Receta Captura TP Integrador 2019

Este es una especie de racconto para Ayudantes y Docentes, con notas y tareas que se deben efectuar a fin de preparar el aula y los equipos para efectuar la Captura Final de Teleinformática y Redes con pocas (o nulas) dificultades.

Este documento describe las configuraciones mínimas requeridas para llevar a cabo la captura del Trabajo Práctico Final Integrador de 2019 disponible en:

http://www.labredes.unlu.edu.ar/sites/www.labredes.unlu.edu.ar/files/site/data/tyr/TYR-2019-TP-Integrador.pdf

En cuanto a hardware

- Designar qué equipos operarán como Routers, y cual será el DNS.
- Conectar las interfaces de todos los equipos intervinientes, incluyendo servidores y clientes, en las bocas del HUB.

En todos los equipos que participan

Antes de desconectar la red de Internet, instalar los siguientes paquetes:

```
apt-get install ethtool           # en todos los equipos
apt-get install netsurf           # en el cliente
apt-get install squid            # en el servidor proxy
apt-get install apache2           # en los servidores web
apt-get install bind9             # en el servidor dns
```

Escribir estos pasos en el pizarrón para que todos puedan leerlos y ejecutarlos.

- Detener los servicios superfluos:

```
#!/bin/sh
service apache2 stop   # salvo en los webservers
service exim4 stop
service nfs-common stop
service openbsd-inetd stop
service rpcbind stop
service ssh stop
service squid stop     # salvo en el proxy
service avahi-daemon stop
service ntpdate stop
service ntp stop
pkill apache
pkill squid
apt-get purge rtkit
systemctl stop systemd-timesyncd
systemctl disable systemd-timesyncd
systemctl disable avahi-daemon
```

- Para verificar los procesos que están corriendo y ver si es necesario terminar alguno adicional:

```
netstat -tplnu
```

- Eliminar las direcciones de red existentes:

```
ip addr flush dev ethN
```

- Deshabilitar TCP Segmentation Offloading

```
ethtool --offload ethN tso off
```

- Desactivar el uso de IPv6 a nivel global y en las interfaces de cada equipo:

```
echo 1 > /proc/sys/net/ipv6/conf/all/disable_ipv6
echo 1 > /proc/sys/net/ipv6/conf/INTERFAZ/disable_ipv6
```

- Previo a cada captura, eliminar la tabla ARP con: (Indicar y obligar que lo hagan):

```
ip neigh flush all
```

- Una vez finalizadas las configuraciones por parte de los estudiantes, recomendar cerrar la sesión gráfica en todos los equipos (menos el cliente) y recomendar seguir los pasos de captura en una interfaz de texto.

En los equipos que capturan

- Realizar la captura con tshark para evitar resoluciones innecesarias:

```
tshark -i eth0 -n -w legajo.pcap
```

- Para ver la salida por CLI (1 trama por linea)

```
tshark -i eth0 -n
```

En el cliente HTTP

- Configurar las interfaces de red, la resolución DNS y las rutas necesarias. [1]
- Configurar que el navegador utilice el proxy asignado. [2]
- Preferentemente utilizar el navegador NetSurf en el cliente, ya que Mozilla Firefox realiza una gran cantidad de peticiones a sitios externos para actualizar listas de páginas bloqueadas, extensiones y otros motivos que desconozco.
- En caso de utilizar Firefox, deshabilitar la descarga de `favicon.ico` en `about:config`

```
browser.chrome.favicons false
browser.chrome.site_icons  false
```

- Deshabilitar el uso de caché en el navegador. Encontrado en el foro de Mozilla:

```
Ingresar en about:config
Buscar browser.cache.disk.enable y setear en false
(Reiniciar Firefox)
Repetir los ultimos 2 pasos para browser.cache.memory.enable
```

- Deshabilitar DNS Lookup para registros AAAA desde el navegador:

[1] tarea de los estudiantes.
[2] tarea de los estudiantes.

`network.dns.disableIPv6` `true`

Esto evita que firefox realice consultas al registro AAAA que son innecesarias para el TP

- Agregar las direcciones siguientes a `/etc/hosts`

```
127.0.0.3   safebrowsing.google.com
127.0.0.3   adblockplus.mozdev.org
127.0.0.3   www.netsurf-browser.com
127.0.0.3   tiles.services.mozilla.com
127.0.0.3   location.services.mozilla.com
127.0.0.3   tiles-cloudfront.cdn.mozilla.net
127.0.0.3   safebrowsing-cache.google.com
```

127.0.0.3 safebrowsing.googleapis.com 127.0.0.3 detectportal.firefox.com 127.0.0.3 shavar.services.mozilla.com.unlu.edu.ar 127.0.0.3 shavar.services.mozilla.com

a fin de evitar que se consulte DNS por esos dominios.

- Agregar las direcciones siguientes como excepciones al proxy en el navegador:

```
safebrowsing.google.com, safebrowsing-cache.google.com,
.mozdev.org, .mozilla.com, .mozilla.net, .mozilla.org,
www.netsurf-browser.com, detectportal.firefox.com, safebrowsing.googleapis.com
```

- Preferentemente, quitar los servidores DNS que estén definidos en `/etc/resolv.conf`
- Verificar que es posible consultar las páginas solicitando el archivo `000000.html` que debería instalarse en el webserver previamente.

Nota:

- La respuesta HTTP resulta ser de tipo HTML (`Content-Type: text/html`), sin embargo la codificación es GZip (`Content-Encoding: gzip`) tanto en el mensaje del servidor web como en el servidor proxy (visible si se realiza `Follow TCP stream` sobre el flujo). Una posible solución a este comportamiento se adjunta en la sección destinada al webserver.

En el servidor DNS

- Configurar las interfaces de red y las rutas necesarias. [3]
- Instalar BIND:

```
apt-get install bind9
```

- Copiar la configuración local a `/etc/bind` (anexa al final)

```
cp named.conf.local /etc/bind/
```

- Copiar la base de datos de zona a `/var/cache/bind` (anexa al final)

```
cp example.com /var/cache/bind/
```

- Desactivar el uso de DNSSEC añadiendo a `/etc/bind/named.conf.options` las sentencias siguientes:

[3] tarea de los estudiantes.

```
dnssec-enable false;
dnssec-validation false;
```

- Reiniciar el demonio BIND, verificar que se inició correctamente:

```
service bind9 restart
tail /var/log/syslog
```

- Realizar una consulta al DNS local y verificar que existe respuesta:

```
dig @127.0.0.1 www.example.com
```

En el servidor Proxy HTTP

- Configurar las interfaces de red, la resolución DNS (Archivo `resolv.conf`) y las rutas necesarias. [4]
- Instalar Squid3 [5]

```
apt-get install squid
```

- Establecer las siguientes configuraciones en `/etc/squid/squid.conf`

```
# habilitar el servicio a todas las direcciones
# http_access deny all
http_access allow all

cache deny all     # evitar que se haga caché de recursos

# disminuir el tiempo de vida de peticiones dns
negative_dns_ttl 1 seconds
positive_dns_ttl 2 seconds

client_db off      # desactivar la creación de estadísticas de clientes
                   # esto evita que squid pregunte por el puntero
                   # reverso del router C

log_fqdn off       # desactivar la resolución de nombres en el registro
pinger_enable off  # desactivar que haga PING (!)
```

  - Documentación respaldatoria:
    * http://wiki.squid-cache.org/SquidFaq/ConfiguringSquid#Can_I_make_Squid_proxy_only.2C_without_caching_anything.3F
    * http://www.squid-cache.org/Versions/v3/3.3/cfgman/positive_dns_ttl.html
    * https://www.safaribooksonline.com/library/view/squid-the-definitive/0596001622/re59.html
    * https://wiki.squid-cache.org/SquidFaq/OperatingSquid#Using_ICMP_to_Measure_the_Network

- En las capturas 2018 vimos pings entre el proxy y otros equipos, algo realmente curioso, que resultó ser una funcionalidad (nueva?!) de squid3. Además de las líneas `client_db off` y

[4] tarea de los estudiantes.
[5] tarea de los estudiantes.

`log_fqdn off` en la configuración de Squid, conviene agregar la dirección IP del equipo cliente y del router que lo interconecta en el archivo `/etc/hosts` del proxy:

```
DIRECCION-IP-ROUTERC    routerc
DIRECCION-IP-CLIENTE    usuario
```

- Salvo que esté desactivado (por pasos previos), squid hace caché en memoria y opcionalmente en disco. Si en algún momento es necesario vaciar el caché, utilizar el siguiente script para vaciar el caché:

```
#!/bin/sh
service squid stop
rm -r /var/spool/squid/*
squid -z
service squid start
```

  Esto es necesario solo en casos donde se solicite algo al proxy previo al momento de las capturas y haya que repetir el request.

- Alternativamente a disminuir el TTL de las consultas DNS„ en la definición de la zona DNS en BIND se puede acortar el TTL del SOA para reducir la chance de que las resoluciones DNS se almacenen entre distintas capturas.

Por las pruebas realizadas, debe asegurarse que se cierren las conexiones TCP con el web server.

En los routers

- Previamente a que los estudiantes configuren las direcciones, establecer las siguientes configuraciones en el archivo `/etc/sysctl.conf` (y luego reiniciar)

```
  net.ipv4.ip_forward=1             # habilita el reenvío de paquetes
net.ipv4.conf.all.arp_filter=1  # solo responde arp en la interfaz adecuada

  net.ipv4.conf.all.accept_redirects = 0    # deshabilitar ICMP redirect
  net.ipv4.conf.all.send_redirects = 0      # deshabilitar ICMP redirect
```

- Alternativamente puede realizarse con el siguiente script:

```
sysctl -w net.ipv4.ip_forward=1
sysctl -w net.ipv4.conf.all.arp_filter=1
for i in /proc/sys/net/ipv4/conf/*/{accept,send}_redirects; do
    echo 0 > $i;
done
```

- Configurar las interfaces de red y las rutas necesarias. [6]

Notas:

- Según lo visto (por los estudiantes), la respuesta ARP a una consulta se realiza sobre **todas** las interfaces de red en las que se tenga asignada una dirección IP, según lo documentado en http://linux-ip.net/html/ether-arp.html, https://openvz.org/Multiple_network_interfaces_and_ARP_flux, y en la documentación del kernel linux `Documentation/networking/ip-sysctl.txt` . Una solución a este comportamiento es la indicada con `arp_filter` en la

[6] tarea de los estudiantes.

configuración anterior, o sino definir `arp_ignore` y `arp_announce` , pero sería interesante que ellos mismos detecten el comportamiento extraño.

- Cuando se definen distintas redes IP sobre una misma red Ethernet, es posible que los equipos en distintas redes omitan pasar por los routers asignados en rutas estáticas. Para corregir este comportamiento, la configuración anterior desactiva el envío y la aceptación de ICMP redirect en todas las interfaces (all).

En el router con NAT (Router C)

- Configurar las interfaces de red y las rutas necesarias. [7]
- Habilitar NAT con el script siguiente:

```
#!/bin/sh
IF_INTERNA=eth0
IF_EXTERNA=eth1
IP_EXTERNA=200.18.10.2
# elimino las configuraciones previas
iptables -F; iptables -t nat -F; iptables -t mangle -F

# alternativa 1 (snat). Preferida
iptables -t nat -A POSTROUTING -o $IF_EXTERNA -j SNAT --to $IP_EXTERNA

# alternativa 2 (masquerade)
# iptables -t nat -A POSTROUTING -o $IF_EXTERNA -j MASQUERADE
# habilito el reenvio
echo 1 > /proc/sys/net/ipv4/ip_forward
```

En los servidores HTTP (ambos)

- Configurar las interfaces de red y las rutas necesarias. [8]
- Instalar apache2 [9]

```
apt-get install apache2
```

- Copiar los recursos a servir en `/var/www/html/` y asignar permisos de lectura a todos los usuarios.
- Verificar que es posible obtener un recuro con wget:

```
wget http://127.0.0.1/
```

- Para evitar tener que cerrar el browser para que se produzcan los cierres de conexion TCP, se puede deshabilitar KeepAlive desde el web server. En el archivo `/etc/apache2/apache2.conf`

```
KeepAlive Off
```

- Deshabilitar gzip en el Virtualhost editando el archivo `/etc/apache2/sites-enabled/000-default.conf` y agregando dentro del tag `Virtualhost` la siguiente directiva de apache:

[7] tarea de los estudiantes.
[8] tarea de los estudiantes.
[9] tarea de los estudiantes.

```
SetEnv no-gzip 1
```

A continuación se debe reiniciar el servicio

```
service apache2 restart
```

Esto impide que las respuestas HTTP se compriman con gzip (ver nota previa en la sección relativa al cliente HTTP).

En el servidor de imágenes y CGI

- Configurar las interfaces de red y las rutas necesarias. [10]
- Instalar apache2

  ```
  apt-get install apache2
  ```

- Copiar los recursos a servir en `/var/www/html/` y asignar permisos de lectura a todos los usuarios.
- Agregar un conjunto de datos `000000.html`, `000000-1.png` y `000000-2.png` para pruebas sin necesidad de utilizar los archivos de los alumnos.
- Script CGI:
  - Copiar el archivo `/usr/lib/cgi-bin/pie.pl` (Adjunto al final)
  - Cambiar permisos y dueño:

    ```
    chown www-data.www-data /usr/lib/cgi-bin/pie.pl
    chmod 750 /usr/lib/cgi-bin/pie.pl
    ```

  - Por default hay que habilitar el modulo de cgi:

    ```
    a2enmod cgi
    service apache2 restart
    ```

- Verificar que es posible obtener los recursos con wget:

  ```
  wget http://127.0.0.1/
  wget http://127.0.0.1/cgi-bin/pie.pl
  ```

En equipo de captura

Tener Wireshark o Tshark encendido para monitorear el tráfico de la red.

Pasos para la captura

Estos pasos son los mínimos para realizar la captura de cada uno de los legajos.

1. dhclient -r *interface*
2. ip neigh flush all
3. Iniciar capturas en equipos designados. legajo.pcap
4. dhclient *interface*
5. Abrir navegadores en equipos designados.
6. Ir a URL http://www.example.com/legajo.html

[10] tarea de los estudiantes.

7. Esperar que se descargue toda la pagina
8. Esperar 10seg
9. Cerrar navegador
10. Finalizar Captura

Repetir estos pasos por cada legajo.

Archivo /etc/bind/named.conf.local

Esta versión es como debería ser en Jessie. Validar que en stretch es similar.

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "example.com" {
    type master;
    file "example.com";
};
```

Archivo /var/cache/bind/example.com

Esta versión es como debería ser en Jessie. Validar que en stretch es similar.

```
; ******************************
; * Base de Datos: example.com  *
; ******************************

$TTL 30
@   IN  SOA ns1.example.com florge.example.com (
                2018052401  ; Serial
                7200    ; Refresh
                3600    ; Retry
                432000  ; Expire
                36000   ; Minimun (negative caching TTL)
                )

; ******************************
; * Name servers del Dominio    *
; ******************************
        IN  NS  ns1.example.com.

; ******************************
; * Datos de hosts      *
; ******************************
ns1 IN A    200.18.10.100
proxy   IN A    200.18.10.99
web1    IN A     200.28.0.89
web2    IN A     200.28.0.90
www IN  CNAME web1
img IN  CNAME web2
```

Archivo /usr/lib/cgi-bin/pie.pl

```
#!/usr/bin/perl -wT
use strict;

print "Content-type: text/html\n\n";
my $now = localtime;

print <<END_HTML;
<html>
  <body>
    <p>Hora de acceso: $now</p>
    <p>Accedido desde: $ENV{REMOTE_ADDR}</p>
    <p>Referenciado desde: $ENV{HTTP_REFERER}</p>
  </body>
</html>
END_HTML
```