SANTA LOGS

Descargamos el zip de la plataforma de los

amigos de The Hackers Labs.

Nos aparece 1 .pdf)

Leemos el pdf

"La Gran Patrulla de Santa Logs"
En el Polo Norte, los elfos tienen mucho trabajo asegurándose de que todo funcione correctamente en la noche de Navidad. Sin embargo, algo
extraño ha comenzado a suceder en el sistema
informático de Santa Claus.
Todo comenzó cuando los
trolls traviesos, enemigos naturales de
los elfos, lograron infiltrarse en la
Red de Regalos 3000, ¡el
sistema principal que rastrea quién ha sido bueno o malo! Al principio, solo cambiaron pequeñas listas: regalaron carbón a niños que habían sido ejemplares y juguetes a los más traviesos.
Pero luego, ¡las cosas se salieron de control!
Los
elfos técnicos pidieron ayuda a "Santa Logs", un equipo de
élite compuesto por Santa Claus, su reno Rodolfo (experto en

redes) y un grupo de elfos rastreadores. La misión es clara:
A saber
Login : santa
Password : Cl@us
1.
Revisar los logs del sistema para descubrir cuándo , dónde , cómo se infiltraron los trolls.
2.
Encontrar el virus escondido en el sistema, una trampa que los trolls dejaron para sabotear la operación de entrega de regalos. Este virus contiene una flag secreta que debes descubrir para eliminarlo y restablecer el sistema.
3.
Restablecer el sistema antes de la medianoche del 24 de diciembre, ¡de lo contrario, el trineo se quedará sin energía y no podrá despegar!

LOCALIZACIÓN

```
sudo arp-scan --interface eth0 -l

192.168.0.13   08:00:27:6b:19:17      PCS Systemtechnik GmbH
```

CONECTIVIDAD

```
ping -c1 192.168.0.13
```

```
└─# ping -c1 192.168.0.13
PING 192.168.0.13 (192.168.0.13) 56(84) bytes of data.
64 bytes from 192.168.0.13: icmp_seq=1 ttl=128 time=0.864 ms

── 192.168.0.13 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.864/0.864/0.864/0.000 ms
```

ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 192.168.0.13 -T 2
```

```
└─# nmap -p- -Pn -sVCS --min-rate 5000 192.168.0.13 -T 2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-15 18:24 EST
Nmap scan report for 192.168.0.13
Host is up (0.00098s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49668/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:6B:19:17 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -14s, deviation: 0s, median: -14s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: WIN-VRU3GG3DPLJ, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:6b:19:17 (Oracle VirtualBox virtual NIC)
| smb2-time:
|   date: 2024-12-15T23:26:55
|_  start_date: 2024-12-15T22:55:15
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```

ENUMERACIÓN

En el puerto 445, disponemos de un servicio SMB, por lo que

primero que haremos es validar las credenciales con crackmapexec

crackmapexec smb 192.168.0.13 -u 'santa' -p 'Cl@us'

Con el propio crackmapexec, listamos los recursos compartidos

crackmapexec smb 192.168.0.13 -u santa -p Cl@us --shares

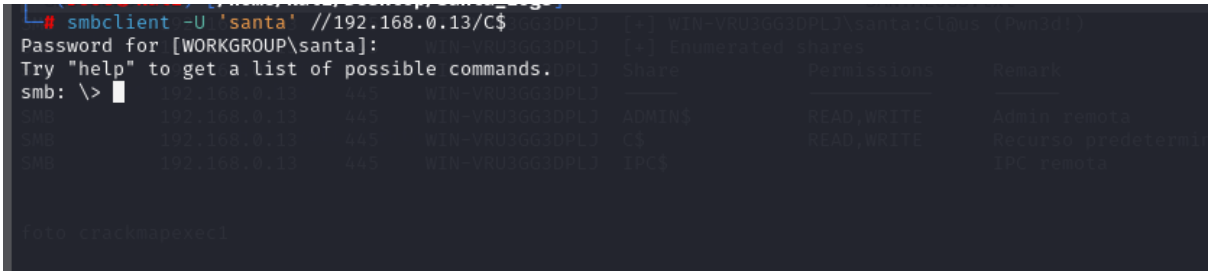
```
└─# crackmapexec smb 192.168.0.13 -u 'santa' -p 'Cl@us'
SMB         192.168.0.13    445    WIN-VRU3GG3DPLJ  [*] Windows Server 2016 Datacenter 14393 x64 (name:WIN-VRU3GG3DPLJ) (domain:WIN-VRU3GG3DPLJ) (signing:F
alse) (SMBv1:True)
SMB         192.168.0.13    445    WIN-VRU3GG3DPLJ  [+] WIN-VRU3GG3DPLJ\santa:Cl@us (Pwn3d!)
```

```
└─# crackmapexec smb 192.168.0.13 -u santa -p Cl@us --shares
SMB         192.168.0.13    445    WIN-VRU3GG3DPLJ  [*] Windows Server 2016 Datacenter 14393 x64 (name:WIN-VRU3GG3DPLJ) (domain:WIN-VRU3GG3DPLJ) (signing:
False) (SMBv1:True)
SMB         192.168.0.13    445    WIN-VRU3GG3DPLJ  [+] WIN-VRU3GG3DPLJ\santa:Cl@us (Pwn3d!)
SMB         192.168.0.13    445    WIN-VRU3GG3DPLJ  [+] Enumerated shares
SMB         192.168.0.13    445    WIN-VRU3GG3DPLJ  Share           Permissions     Remark
SMB         192.168.0.13    445    WIN-VRU3GG3DPLJ  -----           -----------     ------
SMB         192.168.0.13    445    WIN-VRU3GG3DPLJ  ADMIN$          READ,WRITE      Admin remota
SMB         192.168.0.13    445    WIN-VRU3GG3DPLJ  C$              READ,WRITE      Recurso predeterminado
SMB         192.168.0.13    445    WIN-VRU3GG3DPLJ  IPC$                            IPC remota
```

Ahora, enumerados los recursos, con smbclient podemos

acceder a cada recurso

smbclient -U 'santa' //192.168.0.13/C$



Siguiendo las pautas del reto,sabemos que los logs, comúnmente,

están en la siguiente ruta \Windows\System32\winevt\Logs

```
smbclient -U 'santa' //192.168.0.13/C$
Password for [WORKGROUP\santa]:
Try "help" to get a list of possible commands.
smb: \> cd \Windows\System32\winevt\Logs
smb: \Windows\System32\winevt\Logs\> dir
```

estracto

```
  Santalogs.evtx                A       69632  Wed Dec 11 05:36:45 2024
  Security.evtx                 A    20975616  Tue Dec 17 02:43:04 2024
  Setup.evtx                    A       69632  Wed Dec 11 05:58:33 2024
  SMSApi.evtx                   A       69632  Wed Dec 11 05:45:33 2024
```

Nos traemos a local el Santalogs.evtx

```
smb: \Windows\System32\winevt\Logs\> get Santalogs.evtx
```

Con la herramienta evtx_dump.py, cambiamos a .txt

```
evtx_dump.py Santalogs.evtx > archivo.txt
```

Analizamos el archivo.txt

```
cat archivo.txt
```

Admin Note: The temporary access key is 'FTP25_SMB192.168.1.101'

Elf Report: Naughty Virus detected! Santa's logs have been tampered with!

Elf Alert: Suspicious script 'malicious_script.py' detected in C:\tmp. It

seems to require a special key for decryption! login attempt for user: user23'

Recapitulando un poco:

-tenemos un script en /tmp

-una clave en FTP25_SMB192.168.1.101

- usamos el comando grep para ir buscando las respuestas del reto.

- ejecutamos el script que me pide la clave

python3 malicious_script.py
Introduce la clave AES:

[+] Mensaje desencriptado: FLAG: oscar_feliz_navidad

🖖 **Buen día.**