# Descripción de escenarios

## Escenario de Ettercap

En la implementación de la herramienta se utilizaron dos computadoras una virtual de Kali linux y una física de Windows 8.1. Donde el objetivo final era capturar las credenciales de la maquina victima Windows que viajaran por el método POST en las paginas que trabajaran por el protocolo http. Las dos máquinas estarán en la misma red y compartirán el servicio de internet por conexión puente de la maquina física a la virtual.

## Escenario de Arpspoof

En la implementación de la herramienta se utilizaron dos computadoras una virtual de Kali linux y una física de Windows 8.1. Donde el objetivo final era capturar las credenciales de la maquina victima Windows que viajaran por el método POST en las páginas que trabajaran por el protocolo https. Las dos máquinas estarán en la misma red y compartirán el servicio de internet por conexión puente de la maquina física a la virtual.

## Escenario de Evil Foca

En la implementación de la herramienta se utilizaron dos computadoras una virtual de Kali linux y una física de Windows 8.1. Donde el objetivo final era capturar las credenciales de la maquina victima Kali Linux que viajaran por el método POST en las páginas que trabajaran por el protocolo http. Las dos máquinas estarán en la misma red y compartirán el servicio de internet por conexión puente de la maquina física a la virtual.

## Escenario de Bettercap

En la implementación de la herramienta se utilizaron dos computadoras una virtual de Kali linux y una física de Windows 8.1. Donde el objetivo final era capturar las credenciales de la maquina victima Windows que viajaran por el método POST en las páginas que trabajaran por el protocolo http. Las dos máquinas estarán en la misma red y compartirán el servicio de internet por conexión puente de la maquina física a la virtual.

# Tabla MITM

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Herramienta | Ventajas | Desventajas | Diferencias | Vulnerabilidades Detectadas |
| MITM-ETTERCAP  A: KALI LINUX  V: WINDOWS 8.1  (Linux1Mtm) | -Invisible para la victima  -Funciona con http  -Muestra las credenciales de manera organizada  -Muestra las MAC y IPv4 conectadas a la red  -Capturas credenciales | -No funciona con https  -No muestra el tráfico por la web de la victima  -No funciona con todos los navegadores  -Inconsistente en la captura de credenciales sucesivas | Necesita modificar las tablas ARP por medio de ARP poisong  Funciona con el navegador Google Chrore  No funciona con el navegador Brave | -Cambio de direccionamiento de paquetes  -Cambio de tablas ARP  -Escaneo de red  -Captura de información que viaja por el método POST |
| MINT-ARPSPOOF  A: KALI LINUX  V: WINDOWS 8.1  (Linux2Mtm) | -Funciona para http y https  -Capturas credenciales  -Deniega servicio de internet  -Muestra el tráfico por la web de la victima  -Consistente en la captura de credenciales sucesivas | -Visible para la victima  -Necesita herramientas complementarias  -NO muestra las MAC y IPv4 conectadas a la red  -Necesita configuraciones complementarias  -NO muestra las MAC y IPv4 conectadas a la red  -No muestra las credenciales de manera organizada  -No funciona con todos los navegadores | Necesita Habilitar reenvió de paquetes  Necesita cambiar la fecha con delorean.py  Necesita cambiar tablas de direccionamiento de paquetes  Necesita  monitorear puerto 8080 con Sslstrip.py  Necesita visualizar cambios con Tail -f al Sslstrip.log  Necesita envenenar Arp -a (Tablas Arp)  Necesita modificar las Iptables -t nat -L  (tablas de nateo) con  80->8080 tcp  443->8080 tcp  123 ->123 udp | -Modificación de fecha  -Denegación de servicio de navegación web  -Cambio de protocolos con los que trabajo las paginas web  -Cambio de direccionamiento de paquetes  -Cambio de tablas ARP  -Escaneo de red  -Captura de información sensible de las paginas  -Captura de información que viaja por el método POST |
| MINT- EVIL FOCA  A: WINDOWS 8.1  V: KALI LINUX  (Windows1Mtm) | -Invisible para la victima  -Funciona con http  -Consistente en la captura de credenciales sucesivas  -No visible para la victima  -Muestra las credenciales de manera organizada  -Muestra las MAC y IPv4 conectadas a la red  -Muestra el tráfico por la web de la victima  -Muestra información extra de la paginas en la navegación  -Muestra la Ipv4, Ipv6 y el tipo de sistema conectado a la red | -No funciona con https  -Necesita herramientas complementarias  -No capturas credenciales directamente  -Necesita herramientas complementarias | Necesita filtrar por Request method POST para filtrar credenciales  Necesita visualizar tráfico con wireshark | -Captura de información sensible de las paginas  -Cambio de direccionamiento de paquetes  -Cambio de tablas ARP  -Escaneo de red  -Captura de información que viaja por el método POST |
| MINT- BETTERCAP  A: KALI LINUX  V: WINDOWS 8.1  (Windows2Mtm) | -Invisible para la victima  -Funciona con http  -Ataca toda la red  -Permite capturar un protocolo en especifico  No necesita herramientas complementarias  -Muestra la Ipv4, Ipv6 y el tipo de sistema conectado a la red  -Muestra información extra de la paginas en la navegación  -Consistente en la captura de credenciales sucesivas  -Muestra el tráfico por la web de la victima | -No funciona con https  -Necesita módulos internos extra. | -Detecta dispositivos inalámbricos en la red  -Muestra estructurada de información captada en las paginas  -Muestra información del servidor de las paginas http  -Funciona con navegadores actuales como Brave | -Captura de información sensible de las paginas  -Cambio de direccionamiento de paquetes  -Cambio de tablas ARP  -Escaneo de red  -Captura de información que viaja por el método POST |

# Tablas Keylogger

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Herramienta | Descripción | Ventajas | Desventajas | Vulnerabilidades Detectadas |
| Spykey  (KALI LINUX) | Se realizo en Kali Linux un “virus” en el cual se envía el virus a la victima por ejemplo a otro sistema operativo como Windows y se procede a esperar que la victima lo ejecute para así realizar el ataque Keylogger vía remota | -Es remoto y no local  -Capta los datos sin que la víctima se dé cuenta  -Fácil de realizar | -No es 100% efectivo para Windows 10 debido a su seguridad | -Como el ataque se realizó para Windows 10 no se encontraron vulnerabilidades para este sistema operativo |
| Web Check  (WINDOWS10) | Se realizo la instalación de la herramienta para Windows la cual se ejecutó en el equipo y atreves de las opciones se inicio la captura de datos tipiados por la victima pudiendo obtener la contraseña de facebook | -No es Visible para la victima | -No es remoto  -No se puede enviar al correo los datos capturados  -Hay que pagar para poderlo usar | - Se encontraron vulnerabilidades para este sistema operativo (Windows10) en la seguridad por dejar instalar software como este que es malicioso |
| Free Keylogger  FLK  (WINDOWS10) | Se realizo la instalación de la herramienta para Windows 10 la cual se ejecutó en el equipo y atreves de las opciones se inició la captura de datos tipiados por la victima pudiendo obtener la contraseña del correo | -Buena interfaz de usuario.  -No es Visible para la victima. | -No es remoto.  -No se puede enviar al correo los datos capturados.  -Hay que pagar para poderlo usar otras opciones. | -Se encontraron vulnerabilidades para este sistema operativo (Windows10) en la seguridad por dejar instalar software como este que es malicioso . |
| Free Keylogger  (WINDOWS10) | Se realizo la instalación de la herramienta para Windows 10 la cual se ejecutó en el equipo y atreves de las opciones se inició la captura de datos tipiados por la victima pudiendo obtener la contraseña del correo | -Seguro al momento de abrir porque pide contraseña  -Se pueden enviar al correo los datos captados | -No es remoto.  -Hay que pagar para poderlo usar otras opciones. | -Captura de información sensible de las paginas  -Cambio de direccionamiento de paquetes  -Cambio de tablas ARP  -Escaneo de red  -Captura de información que viaja por el método POST |