Webinar Gratuito

Filtros para Captura con Wireshark

Alonso Eduardo Caballero Quezada

Instructor y Consultor Independiente en Ciberseguridad

Sitio Web: www.ReYDeS.com -:- Correo: ReYDeS@gmail.com

Jueves 6 de Junio 2024

Alonso Eduardo Caballero Quezada

ISC2 Certified in Cybersecurity (CC), LPI Security Essentials Certificate, EXIN Ethical Hacking Foundation Certificate, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing, Ransomware Techniques, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS), OPEN-SEC Ethical Hacker (OSEH), Codered Certificate of Achievement: Digital Forensics Essentials (DFE) y Ethical Hacking Essentials (EHE).

Más de 20 años de experiencia como consultor e instructor independiente en las áreas de Hacking Ético, Forense Digital, GNU/Linux, y áreas relacionadas.

Redes Sociales

https://www.linkedin.com/in/alonsocaballeroquezada/

https://twitter.com/Alonso_ReYDeS

https://www.youtube.com/c/AlonsoCaballero

https://www.facebook.com/alonsoreydes/

https://www.instagram.com/alonso_reydes/

reydes@gmail.com

www.reydes.com

+51 949 304 030

@ReYDeS

¿Qué es Wireshark?

Wireshark es un analizador de paquetes de red. Presenta los datos de los paquetes capturados con tanto detalle como sea posible.

Se podría pensar en un analizador de paquetes de red, como un dispositivo de medición para examinar aquello sucediendo dentro de un cable de red, tal como un electricista usa un voltímetro para examinar lo sucediendo dentro de un cable eléctrico (pero a un nivel superior).

Antes estas herramientas eran muy costosas, propietarias, o ambos. Sin embargo con la llegada de Wireshark esto cambió. Wireshark está disponible de forma gratuita, es fuente abierta, y es uno de los mejores analizadores de paquetes disponibles actualmente.

* https://www.wireshark.org

Filtro para Captura

Los filtros para captura (como **tcp port 80**) no deben confundirse con los filtros para visualización (como **tcp.port == 80**). Los primeros son mucho más limitados y son utilizados para reducir el tamaño de una captura de paquetes en bruto. Los últimos son utilizados para ocultar algunos paquetes desde la lista de paquetes.

Los filtros para captura se configuran antes de iniciar una captura de paquetes, y no pueden ser modificados durante la captura. Los filtros para visualización no tienen esta limitación, y pueden ser cambiados al vuelo.

En la ventana principal, se puede encontrar el filtro para captura justo encima de la lista de interfaces y en el cuadro de diálogo de interfaces.

* https://wiki.wireshark.org/CaptureFilters

BPF

Es un filtro de paquetes y derivación de red, el cual permite capturar y filtrar paquetes a nivel del sistema operativo. Proporciona una interfaz en bruto para las capas de enlace de datos, lo cual permite enviar y recibir paquetes sin procesar desde la capa de enlace, además permite un proceso de espacio de usuario proporcione un programa de filtro especificando cuales paquetes desea recibir.

Por ejemplo, es posible que un proceso wireshark requiera recibir solo paquetes iniciando una conexión TCP. BPF devuelve únicamente paquetes pasando el filtro el cual proporciona el proceso. Esto evita copiar paquetes no deseados del kernel del sistema operativo hacia el proceso, lo cual mejora enormemente el rendimiento. El programa de filtrado tiene la forma de instrucciones para una máquina virtual, los cuales se interpretan o se compilan en código de máquina mediante un mecanismo justo a tiempo (JIT) y se ejecutan en el kernel.

BPF (Cont.)

BPF es utilizado por programas necesitando analizar tráfico de red. Si el controlador de interfaz de red admite el modo promiscuo, se pueden recibir todos los paquetes desde la red, incluso aquellos destinados hacia otros hosts.

El mecanismo de filtrado BPF está disponible en la mayoría de los sistemas operativos tipo Unix. Algunas veces BPF se utiliza para referirse solo al mecanismo de filtrado, en lugar de toda la interfaz. Algunos sistemas, como Linux y Tru64 UNIX, proporcionan una interfaz sin formato para la capa de enlace de datos diferente de la interfaz en bruto BPF, pero utilizan los mecanismos de filtrado BPF para esa interfaz en bruto.

El kernel de Linux proporciona una versión extendida del mecanismo de filtrado BPF, llamado eBPF, el cual utiliza un mecanismo JIT y que se utiliza para el filtrado de paquetes, así como para otros fines en el kernel.

Curso Forense de Redes

Curso Virtual Forense de Redes 2024

Domingos 9, 16, 23 y 30 de Junio 2024. De 9:00 am a 12:00 pm (UTC -05:00)

Presentación

En la actualidad es muy común trabajar en cualquier investigación forense relacionada a un componente de red. El forense de computadoras siempre será un habilidad fundamental y crítica para esta profesión, pues obviar las comunicaciones de red, es similar a ignorar las imágenes proporcionadas por las cámaras de seguridad correspondientes a un crimen cometido. Ya sea se enfrente un incidente relacionado con una intrusión, un caso de robo de datos, uso indebido por parte de los empleados, o se esté involucrado en el descubrimiento pro activo del adversario, la red frecuentemente proporciona una vista incomparable del incidente. Esta evidencia puede proporcionar la prueba necesaria para mostrar intención, descubrir los atacantes han estado activos por meses o más, o incluso puede resultar útil para probar definitivamente la ocurrencia de un delito.

Objetivos

Este curso enseña a construir los conocimientos fundamentales necesarios para realizar investigaciones eficientes y efectivas. Enfocándose en aquello necesario para expandir la mentalidad del forense digital, desde los datos residuales contenidos en los medios de almacenamiento de un sistema o dispositivo, hasta las comunicaciones transitorias las cuales ocurrieron anteriormente o continúen ocurriendo. Incluso si un atacante remoto muy hábil compromete un sistema con un exploit no detectable, el sistema debe comunicarse a través de la red. Sin los canales de comando y control para la extracción de datos, el valor de un sistema comprometido se reduce casi a cero. Expresado de otra manera; mientras los atacantes se comunican a través de la red, este curso enseña como escucharlos y analizarlos de diversas maneras.

Fechas & Horarios

Duración: Catorce (14) horas. Una (1) sesión previamente grabada de dos (2) horas, y cuatro (4) sesiones en vivo de tres (3) horas de duración cada una.

Fechas:

Domingos 9, 16, 23 y 30 de Junio 2024

Horario:

De 9:00 am a 12:00 pm (UTC -05:00)

Alonso Eduardo Caballero Quezada.

ISC2 Certified in Cybersecurity (CC), LPI Security Essentials Certificate, EXIN Ethical Hacking Foundation Certificate, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing, Ransomware Techniques, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS), OPEN-SEC Ethical Hacker (OSEH), y Codered Certificate of Achievement: Digital Forensics Essentials (DFE) y Ethical Hacking Essentials (EHE). He sido instructor, expositor y conferencista en el OWASP LATAM Tour, OWASP Perú Chapter Meeting, OWASP LATAM at Home, PERUHACK, PERUHACKNOT, 8.8 Lucky Perú, Ekoparty University Talks Perú. Cuento con más de veinte años de experiencia en el área, y desde hace dieciséis años laboro como consultor e instructor en Hacking Ético & Forense Digital. Pertenecí por muchos años al grupo internacional RareGaZz y grupo Peruano PeruSEC. He dictado cursos para España, Ecuador, México, Bolivia y PerúMi correo electrónico es ReYDeS@gmail.com y mi página personal está en: www.ReYDeS.com

Más Información

Para obtener más información sobre este curso, tiene a su disposición los siguientes mecanismos de contacto.

Correo electrónico:

reydes@gmail.com

Teléfono: +51 949 304 030

Sitio Web: www.reydes.com

Temario

- Introducción al Forense de Redes
- Brechas de Datos
- Diferencias entre Forense de Computadoras y Redes
- Profundizar Conocimientos Técnicos
- Entender la Seguridad de Red
- Objetivos de la Seguridad de Red
- Consideraciones sobre Manipulación de Evidencia
- Identificar Fuentes de Evidencia
- Conocer el Manejo de Evidencia
- Recolección del Trafico de la Red
- Recolección de Logs de la Red
- Captura de Memoria
- Capturar y Analizar Paquetes de Datos
- Interceptar el Tráfico de la Red
- Sniffing y Análisis de Paquetes
- Evidencia en Redes Inalámbricas
- Entender la Protección y Seguridad Inalámbrica
- Ataques Comunes a Redes Inalámbricas
- Analizar y Capturar Tráfico Inalámbrico
- Rastrear un Intruso en la Red
- Entender los Sistemas de Detección y Prevención de Intrusos.
- Diferencias entre IDS e IPS
- El Registro de Sucesos
- Entender los Formatos de los archivos de Registro de eventos (Logs)
- Descubrir la Conexión entre los Logs y el Forense
- Proxys, Firewall y Routers
- Analizar un Proxy
- Investigar un Firewall
- Conocer un Router
- Saltándose Protocolos Prohibidos
- Entender los VPNs
- Funcionamiento de "Tunneling"
- Tipos de Protocolos para "Tunneling"
- Investigar Malware
- Conocer el Malware
- Tipos de Malware y su Impacto
- Entender el Comportamiento de un Malware
- Realizar un Forense a Malware
- Cerrando o Resolviendo el Caso
- Revisar la Adquisición y Análisis de la Evidencia
- Reportar el Caso

Material

- SIFT Workstation
- Herramientas Windows

Inversión y Forma de Pago

- Acceso a las sesiones en vivo
- Acceso al aula virtual por 45 días
- Video de las cinco (5) sesiones
- Material utilizado durante el desarrollo del curso
- Asesoría personalizada
- Libro "Fundamentos de Forense Digital" escrito por el instructor
- Certificado digital de participación
- Certificado digital de aprobación (CMFR). Puntuación mínima 70/100). Por una duración total de 24 horas

S/. 450 Soles o $ 140 Dólares

El pago del curso se realiza:

Residentes en Perú

Depósito bancario Scotiabank

Cuenta de Ahorros en Soles: 324-0003164
A nombre de: Alonso Eduardo Caballero Quezada

O también pagos con Yape o Plin. Escriba un mensaje de correo electrónico a reydes@gmail.com para proporcionarle los datos pertinentes.

Residentes en otros países

Pago a través de Paypal PayPal

O también transferencia de dinero mediante Western Union y MoneyGram

Escriba por favor un mensaje de correo electrónico a reydes@gmail.com para proporcionarle los datos.

Confirmado el pago se enviará los datos para conectarse hacia la plataforma

Certificados

Certificados; constancias de participación y aprobación; expedidos a nombre de la empresa Peruana MILESEC EIRL.

Sitio Web:

www.reydes.com

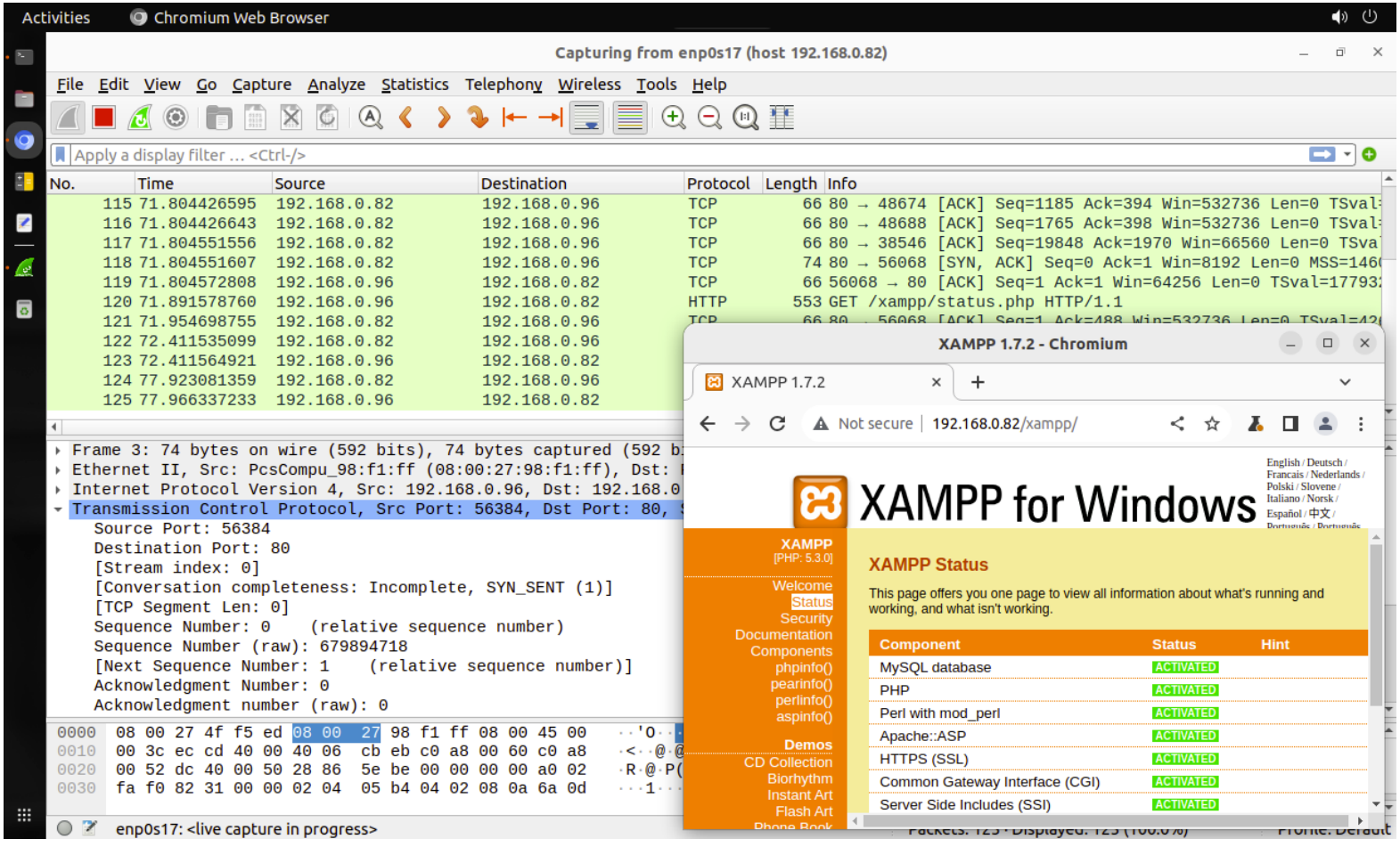
Correo:

reydes@gmail.com

Más Información:

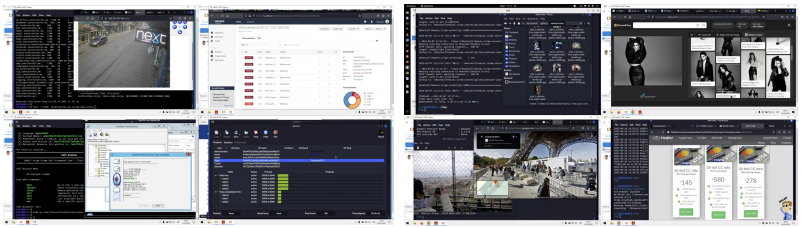
https://www.reydes.com/d/?q=Curso_Forense_de_Redes

Prácticas

- 
Activities
Chromium Web Browser
Capturing from enp0s17 (host 192.168.0.82)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
115 71.804426595 192.168.0.82 192.168.0.96 TCP 66 80 → 48674 [ACK] Seq=1185 Ack=394 Win=532736 Len=0 TSval
116 71.804426643 192.168.0.82 192.168.0.96 TCP 66 80 → 48688 [ACK] Seq=1765 Ack=398 Win=532736 Len=0 TSval
117 71.804551556 192.168.0.82 192.168.0.96 TCP 66 80 → 38546 [ACK] Seq=19848 Ack=1970 Win=66560 Len=0 TSva
118 71.804551607 192.168.0.82 192.168.0.96 TCP 74 80 → 56068 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=146
119 71.804572808 192.168.0.96 192.168.0.82 TCP 66 56068 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=17793
120 71.891578760 192.168.0.96 192.168.0.82 HTTP 553 GET /xampp/status.php HTTP/1.1
121 71.954698755 192.168.0.82 192.168.0.96 TCP 66 80 → 56068 [ACK] Seq=1 Ack=488 Win=532736 Len=0 TSval=42
122 72.411535099 192.168.0.82 192.168.0.96
123 72.411564921 192.168.0.96 192.168.0.82
124 77.923081359 192.168.0.82 192.168.0.96
125 77.966337233 192.168.0.96 192.168.0.82
Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 b
Ethernet II, Src: PcsCompu_98:f1:ff (08:00:27:98:f1:ff), Dst:
Internet Protocol Version 4, Src: 192.168.0.96, Dst: 192.168.0
Transmission Control Protocol, Src Port: 56384, Dst Port: 80,
Source Port: 56384
Destination Port: 80
[Stream index: 0]
[Conversation completeness: Incomplete, SYN_SENT (1)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 679894718
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
0000 08 00 27 4f f5 ed 08 00 27 98 f1 ff 08 00 45 00
0010 00 3c ec cd 40 00 40 06 cb eb c0 a8 00 60 c0 a8
0020 00 52 dc 40 00 50 28 86 5e be 00 00 00 00 a0 02
0030 fa f0 82 31 00 00 02 04 05 b4 04 02 08 0a 6a 0d
enp0s17: <live capture in progress>
XAMPP 1.7.2 - Chromium
XAMPP 1.7.2
Not secure 192.168.0.82/xampp/
XAMPP for Windows
English / Deutsch / Francais / Nederlands / Polski / Slovene / Italiano / Norsk / Español / 中文 /
XAMPP [PHP: 5.3.0]
Welcome
Status
Security
Documentation
Components
phpinfo()
pearinfo()
perlinfo()
aspinfo()
Demos
CD Collection
Biorhythm
Instant Art
Flash Art
XAMPP Status
This page offers you one page to view all information about what's running and working, and what isn't working.
Component Status Hint
MySQL database ACTIVATED
PHP ACTIVATED
Perl with mod_perl ACTIVATED
Apache::ASP ACTIVATED
HTTPS (SSL) ACTIVATED
Common Gateway Interface (CGI) ACTIVATED
Server Side Includes (SSI) ACTIVATED

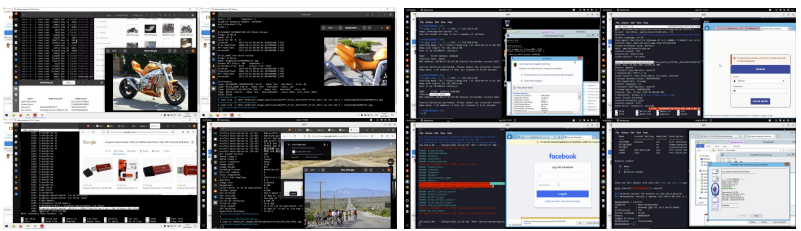
Cursos Disponibles en Video

Curso Hacking Ético
https://www.reydes.com/d/?q=Curso_de_Hacking_Etico



Curso Hacking Aplicaciones Web
https://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

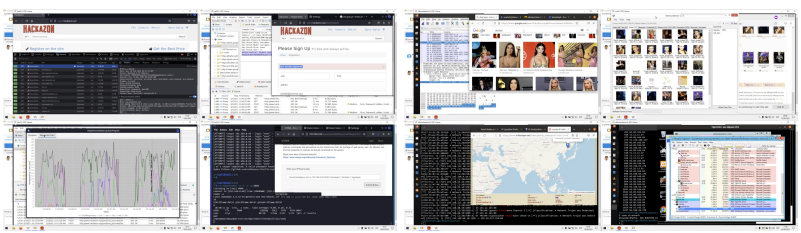
Curso Informática Forense
https://www.reydes.com/d/?q=Curso_de_Informatica_Forense



Curso Hacking con Kali Linux
https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

Curso OSINT - Open Source Intelligence
https://www.reydes.com/d/?q=Curso_de_OSINT

Curso Forense de Redes
https://www.reydes.com/d/?q=Curso_Forense_de_Redes



Y todos los cursos virtuales:

https://www.reydes.com/d/?q=cursos

Más Contenidos

Videos de webinars

https://www.reydes.com/d/?q=videos

Diapositivas de webinars

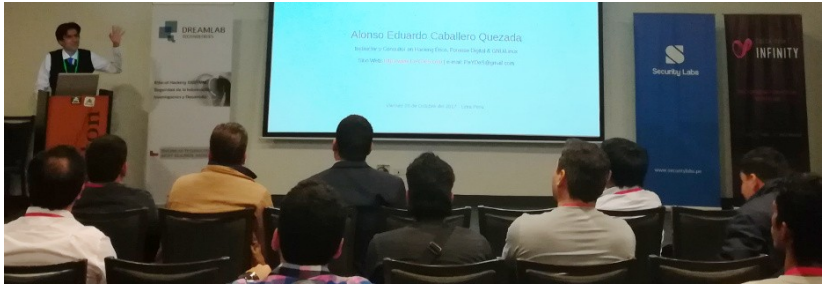
https://www.reydes.com/d/?q=eventos

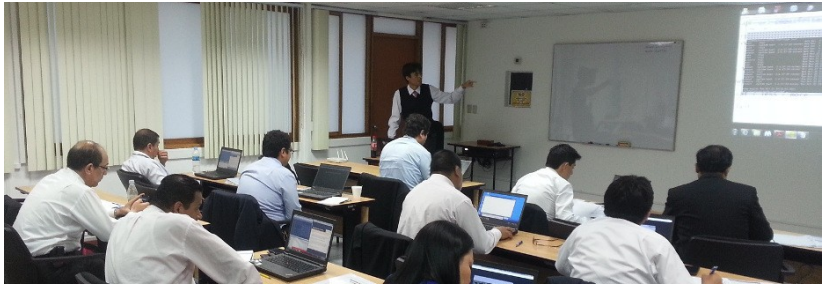
Libros y artículos

https://www.reydes.com/d/?q=documentos

Blog

https://www.reydes.com/d/?q=blog/1





Webinar Gratuito

Filtros para Captura con Wireshark

Alonso Eduardo Caballero Quezada

Instructor y Consultor Independiente en Ciberseguridad

Sitio Web: www.ReYDeS.com -:- Correo: ReYDeS@gmail.com

Jueves 6 de Junio 2024