

**Nombre:**

**Ricardo Jara**

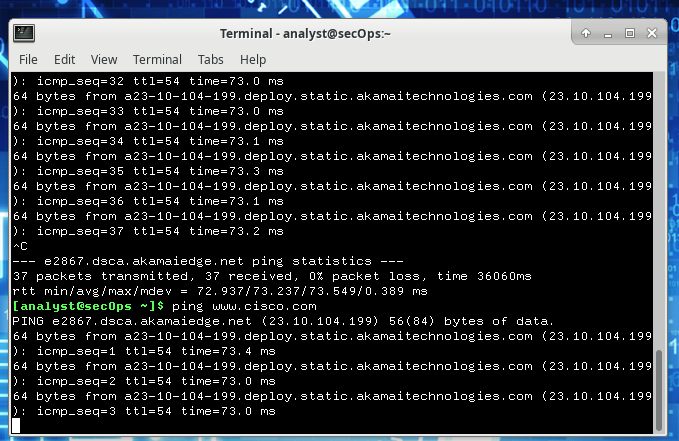
**Materia:**

**CYBEROPS**

Práctica de laboratorio 12.4.1.1

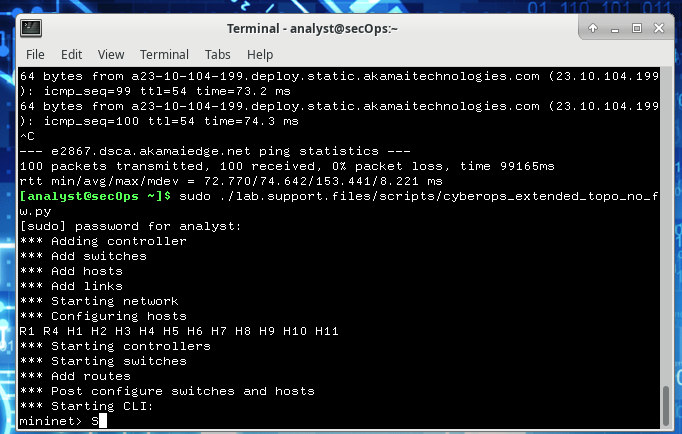
**Parte 1: Preparar el entorno virtual**

* ping [www.cisco.com](http://www.cisco.com)

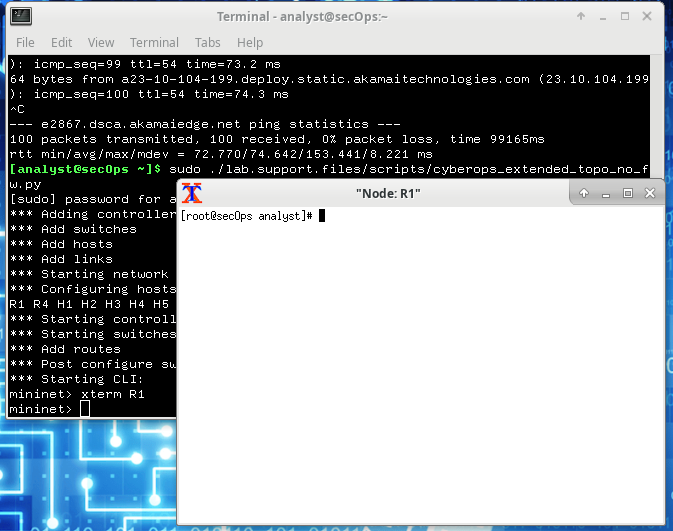


**Parte 2: El firewall y los archivos de registro de IDS**

* En la VM CyberOps Workstation VM, ejecuten el script para iniciar mininet.



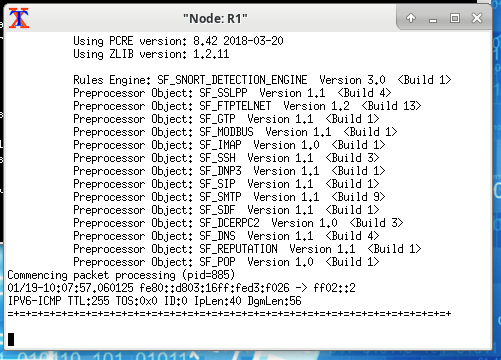
* xterm R1



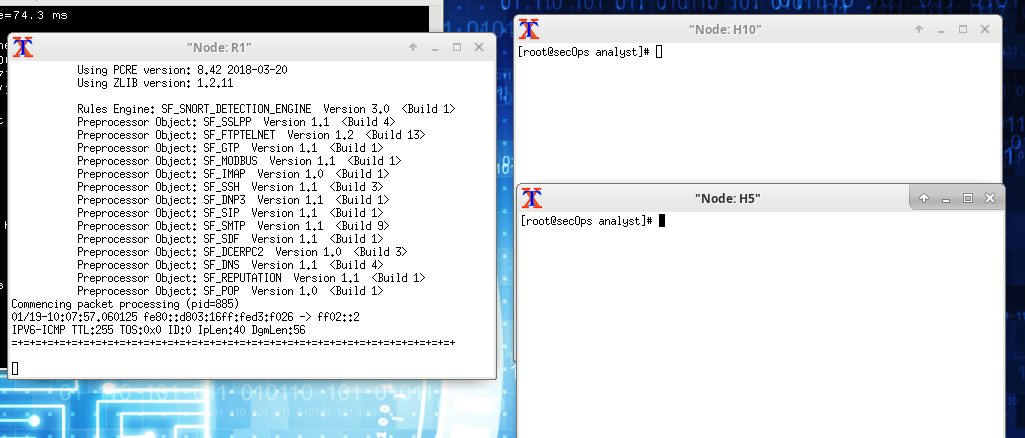
* El shell de R1 se abre en una ventana del terminal con texto negro y fondo blanco. ¿Qué usuario ha iniciado sesión en ese shell? ¿Qué nos lo indica?

Inicia sesión con el usuario Root, lo que indica de que se trata de un super usuario es el #

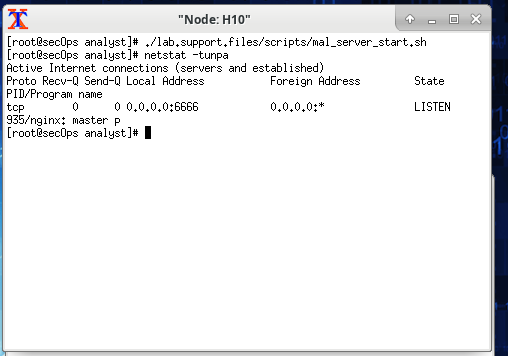
* [root@secOps analyst]# ./lab.support.files/scripts/start\_snort.sh



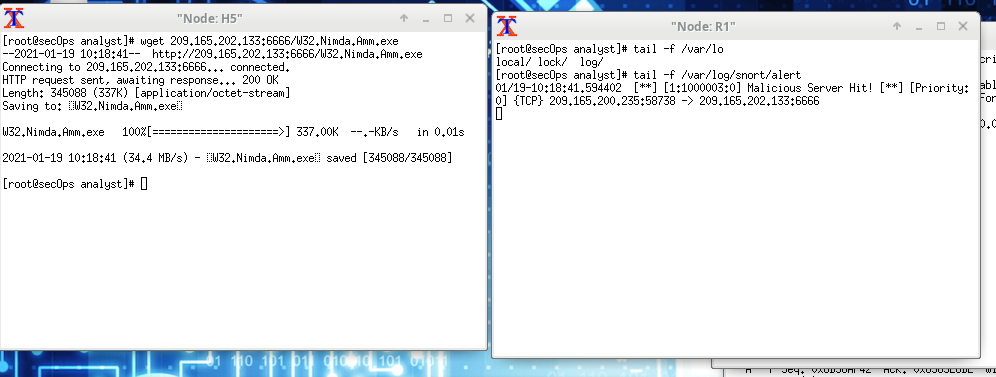
* xterm H5 | xterm H10



* H10: [root@secOps analyst]# ./lab.support.files/scripts/mal\_server\_start.sh | netstat -tunpa



* R1: tail -f /var/log/snort/alert
* R5: wget 209.165.202.133:6666/W32.Nimda.Amm.exe



* ¿Qué puerto se utiliza al comunicarse con el servidor web que aloja malware? ¿Qué nos lo indica?

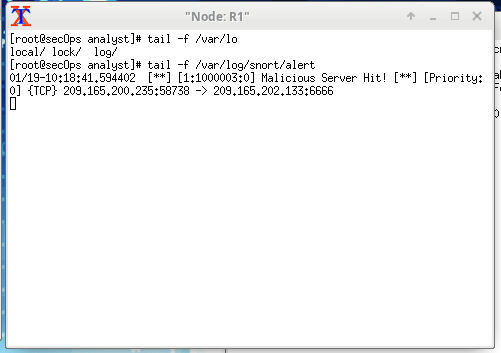
Se usa el puerto **6666**, lo que nos indica son los dos puntos ya que después de los dos puntos **“:”** de una dirección va el puerto.

* ¿Se descargó completamente el archivo?

Si. La descarga se completo correctamente.

* ¿El IDS generó alguna alerta relacionada con la descarga del archivo?

Si. Este fue capturado por R1



* En función de la alerta que se muestra arriba, ¿cuáles fueron las direcciones IPv4 de origen y de destino que se utilizaron en la transacción?

IP Origen: 209.165.200.235, IP Destino: 209.165.133

* En función de la alerta que se muestra arriba, ¿cuáles fueron los puertos de origen y de destino que se utilizaron en la transacción?

Puerto Origen: 58738, Puerto Destino 6666

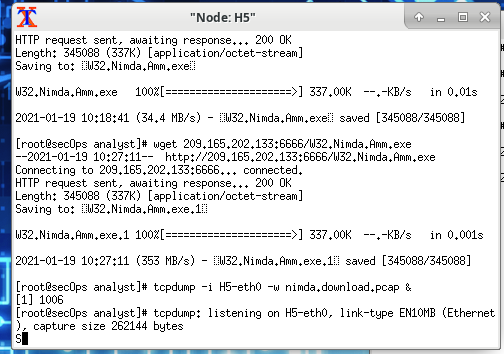
* En función de la alerta que se muestra arriba, ¿cuándo tuvo lugar la descarga?

Dia: 01/19/2021, Hora 10:18

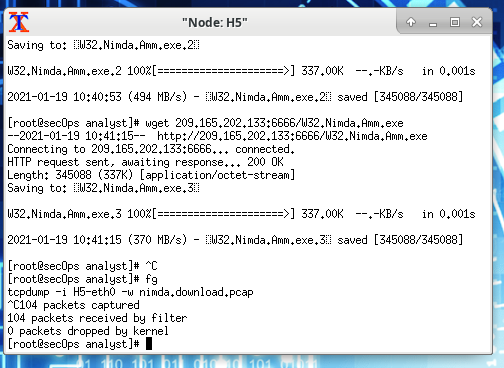
* En función de la alerta que se muestra arriba, ¿qué mensaje registró la firma del IDS?

Malicious Server Hit!

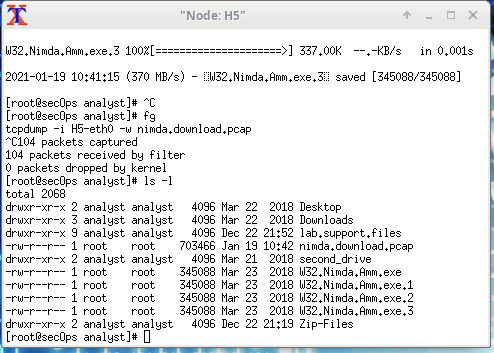
* H5: tcpdump –i H5-eth0 –w nimda.download.pcap &



* H5: wget 209.165.202.133:6666/W32.Nimda.Amm.exe | fg | ^c



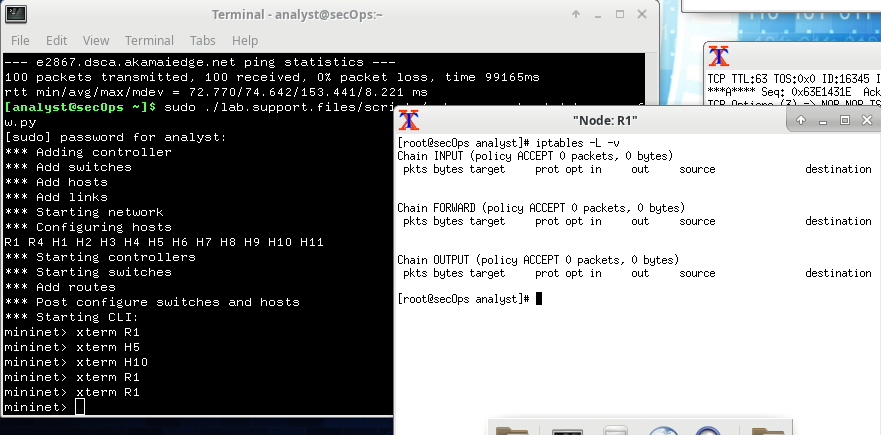
* H5: ls -l



* ¿Qué beneficios puede aportar este PCAP al analista especializado en seguridad?

PCAP nos ayuda a detectar el trafica por la red, de esta manera encontramos la comunicación entre redes maliciosas. PCAP rastrea eventos de red.

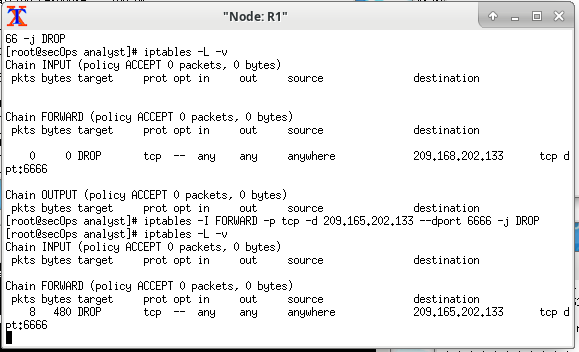
* Tercera R1 | xterm R1 | iptables -L -v



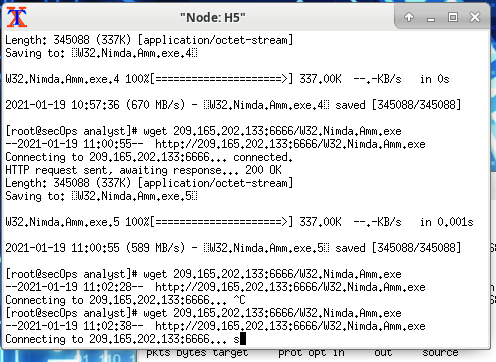
* ¿Qué cadenas está utilizando R1 en este momento?

INPUT (Entrada), FORWARD(Avance), OUTPUT(Salida)

* R1: iptables -I FORWARD -p tcp -d 209.165.202.133 --dport 6666 - j DROP | iptables -L -v



* H5: wget 209.165.202.133:6666/W32.Nimda.Amm.exe



* ¿Esta vez la descarga se completó correctamente? Explique.

No. Existe un bloquea las conexiones al servidor.

* ¿Cuál sería un enfoque más agresivo (pero válido a la vez) cuando se está bloqueando el servidor malicioso?

Recientemente se bloque solo una dirección IP, en la que se especifico el puerto y el protocolo. Si bloqueáramos la dirección IP del servidos bloquearíamos cualquier conexión que se tenga a la misma. Siendo esto un enfoque agresivo.

* quit | sudo mn –c

