XUNTA DE GALICIA

FORMACIÓN PROFESIONAL INNOVA

IES San Clemente **CIFP Rodolfo Ucha Piñeiro**

MITRE - C2C -Postexplotación

Ciberinteligencia

1. Vai á páxina web de MITRE ATT&CK. Unha vez na web de MITRE ATT&CK, marca como resposta OK e pasa á seguinte pregunta (5 puntos)
2. O framework ten unha lista de 19 técnicas baixo a táctica que busca manter o acceso nos teus sistemas. Cal é o ID da táctica? Formato: nº de ID (p.e. TA2222) (10 puntos)

   TA0003
3. Cantas técnicas caen baixo a táctica que empregan os adversarios para roubar datos da túa rede? Formato: número (p.e. 5) (00 puntos)

   9
4. Os teus sistemas de monitorización alertan da execución do software sqlmap. Atendendo ao mostrado na matriz MITRE, en que fase do ataque (técnica) atópase o atacante que executou o comando? Formato: ID (p.e. T2222) (15 puntos)

   T1190
5. Analizando logs atopas entradas asociadas ao porto 1058. De que grupo APT pódese tratar? Formato: nome do grupo (p.e. Iron Maiden) (60 puntos)

   Lazarus Group
6. Sospéitase que grupo *Sandworm Team* atacou en 2015 e 2016 compañías eléctricas e organismos do goberno de Ucraína.Ademais, crese que é o responsable do 'deface' duns 15.000 sitios web do goberno xeorxiano. Que acción de mitigación recomenda MITRE para este último tipo de ataque? Formato: nome da técnica de mitigación (p.e. Network Segmentation) (60 puntos)

   Data Backup
7. Entre novembro de 2019 e xaneiro de 2021 lanzouse unha campaña contra empresas metalúrxicas de países suramericanos, onde os adversarios enviaron correos electrónicos de phishing que incluían un documento PDF, que nalgúns casos levou á descarga e execución de malware. Dei un dos servizos de aloxamento lexítimos usados para aloxar ese malware? Formato: nome dun dos servizos de aloxamento (p.e. Megaupload) (60 puntos)

   OneDrive o MediaFire
8. Os grupos APT28, APT29, Dragonfly e Ember Bean crese que están financiados por Rusia. Valorándoos en conxunto, que técnica de mitigación propón MITRE para loitar contra a técnica de C2C máis empregada por estes grupos? Formato: ID da técnica de Mitigación (p.e. M2222) (80 puntos)

   M1031
9. Seguindo cos APTs ruso e centrándonos na técnica máis empregada por estes grupos para lograr credenciais de acceso. Que software empregou o APT39 para obter credenciais? Formato: Nome da ferramenta (p.e. revelator) (80 puntos)

Ncrack

Exfiltración

10. Como analista do SOC (Security Operations Center) investiga o tráfico de rede para determinar se houbo incidentes na túa organización. Usa os teus coñecementos de Wireshark, analiza o arquivo de captura exfiltracion.pcapng e resposta ás seguintes cuestións. Unha vez descargado o arquivo exfiltracion.pcapng, indica como resposta OK e pasa á seguinte pregunta.. (25 puntos)

    OK

11. Cantos paquetes ten a captura? (50 puntos)

    1057

12. A que hora capturouse o primeiro paquete?. NOTA: tempo UTC e formato de resposta: aaaa-mm-dd hh:mm: ss (50 puntos)

    2021-12-21 01:01:00

13. Duración da captura?. Formato: hh:mm:ss (50 puntos)

    01:02:26

14. Cal é o equipo máis activo a nivel de enlace?. Formato: xx:xx:xx:xx:xx:xx (50 puntos)

    08:00:27:5c:00:14

15. Fabricante da NIC do segundo equipo máis activo a nivel de enlace. Formato: A.... C..... C... (50 puntos)

    Askey Computer Corp

16. País onde está o cuartel xeral do fabricante da NIC do segundo equipo máis activo a nivel de enlace (50 puntos)

    Taiwan

17. Tendo en conta o modelo TCP/IP, Que protocolo de nivel de aplicación da captura é o máis activo? Formato: nome do protocolo (siglas do protocolo) (50 puntos)

    TLS

18. A organización traballa con direccionamento privado. Cantos equipos da organización interveñen na captura?. (75 puntos)

    6

19. ¿Equipo más activo a nivel de red?. Formato: x.x.x.x <-- indica la IP (75 puntos)

    192.168.1.36

20. Cantos paquetes teñen orixe España? Formato: número de paquetes (p.e. 131) (100 puntos)

    291

21. Cantos equipos usan IPs de Google? Formato: número de equipos (p.e. 131) (100 puntos)

    3

22. Parece ser que o equipo 192.168.1.36 está implicado nalgún incidente. Cal foi o primeiro comando executado polo asaltante no equipo vítima mediante shell? (200 puntos)

    whoami

23. Nº do paquete no que viaxa o primeiro comando executado polo asaltante no equipo vítima mediante a shell (200 pts)

4

24. Con que usuario logrou acceder o atacante no equipo vítima? (200 pts)

    manuel

25. Contrasinal do usuario co que logrou acceder o atacante no equipo vítima? (200 pts)

    abc123.

26. Esta conexión correspóndese cunha bind shell ou cunha reverse shell? Formato: indicar bind shell ou reverse shell segundo corresponda (200 pts)

    reverse shell

27. O atacante roubou algúns arquivos do equipo 192.168.1.36. Recupera o pdf roubado e indica cal é o primeiro comando que aparece na sección Networking dese documento. Formato: n..... s..... (210 pts)

    networkctl status

28. XMP Toolkit do pdf recuperado? Formato: Adobe XMP Core X.X-xxxx (210 pts)

    Adobe XMP Core 5.6-c148

29. Nome dos programas que instalará o script roubado da máquina 192.168.1.36. Formato: nome1, nome2 (orde alfabético) (210 pts)

    apache, htop

30. Reportáronse mais incidentes e hai sospeitas de que o asaltante estableceu unha canle de mando e control empregando a técnica *T1095 - Non-Application Layer Protocol*. Sabendo que nesta ocasión o adversario descartou o uso do protocolo TCP, en qué carpeta da nova vítima está situado? Formato: ruta absoluta (p.e. /hombre/manuel/Escritorio) (250 pts)

    /home/magasix/Descargas

31. Indica o nome dos dous usuarios activos presentes no arquivo exfiltrado pola canle de mando e control da pregunta anterior. Formato: nome1, nome2 (respectando o orde de aparición no arquivo exfiltrado) (250 pts)

    magasix, ctfd

Postexplotación

32. Sabemos que o equipo 10.10.4.64 está implicado nun incidente relacionado coa vulnerabilidade CVE-2021-44228 que permite a execución remota de código. O teu traballo é abrir o arquivo postexplotacion_CVE-2021-44228.pcapng e continuar a investigación para descubrir que accións realizou o adversario. Unha vez descargado o arquivo postexplotacion_CVE-2021-44228, indica como resposta OK e pasa á seguinte pregunta.. (0 pts)

    OK

33. Sospéitase que o atacante estableceu un mecanismo de persistencia usando algunha das subtécnicas da técnica T1053 - Scheduled Task/Job da matriz Mitre ATT&CK. Cada cantos minutos contacta o equipo vítima co equipo atacante? Formato: nº de minutos (p.e. *10*) (150 pts)

    1

34. Cal é a IP do equipo do atacante ao que chama a vítima regularmente? (150 pts)

    172.45.176.1

35. O intruso crea o directorio lu2910312cgb.tmp/ imitando un directorio lexítimo para pasar desapercibido. Cal é o ID desta subtécnica según MITRE ATT&CK? Formato: Txxxx.xxx <-- indica o ID da subtécnica segundo a matriz MITRE ATT&CK (150 pts)

    T1036.005

36. Que ferramenta ou script de enumeración empregou o atacante? Formato: nome da ferramenta ou script (155 pts)

    linpeas

37. Cal é a versión do kernel da máquina vítima? Formato: x.x.x-xx-generic (155 pts)

    5.4.0-81-generic

38. Que distribución Linux e versión está a correr a máquina vítima? Formato: nombre xx.xx.x (155 pts)

    Ubuntu 20.04.3

39. Indica o nome e versión do sistema xxestor de base de datos instalado no equipo vítima Formato: Nombre x.x.xx (p.e. Caixa 1.1.11) (155 pts)

    Mysql 8.0.29

40. Como se chama o programa/script que se executa para lograr a persistencia como usuario solr? Indica a ruta completa. Formato: /xxx/xxxx/xxxxxx.xx (200 pts)

    /var/solr/backup.sh

41. Cantos usuarios do sistema vítima teñen como shell /bin/bash? (200 pts)

    3

42. Que vulnerabilidade aproveita o atacante para promocionar a root? Formato: CVE-XXXX-XXXX (250 pts)

    CVE-2021-4034

43. Que técnica de persistencia usa o atacante unha vez que conseguiu promocionar a root? Formato: Txxxx.xxx <-- indica o ID da subtécnica segundo a matriz MITRE ATT& CK (250 pts)

    T1098.004

44. Indica o n.º de paquete no que se inicia unha conexión ssh cara á vítima desde unha IP da organización do atacante (250 pts)

    8448