**SOLUCIONARIO CERTIFIED OFFENSIVE AND DEFENSIVE SECURITY PROFESSIONAL LEVEL EXTREME**

**Autor:**

**ULTRAMAGNU**

**Tabla de Contenido**

**INTRODUCCION**

Este Solucionario se realiza con el Material suministrado por el docente el cual consta de 20 Retos Informáticos y las Herramientas Para Dar Solución a cada uno de los mismos para así lograr la Certificación CODSP Nivel Extremo

**Reto Informático N.º 1**

Enunciado: Se tiene el siguiente servidor web. Este sería un buen lugar para obtener la bandera numero 1:

Ip server web

http://52.207.240.228/

**R/** para dar Solución a este Reto Informático debemos usar Kali Linux y dentro su Herramienta Dirb

Texto

Descripción generada automáticamente

Luego de esto abrimos esta dirección en el Buscador <http://52.207.240.228/webadmin/>

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Abrimos el Archivo crackeame.txt y ahí encontramos el Siguiente HASH

E1A04996A37395FCD9C7B7C5286270F7

Debemos de saber qué tipo de HAHS es y para ello usamos la Herramienta “hash-Identifier “Ubicada en Kali Linux

Ya sabiendo que el Hash encontrado es un MD5, usamos la página Crackstation.com y ahí colocamos el hash a desencriptar

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media

Entonces el **CTF= liverpool123**

Reto Informático N.º 2

se tiene el siguiente servidor WEB Y URL

http://52.207.240.228/

Pista: Este sería un buen lugar para obtener la bandera numero 2

-Flag final: El flag final de este reto es obtener y romper un hash

**R/** entonces según esto el hash a romper se encuentra dentro del código fuente de LA URL mencionada en el reto

Interfaz de usuario gráfica

Descripción generada automáticamente

Luego de esto miramos el código fuente donde en los comentario encontramos un HASH

Texto

Descripción generada automáticamente

Lel HAHS a Romper es el Siguiente:

d3bf679621db5a9b7bc6774af584082065dd9c7f22af5f1edd126c4bb70b5b94

al usar la Herramienta “hash-Identifier “donde nos Revela que es un SHA-256 el cual usaremos un archivo en Kali Linux para guardarlo y usando “Hashcat”

Texto

Descripción generada automáticamente

Ya Guardado usaremos la Herramienta anteriormente mencionada Usamos Hashcat 1400 debido a que es un sha-256 y al realizar un ataque por Diccionario es -a 0 y le damos la ruta donde tenemos el Diccionario Rockyou.txt

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Entonces el **CTF= gunsandroses**

Reto Informático N.º 3

se tiene la siguiente url

http://52.207.240.228/steganography/

--Pista: ¡¡Tus conocimientos en esteganografía y Password cracking te vendrían bien!!

--Flag final: El flag final de este reto es des ocultar un archivo, y crackear un Password

**R/** En la siguiente Imagen ya podemos ver que nos esta guiando que debemos hacer

Código QR

Descripción generada automáticamente

Por que No esta señalando que dentro de la Imagen hay alguna Información, pero antes debemos desencriptar el código de abajo que es en código base64 que seria Nuestra llave para poder abrir lo que contiene la Imagen, para ello debemos de descargar la Imagen y Guardarla e instalar el programa llamado “camuflaje”. Luego colocamos el cursor con botón derecho en las opciones aparece la de “Uncamouflaje” y aparece la Siguiente Ventana

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

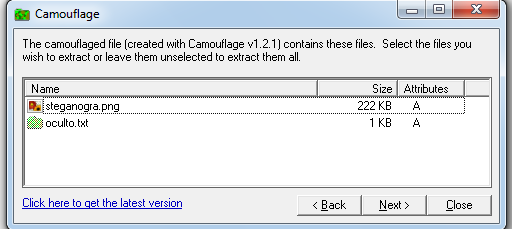
En este campo escribimos el resultado de bXJyb2JvdA==

Desencriptada y para ello vamos al siguiente página <https://www.base64decode.org/>

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Justo en esta pagina escribimos la Palabra encriptada y luego le optáramos al botón “DECODE”, dándonos como respuesta “mrrobot” justo esta la escribimos en la ventade de Camuflaje



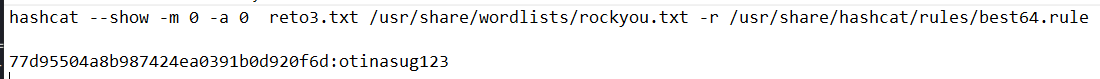
Y seleccionamos el Archivo oculto.txt donde encontraremos el Siguientes Hash

77D95504A8B987424EA0391B0D920F6D

Usando la herramienta “hash-Identifier “Ubicada en Kali Linux logramos demostrar que es un Hash MD5, luego lo guaramos en un Archivo dentro de kali para luego romperlo con Hashcat

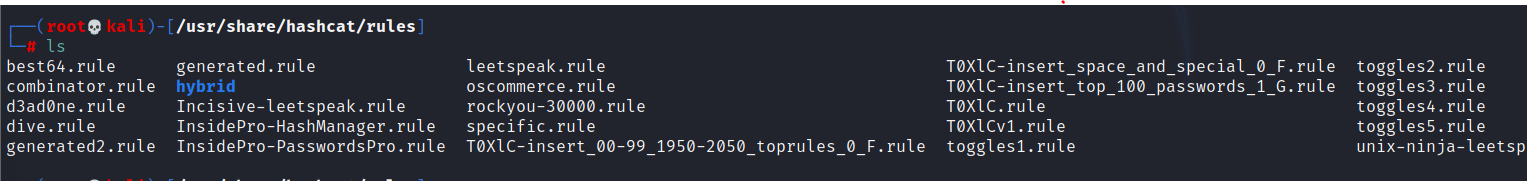
Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente



Por que Vemos esto. El –show es Debido a que este ejercicio lo hice Anteriormente

NOTA para solucionar este HASH debemos utilizar reglas y para eso las llamamos con “-r” y ya buscamos dentro de su directorio el cual es “cd /usr/share/hashcat/rules/” y ahí veríamos lo siguiente



Entonces el **CTF=otinasug123**

Reto Informático N.º 4

Se tienen los hashes

89337CF7FAFB6110A2C72E5AA711639E5F3F37E2

16BD2368D9E7789B28BEB978D394B4EED8DE8641

F0F84313C7ADA13F4DDA289DDC683EEF41E83185

E9045AE52E2CA70232C5678F506CA3ECE9C7BAA0

54D5F411F4ADA02512E69B81CC68EF28F9D83940

9D0C2FC4A62F8846433799533720C5C43B0A0414

--Pista: ¡¡¡Tus conocimientos en Password cracking con reglas seria genial!!!

--Flag final: El flag final de este reto son 6 Password crackeados

**R/** Primero verificamos con “hash-Identifier “que clase de HAHSES son SHA-1Luego de ello guardamos los Hashes dentro de un Archivo para luego romperlos debido a que todos son sha1

Texto

Descripción generada automáticamente

Luego escribimos hashcat -m 100 reto4.txt /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule

Se le da 100 debido a que es un sha1 el Nombre del Archivo que en este caso es reto4.txt y la Ubicación del Diccionario “Rockyou” y -r que es la Regla en este caso la regla ”best64.rule” y su ubicación como mencionamos en el ejercicio Anterior

hashcat -m 100 reto4.txt /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule

hashcat (v6.1.1) Stirling...

OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL\_DEBUG) - Platform #1 [The pocl Project]

=============================================================================================================================

\* Device #1: pthread-Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz, 1417/1481 MB (512 MB allocatable), 4MCU

Minimum password length supported by kernel: 0

Maximum password length supported by kernel: 256

INFO: ¡All hashes found in potfile! Use --show to display them.

Started: Fri Feb 25 19:29:00 2022

Stopped: Fri Feb 25 19:29:00 2022

NOTA: cuando Aparece este mensaje es por que ya Realizo la Consulta Anteriormente y por eso se usa el siguiente código

hashcat --show -m 100 reto4.txt /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule

89337cf7fafb6110a2c72e5aa711639e5f3f37e2: ecuaestilolatino

16bd2368d9e7789b28beb978d394b4eed8de8641: Ecuaestilolatino

f0f84313c7ada13f4dda289ddc683eef41e83185: ECUAESTILOLATINO

e9045ae52e2ca70232c5678f506ca3ece9c7baa0: onitalolitseauce

54d5f411f4ada02512e69b81cc68ef28f9d83940: ecuaestilolatino99

9d0c2fc4a62f8846433799533720c5c43b0a0414:1ecuaestilolatino

Entonces **el CTF= ecuaestilolatino**

**Ecuaestilolatino**

**ECUAESTILOLATINO**

**onitalolitseauce**

**ecuaestilolatino99**

**ecuaestilolatino**

Reto Informático N.º 5

Se tiene el siguiente archivo reto5.cap, debes de extraer los usuarios y password de protocolos de red que no requieren autenticación.

--Pista: Tus conocimientos en análisis de tráfico de red y protocolos que no aplican cifrado te vendrían de mucha utilidad

--Flag final: El flag final es obtener un usuario y un password

**R/** primero tenemos que abrir el Archivo “.cap” en Kali Linux, debido que es un Archivo que necesita Wireshark

Captura de pantalla de un celular

Descripción generada automáticamente

Abrimos el Archivo Reto5.cap

Texto

Descripción generada automáticamente

Luego nos Va a Abrir la Traza de Red, y para segmentar la búsqueda en la parte superior le escribimos “http” esto con el fin de que nos ayude en la búsqueda del flag

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Vemos Algo que nos puede Ayudar que es el “GET” en este optáramos el Botón derecho del Mouse en la sección de “follow” y luego “TCP Steam” y esto Nos Generara una Nueva Ventana

Texto

Descripción generada automáticamente

Y ya podemos ver su Login y password

Entonces el **ctf=username=pablo**

**password=letmein**

Reto Informático N.º 6

Se tienen los siguientes hashes, hay que tratar de romperlos

61DA2C8562576685719DC8FA1DCA0E62

51BD4343528792C4BADF734D2119391B

2E3C180811AD56EAFA8FD69A6D8E30

CB6E05C7FCF884621951883C77005BD1

64D791D55E366146C39367631B5AF31B

343BFABA861604E67E4B70D0D36BD0F7

--Pista: Tus conocimientos en password cracking y técnicas de rainbow tables te serian de mucha ayuda

--Flag final: El flag final es obtener y-o reventar 6 hash

**R/** La Solución e la Pista debemos Usar Las Tablas Arcoíris; estos son NTHASH es decir que viene desde Windows Vista para la Autenticación Local y pues para hacer este solucionario mas corto usaremos un Recurso encontrado en Internet <https://www.objectif-securite.ch/ophcrack>

Ingresamos el Hash a Romper y opturamos el botón ir y Nos Genera su Respuesta

Interfaz de usuario gráfica

Descripción generada automáticamente

Otro Método es usar “OPHCRACK”; para usar este Programa Primero debemos de Modificar los Hashes otorgados en el punto 6, sino que los debemos convertir en NTHASH

Lo cual seria así

Imagen en blanco y negro

Descripción generada automáticamente con confianza baja

Y lo guardamos como SAMreto6

Luego de ello debemos de Cargar las tablas que vamos a usar las cuales se encuentran en

<https://ophcrack.sourceforge.io/tables.php> descargamos las tablas “vista Special” y “vista num”

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Luego las cargamos al sistema en la sección de “tables” y le damos “install”

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Y luego cargaremos el Archivo que vamos a usar “SAMreto6” en la sección “load” y luego “PWDUMP file” y lo seleccionas

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Y por último le damos Crackear

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Y esperamos a que nos arroje los resultados

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Y los cuales son coincidentes con la Primera parte de este punto, donde gracias a una aplicación web pudimos descifrar o romper estos hashes

Entonces el **CTF= B@T+3n**

**=$P1rm**

**AA99a2**

**236699852147**

**012345678900**

**11119999333**

Reto Informático N.º 7

Se tienen los siguientes 2 archivos:

Tramared.cap & dicc.txt

--Pista: Tus conocimientos en análisis de tráfico de red y password cracking seria ideales

--Flag final: El flag final es obtener un Password crackeado

**R/** Para dar solución a este Reto debemos usar los elementos dados por el profesor pero al ver que uno es un “.cap” podemos intuir que debemos usar “Wireshark” y por ende usar Kali Linux

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Luego de Abrir el Archivo “Tramared.cap” podemos Analizar que la captura de red es sobre una red Inalámbrica

Interfaz de usuario gráfica

Descripción generada automáticamente

Entonces al Ver que tenemos una trama de red Inalambrica y un diccionario vamos a usar

La opción “aircrack-ng” herramienta encontrada dentro de Kali Linux, en la cual consiste en el análisis de paquetes WEP Y WPA/WPA2; le damos la opción “--h” que es la Ayuda

Texto

Descripción generada automáticamente

Usamos el comando “-w” y luego usamos el Diccionario y por Ultimo la Trama de Red

Imagen que contiene Forma

Descripción generada automáticamente

Y lanzamos el ataque

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Entonces el **CTF= gaUoCe34t1**

Reto Informático N.º 8

Se tienen dos archivos: un archivo cifrado, y una llave criptográfica.

--Pista: ¡Tus conocimientos en criptografía te vendrían muy bien! Usa el password crackeado en el reto anterior como ayuda para descifrar el archivo.

--Flag final: El flag final de este reto es lograr descifrar un archivo y lograr ver su contenido

**R/** Para este Reto Vamos a Usar la Herramienta “openssl” y a su vez usaremos la llave del reto Anterior “**gaUoCe34t1**”; antes de ello pasamos los Archivos suministrados por el Profesor los cuales serían: “bandera8cifrada” y “privadacert” los copiamos y los pegamos en la Siguiente Ruta “C:\openssl\bin”

Interfaz de usuario gráfica, Aplicación, Tabla

Descripción generada automáticamente

Luego de ello Abrimos una Terminal CMD y ahí abres la ruta “C:\openssl\bin”

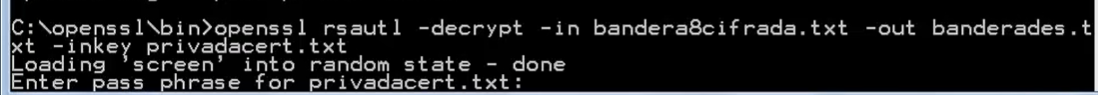
Texto

Descripción generada automáticamente

Luego de ello debemos de escribir en el CMD



Donde el comando “-descrypt” es para desencriptar un archivo que dentro de nuestro ejercicio es “bandera8cifrada.txt” y luego escribimos a donde queremos que nos guarde la solución o el ctf de nuestro ejercicio que dentro del mismo vamos a usar el siguiente “banderades.txt” y usamos el comando “-inkey” que es que nos va a solicitar una llave, em este caso una llave privada que es el archivo “privadacert.txt” y ahí cuando nos pida una clave usaremos la revelada en el ejercicio anterior “**gaUoCe34t1**”



Luego de ello vamos al Archivo “banderades.txt”

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Entonces el **CTF=MAZINGERLISTO2020**

Reto Informático N.º 9

Se tienen una copia (Backup) cifrada de un sistema firewall perimetral, debes de cargar al respectivo firewall

--Pista: ¡¡Tus conocimientos en firewall perimetrales como PFSENSE, serian ideales!!

--Flag final: El flag final de este reto es lograr obtener 7 hashes que están en las descripciones de las reglas LAN de la copia de seguridad que se debe de restaurar en un firewall pfsense nuevo (Instalado desde cero). La contraseña obtenida en el reto 8 te será de mucha utilidad para resolver este reto 9.

**R/** Primero para realizar este reto debemos instalar este firewall desde cero y para ello vamos a la pagina <https://www.pfsense.org/download/> y lo descargamos

Interfaz de usuario gráfica, Texto, Aplicación, Sitio web

Descripción generada automáticamente

Luego de ello lo Instalamos en su Software favorito de Virtualización y este archivo descargado lo subimos como una nueva maquina virtual y seguimos los pasos para su Instalación

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Luego agregamos otra tarjeta de red y ambas deben estar en modo NAT esto para que ambas se puedan comunicar

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Antes de cerrar esta ventana nos vamos hacia “Advanced” y ahí se nos abre una nueva ventana “Network Adapter Advanced Settings” y en la sección de “MAC Adress” le opturamos en el botón Genérate

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media

Esto se hace para verificar que tarjeta vamos a seleccionar a la WAN y a la LAN. Luego de Reiniciarse el mismo lanza esta venta y es para su Instalación

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Luego lo reiniciamos

Texto

Descripción generada automáticamente

Y le damos las Opciones para asignar tarjetas antes de realizar el reto

Le damos la opción 1

Texto

Descripción generada automáticamente

Asignándole a la LAN la em0 y a la WAN em1, le damos la opción 2 esto con el fin de configurar la “ip”

Texto

Descripción generada automáticamente

Luego ya escribimos nuestra dirección en el buscador del sistema operativo que estemos usando “https://192.168.64.48/”

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Le damos clic en “Avanzado” y luego nos tiene que aparecer el acceso del firewall le damos sus credenciales “Login=admin” y “password=pfsense”

Interfaz de usuario gráfica

Descripción generada automáticamente

Ahora procedemos a configurar el firewall. Lo llamamos “pfsenseReto9” y configuramos y le opturamos en el botón siguiente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Luego nos aparece una pantalla donde Ajustamos zona Horaria y luego le opturamos en el botón de Siguiente/Next, ahí quitamos el “Chuck” que aparecen a continuación

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

y luego el botón de Next

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Le escribimos cualquier clave simpe que queramos le opturamos en Next y esperamos para que haga una recarga

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Ahora en la siguiente ventana le damos “finalizar” y por fin dar Inicio al Reto como tal

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Nos dirigimos dentro del menú superior, Diagnostico y “Backup & Restore” y es aquí donde subiremos el Archivo “Restore” para dar solución al punto 9

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Le confirmamos en el cuadro de verificación, y Usando el flag o respuesta del Anterior reto,” **MAZINGERLISTO2020**” la vamos a agregar en el campo de Password y en el campo “Examinar” le damos la ruta donde tenemos el Archivo

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Y Por Ultimo Restauramos el Archivo, y le Chicleamos en Aceptar

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Luego de esto el “Firewall” se Reinicia, pero con otra dirección “Ip”

Texto

Descripción generada automáticamente

Y si no te abre el “pfsense” podemos reasignarle la dirección “Ip” como hicimos Anteriormente con la Única Variación es que elegiremos una nueva dirección “Ip” pero que se encuentre dentro del segmento de virtualización; al Iniciar este “Firewall” ya lo debemos de realizar con el “password ” del reo anterior “MAZINGERLISTO2020” y luego de ello podemos ya ir a la parte de “firewall/rules/LAN”

Tabla

Descripción generada automáticamente

Entonces los **CTF= 50A370199AA13131DEA546CEFEC233C6**

**F7247211BEA358BF5D8D44130EDDB3CB**

**76AA211D3C67CCA1F84EC12F9225067C**

**43B36CA2C59434925CD83A2B21B000D2**

**C420F35DB4C65685A08787A703065759**

**AADFCBD95C8C096472D98742227F36F9**

**DBC54C6A87719181BF21631CB2C17964**

Reto Informático N.º 10

Reventar (Crackear) los 7 hashes (Password) obtenidos en el reto número 9

--Pista: Tus conocimientos en password cracking, te serian de mucha utilidad

--Flag final: El flag final de este reto es lograr crackear los 7 hashes

**R/** Primero vamos a Identificar qué tipo de hashes son con la Herramienta “hash-Identifier “ en Kali Linux; y Podemos observar que son MD5

Texto

Descripción generada automáticamente

Luego vamos a crear un Archivo que se va a Llamar “reto10.txt” con la Herramienta nano y verificamos con el comando “cat”

Texto

Descripción generada automáticamente

Vamos a usar la herramienta “hashcat” y como es un hash MD5 vamos a usar -m 0 y como también vamos a usar un diccionario usaremos -a 0



Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Entonces el CTF=yo3165867463

Phillipkingforever

kliplev

berzuit2286

Jesus8892

yo0135445216

Reto Informático N.º 11

Reventar los siguientes hashes:

AB3DDA54E04A3FAC61F51ACD1E21233EBF28A73C3DC3C47A2B19DF0733621578

1B87E42914B4E7682588A91E6FD1020F8B905E7D

10F560DA63EF7D0DD0748AB410ED8B0ACE9F425E

--Pista: ¡¡Tus conocimientos en password cracking usando la técnica de ataques por reglas, te vendría muy bien!!

--Flag final: El flag final de este reto es reventar (Crackear) un password

**R/** Primero vamos a Identificar qué tipo de hashes son con la Herramienta “hash-Identifier “en Kali Linux;

El Primer has es un SHA256 y los otros dos son SHA1

Entonces vamos a guardarlos en dos archivos diferentes debido a que son diferentes hashes y con la herramienta “hashcat” vamos a Romper esos hashes y vamos a usar las reglas que también las ubicamos en “/usr/share/hashcat/rules”

Texto

Descripción generada automáticamente

Ya en el Archivo dos del punto 11 hemos cambiado la regla, usando la regla “combinator. rule” pero usando siempre el diccionario “Rockyou.txt” y en la ultima regla vamos a usar la regla “dive.rule ” que s una de las reglas más fuertes y Robustas





Reto Informático N.º 12

Construir un diccionario con los personajes de la famosa serie de televisión mexicana el chavo del ocho. Una vez que se construye el diccionario en mención, crear una regla personalizado con los primeros 12 items de las reglas de la aplicación hashcat

(Implemented compatible functions)

https://hashcat.net/wiki/doku.php?id=rule\_based\_attack

Luego debes de romper (Crackear) los siguientes hashes:

DEDB6F3A8CDBD055AB3710890EB1D974

2427f3d7e91d20e31a2ee49607bd189144559886

--Pista: Tus conocimientos en password cracking usando la técnica de ataques por reglas, te vendría muy bien!!. ¡¡Usar una regla personalizada sería una gran idea!!

--Flag final: El flag final de este reto es reventar (Crackear) varios password

**R/** Primero que todo vamos a Realizar laregla ”chavo.rule” y para ello se nos indica que debemos crear una regla personalizada con los 12 items de las funciones ” Implemented compatible functions” las cuales las Encontramos en el vínculo suministrado “https://hashcat.net/wiki/doku.php?id=rule\_based\_attack”

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Nota: en el área de la “Description” Nos dice la labor de la Función, ejemplo: “l” y su descripción nos dice que todas son minúsculas y así con cada una de las 12 funciones. Y el Archivo debe estar en donde van todas las “.rules”

Texto

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Ahora vamos a realizar el diccionario “dicChavo.txt“con todos sus personajes

Texto

Descripción generada automáticamente y por último debemos de verificar que tipo de hashes son los dos elementos que tenemos que romper para dar solución al ejercicio. Y para ello usaremos la herramienta “hash-Identifier “en Kali Linux; lo cual nos Dice que el Primer hash “DEDB6F3A8CDBD055AB3710890EB1D974” es un MD5 y el segundo hash “2427f3d7e91d20e31a2ee49607bd189144559886” un SHA1

Texto

Descripción generada automáticamente con confianza media

Podemos ver que al llamar la Herramienta “hashcat” primero va la clasificación del hash y luego el uso del diccionario y luego se usa donde hemos guardado el hash y luego el diccionario y luego la regla que vamos a utilizar.

Entonces el **CTF=brujadel71brujadel71**

**Señorbarrigaseñorbarriga**

Reto Informático N.º 13

Se tiene un volcado de memoria RAM, el cual es resultante de una investigación forense digital, y hace parte de una prueba forense. Respecto a este dump (volcado de memoria) se debe de obtener lo siguiente:

A tener en cuenta: (El volcado de memoria esta localizado en la carpeta reto 13 y se llama: memserver.mem)

IP Agresor Informático:

Nombre Malware (Ejecutado) por el agresor:

Puerto Origen conexión Malware:

Puerto Destino por donde entro el malware a la victima:

PID del malware:

Firma del malware antivirus MICROSOFT (Virus total) :

Hash del Malware MD5:

Hash del Malware SHA1:

IP donde se conectan a la victima pro el RDP:

Ruta donde se infecto el malware en el equipo victima:

--Pista: Tus conocimientos en análisis forense de memoria RAM usando la herramienta volatility Framework, te vendría muy bien!!

https://www.volatilityfoundation.org/26

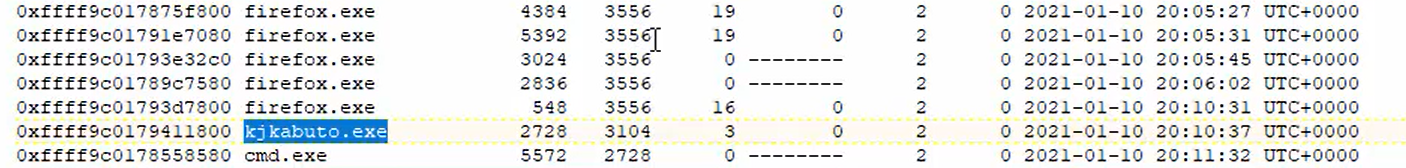
--Flag final: El flag final de este reto es obtener la información solicitada en el enunciado del reto

R/ Entonces nuestro Dump de memoria “memserver.mem” lo descargamos en un disco diferente a “C:\” luego de ello usamos la Herramienta “Volatility” para verifique el perfil

Texto

Descripción generada automáticamente

Con la Imagen Anterior podemos intuir que es un Windows 10, luego de esto vamos a ejecutar otro comando el “pslist” que es la validación del perfil de Windows 10, que habíamos visto anteriormente



Como podemos ver la la imagen el archivo “Kjkabuto.exe” No es un Archivo Normal de Windows pero por ende lo dejamos enlistado y señalado para seguir observándolo, vamos a usar el comando “pstree” para mostrarnos el orden jerárquico

Tabla

Descripción generada automáticamente con confianza media

Ahora vamos a usar el comando “netscan” y este comando nos ayudaría a encontrar “puerto Origen”, “puerto destino” y la “Ip” donde se conecta a la victima por el Puerto RDP

Imagen que contiene Calendario

Descripción generada automáticamente

Aquí podemos observar una conexión, la cual seria que desde la “Ip” 201.233.17.174 desde el puerto 4815, hizo conexión al “RDP” a la “Ip” victima 172.31.55.117 por el puerto 3389 este ultimo es desde donde se origino el “Malware” y lo vamos a extraer para hacer un análisis n la web de “virustotal” en línea, antes de ello debemos de nuestro sistema de Antivirus detenerlo por que detectaría el “Malware” y lo eliminaría

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Entonces el **CTF=**

**IP Agresor Informático: 172.31.55.117**

**Nombre Malware (Ejecutado) por el agresor: kjkabuto.exe**

**Puerto Origen conexión Malware: 49822**

**Puerto Destino por donde entro el malware a la víctima: 4443**

**PID del malware: 2728**

**Firma del malware antivirus MICROSOFT (Virus total) : Trojan:Win64/Meterpreter.B**

**Hash del Malware MD5: 590eb099ec4833d72a64b9573f527ce**

**Hash del Malware SHA1: 8927b1ab1762ee387fb51d7a21a75b7c6423ed0a**

**IP donde se conectan a la víctima pro el RDP: 201.233.17.174**

**Ruta donde se infectó el malware en el equipo victima: C:\Users\Administrator\Downloads\kjkabuto.exe**

======================================================================

Reto Informático N.º 14

Se tiene como consecuencia de un ataque a un servidor Windows 2016 server la siguiente SAM database. Proceder a crackear los password cifrados que se encuentran en los archivos en mención

--Pista: Tus conocimientos en password cracking a tipos de Hash NTLM HASH te serian de gran ayuda!!. Además, se te suministran dos diccionarios para ayudarte a reventar los password.

--Flag final: El flag final de este reto es reventar (Crackear) varios password

**R/** Primero se nos suministra 3 Archivos Adicionales Además del enunciado “SAM DATABASE WIN 2016 SERVER” , “dicc1” y “dicc2”; al ver el Archivo de la “SAM” tenemos que separar los Hashes del resto que contiene el Archivo

Texto

Descripción generada automáticamente

Luego de ello vamos a usar el “hash-identifier” para verificar que tipo de hashes son los que tenemos, y así poder junto a “hashcat” para romperlos y completar el reto

Texto, Carta

Descripción generada automáticamente

Como podemos ver el resultado es que es MD5 y así con cada uno de los demás Hashes

Nos vamos a la Ayuda de “hashcat” miramos como podemos combinar los dos diccionarios

Calendario

Descripción generada automáticamente

Para Este Ejercicio vamos a usar la Ultima Regla “combinator” el cual nuestro ejecutable de “Hashcat quedaría ”



Pero dado que ya Habíamos ejecutado este mismo vamos a usar el comando “–show “

Para que nos muestre el comando y su resultado

Imagen que contiene interior, botella, tabla, foto

Descripción generada automáticamente

Entonces el **CTF=spiderman2021SPIDERMAN**

**batman2121BATMAN**

**superman2020SUPERMAN**

**venom2020VENOM**

Reto Informático N.º 15

Se tienen los siguientes hashes. Proceder a romperlos

hash1

f99452d280d7310e26ba2362cfc62ae2f090a7b1

Nota: el anterior hash contiene minúsculas y números

hash2

810F91EBBD575F21C07C60B1866D6BE309503388366DECD165D74A712AA0B25D

hash 3

5DF5D06DDC1913B052C124B5796E5741

Nota: Se tiene el precedente de que la contraseña es LA PALABRA megatron seguida de 3 caracteres, pero se desconocen los últimos 3 caracteres de la contraseña completa megatron???

hash 4

2faab50573cc59de5ccb7d72be270eb0

Nota:: el password se compone de dos mayúsculas, dos minúsculas, dos números y dos caracteres especiales

--Pistas: Tus conocimientos en password cracking utilizando la técnica de fuerza bruta y mascaras te serian de mucha utilidad para resolver este reto informático.

--Flag final: El flag final de este reto es reventar (Crackear) varios password

**R/** Primero para realizar este reto debemos de tener en cuenta que estos son “ataques de Fuerza Bruta”, en el Primer hash, antes de Identificarlo; Nos dice la pista: **“Nota: el anterior hash contiene minúsculas y números”**. Para ello debemos de ir a la Ayuda de “hashcat” y esto con el fin de que ahí se encuentra una norma o regla que nos dice como debemos de realizar este tipo de ejercicios

Texto, Carta

Descripción generada automáticamente

Entonces para el Primer ejercicio al decirnos que tiene minúsculas y números, y es por ello que vamos a usar “l” y “d” pero siempre Antecedida por un signo de “?”, y para su cantidad debemos de jugar con las mismas es decir 6 letras y 2 números, ajora vamos a ver que clase de hash es,

Texto

Descripción generada automáticamente con confianza baja

Y ahora formamos la secuencia del hash para ejecutarlo



Entonces -m es para invocar a nuestro hash que en este caso el 100 que es el SHA-1 y -a por que vamos a usar diccionario y el “3” por el uso del “Fuerza Bruta ” el Nombre del Archivo donde guardamos el Hash y su “charset”, comentado anteriormente

Imagen de la pantalla de un celular con texto e imagen

Descripción generada automáticamente con confianza media

Hash2

Como No nos Dieron Pista alguna para este Hash nos vamos a usar la “a” debido a lo mismo que comentamos anteriormente, debemos recordar que cada letra debe ser antecedida por el signo de “?” y colocamos 6 de cada una.

Ahora vamos a ver que tipo de Hash es y como armar la secuencia para “Hashcat”

Texto

Descripción generada automáticamente con confianza baja



Entonces el 1400 es por que es un SHA-256 y el 3 es porque estamos usando “Fuerza Bruta” , nombre de nuestro archivo donde almacenamos el hash y el “charset” mencionado en el párrafo Anterior

Imagen de la pantalla de un celular de un mensaje en letras blancas

Descripción generada automáticamente con confianza baja

Hash3

En este caso tenemos parte del Hash como lo cita en el punto “**Nota: Se tiene el precedente de que la contraseña es LA PALABRA megatron seguida de 3 caracteres, pero se desconocen los últimos 3 caracteres de la contraseña completa megatron???**”, entonces sabemos que tenemos que agregar 3 caracteres, y recordemos que siempre el carácter que valla a ser tiene que ser antecedido por un “?”, pero al No saber si estos sean numero o letras podemos usar la letra “a”

Por Otra parte, vamos a ver qué tipo de Hash es

Texto

Descripción generada automáticamente con confianza baja



Entonces el “0” es porque es un Hash MD5, el 3 es “Fuerza Bruta” Nombre de archivo y por último el “Charset”, que en este caso ya teníamos la palabra “megatron” y adicionamos los 3 caracteres

Una captura de pantalla de un celular con texto e imagen

Descripción generada automáticamente con confianza media

Hash4

En este caso nos indica el “charset” que debe contener y eso lo vemos **“el password se compone de dos mayúsculas, dos minúsculas, dos números y dos caracteres especiales”** podemos decir que llevados caracteres que menciona, es decir llevaría para este ejercicio dos “u”, dos “l”, dos “d” y dos “s”. Recordemos que su antecesor es el signo de “?”

Ahora vamos a verificar el Hash del ejercicio mencionado

Imagen que contiene Texto

Descripción generada automáticamente



Entonces es “0” por qué es MD5, “3” por “Fuerza Bruta” Nombre del Archivo donde tenemos el Hash y el “charset” mencionado anteriormente

Imagen de la pantalla de un celular de un mensaje en letras blancas

Descripción generada automáticamente con confianza baja

Entonces el **CTF=dajuan90**

**mar8ia**

**megatron8M+**

**OPti44\*-**

Reto Informático N.º 16

Se tiene el siguiente hash:

dba\_juan:01003

aca1ce588ca08bb1de64bd69fde4d2d7332723a058aca0e

Se debe de identificar el tipo de hash, y una vez identificado el tipo de hash, proceder a romperlo (Crackearlo)

--Pista: Tus conocimientos en password cracking e identificación de tipos de Hash te serian de mucha utilidad para resolver este reo

--Flag final: El flag final de este reto es reventar (Crackear) una contraseña

**R/** Entonces para realizar este ejercicio vamos a usar la herramienta Caín y para ello tenemos que dividir nuestro hash “Caín”

Y para ello separamos la parte del usuario dba\_juan:01003

Y luego volverlo a cortar

e588ca08bb1de64bd69fde4d2d7332723a058aca0e

Interfaz de usuario gráfica, Aplicación, Tabla, Excel

Descripción generada automáticamente

Para Agregar el hash debemos de ir primero a la parte de “MySQL Hashes” y de ahí “Cracker” y le damos ene el signo “+” y agregas el hash, y ahí cuando te pide un nombre escribes “root” y ahí se Genera la ventana que va haciendo el “cálculo del hash”

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Entonces **el CTF= revitalization**

Reto Informático N.º 17

Se tiene un volcado de memoria RAM, el cual es resultante de una investigación forense digital, y hace parte de una prueba forense. Respecto a este dump (volcado de memoria) se debe de obtener lo siguiente:

(El volcado de memoria está localizado en la carpeta reto 17 y se llama: memdump.mem)

Se deben de extraer los hash de la SAM data base que se encuentran en el volcado de memoria, y proceder a crackearlos (Solo crackear los hash de los usuarios oscorp , jean.claude y juanes)

--Pista: ¡¡Tus conocimientos en análisis forense de memoria RAM usando la herramienta Volatility Framework, te vendría muy bien!!

https://www.volatilityfoundation.org/26

¡¡Además de los conocimientos en password cracking a hash en formato NTLM HASH usando ataques combinados, seria de utilidad!!

Como ayuda extra se te suministra un diccionario

--Flag final: El flag final de este reto es cracking de varias contraseñas 3 en total. Solo crackear los password de los usuarios extraídos de la san data base llamados: Oscorp , Jeanclaude y juanes

**R/** primero que todo tenemos que ir al volcado de Memoria; y tenemos que hacer el proceso de la Info de la Imagen que tenemos esto con el fin de ver que comandos podemos aplicar al mismo

Imagen que contiene Código QR

Descripción generada automáticamente

ya con esta información lanzamos el comando “hiverlist” esto con el fin de saber dos registros que tiene el mismo sistema para que el sistema nos entregue los hashes

Texto, Código QR

Descripción generada automáticamente

De todos estos registros necesitamos dos Números; el Primero es “Volatility Virtual” del “\REGISTRY\MACHINE\SYSTEM” y el segundo es “Volatility Virtual” del “\SystemRoot\System32\Config\SAM”

Luego de tener estos dos números usaremos el comando “hashdump”

F:\vol>volatility.exe --profile=Win7SP0x86 -f memdump.mem hashdump -y 0x8901c008 -s 0x899379c8 >reto17.txt

Texto

Descripción generada automáticamente

Ya teniendo los Hashes seleccionamos los tres hashes que se nos pidieron para el reto ue son el de Oscorp, Jeanclaude y juanes

Imagen en blanco y negro

Descripción generada automáticamente con confianza baja

Al Usar La Herramienta “hash-identifier”, nos comprueba que los 3Hashes son MD5, y los Guardaremos en un archivo de texto dentro de Kali Linux para romper los hashes por medio de la herramienta ”Hashcat”

341963933ecd3f7eb820da843ce57635

141cc94ef8fe0c74c0bec1ae41bd3f41

54d5ed205882ecfc551d68b1c2ab3fa0

juanes:1005:aad3b435b51404eeaad3b435b51404ee:54d5ed205882ecfc551d68b1c2ab3fa0:::

oscorp:1006:aad3b435b51404eeaad3b435b51404ee:341963933ecd3f7eb820da843ce57635:::

jean.claude:1009:aad3b435b51404eeaad3b435b51404ee:141cc94ef8fe0c74c0bec1ae41bd3f41:::

juanes:1005::54d5ed205882ecfc551d68b1c2ab3fa0:::

oscorp:1006::341963933ecd3f7eb820da843ce57635:::

jean.claude:1009::141cc94ef8fe0c74c0bec1ae41bd3f41:::



hashcat -m 1000 -O -a3 -i reto17.txt

Reto Informático N.º 18

Se tiene un archivo de texto llamado code-decode.txt

Proceder a validar que tipo de información contiene, y luego decodificarla.

--Pista: Usa la información que se decodifica , para usarla como contraseña, para descomprimir el archivo llamado felicidades.rar

--Flag final: El flag final de este reto es obtener (Visualizar) el contenido del archivo felicidades.rar

**R/** se tiene el Archivo “decodifica” y vamos a darle los permisos como llave publica

Texto

Descripción generada automáticamente

Luego para darle permisos

Reto Informático N.º 19

Se tiene un archivo llamado data. Lo que debes de hacer es identificar el tipo de archivo es, y además extraer datos (Análisis básico de binarios y de metadatos) de este archivo

--Pista: De este archivo puedes extraer información relacionada con el password de un usuario llamado guest. Además tus conocimientos en extracción de metadatos y análisis básico de archivos ejecutables (Análisis básico de binarios) e ingeniería reversa básica te serian de mucha ayuda.

--Flag final: El flag final de este reto es obtener el password de un usuario llamado guest y luego descomprimir el archivo llamado decepticos.rar y observa el respectivo contenido del archivo comprimido en mención. Para obtener el password del archivo a descomprimir, debes de concatenar los valores del usuario y password encontrados en el archivo data (Análisis básico de binarios), en lo que respecta al análisis del archivo binario, y no de la información extraída de los metadatos.

R/ Primero Tenemos que analizar el Archivo” data”

Imagen que contiene Forma

Descripción generada automáticamenteImagen que contiene Logotipo

Descripción generada automáticamente

Para poder realizar un mejor análisis vamos a la siguiente página web “http://www.x-ways.net/winhex/” y ahí descargamos el ejecutable (esto con el fin que nos Ayude a Analizar el Archivo Data)

Luego de ello descargamos descomprimimos y ejecutamos; inicialmente le damos Archivo en el menú principal y abrir, copiando la ruta donde tenemos el Archivo “data”

Empezamos a realizar un análisis en todo el Programa y vemos un usuario y su Hash

Una captura de pantalla de un celular con texto e imagen

Descripción generada automáticamente con confianza media

Guest&7R1n17yN30

Pero recordemos que se nos dice:” Para obtener el password del archivo a descomprimir, debes de concatenar los valores del usuario y password encontrados en el archivo data (Análisis básico de binarios),”

username=guest&password=7R1n17yN30

guest&7R1n17yN30

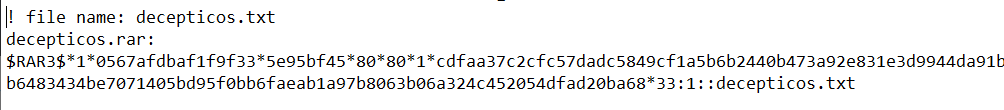
guest7R1n17yN30

guest:7R1n17yN30

quest=Trinity&Neo

k1ll0r7n

ver que ninguno funciono, procedí a usar la función “rar2john”, y luego agregarnos el archivo.rar.



Luego, vamos a llamar a la función “John The Ripper” y agregamos un archivo nuevo donde van a quedar los hashes descifrado



Como mostramos en los Párrafos Anteriores señalamos “guest:7R1n17yN30 vamos a la parte de “Herramientas” y le damos “Calcular Hash”

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Y me genera un hash 2B9DB39FBEFCD194997E8D8C8CDF415

2B9DB39FBEFCD194997E8D8C8CDF415C

2B9DB39FBEFCD194997E8D8C8CDF415C

Entonces **CTF=7R1n17yN30**

Reto Informático N.º 20

Se tiene este hash

61125D499BF34357626AB61E4731AE671CEEA39455FF9937ECE4C8B70ACDF502

--Pista: Utilizar los metadatos obtenidos del análisis del archivo llamado data del reto 19 como diccionario para crackear este hash. Importante no usar el mismo password que lograste obtener en el análisis binario del archivo data del reto 19.

--Flag final: El flag final de este reto es obtener reventar (cracking) el hash suministrado