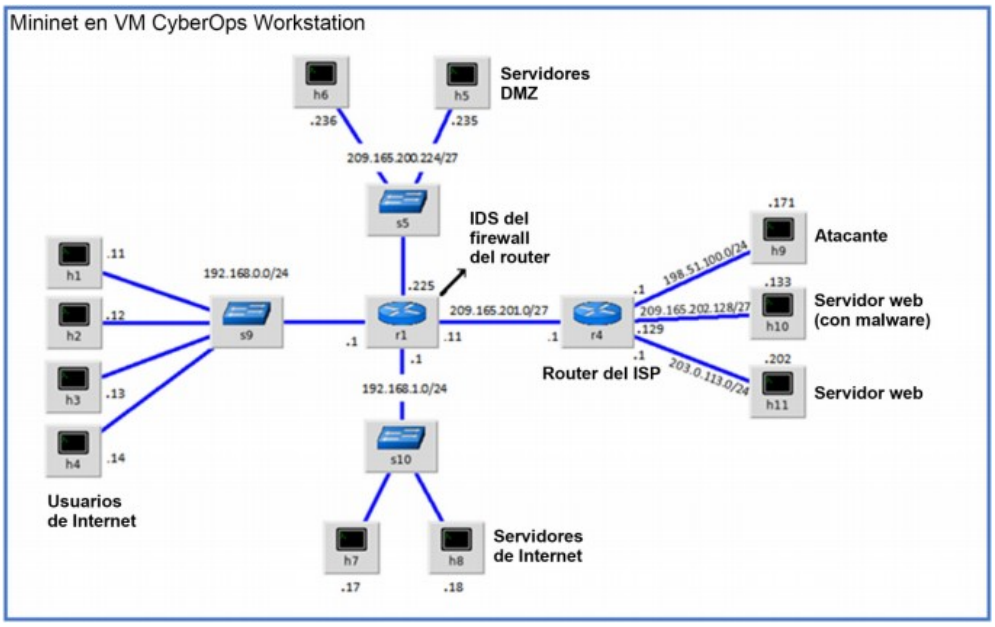
ACTIVIDAD 4 : SNORT – WIRESHARK - IPTABLES

- Recurso: VM CyberOps Workstation + topología para pruebas Mininet creada con script python
- Instrucciones: Entregar en la plataforma de Netacad un único documento en formato .pdf con capturas de pantalla y los comentarios correspondientes, por cada uno de los puntos del enunciado.



Usando la máquina virtual CyberOps Workstation del curso realizar las siguientes tareas:

1. Iniciar el entorno *Mininet* a partir del script de python "*cyberops_extended_topo_no_fw.py*"
2. Arrancar snort en *R1*
3. Arrancar un servidor web "malicioso" en *H10* en el puerto 6666/tcp
4. Desde *H5* descargar el ejecutable "*W32.Nimda.Amm.exe*" que se encuentra en la raiz del servidor web
5. ¿Snort ha detectado alguna alerta? Muestra el contenido de la alerta
6. Activar tcpdump en *H5* y llamar al fichero con las capturas "*analisis-trafico.pcap*"
7. Vover a descargar el ejecutable "*W32.Nimda.Amm.exe*" que se encuentra en la raiz del servidor web
8. Analizar con Whireshark el contenido del "*analisis-trafico.pcap*" generado, mostrando el contenido del paquete que ha realizado la descarga del .exe malicioso.
9. Extraer desde whiresahark el ejecutable malicioso para su posterior análisis con el nombre "*posible-virus.exe*"
10. Añadir una regla en el firewall del *R1* para que nadie pueda descargar ficheros del servidor web malicioso
11. Comprobar desde *H5* que ya no se pueden descargar ficheros de la web maliciosa