Ciberseguridad

Transcribed on July 6, 2025 at 10:19 PM by Minutes AI

Speaker 1 (00:06)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a hablar sobre los grandes jugadores y las metodologías existentes en el mundo de la ciberseguridad.

Lógicamente no podemos hablar de todos los grandes players que existen, pero sí que vamos a ver algunos que son importantes porque durante el desarrollo de la formación vais a ver sobre probablemente términos como CV, CW, CPE.

Y bueno, pues tendréis que tenéis que ir conociendo un poco, sabiendo de dónde viene todo esto.

También hay una parte donde hablaremos de metodologías.

Las metodologías son muy útiles sobre todo cuando uno está comentando en la parte de auditoría, red, team, etc.

Y bueno, vamos a dejaros algunas metodologías aquí para que podáis profundizar por vuestra cuenta.

Lo que vamos a ir viendo es primero, por qué utilizar metodologías.

Mucha gente se pregunta por qué utiliza la metodología y vamos a ver por qué utilizar la metodología es bueno en un proyecto de genético, por ejemplo.

Vamos a ver también un apartado donde vamos a hablar de los principales, de los grandes players.

Ya digo que no son todos, existen, pero hemos hecho una pequeña recopilación.

Hablaremos de Owas, hablaremos de Mitre, hablaremos del First, hablaremos de Isaca, también está Nist y Nisa, que los queremos nombrar como fundamentales en la parte de América y en la parte de la Agencia Europea de Seguridad.

Así que, y luego pondremos el foco un poco para explicaros premetologías brevemente, daros pinceladas de lo que hay y luego que podáis profundizar.

¿Lo primero, por qué utilizar la metodología?

Pues bueno, por diferentes cosas.

Vamos a estructurarlo por organización y estructura.

Pues una metodología nos proporciona un conjunto de información estructurada con el objetivo de poder llevar a cabo las diferentes pruebas de un entorno de seguridad.

Es decir, me proporciona todo lo necesario para yo poder realizar una auditoría, realizar un tipo de intrusión o realizar otro tipo de auditoría diferente o cualquier prueba dentro del ámbito de la seguridad.

La metodología me permite saber el paso a paso, aunque ya os digo que cuando uno va cogiendo experiencia, ese paso a paso cada uno lo va haciendo cada vez más suyo.

La metodología nos puede dar los pasos adecuados para llevar a cabo una auditoría web, una auditoría interna, auditoría de sistemas, un pentest, pero al final con la experiencia uno va cogiendo agilidad e incluso va interiorizando o haciendo un poco suya esa metodología.

También puede ser que cuando una empresa contrata el servicio de otra empresa, pues le obligue a utilizar metodología, sobre todo para el tema de reporte, para el tema de informe, con el objetivo de poder comparar futuras auditorías que haga con otras empresas y estandarizar ese reporte.

También la metodología se utiliza por eficiencia y consistencia, es decir, cuando se utiliza la metodología vamos a asegurarnos una ejecución eficiente de las actividades que tenemos que llevar a cabo.

Esto nos va a permitir optimizar tanto uso de recursos, tanto uso del tiempo y va a evitar que dupliquemos actividades, pruebas, esfuerzo.

Y vamos a asegurarnos también que todas las tareas, todas las actividades importantes que debemos realizar en un trabajo lo llevemos a cabo.

Luego hay que tener en cuenta también que las metodologías no siempre se pueden utilizar al pie de la letra, porque tenemos que tener en cuenta que las metodologías a veces son o abarcan muchísimos tipos de pruebas.

No tenemos tanto tiempo, igual tenemos un trabajo, una auditoría que realizar en cinco jornadas.

Si aplicamos una metodología concreta durante ese tiempo no llegaríamos a abordarla completamente por el volumen de activos que pueda tener la organización o por el volumen de activos que pueda tener esa auditoría.

Como tercer punto vemos ahí el de mejores prácticas.

Las metodologías al final son basadas en buenas prácticas.

Utilizar una metodología o basarse en una metodología para llevar a cabo una metodología o un pentest siempre es una buena práctica en sí mismo porque nos va a ayudar a tener calidad y efectividad en actividades que vamos a realizar en ese entorno.

El cuarto punto nos habla de un enfoque estructural para la gestión de riesgos.

Aquí hablamos de gestión de riesgos.

Fijaos cómo estamos de nuevo uniendo, mezclando la parte de análisis y gestión de riesgos con la parte ciber relación, como hemos ido viendo.

Y bueno, nos permite hacer un enfoque estructurado para esta gestión de riesgo, siempre buscando lo mismo, que la gestión sea más efectiva de los riesgos, imperializar recursos que debemos utilizar después para evaluar esos controles.

Si tenemos que enumerar a los grandes jugadores, ya digo que no son todos los que son, pero bueno, estos son alguna recopilación de algunos importantes Owaf, Mitre, Fer, Zaka, Nist e Nisa son nombres que tenemos que conocer.

Organizaciones líderes en el campo de la seguridad, aunque hay otras que también son líderes, no están en este listado y desarrollan o han desarrollado y han promovido la utilización de metodologías, han hecho estándares, han hecho guías de buenas prácticas y lógicamente son ampliamente reconocidos.

1 Fuente de información muy interesante y muy potente que se debe conocer, tenemos estudiar y que se debe en algunos casos aplicar.

Por ejemplo, las buenas prácticas siempre que la competencia nis de Nisa, OWas, pues son una fuente muy potente.

Vamos a empezar hablando un poco de OWAS.

Owas es una guía de buenas prácticas de desarrollo de autoevaluación.

Es un documento que que proporciona el propio OWas, que proporciona las recomendaciones para llevar a cabo un desarrollo seguro de aplicaciones web.

Es cierto que OWAs ha ido evolucionando y después empezó en la parte de aplicaciones web y ha evolucionado también a tener una sección dentro del desarrollo de aplicaciones móviles, del desarrollo de sistemas IoT inclusivo ahora mismo, ahora mismo tienen también un apartado para los LLMs en inteligencia artificial.

Así que OWAx estaba riendo bastantes ámbitos de la ciberseguridad, aunque el comienzo fue en la parte de aplicaciones web y es donde son realmente más potentes.

Luego tenemos el OWAS Top Ten, que es una lista de 10 vulnerabilidades de seguridad que proporciona uvas cada x años, cada tres o cuatro años publican un top 10 donde ellos dicen las vulnerabilidades web que más han encontrado en Internet.

Este top 10 es una revisión importante y que debemos también conocer.

Lo que pasa que no es solamente lo que aparece ahí todo lo que hay en Internet.

Lógicamente las vulnerabilidades web son mucho más de lo que aparece en el top 10 de Owas, pero bueno, siempre es una fuente a tener en cuenta y veo un poco la evolución de las vulnerabilidades web en Internet.

Tenemos también el Mitre.

El Mitre es una organización sin fines de lucro que se enfoca en resolver problemas críticos y que nos proporciona algunos frameworks bastante potentes como es el Attc key o Latac, el cue Súbele el Attack es el marco de evaluación de tácticas, técnicas, procedimientos de adversarios.

Hemos hablado de esto en el ámbito del Red Team, pero bueno, es una base de conocimiento desarrollado por Mitre que nos describe las tácticas y técnicas que utilizan los adversarios con el objetivo de comprometer y operar en sistemas de información.

Es decir, son una gran base de conocimientos.

Una gran base de conocimiento que refleja cómo son las amenazas o cómo son los adversarios reales, qué técnicas y qué tácticas utilizan y debemos conocer para poder configurar las protecciones adecuadas para estar preparados para amenazas similares a las que ya conocemos.

Es un poco el objetivo del framework.

Luego tenemos el 105.º, que es otra cosa importantísima que nos deja el Mitre, que es una de las cosas más utilizadas en los estándares de ciberseguridad.

Es el diccionario de vulnerabilidades y exposiciones que se llama.

Entonces este lo que refleja es cada vulnerabilidad que aparece se le puede proporcionar un identificador único donde se describe la vulnerabilidad y se indica cómo afecta, cómo se puede explotar.

Y este CVE es un estándar que bastante conocido.

Luego tenemos el cw, que es la lista de debilidades.

Es un diccionario también que utiliza donde agrupamos las vulnerabilidades por tipos de debilidad.

Si por ejemplo tenemos diferentes tipos de inyección, todas comparten algo en común que es que son inyecciones.

Entonces el cvle de todas esas vulnerabilidades sería el mismo, son de tipo inyección, lo que pasa que luego cada una de ellas podría tener un cve diferente que corresponda a cada vulnerabilidad.

Y luego segunda unidades podemos agruparlas en un cw único para colocarlo en luego tenemos el FES, que es otra de las organizaciones a nivel mundial más conocidas.

Nos aporta el cvss que es una forma de puntuar, una forma estandarizada de puntuar las funcionalidades.

El CVss proporciona una métrica que nos permite calificar y priorizar las vulnerabilidades que podemos encontrar en función de la gravedad o de la severidad.

Entonces podemos encontrar que la vulnerabilidad tiene un Cvss de 10 o de nueve o de 9,5 o de ocho.

Entonces nos haremos una idea de la criticidad que tiene esta bolia.

Si nos fijamos tenemos también el concepto de base score.

Esto es lo que se publica cuando sale una vulnerabilidad, se publica un base score que es la gravedad de esa vulnerabilidad independientemente de cómo afecta en tu organización.

Para ello el TWS proporciona una serie de valores que es el Temporal Government Score, que corrigen el volumen o la calificación que se le ha puesto en el Bscore una vulnerabilidad.

Por ejemplo, podemos tener una vulnerabilidad que afecta a mi empresa, una segunda empresa que tiene la misma vulnerabilidad que también afecta, pero no nos afectan igual porque los sistemas afectados no tienen la misma criticidad, por lo cual aunque anteojos del pace score tendrían la misma criticidad, a los ojos del temporal y el environment score no es así.

Entonces cada uno corrige y a una empresa puede ser más crítico y para otra puede ser menos crítico.

Llegamos a IS, es otra de las organizaciones a nivel mundial más reconocidas, fue fundada en 1969 creo recordar y usa que ya tiene muchísimos años y tiene un framework que es Covid que es bastante conocido.

El framework de Covid es un conjunto de prácticas estándares para gobierno y gestión de TI.

Es un frame que está ampliamente aceptado con diferentes organizaciones y que va a permitir establecer y mantener un control sobre los sistemas tecnológicos.

Así que bueno, es otro de los puntos más orientado a la parte de análisis y gestión del riesgo, a la parte del gobierno.

Pero también hay que entender que todo lo que es la seguridad de información está aislado, las cosas de ciberseguridad, pero todo bilado con el objetivo global que es proteger la confidencialidad, la disponibilidad, la integridad de la información.

Bien, ahora vamos a poner un poco el foco en las metodologías.

Hemos elegido tres metodologías para comentaros, existen más, podéis investigar o podéis mirar por el resto de metodologías.

Vamos a hablar de no sólo el OSSTM, es una metodología que tiene 15 capítulos donde se van describiendo diferentes tipos de auditorías y diferentes tipos de intrusión con las diferentes pruebas que se tienen que ir realizando.

Está bastante bien a la hora de cuando uno es un perfil junior y no tiene experiencia en este trabajo, pues puede hacer uso de esta metodología para poder aprender y sobre todo poder en práctica cuando me toque hacer una auditoría o hacer con desintrusión, poder llevarlo a cabo.

Una cosa interesante del OSSTM es la estandarización de los informes.

Tiene un capítulo dedicado a los informes y siempre viene bien porque siempre tenemos dudas sobre cómo hacer un informe ejecutivo, cómo hacer un informe técnico, pues el ostm al final nos proporciona ese tipo de información.

Luego también tenemos el Pts, tenemos Esav, que es otra metodología que también podéis revisar.

El Pts es una metodología muy especial porque está orientada solamente al tema de intrusión, solamente al pentesting.

Y bueno, son una serie de capítulos donde va indicando las herramientas que se pueden utilizar y las diferentes fases que podemos encontrar en Opentest.

Hay que recordar la parte de recopilación información, la parte de análisis de vulnerabilidades, la parte de explotación de vulnerabilidades, la parte parte de postulación y luego hay un capítulo dedicado a la parte de reporting.

También estandarizan o intentan estandarizar cómo debe ser un informe de test intrusión o de pentest.

Bueno, las metodologías, como digo, hay que ponerle bastante foco, son importantes, hay que conocerlas.

Como conclusiones a este vídeo, a esta sesión, pues hemos visto por qué utilizar metodologías importantes, sobre todo en el ámbito más profesional.

La metodología te da la parte de estandarización de informes y te da la parte de cómo hacer el trabajo.

Eso es lo más importante.

Luego un poco de historia acerca de hemos visto un poco de historia acerca del Mitre, de OWas, de First Isaca, hemos visto también un poco lo que ofrecen, lo que nos han dado al mundo de la ciberseguridad y al mundo de la seguridad e información.

Y luego hemos visto un poco las diferentes metodologías de forma muy resumida, pero para que vosotros las conozcáis y podéis profundizar un poco sobre ellas.

Bien, con esto llegamos al final de la sesión.

Nos vemos en la siguiente sesión.