

16. Aufgabe: SSH in Wireshark

Greifen Sie mit einem geeigneten SSH-Client wie z.B. Putty oder der Kommandozeile auf den Server

ssh.hochschule-trier.de

zu und schneiden Sie den Traffic mit Wireshark mit. Beantworten Sie dann folgende Fragen:

- Wie stellen Sie sicher, dass es sich tatsächlich um den SSH-Server der Hochschule handelt und Sie nicht gerade Opfer eines MITM-Angriffs werden?
- Was für ein SSH-Server wird verwendet?
- Welche Verschlüsselungs- und MAC-Algorithmen werden vorgeschlagen? Welche werden ausgewählt? Wo können Sie die Reihenfolge der Algorithmen, die von Ihrem Client vorgeschlagen werden, ändern?
- Welche Kompressionsverfahren werden vorgeschlagen? Welche werden ausgewählt?
- Wie lautet die für den Diffie-Hellman-Schlüsselaustausch verwendete Primzahl p und Primitivwurzel g bzw. die verwendete elliptische Kurve?
- Wie lauten die für den Diffie-Hellman-Schlüsselaustausch ausgetauschten Werte e und f ?
- Wie lautet der für den Diffie-Hellman-Schlüsselaustausch verwendete öffentliche Schlüssel des Servers?
- Wie lautet der Wert für die Signatur von H ?

-Wir müssen ja unsere Kennung und Passwort mitgeben. Die wissen ja (Im besten Fall) nur wir und der Server.

Rechnernetze VM - VMware Workstation 16 Player (Non-commercial use only)

Player

*ens33

Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telefonie Wireless Tools Hilfe

ssh

No.	Time	Source	Destination	Protocol	Length	Info
12	0.072456670	143.93.63.8	192.168.74.128	SSHv2	95	Server: Protocol (SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7)
17	0.098482509	143.93.63.8	192.168.74.128	SSHv2	1126	Server: Key Exchange Init
36	0.072235151	143.93.63.8	192.168.74.128	SSHv2	810	Server: Encrypted packet (len=756)
28	0.318722566	143.93.63.8	192.168.74.128	SSHv2	106	Server: Encrypted packet (len=52)
38	6.263241875	143.93.63.8	192.168.74.128	SSHv2	98	Server: Encrypted packet (len=44)
25	0.292299895	143.93.63.8	192.168.74.128	SSHv2	98	Server: Encrypted packet (len=44)
43	6.442506429	143.93.63.8	192.168.74.128	SSHv2	90	Server: Encrypted packet (len=36)
32	5.730233898	143.93.63.8	192.168.74.128	SSHv2	82	Server: Encrypted packet (len=28)
42	6.442505767	143.93.63.8	192.168.74.128	SSHv2	1122	Server: Encrypted packet (len=1068)
20	0.199697952	143.93.63.8	192.168.74.128	SSHv2	506	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=172)
10	0.039997234	192.168.74.128	143.93.63.8	SSHv2	95	Client: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.4)
21	0.202661807	192.168.74.128	143.93.63.8	SSHv2	70	Client: New Keys
14	0.073315409	192.168.74.128	143.93.63.8	SSHv2	1566	Client: Key Exchange Init
26	0.292459875	192.168.74.128	143.93.63.8	SSHv2	122	Client: Encrypted packet (len=68)
22	0.202106068	192.168.74.128	143.93.63.8	SSHv2	98	Client: Encrypted packet (len=44)

> Frame 12: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface ens33, id 0

> Ethernet II, Src: VMware_f0:4b:78 (00:50:56:fd:4b:78), Dst: VMware_9a:e9:b7 (00:0c:29:9a:e9:b7)

> Internet Protocol Version 4, Src: 143.93.63.8, Dst: 192.168.74.128

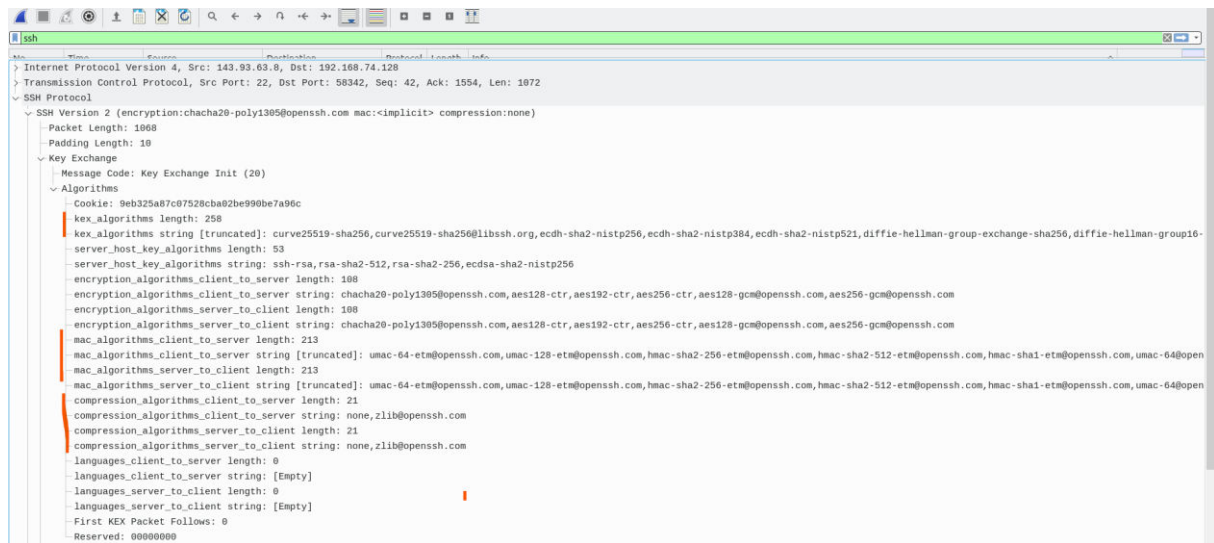
> Transmission Control Protocol, Src Port: 22, Dst Port: 58342, Seq: 1, Ack: 42, Len: 41

SSH Protocol

Protocol: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7

[Direction: server-to-client]

-Versch. Max und Komp



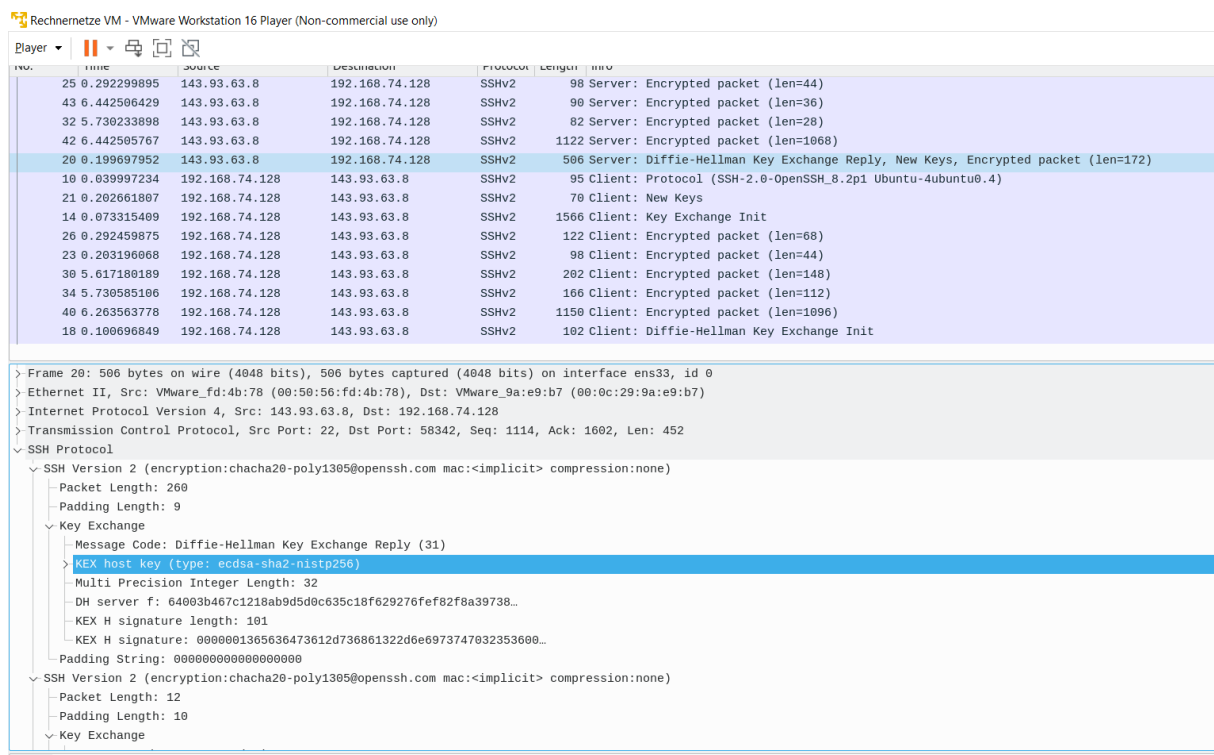
- Es wird sich auf den ersten Alg. in der Liste geeinigt.

Man muss das SSH-Serverprofil bearbeiten um die Reihenfolge zu ändern

-Kompr Auswahl



-Kurve



-e (Hoffentlich in Vorlesung sah das anders aus)

No.	Time	Source	Destination	Protocol	Length	Info
32	5.730233898	143.93.63.8	192.168.74.128	SSHv2	82	Server: Encrypted packet (len=28)
42	6.442505767	143.93.63.8	192.168.74.128	SSHv2	1122	Server: Encrypted packet (len=1068)
20	0.199697952	143.93.63.8	192.168.74.128	SSHv2	506	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=172)
10	0.039997234	192.168.74.128	143.93.63.8	SSHv2	95	Client: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.4)
21	0.202661807	192.168.74.128	143.93.63.8	SSHv2	70	Client: New Keys
14	0.073315409	192.168.74.128	143.93.63.8	SSHv2	1566	Client: Key Exchange Init
26	0.292459875	192.168.74.128	143.93.63.8	SSHv2	122	Client: Encrypted packet (len=68)
23	0.203196068	192.168.74.128	143.93.63.8	SSHv2	98	Client: Encrypted packet (len=44)
30	5.617180189	192.168.74.128	143.93.63.8	SSHv2	202	Client: Encrypted packet (len=148)
34	5.730585106	192.168.74.128	143.93.63.8	SSHv2	166	Client: Encrypted packet (len=112)
40	6.263563778	192.168.74.128	143.93.63.8	SSHv2	1150	Client: Encrypted packet (len=1096)
18	0.100696849	192.168.74.128	143.93.63.8	SSHv2	102	Client: Diffie-Hellman Key Exchange Init

> Frame 18: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface ens33, id 0

> Ethernet II, Src: VMware_9a:e9:b7 (00:0c:29:9a:e9:b7), Dst: VMware_fd:4b:78 (00:50:56:fd:4b:78)

> Internet Protocol Version 4, Src: 192.168.74.128, Dst: 143.93.63.8

> Transmission Control Protocol, Src Port: 58342, Dst Port: 22, Seq: 1554, Ack: 1114, Len: 48

> SSH Protocol

SSH Version 2 (encryption:chacha20-poly1305@openssh.com mac:<implicit> compression:none)

Packet Length: 44

Padding Length: 6

Key Exchange

Message Code: Diffie-Hellman Key Exchange Init (30)

Multi Precision Integer Length: 32

DH client e: e67158a35b31bb69c7dc37d808d76fb8f7460a6e4ee6183e...

Padding String: 000000000000

[Direction: client-to-server]

-f

20	0.199697952	143.93.63.8	192.168.74.128	SSHv2	506	Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=172)
10	0.039997234	192.168.74.128	143.93.63.8	SSHv2	95	Client: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.4)
21	0.202661807	192.168.74.128	143.93.63.8	SSHv2	70	Client: New Keys
14	0.073315409	192.168.74.128	143.93.63.8	SSHv2	1566	Client: Key Exchange Init

SSH Version 2 (encryption:chacha20-poly1305@openssh.com mac:<implicit> compression:none)

Packet Length: 260

Padding Length: 9

Key Exchange

Message Code: Diffie-Hellman Key Exchange Reply (31)

> KEX host key (type: ecdsa-sha2-nistp256)

Multi Precision Integer Length: 32

DH server f: 64083bd57c1218ab9d5d0c635c18f629276fe82f8a39738...

KEX H signature length: 101

KEX H signature: 0000001365636473612d736861322d6e6973747032353600...

Padding String: 000000000000000000

SSH Version 2 (encryption:chacha20-poly1305@openssh.com mac:<implicit> compression:none)

Packet Length: 12

Padding Length: 10

Key Exchange

Message Code: New Keys (21)

Padding String: 000000000000000000

Signatur

KEX H signature length: 101
KEX H signature: 0000001365636473612d736861322d6e6973747032353600...
Padding String: 0000000000000000
SSH Version 2 (encryption:chacha20-poly1305@openssh.com mac:<implicit> compression:none)
Packet Length: 12
Padding Length: 10
Key Exchange