**INSTITUTO TECNOLÓGICO DE DURANGO**

**Seguridad Web**



**Reporte de Práctica**

**Máquina vulnerable Windows 7**

**Docente:**

López Quiñones José Roberto

**Alumno:**

Deyanira Idaly Campos Romero 15041193

**Fecha de entrega**: 18 Febrero de 2019

**Objetivo**

Comprobar si existen vulnerabilidades dentro de una máquina virtual con un sistema operativo Windows 7. Esta práctica tiene diversos objetivos, pero el general y más importante de ellos , es el mencionado anteriormente.

El primer objetivo es reconocer los puertos que se encuentran abiertos para esa máquina virtual haciendo uso de la herramienta nmap, donde se dará una lista de todos los puertos abiertos en la máquina virtual donde se pueden tratar de buscar exploits, después de esto se identifican dichos puertos, este paso es donde se ve cuáles de ellos se logran identificar (sus servicios) para poder buscar un exploit correspondiente (Este es el siguiente paso llamado búsqueda), donde dentro de una base de datos de exploits, se buscan exploits para los diferentes puertos según el sistema operativo y se pueden buscar posibles vulnerabilidades, por último se hace la ejecución de los diversos exploits donde se comprueba si alguna de ellos funciona correctamente haciendo uso de la herramienta armitage.

Se realizará dicha práctica utilizando las herramientas necesarias para realizar diferentes pasos dentro de las mismas como kali. Todos los pasos que se requieren dentro de esta práctica para comprobar si una máquina virtual es vulnerable se harán aplicando las habilidades adquiridas en la clase de seguridad web, sobre los diferentes conceptos, ya que se han realizado practicas donde se aplican los mismos anteriormente, también se pretende ampliar todos aquellos conocimientos que se tienen sobre algunos conceptos como bases de datos de exploits, comandos y hosts.

Otro de los objetivos importantes de la práctica es el darse cuenta de las dificultades que se presentan al querer implementar una máquina virtual que sea vulnerable en muchos aspectos, en este caso se trató con una máquina virtual con el sistema operativo Windows 7 en sus primeras versiones.

Ampliando un poco más el objetivo se pretende detectar y aprovechar aquellas vulnerabilidades dentro de maquina como ya se mencionó y el correcto manejo de la información que se encuentre dentro de los mismos (solamente para uso informativo y verificación de comandos, sin hacer mal uso de la misma).

**Desarrollo**

**Armitage**

Armitage es una Herramienta e colaboración en equipo que permite el uso de Scripts para Metasploit que permite visualizar objetivos, recomienda exploits y expone las características avanzadas de post-explotación que tiene el framework.

A través de una instancia de metasploit, su equipo (grupo de trabajo) podrá realizar lo siguiente:

* Usar las mismas sesiones.
* Compartir host, datos capturados y archivos descargados.
* Comunicarse a través de un registro de eventos compartido.
* Ejecutar bots para automatizar las tareas del equipo (grupo de trabajo).

Armitage es una herramienta gráfica del conocido framework Metasploit la cual nos permite buscar vulnerabilidades sobre cualquier equipo que esté en una red a la que tengamos acceso. Esta herramienta se puede encontrar en distribuciones de pentesting como Kali Linux.

**Reconocimiento**

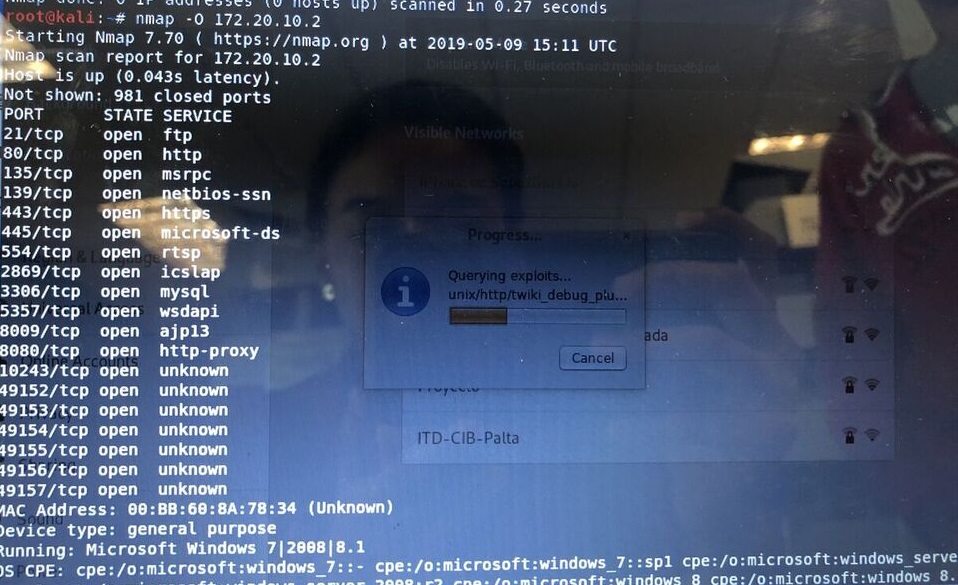
Esta es la primera etapa y consiste en, como su nombre lo dice, reconocer todos los puertos que se encuentran abiertos dentro de la máquina virtual que se creó anteriormente, haciendo uso del comando nmap en kali Linux.

1. Se enciende la máquina virtual vulnerable con sistema Windows 7, donde se deshabilita el firewall.



En esta misma maquina se consulta su dirección IP entrando al cmd y ejecutando el comando ipconfig.

1. Dentro de kali se ejecuta el comando: nmap –O direccionip, para poder conocer los puertos abiertos dentro de dicha máquina. En este caso la ip era: 172.20.10.2



Se pudo observar que existen muchos puertos abiertos dentro de la maquina con Windows 7.

**Identificación**

En esta parte de la práctica se identifican aquellos puertos que se conocen o se sabe cuál es su finalidad para en la siguiente etapa buscar sus exploits correspondientes.

1. Una vez que se da la lista de los puertos abiertos se observa cuáles de ellos se conocen y de qué servicio se tratan. En este caso se reconocieron los puertos:

* **FTP 21/tcp:** FTP (siglas en inglés de File Transfer Protocol, ‘Protocolo de Transferencia de Archivos’), es un protocolo de red para la transferencia de archivos entre sistemas interconectados o enlazados a Internet, basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.
* **HTTP 80/tcp:**Hypertext Transfer Protocol (HTTP) (o Protocolo de Transferencia de Hipertexto en español) es un protocolo de la capa de aplicación para la transmisión de documentos hipermedia, como HTML. Fue diseñado para la comunicación entre los navegadores y servidores web, aunque puede ser utilizado para otros propósitos también. Sigue el clásico modelo cliente-servidor, en el que un cliente establece una conexión, realizando una petición a un servidor y espera una respuesta del mismo.
* **MSRPC 135/tcp:** Microsoft RPC ( llamada a procedimiento remoto de Microsoft ) es una versión modificada de DCE / RPC . Las adiciones incluyen soporte parcial para cadenas UCS-2 (pero no Unicode ), mangos implícitos y cálculos complejos en los paradigmas de estructura y cadena de longitud variable ya presentes en DCE / RPC.
* **NETBIOS SSN 139/tcp :**NetBIOS, "Network Basic Input/Output System", es, (en sentido estricto) una especificación de interfaz para acceso a servicios de red, es decir, una capa de software desarrollado para enlazar un sistema operativo de red con hardware específico. NetBIOS fue originalmente desarrollado por IBM y Sytek como API/APIS para el software cliente de recursos de una Red de área local (LAN). Desde su creación, NetBIOS se ha convertido en el fundamento de muchas otras aplicaciones de red.
* **RTSP 554/tcp:** ( Real Time Streaming Protocol ), es un protocolo de transmisión de vídeo o audio a través de UDP o TCP principalmente lo que nos permite tener el control remoto de cualquier dispositivo que tenga dicha compatibilidad. Esto para poder centralizar cámaras de videovigilancia o NVR´S a un CMS para así tener la posibilidad de integrar todo un sistema de CCTV a un centro de control.
* **ICSLAP 2869/tcp:** El puerto TCP 2869 es comúnmente utilizado por el servicio o programa ICSLAP. Este puerto es un proxy interno integrado en Microsoft Internet Connection Firewall (ICF) o Internet Connection Sharing (ICS), que se conecta a Microsoft para enviar los registros de errores.
* **WSDAPI 5357/tcp:** La API de servicios web en dispositivos (WSDAPI, por sus siglas en inglés) se utiliza para desarrollar aplicaciones cliente que encuentran y acceden a dispositivos, y para desarrollar hosts de dispositivos y servicios asociados que se ejecutan en Windows Vista y Windows Server 2008. La API de descubrimiento de funciones y la herramienta WsdCodeGen son herramientas complementarias que se puede utilizar para el cliente, el dispositivo host y el desarrollo de servicios. Las interfaces WSDAPI se pueden usar directamente para exponer una funcionalidad avanzada.
* **HTTPS 443/tcp:** HTTPS (HyperText Transfer Protocol Secure, Protocolo de transferencia de hipertexto) es un protocolo de comunicación de Internet que protege la integridad y la confidencialidad de los datos de los usuarios entre sus ordenadores y el sitio web, hace uso de cifrado, integridad y autenticación.
* **MYSQL 3306/tcp:** MySQL es un sistema de gestión de base de datos relacional (RDBMS) de código abierto, basado en lenguaje de consulta estructurado (SQL).
* **HTTP-PROXY 8080/tcp:** Un servidor proxy es un equipo dedicado o un sistema de software que se ejecuta en un equipo de cómputo que actúa como intermediario entre un dispositivo de punto final, como una computadora, y otro servidor del cual un usuario o cliente solicita un servicio. El servidor proxy puede existir en la misma máquina que un servidor de firewall o puede estar en un servidor independiente, que reenvía las solicitudes a través del firewall.
* **MICROSOFT-DS 445/tcp:** El protocolo SMB (en inglés, Server Message Block) es un protocolo para compartir archivos que se ejecuta en el puerto 445.
* **AJP13 8009/tcp:** El Apache JServ Protocol (AJP) es, en el contexto de la World Wide Web un protocolo binario que permite enviar solicitudes desde un servidor web a un servidor de aplicaciones que se encuentra detrás del servidor web. También permite monitoreo dado que el servidor web puede enviar un ping al servidor de aplicación.

El protocolo AJP suele utilizarse en un despliegue de balance de carga en el que uno o más servidores web front-end envían solicitudes a uno o varios servidores de aplicaciones. Las sesiones se redirigen al servidor de aplicaciones correcto utilizando un mecanismo de enrutación en el que cada servidor de aplicaciones recibe un nombre (denominado ruta).

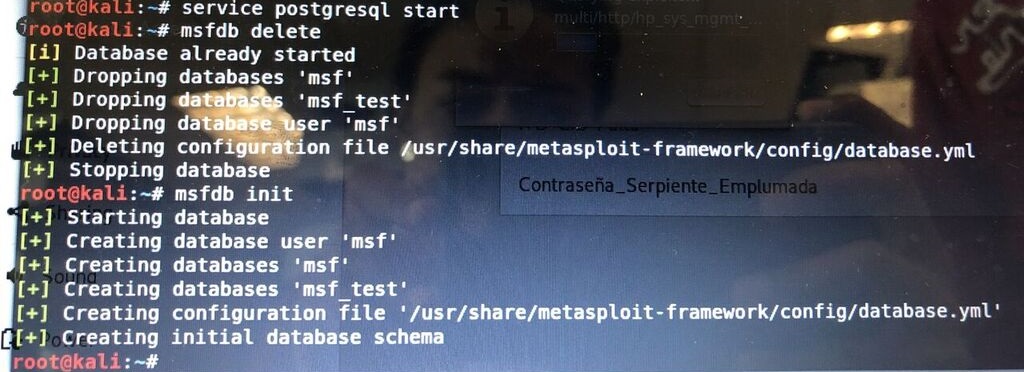
**Búsqueda**

1. Se ingresa a la dirección <https://www.exploit-db.com/> para buscar dentro de la base de datos que se encuentra en dicha URL, los exploits que se pueden realizar para los puertos que fueron identificados.
2. En este caso se pudieron encontrar los siguientes exploits para los puertos reconocidos.

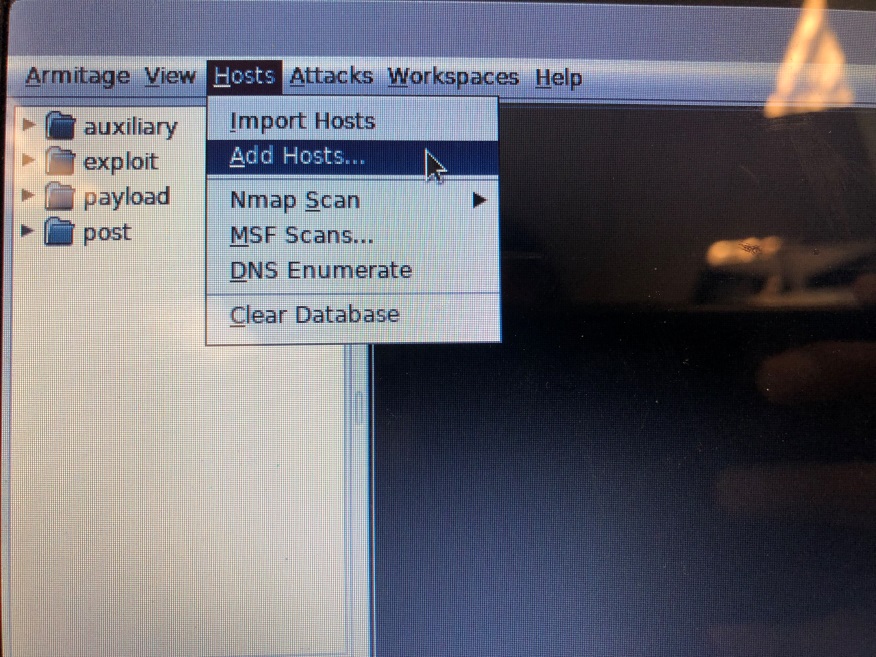
**Ejecución**

1. Se ingresa a kali y se ejecuta en la consola, los siguientes comandos, antes de ejecutar la herramienta armitage.

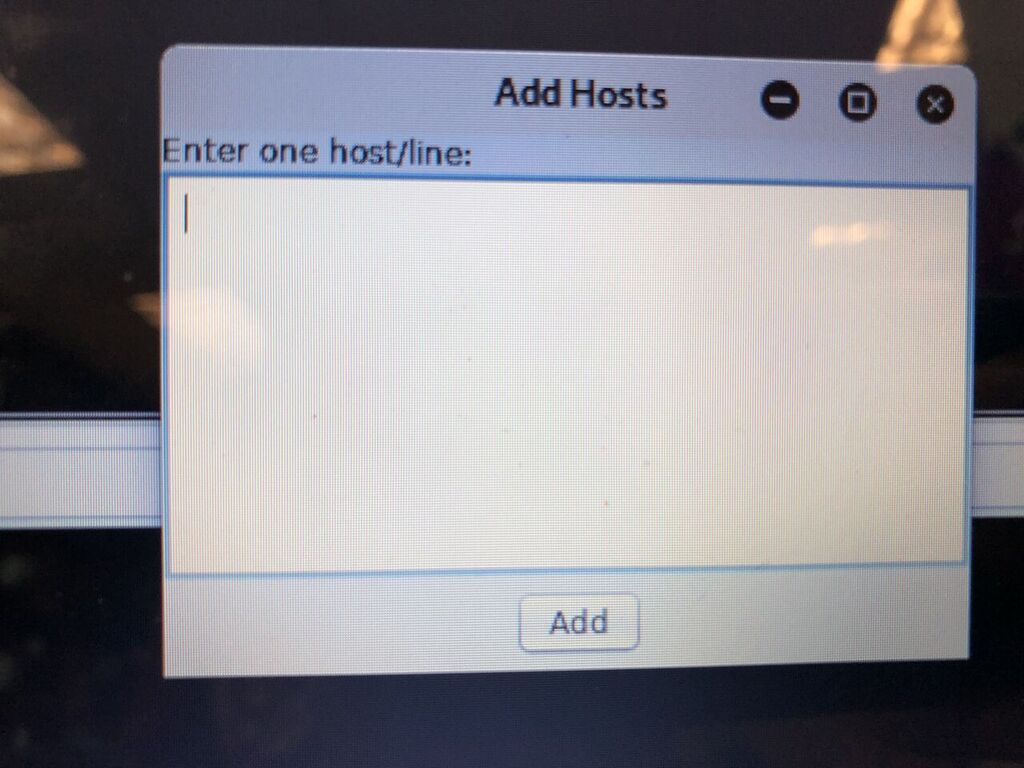
Para iniciar el servicio, borrar la base de datos e inicializarla de nuevo.



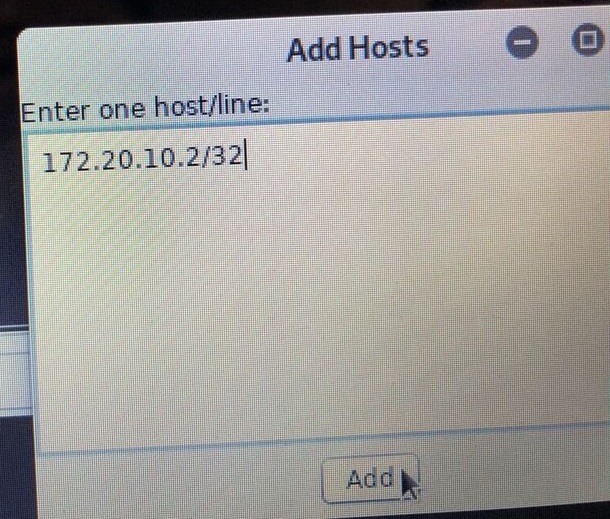
1. Una vez que se ejecutaron correctamente dichos comandos, se da clic en la herramienta para comenzar con su ejecución, nos aparecerá un recuadro, todos los parámetros se dejan de la misma manera que aparecen predeterminadamente.
2. Una vez que se abre la herramienta aparece una ventana, donde en el menú superior se da clic en la opción HOST>ADD HOSTS , Para agregar el host se siguen los siguientes pasos:



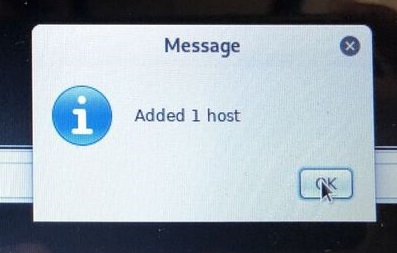
Después aparecerá una ventana como la siguiente:



En esta ventana se coloca la dirección IP de la máquina virtual que se quiere atacar y se da clic en add.

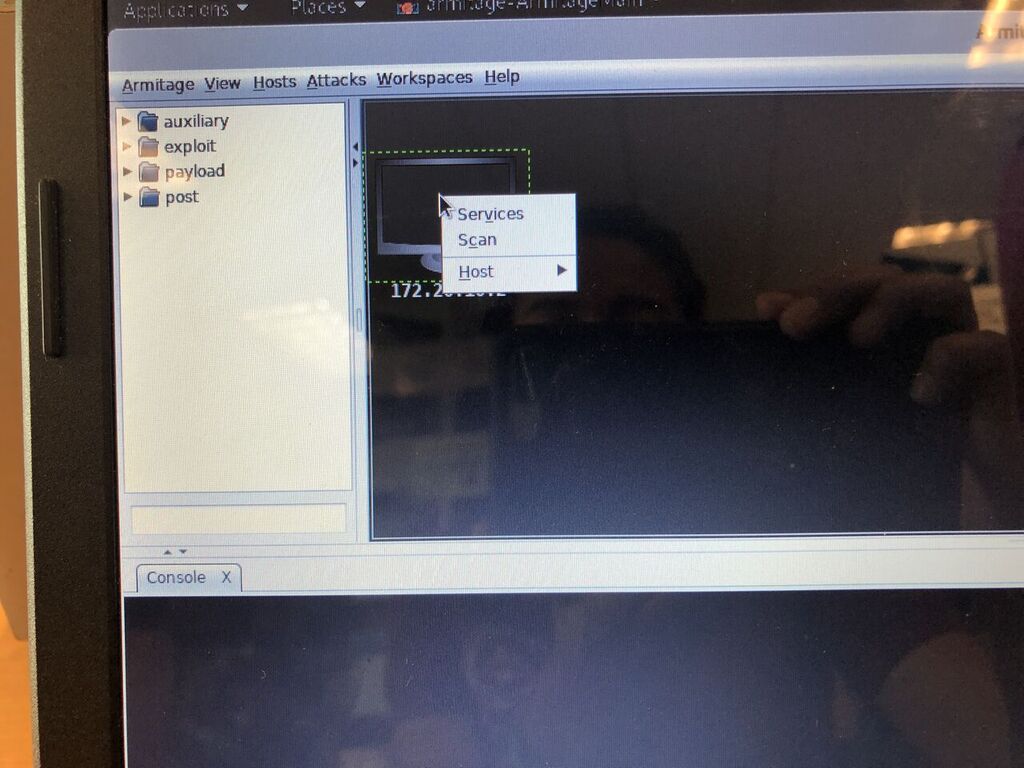


Dando clic en add y agregado correctamente nos aparecerá este mensaje. Y dando clic en Ok se mostrara una pequeña imagen de una computadora dentro del espacio de trabajo (el host).

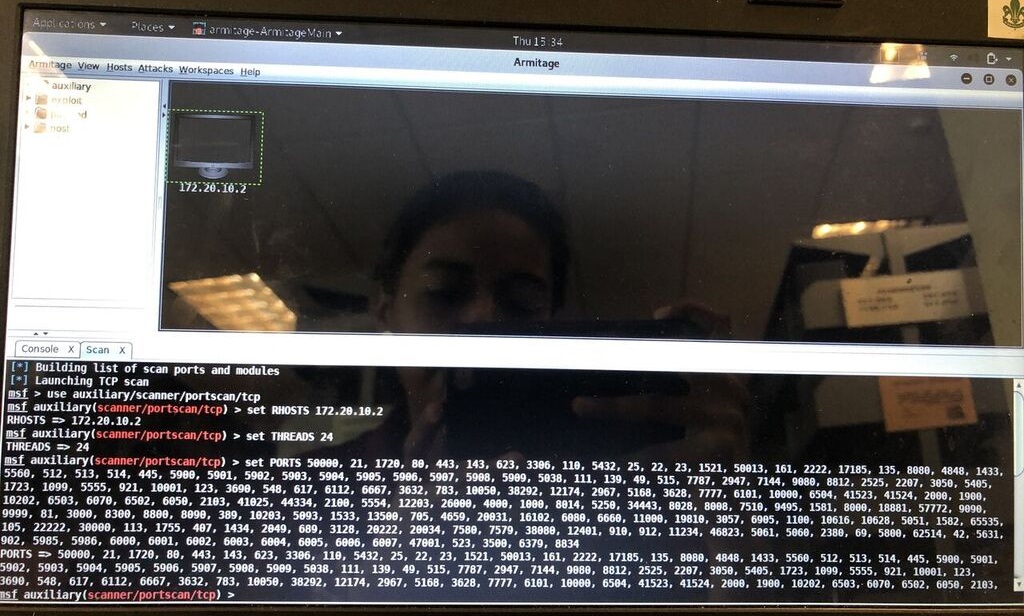


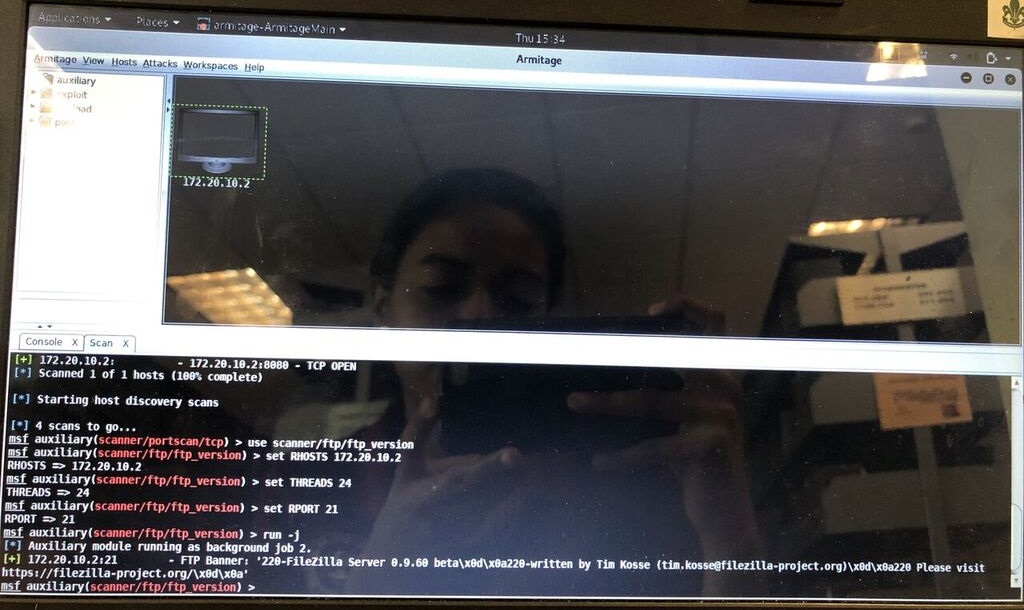
1. Una vez agregado el host se hizo primeramente un scaneo a la red para ver los puertos disponibles (reconocerlos), identificarlos, buscarlos y después ver su exploit.

* Se da clic derecho sobre el host agregado.
* Se da clic en la opción scan.



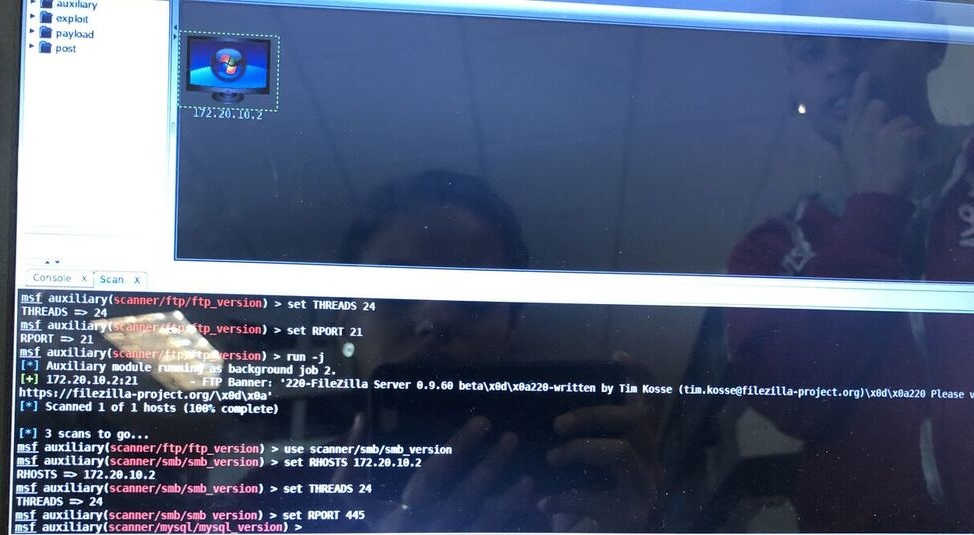
* Aquí comienza el scaneo, donde se pueden ver los puertos, los servicios que utilizan, su estado, etc.

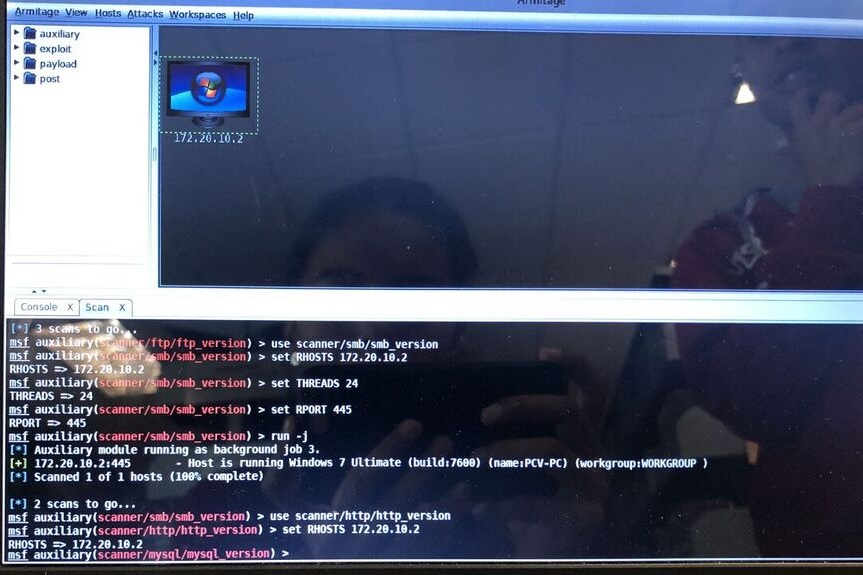


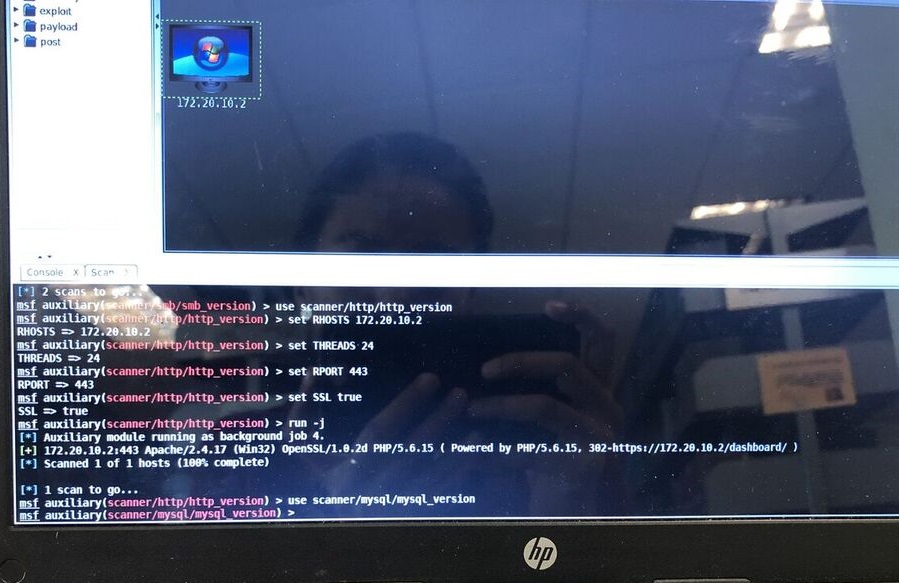


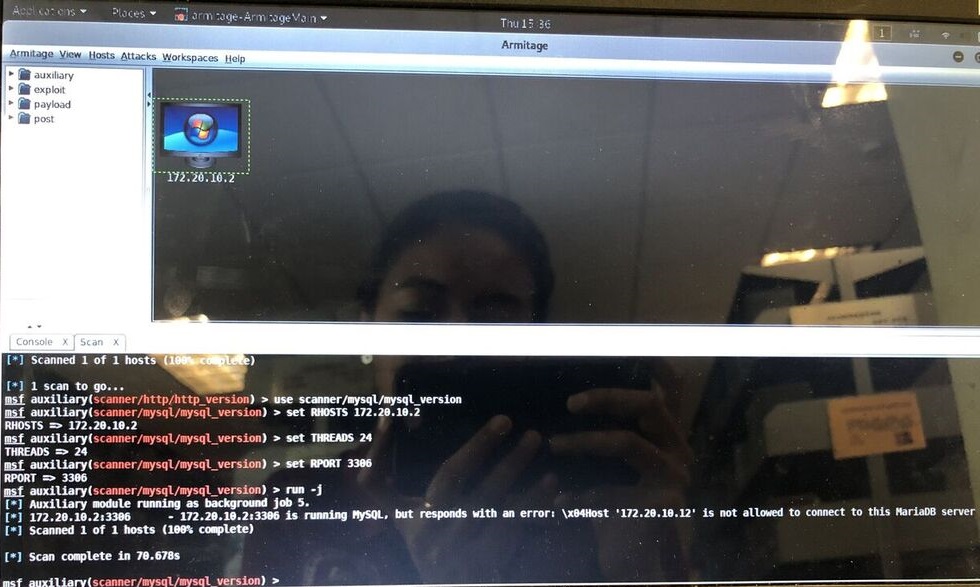
Estado de los puertos:









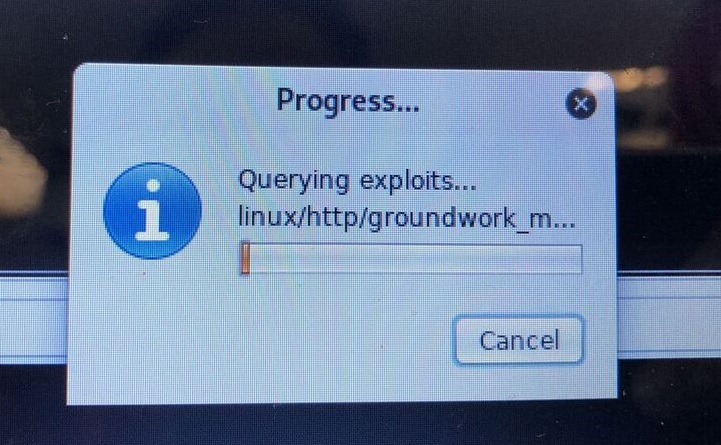


1. Después del scaneo y conocer en promedio los puertos y sus servicios, se hará para buscar los exploits disponibles para cada uno de ellos ahora desde armitage.

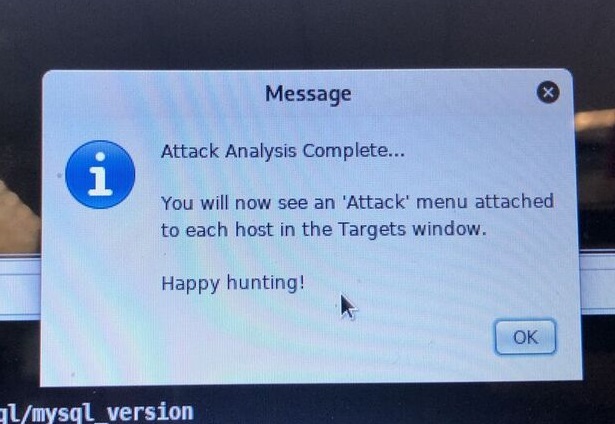
Para esto se da clic en la opción del menú superior ATTACKS > FIND ATTACKS.



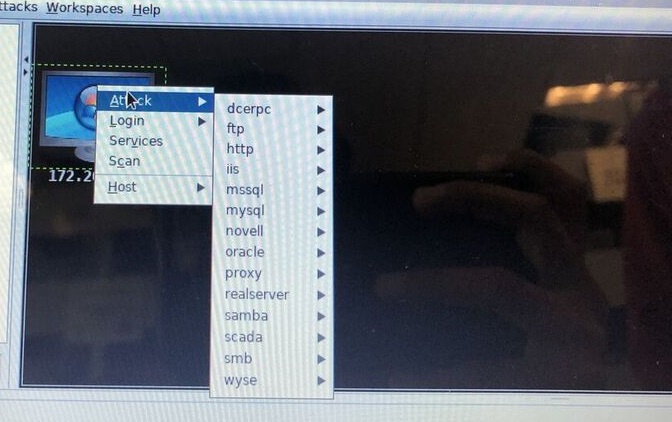
Comienzan a buscarse los ataques disponibles (exploits).

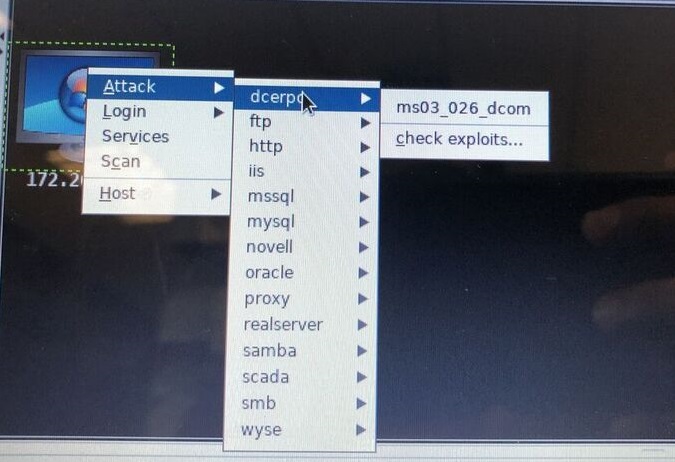


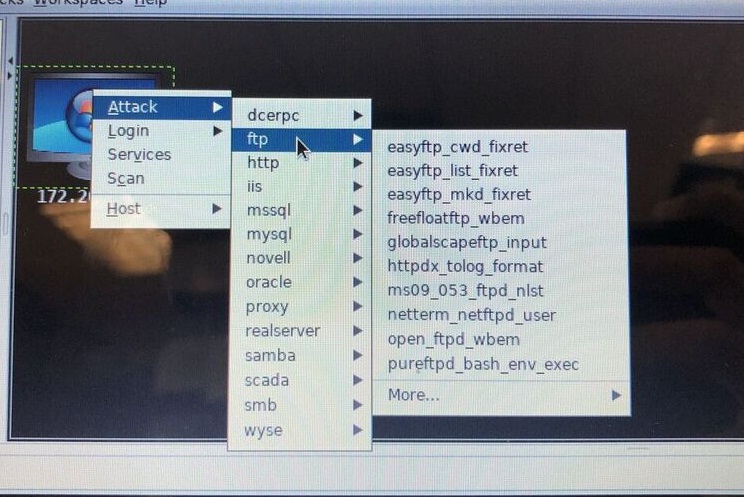
Una vez finalizada la búsqueda nos aparece el mensaje como el siguiente: donde indica que el análisis está completo y que ahora se pueden ver los distintos ataques para cada puerto en el menú correspondiente.

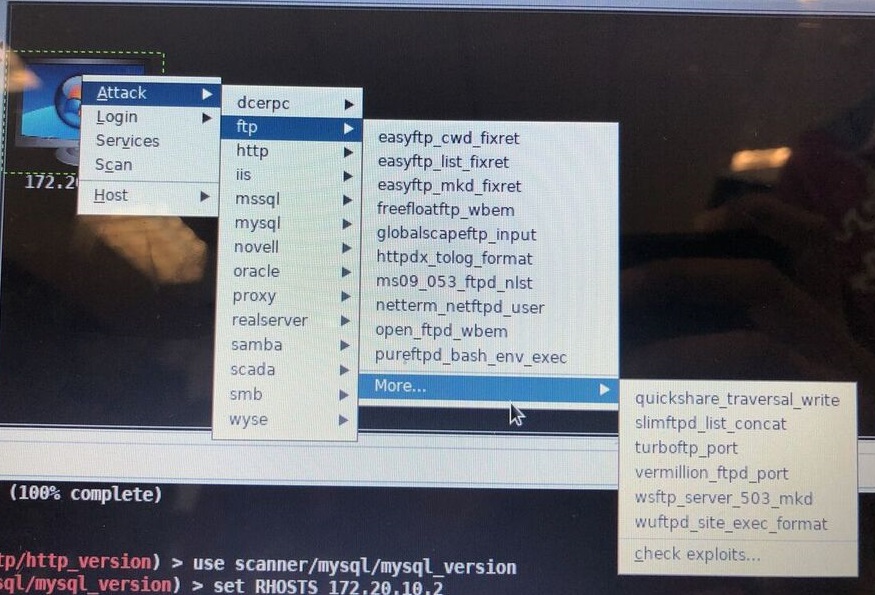


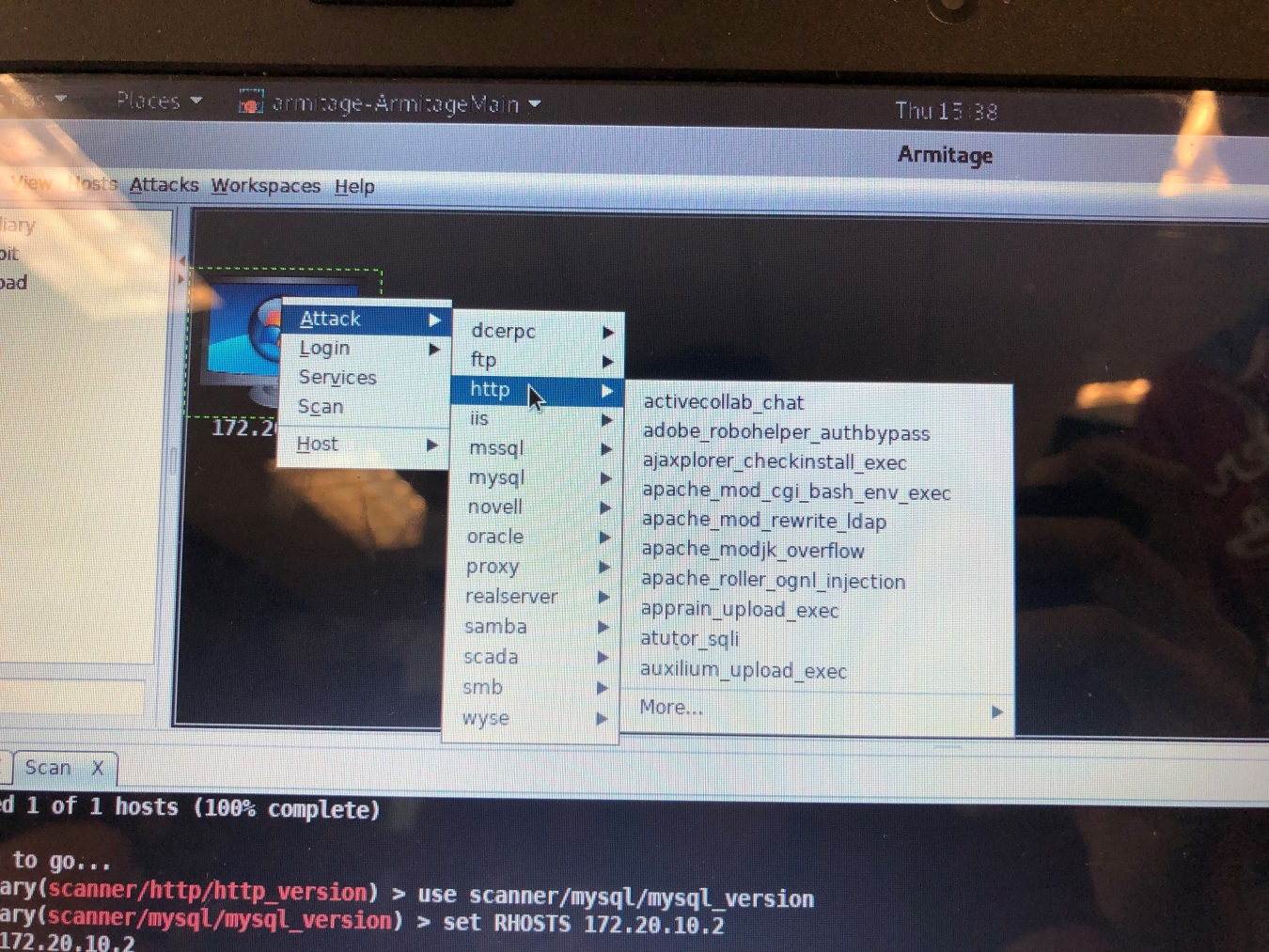
1. Se pueden realizar los ataques manualmente, si se da clic derecho en el host y se selecciona la opción attack, se despliega un menú con todos los puertos donde se encontraron exploits, si se selecciona alguno de ellos se despliega otro submenú con los exploits disponibles.

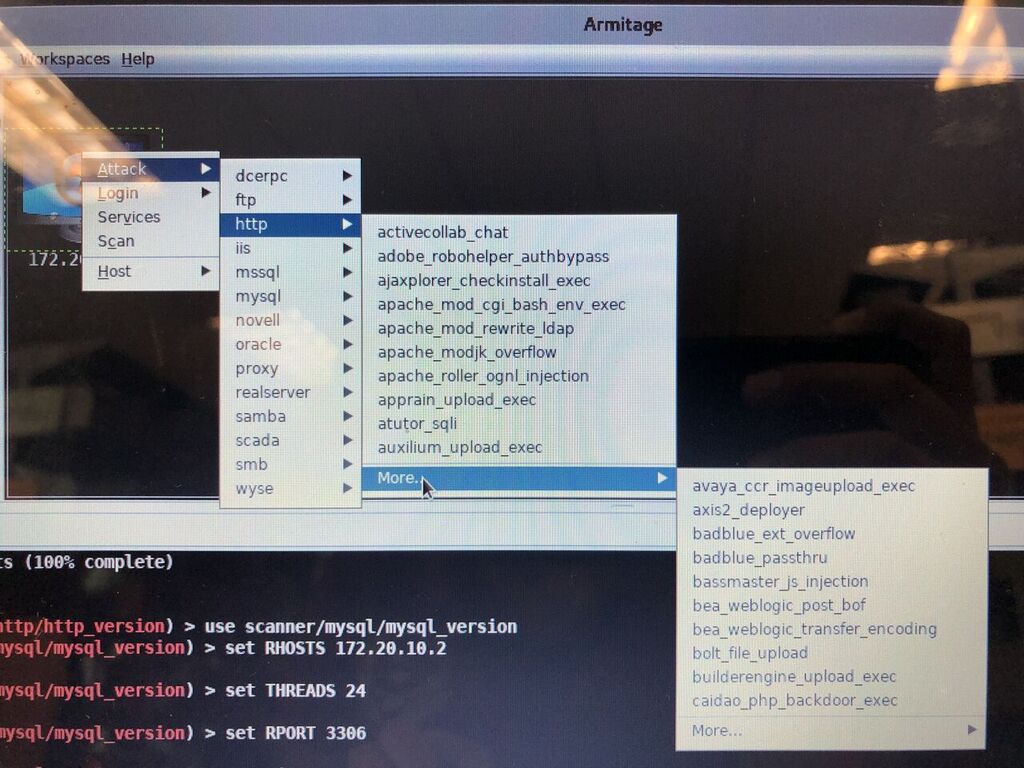


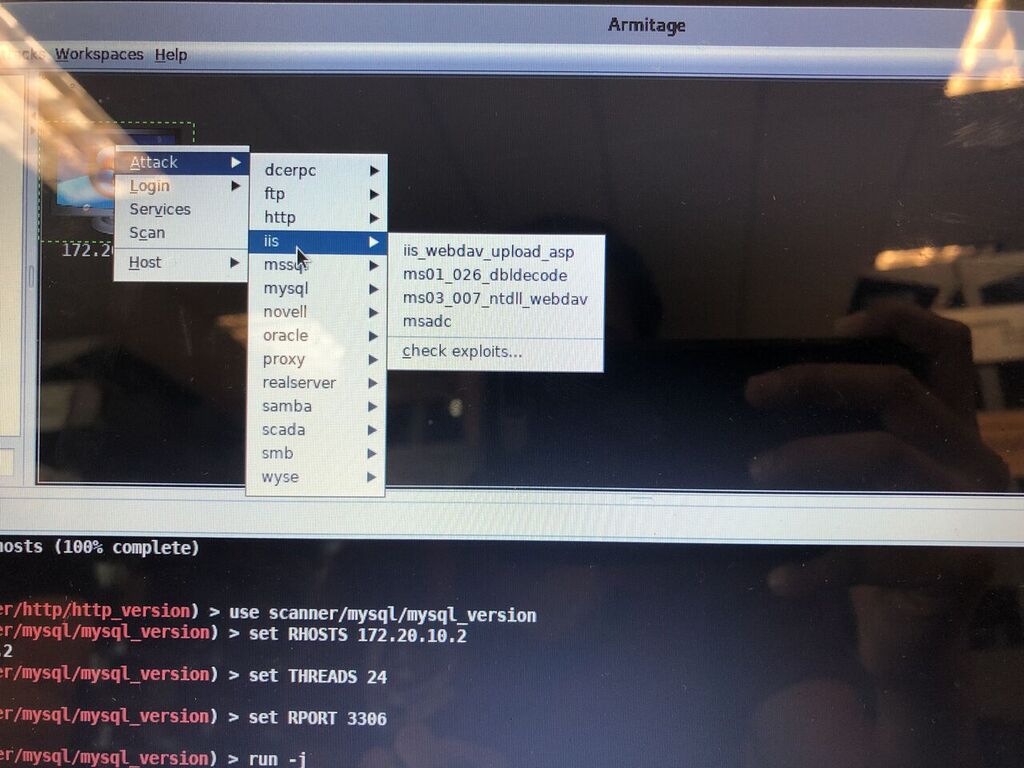


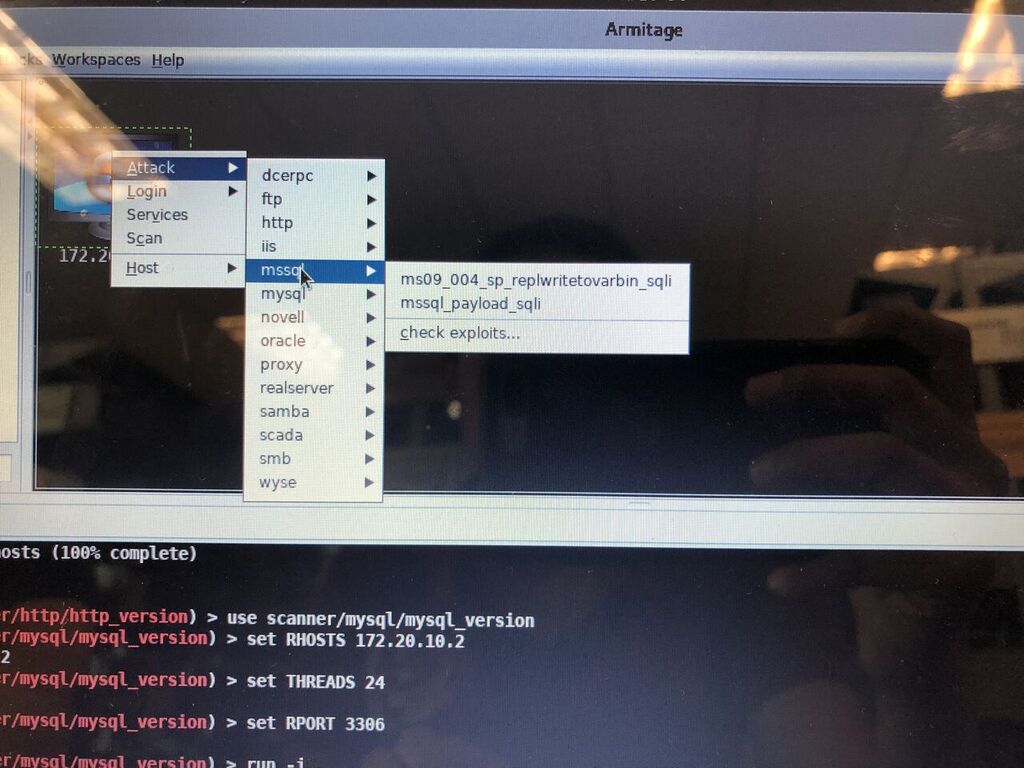


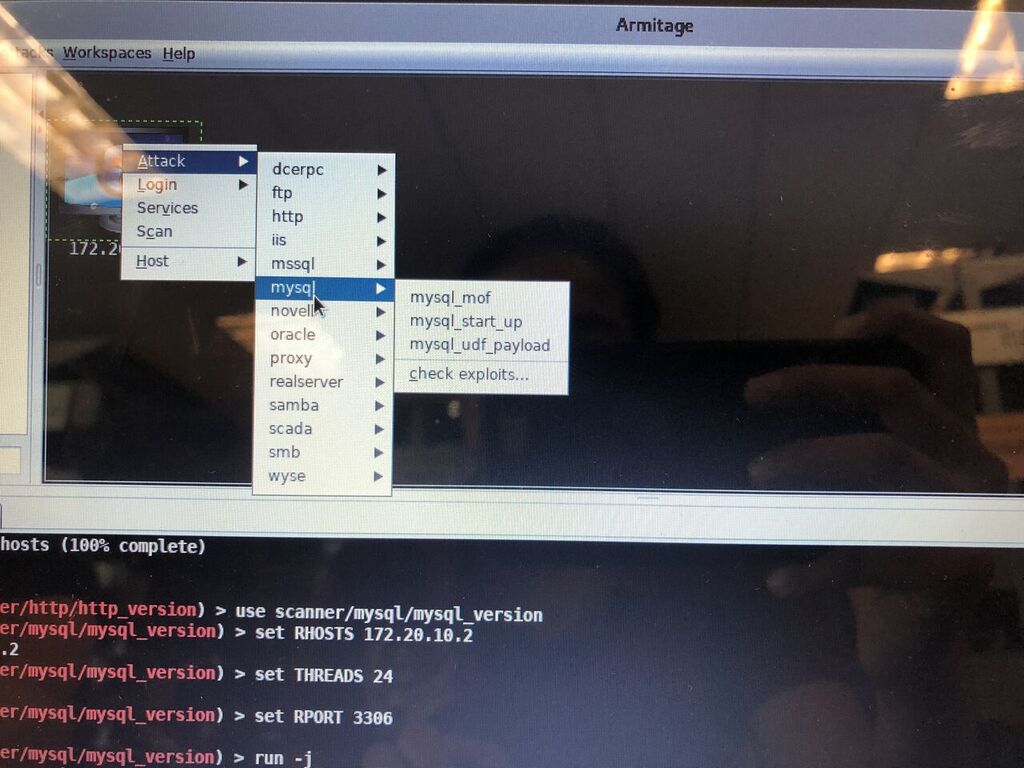


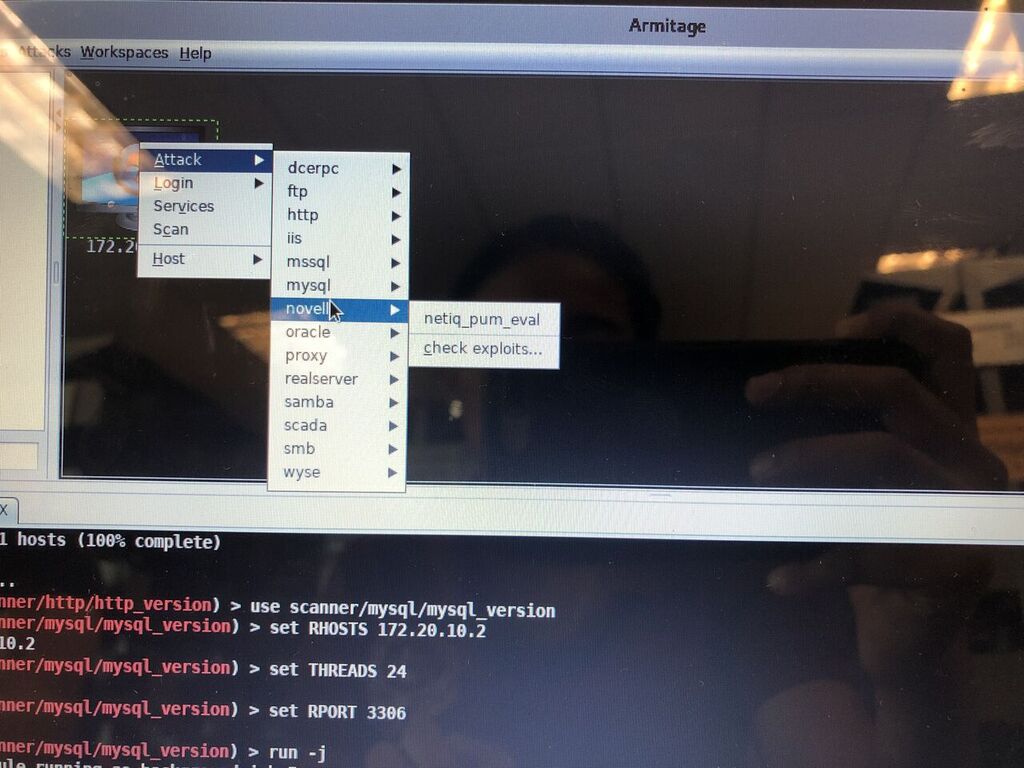


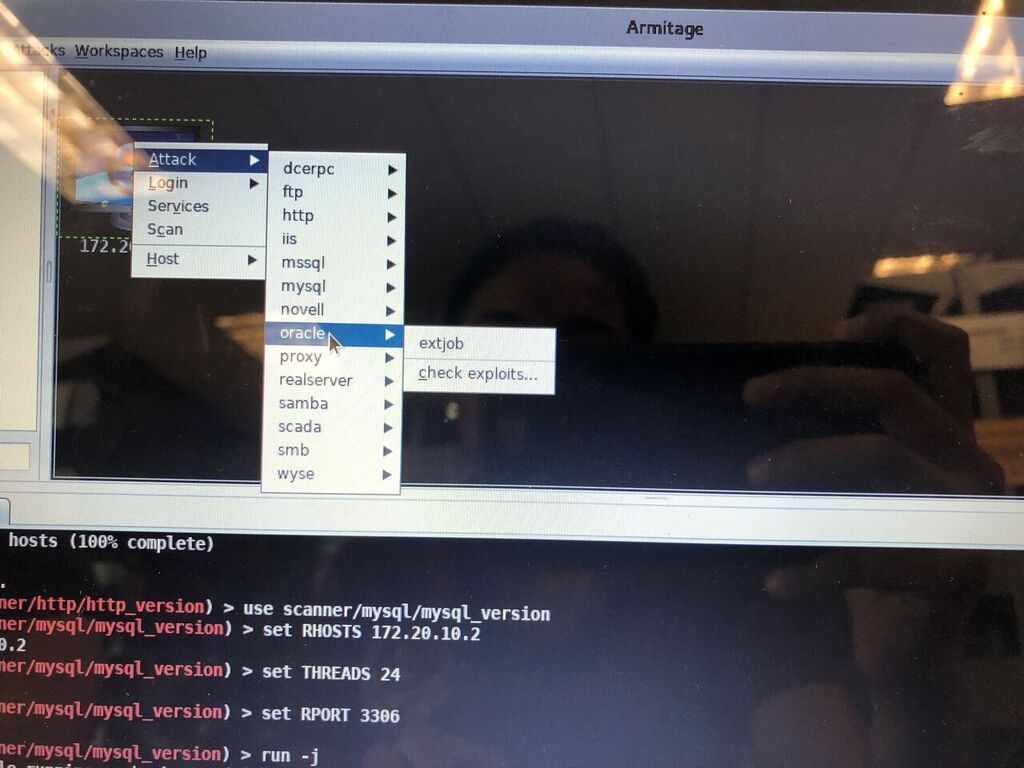


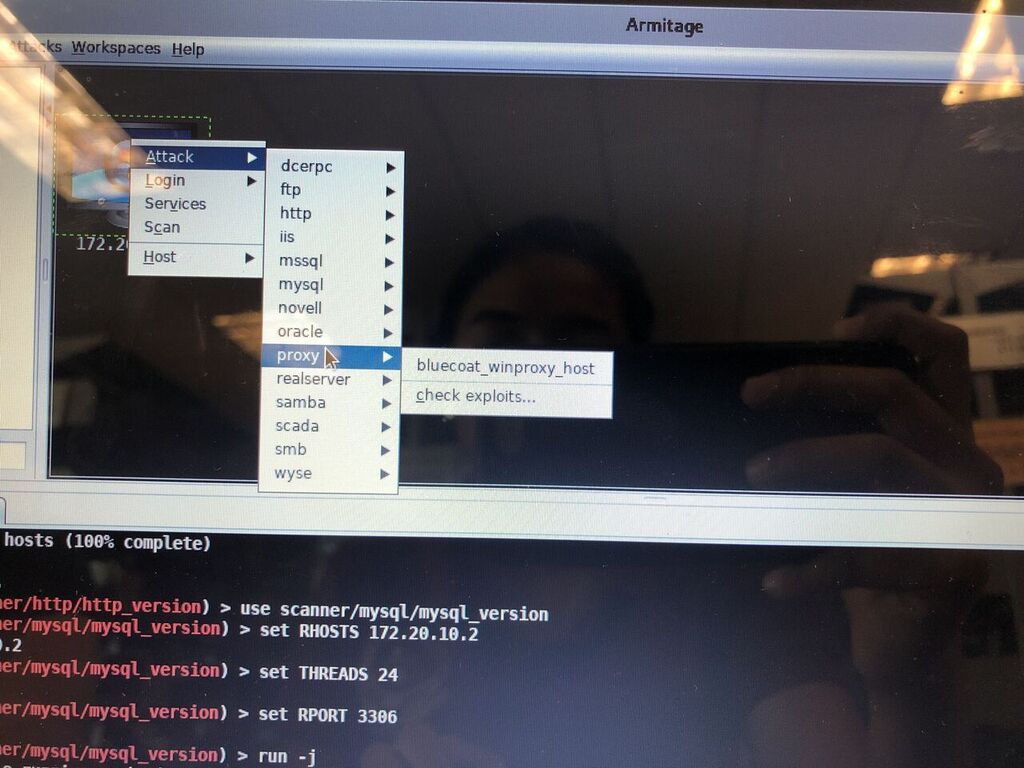


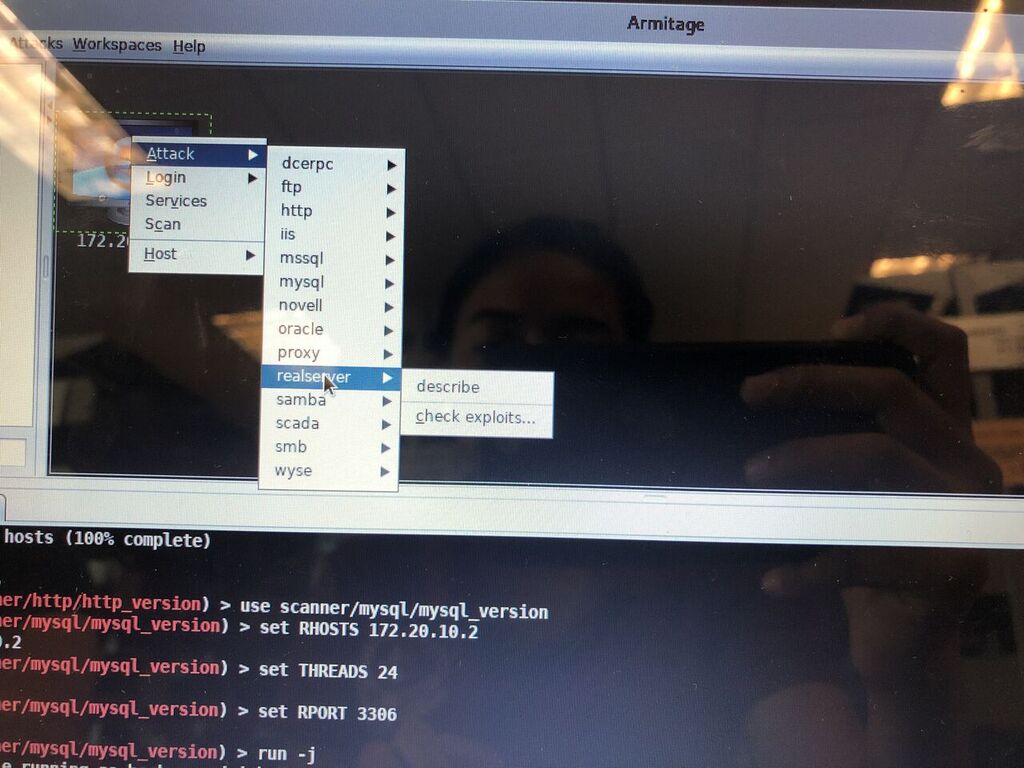


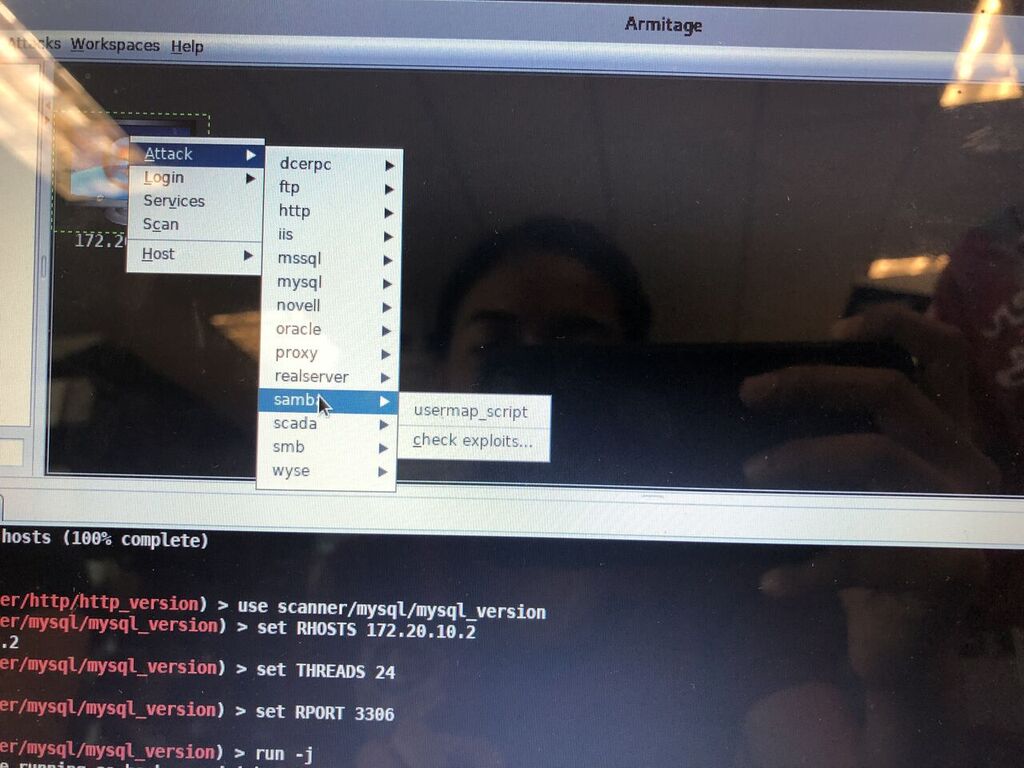


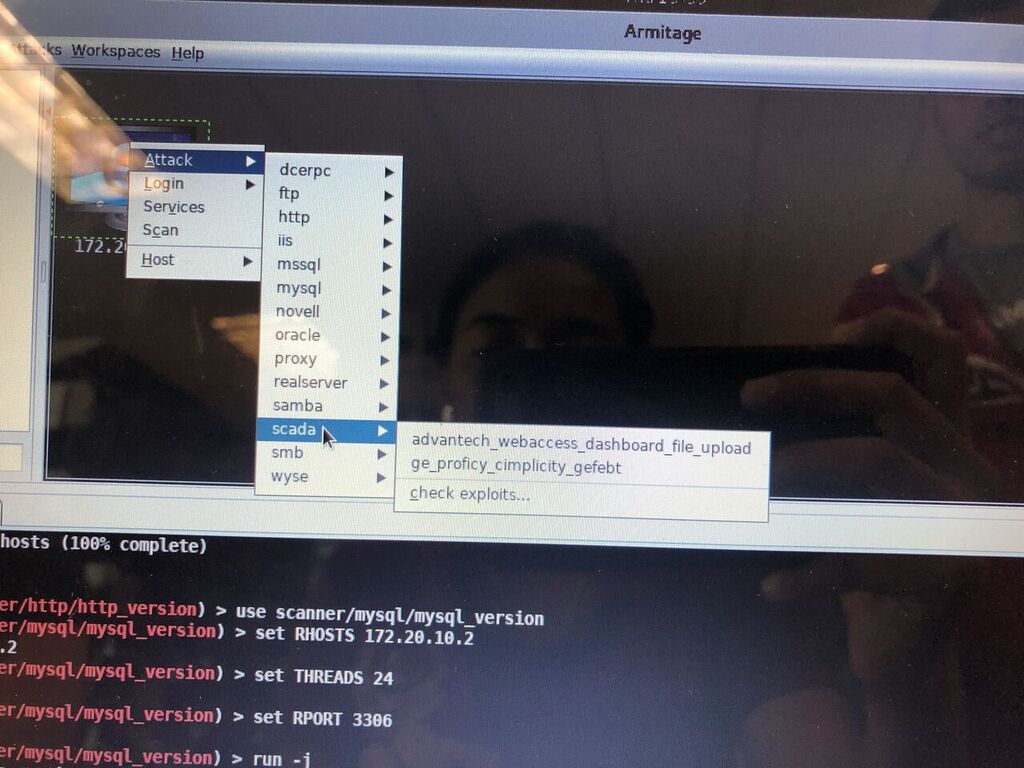


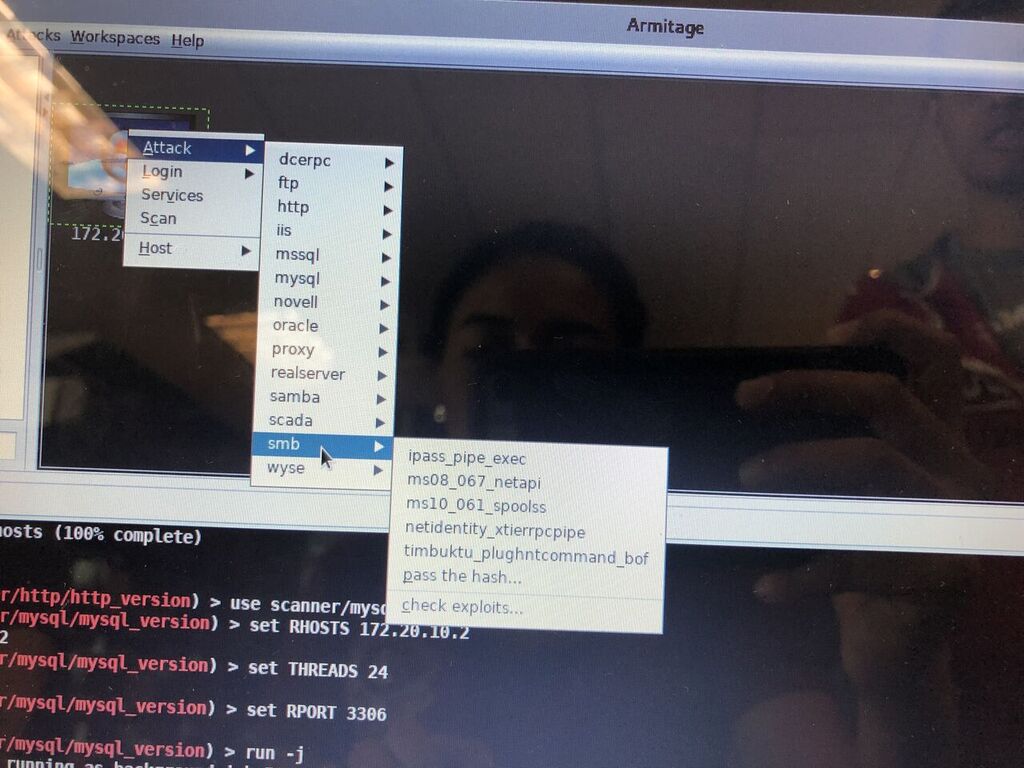


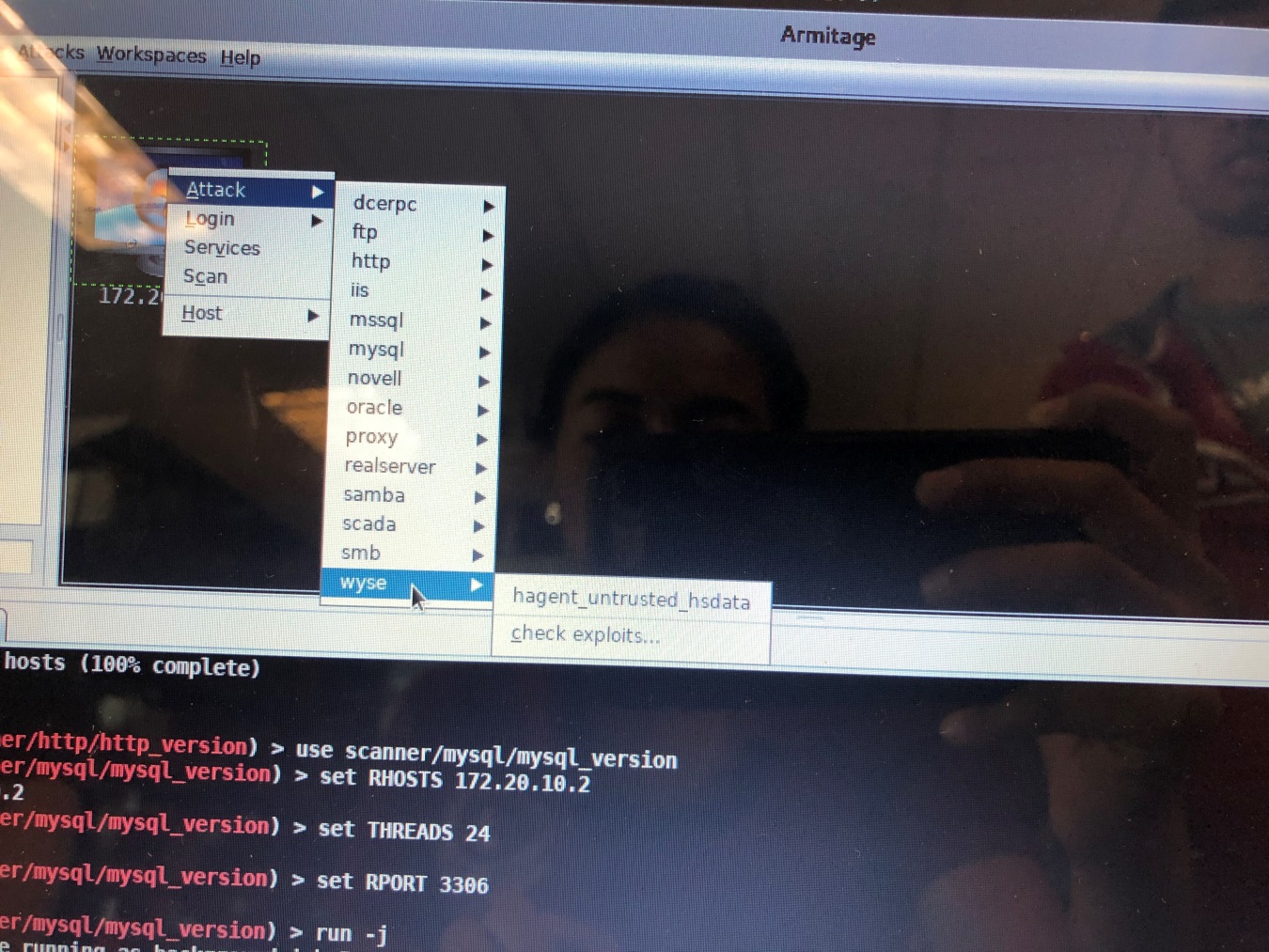






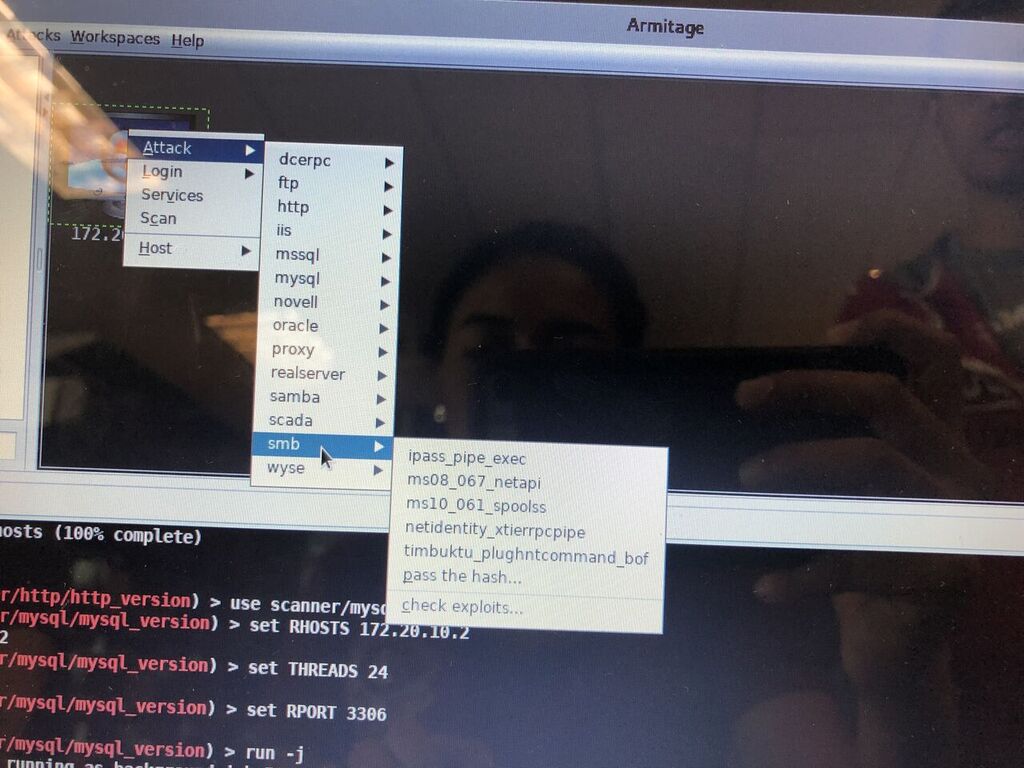




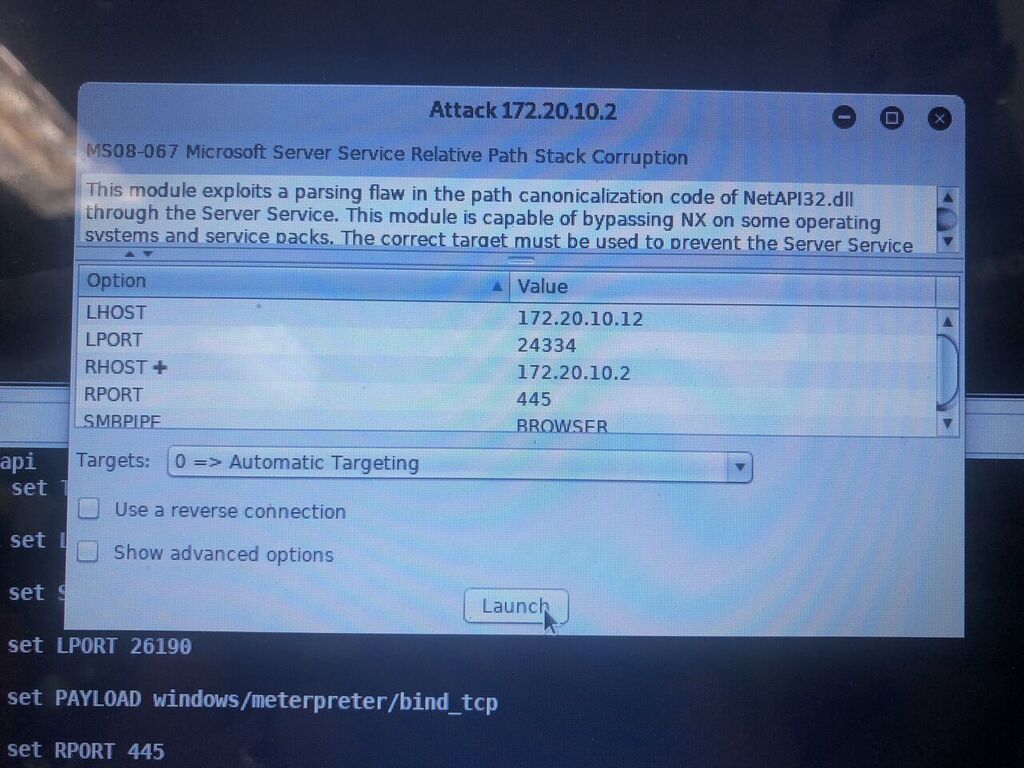


Se puede observar que aparecen más puertos abiertos que en nmap, se pueden hacer los ataques como ya se mencionó de forma automatizada, en este caso se hizo un ejemplo con el exploit netapi, dicho exploit permite controlar la máquina de manera remota entrando al Shell.

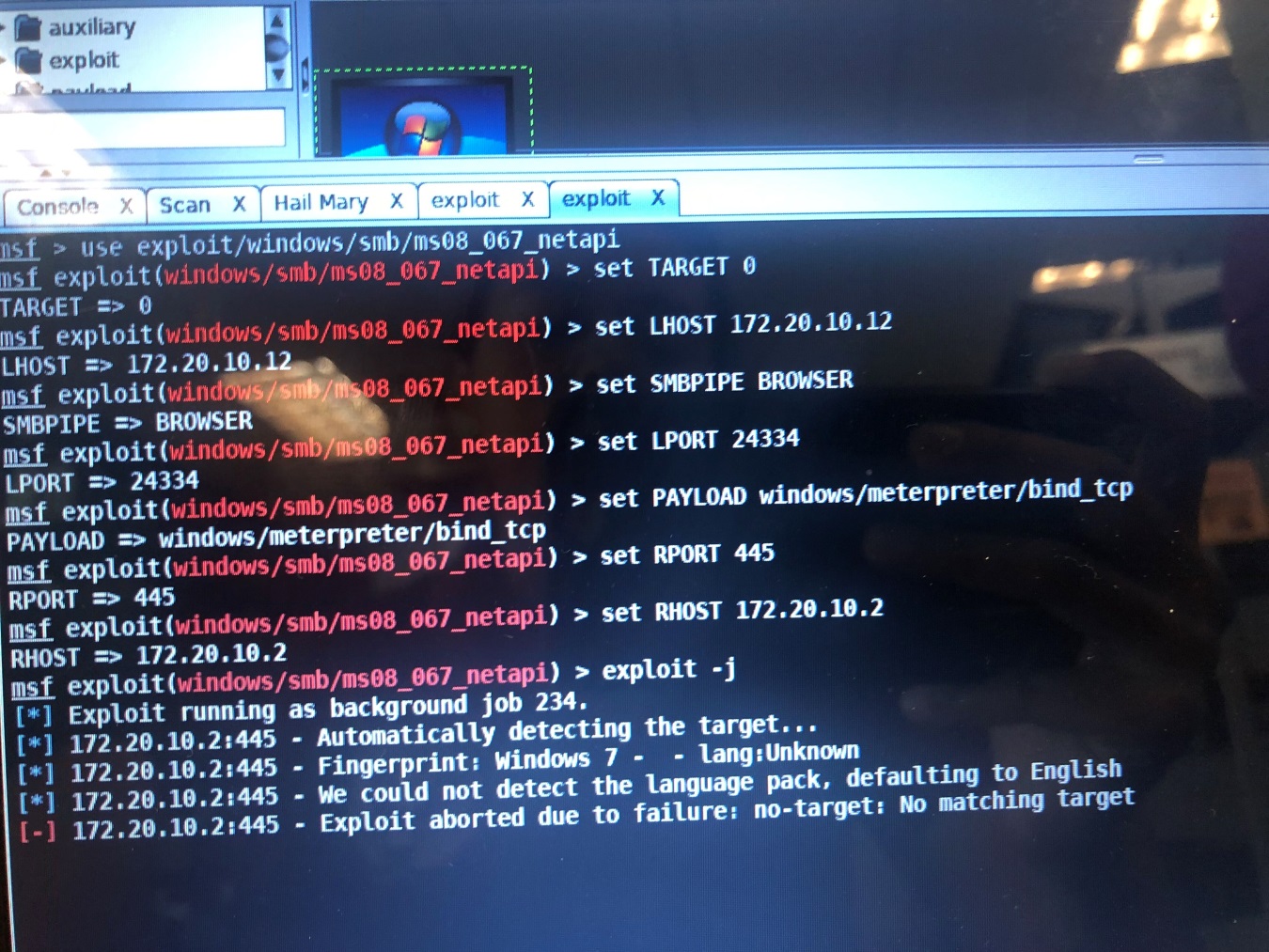
* Se da clic en smb, luego se selecciona MS08\_067\_netapi.



* Después aparece esta ventana donde nos indica algunos valores requeridos, si son correctos se da clic en launch, para comenzar a ejecutarlo.



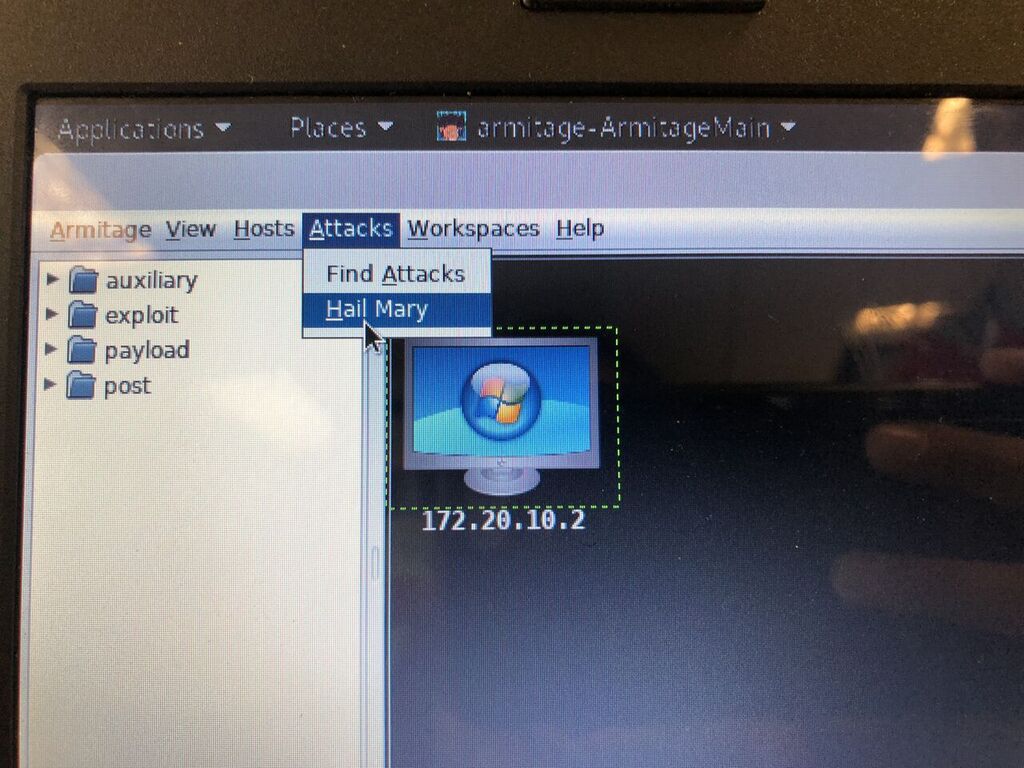
* En la parte inferior (consola) se comienza a realizar el ataque de manera automática.



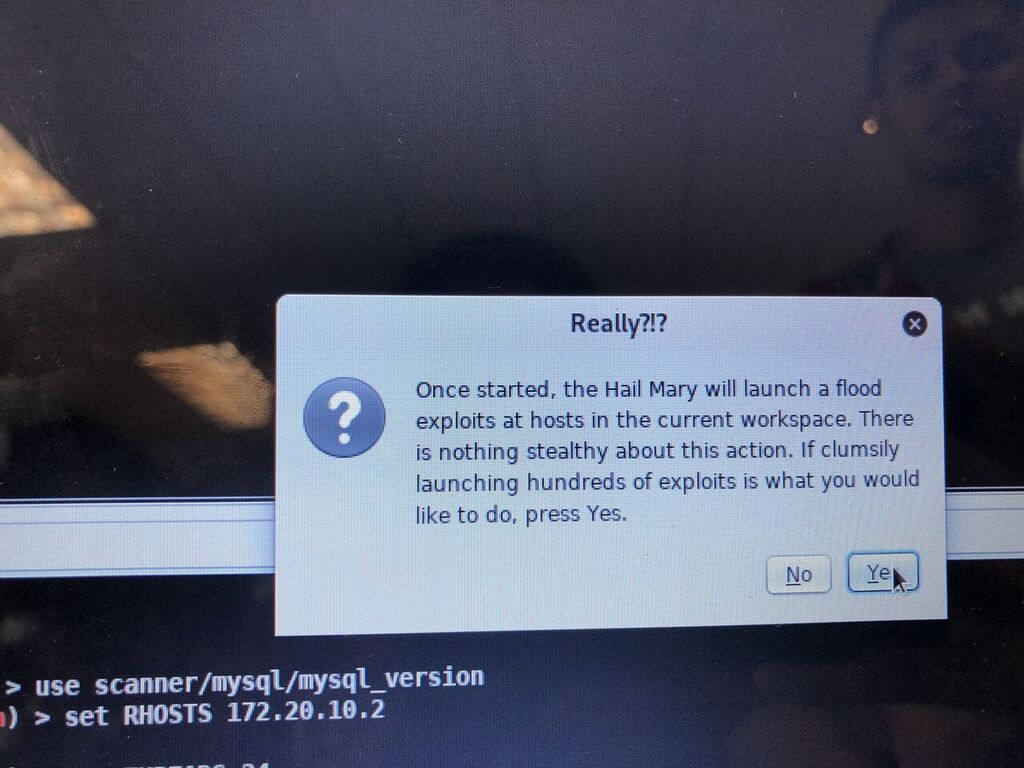
En esta pantalla podemos observar que el exploit no se pudo realizar correctamente, entonces la maquina no es vulnerable para dicho exploit.

1. Para realizar todos los exploits automáticamente y de una manera más rápida, se hace uso de una función llamada hail mary, dicha función realiza los exploits de forma automática, hasta encontrar alguno que si funcione y si alguno funciona nos muestra si se estableció una sesión.

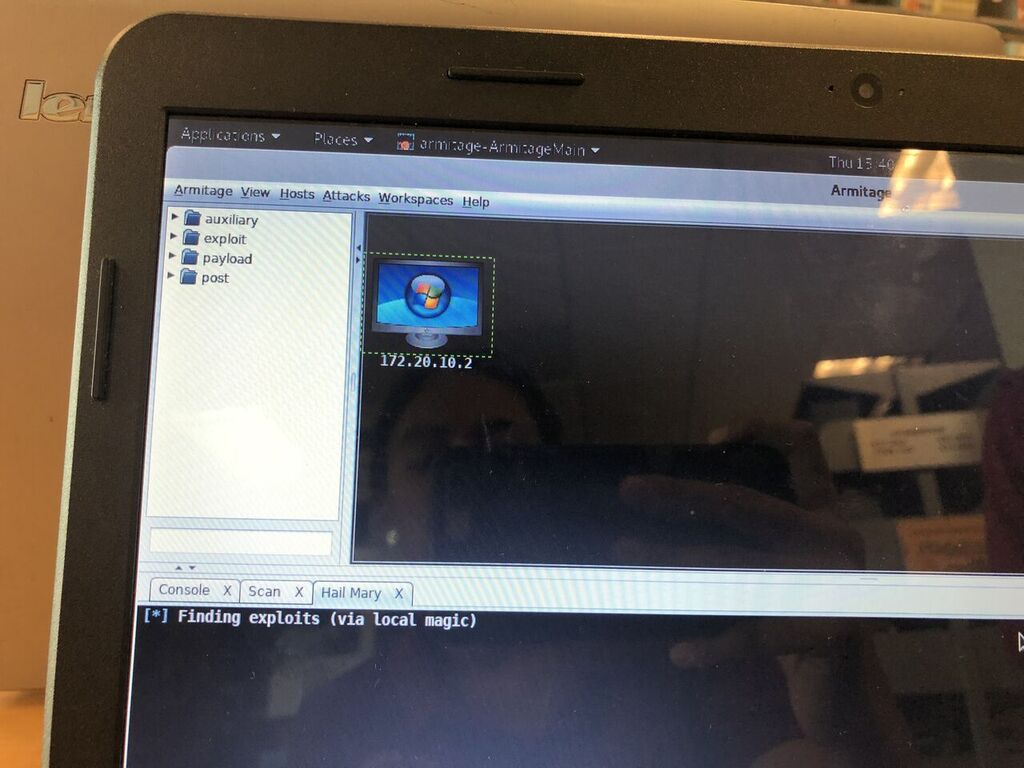
* Se da clic en el menú superior en la opción Attacks.

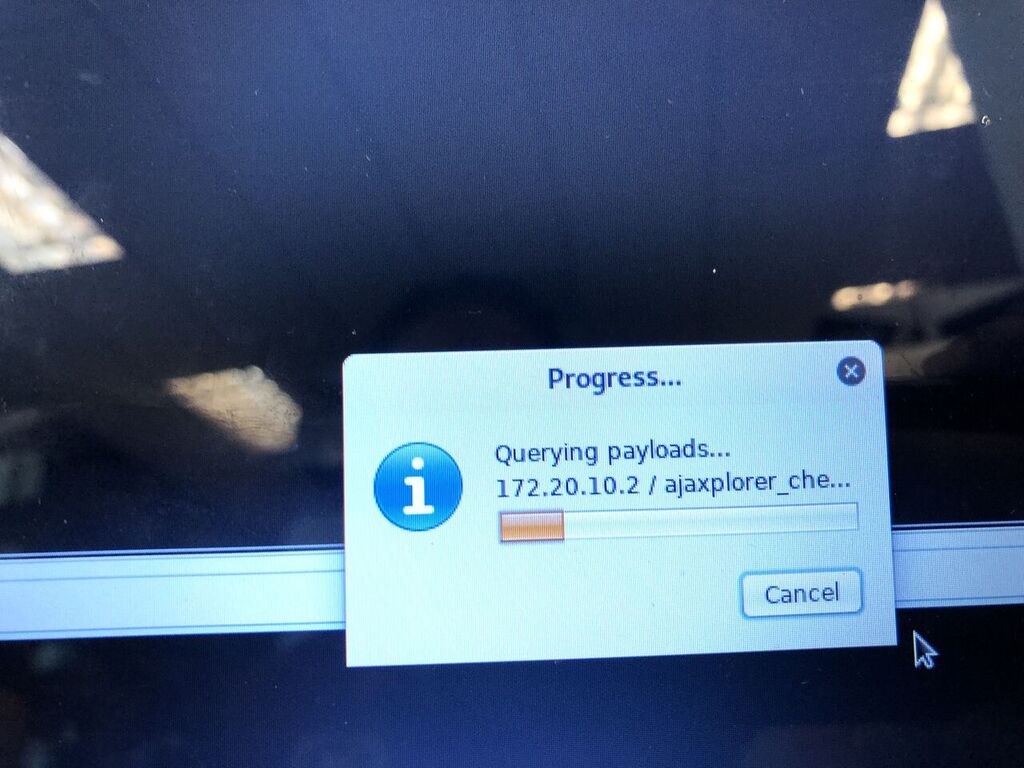


* Nos aparece el siguiente mensaje, damos clic en yes, nos dice que una vez iniciado el hailmary se van a ejecutar exploits automáticamente.

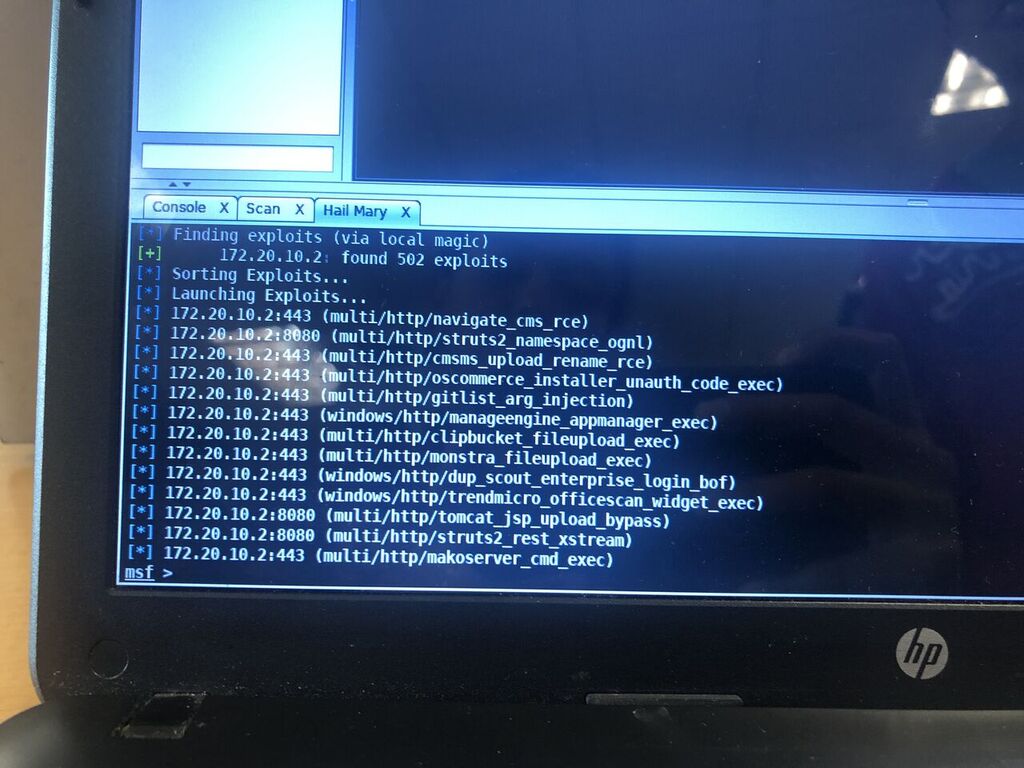


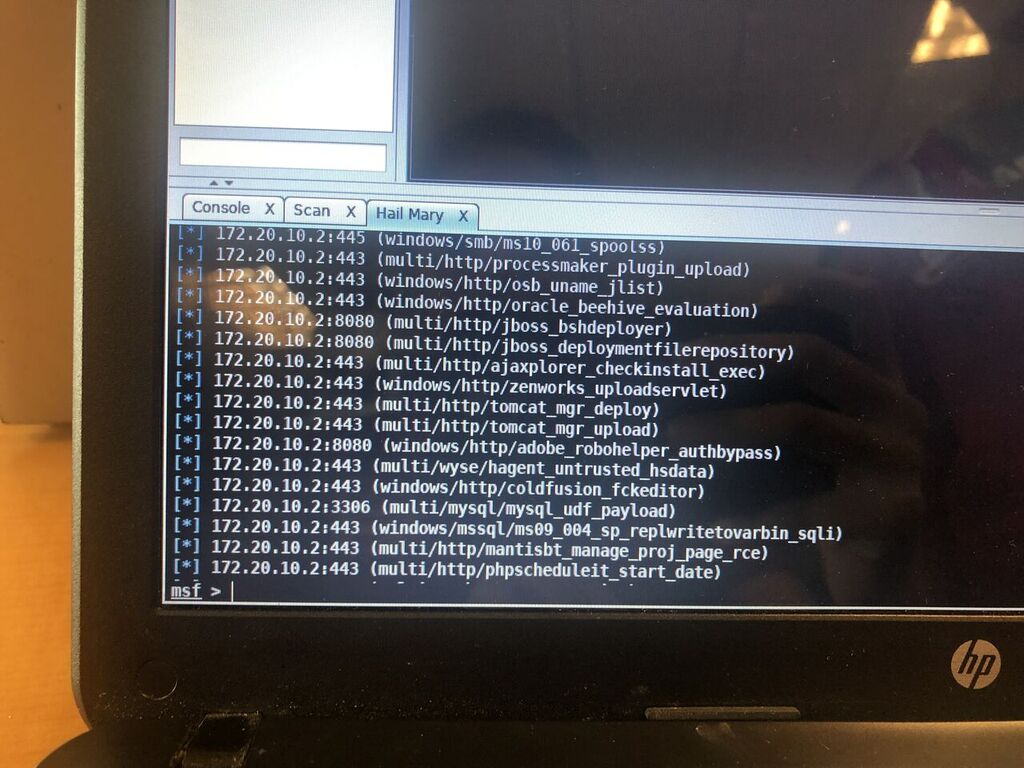
* Aquí se puede observar que ya inicio con el hail mary.





* Se comienzan a ejecutar los exploits.

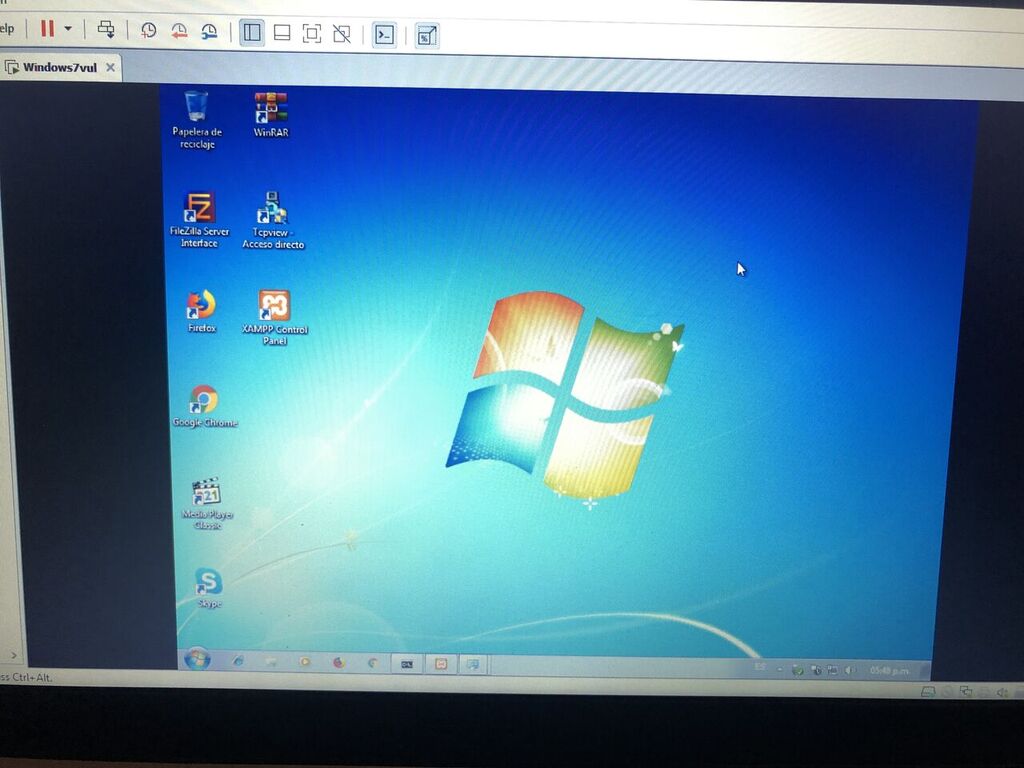




1. En este caso no se pudo establecer ninguna sesión por lo que se deduce que la máquina virtual que se creo, no es vulnerable o está protegida en algún aspecto aun.



1. Podemos comprobar visitando la máquina virtual y ver que no tiene ningún cambio en ella.



**¿Cómo protegerse?**

**Conclusiones**

Crear una máquina virtual que cuente con vulnerabilidades o que en otras palabras sea vulnerable no es un trabajo fácil, como la mayoría de las personas piensan, al contrario, se debe pensar en todos los servicios y las posibles vulnerabilidades que deben tener los mismos, así como desactivar actualizaciones o buscar la manera en otras palabras de que sea fácil de entrar en ella haciendo uso de diferentes exploits.

En esta práctica se pudo poner en marcha muchos aspectos y aplicar muchos conocimientos que ya se han adquirido a lo largo del semestre, pero como siempre, nunca está de más ampliar dichos conocimientos. Esto se debe a que la práctica consistía en aplicar en su conjunto, aquellos pasos que hemos realizado por separado en otras prácticas anteriores, por ejemplo: el buscar puertos abiertos en un equipo, identificar exploits y tratar de aplicarlos para ver si funcionaban dentro de la máquina.

Para protegerse de todos los exploits que se encuentran disponibles gracias a la herramienta armitage existen infinidad de recomendaciones y herramientas, pero sobre todo es recomendado mantener actualizado el sistema y toda nuestra computadora. Cuando se trata de buscar vulnerabilidades, la mayoría de las ocasiones el resultado es exitoso, debido a que muchos usuarios no cuentan con la precaución de proteger su equipo, pero en este caso fue un poco más complicado debido a que se tuvo que desarrollar la maquina vulnerable con la que se quería trabajar.

Es importante mantenerse informado sobre todos los ataques que van saliendo día con día en la red y sobre qué tan maliciosos podrían llegar a ser para nuestro equipo, sobre todo es importante buscar información si en algún momento nuestro equipo llega a fallar ,por otro lado si se quieren conocer las vulnerabilidades del equipo donde se está trabajando solo son necesarias herramientas sencillas como armitage, con las que cuenta kali, en las que con solo unos clicks se puede saber si nuestro equipo tiene exploits que están funcionando dentro de él y poder tomar algunas precauciones para protegerse más específicamente.

Por ultimo como conclusión personal, me impresiona la idea de poder realizar una práctica un poco más real aplicada al ambiente en la actualidad, donde desde cero se puede buscar y comprobar si un equipo tiene vulnerabilidades y sobre todo lo fácil que es en algunas ocasiones lograr tomar el control de otro equipo, inclusive sin tener que introducir usuarios o contraseñas.

**Bibliografía**

Dragonjar.org(Octubre 17,2018).Manual de armitage. Recuperado el 11 de mayo del 2019 de: <https://www.dragonjar.org/manual-de-armitage-en-espanol.xhtml>

Hacking-etico.com(Octubre 21,2013). Armitage. Recuperado el 11 de mayo del 2019 de: <https://hacking-etico.com/2013/10/21/armitage/>

Puertos

Internetya.co(Abril 16,2017).Que es FTP. Recuperado el 11 de mayo del 2019 de: <https://www.internetya.co/que-es-el-servicio-ftp-file-transfer-protocol/>

Developer.mozilla.org(Junio 6,2014). HTTP. Recuperado el 11 de mayo del 2019 de: <https://developer.mozilla.org/es/docs/Web/HTTP>

Wikipedia.org(Mayo 2,2019).Microsoft\_RPC. Recuperado el 11 de mayo del 2019 de: <https://en.wikipedia.org/wiki/Microsoft_RPC>

Wikipedia.org(Enero 29,2019).NetBIOS. Recuperado el 11 de mayo del 2019 de: <https://es.wikipedia.org/wiki/NetBIOS>

Tecnosinergia.zendesk.com(S.F). RTSP. Recuperado el 11 de mayo del 2019 de: <https://tecnosinergia.zendesk.com/hc/es/community/posts/115000357991-Protocolo-RTSP-Para-que-sirve->

Community.norton.com(Septiembre 10,2015).ICSLAP. Recuperado el 11 de mayo del 2019 de: <https://community.norton.com/en/forums/icslap-dangerous>

Docs.microsoft.com(S.F).wsdapi. Recuperado el 11 de mayo del 2019 de: <https://docs.microsoft.com/en-us/windows/desktop/wsdapi/overview-of-the-wsdapi-interfaces>

Support.google.com(Mayo 6,2015). Webmaster. Recuperado el 11 de mayo del 2019 de: <https://support.google.com/webmasters/answer/6073543?hl=es>

Searchdatecenter.techtarget.com(Agosto 2,2018).MYSQL.Recuperado el 11 de mayo del 2019 de: <https://searchdatacenter.techtarget.com/es/definicion/MySQL>

Searchdatacenter.techtarget.com(Mayo 7,2019).PROXY. Recuperado el 11 de mayo del 2019 de: <https://searchdatacenter.techtarget.com/es/definicion/Servidor-Proxy>

Wikipedia.org(Junio 6,2018).Apache\_JServ\_Protocol. Recuperado el 11 de mayo del 2019 de: <https://es.wikipedia.org/wiki/Apache_JServ_Protocol>

Kb.iweb.com(S.F).Windows SMB y NetBios. Recuperado el 11 de mayo del 2019 de: <https://kb.iweb.com/hc/es/articles/115000274491-Proteger-los-servicios-Windows-SMB-y-NetBios-NetBT>