Guía de uso – Script de Auditoría del Sistema (Blue Team)

Este script ejecuta una auditoría básica del sistema desde la línea de comandos. Recolecta información sobre usuarios, puertos abiertos y servicios del sistema de manera automática.

Características principales

El script realiza tres tareas de auditoría:

Listado de usuarios del sistema

Obtiene los usuarios configurados en el sistema operativo, tanto en Windows como Linux.

Escaneo de puertos comunes (TCP)

Verifica los puertos más utilizados (21, 22, 80, 443, 3389, etc.) dentro del host especificado en la variable TARGET_IP.

Listado de servicios activos

Recupera los servicios ejecutándose en el sistema mediante systemctl (Linux) o sc query (Windows).

Uso del script

El script está preparado para ser ejecutado directamente desde consola. Funciona sin argumentos externos gracias a que la IP objetivo se define dentro del archivo.

1. Establecer la IP objetivo

Dentro del código modificar:

TARGET_IP = "127.0.0.1"

Puede ser:

La IP local

La IP de una máquina virtual

Una IP remota (si la red lo permite)

2. Ejecutar el script

Ubicarse en el directorio donde se encuentra el archivo os_audit.py:

cd ruta/del/archivo

Ejecutar:

python os_audit.py

Resultados que genera

El script mostrará en pantalla:

Lista de usuarios del sistema

Puertos abiertos entre los más comunes

Lista completa de servicios en ejecución

Al finalizar imprime:

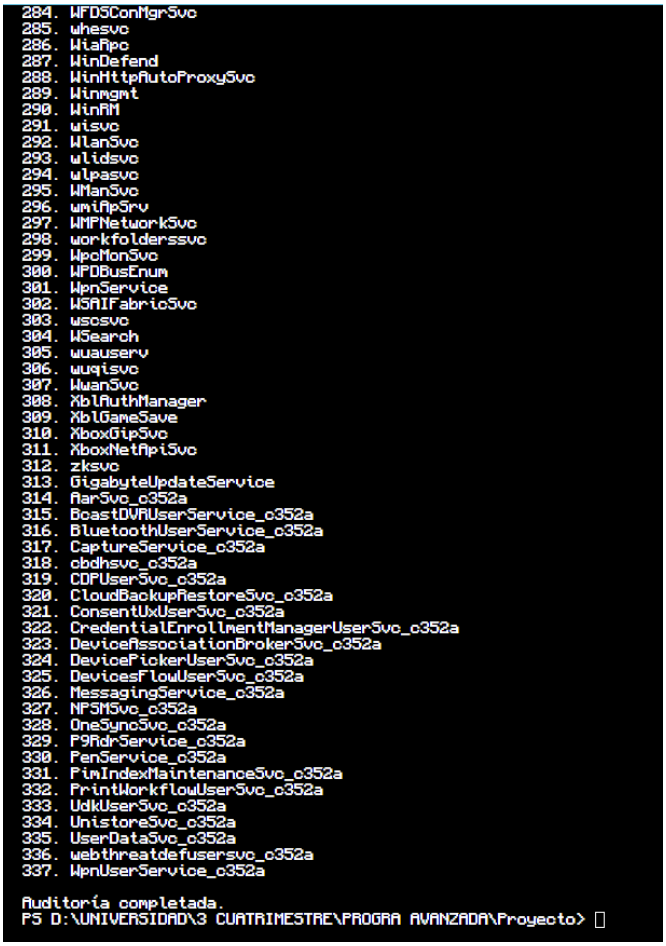
Auditoría completada.

```
PS D:\UNIVERSIDAD\3 CUATRIMESTRE\PROGRA AVANZADA\Proyecto> python os_audit.py
---------- Informacion del sistema ----------

===== USUARIOS DEL SISTEMA =====
'net' is not recognized as an internal or external command,
operable program or batch file.

===== PUERTOS ABIERTOS EN 127.0.0.1 =====
• Puerto 53
• Puerto 135
• Puerto 445

===== SERVICIOS DEL SISTEMA =====
1. AcrylicDNSProxySvc
2. ADPSvc
3. ALG
4. AnyDesk
5. AorusLcdService
6. AppIDSvc
7. Appinfo
8. AppMgmt
9. AppReadiness
10. AppVClient
11. AppXSvc
12. Apx3vc
13. asComSvc
14. AssignedAccessManagerSvc
15. asus
16. AsusCertService
17. asusm
18. AsusROGLSLService
19. AudioEndpointBuilder
20. Audiosrv
21. autotimesvc
22. AxInstSV
23. battlenet_helpersvc
24. BDESVC
25. BEService
26. BFE
27. BITS
28. Bonjour Service
29. BrokerInfrastructure
30. BTAGService
31. BthAvctpSvc
32. bthserv
33. camsvc
34. CCleanerPerformanceOptimizerService
35. CDPSvc
36. CertPropSvc
37. ClickToRunSvc
38. ClipSVC
39. cloudidsvc
40. COMSysApp
41. CoreMessagingRegistrar
42. cplspcon
43. CryptSvc
44. CscService
45. DcomLaunch
```


284. WFDSConMgrSvc
285. whesvc
286. WiaRpc
287. WinDefend
288. WinHttpAutoProxySvc
289. Winmgmt
290. WinRM
291. wisvc
292. WlanSvc
293. wlidsvc
294. wlpasvc
295. WManSvc
296. wmiApSrv
297. WMPNetworkSvc
298. workfolderssvc
299. WpcMonSvc
300. WPDBusEnum
301. WpnService
302. W5AIFabricSvc
303. wscsvc
304. WSearch
305. wuauserv
306. wuqisvc
307. WwanSvc
308. XblAuthManager
309. XblGameSave
310. XboxGipSvc
311. XboxNetApiSvc
312. zksvc
313. GigabyteUpdateService
314. AarSvc_c352a
315. BcastDVRUserService_c352a
316. BluetoothUserService_c352a
317. CaptureService_c352a
318. cbdhsvc_c352a
319. CDPUserSvc_c352a
320. CloudBackupRestoreSvc_c352a
321. ConsentUxUserSvc_c352a
322. CredentialEnrollmentManagerUserSvc_c352a
323. DeviceAssociationBrokerSvc_c352a
324. DevicePickerUserSvc_c352a
325. DevicesFlowUserSvc_c352a
326. MessagingService_c352a
327. NPSMSvc_c352a
328. OneSyncSvc_c352a
329. P9RdrService_c352a
330. PenService_c352a
331. PimIndexMaintenanceSvc_c352a
332. PrintWorkflowUserSvc_c352a
333. UdkUserSvc_c352a
334. Unistore5vc_c352a
335. UserDataSvc_c352a
336. webthreatdefusersvc_c352a
337. WpnUserService_c352a
Auditoría completada.
PS D:\UNIVERSIDAD\3 CUATRIMESTRE\PROGRA AVANZADA\Proyecto>

Guía de uso Scanner de Nmap, Red Team.

Este script es un wrapper de Nmap que permite realizar escaneos de red de forma interactiva mediante línea de comandos.

Características principales:

La clase NetworkScanner gestiona la ejecución de Nmap con diferentes perfiles predefinidos. Cada escaneo genera tres archivos de salida: XML, TXT y JSON con metadatos del escaneo.

Los perfiles disponibles son:

- stealth: Escaneo sigiloso TCP SYN
- version: Detección de versiones de servicios
- aggressive: Escaneo completo con detección de OS
- quick: Escaneo rápido de puertos comunes
- comprehensive: Escaneo exhaustivo con scripts NSE

Uso del argparse:

El argumento target permite especificar una IP o hostname individual. Como alternativa, target_file permite cargar múltiples objetivos desde un archivo de texto.

El parámetro scan_type define el perfil de escaneo a utilizar. Por defecto usa el modo stealth.

El argumento ports permite especificar puertos específicos en formato individual (22,80,443) o rango (1-1000).

El parámetro output_dir define dónde se guardarán los resultados.

Ejemplos:

Escaneo básico: python scanner.py -t 192.168.1.1

Escaneo con detección de versiones en puertos específicos: python scanner.py -t 192.168.1.1 -s version -p 22,80,443

Escaneo de múltiples objetivos: python scanner.py -T targets.txt -s quick

El script incluye manejo de errores para timeouts, Nmap no instalado, y archivos no encontrados. Los resultados se organizan con timestamps para mantener un historial de escaneos.

```
┌──(jander㉿Lolo)-[~/Documentos]
└─$ python scanner.py -t 192.168.1.0/24 -s version -p 22,80,
[*] Ejecutando: nmap -sV -T4 -Pn -p 22,80, 192.168.1.0/24 -oX scan_results/192.168.1.0_24_20251105_113911.xml -oN scan_results/192.168.1.0_24_20251105_113911.txt
[*] Target: 192.168.1.0/24
[*] Tipo de scan: version
[*] Guardando resultados en: scan_results
[+] Scan completado exitosamente
[+] Resultados guardados:
   - XML: scan_results/192.168.1.0_24_20251105_113911.xml
   - TXT: scan_results/192.168.1.0_24_20251105_113911.txt
   - JSON: scan_results/192.168.1.0_24_20251105_113911.json
```

```
# Nmap 7.95 scan initiated Wed Nov  5 11:39:11 2025 as: /usr/lib/nmap/nmap --privileged -sV -T4 -Pn -p 22,80, -oX scan_results/192.168.1.0_24_20251105_113911.xml -oN scan_results/192.168.1.0_24_20251105_113911.txt 192.168.1.0/24
Nmap scan report for 192.168.1.0
Host is up.

PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
80/tcp filtered http

Nmap scan report for 192.168.1.1
Host is up.

PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
80/tcp filtered http

Nmap scan report for 192.168.1.2
Host is up.

PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
80/tcp filtered http

Nmap scan report for 192.168.1.3
Host is up.

PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
80/tcp filtered http

Nmap scan report for 192.168.1.4
Host is up.

PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
80/tcp filtered http

Nmap scan report for 192.168.1.5
Host is up.

PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
80/tcp filtered http

Nmap scan report for 192.168.1.6
```