AWS Essentials

1) Ip address (Private ip and public ip)
2) Virtualization
3) Linux (ssh, install and uninstall a package,cat,permissions,ls,passwords,Bash shell scripting) and windows (RDP,powershell script,Manage users, Networking)
4) Cryptography (private key and public key)
5) ACL
6) NAT
7) how to calculate a subnet
8) How to manage firewalls (s/w firewall)
9) Private and public subnets
10) Http/Https/tcp/smtp/pop/icmp/ping/telnet
11) Encryption algorithms (RSA/SHA), VPN
12) Working with CLI commands (Linux and windows)
13) Storage
14) Gateways and DHCP/DNS
15) Load balancer and web server

Ip address (Private ip and public)

private ip = This ip will work only in LAN network
This ip does nt have access to internet
This ip address is non-routable address
This ip is unregistered

Public Ip = This ip will work globally WAN network
This ip have access to the internet
This ip address is routable in internet
This ip is registered

Virtualization

i) Virtualization is a technology to run multiple different or same os, which is completely isolated from each other

How it is different from dual boot ?

Hypervisor = HV is a software layer sits between hardware and OS which interact with hardware and resources and provide an interface to share the avaliable resources to virtual containers.

ii) Two types of hypervisor = Bare metal and Hosted

BareMetal = Vmware ESXi,Microsoft Hyper-v,xen server
Hosted = vmware,virtual pc,virtual box,QEMU,KVM

Working process:

Bare Metal = Hardware ---> Hypervisor ---> VM
Hosted = Hardware ---> OS ---> HV ----> VM

Issues in Virtualization

i) Re-Build OS
ii) Data recovery
iii) same vendor and same model

Linux (ssh, install and uninstall a package,cat,permissions,ls,passwords,Bash shell scripting) and windows (RDP,powershell script,Manage users, Networking)

i) SSH (Secure Socket Host) = port no 22

Remote connection for the Linux Machines

Telnet,rcp,rlogin = ssh

ii) SSH Security = confidentiality (no body can read the message content)
Integrity (Gurantee the data is unaltered on transit)
Authentication (of client and server)

SSH gives security Over = ip spoofing,ip source routing,DNS spoofing,Password interception,Evesdropping
SSH = 1, 2

SSH encryption = symmetric and asymmetric key (public/private) keys for encryption
SSH supports different encryption algorithms 3DES,AES,Blowfish,IDEA

SSH can be used to = secure remote shell
port forwarding
X11,vnc sessions

SSH comes with different administration tools = SSH keygen,ssh-agent,ssh-add,make-ssh-known-hosts

Popular SSH Clients = windows (Putty,TTSSH,Winscp)
                                       Linux = OpenSSH,Client

RDP Protocol (3389)

i) Virtualization Technology that provide access to session based desktops, virtual machine based desktops and applications

passwords (Linux and windows)

Linux = passwd
(non-root user) = passwd (old passwd and change the new password)
(Root user) = passwd rhce (changing the password for the user)

windows = net user username password (Runas)

cat (Content command in Linux)

Installing and Removing Packages in Linux Machines

Installing SQL workbench

1) Yum install epel-release -y ---> This will check the latest release for the Linux machine
2) wget http://repo.mysql.com/mysql-community-release-el7-5.noarch.rpm
3) yum install mysql-community-release-el7-5.noarch.rpm
4) yum install mysql-workbench -y

permissions

1) Owner
2) Group
3) all users

```
    Dir = file owner (user1)
             group (Mysolutions)
            file permission (660)
```

group1 (Mysolutions) = user1,user2,user3
group2 (demo) = user4,user5,user6

file permission 660

read = 4
write = 2
execute = 1
deny = 0

user1,2,3 = r/w
user4,5,6 = deny

Permissions Types

i)read
ii) write
iii) execute

```
drwxr-xr-x. root root 2 ---> directory permission
-rw-r--r--.   root root  1 ---> file permission
```

drwx(Owner permission)
r-x (Group permission)
r-x (user permissions)
root (user ownership)
root (group ownership)

-rw-

File permissions

every file owned by UID, GID
every process is referred as UID and one or more GID

permission order

i) if UID match, owner permission will apply
2) if GID match, group permission will apply
3) if none of these match, other permission will apply

Modifying the permissions

1) Symbolic Link
2) By using binary reference or numeric mode, octal mode

Hardlinks

1) same inode number

Symbolic Link

Explicitly defined the permissions

owner --> u
group ---> g
all other users --> 0
all user (owner+group+all other users) --> a

+ (add)
- (remove)
= (replace the existing permission)

To add permissions

chmod +
chmod -

passwords
Windows/Linux = passwords
Passwords are two types (Direct password, Indirect passwords)
All passwords = Hashing algorithms (MD5/SHA1)

u)?eUYg7%DtBy$bI8bk29ic&UymY;i$w (Strong Passwords)

Types of passwords:

1) Contextual authentication
2) Multi-factor authentication
3) Two-factor
4) OTP (One-time password)

OTP Generated Methods

1) Time-synchronized = security tokens
2) Mathematical algorithm = Previous password based, challenge-response based

OTP Algorithms

```
 1) TOTP
 2) HOTP


Types of passwords attack

1) Dictionary attack
2) Brute force attacks
3) Rainbow table attacks
4) Phishing
5) Social Engineering
6) Malware
7) Offline cracking
8) Guess

Linux = root and non-root user
             (Full Rights)   (Limited Rights)

if non-root user wants to access the Temporary rights in linux than he must
use sudo command
This is same as Runas command in the windows Os

Linux = /etc/passwd, /etc/shadow,
p, /etc/gshadow
Linux = root,normal,service

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

root = username
x = password placeholder
0 = UID
0 = GID
Root = comments
root = home dir
bin/bash = shell

rhce:$6$QyPcAqvik$dIFvdXDcD1tFCU3jwna/dDxInbO64.j7k9YOgPuLwx51iGDkv0ggmD13pf
8DQ2z0MIwGsNNTSguvOug1WfVW1.:17514:0:99999:7:::

rhce = username
$6$QyPcAqvik$dIFvdXDcD1tFCU3jwna/dDxInbO64.j7k9YOgPuLwx51iGDkv0ggmD13pf8DQ2z
0MIwGsNNTSguvOug1WfVW1.: = encrypted passwords

17514:0:99999:7:::

rhce:x:1000:
```

rhce:!::

Bash shell scripting
poweshell scripting

Manage users

Networking = Netwoking is common for all devices may be we have different kind of devices (server,router,switch) etc
if user want to understand the complete process of the network than user have to understand OSI model
protocols,portno,the complete networking process is transparent to the user

permissions in network and hidden sharing
windows = Full control/Deny/Read
Each network have the 3 components (Authentication,Authorization and Accounting)
username and password = authentication
permission are allows to the user = Authorization
Accounting = Following the rules of the Network

Cryptography (private key and public key)
i) ATM
ii) Email-passwords
iii)E-payment
iv) Electronic voting
v) Securing data

encryption --> plaintext to ciphertext
Decryption ---> Ciphertext to plaintext

symmetric encryption = an encryption system in which the sender and recevier of a message share a single, common
key that is used to encrypt and decrypt the message

DES,3DES,AES

Asymmetric encryption

RSA/DSA/DHA/ECDSA

ACL (Access control List)

permit
Deny

how to calculate a subnet

CIDR = Classless inter-domain Routing

How to manage firewalls (s/w firewall)

Private and public subnets

Http/Https/tcp/smtp/pop/icmp/ping/telnet
http = Hyper-Text transfer protocol (80)
Https = 443
Tcp = Transmission control protocol (6)
smtp = 25
pop = 110
icmp/ping = error messages
informational messages
Source quench
Echo request/Reply
Time exceeded
Address mask request/reply
Destination HostUnreachable Router Discovery
Redirect
Fragmentation Required

0 = echo reply
3 = Destination Unreachable
4 = source quench
5 = redirect
8 = Echo request

ping = ping

telnet = 21

Encryption algorithms (RSA/SHA), VPN