS servers in DHCP configuration).

5. Connect VyOS-1 eth1 to GUI-Desktop eth0. Make sure GUI-Desktop obtains the correct address and DNS servers.

6. Conduct the following DNS queries from GUI-Desktop:
   a. Use the DIG command to look up www.ohio.edu, www.osu.edu and www.microsoft.com
   b. Use DIG: `dig +trace www.its.ohio.edu @172.X.X.X`
   c. Use DIG to look for records of type "NS" under cs.ohio.edu
   d. Use DIG to look for records of type "SOA" under cs.ohio.edu
   e. Use DIG to look for records of type "NS" under the root domain "."
   f. Use DIG to map the address 132.235.1.1 to its name (a "reverse" lookup)
   g. Use DIG to get MX records for ohio.edu and osu.edu

Setup Authoritative DNS Server

7. Build **DMZ Net** using Cloud and Ubuntu-GUI objects. See network diagram.

8. Rename Ubuntu-GUI object to DNS Server. Configure static IP on DNS Server using assigned public IP. For DNS server use 132.235.160.10. It should now be possible to SSH to the DNS Server from your personal machine since IP is available from the VPN.

9. Install Bind on Ubuntu

```
sudo apt install -y bind9 bind9utils bind9-doc
```

10. Reboot `sudo reboot`

11. To verify that the named process is listening on port 53 SSH back into DNS Server and run:

    ```
    netstat -nlpu
    ```

    There should be entries on port 53 (DNS).

12. The newly installed the DNS server is configured to only reply to requests on the local server. Test the DNS service from with the DNS machine (i.e. bind on the local machine is serving as a caching DNS server like the DNS forwarder in VyOS).

    ```
    dig ip6echo.net @localhost
    ```

Add security features to the DNS server

Unsecured DNS servers are a significant hazard on the Internet. It is extremely easy to use them in a denial of service attack as a traffic amplifier. In a “Smurf Attack” or “Amplification Attack”: https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack

The Bind DNS server has extensive security controls built into it. These controls MUST we adapted to the situation in which the server is installed. For use in our lab we are relying on a number of external controls that are provided by OIT and the ECT firewall. The following configuration is a reasonable starting point for deploying a secure DNS service. Do NOT use it for future work without carefully considering the security of the service you are deploying

13. Open the config file:

    ```
    sudo nano /etc/bind/named.conf.options
    ```

    Remove the existing file contents (in nano ctrl-k deletes lines) and then insert the following. No other changes to the file will be needed.

    ```
    acl secondaries {
            132.235.160.115;
    };

    acl trusted {
            132.235.160.0/24;
            132.235.201.0/24;
            2610:a8:4831:300::/56;
            2610:a8:4831:1095::/64;
            localhost;
    };

    options {
            directory "/var/cache/bind";

            listen-on port 53 { any; }; #{ 127.0.0.1; };
            listen-on-v6 port 53 { any; }; #{ ::1; };
            allow-query     { any; };
            allow-transfer  { secondaries; };
            allow-recursion { trusted; };

            recursion yes;
            auth-nxdomain no;    # conform to RFC1035
            max-ncache-ttl 60;

            dnssec-enable no;
            dnssec-validation no;

    };
    ```

14. Reload the bind service so it will start using the new configuration. Run this command after every change to any of the DNS server config files.

```
systemctl restart bind9
```

15. Check the system log for debugging information coming from the Bind service. Do not proceed until you resolve all of the errors:

```
tail –f /var/log/syslog
```
OR
```
tail –n 50 /var/log/syslog
```

16. Check the operation of your new DNS server from the Ubuntu-GUI-1 on Secure Net network.

```
dig google.com @132.235.160.XXX
```

17. Create a zone file on DNS Server:

```
sudo nano /etc/bind/sY.lab.headwallram.com.zone
```

```
$TTL 60
@       IN      SOA     ns1-lab.its.ohio.edu. saundeb1.ohio.edu (
                        2019100301 ; serial
                        7200 ; refresh
                        7200 ; retry
                        604800 ; expire
                        3600 ; ttl
                        )

;  Zone NS records
@       IN      NS      ns1.sY.lab.headwallram.com.

;  Other Records
@       IN      A       132.235.160.XXX
ns1     IN      A       132.235.160.XXX
www     IN      CNAME   @
```

18. Include zone file in Bind configuration:

```
sudo nano /etc/bind/named.conf.local
```

```
zone "sY.lab.headwallram.com" {
      type master;
      file "/etc/bind/sY.lab.headwallram.com.zone";
};
```

19. Test your DNS config from Secure Net Desktop. It should work.

```
dig www.sY.lab.headwallram.com @132.235.160.XXX
```

20. Report your sub-domain's name, your name servers IP address to Bob in the department of Insane Coffee Swirlers, to connect your subdomain to the rest of the name tree. IMPORTANT: These guys work 9 to 5 on most WEEKDAYs with very regular coffee breaks and months of accrued vacation time. (i.e. You will **no**t be able to finish this part of the project if you wait until Sunday to complete the work.)

21. Determine a query that you can use to prove that your new DNS server is configured to NOT providing caching DNS services on.

22. Go back into your zone file and create three **additional** A records.
    flir = 10.101.8.170
    prtg = 132.235.10.53
    lmgtfy = 52.203.61.249

23. Create an **additional** A record of your name use an IP of your own choosing.

24. Work with a class colleague to setup a zone transfer and a secondary DNS ("offsite"). You will need an allow-transfer directive on your primary server. Here is an example of a zone directive for your secondary server. Negotiate this agreement with other students in class.

    A = Partner's Student Number
    BBB = other studet's DNS server IP

```
zone "s A.lab.headwallram.com" {
        type slave;
        masters { 132.235.160.BBB; };
        file "s A.lab.headwallram.com.zone";
};
```

    Once configured you will need to notify Bob about the new NS server again.

Lab Report Guidelines

Each report is to be written individually, although the data for the lab is collected with your partner. Reports will be uploaded to Blackboard electronically in PDF format. Each lab report must have a header on the first page that includes:

- Your Name
- The lab section you attended
- Your affiliation (CS ugrad, CS grad, ITS ugrad, ITS grad)

Questions for Lab

1. From step 6, include the output from the DIG commands, and briefly explain the output. Summarize by section for repetitive information rather than explaining line by line.

2. From DIG (all) in step 6, show how each section of the output corresponds with the record in the Wireshark capture that requested that information.

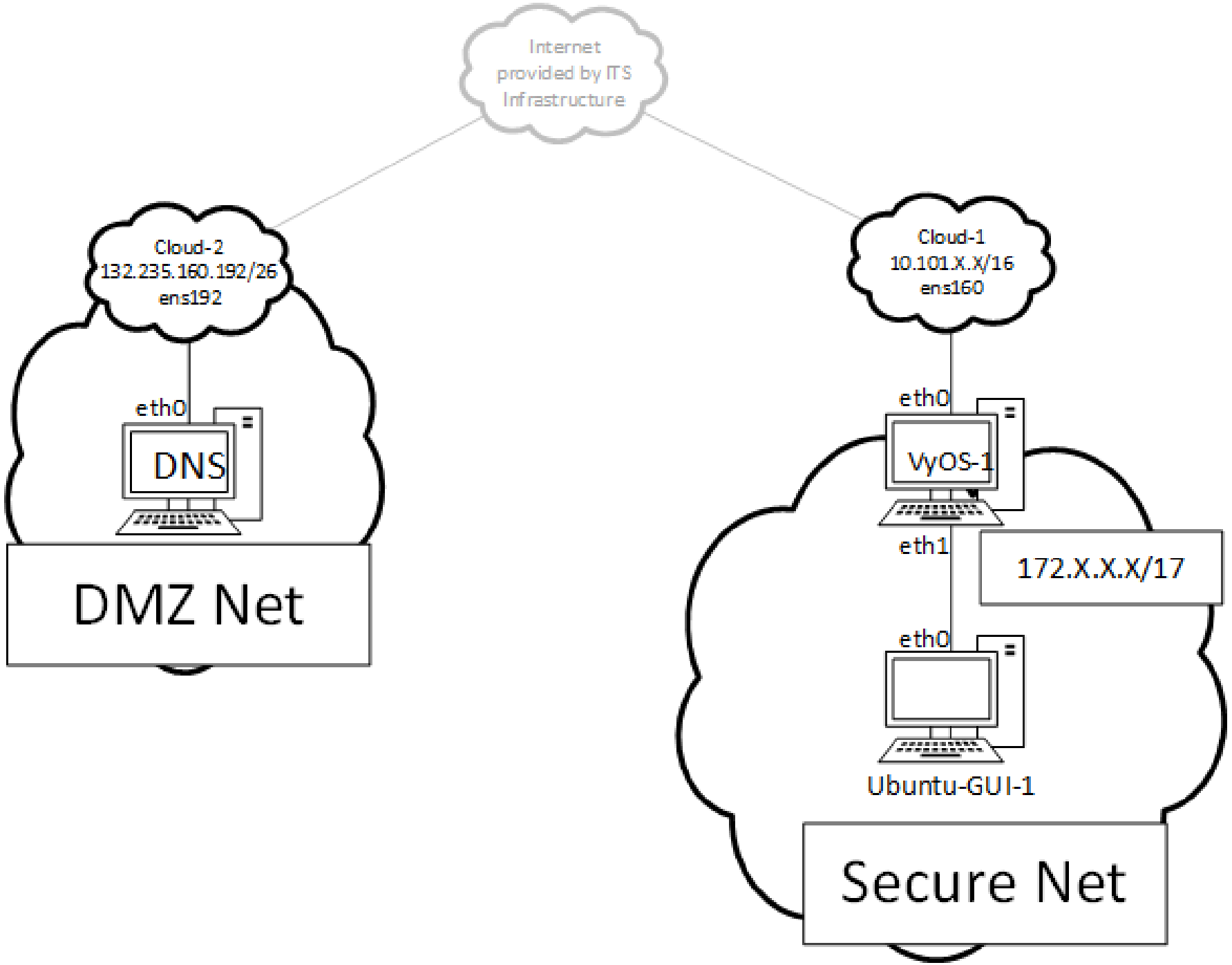
3. Show complete DNS zone file from end of lab.

4. Show Dig output using your DNS server for the records you created in step 22.

5. Show Dig output using your DNS server for the record you created in step 23.

6. Using a network diagramming software (like Visio or http://draw.io) re-create a copy of the network diagram that was used. IP addresses and connections MUST be readable. Do not use a photo and do not copy and edit the diagram from this lab writeup. The purpose is the learn to use network documentation tools.

7. Graduate Students/Undergraduate Extra credit – Suggest a configuration to enable DNSSec on the zone that you created.


Internet
provided by ITS
Infrastructure
Cloud-2
132.235.160.192/26
ens192
eth0
DNS
DMZ Net
Cloud-1
10.101.X.X/16
ens160
eth0
VyOS-1
eth1
172.X.X.X/17
eth0
Ubuntu-GUI-1
Secure Net