SSH Protokolünde Araya Girve ve Veri Okuma & Değiştirme

- SSH Protokolünde Araya Girilebilir mi?

SSH Protokolü

- SSH (Secure Shell/Güvenli Kabuk) ağ üzerinden başka bilgisayarlara erişim sağlamak, uzak bir bilgisayarda komutlar çalıştırmak ve bir bilgisayardan diğerine dosya transferi amaçlı geliştirilmiş bir protokoldür.
- Bir iletişimde SSH aşağıda belirtilen temel unsurları sağlar.
  - Authentication /Kimlik denetimi
  - Encryption /Şifreleme
  - Integrity /Bütünlük

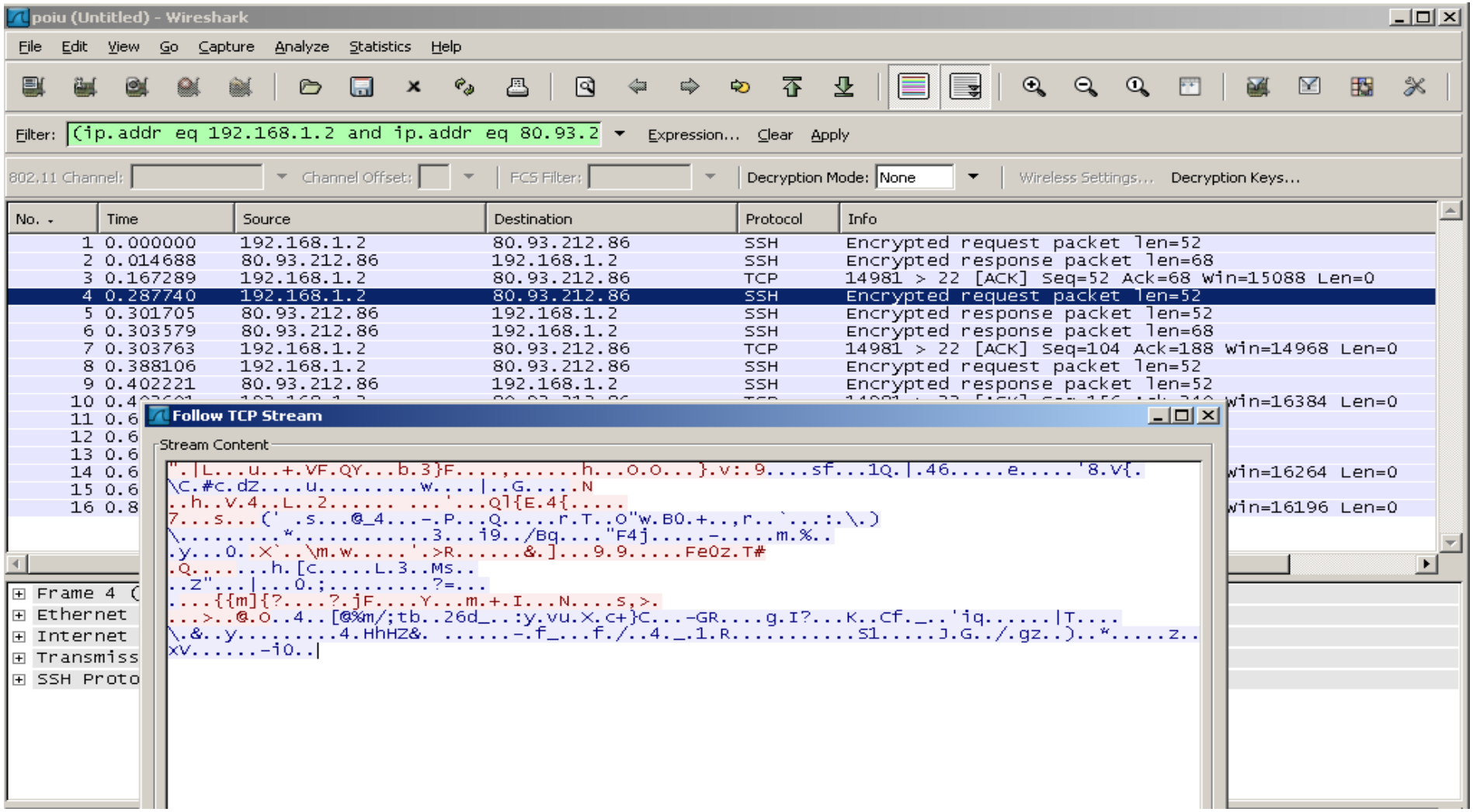
SSH Temel Bilgiler

- **SSH1**, Tatu Ylönen tarafından geliştirilen ilk orjinal SSH ürünü. SSH-1 protokolü temel alınarak geliştirilmiştir.
- **SSH2**, Tatu Ylönen tarafından geliştirilen SSH-2 ürünü. www.ssh.com
- **SSH-1**, SSH protocol 1.
- **SSH-2**, SSH protocol 2 . Günümüzde yaygın kullanımda olan ve kullanımı tavsiye edilen ssh sürümü. IETF SECSH çalışma grubu tarafından standartları belirlenmiştir.

OpenSSH

- OpenSSH son özgür SSH versiyonu olan **ssh1.2.12** den türetilmistir
- Ticari SSH sunucular kadar özelliğe sahip
- Dünya SSH servisinin %90~
  - Sshscan araciligi ile alinmis resmi bilgi.

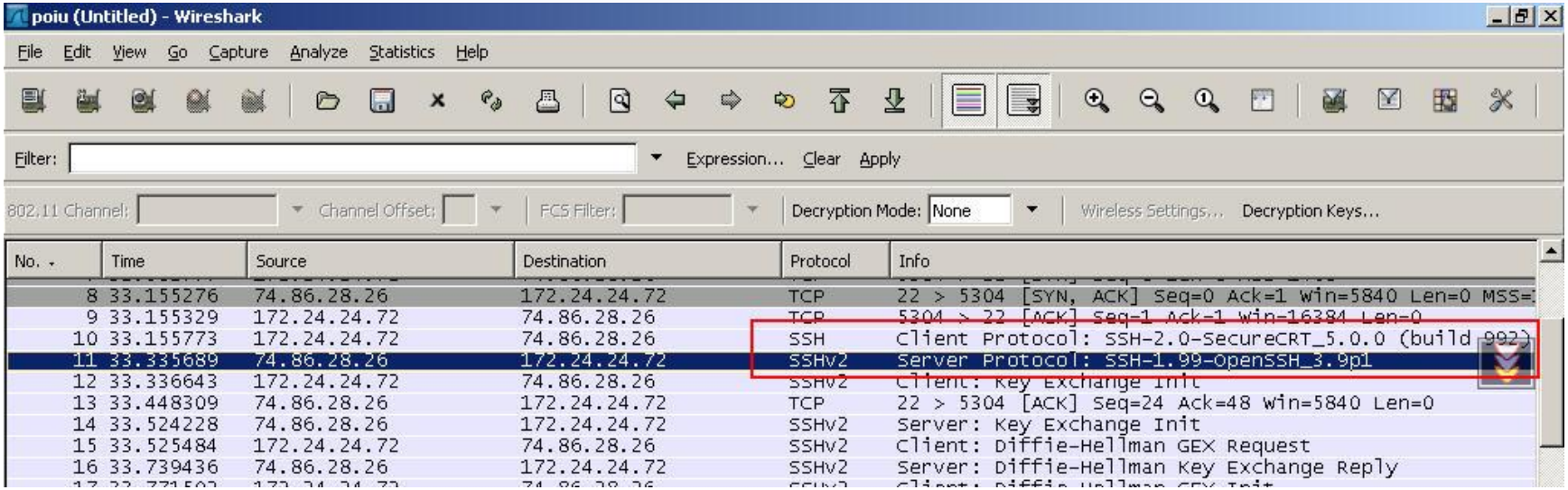
SSH Protokolü Analizi

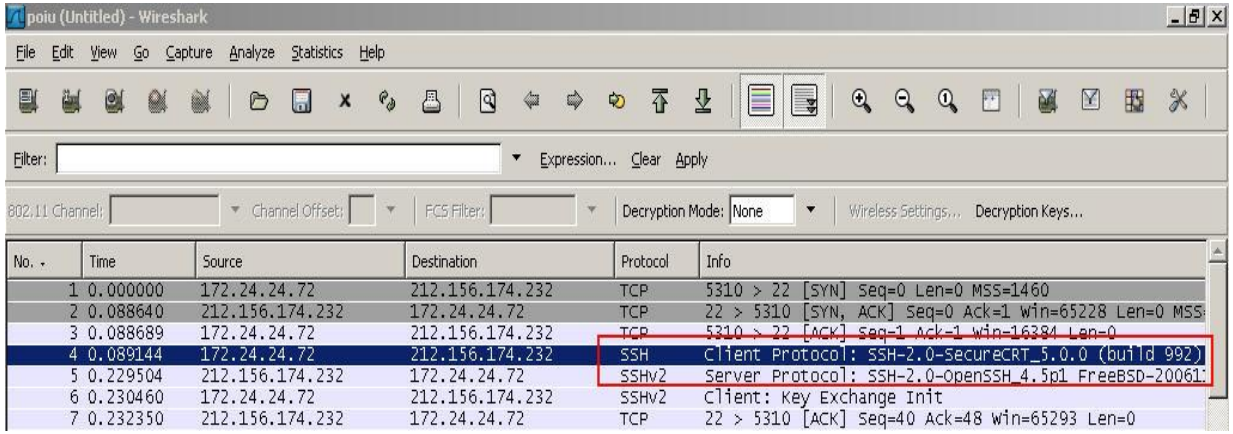


Araya girme nasıl olur?

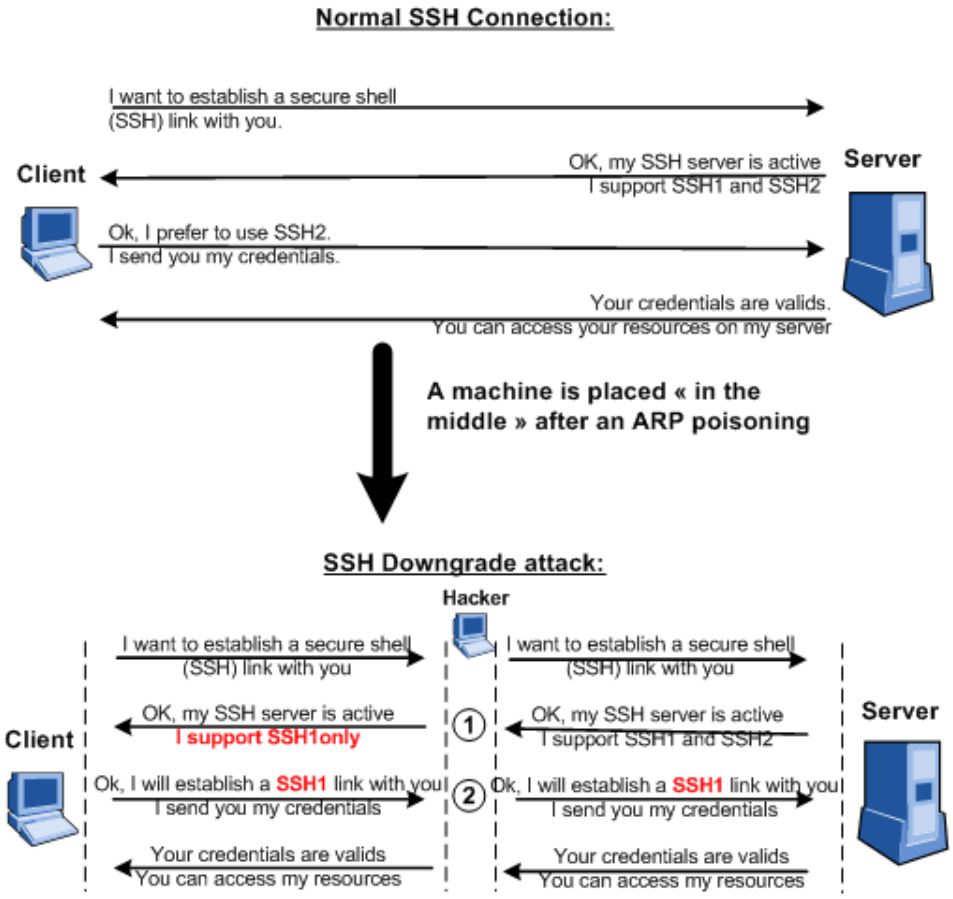
- SSH-1 protokolü çeşitli tasarımsal güvenlik açıklarına sahip.
- SSH-2 de bunlar giderildi.
- Fakat çoğu sunucu hem ssh-1 hem de ssh-2 destekler.
- Ssh-1 kullanan sistemlerde araya girip veri okuma & değiştirme yapılabilir.
- Ssh-2 sistemler eğer ssh-1 destekliyorsa “downgrade attack” gerçekleştirilerek ssh-1 kullanmaya zorlanır ve saldırı yine başarılı olur.

SSH1, SSH2 Destekli Sunucu Trafiği





SSH MITM



1. The hacker changes the server response from 1.99 to 1.51
2. The credentials are captured by the hacker because ot the ssh1 weak password authentication mechanism.

SSH MITM Çalışması

- Lab Çalışması NO:21
- Saldırı Araçları
  - Cain&Abel, Ettercap, sshmitm

RDP(Remote Desktop Protocol) Araya Girme

- RDP şifreli bir protokoldür
- Public-priv key kullanılarak güvenlik sağlanır
- Prive key tüm bilgisayarlarda aynıdır
  - "Public" private key mantığı
- Cain&Abel kullanılarak authentication bilgileri alınabilir