Reporte de la Práctica 11 para el laboratorio de Redes A

Network Applications: HTTP, DHCP and FTP

Estudiante: Héctor Andrey Hernández Alonso

Grupo: 282001

Instructor: M.I. González Grimaldo Raymundo Antonio

Fecha: 15 - mayo -19

Introducción

HTTP

El Protocolo seguro de transferencia de hipertexto (en inglés: Hypertext Transfer Protocol Secure o HTTPS), es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP.

DHCP

El protocolo de configuración dinámica de host (en inglés: Dynamic Host Configuration Protocol, también conocido por sus siglas de DHCP) es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP. Este servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme estas van quedando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

FTP

El Protocolo de transferencia de archivos (en inglés File Transfer Protocol o FTP) es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

El servicio FTP es ofrecido por la capa de aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21. Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad, ya que todo el intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante puede capturar este tráfico, acceder al servidor y/o apropiarse de los archivos transferidos.

Para solucionar este problema son de gran utilidad aplicaciones como SCP y SFTP, incluidas en el paquete SSH, que permiten transferir archivos, pero cifrando todo el tráfico.

Reporte de la Práctica 11 para el laboratorio de Redes A

Network Applications: HTTP, DHCP and FTP

Estudiante: Héctor Andrey Hernández Alonso

Grupo: 282001

Instructor: M.I. González Grimaldo Raymundo Antonio

Fecha: 15 - mayo -19

Desarrollo de la práctica

Configuración de HTTP y FTP para poder conectar la red en un cliente al servidor que está en una máquina virtual.

```
redesa@redesa:~$ systemctl restart isc-dhcp-server

Command 'ystemctl' not found, did you mean:

  command 'systemctl' from deb systemd

Try: sudo apt install <deb name>

redesa@redesa:~$ systemctl restart isc-dhcp-server
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to restart 'isc-dhcp-server.service'.
Authenticating as: redesa
Password:
polkit-agent-helper-1: pam_authenticate failed: Authentication failure
==== AUTHENTICATION FAILED ===
Failed to restart isc-dhcp-server.service: Access denied
See system logs and 'systemctl status isc-dhcp-server.service' for details.
redesa@redesa:~$ sudo systemctl restart isc-dhcp-server
redesa@redesa:~$ sudo systemctl restart isc-dhcp-server
redesa@redesa:~$ systemctl restart isc-dhcp-server
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to restart 'isc-dhcp-server.service'.
Authenticating as: redesa
Password:
==== AUTHENTICATION COMPLETE ===
redesa@redesa:~$ _
```

```
# A slightly different configuration for an internal subnet.
subnet 100.0.0.0 netmask 255.255.255.0 {
  range 100.0.0.50 100.0.0.100;
  option domain-name-servers ns1.internal.example.org;
  option domain-name "internal.example.org";
  option subnet-mask 255.255.255.224;
  option routers 10.5.5.1;
  option broadcast-address 10.5.5.31;
  default-lease-time 600;
  max-lease-time 7200;
}
```

Reporte de la Práctica 11 para el laboratorio de Redes A

Network Applications: HTTP, DHCP and FTP

Estudiante: Héctor Andrey Hernández Alonso

Grupo: 282001

Instructor: M.I. González Grimaldo Raymundo Antonio

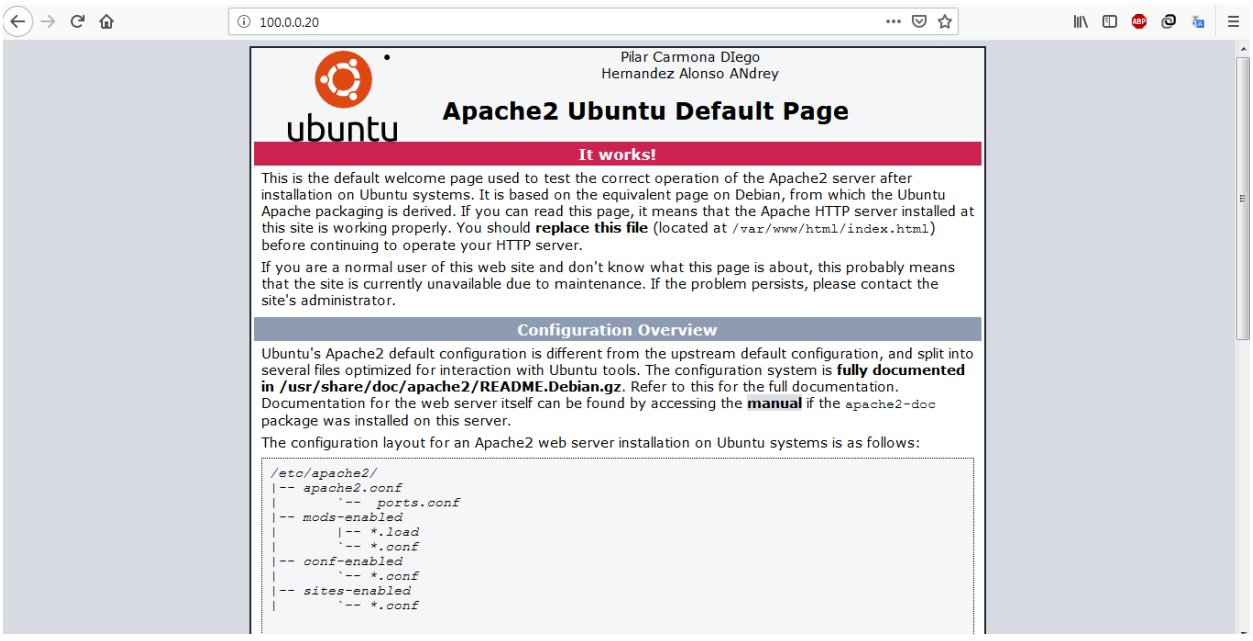
Fecha: 15 - mayo -19

```
    </style>
  </head>
  <body>
    <div class="main_page">
      <div class="page_header floating_element">
        <img src="/icons/ubuntu-logo.png" alt="Ubuntu Logo" class="floating_element"/>
        <li>

        <ul>Pilar Carmona DIego</ul>
        <ul>Hernandez Alonso ANdrey </ul>
        </li>

                <span class="floating_element">
          Apache2 Ubuntu Default Page
        </span>
      </div>
<!--      <div class="table_of_contents floating_element">
        <div class="section_header section_header_grey">
          TABLE OF CONTENTS
        </div>
        <div class="table_of_contents_item floating_element">
          <a href="#about">About</a>
```

Ventana de Apache vista desde el cliente



Reporte de la Práctica 11 para el laboratorio de Redes A

Network Applications: HTTP, DHCP and FTP

Estudiante: Héctor Andrey Hernández Alonso

Grupo: 282001

Instructor: M.I. González Grimaldo Raymundo Antonio

Fecha: 15 - mayo -19

Conclusiones

Para preparar un servidor web que acepte conexiones HTTPS, el administrador debe crear un certificado de clave pública para el servidor web. Este certificado debe estar firmado por una autoridad de certificación para que el navegador web lo acepte. La autoridad certifica que el titular del certificado es quien dice ser. Los navegadores web generalmente son distribuidos con los certificados raíz firmados por la mayoría de las autoridades de certificación por lo que estos pueden verificar certificados firmados por ellos.

Bibliografías

https://es.wikipedia.org/wiki/Protocolo_de_transferencia_de_archivos

https://app.schoology.com/attachment/859653532/docviewer

https://es.wikipedia.org/wiki/Protocolo_seguro_de_transferencia_de_hipertexto

https://es.wikipedia.org/wiki/Protocolo_de_configuraci%C3%B3n_din%C3%A1mica_de_host