

# Protokoll - Network Sniffing und Portscanning

Manuel Neufeld, Dennis Tobias Rautenberg

October 19, 2016

# Chapter 1

## Intro

### 1.1 Versuchsaufbau

Bei unserem Versuchsaufbau in unserem Labor wurde der bestehende Switch durch einen Hub ersetzt, um so alle Datenpakete aller Teilnehmer mitlesen/sniffen zu können.

### 1.2 Software

Wir verwenden für die uns bevorstehende Aufgabe das Betriebssystem Ubuntu und die Software Wireshark.



Figure 1.1: Wireshark Logo

## Chapter 2

# Grundlagen des Network-Sniffing

## Chapter 3

# Aufgaben

### 3.1 a.) Analyse von typischem Netzwerkverkehr

#### 3.1.1 Aufbauen einer TCP Verbindung

Bauen Sie eine TCP Verbindung zu einem Dienst (z.B. http(s), ftp, smb, ssh, telnet) ihrer Wahl auf und beschreiben sie den Ablauf des Verbindungsaufbau/Verbindungsabbau (Sequenzdiagramm).

401	76.515640806	141.62.66.1	141.62.66.235	TCP	74	58827	>	80	[SYN]	Seq=0	Win=29280	Len=0	MSS=1460	SACK_PERM=1	TSval=321676	TSecr=0	WS=128	
402	76.515917006	141.62.66.235	141.62.66.1	TCP	74	80	>	58827	[SYN, ACK]	Seq=0	Ack=1	Win=14480	Len=0	MSS=1460	SACK_PERM=1	TSval=3233767844	TSecr=321676	WS=128
403	76.516354006	141.62.66.1	141.62.66.235	TCP	66	58827	>	80	[ACK]	Seq=1	Ack=1	Win=29312	Len=0	TSval=321677	TSecr=3233767844			

Figure 3.1: TCP Connection - HTTP Port: 80

#### 3.1.2 Verbindungsversuch - geschlossener TCP Port

Was passiert bei einem Verbindungsversuch auf einem geschlossenen TCP Port (Sequenzdiagramm), z.B. telnet auf Port 161 (Befehl: telnet < ip > 161).

```
praktikum@rn07:~$ telnet 141.62.66.235 161
Trying 141.62.66.235...
telnet: Unable to connect to remote host: Connection refused
praktikum@rn07:~$
```

Figure 3.2: Verbindung per Telnet zu einem geschlossenen Port

Gescheiterter Verbindungsversuch aufgezeichnet mit Wireshark.

```
praktikum@rn07:~$ nmap 141.62.66.235 -p161

Starting Nmap 6.40 ( http://nmap.org ) at 2016-10-14 11:19 CEST
Nmap scan report for 141.62.66.235
Host is up (0.00070s latency).
PORT      STATE      SERVICE
161/tcp    closed     snmp

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
praktikum@rn07:~$
```

Figure 3.3: Nmap Port Scan - Closed Port

Filter: tcp.port == 161    udp.port == 161							
No.	Time	Source	Destination	Protocol	Length	Info	
258	82.064660000	141.62.66.7	141.62.66.235	TCP	74	39243 > 161 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=446310 TSecr=0 WS=128	
259	82.065351000	141.62.66.235	141.62.66.7	TCP	60	161 > 39243 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
284	89.392530000	141.62.66.7	141.62.66.235	TCP	74	39244 > 161 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=448142 TSecr=0 WS=128	
285	89.393115000	141.62.66.235	141.62.66.7	TCP	60	161 > 39244 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	

Figure 3.4: Capturing mit Wireshark

### 3.1.3 Beobachtung - DNS Traffic

Sniffen Sie den DNS Traffic aus dem Netzwerkverkehr heraus, was beobachten Sie?

Filter: tcp.port == 53    udp.port == 53							
No.	Time	Source	Destination	Protocol	Length	Info	
66	14.678365000	141.62.66.7	141.62.66.250	DNS	77	Standard query 0xfbb3 A 141.62.66.235:161	
67	14.678380000	141.62.66.7	141.62.66.250	DNS	77	Standard query 0x79a3 AAAA 141.62.66.235:161	
68	14.683921000	141.62.66.250	141.62.66.7	DNS	152	Standard query response 0xfbb3 No such name	
69	14.684639000	141.62.66.250	141.62.66.7	DNS	152	Standard query response 0x79a3 No such name	
70	14.684723000	141.62.66.7	141.62.66.250	DNS	102	Standard query 0x9575 A 141.62.66.235:161.rnlabor.hdm-stuttgart.de	
71	14.684733000	141.62.66.7	141.62.66.250	DNS	102	Standard query 0xf753 AAAA 141.62.66.235:161.rnlabor.hdm-stuttgart.de	
72	14.690029000	141.62.66.250	141.62.66.7	DNS	163	Standard query response 0x9575 No such name	
73	14.690407000	141.62.66.250	141.62.66.7	DNS	163	Standard query response 0xf753 No such name	
385	117.675832000	141.62.66.2	141.62.66.250	DNS	69	Standard query 0x0f9d A google.de	
386	117.676582000	141.62.66.2	141.62.66.2	DNS	85	Standard query response 0x0f9d A 216.58.208.35	
389	117.682058000	141.62.66.2	141.62.66.250	DNS	86	Standard query 0x37ac PTR 35.208.58.216.in-addr.arpa	
390	117.682592000	141.62.66.250	141.62.66.2	DNS	163	Standard query response 0x37ac PTR fra15s12-in-f3.1e100.net PTR fra15s12-in-f35.1e100.net	

Figure 3.5: Capturing mit Wireshark

### 3.1.4 Filtern von nicht IP basiertem Traffic

Filtern Sie den nicht IP basierten Traffic heraus. Was bleibt nun noch übrig?

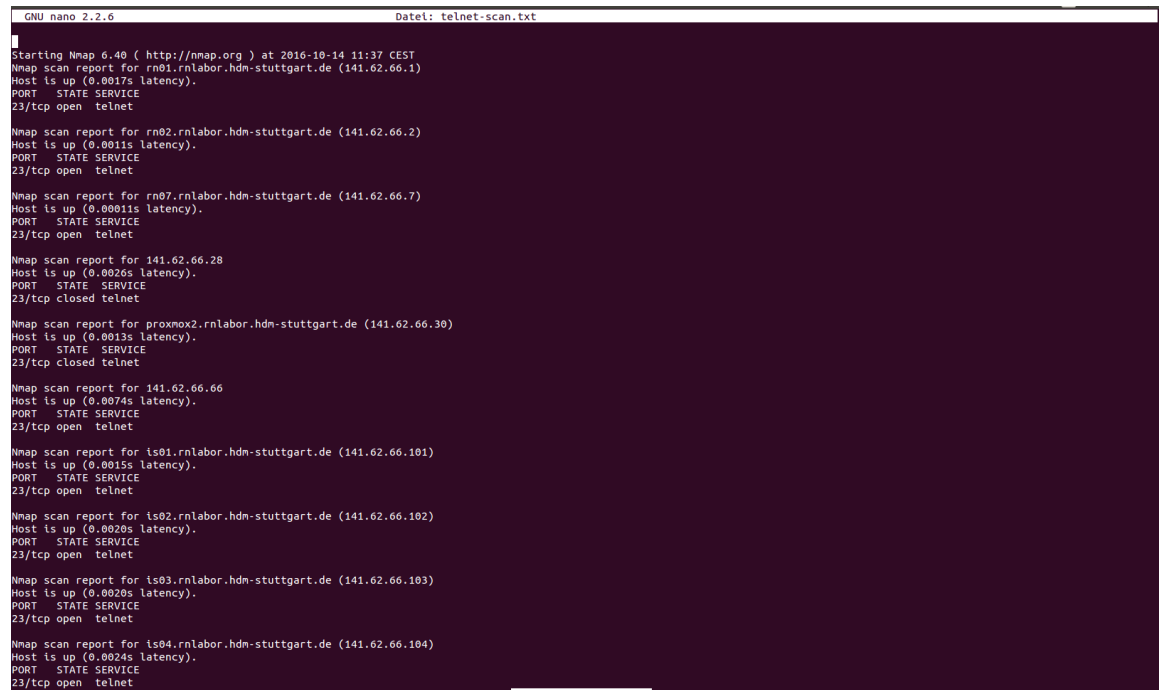
Filter: <b>not ipv6 and not ip</b>		Expression...	Clear	Apply	Speichern
No.	Time	Source	Destination	Protocol	Length Info
1	0.000000000	00:1d:b3:bb:5b:ae	01:80:c2:00:00:00	STP	119 MST. Root = 32768/0/00:1d:b3:bb:5b:a0 Cost = 0 Port = 0x8012
2	0.000157000	00:1d:b3:bb:5b:ae	01:80:c2:00:00:00	STP	119 MST. Root = 32768/0/00:1d:b3:bb:5b:a0 Cost = 0 Port = 0x8012
3	4.000562000	00:1d:b3:bb:5b:ae	01:80:c2:00:00:00	STP	119 MST. Root = 32768/0/00:1d:b3:bb:5b:a0 Cost = 0 Port = 0x8012
4	4.528432000	00:1d:b3:bb:5b:ae	01:80:c2:00:00:0e	LLDP	167 Chassis Id = 00:1d:b3:bb:5b:a0 Port Id = 18 TTL = 120 System Name = ProCurve 2810-24_215
12	5.999789000	00:1d:b3:bb:5b:ae	01:80:c2:00:00:00	STP	119 MST. Root = 32768/0/00:1d:b3:bb:5b:a0 Cost = 0 Port = 0x8012
33	7.999696000	00:1d:b3:bb:5b:ae	01:80:c2:00:00:00	STP	119 MST. Root = 32768/0/00:1d:b3:bb:5b:a0 Cost = 0 Port = 0x8012
34	8.209573000	00:1d:b3:bb:5b:a0	09:00:09:00:00:67	HP	106 HP Switch Protocol
35	8.237516000	b4:39:d6:08:b5:30	01:80:c2:00:00:0e	LLDP	167 Chassis Id = b4:39:d6:08:b5:20 Port Id = 16 TTL = 120 System Name = ProCurve 2810-24_214
36	8.248847000	00:1f:fe:4a:c1:20	09:00:09:00:00:67	HP	122 HP Switch Protocol
37	8.975322000	b4:39:d6:08:b5:20	09:00:09:00:00:67	HP	122 HP Switch Protocol
48	9.999645000	00:1d:b3:bb:5b:ae	01:80:c2:00:00:00	STP	119 MST. Root = 32768/0/00:1d:b3:bb:5b:a0 Cost = 0 Port = 0x8012
59	11.999024000	00:1d:b3:bb:5b:ae	01:80:c2:00:00:00	STP	119 MST. Root = 32768/0/00:1d:b3:bb:5b:a0 Cost = 0 Port = 0x8012
60	12.219791000	c0:39:35:5f:36:1e	ff:ff:ff:ff:ff:ff	ARP	60 Who has 141.62.66.110? Tell 141.62.66.112
63	13.061040000	00:c1:6e:e0:1b:0f	ff:ff:ff:ff:ff:ff	ARP	60 Who has 141.62.66.250? Tell 141.62.66.111
64	14.016498000	00:1d:b3:bb:5b:ae	01:80:c2:00:00:00	STP	119 MST. Root = 32768/0/00:1d:b3:bb:5b:a0 Cost = 0 Port = 0x8012
85	16.009813000	00:1d:b3:bb:5b:ae	01:80:c2:00:00:00	STP	119 MST. Root = 32768/0/00:1d:b3:bb:5b:a0 Cost = 0 Port = 0x8012
86	18.009809000	00:1d:b3:bb:5b:ae	01:80:c2:00:00:00	STP	119 MST. Root = 32768/0/00:1d:b3:bb:5b:a0 Cost = 0 Port = 0x8012
88	19.685751000	78:ac:c0:c4:21:09	00:0d:b9:3e:b4:a5	ARP	42 Who has 141.62.66.250? Tell 141.62.66.7
89	19.686321000	00:0d:b9:3e:b4:a5	78:ac:c0:c4:21:09	ARP	60 141.62.66.250 is at 00:0d:b9:3e:b4:a5
90	20.009764000	00:1d:b3:bb:5b:ae	01:80:c2:00:00:00	STP	119 MST. Root = 32768/0/00:1d:b3:bb:5b:a0 Cost = 0 Port = 0x8012
91	22.009808000	00:1d:b3:bb:5b:ae	01:80:c2:00:00:00	STP	119 MST. Root = 32768/0/00:1d:b3:bb:5b:a0 Cost = 0 Port = 0x8012
92	24.009544000	00:1d:b3:bb:5b:ae	01:80:c2:00:00:00	STP	119 MST. Root = 32768/0/00:1d:b3:bb:5b:a0 Cost = 0 Port = 0x8012
104	26.009585000	00:1d:b3:bb:5b:ae	01:80:c2:00:00:00	STP	119 MST. Root = 32768/0/00:1d:b3:bb:5b:a0 Cost = 0 Port = 0x8012
113	28.009452000	00:1d:b3:bb:5b:ae	01:80:c2:00:00:00	STP	119 MST. Root = 32768/0/00:1d:b3:bb:5b:a0 Cost = 0 Port = 0x8012
117	30.009563000	00:1d:b3:bb:5b:ae	01:80:c2:00:00:00	STP	119 MST. Root = 32768/0/00:1d:b3:bb:5b:a0 Cost = 0 Port = 0x8012
118	32.009582000	00:1d:b3:bb:5b:ae	01:80:c2:00:00:00	STP	119 MST. Root = 32768/0/00:1d:b3:bb:5b:a0 Cost = 0 Port = 0x8012
Frame 88: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0					
Ethernet II, Src: 78:ac:c0:c4:21:09 (78:ac:c0:c4:21:09), Dst: 00:0d:b9:3e:b4:a5 (00:0d:b9:3e:b4:a5)					
Address Resolution Protocol (request)					
1000	00 0d b9 3e b4 a5 78 ac	c0 c4 21 09 08 06 00 01	...	X.	...
1010	00 00 06 04 00 01 78 ac	c0 c4 21 09 8d 3e 42 07	.....	X.	...>B.
1020	00 00 00 00 00 00 8d 3e	42 fa	.....>	B.	

Figure 3.6: Capturing mit Wireshark

## 3.2 b.) Sniffing von Passwörtern

### 3.2.1 Verbindung zu Telnet und FTP

Verbinden Sie sich mit anderen Telnet und FTP Servern, nutzen Sie den PC Ihres Nachbarn!



```
GNU nano 2.2.6                                Datei: telnet-scan.txt
Starting Nmap 6.40 ( http://nmap.org ) at 2016-10-14 11:37 CEST
Nmap scan report for rn01.rnlabor.hdm-stuttgart.de (141.62.66.1)
Host is up (0.0017s latency).
PORT      STATE SERVICE
23/tcp    open  telnet

Nmap scan report for rn02.rnlabor.hdm-stuttgart.de (141.62.66.2)
Host is up (0.0011s latency).
PORT      STATE SERVICE
23/tcp    open  telnet

Nmap scan report for rn07.rnlabor.hdm-stuttgart.de (141.62.66.7)
Host is up (0.00011s latency).
PORT      STATE SERVICE
23/tcp    open  telnet

Nmap scan report for 141.62.66.28
Host is up (0.0026s latency).
PORT      STATE SERVICE
23/tcp    closed telnet

Nmap scan report for proxmox2.rnlabor.hdm-stuttgart.de (141.62.66.30)
Host is up (0.0013s latency).
PORT      STATE SERVICE
23/tcp    closed telnet

Nmap scan report for 141.62.66.66
Host is up (0.0074s latency).
PORT      STATE SERVICE
23/tcp    open  telnet

Nmap scan report for is01.rnlabor.hdm-stuttgart.de (141.62.66.101)
Host is up (0.0015s latency).
PORT      STATE SERVICE
23/tcp    open  telnet

Nmap scan report for is02.rnlabor.hdm-stuttgart.de (141.62.66.102)
Host is up (0.0020s latency).
PORT      STATE SERVICE
23/tcp    open  telnet

Nmap scan report for is03.rnlabor.hdm-stuttgart.de (141.62.66.103)
Host is up (0.0020s latency).
PORT      STATE SERVICE
23/tcp    open  telnet

Nmap scan report for is04.rnlabor.hdm-stuttgart.de (141.62.66.104)
Host is up (0.0024s latency).
PORT      STATE SERVICE
23/tcp    open  telnet
```

Figure 3.7: Capturing mit Wireshark

### **3.2.2 Passwort Sniffing**

Versuchen Sie Passwörter und Benutzernamen anderer Benutzer, mitzusniffen.  
Filtern Sie gezielt die entsprechenden Pakete heraus.



### **3.2.3 Unterschied des übermittelten Passworts**

Beschreiben Sie den Unterschied zwischen dem FTP und Telnet Protokoll bezüglich der Passwort Übermittlung.

## **3.3 c.) Portscanning / Nmap**

### **3.3.1 Scannen vom Labornetz**

Scannen Sie das gesamte Labor Netz um aktive Systeme zu erkennen.

### **3.3.2 Genauere Untersuchung eines Rechners**

Nehmen Sie einen Rechner genauer unter die Lupe und führen Sie einen detaillierten Portscan sowohl für TCP als auch für UDP Dienste durch.

### **3.3.3 Verschiedene Scanverfahren**

Beobachten Sie die unterschiedlichen Scan-Varianten (Syn, Fin, Xmas, etc.) in Wireshark und analysieren Sie diese.

## Chapter 4

# Unterschied - Hub / Switch

### 4.1 Hub

Ein Hub ist ein Kopplungselement, das mehrere Hosts in einem Netzwerk miteinander verbindet. In einem Ethernet-Netzwerk, das auf der Stern-Topologie basiert, dient ein Hub als Verteiler fuer die Datenpakete. Hubs arbeiten auf der Bituebertragungsschicht (Schicht 1) des OSI-Schichtenmodells und sind damit auf die reine Verteilfunktion beschraenkt. Ein Hub nimmt ein Datenpaket entgegen und sendet es an alle anderen Ports weiter. Das bedeutet, er broadcastet. Dadurch sind nicht nur alle Ports belegt, sondern auch alle Hosts. Sie bekommen alle Datenpakete zugeschickt, auch wenn sie nicht die Empfaenger sind. Fuer die Hosts bedeutet das auch, dass sie nur dann senden koennen, wenn der Hub gerade keine Datenpakete sendet. Sonst kommt es zu Kollisionen.<sup>1</sup>

### 4.2 Switch

Ein Switch ist ein Kopplungselement, das mehrere Hosts in einem Netzwerk miteinander verbindet. In einem Ethernet-Netzwerk, das auf der Stern-Topologie basiert, dient ein Switch als Verteiler fuer die Datenpakete. Die Funktion ist aehnlich einem Hub, mit dem Unterschied, das ein Switch direkte Verbindungen zwischen den angeschlossenen Geraeten schalten kann, sofern ihm die Ports der Datenpaket-Empfaenger bekannt sind. Wenn nicht, dann broadcastet der Switch die Datenpakete an alle Ports. Wenn die Antwortpakete von den Empfaengern zurueck kommen, dann merkt sich der Switch die MAC-Adressen der Datenpakete und den dazugehoerigen Port und sendet die Datenpakete dann nur noch dorthin. Waehrend ein Hub die Bandbreite des Netzwerks limitiert, steht der Verbindung zwischen zwei Hosts, die volle Bandbreite der Ende-zu-Ende-Netzwerk-Verbindung zur Verfuegung.<sup>2</sup>

---

<sup>1</sup><http://www.elektronik-kompodium.de/sites/net/1405161.htm>

<sup>2</sup><http://www.elektronik-kompodium.de/sites/net/0811021.htm>