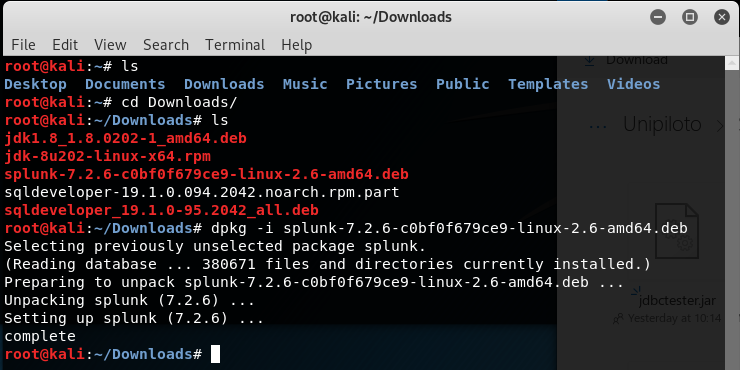
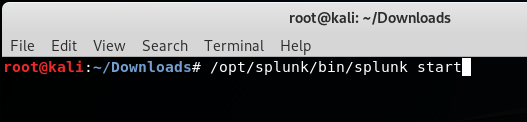
**TALLER 4**

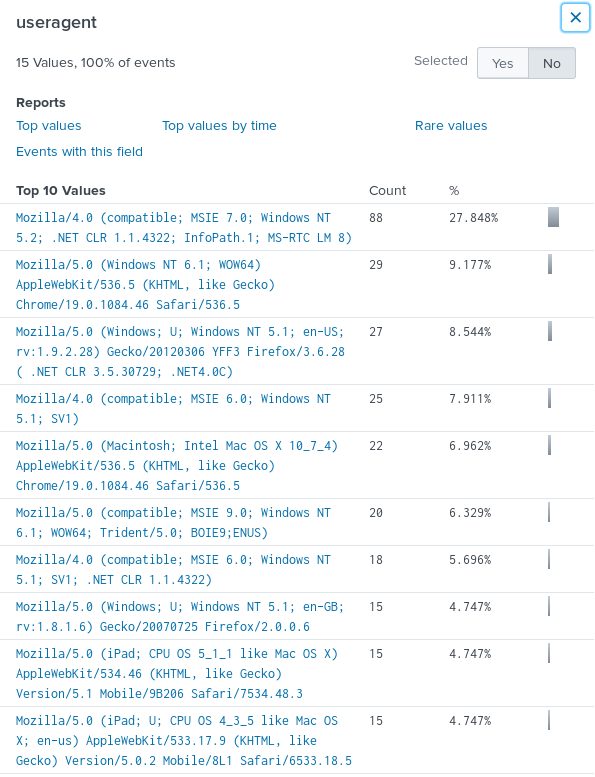
1. Instalar splunk en la máquina virtual



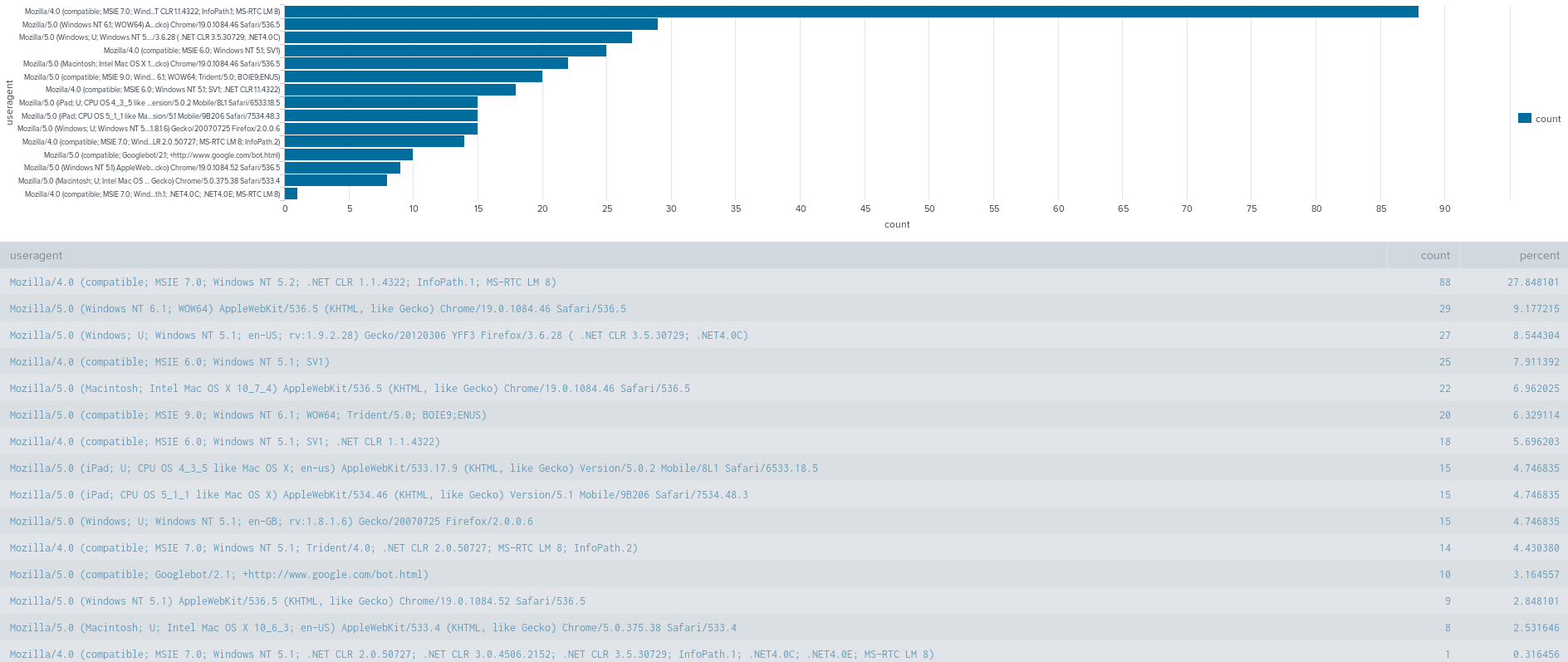
Inicializamos el splunk

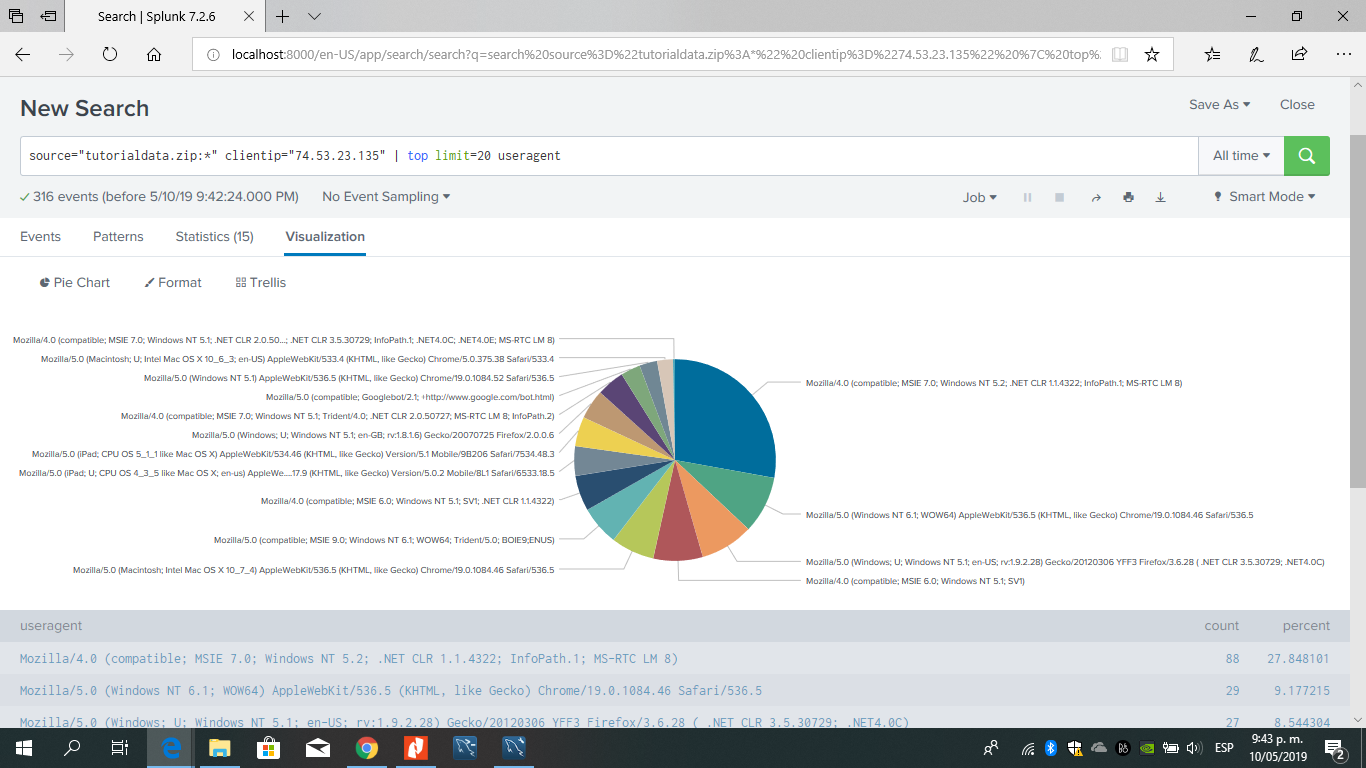


1. Hacer tutorial: buscar los navegadores utilizados por la dirección 74.53.23.135



Se filtra por el top 20





1. Configure la BD mysql en la maquina virtual.
2. Seleccione 2 riesgos que considere críticos detectarlos y que se puedan detectar en un SIEM.
3. Configure splunk para detectar esos 2 riesgos.
4. Pruebe que splunk puede detectar esos 2 riesgos.
5. Cree un repositorio en GitHub para colocar todas las evidencias y resultados del taller.