tierra de hackers contesta todas las preguntas que le plantean los oyentes para celebrar los 100 episodios estamos de celebración 100 episodios es una meta que bien lo merece comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast publicamos este episodio el 6 de julio de 2023 episodio número 100 yo sigue siendo Martín vigo y está conmigo sigue conmigo y seguirá conmigo Don Alexis porros Hola Alexis qué tal ahí ahí aplaudiendo ánimos episodio 100 pues muy contento contigo Martín Espero no haber dejado sordo a nuestros oyentes pero en episodios Crees que nos han llegado 100 preguntas o sería lo suyo no 100 episodios 100 preguntas llegaron muchas tío y muchos audios también los audios me gustan son más divertidos porque la gente le da su tono y su gracia que que si la tenemos que leer nos mandan saludos y todos muy chulo Lo Vais a escuchar ahora Pues nada adelante a ver no sé aquí estoy con el pastel a punto de cortarlo pero primero quería acabar el episodio y luego iba a soplar las velas pues tenemos preguntas del episodio quieres decir aquello de tu intro habitual de por dónde nos pueden contactar sé que este es un episodio un poco fuera del ordinario pero ya te veo gesticulando corriendo a Twitter y yo aquí matando tiempo hasta que abras Twitter y ya está pero bueno Este es un episodio especial es lo que hay no todos los días se llega a las tres cifras a los 100 episodios yo creo que llegaremos como mínimo a las cuatro cifras hablamos de mil eh Ya van a ser horas pero bueno Alexis tienes los resultados de la nuestra típica encuesta del último episodio del episodio 99 por ahí los resultados de la Quiniela son Barcelona x minutos resultado Pues sí La pregunta era estás A favor o en contra de la excepción de Carta blanca por la que gobiernos pueden utilizar spyware contra periodistas justificando asuntos de seguridad nacional todo esto viene por una modificación reciente de una ley europea que permitía gobiernos o quiere permitir a gobiernos que utilicen spyware como los famosos pegasus similares que hemos comentado en otros episodios para atacar o comprometer dispositivos de periodistas en principio pero bueno se podría utilizar contra cualquier ciudadano en un futuro No pues si empiezas con un periodista luego quién Define que es un periodista somos periodista Martín tú y yo bueno eso lo dejamos pero los resultados fueron la más votada es un no rotundo con un 7 25% seguida de Sí si es auditado Es decir a ver ahí Tenemos aquí evidencia por si hay una mala práctica y luego se puede ir a poner en prisión a quien haya abusado de este proceso con un 14% tenemos luego seguida de un no extendería a los demás a los ciudadanos a nosotros a ti y a mi querido oyente con un 7% y finalmente el resto es para sí por tiempo limitado es decir pues bueno Supongo que si es por alguna causa justa o justificada digamos y por un tiempo limitado no para toda la vida pues entonces igual sí perfecto genial incluso nuestro episodio 100 seguimos manteniendo la tradición y yo siguiendo con la tradición primero de todo nuestros patreos nuestros mecenas que en patrón aportan para poder seguir y llegar a los 100 darles la bienvenida a este maravilloso grupo de personas a perúneffer a Ana y un agradecimiento también especial a Guillermo por subir su aportación en patrón Muchísimas gracias a los tres y al resto por supuesto que seguís ahí aportando y a nuestros sponsors brawler Pro que es la herramienta más completa de seguridad en aws empresas de todos los tamaños se apoyan diariamente en prauer pro para que sus equipos puedan confiar en su modelo de seguridad de aws puedes probar brawler Pro hoy mismo y de manera totalmente gratuita y vas a obtener paneles y gráficas con información concisa y accionable con todo lujo de detalles sobre la madurez de tu modelo de seguridad y visión completa de tu infraestructura en de aws y tendrás todos los resultados en apenas unos minutos empiezo a usar brawler pro y benefíciate de sus resultados visitando tierra de hackers.comler prowlerpro y también queremos dar las gracias a otro de nuestros patrocinadores monat una empresa que comparte los mismos valores que tierra de hackers hacer la seguridad más accesible y transparente nosotros a través de un podcast y monat a través de una herramienta de gestión y visualización de telemetría y

datos de seguridad fundada en silicon Valley está buscando ingenieros con experiencia en ciberseguridad para ayudarles a construir y hacer realidad su misión contratan en todo el mundo y en remoto así que ya sabéis echadle un vistazo a su web monat.com y mandadles vuestro currículum a tierra de hackers@monat.commod.com perfecto pues ya sin atrasarnos más como siempre Gracias por estar ahí empezamos con las preguntas vamos con la primera querido Alexis te la pongo a ver qué opinas que sepáis que tengo yo todas las preguntas Alexis no así por lo menos tenemos del lado de Alexis que ni siquiera sabe las preguntas que han entrado y así lo tenemos contestando sobre sobre lo que se le ocurre sobre la marcha Hola amigos de tierra de hackers Les saluda Jorge felicitaros por sus 100 episodios y desearles Muchos éxitos Mi pregunta es Qué medidas debemos tomar con respecto al fishing y al malware tanto a nivel de usuario como de empresas y un saludo a toda la comunidad de Tierra de hacker saludos Bueno qué te parece Alexis Qué dices al respecto cuál es tu respuesta Saludos Jorge Saludos Muchas gracias por tu pregunta pues te diría Vete a nuestra web tierra de hackers.com y busca por etiquetas malware y fishing y ingeniería social no fuera bromas a ver tu pregunta es muy abarca muchos temas que no creo que podamos cubrir en los par de minutos que le podamos dedicar a la respuesta pero sobre fishing Pues a ver si utilizas en principio plataformas Las mayores plataformas digamos de email en plan Gmail o la de Microsoft y similares normalmente ya tienen filtros que intentan marcar le añaden etiquetas al principio del asunto no que pone externo o incluso aplicaciones de mail como la de mail de iPhone te marcan los remitentes como rojos y son si son digamos externos pero lo típico es antes de hacer clic en cualquier link Mira a ver realmente Cuál es la url Y si puedes y si tienes conocimientos pues lo suyo es que Bueno de hecho puedes copiar la URL en sistemas online como URL void.com o digamos wirelescann.io que esa esa también la cubrimos en un episodio o virus total por ejemplo también aunque donde lo suelo poner yo cuando no es tan tan evidente que es un phishing claro y también hay que tener cuidado porque si te equivocas y no es fishing Y ese esa URL tiene algo que es específico para ti podría pasar el tema de la count cover este que comentamos en el episodio de wrescant.io que no me acuerdo cuál era pero el problema era que cuando la gente los sistemas de seguridad que analizaban estas urls que un sistema analizaban estas urls digamos en tiempo real las enviaban urlscan.io Pues de alguna forma esto ya es arreglado pero la web scan.ayo mostraba creo que al menos las últimas 10 urls enviadas sin tener ni que está registrado en la web y esto lo utilizaban los cibercriminales para intentar hacer una County cover Pero bueno sobre todo fijarse en las urls antes de hacer clic y fijarse también en el en el lenguaje si te hace te incita te motiva de forma muy inminente a actuar de alguna forma en plan solo te quedan dos horas para para entrar en el sorteo de un viaje por el Caribe o yo que sé alguna historia así Pues ten mucho cuidado y sobre mauer Pues también no no te descargues cualquier archivo por ahí que te envíe algún conocido reciente y sobre Yo diría que yo diría que en eso volviendo un poco tú si lo tienes que ver Pues al igual que te copias y pegas la URL en un alien bold tengo un malware se me ha ido la cabeza en virus total con el malware pues lo siempre lo puedes ejecutar en una máquina virtual eso es una puedes tener una ahí lo ejecutas ahí sin conexión a internet y ya ves si tiene sentido o no Sí esa es la que iba a decir también lo mismo cuidado depende de si trabajas en empresas como has preguntado tema de usuario tema empresa si trabajas en una empresa y es un archivo de cierta confidencialidad y o incluso si porque si lo subes puedes estar exponiendo datos confidenciales a virus total y los usuarios este archivo se lo puedes descargar cualquier usuario incluso también le puedes decir a le puedes dar un tip digamos a los cibercriminales porque saben que alguien lo ha subido la otra forma es hacer un Hash de ese archivo y buscarlo en virus total y ver qué pasa vale siguiente pregunta esta nos llega por nuestra fantástica comunidad de discord por parte de Pepe bus que nos dice que le contemos Qué perfil

profesional trabaja en un shock en un blooting y en un reptil aquí entiendo que sabe perfectamente lo que es Pero cuál es el perfil cuál sería las cualidades entiendo yo así la pregunta que tiene una persona que trabaja en un shock en un Blue Team en un reptil Mira yo me encargo de la del reptil en la Sí porque pero por si no lo recordáis pues es básico básicamente el equipo que se dedica a poner a prueba las defensas digamos el equipo ofensivo nosotros cuando cuando trabajaba en Facebook y tal una de las cosas que mirábamos mucho en la entrevista era una parte súper importante y que más de las que más contaba y a veces la gente se cree que la parte técnica y tal era el hacker mindset la mentalidad de poder ponerte en el lugar del malo y con ello que te venga la creatividad Porque al fin y al cabo estás intentando testear sistemas que ya están a prueba de balas no Entonces tienes tú que tener creatividad ese hacker mindset para que se te ocurran cosas que los que los defendieron que los que implementaron defensas que los que desarrollaron el sistema no han pensado claro no te vale ir a lo fácil y lo ir a lo habitual incluso a lo que americanos le gusta llamarlo de aquello del loweng fruit tienes tú que tener esa creatividad ese hacker mindset para poder formar parte de un retín potente Y ser un operador pues eficaz Y nosotros hacíamos entrevistas tipo Oye pues tienes una máquina expendedora de la venta de qué manera la hackearías la típica pregunta si abierta solo para ver cómo se desarrolla el candidato yo creo que para un retimer el hacker mindset es esencial tú qué dices de un Blue Team que has tocado más Bloom que yo Sí a ver yo no soy blue timer pero ayuda Blue timers de hecho ahora hago funciones más de Purple digamos cuando porque yo de background soy timer como Martín Aunque ahora estoy ayudando un poco a los Blue teams diría que algo que es muy valioso en ese caso es el tema de Bueno pues fijarse en los detalles y utilizar temas por ejemplo como la Pirámide del dolor no esta pirámide of Paint el concepto este de los atacantes siempre tienen que hacer todas sus actividades bien porque si no no pueden conseguir su objetivo en cambio Si con que hagan un fallo los Blue timers pues podrían detectarlos Pues por esa parte diría que fijarse ser curioso en todos los digamos las tácticas las técnicas y procedimientos de los atacantes ya sea reptiles que te están ayudando o cibercriminales en Sí y enfocarse si se puede en las partes más altas de esta pirámide del dolor no sé pues enfocarse en temas de herramientas Por lo cual diría que un Blue timer a pesar de estar enfocado más en detección y prevención debería también conocer las herramientas reptiles o de los cibercriminales y muchas veces esta herramienta son herramientas que encontramos en github porque ya hemos visto que la mayoría de los apts utilizan mímicads sobre todo empaquet y muchas herramientas similares Así que para un Bloom yo diría ser curioso y toca un poquito de retín porque eso te va a servir mucho en tu en tu tarea como defensor efectivamente Al fin y al cabo para poder defenderte de los malos tienes que saber cómo actúan los malos y luego nos quedaría por aquí un shock que va más en torno al tema de respuesta de incidentes vuelvo a contestar porque si no nos alargamos mucho con solo una de las cualidades que yo destacaría que alguien que trabaja en un shock debe de tener que su capacidad analítica porque al final al cabo tienes que poder conectar muchos datapoints mucha información suelta y poder hacer que todo tenga sentido no esto es como como un detective que va cogiendo una pista por aquí ve una huella por allá encuentra un papelito con una frase críptica por aquí y Back recolectando cosas que por separado Pues no le dicen mucho pero cuando tiene esa capacidad analítica de coger todo y Connect the Dodge como decía Steve Jobs y de repente pues saca llega una conclusión o completa El puzzle no con todas las piezas sueltas Pues yo creo que eso para alguien que trabajamos en un shock es una una de las cualidades esenciales nos vamos con la siguiente pregunta y esto nos viene vamos a coger una de Instagram o mira otra de discord que tengo por aquí porque aparte la acabo de ver y me ha hecho gracias que yo realmente tampoco las he leído antes o sea que Iba contestando pero sin más esta nos viene por parte de katnet y nos dice alguna historia

vergonzosa que nos haya ocurrido durante nuestra carrera profesional ostras pues me pillas Así un poco algo vergonzoso Ah bueno yo puedo contar una A ver no es el fin del mundo pero sí que fue vergonzoso era cuando estaba no diré la empresa Pero bueno yo estaba más en la parte de product Security entonces pues algo de lo que hacía era Pues cuando nos llegaban reportes de backbountys y cosas así pues verificábamos no cuando alguien nos reportaba una vulnerabilidad verificábamos que eso era cierto porque muchas veces la verdad te entra mucha tontería de gente que quiere casi dinero rápido no y entró un reporte de que éramos vulnerables a un ataque básicamente a sistemas como era sistemas Windows que llevaba un the naial of service básicamente que alguien podía utilizar el típico exploit que te encuentras por ahí y había un fallo en nuestro servidores y que con solo básicamente poner la IP tiraba nuestro servidor y era un ataque que acababa de salir que alguien había escrito un exploit y a mí no se me ocurrió otra cosa que poner la ip de nuestro servidores y lanzar el exploit para ver si funcionaba claro yo en mi mente sabía que no iba a funcionar pero básicamente lo que hice es probar en producción si funcionaba un exploit que me tiraba toda producción en vez de montar un sistema de testing y Y entonces probarlo ahí no un sistema de laboratorio es que es como si alguien te viene por explicar de otra manera se me ocurre así sobre la marcha y te dice Oye mira que con esta pistola Parece ser que puedes matar a gente Mira a ver y voy yo cojo la pistola apunto a Alexis disparo y dice Ah pues sí pues sí que se puede matar a gente en vez de probarlo con un muñeco y recuerdo que mandé un email yo en plan todo tal Oye Mirad a mi equipo Oye Mirad que he probado esto en estos rangos de IP y no funciona pero me insiste el tío en que sí que no sé qué Y claro me llevo una respuesta del ciso y me dice espera acabas de probar esto en producción y yo Ups fue ahí como cuando me di cuenta tío la verdad muy lamentable por mi parte lección aprendida me cayó mucho puteo mucho puteo porque la verdad queremos un equipo muy muy Guay nos llevábamos todos muy bien a ver está buena es a ver puede pasar Supongo la mía para no enrollarme mucho fue algo algo que me he encontrado que le ha pasado a otras personas estás haciendo en un digamos en un Security para una empresa y tienes ahí unas máquinas que tienes que escanear y lanzas un nene map y las máquinas Son de hace mucho tiempo en plan Windows yo que sé no era Windows 98 eran Windows server pero no me acuerdo qué versión era esto ya hace años 12 15 años no me acuerdo cuánto Total que y esto era una empresa sin decir nombres una empresa que fabrica vehículos automóviles Total que estamos haciendo el escaneo en lanzando enemap y Aparentemente en esta cadena de producción deja se paran los sistemas los las manos robóticas los brazos robóticos y todo eso porque Aparentemente habíamos tumbado el servidor Windows la actividad Electric que se utiliza como dns Y estos sistemas que no tienen que utilizar dns porque es una plataforma estática de por sí un entorno Industrial no vas añadiendo y quitando sistemas sabes los que tienes Por lo cual no hace falta que usen dns Pero bueno Estaba utilizando dns y pues nada dejamos de dejar esa empresa dejó de producir durante dos horas porque estamos escaneando puertos de los sistemas en en lo que el digamos teníamos permiso para escanear y nos dijeron eh parar un poco esto hasta que se recupere Porque ahora mismo no estamos produciendo y nada también fue fue un poco sonrojoso digamos sonrojoso Sí bueno Tú lo has dicho como tono Oye podéis parar un poquito esto seguro que utilizaron otro tono y otras palabras pero pero sí todo el mundo tiene tiene anécdotas muy buena pregunta vamos con la siguiente esta de audio nos llega por Twitter por parte de Francisco Javier Ahí va Qué tal equipo de tierra de hackers Les saluda Francisco Fuentes desde México y muchas felicidades por estos 100 episodios soy un fiel seguidor de cada uno de sus podcast me gustaría que hablaran de la accesibilidad Y si la accesibilidad es o no parte fundamental de la ciberseguridad soy usuario de tecnologías de asistencia y la accesibilidad juega un papel fundamental para mí y para personas con discapacidad muchos

dicen que la accesibilidad hace que la ciberseguridad esté un poco vulnerable pero me gustaría conocer su opinión Muchas gracias y saludos Muy bien pues este usuario es una pregunta realmente curiosa porque nos dice que él es un usuario que utiliza sistemas de accesibilidad para recordárselo a los usuarios Pues gente ciega sordos o con algún tipo de otra discapacidad Pues los sistemas operativos hoy en día tienen sistemas de accesibilidad para hacerle fácil utilizar tecnología lo cual es algo fantástico y este querido oyente de tierra de hackers Pues nos dice que no solo él es un usuario y trabajan esos temas sino que claro es cierto que a veces esto se ha usado para abusarlo como digamos una vía para temas de explotar un dispositivo y que como como encaja todo eso en la ciberseguridad Bueno yo por un lado nunca claro como yo no requiero de esa tecnología Pues no sé si las herramientas de pen testi por ejemplo las que utilizamos por los hackers suelen integrar sistemas de accesibilidad la verdad es que deberían o bueno en general muchas veces pues como es el propio sistema operativo pues ya lo aprovecha cualquier herramienta que lo tengas instalado pero por ese lado claro no tendría mucho que decir pero sí que es curiosa esta pregunta por el tema que yo recuerdo de varios sistemas de por temas de accesibilidad por ejemplo con Siri que se podía hacer muchas cosas para abusar sistemas de acceso aplicaciones o resetear contraseñas yo mismo hice un tema de ransonville utilizando esos sistemas tú Alguna vez has explotado algo abusando un sistema de accesibilidad Alexis no lo he explotado pero voy a referir a nuestros oyentes al episodio 72 en el que cubrimos el tema de Siri Spy que era aquella vulnerabilidad Bueno más que vulnerabilidad es una ficha no como siempre se dice que abusa abusó un investigador de seguridad para poder escuchar de forma remota lo que estaba sucediendo cerca de los airpods porque se conectaban vía Bluetooth y por temas así de asistencia pues se podían capturar conversaciones de forma remota a través de a través de esto es es una es una funcionalidad que se llama Life Listen que bueno está implementada para para ayudar a personas que necesitan esa ayuda Qué bueno qué bueno pues nada nos vamos con la siguiente pregunta venga pongo pongo otra de Twitter que nos llegó de DJ muela otro oyente que nos Comenta mucho además Y esta es su pregunta ahora amigo de tierra de hackers soy un oyente vuestro Me llamo David o os escucho desde elche y la pregunta para este Centenario Felicidades Felicidades por el centenario es Alexis tú que echas de menos laboralmente hablando y personalmente de España y la pregunta para Martín es lo mismo que echas de menos laboralmente y personalmente de Estados Unidos vale venga a seguir así chicos un abrazo Qué buena eh Gracias Dj muela por tu pregunta decir que sé que se va a escuchar un poco bajo los audios he tenido que montar aquí un pollo para poder hacer que se escuche directamente el audio que me escucha Alexis vamos me he convertido en un ingeniero de sonido Pero bueno volviendo a la pregunta de DJ muela Alexis que echas de menos de España aparte del pantumaca y él fue el jamón ibérico pero no sé haber ha dicho dos temas y personal también ha dicho personal A ver laboralmente no lo sé yo solo tuve experiencia y de consultoría en deloitte lo que igual lo relacioné lo relacionaría con el tema laboral es la capacidad que te permitía depende que proyecto viajar gracias a tu trabajo por Europa que es digamos un continente igual de grande o bueno Más o menos que Estados Unidos No aquí en cambio cuando he tenido que viajar que he viajado mucho vamos he llegado a tener más de 150.000 millas en alguna aerolínea en algún año pues viajaba pero por Estados Unidos que sin desmerecer pero más o menos se nota como todo igual no no tiene la riqueza digamos de la diversidad cultural de Europa y eso si lo combinas con si tienes que viajar por trabajo y ahora vas a no sé a Bélgica Ahora vas a Francia aquí allá Pues un poco que mejora no la estancia y tu trabajo sobre el tema personal bueno Martín ya lo ha dicho no el tema del jamón un poco la cultura Los Americanos y tú lo puedes confirmar o no Martín pero van mucho al tema profesional no el tema de socializarse lo hacen lo hacen también pero no es de la misma forma

la que veo yo que lo hacemos en España no sé si diría que en España es mejor Pero yo creo que en España digamos somos más abiertos No aquí diferencia es en plan más igual por interés o por conexiones o es un poco diferente Sí sí buena respuesta a mí me lo ha puesto un poco difícil Dj muela porque Claro que he hecho yo de menos desde España en bueno no perdón al revés te lo había puesto difícil a ti porque laboralmente echar de menos algo en España trabajando en Estados Unidos complicado yo lo tengo fácil a ver qué echo de menos el sueldo esa es una clarísima luego la proyección de carrera yo a ver realmente no es mi situación personal porque yo ahora pues acabo de montar mi propia empresa y hago temas de consultoría entonces Bueno un poco trabajo para mí mismo No pero de cuando recuerdo que trabaje trabajaba en España antes de irme a Estados Unidos Pues claro allí sobre todo pues yo que estaba en silicon Valley Pues claro la proyección de carrera tú vas allí todas las empresas si no son las más grandes de todas un Google un Facebook un Apple o un Twitter un tal pues es la startup del momento con gente súper inteligente está rodeado de Auténticos cracks da igual si estás en Data minein Inteligencia artificial hacking software ingeniering da igual vas a estar rodeado de Auténticos cracks de todo el mundo no solo americanos o sea Allí está la creación de la creme en España es brutal El Talento que hay igual que en Latinoamérica igual que cualquier otro lado pero Allí es donde se concentra todo entonces echo de menos eso pues la digamos el estar rodeado de los gurús de cualquier campo y el sueldo y luego a nivel personal Pues mira el Branch tío los ex benedict y los breakfes burritos Qué quieres que te diga todavía no lo he encontrado aquí en Barcelona Alexis Qué pasa hace Mira idea de negocio que alguien Monte hay algunos de Branch que sí que no sé qué pero un break es burrito el de El de huevos el de tal aún no lo he encontrado ex benedict Sí pero va mediocres diría yo Ok pues nada Mira idea de negocio implementemos los trans los de tierra de hackers Branch bueno pregunta que nos llega Por linkedin de Juan Eduardo Álvarez Y nos dice Cuál es la ruta de aprendizaje básica que se debe tomar en cuanto al lenguajes y manejo de ciertos softwares no se dice y que le gusta mucho el podcast nos saluda desde Argentina bueno esta pregunta va a ser bastante recurrente en general O sea que la voy a hacer ahí un compendio de todas en las que básicamente viene a ser como la típica pregunta no cómo cómo se convierte uno en hacker Cómo empiezan esto Cuál es el primer paso y todos hemos estado ahí como estudiantes nos todo empieza por la emoción que es donde entra tierra de hackers nosotros no solo queremos tener a la gente informada sino atraer a la gente a este mundo y por tanto tenemos que dar una respuesta a ese segundo paso el primero es que hayan descubierto un podcast que les anime y les emocione el entrar en la ciberseguridad ahora hay que dar respuesta a cuáles son esos primeros pasos y aquí concretamente Bueno nos dice para hacerla más concreta esta pregunta lenguajes de programación y qué tipos de aplicaciones O sea que vamos a contestar primero a eso dime un lenguaje de programación para hacer la pregunta corta y una aplicación que Juan Eduardo puede empezar a toquetear vale como no me has dicho mi nombre digo no sé si vas a poner otro audio o tal Sí pues a ver la pregunta habría que estudiarla sin sin pararme mucho en ello pero el tema es plantéate que qué quieres hacer en tu vida laboral digamos porque Depende lo que quieras hacer Igual te interesa más aprender un lenguaje de programación de scripting o cualquier otro tema en plan me interesa aprender python o Java o quiero ir más assembly porque quiero desarrollar exploits o esto O yo voy a hacer un ziphud mini con Bach y temas similares y ya me vale entonces eso sería primero lo que te tienes que plantear hay stack overflow si no me equivoco publica cada año una guía un estudio de todos los lenguajes de programación y las posiciones que te permite llegar cada uno de esos en plan si estudias r pues puedes hacer un plan tema de similares o escala y también publican los salarios asociados obviamente esto creo que es todo en plan Estados Unidos pero bueno Más o menos se puede se puede extrapolar no Argentina Pues igual la escala de lenguajes de la

importancia Pues sería la misma Solo que los salarios sabría que bueno modificarlos no pues eso sería un tema pero no sé yo creo que uno de los más famosos todavía de momento Bueno yo diría python no pero es que javascript creo que esta es de los top 3 y sería uno de los que igual se podría aprender de forma más fácil básicamente porque yo siempre lo digo en javascript está en toda tu vida o sea lo tienes en navegadores que lo utilizas cada día Ya sea en tu ordenador o en tu teléfono móvil y se utiliza tanto en el Front en es decir la página que estás viendo que se carga como en el backen porque hoy en día no huye es una plataforma de backen basada en javas Script que se utiliza mucho así que te recomendaría mirar por ahí no sé para aprender Pues el tema es meterle horas estar pensar alguna idea que te haga gracia implementarla y si no pues lo que puedes hacer también es participar en en competiciones por ejemplo páginas como Live lit creo que se llama o hay algunas de estas o si no en stack overflow Hay comunidades de cualquier lenguaje que elijas y bueno hacerte digamos socio o añadirte alguna de ellas sí yo voy a contestar concretamente como decía a su pregunta de un software y un lenguaje de programación ya que Alexis ya se extendió en la parte de cómo empezar lenguaje de programación ya que has dicho python yo digo Go Por qué desde el punto Alexis lo explicó muy bien Depende de lo que quieras hacer pero si quieres temas de hacking y de todo esto sobre todo en temas de retín Y así pues python sería uno pero Go para escribir malware es muy bueno porque se puede correr en todas las plataformas Entonces eso para el lenguaje de programación y una aplicación Pues mira burp Suite que te lo puedes bajar gratis además el Community Edition y es para hacer temas de web que entiendas un poco Cómo funcionan los navegadores cómo funciona una página web empieces a hacer análisis de tráfico sencillo con el protocolo http así que por un lado como software y Go como lenguaje de programación nos vamos a la siguiente Alexis y viene por parte de Rocky en nuestra comunidad de discord y dice tenéis alguna bibliografía que nos puede recomendar un tipo de programa de certificaciones estudios o estrategia para seguirnos preparando en esto de la seguridad de la información y nos da saludos desde México así que qué recomendarías Alexis a ver claro todo depende Supongo que está abierto en inglés no porque en español Las hay hay muchos libros Y tal Pero igual son más reducidos a ver yo he bibliografía no sé si se refiere a un libro en concreto yo creo que los libros por si están bien en plan como temas de referencia pero se estancan y la pregunta dice alguna bibliografía que nos puede recomendar dice un tipo un tipo un tipo programa de certificaciones quiero entender que la bibliografía es para sacarse certificaciones estudios o estrategia para sí macho Rocky te has liado aquí preguntándolos no sé si no pregunto por un lado bibliografía y por otro lado certificaciones o bibliografía para certificaciones bueno Alexis Qué te parece Mira recomiendas un libro en general y luego un tipo de certificación Y qué libro utilizar para ello así Le damos una respuesta completa es que sería difícil a ver hay una plataforma se me ocurre un libro que así te doy tiempo para pensar uno que me recomendaron a mí para entrevistas en ciberseguridad sobre todo muy centrado en tema navegadores y web que es de tangle web un libro muy completo muy a fondo sobre javascript sobre cómo funciona el navegadores es brutal se llama de tangle web que es como la web enrollada o la web lios es un libro así naranja muy muy bueno muy técnico pero muy fácil de entender porque al fin al cabo pues hablamos de navegadores de javascript de html muy buen libro vas a entender todos los eloas top 10 pues ahí te lo explica de lujo sí por esas también como digo estos libros es también para para aprender las bases pero luego como el estándar de los navegadores evoluciona muy rápido pero bueno el de web application hackers handbook también es uno bastante interesante que recomendaría y luego de nuevo volviendo de forma similar al tema de la pregunta sobre los lenguajes de programación depende cuál sea tu interés si te interesa más el tema de web te interesa más el tema de no sé de explotación o carhaking o temas similares pues últimamente hay libros para todas estas áreas en temas de

seguridad incluso hay un libro ahora nuevo hace poco que se llama hacking apis apis que me ha parecido bastante interesante que se puede hacer un libro únicamente de hackear apis Sí sí sí lo he visto lo visto también me sorprendió de hecho yo he visto uno que era un libro sobre bypasses autenticación de doble factor un libro solo en una conferencia Y sí que he encontrado por ahí he encontrado lo típico que te puede estar Pero había como truquitos y tal eh me pareció muy bueno tío se puede hacer y como dices tú hay libros para todo hay libros para temas muy específicos Y luego tiene vídeos de YouTube también cursos online tienes de todo yo si tuviese que decir una certificación para saltar a la parte de certificación como bien Dice Alexis depende Pero yo te digo pareces tú el Gallego eh Alexis que estás haciendo tú todo lo de depende Pero y el gallo que soy yo pero yo diría lo scp tío si te gusta el tema de hacking es una certificación de las menos caras y va a decir barata pero de las menos caras que más te aporta no solo eso sino que no es a nivel teórico tiene parte teórica pero tienes que demostrar nivel práctico que has aprendido las cosas no solo eso sino que hay cosas que tienes que aprender por tu cuenta es decir te da la base por tanto es una certificación que si te la sacas te la has merecido porque tenemos que buscarte la vida es muy práctica tienes 24 horas para pasar el examen a mí de verdad me parece una certificación muy top Sí estoy de acuerdo con lo que dice Martín además de ser interesante y no de las más caras aunque le han incrementado el precio un poquito es una de las más reconocidas así que te recomendaría esa hay otras similares pero no están tan reconocidas como no sé por ejemplo Hack de box Ahora tiene alguna depenthestero backbounty Depende lo que te interese si te interesa el backgrounty que también es una un área en la que se gana bastante si eres bueno y le dedicas horas Pues igual eso te ayuda a entrar en el temilla del backbounty y ponerte al día en Europa algo que es interesante es que los scp es igual más a nivel global pero en Europa la que se una también que es muy equivalente es el crest de la certificación crees que es es muy está muy muy bien vista en como digo en Europa y sobre todo en Inglaterra que según dicen es también tema similar o scp muy bien Pues venga nos vamos con una por audio y esta nos viene a través de Instagram de nuestro amigo David barajona Bueno amigos de tierra de hackers les habla David Barahona desde Costa Rica Saludos esperando tenerlos por acá pronto me gustaría saber si nos pueden dar recomendaciones a las personas que queremos este incursionar en esto de la ciberseguridad tomando en cuenta ahora todas las plataformas que hay este para educarse al respecto y para este entrenarse también entonces este con base a esto Me gustaría saber que qué nos recomiendan Cómo podemos empezar qué pasos podemos seguir para no este estropear el camino desde el principio sino incursionar como tiene que ser en esto de la ciberseguridad Muchas gracias saludos pues una pregunta muy relacionada con la anterior O sea que en parte ya la hemos contestado pero creo que hablaba de plataformas en concreto qué plataforma recomiendas Alexis yo la que me parece bastante interesante jugosa divertida es Hack de box sobre todo porque es gratis tiene máquinas que son divertidas y las puedes hacer digamos en solitario o no sé colaborando con alguien en plan Oye vamos a aprender los dos juntos Y vamos a resolver esta máquina o este laboratorio también los laboratorios creo que son pagando algo pero bueno el Hack de box lo que tiene también es que hay una persona famosa que se llama ipseck que tiene su página ipseck.rocs que puedes ir ahí y buscar en plan Quiero aprender temas de secuela injection pues pone secuela injection y te salen todas las los vídeos que publica en YouTube sobreexplotación o abuso de sicola injection en máquinas en Hack de box y te va directamente al trozo a la parte en su vídeo en la que muestra como abusar el tema de secuela injection hay otras plataformas también similares como tryhack me que también son interesantes esas más de si no me equivoco descargarse una máquina virtual y correrla en local a diferencia del hack debox que se corre en una nube Pero bueno esas dos yo diría para empezar son bastante interesantes el tema también que igual si te gusta competir

Pues hay un Dash por ahí no que puedes competir en plan con tus colegas o con tu equipo de trabajo también y decir Oye mira Cuántos puntos tengo mira cuántas máquinas comprometido y Bueno ahí divertirse Sí muy buena yo añadiría eso bueno primero ipseck es un tío americano vamos a tirar aquí a los que hablan nuestro idioma hablo español y de hecho en España tenemos a las chicas de securitys que son unas cracks y hacen mucho vídeo en Twitch de resolver máquinas y también estás habitar Por supuesto que hace eso Entonces es correcto si lo queréis en español seguro que por latino saludito y seguro que por latinoamérica Pues también tenemos a youtubers que hacen temas de estos y luego diría para Añadir a ti pues plataformas es que están pensando por contestar un poco más personal Cómo aprendí yo hacking pues yo realmente no utilicé ninguna plataforma Para mí fueron más backbountys O sea lo que iba aprendiendo me metía en un hacker One en un background y fue como fui aprendiendo hackeando de hecho sistemas reales y además puedes ganar dinerito que está muy Guay no es que una sea mejor que la otra es más que las máquinas de un try hack ni de un Hack de box están específicamente diseñadas para ser hackeadas mientras que un backbounty Pues claro Va sobre un sistema real pero a mí por ejemplo me ayudó para ir encontrando vulnerabilidades y además me pagaron por tanto como plataforma los programas de backgrounty también están muy bien para para ir aprendiendo sí correcto estoy de acuerdo y sobre todo los write Apps las soluciones si te ves que no no tienes conocimiento para resolver algo yo a veces he aprendido un montón leyéndome los writaps viendo los vídeos también pero leyéndote en estas hacker one o similares cuando los ponen ahí también una polaridad real es muy interesante ver como como lo han explotado Sí Sí aparte hay gente que te pone unos wright Ups súper detallados y te puedes escribir al suscribir al rss y te va llegando y es fantástico Muy bueno muy bueno ese detalle y yo incluso añadiría también los subraitaps de ctfs te puedes coger un challenge lo intentas bueno pues no me ha salido pum Pues venga me voy a leer el Cómo se resolvía y luego te vas al siguiente Y por último diré que para temas de web y tal pues tenemos el web el Google que es una especie de Hack de box pero centrado en temas web o sea una página web vulnerable o está la de vulnerball Mobile up o algo así que es una una aplicación de Android que está tiene muchos agujeros de seguridad para que vayas aprendiendo O sea hay muchas plataformas así que digo para cuando el web manchego has dicho el webger Alguien tiene que hacer hay una versión española tío es verdad es verdad pero no yo haría el web tetilla que soy de soy Gallego tío es el queso que tenemos allí que eso de tetilla está cojonudo con con membrillo tío aquí haciendo publicidad de Galicia Cómo no un saludito a Estrella Galicia a ver si nos patrocinan Bueno vamos con el siguiente siguiente audio venga va Hola tierra de hackers este aprovecho para hacer una pequeña pregunta desde Buenos Aires uno cuando van a venir esa pregunta no estaba previsto pero los esperamos por acá con ansias de poder verlos y compartir un rato y dos la pregunta real es Qué recomiendan ustedes para evitar que la computadora sea Windows Mac lo que fuese Linux termine siendo una computadora zombie de estas que utilizan en los ataques de de s un abrazo grande y felicidades por el episodio número 100 y el logrado Muchísimas gracias Carlos desde Argentina bueno allí tenéis una conferencia súper top un saludito allí a la gente de la ecoparty así que ya iremos por allí Alexis qué lo comentas a Carlos Cómo evitamos que nuestra máquina forme parte de una red de Bots que se utilice para el mal desconectar la internet y apagarla el primer contenedor que tengas al lado de tu casa vas la tiras y ya está Carlos no es tan complicado cómprate un ábaco y una libretita y un boli Y hoy vas haciendo No pues a ver tema contraseñas no un buen gestor de contraseñas te diría que lo tuvieras a mano tanto en tu portátil ordenadores sobremesa móvil y que utilices contraseñas fuertes digamos complejas y que actives en todos los sitios que te permitan el doble factor y que también tengas si puedes activar las actualizaciones automáticas de todos tus dispositivos pues mucho mejor que mejor

o si no Si no lo puedes hacer de algún por algún motivo o no se actualizan por algún motivo estate al corriente de no sé si tienes un mac o s pues estaría al corriente de los parches que van publicando y en cuanto salgan pues intenta instalarlos y aparte de eso pues obviamente no expongas tus sistemas a internet y bueno tampoco sé que muchos Gamers no que a veces tienen que abrir puertos a internet no para conectarse a ciertos servidores Pues si es tu caso pues vigila ver Qué puertos abres al exterior y en la medida de lo posible No abras demasiados Pues yo diciendo siguiendo un poco el papel de antes de que Alexis da como un poco la respuesta genérica y varios puntos yo solo voy a decir una y me ha gustado mucho lo que has dicho Alexis voy a decir revisa tu router que no esté expuesto el panel de administración de manera externa y que cambiarle los credenciales porque ya os hemos contado muchas veces que con shodam es muy fácil acceder a eso Y a partir de que alguien tiene desde fuera acceso a tu red interna Ahí es donde donde empiezan los problemas no solo tu router sino tu red inalámbrica a mí me ha pasado alguna vez que un familiar si lo digo breve me dijo Oye Alexis mi red me da un poco lenta no sé por qué o qué deja de mirarlo entró en el router miro y digo Oye estos clientes por dhcp no que están aquí conectados Este es tu teléfono este es tu móvil este el de tu hijo este no sé qué Y este quién es Pues no sé me puse a investigar y dice hice maní in the middle a esa conexión pude capturar Las Cookies de Facebook las utilicé para loguearme en la cuenta de esa persona y era era otra persona Obviamente que no conocía mi familiar y era uno de los vecinos que se había conectado a su WiFi porque Supongo que habría quedado la contraseña Así que eso también lo puedes ir monitoreando que nadie se te conecte así de vez en cuando cambiar la contraseña de la WiFi pero sí es un tema interesante que me ha venido a la mente Qué bueno cuando dije me gusta mucho utilizar como persona x el nombre de Manolo no pero es que el otro día estaba con un amigo de Perú y tío que tiene la gente en Latinoamérica o por lo menos en Perú de cuando quieren hablar de un español dicen venancio tío yo me partía de risas en plan Sí porque venancio tal como si fuera un hombre común en España que vamos venancio existían el siglo XVIII y era un benedictino de una abadía macho es el típico nombre de monje pero si decía sí porque los chistes allí los hacemos de venancio tío joder hazlos de Manolo no de venancio bueno en fin nos vamos con la siguiente con la siguiente pregunta de Es que quiero darle un poco de prisa aquí que vamos por el minuto 54 y queremos ahí mantener a los oyentes es que si ya ya sabéis Alexis y yo aquí nos le tenemos rollo para para dar y de sobra discord reddef nos dice algún delito ya prescrito que hayáis realizado sin querer bueno Me gusta esto de puntualizar sin querer durante vuestro aprendizaje Alexis contestas tú primero pero delito que significa que te hayan metido en prisión o algo o porque igual has comido no Bueno claro pero tú puedes cometer un delito y que no te hayan pillado que me imagino que es a lo que se refiere aquí red yo en mi caso el primero que me viene a la cabeza supo Bueno vamos a decir un amigo mío me contó que cuando estaba aprendiendo claro esto era en los años 90 Pues sí supongo que en ese momento era un delito pues utilizar troyanos para robar las contraseñas de internet del daiala app en su momento yo utilizabas fue como aprendí lo que era una IP hacía un barrido y de repente le podía sacar las contraseñas a la gente de televisión que era un poco lo que se utilizaba de aquella para conectarse a internet y con eso robaba los credenciales y te conectabas a un número creo que era un 902 o algo así solo pagas la llamada no tenía que pagar el propio servicio a internet tú Alexis pensandolo así el comentario de antes que robe la Cookie de Facebook de esa persona no sé si es muy muy legal eso no pero eso no no ha prescrito tío y claro aquí esto nos dice la Cuqui ya no es válida así que ya no yo creo que similar a lo tuyo un amigo me contó que en los años 90 te conectabas al irc y en esa época ahora la ip es virtualizada no digamos pero en aquella época podéis hacer un whois si no y veías la ip de cualquier nickname en el Canal de irc en el que estabas entonces podrías hacer lo típico el ping

Of Dead este Blue screen of Death o también directamente en aquella época los routers o tus ordenadores están conectados no sé si os acordáis están conectados directamente a internet y el puerto 445 y similares Pues también estaba abierto y podéis hacer un simple una simple conexión smv Samba a esos ordenadores Sabiendo la IP y ver si tenía recursos compartidos pues podías Ver todos sus documentos y copiartelos o no o decirle Oye no expongas esto a internet muy buena Pues mira en esa línea también por discord nos pregunta Juan gandalf para los amigos eso es su nombre nos dice si nos han ofrecido alguna vez hacer algo poco ético o ilegal y si es así que era no igual que no sé igual que no tengo no tengo cara de que vaya a aceptar nada de esa índole eres muy buen niño tienes cara de buen niño no no igual eh Sí no la verdad es que en principio no a mí a ver directamente no indirectamente estaba convencido de que sí me explico yo he presentado varias herramientas que he escrito pues para hackear buzones de voz Pues con Apple el tema de reversar protocolos y dejar el micrófono abierto cosas así que presentaban el pasado y ha habido herramientas que yo las las publiqué un poco captadas no digamos limitadas para que no fuese fácil pues usarla y ya está y me llegan aún a día de hoy muchos correos electrónicos se oye dame el código me lo vende me lo vende está O sea me han ofrecido hasta pasta por por el tal que tampoco es que yo no quiero que no quiero que esto suene a que yo tengo aquí un cero d y que no lo quiero vender y no no alguien con un poco de conocimiento y que se vea mi charla vamos lo implementa En una tarde porque tampoco quitaba mucho del programa pero vamos que era evidente por los emails por la manera de escribir el lenguaje pues mucho era se notaba que era pues para luego scans o para hackear y cuentas y cosas así entonces pues sí me han ofrecido pasta colaboraciones y cosas así pero bueno directamente algo ilegal de Oye hackea este porque lo queremos Matar o algo así no de momento no y que nadie se aventure porque le voy a decir que no Oye pero si no ahora que lo pienso estamos mintiendo los dos hemos recibido un montón de estas peticiones en plan Oye me puedes ayudar a hackear esta cuenta de Hotmail Ah bueno Sí claro es que macho ya ni las cuento muchísima gente sobre todo por Instagram es Oye quiero hay algunos que que van y te vienen con no no la cuenta es mía he perdido acceso tal Y ves que es un tío y la cuenta es no es una tía y la cuenta es Manolo y la cuenta esencia justo venancio 69 pues vaya jander más raro para ser una tía pero no muchísimo de eso de hecho por un lado a mí me quedan las ganas de trolear de decirles Sí sí dime qué cuenta porque hay veces que son directos y dice creo que mi novio o mi novia porque es independiente si es tío tía nos pasa con los dos Me está poniendo los cuernos y solo quiero ver sus redes sociales y tal sabes a veces me dan ganas de pedirle el handle Sí sí yo te la hackeo y luego escribirle directamente con una captura de pantalla a esa persona diciéndole Oye deja está a tu novio o novia porque es una persona con muchos celos que puede haber razones para para que tenga esa preocupación pero vamos que esa relación no va a ningún lado si si tu solución es intentar comprometer una cuenta así Que supongo que esa la respuesta buena Qué te parece si nos vamos con otro audio venga me voy otra vez a Instagram a ver qué tenemos por aquí Hola Qué tal mi nombre es Raúl me gustaría felicitaros por haber llegado al episodio número 100 de verdad que os lo merecéis Como nadie y no tengo palabras para agradecerlo no me pierdo ningún capítulo conocí a Martín por su herramienta de email too for number por un vídeo rarísimo de YouTube No me preguntes cómo llegué cuando descubrí que era español ya me dirigía al blog que vi que tenían o sea el podcast que teníais Y desde ese momento pues aquí sigo y yo Actualmente estoy estudiando desarrollo web y todo nace por la por la curiosidad que me empezó a dar el tema de las ciberseguridad a mí en mi tema Favorito pero a la hora de trabajar Me gustaría enfocarme al desarrollo web pero vaya que me encanta la comunidad que se ha creado con vuestro podcast me encanta el contenido que hacéis se hace súper ameno Y de verdad que no tengo palabras para agradeceros el esfuerzo que hacéis por subir los podcast y lo que no es lo

que me entretiene y lo bien Cómo te va desde la situación Estos son las cosas que las horas que invertimos Alexis y yo hace que todo valga la pena de verdad Muchísimas gracias Raúl por esas palabras nos alegra tanto que le encuentres valor al podcast muchísimas gracias de verdad y su pregunta nos dice alguna vez habéis realizado alguna compra en la Deep web o tenéis experiencia trabajando navegando en este submundo Sí luego nos preguntó un par de cosas más Pero supongo que la respuesta es sí Alexis Alguna vez has metido la Deep web y has comprado cositas primero de todo muchas gracias por los comentarios Raúl y segundo el tema de la Deep web últimamente no tanto pero antes cuando me dedicaba un poco a hacer más inteligencia de amenazas tuve para algún cliente que otro tuve que mirar Qué información Se barajaba en la Deep web y hacerle lo que llamamos un saber profile y sí que encontré temillas como tarjetas de crédito que se Estaban vendiendo de esa empresa información sobre poco de doxing de los empleados y temas similares pero nada en plan terrorismo o temas similares era eso sobre la de comprar no he tenido que llegar a tanto pero Oye si el cliente este me lo ha dicho Oye tienes que hacerte pasar como alguien de mi empresa y comprar algo pues lo hubiera hecho pero no en otro caso yo en mi caso no he comprado en plan si la pregunta iba por el tema de cosas ilegales yo que sé desde documentación falsa drogas y cosas de estas o acceso ordenadores no he comprado nada de eso pero sí para operaciones de retín he montado mi propia mi propia web en la Deep web digamos un punto onion para emular un ataque de ransomware era donde poníamos como los datos Y tal Y bueno en general sí que lo he utilizado pues ayudando a ciertas personas en algún temilla de terrorismo y tal porque es donde se suele publicar no por lo el anonimato que te da pero sí sí la verdad es un submundo Por así decirlo muy interesante tampoco es nada del otro mundo a veces exagero un poquillo y se da como esa imagen de que meterse ahí pues es como un peligro y tal no es como Navegar en internet donde Pues hay algunas páginas que son más chungas tampoco tiene mucho más nos pregunta también Raúl Cuántas veces nos hemos puesto el sombrero negro y alguna anécdota que se pueda contar Bueno yo creo que hemos cubierto ya las anécdotas y el sombrero negro Si entendemos por la parte ilegal Bueno yo creo que eso lo dejamos cubierto con la con la respuesta anterior sobre el tema de si hemos cometido alguna ilegalidad que ya prescrito ahí ya había sombrero negro Muchas gracias Raúl lo intentamos poner cada verano si podemos no yendo a Las Vegas pero a las blancas sigo es para para hacer el blentín no Para pasar desapercibido claro y entre tanto tío con sombrero negro pues este no vas a ir con uno blanco justo tenemos otra pregunta por Instagram esta vez de Álex callazo que nos dice Cuál fue la vulnerabilidad más descarada que habéis encontrado y por descarado se refiere a por ejemplo tipo or one one Algo súper básico Alexis descarada el tema de que es muy básica que es muy me imagino una vulnerabilidad en plan macho como tienes esto aquí si quieres mientras la piensas puedo yo contestando a una en concreto A ver no es que fuera una vulnerabilidad crítica Pero me gusta en plan descarada porque me pagaron mucho dinero y yo que sé a lo mejor tarde 10 minutos en encontrarla resulta que hay una aerolínea bueno esto esto creo que es público en hacker One Así que yo lo digo sí era Era público es una tontería la verdad Porque de eso va la pregunta United Airlines tiene un Back un programa de backbounty donde te dan millas para poder viajar si encuentras vulnerabilidades pues yo en plan estaba haciendo checking para un vuelo digo déjame aquí mirar un poquito inspeccionar el tráfico en el navegador y tal a ver si encuentro algo de algo básico y lo puedo reportar no antes de antes de pillar el vuelo y me di cuenta que como todas las aerolíneas cuando te email de hacer el cheque y no tú le das al botón y te Abre directamente el navegador desde tu correo y ya estás digamos logueado donde tú puedes elegir tu asiento puedes hacer chequen y todo eso y ahí hay información personal tuya a veces hay datos de tu pasaporte y tal No ese email que después de comprar un vuelo te llega y te dice Oye Haz checking y tal vale esto es como un

estándar las aerolíneas para poder hacer check-in cuando tú no tienes una cuenta en esa aerolínea lo que te pide es el localizador de tu reserva y tu apellido No lo típico te das en la web localizador y apellido y cuando te llega un correo de esos realmente el botoncito al que le das es un enlace que ya contiene en el propio enlace en el propio link esas dos piezas de información el localizador y el apellido que lo podrías entender como un nombre de usuario y contraseña el apellido siendo el nombre de usuario y la contraseña el localizador Pues bien al estar en el en la propia dirección en la URL eso puede filtrarse y yo pensé esto puede filtrarse en una cabecera que existe en el protocolo http que es el referer el referer header y digo con que haya en la propia página a donde me lleva esto un enlace a otro dominio pues ya se estaría filtrando si no lo hicieron bien y me fijé en el lateral una vez el tú vas a hacer el checking tienes la típica ventanita de necesitas ayuda pues ese necesitas ayuda lo habían subcontratado y era Pues un Zelda es con No me acuerdo qué servicio pero claro al darle un clic ahí Se está enviando desde que URL vienes y la URL de la que vienes contiene tu nombre usuario y contraseña por tanto vulnerabilidad en la que se están filtrando tu apellido y el localizador a un ser Party a un servicio que no debería tenerlo y con el cual ellos pueden ahora meterse en tu digamos en toda tu información de la aerolínea que contiene tu pasaporte nombre apellidos dirección teléfono pueden anularte el vuelo cambiarte los asientos y hacer todo lo que quieras me llevo 10 minutos y creo que me dieron en millas algo así como como 5.000 euros o algo así muy buena esa Martín yo la verdad no tengo ninguna publicada Pero de alguna que he encontrado durante algún asesme hace años puedo decir que encontré un kiosco de estos es un ordenador que tiene muchas funcionalidades limitadas restringidas en este caso era un Linux y no permitía acceso a internet solo a los sistemas de esta empresa que estaban hospedados en un proveedor de nube tenía disponible en el navegador firefox y no tenía acceso a consola ni nada por el estilo para ejecutar comandos Entonces yo me di cuenta de que el gestor de ventanas es el jwm que este también hay otros similares también que gestionan su menú a través de hacer clic en el ratón pero es un archivo xml que está en alguna directorio del sistema de ficheros bueno Total que con el utilice el firefox como explorador de ficheros control o para abrir el navegador de ficheros encontré ese archivo lo cargué en firefox vi Su contenido y dije Y si añado una línea aquí que ponga x termo no lo hice con javascript para escribir en la página html el contenido de ese menú añadiendo una nueva línea que contiene el comando xtern luego con control S lo guardé reemplazando el archivo del menú del gestor de ventanas actual y luego lo único que había que hacer era recargar este menú porque hay una funcionalidad en el menú contextual que te permite hacer eso que se podría Deshabilitar se recargó el menú y ahí tenía de nuevo la línea esta de xterm abrí una consola y no estaba protegido incluso por contraseña para hacer sudo así que dice sudo suv y obtuve una Rut Story bueno y ahí pude obviamente a acceder a datos confidenciales que estaban en ese sistema muy Guay todo muy Guay Pero cuánto te pagaron pues parte de mi trabajo así que no no fue como lo tuyo que te dieron hay para volar Pues mira nos vamos a Twitter aquí con una pregunta de Álex comanescu que nos dice Cómo ves el futuro de la ciberseguridad en los próximos años Pues bueno Yo diría que evolucionando y sobre todo en el sentido de la Inteligencia artificial a ver estamos hartos de ver en las conferencias en las en las expos en los congresos más bien todo el mundo vendiendo edrs xdrs antivirus que predictivos o sea el digamos el bus no el run run de la Inteligencia artificial ya viene de años atrás pero ahora con todo esto de gpt ahora que ha habido una evolución muy seria y alcanzable para todos los usuarios en tecnologías de Inteligencia artificial Yo sí veo que va a haber ahí digamos un paso grande en los sistemas de defensa basados en Inteligencia artificial en la ciberseguridad y luego yo creo que habrá otra cosa importante que será el tema de la privacidad yo creo que cada vez más gente es consciente de las implicaciones que tiene el desarrollo de la tecnología hacia

nuestra privacidad Yo creo que la gente es consciente de que la El Avance tecnológico va más rápido que la protecciones a nuestra privacidad doy un ejemplo los coches autónomos llenos de cámaras grabando en todo momento tú te compras un tesla te registras como la persona sabe tener una empresa privada en todo momento dónde estás A qué hora vas Qué botones tocas en tu coche eso hace cinco años no era así y nadie está poniendo el cripto en el cielo como normal porque el tesla es un cochazo Yo quiero un tesla también entonces yo creo que va a evolucionar también hacia hacia temas de privacidad y ojalá tomárselo un poco más serio con normativa más potente y bueno yo es digamos que los dos Pilares donde veo que va a haber avances tú Alexis yo digo que el blockchain va a subir se va a poner de moda de nuevo y los nfts Es broma yo lo que digo es que sí si estoy de acuerdo contigo Martín también el tema de vamos vamos a ver los lms son los chat gpts en muchas partes del tema de la ciberseguridad sobre todo porque van a aumentar no es que van a automatizar a reemplazar humanos eso todavía no lo veo pero mejorar la eficiencia de esas personas que están por ejemplo respondiendo a incidentes va a ser muy importante y va a ser muy útil el otro tema también que veo que se va a meter mucho más es el tema del no sé la meta Versa o en la realidad aumentada o tema que era femenino que está muy bien pero es la primera vez que lo escucho como la metaversa Pues sí claro que tiene ese tiene los dos vamos porque el yin y el yang pero nada es que viendo lo que lo que ha sacado Apple de nuevo en la en la conferencia esta de developers no su visión Pro la verdad es que es bastante interesante lo que ha sacado Aunque el precio también es bastante interesante no pero luego vemos como meta también se está poniendo las pilas no es interesante la palabra para definir el precio del visión Pro Pero bueno aparte de aquí un saludito a un oyente que nos mandó hace tiempo un mail y nos vacilaba porque siempre decimos interesante que todo es interesante y tiene toda la razón claro es que no sabría como posicionarme la verdad que sí es bastante caro para lo que es diría yo pero podría ser más barato pero Oye yo no sé si si Apple ha decidido que ese producto vale ese precio algo deben de saber de marketing estrategia y Vender productos y yo igual no sé nada porque no no vende este tipo de productos pero sí a mí me parece caro y no lo voy a comprar hasta que no se ponga más barato de segunda mano o temas similares vamos me ha gustado porque es como reivindicate y no lo voy a comprar no pienso comprarlo señor Team Cook hasta que me baje usted el precio me gusta me gusta Alexis Sí señor ahí defendiendo al resto de la gente otra de Twitter venga va que está esta Mola nos pregunta Pablo Pacheco aparte de felicitarnos por el programa Muchas gracias nos dice cómo fue la evolución de tu salario en el mundo de la ciberseguridad Y cómo está y cómo este ha cambiado en estos años se gana más en el mundo de las ciberseguridad Comparado con años anteriores voy a Yo sí muchísimo más y te digo por lo menos en mi caso yo recuerdo cuando era como 2014 tal que estaba en una empresa me acuerdo que en esa empresa cuando yo entré justo había cambiado que la gente de ciberseguridad se empezaba a considerar se empezaba no se justo que se empezó a considerar como ingenieros en las empresas en Estados Unidos muchas veces tienen como Diferentes escalas y por ejemplo hay analistas hay ingenieros hay digamos diferentes categorías y de esas categorías depende el sueldo pues yo me acuerdo que el año que yo entré que era 2014 el año anterior todavía no se consideraba a un ingeniero informático porque en la mayoría son ingenieros informáticos que en la parte de ciberseguridad como si fuera un ingenieros se consideraba analista y por tanto el rango de sueldos era mucho más bajo que el de un software ingenier eso ya te digo que ha cambiado radicalmente ahora mismo en parte por la falta de talento sobre todo falta de talento senior porque el tema es que el mundo de la ciberseguridad es muy joven Comparado con otros con otros Campos pues es muy difícil encontrar a gente con mucha experiencia Entonces yo por lo menos mi impresión es que Los sueldos para los digamos que está muchísimo más reconocido alguien que trabaja en algo

relacionado con la ciberseguridad de lo que estaba hace pues cinco o seis años sí Totalmente de acuerdo y a ver para esto como he dicho antes por ejemplo bueno el tema de lenguajes no el tema está overflow puesto publicado esos estudios que de cada año no en plan si sabes programar en esto pues te puedes llegar este salario Pero hay otras empresas grandes o incluso en linkedin a veces salen estudios de salarios lo interesante por ejemplo en Estados Unidos ciertos estados Ahora por ley están las empresas obligadas a publicar el salario de cada oferta que publican Así que eso te puede dar una idea sobre todo creo que California lo hace Nueva York Colorado Ahora cuando en Estados Unidos y Colorado la primera que lo hacía California lo hacía también o no Yo cuando veo ofertas de trabajo en Estados Unidos siempre te pone abajo la línea de en Colorado tal pues cobrarías tanto no he visto la de California todavía Ah vale pues desde hace muy poquito un mes o un par de meses en Nueva York es de obligado cumplimiento eso también que es muy interesante y recordemos que en la mayoría de estas empresas cuando dicen que es algo confuso al mía al menos cuando llegué aquí te dicen salario pero el salario es la base y luego tienes el bonus y luego está el stock si es una empresa pública y luego pueden haber temas similares En referencia a comparación por ejemplo no sé yo diría comparando salarios de España con Estados Unidos te puedes encontrar desde en empresas normales una diferencia de Entre más o menos tres cuatro veces se cobra más en Estados Unidos que en España yo diría Y si te vas a las top las no sé las en plan las fans y similares o incluso startups tipo opening bueno no estar todavía porque con todo lo que está en los billones que está valorado pero ese tipo de empresas te puedes llegar a encontrar a que puedes llegar a un salario de seis veces la cantidad que puedes encontrar en países como España o en otros países en Europa efectivamente Mira me voy con la siguiente en Twitter que veo por aquí de Don jacote que está muy relacionada que es cómo fue vuestra carrera profesional para llegar a trabajar en Estados Unidos y también lo enlazo con cuál es ahora mismo nuestra actividad profesional habitual si es pentéster auditores o cualquier otra Alexis Cómo llegaste a Estados Unidos solo de web Rabbit me metí como Alicia y lo digo qué hago aquí qué es esto no yo en mi caso un compañero de trabajo se vino para aquí sin decírselo a nadie y luego envío un email dijo que se iba no de la empresa Pero no dijo A dónde se iba Ni si se iba fuera de España o no entonces luego envió un email a todos los que estamos en España pero en lugar de desde la dirección punto es de la puntocom me dice muchas gracias Ah así que estás ahí no entonces luego le dije Oye sabes qué que a mí también me interesa el tema también mi currículum y se lo enseño a sus jefes o jefes se ve que les hice gracia me entrevistaron de forma remota y pude hacer una transferencia lo interesante en mi caso es que hay empresas que sería una recomendación que yo haría si estáis trabajando en alguna empresa en cualquier país en el que estéis que tenga también o que las sede si la sede está en Estados Unidos mucho más fácil pero si tiene alguna oficina en Estados Unidos igual También sirve Pero eso os puede ayudar a hacer una transferencia que las visas normalmente la l1 L2 similares son mucho más fáciles de conseguir que las h1b o similares que que están contadas no entonces Ese fue mi caso yo hice una transferencia y después de eso pues ya Bueno ya aplicas a otro tipo de Visas que ya me permiten estar aquí más tiempo y aquí estoy Esa fue la pregunta no sí efectivamente pues en mi caso fue a base de borracheras lo que la gente llama networking pero que en realidad es tomarse copas con gente desconocida nada fuera broma realmente un componente fuerte de eso yo me fui de erasmus cuando estaba en la universidad bueno para los que nuestros compañeros de latinoamérica un Erasmo es básicamente una beca un programa en el que puedes ir a estudiar una universidad extranjera dentro de Europa pues yo me fui a Alemania y entonces pues me moló un montón ese año fue brutal y cuando volví pues empecé un máster en Madrid y en vez de juntarme con la gente española pues me juntaba con todos los erasmus porque ese mundillo me molaba y de fiesta en fiesta y tiro

porque me toca Pues un chaval libanés que conocí en una fiesta de disfraces Pues justo se iba para Apple a trabajar a San Francisco y nos mandó el iba a hacer como básicamente Pues el becario de toda la vida un programa de digamos de no de prueba pero de seis meses para pues para los que acaban de salir de la universidad y tal y nos mandó un email a todos los que habíamos ido a esa fiesta diciendo Oye en Apple están contratando y tal pensad que esto era yo creo que 2008 y en España estaba el iPod y poco más O sea Apple Era muy poco conocido y yo tenía justo el currículum hecho en inglés de milagro para subirlo a infojobs Pero bueno porque estaba trabajando de becario en un departamento de Inteligencia artificial de la de una universidad en Madrid Total que dije yo como lo tengo hecho en inglés venga yo lo mando y nada pues como el inglés no se me daba mal porque Yo viví pues varios años en Suiza y hablo alemán y tal Y bueno los idiomas no se me dan mal pues me llamaron para hacer la entrevista yo simplemente se lo mandé a él no se lo mandé Apple le dije sí sí toma toma y de repente me mandaron y yo creo que me pillaron porque yo estaba tan convencido que ni de coña me iba a ir yo a Estados Unidos a United States of America tío que tenía tal confianza en la entrevista en plan contestando porque total pero yo iban contestando y yo me sabía las respuestas Pues porque evidentemente pues me Mola el mundo de los ordenadores y tal Y fue entrevista otra entrevista otra entrevista me acuerdo que fueron cuatro y de repente tío me llega un mail que sí que me cogen Vente para California y yo flipando tío Y fue así y me fui para allí en principio que era para seis meses recuerdo perfectamente el primer día que aterricé Y fui a la sede de Apple ahí a cupertino porque te dan una casa Durante un mes y quedarme flipando digo dónde estoy tío esto Qué es por no hablar la primera semana que es la semana de orientación claro yo lo máximo que había visto era el departamento donde estaba de becario de la universidad que era con todos los respetos un cuchitril no donde hacía yo ahí mis cositas y de repente llegó allí yo estaba flipando y yo fui hablando de visados Pues con un visado que es muy fácil de obtener que es como de estudiante para Pues eso para hacerte que es una j1 en mi caso pero es esa vía de entrada me vino muy bien porque yo en cuanto Estuve allí a la semana lo que decía yo ya quería quedarme más pedí seis meses más O sea que cuando se me acabaron esos seis meses puedes alargarla otros seis meses y ya cuando llevaba ocho Es decir me la alargaron a las dos meses ya me ofrecieron quedarme allí trabajando que es con el famoso visado h1b Lo bueno que que de aquella en 2009 que era esto sobraban las h1b ahora para que os hagáis una idea conseguir una uno ve pues hay 60.000 creo porque 20.000 están reservadas para militares y gente creo que con discapacidad si no recuerdo mal pues hay 60.000 Y hay como 350.000 solicitudes V o en 2019 o algo así O sea que ahora está muy difícil O sea no Solo tienes que pasar entrevistas conseguir un trabajo que te quieran exponsorizar sino que luego vas y tiras un dado porque literalmente tienes una entre seis posibilidades de que te toque pero bueno así entonces ya me quedé la h1b de la 89 a la Green Card y así 12 años y hora de vuelta en España a todo esto decir que los becarios en Estados Unidos están muy bien tratados mucho más que en España o no sé en otros países pero en español algo Igual me parece mucho en Estados Unidos tienen un salario decente que les permite vivir independizarse como tú vivía solo y podías comer no te faltaba agua ni comida verdad O sea estoy pensando si decirlo pero es que a mí por un lado Me gusta compartir prácticamente ni hoy en España un senior tío o sea y yo llegué allí te lo juro esto no te miento eh Alexis yo llegué allí pensando que no tenía sueldo yo cuando te lo juro tío yo en plan aquí no me van a pagar y ya cuando llego allí y tal Bueno claro cuando llego allí veo el precio del alquiler digo Bueno no duro ni una ni un mes pero cuando veo el sueldo me quedé flipando tío flipando y está el cual lo que dices tú es lo bueno que allí no hay diferencia con un becario con un ingeniero te van a tratar genial Te van a enseñar el sueldo es el que te mereces y nada una pasada una pasada o sea yo a cualquier amigo mío a cualquier persona con la que hablo le digo si tienes la posibilidad vete allí porque no no solo

por el sueldo que también que no nos engañemos es algo importante pero por la proyección de carrera o sea yo allí de repente Estaba rodeado de cracks yo iba a comer con un tío que era experto en esto lo que hablaba un poco antes no la verdad Para mí fue una experiencia increíble y aprendí muchísimo vale vamos con la siguiente que vamos por la horita y media este episodio más largo pero que no queremos dejar ninguna pregunta en el tintero Y eso que para mí son las tres y media de la mañana y tengo un gripazo del copón y Alexis además se va de viaje pero aquí estamos dando cañita vamos a ver venga a ver qué tenemos por aquí ya habéis creado nos pregunta nona Fer si hemos creado alguna herramienta específica para Austin human e-main etc o dependes ciberseguridad o similar incluso para intrusión en sistemas alguna para Haití o y luego desde podrías pasarla a ver yo yo personalmente Sí he creado muchas de desde herramientas eso lo que decía Papá hackear buzones de voz últimamente Pues en temas de Hosting para hacerte más con números de teléfono he creado una herramienta Pues para automatizar el reseteo de contraseñas y poder comprometer teléfonos que bloqueados bueno los teléfonos no las cuentas y otras cositas está todo mi github git happ.com/h Martin vigo Así que ahí las tienes hay un módulo de meta exploit para extraer las contraseñas del aspas si tienes pues un meter preter o así pues se llama Las pad barra Baja creds pues si se lo he escrito yo con un compañero con Alberto y lo presentamos en Black hat Y pues también también va muy Guay tú Alexis algo que hayas publicado yo público poco porque casi todo lo que he hecho fue para empresas y las herramientas que he desarrollado fueron alguna por ejemplo para obtener información de temas como sistemas que te dan reputación de direcciones ips o similares como carbón Black no y sacando obteniendo eso Pues digamos haciendo un plotting en Google Maps y dándole color un poquito para tener un dashboard digamos en tiempo real de lo que de cada dirección IP otra herramienta que está sí que la utilizamos durante bastante años Fue un entorno de una plataforma de fishing para enviábamos miles de estado automatizado Así que si digo Milo un millón da lo mismo no enviamos miles de emails a diferentes clientes que nos decían Oye podéis hacernos una campaña de fishing para educar a nuestros usuarios pues eso sí que lo desarrollé desde el principio el fronten digamos lo hice en php el Back en python lo interesante de eso es que eran tiempo real Así que cuando se recibían nuevos clics pues se veía en el dashboard este y con los iconos digamos del sistema operativo y la aplicación que había utilizado para abrir el email pero sí herramientas de este tipo pero nada publicado porque es todo digamos para uso interno para los clientes de las empresas en las que trabajaba y no me permitían publicar nada y seguro que no soy un desarrollador de software y esas herramientas como las que desarrollé seguro que las Hay mejores en No hombre tú eres un crack sé que hacías cositas internas yo soy muy de publicar y de conferencias pero nada nos tenemos pendiente Alexis dar una charla Y juntos de alguna investigación que hagamos no tanto por la parte de divulgación que hacemos Que ya hemos hecho varias tú y yo bueno divulgación también pero hacer ahí petar algo tuyo reventar algo Hay millas de aerolíneas eso eso venga nos vamos con la siguiente vamos a ir dándole vidilla vamos con un audio de Félix a través de Instagram Hola Estoy aquí en la piscina que estoy trabajando sobre risa que su hijo siempre el podcast que os quería preguntar que yo ahora mismo Estoy en una fp media y qué recomendáis para la superior desarrollo web administración de sistemas o hacer superior de ciberseguridad para llevársela a la seguridad que recomendáis y luego metes una carrera no muy bien Félix para nuestro querido audiencia de latinoamérica Bueno un ciclo un ciclo medio es pues es unos estudios digamos preuniversitarios que se hacen en España De hecho yo tengo un ciclo Superior y nos pregunta aquí Félix nuestro amigo socorrista que está ahí dando el Tajo para mantener a la gente a salvo Claro que sí pues qué ciclo superior recomienda y además Cómo meterse en esto de la ciberseguridad es un poco ya lo hemos contestado la segunda

parte qué ciclo superior recomiendo Mira te digo el que yo hice fue ciclo superior de administración de sistemas informáticos fue lo que me dio acceso luego a la universidad para estudiar ingeniería informática y luego hacerme mi Master Así que es un camino pues muy bueno o te puedes quedar o incluso con el ciclo superior pues ya se pueden aprender cosas muy interesantes evidentemente si lo que te interesa es la ciberseguridad y ahí ahora en mi época no lo había hay ahora un ciclo superior específico de ciberseguridad Oye pues dale a eso si te interesa más la programación el de administración de sistemas informáticos que yo hice en su momento que te hablo hace muchísimos años Pues estaba muy bien porque te enseña eso los fundamentos de informática programar Cómo funcionan los ordenadores y con eso pues ya puedes encontrar trabajo a ver yo diría lo mismo que Martín directamente fui a la universidad pero diciendo esto en retrospectiva he visto que muchos digamos lo investigadores de seguridad o incluso backbound y hunters que no creo que no han pasado por la universidad y que hacen millones de dólares al año que es mucho más de lo que gano yo así que Oye que si eres apasionado y se te da bien el tema de ciberseguridad y eres autodidacta a veces no hay ni que pasar por temas de estudios regulados no como una universidad o incluso un grado medio superior o lo que sea de hecho Si te vas a hacker One hay algunos de los top backgrounty hunters que yo creo he escuchado no te puedo confirmar no pero sabría que mirarlo caso por caso pero algunos de ellos creo que no fueron a la universidad o igual ni la acabaron Sí claro la universidad no es algo esencial está fantásticamente bien yo estudiar ingeniería informática en la universidad me ayudó muchísimo pero no es la única vía y desde luego todos los ciclos medios superiores y una excelente herramienta para conseguir esa esos conocimientos iniciales O sea que perfecto cualquier cosa que hagas que estudies Bueno será si no no quería desmerecer la universidad quería decir lo que no te desesperes si no es lo tuyo hay gente que la empezó hizo su negocio on the Side como se dice y le fue más mejor muy de forma muy exitosa el negocio y dejó la universidad Porque y casos de esos Los vemos en muchas en muchas empresas Así que quería decir eso que que no te desesperes y ánimos perfecto me vuelvo por aquí a discord donde nos pregunta pape si hemos vulnerado comprometido algún equipo no autorizado por error está me la tengo que pensar Bueno aparte de lo que contaba antes de la anécdota esta de que te esté en producción un exploit pero no llegué a tirarlo por tanto no no llegué a comprometerlo Mira la voy a contar de esta manera haciendo un ejercicio de retín no es que comprometí somos algo que no estuviésemos autorizados sino que lo comprometimos cuando no estábamos autorizados o más bien cuando No deberíamos Qué quiere decir esto pues como el retín es un ejercicio real y que lo haces digamos un poco en secreto para poner a prueba al equipo defensivo como si fuera una situación real Pues resulta que nosotros lanzamos empezamos a ejecutar un jueves y claro yo os lo detectaron un viernes un viernes antes de creo que era la labor day Que básicamente el lunes era festivo es un fin de semana donde la gente viaja y claro nosotros digamos que petamos bastante la empresa y claro y ahí se vieron todo el equipo de respuesta de incidentes un viernes antes de un fin de semana largo respondiendo un incidente crítico y claro mi jefe no siempre en ejercicios de retín Pues le dices a alguien muy senior o siempre tienes una persona del lado defensivo que sabe que por si cualquier cosa sucede que lo el excedente realmente es un ejercicio reptil Pues digamos que nos cayó una buena y yo tuve que porque aparte yo era el responsable de esa operación pues pues porque no decirlo ahí cometimos cometimos un error no tuvimos en cuenta que era un fin de semana con antelación Es verdad que ejecutar ejecutamos el jueves y cuando ellos se dieron cuenta era el viernes nosotros ejecutamos el jueves por la mañana pero bueno deberíamos haber sido más precavidos yo era el responsable al ser yo quien lideraba el equipo y bueno me tocó pedir disculpas con varios managers Pero bueno Al fin al cabo luego escribes un post mortem lecciones aprendidas y mira desde aquella no nos volvió a pasar

interesante a mí yo se me ocurre una que a ver Esta sí fue un poquito por error ahora que me pienso pero lo paramos en cuanto nos dimos cuenta que fue casi de forma inmediata eso que estás haciendo una auditoría un Security session y te pasan las direcciones IP no y te ha pasado Martín te las pasan en una hoja de cálculo o algo así y las direcciones IP por ejemplo digamos que son 10.1.1.1 10.1.1.2 Pero de alguna forma han puesto el cero delante del 10 010.1.1.1 no sé si os la habéis encontrado esto pero si por ejemplo Vais a una línea de comandos y ponéis hacéis un pin 010.1.1.1 el 0 10 por tener el 0 delante se interpreta como si fuera un número en notación octal que digamos que 010 sería cada número va del 0 al 7 y sería el menor el 0 1 0 el último a la derecha iría del 0 al 7 el que está como 1 es en realmente no vale uno no es sería un 10 sería un 8 porque es la forma en la que se representa no Y entonces la dirección IP no era 10.1.1.1 que el sufijo el digamos el rango 10.0.0/8 está está reservado para direcciones ips privadas internas no esto transformaba el 10.1.1.1 con el cero delante del 10 a una dirección pública la 8.1.1.1 Y entonces empezamos a hacer Bueno escaneo de puertos y vulnerabilidades y temas similares pero como digo nos dimos cuenta pronto porque Bueno siempre que echar un ojo a lo que lo que van haciendo tus herramientas no y nos dimos cuenta y dijimos Oye y esto o mira porque está en formato octal con el cero delante hay que borrar y digamos darle de nuevo las direcciones ips a nuestras herramientas para que usen las privadas las direcciones privadas no no las direcciones públicas tenemos por aquí una pregunta con un punto filosófico de Danny aescu que nos dice para trabajar en ciberseguridad se nace o se hace como siempre yo creo que esta pregunta No no es no la tocamos por primera vez en tierra de hackers en muchos otros personas que se dedican a esto no a pensar sobre estos temas como dice Martín filosóficos Yo creo que es un poco de ambos no se tiene que tener un poco la naturaleza curiosa porque si no si no te entra y yo conozco gente que le da igual como funciona un ordenador por dentro mientras puedan abrir el navegador y ya les sirve pero le da igual cómo funciona por dentro que que se puede hacer Entonces primero tienes que tener un poquito eso y luego después de ahí pues obviamente tienes que ponerle muchas horas para hacerte pues alguien en tema de ciberseguridad ese sería mi respuesta Sí mira yo para completar tu muy buena respuesta un hacker puede hacerse sin nacer pero dudo que un hacker pueda nacer y no hacerse luego es decir puedes nacer con ciertos skills que se te dan bien y que son muy útiles para esto pero si solo te quedas en eso y no le echas las horas no vas a ningún lado mientras que alguien que puede dedicarse algo totalmente que no está relacionado yo he conocido a hackers que eran bibliotecarios por ejemplo gente que era o se consideraba completamente nula en temas de tecnología por no decir específicamente de ordenadores pues se ha hecho hacker por tanto lo importante aquí es echarle las horas Alexis nos pregunta por aquí en discord Iron nakamura la noticia que hemos dado más Absurda y la que más nos ha impactado hombre a ver no hay ninguna noticia Absurda en tierra de hackers a ver a ver a ver qué estamos diciendo a ver claro yo pero Absurda quizá de esto de de qué es esto claro yo pienso en la que comentamos te acuerdas el Endo vibrador esa es un poquito graciosa Absurda como quieras decirlo sí es es no no tanto absurdo pero sí a la vez es como pero desde que estamos hablando No aquí algo esa pero fue más graciosa que otra cosa yo creo pero Absurda yo pienso la de la del candado ese de la parte privada humana esa también me pareció un poco pero Pero ha intentado Esto sí sí sí Mira qué buena porque aparte Ese yo creo que es el episodio 6 o 7 o algo así sí algo del hackeo es verdad de un cinturón de castidad de castidad no sí sí es en plan pero qué absurreces esto Cómo podemos estar hablando de que alguien hackeó un cinturón de castidad y que no y que puede hacerle un dena y a los service literal a una persona tío de nadie los Services sexual pero sí es como en plan y cómo es que esto se puede acceder desde internet Pero bueno ya ves y luego que más me haya impactado Pues mira hablando de naval ni no es que la noticia Me impactó el poder saber todos los detalles la parte

de ingeniería social Pero yo creo Uff que más me impactó haber impactar por la por la curiosidad todas estas que hablamos de cuando se encuentran ataques de canal lateral no los ha echado por ejemplo lanfon a este que alguien puede escuchar conversaciones sí midiendo el tintineo de una lámpara o sea eso es como que me estás contando tío Holi Yo creo que esa es muy buena Sí yo igual yo te iba a decir todas estas de canal lateral de que sea en plan de James Bond de película de Hollywood Son son las que a mí me han dejado me han abierto la boca de los ojos en plan madre mía lo que se puede hacer ya ves yo creo que más o menos hemos cubierto todo y he dejado para el final una de las preguntas un audio aquí especial de los compañeros de lo de los hackers y yo creo que podemos ya terminar con esta porque con otras preguntas que aún tenemos más o menos hemos contestado ya todas ellas y además ya nos vamos a las a las dos horas vamos con la con la última pregunta a ver qué se cuentan Qué pasa hackers somos Alex y Harvey del podcast todos los hackers y aquí van esta pregunta Cómo deben necesario consideras realizar un curso de inglés en Hawaii para adentrarse en el mundo ciber Felicidades por estos 100 programazos y manteneros ciberseguro aloja Loja chao Muchísimas gracias gran podcast también lo de los hackers lo recomendamos desde aquí que son unos compis súper majos y hacen un curro muy guapo con temas de entrevistas a gente muy interesante nos preguntan si hace falta hacer un curso de inglés en Hawaii para dedicarse al hacking esto es porque uno de ellos uno de lo de los hackers resulta que yo le conocí en Hawai en 2009 y no nos habíamos dado cuenta si tú recuerdas Alexis nos entrevistaron a nosotros y Sabes Para mí era eran dos personas que acabábamos de conocer y luego en navaja negra en una conferencia con uno de ellos no el que había conocido en Hawai Pues de esto hablando tal Y él me decía estábamos ahí de borrachera y tal y me decía así yo estuve en Hawaii tal y yo Ah pues yo también con una beca pero yo también qué año yo somos este año tal Y empezamos a atar y los tío y me dice ostras que yo llegué una semana después tío pero mi compi de lo de los hackers él fue una semana antes por tanto tuviste que estar allí y tal Y aparte como somos los españoles que estemos donde estemos nos juntamos todos y de repente digo ostras tío y empecé a buscar fotos y pum ahí estábamos los dos también con copas en la mano porque habíamos estado en Hawai juntos tío y no nos acordábamos con una beca de esas de aprender inglés que podías ir a un país angloparlante y dijimos yo yo en su momento dije vuestro Hawái tío ahí se habla inglés por tanto vale Y ahí me fui a Hawaii a aprender inglés Pero dónde sale Yo no no me interesa becas si no hubiera me hubiera ido con vosotros Bueno yo me fui a Hawaii me fui a Malta otro verano era unas becas que había por ahí en 2007 2008 de España o de la Universidad del gobierno de España tío y se puede si era s estudiante universitario las podías pedir y era un poco ilógico porque si te la daban un año tenías más posibilidades que te la dieran al siguiente tío y yo porque eso lo pillé dos años pero eso me la dieron para Malta me pasé un verano en Malta que flipas aprendí inglés ahí estoy acabé que Estados Unidos pero también había tiempo para pasárselo bien y para el año siguiente dije joder ya está un Malta Pues venga nos vamos al otro lado Hawai y ahí conocí a esto es unos cracks la verdad madre mía Pues sí muy interesante Yo diría que en en Hawaii puedes aprender inglés cierto cierto aunque Sí la verdad es que me tenía que ver con vosotros me tenía que haber avisado Martín eso es lo que iba a decir Ya ves para allá ya conseguiremos más becas no no hay problema Bueno queridos oyentes Gracias de verdad Ya sé que siempre lo decimos pero es que habéis estado con nosotros 100 episodios en horas eso yo que sé estamos en las 300 si multiplicamos que al principio decíamos por seis tales estamos hablando de 200 noticias toda las semanas estáis ahí nos escribís nos apoyáis Muchísimas gracias En serio es todo un lujazo como decimos siempre Esto empezó como una idea de nuestra Pasión por la divulgación y gastarse en cuenta euros en un micrófono y venga nos ponemos a ello y aprendemos todo sobre la marcha y aquí estamos 100 episodios después con apoyo de

sponsors de la gente una una pasada muchísimas gracias y por muchos muchos más episodios juntos sí como dice Martín no tengo palabras como como ha dicho uno de nuestros oyentes para deciros lo agraciados que estamos de que con nosotros episodio 3 episodio en todas nuestras aventuras online y en persona también porque hemos conocido a muchos de vosotros como menciona Martín en conferencias como navaja negra pero también en defón en Vegas y similares Así que muchas gracias a todos los sponsors patreons oyentes y sobre todo a esos investigadores seguridad y eso ha sido el criminales que sacan noticias semana tras semana porque si no No tendríamos algo que contaros por queridos oyentes hoy más que nunca nos vemos y nos escuchamos en el siguiente episodio de tierra de hackers Adiós adiós chao chao si te ha gustado este episodio y quieres ayudarnos a seguir con el podcast compártelo con tus amigos y compañeros con tu apoyo podremos atraer y despertar el interés por la ciberseguridad de mucha más gente Acuérdate de dejarnos un comentario y una valoración donde nos estés escuchando también puedes seguirnos en Twitter Instagram y Facebook te esperamos en el próximo episodio de tierra de