La RUTA del HACKER (Cómo EMPEZAR Desde CERO) 2023

bueno bueno chavales Qué tal Cómo estáis Bienvenidos a todos y a todas a un nuevo vídeo del canal en el que vamos a estar hablando un poquito acerca de cómo empezar en todo esto de la ciberseguridad yo creo que ya iba tocando no al ser un vídeo bien estructurado acerca de toda esta temática Para los que me lleváis siguiendo desde hace tiempo desde hace años hablo de hace años sabréis que en mi canal ya hay un vídeo acerca de cómo empezar en todo esto de la ciberseguridad supuestamente y claro digo supuestamente porque es un vídeo del cual no estoy muy contento que digamos no estoy muy orgulloso porque se convirtió más en una charla motivadora en un discurso inspirador que otra cosa o sea realmente nos doy pautas De nada se os doy la chapa ahí realmente y claro uno se queda sin saber realmente Cómo empezar me ponía a ver los comentarios y era en plan Oye Javi la piel de gallina un discurso muy bonito pero cómo empiezo así que bueno visto lo visto he tomado la decisión de hacer un nuevo vídeo pero esta vez bien estructurado porque claro aquel vídeo es de hace 4 años creo más o menos y recién estaba empezando a crear contenido pero a lo largo de estos años hemos creado tanto contenido que ahora sí que os puedo decir que ya hay un camino fijado para poder aprender y empezar con todo esto yo en este vídeo voy a tratar de trasladaros Pues todo lo que necesitáis para empezar con todo esto de la ciberseguridad en cuanto al contenido que de mi lado he aportado vale porque hay muchas horas de contenido y están tan desperdigadas por tantos lados que igual uno se pierde y no sabe por dónde arrancar con todo lo que yo de mi lado ofrezco así que bueno vamos a ofrecer en este vídeo dos modalidades vale la modalidad digamos reglada de pago y la modalidad gratuita os puedo garantizar que con ambas modalidades Vais a aprender un porrón tanto de forma gratuita como pagando pagando Pues bueno Vais a tener un contenido digamos de una forma un poco más estructurada que ahora os comento Pero bueno tanto si pagáis como si no al final es inversión de tiempo sobre todo Vais a aprender un montón Así que bien con canitas de comentaros todo pero primero que nada es una página la cual ofrece claves de software OEM baratas y completamente legales las cuales son 100% oficiales y pueden ser activadas en línea en esta ocasión a través del enlace que os compartimos en la descripción de este vídeo podréis adquirir múltiples productos al mejor precio entre ellos claves de producto para la suite de Microsoft Office claves de activación para Windows 10 y Windows 11 y también van del products a un precio bastante asequible Cabe destacar que en este caso no se necesitan cupones de descuento dado que tras acceder a la página con el enlace que os compartimos ya dispondréis del descuento directamente aplicado en la página para adquirir el producto recordad que simplemente tenéis que añadirlo al carrito darle a tramitar pedido y proceder ya al pago posteriormente proporcionando los datos correspondientes gracias a casefam por patrocinar este vídeo y ahora continuemos con el vídeo de hoy Bueno chavales vamos a ver un poquito Cómo empezar en todo esto lo primero que os quiero mostrar obviamente es nuestra propia pandemia de ciberseguridad vale aquí por detrás Pues yo soy el profesor y por ahora tenemos tres cursos creados que son bastante extensos sobre todo la introducción al hacking que es del que quiero hablar ahora y bueno como podéis ver pues ahora mismo tendríamos tres cursos disponibles vale el curso de introducción al hacking por un lado el de personalización de entorno en Linux por otro lado y ya por último el de introducción a Linux De todas formas cabe decir que estamos trabajando en muchos más cursos vale aquí podéis ver en todo momento en los que estamos trabajando ahora mismo estamos con el de python ofensivo un

curso muy chulo que lo Sacaremos en breve y Próximamente el de hacking web vale Bueno antes que nada tema precios que ya os veo yendo en los comentarios en plan Oye sí vale Pero cuánto cuesta bueno la página es hack for you.io y en la propia página principal abajo aquí tenéis los precios disponibles vale disponéis de tres planes de membresía Por un lado pues la membresía hackshore que es para pagos mensuales que hagáis por otro lado Pues tendríais el plan Pro hackshore que sería para pagos trimestrales cada tres meses y ya por último la membresía Elite hackshore para pagos obviamente pues en función del tipo de membresía que tengáis pues tenéis acceso a ciertas ventajas exclusivas de forma que por ejemplo si pagáis la trimestral pues tenéis acceso a reuniones grupales en disco que hacemos cada semana donde en caso de cualquier duda si por ejemplo estáis haciendo una clase y no os queda claro algún concepto Pues en la propia llamada grupal estoy yo me preguntas lo que necesites y te echo un cable vale para que esa duda pues quede solucionada Asimismo Pues bueno para las membresías de tipo Elite hack sour las que son de pago anual pues tenéis acceso a un soporte prioritario así como tutorías personalizadas esto básicamente es a través de un calendario que gestionamos con calenday pues ahí veis Qué días están disponibles para concertar una cita privada conmigo y bueno tenemos un trato mucho más cercano y os he hecho un cable Al toque el mes estar todos en grupo Pues estamos reunidos tú y yo de todas formas esto que quede claro independientemente del plan de membresía que pille ahí tenéis soporte hay una sección en vuestro perfil de usuario donde podéis vincular vuestra cuenta de la academia con discord y a través de un Bot que tenemos configurado pues se otorga un un rol específico en base a la membresía que hayáis adquirido y tenéis acceso Pues a canales exclusivos donde debatimos dudas y Bueno estamos ahí siempre echando un cable en lo que podemos bueno en cuanto a los cursos respecta vamos a hablar un poquito acerca de Cómo comenzar no con todo esto yo siempre digo que la clave es Linux O sea si no sabes Linux malvama por tanto en base a esto hemos creado un curso de 15 horas bastante potente para que desde cero sin que sepáis nada de Linux pues os guiemos paso a paso la idea de este curso es que tengáis o adquiréis una buena soltura por consola y entendáis pues un sistema Linux como está compuesto Y cómo operar sobre este el curso la verdad estamos muy contentos por ahora hay 3.700 estudiantes inscritos que es un disparate y Bueno siempre el contenido de los cursos lo podéis ver aquí en la pestañita contenido vale aquí siempre Vais a poder revisar todo lo que se ve en este curso cada clase tiene una descripción adjunta para que sepáis qué es lo que se está tratando y Bueno hay cuestionarios hay preguntas para ir viendo si os están quedando claros los conceptos estáis totalmente distraídos os invito si queréis a que veáis el contenido de este curso yo os quiero hablar sobre todo del curso de introducción al hacking que es el que os va a preparar bien para empezar con el hacking así que bueno aquí podéis ver que es bastante largo hay un examen final de tensada máxima y unas prácticas muy muy chulas de proyectos en bash O sea que se os Mola mucho el scripting en bash esto es un disparate lo dicho hay un examen final de tensada máxima con 60 preguntas de todo lo que hemos visto para ver si os ha quedado todo claro y luego podéis optar también a un certificado final vale cada curso tiene su certificado con un identificador para que la gente lo pueda validar para ver si es real o no y lo dicho este sería el curso de introducción a Linux vale paralelamente otro que recomendamos es el de personalización de entorno en Linux Para los que me seguís en Twitch sabréis que tengo un entorno un tanto especial en el que opero y bueno todo este entorno de trabajo está completamente personalizado a mano desde cero Y en este curso pues os guiamos paso a paso para que sepáis pues como tenerlo igual a como lo tengo yo Pues en este caso tiene 3011 estudiantes otro auténtico disparate Y bueno

mismamente pues ahí en la pestañita contenido podéis ver todo lo que se abarca No todo lo que se explica y es básicamente pues cada cosita para que tengáis todo tal y como lo tengo yo el entorno de trabajo aquí en este caso no hay examen final simplemente optas al certificado porque Bueno realmente aquí un examen consideramos que no tenía mucho sentido y bueno Ya teniendo el de Linux y teniendo Incluso el entorno personalizado que esto es más opcional que otra cosa ya podéis saltar al de introducción al hacking vamos a echarle un ojo de introducción al hacking Bueno este curso lo hemos sacado hace unas semanas recientemente y es un curso de 53 horas vale un curso bastante denso que sumado a la práctica porque hay mucha práctica es full practico nada de teoría todo con laboratorios despliegues manuales con docker de Laboratorios es un espectáculo Pues bueno con la práctica se puede llegar perfectamente a superar las 100 horas de curso este curso está diseñado para quien no sepa nada pues que se ha guiado paso a paso por mí que yo soy el profesor de por todo este contenido vamos a echarle un ojo a la pestañita contenido Aquí sí que me quiero detener para que veáis un poco la estructura del curso Bueno lo primero de todo una pequeña introducción al curso ahí vemos Bienvenido al curso y explotando las funcionalidades de las clases claro lo cómodo es que hemos hecho para que cada clase tenga un foro activado internamente de forma que tú puedes dejar tus dudas y puedes buscar por dudas de forma que tanto nosotros como la propia comunidad puede responder y nos echamos un cable entre todos está bastante bien bueno aislado a esto pues saltaríamos directamente a la parte de conceptos básicos vale empezamos ya ahí a darle caña esta parte obviamente pues cabe decir que es introductoria pero es necesaria para abordar todo lo que se va a ver a posteriori así que bueno ahí podéis ver no empezamos viendo que es una dirección IP diferencias entre ipv4 e ipv6 hablamos de direcciones Mac diferencias entre alway y Nick protocolos comunes udp tcp el famoso triway handshake y por otro lado el modelo Osi tan conocido donde Bueno podemos En qué consiste y cómo se estructura la actividad de red en capas Cabe destacar que las primeras clases son más teóricas que otra cosa Aunque Bueno siempre acompañamos de una parte práctica las clases para desde consola puedes hacer alguna que otra triquiñuela Pero bueno todo esto es una introducción para irnos preparando de forma gradual para la que se viene vale que ahora lo Vais a ver bueno una vez visto esto nos adentramos ya profundamente a la parte de subneting que es y cómo se interpreta una máscara de red y cálculo total de hosts máscaras de subred tipos de clase e interpretación de prefijos de red interpretación de los rangos de red que el cliente nos ofrece para auditar y ya por último redes extrañas y casos particulares claro la idea en esta sección es que cuando tú vayas a un cliente Pues digamos que sepas en base a la IP que te da con el 6 de r a una máscara de red dada Pues que sepas qué Rango es el que tienes que auditar o en qué Rango operas para que así cuando el cliente pues te lo diga no te quedes a cuadros pensando así mismo Pues bueno Luego tendríamos un cuestionario de subnetting y redes un cuestionario de 24 preguntas en base a todo lo visto y adicionalmente hace muy poco hemos incorporado una clase más que es esta la de tips de subneting y cálculo direccionamiento en redes donde Bueno pues en 22 minutos que ahí podéis ver en todo momento Cuánto dura cada clase hay algunas que son de una hora y pico Así que cuidado pues os comento varios truquitos para rápidamente calcular de forma veloz Pues eso el saber en qué Rango operamos y demás posteriormente nos adentramos a la etapa de reconocimiento como veis enemap y sus diferentes modos de escaneo vemos algunas técnicas de pasión de firewall jugando con mtu Data Lenin entre otros uso de scripts y categorías en nmap para aplicar reconocimiento creación de tus propios scripts en Lua para nmap alternativas para la enumeración de puertos usando descriptores de

archivos descubrimiento de equipos en la red local empleando arp e icmp y algunos tips y Bueno mucho cuidado aquí que empezamos a jugar con hacker One ya para fijar dominios reales a los cuales pues emplearles reconocimiento vemos por ejemplo como aplicar descubrimiento de correos electrónicos Cómo aplicar reconocimiento de imágenes enumeración de subdominios credenciales y brechas de seguridad varias herramientas para identificar las tecnologías que una página web emplea y bueno En las siguientes Dos clases pues mostramos herramientas especializadas en fusil para enumerar los archivos de un servidor web Asimismo Pues bueno vemos un poquito de Google doc Google hacking los 18 doorgs más usados Y por último identificación y verificación externa de la versión del sistema operativo esta parte sería para que sepas cómo atacante como proceder para determinar si estás ante una máquina Linux o una máquina Windows por ejemplo una vez más pues tendríamos el cuestionario de reconocimiento otro cuestionario de 24 preguntas relacionadas con toda la temática que hemos visto y Bueno atentos aquí entraríamos a una sección de configuración de Laboratorios locales en docker una sección muy chula Porque la idea en todo el curso es que os enseñamos a crear y desplegar vuestros propios laboratorios en local desde cero con docker todo lo que vamos a estar empleando para desplegar los laboratorios prácticos va a ser puramente con docker no vamos a irnos a una plataforma para descargarnos una VPN o tener que pagar algo adicional no todo montado desde cero a mano tirando de docker puramente de si no sabéis utilizar docker no os preocupéis las hay de introducción a docker instalación de docker en Linux definiendo la estructura básica de docker file es justamente en este archivo donde vamos a definir el Core de lo que sería el laboratorio que vamos a desplegar clase de creación y construcción de imágenes carga de instrucciones en docker y desplegando nuestro primer contenedor comandos comunes para la gestión de contenedores por forwarding en docker y uso de monturas y despliegue de máquinas vulnerables con docker compost con dos ejemplos prácticos y bueno Obviamente el cuestionario de docker de 23 preguntas no que no falte después de esto pues saltaríamos directamente a la sección de enumeración de servicios comunes y gestores de contenido empezaríamos enumerando servicios básicos como ftp ssh http y https smd y nos adentraríamos a una sección donde aprendemos a enumerar gestores de contenido vale algunos MS como wordpress jungla drupal magento para que cuando os enfrentéis a estos gestores de contenido pues sepáis perfectamente como proceder y cuidadito con esta clase de toma de con obsidian esta clase de media hora ahí potente o vamos a enseñar a tomar apuntes con obsidian que es una locura esta herramienta empleamos Mark down mayoritariamente pero te quedan los apuntes de una forma espectacular muy muy profesional y elegante y bueno cuidadito que ya estamos adentrándonos a la parte chula que por ahí debajo se ve asomando aguas top ten y vulnerabilidades webff Ya huele aquí a que se está tensando eh Bueno antes que nada conceptos básicos de enumeración y explotación como veis Introducción a la explotación de vulnerabilidades una pequeña clase introductoria hablamos de reversials de videls y de Forward Shields con varios ejemplos prácticos tipos de payloops distinciones entre stegen y Non staget tipos de explotación distinciones entre manuales y automatizadas formas de enumerar un sistema en una clase de media hora de todas formas más adelante hay una sección específica de escalada de privilegios y ahí metemos mucho más hincapié en esta parte y posteriormente una clase de 40 minutos de introducción a burk Suite sobre todo porque ahora es cuando se viene lo tocho lo chi por tanto bueno conviene saber utilizar Bueno atentos aquí os voy a leer del tirón todo lo que se va a ver en la parte del owas top ten y vulnerabilidades web todo esto es hacking web puro o sea con unos laboratorios hay de la leche para poder practicar y como veis

las clases pues son ciertamente largas es una hora y media 50 minutos 40 minutos una hora y 12 minutos cuidado os leo todo lo que vamos a ver en esta sección sql injection por un lado Cross site scripting Dos clases ahí bastante potentes que llegan casi a las 2 horas xml external entity injection los famosos XXI aprendemos a Identificar y explotar los local file inclusión los lfi son unas clases prácticas que Uff cuidado Remote inclusión la variante rfi no como vía potencial de convertir un lfi a una ejecución remota de comandos una clase de media hora de Cross sidere Quest forget y los CSR una clase de 40 minutos de server cytrided que sería el ssrf la variante server Side temper injection los scti client los cst una clase de media hora donde hablamos de los ataques de oráculo de relleno los famosos padding Oracle ataks aprendemos a identificar los ya explotarlos sobre todo y bueno vemos toda la aritmética que hay por detrás que se esconde detrás de los ataques de oráculo de relleno ataques de tipo jogging inyecciones no sql una clase de media hora una clase de una hora y media cuidado de inyecciones elevadas una clase de 40 minutos de ataques de deserelización con varios casos Los vemos en no Djs y en php y más adelante vemos otros ahora lo vemos una clase de 40 minutos literal de inyecciones latex una clase de una hora y 3 minutos cuidado de abuso de apis muy chula una clase de una hora de abuso de subida de archivos hemos varios casos prácticos para que sepáis cómo abusar de una subida de archivos con el objetivo de subir un archivo malicioso vemos varios casos prácticos de los prototype lution las contaminaciones de prototipo así como bueno ataques de transferencia de zona a xfr full son transfer ataques de asignación masiva los más a saintment Attack o para meter binding que se les llama también una clase de Open redirect donde vemos pues como explotar un Open redirect paso a paso con varios casos prácticos enumeración y explotación de webdaf enumeración y explotación de squid Proxy ataque shell shock inyecciones xpad una clase de 50 minutos ahí potentes aprendemos a explotar los inseguros Direct object reference los famosos y Doors así como el Kors una clase de 22 minutos donde aprendemos abusar de esto del intercambio de recursos de origen cruzado una clase cita de 22 minutos de ataques de truncado sql los sql truncation una clase donde aprendemos a explotar los session Y session overloading es más o menos todo lo mismo una clase de enumeración y explotación de los Jason web tokens los famosos jwt una clase de casi media hora donde vemos varios casos prácticos de condiciones de carreras aplicado Los Reyes condition bueno Last condition inyecciones css sin comentarios ataques de tercerización yammel desk yammel en python y ataques de deserenización pikel en python también ya por último una clase de 18 minutos donde Pues bueno vemos todo esto de grafqele introspection mutation y doorsql esto está bastante chulo y bueno por último un cuestionario de vulnerabilidades de 60 preguntas para lo dicho ver si habéis estado prestando atención o habéis estado viendo Netflix de fondo Bueno una vez visto esto saltamos a la parte de técnicas de escalada de privilegio Y todavía falta un montón de cursos Bueno vamos a leer esto rápido esto es para una vez comprometido un sistema pues explicamos varias vías potenciales para Elevar tu privilegio vale por un lado abusando de privilegios a nivel de sodoers abusando de privilegios s.wid detección y explotación de tareas Chrome pathfiyaking python library jacking abuso de permisos incorrectamente implementados detección y explotación de las capabilities explotación del kernel abuso de grupos de usuarios especiales abuso de servicios internos sistema abuso de binarios específicos secuestros de la biblioteca de objetos compartidos enlazados dinámicamente y bueno una clase luego bastante potente de la cual estoy bastante orgulloso de 50 minutos donde bueno vemos este concepto no de docker break out es básicamente estando en un contenedor como escapar de este tanto que hablamos y jugamos con docker para llegar o

alcanzar la máquina Josh posteriormente un pequeño cuestionario de 22 preguntitas ahí y bueno acto seguido nos meteríamos de lleno a la temida parte del buffer Flow Cabe destacar que en alguna que otra clase vemos algún que otro buffer overflow avanzado para que veáis un caso práctico Pero bueno aquí tratamos el más básico de todos el que os puede caer en el sppt y el que os caía en el scp pero el ossp está siendo un montón de cambios ahora mismo ya no te cae la parte del vagero ver Flow Pero bueno os enseño paso a paso a tratar con el buffer overflow más básico vale Sacaremos más adelante un curso de buffer overflow avanzado como los que hemos hecho en Twitch de máquinas bastante avanzadas pero bueno aquí vemos creación de nuestro laboratorio de pruebas e instalación de immunity de booker fase inicial de fuzzing y tomando el control del registro e IP asignación de espacio para el cel code generación de byte a raíz y detección de bad charts búsqueda de opcodes para entrar al SP y cargar nuestro shellco de uso de nobs desplazamientos en pila e interpretación del circo de para lograr ejecución remota de comandos modificación del circo de para controlar el comando que se desea ejecutar explotando un nuevo binario para reforzar lo aprendido y ya por último pues funcionamiento y creación manual de shellcode una clase de media hora bastante interesante donde os enseño a crearse el code estirando de ensamblador abajo nivel de forma manual en vez de tirar de herramientas como msc Venom Pues que entendáis la lógica de lo que hay por detrás en cuanto a creación de shell code y un cuestionario de buffer overflow que no falte con todo lo aprendido que no es poco La idea es que resolvemos 5 máquinas para que veáis como en base a todo lo aprendido ya muchos conceptos os va a sonar vale es la idea del curso entonces son unas máquinas que nos llevan un tiempito en resolver una hora y media una hora 50 minutos etcétera Pero resolvemos 5 máquinas en conjunto todas las máquinas que resolvemos son gratuitas las descargamos mayoritariamente de Boom Hub una plataforma donde te descargas la máquina y la importas posteriormente en vmware o en virtualbox y bueno como material adicional Pues por qué no Introducción a metas exploit venga me la juego e introducción sql Mac me la juego totalmente una clase de 6 horas y media se me fue ya vamos espectacular una clase de 6 horas y media de introducción al pivote Oye qué es esto de pivote Bueno pues te vas al curso y ahí lo explicamos vale en 6 horas y media te lo explico todo una parte que nos habéis pedido mucho pues la hemos contemplado reportes y redacción de informes profesionales hechos en látex en mi canal de YouTube hay un vídeo donde os enseño a crear un documento profesional en látex Pero bueno aquí son dos clases específicas que he grabado para la academia donde entramos mucho más en materia vale una vez hecho pues examen final de tensada máxima un examen de 173 preguntas y bueno ya luego La despedida y tendrías el certificado final que está muy muy chulo la verdad es que es un curso muy muy completo en el que he puesto ahí toda la carne en el asador es un curso lo he diseñado tal y como me gustaría habérmelo encontrado a mí cuando estaba empezando en su día no había nada de esto pues uno bien completito Así que nada esta serie digamos la parte reglada o la parte de pago en la que aprendes de una forma más por secciones todo más desgranado y más correcto Por así decirlo hay gente que le gusta aprender de esta forma y no hay ningún problema o sea es totalmente correcto pero bueno yo Siempre os digo que todo está en internet realmente Y es que yo también aislado a la Academia que hemos metido mucho curro y esfuerzo he estado creando contenido en Twitch y no os preocupéis que lo hemos estado ahí todo organizando bien crema atentos esta serie Eso sí la forma gratuita vale Si no os podéis permitir el costear la suscripción a la academia lo que corresponda Pues esta sería ahora lo que voy a mostrar una forma gratuita vale vamos a echarle un ojo Desde hace dos años yo dejé el trabajo yo trabajaba en Eleven y Me

dediqué a full a Twitch una plataforma de streaming donde todos los días sin parar todos los días hacíamos una máquina cada máquina la fuimos contemplando en este Excel comunitario de forma que bueno si yo por ejemplo traía en ese día concreto la máquina tentacle pues la contemplábamos en este Excel poniendo la dirección IP indicando si era una máquina Linux o una máquina Windows el nivel de dificultad si era difícil fácil insane que es mucho más complicada que las difíciles supuestamente bueno supuestamente no son complicadas todas las técnicas vistas que ahora veréis lo cómodo de todo esto que hemos representado en el Excel y bueno la certificaciones para la que para las que esta máquina digamos que os prepara Por ejemplo tú te haces la máquina tentacle de Hack de box y esta máquina pues te sirve bastante para prepararte de Cara a las certificaciones oscp o SEP ftx fpt de elon Security o defensive Security las de ostp yosep ahí veis que se toca directorio activo también y bueno cada máquina la resolución la tenéis en mi canal secundaria vale vamos a echarle un ojo rápidamente esto que estáis viendo por aquí es mi canal secundario de YouTube el de Xavi online conocéis a lo mejor el principal pero el secundario es este y en este canal Pues todo esto que estáis viendo por aquí son máquinas máquinas que máquinas que hemos hecho Bueno las miniaturas olvidarlas un poco pero a partir de aquí por ejemplo todo esto son máquinas máquinas Stream iOS máquina doctor máquina reel máquina máquinas por un tubo máquinas máquinas máquinas todo el rato desde que dejé la empresa para eso dedicarme a Twitch todos los días estábamos haciendo máquinas Pues todo esto es formación gratuita claro Cabe destacar que en Hack de box para tu poder hacer las máquinas retiradas tienes que pagar el bip Pero bueno Yo a lo que me refiero es a que la explicación como tal es accesible es gratuita aquí os explico paso a paso pues como resolver cada máquina y bueno quieras o no pues el ponerte en modo esponja para absorber todo lo que uno está explicando es la clave para luego el día de mañana pues cuando te puedas permitir el VIP o lo que corresponda Pues que ya tengas digamos una cierta base no que algunos conceptos te suenen que eso es lo importante y bueno como podéis ver pues nos hemos metido el curro el curraso ahí veis todas las máquinas que tenemos resueltas y cuidado que esto es una pestaña la pestaña de hac ahora vemos las demás Pero lo dicho es un disparate hemos estado aquí invirtiendo muchas horas hay más de 600 horas de contenido en el canal secundario con todo esto que estáis viendo es un disparate y bueno Esto es infinito tendríamos la pestañita de Boom Hub que Boom Hub es otra plataforma aislada a Hack de box para practicar la idea de todas estas plataformas es que te ofrecen máquinas vulnerables que otra persona ha diseñado para que tú la puedas desplegar ya sea importando la en una máquina virtual o conectándote por VPN como es el caso de hack debox o tryhakny y que trates de hackearla la Tú tienes la máquina y tiene una vulnerabilidad o múltiples vulnerabilidades dependerá de lo que se haya diseñado para esa máquina y tu objetivo como tal es ganar acceso a la máquina Pues esa es una forma de aprender en todo esto de la ciberseguridad brutal es algo que yo recomiendo y si os interesa todo esto del pen testing con la resolución de máquinas Vais a pillar un nivel brutal La idea es ver múltiples casos a más máquinas hagáis mejor Siempre os lo digo y bueno Boom Hub es otra plataforma donde tú te descargas la máquina esto ya sí que es totalmente gratuito O sea que no habría que pagar nada y bueno para cada máquina yo he adjuntado por aquí el enlace de descarga de esa máquina fijaros que si me vengo para acá pues ahí la tengo en la página de bull hat y yo podría pues Descargarme el comprimido donde está la máquina virtual no el punto va que importo en vmware en mi caso pues aquí tenéis un disparate también de máquinas resueltas muy muy chulas siempre he tratado de traer máquinas chulas o contemplar máquinas muy muy chulas de las que aprendamos mucho en este Excel y además

Pues también tendríamos la web de Port sugerir donde vemos un montón de cositas vale de hacking web ese pool injection múltiples tipos de inyecciones sql a ciegas para Oracle para mysql bueno de todo xml external entity injection director y transversal server y bueno de todo que es lo cómodo de este Excel Y esto es algo que la verdad creo que es la clave para poder empezar fijaros tenemos un Buscador de máquina no sé si lo sabíais pero infotec machines.io atentos a esto que esto os va a gustar para el que no lo conoz todas las máquinas que están en este Excel están sincronizadas aquí de forma que imaginaros que hay un día digo Oye me apetece aprender a explotar las sql injection lo escribes aquí sqli le das al enter todas estas máquinas que te salen son máquinas que están aquí contempladas en las cuales tocamos ese cuello injection cada máquina pues tiene Esto vale que se desglosa para ver lo que estamos tocando si os fijáis en Amarillo Ahí está de la búsqueda que yo he hecho pues me lo está marcando puedo ver la dificultad si es una máquina Linux la certificaciones para las que te preparas y Bueno luego la resolución en el canal de YouTube que pincháis y ya os lleva vale pero es que la cosa no acaba aquí imaginaros que decís Bueno yo quiero en este caso una máquina fácil de nivel de dificultad Y sí pues le damos al enter Ahora son siete máquinas imaginaros que quiero que sean de Boom Hub no de Hack de box porque no me puedo pagar el VIP pues pongo por aquí Boom Hub y ahí está imaginaros que además decís Bueno yo me quiero certificar o preparar para el ew es una certificación de hacking web de elon Security pues pones por aquí ewpt le das al enter Y bueno curiosamente pues son las mismas también si tú por ejemplo esto lo despliegas ewpt Y jpt si yo hubiera puesto por ejemplo ejpt únicamente Pues hay una única máquina entonces claro aquí puedes filtrar por una de cosas que es un disparate o por ejemplo hoy Quiero aprender XXI con una máquina insane por ejemplo Pues mira tenemos una que es la full Chrome donde al parecer pues tocamos XX justamente y externa lentitis para meter entity Blind ssrf esta máquina estaba muy muy chula combinada con xxg con un rfi para derivarlo a un rc a una ejecución remota de comandos era un disparate que queréis aprender de directorio activo Bueno pues ponéis active directory le dais al enter y ahí tenéis todas las máquinas que queréis que sea en Hack de box para máquinas Art que os prepare para el osset por ejemplo Ahí está podéis filtrar por de la gana que sean máquinas Windows pues Windows que sea maquina Linux pues Linux Y en este caso hay una la atenta con muy muy chula Que Quiero aprender buffer overflow Bueno pues ponemos por aquí va a hacer overflow un buffer Flow que sea un poquito avanzado que emplee Rock por ejemplo para 64 bits enter y bueno eso no le ha gustado pero si le quito esto Ahí está pues ahí lo tenemos lo de 64 bits creo que está representado de esta forma a ver Search Ahí está está representado como x64 no como 64 bits pero es lo mismo yo la verdad es que con este buscador y esto Esta es vuestra guía de trabajo esto es Jesucristo ya me hubiera gustado a mí el bien el que empecé con todo esto de la ciberseguridad el haber tenido algo así tan accesible o sea ahora mismo la información que hay que por lo menos de nuestro lado hemos aportado Qué es lo que no pude aportar Hace cuatro años que hicimos Este vídeo de cómo empezar en ciberseguridad que claro no teníamos nada de esto Pues ahora ya es que nos lo hemos currado tanto tío que podéis aprender de cosas lo tenéis todo accesible desde vuestra casa en vuestra silla con vuestro ordenador os ponéis a practicar a escuchar cada uno de los vídeos que tenemos grabados de las cosas que explicamos Y es que no hay excusas si no quieres aprender es porque no quieres no porque no puedes y nada chavales poco más realmente para empezar en la ciberseguridad lo que yo recomiendo Es que hagáis muchas muchas máquinas Y si veis que por ejemplo necesitáis de una forma más desgranada y más paso a paso por secciones pues aprender pues tenéis la Academia y bueno tampoco está tan cara lo hemos puesto un precio bastante

razonable y asequible y ahí ya Pues pilláis primeramente una buena base y ya luego os ponéis a ser máquina yo la verdad es que os recomiendo el curso de introducción al hacking y que os hagáis los otros dos que hay disponibles porque ahí Vais a pillar una muy buena base Porque empezamos desde cero Y es que claro las resoluciones que hacemos de las máquinas ya damos por hecho que me entendéis lo que estoy haciendo y vamos a tiro hecho En algunos momentos pero claro en la academia es todo partiendo desde cero cada concepto se va complicando luego va siendo de forma gradual el tema de la complejidad por tanto bueno poco más no sé en cuánto se va a quedar Este vídeo es un vídeo que quería grabar desde hace tiempo para promocionar un poco la Academia y que sepáis ahora bien por dónde empezar que creo que tenemos un montón de información accesible y nada poco más yo creo que lo vamos a dejar por aquí espero que se hayan resuelto vuestras dudas que tengáis ahora un camino un poco más iluminado para saber por dónde empezar y nos vemos en el siguiente vídeo un saludo chao