**Challenges Answer**

**Host discovery**

1. Whoislookup

Ans:

a.) www.hackedemist.com

b.) BigRock Solutions Limited

c.) United States

1. Ping [www.hackedemist.com](http://www.hackedemist.com)

Ans: 192.185.129.21

1. Nmap -a [www.hackedemist.com](http://www.hackedemist.com) / 192.185.129.21

Ans: linux

1. Nmap [www.hackedemist.com](http://www.hackedemist.com) / 192.185.129.21

Ans: 21

1. Nmap -sV [www.hackedemist.com](http://www.hackedemist.com) / 192.185.129.21

Ans:

Option 1 & option 3

1. Dnsmap [www.hackedemist.com](http://www.hackedemist.com)

Ans:

No of subdomains: 9

No of ips: 25

1. Dnsenum www.hackedemist.com

Ans: 3

**User enumeration**

1. Command:getent passwd {1000..60000} | wc -l

Ans: 11

1. Command: find . -user root -group ue\_level01 strings file022.txt | grep pass

Ans: skiwn\*mi!

**Web app attacks**

1. ‘ or ‘1=1
2. ‘ or ‘1=1

**File based attacks**

1. Command: cat password.txt

Ans: aloWun2

1. Command: cat ./-

Ans: We11 D0N3

1. Command: cat i/ am/ password

Ans: G0 g0 Go!

1. Command: cat .pass

Ans:Qpi&n@

1. Command: john shadow

Ans:1234

1. Command: find . -type f -readable ! -executable -size 4096c

Ans:Zmsiwn20jn10ke8

1. Command: cat password.txt | sort | uniq -u

Ans: UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR

1. Command: strings password.txt | grep ===

Ans:P1mT2@zw

1. Command: fcrackzip

Ans: lahfuwQ

**Cryptography**

1. Rot13.com **ans= Jrypbzr gb gur svefg yriry bs pelcgbtencul**

**Welcome to the first level of cryptography**

2. Atbash cipher **ans= sfiizb! blf ziv mld jfzorurvw uli gsv mvcg ovevo**

**hurray! you are now qualified for the next level**

3. Md5 encryption **= ef22cbee172258880fd316cb2b0cd2ed**

**ans= lkjhgfdsa**

**Practicals-**

SETOOLKIT :-Set up a listener and see if you can get

the passwords on terminal through listener.

a. Command : setoolkit

b. Use Credential harvesting method

c. Enter any web login page to clone. For example,

www.facebook.com

d. Set up the listener as your Host IP by starting apache

service on the terminal.