Taller de seguridad

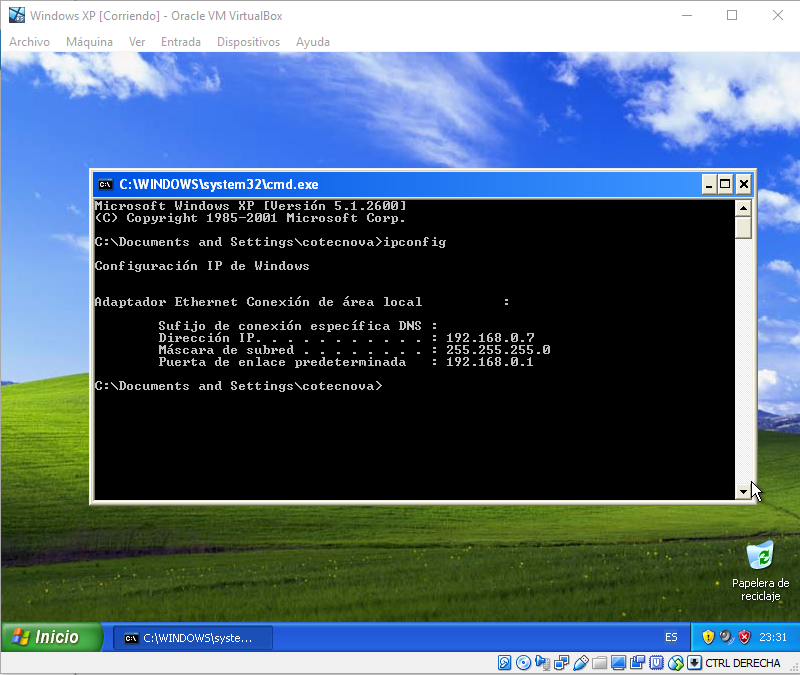
Usando Kali Linux y las máquinas virtuales (Windows 7, Windows XP y Metasploitable 2) implementar una auditoria interna que cumpla los siguientes ítems.

1. Obtención de Información
2. Enumeración de Sistemas
3. Análisis de Vulnerabilidades
4. Explotación de Vulnerabilidades
5. Post-Explotación de Vulnerabilidades
6. Ataques contra credenciales
7. Informe

La auditoria sera en un sistema operativo Windows XP

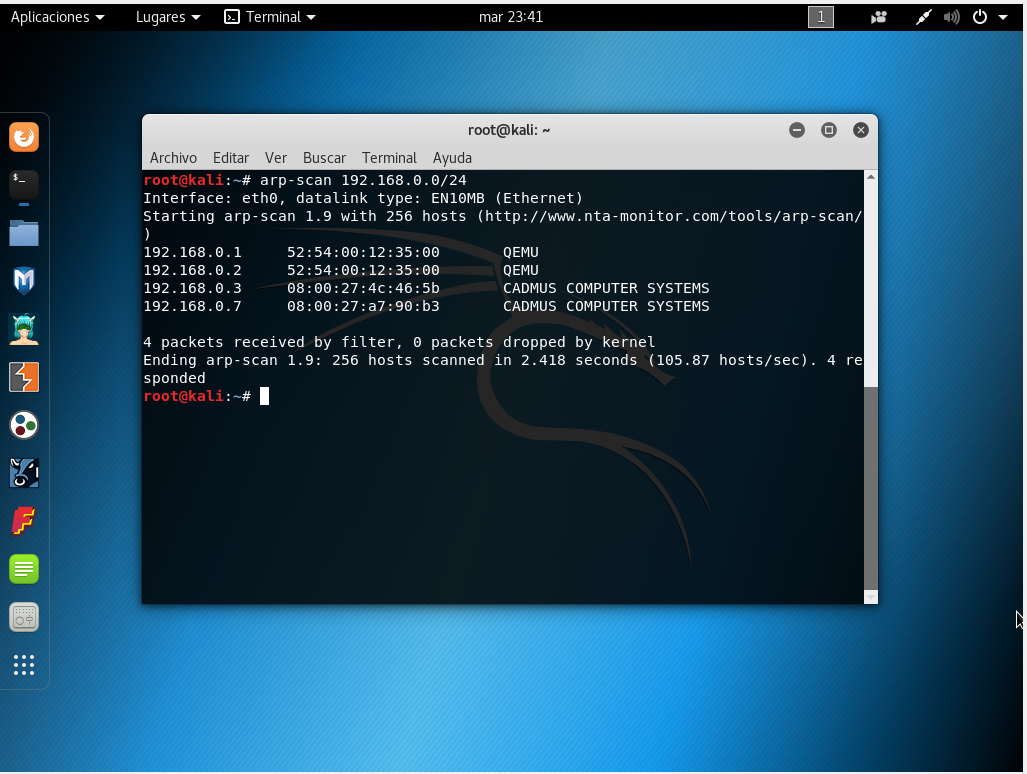
1. Obtención de Información

Obtenemos la ip de la maquina

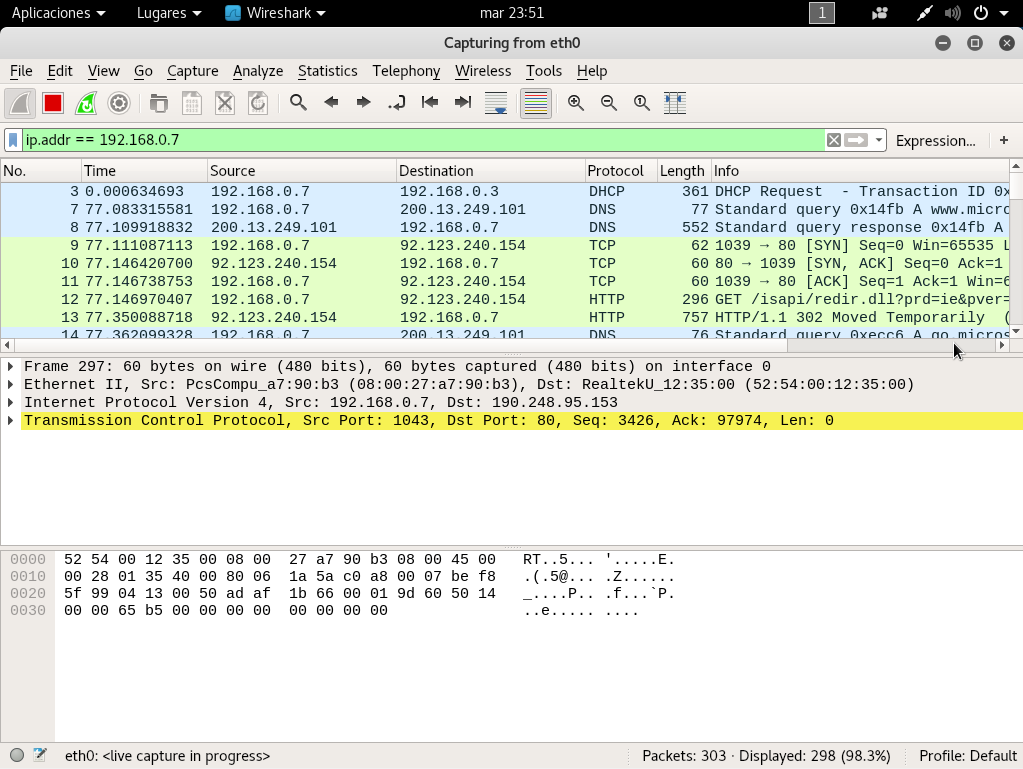


1. Enumeración de Sistemas

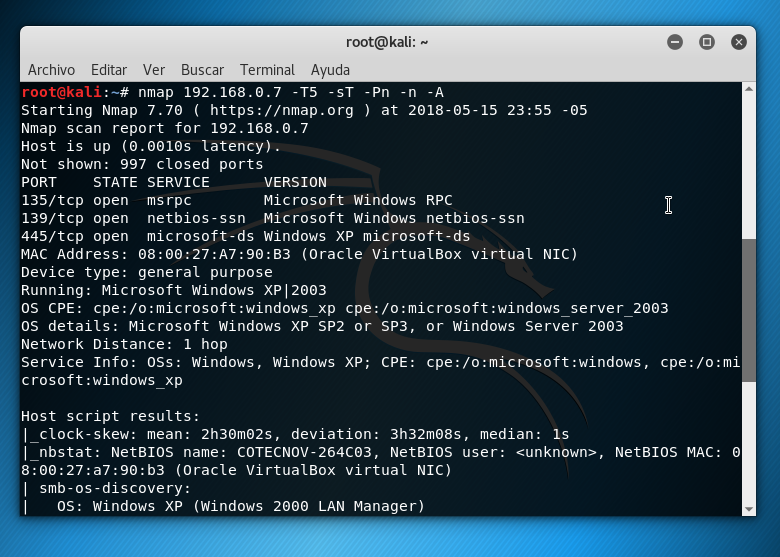
Desde Kali Linux se realiza un arp-scan

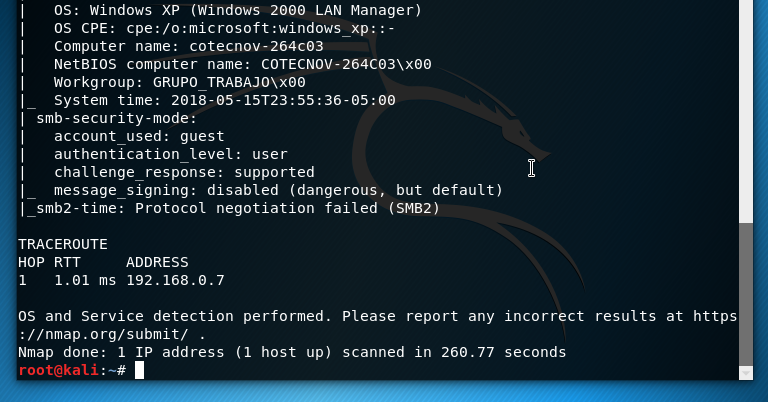


Se ubica la dirección ip de la maquina Windows XP y se realiza un análisis mediante el Wireshark

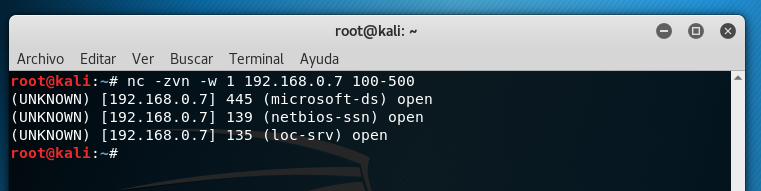


Se realiza un escaneo de Puertos y verificación del sistema operativo e información

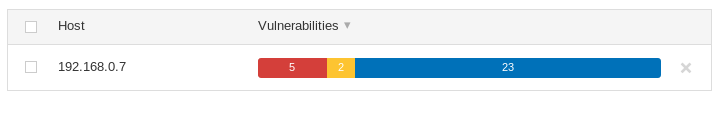


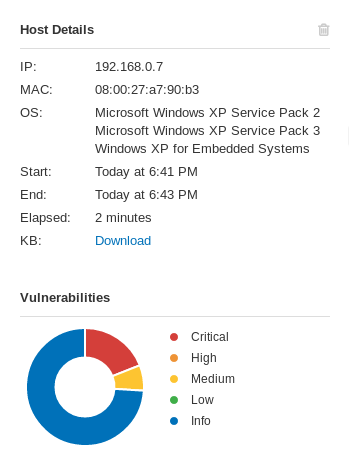


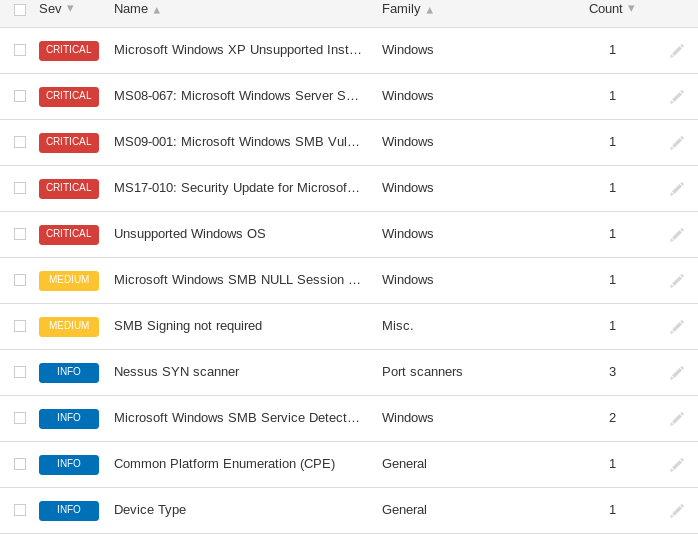
Usamos el comando nc

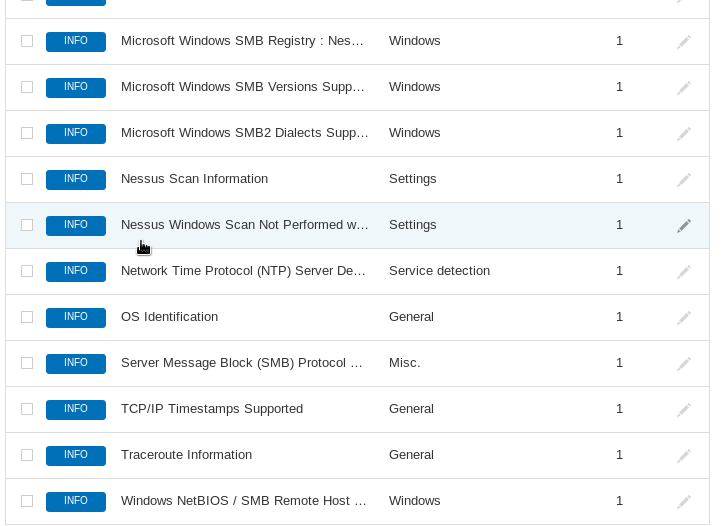


1. Analisis con nessus



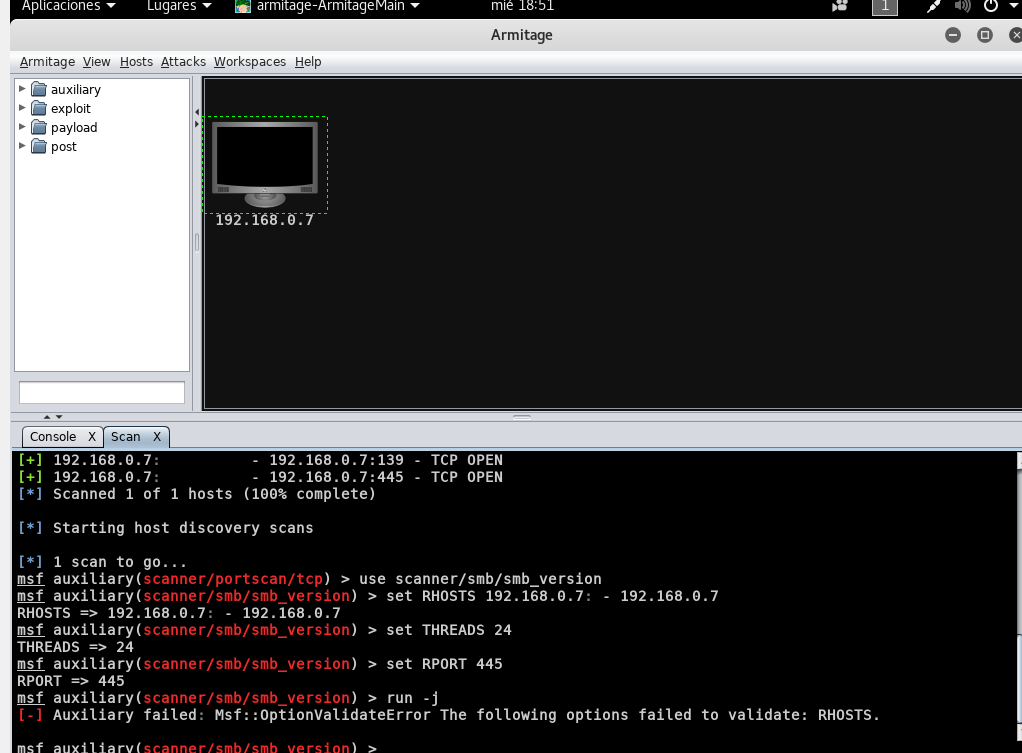


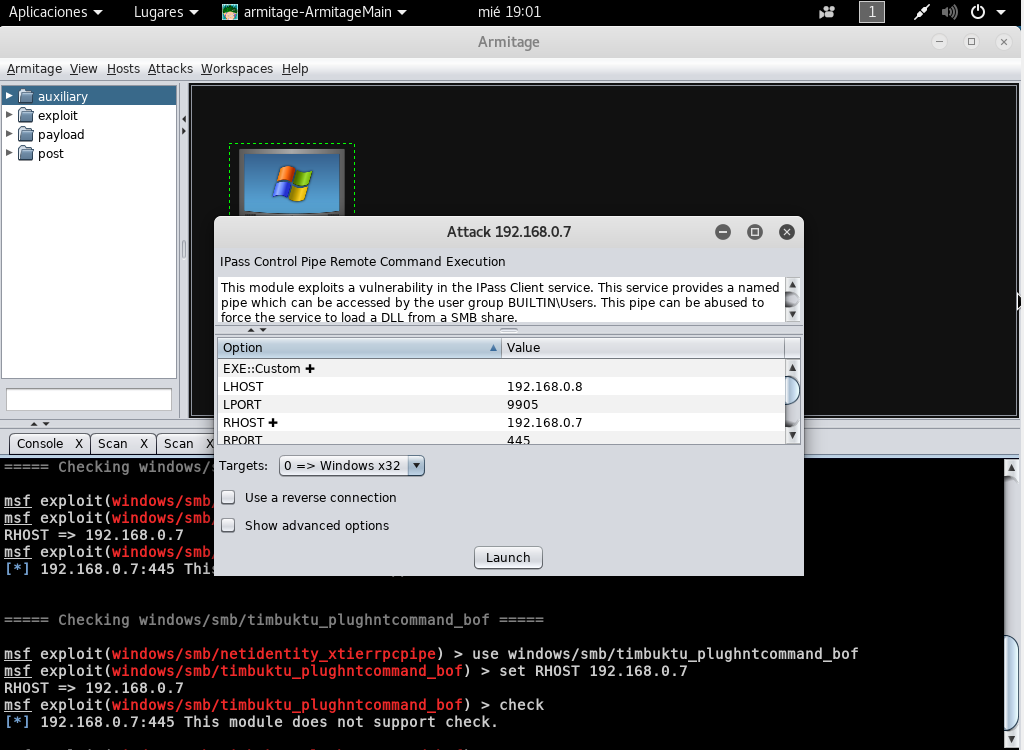




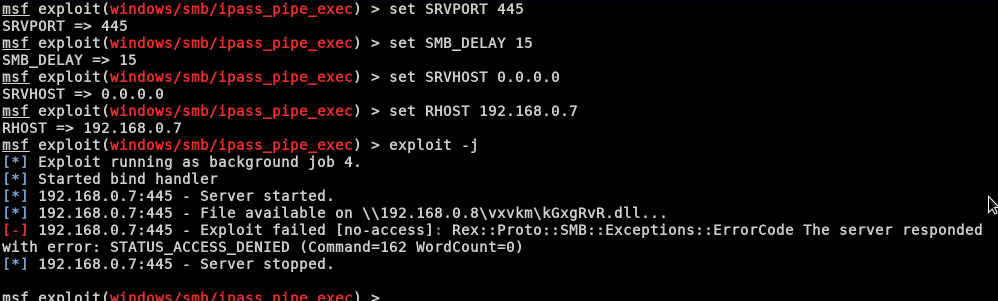
1. Explotcion de vurlnerabilidades

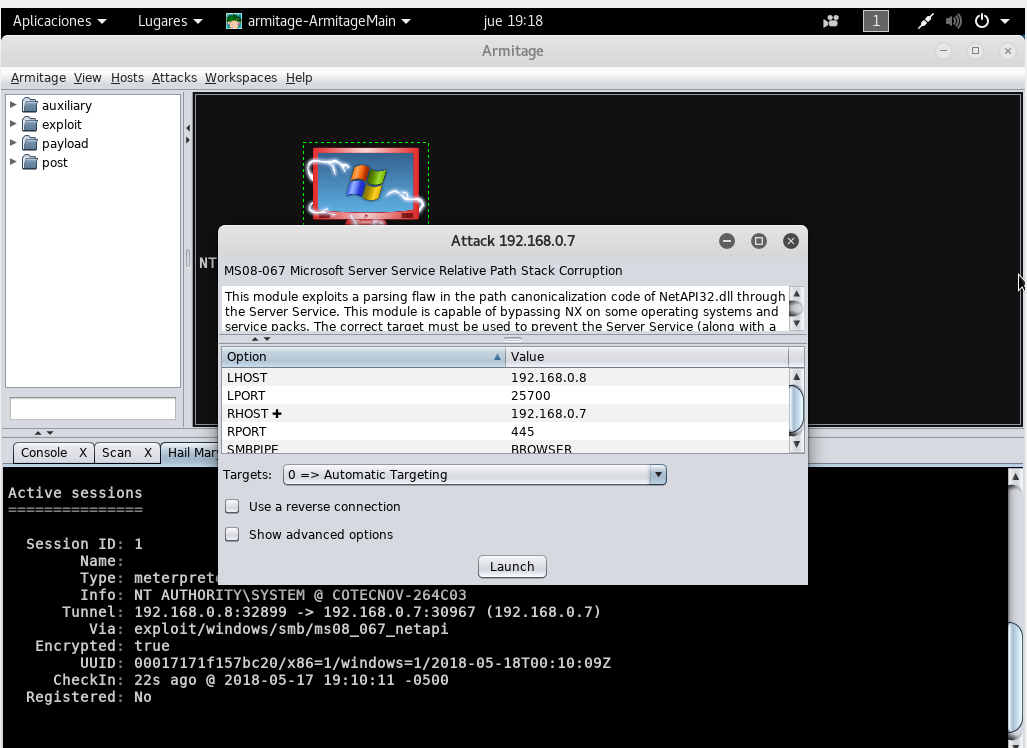
Trabajando con armitage

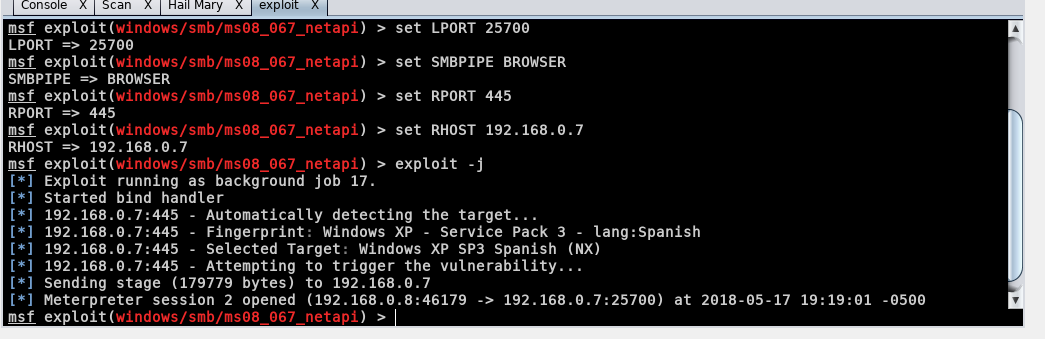


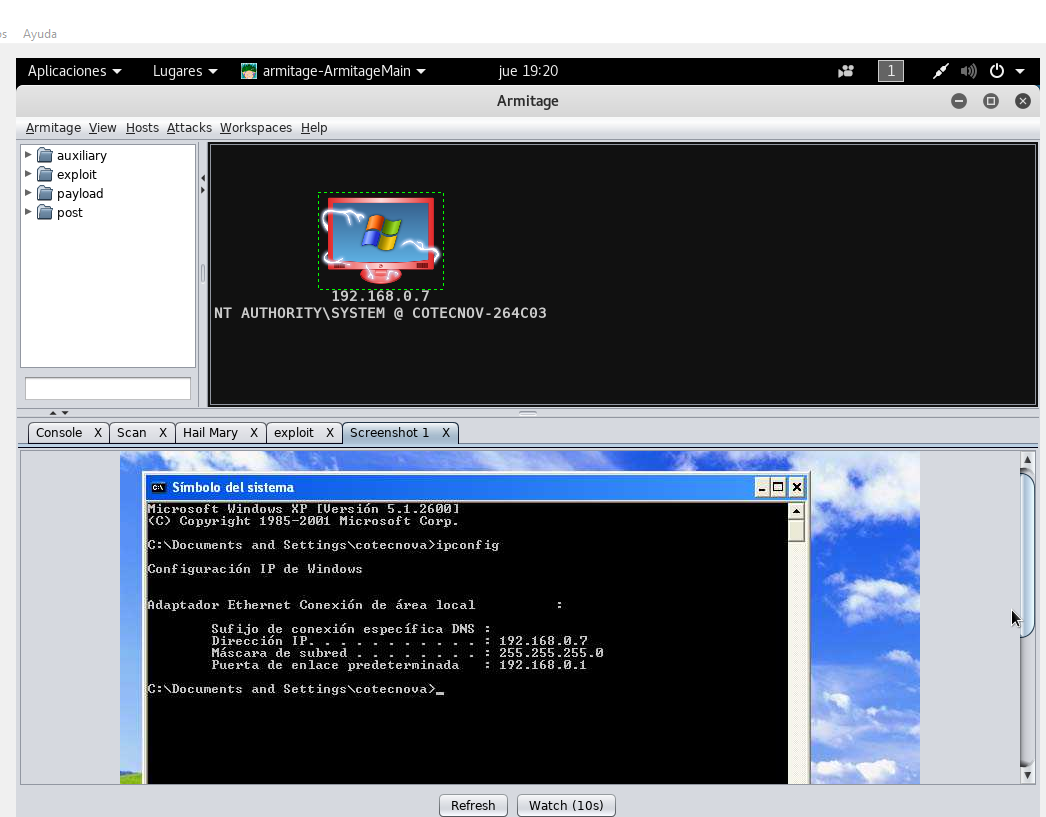


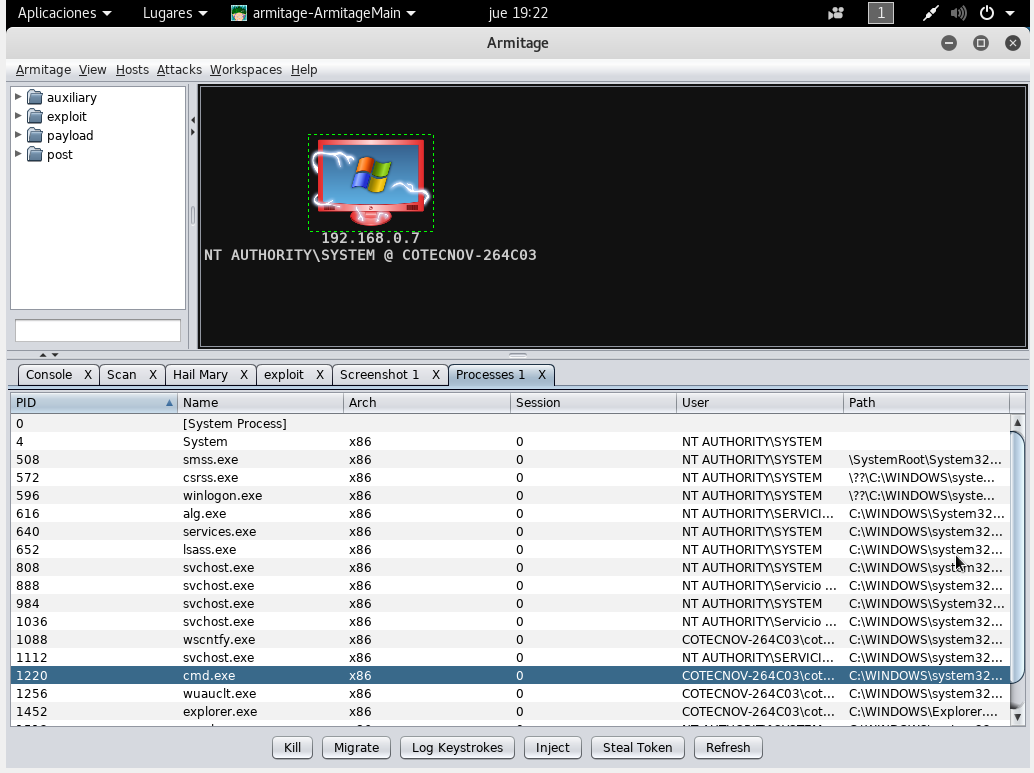












6. Ataques contra credenciales

