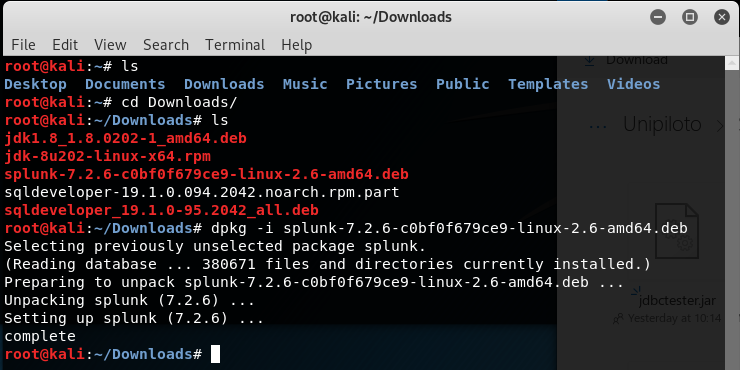
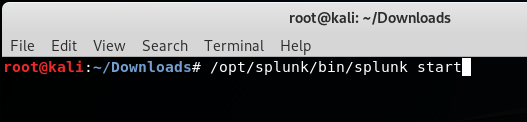
**TALLER 4**

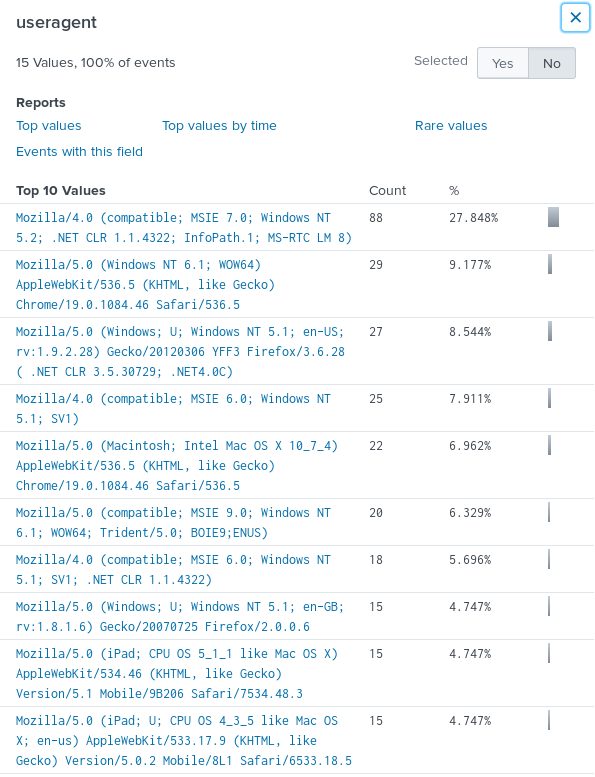
1. **Instalar splunk en la máquina virtual**



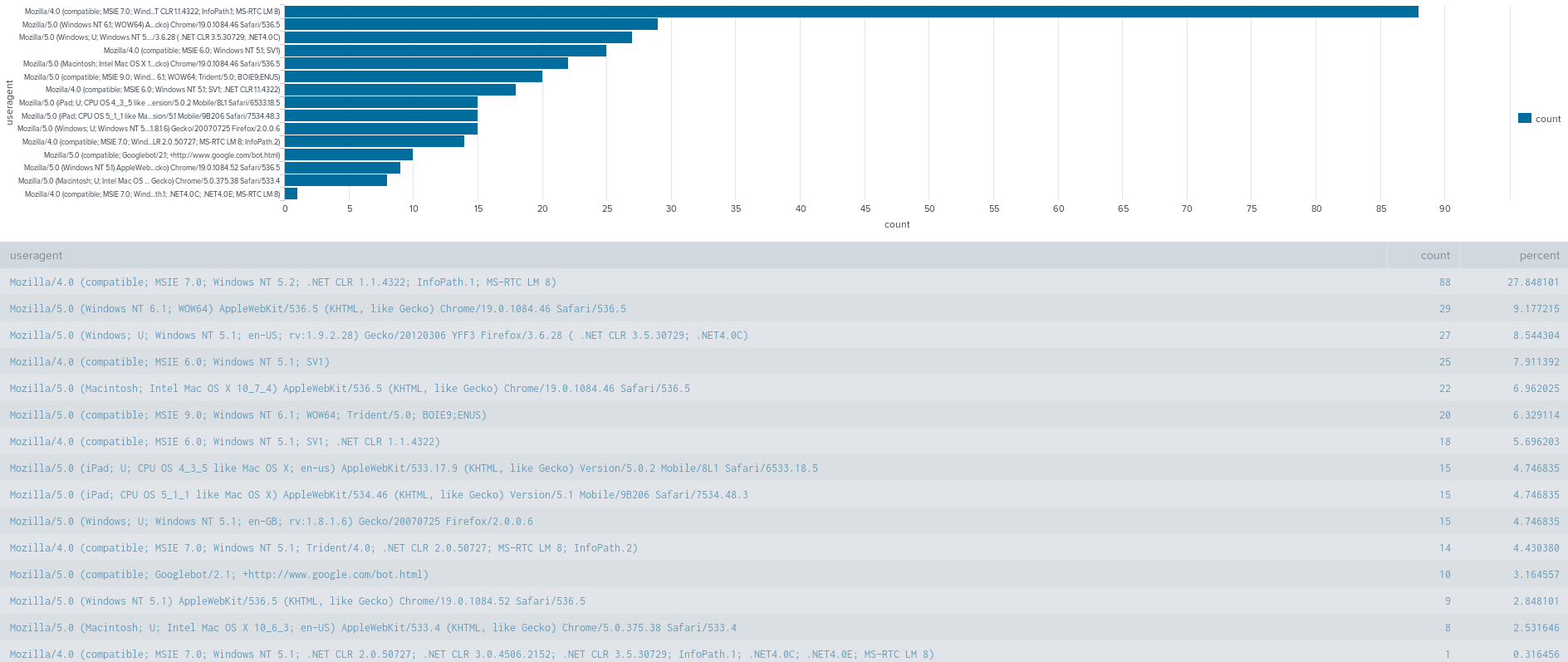
Inicializamos el splunk

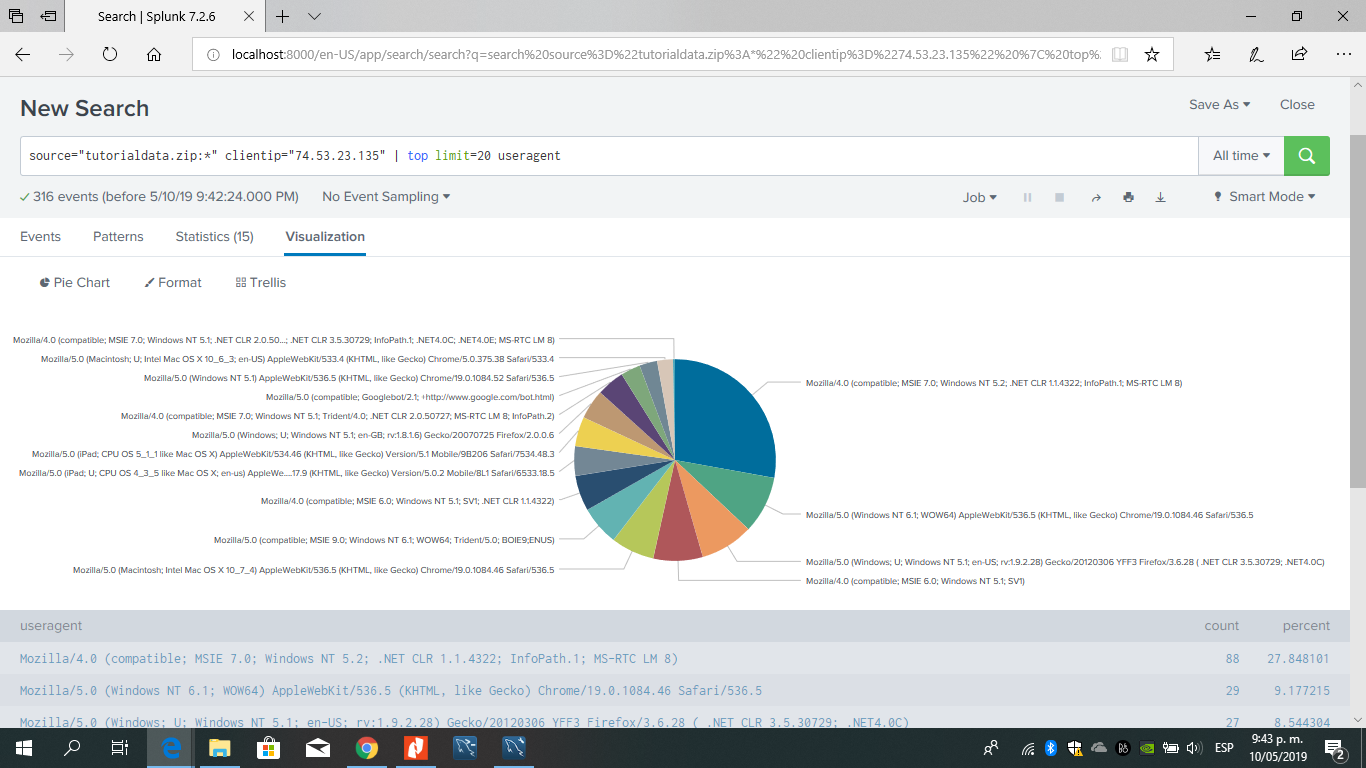


1. **Hacer tutorial: buscar los navegadores utilizados por la dirección 74.53.23.135**

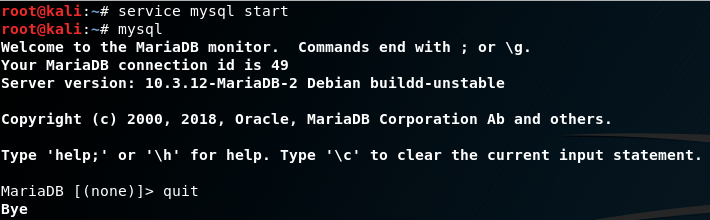


Se filtra por el top 20





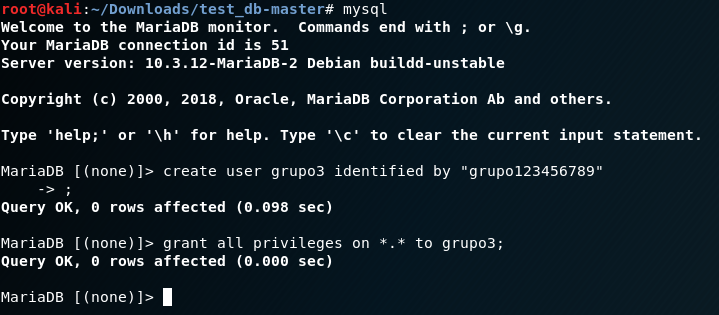
1. **Configure la BD MySql en la máquina virtual**



Luego procedemos a realizar la creación de la estructura de la base de datos:



Inicializamos la base de datos



1. **Seleccione 2 riesgos que considere críticos detectarlos y que se puedan detectar en un SIEM**
2. **Configure splunk para detectar esos 2 riesgos**
3. **Pruebe que Splunk puede destectar esos riesgos.**
4. **Cree un repositorio en GitHub para colocar todas las evidencias y resultados del taller.**