CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

EDWIN MAURICIO FAJARDO OLARTE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
VELEZ-SANTANDER
2020

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

EDWIN MAURICIO FAJARDO OLARTE

INFORME: ETAPA 5: SOCIALIZACIÓN INFORME TÉCNICO

JOHN FREDDY QUINTERO
DIRECTOR DEL CURSO: Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team - (202337164A_780)
M.sc.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
VELEZ-SANTANDER
2020

Resumen:

El presente documento da a conocer el resultado del desarrollo de las actividades propuesta en el seminario especializado de equipos estratégicos en ciberseguridad: Red Team y Blue Team, a lo largo de su contenido se entregarán los resultados de las consultas y las practicas llevadas a cabo en un entorno simulado, compuesto por máquinas que normalmente se encuentran en una organización.

Inicialmente se realizará la contextualización en torno a la legislación y normatividad que aplica en nuestro país y que tiene que ver con delitos informáticos y protección de datos, posteriormente se entregará al lector una explicación detallada de las características de los equipos conocidos como Blue Team y Red Team y cuál es la diferencia de este último con un equipo de atención de incidentes informáticos en una empresa,

Teniendo en cuenta que una de las actividades propuestas durante el seminario, tiene que ver con la ejecución de un ataque informático a dos máquinas conectadas a una infraestructura de red, simulando un entorno real, y en vista de que a partir de esta práctica se reconocieron herramientas de inspección e identificación de vulnerabilidades, así como herramientas que permiten realizar el acceso no autorizado, este documento dará a conocer el listado de dichas herramientas y sus principales características, por último se dará a conocer la propuesta seguridad que se debería implementar en un equipo que está siendo atacado.

CONTENIDO

Pág.
2. OBJETIVOS 8
2.1 OBJETIVO GENERAL 8
2.2 OBJETIVOS ESPECÍFICOS 8
3 DESARROLLO DE LA ACTIVIDAD 9
3.1 Marco Teórico 9
3.2 Marco Legal 10
3.3 Informe Técnico 11
3.3.1 Accionar del equipo Red Team 11
3.3.1 Accionar del equipo Blue Team 14
CONCLUSIONES 16
RECOMENDACIONES 17
Referencias 18

Glosario

Blue Team: Equipo experto en ciberseguridad cuya función principal corresponde a la contención de los ataques realizados por el equipo Red Team

Contención: medidas aplicadas sobre un sistema informático que evitan facilitar el acceso a intrusos informáticos

Dato: Elemento que se suministra a un sistema para convertirlo en información más estructurada

Equipo de respuesta a incidentes: grupo de personas dedicadas a actuar de manera reactiva en caso de que haya ataques informáticos.

Hardening: Término técnico usado en el área de sistemas el cual hace referencia al fortalecimiento de los equipos para evitar el acceso a ellos por personal no autorizado

Herramientas de intrusión: Herramientas software que al ser ejecutadas permiten el acceso no autorizado a sistemas informáticos que normalmente se encuentran interconectados.

Intrusión: Acceso no autorizado a un sistema informático puede ser con fines de identificación de vulnerabilidades o con fines maliciosos.

Ley: Reglamento que establece un estado para organización y reglamentar las acciones de sus ciudadanos.

Pentesting: Pruebas de penetración aplicadas sobre un sistema informático para verificar su grado de vulnerabilidad

Protocolo: reglas que se deben seguir para ejecutar una acción relacionada con un sistema informático.

Red Team: Equipo compuesto por personas expertas en ciberseguridad que tienen como fin realizar ataques informáticos a fin de detectar vulnerabilidades.

Sistema Operativo: Parte intangible de un sistema informático que permite controlar la parte física del mismo.

Vulnerabilidad: debilidad que presenta un sistema informático que se convierte en una puerta de entrada a los intrusos.

INTRODUCCION:

Los equipos de seguridad Blue Team y Red Team, hasta hace poco eran escasamente conocidos en el entorno de las empresas, sin embargo, en vista del aumento de los ataques informáticos que diariamente se evidencian en el mundo y teniendo en cuenta estudios realizados en relación con las estadísticas de los costos generados por los ciberataques, en los que se calcula que los daños producidos a nivel global superan los 11 billones de dólares anuales. (Prey, 2018), convierten, además de los equipos antes mencionados, a los términos ciberataque y ciberseguridad en conceptos que dejan de ser prioritarios para personas que se encuentren adelantando algún tipo de formación en el área de sistemas o personas expertas en seguridad informática. De tal suerte que ya hablar de equipos de contención, escaneo de vulnerabilidades herramientas de intrusión, son temas que se van incorporando en el léxico de la comunidad de manera mas normal que lo que se daba hace unos años ocurría.

El creciente aumento de la conectividad ha permitido que actividades que hasta hace algunos años eran realizadas de manera totalmente diferente a la actual, ahora se realicen de forma automática y sistematizada, para algunos casos, existe modernos términos como la domótica y el internet de las cosas, este último concepto nación entre 2008 y 2009 y en este entonces se pronosticaba que la cantidad de dispositivos conectados en el 2020 superaría los 50 mil millones, lo cual presenta un incremento considerable si se tiene en cuenta en el 2003 no se superaban los 500 millones (Evans, 2011); lo anterior es una muestra clara que nuestras vidas están profundamente relacionadas con los sistemas informáticos, con las redes de computadores y por ende con los ciberataques y con la ciberseguridad y todo lo que estos dos conceptos implican.

El presente documento realiza un recorrido iniciando por la legislación y la reglamentación actual de nuestro país y relacionada con la seguridad informática y con la protección de los datos, de esta manera se presenta en detalle el contenido de la ley 1273 del 2009 y la Ley 1581 del 2012, posteriormente se dan a conocer los resultados obtenidos luego de ejecutar una actividad de intrusión en un entorno simulado el cual recrea una red de datos, la cual puede estar dispuesta en cualquier empresa de nuestro entorno, y finalmente se entrega una seria de recomendaciones y estrategias de protección y contención las cuales, una vez implementadas se espera que minimicen los riesgos de un ataque informático.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

- Brindar un informe final gerencial en el que se de a conocer el resultado de las acciones ejecutadas por los equipos Blue Team y Red Team en torno a los escenarios propuestos para le empresa The WhiteHose Security.

2.2 OBJETIVOS ESPECÍFICOS

- Conceptualizar acerca de la legislación y reglamentación existente en nuestro país en torno a la seguridad de la información y la protección de datos personales.

- Dar a conocer el resultado de las acciones ejecutadas por los equipos Blue Team y Red Team de acuerdo con los escenarios propuestos para la empresa The WhiteHose Security.

- Proponer acciones de protección para evitar la intrusión de delincuentes informáticos.

3 DESARROLLO DE LA ACTIVIDAD

3.1 Marco Teórico

A manera de contextualización, y antes de dar a conocer los resultados de las prácticas realizadas en el marco del seminario de equipos estratégicos en ciberseguridad, es necesario mencionar y reconocer conceptos propios del área de seguridad informática los cuales permitirán un mejor entendimiento al momento de analizar los resultados de las pruebas efectuadas.

En la actualidad es muy común escuchar conceptos que hasta hace unos años eran extraños para la comunidad en general, sin embargo, un concepto como pentesting (pruebas de penetración) el cual hace referencia a un ataque controlado para identificar vulnerabilidades de los sistemas informáticos para que, de manera consciente, se puedan encontrar medidas de control endurezcan las puertas de acceso a dichos sistemas (Alcaldía de Bogotá, 2018) para llevar a cabo estos ataques, existe una gran cantidad de herramientas, metodologías, marcos de trabajo que permiten que personas que no sean tan expertas en temas ciberseguridad, puedan poner en práctica ataques de manera no tan compleja.

Para el desarrollo de las actividades del seminario especializado, se conocieron las características de los equipos Red Team y Blue Team, los primeros se componen de un grupo de personas expertas en ciberseguridad las cuales, de una manera controlada, intentan acceder de manera intrusiva a los equipos informáticos de una empresa, mientras que los equipos Blue Team, intentan contener los ataques del equipo Red haciendo uso de herramientas especializadas de detección y contención de tal manera que permita tener insumos técnicos para elaborar un informe técnico que presente a la organización un informe detallada de las vulnerabilidades y las estrategias y prácticas de endurecimiento que se deben implementar para evitar fuga de información, o interferencia en los sistemas o servidores o cualquier otra efecto negativo producto de la intrusión. (PurpleSEC, 2019)

Las herramientas usadas para el ejercicio de intrusión propuesto en el seminario fueron algunas de las recopiladas en la distribución de Linux Kali LINUX, este sistema operativo basado en DEBIAN orientada a realizar pruebas avanzadas de penetración, según su portal oficial, este sistema operativo contiene cientos de miles de herramientas a analizar actividades relacionadas con seguridad informática.

(Kali, by Ofensive Security, 2020). De esta manera se hizo uso de herramientas como NMAP, METAEXPLOIT para poder acceder de manera remota a dos equipos configurados con el sistema operativo Windows 7.

3.2 Marco Legal

En Colombia los delitos informáticos están regulados por la ley 1273 del 2009, dicha ley pretende proteger de manera integral todos los sistemas que utilicen las tecnologías de la información y las comunicaciones, de tal suerte que quien acceda de manera fraudulenta, acceda de manera abusiva, intercepte sin autorización, dañe, obstaculice o suplanta sitios web, tenga claro cual será la pena en prisión o económica que debe cancelar en caso de incurrir en alguna de esas conductas. (Congreso de la República, Ley 1273 del 2009, 2009)

Adicionalmente la Ley 1581 del 2012 regula el tratamiento y controla los datos personales que reposan en bases de datos publicas y privadas en el país, dando cumplimiento al articulo 15 de la constitución política de Colombia. (Congreso de la República , Ley 1581 del 2012, 2012).

La ley 842 del 2003 mediante la cual se adopta el código de ética para el ejercicio de la profesión de las ingenierías, entrega las bases para la construcción del código de ética propuesto por el Consejo Profesional de Ingeniería COPNIA (Congreso de la República, Ley 842 de 2003, 2003).

3.3 Informe Técnico

3.3.1 Accionar del equipo Red Team

Las actividades realizadas por los equipos Red Team y Blue Team en la organización The WhiteHose Security se llevó a cabo en un ambiente simulado conformado por las siguientes máquinas:

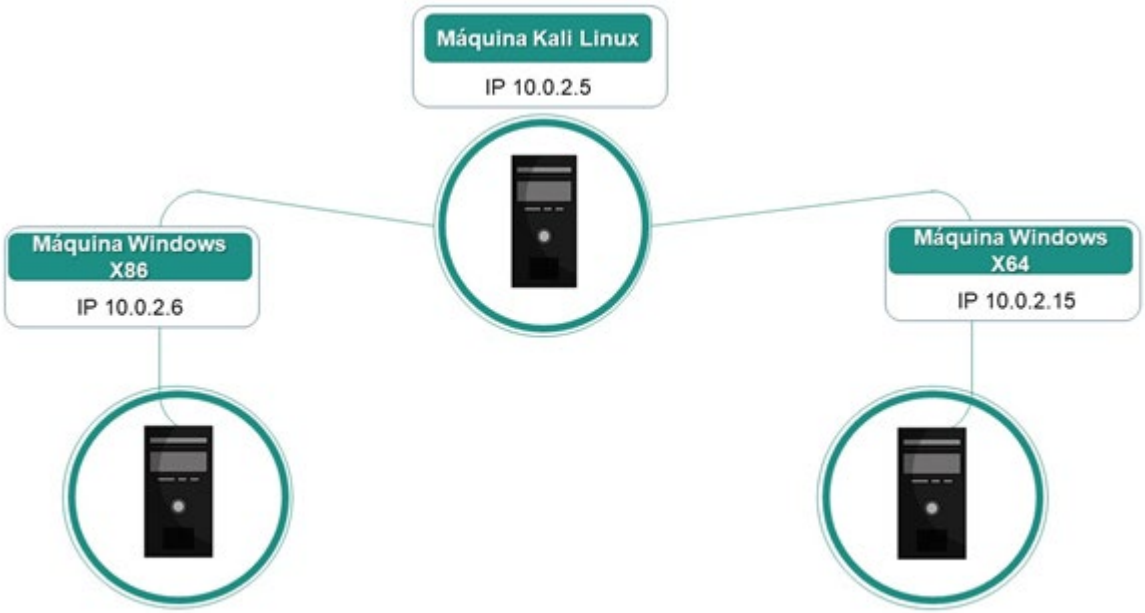

Figura 1 Estructura de la red White House Security

Fuente: Edwin Mauricio Fajardo

Como se puede notar en la anterior imagen, la estructura de la red de la organización White House Security está conformada por dos maquinas en las que se tiene instalado el sistema operativo Windows 7, una con versión de 64 bits y otra con versión de 32 bits, la maquina con la que se produce el ataque tiene instalado el sistema operativo Kali Linux.

A partir de la información suministrada, el primer paso fue realizar el escaneo de la red para detectar las maquinas conectadas a la infraestructura de la red, para esto se uso el segmento de red con direcciones IP 10.0.2 desde la 01 hasta la 200 y el comando nmap con el modificador -sS, esta excelente herramienta de escaneo es indetectable para los firewalls, su acción la cual se realiza sobre un rango especifico de direcciones IP, es capaz de detectar hosts, puertos, servicios activos, tipo de sistema operativo, firewall y aplicaciones que están utilizando la red (ZONE Redes, 2013).

Luego de identificadas las maquinas que componen la red se procede a realizar el escaneo directamente en las maquinas que la componen, de esta manera se procede a identificar los puertos abiertos en las máquinas Windows encontrando lo siguiente:

Archivo de texto de la ejecución de nmap sobre la maquina Windows X64:

```
# Nmap 7.80 scan initiated Mon Sep 21 09:58:29 2020 as: nmap -p445 --
script=smb-vuln* -o nmap_smb.txt 10.0.2.15
Nmap scan report for 10.0.2.15
Host is up (0.00045s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-
010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
```

| Disclosure date: 2017-03-14
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
| https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done at Mon Sep 21 09:58:34 2020 -- 1 IP address (1 host up) scanned in 5.47 seconds

Archivo de texto de la ejecución de nmap sobre la maquina Windows X86:

Nmap 7.80 scan initiated Mon Sep 21 10:19:26 2020 as: nmap -p445 --script=smb-vuln* -o nmap_smb_x86.txt 10.0.2.6
Nmap scan report for 10.0.2.6
Host is up (0.00045s latency).

PORT   STATE SERVICE
445/tcp open microsoft-ds
MAC Address: 08:00:27:F6:A7:6C (Oracle VirtualBox virtual NIC)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
| VULNERABLE:
| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
| State: VULNERABLE
| IDs: CVE:CVE-2017-0143
| Risk factor: HIGH
| A critical remote code execution vulnerability exists in Microsoft SMBv1
| servers (ms17-010).
|
| Disclosure date: 2017-03-14
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
| https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

|_ https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done at Mon Sep 21 10:19:31 2020 -- 1 IP address (1 host up) scanned in 5.42 seconds

Como se evidencia en los archivos de texto de salida presentados, en la línea 11 de cada uno de dichos archivos se puede notar que las maquinas que conforman la red presentan una vulnerabilidad conocida como smb-vuln-ms17-010, dicha vulnerabilidad presenta las siguientes características:

IDs: CVE:CVE-2017-0143
Risk factor: HIGH (Factor de riesgo: Alto)
A critical remote code execution vulnerability exists in Microsoft SMBv1 servers (ms17-010). Es una vulnerabilidad de alto riesgo que permita le ejecución remota de código en sevidores Microsoft.
Disclosure date: 2017-03-14 (Fecha de divulgación)
References:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Al consultar más a profundidad acerca de esta vulnerabilidad se puede encontrar que CVE-2017-0143 es una ventana abierta para atacantes ya que el servidor SMBv1 en Microsoft Windows Vista SP2; Windows Server 2008 SP2 y R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold y R2; Windows RT 8.1; y Windows 10 Gold, 1511 y 1607; y Windows Server 2016 permite ejecutar paquetes maliciosos de manera remota (Common Vulnerabilities and Exposures, 2020)

3.3.1 Accionar del equipo Blue Team

Una vez conocidas las vulnerabilidades y el resultado de la intrusión llevada a cabo por el equipo Red Team, se procede a ejecutar una serie de actividades que le corresponde al equipo Blue Team, de esta manera se proponen las siguientes acciones en aras de prevenir futuros ataques y de esta manera minimizar la

posibilidad de los riesgos a los que se ven expuestas las maquinas de la empresa White House Security.

1. De acuerdo con lo manifestado por la empresa Withe House Security, el presupuesto para adquirir software licenciado no es muy alto, por lo tanto se decide hacer uso del analizador de paquetes de libre distribución Wireshark.
2. Su sugiere mantener actualizado el antivirus en las maquinas Windows lo cual garantiza la protección ante la ejecución de paquetes sospechosos sobre las maquinas de Withe House Security.
3. Configuración y activación de actualizaciones automáticas, esta práctica garantiza la ubicación de parches al sistema operativo los cuales contienen mecanismos de protección ante vulnerabilidades conocidas.
4. Configuración adecuada de archivos del sistema, colocando restricciones a archivos y particiones críticas del sistema
5. Desactivación de acceso remoto en caso de no requerirse

Como apoyo al presente documento, se presenta el siguiente video que contienen la sustentación de lo desarrollado en el curso: Seminario especializado EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM,

https://youtu.be/1P9q_LEoMJ8

CONCLUSIONES

Al realizar las actividades propuestas en el seminario Equipos estratégicos en ciberseguridad: Red Team & Blue Team se puede concluir que:

Es necesario conocer la reglamentación y las leyes que regulan el acceso a los sistemas informáticos en nuestro país, así como las que contemplan la protección de datos, esto se argumenta ya que, en el desarrollo de una de las actividades propuestas, se logró identificar que algunas personas, probablemente por desconocimiento de las leyes, realizaron actividades que las infringen razón por la cual en estos momentos se encuentran privados de su libertad o en el mejor de los casos, cancelando multas producto de las acciones ilegales ejecutadas.

A pesar de los costos que significa contar con equipos Blue Team y Red Team para las empresas, estas deberían considerar incluir estos grupos de profesionales para protegerse de ataques informáticos, toda vez que el creciente auge de la interconectividad hace que el activo mas preciado de las organizaciones, la información, día a día se ve más expuesto y vulnerable y según un artículo de la revista portafolio, por culpa de los ataques informáticos las organizaciones a nivel mundial puede perder entre uno y dos millones de dólares anuales, (Revista Portafolio, 2018)

No hace falta ser una persona experta en sistemas informáticos para identificar y explotar vulnerabilidades presentes en equipos de computo conectados a una infraestructura de red, esto debido a que hay una gran cantidad de herramientas como las incluidas en el sistema operativo Kali Linux donde se encuentran un número bastante grande de utilidades que permiten escanear segmentos de red y maquinas especificas para reconocer puertas abiertas que permiten el acceso a estas.

RECOMENDACIONES

1. Reconocer de manera amplia la legalización que regula la protección de datos y el uso de sistemas informáticos que se basen en las tecnologías de la información y las comunicaciones
2. Reconocer las características y la importancia de los equipos Blue Team y Red Team a la hora de protegerse de posibles ataques informático.
3. Identificar las herramientas existentes para la detección y explotación de las vulnerabilidades de los sistemas informáticos
4. Reconocer las herramientas de contención y de prevención de ataques informáticos e identificar claramente las diferencias entre cada una de ellas.
5. Darle la importancia que requiere la seguridad informática en las organizaciones toda vez que se está poniendo en juego el activo mas importante de estas, la información.

Referencias

Alcaldía de Bogotá. (2018). *Guardianes de la información - Penetration Testing.* Bogotá .

ALVAREZ INTRIAGO, V. (2018). *PROPUESTA DE UNA METODOLOGÍA DE.*

Ciberseguridad. (2018). *https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/*. Obtenido de https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/: https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/

Common Vulnerabilities and Exposures. (2020). Obtenido de https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Congreso de la República . (2012). Ley 1581 del 2012.

Congreso de la República. (14 de Octubre de 2003). Ley 842 de 2003. Bogotá colombia.

Congreso de la República. (5 de Enero de 2009). Ley 1273 del 2009. Bogotá, Colombia.

Congreso de la República. (17 de Octubre de 2012). Por la cual se dictan disposiciones generales para la protección de datos. Bogotá, Colombia.

EL TIEMPO. (23 de Enero de 2015). Fachada Andrómeda era legal. *El Tiempo.com* , pág. 1. Obtenido de https://www.eltiempo.com/archivo/documento/CMS-15141236

Evans, D. (2011). *Internet de las cosas: Cómo la próxima evolución de Internet lo cambia todo.* San Jose California: CISCO .

Hacking Para Novatos. (2017). *Hacking Para Novatos*. Obtenido de Hacking Para Novatos: https://hackingparanovatos.wordpress.com/2017/09/04/fases-de-una-auditoria-pentesting/

Kali, by Ofensive Security. (2020). *https://www.kali.org/docs/introduction/what-is-kali-linux/*. Obtenido de https://www.kali.org/docs/introduction/what-is-kali-linux/.

Ministerio de Comercio Industria y Turismo, R. (27 de Junio de 2013). Decreto Número 1317 DE 2013 . Bogotá .

Ministerio de las TIC. (2018). Guía para la Gestión y Clasificación. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

Ojeda Pérez, J. E., Rincón Rodríguez, F., Arias Flórez, M., & Daza Martínez, L. (23 de Mayo de 2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Delitos informáticos y entorno jurídico vigente en Colombia*. Bogotá, Cundimarca, Colombia: Cuadernos de Contabilidad. Obtenido de

http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

Prey. (3 de Diciembre de 2018). *preyproject.com*. Obtenido de preyproject.com: https://preyproject.com/blog/es/24-estadisticas-seguridad-informatica-2019/

PurpleSEC. (2019). *Red Team VS Blue Team: What's The Difference?* Obtenido de Red Team VS Blue Team: What's The Difference?: https://purplesec.us/red-team-vs-blue-team-cyber-security/

Revista Enter. (9 de Diciembre de 2015). Detrás de Buggly: la historia de la fachada Andrómeda. *Revista ENTER.co*, 1. Obtenido de https://www.enter.co/cultura-digital/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

Revista Portafolio. (20 de Octubre de 2018). *El costo de los ataques cibernéticos a las organizaciones en el mundo*. Obtenido de El costo de los ataques cibernéticos a las organizaciones en el mundo: https://www.portafolio.co/economia/el-costo-de-los-ataques-ciberneticos-a-las-organizaciones-en-el-mundo-522476

SOFECOM. (01 de 01 de 2018). *https://sofecom.com/que-es-un-siem/*. Obtenido de https://sofecom.com/que-es-un-siem/: https://sofecom.com/que-es-un-siem/

Una al Día. (1 de 1 de 2009). *Una al dia*. Obtenido de Una al dia: https://unaaldia.hispasec.com/2009/09/pantallazo-azul-bsod-en-windows-vista-y-7-a-traves-de-unidades-compartidas.html

ZONE Redes. (21 de Mayo de 2013). *Updated Security+*. Obtenido de Updated Security+: https://www.redeszone.net/seguridad-informatica/realiza-escaneos-de-puertos-en-linux-con-nmap/

Zuluaga Mateus, A. (2017). *Hacking ético basado en la metodología abierta de testeo de seguridad - OSSTMM .* Armenia.