Tech Session #1 - ¡TODOS los secretos de los HACKERS! Con Seifreed

Bueno pues nada gente hoy estoy aquí con Marc Rivero experto en ciberseguridad ya estuviste aquí conmigo una vez hace poco relativamente poco en verano creo que fue eso es que estuvimos Charlando un poco de Bueno un poco de antivirus o sea el tema principal aquel día fue antivirus Lo que pasa que lo que no sabe la gente es que hablamos muchísimas cosas realmente O sea la charla nuestra creo que duró como una hora y media dos horas algo por el estilo Y claro luego publicado en el vídeo en Sí quedó mucho menos sabes porque bueno era el tema principal en antivirus y no quería sacar un vídeo de 40 horas sabes hablando de todo y bueno aparte había esos diseños gráficos también que ayudaban a entender a todo el mundo lo que hablábamos que también fue superútil también te voy a decir que en parte quite cosas para no tener que hacer más dibujos porque era como vale si tengo que hacer más dibujos me voy a morir Cuéntame un poco a qué te dedicas y Bueno quién eres qué haces Y a qué te dedicas Vale pues yo siempre digo que acabé en el sector de la ciber un poco por rebote porque cuando yo empecé en esto ciberseguridad como tal no se hablaba es decir un tema de la estaba dentro de los equipos de informática no irá digamos una pieza dentro del equipo de Haití seríamos dentro del equipo informáticos de la empresa tipo que estás ahí manejando servidores instalando Windows y todo esto Pues hay una rama del que se encargaba de las habilidades que sabía de ciberseguridad no de seguridad en general pero mucho más enfocado a la administración de sistema redes y seguridad estaba un poco más enfocado en redes y seguridad y ahora qué ha pasado ha cambiado la cosa dice no esto ha multiplicado hasta el infinito y seguirá un poquito más allá no es decir ahora ya es un ente propio de hecho en las figuras de cto ceo está elciso no el responsable de ciberseguridad de una organización Cómo es la sigla de Chief information y es un cargo ya importante está a la misma altura digamos que un cto por ejemplo Y qué ha pasado para que haya tanto cambio en el mundo de la informática realmente llevamos Cuántos años ya en la era de la información y han habido ataques desde los años 80 incluso antes no Por qué últimamente se ha vuelto todo más más serio no más formal Yo te diría que es el power del impacto no el impacto que tienen las organizaciones cuando las vulneran y los datos acaban publicados en de forma pública no datos confidenciales como yo que sé tenéis pasaportes números de seguridad social correos electrónicos contraseñas que eso tiene un impacto súper masivo y además la legislación está muy encima de esto de Oye ten cuidado porque si publicas datos te puede caer una una multa no te pueden multar No creo que o sea digamos que es un tema también de preocupación en cuanto a que las leyes han puesto las pilas con esto y sobre todo que la privacidad al nivel sobre todo europeo está muy en boga ahora no se habla mucho de Data sino lo están forzando a gente como meta Twitter y demás a que sobre todo en Europa la legislación de datos se la tomen en serio Guau o sea es curioso este enfoque O sea no es tanto el hecho de que haya más ataques que nunca si no es el hecho de que los gobiernos están empujando las empresas para que tengan más cuidado con esos datos incluso multándoles No si tienen alguna fuga de datos o sea pongamos que yo que sé yo por ejemplo tengo una empresa de telefonía Vale tengo una base de datos ahí con todos los datos de mis clientes no tengo yo que sé imagínate dni nombre apellido nacionalidad sexo todo esto si a mí me hackean y me roban esto yo tengo problemas legales con él o sea O sea primero de todo dependiendo del sector estarías como obligado a anunciar que ha sido hackeada que te tienes que hablar con la agencia de datos que trabajas en España y decir Oye sufrir Una

vulneración de datos y un poco también para que ellos también evalúen el impacto también no que eso tiene porque al final ya estás trabajando con datos de terceros esto antes no estaba tan legislado Ahora sí Y este es el motivo por el cual hace falta tanta digamos que las empresas tienen tantos datos digitales y todo el mundo está como en Cloud que está tomando muy en serio muy en serio esto no así que es verdad que hay muchos más ataques que de hace 10 años evidentemente pero sí que es verdad que a nivel países está poniendo mucho enfoque y a nivel legislativo muy enfoque en proteger Esto vale vale Y bueno sigue contando me empezaste entonces en siendo un informático más eso es yo hice una formación profesional de administración de sistemas y bueno en el caso es que siempre me gustaba digamos publicar un poco lo que hacía me abrí un blog que le recomiendo a todo el mundo que lo haga y empecé a publicar ahí los apuntes de clase no Oye Cómo montar un servidor ssh o cómo montaron y bhp Cómo montar ese tipo de cosas que hacían clases las publicaban en el blog Okay y mis compañeros de clase consumían ese contenido no y apuntes porque me da mucha pues a tomarnos digamos lo pongo ahí y alguien lo consumirá esto es súper útil y genera una cantidad de visitas es decir yo llegaba a tener en la época de estudiante que no es como ahora como mil visitas a la semana o así que era como Pero tú O sea que tenías un Word no me imagino y una época así muy Friki pensé hacer algo parecido pero tomaba los apuntes en html directamente Pero sí yo hice algo parecido pero me cansé muy rápido un poco es que realmente no guarda el contenido los posts Pero bueno que no le importa a nadie en realidad En aquel momento no Entonces me metí a coordinar un congreso de cirugía en Barcelona que se llama con name que tiene cómo se llama No con name Okay que tiene un montón de años de historia de hecho creo que es como los primeros congresos de hacking que hay en España y si se movió a Barcelona y entonces ayudé a coordinarlo y uno de los que estaba la organización me Bueno me dijo que si buscaba trabajo y bueno aplique para para la oferta y ahí empecé pero en ese momento tuve evidentemente ya no eras estudiante no Simplemente ya estaba en el mercado laboral trabajando pero sistemas y me gustaba mucho la ciberseguridad probaba herramientas me hacía mis setups mis laboratorios y probaba cosas pero realmente no me dedicaba a modo profesional a ello no era un poco más todo muy autodidacta Sí sí yo recuerdo también cuando cuando hacía yo también hice un año del grado superior de grado medio Perdón luego salté al superior pero hice el primer año y me acuerdo que en clase Se llevaba mucho lo típico de hackear la WiFi de todo Sí hoy en día no es tan fácil Por cierto genial WiFi ahora me dirás Bueno en realidad sí un poco siguiendo el mismo ecosistema no que es este fichero semilla que una vez que ves auténticas a un cliente autenticado de coger la semilla y por fuerzas vota con el diccionario acaba sacando la password si es algo sencillo No claro antes era una locura porque cuando tenías que era la web no tenías web que era como un algoritmo muy débil de cifrado Entonces qué pasaba que cuando me acuerdo a ver cuando tú tú escuchabas paquetes te ponías tu tarjeta de wifi en modo escuchar los paquetes de distintos ordenadores y de repente cuando capturabas alguno Que era de calidad que no sé qué significa O sea que era más que nada cantidad de paquetes una cantidad sino cantidad de paquetes para poder calcular y ya está Vale Pero entonces para yo luego voy a hacer una inyección no inyectar tráfico para generar más paquetes de respuesta o sea para que os hagáis una idea el rollo sería que yo capturo mensajes que es como si hay Sebas y que están aquí hablando en alemán yo me pongo a escuchar y no tengo ni idea pero me apunto aquí palabras que he entendido Entonces yo se las empiezo a decir a Sebas cuando él no está mirando y le empieza a repetir esas palabras en bucle Entonces él me responde todo el rato y aprovecho ese tráfico que me está respondiendo para desencriptar la contraseña No eso es eso era bastante que esto como

en 15 minutos o menos tenías la clave ya de wi-fi lo que me acuerdo que en aquella época no se llevaba tanto esto de tener las distros como ahora no que ahora te instalas un Linux o incluso levantas un con una Life CD levantas ahí un cálido Cualquier cosa le vas al menú le das ahí y me acuerdo que tienes que Instalar los paquetes normalmente la cosa a todo el mundo y lo complicado era encontrar tarjetas WiFi que puedas ponerlas en modo monitor porque no todos los drivers lo soportaban si si yo he pasado horas bajándome los drivers para el portátil y al final nada no pillaba una marca que no sé si se vende ya que era güisacom Sí sí sí yo pensaba esto de un vatio esto era una maravilla y luego mis amigos claro en aquella época no había Amazon que decía no vi una antena en Amazon íbamos por tiendas de informática a ver si tienen antenas y Barcelona está en la calle Sepúlveda y pues comprábamos todo esto sí sí sí pero tiene amigos que tenían las antenas estas de un metro sabes este rollo para ver si pidábamos más luego hay mucha gente que no sabía mucho de antenas No porque las que son digamos que son un palo esto es una omnidireccional cobertura pero pues queremos si quieres hacer algo direccionante comprarte una yagi que el tubo no que direccionas hacia un sitio y Alguna vez has hecho una antena en casa de estas con papel de plata siempre la hicimos eh la verdad que como siempre he sido muy malo con el tema de Hardware manitas y demás siempre o tiraba de un colega o la compraba esta que también nosotros decimos una pero no no no no funciona es mucho más seguro no y se utiliza wpa2 que sería con certificado vale Y qué es lo que hace que hoy en día sea más seguro o sea porque no es tan fácil como antes pues hemos pasado también tú te acuerdas aquellas autoridades que había de cripter jaztel de clipper te acuerdas porque las claves estaban Ya precalculadas no esto para que os hagáis una idea porque seguro que hay gente que ahora mismo Está está flipando eso la mítica del bote de Pringles le ponías dentro de la antena y Bueno pero eso no no funcionaba para que os hagáis una idea Claro porque pusieron o sea el web se decó soy honesto ya no lo uséis porque esto lo hackea hasta un chaval de 15 años vamos a usar algo más seguro salió WPA que lo que hace es ir cambiando la clave no O sea y hay una parte de clave privada clave entre el router y los clientes digamos Ok Ok entonces el tema sería que con esto no es tan fácil pillarla pero lo que lo que hacían era que cuando tú compras Bueno te instalas internet o sea ya más allá esté la quien sea y le pides un router te mandan el router a tu casa lo instalas y ese router viene con una contraseña por defecto y un nombre de WiFi por defecto entonces alguien se dio cuenta de que había una relación había un algoritmo que calculaba la contraseña en base al nombre no entonces había como aplicaciones que te sacaban para móvil o sea para móvil y hoy en día ya no no Hoy en día eso ya está más que resuelto y los operadores ya se han puesto las pilas con esto porque eso imagino que el que lo diseño pues está yo que sé está escondido pero pero ya no y a día de hoy Realmente si quieres hacer eso tienes que hacerlo tradicional de un cliente conectado inyectas tráfico mismo modo operandi y una vez que digamos Perdona encuentras clientes desatenticas al cliente y cuando este se vuelve a reconectar capturas el fichero de semilla entonces aplicas Fuerza bruta con un diccionario para poder sacar el password vale Pero qué pasa que necesitas un diccionario o sea un diccionario para que os hagáis una idea es es un archivo verdad Porque tienes un montón de palabras y pruebas a ver si alguna Eso suena la flauta no pero como te imaginarás en el momento que vivimos Ahora hay servicios Cloud que subes tu Hans check Okay y se revienta cuando no sé cuántas envidias ostia claro mirar esto no lo sabía Eh sí sabes dónde mirar hay gente que se ha montado datacentes de herramientas para hacer Blood Force con envidias gpus y demás para poder hacer una cracking mucho más rápido o sea digamos que esto para que os hagáis una idea O sea tú de autenticas auténticas al cliente esto significa que

tú para desconectarte no sé a esta cámara estaba mirando qué cámara está no entendía nada tú para desconectarte O sea imagínate que yo aquí ahora en mi iPad le voy al WiFi lo voy a desconectar cuando me desconecto el iPad manda un paquetito al router y le dice oye hoy y ese paquete no tiene nada encriptado no o sea es un paquete bastante simple es decir simplemente indica que vas a conectarte o porque la funciona así no Oye me llamo iPad de nate que me Quiero conectar hasta WiFi entonces la WiFi te pregunta un poco Bueno quién eres no entonces Oye pues ya tengo yo confirmada la conexión y puedo autenticarme no pero la idea sería que yo cuando me autentifico O sea me desconecto de esa red no estoy mandando nada encriptado no mandas nada cifrado Lo que pasa es que si quieres estar diciendo al mundo que soy interesante comentarlo con un modo monitor aquí probablemente este iPad no se utiliza fuera del estudio pero lo tienes en casa por ejemplo estarías haciendo bitcoin de cómo se llama la red de tu casa en serio Claro en los dispositivos están hechos para conectarse Ok entonces si tú no tienes una Jaula de faraday es decir que no que una caja estancada es un sitio donde tú colocas los dispositivos electrónicos y está diseñado otra forma de que no pueden hacer comunicaciones radio hacia el exterior es una caja de metal principal lo que digo es que los dispositivos están hechos para conectarse entonces Ellos están preguntando todo el rato nos hemos llamado estudio pero está la WiFi activa estará muy bien activa y va preguntando o sea digamos que si yo este iPad lo he conectado a 20 wifis y ahora empiezo a escuchar con un ordenador o con cualquier dispositivo que me permite hacer eso voy a ver que él todo el rato está preguntando por todas las redes que conoces y además eso viene un poco a explicar otro método de ataques que es Oye pues si yo quiero vulnerarte lo que hago es si tu iPad me pide la red de Marc te la doy tú te conectas y yo te pongo un portal cautivo con un Gmail donde tú te piensas que es el Gmail de verdad y te estoy robando la Pascua pero cómo me puedo meter o sea cuando te conectas a una WiFi hay una contraseña no Cómo puedo yo fingir que soy esa wifi si no sé la contraseña hay tecnología de hoy que simplemente simulas un punto de acceso falso y como tú lo tienes ya configurado lo tienes ya guardado él no comprueba si la validación contraseña no sé qué es está digamos al día sino que simplemente se va a conectar hay cifras operativos modernos creo que la versiones de iPhone o iOS últimas lo comprueban que comprueban que la mac address se relacione con el nombre de la red y si no es lo mismo te va a advertir Oye la maca3 no pertenece al punto de acceso conectado de hecho me dijeron una cosa muy interesante hace poco me dijeron que los los iphones van cambiando la marcadores de forma dinámica para eso hacen este cómo se llama la técnica pero si van cambiando aleatorizando esto para que no sea tan fácil de poder pillar eso esto para que os hagáis una idea para los que no entiendan muy bien de lo que hablamos el iPhone o sea todos los dispositivos que se conectan a la red tiene una dirección es como la matrícula a un coche por decir algo no entonces tiene una dirección y cuando tú te conectas router o a un punto de acceso los paquetes Los firmas con tu dirección Bueno pues resulta que el iPhone lo que está haciendo ahora es generar la dirección Random y la va cambiando todo el rato está interesante intenta evitar un poco los esquemas de ataque que te comentaba de colocar un punto de acceso falso y entonces no te puedes conectar pero lo mismo pasa con la telefonía móvil es decir si yo coloco una estación base que tiene más Potencia de emisión que la que tú te conectas de que está en el aire o sea una antena de antenas te vas a conectar a una mía no a la otra y y cuando tenga permisos para emitir los certificados privados y vale vale vale o sea tendría que literalmente Pero esto no es tan fácil de hacer no todo el mundo pero es posible pero es posible una organización criminal podría venir aquí a la puerta plantarme una antena bien bien hecha y qué haría interceptaría mis llamadas mis datos todo

podría saber un poco qué es lo que estás haciendo claro te contarías un poco a ellos te podían track ar un poco la actividad claro muy experto en eso pero pero vamos he visto auténticas locuras con esto y esto que me has dicho antes de que cuando yo estoy en un sitio simplemente con mi portátil o lo que sea y está todo el rato preguntando por todos los juicios a los que me conecté esto es súper peligroso no sí sí claro el hecho de que tú estés haciendo bitcoin preguntando no Oye está la red la red cuál claro supone un problema a nivel de acidez pero claro cómo solucionas esto no si realmente el dispositivo está hecho para tener conexión o sea pero de esta forma yo sí estoy yo podría saber todos los sitios donde has estado Sí claro inferir por el nombre sí imagínate McDonald's o Star o algo O sea no podría saber exactamente a qué hora ni qué días estuviste ahí pero podrías haber por el nombre de la wifi si estuviste en un hotel por ejemplo Imagínate que estás en una ciudad y yo quiero captar que esto ya es muy turbio no estamos citando la gente a hacer si hay un turista en una ciudad y yo voy a una cafetería lo veo que está ahí puedo mirar en qué hotel está Sí claro lo que está preguntando como el nombre de la como el nombre de la WiFi sea va a salir claro entonces así podría saber dónde está el huésped y madre mía pues y no hay forma de evitar esto creo que se puede hacer configuraciones Sí de hecho creo que es una opción de no cambies o no hagas bitcoin pero creo que tienes que enfriarlo a mano o sea tienes que comprarlo yo preferiría que no lo haga el móvil al wifi ni siquiera le has pedido que lo haga lo hace solo y a mí me molesta más que otra cosa Sabes concretamente Puedes configurar el rollo Pregúntame antes y hacer esta movida la pregunta vale vale preguntan aquí si tienes 300 wifis claro se va a intentar Conectar a todas no bueno va a hacer como una sesión no sé si aleatorio como lo hace Pero va a intentar conectarse la pregunta que yo tuve en todo esto en realidad es yo antes tenía el filtro de marcadores eso ya no sirve Sí sí que sirve porque estás evitando que nadie que no tenga esa hamaca tres pero claro para alguien que realmente esté en el lado de los que saben que me cambio la mac me pongo la tuya y me conecto sí sí sí sí eso sí pero me refiero que claro no funciona funciona Porque yo creo lo que creo que hace si no me equivoco es que tú sigues teniendo la mac Solo que estás haciendo bitcoin con la otra es decir tú mantienes la otra sala que tú estás diciendo me Quiero conectar Esa es la que va digamos cambiando vale vale Entiendo entonces me contabas que estabas en grado medio y medio explotación de sistemas informativos informáticos y redes no me acuerdo la sigla pero sí sí yo hice primero luego me fui a la prueba acceso grado superior y porque yo tenía muy claro que quería celebrar superior entonces dije voy directo a la prueba de acceso y ya está sabes pues yo Alcatel en la prueba Catalán no sé cómo aprovecha Bueno o sea literalmente tengo un amigo que sacó un dos creo en la prueba en general y me decía no puede ser que hayas aprobado Catalán tío me daba vergüenza ajena estar al lado tuyo en clase de Catalán y ver cómo Catalán puedo hacerlo me gusta mucho o sea no O sea si lo escucho lo entiendo todo bien pero es como que las palabras no me salen muy lento hablando porque no tengo la costumbre el tema de la prueba de acceso era que para la gente que hayamos llegado en medio era como estás haciendo cosas de informática que te molan ya tienes que hacer una prueba de matemáticas era como Pero qué narices estamos haciendo aquí no entonces exactamente cadáveres por el camino mucha gente por el camino yo no tengo ni idea de cómo la pruebe tío pero como un 5 con algo o sea estudié lo justo justo justo para un colega se la aprobó yo suspendí entonces seguí curando en el mercado laboral y Hace 2 años me convalidé todo el grado superior experiencia laboral Qué bueno se puede hacer eso en Cataluña que se llama rakuna y no sé qué que haces una haces un examen O sea te examinan Y si apruebas el examen te convalidan todas las asignaturas con las que tú digamos has aprobado el examen Bueno entonces me

quedaba solamente el trabajo de final de grado superior y emprendeduría y no sé qué y empresa que tienes que creo que es eso es entonces acabé eso y tengo título de grado superior vale vale Yo la asignatura de eye nos la pasamos todo todos los dos años no creo que solo está un año esa que creo que es un año y orientación laboral nos la pasamos todo el año jugando al enchufe empire's en clase o sea nos quedamos en el aula de informática y sacamos el pendrive con el portable del Age of Empires y a jugar y no fui a clase ni un solo día no sé cómo aprobé no me acuerdo Creo que son cosas muy pocos básicas hacerte un currículum que es un contrato si más hay una experiencia laboral además hay profes que más o menos te aprueban es como bueno no le voy a suspender por esto sabes son benevolentes Mira yo sinceramente Tendría que haber prestado mucha atención en esa clase Lo que pasa que es como todo no cuando te enseñan cosas hay veces que no te las hacen atractivas O sea a mí por ejemplo hoy en día tema de contratos tema de empresas temas de impuestos de Cómo dar de alta o sea todos son cosas que además vivo he hecho en esta última época y me parece súper Interesante pero en aquel momento es como tan aburrido no le importa a nadie nunca voy a hacer esto no me fío de contacto exacto y ahora ahora estoy mirando las nóminas en plan aquí interesante esto Qué interesante esto porcentaje de la lucha de las pensiones pero bueno entonces cómo pasaste de grado medio a saber de hacking esa parte es la que tengo aquí la super mega velocidad la cogí con la primera empresa que es una empresa que se llama s21 sech que casi toda la Industria Del hacking ha pasado conoce tiene conocidos o está ahí fue una cantera para mucha gente y ahí me acuerdo que aprendí Pues un montón de cosas estaban muy avanzados para aquella época Pero tú encontraste ahí ya sabías sabías tirar cuatro herramientas Hace cuatro análisis pero realmente no sabes no sabes Hasta que no te dedicas profesionalmente a ello y entonces todo eso lo fui aprendiendo en esa primera empresa pero realmente en el mundo de la ciberseguridad hay como muchos Pilares No si hay muchas ramas es el problema a día de hoy que realmente cuando cuando yo empecé y muchos temas de malware cibercrimen análisis de malware básicamente pero también está el hacking arquitectura de seguridad Hay un montón de disciplinas no y a día de hoy Pues imagínate toda ramificado ahora y se están buscando y se está pagando un montón de un montón de dinero para gente que hace seguridad en blockchain Ah Sí sí claro esto es vamos a la gente que Smart Contract todo esto se está apagando auténticas salvajadas el otro día Vi una oferta de trabajo como analista de inteligencia senior en coinbase el exchange y están pagando para una posición remota en Estados Unidos 210 mil dólares no está mal nada mal no está nada mal eh claro tienes que ser una persona que conozca muy bien la tecnología de blockchain smart contras que están basados en solidity y otros lenguajes que parecen javascript si no me equivoco si has visto algo he visto algo porque estábamos haciendo un curso hace tiempo pero ahí está todavía en producción pero no no estoy muy metido creo que es algo orden del día y yo le digo a la gente meter también foco ahí porque es un mercado en auge ha bajado un poco por eso no el tema hay un hype y luego la cosa rebaja un poquitín Sí sí pero da un poco la sensación Como de que todo el cripto mundo ha muerto yo creo que no que no es así pero da un poco vosotros qué pensáis gente está está muerto el mundo cripto o sigue claro es que evidentemente vivimos una época con todo el tema del covid y esto que hubo como una burbuja súper grande subieron un montón todo el mundo estaba hablando de eso todo el día había mucho ven de humo entonces claro los nfts también todo el tema y con todo esto yo creo que la gente acabó un poco causandole rechazo sabes o sea saturación quizás no Y también que yo creo que para cierta gente yo creo que el concepto puede llegar a ser complejo no de explicar y de entender un poco este dinero virtual no lo tengo realmente

pero está en la blockchain pero el banco realmente no puedo comprar nada o lo que quería comprar no puedo comprarlo y luego la volatilidad es un problemón evidentemente es que justamente hablando de criptomonedas justamente La idea inicial La idea inicial del bitcoin era justamente que no fuera volátil O sea que no que no tuviese inflación como el dólar o sea como está desvinculada de todas las otras monedas La idea inicial era como que fuera más estable no Buenas tardes señor ney qué tal le va su día a usted y Compañía Pues muy bien diga aquí estamos aquí estamos últimamente me tratan mucho de señor pero bueno me hago sentir un poco más viejo pero no Bueno estamos ahí Bueno digo pues eso que yo creo que el tema cripto ha bajado bastante pero sigue ahí no O sea Sigue Sí yo creo que sí es un cosa que yo creo que no va a desaparecer yo creo que estar ahí quizás no tiene la importancia que tiene a día de hoy pero han hecho un montón de proyectos súper chulos por ejemplo de yo que sé pues hago una una aplicación y febrero los datos en una blockchain para hablar del no repudio no sé qué no todo esto sí el tema de trazabilidad también nos queda cosas para explorar no Y tú crees que realmente llegaremos algún día a tener O sea a que el dinero basado en blockchain sea algo relevante para el día a día ha pasado en países creo que es no sé si no es que no me querría equivocar pero creo que Bolivia o Ecuador utilizó No me acuerdo qué países creo que es Bolivia pero no no es otro es el Salvador El Salvador no que utilizaba bitcoin como como la moneda y realmente no les ha ido bien eh Tenemos aquí El Salvador vale no les ha ido no les ha ido bien digamos eh creo que era un poco mafias también el rollo que se llevaba una pregunta más concreta Vale qué tan seguro es el blockchain Pues yo creo que está diseñado de base para que sea o sea seguro para qué es no lo de siempre no O si quieres aunque no repudio transparencia no sé qué la tecnología que está bien de base cuál es el problema yo creo de blockchain pues para ciertas aplicaciones la velocidad no es nada tengo súper lento rápida entonces Claro si quieres federar tus datos en una blockchain y tal depende Qué tipo de tráfico tengas no te va a funcionar bien y Pero y esto de que se suele ir de que le han robado es que no estoy muy metido en este tema Pero ha salido como varios casos de que han robado a la gente han hecho estafas o han robado lo que pasa siempre no es decir si yo tengo una dirección de wallet que es mi dirección de moneda y de monedero y voy a hacer una transferencia hacia ti y Sebas me instalo un malware que en el portapapeles me cambia la dirección de la tuya por la de Sebas a esta buena esta me la contaste no sé si salió en el vídeo al final pero esta la contamos no y pasa eso no se ha ido no no hay una entidad financiera que tú puedas decir hola Perdona que me he equivocado con la transferencia está fuera ya se ha ido ya se ha ido lo has perdido etcétera etcétera los clickball managers son una comunidad y ultra mega agujero de seguridad manager sería como que sería una aplicación en la que tú puedes coger y decir yo voy a copiar diferentes de diferentes puntos de información en lugar de coger y decir copiar una dirección copio el email y copio una de cumpleaños pues lo pongo en el equipo manager y puedo acceder cuando quieras nunca usado eh No sabía No sabía que eso estas aplicaciones me dan mucho miedito porque hostia no sé cómo se almacenes ahí nunca me lo he mirado si no y qué tan fácil es acceden esa información pero es algo que está accediendo al sistema operativo es esta interceptando el tema de copiar y no no Mola no imagínate pues la gente que tiene diógenes de datos no bueno Perdona sigo contándome tu historia Cómo básicamente fue un poco eso empecé Y entonces me interesé mucho por el tema del malware y tal que en aquel momento yo creo que era algo que se hacía incluso menos o digamos que la industria era mucho más pequeña o conocida En aquel momento y eso ya tiene cuando he salido esa empresa realmente estaba como estábamos como avanzados a lo que estaba haciendo fuera no y ya me metí un poco en este tema

de la ciberamenazas los ataques de persistentes avanzados el mundo del cybercrimen que que es una industria que mueve muchísimo dinero en el mercado negro o sea es hay empresas del mal ahí enorme hay una escena del mal importante no Mira solo para hablar de datos hay un informe del cincel americano que dice que los pagos de ramsomware por ejemplo los han digamos datado de 5,2 billones Guau de lo que saben lo que la gente lo dice no la gente que ha podido trazar en la blockchain de esos pavos pero imagínate aquello que no se sabe o que se ha hecho otras criptomonedas como monero que la estás haciendo son públicas y te iba a preguntar ahora mismo estás en caspersky en el equipo greates Cómo acabaste pues es difícil entrar ahí sí claro yo creo que es como una élite es un equipo analistas de mucho renombre no Que obviamente pues la prueba es complicada se tiene que hacer un análisis te puedo preguntar que hace falta Cómo es la prueba Sí claro Mira te dan una pero pasa también similares eh te da una muestra software y te dice necesito que me digas Qué es qué hace si se puede atribuir algún grupo de actividad maliciosa que tú conozcas y que me expliques me hagas un informe de inteligencia sobre eso esa es como tu rama de especialización no inteligencia Y análisis de amenazas vale o sea digamos que tú analizarías malware directamente o lo que sea y lo que hago es un poco intentar ver si es un grupo de actividad malicioso Cuáles son las motivaciones para hacer esa campaña es decir Hay algún evento importante en el índice en el lindo Pacífico por el cual hacen la campaña están atacando un grupo de disidentes atacan periodistas atacan empresas por lo que sea las motivaciones no que son muy importantes y cómo sacas esta info de un de un programa Pues imagínate pues es un trabajo más de analista no es decir tú mandas tu imagen de una campaña de fishen dirigido en el que tienes un documento ofimático cuando tú lo abres te aparece información sobre una feria que se va a hacer en cualquier país x que lo ponga tu audiencia el país Aquí es que es un evento que va a ocurrir a futuro no va a cubrir por ejemplo en dos semanas entonces poner un documento allá la gente lo abre por debajo eso cuando habitas las macras por ejemplo spawnea lanza por ejemplo un comando en tu máquina que descarga un fichero de internet y te infecta la máquina con un skiller que te roba los datos por ejemplo no aprovechando el gancho tengo algo con responsabilidad tienes pues un ataque contra gente que va al Mobile si solamente se ha enviado a un sector rollo empresas de negocios o empresas de retail pues ya sabes que tampoco van a ese sector si el mensaje pone algo que está Solamente yo que sé yo que sé para aquellos interesados interesadas que van allá que van a llevar un gorro rojo y chaqueta negra Pues sabes que solamente van a hacer un sector concreto de usuarios Pues todo eso analizas los datos hay digamos técnicas de análisis de inteligencia donde tú haces una cosa que se llama por ejemplo no ach que son técnicas de teoría de análisis de hipótesis competidoras que no que tú haces una matriz no Y tú aplicas una puntuación a cada matriz y es un poco para quitar el sesgo no del Análisis si yo sentía que vivo aquí y tal pues puedo aplicar un sesgo no En los análisis técnicas humanas no es un programa que lo ejecutas y te lo hace sino que eres tú con un papel a día de hoy haría cosas interesantes y tienes que hacer hipótesis sobre los datos eso es vale o sea a ti a tu mesa te llegan unos datos de un email de ejemplo a quien le llegó este email ips no a lo mejor tienes que intentar mapear esa infraestructura donde está colgando siempre también a un grupo criminal no hay una cosa que se llaman las ptps que son las tácticas técnicas y procedimientos que es un poco como clasificamos desde la industrialidad a estos actores para decir hostia pues este grupo que siempre compra vps en digital option que siempre utiliza documentos para infectar a los usuarios y que siempre utiliza steelers se llama nate gentiles y el nombre como lo dije pues el primero que lo descubre Sí vale Okay entiendo eso sí básicamente y esta especialización como

hemos dicho que se llama bueno analista de inteligencia o la lista de malware o investigador depende un poco la empresa que te contrate Y esto es tu especialización o sabes hacer más cosas de consultoría he hecho un poco de todo porque he pasado al final por múltiples equipos al final me gusta tocar un poco de todo también y puedo hacer hacking puedo hacer después encientos análisis forense pero lo que me gusta mucho es analista de inteligencia Y antes me comentaste fuera de cámara una cosa que me dejó un poco un poco loco dijiste que hoy en día es más difícil que nunca a ver Bueno no sé si más difícil que nunca porque es más difícil ciberseguridad Sí es muy fácil de entender es decir tú cuando empiezas hace años la cantidad de tecnologías cosas a proteger cosas a proteger y demás estaba muy muy limitado realmente había había poca digitalización era mucho más digamos estanco no y la y la manera de explotar esas vulnerabilidades Era realmente algo nimio no a día de hoy la superficie de ataque es decir aquello que publicamos en internet es decir si tú y yo la montamos un servidor web que puertos pondríamos a escuchar 22 para ssh si no lo cambia por cuando cuando tienes 80 no y internamente hacia dentro del 3306 para la base de datos por ejemplo Cuántos servidores de internet hay de esto millones es decir y cuántas maneras de explotar eso hay a día de Cuántas versiones de software hay tenemos Los Apaches y SS Cuántas bases de datos tenemos versiones diferentes el abanico es gigante las tecnologías es gigante y las posibilidades son gigantes Entonces tienes que decir algo no O sea tienes que empezar por algo es lo que digo yo a la gente toca un poco de todo De hecho los programas de Master ayudan mucho a tocar un poco de cada palo y luego digo hostia Pues a mí me gusta mucho el hacking Ya pues enfócate en eso y ser el maldito Master de hacking Cuando hable de hacking A qué te refieres O sea que es que analizar infraestructuras y páginas webs y aplicaciones o aplicaciones móviles y decir hostia Pues yo soy muy bueno rompiendo la seguridad de estas aplicaciones me encanta eso vale que le das una aplicación y otra intento romper eso es por ejemplo un formulario o un buscador y intento inyectar comandos para poder sacar es el típico de comilla uno igual a uno puede inyectar en un buscador y que te devuelva datos no al final aplicar técnicas de hacking pero claro qué necesitas para eso conocimientos de sistemas operativos conocimientos de redes si haces aplicaciones móviles jamás Swift o algo de esto para realizar código y evidentemente técnicas de hacking de cómo hacer inyecciones hacer bypasses porque obviamente los sistemas de seguridad avanzan y te filtran las comillas te filtran las comidas simples te prohíben alguna el uso algunas palabras y tienes que cambiar hexadecimal tienes que hacer un montón de cositas No es tan fácil como el tema es que imagino yo por ejemplo bueno trabajé de desarrollador mucho tiempo diez años estuve y bueno Toqué mucho frameworks de php pero también de python sobre todo y rubion Race también no de y claro Igualmente tengo una versión parcial no conozco otras versiones no conozco todas las vulnerabilidades hay cosas que no entiendo cómo funciona del todo porque nunca me las he mirado porque me dan igual y claro o sea sí que es verdad que en algún momento he hecho alguna inyección sql así de risas y salió bien pero o sea realmente yo dedicándome a eso tampoco conozco todo no o sea es como que si tú me dices me sueltas una aplicación web en un frame porque yo nunca he usado yo igual no no te sabría cuando llevas mucho tiempo en esto sabes que cuando ves la URL Y ves yo que sé natile.com barra ID igual dices aquí si yo por ejemplo pone ida igual al 98 yo cambio 99 y la página web me actualiza la que la que yo quiero digo Aquí hay numeración es decir puedo ir enumerando por los por ejemplo metodología estándar o sea tienes una checklist de cosas claro de hecho Ahí está ahí digamos organismos hay uno que se llama la hoguas que mundial en el que cada año Perdona cada año cada ciertos años sacan como el top

ten de vulneralidades que se están explotando Ok Ok entonces tú tienes una metodología para probar De hecho hay muchas empresas que te dicen no no estoy alineado a la owas que ya he probado los 10 ataques más más posibles digamos y pero todo el día todos los días van saliendo cosas nuevas realmente muchas cosas derivan de ataques existentes no hay por ejemplo un truquito que se hace con closet scripting para robar el hacer haciendo un documento Cookie para robar los datos de sesión de otras digamos hay otros ataques que quizás roban la sesión pero que se va a ser un poco en este principio porque hay alguien que encontrado una manera novedosa de Cómo explotar eso Entiendo entiendo entonces si yo sé que es muy extenso a esta pregunta pero si me pudieras contar un poco qué roles y cuáles son las especializaciones dentro del mundo de la ciberseguridad vale es muy amplio no esto es como si me preguntas a mí Cuántos tipos de programadores existen pues tío Cuántas tecnologías existen infinitas que son la gente que hace defensa aquí tienes puedes encontrar gente que pueda ser capaz de accionar un sistema operativo es decir aplicar todas las minas de protección aumentar las defensas a fijar los firewalls poner sistemas de detección de intrusos todo eso tecnología de defensa que te la pueda configurar o sea por ejemplo si yo un arquitecto de seguridad por ejemplo pongo mi Access Point y hago que no se puede acceder a la red interna que esté en otra red por ejemplo pongo antivirus en todos los ordenadores que sea obligatoria la contraseña que caduque a la hora de aplicar todo eso tienes que pensar en políticas de ciberseguridad es decir por ejemplo No permito la conexión de usbs en las máquinas corporativas por ejemplo vale del usuario caduca cada tres meses esos son políticas que se aplican a nivel de interno Y qué más por ejemplo si más difícil Bueno creo que lo más difícil que puedas hacer como en la parte de defensa sería intentar aplicar medidas de seguridad que no rompan el negocio es decir tú Imagínate lo más seguro que sería pues no dejo que se conecten segura No esto lo hice hace poco dije claro el WiFi de hecho puse más te acuerdas el rollo y la contraseña que puse que era como y estaba como 10 minutos una serie de reglas nemotécnicas y era larguísima tío y al final dije nada igual una un poco más simple también cambiamos el el lo cambiamos para que sea como Random total O sea no tiene ninguna lógica no tiene ningún sentido el nombre hemos cambiado los los bueno los Access y Bueno un poco todo eso está eso está bien pues aparte de lo de la parte de Blue Team Lo más complicado es aplicar medidas de defensa sin romper la operatividad de la empresa es decir por ejemplo Imagínate que sea una buena calidad vale Y esa vulneralidad no puedes no puedes parchearla pues para echarla porque se ha descubierto que el parche cuando lo aplicas te rompe la impresora por eso te rompe el ordenador porque no O te hace un Blue screen o una movida de estas hay muchos en points por ejemplo que hablamos en el vídeo que hicimos que tiene una cosa que se llama virtual patcher aplica el parche de forma virtual para mitigar esa voralidad no pues eso es una solución que hay para digamos que las empresas no tengan unalidades presentes porque igual no las pueden aplicar claro esto es una pregunta que siempre me he hecho porque realmente gran parte de los problemas que existen hoy en día en empresas es porque tienen software obsoleto no súper viejo sin parchear lo que se llama el Legacy tío lega que es la condena de muchas empresas y muchos equipos que tienen que verse obligados a mantener ese parque porque no tienen presupuesto para comprar nuevas máquinas o porque digamos que las aplicaciones que sustentan esos sistemas Legacy no hay nuevas versiones porque El fabricante igual ha desaparecido hace muchos años trabajé nada un añito en cuando tenía 18 o así en el departamento de informática de gas natural gas natural que luego compró Unión fenosa o sea no sé si justo en ese momento cuando se unieron y me acuerdo que los ordenadores o sea las web corporativas sólo se podían utilizar con Internet

Explorer tiene que ir tan lejos en para hacer una declaración de la renta hace un tiempo Java 1.6 y interés por el 6 o 7 es decir que en serio hace tiempo ahora ya está solventado algún momento yo tenía una máquina virtual solo para hacer operaciones con la administración electrónica qué fuerte nosotros en la empresa recuerdo eso que teníamos como ordenadores que tenían Windows no me acuerdo si era XP o anterior no me acuerdo Creo que creo que era XP que tenían Internet Explorer que tenía era una versión concreta que no sé si a las 6 o las 7 y eso lo necesitaban para acceder a la intranet que era una web que petaba un montón que nosotros hacíamos también reportar Banks y cosas de estas y era horrible y claro eso era Mira mi agujero de mi primer trabajo de informática Fue en un call center en el que yo daba soporte cuando la gente hacía la renta quizás el programa padre técnico uno de ellos era yo y te decía no acaba de salir Windows Vista para que la gente un poco haga idea de cuando es la época Y entonces estaba aquello con Windows Vista de ejecutar como administrador que eso era nuevo cuando estaba entonces si tú quieres instalar Java por ejemplo tienes que hacer ejecutar como administrador o te daba error no Entonces yo tenía un manualillo que me habían hecho de cómo explicar a la gente de veis acciones de internet esa dirección de confianza Pon aquí https://at.es y añadelo como confianza porque cuando hacías las operaciones electrónicas si no tenías eso añadido por tema de certificados y tal la web fallaba y la gente no podía hacer la renta y había un equipo solamente nos dedicamos a solucionar el rollo esto era lo que hacían natural me llamaban y me decía no me vale intranet vale vamos a ver vamos a ver qué le pasa al Internet Explorer no me acuerdo hace muchos años no pero también era como Vete a la página de opciones de Internet Explorer dale un instalador que tú lo ejecutas y te configuras el sistema no pero antes era a manija eh Y me acuerdo una anécdota con una señora que le dije que estaba viendo la pantalla y me dice no veo una ventana y me dice vale ciérrala y Señora señora y se había levantado el ordenador era como claro te podía Llamar cualquier persona desde aquí quiero utilizaba nunca la ordenador hasta gente que la que sabía lo que hacía me llamaba un tío un tío una vez que era de yo que sé de un sitio de Galicia Mira donde estaba esa Unión fenosa nos decía el ordenador que tengo aquí es muy importante aquí está la puerta que deja pasar el gas a España desde no sé dónde y este ordenador tiene que funcionar como Dios Qué presión No sé igual nadie rarísimo en el ordenador y me acuerdo una cosa muy turbia que me decían no no Yo es que enciendo el ordenador me voy a tomar el café y vuelvo a los 15 minutos porque tarda 15 minutos en arrancar mira como What the fuck O sea no me puedo creer que estén trabajando en estas condiciones a mí la gente se sorprende cuando yo le digo cada cinco o seis años hace cambiar el PC o el portátil y la gente me dice que estoy loco digo a ver qué quieres es lo que hay y bueno nosotros cada menos seguramente No pero bueno probablemente probablemente depende lo que te compres la adquisición buena y bueno pues espero tenerla más tiempo y ahora lo que te comentaba que claro yo entiendo en el caso de hace muchos años yo creo que ahora Ha cambiado todo seguramente o no igual voy ahí un impacto que te cagas encima esto eh Porque es lo que te quería decir no que esto es como súper peligroso tener estos sistemas operativos tú imagínate un caso que me encontré que es interesante explicarlo no diremos nombres pero ultra mega grande vale que la gente va por el centro de las grandes ciudades y lo puedes ver es un sitio muy grande vale Y tenía que hacer una respuesta incidente es decir dar respuesta a un incidente se había pasado algo había pasado alguna infección de malware vale Y tenía que adquirir evidencias de las máquinas Entonces era un parque igual no sé de no sé de cuatro o cuatro mil equipos algo grande no si tengo que ir uno por uno para mi empresa perfecta porque va a facturar un montón de horas Pero el cliente estaba muy enfadado porque tiene que

pagar mucho dinero no perder mucho tiempo qué tienes que hacer automatizar pero qué pasa si por ejemplo quizás automatizar con power shell y tiene Windows XP y las máquinas no tienen Powers es problemón o algo no de los ordenadores traiga unos ficheros y nos traiga un ordenador central para poder analizarlos No si yo no tengo capacidad de poder automatizar con sistemas operativos Legacy tengo un problemón realmente no y tengo que buscar historias para hacer cosas ahí Y qué hicisteis pues lo que hicimos fue con un amiguete utilizar el propio antivirus que tenía los sistemas instalados para usarlo para recoger ficheros de las máquinas Wow Como te estás ejecutándose como como System no como súper administrador podemos recoger ficheros y memoria de las máquinas con la ventaja que tiene estar en la empresa del antivirus que tiene la gente no o sea esto pasa queda un poco de miedo no que tenga tanto acceso a cosas el antivirus también Bueno al final también lo tienes son otros programas Lo que pasa que obviamente pues cuando hablas cuando miras un poco cuando eres consciente un poco lo que puedes hacer pues obviamente entiendo que puede haber ciertas eficacias no pero al final si quieres un software que pueda acceder a ciertos niveles de sistema operativo necesitas que ejecute con estos permisos al final y bueno al final es eso no que incluso otra cosa que causan muchos problemas en las empresas es director y no es maldito programa de Microsoft Bueno yo de hecho soy Soy bastante fan tío bastante fan Sí porque es una buena manera centralizada de aplicar permisos hacia todo hacia todo forzar unos premios a toda organización que es cuál es el problema que muchas veces no se configura bien o no se aplica las políticas de seguridad correspondientes os explico un momento que es vale para que sepáis y Bueno deja de ser un software que ofrece Microsoft para poder organizar una empresa los equipos de una empresa con políticas de seguridad con y puedes digamos crear grupos de trabajo grupos de usuarios y al final tus acciones de formas centralizada usando esto que se llama o sea sería como que por extender un poco en lugar de Iniciar sesión en un ordenador con Windows por mi cuenta hay un usuario de red no o sea es un usuario que me ha creado un tío en un ordenador en un servidor y yo cuando accedo esa máquina inicio sesión con mi usuario y mi usuario tiene permisos digamos no tiene tiene un perfil aplicado a ti no con donde dice que programas puedes tener Qué tipo de configuración que si puedes cambiar esa pantalla o no incluso puedes hacer que cuando inicias sesión se ejecute algo Sí claro de hecho Ahí lo que se llaman los logone scripts que cuando tú inicias por ejemplo te mapee las impresoras que esto falla a veces me acuerdo que era una de las incidencias que bueno por lo menos En aquel momento cuando los grupos de ram software hasta acá las empresas lo que hacen colocar este ramsemware en el sismol en la carpeta de Logan y cuando alguien arranca cifra todas las máquinas a la vez es eso no es un arma de doble filo va muy bien para manejar nosotros por ejemplo aquí yo yo tampoco quiero explicar cómo lo tengo aquí montado públicamente porque es peligroso verdad bueno Vale podemos hacer otro programa así pero realmente sería peligroso no que yo que yo explique ahora mismo aquí en Twitch a todo el mundo como tengo montado todo aquí explicando las conversaciones que tiene sino más incluso podrías explicar Oye pues mira he intentado alinear la seguridad a este estándar ISO o a estas políticas de seguridad para la gente también sepa un poco lo que tiene que aplicar Pero bueno intentar daros menos detalles posibles vale vale vale entonces voy a decir nada mejor porque es bastante bastante como muy tal sabes vale Vale pero digamos que algún consejo para Bueno vamos a hablar directamente de esta pregunta cuáles son los ataques más típicos que ocurren en una una empresa que es lo más probable que me puede pasar vale hay que diferenciar un poco ataques por parte de los entes externos y también hablaremos también de cuando entran dentro Pues los ataques que

observamos no esa diferencial cuando los atacantes están fuera de la empresa fuera físicamente si fuera digamos que no están con un usuario autenticado dentro y una vez que consiguen accesos porque el paradigma cambia un poco vale si están fuera lo que normalmente hacen es intentar explotar una aliadas vale lo que hacen es buscar en soda o páginas similares y la empresa que software tiene publicado en el hostia Pues tiene un wordpress que no actualiza desde hace un montón y tiene una inyección sql o sea como pueden ver esto Pues has utilizado alguna vez sí pero no sabía que podía Buscar una empresa ahí puedes buscar todas las empresas bueno todas las direcciones IP por ejemplo de España que te hagan corriendo wordpress 4.5 por ejemplo Y cómo sabrían que es mío en wordpress Bueno pues si hago mapeo de una dirección IP a un dns yo puedo saber que que la IP LP es tuya Yo podría mirar mi página web no O sea miraría en agenda.com hago un Quiz o un Pink o un ping Entonces me dice la IP y además balanceador como como sí que estoy Vale qué es lo que hay que hacerlo cogeremos yo que sé con cualquiera de los que hay ahí y digamos que si no es un balanceador pues sobre la IP la que está sirviendo ese contenido que puede ser su servidor propio solo una IP a un dns o una IP compartida con un Hosting que tenga más webs vale entonces a partir de ahí con este IP por ejemplo le puedo mirar en shodam que puedo mirar con esta IP sabes que yogan va escaneando todo internet todo el rato entonces lo que haces almacena un estado del tiempo que es lo que está corriendo en esa en esa IP y podría decir pues tiene corriéndose sh en el puerto 22 y está configurado con usuario y contraseña o certificado tiene un apache o una engine corriendo en 443 entonces y la versión Si la tienes si el banner lo tienes publicado digamos entonces lo que hay que hacer es buscar exploits para esa versión Y si tiene la suerte que tienes uno que es lo que se llama rc Remote Pues ya sabes al azar utilizan mucho por ejemplo las historias que sube la gente a Instagram sacándole foto al montior del trabajo para robar datos Y ser más fácil el hacking qué pregunta es lo que se llama como shaders no el poder yo más gente Pues antes he visto que cogías el iPad y ponías el post no me quedaba con todo el resto pero es algo mirar un poco lo que está haciendo otro para para coger la contraseña esto se hizo muy famoso en la época del hacking antiguo que se descubrió la password que lo de un nodo de uno de los operadores de aquí y todo el mundo tenía como acceso a internet gratis y estaba ahí manejando Pues aquí mira por encima del hombro de Sebas Pues se ve el password escondes tú te escondes así desbloquear el móvil bueno sigamos con el tema de los ataques no externos la página web publicada no Y eso sería en cuanto a cosas pasivas es decir no vamos a Escanear la empresa en ningún momento pero también hay scan en qué sentido no vamos a Escanear la empresa porque yo si yo miro el shodal yo puedo mirar y tú no sabes que has mirado vale vale esta esta es una pregunta que tenía y me las contestado ahora mismo vale mirar en una base de datos lo que hay sobre ti digamos que yo podría tener un ordenador Y desde ese ordenador mirar Qué puertos tienes abiertos en esa IP Pero estaría haciendo algo no de forma pasiva de forma pasiva de forma activa yo puedo escanear activamente una máquina entonces tus perimetrales tu servidor si tú lo miras tú verías que alguien te está escaneando está preguntando qué puertos tienes abiertos Ah o sea es un comando que pregunta que puertos tiene abierto Así es un comando que lo que hace es va probando puertos no O sea vas probando todos los puertos a ver si hay servicio vale Sí entiendo entonces Claro mi sistema podría estar configurado para tener algún tipo de log que diga Aquí hay un tío que está probando los puertos no está preguntando de hecho a ir como creo que dos maneras de configurar esto en modo de respuesta que una es te mando un reset o directamente no te contesto o directamente no te digo no te digo nada también te aparezco como que está cerrado en realidad Está abierto Solo que no te dejo que preguntes vale

vale Por ejemplo si me conecto por ssh Y yo que sé cómo harías o sea tendrías que si no mandar usuarios y contraseña no le contesto o algo así no lo que puedes hacer por ejemplo si en el banner en la herramienta que estaba utilizando por ejemplo viene más no sé si conoces la herramienta Pues no te voy a no te voy a contestar y además te voy a bloquear un patrón digamos el banner de la herramienta o digamos que el modo de escaneo es conocido no es un patrón conocido que yo veo que alguien me estás cañando Yo ya lo tengo fichado de alguna forma si por ejemplo por ejemplo pruebas varios intentos de conexión a un puerto o preguntas de manera muy rápida este Puerto ese puerto ese puerto ese puerto de manera muy rápida Oye me estás escaneando Te reseteo la conexión sería el equivalente a que yo Viva en una casa y se pase un tío hasta que tú digas tío las cámaras este tío quiere hacer algo Antes de hecho hay gente que mantiene direcciones de salida de ip de salida de shodan para lecturas para bloquear en tus sitios y que no permitas que escanee evidentemente no tienes porqué estar en soda si no quieres no sudan para que os hagáis una idea es es una Bueno un servicio es una empresa que se dedica a vender estos datos que tiene un montón de servicios súper chulos vale Pues básicamente eso dan lo que haces escanear internet o sea escanea todo prueba todo se intenta Conectar a todo y te dice aquí hay una Webcam Aquí hay un servidor tal o sea escanea internet básicamente por ti no entonces ahí pues es una y esto Es legal no realmente no hay nada de malo a nivel legislativo Pero yo siempre diría Oye gaita para escanear mi red No lo que pasa que lo dice que lo hacen con ánimos de research claro es como si yo voy a picar a todas las puertas de todas las casas es ilegal quizás alguno cuando piques se hace así no pero claro igual le puedo denunciar o sea Exacto ilegal picar en puertas no es realmente sabes o sea pasiva entiendo que no hacen mucho ruido si no ya estaría más que denunciado este tema pero hay más proyectos eh es otro proyecto que también hace hace eso y hay otros proyectos también lo hacen hay muchos proyectos que hacen esto de hecho hay universidades que tienen escáneres que van escanean internet y que he hecho en el envío de la conexión http te dicen Oye soy de la universidad tal que es como quieres que te escanee avísame flipa un poco la historia yo te escaneo Pero si no quieres que te escanea avísame y te quito del pool y es como no preguntarme antes no sí sí sí sí sí Exacto es un poco ese rollo entonces bueno vamos primero en soda miro de forma pasiva forma pasiva encontramos una Sí pero necesito la ip de esa persona objetivo vulnerables que son de tu interés Okay entonces el primer ataque sería un ataque directamente la web Pero bueno la web normalmente no está aquí o sea si yo tengo una página web normalmente la tengo en un Hosting en lo que sea eso pero tú puedes coger y probablemente probablemente parte de tu infraestructura la tengas en el mismo datacenter que tu página web Okay Vale no suele ser raro que tú tengas un vps guarro con la web en un sitio y toda tu información informática la tengas en otro tipo así es el mismo parque para para todo no entonces lo que hacen es una vez que ven ese objetivo miras avisa de alguna manera de explotar vale si la consigue el acceso vale Y ya tiene la primera la primera víctima que yo siempre lo llamo el paciente cero Ok vale que es como no sé si te muevas de zombies pero sería como llegar a alguien de dentro de la empresa te refieres ya como comprometer primero la el servidor inicial vale estamos hablando de comprometer una infraestructura luego hablaremos de mandar un espíritu físico y comprometer a un usuario Okay Vale hemos comprometido una máquina virtual una máquina virtual donde sea una vez que conseguimos este acceso lo que hacemos Es intentar recabar más información por ejemplo contraseñas navegamos pues sistema operativo y encontramos que los pagos están en un ficheros de texto otro tendrías que conseguir entrar en ese servidor por ssh o algo no no O sea lo que haríamos es una vez que lanzamos este Comando de exportación nos daría una shellmanca tienes

Estás vendido es un queso gruyer importante aplicar medidas de protección ahí y luego también por De hecho hay una web que se llama cheese o algo así que te mira los agujeros de tu webs hay varias empresas que se dedican a mirar a hacerte una de riesgo Depende lo que hayas publicado y que a lo mejor encontrarías una vulnerabilidad en wordpress o algún tipo de php es que te permitirá Añadir usuarios a base de datos o subir una shell que te dé acceso remoto para luego tú puedes hacer operaciones como dumpear la base de datos que tienes un montón de usuarios o llevarte ficheros del servidor por ejemplo me llevo ltc Shadow Linux pero lo que sea es todo lo que pueda robar de ese servidor desde desde temas de usuarios de administradores que se conectan al sistema otras cosas que si yo lo pienso realmente cuando estoy cuando estás conectado a esta máquina virtual a este ordenador remoto a veces dices voy a tener la contraseña en el comando sabes menos p y pones la contraseña Claro claro exactamente Aunque hay algunos que te borran el historial Sí hay mucha gente que tiene el base rc o en el zshrc tienen una alias o una configuración que cuando salen de terminal Borra el historial vale vale eso también es posible son cosas de seguridad operacional que tienes que aplicar para para Pero bueno cuando vas tiras un sistema operativo estas cosas ya te dicen que las tienes que hacer hay una lista que hay para todos los operativos del mundo en el que tú te bajas la guía aplicas los lo que te dicen y el sistema operativo se vuelve más seguro Okay okay vale Vale entonces hemos dicho la web Y luego qué más conseguimos usuarios de acceso y lo que hacemos Es pivotar es decir saltar a otras máquinas Porque si consigo por ejemplo el usuario o la clave privada del usuario ssh significa que igual me puedo lograr en más servidores si consigo la clave privada claro podría Conectarme a servidor de servidores además normalmente no digo que pasen todos los sitios pero en muchos sitios quizás la puerta de entrada está un poco más cerrada pero por dentro es un maldito drama no hay firewalls intermedios no hay está todo digamos un montón de máquinas no hay segmentación por tanto un poco el atacante un poco se pone las botas Hablamos de una situación ideal quizás no yo creo que pasen todos los sitios pero muchos sitios pasa que la puerta de fuera está como muy cubierta esta gente se la toma En serio y cuando ves dentro está es un drama no hay nada no hay nada puesto y qué más y ahí qué podrías hacer pues pivotar otras máquinas para conseguir más accesos y acabar por ejemplo cuál es tu objetivo robar datos pues empiezas a llevarte datos bases de datos datos de clientes Esto es lo mítico que sale de vez en cuando que por ejemplo cuando se filtró todo el código de Twitch con todas las bases de datos todo lo que ganaban todos los streamers son cosas que pueden suceder a raíz de una vulneración de datos donde no toca por un error de configuración porque al ser protalidad por ejemplo entonces La idea es llevar una cifra estructuras conseguir por ejemplo también alojar contenido malicioso o contenido pornográfico pedófilo y luego te pueden denunciar Y quién alojar contigo a veces vigilar un poco lo que la seguridad de nuestro sistema porque podemos ser digamos podemos hacer Delivery de un montón de cosas que no queremos esto me pasó a mí cuando hace muchos años Cuando recién lancé lo que era la anécdota Academy que era la antigua mastermind que era Bueno yo subía mis cursos ahí de python y de javascript y tal Y ahí recuerdo que era un wordpress y no sé si me entraron por el plugin del banner o algo de eso los clubes este no lo tenía nada de hecho lo actualizado cuando me acordaba y recuerdo que me pusieron algo un código malicioso que era que yo cuando accedía la web no veía nada raro vale pero la gente que hacía desde fuera x Random entraban en una web que era un Clon de la mía y tenía un montón de bueno robaban contraseña y aparte había un montón de cosas vale había de todo era el demonio esa web esto esto pasa esto pasa y de hecho yo le digo a otro mundo que cuidado con los plugins de wordpress Porque primero

que te impacta el imperformance segundo a veces la gente lo quiere hacer porque no sabe programar una funcionalidad concreta entonces utiliza un plugin Okay les impactan performance de seguridad que hay que mantener es decir que cuando acceda la web me salga el banner de suscríbete al Canal de twit vale Sí sí pero yo como de su radiador un día decido Bueno quiero trabajar más en esto olvidado no lo actualizo y sale una como administrador esto Pues igual te tocaba mantener este tipo de plugins no o también los temas estos no que compras un tema en la típica web está Team Forest y tal que viene con un montón de cosas y claro eso igual eso es aún más peligroso porque tiene capas y capas de software y plugins y cosas y sistemas propios no y de hecho con colegas nos hemos encontrado que instalamos por ejemplo yo que es el plugin este no sé el elemento uno de estos de golpe y depende que O te das un plugin de touring de base de datos y despegar unas bases de datos con opciones de operaciones de escritura lectura y tal que os cuidaos ella tiene cuidado eso es un problema muy grave tío Además porque mucha gente que programa plugins de wordpress no es que sean hachas en programación y lo hacen para su caso de uso y gracias a ellos Es verdad que a liberar el plugin y lo hacen gratuitos pero sí sí totalmente Pero y no hay que quitarles ese valor evidentemente instalando código de un tercero se han visto casos muy chungos de cosas muy muy peligrosas que habían hecho o muy poco eficientes o de hecho es lo que pasa a veces que son una obligación que utiliza miles de millones de personas y claro pues un atacante que tenga una ejecución remota de código dice A dónde le pego Es que le puedo pegar a todo el mundo Sí sí sí increíble yo os recomiendo a todo el mundo que tiene wordpress seguirá su web y hacer barra en realidad me punto html radio html y si salta la versión quita ese fichero porque todo el mundo sabe la presión que tienes vale esa es buena eso y el WPA admin también porque mucha gente se lo deja se lo deja abierto y ahí puedes ver todos el problema es ese que mucha gente cualquiera se puede mandar un wordpress no Claro pero saber cómo tienes que proteger de uso de mortales que llamo yo que son los que te cuestan dos euros al mes y tal que tú te puedes decir instálame un wordpress desde un botón no tienes que hacer nada que eso es bueno de hecho porque ni nada de eso sabes qué otros ataques tenemos en empresas posibles así tendríamos por ejemplo los que son dirigidos a empleados no por ejemplo normalmente suele ser una campaña de phishing en la que te envían un correo electrónico que acabas abriendo que acabas o bien metiendo una creencial entonces luego se usa para acceder a los recursos de la empresa o bien instalado de un malware que alguien de forma remota controle ese ordenador nosotros nos pasó esto de hecho es como le roban a mucha gente de hecho hay muchos han pasado muchas cosas estos últimos años vale De hecho hay un hackeo muy famoso en los canales de YouTube que es que te borran todos los vídeos te cambian el nombre del Canal y te lanzan un directo de elon más que hablando con unos inversores no sé si lo has visto y te ponen ahí no sé muy bien Qué hacen Supongo que te piden que inviertas pues yo hay una cosa que veo incluso peor que aún estoy viendo un poco como lo hacen que es que te roba la cuenta de Instagram y te borras la cuenta para qué pues eso pasa no puedes hacer nada porque no hay vaca no hay ya imagino ya y esto le ha pasado algunas empresas de renombre y es como han perdido Cuánto cuesta subir followers y tal Sí sí es una pasta y no hablamos solamente de dinero en hablamos de inversión de tiempo de trabajo esto por suerte sí que te lo recuperan O sea hay incluso colegas míos de hecho uno de los casos de hace poco que fue sfd es un canal que hace contenido de tecnología también suele hacer como un poco ordenadores locos los arregla así como cosillas en casa y tal está bastante Guay arreglas gráficas y todo esto que se ve que tuvo un problema que borró no sé qué le pasó perdió datos en su ordenador y se bajó un programa pirata

de recuperación de datos vale Y parece ser que este programa Le leyó la sesión de YouTube del browser En serio sí y con esto o lo que estaba subiendo no no O sea el programa que se instaló en local vale parece ser que le copió la sesión de Youtube de su browser Vale entonces se la mandó al atacante y el atacante usando los archivos se conectó a su cuenta de YouTube Porque claro Es realmente Google lo tiene muy bien montado en Principio o sea tú es muy difícil robar una cuenta de Gmail no me dices que no que es súper fácil No es fácil pero si no lo tienes pero lo que estoy viendo es que aún teniéndolo muchas veces te clonan la Cookie de la sesión y pueden entrar como tú sin seguridad no es tan fácil No es tan fácil No es tan fácil no hay otros mecanismos no solamente es la copia de sesión sino que también es la localización desde donde entras el navegador a través de tu ordenador quizás directamente yo creo que va a ir más por ese estilo India y pongo mi usuario contraseña me va a pedir un top factor te voy a decir aquí lo que harían realmente sería que yo tengo este malware en mi ordenador y el atacante está actuando a través de mi ordenador o sea se conecta podría ser un caso plausible por ejemplo o que el usuario a veces no se percate que le han pedido el factor y no se lo ha pedido Wheels no se lo ha pedido él vale eso también pasa otro también que pasó muy muy fuerte este año fue que muchos creadores que fueron al cs al ces de Las Vegas cuando volvieron le hackearon el canal creo que fue chataca Michael Quezada hubieron como varios tecnológicos que estuvieron en eventos allí y que ahí pasó algo y de repente todos estos canales hay algunas conferencias de hacking en la que no actives O sea voy yo voy en modo avión y hay gente muy inteligente y fuera que puede hacer millones de cosas de estas conferencias de hacking tan famosas ni en el hotel de la conferencia porque te abren la puerta del hotel con con bueno flipceros el sistema Atlético de la puerta te hable y te roban todo por nosotros hace tiempo yo hice un vídeo en un hotel de cinco estrellas de tenerife pero voy a decir cuál es y bueno grabé ahí hicimos una simulación de cosas que pueden pasar porque no queríamos problemas vamos una simulación en plan Hacemos como que vale fuera de cámaras intentamos clonar una tarjeta luego lo conseguimos eh No no la de la habitación no lo conseguimos Pero eso lo hiciste con algún programa lo hicimos con con un lector vale en un ordenador vale leímos los datos de la tarjeta Pero había algo que no no sé qué era vale Y no conseguíamos clonarla se la clonamos y no iba yo he probado con flipper 0 a hacer esto y se puede configurar cero es el portal es brutal al alcance mucho más fácil cosas que hasta ahora no era mucho más difícil de poder hacerlo y bueno sigue contándome esos ataques de empresa qué más puedes hacer ataques hay una cosa que se llama mitre vale que es un estándar que ahora está muy de moda la industria que te hace una matriz en la cual tienes evasión de defensa escala de privilegios compromiso de credenciales coman en control evasión y para cada una de esas tácticas Tienes unas técnicas por ejemplo compromiso de credenciales pues utilizar una herramienta que se llama mimicats que la ejecuta si te rompe las credenciales del sistema operativo así fácil vale o sea en un ordenador ejecutas eso y te rompes las creencias tiene mecanismos para poder sacar las pagos esto en Windows no sé si sigue siendo en el archivo Sam Este sí señor que te protegía el archivo de las contraseñas para podertear eso vale digamos te pone una técnica que credenciales y un procedimiento que es ejecutarse pues hay empresas que dicen hostia como no sé por dónde empezar a protegerme voy a coger la matriz de mitre y voy a probar y voy a intentar ver cuáles son los esquemas de ataques utilizan y voy a aplicar de fechas contra eso no es fácil eh decir por dónde empiezo en la pared también Sí claro esto pasó hace bueno en una empresa por aquí cerca pasó que les hiciera un agujero en la pared de la nave y les entraron y con un inhibidor Es que de hecho toda la gente a mí me encantaba yo no la verdad que no soy experto

en eso que sí que hacer hacking más físico de que saben cómo inhibir una señal hay una serie que estoy viendo ahora no recuerdo cómo se llama que hablas sobre uno de los especialistas en robo más famosos El sapo no recuerdo cómo se llama sí sí sí sí sí es brutal eh un banco y ni bien la señal el tío Y entonces le preguntan Cómo lo haces así te lo voy a explicar esto O sea que toda la gente hace aquí en físico cuidado que son muy buenos o lo que yo había visto mucho y lo he probado un kilover por Hardware un kiloger es decir tú bájate te acuerdas aquellos teclados que van por PS2 Vale pues yo saco el PS2 coloco un kilo un kilo por Hardware y luego es un módulo Bluetooth que manda hacia un sitio todo lo que tecleas esto básicamente es un USB o un PS2 que lo enchufas en el entre el teclado y el ordenador no esto creo que salía no sé si salían Mister robots puede ser no sé Ah podría ser Pues sí podría ser es muy llamativo que suena así o el flipper 0 el flipper cero tú puedes confiar unos scripts Sí sí lo he visto lo he visto eso conectas un pendrive al ordenador El que es un pendrive que lo conectas al ordenador y de repente empieza a hacer cosas como si fuera un teclado o sea claro un montón de cosas empieza por ejemplo hable a inicio mi PC no sé qué Y o sea como si fuera una persona normal está brutal cuando llegas contigo mientras prepares aquí el Setup Y si tengo la inteligencia o la capacidad de evadir tu solución de antivirus preferida pues te da un plato lo que tengas ahí wifis usuarios que estén en memoria todo lo que pueda ser Okay okay O sea volviendo lo que hablábamos antes del tema del fishing al final es un malware que acaba derivando en un malware que o bien recaba credencial y las Envía un panel de control externo que luego se utilizan o bien la máquina de forma remota para poder hacer operaciones como listar usuarios ver recursos hacer unidades de red todo esto y la idea Cuál es en una red Windows cuál sería a dónde intentarías llegar tú al activo directorio puedes hacerte usuarios de administrador el grupo de administradores y ya tengo puedo hacer lo que quiera claro y por ejemplo entonces un poco el resumen sería que el primer punto de acceso suele ser la web no a ver si pasa si haces infraestructura solo es intentar comprometer algo que lo que se llama de la dmz lo que está digamos publicado al exterior esto desde fuera y luego por ejemplo yo he escuchado mucho que las VPN de las empresas también son muy vulnerables a mí me dio bastante miedo mucho tiempo porque como yo no tengo o sea yo soy el informático de vale es lamentable pero es así porque bueno no me fío de momento no he encontrado nadie que le dé las llaves soy el informático monto todo yo los servidores todo entonces La idea es que durante mucho tiempo por falta de tiempo para investigar y asegurarme de que todo estaba bien he preferido imitar la VPN como opción durante un tiempo La tuve y ahora ha vuelto a quitar porque no hace falta y cómo te conectas entonces aquí a los recursos internos soy muy contrario a este tipo de software Bad Bunny hacia afuera sin permisos ahí todo tráfico cifrado no ves Nada es como es raro no me gusta este tipo de software luego te lo digo después del programa Vale pues eso que la VPN es tan vulnerable como dice no es que si hago en la web en el sí sino que quizás el Software que está sustentando la VPN o sea las virtuales Son son seguras el tema es que salga una vulnerabilidad por ejemplo que El fabricante no tiene controlado y por tanto alguien de hecho ha pasado un amigo mío Lorenzo que explicó una de sus charlas que había una un fallo de seguridad en una VPN de sofos en el que se conseguía hacer al cacharlo digamos y poder leer los usuarios y las contraseñas de la VPN por ejemplo pero en sí el túnel es seguro Es algo seguro el tema del Software de gestión o lo que hay alrededor de la upn como tal Open VPN estándar o ahora que está muy de modo eh Muy de moda el wireguard este es muy bueno no es brutal Además yo cuando lo probé rápido eso eso súper fácil de configurar mi fichero de configuración Igual igual es como clave pública Clave privada servidor destino no sé qué Déjate nada más Sí sí sí es súper fácil y además es como que el ancho de banda

es mucho más alto es mucho más rápido porque no tiene tanto no sé no sé que no sé por qué y curva eléctrica para la seguridad es decir es de último estándar ahora igual pero pero ya y hay otros últimamente que son tipo creo que hay uno que se llama Tail o algo por el estilo que van con un servidor de terceros que es como que tú les pagas vale Y ellos te hacen de pene Qué miedo eh Sí claro utilizar una VPN como la de yo que sé pues vamos a decir varias marcas North tu VPN cyberg cualquiera de estas son mula cualquiera de estas no okay Porque para mirar contenido Y tal Pero la web a tu empresa y una vez que estoy dentro de la empresa Imagínate que estoy aquí en persona físico qué puedo hacer me puedo coger ir a tu datacenter y llevarme un disco duro Bueno claro directamente más que más que eso o pincharte un malware directamente en tu red interna o clorarte un disco duro o añadimos usuarios no sé si recordar ese capítulo este robot en el que el tipo este tiene que resolver un incidente y está dentro del Data Center y consigue digamos enrutar el tráfico hacia otro sitio es el que va al baño y pone un aparato en la pared del baño o algo así es otro capítulo es cuando se encuentra el fichero que dice no no remuevas de aquí que habla sobre el grupo este que no recuerdo cómo sé cómo se llama pero pero es eso es eso o sea que se puede hacer o sea una crítica de acceso físico puedes hacer lo que quieras instalarte algo en el en el proceso de arranque que tú no lo veas porque está por encima de puesta por debajo de acceso al sistema operativo y por ejemplo vale hablemos un momento de las VPN vale que esto es un tema bastante controvertido mucha gente O sea a ver nosotros los youtubers anunciamos vpns todo el rato vale eso son una fuente de ingresos de YouTube mítica o sea muchos lo hacéis o sea entiendo que venden mucho y que les sale muy barato yo creo que la VPN es un negocio que es muy barato o sea montas unos servers pones ahí una serie de servicios una interfaz de usuario que sea así Ya está ya tienes a cobrar sabes a facturar le pongo cuatro youtubers supongo que no que habrá más temas de o sea Habrá más infraestructura más personas gestionando Eso temas de ciberseguridad también Y tal Pero yo creo que es un servicio un negocio fructífero bien no mucha gente dice que no valen para nada tú qué opinas Pues yo creo que son esenciales es decir Establecer un canuto privado desde Punto a Punto B donde solamente voy a estar cuando voy a estar solo que más seguridad hay en eso no decir yo por ejemplo y lo digo abiertamente yo tengo la web hinchada en el móvil así claro por datos y todo eh pero realmente o sea yo lo que lo que pienso o sea te voy a decir un poco mi proceso lógico y tú luego me dices está mal no sé qué vale Yo lo que pienso es sí que es verdad que hoy en día todas las web van cifradas O sea tú cuando hablas con la web todo el tráfico va cifrado entonces realmente un tercer malicioso que está escuchando mi tráfico no puede ver mi tráfico en teoría en teoría primera conexión sí no la primera conexión hacia dónde vas voy a ir a la web de nate gentiles si puede ver la URL la que estoy accediendo porque eso no va no va cifrado Y estás seguro que la web destino está forzando el tráfico por el 443 siempre y no carga el contenido http no sabes vale Pero y otro tema por ejemplo que esto esto lo leí en un libro de Kevin que decía que aunque el tráfico esté cifrado tú simplemente leyendo los asuntos los emails por ejemplo el asunto del mail no ha cifrado la URL a la que accedes a la web tampoco entonces tú viendo por las webs a las que navegas las urls o viendo los asuntos de los mails o las fechas o las personas implicadas pues recabar muchísima información en una cafetería ponemos una tarjeta modo y nos sentamos a la red de cualquiera de los operadores que la ofrecen de cafetería restaurantes etcétera y nos ponemos a escuchar ponemos una analizador de tráfico y ya verás la cantidad de cosas que puedes ver ahí sea igual no estoy viendo el usuario y contraseña de la persona pero veo que está viendo una tienda de ropa que zapatos ha mirado qué restaurante está reservada están transmitiendo en claro hacia fuera y tú no lo sabes vale como WhatsApp yo le comento a la gente

siempre que encienda un WhatsApp en su máquina y que vea lo que está pasando en la empresa metiendo cosas que no molan sabes Okay Okay entonces lo que yo pensaba eso que la VPN en principio sí que es verdad que hoy en día el tráfico ha cifrado pero todo esto Esto es público no y con la VPN crearía un túnel entre yo un servidor de unos señores de los que confío y el destino final Por lo cual mi tráfico va a través de un socket full encriptado y nadie puede ver lo que estoy haciendo lo que sale utilidad y además hay que usar proveedores que fomenten el nolox es decir que ellos no guarden nada Sí porque si lo hackean o sea por muy buenos que sean si los hackean y tienen locks incluso pues esto seguro que hay muchos más claro Sí sí cuando el producto es gratis Entonces esta lógica que te he dicho Qué te parece no me parece Me parece bien aunque esté encriptado no no no no hay VPN y es Punto a Punto si yo no tengo VPN y estoy navegando en un sitio público aunque esté conectado a una web con https podrías ver cosas Habría que ver el caso concreto de la web lo que estás transmitiendo los protocolos también No no es lo mismo mirar rtp para transmisión de video por ejemplo https o Ema popop3 que no van encriptadas por ejemplo el vídeo yo no es tanto que vaya cifrado no sino si el inicio de la conexión es seguro si haces un túnel y luego conecta si el protocolo permite también transmitirlo en claro si podemos hacer un downgrade te acuerdas aquel programa que había de es el strip en el que hacíamos él entonces transmitidas con una se puede ver el usuario contraseña por ejemplo contacto en un Gmail es como no digo sea tan fácil pero que se puede hacer cositas hace cositas Aunque entonces VPN sí Yo siempre digo VPN así siempre hombre depende tu nivel de paranoia como siempre Eres un maldito agente 007 siempre o te da un poco igual porque solamente meas el canal de nate y juegas con tres Y luego el tema es Yo últimamente lo que hago es siempre que claro con todo todos los vídeos que he hecho de ciberseguridad paranoico también vale Y con el canal y ver que a toda la gente las que la están hackeando mis compañeros y tal yo no me conecto nunca a wifis públicas bueno en general de nadie uso siempre el Access Point del móvil Vale qué opinas Habría que ver la contraseña de que tienes en el Access Point eso sería interesante y yo por ejemplo hago tettering pero siempre lo hago por cable Ok por cable el iPhone lo permite y de hecho hay una aplicación que te recomiendo Mira es esta de Aquí vamos a abrir la aplicación y como veis se está escaneando mi dispositivo y esto lo que me va a permitir aplicar son primero aprender guías sobre cosas que tengo que aplicar en el teléfono yo que sé protección y robo pues te dice Oye pues hubiera el teléfono o la última versión habilita las tendencias automáticas usar temas de biometría habilita El Fight iPhone no sería como diferentes guías de hecho me quedan algunas como veis algunas son guías y luego además te dice cosas que tendrías que activar no Oye por qué tienes que activar el Face ID Cómo se activa vale esto es una aplicación que te permite pues ver si está la última versión de iOS como saberlo si tienes activado el screenlock Cómo desactivarlo Qué medidas tienes que poner Y esto es súper Útil para decir voy a hacer un bastinado de mi teléfono y voy a ver si tengo la última versión de todo corriendo y si tengo las últimos parches o configuraciones aplicadas está para Android también no no habrá alguna equivalencia seguro y además tienes Aquí también noticias de cosas Apple descubre una nueva features que permite bloquear spyware gubernamental y un poco la noticia de Washington no es gratis dicen ahí bueno igual no es gratis vale Te quería preguntar he visto que tú eres usuario de Apple Sí por qué de seguridad o tema de comodidad no es un tema porque hubo un momento que quería un sistema operativo que me gustara que ahora no estoy muy contento la verdad con las últimas actualizaciones también debo decir sí no sé el han hecho un poco hecho ahí que no acabo de entender muy bien a ciertas cosas han añadido cosas chulas pero han fastidiado otras En mi

opinión en mi opinión como usuario de Mac pero quería algo voy a tener una nativa y un Microsoft Office nativo para poder hacer informes entonces solo tienes sí Bueno ahora con la última versión de Windows va muy bien va muy bien o sea y la consola este va súper bien a mí me pasó lo mismo que a ti en su momento yo era muy linuxero y cuando probé Mac dije Dios esto es buenísimo o sea como el paso natural a los a los linuxeros que les gusta un poco más el rollo de estético y tal todos acababan en Mac siempre eso es pero claro luego con el canal de YouTube rollo Gaming rollo gráficas y todo lo que hago de Hardware y tal al final acabo Windows luego sobre todo bueno Adobe Premier y tal funciona en Mac Pero bueno acá va a ser un Windows no pero digamos que ahora estoy muy contento tío con Powers por la cual soy usuario de Mac yo ahora salimos a la calle tirón Mac a la basura lo tiro me compro otro configuro mi cuenta de iCloud y lo tengo todo eso es verdad eso qué precio le ponemos pero al tiempo que es todo todo si tienes configurado Apple de iCloud Drive de tengas un Time Machine en el Cloud que yo lo tengo vale máquina al día de hoy creo que esto también lo hace Microsoft pero no lo he usado nunca porque yo tengo todo desactivado la máquina no sé vosotros lo sabéis gente si te permite hacerlo esto el one Drive a mi Microsoft me parece o sea tengo como yo soy el típico que cuando está la Windows es como no no Desactiva lo contrario es como que quieres activar todo porque quieres usar los futuros pero yo Microsoft tengo como una desconfianza ya de naturaleza hay una página que me encanta que te permite te permite esforzar un Script para Windows para niños para Mac en el que desactivas todas las telemetría de un golpe lo ejecutas y Desactiva todo Qué bueno eso en Windows empieza a hacer bitcoin en aquello de la mañana aquí dice onedrive solo copia carpetas que elijas Pero hay una opción que sí que te copia todo el escritorio con los archivos de escritorio incluso algunos programas que todas tus configuraciones que vino aquí a la oficina y cogí un pc mío inició sesión con su cuenta de Microsoft y se me puso su fondo de pantalla todos sus archivos y bueno no sé si realmente la personalización de no tener que volver a hacerlo yo lo que tengo es el ecosistema Google claro Incluso en iPhone yo creo que todos aquí presentes usamos eso el Google Chrome tienes el bueno Google Drive tienes Incluso un sistema de dominios y hay muchas cosas y realmente luego tienes el doble factor de notificación que lo tienes Incluso en la aplicación de YouTube en cualquiera y Google fotos también me Mola mucho eh ha sido la salvación para no estar condenado a ser el informativo de la familia Sí sí sí papá mamá Pon las fotos en Google fotos Olvídate si yo le cogí el móvil a mi madre le dije mira te lo pago yo un euro al mes creo que es Google y ahí está y te olvidas y es como nunca más va a venir nadie a llenarte de es que perdió las fotos Exacto usa la resolución de Google que ya está muy bien Yo creo que no se entendí de fotos pero está muy bien Está súper bien Está súper bien si te dedicas a la fotografía claro lo que sea pero si eres un usuario mortal o puede ser mi familia que no se dedican a esto ponlo ahí y te olvidas yo tengo todo ahí bueno los vídeos del Canal no porque están en el nas pero sí y luego por ejemplo el tema de Apple Apple es más seguro que Microsoft que Android y que otros sistemas en cuanto al sistema operativo en general porque claro hay muchos muchos matices aquí por ejemplo a mí me gusta mucho el Face ID o sea todos los directos digo el Face ID Dios o sea me encanta si tú haces el el a ver también esto es debatible No porque yo estoy hablando con por ejemplo la empresa Nothing que ha sacado móviles Android hace poco estoy hablando con ellos del Face ID que tiene a Android y claro yo les digo eso lo comparas con el iPhone y es una mierda bueno depende o sea es que no sé tío o sea Quién te va a desbloquear el móvil tampoco te van a ir a reproducir una o sea no sé sabes bueno todo lo que ahora con con todo esto con Inteligencia artificial te pueden reproducir la cara Eh quiero decir Claro claro pero digamos que el nivel de paranoia también llega

un momento que qué tan seguro necesitas que sea yo creo que hemos de ver un poco Cuál es nuestro caso de uso Cómo se llama la tecnología y ver un poco que mitigamos es decir que a qué estamos remediando acceso tenemos tu factor pagos No sé qué o Face aire no Claro además Funciona muy bien porque un sensor creo que es un líder si no me equivoco que te mide la distancia como en Android muchos móviles te hace una foto con la cámara y ya está Y eso es el autentificación hace 10 años yo había paseado móviles Android con comparten una foto y va Y pase a esas muy fáciles que podemos conseguir buenos resultados si tenemos alguien ahí vamos estoy seguro estoy seguro se pueden hacer cositas claro además el tema del 3D pero bueno entonces qué opinas en general de Apple no es el resto Yo opino Qué estás haciendo un curro chulo además las últimas versiones de iOS tienen Incluso el modo Relay este privado no que también te permite tener tu servidor de Relay eso pues en lugar de usar el enrutador que usa los de Google de iOS de Apple te puedes montar el tuyo para qué Para que vaya todo con tu con tu Relay privado en lugar de servidores hay una opción creo que es aquí en el iCloud vale si esto es para para cortar navegación en Safari a la vez que tu tráfico de internet sin encriptar para que nadie ni siquiera Apple pueda ver quién eres Ni Qué sitios visitas Vale entonces puedes poner tu ley privado sabíamos que Apple está muy metida en el tema de la O sea es un poco el valor añadido que quieren dar ellos no sí imagino que se ponen las pilas también para dar más fichos de seguridad a los usuarios no un valor de poner algún valor en la empresa no eso es Claro porque al final del día es una carta que juega muy bien Apple porque claro Google es una empresa de servicios es una empresa de publicidad o sea Google vive de tus datos claramente no O sea Cuantos más datos tuyos tengan más datos de los usuarios y más enfocada puede hacer la publicidad que ellos venden mejor entre empresas que dicen Oye pues por utilizar el por tener por defecto el Buscador de Google el navegador millones por poner el navegador de Google no sé qué o por ponernos seguidos aquí este juego de empresas También de todo el mundo Google está muy interesado en que el navegador por defecto claro De hecho muchos navegadores viven de eso no literalmente o sea es como gano dinero porque me pagan por tener por tener el navegador ahí funcionando curioso y no eso La pregunta sería no la reflexión era claro Google es una empresa que vive la publicidad tú ya sabes que estás vendido con Google digamos no Ah pero está jugando la carta de nosotros somos una empresa de Hardware nos dedicamos a hacer los mejores móviles los mejores tablets portátiles que podamos hacer que eso ya es debatible cada uno tiene su opinión y los precios Son los que son pero el tema de la privacidad la seguridad y todo esto es algo en lo que nosotros no ha salido un Google termina de configurar tu tv se está escuchando Google a esto no incluso están bloqueando el tema de rastreo de aplicaciones como Facebook y otras aplicaciones que es que bueno antiguamente recogían datos de tu móvil para para mejorar la publicidad la pregunta que tengo es que es algo que realmente no lo sé será que Apple está rastreando esos datos Y luego esos datos los venden es una buena pregunta y hay mucha gente imagino mirando estos temas que hacen con nuestros datos no decir cuando somos usuarios del teléfono que estamos realmente compartiendo que uso hacen esos datos Pues yo creo que todos los fabricantes viven un poco también de también de lo que llaman telemetría de poder recoger estos datos para uso de todo tipo desde desarrolladores para ver usabilidades y demás Hasta salir ese software para ver cómo interactúan con las pantallas hasta ver qué uso a nivel de marketing acá picas allá a todo se basa en el maldito marketing y la venta dirigida de hecho de hecho por ejemplo en cualquier página web mismamente la bueno en mi web en la web de la empresa no pero por ejemplo la web de mastermine tenemos un heatmap de estos de clics que yo puedo ver la gente

donde o sea puedo ver dónde la gente se ha pasado con el mouse Donde ha estado más tiempo y tal para saber que les llama la atención de la los departamentos de marketing y tal necesitan poder coger estos datos para poder hacer en mil operaciones de hecho o como aquello de Oye cuando una aplicación no en cualquier sistema operativo me permite recoger los datos de crasheo para ver un poco donde Pues hay gente que siempre dice no pues yo creo que esto según qué entornos ayuda mucho el desarrollador pero sí que es verdad que a veces si el programa me gusta el problema es que estás enviando tu nombre de máquina tu nombre de usuario está operativo variables muchos datos que luego al final es al final es para esa empresa para solucionar ese problema pero nunca saben paranoicos con esto y luego nos vamos yo que sé a cualquier país en tu caso por ejemplo que hablabas antes de andorra por ejemplo no vas a andorra te vas al Starbucks no tienes internet y me contestas al Starbucks Y dices social login y compartes una cosa da igual no Entonces en ese caso tú me dijiste algo interesante antes el tema o sea tienes alguna en concreto en plan algún servicio de estos a nivel mundial hay una aplicación que que está muy Chula déjame que mire a ver cómo cómo se llama para una aplicación bastante guapa que tú le dices al país a dónde vas y te permite ver una lista de precios de las de las Sims que hay en el que hay locales allá pero como tengo 300 millones de aplicaciones en el móvil porque tiene que existir algún servicio que tengas una de SIM que te funcione en todo el planeta Tiene que existir eso te puedes comprar el Sims que son globalmente utilizables que se comienzan me molaría Aquí está mira ahora podemos enfocar si queréis se llama movie maters bajar el brillo vale Movie Maker si arranca Guay pero esta esta aplicación te permite seleccionar el país destino y con eso compraron compraron Así vamos a ver si podemos eh Ah mira está cargando ya bien me preguntan aquí Marc viste que las esima ahora las quieren reemplazar por icing Apenas ha comenzado Las esim y ya quieren cambiarlas mirar esta aplicación aquí tienes un montón de operadores vale un montón de operadores se ve bien Sí ahí lo tienes entonces tú puedes coger y decir dónde dónde hay que no te gustaría Disney te gustaría ir a México por ejemplo sí venga a México venga cogemos México y aquí tienes los operadores que hay en México que sirven contenido con la con los datos lo que cuesta la validez y tal cogemos uno de esto le damos a comprar Ahí está ya tienes el móvil con eso sí compramos la SIM bueno Esto que dice aquí le vamos a proceder por ejemplo no no pagaremos nada y bueno dejar mi correo Es más que público pero podemos proceder y hacer la compra y pagas con Apple Pay directo eh pagas con Apple pay y te llega el correo un QR buenísimo esto yo cuando lo vi cómo se llama Javier a mí me gustó por la simplicidad que tiene esta aplicación obviamente seguro que hay mogollón de cosas eh Por ahí pero movie Mater me encanta porque depende donde vayas utiliza una SIM local te va a ser mucho más barato que no hacer roaming antes de viajar al país No preferiblemente porque si llegas ahí sin las es importante activarlo Antes de antes de salir porque claro llegas allí igual No te funciona y está la comunidad apn dentro de dentro de nuestro sistema el tema La verdad que es una pasada eh De hecho hay proveedores que de hecho ya no te habla sin física te dan el SIM y ya está eh Hace mucho que no la cambio pero hay probadores que te dan que te dan solamente siempre además el otro día probé porque fui al Mobile hice streaming con un móvil y con el otro estaba con conexión y me pillé una una SIM que es como un duplicado la que tengo y permite que uses en los dos móviles la conexión eso está muy chulo bueno menos mal porque me gaste 400 GB de datos por el pasillo sí sí sí sí sí estuviste por ahí y tal Estuve por ahí los estuve tres días tío haciendo ahí entrevistas a full mirando cosas que hayan publicado publicaron cosas atrajeron cosas chulas este año eh tecnología de robots y tal y una movida que me flipó mira que yo sé que es fácil eh o sea fácil que con las cosas que se ven que

no es algo súper Guau Pero me flipó una empresa que no recuerdo cómo se llamaba no no sé si era ahí o no en el stands de vale que miraban a la persona y la bebía en el esqueleto órganos y tal Voy a escoger el pulmón y mirarlo era como Guau tío esto es flipante sabes Supongo No imagino imagino que imagino que sí estaba en directo Que bueno hay cosas que las pasemos el intestino lo mirabas ahí con lo dejas en el sitio me parece a nivel educacional a nivel de formación me parece brutal ese tipo de cosas sinceramente sí Mola mucho tío Entonces el Mobile Por qué fuiste tú fuiste con la empresa contestar entrevistas y tal algunas reuniones con con gente que tenía que estar allí y poder un poco vivir el espíritu del Mobile que pues cada año un poco se supera no con lo que hay gente es el primer año que iba eh yo fui la primera vez hace dos años eh tampoco te quedas tú que yo había ido nunca antes me han contado no sé si es verdad que alguno lo puede confirmar que en las primeras ediciones regalaban móviles pero yo nunca ni idea tío yo no puede Yo nunca lo a ver si alguien lo sabe a ver si alguien lo sabe Bueno pues el tema de Bueno yo normalmente voy al cc Las Vegas Al computex Pero porque son más de ordenadores No yo móviles hasta este año prácticamente no no me interesaba mucho porque al final bueno no se puede abarcar todo pero este año con los directos he empezado a hacer reviews de móviles aquí y nada voy voy trayendo traigo cositas entonces dije voy a ir al Mobile la verdad me gustó mucho eh auténtico profano No tengo ni idea de Yo sé que yo usuario de iPhone y conozco pero iPhone hostia Cuál es el móvil Android que ahora pues algún Pixel entiendo porque son los que Pixel es el nuevo Galaxy también que es una pasada del s23 compré este que es como la como se abre como una especie como el Notebook el Motorola no es Motorola hay varios que puedes abrirlo y se hace como muy mucho más grande es que ahora hay muchos Eh vale vale o sea ahora este año literalmente menos Apple todas las marcas han sacado es increíble o sea estoy flipando bastante Exacto del Samsung está el flip Z y el flip No me acuerdo qué más luego está el Motorola también que es el flip vale luego está el Motorola que tiene que lo tengo por aquí que lo quiero traer un directo que es el razer de toda la vida El como el Antiguo de tapita pues plegable y ahora todos honor qué opinas de esto me interesa porque yo la verdad que para mí es un poco chocante ese tipo de muebles que se pliegan no acabo de ver rollo hace un tiempo que estuve bastante estuve con un mes probando uno usándolo y tal a mí y me pareció bastante inútil sinceramente aparte que se ve se ve la separación a ver eso al final lo ignoras o sea tu cerebro lo ignora al final pero no sé lo veo como quizás que eso ya me he vuelto viejo para estas cosas pero pero lo veo y digo no me acaba de mudar mucho a mí eso Bueno al final lo que comentabas eso no que es como cuando ves esta pantalla hay un reflejo aquí pero no te estás fijando sí no me fijo no no con la fisura pasa lo mismo que al final no la ves estás por hecho que simplemente para usar el Mobile o sea es que yo creo que no Pero porque o sea hay varios problemas el primero es el radio Que bueno que ya los móviles se lo están pasando por porque ves un vídeo en YouTube y tiene unas barras negras a los lados O sea no tiene ningún sentido Pero bueno pues esto es lo mismo o sea tú abres el móvil enorme y es como cuadrado sabes es como que los vídeos tienen dos barras gigantes de negras los juegos Bueno hay algún juego que se adapta otro que no O sea no le veo tampoco mucho el uso la verdad es como estos juegos alguno me da un slack pero como estos Gamers que tienen cuatro Ultra whites para jugar que yo digo pues tiene que ser incómodo tampoco no a mí Lo que más me Mola Esa es la mejor opción para jugar para mí una un monitor grande tamaño estándar de este o sea aspecto estándar 16 novenos lo típico pero grande pero bueno ahora sí que está muy de moda el Ultra 50 pulgadas Tengo una maldita única Ultra White y ahí me divido el escritorio y solo tengo una pantalla de Samsung No creo que es el Samsung Sí claro el tema es ese que para currar sí que es verdad que

bueno para jugar también pero bueno no a mí me gusta el rollo El Rollo está Chula vale vale Bueno lo que lo que está más en rollo Gaming y tal lo que está más más mejor calidad precio son las LG las LG C2 por ejemplo la CX han sacado como unas teles que valen bueno son caras 1000 euros o así mil y pico pero son como oled tienen muy buen tipo de respuesta para jugar a Playstation al son muy buenas y bueno yo me he hecho muy fan de hecho en mi casa antes tenía que hice mi primer Setup me puse una de estas pero en plan aquí a esta distancia irá más grande que será como hice el vídeo la gente me decías tan loco Yo que no que soy un visionario ya veréis ya veréis probando que y bueno igual sí que me bajó un poco la visión puede ser alguna afectiva secundario en estas tiendas tipo media Mark que valen la tele 6000 grandes tío digo algún día tendré ahora con el lga es es la marca que ha democratizado un poco esto ha hecho como eh economía de escala en plan voy a vender la súper baratas yo me pillé una Hace poco pero barata una LG de estas baratas pero LG Mola por eso porque o sea la Sony por ejemplo te cuestan 10.000 euros para arriba y tal bueno 5000 5.000 10.000 pero es como que ha democratizado esto sea por mil euros puedes tener una tele oled muy buena no es un sponsor y me cuesta trabajo como convertir como en la tele es algo que te da mucho palo cambiarlo eso es yo la compré porque haces la mía le pasaba eso tenía manchas verdes y por eso la cambié Podría tener una tele 1080 de hace 10 años y ya y mis padres me regalaron la tele una una LG pero de las primeras planas que había No pues me la cambié O sea me la acabé Cambiando al cabo de los 89 años y me acuerdo que puse la película de Los Vengadores y dije hostia lo que me estaba perdiendo calidad hablamos siempre de que ella dice Ah no quiero ir al cine porque si es que en casa las pelis yo las vemos la que compré hace poco también es un O sea la que tenía era Ponle que era de 75 pulgadas vale o 65 y la de ahora es de es como yo de larga eso 85 es una cosa enorme 85 pulgadas Y eso Lee haces ese ratio de a tanto el sofá y todo eso no no no no había comprado y dije espero que quepan ese agujero y al final por gente que ha desmontado por los pelos pero cabe y le estoy diciendo siempre Sara Mira cómo se ve mira aquí los negros aquí y ella me dice Cállate que me estoy enterando la peli me da igual compartir con nadie tienes suerte de que tu pareja lo valore porque nosotros pasábamos también de una tele donde tuvo pero las primeras planas a una tele ya condiciones por eso la tecnología pasa mucho eso de que si no si no pruebas Nada mejor eres feliz con lo que tienes totalmente totalmente de hecho con la primera vez que probé un iPhone dije No creo que a través de móvil a estas cosas y de hecho no he vuelto a cambiar soy usuario de iPhone desde el iPhone 5 a ver ahora yo por ejemplo sí que estoy obligado a cambiar o sea porque yo estoy obligado una vez al año tuve Pixel me gustó mucho Y tal Pero bueno al final he dicho iPhone y bueno voy tirando con los iphones pero seguramente si no fuera creador de contenido no tendría ni idea de nada de Android No sabría nada tendría mi iPhone y ya está pero no puedo hacer ahora y me cuesta encontrar las opciones ya ya y digo y la gente te dice pero tú no sabes esto dice ya Coño pero no sé demo no no me preguntes de la opción donde está la opción de la peli en Android porque no quizás no me acuerdo pero pregunta concreta es más seguro el iPhone que el Android por el simple hecho de que no puedes instalar aplicaciones que no estén fuera del Market ya le de seguridad a iPhone si no te instalas una APK ha bajado de internet o sea si tienes esa prudencia dejando la responsabilidad en el usuario que nunca sabes si va realmente a hacer eso que sería un poco ese no el el punto de entrada principal que eso no quiere decir que no haya habido casos en los que la propia aplicación del App Store tuviera infectada eh decir esto ha pasado también eh No es rollo habitual pasa una vez cada mil años después pasa muy pocas veces Pues también pero también ha habido eh Pero obviamente solamente por eso el ámbito de explotación ya se reduce muchísimo muchísimo

aunque Bueno también bueno Chema Alonso muchas veces ha salido en el pasado no sé si ahora ahora quizás no tanto hackeando cosas de o sea hackeando iPhone directamente no usando Sí porque usa mucho el tema de usar Siri si ocurre siempre muchas ideas locas y tal de cómo usar siri para que tener infusor el teléfono no Ok o por ejemplo yo por ejemplo tengo qui a previo de los mensajes porque si no en el centro notificaciones yo ahora cojo tu teléfono Estoy seguro que hago así hablo Ahora que no lo pongas la cámara pero no me va al centro de notificaciones no sé por qué Abre Abre abre el teléfono vale Y ahora baja desde arriba no tengo nada No es que ahora no tengo no tienes notificaciones pero no no veo el previo por ejemplo eso es muy importante yo tampoco y has probado alguna vez los filtros estos de privacidad para que no te vean del audio Reconozco que me encantan pero que son un poco coñazo cuando vives en sociedad viste lo que he presentado en el Mobile el panzer glasses eh No no lo vi una locura eso un teléfono con una con un protector de pantalla que se llama panzer glass le ponen encima le dan con un Mazo encima del teléfono con un cúter y no Qué bueno no pasa nada tío Creo que vi que estaba en el stand de Creo que creo que pillar uno Pero además no lo vendían allí porque no puedes comprarlo ahí pero dije Wow qué pasada chaval el tío pegando con el mazo ahí no rompías el teléfono me pareció brutal la verdad que igualmente el tema de los ríos cristal y eso en el móvil yo digo nada tío yo llevo lo llevas ahí a pelo este año le puse una funda y llevo como ves un cristal está bien protegido yo antes llevaba lo llevaba sin funda Lo que pasa que se acaba cascando a mí que a veces lo saco porque no me acuerdo cómo es el iPhone Ay Mola Este es el 14 promax tú estás allá en la última Sí porque por eso lo voy o sea a ver en realidad es una excusa Yo hasta ahora hacía muy pocos vídeos de móviles y todos los años digo voy a comprar el iPhone nuevo para hacer el vídeo y nunca lo hago dice una vez yo me lo cambié porque yendo al gimnasio me robaron el móvil Y me tuve que cambiar el 12 Pro Max Pero antes tenía la fiebre cada año de cambiarme el móvil y ahora es una chorrada exactamente Me costó mucho comprarme este o sea decidirlo me costó en plan y si nos ponemos a pensar realmente qué fichos realmente tienen nuevas no tienen tanto aprovechable ninguna aprovechable ninguno y hago unas fotos brutales con este teléfono y no con la fotografía no tengo ni idea y Nosotros hemos Comparado este con el anterior y tampoco hay mucho mucha diferencia entonces un poco el tema de Android versus iPhone sería el apk no que puedes instalar apk en el Android sin bajados de cualquier web y ya está o sea realmente a no ser que hagas jailbreak y hasta el enclave ya seguro ya es todo muy seguro pero sin embargo ha habido hace tiempo salió a la luz una aplicación que podía espiar los iphones no hay aplicaciones hay aplicaciones que se usan en operaciones de espionaje por eso estamos hablando de algo que es más a nivel gubernamental no hablamos de aplicaciones que normalmente lo utilizan no tienen acceso las agencias de inteligencia tiene acceso inteligencia Y empresas que se dedican al mundo de la maldad vale en el que utilizan este tipo de aplicaciones en el cual explotan fallos de seguridad existentes en el sistema operativo las aplicaciones o lo que sea para instalarse en malware y puede tener acceso a lo que se hace en tu teléfono pero entonces algún tipo de vulnerabilidad cero d no que no está cubierta y que se aprovecha y que bueno Y esto por eso es importante aplicar los últimos parches y de vez en cuando yo lo hago el iberify que avisa cada semana de que realices el teléfono y esto de a través de pegasus habían espiado mucha gente del gobierno incluso no Sí de hecho también lo de aquí en Cataluña o lo del catalángate no que se espió a políticos aquí y también lo ha habido por un periodistas con con disidentes y se sabe cómo funciona se sabe cuál es el vector de ataque como las empresas de seguridad analizan un poco Cuáles son los vectores de entrada algunos no se conocen hay publicaciones buenísimas de Google que explican cómo funciona la explotación de

los fallos que realizan de hecho podemos que puedo pasar luego Un par de links para que los revises pero es una locura el proceso de explotar un fallo de seguridad porque no es fácil explotar un fallo de seguridad del Safari o en aimisatch o en mail de Mac que te lleve a estar un malware como súper usuarios en un iPhone he jodido no no está al alcance de casi nadie pero es factible es factible porque ha pasado claro Sí sí pero esto está parchado a día de hoy o sigue funcionando imagino que bueno no sabemos no sabemos pero de estos móviles que en los que se había hecho el espionaje utilizando esta aplicación algunos fue un laboratorio y se hizo algún tipo de artículos explicando hay una un equipo de investigación pionero que se llama citiesen lab que están en la universidad de Toronto pero no equivocarme en el que son los especialistas en sacar ese tipo de publicaciones Okay en decir analizamos este teléfono móvil y podemos sacar Digamos si está si está digamos infectado o no y hay un proyecto de amnistía internacional liderado por Claudio la unier y también en el que tienen un un software como ya lo podemos mirar si queréis es un software que te permite conectar tu teléfono y hacer un testeo para ver si está comprometido también pero es posible por ejemplo a ver igual en mí nadie tiene interés pero es posible que mi móvil ahora mismo tenga un software espionaje que me estén interceptando llamadas mensajes y todo tipo de cosas todo Sí sí claro se puede se puede si estamos en un entorno donde haya temas vul se puede hacer claro y esto lo hacen es un tema de espionaje directamente gubernamental son empresas que se dedican a desarrollar este tipo de exploits o de aplicaciones y los clientes de estas empresas son los gobiernos directamente no son son digamos son actores que tienen interés en un grupo a nivel de sociedad civil concreto en el que Oye pues me interesa investigar este grupo de periodistas investigar a este grupo político aumentares a investigar a este grupo de disidentes o de usuarios de estos problemas de exclusión social en el que pues lanzan por ejemplo pegasus para poder saber todo lo que hacen esta este tipo de personas con el seguimiento con seguimiento de organización si evento de mensajes de la agenda de contactos etcétera Y tú crees que a pesar de porque ahora yo creo que hay un esfuerzo mucho más grande que de lo que había hace años en cuanto a ciberseguridad no O sea tanto a nivel gubernamental quiero creer porque sí que hace años la del gobierno eran un poco siguen siéndolo No lo sé No lo sé pero digamos que seguro que hay como siempre en dolorcitos asuntos pendientes seguro siempre asuntos pendientes a esto no actualizar esto a mejorar esto pero digamos que hoy en día tú crees que con toda la seguridad que tenemos se siguen interceptando comunicaciones en los gobiernos y hay Cuál es el estado del espionaje podríamos poner una gorra ahora de modo paranoia on no en el que podíamos hacer hipótesis conspiranoicas sobre lo que puede estar ocurriendo Obviamente el vector de ataque está ahí sería inútil lo estúpido negarlo que esto es posible tecnológicamente es posible Entonces es cuestión de que la lucha gasta entre la industria de ciberseguridad en conseguir parchear podemos venir Las investigaciones y poner el trabajo más difíciles a ese tipo de softwares y demás y por otro lado estas empresas en la búsqueda de nacionalidades explotación y poder Entonces es un juego de gases razón a veces ganan ellos a veces ganamos nosotros Ok he oído mucho he visto mucho últimamente muchas personas subiendo artículos de Blog vídeos a Youtube etcétera hablando de Cuál es el mejor sistema operativo o el PC ideal de un hacker o sea vale Así es el ordenador de un hacker de poner un Linux o un perro o algo así instalado en un equipo y ese es el ordenador de hacker es esto verosímil pero es que sabes qué pasa que hace tiempo que huir de lo de la guerra de sistemas no que es mejor bueno pues depende Yo es que uso los tres durante siempre Entonces qué es mejor realmente no hay un sistema único tienes que manejarlos todos Yo creo que tú tienes que ser lo que más se valora a día profesional es tu capacidad de adaptabilidad

no es decir cuánto te cuesta adaptarte a un cambio no entonces poder ser bueno utilizando un sistema mal y un sistema Linux Yo creo que es importante y luego utilizarlo pues vale que luego tú como acción personal decidas Oye quiero usar solamente ma Vale pues ya me parece bien pero es tu caso por ejemplo pero no es es esta guerra de sistemas tenemos que dejarla ya enterrada ahí los contra los demás en el mundo de la programación eh Claro que es mejor visual Studio code o la solución está de Jet brains que es mejor depende un tema de preferencia personal luego como plataforma de desarrollo sí que es verdad que hace años intentar desarrollar algo basado en python jungo php etcétera en Windows era buscar problemas eso es Ahora no ahora no tanto eh sobre todo con el con el subsistema este de ubuntu y a muchas cosas la gente ahí pone las librerías luego te Peta todo esta guerra de sistemas siempre digo terminémosla sabes luego otra cosa en cuanto a Por ejemplo si tú quieres hacer actividades de hacking obviamente distribuciones como parte y demás son ideales porque vienen ya con todas las librerías instaladas configuraciones el tuling los menús ya está todo hecho no tienes que hacer prácticamente nada salvo configurarte el turing a tu medida entonces que es para mí sería un buen sistema de hacking Pues si te vas a hacer desde tu casa un buen PC con una buena máquina virtual Yo creo que es ideal y tener tu cara Linux instalada con tus configuraciones y vas a estar moviéndote Pues un equipo que te permita tener esa movilidad con ultrabook o algo así que te permita por ejemplo tener varias interfaces de conexión USB fire diferente tipo de cosas que te pueden hacer falta y que te puedas moverte por la ciudad para hacer lo que te interese más que para eso es ideal y buena batería siguiendo las gpu pues no gastes pasta en eso y poco más y el tema de yo lo que tengo entendido es que normalmente cuando vas a trabajar y yo que sé hacer cualquier tipo de actividades de ciberseguridad lo suyo es montarte una máquina virtual trabajar en esa máquina virtual y luego destruir todo no esto es básico es decir el poder tener esto se llama offset no la seguridad operacional es decir tú creas un sistema virtual randomiza además la mac para que nadie sepa que está utilizando O virtualbox tú qué prefieres por encima de todas las cosas ahora con los Max M1 pues me tenía que comer un poco al principio del paralele pero está muy bien De hecho a mí me salvó bastante la papeleta pero yo soy Pro bien World pero desde hace un montón para máquinas virtuales de tu local estudios locales para servidor sin duda los próximos ya y todo Esta cosa que no vale bueno ojo el próximo si está Guay para hacer para montar un pc bueno es igual vamos pero yo te digo yo creo que en performance un buen colega mío y es brutal el perfume es brutal Entonces ya te digo tener un sistema con calidad Yo creo que es básico es básico pero aparte de eso pues vas tirando de máquinas virtuales y para crear tu sistema digamos allá VPN sí siempre o doble VPN o triple VPN servicios en el mercado negro que te voy a intentar pero o sea Serían como servicios de terceros de salida ahora ahora y poder tener un sistema desechable Entonces lo más importante diría es que es bastante deseable manejarse bien con todos los sistemas operativos y además tener la capacidad de montar y desmontar sistemas desechables y de en cuanto a una persona que quiere aprender ciberseguridad qué le recomiendas qué debería aprender o sea como skill autoridad que voy a aprender esto yo diría que tengas muy claro que tienes que tener capacidad de adaptación vale de poder pivotar entre entre topics no hay que olvidar los fundamentales es decir hay que la gente quiere hacer un curso de hacking de 30 horas y ya con eso se cree que va no se puede es imposible no se puede o sea sí O sea hay tanta demanda de empleo que probablemente consigas trabajo y además seguro que además la persona lo hará bien con muchas ganas no sé qué pero es importante tener en cuenta que hay que saber muchísimas cosas desde cuando vas a trabajar de hackeando webs tienes que saber programar es

fácil esto Me acuerdo cuando cuando yo tuve mi primer trabajo de programador que se sabía php y html y css y un poco de javascript Pero recuerdo que tenía problemas a veces que preguntaban foros y me decían bueno es que tú estás programando pero no entiendes http Y decía me cago en ti claro y decía recomendando libros que Quiero aprender más pero este te hablo hace muchos años no Y sí que es verdad que es eso Si tú no entiendes la tecnología con la que estás trabajando eres muy limitado y yo tenía muchos problemas de no entender cómo funcionaban ciertas cosas del protocolo de cómo vas a hacer una inyección sql si no sabes sí okay Está Guay pero cuando ese problema te falla Qué vas a hacer cuando la herramienta te falle es muy importante ver por qué no es muy importante saber qué hace las herramientas por debajo yo soy muy fan de automatizar cosas pero quiero entender lo que hace porque el día que falla tengo que poner de lugar eso Entonces antes antes de la pregunta de qué recomendarías aprender para hackear Cuáles son las habilidades que crees que debería tener todo hacker o experto en ciberseguridad que no sean relacionadas con el con la ciberseguridad hablamos de software quiere decir Bueno te hablo más de programación conocimientos de redes Pues yo diría que para poder ser alguien digamos competente a día de hoy Yo creo que tienes que saber de sistemas operativos ya sea Linux tampoco te pido que seas un experto en todo pero por lo menos conocer Linux por ejemplo sería yo básico por ejemplo conocer la estructura de ficheros donde me hacen las configuraciones cuando está los software Dónde está lo en opete en USB local donde está la gente lo pongo siempre no siempre no Pete siempre no sé Hay un porqué de las cosas no O pts opcional software hay que poner las cosas algunas cosas depende de la distribución hay que entender el motivo de las cosas no Entonces eso por un lado saber del sistema operativos luego redes y quieres hacer temas de hacking por ejemplo tienes que saber que es una IP local Cómo funciona un dns este tipo de cosas tienes que conocerlas no tcpv Para qué sirve no porque cuando hay un servicio que lanza una conexión y no me responde a quitarse un servicio y no me va a contestar nunca No ese tipo de cosas no Y luego evidentemente el poder automatizar es clave puedes saber ni que sea scripting básico nivel que nos permite prototipar muy rápido entonces todo eso es para mí es esencial sea un poco el resumen sería sistemas operativos redes y Nice to have programación significa que si no sabes programación no puedes hacer ciberseguridad No no precisamente no límite ahí a la hora de automatizar y sobre todo de no repetir operaciones que nadie quizás le gusta repetir claro el tema sería que yo recuerdo hace muchos años que tenía un amigo que era muy crack muy muy muy muy muy crack y el tío lo que había hecho pero me estoy acordando había modificado el código de Esto hace mucho muchos años de Linux para crear él un randomizador de makadres y había había modificado el código de Linux en C directamente lo había compilado y lo había metido en su sistema operativo y claro Yo decía joder o sea nunca voy a saber todo lo que sabe él como para buena gente que se especializa en esas movidas No yo tengo también conocidos que se han hecho su propiedad dentro de Linux hostia pues es una locura mucho vivir 80 vidas una cosa Yo soy de esta opinión Cuanto más aprendo cosas más me di cuenta que sé menos sí totalmente de agua fría para para la gente que no te dedicamos a esto porque piensas joder es que me gustaría hacer eso pero es que el esfuerzo que me supone aprender esa movida no vale la pena no vale la pena pero el tema es que necesita o sea hay ciertas ramas de la ciberseguridad donde es muy importante la programación no para entender o sea poder hacer cracks o poder leer el código fuente todo hace falta en todo porque al final tú vas a querer a veces llevar eso a escala o poder automatizar cosas o poder programartelas no es muy bonito el poder programarte robots hacer cositas que hagan cosas por ti no básica programación yo para mí es algo que tenemos que dedicar mucho tiempo y

hay que hay que fomentar esto de hecho en el máster que yo llevo digo la gente tío programación hay que meterse con esto de hechos de las más de las cosas que de informática Yo creo que es una de las cosas que más cuesta de la gente a veces no y yo te voy a decir una cosa que siempre lo he creído lo has decidido solía somos muy malos programadores Sí sí pero bueno quizás las generaciones ahora han cambiado a ver eso eso normalmente O sea yo lo que como programador que he sido gran bueno no gran parte Pero si ya debería gran parte de mi vida Estuvimos viendo ahí las cosillas tú sigues programando pero no me dedico 8 horas al día entiendes el rollo Y sigues todavía con ello Sí claro claro me encanta O sea me gusta mucho siempre que puedo saco tiempo y lo hago Pero lo que sí que veo es eso que es una skill que primero cuando tú vas a clase de programación seguro que bueno no sé si tú tuviste y aprendí yo en mi proyecto final de grado medio era una web de cines que era phpm Pues no sé si te pasó que la más de la mitad de la clase suspendían programación y Había otro problema que en mi caso si suspendieras el proyecto final de grado mayor te suspendían bases de datos y programación que era un putazo y yo por ejemplo la primera vez en el proyecto y tenía que hacer una web que tú querías Ver la película de Hulk y reservamos los asientos y en mi caso por ejemplo podía reservar más entradas en la sala vale Pero bueno pero un poco son las dos asignaturas donde más se suspende no bases de datos y programación en este tipo de ciclos y yo sí que viví por ejemplo de cuando fui al grado superior en primero de programación que estaba como el das six crear el desarrollo de no el Damme y luego eso es la gente hacía el primer año creo que era común y todo el mundo que venía con la idea de estudiar programación se cambiaba y al final la inflamación que creo que éramos tres el año siguiente y gente que venía de fuera pero es como que la programación hay gente que le entra y hay gente que no le entra eso va a empezar hay una cosa que me dijo un colega una vez y que en su momento le negué pero que cada vez estoy como más alineado a esa idea y él me dijo hay gente que por mucho que lo intente No lo sé pero hay algo ahí en tu cabeza como de estructuras no digo que no seas capaz de hacer Sí igual es una persona súper inteligente Pero eso no le entra yo lo he visto esto pero no sé si es superable porque la gente Normalmente se rinde eso es y yo creo que seguro que alguien alguna de tu canal puede ser que sea un maestro de formaciones con este método seguro eh De verdad seguro que es así pero que hay gente que lleva yo que sé lleva seis siete años intentándolo y que no hay manera si lo he visto lo he visto Además yo también tengo mis cursos de programación Y tenemos la Academia mastermind y tal y normalmente la gente le va bien pero también Es que yo lo he explicado muy muy he intentado hacerlo muy muy fácil a saco Pero al final si sois gente que no le entra o no le gusta pero sobre todo si no si no lo estás disfrutando no haces el esfuerzo A lo mejor también es como buah me encanta Esto me está gustando muchísimo es un programa adrenalina me funciona sabes y hay gente que es como odio esto sabes no lo quiero hacer crees que el uso de la ia chat gpt similares va a acabar son parte de los programadores o no no tengo ni idea Yo creo que yo creo que es una herramienta muy útil que va a ayudar a los programadores a trabajar más rápido Yo estoy seguro que vas a tener un momento Bueno de hecho ya se puede hacer con algunas aplicaciones que tú el lenguaje natural tiene una aplicación que tenga un formulario y ya pasa eso eso ya pasa lo que pasa que claro está el tema de diseñar tu sistema la parte de pensar hay veces que le tienes que decir por ejemplo quiero que más una función que el modelo no está entrenado pero esto sabemos que es cuestión de hecho es alucinante en las cosas que se pueden hacer y han habido demos de openia y que es la empresa esta que ha hecho chat gpt que son increíbles que sin saber programar nada puedes hacer cosas muy complejas y de hecho en un directo el primer directo que lo probé el chat gpt me quedé

helado o sea no me lo esperaba para nada para cosas chulas pongo un código fuscado y le digo tío Búscame Sí claro sácamelo en Normal Mola Mola a ver a mí me da igual en el sentido de que cuantas más herramientas hayan para hacer software más rápido mejor sí claro pero tiene que ver sí sí eso está en otro nivel está genial pero sí que es verdad que te voy a decir una cosa cuando yo trabajaba de programador full time había una cosa que no que yo nunca entendí Me parece muy no he encontrado mucha gente que comparte esta opinión conmigo porque no no lo sé vale No sé por qué pero siempre he visto como que cuando montas un proyecto Hay un montón de tareas repetitivas Hay un montón de código que lo picas 80 veces hay un montón de configuraciones que siempre son iguales y de hecho yo en su momento me desarrollé un ya en una empresa que estaba haciendo como trabajar una empresa videojuegos que no teníamos ningún juego para lanzar en ese momento y estaba un poco de research vale Y me creo un sistema donde tenías un archivo donde definía un poco con lenguaje natural algunas cosas y me generaba la aplicación como yo quería vale Y me ahorraba muchísimo tiempo en general los modelos la base de datos la Api Rest todo yo digo no puede o sea debería haber muchas más cosas de estas O sea no tiene sentido que cada vez que voy a hacer esto tenga Que picar el código no le veo ninguna lógica yo creo que también el uso de frames facilitan gran parte todo esto no en el caso de gran parte Exacto hay dos puntos el punto del framework que el framework directamente te da muchas cosas hechas a día de hoy Quién hace vanir la php no no nadie nadie pero aún así O sea imagínate que yo tengo un árabe y quiero montar un proyecto y quiero poner y Quiero crear una Api Rest exponer ciertas cosas y quiero montarme un admin tengo que picar bastante código si volaría que tenga un configurador que le dé un botón y me lo hace de que deje de batería Sí claro que se podría hacer por eso yo en su momento trabajé mucho en esto en crear generadores para mi trabajo que me generen código y de hecho hoy en día casi pero luego eso es un poco template spoiler Plate y todo esto que se llama y aparte de eso hay muchos frames que te hacen muchas cosas pero yo creo que la Inteligencia artificial lo que tiene de bueno es que es más específica o sea tú para poder generar tú dices quiero generar una aplicación que tenga estas estos modelos que tengo una Api de este tipo y que exponga estos Campos Esto lo puedes hacer si hay algo que está programado para ese caso y funcionará para ese caso pero la guía te permite inventar cualquier cosa Sí claro donde quieres o hay muchos colegas que son programadores que a veces dicen es que no sé exactamente lo que quiero pero o sea Perdón sé lo que quiero pero es exactamente como comenzar Entonces el chat por ejemplo podrías empezar por aquí no o por ejemplo de otra persona Y dices exactamente esta persona que narices quería hacer aquí coger la función la pegas hecha geometría Explícame y hace esto buah es que es verdad pero es también vagancia y le dices optimízame este código claro es que yo veo yo veo a Chad y todas estas utilidades veo como que los programadores Ahora son cyborgs una fábrica de programadores no es como que tú eres programador pero estás aumentado con la guía hay un colega que me dice una cosa que siempre hace Muchas gracias cuidado que no te reemplace por un Script es decir el valor que vas a tener que aportar va a ser otro no es generar ese código Sí yo creo que esto lo hemos vivido que también hay mucho reino de tarifas cuando desarrolladores no un poco y luego pasas una herramienta de cod coverage Y ves que realmente están multiplicando O sea están multiplicando el código repitiendo el código un montón de veces perdón si se ha vuelto muy técnica la conversación que el trabajo de los programadores o sea lo que lo que veo es que todo el trabajo o sea sí que es verdad que en el mundo la programación hay mucha gente que calienta sillas Sí mucha y en el mundo de la informática en general seguro que pasan ciberseguridad también entonces yo creo que lo que sí hace falta es es un jefe un supervisor

alguien que un cto un ciso me has dicho no ese tipo de figuras siempre va a estar pero sí que es verdad que luego hay muchos puestos que pueden ser sustituidos o asistidos por una guía es importante nate aportar valor aquello que haces por eso yo creo que es importante lo que decías tú conocer las bases O sea no puede ser que seas un es un tema que quería hablar hoy también contigo veo mucho experto en ciberseguridad o que trabaja en ciberseguridad que conoce muy bien las herramientas pero no sale de ahí y también pasa en el mundo de la programación conoce el framework pero no sabe qué hay debajo conoce la herramienta pero no sabe qué hace exactamente sabe cómo la tiene que usar que la tiene que usar pero no entiende sabes y esto creo que es un fallo por parte o sea está bien porque cumples un trabajo tienes un puesto quizás estás bien ahí la empresa te quiere ahí pero limita mucho verdad te limita muchísimo y además no te permite tener capacidad de adaptabilidad a problemas que puedas tener Es decir en el día a día hacemos el curro estamos inmersos en eso y si se haces hacking haces lo que sea o desarrollas estás acostumbrado a trabajar con tu vídeo de confianza o con tu próxima con lo que sea lo que hagas pero claro cuando hay un problema tienes que tirar quizás de hacer de googlear eso no tienes que entender bien cómo funcionan las herramientas exactamente puedo simularla yo puedo hacer un Script que no que simule el problema o Modificar el código o Modificar el código exactamente y Añadir algo que te hace falta o lo que sea hay gente que se hace súper pesadas herramientas en base a herramientas que ya están publicadas porque no tienen aquello que aquello Exactamente para su caso de uso que necesita Entonces es importante y luego otra cosa que hablábamos antes lo repetimos Ahora hay gente que hace un curso de cierra las de desarrollo en python y ya desde que es full stack o de joder Pues no te falta a ti tiempo para hacer eso no o un curso de de la plataforma que sea da igual y ya te crees que es un hacker no va mucho más allá todo esto sí sí sí o sea realmente que dedicar tiempo y son los años de experiencia también por lo que o sea tú realmente para qué quieres hacer esto no es que yo quiero ganar pastas que ahora está muy de moda eso tío eh hace poco estaba en un íbamos para una conferencia de ciberseguridad y me acuerdo que con uno de los que estaba ahí decía más que me hacía gracia decía quiero que Quiero ganar pasta ya ya pero es que yo para ganar x sueldo que tenía que ser x sueldo me tienes que tirar 14 horas en esto que no quiere decir con eso ahora no nada que te tiras un viejo entonces me refiero que hay una trayectoria Claro claro o sea el día uno no es que cobres ese sueldo claro tampoco y pasa lo mismo en desarrollo que mucha gente dice hay un montón de trabajo en programación se gana mucha pasta y hay veces que que he conocido casos que no entiendo que es como gente que ha hecho un bootcamp y ha encontrado un trabajo y cobra bien que no lo entiendo No sé si no sé si es porque esta persona tiene mucho talento le ha ido muy bien y sea en casa empollado todo o a lo mejor trabajar una empresa donde tienen todo Juniors y los paga muy bien porque los necesitan como agua de mayo no sé muy bien Cuál es el caso pero normalmente cuando tú haces un curso un cursito un bootcamp o algo así este tipo de formación tan limitada y tan específica no es que sales al mercado laboral y ya tienes trabajo de eso cobrando un buen sueldo o sea incluso conozco casos de gente que le cuesta mucho o sea después de haber hecho este tipo de formaciones y con eso no quiero estigmatizarlos ni mucho menos pero hay como dos tipos de bootcamp yo los diferentes meses que los hay que dices tres meses tú eres programador tres meses para aprender a programar alguien que hace que sea camarero camarera No no es muy difícil eso eh Y luego están los buscan de siete meses bueno es que está un poco la misma línea en realidad yo entiendo que los bootcamps te venden mucha caña pero es como yo siempre lo comparo porque yo también toco la guitarra vale Y cuando tocas la guitarra cuando ves

a un chaval que lleva un año Por muy bueno que sea te das cuenta que no lleva años y años no claro lo ves lo ves ves algo ahí ves un verdor ahí yo toco la batería y entonces y cuando ves la gente que lleva 10 años o 20 años dices lo notas joder Es que esto esto ya no es que este me quedo un poco es que estoy años luz pero ves a alguien que lleva un año igual ese año se ha machacado entero todos los días igual es muy bueno ya he conseguido muy buen nivel pero te das cuenta de que no llevo aprendizaje capacidad de adaptación Hay un montón de cosas que quizás van en tu favor la experiencia es un grado tío eso Entonces qué pasa con lo que me cuenta Por ejemplo un colega que tiene una empresa de desarrollo que cuando cuando coge a gente de bootcamps se da cuenta que cuando lo sacas un poco del stack que ha visto en el Boot están jodidos tío es que va mucho más allá de lo que nos pensamos el tema de desarrollar es un tema estructural de la cabeza es un tema de conocer las tecnologías es una es una serie de preguntas hostia esto es básico Eh sí sí sí sí le dices que haga una conexión con una Api dice cuidado eh Y a mí me da complicado eh A ver yo aquí no puedo ser Imparcial porque yo tengo una academia de cursos pero o sea lo que voy a decir ahora evidentemente soy Imparcial pero una cosa que a mí siempre me molestó muchísimo y que justamente ahora que estamos haciendo un poco preparando la campaña de las campañas de marketing de este año cómo vamos a enfocar todo el tema de cómo nos vamos a vender etcétera analizando lo que hacen otros otras academias te venden eso te venden claro yo intento de hecho lo que le he dicho al equipo es vamos a enfocarnos vamos a hacer todo lo opuesto vamos a decirle a la gente no vas a ser programador en tres meses es imposible pero vas a aprender todas las bases que necesitas para hacer un profesional de la voz o sea de hecho nosotros por ejemplo tenemos eso cursos básicos cc enseñamos las bases de la todo el don o sea cursos para entender las bases de sql o sea es como que cantamos muy bien las bases pequeños con píldoras pequeñas y sobre todo mucho learning mucho proyectos mucho proyecto que tengas mucho proyecto para desarrollar Pero esto que hace muchas empresas de decirte o sea se está jugando mucho con la ilusión de la gente lo que veo no me Mola no soy Imparcial en esto porque también estoy metido ahí yo intento hacer todo o sea nosotros intentamos hacer todo lo contrario pero sí que es verdad que me parece que se está monetizando la ilusión de la gente las ganas de salir adelante de ganar dinero el prometerle en tres meses vas a trabajar de esto y eso me parece poco ético sinceramente un experto después de un año todo después de un año habrás visto muchas tecnologías se han plantado una semillas como entra en este máster el año estarás cobrando tanto cada día y más trabajo de marketing O sea ya te digo cuando estamos haciendo esto y empezamos a analizar el mercado Y empezamos a ver todo lo que está haciendo la competencia dije madre mía tío me parece y además un gran problema es competir con los udemys con Los pulseras no Pero además que hay cursos por dos euros sabes que es complicado a veces competir pero son o sea nosotros es un enfoque diferente no somos nada caros somos muy competitivos pero la calidad o sea esto ya da para una conversación mucho más larga y tampoco me Mola decir mucho estas cosas porque no soy Imparcial sabes pero yo veo un problema de calidad muy grande tío la formación online Es que yo he comprado muchos cursos y son para yo que sé tío para matarlo y que lo ha hecho sabes compras un curso que igual se hizo Hace cuatro años lo que pasa es que obviamente pues de tus expectativas el tema son las expectativas pero si las expectativas pueden ser erróneas lo que me parece poco ético es que te vendan eso sabes que te hagan campañas de marketing diciendo dedícate a esto en tres meses vas a trabajar de esto y te venden así el curso yo creo que todos tenemos que partir contigo corresponsables en eso y cuando lo veamos denunciarlo Obviamente con positividad siempre se

ha dado el truco Body positive ahí a muerte ser positivo pero también para decirlo Oye esta movida no no funciona todo es falso no me jodas sabes y también la gente que está quizás más haciendo las cosas como debe Como vuestro caso pues Oye seguir haciendo seguir fomentando esas prácticas es lo que intentamos y una pregunta tío a ver vamos a meternos un poco más en tema Bueno es posible Cuéntame el ataque más chungo que has visto en tu vida el ataque que he visto Lo que te puedo contar son que yo diferencio como dos grandes particularidades una serían los ataques que se aman de los grupos apt que serían aquellos ataques en los que el objetivo es recabar la inteligencia por tanto son grupos que intentar permanecer inteligencia que serían datos datos de gobiernos vale en el que intenta permanecer lo más ocultos posibles durante mucho tiempo vale ese sería como como un paradigma diferente y lo otro sería el mundo del crankware lo que hablamos de más lo que se llama final malware que sería malware que es el objetivo es recabar credenciales o agendas de contactos o yo que sé robarte información del pc no que se llama igual que te podía atacar a ti y a mí sabes a quien sea no Claro los ataques de los grupos de apt son muy sofisticados porque son piezas de malware que son complejas son lenguas grandes que tiene mucha cifrado las comunicaciones Son son cifradas que cuesta analizarlas que el Software que o sea el malware está muy bien protegido entonces todo esto digamos que dificulta mucho a alguien que está en el lado de los buenos de ver un poco la full Pixar no ver un poco todo todo como cómo funciona no hay un montón de casos Les recomiendo a la gente que se mire por ejemplo el ataque de Residen o ataque de la campaña de flare o equation o spagnet no en su momento por ejemplo un grupo de apt que el sistema de command control es decir donde estaban las conexiones para enviar los datos era una red de satélites qué loco No es muy locura es una red de satélites que pero esos satélites o sea los satélites que tienen Linux instalados pues tienen sistema operativo que tú enviaba los datos por ejemplo esto es una locura es una locura no o en el caso de Racing por ejemplo creo que utilizaban alguna movida de centrales eléctricas para enviar los datos Y esas unas locuras también que flipas o por ejemplo hay una novia también muy chula Que es que en la víctima colocar unos unos como unos virtual Drive como unos archivos que has utilizado una vez truck no vale esto es un software que tú creas un fichero un contenedor cifrado y tú lo montas como en una unidad virtual Ok pones un password y solo montas con y puedes copiar datos ahí y tú lo lo desmontas Y entonces queda como un fichero estanco Y eso es lo que utilizaban por ejemplo todo lo que ha pasado con villarejo y todo esto y tenía un tenía un volumen intentando pues petarlo y todo eso Entonces por ejemplo el caso de algunos grupos de apelle pues colocan estos virtual drive y dentro de ese colocan datos de la campaña de datos que han robado y tal entonces tú como analista vas a mirar eso está cifrado y no puedo romperlo por fuerza tampoco hay forma porque hay forma estaría demasiado poder entender cómo está cifrado primero también no Claro sí Entonces ahí como ataques complejos que utilizan este tipo de cosas No pero sobre todo sería Marvel que es digamos que son que son multicomponentes vale o piezas de malware que tengan movimientos funcionalidades en plan de yo que sé dibujación de teclado robo de pantallazos tema de robo de credenciales pero que son digamos de analizar porque vienen muy protegidos estos días Lo más complejo Que te puedes encontrar a día de hoy o malware que cuando una vez que te infecta la máquina y esto se reinicia desaparece todo el rato está solo en memoria por ejemplo no si esto pasaba con Es que yo he hecho a ver yo de ciberseguridad no sé tanto vale o sea de hecho no sé nada Sé muy poco pero lo poco que sé es por mis años de Friki y los vídeos que he hecho de YouTube y recuerdo el cómo era mira ahí vale mira ahí hacía eso cuando reiniciaba se borraba en memoria se borraba Pero estabas en el CNC en la lista y debería

infectar eso es eso es no hay malware que piensa que Cuál es el objetivo del malware normalmente sobrevivido al inicio es como un virus son parásito no Entonces para los grupos de apt que el objetivo básicamente inteligente permanecer ocultos pues lo que quieren es Oye robo lo que necesito estoy aquí no hago mucho ruido Cuando pueda me voy y si no me has pillado pues mejor sí entiendo Pero hay familias de que han permanecido ocultas durante más de 10 años eh Y que al final las han pillado porque han visto una unas funciones en un malware que luego han hecho una regla de búsqueda con esto entonces han encontrado en un Corpus en una base de datos grandes de ficheros de malware han encontrado esta muestra de Mago han dicho hostia esto qué coño es una cosa y como por ejemplo el eternal Blue creo que se llamaba el exploit que se utilizaba para eso cuánto llevaba eso por ahí claro es que el eternal de Windows si no me equivoco y esto lo usaba el gobierno de los Estados Unidos para se utilizaba creo que era la nsa si no me equivoco y estaba bueno es que claro son muy peligrosos o sea básicamente para ponernos en contexto la nsa conocía una vulnerabilidad muy bestia de Windows y no la divulgaba porque le interesaba usarla Claro pero claro eso es muy peligroso al mismo tiempo no la divulguen es importante los países tienen capacidades ofensivas y esto lo lo utilizan no es decir para defenderse también no Y para un poco también atacar a países extranjeros Esto está a la orden del día la ciberguerra es real no O sea sí claro ahí estamos en medio de Ciber guerras todos los días hay digamos ataques que se hacen de que ocurren en países que los ataques vienen de otro hay casos no como el caso de Estonia es un caso claro ejemplo de que los dejaron sin enlaces internet Bueno pues hubo no se quedó en movimiento una figura No sé qué hostias de algo pasó a nivel de país que atacaron y dejaron a Estonia sin acceso internet por eso a Estonia ahora es un referente en centro de respuesta de incidentes tiene un equipo ciber muy muy bueno y de reservistas muy bueno yo recuerdo también una cosa que me chocó mucho cuando cuando leía acerca de ella que fue cuando Ucrania comprometieron la infraestructura de red eléctrica atacando los plcs de las centrales Claro que no sé hoy en día como cómo está el tema pero cuando tú vas a una central eléctrica o a infraestructura básica del país el tipo de ordenador que se usa como por ejemplo los plcs son ordenadores como muy básicos muy rudimentarios no que realmente no tienen ni sistema de usuarios o sea son como máquinas que controlan como robots claro eso es un problema porque ahí no existe la seguridad no en ese tipo de por suerte va las cosas Sí de hecho hay empresas líderes que se dedican a temas de seguridad industrial que son muy buenos aplicando medidas de mitigación Yo tengo un colega que trabaja en alguna de estas Sí sí Borja compañías algún día veis el vídeo puedo decir el nombre son súper buenos en esto y son empresas que se dedican desde temas de seguridad industrial y se dedican un poco a estas seguras Claro porque Supongo que es eso no O sea yo cuando leí eso me chocó porque hubo un caso muy famoso de Ucrania que en invierno en pleno invierno en Ucrania dejaron sin electricidad a la ciudad durante un tiempo no se sabe quién fue Se supone que se sospecha que fue Rusia evidentemente Quién va a ser y nada fue bastante heavy porque la gente se podía morir congelada o sea literalmente ahí si no tienes los ataques de Ciber que al final radican en el mundo físico tenemos el caso de stacknet en el que pues para mí es el primer ataque en el que pasas del mundo ciber si se puede llamar así al mundo físico en el que tú modificas la temperatura o el control de temperatura de un maldito reactor nuclear el rollo era lo mismo no porque eran también pelleces eran ordenadores de estos que eran como distintos eh era una movilidad había como que podías lo hacían con pendrive o algo en un sitio que luego los enchufaban en el ordenador luego tenía como un montón de posibilidades distintas para infectar realmente se encontraron dijeron tu equipo Era

realmente complicado también que infectaban el firmware del disco duro Wow el firmware del disco duro como lo detectas eso complicado eso es una locura eso el sistema operativo no tiene acciones una locura eso claro el sistema operativo realmente a nivel complejo no y es verdad que a veces dices hace falta de todo eso y luego al final inigualacion operativo y pongo un estilo y me lo llevo todo sí Ok hay en sitios que te hace falta hacer un Chain de ataque mucho más complejo el tema de stucknet que fue bueno que da para otra hora más así que tampoco me quiero enrollar tanto pero fue muy loco no O sea fue un virus que estaba creado para descalibrar unas máquinas de enriquecimiento de uranio en Irán Si la gente quiere ver un poco todo esto yo le recomiendo que se vea la película Hasta donde sale el tío este de Thor Cómo se llama el Chris explicando toda la historia que se llama Black hat en el que el protagonista hacker es el tío de Thor Aunque bueno en el que la película en realidad explica eso de hecho la película La vas a ver o no sí sí entonces interesantes para celebrar el lanzamiento del vídeo y la entrevista de hoy que me está molando mucho tío vamos está son cuestiones interesantes pues la película de blackhad explica esto explica que el Chris con un colega suyo desarrollan el malware que utilizan que utiliza un grupo un grupo de malos de la película para sacar las nuclear está explicando lo de realmente en un modelo cinematográfico pero fue un caso que superó la ficción yo creo que fue un antes y un después para la industria sinceramente no a nivel de marketing a nivel de cuidado que estamos hablando de cosas cuidadito que estamos hablando de cosas serias Eh sí sí total o sea porque sí los datos de la gente tal importante no sé qué inteligencia no sé cuánto pero ahora en el momento que inhiben no sé si está en Netflix no tengo ni idea Buscar dónde puedo ver Black hat y sale por ahí sale ahí en las plataformas y otra pregunta que me están haciendo por aquí que es muy interesante qué piensas de Windows defender de Windows defender eh pues como todo nate es decir es mejor que es mejor no tener nada o tener buenos defender obviamente quieres una solución de empo y más profesional y tal coge cualquiera de las que te ofrece el mercado en realidad es un poco más Premium y tal Es verdad que si bien integrada con sistema operativo pues está Guay también es algo que por lo menos ya te viene no pino mal lo que digo es no lo dejes por defecto mientras opciones quizás hay cosas que puedes activar Infórmate un poco o Pregúntale a alguien que sepa un poco más que tú en eso pero obviamente por lo menos en algo pero hay mucha gente que cree que hoy en día ya no hace falta el antivirus eh mucha gente bueno nosotros ya en el vídeo ya me explicaste bastante a fondo cómo funciona este mundillo y tal y el tema es que al final del día estamos viendo por ejemplo ya el último tema de hoy porque tú si fueras policía o militar en una zona de guerra saldría sin chaleco antibalas y sin casco ni militar el de un helicóptero que vas con paracaídas o a la bicicleta saldría sin casco pues entonces pero es lo que te digo por ejemplo yo yo sí que tengo mucha conciencia de tengo una empresa tengo datos tengo un canal de YouTube tengo antivirus en todos los ordenadores y por ejemplo lo que le pasó a sfd que yo pobrecillo que tampoco quiero aquí martirizarlo no lo Hubiese pasado quizás si hubiese tenido un antivirus de Oh sí pero digamos que le está protegiendo encontrar una amalgama grande el tema no es el tema anterior nunca me ha pasado nunca me va a pasar nada no el tema es Oye pongámoselo un poquito más difícil el tema no pongamos las cosas tan fáciles activamos el segundo factor de autenticación cambiamos las pagos usemos pagos managers pongamos antivirus hagamos un poquito más difícil nos han quedado muchos temas tío eh manager qué opinas pues Considero que es esencial no esencial O sea que no lo tenga está perdiendo el tiempo es duro mantenerlo eh qué va es un tema de hábitos claro que es duro pero pero hay que ir yo tengo yo tengo para jugar manager lo que pasa es que yo yo claro yo tengo un hábito que es que uso muchos peces por la

naturaleza de mi trabajo mejor uso muchos peces mejor es más a veces uso de un pc otro dentro de eso como servicio Sas Hay un montón de opciones que puedes usar tanto gratuitas como hosteadas por ti la mejor digo yo soy usuario de One password por ejemplo vale para mí es la aspas las pasasteis un montón de brechas de seguridad joder pues me cambiaré tío hostias funciona muy bien también la funcionalidad está de buscarte el links de si tu contraseña está Pues creo que me pondré esa Sí además tiene está un poco tiene Bugs y cosas raras a veces no va a veces no patrocina Este programa a Juan Pablo tío te veo haciendo un vídeo patrocinando con polvos bueno es que es que hay un montón de vídeos de internet que patrocinado a mí nunca me han ofrecido Pero estaría Guay me preguntan qué opinas el mal el mal absoluto a ver digamos de punto de vista de responsable de seguridad es un problema desde el punto de vista de ahí que haga soporte y tal es la herramienta perfecta con escritor remoto Hace como un año no no sé que tu pareja le entraron en el ordenador muy muy raro qué le pasó mirador abriendo un email por un trabajo vale ella se empezó a trabajos de modelo campañas en diferentes partes de España Entonces le habían mandado una agencia un email para que le para hacer un trabajo en Madrid y le dice Bueno Métete en este enlace y así por esta información para darte de alta en el sistema no sé cuánto y ya no tenía mi papá de informática y entró al enlace se fue a la ducha porque tenía que dejar no sé dijo déjale un rato que tarde en cargardísima y yo y de casualidad paso por o sea paso por enfrente de ordenador y veo el mouse moviéndose y estaban intentando como copiar archivo no copiar nada y nada pero pero por un momento que pasé adelante es un problema es un problema mira tu comunidad estaba preguntando sobre Beat worden buena solución también para hacer gestos de contraseña este pico qué opinas yo no lo pongo ni que me paguen ahora vamos a quitar de la ecuación esa gente que obviamente no pueda ser el precio de una licencia es la marca de la casa vale eso tiene más regalos que eso es como el truco trato sabes de Halloween y el truco y dices hostia no sé si quiero saber lo que hay detrás Sí sí sí yo tampoco lo usaría y que te quería preguntar ya ya está último tema Qué pasó en el hospital ostia lo que ha pasado en Barcelona el hospital Clinic Pues nada muy grande por cierto muy importante Barcelona y lo que ha pasado ha sido que hay un grupo al parecer que se llama ramson House que al parecer habría vulnerado la seguridad del hospital y habría extraído datos no se sabe todavía el alcance la base el alcance de lo que ha pasado y ha sacado a todo el hospital y es un grupo que está especializado en extorsión y eres filtración de datos que yo estaba ahí igual está la agencia con los mossos de escuadra revisando lo que ha podido pasar allí y tal y imagino que harán declaraciones al respecto cuando tengan más datos es importante desde aquí lo digo no inferir lo que ha pasado sino esperar a que comuniques a través de lo que ha pasado Bueno hasta igual estamos aquí hablando y ya se ha publicado todo el directo pasa estas cosas vale vale Pero hay un ransomware claros aunque se llaman ramson House no es un grupo de ramsomware como tal es decir Ellos tienen alianzas con otros grupos de ramsomware que en el que ellos pueden utilizarlo pero ellos no son un grupo al uso sabes Ellos están especializados en excitación y en exportación de vulnerabilidades son como un grupo de hacking super mega especializado y súper mega con capacidades ofensivas son muy buenos en eso y de hecho probablemente vendan el acceso a los grupos criminales para que hagan sus cosas y de hecho el tema de los hospitales es bastante complicado porque tiene muchos datos tuyos muchos datos Y aparte lo que ha pasado ahora con el hombre tiene que volver al papel igual y en muchos casos no O al principio pasaba eso Pero además otra cosa interesante House es que si lo comparamos con otros grupos de rabsonware tienen normas muy estrictas de que no puedes atacar hospitales ya es un poco raro no tiene normas da igual de hecho ellos se venden como una

empresa de ciberseguridad nosotros realmente Simplemente te avisamos que tienes un fallo de seguridad y bueno queremos que los padres por el trabajo no O sea el tema de los hospitales me parece bastante turbio porque claro realmente tiene un montón de información tuya y no la tienen Bien protegida es uno de los grandes problemas que existe que por mucho que yo personalmente haga todo bien tenga todo súper protegido no divulga nada de información mía al final Hay algún sitio vulnerable como el hospital mismamente donde tiene una ficha mía muy detallada con muchas cosas mías y la gente puede podría llegar a filtrarse como monitor.mocilia.org y ponemos tu dirección de correo electrónico personal seguro que vas a estar en siete lo he visto lo he visto yo lo he mirado la cuenta de Gmail es de hace claro el problema es en el hospital que hay datos que son más personales una patología concreta o algo no cáncer o alguna de estos Pues imagínate en este caso una personalidad política o alguien una celebridad por ejemplo en el que tengamos una patología es una patología que nadie lo quiera pero es una patología que tú no quieres pues no quieres decirlo y ahora recibes te dicen Oye te he visto que estás en directo en Twitch con Mark y estáis hablando de esto y hemos visto que tienes yo que sé alopecia y no quieres que se sepa y vamos a decirlo la explosión individual y Qué deberían hacer tío con el tema de hospital es que se puede hacer Pues yo creo que hay que como usuarios estar muy al loro de lo que se está haciendo la gente que espera que sea usuario el Clinic pues está muy atento a lo que se está publicando informarles más no sobre todo también materia de inversión imagino Eh buenas alianzas con partners y alianzas en ciberseguridad concienciación siempre lo decimos evidentemente que también se puede votar de un equipo de expertos en ciber para que les pueda ayudar claro los recursos con los que cuentan la infraestructura que tienen quizás están como muy protegidos Pero quizás ha sido una cosa de estas que no un acceso físico Que también es muy fácil no sabe nadie o mismamente eso de que tú entras en un hospital y nadie piensa que eres un hacker eso es el ordenador está ahí según miran otra cosa pero que toques en los ordenadores cómo sabes que el tío que ha venido detrás de un paquete mientras estaba yo aquí es solamente el tío del la paquetería y tiene que hacerse la física al edificio yo que sé mil mierdas que pueden cosas que pueden pasar pero bueno Así que con el tiempo esperemos que el tema de hospitales se ponga un poco las pilas porque no es la primera vez que pasa y una vez que pasa y estoy seguro que seguirá pasando ya te lo digo porque hay tanta la variedad de ataques y luego otra cosa también el que defiende nunca salen prensa El clínica parado este mes 700.000 ataques que es igual También deberían decirlo Bueno de hecho Mola que Safari ahora Cuando entras te dice este mes hemos bloqueado no sé cuántos accesos que tengo que revisar con cuidado pero es eso yo creo que también es bueno los informes de estadísticas y tal yo creo que son buenos para también decir Oye están haciendo cosas al respecto sabes No es que sea una institución que no tenga que esté ahí a la mar perdido de Dios sino que obviamente tendrán sus recursos y probablemente mucha ayuda bueno tío Yo creo que con esta última reflexión sobre los hospitales lo vamos a dejar básicamente por la hora porque tengo como 40.000 temas más para hablar pero tres horitas se pasan rápido en realidad pero bueno entonces te has pasado bien Sí claro tío joder Pues nada tío tendré que volver otro día porque me han quedado muchos temas y yo creo la gente le ha molado Así que nada tío Muchas gracias por venir y nada espero que vuelvas pronto y claro que sí cuenta con ello y poco más ya sabéis tienes alguna red social que quieras promocionar con mi propio Nick en Twitter O sea que el que quiera que me siga preguntas ahí tengo los abiertos cualquiera que me quiera Preguntar lo que sea O sea que encantados tíos