Project 3

Team Member

1. **You Li – 002824033**
2. **Badrinath Rohith Varma Datla – 002471875**
3. **Cheng Yu-Chang – 002083499**

Workload Balancing: -

1. You Li:

- **Implemented all VMs in "NAT" mode.**
- **Implemented ssh to all VMs in "NAT" mode**
- **Implemented DHCP (IPv6) configuration**
- **Implemented backup server configuration**
- **Summarized and done all VM setting for demonstration**

2. Rohith:

- **Implemented DNS master and slave VM's**
- **Implemented DHCP (IPv4) configuration**
- **Implemented ARP poisoning (MITM)**
- **Gone through references for Ipsec Vpn**
- **Conducting group report**

3. Cheng Yu-Chang:

- **Implemented all VMs in "Bridge Adaptor" mode.**
- **Implemented ssh to all VMs in "Bridge Adaptor" mode**
- **Implemented Apache2 webserver**
- **Implemented VPN server and client VM for nfs file sharing**
- **Create test plan for demonstration**

Index

Jargon of the Project

1.What is Linux?

- **File System**

The Linux file system is structured in a hierarchical manner, beginning with the root directory (/). It organizes files and directories based on their purposes, such as /home for user-specific files, /bin for essential executable programs, and /etc for system configuration files. File management often involves tools like tar for archiving and gunzip for decompressing files:

- **tar: A utility to archive multiple files or directories into one for easier storage or transfer.**
- **gunzip: Decompresses files with the .gz extension, often used alongside tar to handle .tar.gz archives.**

- **Memory in Linux:**

Linux employs a robust memory management system that optimizes physical and virtual memory usage. It utilizes:

- **RAM: For active processes and frequently accessed data.**
- **Swap Space: A fallback disk area used when RAM is fully utilized.**
- **Caches and Buffers: To speed up operations by holding temporary data.**
- **Memory usage can be monitored dynamically using system commands.**

- **Processes in Linux**

Processes are instances of running programs, each uniquely identified by a PID (Process ID). They can be foregrounding applications, system tasks, or background services. Linux processes have:

- **States: Active, sleeping, or terminated.**
- **Hierarchy: Processes are often organized into parent-child relationships. Tools are available to observe (ps, top) and manage (kill) processes effectively.**

2. DHCP

- **Introduction:**

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol that automatically assigns IP addresses and other network configuration settings to devices within a network. By eliminating the need for manual IP address assignment, DHCP provides an efficient solution for managing large-scale networks.

A DHCP server provides:

- **Dynamic allocation: Assigns IP addresses to clients for a limited time (lease).**
- **Reservation: Assigns a permanent IP address to specific devices based on their MAC address.**
- **Exclusion: Reserves a range of addresses within a scope for static assignment to critical devices such as routers and servers.**

- **Behavior of protocol:**

DHCP operates using a client-server architecture. It involves the following key behaviors:

1. **Address Pool Management: Maintains a pool of available IP addresses and assigns them to clients dynamically.**
2. **Lease Assignment: Allocates IP addresses for a specified period. The client must renew the lease before it expires.**
3. **Address Conflict Detection: Ensures no two devices are assigned the same IP address.**
4. **Support for IPv4 and IPv6: Provides seamless configuration for both types of addressing.**

- **Signaling:**

DHCP operates primarily over UDP and involves a series of message exchanges between the client and server.

1. **Discovery: The client broadcasts a DHCPDISCOVER message to find an available DHCP server.**
2. **Offer: The server responds with a DHCPOFFER message, proposing an IP address and other network configuration details.**
3. **Request: The client broadcasts a DHCPREQUEST message to accept the address offered.**
4. **Acknowledgment: The server sends a DHCPACK message to finalize the lease and confirm the allocation.**
5. **Renewal: Before the lease expires, the client sends a unicast DHCPREQUEST to renew the lease.**

3. DNS

- **Introduction:**

The Domain Name System is a hierarchical and decentralized naming system that translates human-readable domain names (e.g., example.com) into machine-readable IP addresses (e.g., 192.168.1.1 for IPv4 or 2001:db8::1 for IPv6). DNS enable users to access websites and services without needing to memorize numeric IP addresses.

Key Features of DNS:

- **Domain Name Resolution: Converts domain names into IP addresses.**
- **Hierarchical Structure: Organized in a tree-like structure, with root servers at the top.**
- **Record Management: Maintains various records like A (IPv4), AAAA (IPv6), MX (Mail Exchange), and CNAME**

- **Behavior of the Protocol:**

DNS operates on a client-server model and uses a query-response mechanism. The primary behaviors include:

1. **Name Resolution: Resolves domain names to IP addresses.**
2. **Caching: DNS servers and clients cache results in reducing lookup times and network traffic.**
3. **Recursive and Iterative Queries:**
   a. **Recursive: The DNS server takes responsibility for resolving the query fully and returns the result to the client.**
   b. **Iterative: The DNS server provides the client with referrals to other DNS servers to resolve the query.**
4. **Zone Management: The DNS database is divided into zones, each managed by a specific DNS server.**
5. **Support for Forward and Reverse Lookups:**
   a. **Forward Lookup: Domain name to IP address resolution.**
   b. **Reverse Lookup: IP address to domain name resolution.**

- **Signaling:**

Master-Slave DNS with BIND9

1. **Zone Update: Master server updates its zone file.**
2. **NOTIFY: Master sends a NOTIFY message to slave servers about the update.**
3. **SOA Query: Slave queries the master for the zone's SOA record to check version.**
4. **Zone Transfer: If the zone version differs, the slave requests an AXFR (full transfer) or IXFR (incremental transfer) over TCP.**
5. **Synchronization: Slave updates its zone file to mirror the master.**
6. **BIND9 facilitates this process with named.conf configurations for both master and slave servers.**

4.WEB-SERVER:

- **Introduction:**

A web server is software or hardware that serves web content to users over the internet or an intranet. It processes client requests (via HTTP/HTTPS) and responds with requested resources, such as HTML pages, images, or files.

Key Features:

- **HTTP/HTTPS Handling: Handles requests and serves web pages.**
- **Static and Dynamic Content: Delivers static files (e.g., HTML, CSS) and supports dynamic content via server-side scripts (e.g., PHP, JSP).**
- **Security: Implements SSL/TLS, IP filtering, and firewalls for secure communication.**

- **Behavior of the Protocol:**

1. **Request-Response Model: The client (browser) sends a request, and the server responds with the requested resource.**
2. **Content Types: Serves static files and dynamically generated content based on the client's request.**
3. **Logging and Monitoring: Maintains logs for each request, aiding in analytics and debugging.**

- **Signaling:**
  1. **Client Request: The browser sends an HTTP request to the server (GET, POST, PUT, etc.).**
  2. **DNS Resolution: Resolves the domain name to the server's IP address.**
  3. **Connection Establishment:**
     a. **Uses TCP to establish a connection (3-way handshake).**
     b. **For HTTPS, performs an SSL/TLS handshake.**
  4. **Resource Delivery:**
     a. **The server locates the requested file or executes server-side scripts.**
     b. **Sends an HTTP response with the requested resource and status code (e.g., 200 OK, 404 Not Found).**
  5. **Connection Closure: Connection is terminated or kept alive based on the Connection header.**
- **Example with Apache Web Server:**
  - **Configures httpd.conf to define document root, virtual hosts, and access controls.**
  - **Supports extensions like PHP and modules for enhanced functionality.**

5.FIREWALL

- **Introduction**

A firewall is a network security tool designed to regulate and monitor network traffic, both incoming and outgoing, according to established security rules. Serving as a protective barrier, it separates trusted internal networks from untrusted external networks, like the internet, to block unauthorized access and safeguard against cyberattacks.

Key Features:

- **Packet Filtering: Inspects and filters packets based on rules (e.g., IP address, port, protocol).**
- **Stateful Inspection: Tracks the state of active connections and makes decisions based on the context.**
- **Application Layer Filtering: Inspects traffic at the application level (e.g., HTTP, FTP).**
- **NAT: Hides internal IP addresses to protect the network.**

- **Behavior of the Protocol**
  1. **Traffic Monitoring: Analyzes packets against defined rules for source/destination IP, ports, and protocols.**
  2. **Access Control: Allows or denies traffic based on rules (e.g., block all external SSH connections).**

3. **Intrusion Prevention: Detects and blocks suspicious patterns indicative of attacks.**
4. **Logging: Records traffic and rule violations for analysis and auditing.**

- **Signaling**
  1. **Packet Entry:**
     a. **Incoming packets are inspected against firewall rules.**
     b. **Outgoing packets are checked for compliance with the rules.**
  2. **Rule Matching:**
     a. **Packets are compared with rule sets (allow, deny, drop).**
     b. **For stateful firewalls, connection states (e.g., established, related) are tracked.**
  3. **Action Taken:**
     a. **Allow: Packet is forwarded to its destination.**
     b. **Deny: Packet is rejected, and optionally a response is sent.**
     c. **Drop: Packet is silently discarded.**
  4. **Logging: Logs details such as source/destination IP, timestamp, and action taken.**
- **Example with iptables:**
  - **Block SSH from outside: sudo iptables -A INPUT -p tcp --dport 22 -j DROP**
  - **Allow HTTP traffic: sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT**

6.BACKUP

- **Introduction:**

A backup system creates a copy of critical data to ensure it can be restored in case of data loss, system failure, or cyberattacks. Backups are an essential part of disaster recovery and data protection strategies.

Key Features:

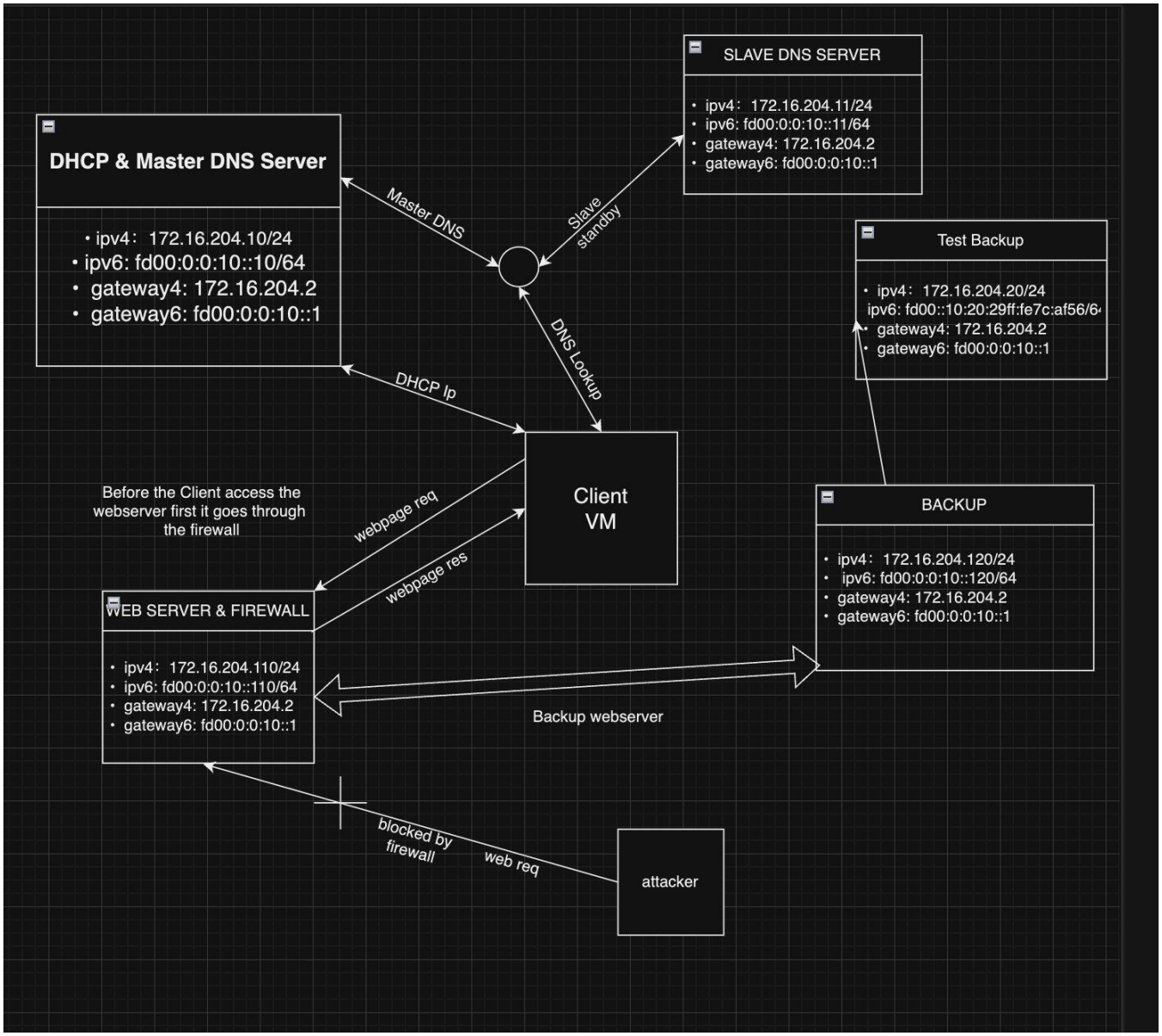
- **Automation: Scheduled backups reduce manual effort.**
- **Compression: Data is compressed to save storage space.**
- **Offsite Backup: Data is stored on remote servers for added security.**
- **Incremental/Differential: Optimizes storage by only backing up changes since the last backup.**

- **Behavior of the Protocol**
  1. **Data Collection: Identifies and selects files or directories for backup.**
  2. **Data Compression: Compresses files to save storage space.**
  3. **Transfer/Storage: Transfers the backup file to a local or remote server.**
  4. **Retention Policy: Manages backup cycles, retention duration, and deletion of old backups.**
  5. **Restoration: Enables restoring data from backups when needed.**
- **Signaling**
  1. **Triggering:**

a. **Backup jobs are scheduled or triggered manually.**
b. **Automation tools like cron initiate backups based on predefined schedules.**

2. **File Compression:**
   a. **Tools like tar and gzip are used to archive and compress files.**
   b. **tar -czf backup.tar.gz /path/to/data**
3. **Transfer: Files are transferred to a remote server using protocols like SCP or RSYNC.**
   scp backup.tar.gz user@remote-server:/backup/directory
4. **Verification: Ensures backup integrity through checksums or logs.**
5. **Restoration: Extracts data from the backup archive when needed.**
   "tar -xzf backup.tar.gz -C /restore/path"

Project topology



Network and machine setup design (IP addressing Plan)

1. **We've set up multiple ubuntu VM machines to meet out project requirements:**
   - **VM1-DHCP+master DNS**
   - **VM2-slave DNS**
   - **VM3-webserver+ firewall**
   - **VM4-backup server**
   - **VM5-test backup server**
   - **VM6-attacker**
   - **VM7-test client server**
   - **VM8-VPN server**
   - **VM9-VPN client**
2. **We are using 172.16.204.X/24 as our network design:**
   - **VM1**
     Pv4: 172.16.204.10/24
     IPv6: fd00:0:0:10::10/64
     Gateway IPv4: 172.16.204.2
     Gateway IPv6: fd00:0:0:10::1
   - **VM2**
     Pv4: 172.16.204.11/24
     IPv6: fd00:0:0:10::11/64
     Gateway IPv4: 172.16.204.2
     Gateway IPv6: fd00:0:0:10::1
   - **VM3**
     IPv4: 172.16.204.110/24
     IPv6: fd00:0:0:10::110/64
     Gateway IPv4: 172.16.204.2
     Gateway IPv6: fd00:0:0:10::1
   - **VM4**
     IPv4: 172.16.204.12/24
     IPv6: fd00:0:0:10::12/64
     Gateway IPv4: 172.16.204.2
     Gateway IPv6: fd00:0:0:10::1
   - **VM5**
     IPv4: 172.16.204.20/24
     IPv6: fd00:0:0:10::20/64
     Gateway IPv4: 172.16.204.2
     Gateway IPv6: fd00:0:0:10::1
   - **VM6**
     IPv4: 172.16.204.60/24
     IPv6: fd00:0:0:10::60/64

Gateway IPv4: 172.16.204.2
Gateway IPv6: fd00:0:0:10::1

- **VM7**
  IPs are dynamically assigned.
  Gateway IPv4: 172.16.204.2
  Gateway IPv6: fd00:0:0:10::1
- **VM8**
  IPv4: 10.100.234.41/24
  Gateway IPv4: 10.100.234.87
- **VM9**
  IPv4: 10.100.234.42/24
  Gateway IPv4: 10.100.234.87

Set up process:

1. **Basic network setting**

Static IP	DHCP Client

sudo apt update
sudo apt upgrade
sudo nano /etc/netplan/ 01-netcfg.yaml
`network:`
`  version: 2`
`  ethernets:`
`  ens160:`
`  addresses:`
`  - 172.16.204.10/24`
`  - fd00:0:0:10::10/64`
`  routes:`
`  - to: default`
`  via: 172.16.204.2`
`  - to: default`
`  via: fd00:0:0:10::1`
`  nameservers:`
`  addresses:`
`  - 172.16.204.10`
`  - 172.16.204.11`
`  - fd00:0:0:10::10`
`  - fd00:0:0:10::11`
sudo netplan apply
	sudo apt update
	sudo apt upgrade
	sudo nano /etc/netplan/01-netcfg.yaml
	`network:`
	`  version: 2`
	`  ethernets:`
	`  ens160:`
	`  dhcp4: yes`
	`  dhcp6: yes`
	`  accept-ra: yes`
	sudo netplan apply

2. **VM1**

Install ISC DHCP Server

Edit the DHCP Configuration File:

- **sudo nano /etc/dhcp/dhcpd6.conf**

```
default-lease-time 2592000;

# IPv6 address preferred lifetime
#  (at the end the address is deprecated, i.e., the client should
#   other addresses for new connections)
#  (set to 7 days, the  usual IPv6 default)
preferred-lifetime 604800;

# T1, the delay before Renew
#  (default is 1/2 preferred lifetime)
#  (set to 1 hour)
option dhcp-renewal-time 3600;

# T2, the delay before Rebind (if Renews failed)
#  (default is 3/4 preferred lifetime)
#  (set to 2 hours)
option dhcp-rebinding-time 7200;

# Enable RFC 5007 support (same than for DHCPv4)
allow leasequery;
```

```
subnet6 fd00:0:0:10::/64 {
    range6 fd00:0:0:10::100 fd00:0:0:10::200;
    option dhcp6.name-servers fd00:0:0:10::10, fd00:0:0:10::11;
}

host exclude110 {
    fixed-address6 fd00:0:0:10::110;
}


host backupserver6 {
    hardware ethernet 00:0c:29:97:d2:e7;
    fixed-address6 fd00:0:0:10::120;
}
```

- **sudo nano /etc/dhcp/dhcpd.conf**

```
# option definitions common to all supported networks...
# option domain-name "example.org";
# option domain-name-servers ns1.example.org, ns2.example.org;

default-lease-time 600;
max-lease-time 7200;

# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;
```

```
subnet 172.16.204.0 netmask 255.255.255.0 {
    range 172.16.204.100 172.16.204.200;
    option routers 172.16.204.2;
    option domain-name-servers 172.16.204.10, 172.16.204.11;
    default-lease-time 600;
    max-lease-time 7200;
}

host exclude110 {
    fixed-address 172.16.204.110;
}

host backupserver {
    hardware ethernet 00:0c:29:97:d2:e7;
    fixed-address 172.16.204.120;
}
```

sudo nano /etc/default/isc-dhcp-server

```
INTERFACESv4="ens160"
INTERFACESv6="ens160"
```

sudo systemctl restart isc-dhcp-server
sudo systemctl enable isc-dhcp-server
sudo systemctl status isc-dhcp-server
sudo apt install bind9 bind9utils bind9-doc -y
sudo nano /etc/bind/named.conf.options

CONFIGURING DHCP POOL IN DHCPD.CONF

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

    recursion yes;
    allow-query { any; };

    forwarders {
        8.8.8.8;      // Google DNS
        8.8.4.4;
    };

    dnssec-validation auto;

    auth-nxdomain no;    // conform to RFC1035
    listen-on { any; };
    listen-on-v6 { any; };
};
```

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

```
// Forward Zone
zone "bostondns.local" {
    type master;
    file "/etc/bind/zones/db.bostondns.local";
    allow-transfer { 172.16.204.11; };  // Slave DNS IP
};

// Reverse Zone for IPv4
zone "204.16.172.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/db.172.16.204";
    allow-transfer { 172.16.204.11; };
};

// Reverse Zone for IPv6
zone "0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.d.f.ip6.arpa" {
    type master;
    file "/etc/bind/zones/db.fd00.0.0.10";
    allow-transfer { 172.16.204.11; };
};
```

sudo mkdir /etc/bind/zones

THIS WILL DEMONSTRATE MASTER DNS

```
$TTL    604800
@       IN      SOA     ns1.bostondns.local. admin.bostondns.local. (
                            2024113001      ; Serial
                            604800          ; Refresh
                            86400           ; Retry
```

```
                            2419200         ; Expire
                            604800 )        ; Negative Cache TTL

; Name Servers
@       IN      NS      ns1.bostondns.local.
@       IN      NS      ns2.bostondns.local.

; Mail Server
@       IN      MX      10 mail.bostondns.local.

; A Records for Name Servers
ns1     IN      A       172.16.204.10
ns2     IN      A       172.16.204.11

; AAAA Records for Name Servers
ns1     IN      AAAA    fd00:0:0:10::10
ns2     IN      AAAA    fd00:0:0:10::11

; A Records for Hosts
www     IN      A       172.16.204.110
mail    IN      A       172.16.204.111

; AAAA Records for Hosts
www     IN      AAAA    fd00:0:0:10::110
mail    IN      AAAA    fd00:0:0:10::111
```

sudo nano /etc/bind/zones/db.172.16.204

```
$TTL    604800
@       IN      SOA     ns1.bostondns.local. admin.bostondns.local. (
                            2024113001      ; Serial
                            604800          ; Refresh
                            86400           ; Retry
                            2419200         ; Expire
                            604800 )        ; Negative Cache TTL

; Name Servers
@       IN      NS      ns1.bostondns.local.
@       IN      NS      ns2.bostondns.local.

; PTR Records
10      IN      PTR     ns1.bostondns.local.
11      IN      PTR     ns2.bostondns.local.
110     IN      PTR     www.bostondns.local.
111     IN      PTR     mail.bostondns.local.
```

sudo nano /etc/bind/zones/db.fd00.0.0.10

CONFIGURING DNS RECORDS AND NAME SERVERS

```
$TTL    604800
@       IN      SOA     ns1.bostondns.local. admin.bostondns.local. (
                              2024113001      ; Serial
                              604800          ; Refresh
                              86400           ; Retry
                              2419200         ; Expire
                              604800 )        ; Negative Cache TTL
```

```
; Name Servers
@       IN      NS      ns1.bostondns.local.
@       IN      NS      ns2.bostondns.local.

; PTR Records
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.d.f.ip6.arpa. IN PTR ns1.bostondns.local.
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.0.d.f.ip6.arpa. IN PTR ns2.bostondns.local.
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.d.f.ip6.arpa. IN PTR www.bostondns.local.
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.1.0.d.f.ip6.arpa. IN PTR mail.bostondns.local.
```

sudo named-checkzone bostondns.local /etc/bind/zones/db.bostondns.local

sudo named-checkzone 204.16.172.in-addr.arpa /etc/bind/zones/db.172.16.204

sudo named-checkzone 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.d.f.ip6.arpa /etc/bind/zones/db.fd00.0.0.10

Sudo ufw allow 53/tcp

Sudo ufw allow 53/udp

sudo systemctl restart bind9

sudo systemctl enable bind9

CHECKING CONFIGURATION AND RESTARTING BIND9 DNS SERVER

3. VM2

sudo apt update

sudo apt install bind9 bind9utils

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

THIS IS SLAVE DNS

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

        recursion yes;
        allow-query { any; };

        forwarders {
            8.8.8.8;
            8.8.4.4;
        };

        dnssec-validation auto;

        auth-nxdomain no;
        listen-on { any; };
        listen-on-v6 {any; };


        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        // forwarders {
        //      0.0.0.0;
        // };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
```

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

```
// Forward Zone
zone "bostonstartup.com" {
    type slave;
    masters { 172.16.204.10; };
    file "/var/cache/bind/db.bostonstartup.com";
};

// Reverse Zone for IPv4
zone "204.16.172.in-addr.arpa" {
    type slave;
    masters { 172.16.204.10; };
    file "/var/cache/bind/db.172.16.204";
};

// Reverse Zone for IPv6
zone "0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.d.f.ip6.arpa" {
    type slave;
    masters { 172.16.204.10; };
    file "/var/cache/bind/db.fd00.0.0.10";
};
```

sudo systemctl restart bind9

CONFIGURING ZONES IN DNS SLAVE

4. VM3

sudo apt update

sudo apt install apache2

sudo apt install ufw

sudo nano /etc/apache2/sites-available/bostondns.local.conf

```
<VirtualHost *:80>
        ServerName www.bostonstartup.com
        ServerAlias bostonstartup.com
        Redirect permanent / https://www.bostonstartup.com/
        DocumentRoot /var/www/bostonstartup.com/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

sudo mkdir -p /var/www/web.local.lab

sudo nano /var/www/bostondns.local/html/index.html

```
<html>
        <head>
                <title>Welcome to bostonstartup.com!!!</title>
        </head>
        <body>
                <h1>Team Mememberss: You Li, Rohith Datla, Cheng-Yu Chang</h1>
        </body>
</html>
```

sudo chown -R www-data:www-data /var/www/web.local.lab

sudo a2ensite bostondns.local.conf

sudo a2dissite 000-default.conf

sudo systemctl reload apache2

sudo ufw reset

```
web_server@webserver:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
Anywhere                   DENY IN     172.16.204.60
80                         ALLOW IN    172.16.204.0/24
443                        ALLOW IN    172.16.204.0/24
22                         ALLOW IN    172.16.204.0/24
Anywhere (v6)              DENY IN     fd00:0:0:10::60
Anywhere (v6)              DENY IN     fd00::10:20c:29ff:fefa:5a66
22                         ALLOW IN    fd00:0:0:10::/64
80                         ALLOW IN    fd00:0:0:10::/64
443                        ALLOW IN    fd00:0:0:10::/64
```

sudo ufw enable
sudo systemctl status apache2
sudo ufw status
sudo apt install fail2ban -y
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
sudo nano /etc/fail2ban/jail.local

```
[apache]
enabled  = true
port     = http,https
filter   = apache-auth
logpath  = /var/log/apache*/*error.log
maxretry = 3
```

sudo systemctl restart fail2ban
sudo systemctl enable fail2ban
sudo apache2ctl -M
sudo a2dismod status
sudo a2dismod autoindex
sudo systemctl restart apache2
sudo apt install certbot python3-certbot-apache -y
sudo certbot --apache -d www.bostondns.local -d bostondns.local
sudo nano /etc/apache2/sites-available/bostondns.local.conf

```
<VirtualHost *:80>
    ServerName www.bostondns.local
    ServerAlias bostondns.local
    Redirect permanent / https://www.bostondns.local/
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

sudo nano /etc/ssh/sshd_config (Port 2222)
sudo ufw allow 2222/tcp
sudo ufw delete allow OpenSSH
sudo systemctl restart sshd

```
[sshd]
enabled = true
port    = 2222
filter  = sshd
logpath = /var/log/auth.log
maxretry = 5
```

sudo systemctl restart fail2ban

5.VM4

sudo apt install rsync -y

sudo mkdir -p /backup/dns

sudo nano /usr/local/bin/backup_dns.sh

```
#!/bin/bash

# Variables
MASTER_IP="172.16.204.10"
BACKUP_DIR="/backup/dns"
LOG_FILE="/var/log/backup_dns.log"

# Rsync Zone Files from Master to Backup
rsync -avz root@${MASTER_IP}:/etc/bind/zones/ ${BACKUP_DIR}/zones/ >> ${LOG_FILE} 2>&1

# Rsync Configuration Files
rsync -avz root@${MASTER_IP}:/etc/bind/named.conf* ${BACKUP_DIR}/bind_configs/ >> ${LOG_FILE} 2>&1

# Log Completion
echo "DNS backup completed on $(date)" >> ${LOG_FILE}
```

sudo chmod +x /usr/local/bin/backup_dns.sh

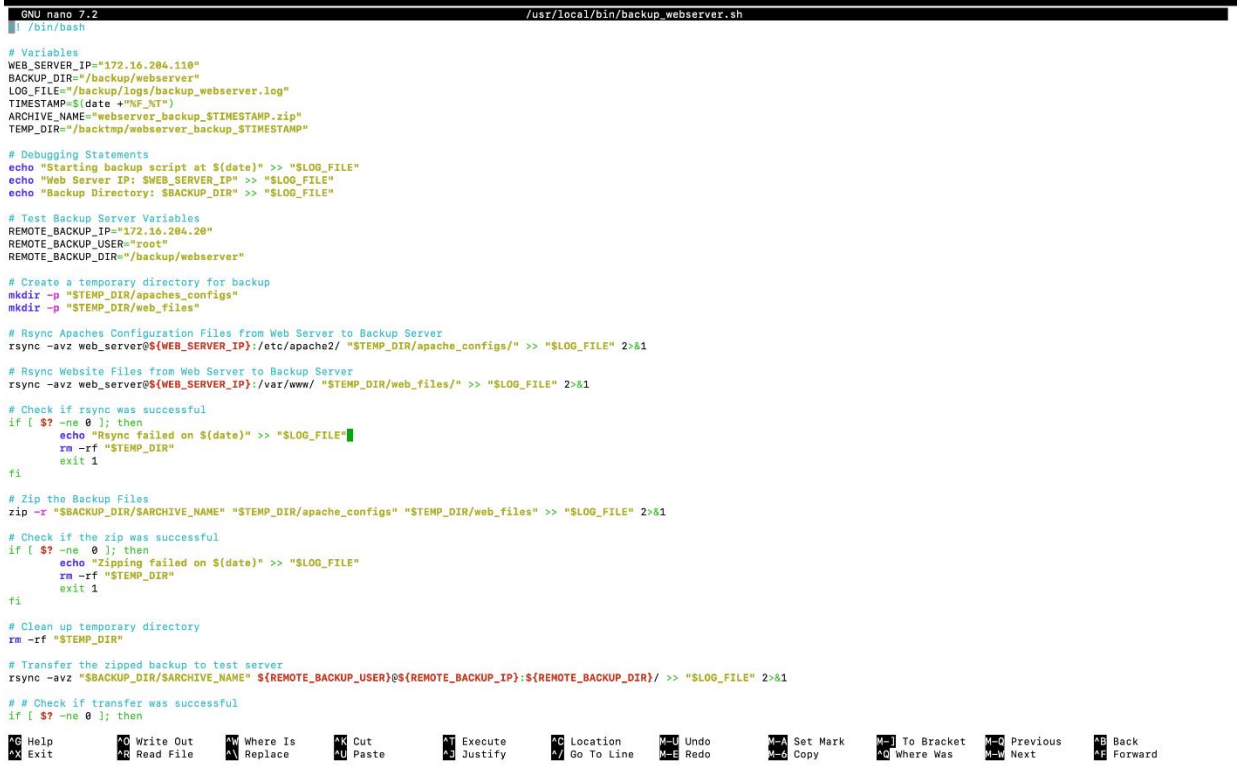
ssh-keygen -t rsa -b 4096 -C backup@bostondns.local

ssh-copy-id root@172.16.204.10

sudo crontab -e

```
0 2 * * * /usr/local/bin/backup_dns.sh
```

sudo nano /usr/local/bin/backup_dns.sh



```
 GNU nano 7.2                                                    /usr/local/bin/backup_webserver.sh
#! /bin/bash

# Variables
WEB_SERVER_IP="172.16.204.110"
BACKUP_DIR="/backup/webserver"
LOG_FILE="/backup/logs/backup_webserver.log"
TIMESTAMP=$(date +"%F_%T")
ARCHIVE_NAME="webserver_backup_$TIMESTAMP.zip"
TEMP_DIR="/backtmp/webserver_backup_$TIMESTAMP"

# Debugging Statements
echo "Starting backup script at $(date)" >> "$LOG_FILE"
echo "Web Server IP: $WEB_SERVER_IP" >> "$LOG_FILE"
echo "Backup Directory: $BACKUP_DIR" >> "$LOG_FILE"

# Test Backup Server Variables
REMOTE_BACKUP_IP="172.16.204.20"
REMOTE_BACKUP_USER="root"
REMOTE_BACKUP_DIR="/backup/webserver"

# Create a temporary directory for backup
mkdir -p "$TEMP_DIR/apaches_configs"
mkdir -p "$TEMP_DIR/web_files"

# Rsync Apaches Configuration Files from Web Server to Backup Server
rsync -avz web_server@${WEB_SERVER_IP}:/etc/apache2/ "$TEMP_DIR/apache_configs/" >> "$LOG_FILE" 2>&1

# Rsync Website Files from Web Server to Backup Server
rsync -avz web_server@${WEB_SERVER_IP}:/var/www/ "$TEMP_DIR/web_files/" >> "$LOG_FILE" 2>&1

# Check if rsync was successful
if [ $? -ne 0 ]; then
        echo "Rsync failed on $(date)" >> "$LOG_FILE"
        rm -rf "$TEMP_DIR"
        exit 1
fi

# Zip the Backup Files
zip -r "$BACKUP_DIR/$ARCHIVE_NAME" "$TEMP_DIR/apache_configs" "$TEMP_DIR/web_files" >> "$LOG_FILE" 2>&1

# Check if the zip was successful
if [ $? -ne  0 ]; then
        echo "Zipping failed on $(date)" >> "$LOG_FILE"
        rm -rf "$TEMP_DIR"
        exit 1
fi

# Clean up temporary directory
rm -rf "$TEMP_DIR"

# Transfer the zipped backup to test server
rsync -avz "$BACKUP_DIR/$ARCHIVE_NAME" ${REMOTE_BACKUP_USER}@${REMOTE_BACKUP_IP}:${REMOTE_BACKUP_DIR}/ >> "$LOG_FILE" 2>&1

# # Check if transfer was successful
if [ $? -ne 0 ]; then

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo         M-A Set Mark     M-] To Bracket   M-Q Previous     ^B Back
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo         M-6 Copy         ^Q Where Was     M-W Next         ^F Forward
```

```
 GNU nano 7.2                                                    /usr/local/bin/backup_webserver.sh
TEMP_DIR="/backtmp/webserver_backup_$TIMESTAMP"

# Debugging Statements
echo "Starting backup script at $(date)" >> "$LOG_FILE"
echo "Web Server IP: $WEB_SERVER_IP" >> "$LOG_FILE"
echo "Backup Directory: $BACKUP_DIR" >> "$LOG_FILE"

# Test Backup Server Variables
REMOTE_BACKUP_IP="172.16.204.20"
REMOTE_BACKUP_USER="root"
REMOTE_BACKUP_DIR="/backup/webserver"

# Create a temporary directory for backup
mkdir -p "$TEMP_DIR/apaches_configs"
mkdir -p "$TEMP_DIR/web_files"

# Rsync Apaches Configuration Files from Web Server to Backup Server
rsync -avz web_server@${WEB_SERVER_IP}:/etc/apache2/ "$TEMP_DIR/apache_configs/" >> "$LOG_FILE" 2>&1

# Rsync Website Files from Web Server to Backup Server
rsync -avz web_server@${WEB_SERVER_IP}:/var/www/ "$TEMP_DIR/web_files/" >> "$LOG_FILE" 2>&1

# Check if rsync was successful
if [ $? -ne 0 ]; then
        echo "Rsync failed on $(date)" >> "$LOG_FILE"
        rm -rf "$TEMP_DIR"
        exit 1
fi

# Zip the Backup Files
zip -r "$BACKUP_DIR/$ARCHIVE_NAME" "$TEMP_DIR/apache_configs" "$TEMP_DIR/web_files" >> "$LOG_FILE" 2>&1

# Check if the zip was successful
if [ $? -ne  0 ]; then
        echo "Zipping failed on $(date)" >> "$LOG_FILE"
        rm -rf "$TEMP_DIR"
        exit 1
fi

# Clean up temporary directory
rm -rf "$TEMP_DIR"

# Transfer the zipped backup to test server
rsync -avz "$BACKUP_DIR/$ARCHIVE_NAME" ${REMOTE_BACKUP_USER}@${REMOTE_BACKUP_IP}:${REMOTE_BACKUP_DIR}/ >> "$LOG_FILE" 2>&1

# # Check if transfer was successful
if [ $? -ne 0 ]; then
    echo "Transfer to remote server failed on $(date)" >> "$LOG_FILE"
    echo "Check permissions for ${REMOTE_BACKUP_DIR} on ${REMOTE_BACKUP_IP}" >> "$LOG_FILE"
    exit 1
fi

# Log Completion
echo "Web server backup completed successfully on $(date)" >> "$LOG_FILE"

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo         M-A Set Mark     M-] To Bracket   M-Q Previous     ^B Back
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo         M-6 Copy         ^Q Where Was     M-W Next         ^F Forward
```

sudo /usr/local/bin/backup_dns.sh

sudo cat /var/log/backup_dns.log

6.VM6

VM7-MITM attack
install python and pip **sudo apt install python3 python3-pip -y** **pip3 install scapy**  **sudo python3 arp_spoof.py**

7.VM8, VM9

Vpn server	Vpn client

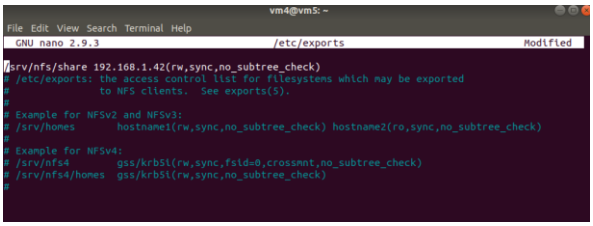
sudo apt update

sudo apt install strongswan strongswan-pki

sudo apt install nfs-kernel-server

sudo nano/etc/exports

/shared_directory 192.168.1.42(rw,sync,no_subtree_check



sudo mkdir -p /shared_directory

sudo chmod 777 /shared_directory

sudo systemctl restart nfs-kernel-server

sudo nano /etc/ipsec.conf

config setup

charondebug="ike 2, knl 2, cfg 2"

conn vpn

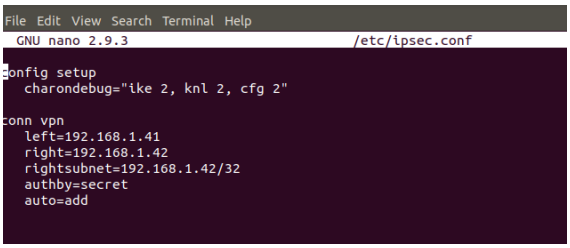
left=192.168.1.41

right=192.168.1.42

rightsubnet=192.168.1.42/32

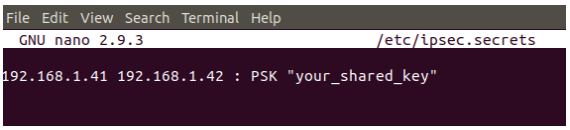
authby=secret

auto=start



sudo nano /etc/ipsec.secrets

192.168.1.41 192.168.1.42 : PSK "your_shared_key"



sudo systemctl restart strongswan

sudo ufw enable

sudo ufw allow 500/udp

sudo ufw allow 4500/udp

sudo ufw allow from 192.168.1.42 to any port nfs

sudo ufw reload

sudo ipsec up vpn

sudo ipsec status

sudo apt update

sudo apt install strongswan strongswan-pki

sudo apt install nfs-common

sudo mkdir -p /mnt

sudo mount -t nfs 192.168.1.41:/srv/nfs/share /mnt

sudo nano /etc/fstab

192.168.1.41:/shared_directory /mnt nfs defaults 0 0

sudo nano /etc/ipsec.conf

config setup

charondebug="ike 2, knl 2, cfg 2"

conn vpn

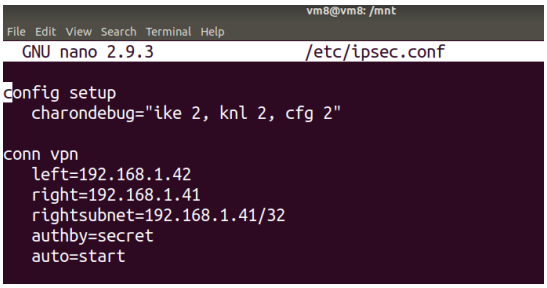
left=192.168.1.42

right=192.168.1.41

rightsubnet=192.168.1.41/32

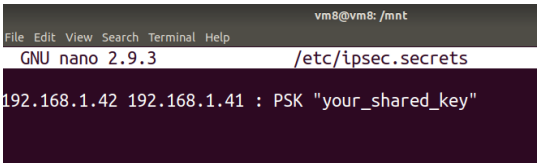
authby=secret

auto=start



sudo nano /etc/ipsec.secrets

192.168.1.42 192.168.1.41: PSK "your_shared_key"



sudo systemctl restart strongswan

sudo ufw enable

sudo ufw allow 500/udp

sudo ufw allow 4500/udp

sudo ufw reload

sudo ipsec up vpn

sudo ipsec status

Test plan:

1.DHCP, Master DNS, Webserver

DHCP:

- Configure VM7 (test client) to request an IP address dynamically using DHCP.
- VM7 should obtain an IP address dynamically from VM1 (DHCP server).

Webserver:

- On VM7 (test client), use Firefox to browse 172.16.204.110 (IP of VM3, which runs the webserver). (If VM did not have GUI try `curl www.bostonstartup.com`)
- VM7 should display the webpage hosted by VM3 (webserver) or HTML code if you're not using GUI.

DNS:

- On VM7 (test client), use Firefox to browse www.bostonstartup.com. (If VM did not have GUI try `curl www.bostonstartup.com`)
- VM1 (DNS server) should resolve www.bostonstartup.com to 172.16.204.110, and VM7 should display the webpage hosted by VM3 (webserver).(IN terminal it will show you the HTML document)

2. Slave DNS

- Setup: Shut down the DNS service on VM1 (master DNS).
    - VM2 (slave DNS) should take over DNS services.
    - On VM7 (client), using Firefox to browse www.bostonstartup.com, VM2 should resolve the domain to 172.16.204.110 (IP of VM3).

3.Backup Server

- Setup: Shut down the webserver service on VM3.
    - VM7 (client) using Firefox to browse www.bostonstartup.com should be directed to 172.16.204.12 (VM4, backup server).
    - VM1 (master DNS) should resolve www.bostonstartup.com to 172.16.204.12.

4. Firewall

- Set VM6's static IP to 172.16.204.60 (outside the allowed subnet range).
- Attempt to curl the www.bostonstartup.com in VM6 terminal
- VM3 (firewall) should block VM6's access to the webserver.

5.VPN tunnel

- VM5(vpn server) and VM6(vpn client) set up vpn tunnel, VM5 create txt file in /srv/nfs/share , and VM6 should see the same txt file in it's /mnt (ls -l /mnt/).

Test results:

1.DHCP, Master DNS, Webserver

```
[test-backup-server@test-backup-server:~$ ping6 www.bostonstartup.com
PING www.bostonstartup.com (fd00:0:0:10::110) 56 data bytes
64 bytes from fd00:0:0:10::110: icmp_seq=1 ttl=64 time=1.49 ms
64 bytes from fd00:0:0:10::110: icmp_seq=2 ttl=64 time=0.760 ms
64 bytes from fd00:0:0:10::110: icmp_seq=3 ttl=64 time=1.46 ms
64 bytes from fd00:0:0:10::110: icmp_seq=4 ttl=64 time=1.19 ms
64 bytes from fd00:0:0:10::110: icmp_seq=5 ttl=64 time=1.88 ms
^C
--- www.bostonstartup.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4068ms
rtt min/avg/max/mdev = 0.760/1.356/1.883/0.370 ms
```

```
● isc-dhcp-server.service - ISC DHCP IPv4 server
     Loaded: loaded (/usr/lib/systemd/system/isc-dhcp-server.service; enabled; preset: enabled)
     Active: active (running) since Mon 2024-12-02 01:43:58 UTC; 21min ago
       Docs: man:dhcpd(8)
   Main PID: 1208 (dhcpd)
      Tasks: 1 (limit: 4550)
     Memory: 5.8M (peak: 6.3M)
        CPU: 67ms
     CGroup: /system.slice/isc-dhcp-server.service
             └─1208 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhcp/dhc>

Dec 02 02:02:39 dnsmaster-dhcp-server dhcpd[1208]: DHCPREQUEST for 172.16.204.104 from 00:0c:29:4e:77:c2 >
Dec 02 02:02:39 dnsmaster-dhcp-server dhcpd[1208]: DHCPACK on 172.16.204.104 to 00:0c:29:4e:77:c2 (webser>
Dec 02 02:03:38 dnsmaster-dhcp-server dhcpd[1208]: DHCPDISCOVER from 00:0c:29:6a:4b:ff (dnsmaster-dhcp-se>
Dec 02 02:03:39 dnsmaster-dhcp-server dhcpd[1208]: DHCPOFFER on 172.16.204.100 to 00:0c:29:6a:4b:ff (dnsm>
Dec 02 02:03:53 dnsmaster-dhcp-server dhcpd[1208]: DHCPDISCOVER from 00:0c:29:df:81:e3 via ens160
Dec 02 02:03:54 dnsmaster-dhcp-server dhcpd[1208]: DHCPOFFER on 172.16.204.102 to 00:0c:29:df:81:e3 (test>
Dec 02 02:03:54 dnsmaster-dhcp-server dhcpd[1208]: DHCPREQUEST for 172.16.204.102 (172.16.204.10) from 00>
Dec 02 02:03:54 dnsmaster-dhcp-server dhcpd[1208]: DHCPACK on 172.16.204.102 to 00:0c:29:df:81:e3 (test-c>
Dec 02 02:04:43 dnsmaster-dhcp-server dhcpd[1208]: DHCPDISCOVER from 00:0c:29:6a:4b:ff (dnsmaster-dhcp-se>
Dec 02 02:04:44 dnsmaster-dhcp-server dhcpd[1208]: DHCPOFFER on 172.16.204.100 to 00:0c:29:6a:4b:ff (dnsm>
```

```
Last login: Mon Dec  2 01:41:31 2024 from 172.16.204.1
test-client@test-client:~$ sudo dhclient -v
[sudo] password for test-client:
Internet Systems Consortium DHCP Client 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/ens160/00:0c:29:df:81:e3
Sending on   LPF/ens160/00:0c:29:df:81:e3
Sending on   Socket/fallback
xid: warning: no netdev with useable HWADDR found for seed's uniqueness enforcement
xid: rand init seed (0x67321488) built using gethostid
DHCPDISCOVER on ens160 to 255.255.255.255 port 67 interval 3 (xid=0x1a4e546c)
DHCPOFFER of 172.16.204.102 from 172.16.204.10
DHCPREQUEST for 172.16.204.102 on ens160 to 255.255.255.255 port 67 (xid=0x6c544e1a)
DHCPACK of 172.16.204.102 from 172.16.204.10 (xid=0x1a4e546c)
Setting LLMNR support level "yes" for "2", but the global support level is "no".
bound to 172.16.204.102 -- renewal in 232 seconds.
```

```
test-client@test-client:~$ sudo dhclient -6 -v
[sudo] password for test-client:
Internet Systems Consortium DHCP Client 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on Socket/ens160
Sending on   Socket/ens160
xid: warning: no netdev with useable HWADDR found for seed's uniqueness enforcement
xid: rand init seed (0x67324ceb) built using gethostid
PRC: Confirming active lease (INIT-REBOOT).
XMT: Forming Confirm, 0 ms elapsed.
XMT:  X-- IA_NA 29:df:81:e3
XMT:  | X-- Confirm Address fd00:0:0:10::200
XMT:  V IA_NA appended.
XMT: Confirm on ens160, interval 1070ms.
XMT: Forming Confirm, 1070 ms elapsed.
XMT:  X-- IA_NA 29:df:81:e3
XMT:  | X-- Confirm Address fd00:0:0:10::200
XMT:  V IA_NA appended.
XMT: Confirm on ens160, interval 2220ms.
XMT: Forming Confirm, 3290 ms elapsed.
XMT:  X-- IA_NA 29:df:81:e3
XMT:  | X-- Confirm Address fd00:0:0:10::200
XMT:  V IA_NA appended.
XMT: Confirm on ens160, interval 3980ms.
XMT: Forming Confirm, 7280 ms elapsed.
XMT:  X-- IA_NA 29:df:81:e3
XMT:  | X-- Confirm Address fd00:0:0:10::200
XMT:  V IA_NA appended.
XMT: Confirm on ens160, interval 2730ms.
Max retransmission duration exceeded.
PRC: Bound to lease 00:01:00:01:2e:dd:6d:3b:00:0c:29:6a:4b:ff.
Setting LLMNR support level "yes" for "2", but the global support level is "no".
```

```
dnsmaster-dhcp-server@dnsmaster-dhcp-server:~$ sudo systemctl status isc-dhcp-server6
● isc-dhcp-server6.service - ISC DHCP IPv6 server
     Loaded: loaded (/usr/lib/systemd/system/isc-dhcp-server6.service; enabled; preset: enabled)
     Active: active (running) since Mon 2024-12-02 03:38:40 UTC; 2h 27min ago
       Docs: man:dhcpd(8)
   Main PID: 1241 (dhcpd)
      Tasks: 1 (limit: 4550)
     Memory: 3.0M (peak: 3.2M)
        CPU: 32ms
     CGroup: /system.slice/isc-dhcp-server6.service
             └─1241 dhcpd -user dhcpd -group dhcpd -f -6 -pf /run/dhcp-server6/dhcpd6.pid -cf /etc/dhcp/dhcpd6.conf

Dec 02 03:38:40 dnsmaster-dhcp-server dhcpd[1241]: Wrote 1 NA, 0 TA, 0 PD leases to lease file.
Dec 02 03:38:40 dnsmaster-dhcp-server sh[1241]: Bound to *:547
Dec 02 03:38:40 dnsmaster-dhcp-server sh[1241]: Listening on Socket/5/ens160/fd00:0:0:10::/64
Dec 02 03:38:40 dnsmaster-dhcp-server sh[1241]: Sending on   Socket/5/ens160/fd00:0:0:10::/64
Dec 02 03:38:40 dnsmaster-dhcp-server sh[1241]: Can't create PID file /run/dhcp-server6/dhcpd6.pid: Permission denied.
Dec 02 03:38:40 dnsmaster-dhcp-server dhcpd[1241]: Bound to *:547
Dec 02 03:38:40 dnsmaster-dhcp-server dhcpd[1241]: Listening on Socket/5/ens160/fd00:0:0:10::/64
Dec 02 03:38:40 dnsmaster-dhcp-server dhcpd[1241]: Sending on   Socket/5/ens160/fd00:0:0:10::/64
Dec 02 03:38:40 dnsmaster-dhcp-server dhcpd[1241]: Can't create PID file /run/dhcp-server6/dhcpd6.pid: Permission denied.
Dec 02 03:38:40 dnsmaster-dhcp-server dhcpd[1241]: Server starting service.
```

DNS look up

```
test-client@test-client:~$ curl www.bostonstartup.com
<html>
        <head>
                <title>Welcome to bostonstartup.com!!!</title>
        </head>
        <body>
                <h1>Team Mememberss: You Li, Rohith Datla, Cheng-Yu Chang</h1>
        </body>
</html>
```

2. Slave DNS

```
● bind9.service - BIND Domain Name Server
     Loaded: loaded (/etc/systemd/system/bind9.service; enabled; preset: enabled)
     Active: active (running) since Mon 2024-12-02 06:32:49 UTC; 2min 4s ago
       Docs: man:named(8)
   Main PID: 2198 (named)
     Status: "running"
      Tasks: 8 (limit: 4550)
     Memory: 5.7M (peak: 6.2M)
        CPU: 41ms
     CGroup: /system.slice/bind9.service
             └─2198 /usr/sbin/named -f -u bind

Dec 02 06:32:49 dns-slave named[2198]: zone 255.in-addr.arpa/IN: loaded serial 1
Dec 02 06:32:49 dns-slave named[2198]: all zones loaded
Dec 02 06:32:49 dns-slave named[2198]: zone bostonstartup.com/IN: sending notifies (serial 2024113001)
Dec 02 06:32:49 dns-slave named[2198]: zone 204.16.172.in-addr.arpa/IN: sending notifies (serial 2024113001)
Dec 02 06:32:49 dns-slave named[2198]: running
Dec 02 06:32:49 dns-slave systemd[1]: Started bind9.service - BIND Domain Name Server.
Dec 02 06:32:49 dns-slave named[2198]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer co>
Dec 02 06:32:49 dns-slave named[2198]: zone 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.d.f.ip6.ar>
Dec 02 06:32:59 dns-slave named[2198]: resolver priming query complete: timed out
Dec 02 06:33:45 dns-slave named[2198]: zone 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.d.f.ip6.ar>
```

3.Backup Server

```
test-backup-server@test-backup-server:~$ sudo ls /backup/webserver
[sudo] password for test-backup-server:
webserver_backup_2024-12-02_05:25:31.zip  webserver_backup_2024-12-02_20:31:16.zip
```

```
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/authz_owner.load (deflated 24%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/ldap.load (deflated 18%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/dump_io.load (deflated 20%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/proxy_ftp.conf (deflated 5%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/authnz_fcgi.load (deflated 24%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/remoteip.load (deflated 22%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/expires.load (deflated 21%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/proxy_fdpass.load (deflated 25%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/auth_digest.load (deflated 22%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/headers.load (deflated 21%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/dav_fs.load (deflated 19%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/authz_host.load (deflated 23%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/proxy_connect.load (deflated 25%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/ssl.load (deflated 15%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/socache_memcache.load (deflated 36%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/proxy_http2.load (deflated 26%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/proxy_html.load (deflated 22%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/cgi.load (deflated 17%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/proxy_html.conf (deflated 57%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/ext_filter.load (deflated 24%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/mime.conf (deflated 62%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/ssl.conf (deflated 52%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/cache_disk.load (deflated 26%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/proxy_uwsgi.load (deflated 24%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/authn_anon.load (deflated 24%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/session.load (deflated 21%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/info.conf (deflated 33%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/cern_meta.load (deflated 23%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/authz_user.load (deflated 23%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/reqtimeout.conf (deflated 51%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/proxy_ajp.load (deflated 23%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/proxy_http.load (deflated 24%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/dav.load (deflated 27%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/alias.conf (deflated 46%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/cgid.load (deflated 18%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/request.load (deflated 21%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/dav_fs.conf (deflated 5%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/log_forensic.load (deflated 25%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/vhost_alias.load (deflated 24%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/lbmethod_byrequests.load (deflated 23%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/brotli.load (deflated 20%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/mods-available/sed.load (deflated 17%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/sites-available/ (stored 0%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/sites-available/bostonstartup.com.conf (deflated 33%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/sites-available/000-default.conf (deflated 46%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/apache_configs/sites-available/default-ssl.conf (deflated 59%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/web_files/ (stored 0%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/web_files/bostonstartup.com/ (stored 0%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/web_files/bostonstartup.com/html/ (stored 0%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/web_files/bostonstartup.com/html/index.html (deflated 20%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/web_files/html/ (stored 0%)
  adding: backtmp/webserver_backup_2024-12-02_20:31:16/web_files/html/index.html (deflated 71%)
sending incremental file list
webserver_backup_2024-12-02_20:31:16.zip

sent 44,089 bytes  received 35 bytes  4,644.63 bytes/sec
total size is 112,887  speedup is 2.56
Web server backup completed successfully on Mon Dec  2 20:31:27 UTC 2024
backup-server@backup-server:~$
```

4. Firewall

```
web_server@webserver:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
Anywhere                   DENY IN     172.16.204.60
80                         ALLOW IN    172.16.204.0/24
443                        ALLOW IN    172.16.204.0/24
22                         ALLOW IN    172.16.204.0/24
Anywhere (v6)              DENY IN     fd00:0:0:10::60
Anywhere (v6)              DENY IN     fd00::10:20c:29ff:fefa:5a66
22                         ALLOW IN    fd00:0:0:10::/64
80                         ALLOW IN    fd00:0:0:10::/64
443                        ALLOW IN    fd00:0:0:10::/64
```

```
attacker@attacker:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:fa:5a:66 brd ff:ff:ff:ff:ff:ff
    altname enp2s0
    inet 172.16.204.60/24 brd 172.16.204.255 scope global ens160
       valid_lft forever preferred_lft forever
    inet6 fd00::10:20c:29ff:fefa:5a66/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86381sec preferred_lft 14381sec
    inet6 fd00:0:0:10::60/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fefa:5a66/64 scope link
       valid_lft forever preferred_lft forever
attacker@attacker:~$ curl http://www.bostonstartup.com
curl: (28) Failed to connect to www.bostonstartup.com port 80 after 133242 ms: Couldn't connect to serv
er
```

5. MITM:

Python Script running

```
attacker@attacker:~$ sudo python3 mitm.py
 [*] Resolving MAC addresses...
 Target MAC: 00:0c:29:df:81:e3
 Gateway MAC: 00:50:56:f6:b6:75
 [*] Starting ARP poisoning. Press CTRL+C to stop...
 [+] Packets sent: 104
```

Before attack

```
test-client@test-client:~$ arp -a
ns1.bostonstartup.com (172.16.204.10) at 00:0c:29:6a:4b:ff [ether] on ens160
_gateway (172.16.204.2) at 00:50:56:f6:b6:75 [ether] on ens160
? (172.16.204.60) at 00:0c:29:fa:5a:66 [ether] on ens160
? (172.16.204.1) at 6e:b1:33:1a:47:65 [ether] on ens160
```

During attack

```
test-client@test-client:~$ ping 172.16.204.2
PING 172.16.204.2 (172.16.204.2) 56(84) bytes of data.
From 172.16.204.60: icmp_seq=1 Redirect Host(New nexthop: 172.16.204.2)
64 bytes from 172.16.204.2: icmp_seq=1 ttl=127 time=3.07 ms
From 172.16.204.60: icmp_seq=2 Redirect Host(New nexthop: 172.16.204.2)
64 bytes from 172.16.204.2: icmp_seq=2 ttl=127 time=4.25 ms
From 172.16.204.60: icmp_seq=3 Redirect Host(New nexthop: 172.16.204.2)
64 bytes from 172.16.204.2: icmp_seq=3 ttl=127 time=4.69 ms
From 172.16.204.60: icmp_seq=4 Redirect Host(New nexthop: 172.16.204.2)
64 bytes from 172.16.204.2: icmp_seq=4 ttl=127 time=1.85 ms
From 172.16.204.60: icmp_seq=5 Redirect Host(New nexthop: 172.16.204.2)
64 bytes from 172.16.204.2: icmp_seq=5 ttl=127 time=2.50 ms
^C
--- 172.16.204.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4018ms
rtt min/avg/max/mdev = 1.852/3.272/4.693/1.061 ms
test-client@test-client:~$
test-client@test-client:~$
test-client@test-client:~$ arp -a
ns1.bostonstartup.com (172.16.204.10) at 00:0c:29:6a:4b:ff [ether] on ens160
_gateway (172.16.204.2) at 00:0c:29:fa:5a:66 [ether] on ens160
? (172.16.204.60) at 00:0c:29:fa:5a:66 [ether] on ens160
? (172.16.204.1) at 6e:b1:33:1a:47:65 [ether] on ens160
```

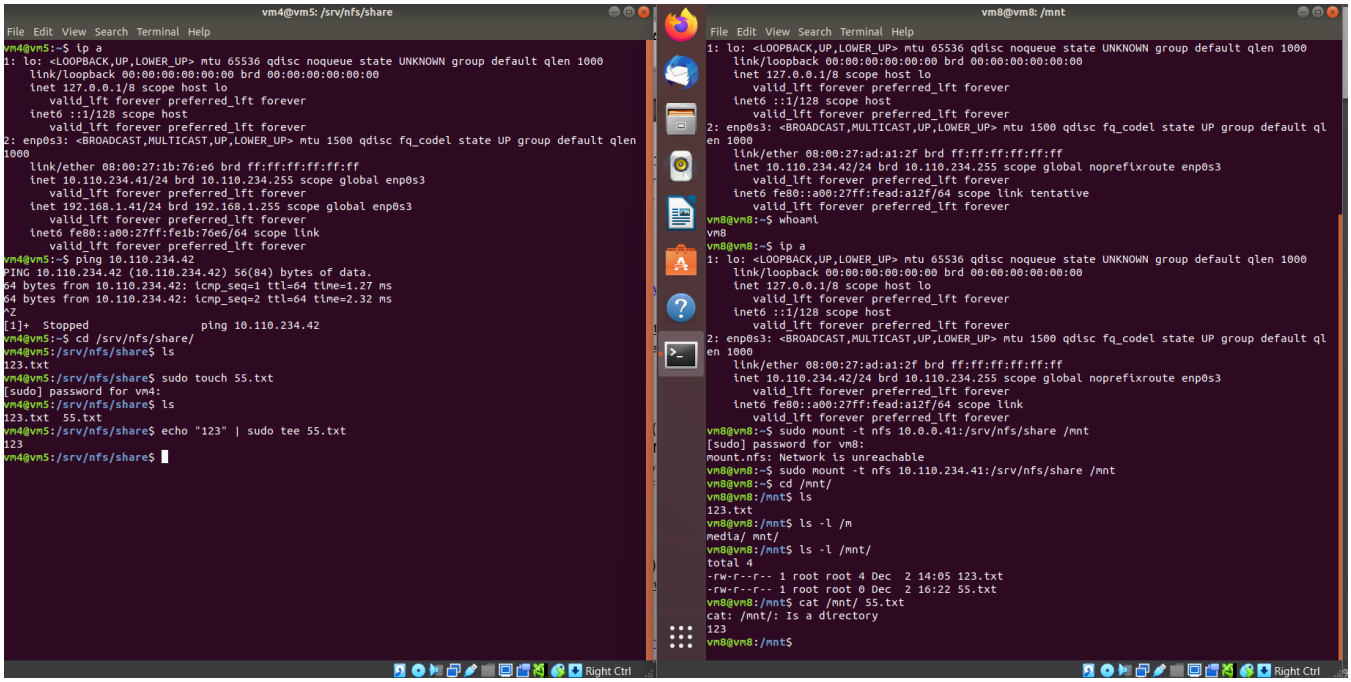
Note: - You can see during the poisoning mac address of gateway is same as attacker’ s mac address

After attack

```
test-client@test-client:~$ arp -a
ns1.bostonstartup.com (172.16.204.10) at 00:0c:29:6a:4b:ff [ether] on ens160
_gateway (172.16.204.2) at 00:50:56:f6:b6:75 [ether] on ens160
? (172.16.204.60) at 00:0c:29:fa:5a:66 [ether] on ens160
? (172.16.204.1) at 6e:b1:33:1a:47:65 [ether] on ens160
```

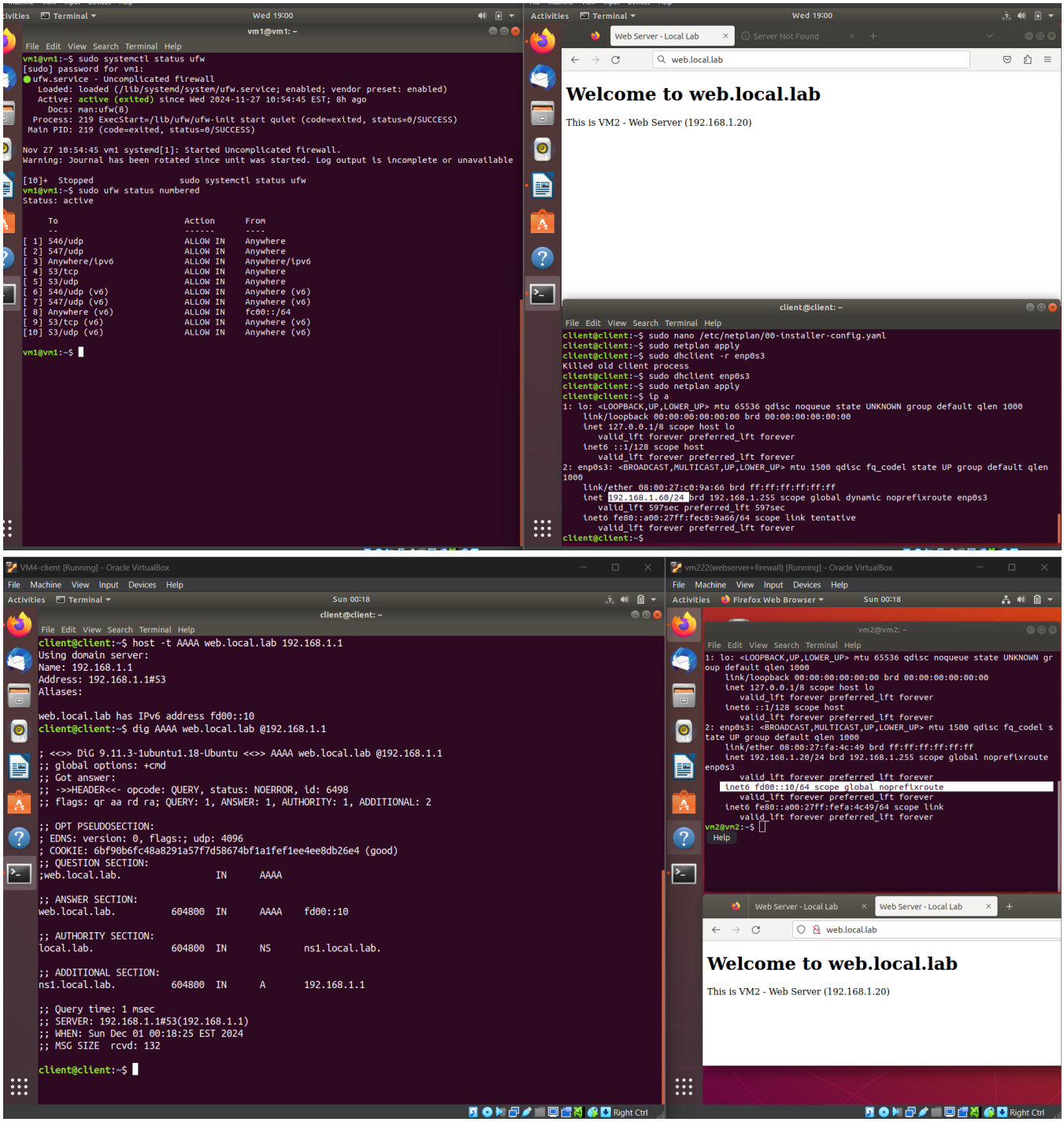
(goes back to normal)

5.VPN tunnel

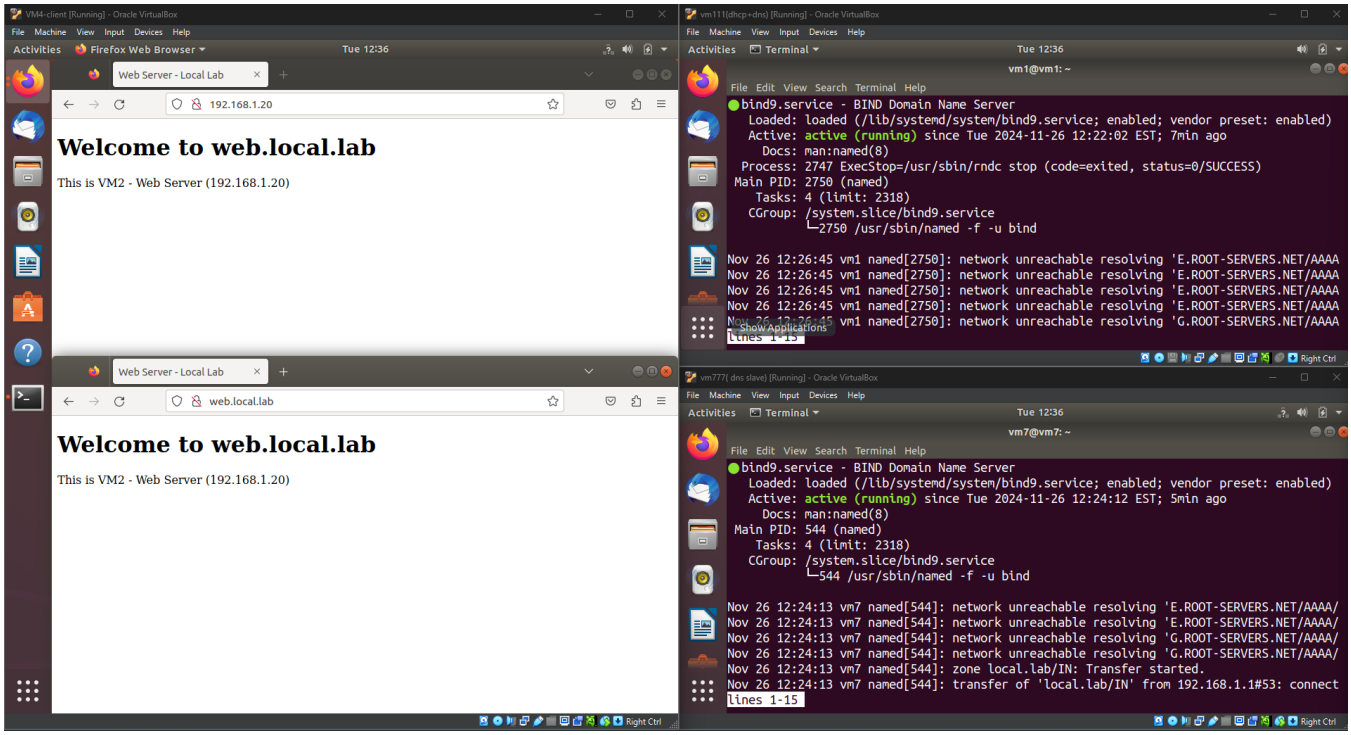


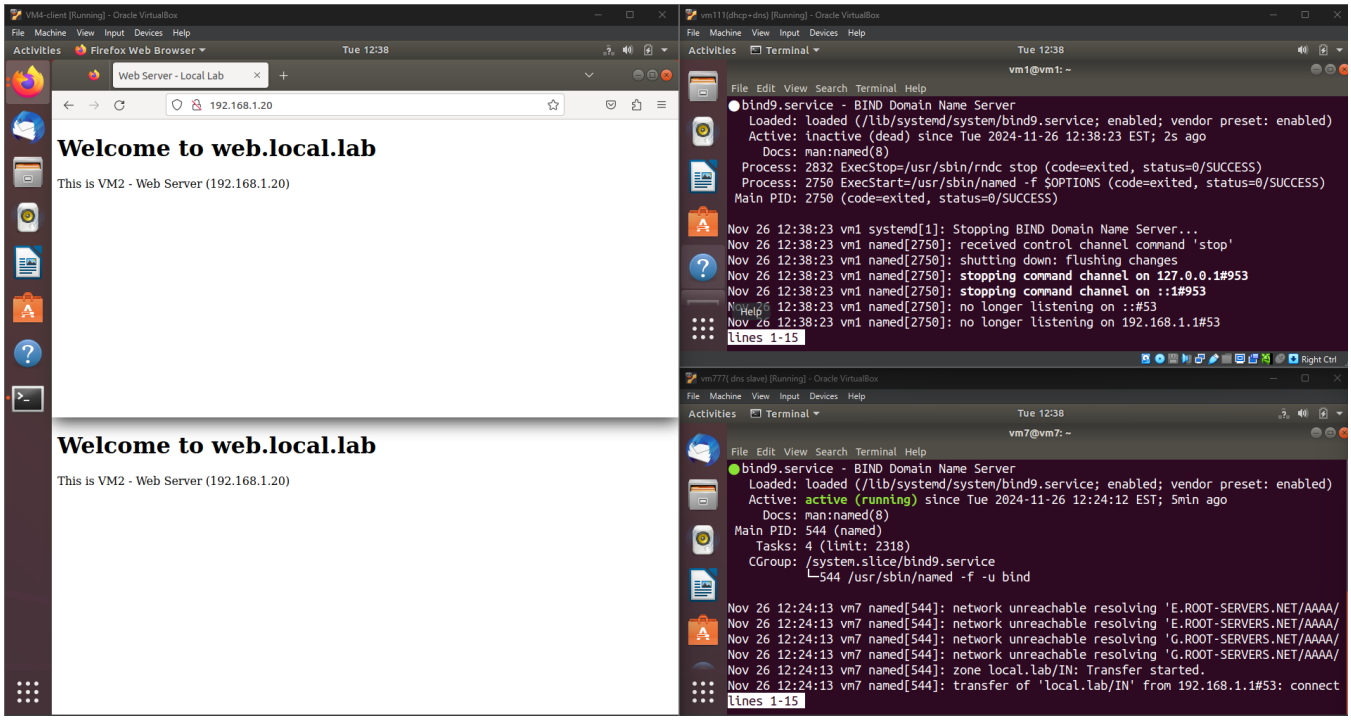
Test result from other VM (windows/ with GUI)

1.DHCP, master DNS, webserver

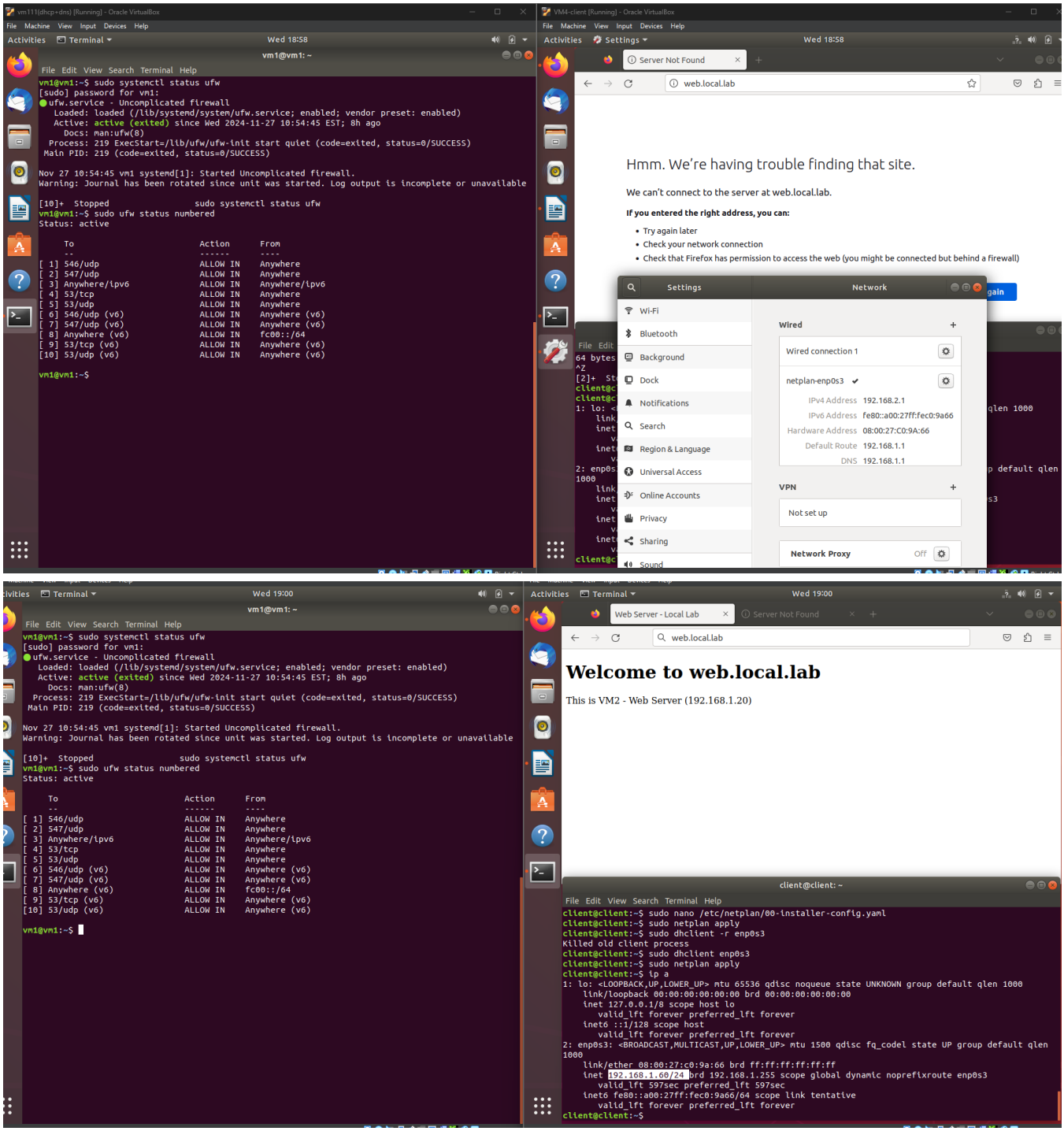

vm1@vm1: ~
vm1@vm1:~$ sudo systemctl status ufw
[sudo] password for vm1:
● ufw.service - Uncomplicated firewall
Loaded: loaded (/lib/systemd/system/ufw.service; enabled; vendor preset: enabled)
Active: active (exited) since Wed 2024-11-27 10:54:45 EST; 8h ago
Docs: man:ufw(8)
Process: 219 ExecStart=/lib/ufw/ufw-init start quiet (code=exited, status=0/SUCCESS)
Main PID: 219 (code=exited, status=0/SUCCESS)
Nov 27 10:54:45 vm1 systemd[1]: Started Uncomplicated firewall.
Warning: Journal has been rotated since unit was started. Log output is incomplete or unavailable
[10]+ Stopped sudo systemctl status ufw
vm1@vm1:~$ sudo ufw status numbered
Status: active
To Action From
[1] 546/udp ALLOW IN Anywhere
[2] 547/udp ALLOW IN Anywhere
[3] Anywhere/ipv6 ALLOW IN Anywhere/ipv6
[4] 53/tcp ALLOW IN Anywhere
[5] 53/udp ALLOW IN Anywhere
[6] 546/udp (v6) ALLOW IN Anywhere (v6)
[7] 547/udp (v6) ALLOW IN Anywhere (v6)
[8] Anywhere (v6) ALLOW IN fc00::/64
[9] 53/tcp (v6) ALLOW IN Anywhere (v6)
[10] 53/udp (v6) ALLOW IN Anywhere (v6)
vm1@vm1:~$
Web Server - Local Lab
web.local.lab
Welcome to web.local.lab
This is VM2 - Web Server (192.168.1.20)
client@client: ~
client@client:~$ sudo nano /etc/netplan/00-installer-config.yaml
client@client:~$ sudo netplan apply
client@client:~$ sudo dhclient -r enp0s3
Killed old client process
client@client:~$ sudo dhclient enp0s3
client@client:~$ sudo netplan apply
client@client:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:c0:9a:66 brd ff:ff:ff:ff:ff:ff
inet 192.168.1.60/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
valid_lft 597sec preferred_lft 597sec
inet6 fe80::a00:27ff:fec0:9a66/64 scope link tentative
valid_lft forever preferred_lft forever
client@client:~$
VM4-client [Running] - Oracle VirtualBox
client@client: ~
client@client:~$ host -t AAAA web.local.lab 192.168.1.1
Using domain server:
Name: 192.168.1.1
Address: 192.168.1.1#53
Aliases:
web.local.lab has IPv6 address fd00::10
client@client:~$ dig AAAA web.local.lab @192.168.1.1
; <<>> DiG 9.11.3-1ubuntu1.18-Ubuntu <<>> AAAA web.local.lab @192.168.1.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6498
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 6bf90b6fc48a8291a57f7d58674bf1a1fef1ee4ee8db26e4 (good)
;; QUESTION SECTION:
;web.local.lab. IN AAAA
;; ANSWER SECTION:
web.local.lab. 604800 IN AAAA fd00::10
;; AUTHORITY SECTION:
local.lab. 604800 IN NS ns1.local.lab.
;; ADDITIONAL SECTION:
ns1.local.lab. 604800 IN A 192.168.1.1
;; Query time: 1 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Sun Dec 01 00:18:25 EST 2024
;; MSG SIZE rcvd: 132
client@client:~$
vm222(webserver+firewall) [Running] - Oracle VirtualBox
vm2@vm2: ~
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:fa:4c:49 brd ff:ff:ff:ff:ff:ff
inet 192.168.1.20/24 brd 192.168.1.255 scope global noprefixroute enp0s3
valid_lft forever preferred_lft forever
inet6 fd00::10/64 scope global noprefixroute
valid_lft forever preferred_lft forever
inet6 fe80::a00:27ff:fefa:4c49/64 scope link
valid_lft forever preferred_lft forever
vm2@vm2:~$
Web Server - Local Lab
web.local.lab
Welcome to web.local.lab
This is VM2 - Web Server (192.168.1.20)

2.slave DNS

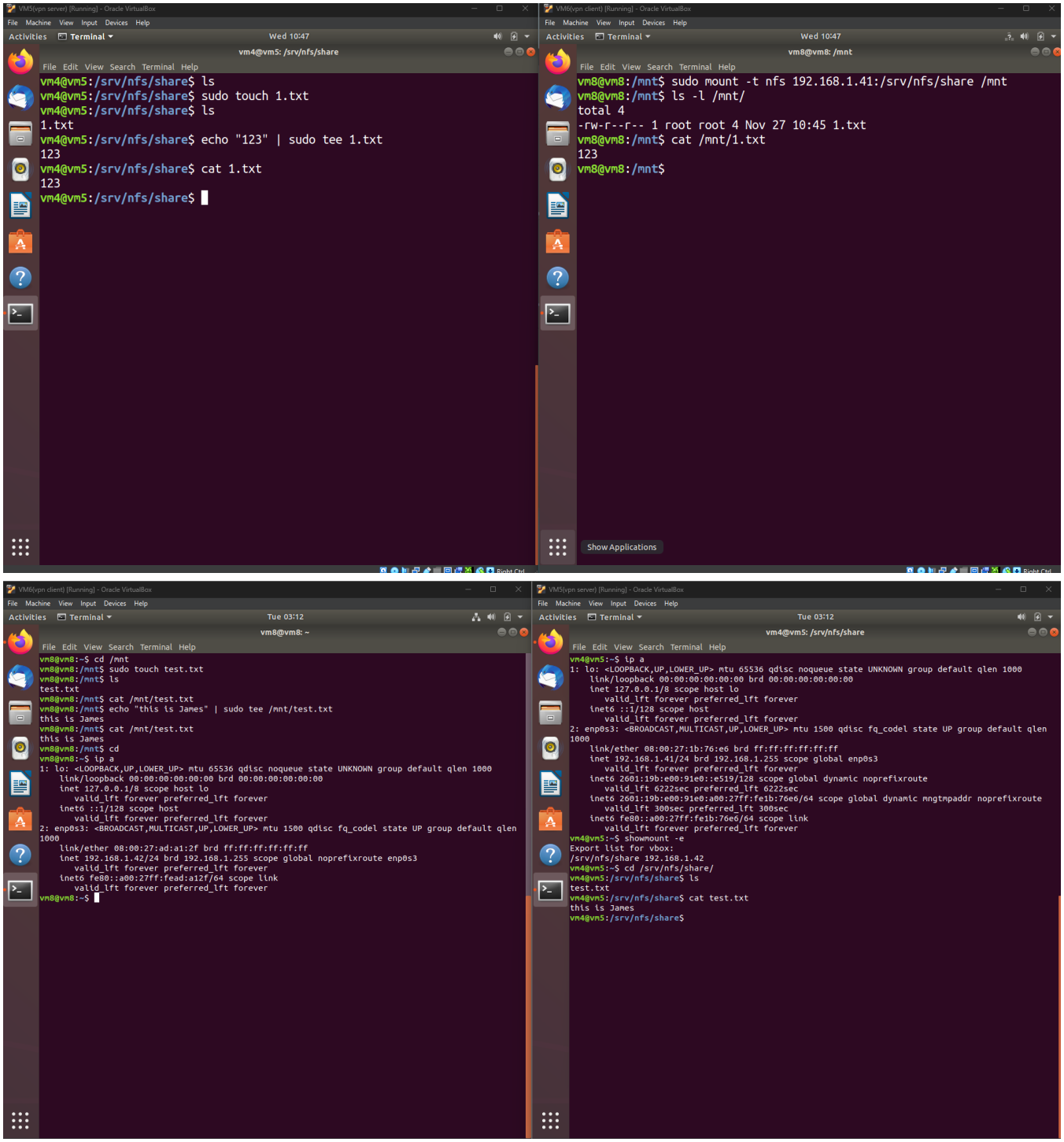

Web Server - Local Lab
192.168.1.20
Welcome to web.local.lab
This is VM2 - Web Server (192.168.1.20)
web.local.lab
Terminal
vm1@vm1: ~
bind9.service - BIND Domain Name Server
Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
Active: active (running) since Tue 2024-11-26 12:22:02 EST; 7min ago
Docs: man:named(8)
Process: 2747 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
Main PID: 2750 (named)
Tasks: 4 (limit: 2318)
CGroup: /system.slice/bind9.service
└2750 /usr/sbin/named -f -u bind
Nov 26 12:26:45 vm1 named[2750]: network unreachable resolving 'E.ROOT-SERVERS.NET/AAAA
Nov 26 12:26:45 vm1 named[2750]: network unreachable resolving 'E.ROOT-SERVERS.NET/AAAA
Nov 26 12:26:45 vm1 named[2750]: network unreachable resolving 'E.ROOT-SERVERS.NET/AAAA
Nov 26 12:26:45 vm1 named[2750]: network unreachable resolving 'E.ROOT-SERVERS.NET/AAAA
Nov 26 12:26:45 vm1 named[2750]: network unreachable resolving 'G.ROOT-SERVERS.NET/AAAA
lines 1-15
vm7@vm7: ~
bind9.service - BIND Domain Name Server
Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
Active: active (running) since Tue 2024-11-26 12:24:12 EST; 5min ago
Docs: man:named(8)
Main PID: 544 (named)
Tasks: 4 (limit: 2318)
CGroup: /system.slice/bind9.service
└544 /usr/sbin/named -f -u bind
Nov 26 12:24:13 vm7 named[544]: network unreachable resolving 'E.ROOT-SERVERS.NET/AAAA/
Nov 26 12:24:13 vm7 named[544]: network unreachable resolving 'E.ROOT-SERVERS.NET/AAAA/
Nov 26 12:24:13 vm7 named[544]: network unreachable resolving 'G.ROOT-SERVERS.NET/AAAA/
Nov 26 12:24:13 vm7 named[544]: network unreachable resolving 'G.ROOT-SERVERS.NET/AAAA/
Nov 26 12:24:13 vm7 named[544]: zone local.lab/IN: Transfer started.
Nov 26 12:24:13 vm7 named[544]: transfer of 'local.lab/IN' from 192.168.1.1#53: connect
lines 1-15


Web Server - Local Lab
192.168.1.20
Welcome to web.local.lab
This is VM2 - Web Server (192.168.1.20)
Terminal
vm1@vm1: ~
bind9.service - BIND Domain Name Server
Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
Active: inactive (dead) since Tue 2024-11-26 12:38:23 EST; 2s ago
Docs: man:named(8)
Process: 2832 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
Process: 2750 ExecStart=/usr/sbin/named -f $OPTIONS (code=exited, status=0/SUCCESS)
Main PID: 2750 (code=exited, status=0/SUCCESS)
Nov 26 12:38:23 vm1 systemd[1]: Stopping BIND Domain Name Server...
Nov 26 12:38:23 vm1 named[2750]: received control channel command 'stop'
Nov 26 12:38:23 vm1 named[2750]: shutting down: flushing changes
Nov 26 12:38:23 vm1 named[2750]: stopping command channel on 127.0.0.1#953
Nov 26 12:38:23 vm1 named[2750]: stopping command channel on ::1#953
Nov 26 12:38:23 vm1 named[2750]: no longer listening on ::#53
Nov 26 12:38:23 vm1 named[2750]: no longer listening on 192.168.1.1#53
lines 1-15
vm7@vm7: ~
bind9.service - BIND Domain Name Server
Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
Active: active (running) since Tue 2024-11-26 12:24:12 EST; 5min ago
Docs: man:named(8)
Main PID: 544 (named)
Tasks: 4 (limit: 2318)
CGroup: /system.slice/bind9.service
└544 /usr/sbin/named -f -u bind
Nov 26 12:24:13 vm7 named[544]: network unreachable resolving 'E.ROOT-SERVERS.NET/AAAA/
Nov 26 12:24:13 vm7 named[544]: network unreachable resolving 'E.ROOT-SERVERS.NET/AAAA/
Nov 26 12:24:13 vm7 named[544]: network unreachable resolving 'G.ROOT-SERVERS.NET/AAAA/
Nov 26 12:24:13 vm7 named[544]: network unreachable resolving 'G.ROOT-SERVERS.NET/AAAA/
Nov 26 12:24:13 vm7 named[544]: zone local.lab/IN: Transfer started.
Nov 26 12:24:13 vm7 named[544]: transfer of 'local.lab/IN' from 192.168.1.1#53: connect
lines 1-15

4.firewall


vm1@vm1:~$ sudo systemctl status ufw
[sudo] password for vm1:
● ufw.service - Uncomplicated firewall
Loaded: loaded (/lib/systemd/system/ufw.service; enabled; vendor preset: enabled)
Active: active (exited) since Wed 2024-11-27 10:54:45 EST; 8h ago
Docs: man:ufw(8)
Process: 219 ExecStart=/lib/ufw/ufw-init start quiet (code=exited, status=0/SUCCESS)
Main PID: 219 (code=exited, status=0/SUCCESS)
Nov 27 10:54:45 vm1 systemd[1]: Started Uncomplicated firewall.
Warning: Journal has been rotated since unit was started. Log output is incomplete or unavailable
[10]+ Stopped sudo systemctl status ufw
vm1@vm1:~$ sudo ufw status numbered
Status: active
To Action From
[1] 546/udp ALLOW IN Anywhere
[2] 547/udp ALLOW IN Anywhere
[3] Anywhere/tpv6 ALLOW IN Anywhere/tpv6
[4] 53/tcp ALLOW IN Anywhere
[5] 53/udp ALLOW IN Anywhere
[6] 546/udp (v6) ALLOW IN Anywhere (v6)
[7] 547/udp (v6) ALLOW IN Anywhere (v6)
[8] Anywhere (v6) ALLOW IN fc00::/64
[9] 53/tcp (v6) ALLOW IN Anywhere (v6)
[10] 53/udp (v6) ALLOW IN Anywhere (v6)
vm1@vm1:~$
Hmm. We're having trouble finding that site.
We can't connect to the server at web.local.lab.
If you entered the right address, you can:
Try again later
Check your network connection
Check that Firefox has permission to access the web (you might be connected but behind a firewall)
Settings
Network
Wi-Fi
Bluetooth
Background
Dock
Notifications
Search
Region & Language
Universal Access
Online Accounts
Privacy
Sharing
Sound
Wired
Wired connection 1
netplan-enp0s3
IPv4 Address 192.168.2.1
IPv6 Address fe80::a00:27ff:fec0:9a66
Hardware Address 08:00:27:C0:9A:66
Default Route 192.168.1.1
DNS 192.168.1.1
VPN
Not set up
Network Proxy
Off
Welcome to web.local.lab
This is VM2 - Web Server (192.168.1.20)
client@client:~$ sudo nano /etc/netplan/00-installer-config.yaml
client@client:~$ sudo netplan apply
client@client:~$ sudo dhclient -r enp0s3
Killed old client process
client@client:~$ sudo dhclient enp0s3
client@client:~$ sudo netplan apply
client@client:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:c0:9a:66 brd ff:ff:ff:ff:ff:ff
inet 192.168.1.60/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
valid_lft 597sec preferred_lft 597sec
inet6 fe80::a00:27ff:fec0:9a66/64 scope link tentative
valid_lft forever preferred_lft forever
client@client:~$

5.vpn


VM5(vpn server) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Wed 10:47
vm4@vm5: /srv/nfs/share
File Edit View Search Terminal Help
vm4@vm5:/srv/nfs/share$ ls
vm4@vm5:/srv/nfs/share$ sudo touch 1.txt
vm4@vm5:/srv/nfs/share$ ls
1.txt
vm4@vm5:/srv/nfs/share$ echo "123" | sudo tee 1.txt
123
vm4@vm5:/srv/nfs/share$ cat 1.txt
123
vm4@vm5:/srv/nfs/share$
VM6(vpn client) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Wed 10:47
vm8@vm8: /mnt
File Edit View Search Terminal Help
vm8@vm8:/mnt$ sudo mount -t nfs 192.168.1.41:/srv/nfs/share /mnt
vm8@vm8:/mnt$ ls -l /mnt/
total 4
-rw-r--r-- 1 root root 4 Nov 27 10:45 1.txt
vm8@vm8:/mnt$ cat /mnt/1.txt
123
vm8@vm8:/mnt$
Show Applications
VM6(vpn client) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Tue 03:12
vm8@vm8: ~
File Edit View Search Terminal Help
vm8@vm8:~$ cd /mnt
vm8@vm8:/mnt$ sudo touch test.txt
vm8@vm8:/mnt$ ls
test.txt
vm8@vm8:/mnt$ cat /mnt/test.txt
vm8@vm8:/mnt$ echo "this is James" | sudo tee /mnt/test.txt
this is James
vm8@vm8:/mnt$ cat /mnt/test.txt
this is James
vm8@vm8:/mnt$ cd
vm8@vm8:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:ad:a1:2f brd ff:ff:ff:ff:ff:ff
inet 192.168.1.42/24 brd 192.168.1.255 scope global noprefixroute enp0s3
valid_lft forever preferred_lft forever
inet6 fe80::a00:27ff:fead:a12f/64 scope link
valid_lft forever preferred_lft forever
vm8@vm8:~$
VM5(vpn server) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Tue 03:12
vm4@vm5: /srv/nfs/share
File Edit View Search Terminal Help
vm4@vm5:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:1b:76:e6 brd ff:ff:ff:ff:ff:ff
inet 192.168.1.41/24 brd 192.168.1.255 scope global enp0s3
valid_lft forever preferred_lft forever
inet6 2601:19b:e00:91e0::e519/128 scope global dynamic noprefixroute
valid_lft 6222sec preferred_lft 6222sec
inet6 2601:19b:e00:91e0:a00:27ff:fe1b:76e6/64 scope global dynamic mngtmpaddr noprefixroute
valid_lft 300sec preferred_lft 300sec
inet6 fe80::a00:27ff:fe1b:76e6/64 scope link
valid_lft forever preferred_lft forever
vm4@vm5:~$ showmount -e
Export list for vbox:
/srv/nfs/share 192.168.1.42
vm4@vm5:~$ cd /srv/nfs/share/
vm4@vm5:/srv/nfs/share$ ls
test.txt
vm4@vm5:/srv/nfs/share$ cat test.txt
this is James
vm4@vm5:/srv/nfs/share$

FUTURE SCOPE:

1. **Expand DNS and DHCP for larger networks and subnets.**
2. **Enhance security with IDS/IPS and encrypted backups.**
3. **Implement redundancy for DNS and DHCP to ensure availability.**
4. **Optimize web servers and DNS caching for performance.**
5. **Integrate automation tools for configuration and monitoring.**
6. **VPN is based on the concept of data encryption or create a secure tunnel, in the future, we could integrate it with ZTA (Zero Trust Architecture) or AES encryption.**

Reference:

https://www.idm.com/thonk/topics/man-in-the-middle

https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

https://claude.ai/chat/bb056325-ad4b-466a-a2bf-78a307f9bf9c

https://aws.amazon.com/tw/route53/what-is-dns/

https://www.cloudflare.com/learning/dns/what-is-dns/

https://phoenixnap.com/kb/ubuntu-dns-nameservers

https://www.cherryservers.com/blog/how-to-install-and-configure-a-private-bind-dns-server-on-ubuntu-22-04

https://chatgpt.com/c/674dbf46-28a8-8005-9269-b64e1cf375ac

https://www.linode.com/community/questions/18145/what-is-the-difference-between-master-and-slave-dns-zone

https://cloudns-net.medium.com/what-is-a-dns-zone-master-and-slave-dns-zone-and-how-to-create-it-24833947b1ea

https://serverfault.com/questions/914688/proper-master-slave-configuration-for-dns

https://www.youtube.com/watch?v=Ru4F0uR6UxY