Webinar Gratuito

Sysinternals

Alonso Eduardo Caballero Quezada

Instructor y Consultor Independiente en Ciberseguridad

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

Jueves 21 de Marzo 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

Sobre Sysinternals

Son utilidades libres, administrativas avanzadas, de diagnóstico y solución de problemas, para Microsoft Windows. Estas utilidades están disponibles para su descarga desde el sitio web de Microsoft. Entre sus características distintivas:

- Cumple las necesidades de una importante audiencia de desarrolladores o profesionales en TI
- Es intuitivo y fácil de utilizar
- Está empaquetado como una única imagen ejecutable, la cual no requiere instalación, siendo posible su ejecución desde cualquier lugar, incluso desde una ubicación de red o un medio extraíble
- No deja ningún dato incidental significativo después de su ejecución

Resumen de las Utilidades

Las utilidades de Sysinternals abarcan un amplio rango de funcionalidades sobre muchos aspectos de Windows.

Si bien algunas de las utilidades más completas, como Process Explorer y Process Monitor, abarcan varias categorías de operaciones, otras pueden agruparse más o menos dentro de una sola categoría, como "utilidades de proceso" o "utilidades de archivo".

Muchas de las utilidades tienen una interfaz gráfica de usuario (GUI), mientras otras son utilidades en consola con interfaces en línea de comandos, diseñadas para la automatización.

* Sysinternals: https://learn.microsoft.com/en-us/sysinternals/

Categorías:

- Utilidades para Archivos y Discos
- Utilidades para redes
- Utilidades para Procesos
- Utilidades para Seguridad
- Información del Sistema
- Misceláneos

https://learn.microsoft.com/en-us/training/modules/explore-support-diagnostic-tools/

Sysinternals Live

Sysinternals Live es un servicio el cual permite ejecutar las herramientas directamente desde la Web, sin descargarlas manualmente.

Únicamente se debe ingresar hacia la ruta de Sysinternals Live desde el explorador de Windows

live.sysinternals.com/<nombreherrramienta>
\\live.sysinternals.com\tools\<nombreherramienta>

También es factible visualizar el directorio completo de herramientas de Sysinternals Live en un navegador o en el Explorador de Windows.

* live.sysinternals.com: https://live.sysinternals.com/

Curso Análisis de Malware

Curso Análisis de Malware 2024

Sábados 23 y 30 de Marzo del 2024. De 9:00 am a 12:00 pm (UTC -05:00)

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:

Presentación

El avance de la tecnología e Internet ha revolucionado la forma en la cual las organizaciones realizan sus negocios. Esta evolución consecuentemente genera también actividades maliciosas. La creciente amenaza de los ciberataques contra infraestructuras críticas, centros de datos, sector privado y público, defensa, energía, gobierno y finanzas, son un reto para todos los involucrados, desde una persona hasta las grandes empresas. Estos ciberataques utilizan software malicioso (también conocido como Malware) para realizar robo financiero, espionaje, sabotaje, robo de propiedad intelectual, o por motivos políticos.

Dado el hecho los ciberdelincuentes son cada vez más sofisticados y realizan ataques de malware avanzados, detectar y responder a estas intrusiones es fundamental para los profesionales en ciberseguridad. El análisis de malware se ha convertido en una habilidad imprescindible para enfrentar el malware avanzado y los ataques dirigidos. El análisis de malware requiere un conocimiento equilibrado de muchas habilidades y temas diferentes.

Este curso proporciona los conceptos, herramientas y técnicas para comprender el comportamiento y las características de malware para Windows, realizando análisis de malware. Para comprender mejor los conceptos, se utilizan ejemplos y demostraciones prácticas durante todo el curso. Además se proporciona suficiente información para comprender los conceptos necesarios. Este curso ayuda a iniciarse en el ámbito del análisis de Malware, o si tiene experiencia en este campo, ayudará a mejorar conocimientos.

Temario

- ¿Qué es Malware?
- ¿Qué es el Análisis de Malware?
- ¿Porque Análisis de Malware?
- Tipos de Análisis de Malware
- Fuentes de Malware
- Análisis Estático
- Determinar el Tipo de Archivo
- Identificar Tipo de Archivos con Métodos Manuales
- Huella del Malware
- Generar Hashes Criptográficos
- Escaneo con Múltiples Antivirus
- Escanear el Archivo Binario Sospechoso
- Extraer Cadenas
- Determinar Ofuscación del Archivo
- Packers
- Cryptos
- Inspeccionar la Información de la Cabecera PE
- Comparar Malware
- Clasificar Malware

- Análisis Dinámico
- Vigilancia del Sistema
- Vigilancia de la Red
- Herramientas para el Análisis Dinámico
- Determinar la Interacción con el Sistemas
- Registrar Actividades en el Sistemas
- Capturar Tráficos de Red
- Etapas para un Análisis Dinámico
- Analizar un Malware Ejecutable
- Análisis de las DLLs

Fechas y Horario

El Curso Virtual de Análisis de Malware tiene una duración total de seis (6) horas, las cuales se dividen en dos (2) sesiones de tres (3) horas cada una.

- **Fechas:**

  Sábados 23 y 30 de Marzo del 2024

- **Horario:**

  De 9:00 am a 12:00 pm (UTC -05:00). 6 horas en total.

[*] El Curso se dicta sin ningún requisito mínimo en el número de participantes.

Beneficios e Inversión

- Acceso a las sesiones en vivo
- Acceso al aula virtual por 45 días
- Video de las dos (2) 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. Puntuación mínima 70/100. Por una duración total de 16 horas

S/. 225 Soles o $ 70 Dólares

El pago del curso se realiza mediante alguno de los siguientes mecanismos:

Residentes en Perú	Residentes en Otros Países
Deposito bancario o transferencia interbancaria en la siguiente cuenta: Scotiabank ScotiaBank	Pago a través de PayPal. O también transferencia de dinero mediante Western Union y MoneyGram PayPal
Cuenta de Ahorros en Soles: 324-0003164 A nombre de: Alonso Eduardo Caballero Quezada CCI: 009-324-203240003164-58	Escriba por favor un mensaje de correo electrónico a reydes@gmail.com para proporcionarle los datos pertinente para realizar el pago.

Confirmado el pago se enviará al correo electrónico del participante, los datos necesarios para conectarse hacia la plataforma, además de toda la información pertinente para su participación en el curso.

Más Información

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

Correo electrónico: caballero.alonso@gmail.com

Teléfono: +51 949 304 030

Sitio Web: https://www.reydes.com

Instructor

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 Technicques, 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). 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, Eksparty University Talks Perú. Cuento con más de dieciocho años de experiencia en el área y desde hace catorce años laboro como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. Pertenezo por muchos años al grupo internacional RareGaZz y grupo Peruano PeruSEC. He dictado cursos para España, Ecuador, México, Bolivia y Perú, presentándome también en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux y Software Libre. Mi correo electrónico es RerTeG@gmail.com y mi página personal está en: https://www.ReYDes.com

Sitio Web:

www.reydes.com

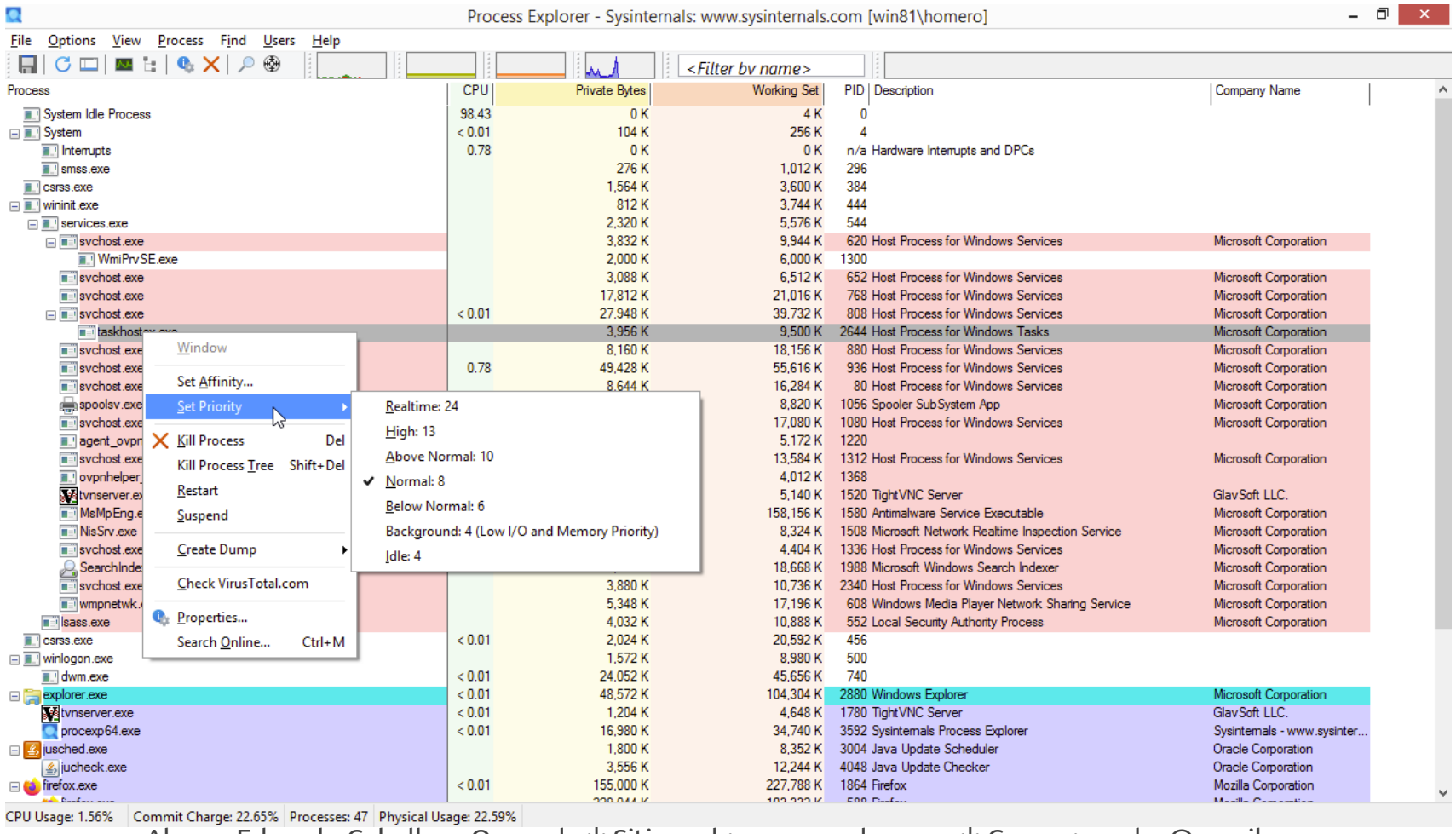
Correo:

reydes@gmail.com

Más Información:

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

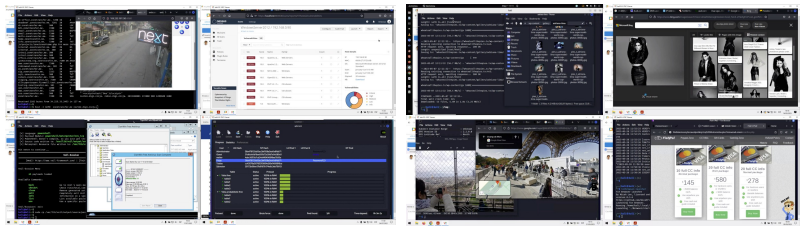
Prácticas


Process Explorer - Sysinternals: www.sysinternals.com [win81\homero]
File Options View Process Find Users Help
<Filter by name>
Process CPU Private Bytes Working Set PID Description Company Name
System Idle Process 98.43 0 K 4 K 0
System < 0.01 104 K 256 K 4
Interrupts 0.78 0 K 0 K n/a Hardware Interrupts and DPCs
smss.exe 276 K 1,012 K 296
csrss.exe 1,564 K 3,600 K 384
wininit.exe 812 K 3,744 K 444
services.exe 2,320 K 5,576 K 544
svchost.exe 3,832 K 9,944 K 620 Host Process for Windows Services Microsoft Corporation
WmiPrvSE.exe 2,000 K 6,000 K 1300
svchost.exe 3,088 K 6,512 K 652 Host Process for Windows Services Microsoft Corporation
svchost.exe 17,812 K 21,016 K 768 Host Process for Windows Services Microsoft Corporation
svchost.exe < 0.01 27,948 K 39,732 K 808 Host Process for Windows Services Microsoft Corporation
taskhostex.exe 3,956 K 9,500 K 2644 Host Process for Windows Tasks Microsoft Corporation
svchost.exe 8,160 K 18,156 K 880 Host Process for Windows Services Microsoft Corporation
svchost.exe 0.78 49,428 K 55,616 K 936 Host Process for Windows Services Microsoft Corporation
svchost.exe 8,644 K 16,284 K 80 Host Process for Windows Services Microsoft Corporation
spoolsv.exe 8,820 K 1056 Spooler SubSystem App Microsoft Corporation
svchost.exe 17,080 K 1080 Host Process for Windows Services Microsoft Corporation
agent_ovpn 5,172 K 1220
svchost.exe 13,584 K 1312 Host Process for Windows Services Microsoft Corporation
ovpnhelper 4,012 K 1368
tvnserver.ex 5,140 K 1520 TightVNC Server GlavSoft LLC.
MsMpEng.e 158,156 K 1580 Antimalware Service Executable Microsoft Corporation
NisSrv.exe 8,324 K 1508 Microsoft Network Realtime Inspection Service Microsoft Corporation
svchost.exe 4,404 K 1336 Host Process for Windows Services Microsoft Corporation
SearchInde 18,668 K 1988 Microsoft Windows Search Indexer Microsoft Corporation
svchost.exe 3,880 K 10,736 K 2340 Host Process for Windows Services Microsoft Corporation
wmpnetwk. 5,348 K 17,196 K 608 Windows Media Player Network Sharing Service Microsoft Corporation
lsass.exe 4,032 K 10,888 K 552 Local Security Authority Process Microsoft Corporation
csrss.exe < 0.01 2,024 K 20,592 K 456
winlogon.exe 1,572 K 8,980 K 500
dwm.exe < 0.01 24,052 K 45,656 K 740
explorer.exe < 0.01 48,572 K 104,304 K 2880 Windows Explorer Microsoft Corporation
tvnserver.exe < 0.01 1,204 K 4,648 K 1780 TightVNC Server GlavSoft LLC.
procexp64.exe < 0.01 16,980 K 34,740 K 3592 Sysinternals Process Explorer Sysinternals - www.sysinter...
jusched.exe 1,800 K 8,352 K 3004 Java Update Scheduler Oracle Corporation
jucheck.exe 3,556 K 12,244 K 4048 Java Update Checker Oracle Corporation
firefox.exe < 0.01 155,000 K 227,788 K 1864 Firefox Mozilla Corporation
Window
Set Affinity...
Set Priority
Kill Process Del
Kill Process Tree Shift+Del
Restart
Suspend
Create Dump
Check VirusTotal.com
Properties...
Search Online... Ctrl+M
Realtime: 24
High: 13
Above Normal: 10
Normal: 8
Below Normal: 6
Background: 4 (Low I/O and Memory Priority)
Idle: 4
CPU Usage: 1.56% Commit Charge: 22.65% Processes: 47 Physical Usage: 22.59%

Cursos Disponibles en Video

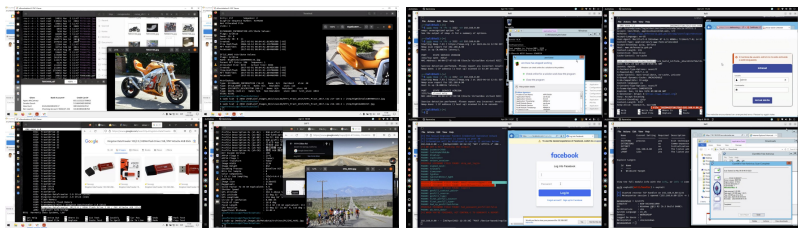
Curso Hacking Ético
https://www.reydes.com/d/?q=Curso_de_Hacking_Etico

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



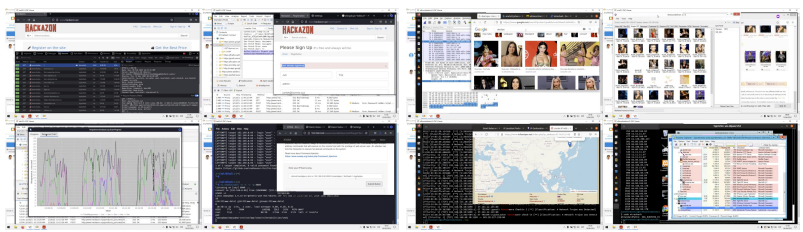
Curso Informática Forense
https://www.reydes.com/d/?q=Curso_de_Informatica_Forense

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

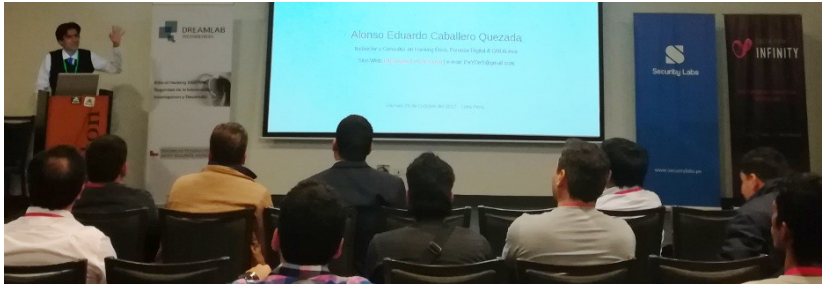
https://www.reydes.com/d/?q=eventos

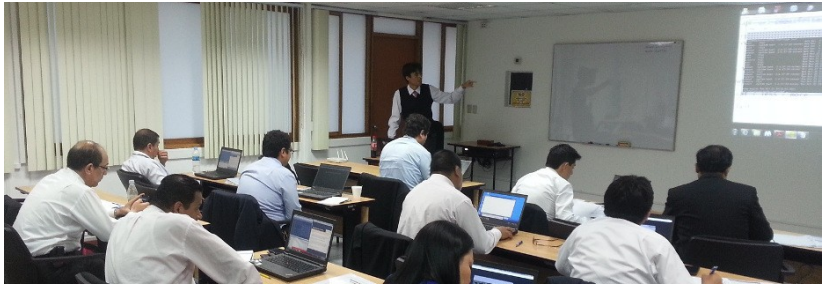
Libros y artículos

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

Blog

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





Webinar Gratuito

Sysinternals

Alonso Eduardo Caballero Quezada

Instructor y Consultor Independiente en Ciberseguridad

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

Jueves 21 de Marzo 2024