Los grupos serán formados por **4 personas como máximo**. Cualquier **copia** **a otro grupo** o **copia-pega** **de internet** será motivo de apartado **suspenso**; en caso de haber copiado a otro grupo, ambos grupos obtendrán ese apartado como suspenso.

En esta práctica **NO SE USARÁ TOR** en ningún caso

|  |
| --- |
| **Miembros de grupo** |
| Jose Daniel Tello |
| Francisco Pujol Álvarez |
| Gullermo Muñoz Serrano |
| Álvaro Willes Padrino |

1. **VPN (3 puntos)**
   1. **Análisis de tráfico VPN a nivel de Sistema Operativo (1,5 puntos)**

En este apartado se ha de instalar **ProtonVPN** en la máquina virtual.

Se trata de navegar a marca.com con VPN activada, capturar el tráfico con wireshark, y hacer lo mismo con VPN desactivada.

También, con VPN activada haz un ping a marca.com.

Comprueba si ocurre lo mismo en todos los casos. Indica qué protocolo VPN estás utilizando.

|  |
| --- |
| **Tabla de capturas** |
|  |

|  |
| --- |
| **Reflexión** |
| Contesta las siguientes preguntas:   * ¿A qué IP estamos enviando el tráfico con el PING?   Se la manda a 149.34.244.154   * ¿A qué IP estamos enviando el tráfico sin la VPN activada?   Se la manda a 34.147.120.111   * ¿A qué IP estamos enviando el tráfico con la VPN activada, y qué protocolo se está utilizando?   UDP e IAX(radio) a 185.107.56.117(hemos reactivado vpn, por lo que el servidor es distinto).   * ¿Por qué ocurre esto?   Cuando buscas MARCA con la VPN el ordenador se conecta al concentrador de Proton que es la que redirige la peticion a MARCA y nos devuelve el resultado, en cambio sin la VPN nos conectamos directamente al servidor con TLS |

* 1. **Análisis de tráfico VPN a nivel de Aplicación (1,5 puntos)**

En este apartado se ha de instalar el navegador **Opera** en la máquina virtual.

Se trata de navegar con Opera con VPN activado a <http://www.edu4java.com/> y capturar el tráfico con wireshark. Después haced lo mismo con VPN desactivado.

Haz un ping a esa misma página. Comprueba en qué casos se cifra el tráfico y con qué protocolo.

|  |
| --- |
| **Tabla de capturas** |
|  |

|  |
| --- |
| **Reflexión** |
| Contesta las siguientes preguntas:   * ¿A qué IP estamos enviando el tráfico con la VPN de Opera desactivada?   216.239.32.21   * ¿A qué IP estamos enviando el tráfico con la VPN de Opera activada, y qué protocolo se está utilizando? * Al estar realizando las peticiones a una página por HTTP, ¿qué ocurre en el caso en que accedemos a ella por VPN? ¿Se puede ver su contenido en texto plano como en una petición HTTP normal? |

1. **Navegación con Proxy Web (3 puntos)**
   1. **Proxy desde navegador (1 punto)**

En Kali, configura el navegador para navegar utilizando un proxy que encuentres por internet.

|  |
| --- |
| **Tabla de capturas** |
|  |

|  |
| --- |
| **Reflexión** |
| Los proxies gratuitos no son muy confiables, dan muchos fallos de conexión . Si quieres usar un proxy confiable, comprate uno |

* 1. **Proxy desde Sistema Operativo (1 punto)**

En kali, instala y configura privoxy para redirigir todo el tráfico del equipo a otros proxys. Para ello habéis de configurar los forward de privoxy para redirigir el tráfico (con /), o para no hacer uso del proxy en casos específicos (con .).

Configura después el navegador para que utilice el proxy. Para ello, verifica en qué puerto corre.

Aquí podéis encontrar información en el apartado 7.5 Forwarding

[https://www.privoxy.org/user-manual/config.html#FORWARD](https://www.privoxy.org/user-manual/config.html" \l "FORWARD)

Despues de instalar con sudo apt install privoxy

|  |
| --- |
| **Tabla de capturas** |
| Despues de instalar privoxy abre por defecto el puerto 8118 tanto para ipv4 como ipv6, si queremos cambiarlo habrá que cambiar la directiva foward en el fichero de configuración y abrir el puerto equivalente en el firewall. Por temas de simplificación lo dejamos con la configuración por defecto.  Añadimos el proxy a firefox:    Y lo probamos: |

|  |
| --- |
| **Reflexión** |
| Privoxy es super fácil de instalar y utilizar pero esto no esta hecho realmente para usar como seguridad primaria para navegación web. |

* 1. **Proxy Chain (1 punto)**

Configura proxychain4 en kali para pasar por 3 proxys al navegar a alguna página.

Desactiva la linea última linea, de uso de tor, cuyo puerto es 9050 para que no haga uso de esta herramienta.

Prueba los modos estricto, dinámico y aleatorio y comenta sus diferencias en el espacio de reflexión.

|  |
| --- |
| **Tabla de capturas** |
|  |

|  |
| --- |
| **Reflexión** |
| Estricto → Todos los proxies en la lista son usados en el orden especificado, pero si alguno falla entonces la conexión falla.  Dinamico → Casi igual al modo estricto pero si algún proxy falla pasa al siguiente en la lista  Aleatorio → Coge los proxies de forma aleatoria. Cada conexión es realizada con una combinación aleatoria de proxies. |

1. **SQUID Proxy (4 puntos)**
   1. **Proxy transparente (1,75 puntos)**

Instalad y configurad SQUID Proxy con los enlaces del aula virtual vistos en clase, para montar un servidor Proxy Transparente que haga uso de lista negra para bloquear el acceso a las páginas y habilitando con ACL a la red que consideréis:

* marca.com
* facebook.com

|  |
| --- |
| **Tabla de capturas** |
|  |

* 1. **Proxy caché (1,25 puntos)**

Tratad de configurar ese mismo proxy para que haga la función de proxy caché almacenando información en un directorio. Hay que tener en cuenta que solo se puede cachear HTTP.

Haced uso de los refresh-patterns, para marcar el contenido a cachear.

http://server1.sharewiz.net/doku.php?id=pfsense:squid:refresh\_patterns

Comprobad también -añadiendo capturas- que, posteriormente, al hacer nuevas peticiones similares a las almacenadas en caché, se devuelve contenido del directorio. Se puede verificar cuando, se obtiene en los logs una petición **TCP\_HIT, TCP\_MEM\_HIT**. En esos casos se estará cargando contenido de la caché. Añadid capturas también del directorio con el contenido almacenado.

Los logs de SQUID los podéis encontrar en /var/log/squid.

|  |
| --- |
| **Tabla de capturas** |
|  |

* 1. **ACL (1 punto)**

Haced uso de ACL para permitir exclusivamente el tráfico de varias IP y crear una lista blanca que solo permita el tráfico a ciertas páginas.

<https://myshittycode.com/2021/04/21/squid-configuring-whitelisted-urls/>

<https://webhostinggeeks.com/howto/how-to-configure-squid-proxy-server-for-ip-whitelisting/>

|  |
| --- |
| **Tabla de capturas** |
|  |