

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 diyebiliriz fakat Ben bu yazımda sizlere SSH protokolü nasıl çalışır ifade etmekten ziyade, Karşı bilgisayar 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 alternatif var. SSH-KEY.

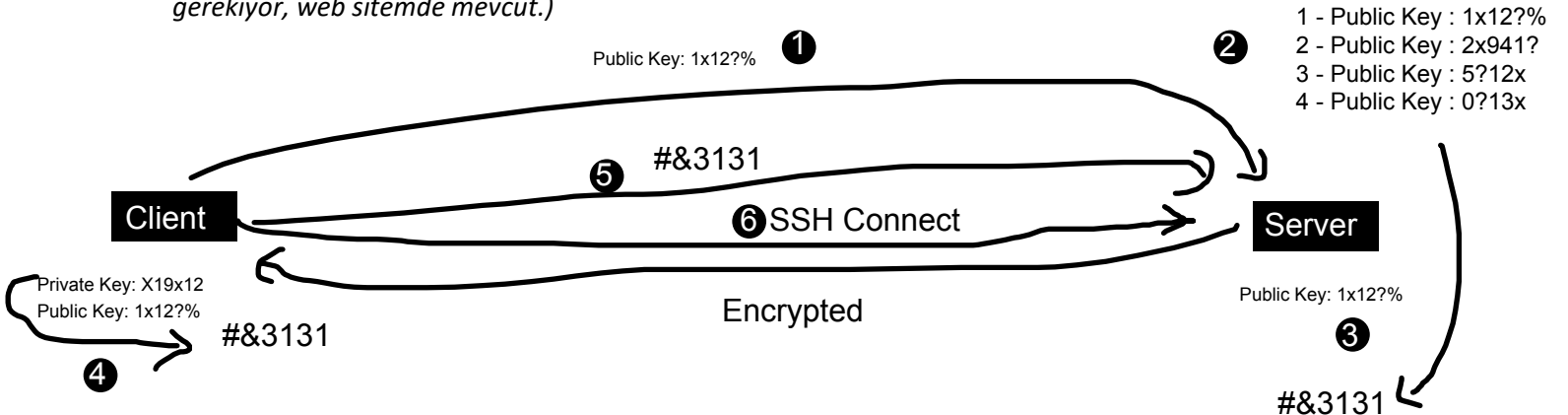
SSH-KEY Nasıl Çalışır

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, ilgili 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.

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,49CAD03909900A66E5DE009F477C89F9

KEYVD0xQASJkAnMpHDud5LTzifhyldlxKPPu1xb79JF7dBaIRF4jAAHvQedzei3
/fD0lAEZ8unzwPpvHeW5j4J+mPLF9ticSdoERT0i2NfuQ0x9NvbwFZhpYdwgGpX
+H4eQF+FHVLn3MenpXrmRxlndRRUhPVY0X465I8Xwcaysti/DzGrCNfIpTsdiap
kGQzLgnZdyk8fLZAWd4Ewjx80YTL7gCd8tTK2uaXgiyv/LVcs5wV0EKxTe7tJhF6
S+RTD0VMHAMH0zXwnJBdw2z6b616uBLFWCehWY9QkgCf1IFzXYMLkNrpZeTqCZCI
jJwXUZXiIcgp+hGA2Mp7fDtX9EgJxFrYzXyZu9+XH/t9ljnE25v3d4l3TG3wMfBX
5L5lstHneuEa7aq4PwDdkWS5Yl9S509mfypHgbdLooq8o0ARg42udUpd85X/Gp/Y
zQFZMo8gWgm7zsc16g4VxFz6e/C7doTewYhczSQfto90B0UU0GR05UEsIkbGC/TS
2Rht5Coywa8N9lWDrnGCB5laC/6ewoarEr1Cym76wRj9pKQ56jo2vldy/YYb/bKJ
nrw+NHvJk5NnUsyHufU491Bvo92YR63LCIK4L3hgU9sAM2kZePqX/V7pmBegguCs
DZMsQWgdXx1Hn89v8ti0M/f3bwXrzIidYtnZmMi5XmHdKhK/+2G2F0fr/JP9uz/
dYpS1oAd0sN90JbTz0kx659DAak8b1Vis9nYoKPa8NNcX/X12Rr8pUhLzwNwGfm1
WpwRE405M8Ulj40jLUY+Gc1M4+E1XVhrNhhTpBHLEi/jT204goodXncN6onJw3nZ
kyp6D9JIAjePMQVj518x7vc6pi3+pcqzauXs0SWe2jW0Mc+cMvDXdameh/fI36zI
zJFXdFy91xQ00mmNT/omMYIGMqZ2peyx7T6uafRPTGbYyTI404H02y5BJifIxopu
/4H52FRRN3Zq6gXgVmJYXJyT+NmNeXxnNYr9A60oEDbg9Bt2o0rtqQjb6h0oA0Ju
qeyCiL5wBcVbhbJ0y2ZqszhKU+EVsmzth/jLEafnyllFPzfsxcVMYJswyWu6EIt
UFFswJPbB4UiJQpze1Ne/nvfPA+e6jfrXbJxfq/9mCcRp0aRPyAr900Wd9P0runy
xES+0JRX2gFwTstJ2rJb6ZBLUKrz/0oDbcZfHM0Js72H4G0JFFUdOpM6w4nkvd
ypAwLEJ0gGf4+lx0ynllwXMM5Z82X7vElqDJTafaESim/DackoQoLaIhfg0CHXe/
dk+Xu0LSMl8aoCJyXD00GNeupKKty7TaIGTchizISEbDutCNSPCKKKNxTi0NbN7Y
YaNwBSqEu0VnGg/vrrDW5t3S2arP3e0aXHxspLHKo7i5s2grspBvpTqB/CXpGrmQ
Es00dkN2lKlvN0yZbJh0B3GEtNKqkL7cqk//hA28maBYH3JWcs8L5zfH9uwz0Yv
VZ6CxoDyBmPM3DQ33jLhsKX6bkGcJo6YVrHLNY+WJAuZPskozAzEvlAykvvX0DC
R4U9KYEWn970mMUNhBEo2iDrXwCtYzlpnVTZChGup+PRLY5kv8cIcQRPiSaJrtM+
-----END RSA PRIVATE KEY-----
id_rsa (END)
```

Tabi ki de SSH protokol n kullanarak baėlantı ger ekleřtirmek isterseniz, Kullandığınız iřletim sistemine  zel yazılımlar mevcut. Eėer bir MacOS veya Linux kullanıyorsanız, terminal  zerinden bu yazılıma ulařabilirsiniz, Windows i in ise en  ok kullanılan uygulama putty diyebilirim. Windows i in řunu ifade etmeyelim ki, indirmiř olduėunuz uygulamalara  ok dikkat etmelisiniz   nk  piyadasa fazlasıyla sahte uygulamalar mevcut. bu gizli anahtarınızın bařka birinin eline ge mesi veya Bilgisayarınıza Virus bulařmasına neden olabilir.

e-mail

berathanakcakaya@gmail.com

linkedin

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