El orden de los bits sí altera el producto:

Talón de Aquiles de los Antivirus

VIII Jornada Nacional de Seguridad Informática

Bogotá – Colombia

: : 2008 : :

Luis Fernando González V.
CEH
iQ Outsourcing S.A
lfgonzalez@iq-online.com

....iQ: :

…. Objetivos

- Mostrar la debilidad de los antivirus, en base a la ejecución y resultados de una prueba de vulnerabilidad realizada a 27 de estos software.
- Evidenciar la necesidad de incluir en las evaluaciones y análisis de seguridad la plataforma antivirus.
- Demostrar la relevancia de las labores del hacker ético dentro de la organización (relación costo-beneficio).

…. Prueba de Vulnerabilidad

Surgió de la necesidad de evaluar el nivel de protección ofrecido por el software antivirus adquirido por la compañía.

Patrones Heurísticos

Técnicas que se emplean para reconocer códigos maliciosos (virus, gusanos, troyanos, etc.) que no se encuentren en la base de datos del antivirus (ya sea porque son nuevos, o por no ser muy divulgados).

- Rec. Código compilado
- Desensamblado
- Firmas Genéricas
- Desempaquetamiento

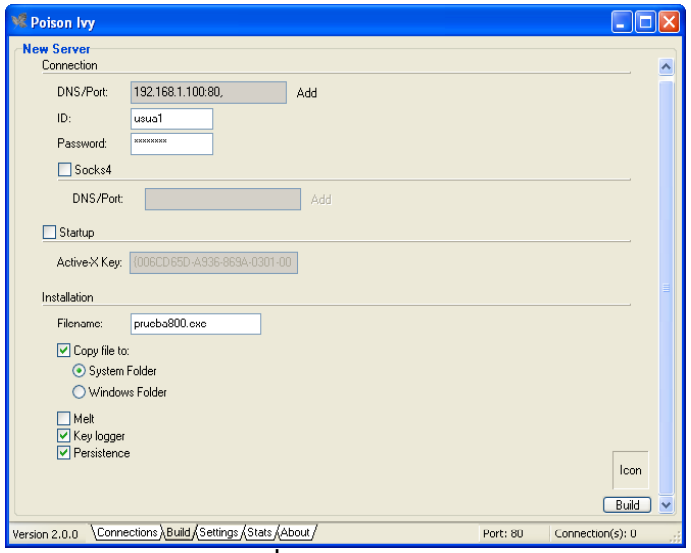
Diapositiva 3

71 Viejo.

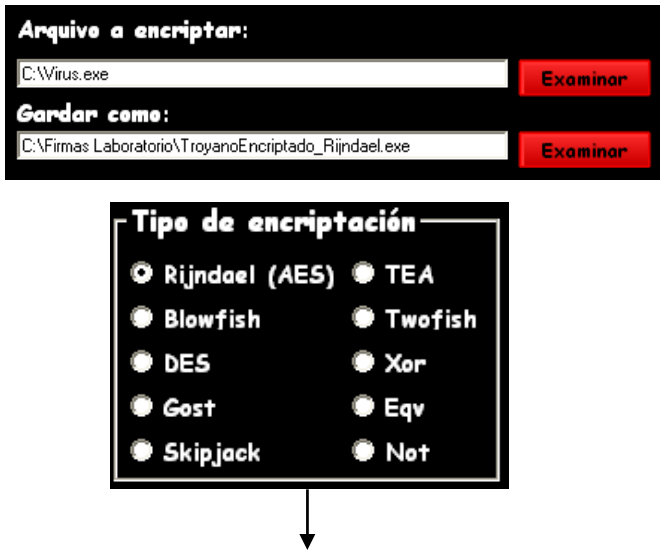
Mi consejo. Utiliza más imagenes que texto. Esto es lo que tu sabes. el hecho de poner tantas letras hace que el público se distraiga.
7141546, 05/06/2008

…. Herramientas

Herramienta Poison Ivy, orientada a prestar un servicio cliente servidor, su principal función es tomar el control total de la máquina victima.



Archivo Ejecutable de 8KB



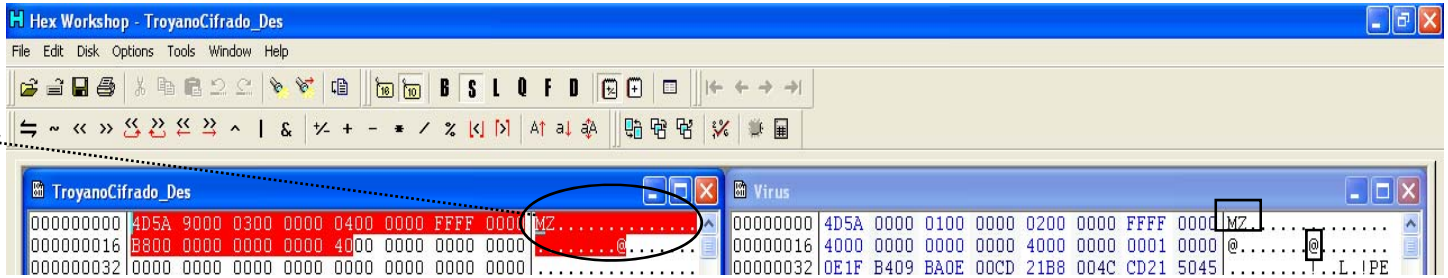
Archivo Ejecutable de 20KB

Herramienta “Crypter” que ofrece 10 distintos tipos de cifrado para evasión de antivirus.

Debe alterar el archivo virus dejándolo **funcional** e **indetectable**, de lo contrario “no sirve” .

72 Ser más claro. Mucha gente quedará lopca cuado le hables de conexión inversa remota. Entre más sencillo mejor.
7141546, 05/06/2008

Se realizó un reemplazo del segmento en el archivo cifrado desde el offset 0 hasta el offset 25. (No se alteraron los dos primeros Offset (MZ) ni atmpoco el 25 (@), de alterarse estos offset el archivo queda inservible)



Del offset 61 al offset 333 se realizó una inserción con datos predeterminados de otros archivos. Esta fracción hace parte de la firma genérica del Virus

Inserción de información empaquetada mediante UPX.

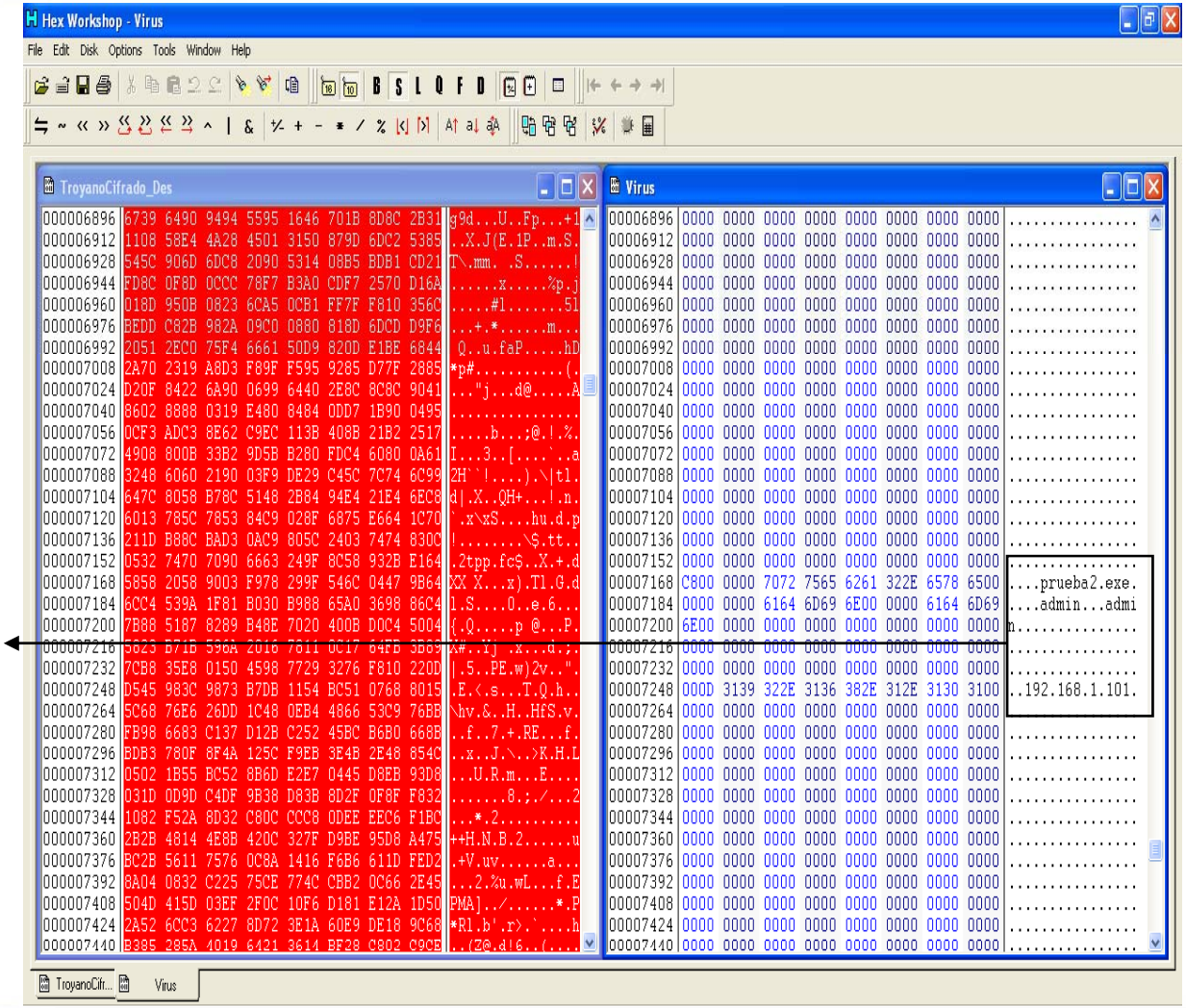
Diapositiva 5

74 Parte la gráfica y los pedazos los muestras, no toda la gráfica completa. Es decir tomas el primer pedazo y explicas, luego el segundo pedazo y luego el tercer. Si quieres ponle animación a la vaina pa que no se ve tan dificil de digerir.

7141546, 05/06/2008

....Cifrado

El trabajo de cifrado se inicia desde el offset 621, dado que de hay en adelante se registra información primordial como la cadena de conexión del troyano, la ruta de alojamiento del mismo e información del proceso que obviamente hace parte de las características del virus y no debe ser detectado por el antivirus.



Diapositiva 6

75 Lo mismo, mucha letra....

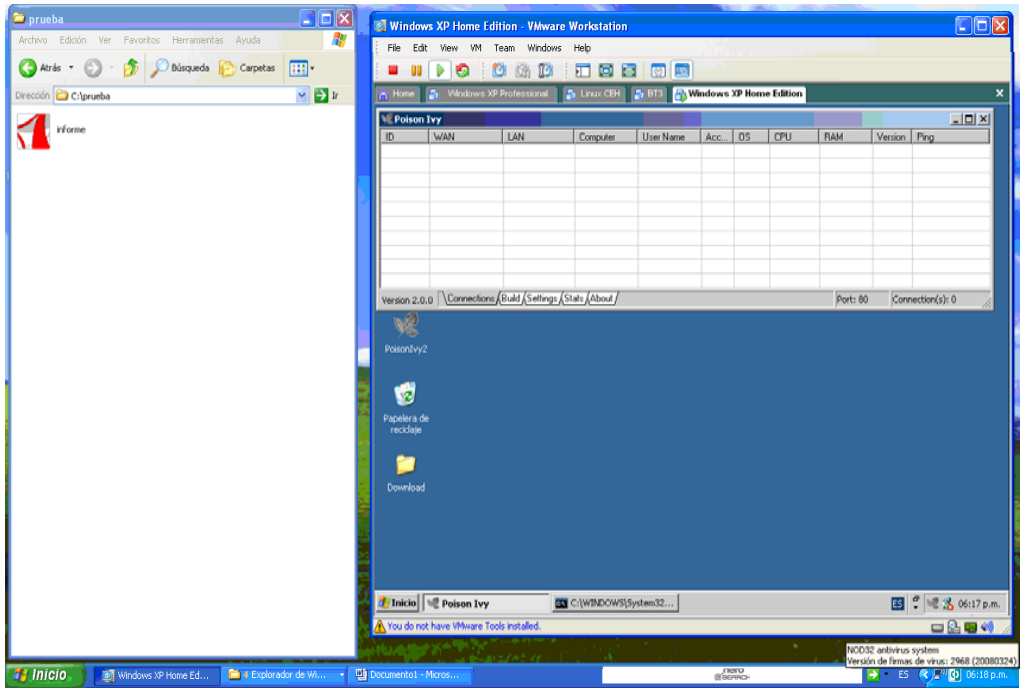
7141546, 05/06/2008

.... Matriz de Resultados

Software Antivirus	Evaluación Virus cifrado Firma RIJNDAEL	Evaluación Virus cifrado Firma TWOFISH	Evaluación Virus cifrado Firma BLOWFISH	Evaluación Virus cifrado Firma DES	Evaluación Virus cifrado Firma EQV	Evaluación Virus cifrado Firma GOST	Evaluación Virus cifrado Firma NOT	Evaluación Virus cifrado Firma SKIPJACK	Evaluación Virus cifrado Firma TEA	Evaluación Virus cifrado Firma XOR
AhnLab-V3										
AntiVir	TR/Spy.VB.SY.2	TR/Spy.VB.SY.2	TR/Drop.VB.SG.37	TR/Drop.VB.SG.22	TR/Dropper.Gen	TR/Drop.VB.SG.3	TR/Crypt.XDR.Gen	TR/Drop.VB.SG.32	TR/Drop.VB.SG.4	TR/Dropper.Gen
Avast	Win32:VB-FLF	Win32:VB-FLF	Win32:Trojan-gen {UPX}		Win32:VB-GVE	Win32:Trojan-gen {UPX}	Win32:Poison-gen			
AVG	PSW.Generic5.JPU	PSW.Generic5.JPU	Dropper.Generic.QLY	Dropper.Generic.QOR	Downloader.Generic6.WJC	Dropper.Generic.QLX	Generic9.AQCB	Dropper.Generic.QOU	Dropper.Generic.QOG	Generic9.AQCA
BitDefender	Trojan.Agent.AFHZ	Trojan.Agent.AFHZ								
ClamAV	Trojan.VB-1335	Trojan.VB-1335	Trojan.Dropper-3054			Trojan.Dropper-4506				
DrWeb										Trojan.Microjo.32
eSafe	suspicious Trojan/Worm	suspicious Trojan/Worm	suspicious Trojan/Worm	suspicious Trojan/Worm	suspicious Trojan/Worm	suspicious Trojan/Worm	suspicious Trojan/Worm	suspicious Trojan/Worm	suspicious Trojan/Worm	suspicious Trojan/Worm
eTrust-Vet										
Ewido	Logger.VB.sy	Logger.VB.sy	Dropper.VB.sg	Dropper.VB.sg	Downloader.VB.buy	Dropper.VB.sg		Dropper.VB.sg	Dropper.VB.sg	Trojan.VB.bkh
F-Prot	W32/Trojan.BXRR	W32/Trojan.BXRR								
F-Secure	W32/VBTroj.HGM	W32/VBTroj.HGM	W32/VBTroj.HXZ	W32/VBTroj.IBZ	W32/DLoader.EHYZ	W32/VBTroj.HXY	W32/Smalltroj.BVJK	W32/VBTroj.INO	W32/VBTroj.HYT	W32/VBTroj.KMQ
Ikarus	Trojan-Spy.Win32.VB.sy	Trojan-Spy.Win32.VB.sy	Trojan.Win32.VB.azd	Trojan.Win32.VB.azd	Trojan.Win32.VB.ayo	Trojan.Win32.VB.azd	Trojan.Win32.VB.ayo	Trojan.Win32.VB.azd	Trojan-Dropper.Win32.VB.sg	Trojan.Win32.VB.ayo
Kaspersky	Trojan-Spy.Win32.VB.sy	Trojan-Spy.Win32.VB.sy	Trojan-Dropper.Win32.VB.sg	Trojan-Dropper.Win32.VB.sg	Trojan-Downloader.Win32.VB.buy	Trojan-Dropper.Win32.VB.sg		Trojan-Dropper.Win32.VB.sg	Trojan-Dropper.Win32.VB.sg	Trojan.Win32.VB.bkh
McAfee	W32/Hlln.worm	W32/Hlln.worm								
NOD32v2	Win32/Spy.VB	Win32/Spy.VB	Win32/TrojanDropper.VB			Win32/TrojanDropper.V		Win32/TrojanDropper.VB		
Norman	W32/VBTroj.HGM	W32/VBTroj.HGM	W32/VBTroj.HXZ	W32/VBTroj.IBZ	W32/DLoader.EHYZ	W32/VBTroj.HXY	W32/Smalltroj.BVJK	W32/VBTroj.INO	W32/VBTroj.HYT	W32/VBTroj.KMQ
Panda	Suspicious file	Suspicious file	Suspicious file	Suspicious file	Trj/Downloader.SIE	Suspicious file	Suspicious file	Suspicious file	Trj/Dropper.YS	Suspicious file
Prevx1	TROJAN.AGENT.GEN	TROJAN.AGENT.GEN								
Rising			Dropper.Win32.VB.sg							
Sophos	Sus/Behav-169	Sus/Behav-169	Sus/Behav-169	Sus/Behav-169	Sus/Behav-169	Sus/Behav-169	Mal/Behav-096	Sus/Behav-169	Sus/Behav-169	Sus/Behav-169
Sunbelt CounterSpy										
Symantec-Norton	Trojan Horse	Trojan Horse	Downloader	Trojan Horse		Trojan Horse			Trojan Horse	
TheHacker	Trojan/Spy.VB.sy	Trojan/Spy.VB.sy	Trojan/Dropper.VB.sg	Trojan/Dropper.VB.sg		Trojan/Dropper.VB.sg		Trojan/Dropper.VB.sg	Trojan/Dropper.VB.sg	Trojan/VB.bkh
TrendMicro										
VBA32	Trojan-Spy.Win32.VB.sy	Trojan-Spy.Win32.VB.sy	Trojan-Dropper.Win32.VB.sg	Trojan-Dropper.Win32.VB.sg	Trojan-Downloader.Win32.VB.buy	Trojan-Dropper.Win32.VB.sg		Trojan-Dropper.Win32.VB.sg	Trojan-Dropper.Win32.VB.sg	Trojan.Win32.VB.bkh
VirusBuster										

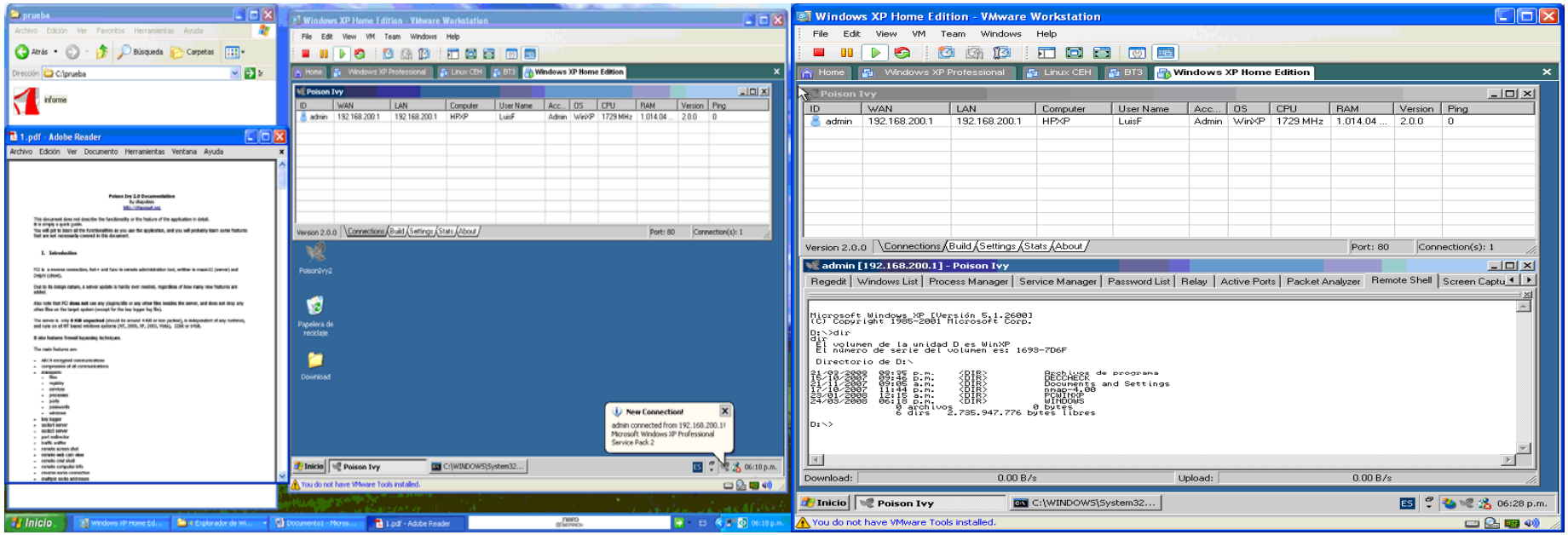
.... Materialización del Riesgo

"De los 27 Software antivirus, solo 9 **NO** son vulnerables a estas amenazas, los 18 restantes por alguno de los 10 algoritmos de cifrado de virus pueden ser vulnerados".



Archivo virus cifrado, enmascarado en un archivo PDF, al antivirus se esta ejecutando normalmente sin detectar la amenaza.

.... Materialización del Riesgo



Se ejecuta el archivo virus, vulnerando los patrones “heurísticos” del antivirus, generando la conexión remota a la consola de administración del troyano.

.... Conclusiones

- Exigir al proveedor del antivirus alta calidad de servicio del producto adquirido.
  - ✓ ¿Por qué tengo que actualizar la versión de mi antivirus para que me preste la funciones básicas?
    - ✓Lo ideal es actualizar únicamente los patrones de detección por firmas y heurísticos, sin importar la versión que se tenga.

      Características Básicas: Análisis heurístico de alta capacidad, diversas técnicas de detección y análisis, actualización de firmas y patrones de detección en línea, protegido por contraseña, bajo consumo de recursos.
- La plataforma Antivirus, un activo mas a involucrar en nuestras pruebas de vulnerabilidad.
  - ✓ ¿Cómo?:
    - ✓ Indagando ultimas vulnerabilidades en el mercado “underground”.
    - ✓ Teniendo un área en la compañía que se encargue de evidenciar y explotar (en la medida de lo posible) la vulnerabilidad.
    - ✓ Contando con personal éticamente calificado para desarrollar la función.
    - ✓ Por un tercero.

Diapositiva 10

78 Mini checklist de que debe tener un antivirus. puntos más importantes.
7141546, 05/06/2008

.... Conclusiones

- Las pruebas de vulnerabilidad adquieren un valor comercial.
  - ✓Vende la gestión de seguridad informática de la compañía ante los clientes.
  - ✓Vende al área de seguridad Informática ante las demás áreas de la compañía.
  - ✓Es un producto tangible, que tiene gran impacto dentro y fuera de la organización.
- El Hacker Ético toma importancia dentro la estructura de seguridad informática de la compañía.
  - ✓ Recurso dedicado que realiza las pruebas de vulnerabilidad y test de penetración en la compañía.
  - ✓Es el encargado de monitorear la eficacia y eficiencia de los controles informáticos.
  - ✓ Realiza sus funciones desde tres enfoques:
    - ✓ Visión Técnica: Realizando evaluación de riesgos a la plataforma TI.
    - ✓Visión de Seguridad: Realizando intrusión a los dispositivos.
    - ✓Visión de Negocio: Realizando auditoria a los controles.
  - ✓ Replantea la seguridad como medida de mejoramiento en el proceso de gestión de la seguridad.

Ref: El valor del Hacker en la organización. Almanza Andres - VI JNSI

77 Fuentes...
7141546, 05/06/2008

.... Referencias

- ✓ “Pruebas de Vulnerabilidad”. Disponible en: http://blownx.com/index.php/seguridad-informatica/44-seguridad-informatica/72-pruebas-de-vulnerabilidad.
- ✓ Madantrax. “Cactus Methamorph”. Disponible en: http://www.elhacker.net
- ✓ BreakPoint Software. “Hex Workshop”. Disponible en: http://www.bpsoft.com.
- ✓ “The Anti-Virus or Anti-Malware Test File”. Disponible en: http://www.eicar.org/anti_virus_test_file.htm
- ✓ “Trece antivirus a examen”. Disponible en: http://www.terra.es/tecnologia/articulo/html/tec6237.htm
- ✓ Shapeless. “Poison Ivy”. Disponible en: http://chasenet.org
- ✓ Nhaalclkiemr. “Crypter”. Disponible en: http://www.elhacker.net
- ✓ Almanza Andrés. “El valor del hacker en la organización”. VI Jornada Nacional de Seguridad Informática.
- ✓ “Heurística en antivirus”. Disponible en: http://es.wikipedia.org/wiki/Heur%C3%ADstica_(antivirus)

Gracias

¿Preguntas?