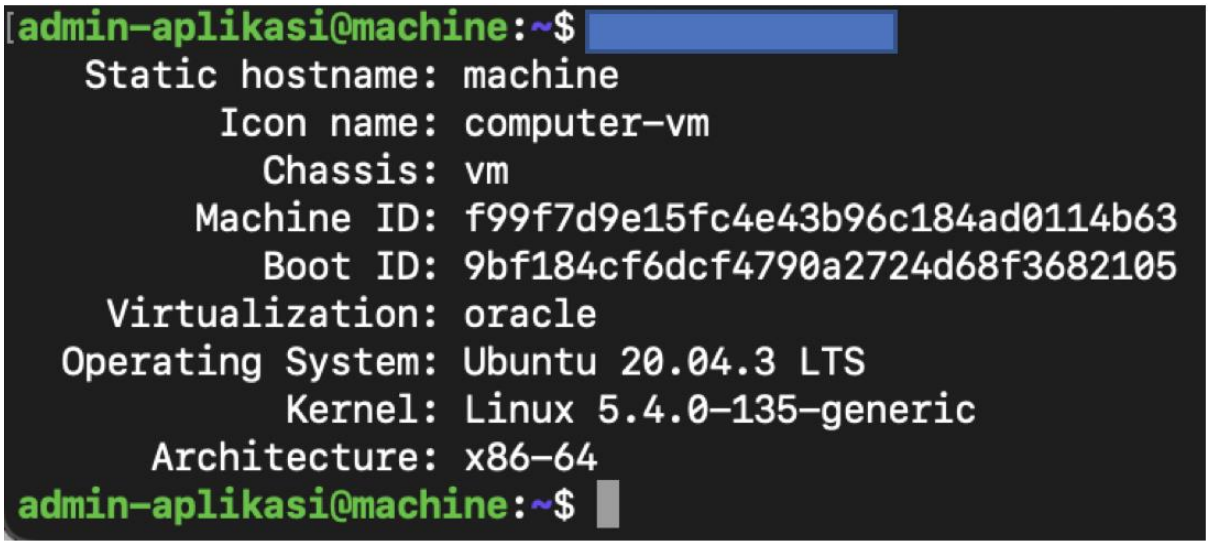
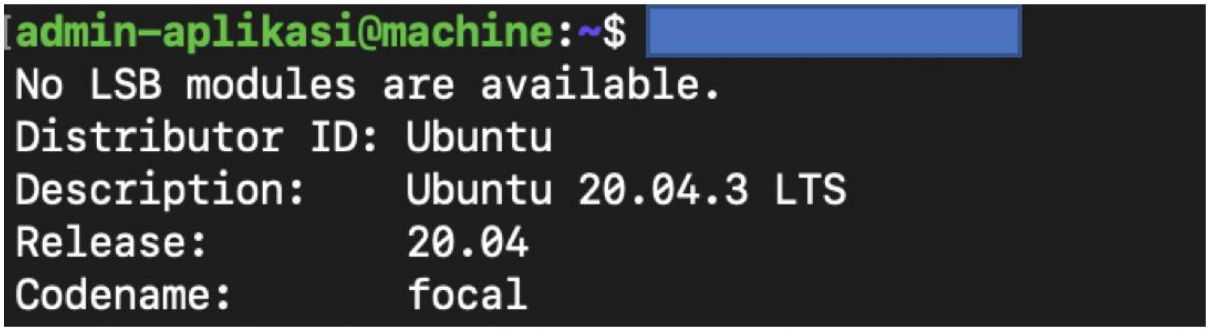
Linux #1



Sebutkan sintaks yang digunakan pada Linux System untuk dapat menampilkan informasi mengenai detail sistem operasi sesuai gambar berikut :

Linux #2



Sebutkan sintaks yang digunakan pada Linux System untuk dapat menampilkan informasi mengenai Versi Sistem Operasi sesuai gambar berikut :

Linux #3

Sebutkan sintaks yang digunakan pada Linux System untuk dapat menampilkan versi Kernel yang digunakan pada sistem operasi sesuai gambar berikut :

Linux #4

```
[admin-aplikasi@machine:~$
 08:02:26 up 9 min,  1 user,  load average: 0.41, 0.44, 0.24
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
admin-ap pts/0    10.0.2.2         07:52    2.00s  0.05s  0.01s w
```

Sebutkan sintaks yang digunakan pada Linux System untuk dapat menampilkan User yang sedang Login sesuai gambar berikut :

Linux #5

```
  CPU[||                                               1.7%]   Tasks: 33, 63 thr; 1 running
  Mem[|||||||||||||||||||||||||||||||||||||||||||||||516M/977M]   Load average: 0.06 0.29 0.20
  Swp[|                                           1.26M/1.92G]   Uptime: 00:11:52

  PID USER      PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
 1244 admin-apl  20   0  8344  3972  3148 R  1.7  0.4  0:00.07 htop
    1 root       20   0  165M 13004  8336 S  0.0  1.3  0:02.04 /sbin/init maybe-ubiquity
  350 root       19  -1 51464 15376 14372 S  0.0  1.5  0:00.20 /lib/systemd/systemd-journald
  383 root       20   0 21532  5536  4004 S  0.0  0.6  0:00.39 /lib/systemd/systemd-udevd
  537 root       RT   0  273M 18144  8232 S  0.0  1.8  0:00.01 /sbin/multipathd -d -s
  538 root       RT   0  273M 18144  8232 S  0.0  1.8  0:00.00 /sbin/multipathd -d -s
  539 root       RT   0  273M 18144  8232 S  0.0  1.8  0:00.00 /sbin/multipathd -d -s
  540 root       RT   0  273M 18144  8232 S  0.0  1.8  0:00.07 /sbin/multipathd -d -s
  541 root       RT   0  273M 18144  8232 S  0.0  1.8  0:00.00 /sbin/multipathd -d -s
  542 root       RT   0  273M 18144  8232 S  0.0  1.8  0:00.00 /sbin/multipathd -d -s
  536 root       RT   0  273M 18144  8232 S  0.0  1.8  0:00.11 /sbin/multipathd -d -s
  595 systemd-t  20   0 90220  6108  5340 S  0.0  0.6  0:00.00 /lib/systemd/systemd-timesyncd
  575 systemd-t  20   0 90220  6108  5340 S  0.0  0.6  0:00.07 /lib/systemd/systemd-timesyncd
  619 systemd-n  20   0 26604  7520  6656 S  0.0  0.8  0:00.05 /lib/systemd/systemd-networkd
  621 systemd-r  20   0 23756 11488  8036 S  0.0  1.1  0:00.06 /lib/systemd/systemd-resolved
  665 root       20   0  233M  9292  8336 S  0.0  0.9  0:00.02 /usr/lib/accountsservice/accounts-daemon
  714 root       20   0  233M  9292  8336 S  0.0  0.9  0:00.00 /usr/lib/accountsservice/accounts-daemon
  633 root       20   0  233M  9292  8336 S  0.0  0.9  0:00.04 /usr/lib/accountsservice/accounts-daemon
  637 root       20   0  6844  2804  2604 S  0.0  0.3  0:00.00 /usr/sbin/cron -f
  638 messagebu  20   0  7636  4536  3776 S  0.0  0.5  0:00.13 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nop
  645 root       20   0 29688 17396  9376 S  0.0  1.7  0:00.06 /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-tri
  683 syslog     20   0  219M  4596  3560 S  0.0  0.5  0:00.00 /usr/sbin/rsyslogd -n -iNONE
  684 syslog     20   0  219M  4596  3560 S  0.0  0.5  0:00.00 /usr/sbin/rsyslogd -n -iNONE
F1Help  F2Setup F3SearchF4FilterF5Tree  F6SortByF7Nice -F8Nice +F9Kill  F10Quit
```

Sebutkan sintaks yang digunakan pada Linux System untuk dapat menampilkan informasi daftar proses sesuai gambar berikut :

Linux #6

Isi file txt :

aris manajer account 881223

sunti asisten account 86366

valak manajer sales 725380

amar manajer account 926388

tari sekretaris sales 63784

deni asisten sales 762930

sungkar manajer sales 672839

satria direktur purchase 63849

Sebutkan sintaks yang digunakan untuk menampilkan nama dan angka pada file terlampir yang sesuai gambar berikut :

Linux #7

Isi file txt :

aris manajer account 881223

sunti asisten account 86366

valak manajer sales 725380

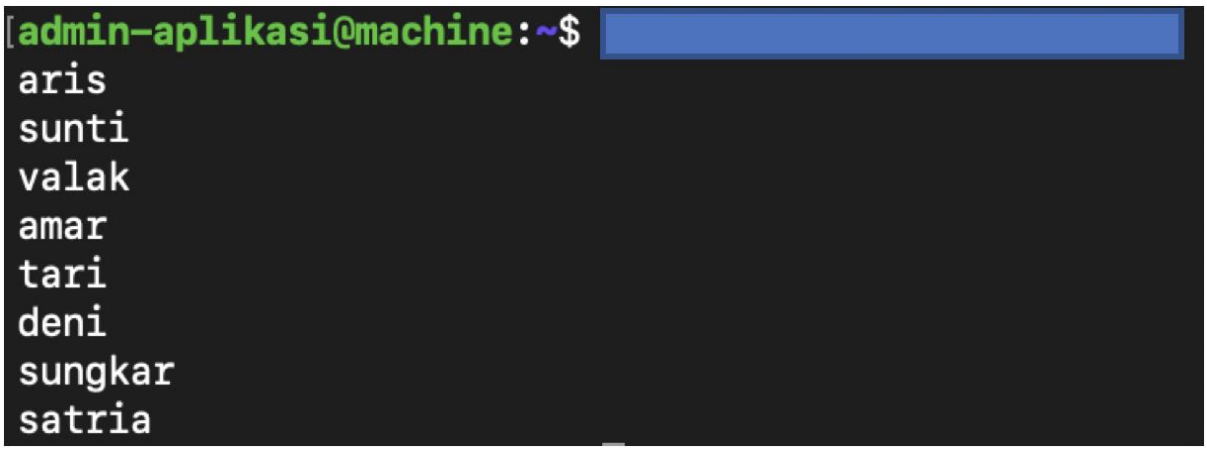
amar manajer account 926388

tari sekretaris sales 63784

deni asisten sales 762930

sungkar manajer sales 672839

satria direktur purchase 63849



Sebutkan sintaks yang digunakan untuk menampilkan hanya nama pada file terlampir yang sesuai gambar berikut :

Linux #8

Sebutkan perintah (sintaks) dalam Linux untuk menampilkan Pengguna (User) yang sedang Aktif Login?

Linux #9

Sebutkan perintah (sintaks) dalam Linux untuk menampilkan informasi mengenai nama Host pada sistem tersebut?

Linux #10

Sebutkan perintah (sintaks) dalam Linux untuk menampilkan informasi mengenai direktori yang sedang aktif digunakan?

Crackme #1

Lakukan decode dari barisan code berikut :

SnVuMTByY3liM3JTM2N1cjF0eUMwbXAzdDF0aTBu

Crackme #2

Lakukan decode dari barisan code berikut :

1a1846de50aa650142bcbfa2a88a04c3

Crackme #3

Lakukan decode dari barisan code berikut :

48efc4851e15940af5d477d3c0ce99211a70a3be

Crackme #4

Lakukan decode dari barisan code berikut :
17f80754644d33ac685b0842a402229adbb43fc9312f7bdf36ba24237a1f1ffb

Crackme #5

Isi file txt :

user01:e6b6afbd6d76bb5d2041542d7d2e3fac5bb05593

user02:7b902e6ff1db9f560443f2048974fd7d386975b0

user03:a4f6a44f8a1dec1f38cc26478886e2ebd3d62e11

user04:6d49504914499c3d5f0f1f0261f3161e6e292db5

user05:6bd7a6010737458b44b15001ba1d0004461e3a2b

Lakukan brute force kumpulan username dan password pada file account.txt. Sebutkan algoritma apa yang digunakan untuk bisa melakukan cracking password tersebut?

Crackme #6

Isi file txt :

user01:e6b6afbd6d76bb5d2041542d7d2e3fac5bb05593

user02:7b902e6ff1db9f560443f2048974fd7d386975b0

user03:a4f6a44f8a1dec1f38cc26478886e2ebd3d62e11

user04:6d49504914499c3d5f0f1f0261f3161e6e292db5

user05:6bd7a6010737458b44b15001ba1d0004461e3a2b

Berdasarkan file account.txt, sebutkan password dari user04 ?

Crackme #7

<file id_rsa di dalam zip>

Lakukan cracking file kunci privat "id_rsa" berikut guna mendapatkan informasi password seorang user?

Crackme #8

Berapa bit RSA yang digunakan pada file kunci privat tersebut (id_rsa)?

Crackme #9

Sebutkan algoritma yang digunakan untuk menghasilkan barisan code berikut :

1a1846de50aa650142bcbfa2a88a04c3

Crackme #10

Isi file txt :

user01:e6b6afbd6d76bb5d2041542d7d2e3fac5bb05593

user02:7b902e6ff1db9f560443f2048974fd7d386975b0

user03:a4f6a44f8a1dec1f38cc26478886e2ebd3d62e11

user04:6d49504914499c3d5f0f1f0261f3161e6e292db5

user05:6bd7a6010737458b44b15001ba1d0004461e3a2b

Berdasarkan file account.txt, berapa Bit panjang password tersebut?

Red #1

File secret.pdf ada di dalam zip

Lakukan cracking dan sebutkan password untuk membukan file secret.pdf berikut?

Red #2

File secret.pdf ada di dalam zip

Sebutkan konten Flag dari file secret.pdf tersebut?

Red #3

File senja.jpeg ada di dalam zip

Carilah Flag pada file berikut !

Red #4

apple.jpeg

Carilah Flag pada file berikut!

Red #5

luffy.jpeg

Carilah Flag pada file berikut!

Red #6

catchme01

Carilah Flag pada file berikut!

Red #7

catchme02

Carilah Flag pada file berikut!

SSHD Log

1.log

Apa Alamat IP dan Port Server SSH

FORMAT: IP_ADDRESS:PORT

Bruteforce SSH

2.txt

Pada percobaan ke - berapa penyerang berhasil masuk ke sistem?

SQL Injection

3.txt

Sebutkan IP Address penyerang!

Lateral Movement

4.txt

Sebutkan IP Address komputer yang compromise sehingga dapat dimanfaatkan penyerang untuk melakukan lateral movement ke dev-server (192.168.1.20) dan prod-server (192.168.1.30)!

User Agent

5.txt

Sebutkan User-Agent penyerang dengan lengkap!

Email Header

6.txt

Sebutkan email penyerang yang digunakan untuk phising email!

Create User

8.yml

Setelah mengambil alih system, penyerang melakukan persistence dengan membuat user baru. Sebutkan akun user yang dibuat penyerang!

Windows

9.zip

Nama account Name yang sukses pertamakali melakukan koneksi RDP?

DNS Exfiltration

10.txt

Apakah password dari akun ajimas?

Hash

f1.evtx

Sebutkan Hash SHA256 dari file tersebut!

Exifool

f2.HEIC

Sebutkan kode telepon negara lokasi foto tersebut diambil!

Format: +XX (Contoh +62)

Stego

f3.jpg

Temukan pesan pada file ini!

Location

File SAM (Security Account Manager) menyimpan hash dari password akun pengguna lokal. File ini tidak dapat diakses secara langsung saat Windows sedang berjalan karena dilindungi oleh sistem, tetapi bisa diakses oleh malware atau penyerang yang memiliki hak administrator dengan metode khusus, seperti booting dari media eksternal atau dumping menggunakan alat seperti Mimikatz.

Dimanakah lokasi File SAM?

Format : C:\Folder\Folder\...\File

Analysis #1

f5.txt

Apakah nama file yang dicuri?

Format : Namafile.ekstensi (Contoh : Namafile.pdf)

Analysis #2

f6.txt

Kapan penyerang melakukan download dan eksekusi malware pada komputer korban?

Format : DD/MM/YYYY HH:MM:SS

Analysis #3

f8.txt

Kapan korban membuka file phising sehingga penyerang dapat mengambil alih komputernya?

Format : DD/MM/YYYY HH:MM:SS

Analysis #4

f9.txt

Apa nama aplikasi yang digunakan penyerang untuk mengetahui kredensial korban?

Analysis #5

f10.pcap

Apakah nama sistem yang terinfeksi?