**Kali Live'den SAM Dosyasını Çekme**

(+) *Bu belgedeki işlemler birebir denenmiştir ve başarıyla uygulanmıştır.*

Bu yazıda Windows kurulu makinayı Kali live USB diski ile başlatıp Windows'taki SAM dosyasını çekme anlatılacaktır. Tüm bu süreç boyunca kullanılan işletim sistemleri şunlar olacaktır:

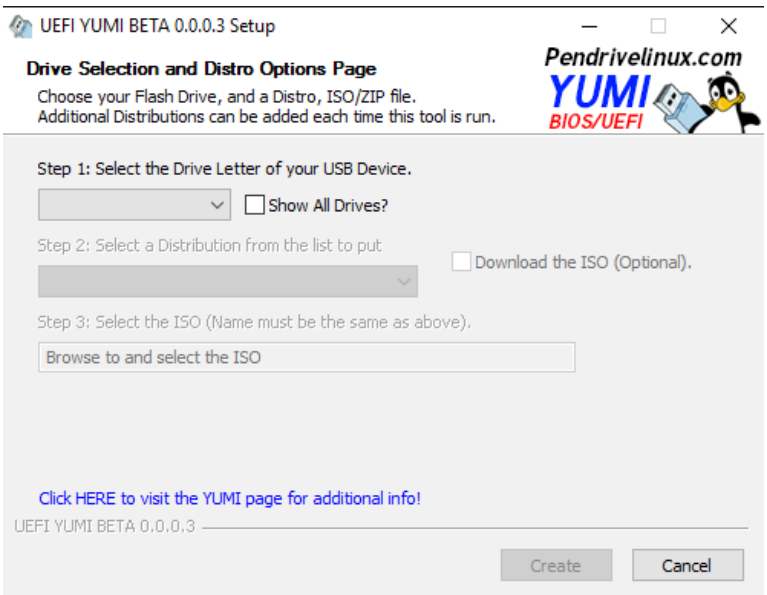
- Windows 10 // Hedef Sistem
- Kali Live 2016 // Hedef Sistemi Boot Edecek İşletim Sistemi

Öncelikle yapılacak adımlardan bahsedelim ve sonra bu adımları teker teker uygulayalım. İlk olarak kendi sistemimizde USB diskimizi Kali iso'su ile bootable yapacağız. USB diskimiz hazırlandıktan sonra yakın çevrede erişim imkanımız olan bir sistemi hedef seçeceğiz ve USB diskimiz ile hedef sistemi boot edeceğiz. Daha sonra Kali Live ile boot ettiğimiz hedef sistemin terminalinden hedef sistemin HDD'si üzerindeki partition'larını listeleyeceğiz ve içlerinden Windows'a ait olan partition'ı Kali Live'deki bir klasöre mount edeceğiz. Sonra o klasörden Windows'un SAM dosyasını barındıran dizine geçip pwdump tool'u ile SAM dosyasını çekeceğiz. Böylece boot ettiğimiz hedef sistemdeki Windows hesap özetlerini (hash'lerini) elde etmiş olacağız.

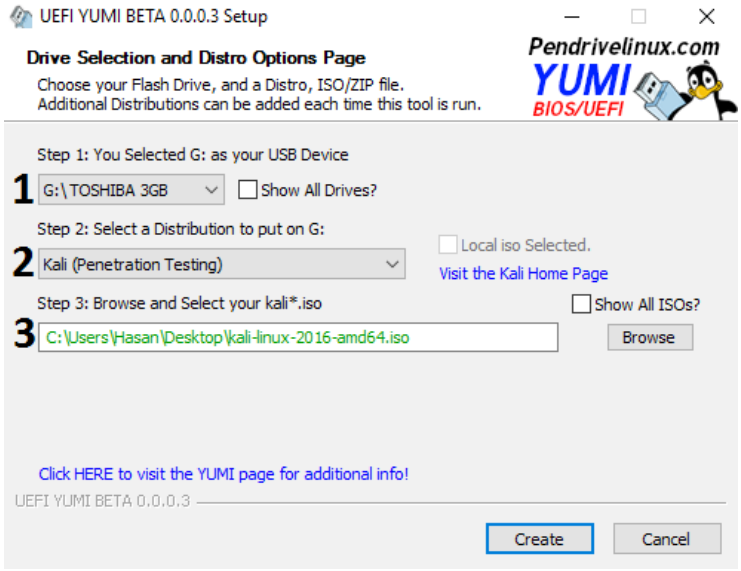
Not: pwdump tool'u bkhive ve samdump2 tool'unun birleşimi mahiyetinde olan bir tool'dur. Kali 2016'yla beraber bkhive tool'u artık gelmediğinden pwdump tool'u kullanımı tercih edilmiştir.

Şimdi anlatılanları birer birer uygulayalım. Öncelikle USB diskimizi kendi sistemimizde bir yazılım ile hazır hale getirelim. UEFI kullanan sistemler Kali gibi linux dağıtımlarını boot edemedikleri için USB diskimizi UEFI sistemlerinde uygun şekilde boot ettirecek YUMI UEFI yazılımını kullanalım.

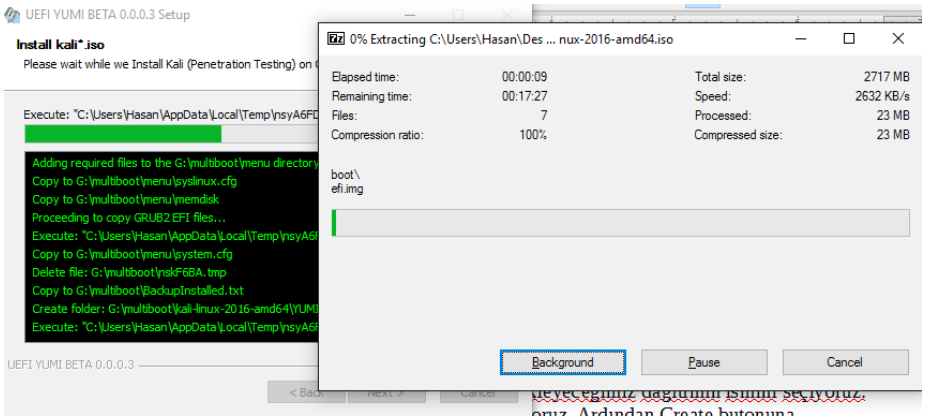
UEFI YUMI Beta exe'sini çalıştırdığımızda aşağıdaki ekran bizi karşılayacaktır (Not: exe dosyasına Windows'taki Not Köşem/Pentest Yazılımları dizininden erişebilirsin):



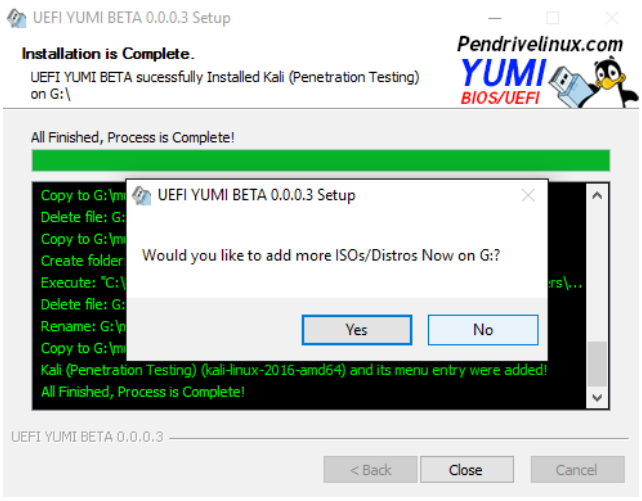
Gelen ekrandaki select box’ları aşağıdaki gibi dolduralım.




1. maddede USB diskimizi seçiyoruz. İkinci maddede yükleyeceğimiz dağıtımın ismini seçiyoruz. Üçüncü maddede Browse ile Kali 2016 iso’sunu seçiyoruz. Ardından Create butonuna tıklıyoruz.

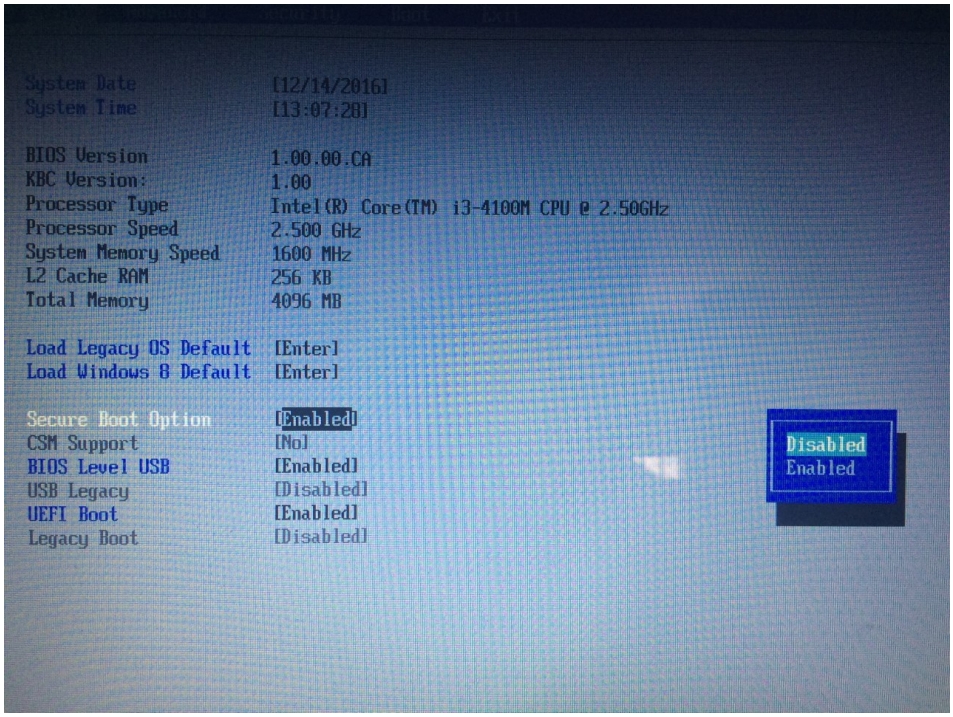



Yükleme sonrası gelen dialog box’a No diyoruz.

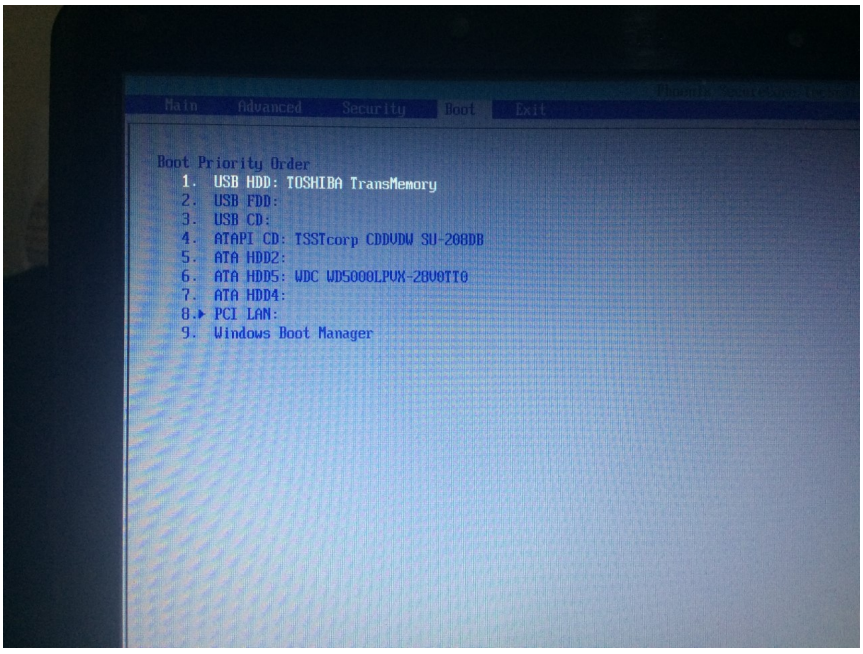


Böylece USB diskimiz UEFI sistemlere uygun bir şekilde hazırlanmış olur. Şimdi gözümüze kestirdiğimiz yakın çevredeki bir bilgisayara USB diskimizi takalım ve hedef sistemi USB belleğimizle başlatalım.

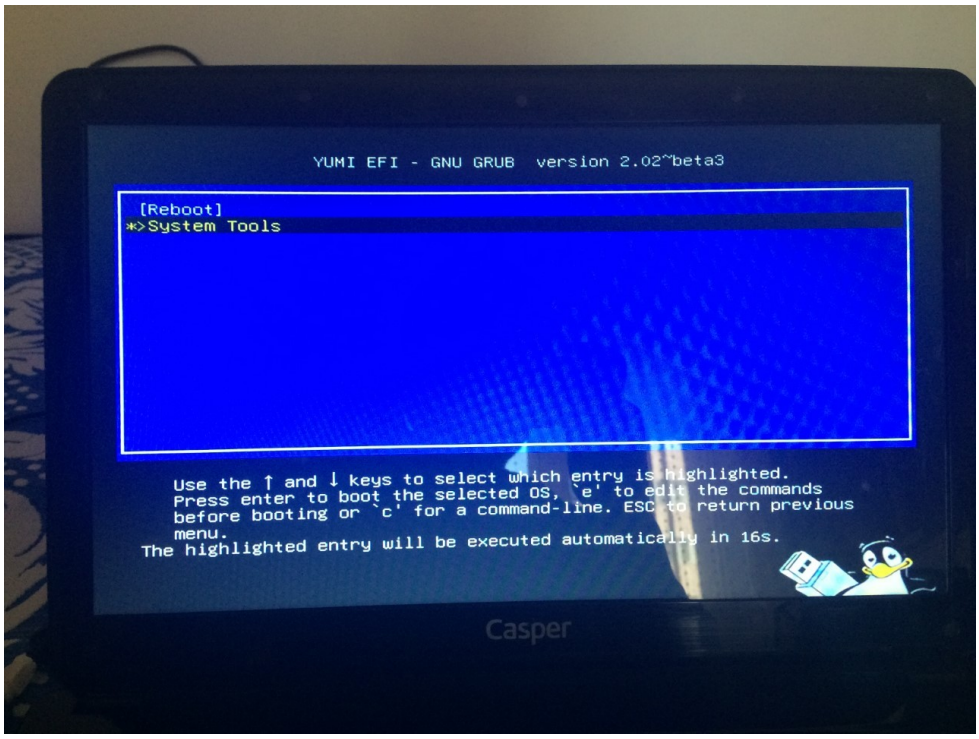
Diyelim ki gözümüze kestirdiğimiz bilgisayar annemin Casper laptop'ı olsun. Gizlice annemin laptop'ını açalım ve F2 tuşuna basılı tutarak BIOS ekranını açalım. Oradan Secure Boot seçeneğini Disabled edelim.



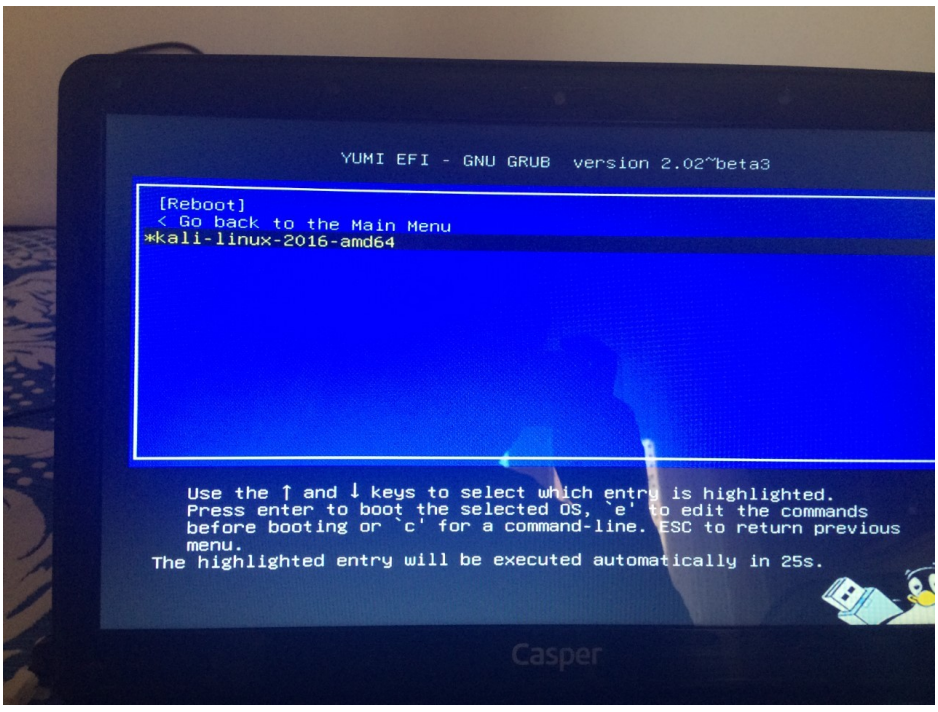

Ardından USB diskimizi boot edilecekler listesinde en üste çıkaralım.



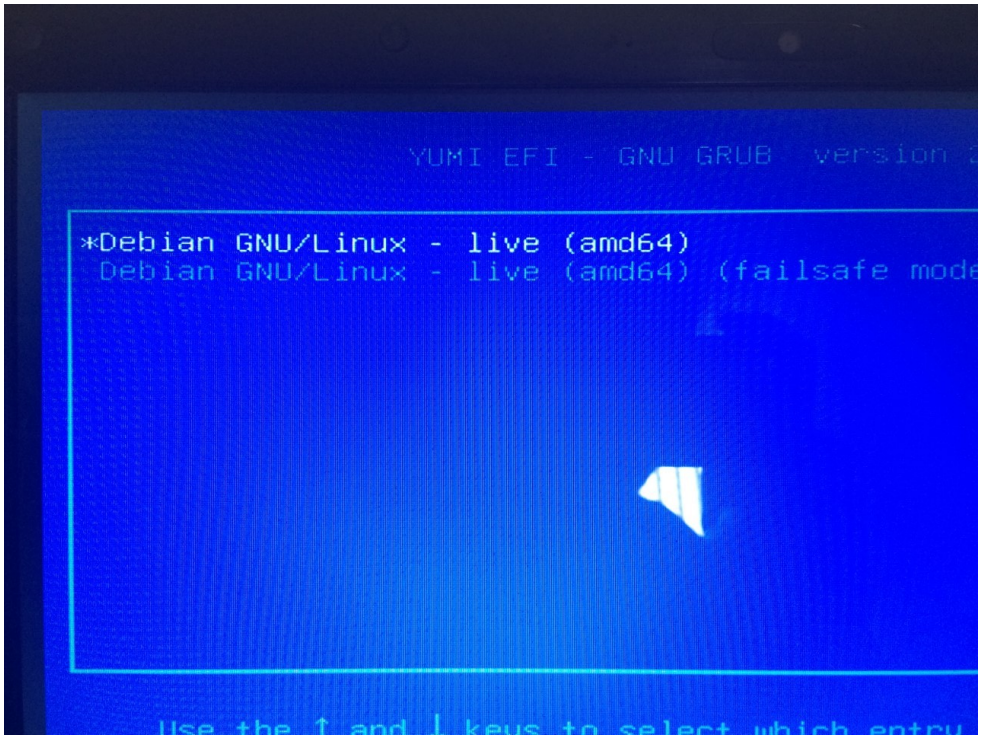
Böylece hedef sistem USB diskimizi boot etmeye hazır hale gelmiş olur. Şimdi USB diskimiz hedef sisteme takılıyken sistemi restart'layalım. Restart işlemi sonrası bizi YUMI yazılımının USB diskimize koyduğu Grub ekranı karşılayacaktır.



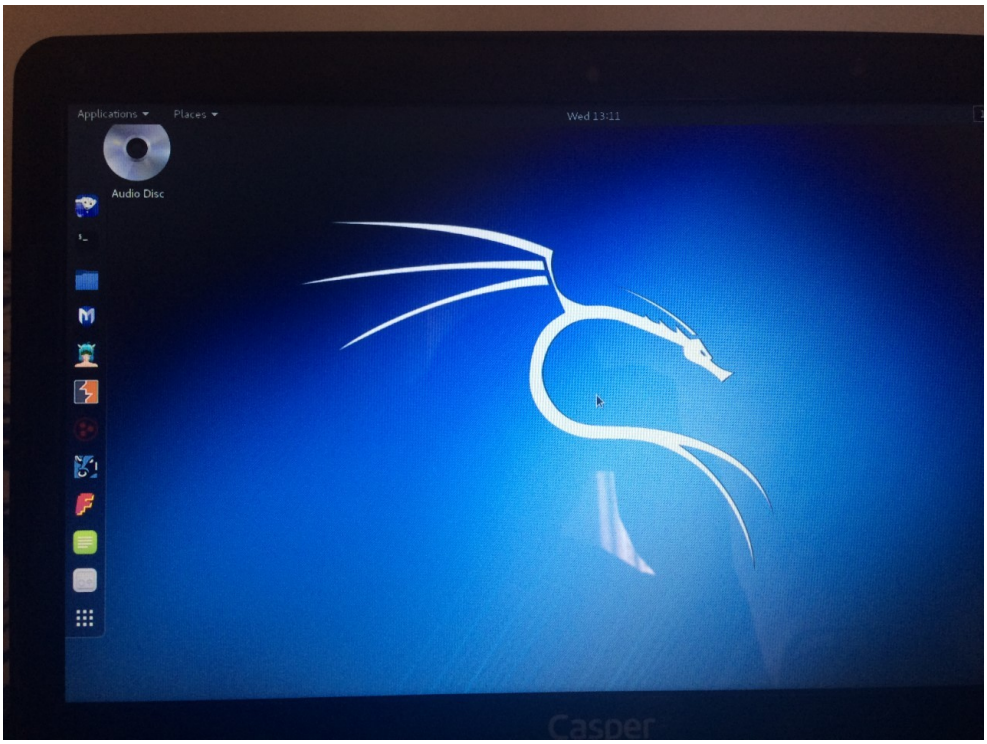

Ekrana gelen System Tools seçeneğine tıklayalım. Sonra akabinde gelen kali-linux-2016-amd64 seçeneğine tıklayalım.



Son olarak da Debian-Linux Live (amd64) seçeneğine tıklayalım.

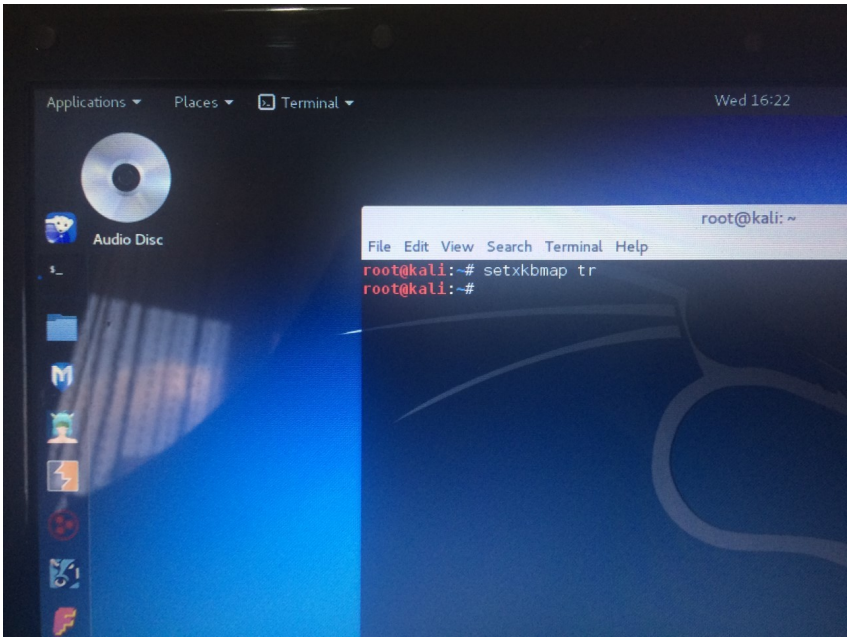



Böylece Kali Live hedef sistemde başlayacaktır.



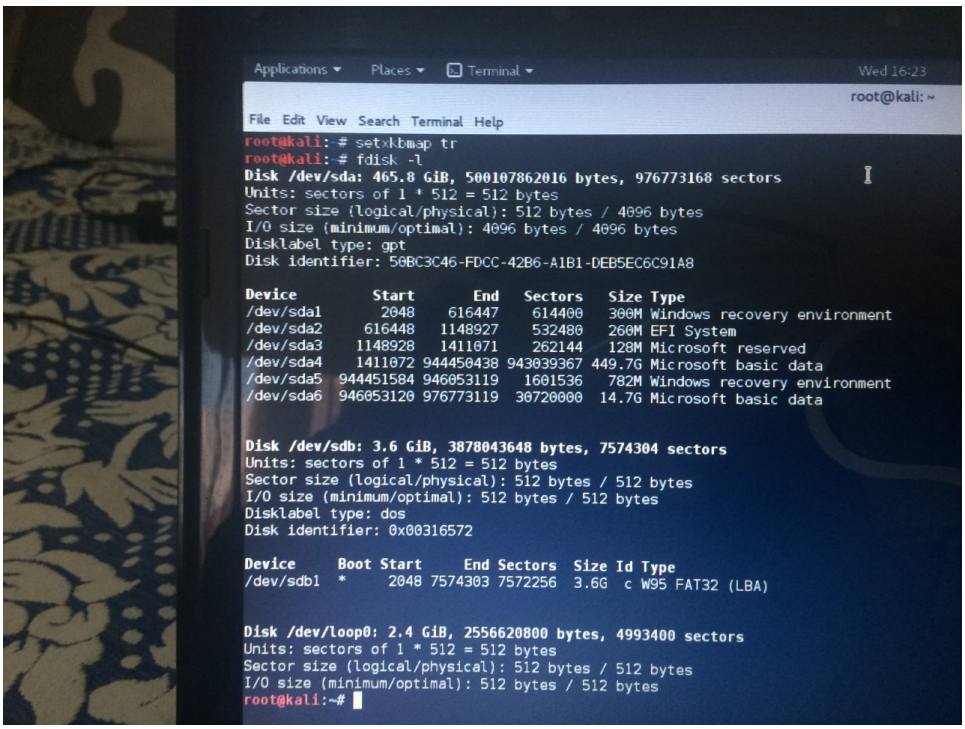
Hedef sistemi Kali Live ile başlattığımıza göre şimdi yapılacaklar hedef sistemin hdd'sindeki Windows partition'ınını bulmak, Kali Live'e mount etmek ve SAM dosyasını çekmektir. Bunları yapmaya başlamadan önce klavyemiz US olacağından kodları yazarken kolaylık olsun diye klavye ayarını TR yapalım.

> setxkbmap tr



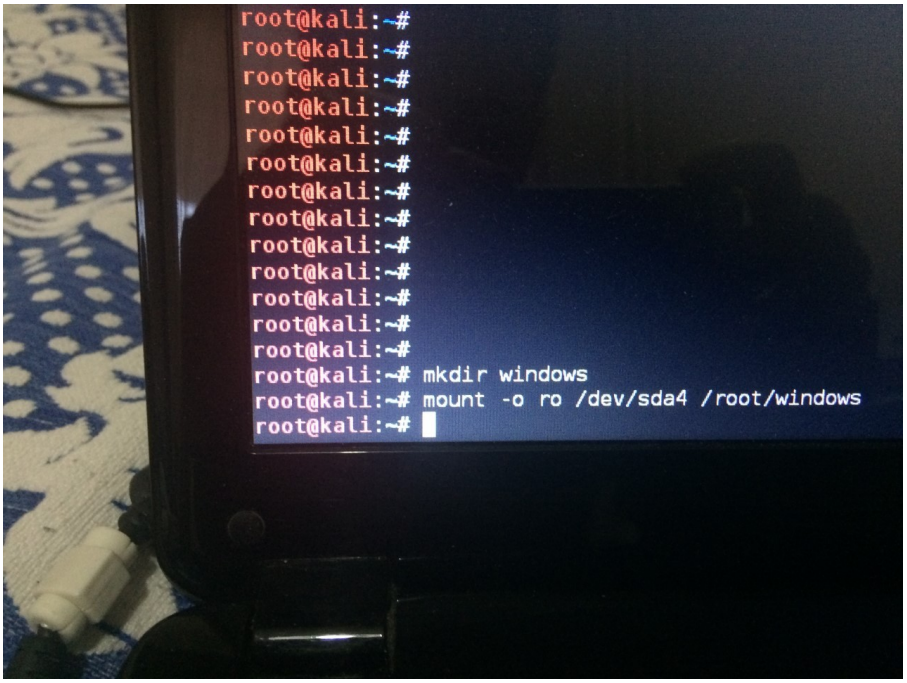

Sonra boot ettiğimiz hedef sistemin Windows partition'ını bulmak için fdisk tool'unu kullanalım.

> fdisk -l



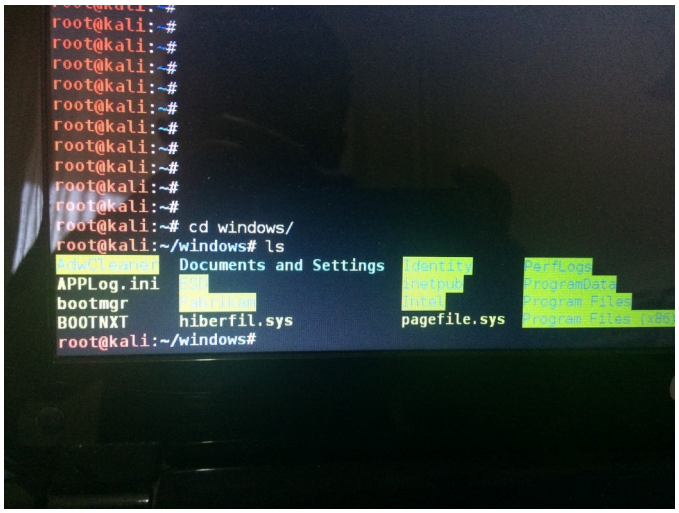
Bir sürü sda partition'ı sıralanmıştır. Bunlardan hangisinin Windows dosyalarını içerdiği birkaç deneme sonrası anlaşılacaktır. Biz /dev/sda4 partition'ınını Kali Live'in /root/windows dizinine mount edelim.

> mkdir windows
> mount -o ro /dev/sda4 /root/windows // ro ile read only olarak mount ederiz. Diğer // türlü mount edilmiyor. Çünkü SAM dosyasına // saldırganlar kullanıcı eklemesinler diye // Windows diske offline'ken write engeli // koymaktadır.




Windows partition'ı /root/windows dizinine mount edilmiş mi diye bakmak için /root/windows dizinine geçelim ve ls yaparak Windows dosyalarını sıralayalım:

> cd /root/windows
> ls

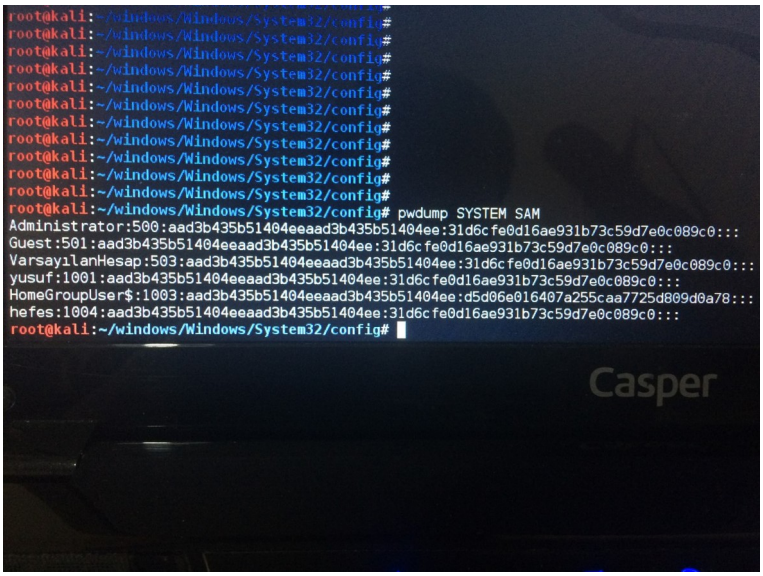


Görüldüğü üzere Windows'un C sürücüsüne ait dosyalar sıralanmıştır. Şimdi C sürücüsü içerisinde SAM dosyasının yer aldığı dizine geçiş yapalım.

> cd Windows/System32/config

Ardından pwdump tool’u ile SAM dosyasının içeriğini dump edelim.

> pwdump SYSTEM SAM // Bazı sistemelerde SYSTEM ve SAM dosya isimleri
// küçük harfli olabiliyor. Enesinkinde öyleydi. Öylesi
// durumda dosya isimlerini küçük yaz. Yoksa
// pwdump çalışmıyor.




Böylece hesap özetlerini elde etmiş olduk. Şimdi yapılacak işlem bu hash'leri not etmek ve kendi bilgisayarımıza çekilip hash'leri hashcat ya da john the ripper tool'ları ile brute force yaparak kırmaktır.

**Sonuç**

Fiziksel manada erişebildiğimiz bir hedef bilgisayarı gözümüze kestirdik. Hazırladığımız USB disk ile hedef bilgisayarı boot ettik. Hedef bilgisayardaki Windows partition'ını Kali Live'in bir dizinine mount ettik. SAM dosyasına doğru ilerledik. pwdump tool’u ile SAM dosyasının içeriğini çektik. Hash'leri alıp hedef sistemi kapattık. Bu noktadan sonra kendi bilgisayarımıza çekilip hash'leri kırmaya çalışabiliriz ve yaptığımız işlemlerden kurbanın ruhu bile duymaz. Hash'leri şayet kırarsak uzaktan hedef sistemde oturum açabiliriz. Böylece hedef sistemin komut satırını alarak hedef sistemin karşısında oturuyormuş gibi dilediğimiz her şeyi yapabiliriz.

**Ekstra**

Annemin bilgisayarından pwdump ile çektiğim hash'ler şu şekildeydi:

> pwdump SYSTEM SAM

Output:

administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Varsayılan:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Yusuf:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroup:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
hefese:1004:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

SAM dosyasının syntax'ı ise şu şekildedir:

<User>:<ID>:<LM hash>:<NTLM hash>:<Comment>:<Path>

Fark ettiysen SAM dosyasındaki hash'ler (hem LM hash'leri hem de NTLM hash'leri) hep NULL'dır. SAM dosyasının her satırında LM hash'i olarak

aad3b435b51404eeaad3b435b51404ee

string'i vardır. SAM dosyasının yine her satırında NTLM hash'i olarak

31d6cfe0d16ae931b73c59d7e0c089c0

string'i vardır. Bu hash'ler LM ve NTLM'de empty password anlamına gelmektedirler. Peki ama annemin bilgisayarı şifreli olmasına rağmen neden tüm hash'ler empty password şeklindeler? Bunun nedeni Microsoft'un Windows 10 yıldönümü güncellemesinde saklı (bkz. http://security.stack exchange.com/questions/145278/pwdump-gives-me-blank-passwords-as-hash-although-there-are-passwords) Gelen yeniliğe göre Windows kullanıcılarının hesap bilgileri artık SAM dosyasına daha farklı şekilde depolanıyormuş. Ayrıca kullanılan hash algoritması olarak da artık AES şifrelemesi kullanılıyormuş. Bu nedenle pwdump tool'u yeni SAM dosyasını okuyamadığından sürekli empty hash döndürmüştür. Bu noktadan sonra yapılacak şey mevcut tool'ların güncellenmesini ya da yeni tool'ların çıkmasını beklemektir. Görünen o ki o zamana dek SAM dosyasından faydalanmamız mümkün değil.

pwdump tool’unun kardeşleri olan lsadump ve cachedump tool’ları da hedef sistemde acaba olur mu diye denenmiştir (Not: pwdump, lsadump ve cachedump’ın üçü de creddump adlı paketin içerisinde yer almaktadırlar) Ancak onlar da empty password yerine syntax hatası vermişlerdir.

> lsadump SYSTEM SECURITY // Bu tool SECURITY dosyasını kullanıyor.

Output:

…, line 135, in get_file_secrets
…, line 126, in get_secrets
…, line 66, in **decrypt_secret**

> cachedump SYSTEM SECURITY // Bu tool SECURITY dosyasını kullanıyor.

Output:

ERR:**Couldn't find subkey** PolSecretEncryptionKey of Policy

Hatalardan anlaşıldığı kadarıyla bu tool’lar ya bug’dan dolayı ya da yıl dönümü güncellemesi dolayısıyla yeni SAM dosyasını okuyamadıklarından dolayı hata vermişlerdir. Dolayısıyla esas şifrelere ait hash’ler elde edilememiştir. Yeni tool’lar gelene kadar ya da mevcut tool’lara güncelleştirmeler gelene kadar beklemek durumundayız.

Not: Bir başka parola elde etme aracı olan mimikatz tool’unun geliştiricisi Benjamin Delphy Windows’un yaptığı yıldönümü güncelleştirmesi sonrası mimikatz tool’unu güncelleştirdiğini duyurmuştur. (bkz. https://twitter.com /gentilkiwi/status/762465220132384770)

Yararlanılan Kaynaklar


https://www.quora.com/How-do-I-boot-kali-Linux-live-usb-in-Windows-10-UEFI-boot-menu-I-couldnt-able-to-boot-from-boot-menu

https://www.unixmen.com/how-to-format-usb-drive-in-the-terminal/

http://www.linuxquestions.org/questions/debian-26/unable-creating-a-booting-usb-stick-4175419998/

https://github.com/Neohapsis/creddump7/issues/2

http://security.stackexchange.com/questions/145278/pwdump-gives-me-blank-passwords-as-hash-although-there-are-passwords

http://www.rixler.com/windows_service.htm