XUNTA DE GALICIA

FP FORMACIÓN PROFESIONAL INNOVA

IES San Clemente **CIFP Rodolfo Ucha Piñeiro**

MITRE - C2C -Postexplotación

Ciberinteligencia

1. Ve a la página web de MITRE ATT&CK. Una vez en la web de MITRE ATT&CK, marca como respuesta OK y pasa a la siguiente pregunta (5 puntos)
2. El framework tiene una lista de 19 técnicas bajo la táctica que busca mantener el acceso en tus sistemas. ¿Cuál es el ID de la táctica? Formato: nº de ID (p.e. TA2222) (10 puntos)
3. ¿Cuántas técnicas caen bajo la táctica que emplean los adversarios para robar datos de tu red? Formato: número (p.e. 5) (00 puntos)
4. Tus sistemas de monitorización alertan de la ejecución del software sqlmap. Atendiendo a lo mostrado en la matriz MITRE, ¿en qué fase del ataque (técnica) se encuentra el atacante que ejecutó el comando? Formato: ID (p.e. T2222) (15 puntos)
5. Analizando logs encuentras entradas asociadas al puerto 1058. ¿De qué grupo APT se puede tratar? Formato: nombre del grupo (p.e. Iron Maiden) (60 puntos)
6. Se sospecha que grupo Sandworm Team atacó en 2015 y 2016 compañías eléctricas y organismos del gobierno de Ucrania. Además, se cree que es el responsable del 'deface' de unos 15.000 sitios web del gobierno georgiano. ¿Qué acción de mitigación recomienda MITRE para este último tipo de ataque? Formato: nombre de la técnica de mitigación (p.e. Network Segmentation) (60 puntos)
7. Entre noviembre de 2019 y enero de 2021 se lanzó una campaña contra empresas metalúrgicas de países sudamericanos, donde los adversarios enviaron correos electrónicos de phishing que incluían un documento PDF, que en algunos casos llevó a la descarga y ejecución de malware. ¿Di uno de los servicios de hosting legítimos usados para alojar ese malware? Formato: nombre de uno de los servicios de hosting (p.e. Megaupload) (60 puntos)
8. Los grupos APT28, APT29, Dragonfly y Ember Bean se cree que están financiados por Rusia. Valorándolos en conjunto, ¿qué técnica de mitigación propone MITRE para luchar contra la técnica de C2C más empleada por estos grupos? Formato: ID de la técnica de Mitigación (p.e. M2222) (80 puntos)
9. Siguiendo con APTs rusos y centrándonos en la técnica más empleada por estos grupos para lograr credenciales de acceso ¿Qué software ha empleado el APT39 para obtener credenciales? Formato: Nombre de la herramienta (p.e. revelator) (80 puntos)

Exfiltración

10. Como analista del SOC (Security Operations Center) investiga el tráfico de red para determinar si hubo incidentes en tu organización. Usa tus conocimientos de Wireshark, analiza el archivo de captura exfiltracion.pcapng y constesta a las siguientes preguntas. Una vez descargado el archivo exfiltracion.pcapng, marca como respuesta OK y pasa a la siguiente pregunta. (25 puntos)
11. ¿Cuántos paquetes tiene la captura? (50 puntos)

12. ¿A qué hora se capturó el primer paquete?. NOTA: tiempo UTC y formato de respuesta: aaaa-mm-dd hh:mm:ss (50 puntos)
13. ¿Duración de la captura?. Formato: hh:mm:ss (50 puntos)
14. ¿Cuál es el equipo más activo a nivel de enlace?. Formato: xx:xx:xx:xx:xx:xx (50 puntos)
15. Fabricante de la NIC del segundo equipo más activo a nivel de enlace Formato: A.... C..... C... (50 puntos)
16. País donde está el cuartel general del fabricante de la NIC del segundo equipo más activo a nivel de enlace (50 puntos)
17. Teniendo en cuenta el modelo TCP/IP, ¿Qué protocolo de nivel de aplicación de la captura es el más activo? Formato: nombre del protocolo (siglas del protocolo) (50 puntos)
18. La organización trabaja con direccionamiento privado. ¿Cuántos equipos de la organización intervienen en la captura?. (75 puntos)
19. ¿Equipo más activo a nivel de red?. Formato: x.x.x.x <-- indica la IP (75 puntos)
20. ¿Cuántos paquetes tienen origen España? Formato: número de paquetes (p.e. 131) (100 puntos)
21. ¿Cuántos equipos usan IPs de Google? Formato: número de equipos (p.e. 131) (100 puntos)
22. Parece ser que el equipo 192.168.1.36 está implicado en algún incidente. ¿Cuál fue el primer comando ejecutado por el asaltante en el equipo víctima mediante la shell? (200 puntos)
23. Número del paquete en el que viaja el primer comando ejecutado por el asaltante en el equipo víctima mediante la shell (200 pts)
24. ¿Con qué usuario logró acceder el atacante en el equipo víctima? (200 pts)
25. ¿Contraseña del usuario con el que logró acceder el atacante en el equipo víctima? (200 pts)
26. ¿Esta conexión se correspondes con una bind shell o una reverse shell? Formato: indicar bind shell o reverse shell según corresponda (200 pts)
27. El atacante robó algún archivos del equipo 192.168.1.36. Recupera el pdf robado e indica cuál es el primer comando que aparece en la sección Networking de ese documento. Formato: n..... s..... (210 pts)
28. XMP Toolkit del pdf recuperado? Formato: Adobe XMP Core X.X-xxxx (210 pts)
29. Nombre de los programas que instalará el script robado de la máquina 192.168.1.36 Formato: nombre1, nombre2 (orde alfabético) (210 pts)
30. Se reportaron mas incidentes y hay sospechas de que el asaltante estableció un canal de mando y control empleando la técnica T1095 - Non-Application Layer Protocol. Sabiendo que en esta ocasión el contrincante descartó el uso del protocolo TCP, ¿en qué carpeta de la nueva víctima está situado? Formato: ruta absoluta (p.e. /hombre/manuel/Escritorio) (250 pts)
31. Indica el nombre de los dos usuarios activos presentes en el archivo exfiltradopor el canal de mando y control de la pregunta anterior Formato: nombre1, nombre2 (respetando el orden de aparición en el archivo exfiltrado) (250 pts)

Postexplotación

32. Sabemos que el equipo 10.10.4.64 está implicado en un incidente relacionado con la vulnerabilidad CVE-2021-44228 que permite la ejecución remota de código. Tu trabajo es abrir el archivo postexplotacion_CVE-2021-44228.pcapng y continuar la investigación para descubrir que acciones realizó el adversario. (0 pts)

33. Se sospecha que el atacante ha establecido un mecanismo de persistencia usando alguna de las subtécnicas de la técnica T1053 - Scheduled Task/Job de la matriz Mitre ATT&CK ¿Cada cuántos minutos contacta el equipo víctima con el equipo atacante? Formato: no de minutos (p.e. 10) (150 pts)
34. ¿Cuál es la IP del equipo del atacante al que llama la víctima regularmente? (150 pts)
35. El intruso crea el directorio lu2910312cgb.tmp/ imitando un directorio legítimo para pasar desapercibido. ¿Cuál es el ID de esta subtécnica según MITRE ATT&CK? Formato: Txxxx.xxx <-- indica el ID de laa subtécnica según la matriz MITRE ATT&CK (150 pts)
36. Qué herramienta o script de enumeración ha empleado el atacante? Formato: nombre de la herramienta o script (155 pts)
37. ¿Cuál es la versión del kernel de la máquina víctima? Formato: x.x.x-xx-generic (155 pts)
38. ¿Qué distribución Linux y versión está corriendo la máquina víctima? Formato: nombre xx.xx.x (155 pts)
39. Indica el nombre y versión del sistema gestor de base de datos instalado en el equipo víctima Formato: Nombre x.x.xx (p.e. Caixa 1.1.11) (155 pts)
40. ¿Cómo se llama el programa/script que se ejecuta para lograr la persistencia como usuario solr? Indica la ruta completa Formato: /xxx/xxxx/xxxxxx.xx (200 pts)
41. ¿Cuántos usuarios del sistema víctima tienen como shell /bin/bash? (200 pts)
42. ¿Qué vulnerabilidad aprovecha el atacante para promocionar a root? Formato: CVE-XXXX-XXXX (250 pts)
43. ¿Qué técnica de persistencia usa el atacante una vez que ha conseguido promocionar a root? Formato: Txxxx.xxx <-- indica el ID de la subtécnica según la matriz MITRE ATT&CK (250 pts)
44. Indica el n.o de paquete en el que se inicia una conexión ssh hacia la víctima desde una IP de la organización del atacante (250 pts)