

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 türetilmiştir
- Ticari SSH sunucular kadar özelliğe sahip
- Dünya SSH servisinin %90~
 - Sshscan aracılığı ile alınmış resmi bilgi.

SSH Protokolü Analizi

Wireshark capture showing SSH traffic between 192.168.1.2 and 80.93.212.86. The filter is set to (ip.addr eq 192.168.1.2 and ip.addr eq 80.93.212.86).

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.2	80.93.212.86	SSH	Encrypted request packet len=52
2	0.014688	80.93.212.86	192.168.1.2	SSH	Encrypted response packet len=68
3	0.167289	192.168.1.2	80.93.212.86	TCP	14981 > 22 [ACK] Seq=52 Ack=68 win=15088 Len=0
4	0.287740	192.168.1.2	80.93.212.86	SSH	Encrypted request packet len=52
5	0.301705	80.93.212.86	192.168.1.2	SSH	Encrypted response packet len=52
6	0.303579	80.93.212.86	192.168.1.2	SSH	Encrypted response packet len=68
7	0.303763	192.168.1.2	80.93.212.86	TCP	14981 > 22 [ACK] Seq=104 Ack=188 win=14968 Len=0
8	0.388106	192.168.1.2	80.93.212.86	SSH	Encrypted request packet len=52
9	0.402221	80.93.212.86	192.168.1.2	SSH	Encrypted response packet len=52
10	0.402221	192.168.1.2	80.93.212.86	TCP	14981 > 22 [ACK] Seq=156 Ack=200 win=16384 Len=0
11	0.6				win=16264 Len=0
12	0.6				win=16196 Len=0
13	0.6				
14	0.6				
15	0.6				
16	0.8				

Follow TCP Stream

Stream Content:

```
"|L...u..+.VF.QY...b.3}F.....h...o.o...}.v:.9...sf...iQ.|.46.....e.....'8.V{.  
C.#c.dz...u.....w.....|.G.....N  
h..v.4..L..2.....Q1{E.4{.....  
7...s...('..s...@_4...-..P...Q...r.T...O"w.B0.+.,r...`.....\.)  
y...0..x'...\m.w.....>R.....&]...9.9.....Fe0z.T#  
Q.....h.[c...L.3..Ms..  
Z"...|.0;.....?=  
...{m}{?.....?..jF....Y...m.+..I...N....s.,>  
>...@.o..4...[xm/;tb..26d...:y.vu.X.c+}C...-GR....g.I?...K..cf..._'iq.....|T....  
&.y.....4.HhHZ&.....-f...f./..4..1.R.....Sl.....J.G../.gz..).*.....z..  
xv.....-10..|
```

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

poiu (Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

802.11 Channel: Channel Offset: FCS Filter: Decryption Mode: None Wireless Settings... Decryption Keys...

No. +	Time	Source	Destination	Protocol	Info
8	33.155276	74.86.28.26	172.24.24.72	TCP	22 > 5304 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=
9	33.155329	172.24.24.72	74.86.28.26	TCP	5304 > 22 [ACK] Seq=1 Ack=1 win=16384 Len=0
10	33.155773	172.24.24.72	74.86.28.26	SSH	Client Protocol: SSH-2.0-SecureCRT_5.0.0 (build 992)
11	33.335689	74.86.28.26	172.24.24.72	SSHv2	Server Protocol: SSH-1.99-openssh_3.9p1
12	33.336643	172.24.24.72	74.86.28.26	SSHv2	Client: Key Exchange Init
13	33.448309	74.86.28.26	172.24.24.72	TCP	22 > 5304 [ACK] Seq=24 Ack=48 win=5840 Len=0
14	33.524228	74.86.28.26	172.24.24.72	SSHv2	Server: Key Exchange Init
15	33.525484	172.24.24.72	74.86.28.26	SSHv2	Client: Diffie-Hellman GEX Request
16	33.739436	74.86.28.26	172.24.24.72	SSHv2	Server: Diffie-Hellman Key Exchange Reply

poiu (Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

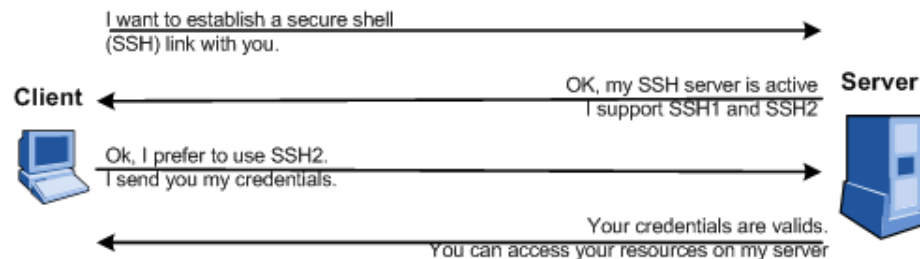
Filter: Expression... Clear Apply

802.11 Channel: Channel Offset: FCS Filter: Decryption Mode: None Wireless Settings... Decryption Keys...

No. +	Time	Source	Destination	Protocol	Info
1	0.000000	172.24.24.72	212.156.174.232	TCP	5310 > 22 [SYN] Seq=0 Len=0 MSS=1460
2	0.088640	212.156.174.232	172.24.24.72	TCP	22 > 5310 [SYN, ACK] Seq=0 Ack=1 win=65228 Len=0 MSS=
3	0.088689	172.24.24.72	212.156.174.232	TCP	5310 > 22 [ACK] Seq=1 Ack=1 win=16384 Len=0
4	0.089144	172.24.24.72	212.156.174.232	SSH	Client Protocol: SSH-2.0-SecureCRT_5.0.0 (build 992)
5	0.229504	212.156.174.232	172.24.24.72	SSHv2	Server Protocol: SSH-2.0-openssh_4.5p1 FreeBSD-20061
6	0.230460	172.24.24.72	212.156.174.232	SSHv2	Client: Key Exchange Init
7	0.232350	212.156.174.232	172.24.24.72	TCP	22 > 5310 [ACK] Seq=40 Ack=48 win=65293 Len=0

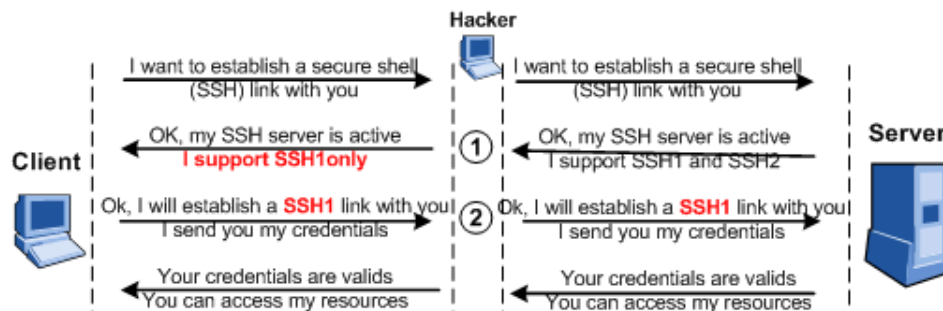
SSH MITM

Normal SSH Connection:



A machine is placed « in the middle » after an ARP poisoning

SSH Downgrade attack:



1. The hacker changes the server response from 1.99 to 1.51
2. The credentials are captured by the hacker because of 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