SSH-KEY

Bu yazımda sizlere günümüz dünyasında çok sıkça kullandığımız ve herkes tarafından bilenen SSH protokolünden bahsedeceğim. Çok kısa ssh tanımlayacak olursak. Güvenli olmayan bir ağ üzerinden bir bilgisiyara güvenli bir şekilde komut göndermek için kullanılan bir yöntem diyebilirz fakat Ben bu yazımda sizlere SSH protokolü nasıl çalışır ifade etmekten ziyede, Karşı bilgisiyar ile nasıl oturum açıyoruz onu ifade etmeye çalışacağım, yani CTF'lerde herkesin gördüğü id_rsa ve id_rsa.pub anahtarlarını.

Günümüz dünyasında sizce Şifreler ne kadar güvenli, Değişik kombinasyonlar halinde Şifreler oluşturmama rağmen, ben bile bazen şüpheye düşüyorum, basit Şifre kombinasyonu oluşturan insanları düşünemiyorum bile çünkü oluşturmuş oldukları şifreler, Dünyanın dört bir yanında meydana gelen veri ihlallerindeki şifreler ile aynı olabilir, bu veri ihlallerindeki şifreleri ise, web siteleri aracılığıyla çok basit bir şekilde ulaşılabilir. bu nedenle SSH Protokolünde şifre kullanımından çok daha iyi, çok daha güvenli bir alternatifi var. SSH-KEY.

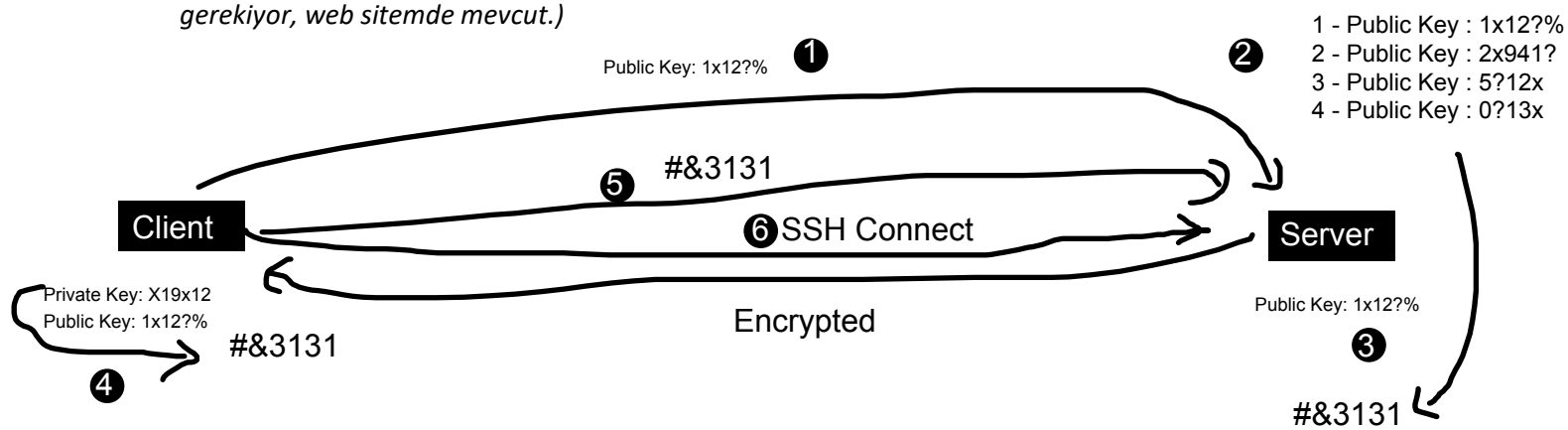
SSH-KEY Nasıl Çalışır

SSH-KEY çalışma prensibi, o herkesin çok duyduğu private key ve Public Key anahtarları ile birlikte çalışır, bunların ne olduğunu başlıklar halinde özetlemek gerekirse

Private Key : *İlgili kişinin, kendisine özel olarak beyan edilmiş anahtar türü olmakla birlikte kesinlikle kimseyle paylaşılmaması gereken bir anahtardır. aksi takdirde bir başkası bu anahtara sahip olduğu bir denklemde, ilgili kişiyi taklit edebilir ve istenmeyen durumlar doğurabilir.*

Public Key: *Adındanda anlaşıldığı üzere, herkes tarafından bilinmesinde bir sorun olmayan anahtar diyebiliriz.*

SSH protokolünü kullanarak Web sunucumuza bağlanmak istediğimiz bir senaryo düşünelim, karşı tarafın bizi tanımlaması için, herkese açık olarak paylaştığımız Public Key'i, ilgili web sunucuzunda bulundurmamız gerekiyor. bu çalışma prensibini, sırasıyla diyagram üzerinden anlatırsam durumlara daha vakıf olacağınız inanıyorum.(olaylara daha vakıf olmanız açısından asimetrik şifreleme bilinmesi gerekiyor, web sitemde mevcut.)



Yukarıdaki Durumu aşağıda maddeler halinde özetlemek gerekirse,

***1.** Public Key anahtarımız kullanarak, ilgili sunucuya SSH protokolü üzerinden bağlanmak istediğimizi beyan ediyoruz.*

***2.** İlgili sunucu ise, vermiş olduğumuzu açık anahtarı, kendisine bulunana açık anahtar listesi ile karşılaştırıp, onaylıyor.*

***3.** Bağlantının kurulması için, İlgili sunucu karşı tarafın gerçek kişi olduğunu tespit etmesi için rastgele bir dize oluşturup, açık anahtar ile şifreleyip karşı tarafa yollar.*

***4.** Client ise Gizli Anahtarını kullanarak, Açık anahtarını çözümler.*

***5.** Client, Sunucuya bu değeri gönderir.*

***6.** SSH bağlantısı kurulur.*

o çok gördüğümüz id_rsa ve id_rsa.pub anahtarlarının aynı dizinde bulunması bundan dolayı diyebiliriz. ayrıca şunuda belirtmemde fayda var ki, Public Key ve Private Key'de vermiş olduğum değerler gerçek dışı. Gerçek dünyada bu değerlerin örnek gösterimi aşağıda vermiş olduğum görselde mevcut.

Tabi ki de SSH protokolün kullanarak bağlantı gerçekleştirmek isterseniz, Kullandığınız işletim sistemine özel yazılımlar mevcut. Eğer bir MacOS veya Linux kullanıyorsanız, terminal üzerinden bu yazılıma ulaşabilirsiniz, Windows için ise en çok kullanılan uygulama putty diyebilirim. Windows için şunu ifade etmeyelim ki, indirmiş olduğunuz uygulamalara çok dikkat etmelisiniz çünkü piyadasa fazlasıyla sahte uygulamalar mevcut. bu gizli anahtarınızın başka birinin eline geçmesi veya Bilgisiyarınıza Virus bulaşmasına neden olabilir.

e-mail

berathanakcakaya@gmail.com

linkedin

https://www.linkedin.com/in/berathan-akcakaya/