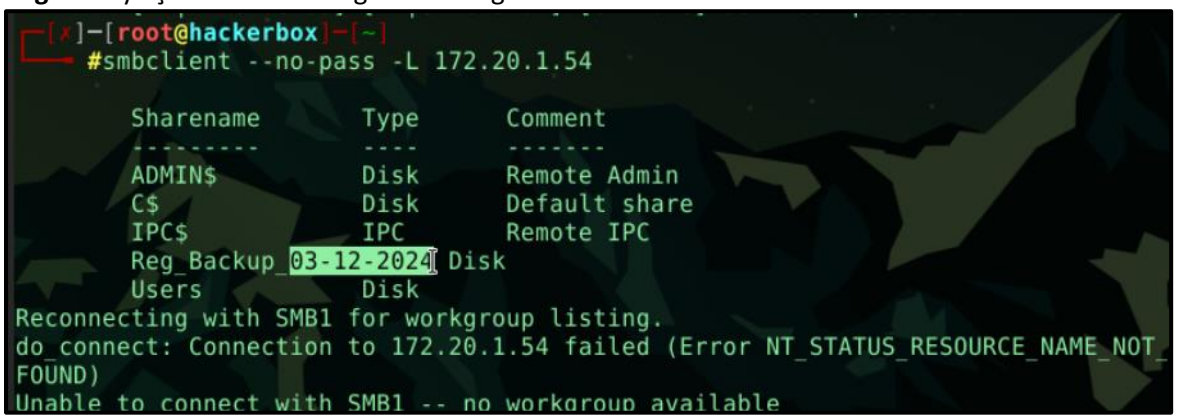
MOONSHADE ISINMASI

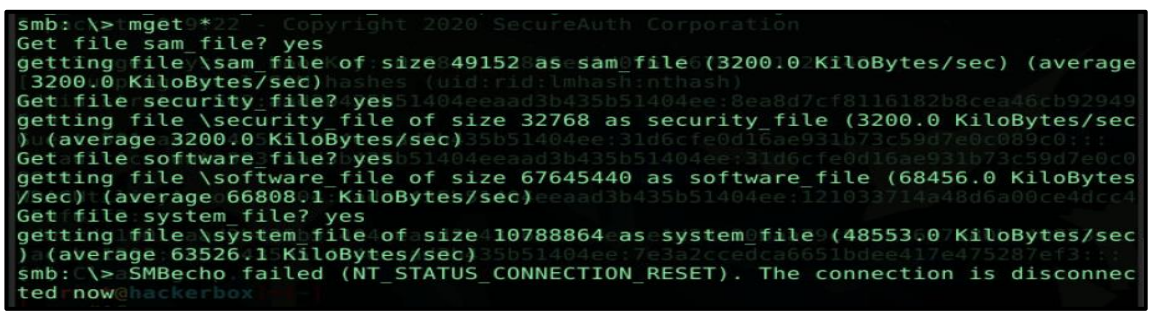
INFO: SAM dosyası, sistemdeki kullanıcı hesaplarının parola hash bilgilerini içeren bir veritabanıdır.

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

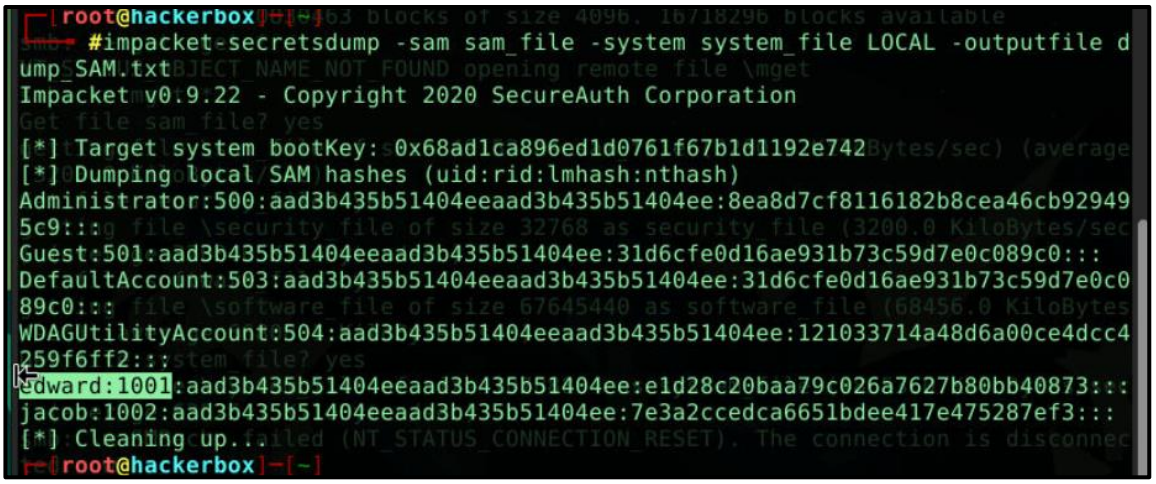
1. *SMB ile paylaşılan registry yedeğinin tarihi nedir?*
   Bilgi: smbye şifresiz olarak bağlanılır ve öğrenilir.



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 çıkartır.
   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.

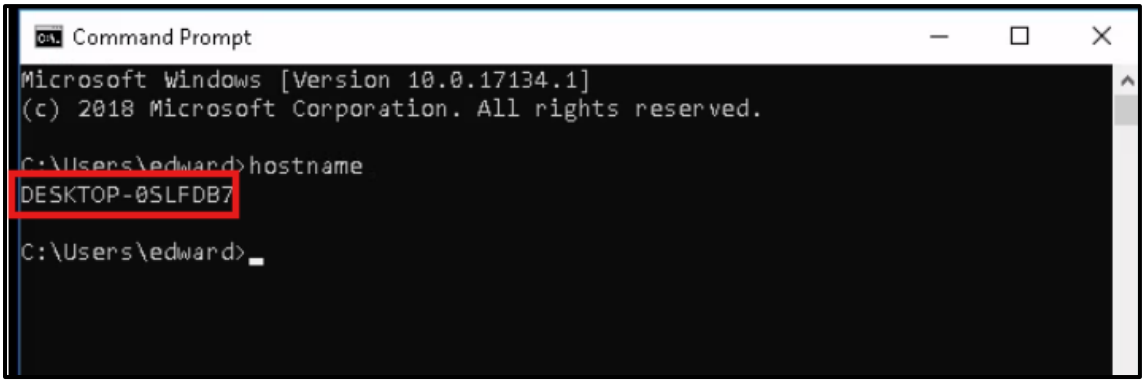


Sonuca ulaşılır.



3. *edward kullanıcısının parolası nedir?*
   Bilgi: hashcat ile parola çözülür.

4. *Bilgisayarın adı nedir?*
   Bilgi: remmina ile rdp yapılır ve hostname komutu ile öğrenilir.



5. *edward kullanıcısının company.hackviser.space'deki kullanıcı adı nedir?*
   Bilgi: Write-up okunarak çözülmüştür.