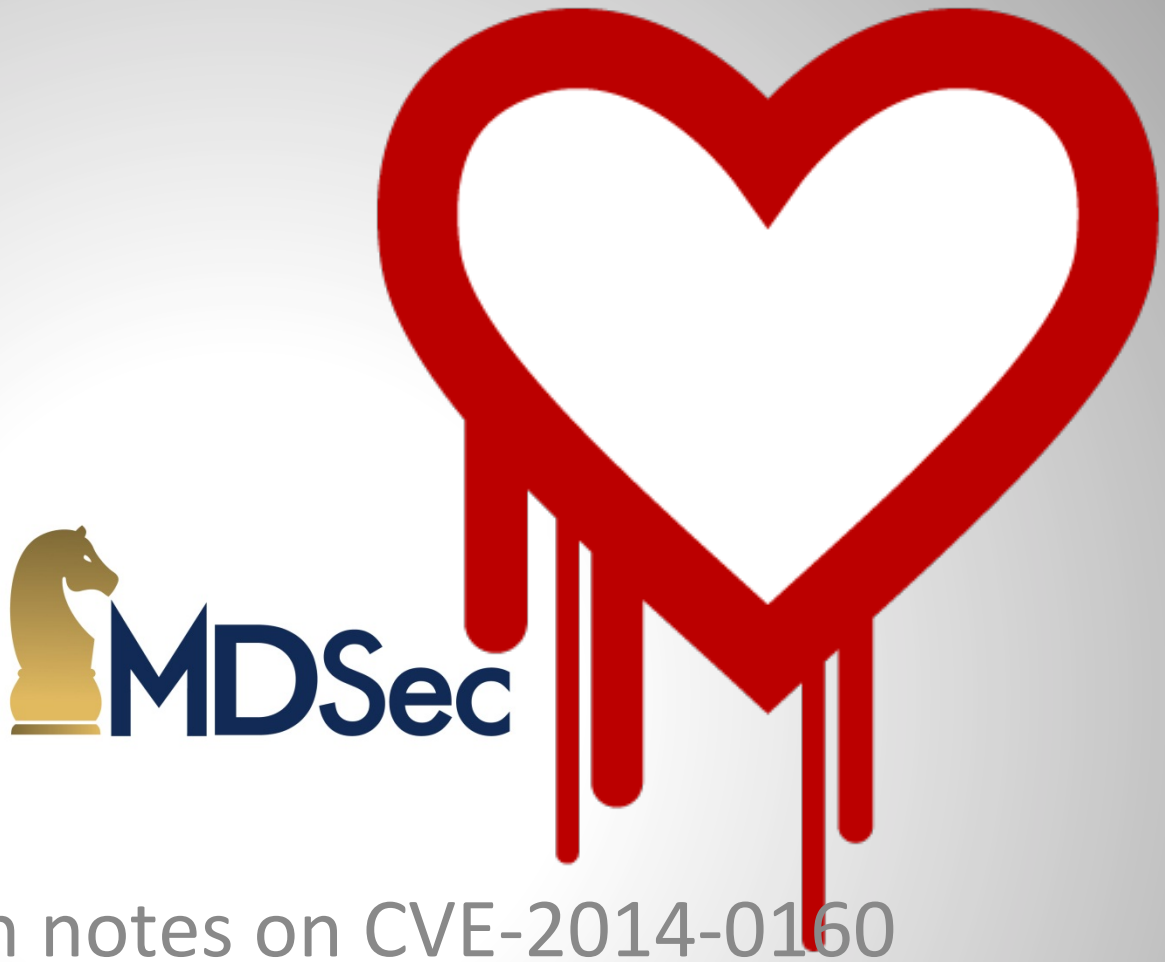
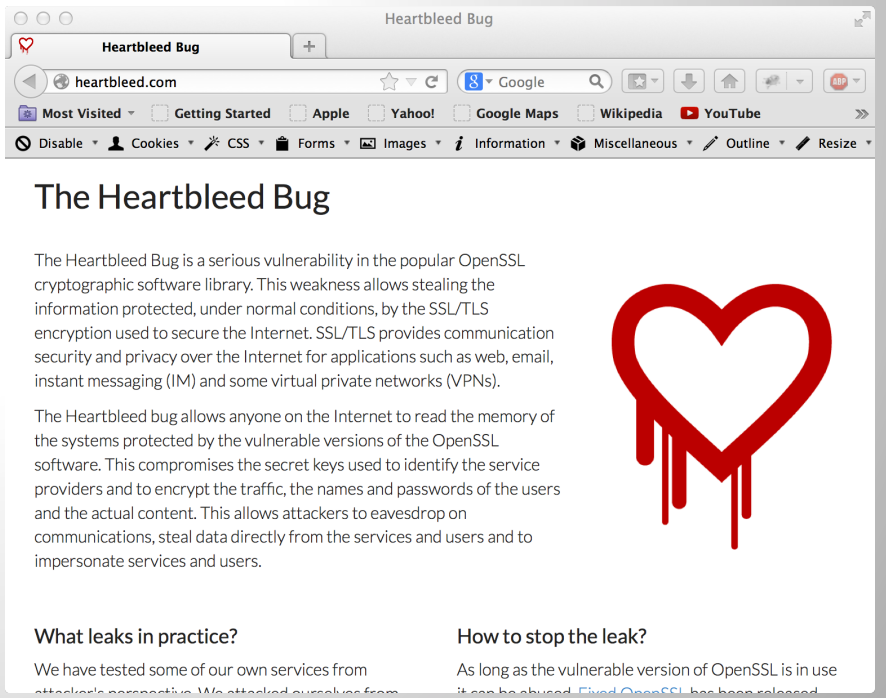


Exploitation notes on CVE-2014-0160

Exploitation notes on CVE-2014-0160

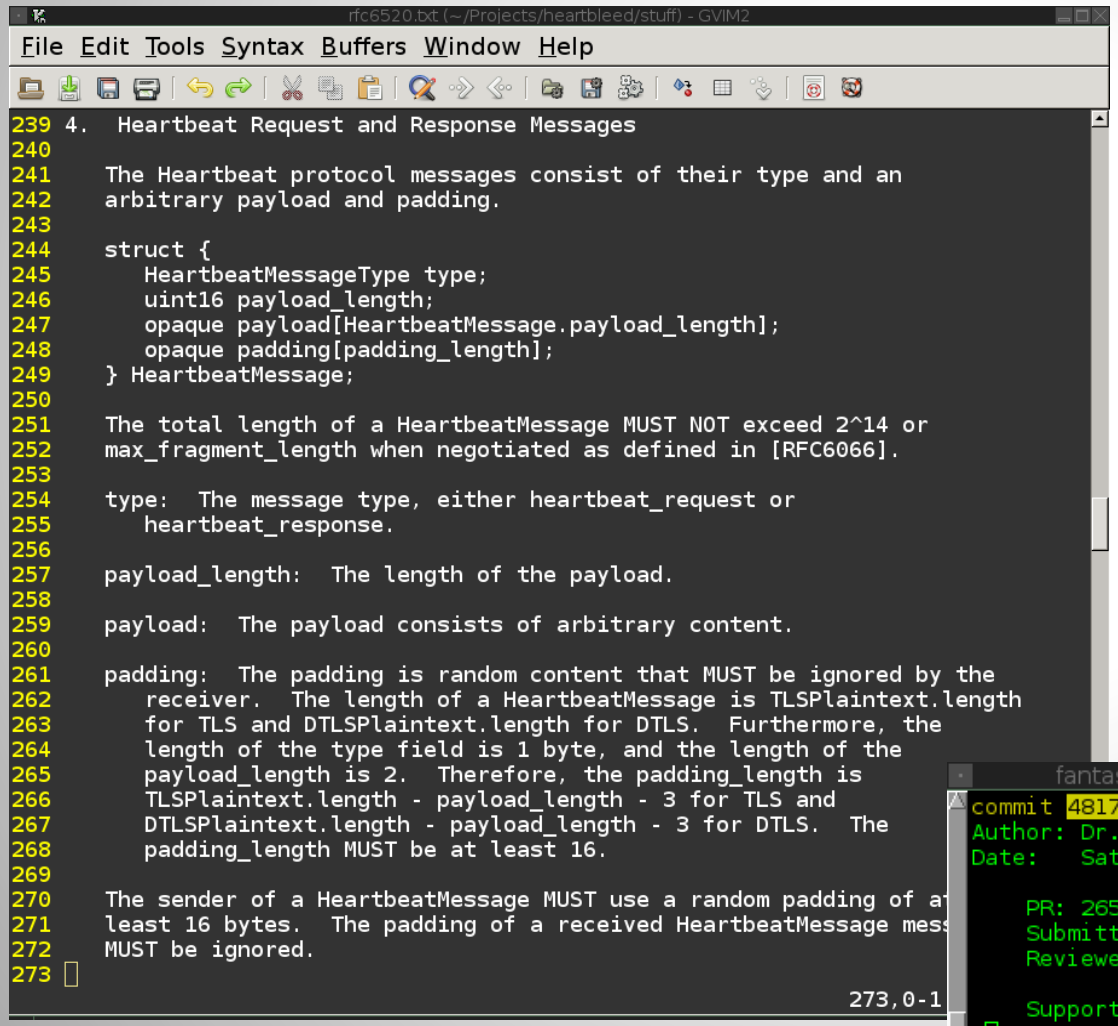
Heartbleed <3

- The vulnerability is announced to the world 7th April 2014 by a website, OpenSSL Security Advisory and OpenSSL 1.0.1g release.
- Discovered by Riku, Antti & Matti and Neel Mehta.
- I searched the page for a web cart.
- Shortly the next day ….
- Jared Stafford released “ssltest.py”
- Security community scrambled to fix.



Exploitation notes on CVE-2014-0160

RFC-6520 Heartbeat Extension

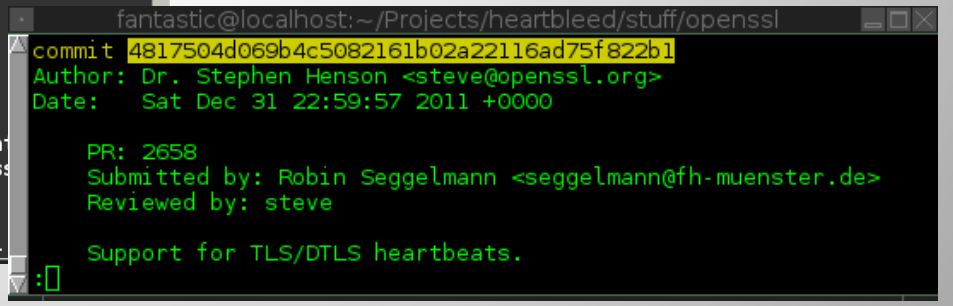


Bug introduced to the world NYE 2011 during implementation of RFC-6520 in OpenSSL 1.0.1

Enabled by default in OpenSSL 1.0.1

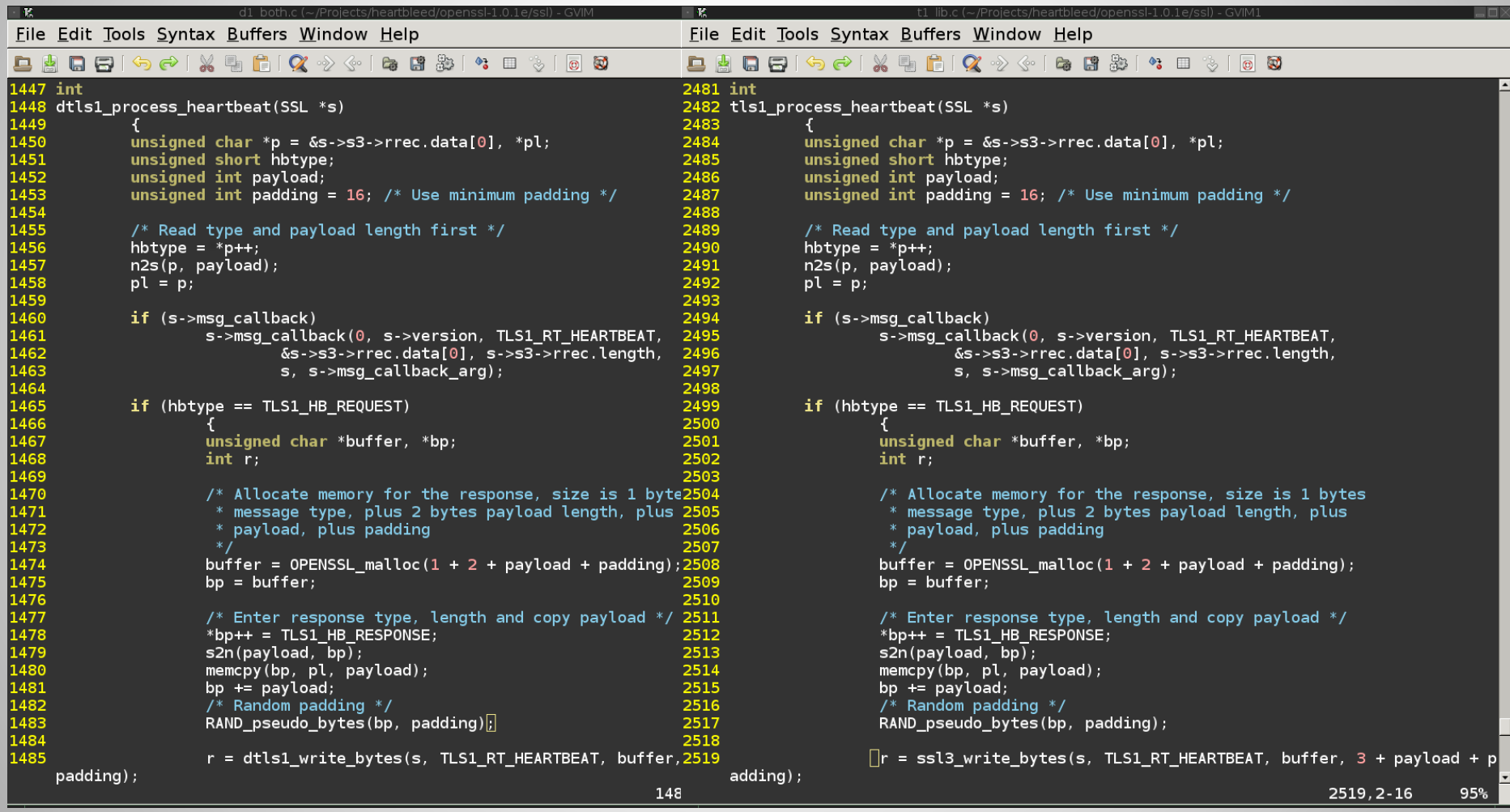
Fixed in OpenSSL 1.0.1g & OpenSSL 1.0.2-beta1 still vulnerable – (git has fix.)

If you run beta code on production servers…



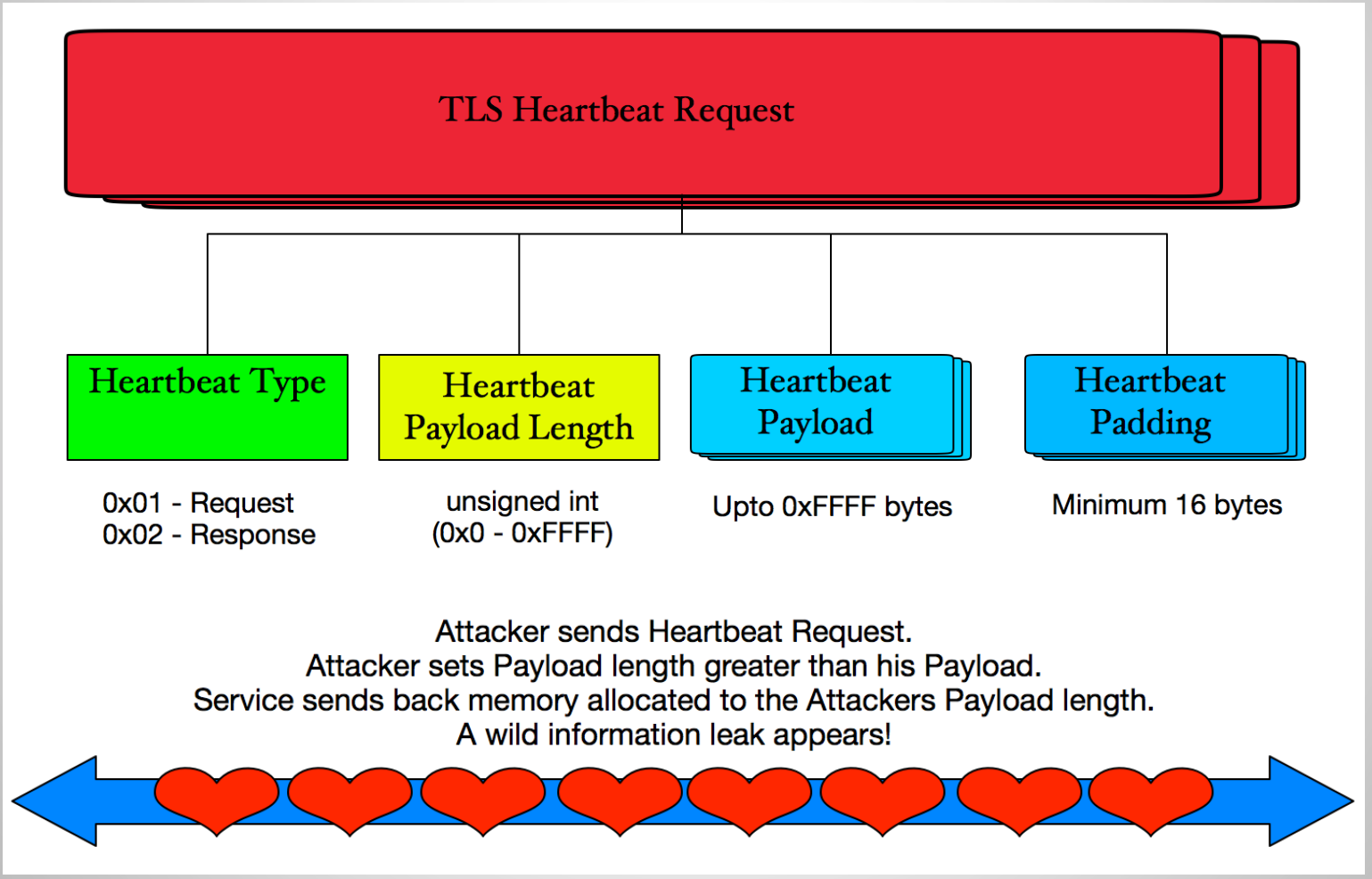
Exploitation notes on CVE-2014-0160

Vulnerability



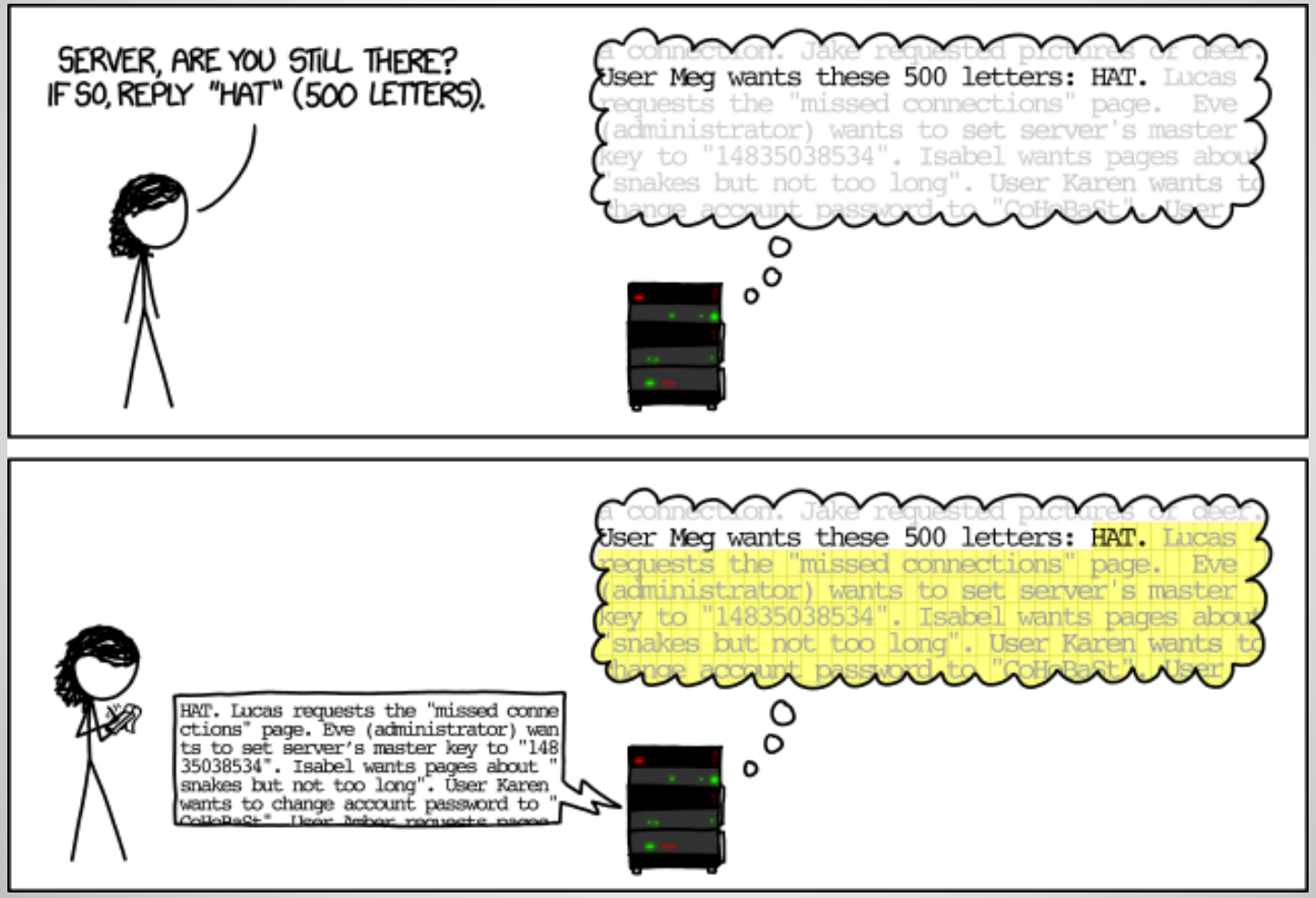
Exploitation notes on CVE-2014-0160

How does it work?



Exploitation notes on CVE-2014-0160

How does it work?



Exploitation notes on CVE-2014-0160

Let the games commence.

Sites ranging from the FBI, Russian Standard Bank, Yahoo!, OpenSSL, Belgian Intelligence Service and many more shown as leaking data.

- Screen shots of “ssltest.py” dumping 16384 bytes of heap memory began to appear on social media sites. The content’s of the memory were alarming.

- IDS/IPS and Security vendors began to release detection signatures & scanners.

- Media frenzy ensued spreading confusing information e.g. #HeartbleedVirus

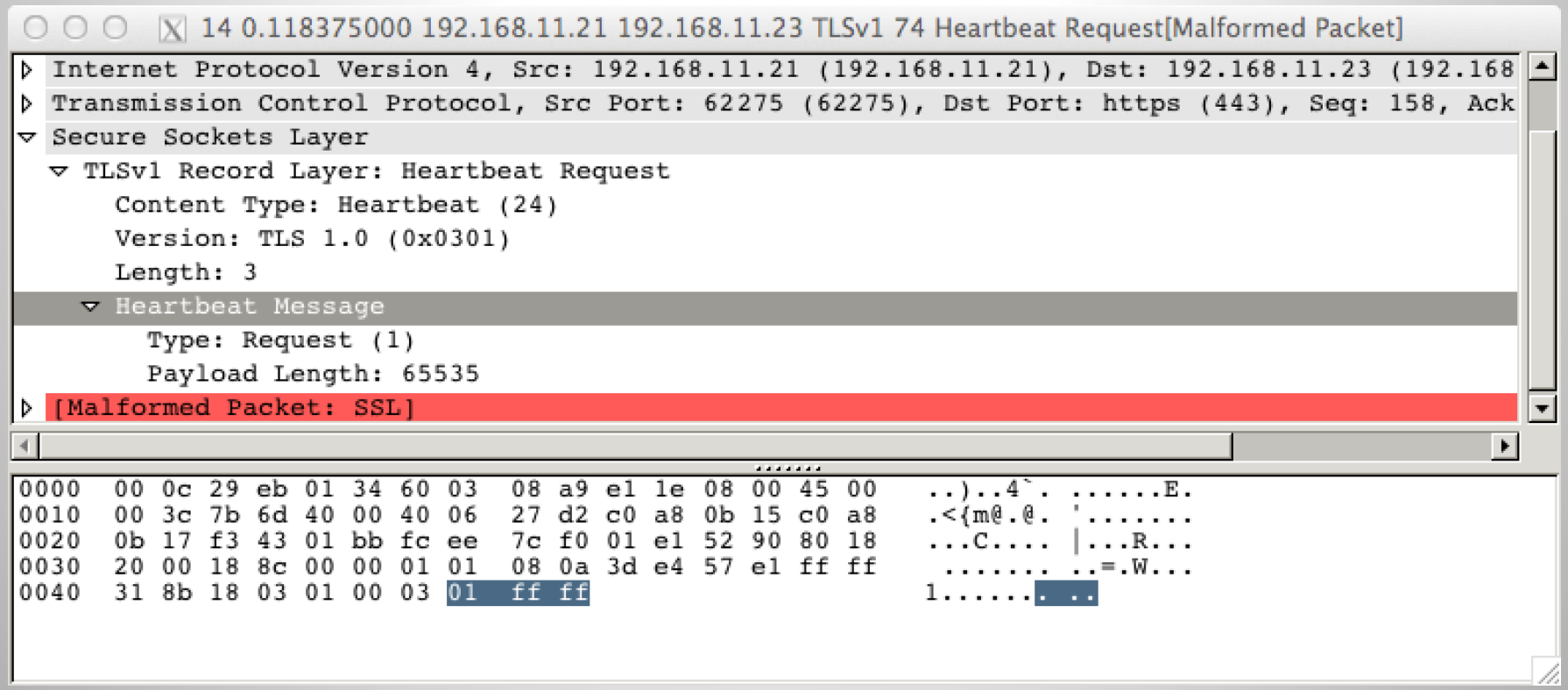
- The vulnerability was still not fully realized. Misconceptions abound.

Source	Destination	Protocol	Length	Info
192.168.11.22	192.168.11.23	SSL	291	Client Hello
192.168.11.23	192.168.11.22	TCP	66	https > 44172 [ACK] Seq=1 Ack=226 Win=30720 Len=0 TSval=4
192.168.11.23	192.168.11.22	TLSv1.1	1407	Server Hello, Certificate, Server Key Exchange, Server He
192.168.11.22	192.168.11.23	TCP	66	44172 > https [ACK] Seq=226 Ack=1342 Win=32000 Len=0 TSva
192.168.11.22	192.168.11.23	TLSv1.1	74	Heartbeat Request

Exploitation notes on CVE-2014-0160

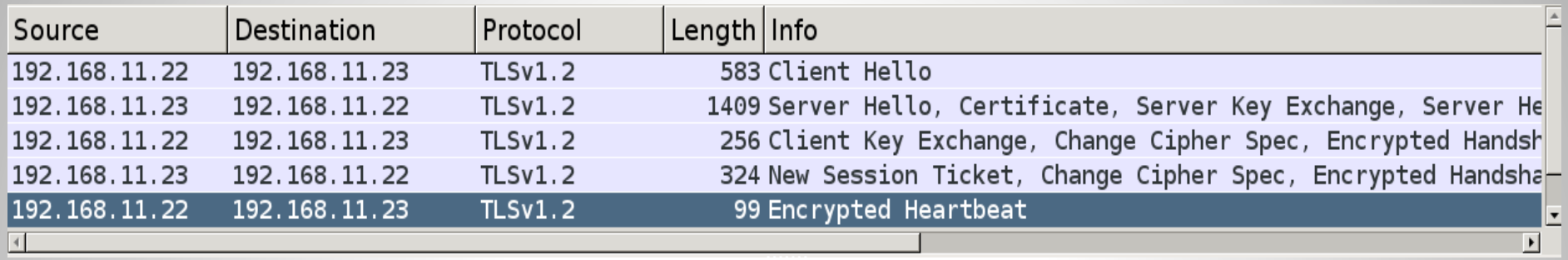
On The Wire

- This is an unencrypted heartbleed attack transmitted on the wire.
- The response is returned in unencrypted packets.



Exploitation notes on CVE-2014-0160

Attack SSL, Encrypt with SSL!



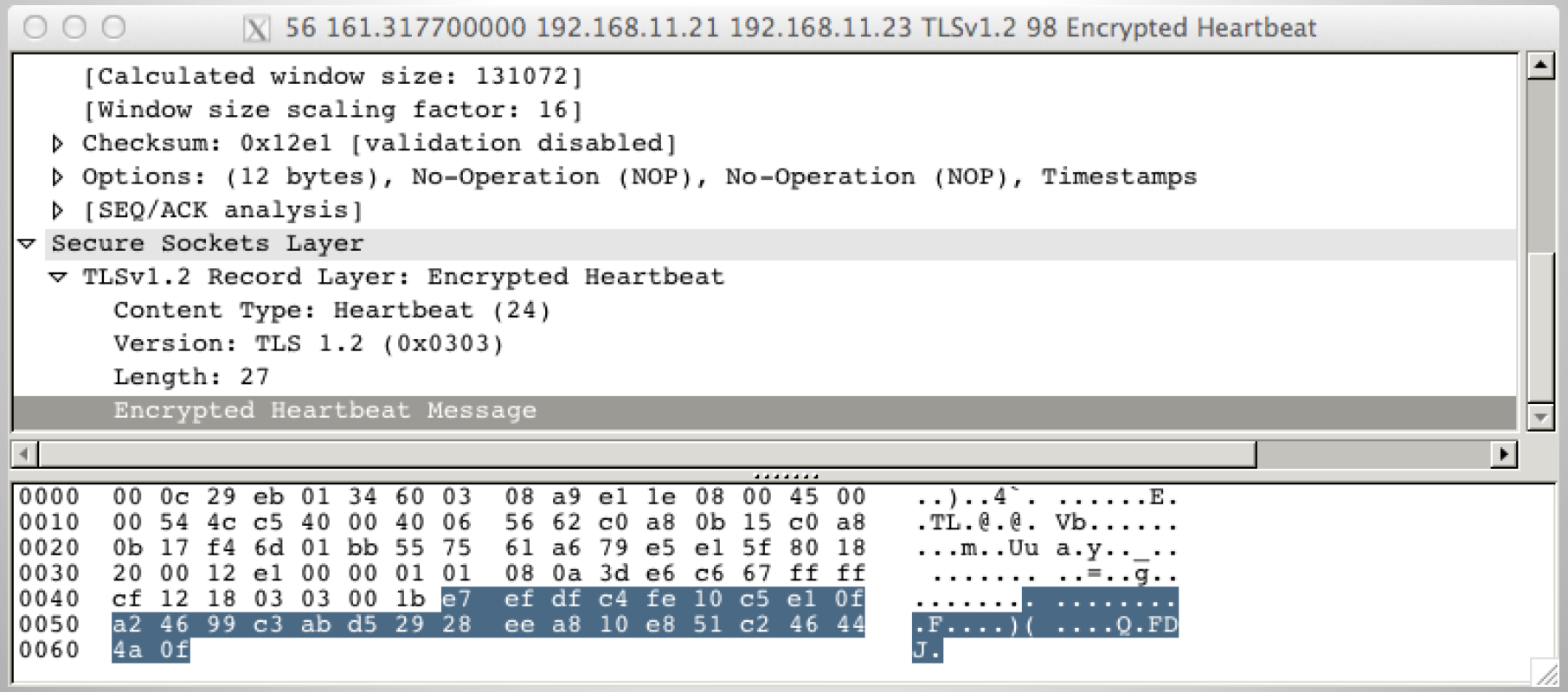
Source	Destination	Protocol	Length	Info
192.168.11.22	192.168.11.23	TLSv1.2	583	Client Hello
192.168.11.23	192.168.11.22	TLSv1.2	1409	Server Hello, Certificate, Server Key Exchange, Server He
192.168.11.22	192.168.11.23	TLSv1.2	256	Client Key Exchange, Change Cipher Spec, Encrypted Handsh
192.168.11.23	192.168.11.22	TLSv1.2	324	New Session Ticket, Change Cipher Spec, Encrypted Handsha
192.168.11.22	192.168.11.23	TLSv1.2	99	Encrypted Heartbeat

- I wrote a stand-alone exploit in C using OpenSSL library to transmit the Heartbeat request in encrypted packet.
- This was intentionally to bypass IPS/IDS signatures – it worked!
- Encrypting attacks on OpenSSL with OpenSSL makes it difficult to detect….
- IDS/IPS vendors began to develop alternative detection signatures.

Exploitation notes on CVE-2014-0160

On The Wire

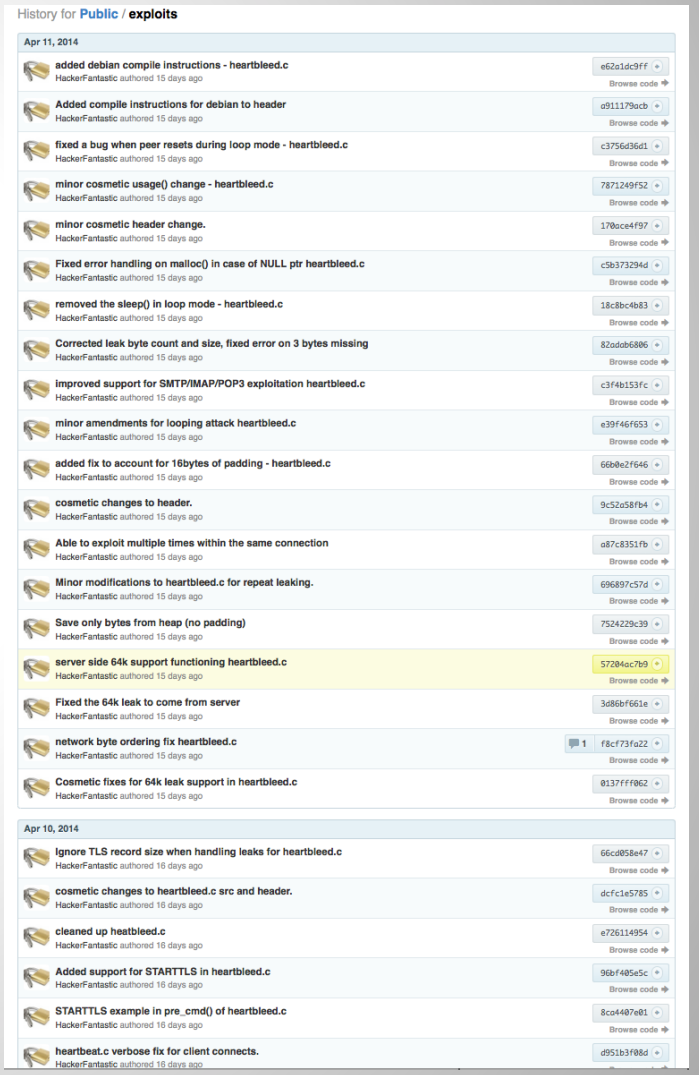
- This is an encrypted heartbleed attack transmitted on the wire.
- The response is returned in encrypted packets.



Exploitation notes on CVE-2014-0160

Exploit Fails & Lessons

- I continued to push updates during the exploit development process.
- I learnt not to commit code changes late at night without review and testing… No, I am not *THAT* OpenSSL developer!
- Internet is awesome, people began to submit compile instructions for different Linux platforms. Builds on most Linux/OS-X.
- Ayman Sagy added needed DTLS support.
- Re-use the code! Patches are welcome!



Exploitation notes on CVE-2014-0160

RSA Private Key Recovery

- Cloudflare announce secret key challenge for heartbleed.
- Provide nginx-1.5.13 web server linked against OpenSSL 1.0.1.f on Ubuntu 13.10 x86_64.
- Fedor Indutny solved the challenge first, others quickly followed.
- “include/openssl/rsa.h:struct rsa_st” holds RSA variables (p & q) in memory.
- RSA n := pq. We can use n to calculate if prime in memory is valid.
- Search for key size/2 primes in memory leak and use to determine remaining prime from modulo n (q % n == 0) – with p & q we generate RSA private key.

Exploitation notes on CVE-2014-0160

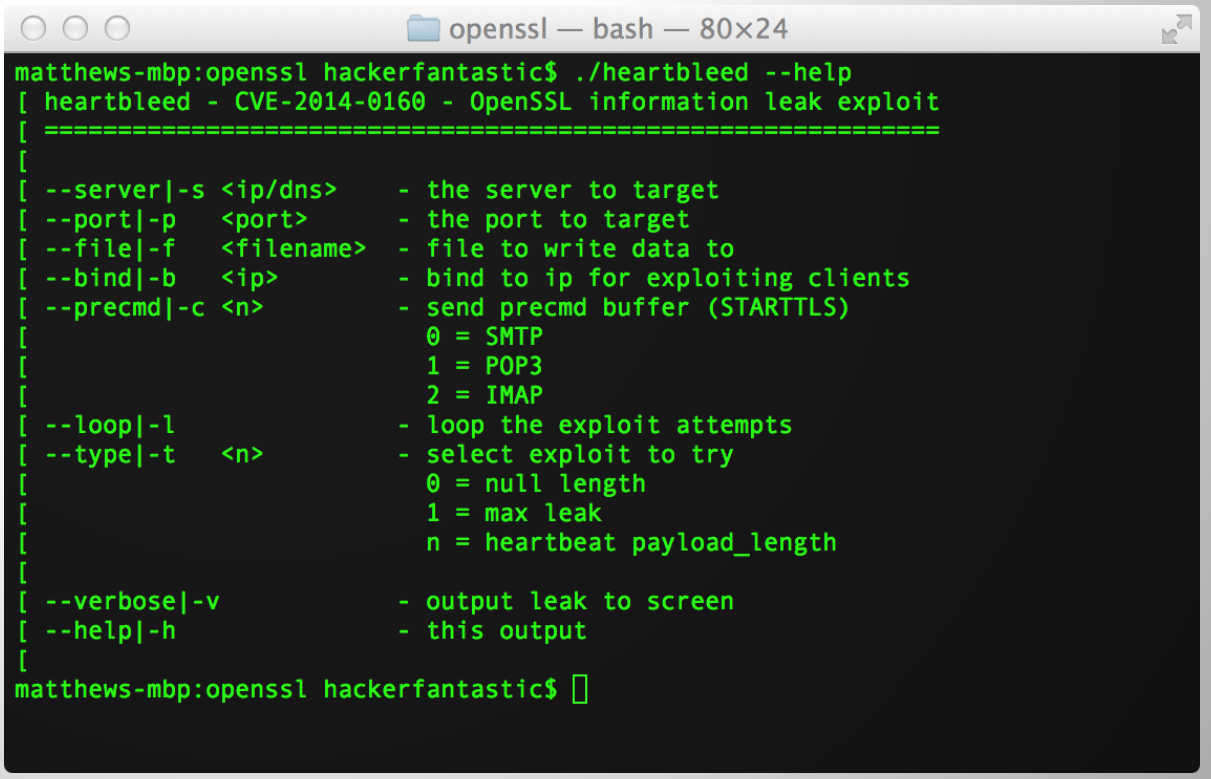
RSA Private Key Recovery

- Obtain certificate “openssl s_client -connect 192.168.11.23:443 < http-get.txt | grep BEGIN –A n > out.pem”
- Improved “keyscan.py” by Einar Otto Stangvik to produce valid RSA private keys.
- Run “keyscan.py” on a memory dump which tests possible values against the certificate modulus n to identify if modulo is 0. The value and its division result by n are checked and if primes we have p & q.
- We then generate the RSA private key from the prime values.
- Metasploit module also supports dumping private keys.

Exploitation notes on CVE-2014-0160

Heartbleed.c

- Exploit works against vulnerable OpenSSL servers and clients.
- Leaks upto 65535 bytes of heap data and 16 bytes of random padding.
- Can re-use connection.
- STARTTLS support.
- Multiple SSL protocols.
- Multiple ciphers.
- Saves leak to file.



Demo

Demo.

Conclusions

- CVE-2014-0160 will exist in appliances & infrastructure for some time.
- Affected servers and devices should be considered compromised.
- Your IDS/IPS cannot always save you.
- Enable Perfect Forward Secrecy.
- Enable Two-Factor Authentication (e.g. X.509).

E-mail: matthew@mdsec.co.uk

Twitter: @HackerFantastic

https://github.com/hackerfantastic/public