Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Labreport, Gruppe 4

Projekt Netzwerk-Infrastruktur WS 2017/18

vorgelegt von

Dewin Bagci: 5bagci@informatik.uni-hamburg.de
Karan Popat: karan.popat@outlook.de
Hanife Demircioglu: h.demircioglu@hotmail.de

MIN-Fakultät

Fachbereich Informatik

Abgabedatum: 01.03.2018

Dozent: Robert Olotu

Inhaltsverzeichnis

1 Abkürzungsverzeichnis

Abbildungsverzeichnis

Part 3: Network Troubleshooting Utilities

Universität Hamburg

DER FORSCHUNG | DER LEHRE | DER BILDUNG

Abbildung 1: Broadcast und Multicast

Exercise 6: Managing Services (Please use pnidX-svr-mu)

Exercise 7: Configure the following network (figure 1) using ifconfig and route add

Exercise 8: Configure the following network (figure 1) using ip and nmcli

Exercise 9: Configure the following network (figure 1) using GUI

Part 4: Network Scanning

Exercise 1: Configure the networks of figure 1

Exercise 2: NMAP

Exercise 3: Nessus network device identification

Exercise 4: OpenVAS Network device identification

Part 5: Sniffing, Virtual Private Network (VPN)

Exercise 1: Configure and set the networks shown below (figure1 and 2)

Exercise 2: Getting started with network monitoring tools

Exercise 3: TCPDUMP

Exercise 4: Wireshark

Question 1: Please type and examine the syntax for a Wireshark command which capture filter so that all IP datagrams with source or destination IP address equal to 10.88.X.? are recorded.

Answer 1: Mit dem Filter: *ip.addr == 10.88.40.70* können wir alle Netzwerkpakete, welche über die Schnittstelle 10.88.40.70 gesendet oer empfangen werden, abfangen und anzeigen lassen.

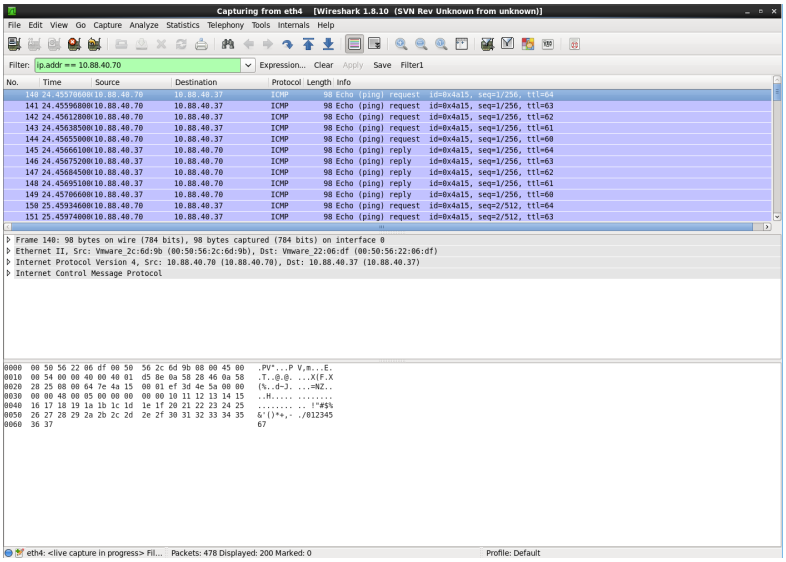

Abbildung 2: Wireshark Filter ip.addr == 10.88.40.70

Question 2: Please type and examine the syntax for a Wireshark display filter that shows IP datagrams with destination IP address equal to 10.88.X.? and frame size greater than 400 bytes.

Answer 2: Um alle Datenpakete abzufangen, die mindestens 400 Byte groß sind, bedarf eine kleine Erweiterung des vorherigen Befehls. Der Filter lautet nun: *ip.addr == 10.88.40.70 && frame.len > 400*. Mit dem Teil *frame.len > X* können wir die Datenpakete nach Bytegröße X Filtern. Für X gilt, $X < 2^{32} \wedge X \in \mathbb{N}$.

Question 3: Please type and examine the syntax for a Wireshark display filter that shows packets containing ICMP messages with source or destination IP address equal to 10.88.X.? and frame numbers between 15 and 30

Answer 3: Der Filter lautet: *ip.addr == 10.88.40.70 && (frame.number > 15 && frame.number < 30)*. ICMP steht für Internet Control Message Protocol und übermittelt hauptsächlich Diagnose-informationen zwischen dem Router und dem Host.

Question 4: Please type and examine the syntax for a Wireshark display filter that

shows packets containing TCP segments with source or destination IP address equal to 10.88.X.? and using port number 23.

Answer 4: Damit wir alle TCP Pakete eines Hosts über die Port 23 abfangen können wird der folgende Filter eingesetzt: *ip.dst == 10.88.40.70 and tcp.port == 23*. Bei TCP handelt es sich um ein Übertragungsprotokoll (Transmission Control Protocol) aus der Familie der Internetprotokolle. Port 23 ist standardisiert für den Service Telnet.

Question 5: Please type and examine a Wireshark capture filter expression for Q4.

Answer 5: Der Filter ist ähnlich wie in Q4, lediglich die Konfiguration findet an einer anderen Stelle statt.

Question 6: Please type and examine the syntax for a Wireshark command which, by default, collects packets with source or destination IP address 10.88.X.? on interface eth4.

Answer 6: Innerhalb des Terminals lässt sich der Filter: wireshark -i eth4 -k -f "host 10.88.40.70", anwenden. Die Argumente bedeuten dabei folgendes: -i eth4 steht für Interface, -k startet das Abfangen von Paketen und -f "host 10.88.40.70", ist der Paketfilter.

Question 7: : Please type and examine the syntax of a display filter which selects the TCP packets with destination IP address 10.88.X.?, and TCP port number 23.

Answer 7: Der Filter lautet: *ip.addr == 10.88.40.70 && tcp.port == 23* und fängt alle ein-/ausgehenden Pakete der Ip Adresse 10.88.40.70 über den Port 23 (Telnet) ab.

Question 8: Please login to the server pnidX-mid-hh and start an ftp client to the server pnidXcnt-bln(vsftpd daemon should be running on pnidX-cnt-bln). Please use wireshark on pnidX-mid-bln to sniff or capture the username and password of the ftp service between pnidX-mid-hh and pnidX-cnt-bln. Is this possible, show your result of the capture

Answer 8: Mithilfe von Wireshark können wir leicht das Telnet login Passwort herausfinden, da bei der Übertragung via Telnet die Pakete unverschlüsselt übertragen werden. Dazu starten wir zunächst Wirehsark auf dem Host pnid4-mid-hh.

Question 9: Please login to the server pnidX-mid-hh and start an ssh client to the server pnidX-cnt-bln(sshd daemon should be running on pnidX-cnt-bln). Please use wireshark on pnidX-mid-bln to sniff or capture the username and password of the ssh service between pnidX-mid-hh and pnidX-cnt-bln. Is this possible, show the result of the capture.

Answer 9: Anders als Telnet werden bei shh (Secure Shell) die Pakete verschlüsselt übertragen, sodass es nicht möglich ist das Passwort mitzulesen. Zuerst starten wir wireshark auf dem Host pnid4-mid-hh.

Exercise 5: Experimenting with network monitoring tools

Exercise: In this exercise you will connect to the webserver pnidX-cnt-bln from pnidX-mid-hh. Let pnidX-cnt-bln determine your IP-address and the OS you are running. Then, connect to a service of your choice (e.g. ftp, http, ssh etc.) on pnidX cnt-bln. Let pnidX-mid-hh determine which services are running on pnidX-cnt-bln.

Solution: Wir führen zunächst nmap auf dem Host pnid4-cnt-bln aus und übergeben dabei die Zieladresse des Hosts pnid4-mid-hh, damit wir sehen können welche Ports geöffnet sind bzw. welcher Service auf dem Zielhost gerade aktiv ist.

[IMAGE]

Wir sehen nun, dass die Ports 21 ftp, 22 ssh, 23 telnet, 80 http und 111 rpcbind offen sind und entscheiden uns via Telnet vom Quellhost pnid4-cnt-bln bei dem Zielhost

pnid-mid-hh anzumelden.
[IMAGE]

Die Ausgabe des letzten Logins zeigt uns, dass die Anmeldung erfolgreich war.

Exercise 6: Set up a host-to-host VPN using preshared key

Exercise 7: Set up a host-to-host VPN using RSA keys

Exercise 8: Set up a network-to-network VPN using preshared key

Exercise 9: Set up a network-to-network VPN using RSA secrets keys

2 Literaturverzeichnis und Quellenverzeichnis