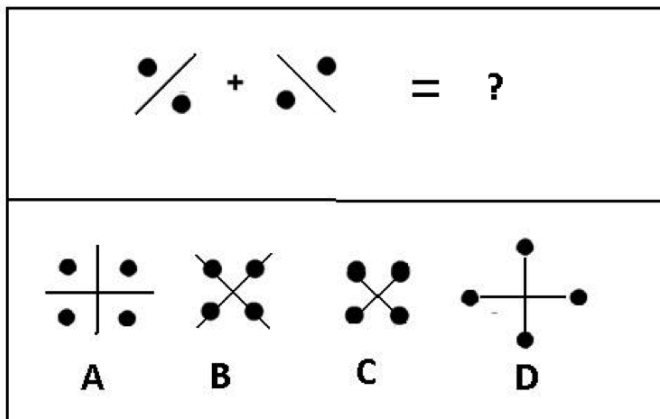# MABCTF-001

Login Details User - peter   Password - apple

1. What is the hostname of the machine?
    : _____ :

2. What is the Linux Distro Description of the machine?
    : _____ :

3. What users have been created on the Machine?
    : _____ :

4. Any users part of a group that they shouldn't be? Which User and what group have they been added to?
    : _____ :

5. What folders are in peter's home directory?
    : _____ :

6. What is the name of the files in that directory?
    : _____ :

7. What is the plaintext in the txt file?
    : _____ :

8. What is in the .secret file?
    : _____ :

9. Can you decode the data inside the file?
    : _____ :

10. Can you log in as another user? They may have sudo access? What is the password?
    : _____ :

11. What is the filename of the file in mikes directory?
    : _____ :

12. What type of ">file filename" is in mikes directory?
    : _____ :

13. What was the file previously named? Mike renamed the file recently.
    : _____ :

14. What device created the file? Exif.
    : _____ :

15. What other key information is hidden within the file?
    : _____ :

1)   What is a computer network?
        (a) A super computer owned only by the government
        (b) A web of connected computers or devices
        (c) A computer vulnerability
        (d) An Internet service provider
        (e) All of the above

2)   Why are cyber vulnerabilities unlikely to ever go away?
        (a) They're protected in a secret base on the moon.
        (b) Criminals need them to steal identities.
        (c) They are side effects of the freedom and ease of communicating online.
        (d) The government won't allow people to fix them.

3)   The size and complexity of networks grew enormously when:
        (a) Only governments and universities owned computers
        (b) Spamware caused some computers to break down
        (c) The number of personal computers greatly increased
        (d) The hacktivists started using the internet

4)   What is the difference between a threat and a vulnerability?

5) Solve the image below?

    Answer._____

6) If a baseball and a bat cost £1.10 together, and the bat costs £1.00 more than the ball, how much does the ball cost?

7) What Program was used to in the following a screenshot?

```
GET /bbc/bbc/s?name=home.page&app_name=homepage%20search
%20responsive&card_campaign_name_served=sg01-02-05-17-radio-4-in-four-
radio-4&module_name=radio_4_in_four&footer_loaded=yes&footer_template_loaded=footer-
template-02&cards_served=4&card_products_served_1=radio_4&card_products_served_2=radio_4&card_products
_served_3=radio_4&card_products_served_4=radio_4&card_types_served_1=audio&card_types_served_2=audio&c
ard_types_served_3=none&card_types_served_4=none&ns_type=hidden&action_name=card-
footer&action_type=load&ml_name=webmodule&ml_version=63&blq_e=orbit&blq_r=orbit&blq_s=orbit&blq_v=defa
ult&language=en&bbc_mc=ad1ps1pf1&app_type=responsive&location_name=&screen_resolution=1280x800&bbc_sit
e=homepage&ns_ti=BBC%20-%20Home&ns_c=UTF-8&ns__t=1493763118066&ns_jspageurl=http%3A%2F%2Fwww.bbc.co.uk
%2F&ns_referrer= HTTP/1.1
Host: sa.bbc.co.uk
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:53.0) Gecko/20100101 Firefox/53.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.bbc.co.uk/
Cookie: BBC-UID=053960e980b4624ad51e5dec5170b7fc58f4d0dc8704d426ea20b7620dd4f2d40Mozilla/
5.0%20(Macintosh%3b%20Intel%20Mac%20OS%20X%2010.11%3b%20rv:53.0)%20Gecko/20100101%20Firefox/53.0;
ckns_orb_fig_cache={%22uk%22:1%2C%22ck%22:1%2C%22ad%22:0%2C%22ap%22:0%2C%22tb%22:0%2C%22mb%22:0%2C
%22eu%22:1}; ckns_policy=111; ckns_policy_exp=1525299115913; s1=200.195.5909042D0008FD00156EF62985
Connection: keep-alivGET /bbc/bbc/s?name=home.page&app_name=homepage%20search
%20responsive&card_campaign_name_served=sg01-02-05-17-radio-4-in-four-
radio-4&module_name=radio_4_in_four&footer_loaded=yes&footer_template_loaded=footer-
template-02&cards_served=4&card_products_served_1=radio_4&card_products_served_2=radio_4&card_products
_served_3=radio_4&card_products_served_4=radio_4&card_types_served_1=audio&card_types_served_2=audio&c
ard_types_served_3=none&card_types_served_4=none&ns_type=hidden&action_name=card-
footer&action_type=load&ml_name=webmodule&ml_version=63&blq_e=orbit&blq_r=orbit&blq_s=orbit&blq_v=defa
ult&language=en&bbc_mc=ad1ps1pf1&app_type=responsive&location_name=&screen_resolution=1280x800&bbc_sit
e=homepage&ns_ti=BBC%20-%20Home&ns_c=UTF-8&ns__t=1493763118066&ns_jspageurl=http%3A%2F%2Fwww.bbc.co.uk
%2F&ns_referrer= HTTP/1.1
```

Packet 4849. 2 client pkts, 1 server pkt, 1 turn. Click to select.

Entire conversation (3285 bytes)   Show and save data as   ASCII   Stream 108

8) What Website was visited?

9) What browser was used to visit that site?

10) What would the port number be that the client would of connected to?

11) What is the Protective Marking of Champ*?

12) Can you briefly explain how you would deal with a potential virus on a Champ* Laptop, the user has multiple USBs and CDs and regularly ImpEx's from the internet?