

Warsztaty - L6 - SK

Prowadzący: Tomasz Wierzbicki

Wiktor Pilarczyk

15 maja 2020

Komputer został skonfigurowany zgodnie z poleceniami zadania.

1 Część 1.

1.1 Co dzieje się, kiedy dodajesz jakiś wpis?

Zostają wysłane odpowiednie żądania i odpowiedzi.

1.2 Dlaczego przeglądarka wyświetla w pasku stanu komunikat **Waiting for sieci.ii.uni.wroc.pl** a odpowiedni wpis nie został dodany?

Komunikat jest wyświetlany, ponieważ czeka na odpowiedź od serwera, ale my „przechwyciliśmy” zapytanie przez co, nie dostaje odpowiedzi, a z tego wynika dlaczego nie zmieniła się zawartość strony.

1.3 Co zapisał ten program do pliku **http request**?

W pliku znajduje się nasze żądanie.

1.4 Ręczne wysłanie żądania

Po komendzie `nc -q 3 sieci.ii.uni.wroc.pl 80 ; http request` odpowiedni komunikat został dodany, również przy zmianie treści żądania.

2 Część 2.

Za pomocą komendy - dig A www.debian.org otrzymujemy adres ip przypisany do domeny - 130.89.148.77

Następnie w jednej konsoli wykonujemy - (while true; do netstat -tan — grep 130.89.148.77 ; done) — tee tcp_log), a w drugiej - wget 130.89.148.77

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	130.89.148.77	10.0.2.15	TCP	76	80->36066 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
2	0.112699425	130.89.148.77	10.0.2.15	TCP	62	80->36066 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
3	0.112648324	10.0.2.15	130.89.148.77	TCP	56	36066->80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	0.112771872	10.0.2.15	130.89.148.77	HTTP	196	GET / HTTP/1.1
5	0.112923661	130.89.148.77	10.0.2.15	TCP	62	80->36066 [ACK] Seq=1 Ack=141 Win=65535 Len=0
6	0.147988324	130.89.148.77	10.0.2.15	HTTP	973	HTTP/1.1 200 OK (text/html)
7	0.148085361	10.0.2.15	130.89.148.77	TCP	56	36066->80 [ACK] Seq=141 Ack=918 Win=63323 Len=0
8	0.291131398	10.0.2.15	130.89.148.77	TCP	56	36066->80 [FIN, ACK] Seq=141 Ack=918 Win=63323 Len=0
9	0.2911315902	130.89.148.77	10.0.2.15	TCP	62	80->36066 [ACK] Seq=918 Ack=142 Win=65535 Len=0
10	0.323998591	130.89.148.77	10.0.2.15	TCP	62	80->36066 [FIN, ACK] Seq=918 Ack=142 Win=65535 Len=0
11	0.323118367	10.0.2.15	130.89.148.77	TCP	56	36066->80 [ACK] Seq=142 Ack=919 Win=63323 Len=0

Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0

Linux cooked capture

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 130.89.148.77

Transmission Control Protocol, Src Port: 36066, Dst Port: 80, Seq: 0, Len: 0

Source Port: 36066

Destination Port: 80

(Stream index: 0)

[TCP Segment Len: 0]

Sequence number: 0 (relative sequence number)

Next sequence number: 0 (relative sequence number)

Acknowledgment number: 0

1019 ... = Header Length: 40 bytes (10)

Flags: 0x002 (SYN)

Window size value: 64240

Calculated window size: 64240

Checksum: 0x22e4 (unverified)

Checksum Status: Unverified

Urgent pointer: 0

Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale

Timestamps

Rysunek 1: Otrzymane pakiety

Większość odpowiedzi jest na podstawie powyższego zdjęcia.

2.1 Jakie gniazda tworzone są do pobierania pliku przez HTTP?

Gniazda strumieniowe.

2.2 Jaki jest port źródłowy a jaki docelowy połączenia?

Z naszego punktu widzenia port źródłowy to 36066, a docelowy 80.

2.3 Jakie z flag SYN / ACK / FIN są włączone dla danego segmentu?

Rodzaj flag widzimy w sekcji info każdego segmentu.

2.4 Które bajty (strumienia danych protokołu HTTP) są przesyłane w segmencie?

Za pomocą SEQ mówimy, które bajty przesyłamy.

2.5 Które bajty strumienia danych są potwierdzane danym segmentem?

Za pomocą ACK potwierdzamy, do którego momentu mamy otrzymane dane.

2.6 Na podstawie diagramu stanów TCP. Które z tych stanów są widoczne w pliku tcp_log?

SYN_SENT, ESTABLISHED, FIN_WAIT2, TIME_WAIT.

2.7 Która strona wykonuje otwarcie aktywne, a która zamknięcie aktywne?

Klient - my wykonujemy otwarcie aktywne i zamknięcie aktywne.