Experiment: 6

Aim:
to write a Buffer - overflow attack with example using C.

Source code:

```
#Include<stdio.h>
#Include<string.h>
#Include<stdio.h>

int main(int age, char *argv[]
{
char buffer[5];
{
printf("strcpy() NOT executed....\n");
printf("syntax: %s <characters>\n", argv[0]);
exit(0);
}
strcpy(buffer, argv[1]);
printf("buffer content = %s\n", buffer);
printf("strcpy() executed....\n")
return 0;
}
```

Description of Buffer overload

In a buffer_overflow attack, the extra data sometimes holds specific instructions for actions intended by a hacker (or) malicious user.

In the examples. we do not Implement any malicious code Injection but just to show that the buffer can be overflow. Modern Compilers normally provide overflow checking option during the compile / link time but during the run time it is quite difficult to check this problem without any extra protection mechanism such as using exception handling

Output:

= Vi hello.c
= cc hello.c
= ls
  a.out hello.c
= ./a.out 2000 09 02
= buffer Content = 2000 09 02
= Strcpy() executed....

Result:

Thus, the demonstration of the Buffer overflow attack using 'C' is executed Successfully

Exp:5

Aim:
to implementation of virtual private database using oracle log or SQL Servers

VPD:
→ If VPD is applied into the code row by default column level VPD using allows you to restrict the rows display only if specified Coloumn are accessed.

SQL:

```
>> Connect system
>> password ; ******
>> show user
   user is system
>> Connect as sysdba
   Connected
>> grant executed dbms_rls to system;
   grant Succeeded
>> Conn system/password
   Connected
>> create or replace function If-Job(owner in varchar,
   oname in varchar2) return varchar2 as varchar(20));
   Begin
   Con':='dept'_no=20';
    return(con);
   END If-job
   /
  function created
>>> Create table emp(emp_no, int, ename varchar(20);
   job varchar(20), mgr int, hiredate date, salary int,
   Comm int, dept_no int));
>> Insert into emp values (101, "Ravi", "teaches", 20 Jan 22,
   10000, 2000, 10);
  Insert into emp values(102, "Mani", "professor", 2003,
    20 Apr 20, 15000, 1000, 10);
  insert into Emp values(103, "chandra", "police", 2004
    20 Mar 19, 20000, 0, 20);
  insert into EMP values (104, "Bharathi", "Post", 2005,
    12 Aug 18, 30000; 50, 20);
```

emp_no	ename	job	mgr	hiredate	Salary	Comm	deptno
101	Ravindra	Teacher	2002	20jan22	10000	2000	10
102	Mani	Professor	2003	20APR20	15000	1000	10
103	Chandra	Police	2004	20Mar19	20000	0	20
104	Bharathi	Post	2005	12Aug18	30000	50	20

Policy

```
BEGIN
Dems_RLS.ADD_Policy(object_schema => 'system',
                    object_name => 'sp_job',
                    function_schema => 'System',
                    Policy_function => 'pf_job',
END;
```

PL/SQL procedure successfully completed

```
=>> Select * from emp1
```

emp_no	emp_name	job	mgr	hire_date	dept_no
101	Ravindra	Teacher	2002	20Jan22	10
102	Mani	Professor	2003	20APR20	10
103	Chandra	Police	2004	20Mar19	20
104	Bharathi	Post	2005	12Aug18	20

```
=>> Select ename, job, hire_date from emp where
    dept_no = 10;
```

e_name	job	hire_date
Ravindra	Teacher	20 jan 22
Mani	Professor	20 APR 20

```
>> BEGIN
   DBMS_RLS.DROP_POLICY(object_schema => 'system',
                        object_name => 'emp',
                        policy_name => 'sp_job');
   END;
>> PL/SQL procedure successfully completed
>> drop function pf_jobs
>> function dropped
>> PL/SQL procedure successfully completed
>> select * from emp;
>> select ename, job, salary from emp;

ENAME      JOB        SALARY
Ravindra   teacher    10000
Mani       Professor  15000
Chandra    Police     20000
Bharathi   Post       30000

>> select ename, job, comm from emp where dept_no=10;

ENAME      JOB        COMM
Ravindra   teacher    2000
Mani       Professor  5000

>> select ename, job, hire_date, from emp;

ENAME      JOB        HIRE_DATE
Ravindra   teacher    20 jun 22
Mani       professor  20 Apr 19
Chandra    Police     20 mar 19
Bharathi   Post       12 Aug 18
```

Result: Implementation of Virtual private database (VPD) using by using oracle log (or) SQL Server was done successfully