**Kurs Linki:** <https://www.udemy.com/course/etik-hacker-olma-kursu/>

*Bu kurs Rıdvan Karasubaşı hesabından satın alınmıştır.*

**Bölüm 2: Kurulumları Yapmak**

**Sanal Makine Nedir?**

Kendi bilgisayarımız üzerinde sanal bir şekilde herhangi bir işletim sistemini çalıştırmaya olanak sağlayan bir teknolojidir.

**Bölüm 3: Linux Kullanımı**

**Kali Linux Klasör Yapısı**

**bin:** Bu klasörde kullanıcının çalıştırdığı komutlar bulunur. (binary)

**sbin:** Sistem komutları bu klasörde bulunur. Daha çok root kullanıcısının çalıştırabildiği komutlar bulunur. (system binary)

**dev:** Donanım dosyaları bulunur.

**etc:** Konfigürasyon dosyaları bulunur. DNS ayarı gibi. Genel olarak ayar dosyaları bu klasörde bulunur.

**var:** Değişken dosyalar burada tutulur. Log dosyaları, cache’ler, backup’lar gibi. Web sunucuları (www klasörü) da bu klasörde bulunur. (variable)

**tmp:** Geçici dosyalar ve geçici klasörler burada tutulur. Programlar geçici bir şey yazacaklarsa gelir bunun içine yazarlar. (temporary)

**home:** Kullanıcıların klasörleri bu klasörde bulunur.

**proc:** Sistemde işleyen süreçlerin bilgilerini depolar.

srv: Servisler bu klasörde tutulur. (services)

usr: Kullanıcıların kullanabileceği uygulamalar bu klasörde tutulur. Yüklediğimiz paketler genelde burada depolanır.

lib: Kütüphaneler burada tutulur. (library)

**Komutlar**

**setxkbmap <ulke\_kodu>:** Bu komut klavyeyi girilen dile çevirir. Örneğin <ulke\_kodu> kısmına tr yazarsak klavyemiz Türkçe olur.

**pwd:** Şu anda bulunduğumuz dizini gösterir. (print working directory)

**ls:** Bulunduğumuz dizindeki klasör ve dosyaları listeler. (list)

**cd <dizin\_adi>:** Başka bir dizinin içerisine girmemizi sağlar. (change directory)

**mkdir <klasör\_adi>:** Yeni bir klasör oluşturmamızı sağlar. (make directory)

**clear:** Konsolu temizler.

**cd ..:** Bir klasör geriye gider.

**touch <dosya\_adi>:** Bir dosya oluşturur.

**cp <dosya\_adi> <yeni\_isim>:** Bu komut girilen dosyayı kopyalar. Eğer bulunduğumuz dizinin altındaki bir klasöre kopyalamak istersek <yeni\_isim> parametresini <dizin\_adi/yeni\_isim> olarak girmeliyiz. Eğer bulunduğumuz dizinin dışındaki bir yere kopyalamak istersek tam yolunu girmeliyiz. Örneğin, </home/kali/…/deneme/yeni\_isim> gibi. (copy)

**mv <dosya\_adi> <yeni\_isim>:** Bu komut girilen dosyayı taşır. Eğer bulunduğumuz dizinin altındaki bir klasöre taşımak istersek <yeni\_isim> parametresini <dizin\_adi/yeni\_isim> olarak girmeliyiz. Eğer bulunduğumuz dizinin dışındaki bir yere taşımak istersek tam yolunu girmeliyiz. Örneğin, </home/kali/…/deneme/yeni\_isim> gibi. (move)

**rm <dosya\_adi>:** Girilen dosyayı siler. (remove)

**rm -r <dizin\_adi>:** Normalde rm komutu ile dizin silemiyoruz fakat -r parametresi sayesinde dizin altındaki dosyalar yinelemeli olarak silinir. Yani en alt dosyadan silinme işlemi başlar, en sonda da klasör silinir. (-r: recursive)

**rm -rf <dizin\_adi>:** Bu komuttaki -f parametresi, girilen dizinin zorla silinmek istendiğini belirtir. (-f: force)

**<komut> --help:** Girilen komutun dokümantasyonunu gösterir.

**sudo su:** Komutu ile root kullanıcısına geçiş yapabiliriz. (superuserdo switchuser)

**apt install <paket\_adi>:** Girilen paketi indirir.

**apt search <paket\_adi>:** Girilen paketi arar.

**NOT:** Farklı Linux sürümleri farklı paket yöneticisini kullanabilir. Örneğin, Debian ve Ubuntu “apt” veya “apt-get” kullanırken CentOS “yum check-update” kullanır. apt ve apt-get arasında çok ufak farklılıklar vardır. İkisini de birbirinin yerine kullanabiliriz.

**cat <dosya\_adi>:** Girilen dosyayı okumamızı sağlar.

**nano <dosya\_adi>:** Girilen dosyayı nano editöründe açar ve dosya üzerinde değişiklik yapmamızı sağlar. Bu editördeki “^” işareti Ctrl işareti anlamına gelmektedir. Örneğin “^X” ifadesinin karşılığı Ctrl+X dir.

**ls -al:** Bulunduğumuz dizinde gizli dosyalar varsa onları da listeler. Dosyaları detaylı olarak gösterir.

**ifconfig:** IP bilgilerimizi gösterir. Buradaki IP adresi yerel IP adresidir. Başkalarıyla paylaşmamızda bir sakınca yoktur.

**passwd:** Şifremizi değiştirmeye yarar. Hangi kullanıcının şifresini değiştireceksek o kullanıcıyı kullanırken bu komutu terminale yazmalıyız.

**Bölüm 4: Ağlara Giriş**

**Router = Modem:** Biz internete routerlar ile çıkıyoruz.

2 tür IP adresi vardır. Birisi Public IP adres diğeri ise Local IP adrestir. Public IP adresi hiç kimse ile paylaşmamalıyız. Çünkü IP adresimizden bizim konumumuzu ve kim olduğumuzu bulabilirler. Local IP adresi paylaşmamızda hiçbir sakınca yoktur.

Public IP adresimizi 2 farklı şekilde öğrenebiliriz. Bunlardan ilki internete “What is my IP address?” yazmak, diğeri ise modem arayüzünden public IP adresimizi öğrenmek.

**NOT:** Modeme bağlı her cihazın public IP’si modemin public IP’si ile aynıdır. Fakat her cihazın local IP’si birbirinden farklıdır. Local IP adresleri modem tarafından cihazlara rastgele atanır. Genellikle cihazların local IP adresleri 192.168 ile başlar. Genelde modemlerin local IP adresleri .1 ile biter. 255 taneye kadar local IP adres atanabilir.

**ifconfig:** Kali Linux’ta local IP adresimizi öğrenmemize yarar. Windows’ta bu komutun karşılığı ipconfig’dir. Eğer kali linux’u bir sanal makineye kurduysak local IP adresimiz 192.168 ile değil de 10 ile başlayacaktır. Eğer bir Wifi kart ile direk modeme bağlanırsak o zaman 192.168 ile başlayabilir. 10 ile başlamasının sebebi sanal bir ağ oluşturmamızdır.

**VPN(Virtual Private Network) Nedir?**

**VPN(Virtual Private Network):** VPN’in çıkış amacı şudur, örneğin bir şirketimiz var ve bu şirketi Berlin’de kurduk ama Londra’da da ofisimiz var. Bütün sunucularımız Berlin’de duruyor ve dediğimiz gibi birçok yerde ofisimiz var. Londra’daki çalışanlarımızda Berlin sunucuları üzerinden internete bağlansın istiyoruz ki şirketin bütün kurallarına uysunlar. Şirketin yasakladığı sitelere giremesinler, firewall’lar vs devreye girsin istiyoruz. O yüzden kendi şirketimiz içinde sanal bir özel ağ oluşturabiliyoruz. Londra’daki çalışanlar sanki Londra internetinden değil de Berlin internetini kullanıyormuş gibi Berlin sunucusu üzerinden bu istekleri yollayabiliyorlar. Eğer bizde VPN kullanırsak yani sanal sunucuları kullanırsak IP adresimizi, sanki oradan geliyormuş gibi gösterebiliriz. Türkiye’de yasaklı herhangi bir siteye sanki Almanya’dan bağlanıyormuş gibi girebiliriz.

Kısaca VPN, public IP’mizi değiştirmeye yarar. Aslında değiştirmez. İstekleri sanki başka bir yerden geliyormuş gibi gösterir. VPN kullanarak bir sunucuya açılıyoruz ve bu sunucu üzerinden isteklerimizi yapıyoruz. Bizim IP adresimiz değil de başka bir IP adresi gözükecektir.

**DNS(Domain Name System) Nedir?**

**DNS(Domain Name System):** Domain bir internet sitesinin adıdır. Örneğin google.com. Biz google.com a gittiğimizde aslında google.com a gitmiyoruz. Google.com nerede host ediliyorsa o sunucunun IP adresine bağlanıyoruz. Google.com ile o IP adresini bağlayan sistem DNS’dir. Yani biz google.com yazdığımızda o IP adresini çözümleyen ve bizi o IP adresine yönlendiren sistem DNS’dir.

İnternet Servis Sağlayıcılar(Türk Telekom, Türkcell, TurkNet vb.) genellikle kendi DNS sunucularını sağlarlar. Biz bir siteye gitmek istediğimizde bu DNS sağlayıcılar, domain name(Alan adı) isteklerini alır. Ardından bu istekleri IP adresine dönüştürür ve son olarak kullanıcının doğru web sitesine bağlanmasını sağlar. Yani DNS sağlayıcılar internetin yönlendirme görevini üstlenir.

**Kali Linux’ta VPN Kullanımı**

İlk olarak ücretsiz bir VPNBook bulmamız gerekiyor. VPNBook bizim için bir formattır. İçerisinde sunucuların bağlantı bilgilerini saklayan çalıştırılabilir dosyalardır. Bu dosyaları indirmek için ilk olarak tarayıcımıza “free openvpn VPNBook” yazıyoruz. Bu kursta biz vpnbook.com web sitesinden birkaç tane VPNBook indirdik. İndirdiğimiz zipli dosyaları zipten çıkarttık. Ardından herhangi birisinin içerisine terminal kullanarak girdik. Bu klasörde farklı portlardan bağlanabileceğimiz dosyalar var(TCP, UDP vb.). VPN’i başlatmak için openvpn komutunu kullanacağız. Bu komut ile VPNBook’umuzu başlatıyoruz. Komutun kullanımı “openvpn <vpn\_adi>” şeklindedir. Ardından bizden kullanıcı adı ve şifre girmemizi isteyecek. Kullanıcı adı ve şifreyi, VPNBook’ları indirdiğimiz yerde bulabiliriz. Bütün VPNBook’lar için kullanıcı adı ve şifre aynıdır. Fakat arada bir kullanıcı adı ve şifre güncellenmektedir.

**NOT:** Eğer VPNBook çalıştırırken SSL hatası(Güvenli bağlantı çözülemiyor hatası) alıyorsak bağlanmak istediğimiz VPNBook’u nano editörü ile açıp içerisine bir komut eklememiz gerekiyor. Nano editörü ile açtıktan sonra herhangi bir satıra bu komutu ekleyebiliriz. Genelde en üste eklenir. En üste tls-cipher “DEFAULT:SECLEVEL=0” komutunu ekliyoruz. Bu sayede SSL hatası çözülecektir. Bu komut düşük güvenlikli şifreleme yöntemlerinin kullanılmasına izin verir. Eğer daha yüksek güvenlikli bir şifreleme kullanacaksak SECLEVEL’i 1 veya 2 olarak ayarlayabiliriz.

**NOT:** Bağlantı sağlanıyor ama internete giremiyorsak DNS server değiştirmeliyiz.

**DNS Server Değiştirme**

VPN kullandığımız zaman bazen DNS sunucumuz bağlanmak istediğimiz web sitesini çözümleyemeyebiliyor. Bu sorunu DNS sunucumuzu değiştirerek çözebiliriz. İlk olarak tarayıcımıza “free DNS server list” yazıyoruz. Ardından istediğimiz herhangi bir DNS server IP’sini kopyalıyoruz. Örneğin Google’unki 8.8.8.8, Cloudflare’inki ise 1.1.1.1 dir. Daha sonra kali linux’da root terminalinde etc klasörü altında bulunan “resolv.conf” dosyasını nano editörü ile açıyoruz. Her ne kadar root da olsak bu dosyaya bir şey yazamıyoruz. Çünkü bu dosya immutable yani değiştirilemez anlamına gelen “i” attribute’ine sahip. Bu dosyada değişiklik yapabilmek için bu dosyanın attribute’lerini yani özelliklerini değiştirmemiz lazım. Bunun için “chattr” komutunu kullanacağız. Bu komutun açılımı change attribute’dür. “i” attribute’ünü kaldırmak için “chattr -i resolv.conf” komutunu kullanacağız. Eğer bu komutu çalıştırdığımızda bir sorun çıkarsa önce bu komutu “-a” parametresiyle, daha sonra ise “-i” parametresi ile çalıştırmalıyız. Buradaki “-a” parametresi dosyaya sadece ekleme yapılmasına izin verir. Yani dosyanın içeriğine sadece yeni veriler eklenebilir. Mevcut veriler değiştirilemez. Bu adımları yaptıktan sonra artık DNS serverlarımızı değiştirebiliriz. resolv.conf dosyasını açtıktan sonra kopyaladığımız DNS server IP’lerini başına nameserver kelimesini ekleyerek yazın. Daha önce dosyada bulunanları ise yorum satırına alabilirsiniz. Bu sayede internet servis sağlayıcılarımızın DNS serverlarını değil de başka DNS serverlarını kullanırız.

**NOT:** “lsattr” komutu ile dizinde bulunan dosyaların attribute’lerini görebiliriz. İstersek yanına dosya ismi vererek sadece o dosyanın attribute’lerini görebiliriz. Örneğin “lsattr resolv.conf” gibi.

**NOT:** VPN kullansak bile internet servis sağlayıcımız hangi sitelere girdiğimizi görebilir. DNS server değiştirerek girdiğimiz siteleri görmelerini daha da zorlaştırarak imkansız hale getiririz.

**Bölüm 5: Dark Web**

**Tor Browser**

.onion uzantılı web sitelerine girmemizi sağlayan bir tarayıcıdır. Tor browser ile normalde giremeyeceğimiz sitelere girebiliyoruz. Tor yüklemek için root terminaline “apt-get install tor” yazıyoruz. Paketleri yüklerken bize yüklemek isteyip istemediğimizi soracak. Eğer hepsini yüklemek istiyorsak bu komutun en sonuna “-y” parametresini ekleyebiliriz. Bu bütün sorulara yes yanıtını verecektir. Eğer yüklemede bir sorun çıkarsa ilk önce “apt-get update” komutunu çalıştırmalıyız. Tor’u başarıyla yükledikten sonra tarayıcımıza “tor browser” yazıyoruz ve torproject.org sitesine gidiyoruz. Daha sonra indirme sayfasından kali linux kullandığımız için linux versiyonunu indiriyoruz. Dosya zipli olarak geliyor. Bunu zipten çıkarın. Ardından root terminalinde bu klasöre giriyoruz ve tor browser’u çalıştırmak için terminale “./start-tor-browser.desktop” komutunu yazıyoruz. Bize bir hata verecektir. Bu hatanın sebebi tor browser’u root kullanıcısı ile açmaya çalışmamızdır. Bu sorunu tor browser’u normal kullanıcı ile açarak çözebiliriz. Ama root ile açmak istiyorsak indirdiğimiz dosyanın içerisinde browse klasörü var. Bu browse klasörünün içerisinde ise “start-tor-browser” shell script’i var. Bu scriptin içerisinde root ile ilgili olan kısmı bulacağız ve yorum satırına alacağız. Ardından dosyayı kaydedip kapatın. “./start-tor-browser.desktop” komutunu tekrardan çalıştırın. Tor browser açılacaktır. Eğer connect’e bastığımızda ilerleme takılıp kaldıysa veya çok yavaşsa configure kısmından “tor benim ülkemde sensörlü” seçeneğini seçtikten sonra “obfs4” köprüsünü seçin. Bu köprü, tor trafiğini gizleyen ve sansür engellerini aşan bir araçtır. İnternet trafiğini gizleyerek tor kullanıcılarının daha güvenli bir şekilde bağlantı kurmasına olanak tanır. Açılımı “obfuscation 4” tür. Bu işlemi bir kere yaptıktan sonra tor browser’u başlatmak için indirdiğimiz dosyada bulunan tor browser’a çift tıklamamız yeterli olacaktır.

**DuckDuckGo Nedir?**

Google gibi bir arama motorudur. Bir arama yaptığımızda aramalarımızı kaydetmez. Google’da çıkmayan sonuçları gösterir.

Dark Web sitelerine giriş yapabilmek için duckduckgo’ya “hidden wiki” yazıyoruz.

**NOT:** Tor browser ayarlarından güvenlik kısmını safer’a alırsak javascript devre dışı bırakılacaktır. Bazı dark web siteleri arkaplanda zararlı javascript kodları çalıştırır. Biz güvenlik modunu safer yaparsak bu kodların çalıştırılmasını engelleriz. Bu saldırılar browser’ı kapattığımızda genelde durur. Kalıcı zarar vermez. İşlemci kullanarak mining yapmaya çalışır.