Actividad [#3] – [Proyecto final]

[Seguridad Informática I]

Ingeniería en Desarrollo de Software

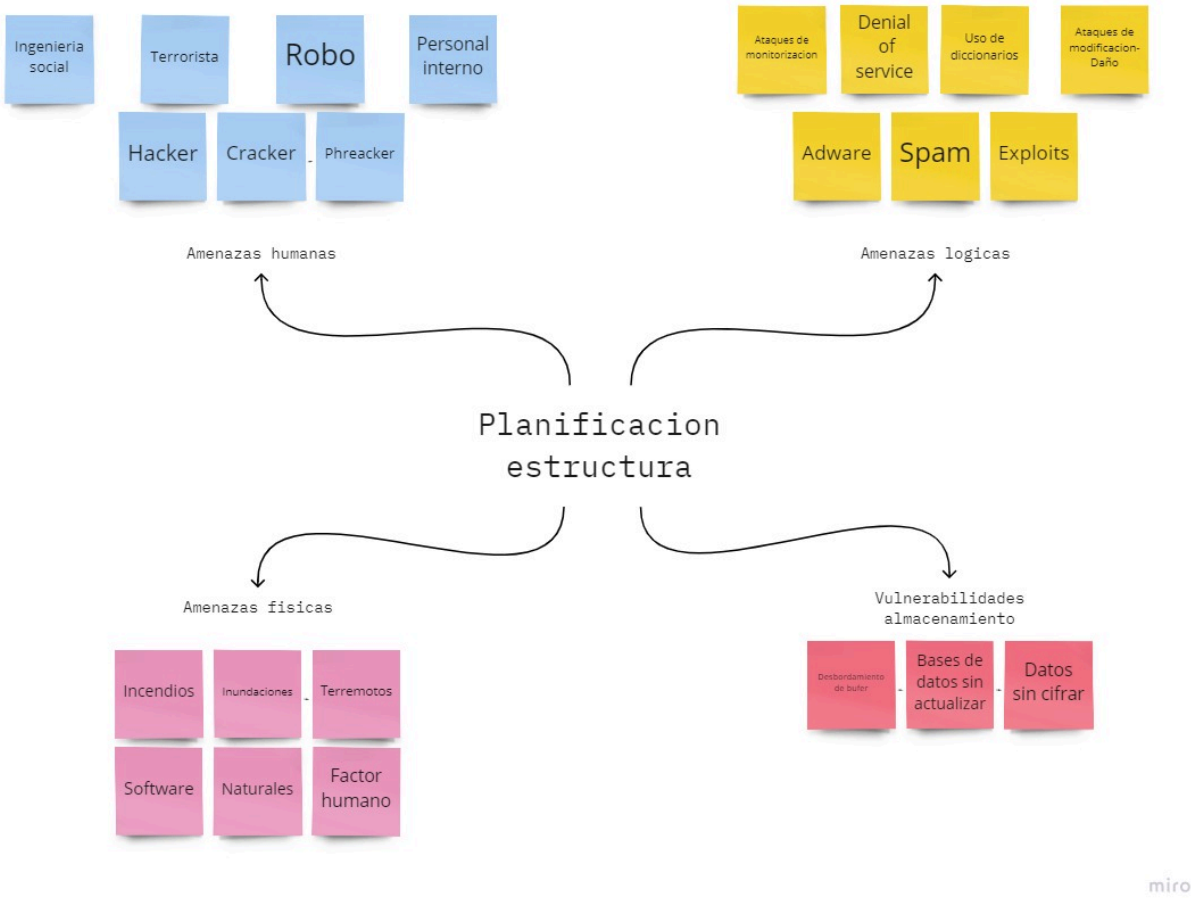
Tutor: Elizabeth Guevara Roa

Alumno: Manuel Enrique Ramirez Lopez

Fecha: 26/04/2022

Indice

Delimitacion del problema



Amenazas humanas

5 amenazas

-De personal interno que encuentre un “bug” sin ser de forma intencionada pero que a su vez se beneficie de ello.(Robo)

-Sabotaje o compra de algun cracker a personal que tenga acceso a computadoras clave (Ya que se usa red lógica y cerrada) con el pretexto de “ten toma esta USB y solo conectala a X maquina”.(Ingeniera social)

-Cracker cuyo proposito es sacar ventaja de los datos de los clientes, ya que por la rama que se maneja de la empresa manejar una informacion tan delicada expone a los familiares de los internos y este sujeto busca enriquecerse a costa de los demás.(Intrusos remunerados)

-Phareakers buscarian obtener una linea oficial de la clinica para con ello gastar bromas a clientes y así afectar a reputación del establecimiento.(Ex-empleados)

-El uso de procesos inadecuados para la destrucción de informacion delicada (cuando rompes recetas, contacto de clientes, datos bancarios). (Trashing)

Amenazas lógicas

5 amenazas

-Aprovechamiento de exploits en el sitio web para así infiltrase dentro de los servidores principales (recordemos que el firewall esta inhabilitado)

-Falta de supervicion en equipos expuesto, es decir equipos que están al alcance de “clientes” que a su vez insertan Gusanos para propagarse en toda la red del establecimiento.

-Pishing para obtener datos mas detallados de los clientes internos y así obtener ganancias a través de fraudes u obtención de informacion bancaria de los familiares de los clientes.

-Ataque “Denail of service (DoS)” para inhabilitar el sistema usado y así colapsar estructura internar, ya que los servidores no están preparados para resistir dicha carga masiva de datos.

-Gracias al caballo de troya se a insertado un malware de monitorizacion en los equipos y dicho craker se dedica a la obtención de informacion vital como los usuarios y contraseñas de cada equipo y así averiguar cual es la funcion que desempeñan.

Amenazas físicas

5 amenazas

-La principal amenaza que pueda en caso ocurrir es inundación ya que recordemos que esta ubicada en la costa y por alguna amenaza de tsunami pueda afectar las oficinas centrales y su informacion.

-Incendios ya que si no se cuenta con una correcta refrigeración como esta ubicada en climas húmedos y calurosos esta pueda afectar o provocar algun incendio electrónico dentro de las sedes principales.

-Adjunto al punto anterior tomas las medidas necesarias para sobre llevar el oxido que se pueda generar gracias al mar ya que las fuentes informáticas o mejor dicho la tecnología no va de mano con la humedad y las sales provenientes del mar.

-Tener una cúpula por manejarlo de una manera mas sencilla en caso de algun siniestro de terremoto ya que en la zona ubicada son mas frecuentes estos y con el movimiento pueda generar inconsistencias en los datos o alguna falla en cadena.

-Instalaciones electricas y reguladores de voltaje para no adquirir ruidos o picos de tension dentro de las instalaciones, adjunto contar con una planta en caso de emergencia o apagón general para así durar horas, días en lo que se restablece por completo.

Vulnerabilidades del almacenamiento

5 vulnerabilidades

-Violación de datos, es decir que algun curioso ya dependiendo sus intenciones podrá ser hacker o cracker acceda de forma ilícita y podrá visualizar, robar, destruir o alterar datos almacenados en los distintos medios de almacenamiento.

-Perdida de datos o mejor dicho destrucción de la informacion almacenada estos acontecimientos pueden ser causados por algun “ataque terrorista”

-Secuestro de informacion, como se menciona en el punto anterior las intenciones pueden variar de los terroristas que van desde destruir a secuestrar informacion y de alguna manera cifrar-la de manera que sea imposible recuperarla a no ser de pagar algun rescate.

-Denegación de servicio “DoS” como forma parte de actos de terrorismo este metodo va de como lo dice la palabra deniega es decir bloquea toda acción de almacenaje, consulta o gestión de la informacion lográndolo de cierta forma saturando todas sus fuentes de procesado, comunicación y almacenaje.

-Malos procesos de mantenimiento en los medios de almacenaje (servidores) que va desde mala ventilación que provoca un mal funcionamiento y deterioro de el equipo usado hasta la mala planificación de cambios físicos de discos duros.

Vulnerabilidades de comunicación

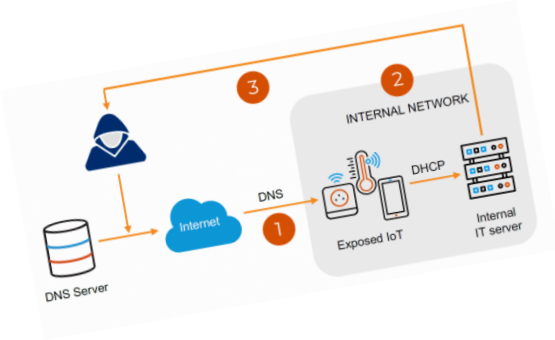
5 vulnerabilidades

-Software vulnerable, el uso inadecuado del software fuera de la estacion de trabajo, que este abierto al publico en general.

-Equipo de desarrollo, establecer las bases para mantener actualizado el sistema y que el equipo de desarrollo en turno este en constante mejora del sistema.

-Falta de activación de firewall en cada equipo ya que esto hace vulnerable al sistema de ataques externos (internet) y perdida de informacion o suplantación de software que conlleva a fraudes.

-Ataques “DoS” Denegación de servicios, con una masiva de conexiones simultaneas buscan saturar o mejor dicho tirar el sistema generando así perdidas importantes.



-Amenazas de malware que este mismo se pueda infiltrar desde la red o directamente con algun personal interno que tenga malas intenciones colocándolo en computadoras-servidores principales.

Bases de datos

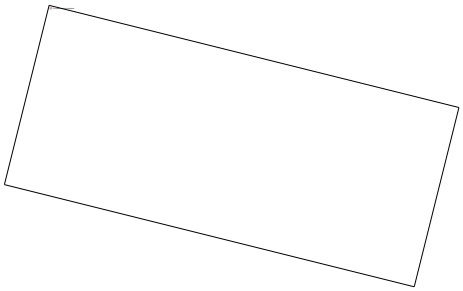
Recomendaciones

-Solo personal autorizado puede acceder a los servidores físicos, a su vez aislar completamente en una sala o piso los servidores y reforzar los accesos, que en las entradas y salidas se tome captura de huellas, iris y tarjeta electronica de identificación del personal que acceso a dicha sala.

-Al momento de diseñar las instalaciones tomar en cuenta factores externos que puedan llegar a afectar dicha instalación como pueden ser riesgos naturales como en este caso lo son los tsunamis y o terremotos, colocarlo de manera estragica para salvaguardar toda la informacion.

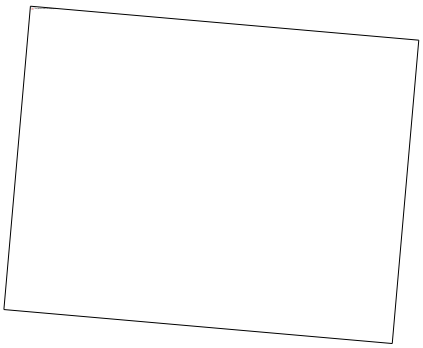
-Contar con respaldos en caso de perdida total del centro principal, con esto implementar las mismas medidas que se mencionaron en los puntos anteriores pero esta vez en una locación mas segura centricamente donde los factores externos (sociales y naturales) sean mínimos.

-Nombres de usuarios y contraseñas seguros y no fáciles de adivinar, es decir no poner datos que sean fáciles de identificar como podrían ser que tu contraseña sea la fecha de tu cumpleaños, tomar en cuenta apartados de datos irreconocibles o al menos que les tome bastante tiempo lograr descifrarlos.



DNS

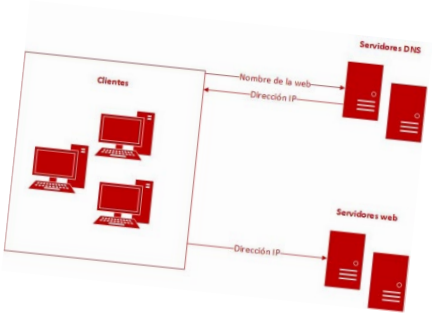
Recomendaciones



-Crear un nombre de dominio fácil de ubicar, es decir es mas fácil recordar “miclinica.com” a “ClinicaGutierrez99.net” con esto logramos que nuestra dirección IP sea mas sencilla de ubicar y así evitamos una suplantación de dominio.

-Contar o hacer que tus clientes sigan tus distintas paginas ya sea Facebook, twiter linkedin o hasta mas personal via chat en whatsapp, ¿Con que fin? Si llegamos a sufrir algun ataque DoS (Denegación de servicio) donde inutilice nuestro sitio web principal y causar confucion con nuestros clientes tener la oportunidad de mantenerlos informados cuando se haya parado el ataque y puedan volver a ingresar a nuestros servidores todo esto de forma “Online” y si hablamos de forma local es decir que algun colaborador no pueda acceder a ningún servicio por lo mismo del ataque y gracias a la copia de seguridad periódica podemos acceder a un modo local con los registros de la copia de seguridad y con la oportunidad de seguir brindando servio aunque en menor medida.

-Dentro de las instalaciones asignar una dirección única que coincida con el metodo de acceso a la red principal , es decir como esta constituida la instalación 21 estaciones de trabajo a la cual a cada una de ellas se les dará un acceso eh identificador para darle “x” derechos de acceso mientras que los de la segunda planta se conectan via Wifi y no están identificados cuantos equipos se quieren conectar, debemos saber el numero exacto de conexiones y equipos para garantizar que no haya equipos infiltrados que puedan acceder a toda la instalación y su informacion.



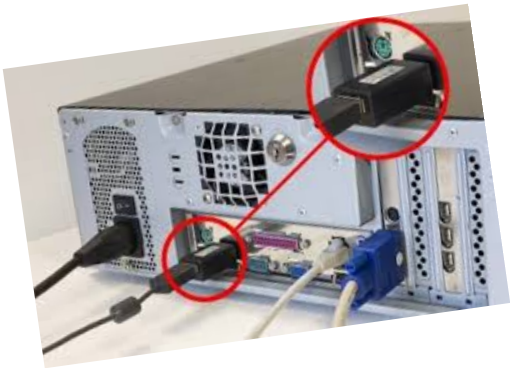
KeyLogger

Recomendaciones

-Poner como regla o bloquear puertos USB de cada estacion de trabajo y dejar unicamente las indispensables para su uso con esto evitamos que se infecte por medio físico que viene siendo la manera mas fácil y tentadora de hacerlo.

-Restringir acceso a internet a cada estacion de trabajo, es decir no permitir el uso “común” de dispositivos que son de uso exclusivo del trabajo y así evitamos que por medio de paginas externas o de dudosa procedencia se descargue algun malware o caballo de troya que comprometa la seguridad y integridad de la informacion.

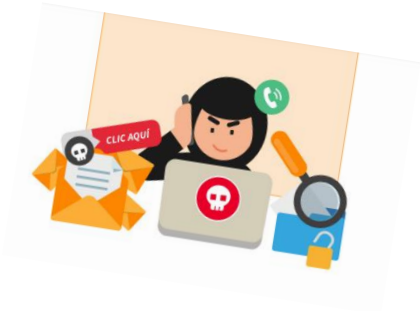
-Siempre usar software oficial, es decir que no este alterado para desbloquear funciones de paga, es mejor contemplarlo en el gasto de la empresa ese pequeño extra de uso de software oficial a usar algun tipo de herramienta que lo desbloquee “gratis” y que este mismo pueda afectar o desplegar malware.



Ingeniería social

Recomendaciones

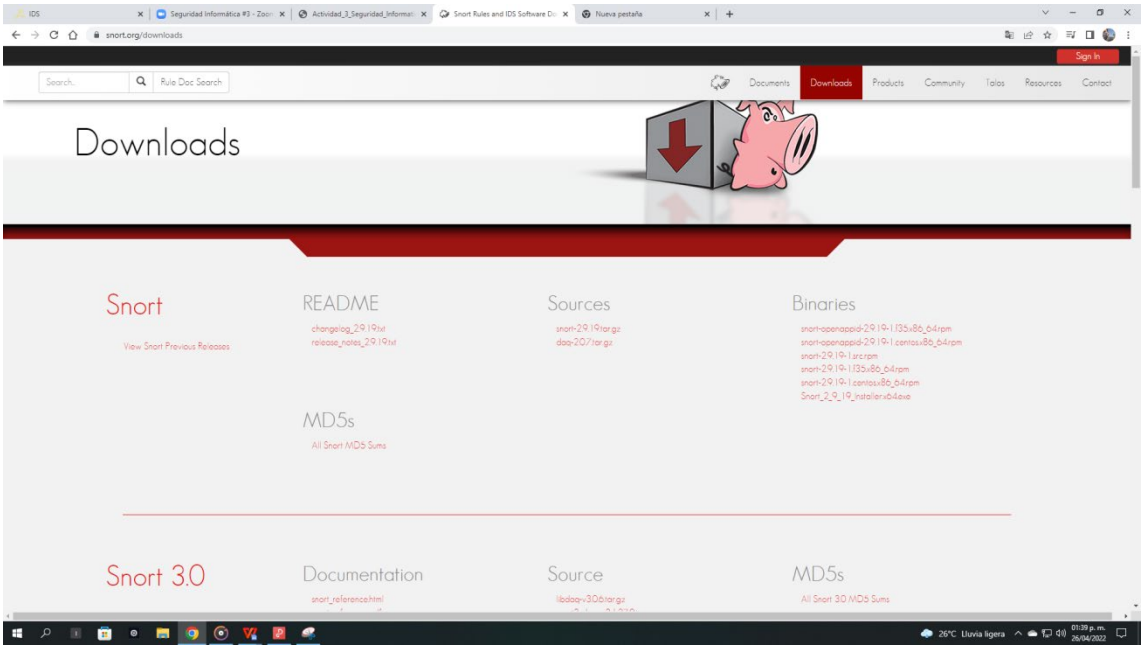
-Colocar letreros de advertencia sobre no insertar o colocar dispositivos externos a las estaciones de trabajo, con esto evitamos caer en algun “anzuelo” de algun hacker que quiera hacer daño a la informacion almacenada y a los equipos.

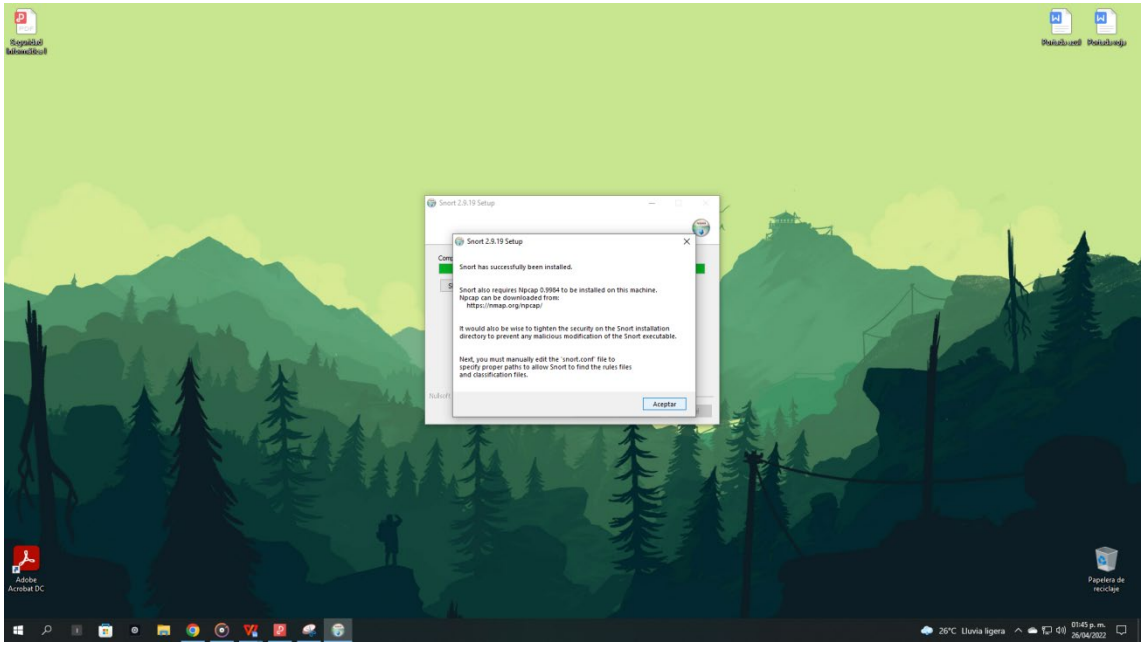


-Platicas de seguridad o prevención de ataques, que van desde las tecnicas mas usadas por los atacantes que son las de Phishing, pretextos y así nos sercioramos que cada uno de nuestros colaboradores están calificados para evitar caer en fraudes.

-Quid pro quo, que se refiere a algun cambio justo, es decir que algun atacante se haga pasar por alguien de “confianza” o técnico externo que viene a hacer mantenimiento prometiendo mejorar el sistema, y así aprovecharse de la vulnerabilidad humana de confiar en alguien.

Selección de software





Plan de acción				
Actividad	***Responsable***	***Estado***	***Duracion***	***Notas***
Capacitacion del personal sobre vulnerabilidades humanas	Fernando alcaraz beltran	Activo	30 Dias	Cuando s econtrate un nuevo colaborador empieza la capacitacion
Capacitacion sobre el manejo de los sistemas utilizados	Andrea zavaleta mendoza	Activo	60 Dias	Cuando s econtrate un nuevo colaborador empieza la capacitacion
Reforzamiento en el sistema para evitar vulnerabilidades (bugs) y retroalimentacion de los colaborades para informar sobre errores y su correccion inmediata	Javier Mendoza Sambrano	Activo	Periodica durante todo el año /mensual	De manera mensual o cada que el sistema lo requiera
Revision en estaciones de trabajo para mantenimiento y bloqueo de puertos y de IP a sitios que no sean para trabajo (redes sociales)	Samuel Salgado Lopez	Activo	Periodica durante todo el año /mensual	De manera mensual o cada que el sistema lo requiera

Plan de acción

Para cerciorarnos de que en verdad los colaboradores no estén en paginas externas y comprometan la seguridad de la empresa, con ello implementamos un identificador IP en cada estacion de trabajo para que se nos notifique cada vez que se trate de burlar la seguridad para poder accesar a paginas externas que puedan comprometer nuestra seguridad.

-Desde el reclutamiento preguntar intenciones o compromiso que pueda dar el futuro colaborador

-Revision de antecedentes o recomendaciones en empresas donde haya colaborado

-Capacitar adecuadamente a los colaboradores sobre el funcionamiento del sistema.

-Mencionar casos que hayan pasado sobre estafas y las consecuencias que conllevo

-Mencionarles cual es la funcion principal de su puesto y su area de responsabilidad (en caso de incidencia)

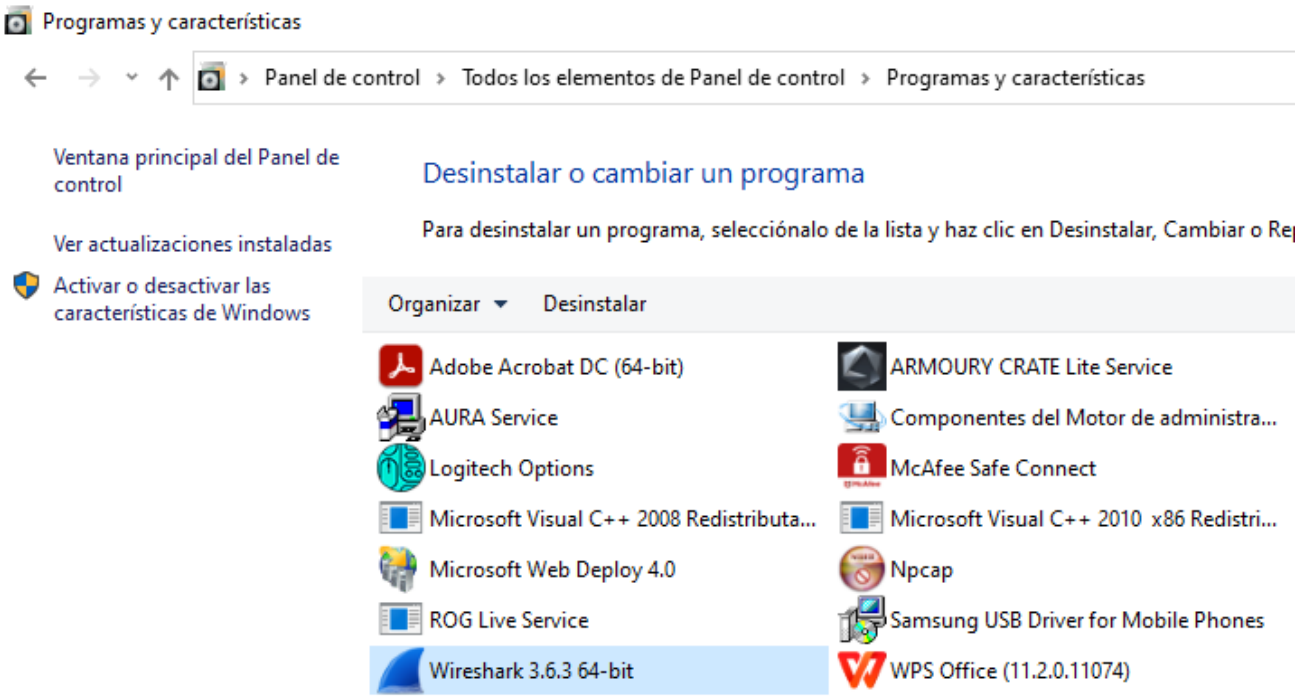
-Mencionar las reglas sobre el uso de las estaciones de trabajo

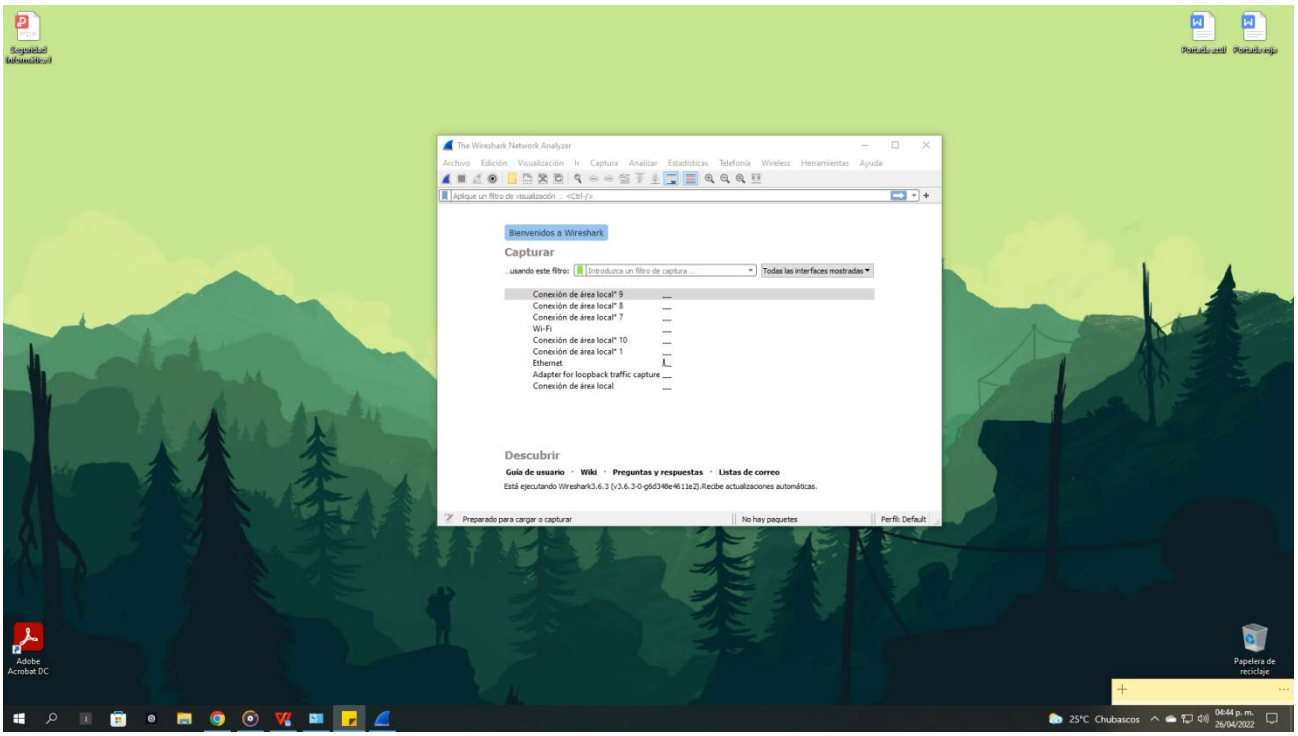
-Fomentar valores que aporten a la empresa para generar un ambiente laboral y confianza "plena"

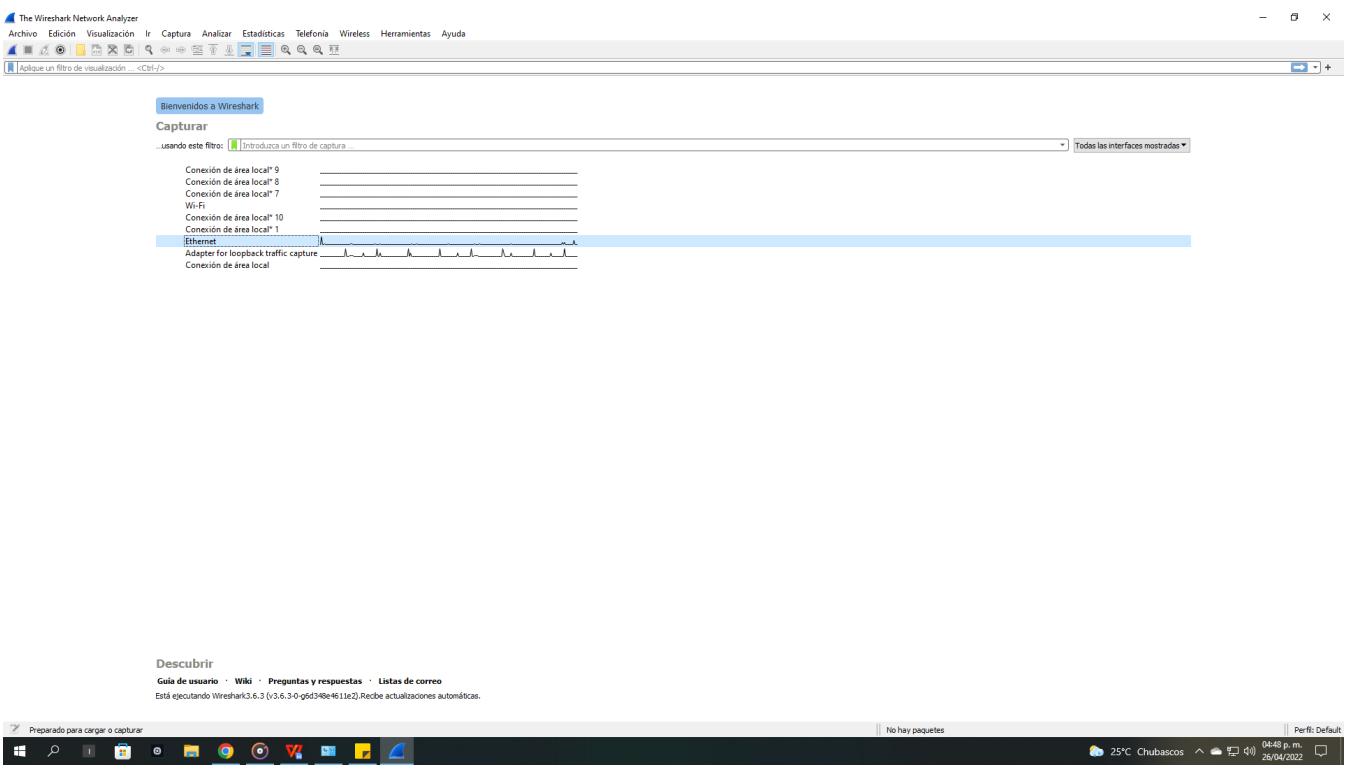
-La prohibición de colocar periféricos externos a las estaciones de trabajo.

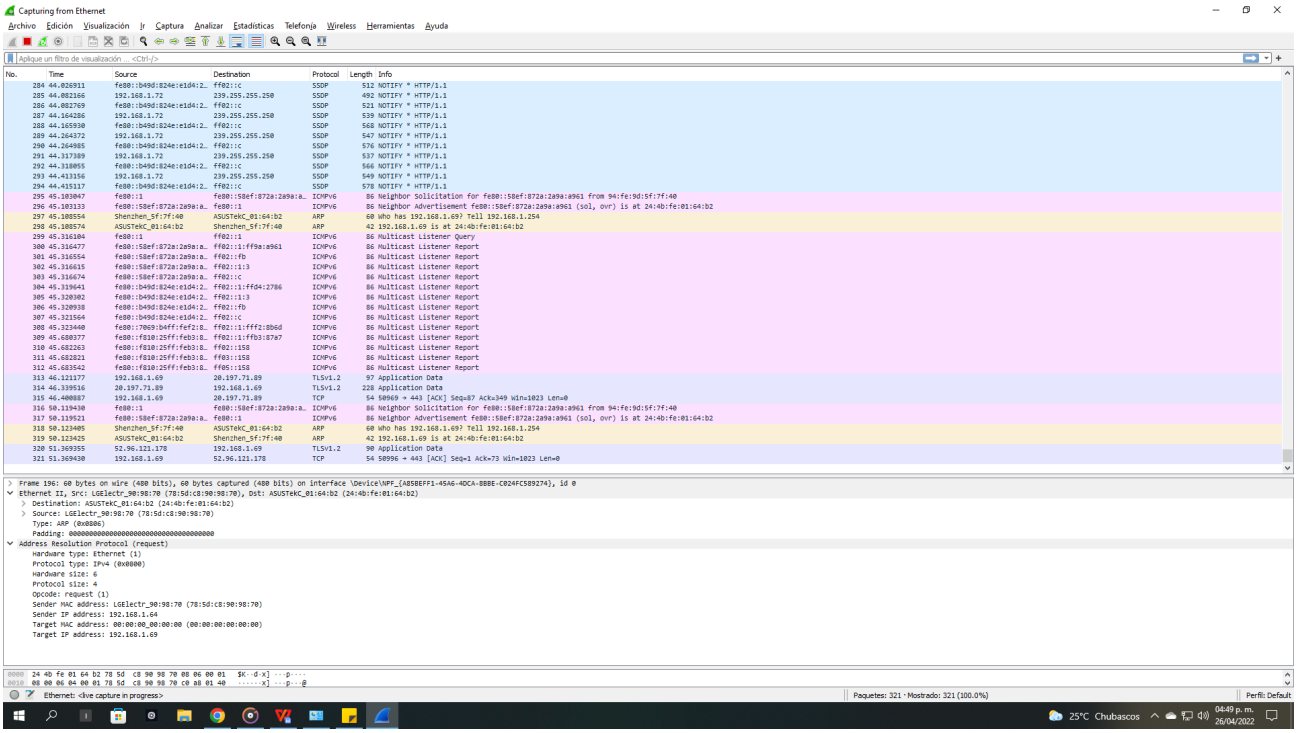
-Que el colaborador no publique nada sobre procesos o que trabaja en "x" empresa para no ser objetivo de terroristas.

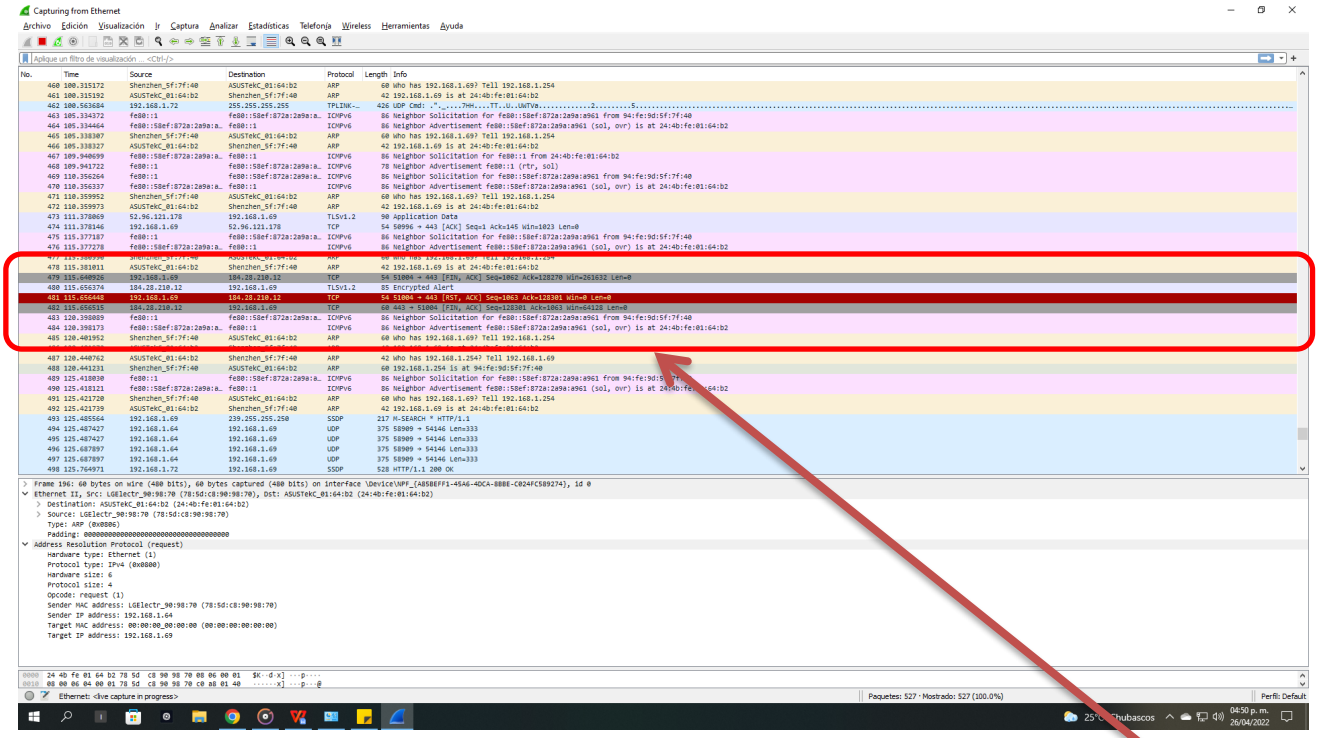
Practica de plan de acción






The Wireshark Network Analyzer
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
Aplique un filtro de visualización ... <Ctrl-/>
Bienvenidos a Wireshark
Capturar
...usando este filtro: Introduzca un filtro de captura ...
Todas las interfaces mostradas
Conexión de área local* 9
Conexión de área local* 8
Conexión de área local* 7
Wi-Fi
Conexión de área local* 10
Conexión de área local* 1
Ethernet
Adapter for loopback traffic capture
Conexión de área local
Descubrir
Guía de usuario · Wiki · Preguntas y respuestas · Listas de correo
Está ejecutando Wireshark3.6.3 (v3.6.3-0-g6d348e4611e2).Recibe actualizaciones automáticas.
Preparado para cargar o capturar
No hay paquetes
Perfil: Default
25°C Chubascos
04:48 p. m.
26/04/2022

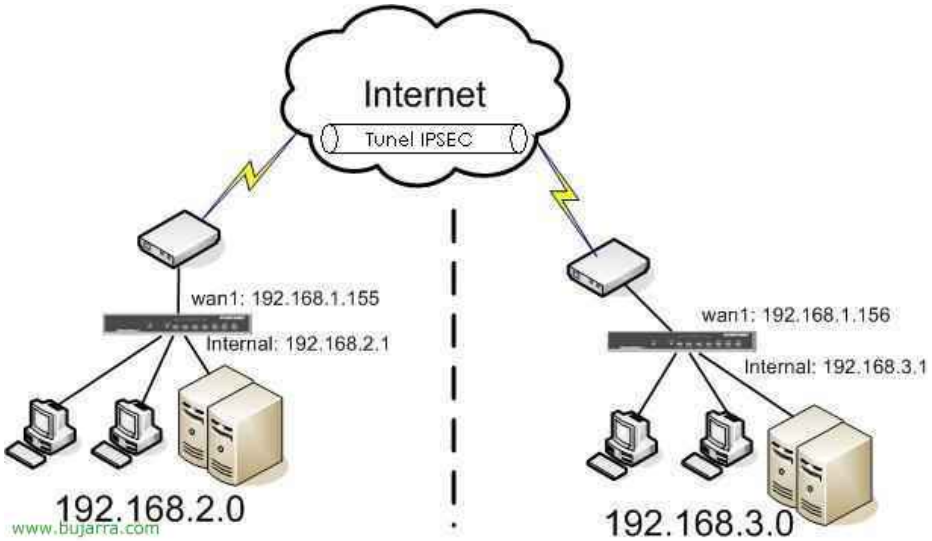

Capturing from Ethernet
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
Aplique un filtro de visualización ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
284 44.026911 fe80::b49d:824e:e1d4:2_ ff02::c SSDP 512 NOTIFY * HTTP/1.1
285 44.082166 192.168.1.72 239.255.255.250 SSDP 492 NOTIFY * HTTP/1.1
286 44.082769 fe80::b49d:824e:e1d4:2_ ff02::c SSDP 521 NOTIFY * HTTP/1.1
287 44.164286 192.168.1.72 239.255.255.250 SSDP 539 NOTIFY * HTTP/1.1
288 44.165930 fe80::b49d:824e:e1d4:2_ ff02::c SSDP 568 NOTIFY * HTTP/1.1
289 44.264372 192.168.1.72 239.255.255.250 SSDP 547 NOTIFY * HTTP/1.1
290 44.264985 fe80::b49d:824e:e1d4:2_ ff02::c SSDP 576 NOTIFY * HTTP/1.1
291 44.317389 192.168.1.72 239.255.255.250 SSDP 537 NOTIFY * HTTP/1.1
292 44.318055 fe80::b49d:824e:e1d4:2_ ff02::c SSDP 566 NOTIFY * HTTP/1.1
293 44.413156 192.168.1.72 239.255.255.250 SSDP 549 NOTIFY * HTTP/1.1
294 44.415117 fe80::b49d:824e:e1d4:2_ ff02::c SSDP 578 NOTIFY * HTTP/1.1
295 45.103047 fe80::1 fe80::58ef:872a:2a9a:a_ ICMPv6 86 Neighbor Solicitation for fe80::58ef:872a:2a9a:a961 from 94:fe:9d:5f:7f:40
296 45.103133 fe80::58ef:872a:2a9a:a_ fe80::1 ICMPv6 86 Neighbor Advertisement fe80::58ef:872a:2a9a:a961 (sol, ovr) is at 24:4b:fe:01:64:b2
297 45.108554 Shenzhen_5f:7f:40 ASUSTekC_01:64:b2 ARP 60 Who has 192.168.1.69? Tell 192.168.1.254
298 45.108574 ASUSTekC_01:64:b2 Shenzhen_5f:7f:40 ARP 42 192.168.1.69 is at 24:4b:fe:01:64:b2
299 45.316104 fe80::1 ff02::1 ICMPv6 86 Multicast Listener Query
300 45.316477 fe80::58ef:872a:2a9a:a_ ff02::1:ff9a:a961 ICMPv6 86 Multicast Listener Report
301 45.316554 fe80::58ef:872a:2a9a:a_ ff02::fb ICMPv6 86 Multicast Listener Report
302 45.316615 fe80::58ef:872a:2a9a:a_ ff02::1:3 ICMPv6 86 Multicast Listener Report
303 45.316674 fe80::58ef:872a:2a9a:a_ ff02::c ICMPv6 86 Multicast Listener Report
304 45.319641 fe80::b49d:824e:e1d4:2_ ff02::1:ff04:2786 ICMPv6 86 Multicast Listener Report
305 45.320302 fe80::b49d:824e:e1d4:2_ ff02::1:3 ICMPv6 86 Multicast Listener Report
306 45.320938 fe80::b49d:824e:e1d4:2_ ff02::fb ICMPv6 86 Multicast Listener Report
307 45.321564 fe80::b49d:824e:e1d4:2_ ff02::c ICMPv6 86 Multicast Listener Report
308 45.323440 fe80::7069:b4ff:fef2:8_ ff02::1:fff2:8b6d ICMPv6 86 Multicast Listener Report
309 45.680377 fe80::f810:25ff:feb3:8_ ff02::1:ffb3:87a7 ICMPv6 86 Multicast Listener Report
310 45.682263 fe80::f810:25ff:feb3:8_ ff02::158 ICMPv6 86 Multicast Listener Report
311 45.682821 fe80::f810:25ff:feb3:8_ ff03::158 ICMPv6 86 Multicast Listener Report
312 45.683542 fe80::f810:25ff:feb3:8_ ff05::158 ICMPv6 86 Multicast Listener Report
313 46.121177 192.168.1.69 20.197.71.89 TLSv1.2 97 Application Data
314 46.339516 20.197.71.89 192.168.1.69 TLSv1.2 228 Application Data
315 46.400887 192.168.1.69 20.197.71.89 TCP 54 50969 → 443 [ACK] Seq=87 Ack=349 Win=1023 Len=0
316 50.119430 fe80::1 fe80::58ef:872a:2a9a:a_ ICMPv6 86 Neighbor Solicitation for fe80::58ef:872a:2a9a:a961 from 94:fe:9d:5f:7f:40
317 50.119521 fe80::58ef:872a:2a9a:a_ fe80::1 ICMPv6 86 Neighbor Advertisement fe80::58ef:872a:2a9a:a961 (sol, ovr) is at 24:4b:fe:01:64:b2
318 50.123405 Shenzhen_5f:7f:40 ASUSTekC_01:64:b2 ARP 60 Who has 192.168.1.69? Tell 192.168.1.254
319 50.123425 ASUSTekC_01:64:b2 Shenzhen_5f:7f:40 ARP 42 192.168.1.69 is at 24:4b:fe:01:64:b2
320 51.369355 52.96.121.178 192.168.1.69 TLSv1.2 90 Application Data
321 51.369430 192.168.1.69 52.96.121.178 TCP 54 50996 → 443 [ACK] Seq=1 Ack=73 Win=1023 Len=0
Frame 196: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{A85BEFF1-45A6-4DCA-BBBE-C024FC589274}, id 0
Ethernet II, Src: LGElectr_90:98:70 (78:5d:c8:90:98:70), Dst: ASUSTekC_01:64:b2 (24:4b:fe:01:64:b2)
Destination: ASUSTekC_01:64:b2 (24:4b:fe:01:64:b2)
Source: LGElectr_90:98:70 (78:5d:c8:90:98:70)
Type: ARP (0x0806)
Padding: 00000000000000000000000000000000
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: LGElectr_90:98:70 (78:5d:c8:90:98:70)
Sender IP address: 192.168.1.64
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.1.69
0000 24 4b fe 01 64 b2 78 5d c8 90 98 70 08 06 00 01 $K··d·x] ···p····
0010 08 00 06 04 00 01 78 5d c8 90 98 70 c0 a8 01 40 ·····x] ···p···@
Ethernet: <live capture in progress>
Paquetes: 321 · Mostrado: 321 (100.0%)
Perfil: Default
25°C Chubascos
04:49 p. m.
26/04/2022



Simulación de como se vería un ataque u acceso no autorizado desde la estacion de trabajo

Evaluación

Motivo: Es una herramienta fácil de usar y se adecua de forma correcta a los intereses de la empresa, adjunto a que puedo generar reglas de que paquetes quiero que si sean almacenados o manejados por la base central sin comprometer la integridad de la misma. Digamos que funciona como intermediario para todas las transacciones que se presentan en todas las estaciones de trabajo, tanto físicas (ethernet) y y Wifi (Whireless) para así bloquear gracias a las reglas propuestas toda acción que no sea exclusiva de la empresa.



¿Que amenazas puedo resolver con esto?

Amenazas lógicas que van desde la suplantación del sitio web hasta la falta de supervision de las estaciones de trabajo, el monitoreo constante ayudaría a dar una idea de las estadísticas de los clientes, es decir si estamos haciendo bien las cosas y aumentando transacciones (Que aumente nuestro numero de clientes) o si estamos haciéndolo mal (Disminuyendo clientes)
y Amenazas humanas el factor que mas llega a afectar ya que por falta de valor a la empresa o descuido humano se comprometa la organización

¿Que vulnerabilidades puedo resolver con esto?

Lograrías gracias a estas medidas de precaución que nos brinda dichas herramientas, el casi inexistente factor humano con esto quiero decir a que los medios de almacenamiento están a salvo ya que se implementaron medias como el bloqueo de los puestos accesibles, el sistema cerrado y con acceso solo por personal capacitado y con estricto control

Bibliografía

Enrique Lopez. (2021). Seguridad Ataques DNS: qué son y cómo protegernos. 2022, de Privada Sitio web: https://www.redeszone.net/tutoriales/seguridad/consejos-evitar-ataques-dns/

Enrique Lopez. (2021). Qué es un Keylogger y cómo protegerse de un Keylogger. 2022, de Privada Sitio web: https://blog.mailfence.com/es/protegerse-de-un-keylogger/

Enrique Lopez. (2020). Maneras de evitar ataques de ingeniería social. 2022, de Privada Sitio web: https://www.kaspersky.es/resource-center/threats/how-to-avoid-social-engineering-attacks

Enrique Lopez. (2020). Sistema de detección de intrusos para Windows (SNORT). 2022, de Privada Sitio web: https://www.youtube.com/watch?v=bQjwSMqCF1g