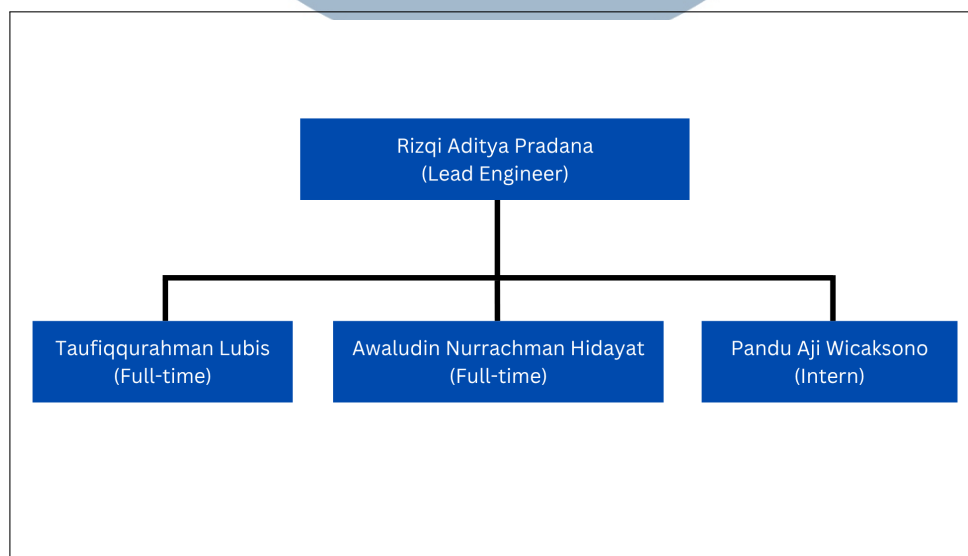


BAB 3

PELAKSANAAN KERJA MAGANG

3.1 Kedudukan dan Koordinasi

Selama magang di PT Sentra Netcomindo, posisi ditempatkan di divisi Engineer sebagai *cybersecurity intern*, yang dipimpin oleh Bapak Rizqi Aditya Pradana selaku *Lead EGINEER*. Magang dikoordinasikan oleh Bapak Rizqi Aditya Pradana sebagai mentor, dengan arahan langsung dan melalui aplikasi WhatsApp. Selain itu, diskusi dengan karyawan tetap juga dilakukan secara rutin untuk membahas tugas yang diberikan, mengklarifikasi kendala yang dihadapi, serta memperoleh *insight* baru yang relevan dengan dunia kerja dan pengembangan keterampilan profesional. Interaksi ini tidak hanya memperdalam pemahaman terhadap tugas, tetapi juga membangun hubungan kerja yang positif. Gambar 3.1 menunjukkan bagan dalam Divisi Engineer yang memberikan gambaran lebih jelas mengenai struktur tim.



Gambar 3.1. Struktur Divisi Engineer

Sumber: [9]

3.2 Tugas yang Dilakukan

Kegiatan magang di PT Sentra Netcomindo diuraikan secara mingguan sebagaimana ditunjukkan pada Tabel 3.1 berikut.

Tabel 3.1. Pekerjaan Mingguan Selama Magang

Minggu Ke -	Pekerjaan yang Dilakukan
1	Mengenal <i>jobdesk</i> , memulai pembelajaran Layer 1 OSI Model, teori dan praktik kabel jaringan, serta melakukan diskusi <i>milestone</i> tahun 2025 bersama tim engineer
2	Memfokuskan pembelajaran OSI Layer 2–4, meliputi MAC Address, protokol jaringan, routing, addressing, TCP/UDP, serta implementasi keamanan jaringan
3	Mempelajari port dan protokol jaringan, menggunakan Wireshark, serta memahami konsep OSI Layer 5–7, termasuk session, enkripsi data, dan protokol HTTP serta DNS
4	Memfokuskan pada dasar cybersecurity, kriptografi (symmetric, asymmetric, digital signature), serta menghubungkannya dengan infrastruktur IT dan kebutuhan keamanan perusahaan
5	Mengenal CipherTrust, mengimplementasikan Windows Server VM, serta mendalami kriptografi melalui pembelajaran dan seminar Thales
6	Membahas kriptografi, ISO 27001, keamanan infrastruktur TI, menggunakan Linux dan SSH, serta memahami firewall dan WAF Imperva, serta pentingnya HSM dalam perlindungan kunci
7	Memahami konsep kriptografi, arsitektur, jenis, dan cara kerja Hardware Security Module (HSM)
8	Memfokuskan pada pemahaman HSM dalam BI Fast, integrasi konsep WAF–CipherTrust–HSM, serta mengikuti pelatihan produk di Exclusive Networks
9	Mempelajari deployment dan pembuatan salah satu prototype produk yang tersedia di CipherTrust Manager
10	Mengembangkan prototype CipherTrust Manager, mengikuti deployment, serta mempelajari Palo Alto dari Network Security hingga Cybersecurity Fundamentals
Dilanjutkan pada halaman berikutnya	

Tabel 3.1 Pekerjaan Mingguan Selama Magang (lanjutan)

Minggu Ke -	Pekerjaan yang Dilakukan
11	Mempelajari Palo Alto terkait Endpoint dan Cloud Security serta melaksanakan Preventive Maintenance di perusahaan bank Jepang di Sudirman
12	Mempelajari Preventive Maintenance HSM, memahami HSM di BI-Fast, dan melanjutkan Cloud Security Fundamentals Palo Alto
13	Mempelajari Security Operations Fundamentals Palo Alto dan melanjutkan konfigurasi HSM
14	Melakukan PM HSM di dua lokasi serta mempelajari dan mendalami produk CTE (CipherTrust Transparent Encryption) dari CipherTrust Manager
15	Mendalami CTE, mempelajari CipherTrust untuk cloud, dan mengeksplorasi Linux dalam konteks peretasan
16	Melakukan PM HSM di BSD dan DCI serta mempelajari HSM dan konsep dasar payment
17	Memahami konsep pembayaran, issuer, switcher, acquirer, dan cara kerja HSM dalam sistem pembayaran

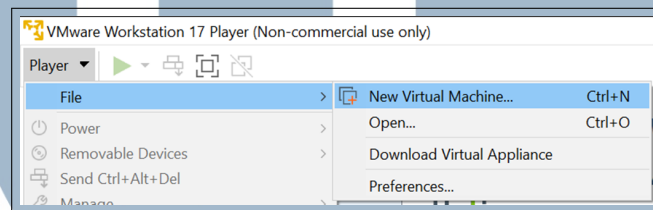
3.3 Uraian Pelaksanaan Magang

Pelaksanaan praktik kerja magang di PT Sentra Netcomindo terbagi ke dalam beberapa tahapan kerja yang disesuaikan dengan kebutuhan perusahaan dan kemampuan. Uraian pelaksanaan magang akan dijelaskan secara rinci sebagai berikut.

3.3.1 Deploy Windows Server VM

Windows Server VM mengacu pada *instance* Windows Server yang berjalan dalam sebuah mesin virtual, biasanya dikelola melalui platform virtualisasi seperti VMware. Perusahaan tempat kerja magang dilaksanakan menggunakan Windows Server dalam bentuk VM dengan tujuan untuk mengoptimalkan sumber daya server fisik dan mengurangi biaya hardware dengan menjalankan beberapa server virtual di atas satu hardware.

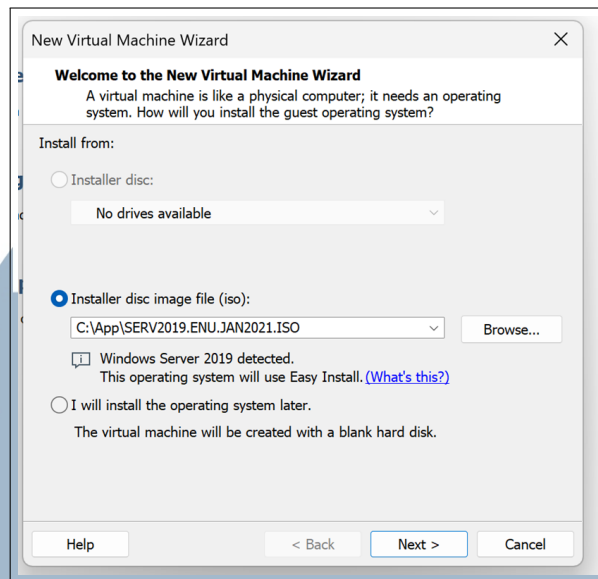
Keuntungan menggunakan Windows Server dalam bentuk VM antara lain adalah efisiensi sumber daya, karena beberapa server dapat dijalankan pada satu perangkat keras fisik. Selain itu, manajemen server menjadi lebih mudah dengan platform virtualisasi, dan VM dapat dibuat, dimodifikasi, atau dihentikan tanpa mempengaruhi server fisik. Ini membantu perusahaan menghemat biaya investasi perangkat keras serta mempercepat pemulihan sistem dengan menggunakan fitur snapshot. Dengan demikian, Windows Server dalam bentuk VM memberikan fleksibilitas dan efisiensi dalam pengelolaan server di lingkungan yang lebih kompleks.



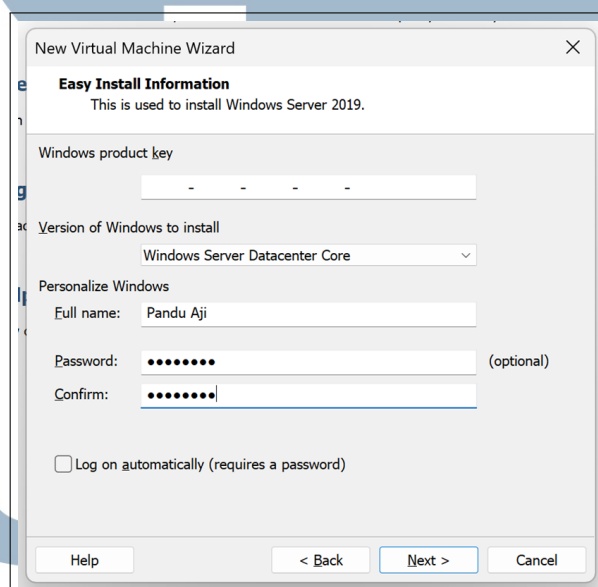
Gambar 3.2. Membuat *Virtual Machine* Baru

Pada Gambar 3.2 proses dimulai dengan pembuatan virtual machine baru menggunakan perangkat lunak VMware Workstation. Konfigurasi awal dilakukan untuk menyiapkan lingkungan virtual yang akan digunakan dalam proses deployment sistem operasi. Setelah konfigurasi dasar selesai, file ISO yang sesuai dipilih untuk instalasi sistem operasi, seperti yang dapat dilihat pada Gambar 3.3. Tahapan ini memastikan bahwa virtual machine siap digunakan dalam implementasi lebih lanjut untuk memenuhi kebutuhan sistem yang telah ditentukan.

U N I V E R S I T A S
M U L T I M E D I A
N U S A N T A R A

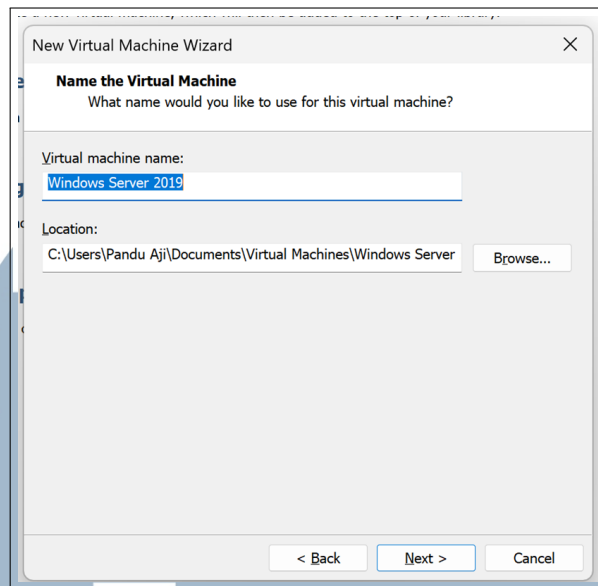


Gambar 3.3. Memilih *File ISO* untuk Windows Server 2019



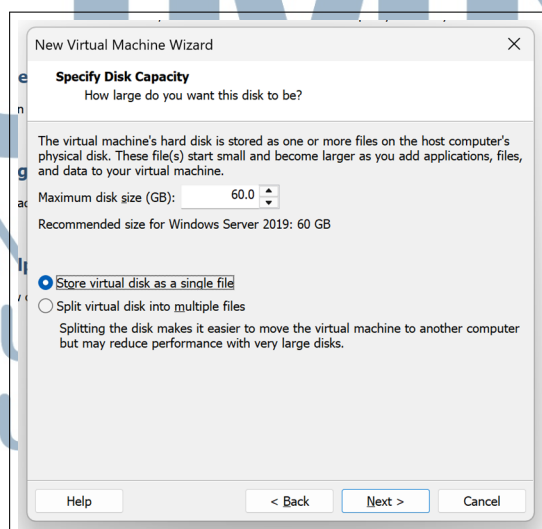
Gambar 3.4. Mengisi Informasi untuk *Administrator* Windows Server

Konfigurasi instalasi Windows Server 2019 dilakukan menggunakan fitur *Easy Install* dari VMware sebagaimana ditunjukkan pada Gambar 3.4. Versi sistem operasi yang dipilih adalah Windows Server Datacenter Core untuk mendukung kebutuhan virtualisasi. Informasi personal seperti nama pengguna dan kata sandi telah diisi dan dikonfirmasi guna memastikan keamanan akses. Proses ini digunakan sebagai dasar pembentukan lingkungan server virtual yang terstandarisasi.

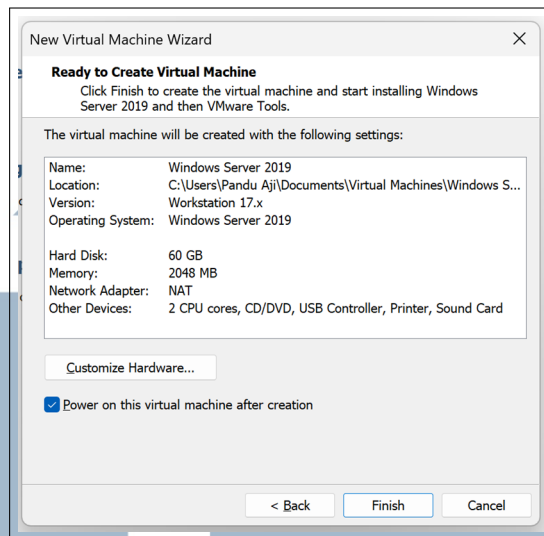


Gambar 3.5. Pemberian Nama dan Lokasi Penyimpanan untuk VM

Pemberian nama dan lokasi penyimpanan untuk virtual machine (VM) dilakukan sesuai dengan langkah yang ditunjukkan pada Gambar 3.5. Selanjutnya, pada Gambar 3.6 pengaturan kapasitas disk dilakukan dengan memilih ukuran 60 GB, yang merupakan ukuran yang direkomendasikan untuk Windows Server 2019. Opsi penyimpanan disk virtual yang digunakan adalah *Store virtual disk as a single file*, yang menyimpan *disk virtual* sebagai satu *file* besar di komputer *host*. Metode ini dipilih karena lebih efisien dalam hal kinerja, mengingat *disk* akan diakses sebagai satu kesatuan.



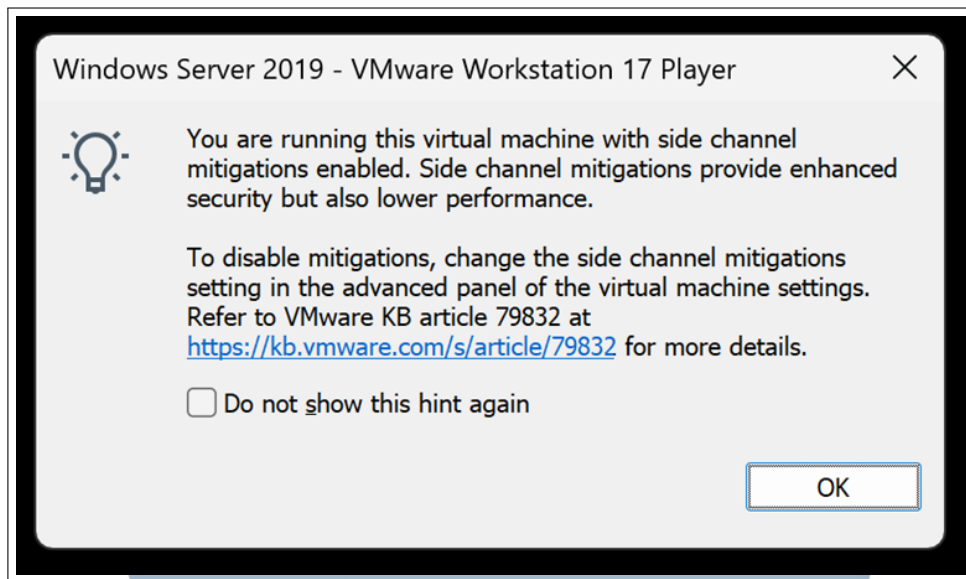
Gambar 3.6. Pengaturan *Disk Capacity* VM



Gambar 3.7. Ringkasan *Settings* VM

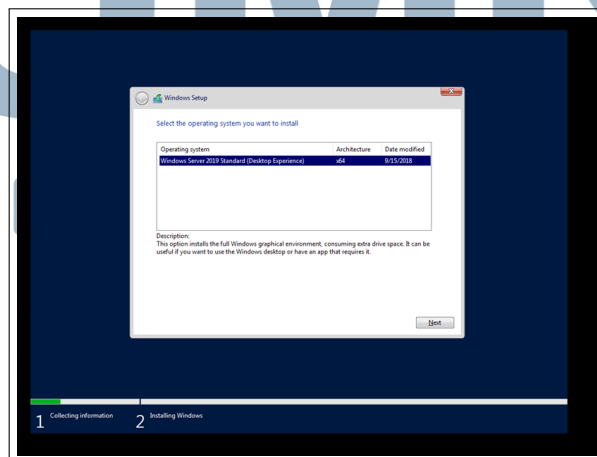
Pada Gambar 3.7 menunjukkan tampilan "Ready to Create Virtual Machine" menunjukkan konfigurasi yang akan diterapkan pada *virtual machine* yang akan dibuat. *Virtual machine* akan diberi nama "Windows Server 2019" dan disimpan di lokasi yang telah ditentukan, dengan kapasitas hard disk sebesar 60 GB dan memori 2048 MB. Pengaturan jaringan menggunakan adaptor NAT, dan dua inti CPU, serta perangkat lain seperti CD/DVD, USB Controller, Printer, dan Sound Card telah ditambahkan. Setelah konfigurasi selesai, opsi untuk menyalakan virtual machine setelah pembuatan dipilih, yang memungkinkan sistem langsung dijalankan setelah proses pembuatan selesai.

U M N
U N I V E R S I T A S
M U L T I M E D I A
N U S A N T A R A

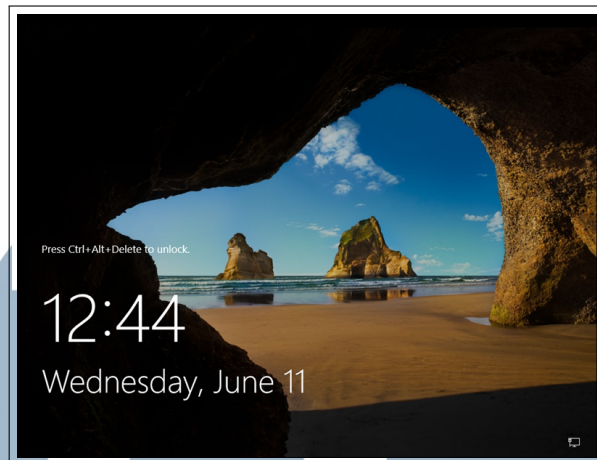


Gambar 3.8. Pemberitahuan *Side Channel Mitigations*

Gambar 3.8 merupakan pesan yang menginformasikan bahwa virtual machine yang sedang dijalankan telah mengaktifkan *side channel mitigation*, yang bertujuan untuk meningkatkan keamanan sistem dengan melindungi dari potensi serangan yang memanfaatkan *side channel*. Meskipun mitigasi ini memberikan perlindungan tambahan, penerapannya dapat menyebabkan penurunan kinerja pada virtual machine. Selanjutnya, Gambar 3.9 menggambarkan pilihan sistem operasi yang digunakan, yaitu Windows Server 2019 Standard (Desktop Experience), yang dipilih untuk mendukung deployment *virtual machine* dengan pengaturan yang telah ditentukan.

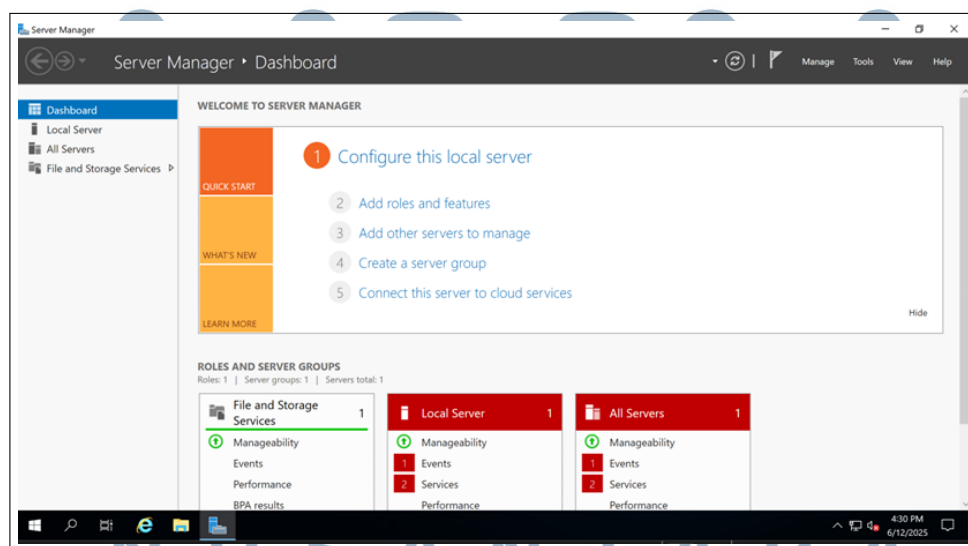


Gambar 3.9. Memilih Versi Windows Server



Gambar 3.10. Tampilan *Lock Screen* Windows Server 2019

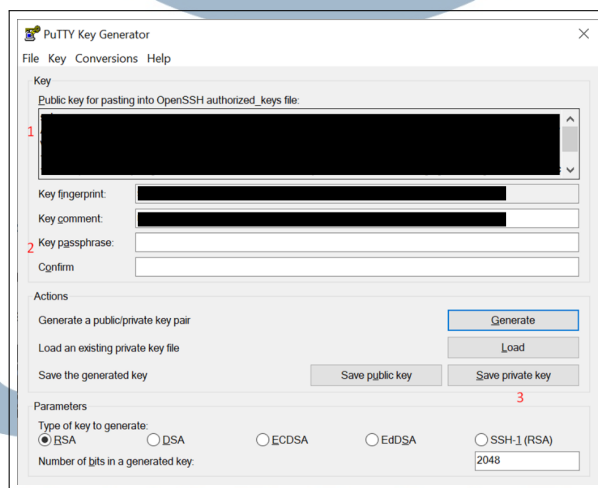
Gambar 3.10 memperlihatkan tampilan *lock screen* Windows Server 2019, yang hanya dapat dibuka dengan menekan kombinasi Ctrl+Alt+Delete. Selanjutnya, Gambar 3.11 menampilkan *Server Manager* di Windows Server, yang menyediakan alat untuk mengelola, memantau, dan mengonfigurasi server secara efisien. Fitur ini memungkinkan *administrator server* untuk melakukan tugas-tugas administrasi dengan lebih mudah dan terstruktur. Dengan adanya *Server Manager*, pengelolaan dan pengaturan server dapat dilakukan secara lebih terorganisir dan efektif.



Gambar 3.11. Tampilan *Server Manager* Windows Server 2019

3.3.2 Deploy CipherTrust Manager

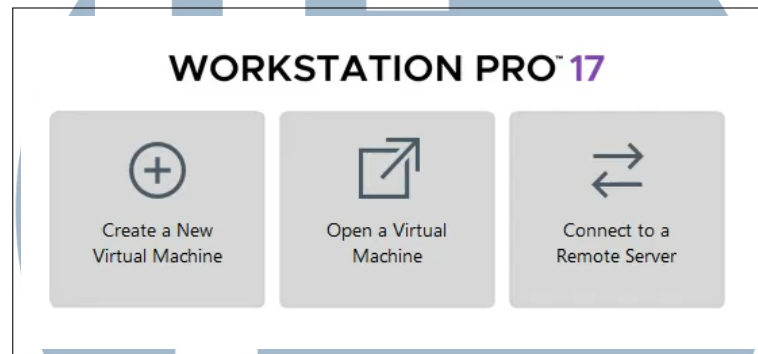
CipherTrust Manager adalah solusi manajemen keamanan data yang dirancang untuk membantu perusahaan dalam mengelola dan melindungi data sensitif dengan menggunakan enkripsi dan pengelolaan kunci secara efisien. Dengan menggunakan CipherTrust Manager, perusahaan dapat mengimplementasikan kebijakan enkripsi yang konsisten di seluruh infrastruktur TI mereka, baik itu di data center, cloud, atau lingkungan hybrid. Solusi ini memungkinkan pengendalian akses yang lebih baik, mitigasi risiko kebocoran data, serta memastikan kepatuhan terhadap regulasi perlindungan data seperti UU PDP. CipherTrust Manager juga mempermudah perusahaan dalam mengelola kunci enkripsi dan mengurangi kompleksitas operasional terkait perlindungan data sensitif, memberikan lapisan keamanan yang kuat bagi aset perusahaan. Langkah pertama untuk mendeploy CipherTrust Manager adalah membuat RSA key yang dibutuhkan oleh CipherTrust Manager. RSA key ini dapat dibuat menggunakan PuTTYgen, sebuah tool yang memungkinkan pengguna untuk membuat pasangan kunci publik dan privat yang digunakan untuk otentikasi berbasis kunci SSH.



Gambar 3.12. Pembuatan Pasangan Kunci RSA Menggunakan PuTTYgen

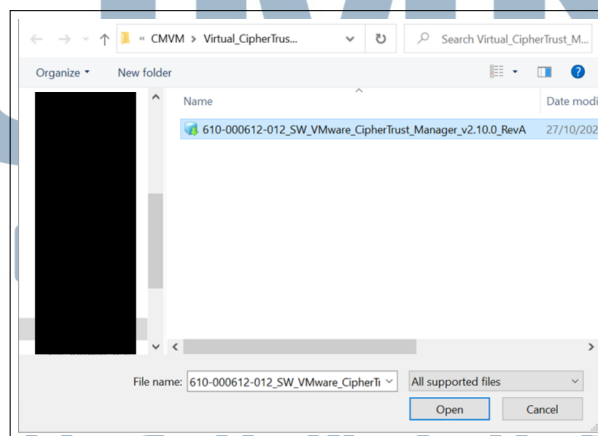
Proses pembuatan *key* dimulai dengan menjalankan aplikasi PuTTYgen, seperti yang ditunjukkan pada Gambar 3.12 diikuti dengan penekanan tombol *generate* untuk menghasilkan data acak yang diperlukan dalam pembuatan *key*. Setelah *public key* dihasilkan, disarankan untuk menyalin *public key* tersebut ke dalam Notepad, dengan menghindari penggunaan tombol Save Public Key karena format yang dihasilkan tidak sesuai dengan kebutuhan. Selanjutnya, *passphrase*

dimasukkan untuk melindungi *private key* dengan mengenkripsi *key* tersebut. Setelah *passphrase* dimasukkan, *private key* disimpan dalam file di komputer untuk digunakan dalam autentikasi SSH, yang memberikan tingkat keamanan lebih tinggi dibandingkan dengan penggunaan kata sandi konvensional, karena mengandalkan enkripsi kunci untuk autentikasi.

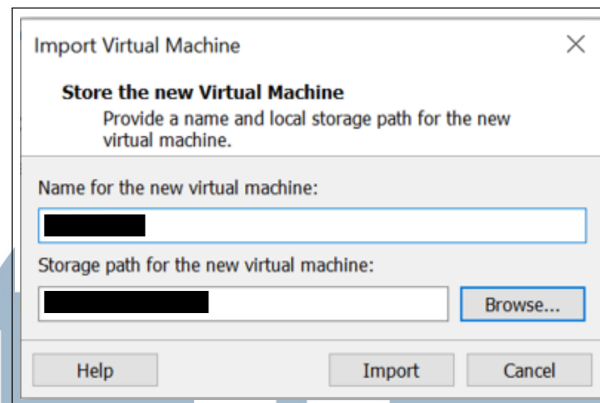


Gambar 3.13. Membuat *Virtual Machine* Baru

Gambar 3.13 menunjukkan langkah yang dilakukan untuk mengelola *virtual machine* menggunakan VMware Workstation. Proses dimulai dengan pemilihan opsi *Open a Virtual Machine* pada VMware Workstation Pro. Selanjutnya, *file* konfigurasi CipherTrust Manager dibuka dengan mencari lokasi *file* yang sesuai dengan folder tempat penyimpanan, sebagaimana ditampilkan pada Gambar 3.14. Setelah *file* konfigurasi ditemukan, tombol *Open* dipilih untuk melanjutkan proses pengelolaan *virtual machine*.

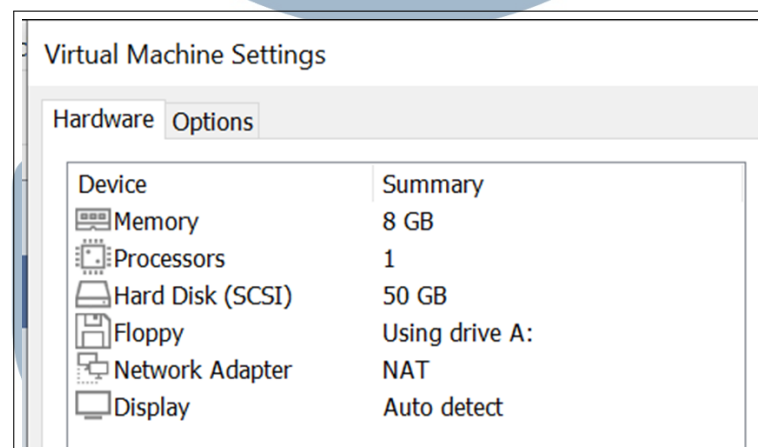


Gambar 3.14. Memilih File Konfigurasi CM



Gambar 3.15. *Import File* Konfigurasi CM

Setelah file konfigurasi dipilih, file tersebut diimpor ke dalam VMware Workstation, sebagaimana ditunjukkan pada Gambar 3.15. Pengaturan *virtual machine* kemudian dilakukan sesuai dengan konfigurasi yang ditampilkan pada Gambar 3.16. Setelah memastikan bahwa pengaturan telah sesuai, *virtual machine* dijalankan untuk melanjutkan proses selanjutnya. Kedua langkah ini memastikan bahwa *virtual machine* siap digunakan dengan konfigurasi yang tepat.



Gambar 3.16. *Settings Virtual Machine* CM

UNIVERSITAS
MULTIMEDIA
NUSANTARA

```
@ciphertrust:~$ kscfg net interfaces list
{
  "skip": 0,
  "limit": 0,
  "total": 1,
  "resources": [
    {
      "name": "ens32",
      "inet": {
        "method": "dhcp",
        "ip": " ",
        "netmask": "255.255.255.0",
        "gateway": " ",
        "dns": [
          " "
        ],
        "force_gateway": true
      },
      "inet6": {
        "method": "auto"
      }
    }
  ]
}
```

Gambar 3.17. Konfigurasi Jaringan CipherTrust

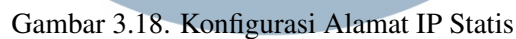
Berdasarkan Gambar 3.17, *command* 'kscfg net interfaces list' akan menampilkan daftar antarmuka jaringan yang dikonfigurasi pada sistem. Dalam hal ini karena output menghasilkan ("total":1), menandakan bahwa konfigurasinya hanya dari satu antarmuka jaringan saja. Selbihnya dalam konteks output perintah, berikut adalah penjelasan tentang bagian utama output.

1. *skip*: Ini menunjukkan jumlah elemen yang akan dilewati (skip) dalam hasil yang ditampilkan.
2. *limit*: Ini menunjukkan jumlah maksimum elemen yang ingin ditampilkan.
3. *total*: Ini menunjukkan jumlah total elemen yang tersedia dalam data yang diproses.
4. *resources*: Ini adalah array (daftar) yang berisi data atau objek yang sebenarnya ingin ditampilkan atau diproses.

Selanjutnya didalam *resources* terdapat output tambahan, berikut merupakan penjelasannya.

1. *name*: Ini merupakan nama interface yang terhubung dengan jaringan internet.
2. *inet*: Output ini merujuk pada konfigurasi IPv4 antarmuka jaringan. Dimana didalam sini ada keterangan, seperti metode yang digunakan, alamat IP yang

3. *inet6*: Output ini merujuk pada konfigurasi IPv6 antarmuka jaringan, sehingga konfigurasinya dilakukan secara otomatis oleh sistem.





Your connection is not private

Attackers might be trying to steal your information from **192.168.153.130** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID



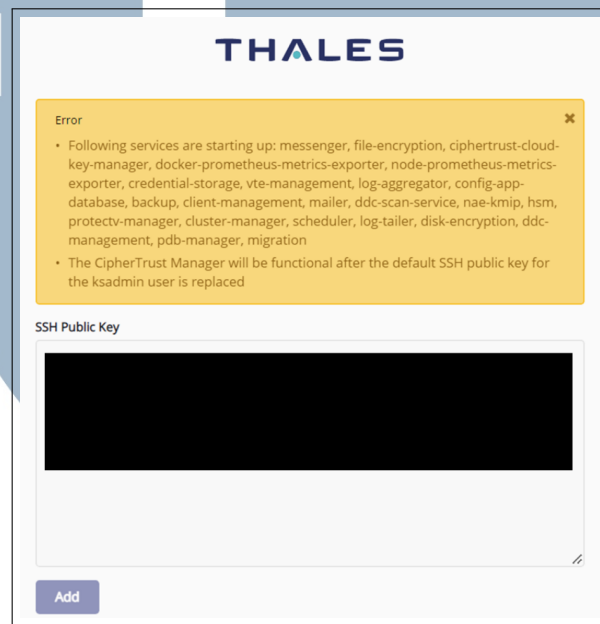
To get Chrome's highest level of security, [turn on enhanced protection](#)

Advanced

Back to safety

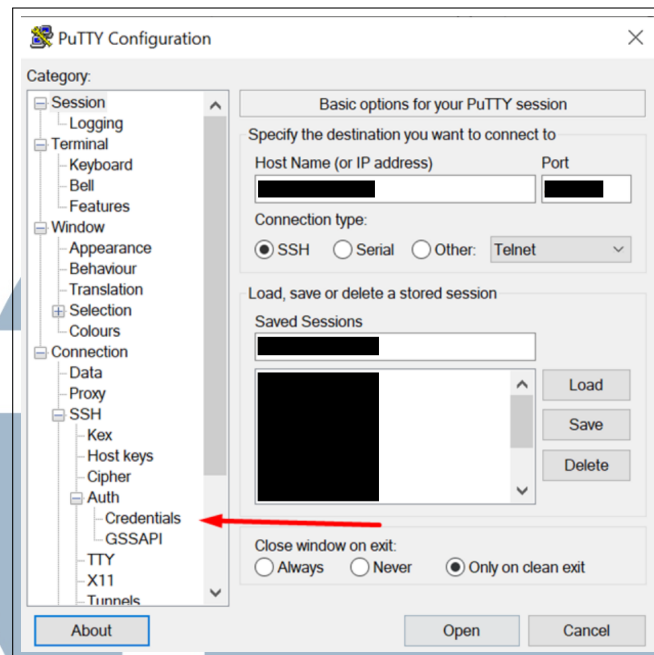
Gambar 3.19. Advanced Connection

Setelah konfigurasi pada antarmuka jaringan selesai, alamat IP yang telah dikonfigurasi dimasukkan ke dalam browser. Selanjutnya, sesuai dengan Gambar 3.19 tombol *Advanced* diklik untuk melanjutkan proses. SSH *public key* yang telah disimpan kemudian diletakkan pada *Text Box*, sebagaimana ditunjukkan pada Gambar 3.20. Langkah-langkah ini memastikan bahwa koneksi aman dapat dibentuk dengan menggunakan metode autentikasi berbasis kunci publik.



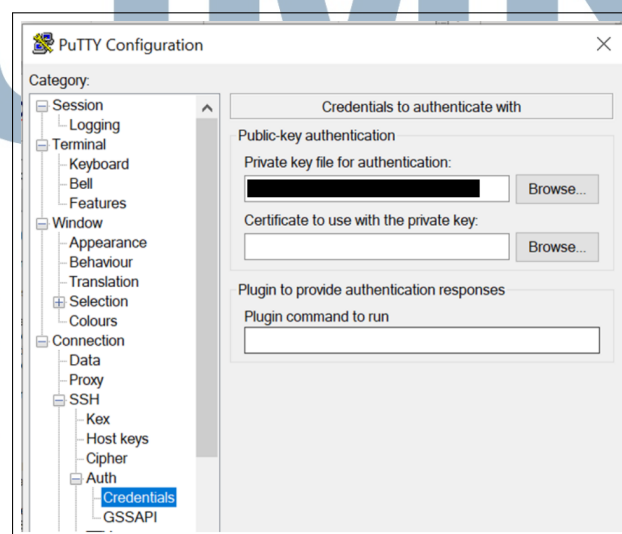
Gambar 3.20. Text Box SSH *Public Key*

UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA



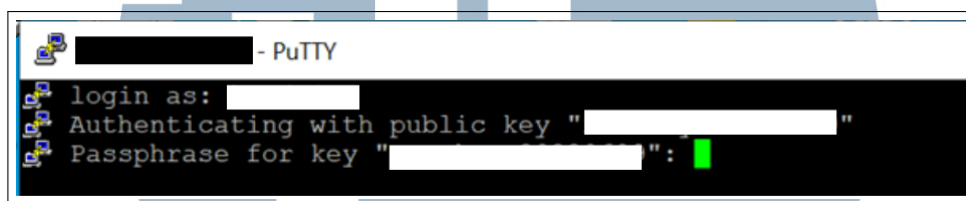
Gambar 3.21. Konfigurasi Jaringan CM pada PuTTY

Pada Gambar 3.21 tersebut, konfigurasi dasar untuk sesi PuTTY ditampilkan, di mana alamat IP CipherTrust Manager dapat dimasukkan pada bagian *Host Name (or IP address)*. Pengaturan koneksi dipilih sebagai SSH, yang memungkinkan koneksi aman melalui protokol tersebut. Pada bagian *Credentials*, opsi untuk memasukkan informasi autentikasi, seperti *private key*, dapat diakses. Setelah pengaturan selesai, tombol *Open* dapat dipilih untuk memulai sesi koneksi ke server yang dituju.

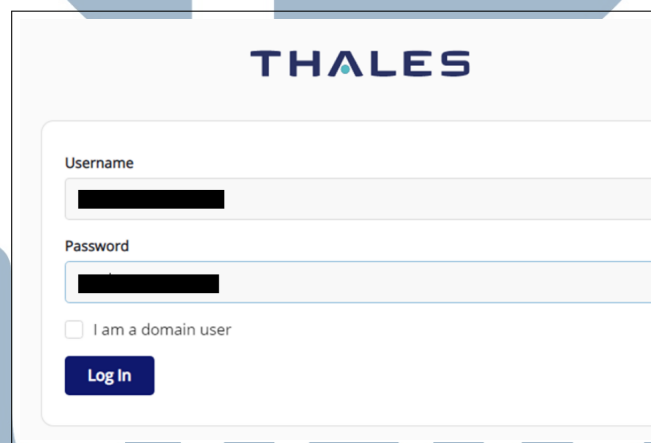


Gambar 3.22. Konfigurasi Autentikasi *Public Key* di PuTTY

Gambar 3.22 menunjukkan konfigurasi autentikasi *public key* yang digunakan pada PuTTY. Pada bagian ini, file *private key* yang diperlukan untuk autentikasi dimasukkan, memastikan koneksi yang aman dan terverifikasi. Selanjutnya, Gambar 3.23 menunjukkan tampilan antarmuka PuTTY yang digunakan untuk melakukan autentikasi dengan *public key*. Pada proses autentikasi, sistem mengonfirmasi penggunaan *public key* yang telah dipilih sebelumnya. Passphrase untuk *private key* yang digunakan akan diminta sebagai langkah tambahan untuk memastikan bahwa kunci tersebut tetap aman dan terlindungi. .



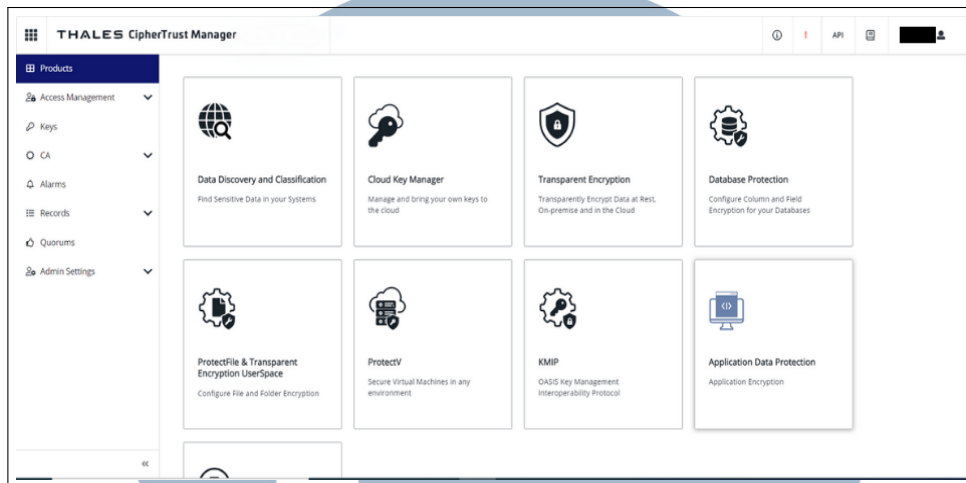
Gambar 3.23. Proses Autentikasi SSH Menggunakan *Public Key* di PuTTY



Gambar 3.24. Login CipherTrust Manager

Sesuai dengan Gambar 3.24 tersebut, untuk mengakses CipherTrust Manager maka kita memerlukan *login* terlebih dahulu. Setelah informasi yang diperlukan dimasukkan, tombol Log In digunakan untuk mengonfirmasi dan melanjutkan ke sesi berikutnya. Proses ini memastikan bahwa hanya pengguna yang terverifikasi yang dapat mengakses sistem dengan kredensial yang sesuai. Gambar 3.25 menunjukkan tampilan antarmuka dari CipherTrust Manager, yang berfungsi sebagai platform untuk manajemen keamanan data, dengan berbagai opsi dan fitur untuk pengelolaan perlindungan data, seperti Data Encryption and Decryption, Cloud Key Manager, Transparent Encryption, dan Data Loss Prevention. Setiap

fitur dilengkapi dengan ikon yang mewakili fungsinya, memberikan kemudahan dalam pengelolaan, konfigurasi, dan pemantauan keamanan data secara efisien.



Gambar 3.25. Antarmuka CipherTrust Manager

3.3.3 Preventive Maintenance untuk HSM

Hardware Security Module (HSM) merupakan alat khusus yang digunakan untuk menjalankan operasi kriptografi secara aman serta untuk mengelola kunci dengan tingkat keamanan tinggi [10]. *Preventive Maintenance (PM)* perangkat HSM adalah langkah-langkah yang diambil untuk memastikan perangkat tetap berfungsi dengan baik, mengurangi kemungkinan kerusakan, serta meminimalkan risiko kegagalan sistem yang dapat mengganggu operasi penting yang terkait dengan pengelolaan kunci dan enkripsi. PM perlu dilakukan secara rutin, minimal empat kali dalam setahun, guna menjaga performa optimal dari perangkat. Frekuensi dan lingkup PM juga dapat disesuaikan berdasarkan kebutuhan dan kompleksitas operasional dari masing-masing klien. Informasi yang akan dibahas adalah hasil dari PM perangkat HSM dimana akan membahas beberapa aspek berikut.

1. Informasi HSM *Data Center (DC)*
2. Informasi HSM *Disaster Recovery Center (DRC)*
3. Informasi HSM *Development*

A Informasi HSM DC

Hardware Security Module (HSM) Data Center (DC) merupakan jenis HSM yang digunakan secara khusus di lingkungan produksi untuk mendukung keamanan sistem operasional inti. Perangkat ini berperan penting dalam menjaga integritas dan kerahasiaan proses kriptografi pada sistem yang bersifat yang sangat penting bagi jalannya operasional perusahaan. Dalam rangka menjaga performa dan keandalannya, sejumlah data dari HSM DC dikumpulkan secara berkala. Data tersebut digunakan untuk memantau kondisi perangkat secara menyeluruh dan memastikan bahwa langkah perawatan dapat dilakukan secara tepat waktu melalui kegiatan *Preventive Maintenance (PM)* yang terstruktur dan berkelanjutan.

A.1 Tinjauan Status Umum Perangkat HSM DC

Status umum perangkat HSM DC ditinjau melalui akses SSH menggunakan *command 'hsm show'*. Berdasarkan Gambar 3.26 perangkat memiliki versi *software 7.2.0* dan *firmware 7.0.3* yang merupakan versi terbaru, sehingga dari segi keamanan akan lebih aman, dan fitur-fitur sudah paling lengkap. Teridentifikasi satu partisi aktif, dari total maksimum lima partisi yang dapat dibuat, yang mana partisi tersebut sudah disesuaikan dengan kebutuhan, jika partisi aktif terlalu banyak atau tidak dikelola dengan baik, bisa menimbulkan pemborosan *resource*. *System temperature* tercatat berada di bawah *warning threshold*, sehingga masih dalam kondisi yang aman, jika suhu sistem melebihi batas *threshold* yang sudah ditetapkan maka HSM akan mengaktifkan fitur *shutdown* untuk mencegah kerusakan fatal.

U N I V E R S I T A S
M U L T I M E D I A
N U S A N T A R A

```
[redacted] lunash:>hsm show

Appliance Details:
=====
Software Version:          7.2.0-220

HSM Details:
=====
HSM Label:                 [redacted]
Serial #:                  [redacted]
Firmware:                  7.0.3
HSM Model:                 Luna K7
HSM Part Number:           [redacted]
Authentication Method:     PED keys
HSM Admin login status:    Not Logged In
HSM Admin login attempts left: 3 before HSM zeroization!
RPV Initialized:           Yes
Audit Role Initialized:    No
Remote Login Initialized:  No
Manually Zeroized:         No
Secure Transport Mode:     No
HSM Tamper State:          No tamper(s)

Partitions created on HSM:
=====
Partition: [redacted], Name: [redacted]

Number of partitions allowed: 5
Number of partitions created: 1

FIPS 140-2 Operation:
=====
The HSM is NOT in FIPS 140-2 approved operation mode.

HSM Storage Information:
=====
Maximum HSM Storage Space (Bytes): 2097152
Space In Use (Bytes): 419430
Free Space Left (Bytes): 1677722

Environmental Information on HSM:
=====
Battery Voltage: 3.072 V
Battery Warning Threshold Voltage: 2.750 V
System Temp: 48 deg. C
System Temp Warning Threshold: 75 deg. C

Command Result : 0 (Success)
```

Gambar 3.26. Informasi Status Umum Perangkat HSM DC

A.2 Tinjauan Status Network Perangkat HSM DC

Status konfigurasi jaringan perangkat HSM DC dapat dipantau melalui akses SSH menggunakan *command* 'network show'. Gambar 3.27 menunjukkan ketiga port ethernet dalam keadaan aktif. Port eth0 dan eth1 berada dalam status *bounding* yang digunakan untuk koneksi data, sedangkan eth2 digunakan untuk koneksi manajemen dan eth3 digunakan untuk koneksi langsung ke HSM DC selama PM. Jika port eth0 dan eth1 tidak melakukan *bounding* terhadap IP yang dituju, hal tersebut mengindikasikan bahwa koneksi data terputus, yang dapat menyebabkan kehilangan akses ke layanan yang tergantung pada koneksi data tersebut, serta menurunnya kinerja sistem secara keseluruhan.

```
[redacted] lunash:>network show

Hostname : [redacted]
Name Server(s) :
Search Domain(s) : <not set>

Interface settings and status

HW Address (eth0) : [redacted]
Bond master (eth0) : bond0
Link detected (eth0) : Yes

HW Address (eth1) : [redacted]
Bond master (eth1) : bond0
Link detected (eth1) : Yes

HW Address (eth2) : [redacted]
IP Address (eth2) :
Mask (eth2) : 255.255.255.0
Gateway (eth2) : [redacted]
DNS (eth2) :
DNS Search (eth2) :
IP Protocol (eth2) : IPv4
Protocol (eth2) : Static
Auto Connect (eth2) : Yes
Activated (eth2) : Yes
Link detected (eth2) : Yes

HW Address (eth3) : [redacted]
IP Address (eth3) :
Mask (eth3) : 255.255.255.0
Gateway (eth3) : [redacted]
DNS (eth3) :
DNS Search (eth3) :
IP Protocol (eth3) : IPv4
Protocol (eth3) : Static
Auto Connect (eth3) : Yes
Activated (eth3) : No
Link detected (eth3) : No

HW Address (bond0) : [redacted]
IP Address (bond0) :
Mask (bond0) : 255.255.255.0
Gateway (bond0) : [redacted]
DNS (bond0) :
DNS Search (bond0) :
IP Protocol (bond0) : IPv4
Protocol (bond0) : Static
Auto Connect (bond0) : Yes
Activated (bond0) : Yes
Link detected (bond0) : Yes
Active Slaves (bond0) : eth1 eth0
Status (bond1) : Not configured

Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 [redacted] 0.0.0.0 UG 100 0 0 eth2
0.0.0.0 [redacted] 0.0.0.0 UG 300 0 0 bond0
[redacted] 0.0.0.0 255.255.255.0 U 300 0 0 bond0
[redacted] 0.0.0.0 255.255.255.0 U 100 0 0 eth2

Command Result : 0 (Success)
```

Gambar 3.27. Informasi Status Network Perangkat HSM DC

A.3 Tinjauan Status Aksesoris Perangkat HSM DC

Untuk memantau *status sensor* dari *fan*, CPU, atau memori pada HSM DC, dapat dilakukan melalui SSH dengan *command* 'status sensors'. Gambar 3.28 menunjukkan kecepatan *fan*, suhu pada CPU dan memori, serta tegangan pada beberapa titik berada dalam kondisi normal. Dengan demikian, tidak ada indikasi kebutuhan untuk penggantian atau tindakan lanjutan. Namun, Jika nilai-nilai tersebut tidak normal, dapat menyebabkan masalah serius seperti *overheat*, kerusakan perangkat keras, dan kegagalan sistem akibat panas berlebih atau tegangan yang tidak stabil.

```
lunash:status sensors

This command displays the fan speed, temperature and voltage of the motherboard and power supply units.

Sensor | Reading | Unit | status | Thresholds
-----|-----|-----|-----|-----
Fan1A | 6000.000 | RPM | OK | 1000.000 | 2000.000 | na | na
Fan1B | 5400.000 | RPM | OK | 1000.000 | 2000.000 | na | na
Fan2A | 6000.000 | RPM | OK | 1000.000 | 2000.000 | na | na
Fan2B | 5600.000 | RPM | OK | 1000.000 | 2000.000 | na | na
Fan3A | 6000.000 | RPM | OK | 1000.000 | 2000.000 | na | na
Fan3B | 5100.000 | RPM | OK | 1000.000 | 2000.000 | na | na
CPU | 65.000 | degrees C | OK | na | na | 95.000 | 100.000
VDD | 37.000 | degrees C | OK | na | na | 105.000 | 110.000
VDS | 35.000 | degrees C | OK | na | na | 95.000 | 100.000
Inlet | 33.000 | degrees C | OK | na | na | 87.000 | 97.000
CSM D181 | 34.000 | degrees C | OK | na | na | 87.000 | 97.000
CSM D181 | na | degrees C | na | na | na | 87.000 | 97.000
CSM D182 | na | degrees C | na | na | na | 87.000 | 97.000
CSM D182 | na | degrees C | na | na | na | 87.000 | 97.000
RAN T18X | 34.000 | degrees C | OK | na | na | na | na
+12V | 12.000 | Volts | OK | na | 11.140 | 12.960 | na
+5V | 4.980 | Volts | OK | na | 4.480 | 5.370 | na
+5Vsb | 3.320 | Volts | OK | na | 3.040 | 3.540 | na
+5Vsb | 4.980 | Volts | OK | na | 4.480 | 5.370 | na
+5Vsb | 3.320 | Volts | OK | na | 3.040 | 3.540 | na
CPU_VCORE | 0.780 | Volts | OK | na | na | na | na
VCCIO | 1.080 | Volts | OK | na | 0.980 | 1.180 | na
VCCIO | 0.980 | Volts | OK | na | 0.880 | 1.020 | na
+12V | 1.230 | Volts | OK | na | 1.130 | 1.290 | na
+12V | 1.230 | Volts | OK | na | 1.130 | 1.290 | na
+12V_RCH | 0.980 | Volts | OK | na | 0.880 | 1.080 | na
+12V_RCH | 1.130 | Volts | OK | na | 1.070 | 1.190 | na
+12V_RCH | 1.230 | Volts | OK | na | 1.170 | 1.350 | na
+12V_RCH | 1.170 | Volts | OK | na | 1.070 | 1.350 | na
VBAT | 3.220 | Volts | OK | na | 2.100 | 2.500 | na
PSU1_V12V_value | 11.880 | Volts | OK | na | 10.800 | 13.200 | na
PSU1_Temp_value | 42.000 | degrees C | OK | na | na | 50.000 | na
PSU1_FAN_value | 7200.000 | RPM | OK | 1000.000 | 1300.000 | na | na
PSU1_V12V_value | 11.820 | Volts | OK | na | 10.190 | 13.200 | na
PSU1_Temp_value | 42.000 | degrees C | OK | na | na | 50.000 | na
PSU1_FAN_value | 7000.000 | RPM | OK | 1000.000 | 1300.000 | na | na
PSU1_Status | OK | discrete | 0x0100 | na | na | na | na
PSU1_Status | OK | discrete | 0x0100 | na | na | na | na
CPU_Thermstrip | OK | discrete | 0x0080 | na | na | na | na
Watchdog | OK | discrete | 0x0000 | na | na | na | na

Notes:
NR: Not Reading (Error)
CR: Critical
O.O: SSI means fan unplugged, failed, or sensor not readable
D181: Dual In-Line Memory Module
PSU1: Power Supply Unit 1
PSU2: Power Supply Unit 2
Fan1, Fan2 and Fan3 are pluggable modules on the front of the appliance.
Each fan unit contains two fans: A and B.

----- Power Supplies Status -----
PSU1_Status | Presence detected
PSU2_Status | Presence detected
CPU_Thermstrip | OK
Watchdog | OK

----- Front Cooling Fans Status -----
Fan1A | OK | 6000 RPM
Fan1B | OK | 5400 RPM
Fan2A | OK | 6000 RPM
Fan2B | OK | 5600 RPM
Fan3A | OK | 6000 RPM
Fan3B | OK | 5100 RPM
PSU1_FAN_value | OK | 7200 RPM
PSU2_FAN_value | OK | 7000 RPM

----- chassis status -----
System Power | na
Power Overload | na
Power Interruption | inactive
Halt Power Fault | na
Power Control Fault | na
Power Restore Policy | restore
Power Restore Policy | no-failed
Last Power Event | na
Chassis Intrusion | inactive
Front-Panel Lockout | inactive
Drive Fault | na
Cooling/Fan Fault | na
Sleep Button Disabled | not allowed
Sleep Button Disabled | not allowed
Power Button Disabled | allowed
Sleep Button Disabled | na
Sleep Button Disabled | na
Sleep Button Disabled | na
Power Button Disabled: na
```

Gambar 3.28. Informasi Status Aksesori Perangkat HSM DC

A.4 Tinjauan Status Partisi Perangkat HSM DC

Status partisi pada HSM DC dapat diperiksa melalui koneksi SSH dengan menggunakan *command* 'partition list' untuk menampilkan daftar partisi dan 'partition show' untuk melihat detail masing-masing partisi. Gambar 3.29 menyajikan informasi terkait kapasitas penyimpanan, status autentikasi, serta indikator keamanan seperti jumlah percobaan *login* yang tersisa. Informasi yang ditampilkan menunjukkan bahwa partisi berada dalam kondisi normal tanpa indikasi masalah pada konfigurasi maupun sistem keamanannya. Namun, apabila terjadi masalah pada kapasitas penyimpanan, autentikasi, atau percobaan *login* yang tersisa dapat menurunkan kinerja, mengganggu akses sah, meningkatkan risiko pelanggaran keamanan, dan memperburuk potensi serangan *brute force* sehingga isi dalam partisi akan terhapus. Hal tersebut menyebabkan pemantauan dan penanganan segera sangat diperlukan untuk menjaga kelancaran dan keamanan sistem.


```

[ ] lunash:>partition list

                                     Storage (bytes)
-----
Partition      Name                  Objects  Total    Used    Free
-----
[ ]             [ ]                  4  409782   3412   406370

Command Result : 0 (Success)
[ ] lunash:>partition show

Partition Name: [ ]
Partition SN: [ ]
Partition Label:
Partition SO    PIN To Be Changed: no
Partition SO    Challenge To Be Changed: no
Partition SO    Zeroized: no
Partition SO    Login Attempts Left: 10
Crypto Officer  PIN To Be Changed: no
Crypto Officer  Challenge To Be Changed: no
Crypto Officer  Locked Out: no
Crypto Officer  Login Attempts Left: 10
Crypto Officer  is activated: yes
Crypto User     is not initialized.
Legacy Domain Has Been Set: no
Partition Storage Information (Bytes): Total=409782, Used=3412, Free=406370
Partition Object Count: 4

Command Result : 0 (Success)

```

Gambar 3.29. Informasi Status Partisi Perangkat HSM DC

A.5 Tinjauan Status Sistem Perangkat HSM DC

Status sistem HSM DC dapat diperiksa menggunakan *command* 'status systat show', yang menampilkan kondisi sistem secara keseluruhan. Pada Gambar 3.30 HSM DC berada dalam status In Service Okay (ISO), yang menandakan bahwa perangkat beroperasi secara normal dan fungsi-fungsi penting berjalan dengan baik. Selain status ISO, terdapat pula beberapa kemungkinan status lain yang dapat muncul pada sistem, seperti *In Service with Trouble* (IST) yang mengindikasikan adanya gangguan pada subsistem meskipun perangkat masih beroperasi, *Off Line* (OFL) yang berarti perangkat tidak terhubung ke jaringan dan tidak dapat memberikan layanan, serta *Out Of Service* (OOS) yang menunjukkan bahwa perangkat menyala tetapi subsistem penting tidak berjalan. Beberapa kode turut ditampilkan, seperti kode 100 yang menunjukkan webserver tidak diaktifkan (biasanya untuk REST API), kode 63 menandakan antarmuka jaringan eth3 tidak terhubung, serta kode 95 menunjukkan bahwa protokol *Simple Network Management Protocol* (SNMP) tidak diaktifkan. Informasi ini penting sebagai indikator stabilitas dan konfigurasi sistem pada HSM DC.

```
[root@hsm] lunash:>status sysstat show

Volatile State:
sysstat is running
Service Status: sysstat is running

Non-volatile State:
Enabled

System Status Monitor - Current Status
=====
Hostname:          bhmhsmdc01
Interface eth0:    [REDACTED]
Interface eth1:    [REDACTED]
Interface eth2:    [REDACTED]
Interface eth3:    not configured
Software Version:  SA:7.2.0-220
System Status:     ISO
System Status Code: 100,63,95
Status Check Time: 15:10 [REDACTED]

System State Description

ISO (In Service Okay):      The appliance is online and the necessary subsystems are operational.
IST (In Service with Trouble): The appliance is online and the necessary subsystems are operational with some troubles.
OFL (Off Line):             The appliance is not currently connected to the Ethernet network and cannot provide service.
OOS (Out Of Service):       The appliance is online but the necessary subsystems are NOT operational.

Command Result : 0 (Success)
```

Gambar 3.30. Informasi Status Sistem Perangkat HSM DC

B Informasi HSM DRC

Hardware Security Module (HSM) Disaster Recovery Center (DRC) adalah jenis HSM yang dirancang untuk digunakan sebagai cadangan dalam situasi darurat atau kegagalan sistem. HSM DRC berfungsi untuk memastikan kelangsungan operasional perangkat HSM yang berada di pusat data utama (HSM DC) jika terjadi gangguan atau kerusakan pada sistem utama. HSM DRC dilengkapi dengan kemampuan untuk mengambil alih fungsi HSM DC dengan cepat, sehingga proses kriptografi yang sensitif dan perlindungan data tetap terjaga. Bagian ini akan menjelaskan tentang aspek dari HSM DRC yang datanya dikumpulkan untuk keperluan *preventive maintenance* (PM).

B.1 Tinjauan Status Umum Perangkat HSM DRC

Status umum perangkat HSM DRC dapat diperiksa melalui akses SSH dengan menggunakan *command* 'hsm-show'. Berdasarkan Gambar 3.31 perangkat ini menggunakan versi *software* 7.2.0 dan versi *firmware* 7.0.3, yang merupakan versi terbaru, sehingga menjamin tingkat keamanan dan fitur yang lebih baik. Ditemukan satu partisi aktif dari total lima partisi yang dapat dibuat, yang telah disesuaikan dengan kebutuhan sistem. Jika jumlah partisi aktif terlalu banyak atau tidak dikelola dengan baik, hal ini dapat menyebabkan pemborosan sumber daya. Suhu sistem tercatat masih berada di bawah ambang batas peringatan, sehingga dalam kondisi aman. Jika suhu melebihi batas yang ditetapkan, fitur *shutdown* akan diaktifkan untuk mencegah kerusakan yang lebih serius.


```
[REDACTED] lunash:>hsm show

Appliance Details:
=====
Software Version:          7.2.0-220

HSM Details:
=====
HSM Label:                 [REDACTED]
Serial #:                  [REDACTED]
Firmware:                  7.0.3
HSM Model:                 Luna K7
HSM Part Number:           [REDACTED]
Authentication Method:     PED keys
HSM Admin login status:    Not Logged In
HSM Admin login attempts left: 3 before HSM zeroization!
RPV Initialized:           Yes
Audit Role Initialized:    No
Remote Login Initialized:  No
Manually Zeroized:         No
Secure Transport Mode:     No
HSM Tamper State:          No tamper(s)

Partitions created on HSM:
=====
Partition: [REDACTED], Name: [REDACTED]

Number of partitions allowed: 5
Number of partitions created: 1

FIPS 140-2 Operation:
=====
The HSM is NOT in FIPS 140-2 approved operation mode.

HSM Storage Information:
=====
Maximum HSM Storage Space (Bytes): 2097152
Space In Use (Bytes):              419430
Free Space Left (Bytes):           1677722

Environmental Information on HSM:
=====
Battery Voltage:              3.093 V
Battery Warning Threshold Voltage: 2.750 V
System Temp:                  36 deg. C
System Temp Warning Threshold: 75 deg. C

Command Result : 0 (Success)
```

Gambar 3.31. Informasi Status Umum Perangkat HSM DRC

B.2 Tinjauan Status Network Perangkat HSM DRC

Status konfigurasi *network* pada perangkat HSM DRC dapat diperiksa melalui akses SSH menggunakan *command* 'network show'. Gambar 3.32 menunjukkan bahwa ketiga port ethernet dalam kondisi aktif. Port eth0 dan eth1 berfungsi dalam status *bounding* untuk koneksi data, sementara eth2 digunakan untuk koneksi manajemen, dan eth3 untuk koneksi langsung ke HSM DRC selama pemeliharaan preventif. Jika port eth0 dan eth1 tidak terhubung dengan IP yang dituju, hal tersebut menandakan bahwa koneksi data terputus, yang dapat mengakibatkan hilangnya akses ke layanan yang bergantung pada koneksi tersebut dan menurunkan kinerja sistem secara keseluruhan.

```

[ ] lunash:>network show

Hostname : 
Name Server(s) : 
Search Domain(s) : <not set>

Interface settings and status

HW Address (eth0) : 
Bond master (eth0) : bond0
Link detected (eth0) : Yes

HW Address (eth1) : 
Bond master (eth1) : bond0
Link detected (eth1) : Yes

HW Address (eth2) : 
IP Address (eth2) : 
Mask (eth2) : 
Gateway (eth2) : 
DNS (eth2) : 
DNS Search (eth2) : 
IP Protocol (eth2) : IPv4
Protocol (eth2) : Static
Auto Connect (eth2) : Yes
Activated (eth2) : Yes
Link detected (eth2) : Yes

HW Address (eth3) : 
IP Address (eth3) : 
Mask (eth3) : 
Gateway (eth3) : 
DNS (eth3) : 
DNS Search (eth3) : 
IP Protocol (eth3) : IPv4
Protocol (eth3) : Static
Auto Connect (eth3) : Yes
Activated (eth3) : Yes
Link detected (eth3) : No

HW Address (bond0) : 
IP Address (bond0) : 
Mask (bond0) : 
Gateway (bond0) : 
DNS (bond0) : 
DNS Search (bond0) : 
IP Protocol (bond0) : IPv4
Protocol (bond0) : Static
Auto Connect (bond0) : Yes
Activated (bond0) : Yes
Link detected (bond0) : Yes
Active Slaves (bond0) : eth0 eth1
Status (bond1) : Not configured

Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 0.0.0.0 0.0.0.0 UG 100 0 0 eth2
0.0.0.0 0.0.0.0 0.0.0.0 UG 101 0 0 eth3
0.0.0.0 0.0.0.0 0.0.0.0 UG 300 0 0 bond0
0.0.0.0 0.0.0.0 255.255.255.0 U 100 0 0 eth3
0.0.0.0 0.0.0.0 255.255.255.0 U 300 0 0 bond0
0.0.0.0 0.0.0.0 255.255.255.0 U 100 0 0 eth2

Command Result : 0 (Success)

```

Gambar 3.32. Informasi Status Network Perangkat HSM DRC

B.3 Tinjauan Status Aksesoris Perangkat HSM DRC

Status sensor untuk *fan*, CPU, dan memori pada HSM DRC dapat dipantau melalui akses SSH menggunakan *command* 'status sensors'. Gambar 3.33 menunjukkan bahwa kecepatan *fan*, suhu CPU dan memori, serta tegangan pada beberapa titik berada dalam kondisi normal. Oleh karena itu, tidak ditemukan indikasi perlunya penggantian atau tindakan lebih lanjut. Namun, jika nilai-nilai tersebut berada melebihi batas normal, hal ini dapat menimbulkan masalah serius seperti *overheat*, kerusakan perangkat keras, atau kegagalan sistem akibat suhu yang berlebihan atau tegangan yang tidak stabil.

```
[root@hsm-drc ~]# lunashibstatus sensors

This command displays the fan speed, temperature and voltage of the motherboard and power supply units.

Sensor | Reading | Unit | Status | Thresholds
-----|-----|-----|-----|-----
Fan1A | 3900.000 | RPM | OK | 1000.000 | 2000.000 | na | na
Fan1B | 5100.000 | RPM | OK | 1000.000 | 2000.000 | na | na
Fan2A | 3900.000 | RPM | OK | 1000.000 | 2000.000 | na | na
Fan2B | 5100.000 | RPM | OK | 1000.000 | 2000.000 | na | na
Fan3A | 4000.000 | RPM | OK | 1000.000 | 2000.000 | na | na
Fan3B | 5100.000 | RPM | OK | 1000.000 | 2000.000 | na | na
CPU | 26.000 | degrees C | OK | na | 95.000 | 100.000
VRD | 26.000 | degrees C | OK | na | 105.000 | 110.000
PCH | 27.000 | degrees C | OK | na | 95.000 | 104.000
Inlet | 23.000 | degrees C | OK | na | 87.000 | 97.000
CHB DIMM 1 | 26.000 | degrees C | OK | na | 87.000 | 97.000
CHB DIMM 0 | na | degrees C | na | na | 87.000 | 97.000
CHA DIMM 1 | na | degrees C | na | na | 87.000 | 97.000
CHA DIMM 0 | na | degrees C | na | na | 87.000 | 97.000
RAM Thx | 26.000 | degrees C | OK | na | na | na
+12V | 12.000 | Volts | OK | na | 11.140 | 12.900
+5V | 4.690 | Volts | OK | na | 4.460 | 5.370
VDDAin | 3.240 | Volts | OK | na | 3.060 | 3.840
SVSB | 4.690 | Volts | OK | na | 4.460 | 5.370
SVSB | 3.240 | Volts | OK | na | 3.060 | 3.840
CPU VCORE | 0.750 | Volts | OK | na | na | na
VCCA | 1.040 | Volts | OK | na | 0.980 | 1.130
VCCIO | 0.990 | Volts | OK | na | 0.880 | 1.020
LV2 | 1.210 | Volts | OK | na | 1.130 | 1.290
JVS VFB | 2.540 | Volts | OK | na | 2.320 | 2.680
LV0_FCH | 0.980 | Volts | OK | na | 0.930 | 1.080
LV3_BMC | 1.820 | Volts | OK | na | 1.470 | 1.930
LV2_BMC | 1.260 | Volts | OK | na | 1.170 | 1.350
LV0_BMC | 1.740 | Volts | OK | na | 1.470 | 1.930
VBAT | 3.200 | Volts | OK | 2.100 | 2.500 | na
PSU1_+12V_value | 11.820 | Volts | OK | na | 10.800 | 13.200
PSU1_Temp_value | 35.000 | degrees C | OK | na | 50.000 | na
PSU1_FAN_value | 5000.000 | RPM | OK | 1000.000 | 1300.000 | na | na
PSU2_+12V_value | 12.000 | Volts | OK | na | 10.800 | 13.200
PSU2_Temp_value | 35.000 | degrees C | OK | na | 50.000 | na
PSU2_FAN_value | 4600.000 | RPM | OK | 1000.000 | 1300.000 | na | na
PSU1_Status | 0x0 | discrete | 0x0180 | na | na | na
PSU2_Status | 0x0 | discrete | 0x0180 | na | na | na
CPU_Thermtrip | 0x0 | discrete | 0x0080 | na | na | na
Watchdog | 0x0 | discrete | 0x0080 | na | na | na

Notes:
UR: Not Reading (Error)
CR: Critical
0.00 RPM means fan unplugged, failed, or sensors not readable
DIMM: Dual In-Line Memory Module
PSU1: Power Supply Unit 1
PSU2: Power Supply Unit 2
Fan1, Fan2 and Fan3 are pluggable modules on the front of the appliance.
Each fan unit contains two fans: A and B.

----- Power Supplies Status -----
PSU1_Status | Presence detected
PSU2_Status | Presence detected
CPU_Thermtrip | OK
Watchdog | OK

----- Front Cooling Fans Status -----
Fan1A | OK | 3900 RPM
Fan1B | OK | 5100 RPM
Fan2A | OK | 3900 RPM
Fan2B | OK | 5100 RPM
Fan3A | OK | 4000 RPM
Fan3B | OK | 5100 RPM
PSU1_FAN_value | OK | 5000 RPM
PSU2_FAN_value | OK | 4600 RPM

----- Chassis status -----
System Power | on
Power Overload | false
Power Interlock | inactive
Main Power Fault | false
Power Control Fault | false
Power Restore Policy | previous
Last Power Event | no-failed
Chassis Intrusion | inactive
Front-Panel Lockout | inactive
Drive Fault | false
Cooling/fan Fault | false
Sleep Button Disable | not allowed
Diag Button Disable | not allowed
Reset Button Disable | allowed
Power Button Disable | allowed
Sleep Button Disabled | false
Reset Button Disabled | false
Power Button Disabled | false

Command Result : 0 (Success)
```

Gambar 3.33. Informasi Status Aksesoris Perangkat HSM DRC

B.4 Tinjauan Status Partisi Perangkat HSM DRC

Status partisi pada HSM DRC dapat diperiksa melalui koneksi SSH dengan *command* 'partition list' untuk menampilkan daftar partisi dan 'partition show' untuk melihat rincian masing-masing partisi. Gambar 3.34 menyajikan informasi mengenai kapasitas penyimpanan, status autentikasi, serta indikator keamanan seperti jumlah percobaan *login* yang tersisa. Informasi yang ditampilkan menunjukkan bahwa partisi dalam kondisi normal tanpa adanya masalah pada konfigurasi atau sistem keamanannya. Namun, masalah pada kapasitas penyimpanan, autentikasi, atau percobaan *login* yang tersisa dapat mempengaruhi kinerja, mengganggu akses sah, meningkatkan risiko pelanggaran keamanan, dan memperburuk potensi serangan *brute force*, yang dapat mengakibatkan

penghapusan data dalam partisi. Oleh karena itu, pemantauan dan penanganan masalah secara cepat sangat penting untuk memastikan kelancaran dan keamanan sistem.

```
[REDACTED] lunash:>partition list

                                     Storage (bytes)
-----
Partition      Name                Objects  Total    Used    Free
-----
[REDACTED]      [REDACTED]                  4  409782   3412   406370

Command Result : 0 (Success)
[REDACTED] lunash:>partition show

Partition Name: [REDACTED]
Partition SN: [REDACTED]
Partition Label: [REDACTED]
Partition SO    PIN To Be Changed: no
Partition SO    Challenge To Be Changed: no
Partition SO    Zeroized: no
Partition SO    Login Attempts Left: 10
Crypto Officer  PIN To Be Changed: no
Crypto Officer  Challenge To Be Changed: no
Crypto Officer  Locked Out: no
Crypto Officer  Login Attempts Left: 10
Crypto Officer  is activated: yes
Crypto User     is not initialized.
Legacy Domain Has Been Set: no
Partition Storage Information (Bytes): Total=409782, Used=3412, Free=406370
Partition Object Count: 4

Command Result : 0 (Success)
```

Gambar 3.34. Informasi Status Partisi Perangkat HSM DRC

B.5 Tinjauan Status Sistem Perangkat HSM DRC

Status sistem HSM DRC dapat diperiksa dengan menggunakan *command* 'status systat show', yang menampilkan kondisi sistem secara keseluruhan. Gambar 3.35 menunjukkan bahwa HSM DRC berada dalam status *In Service Okay* (ISO), yang menunjukkan bahwa perangkat berfungsi normal dan fungsi-fungsi penting berjalan dengan baik. Selain status ISO, terdapat beberapa status lain yang dapat muncul pada sistem, seperti *In Service with Trouble* (IST) yang mengindikasikan adanya gangguan pada subsistem meskipun perangkat masih beroperasi, *Off Line* (OFL) yang berarti perangkat tidak terhubung ke jaringan dan tidak dapat memberikan layanan, serta *Out Of Service* (OOS) yang menunjukkan bahwa perangkat menyala tetapi subsistem penting tidak berfungsi. Beberapa kode juga ditampilkan, seperti kode 100 yang menunjukkan bahwa webserver tidak diaktifkan (biasanya untuk REST API), kode 63 yang menunjukkan antarmuka jaringan eth3 tidak terhubung, dan kode 95 yang menunjukkan bahwa protokol *Simple Network Management Protocol* (SNMP) tidak diaktifkan. Informasi ini berfungsi sebagai

indikator stabilitas dan konfigurasi sistem pada HSM DRC.

```
[redacted] lunash:>status sysstat show

Volatile State:
sysstat is running
Service Status: sysstat is running

Non-volatile State:
Enabled

System Status Monitor - Current Status
=====
Hostname: [redacted]
Interface eth0: [redacted]
Interface eth1: [redacted]
Interface eth2: [redacted]
Interface eth3: [redacted]
Software Version: SA:7.2.0-220
System Status: ISO
System Status Code: 100,63,55
Status Check Time: 15:15 [redacted]

System State Description
ISO (In Service Okay): The appliance is online and the necessary subsystems are operational.
IST (In Service With Trouble): The appliance is online and the necessary subsystems are operational with some troubles.
OFL (Off Line): The appliance is not currently connected to the Ethernet network and cannot provide service.
OOS (Out Of Service): The appliance is online but the necessary subsystems are NOT operational.

Command Result : 0 (Success)
```

Gambar 3.35. Informasi Status Sistem Perangkat HSM DRC

C Informasi HSM Development

Hardware Security Module (HSM) Development adalah jenis HSM yang digunakan di lingkungan *development* dan *testing*. HSM ini dirancang untuk mendukung pengujian dan pengembangan aplikasi serta sistem yang membutuhkan kriptografi tingkat tinggi. Perangkat ini menyediakan platform yang aman untuk mengembangkan dan menguji prosedur enkripsi dan dekripsi tanpa mempengaruhi sistem produksi. Dalam konteks ini, HSM Development memungkinkan simulasi skenario dunia nyata untuk memastikan bahwa sistem kriptografi berfungsi dengan baik sebelum diterapkan ke sistem yang lebih besar dan lebih kritis. Bagian ini akan menjelaskan tentang aspek dari HSM *Development* yang datanya dikumpulkan untuk keperluan *Preventive Maintenance* (PM).

C.1 Tinjauan Status Umum Perangkat HSM Development

Status umum perangkat HSM *Development* dapat diperiksa menggunakan *command* SSH 'hsm show'. Berdasarkan Gambar 3.36 perangkat ini menjalankan versi *software* 7.2.0 dan versi *firmware* 7.0.3, yang merupakan versi terbaru, sehingga memberikan tingkat keamanan yang lebih tinggi dan fitur yang lebih lengkap. Satu partisi aktif terdeteksi dari total lima partisi yang dapat dibuat, dan partisi ini telah disesuaikan dengan kebutuhan sistem. Jika jumlah partisi aktif terlalu banyak atau tidak dikelola dengan baik, hal ini dapat menyebabkan

pemborosan sumber daya. Suhu sistem tercatat masih berada dalam batas aman di bawah ambang batas peringatan, namun jika suhu melebihi batas yang ditetapkan, fitur *shutdown* akan diaktifkan untuk mencegah kerusakan yang lebih parah.

```
[REDACTED] lunash:>hsm show

Appliance Details:
=====
Software Version:          7.2.0-220

HSM Details:
=====
HSM Label:                 [REDACTED]
Serial #:                  [REDACTED]
Firmware:                  7.0.3
HSM Model:                 Luna K7
HSM Part Number:          [REDACTED]
Authentication Method:     FED keys
HSM Admin login status:    Not Logged In
HSM Admin login attempts left: 3 before HSM zeroization!
RPV Initialized:           Yes
Audit Role Initialized:    No
Remote Login Initialized:  No
Manually Zeroized:         No
Secure Transport Mode:     No
HSM Tamper State:          No tamper(s)

Partitions created on HSM:
=====
Partition: [REDACTED], Name: [REDACTED]

Number of partitions allowed: 5
Number of partitions created: 1

FIPS 140-2 Operation:
=====
The HSM is NOT in FIPS 140-2 approved operation mode.

HSM Storage Information:
=====
Maximum HSM Storage Space (Bytes): 2097152
Space In Use (Bytes): 419430
Free Space Left (Bytes): 1677722

Environmental Information on HSM:
=====
Battery Voltage: 3.093 V
Battery Warning Threshold Voltage: 2.750 V
System Temp: 44 deg. C
System Temp Warning Threshold: 75 deg. C

Command Result : 0 (Success)
```

Gambar 3.36. Informasi Status Umum Perangkat HSM *Development*

C.2 Tinjauan Status Network Perangkat HSM *Development*

Status konfigurasi *network* pada perangkat HSM *Development* dapat diperiksa melalui akses SSH menggunakan *command* 'network show'. Gambar?? menunjukkan bahwa ketiga port ethernet berada dalam keadaan aktif. Port eth0 dan eth1 beroperasi dalam status *bounding* untuk koneksi data, sedangkan eth2 digunakan untuk koneksi manajemen dan eth3 digunakan untuk koneksi langsung ke HSM *Development* selama pemeliharaan preventif. Jika port eth0 dan eth1 tidak terhubung dengan IP yang dituju, hal tersebut menunjukkan bahwa koneksi data terputus, yang dapat menyebabkan hilangnya akses ke layanan terkait dan mengurangi kinerja sistem secara keseluruhan.


```

[ ] lunash:>network show

Hostname : 
Name Server(s) : 
Search Domain(s) : <not set>

Interface settings and status

HW Address (eth0) : 
Bond master (eth0) : bond0
Link detected (eth0) : Yes

HW Address (eth1) : 
Bond master (eth1) : bond0
Link detected (eth1) : Yes

HW Address (eth2) : 
IP Address (eth2) : 
Mask (eth2) : 255.255.255.0
Gateway (eth2) : 
DNS (eth2) : 
DNS Search (eth2) : 
IP Protocol (eth2) : IPv4
Protocol (eth2) : Static
Auto Connect (eth2) : Yes
Activated (eth2) : Yes
Link detected (eth2) : Yes

HW Address (eth3) : 
IP Address (eth3) : 
Mask (eth3) : 255.255.255.0
Gateway (eth3) : 0.0.0.0
DNS (eth3) : 
DNS Search (eth3) : 
IP Protocol (eth3) : IPv4
Protocol (eth3) : Static
Auto Connect (eth3) : Yes
Activated (eth3) : No
Link detected (eth3) : No

HW Address (bond0) : 
IP Address (bond0) : 255.255.255.0
Mask (bond0) : 
Gateway (bond0) : 
DNS (bond0) : 
DNS Search (bond0) : 
IP Protocol (bond0) : IPv4
Protocol (bond0) : Static
Auto Connect (bond0) : Yes
Activated (bond0) : Yes
Link detected (bond0) : Yes
Active Slaves (bond0) : eth1 eth0
Status (bond1) : Not configured

Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 0.0.0.0 0.0.0.0 UG 100 0 0 eth2
0.0.0.0 0.0.0.0 0.0.0.0 UG 300 0 0 bond0
0.0.0.0 0.0.0.0 255.255.255.0 U 300 0 0 bond0
0.0.0.0 0.0.0.0 255.255.255.0 U 100 0 0 eth2

Command Result : 0 (Success)

```

Gambar 3.37. Informasi Status Network Perangkat HSM Development

C.3 Tinjauan Status Aksesoris Perangkat HSM Development

Status sensor untuk *fan*, CPU, dan memori pada HSM Development dapat dipantau melalui akses SSH menggunakan *command* 'status sensors'. Gambar 3.38 menunjukkan bahwa kecepatan *fan*, suhu CPU dan memori, serta tegangan pada beberapa titik berada dalam kondisi normal. Hal ini menandakan bahwa tidak ada indikasi kebutuhan untuk penggantian atau tindakan lebih lanjut. Namun, jika nilai-nilai tersebut melebihi batas normal, masalah serius seperti *overheat*, kerusakan perangkat keras, atau kegagalan sistem akibat suhu yang berlebihan atau tegangan yang tidak stabil dapat terjadi.

```
[root@hsm ~]# lunash:status sensors

This command displays the fan speed, temperature and voltage of the motherboard and power supply units.

Sensor      | Reading | Unit | Status | Thresholds
-----
Fan1A       | 3900.000 | RPM | OK | 1000.000 | 2000.000 | na | na
Fan1B       | 3900.000 | RPM | OK | 1000.000 | 2000.000 | na | na
Fan2A       | 4000.000 | RPM | OK | 1000.000 | 2000.000 | na | na
Fan2B       | 4200.000 | RPM | OK | 1000.000 | 2000.000 | na | na
Fan3A       | 4000.000 | RPM | OK | 1000.000 | 2000.000 | na | na
Fan3B       | 5200.000 | RPM | OK | 1000.000 | 2000.000 | na | na
CPU         | 40.000 | degrees C | OK | na | na | 95.000 | 100.000
VRD         | 36.000 | degrees C | OK | na | na | 105.000 | 110.000
PCH         | 37.000 | degrees C | OK | na | na | 99.000 | 104.000
Inlet       | 31.000 | degrees C | OK | na | na | 87.000 | 97.000
CHB DIMM 1  | 33.000 | degrees C | OK | na | na | 87.000 | 97.000
CHB DIMM 0  | na | degrees C | na | na | na | 87.000 | 97.000
CDA DIMM 1  | na | degrees C | na | na | na | 87.000 | 97.000
CDA DIMM 0  | na | degrees C | na | na | na | 87.000 | 97.000
FAN1 Thx   | 33.000 | degrees C | OK | na | na | na | na
+12V        | 12.120 | Volts | OK | na | na | 11.160 | 12.900
+5V         | 5.010 | Volts | OK | na | na | 4.450 | 5.370
VDDMain     | 3.360 | Volts | OK | na | na | 3.060 | 3.540
SVSB        | 5.010 | Volts | OK | na | na | 4.450 | 5.370
SVSB        | 3.340 | Volts | OK | na | na | 3.060 | 3.540
VPU VCORE   | 0.770 | Volts | OK | na | na | na | na
VCCSA       | 1.050 | Volts | OK | na | na | 0.980 | 1.130
VCCIO       | 0.940 | Volts | OK | na | na | 0.880 | 1.020
V12         | 1.130 | Volts | OK | na | na | 1.130 | 1.250
V15_VFB     | 2.520 | Volts | OK | na | na | 2.320 | 2.680
V10_PCH     | 0.990 | Volts | OK | na | na | 0.930 | 1.050
V15_BMC     | 1.540 | Volts | OK | na | na | 1.470 | 1.930
V12_BMC     | 1.260 | Volts | OK | na | na | 1.170 | 1.350
V15_AIN     | 1.760 | Volts | OK | na | na | 1.470 | 1.930
VBAT        | 3.260 | Volts | OK | 2.100 | 2.500 | na | na
PSU1_12V_value | 11.820 | Volts | OK | na | na | 10.800 | 13.200
PSU1_Temp_value | 41.000 | degrees C | OK | na | na | 50.000 | na
PSU1_FAN_value | 7000.000 | RPM | OK | 1000.000 | 1300.000 | na | na
PSU2_12V_value | 11.820 | Volts | OK | na | na | 10.800 | 13.200
PSU2_Temp_value | 41.000 | degrees C | OK | na | na | 50.000 | na
PSU2_FAN_value | 7000.000 | RPM | OK | 1000.000 | 1300.000 | na | na
PSU1_Status | OK | discrete | 0x0101 | na | na | na | na
PSU2_Status | OK | discrete | 0x0101 | na | na | na | na
CPU_Thermtrip | OK | discrete | 0x0000 | na | na | na | na
Watchdog     | OK | discrete | 0x0000 | na | na | na | na

Notes:
UR: Not Reading (Error)
CR: Critical
0.00 RPM means fan unplugged, failed, or sensors not readable
DIMM: Dual In-Line Memory Module
PSU1: Power Supply Unit 1
PSU2: Power Supply Unit 2
Fan1, Fan2 and Fan3 are pluggable modules on the front of the appliance.
Each fan unit contains two fans: A and B.

----- Power Supplies Status -----
PSU1_Status | Presence detected
PSU2_Status | Presence detected
CPU_Thermtrip | OK
Watchdog | OK

----- Front Cooling Fans Status -----
Fan1A | OK | 3900 RPM
Fan1B | OK | 3900 RPM
Fan2A | OK | 4000 RPM
Fan2B | OK | 4200 RPM
Fan3A | OK | 4000 RPM
Fan3B | OK | 5200 RPM
PSU1_FAN_value | OK | 7000 RPM
PSU2_FAN_value | OK | 7000 RPM

----- Chassis Status -----
System Power | OK
Power Overload | false
Power Interlock | inactive
Main Power Fault | false
Power Control Fault | false
Power Restore Policy | previous
Last Power Event | no-failed
Chassis Intrusion | inactive
Front-Panel Lockout | inactive
Drive Fault | false
Cooling/Fan Fault | false
Sleep Button Disabled | not allowed
Diag Button Disabled | not allowed
Reset Button Disabled | allowed
Power Button Disabled | allowed
Sleep Button Disabled | false
Diag Button Disabled | false
Reset Button Disabled | false
Power Button Disabled | false

Command Result : 0 (Success)
```

Gambar 3.38. Informasi Status Aksesoris Perangkat HSM Development

C.4 Tinjauan Status Partisi Perangkat HSM Development

Status partisi pada HSM DRC dapat diperiksa melalui koneksi SSH dengan *command* 'partition list' untuk menampilkan daftar partisi dan 'partition show' untuk melihat rincian setiap partisi. Gambar 3.39 menyajikan informasi mengenai kapasitas penyimpanan, status autentikasi, dan indikator keamanan seperti jumlah percobaan *login* yang tersisa. Informasi yang ditampilkan menunjukkan bahwa partisi dalam kondisi normal tanpa masalah pada konfigurasi atau sistem keamanannya. Namun, masalah pada kapasitas penyimpanan, autentikasi, atau percobaan *login* yang tersisa dapat mempengaruhi kinerja, mengganggu akses sah, meningkatkan risiko pelanggaran keamanan, dan memperburuk potensi serangan *brute force*, yang berpotensi mengakibatkan penghapusan data pada partisi. Oleh karena itu, pemantauan dan penanganan masalah secara cepat sangat diperlukan

untuk memastikan kelancaran dan keamanan sistem.

```
[ ] lunash:>partition list

                                Storage (bytes)
-----
Partition      Name              Objects  Total    Used    Free
-----
[ ]             [ ]                4    409782    3408    406374

Command Result : 0 (Success)
[ ] lunash:>partition show

Partition Name: [ ]
Partition SN: [ ]
Partition Label: [ ]
Partition SO    PIN To Be Changed: no
Partition SO    Challenge To Be Changed: no
Partition SO    Zeroized: no
Partition SO    Login Attempts Left: 10
Crypto Officer  PIN To Be Changed: no
Crypto Officer  Challenge To Be Changed: no
Crypto Officer  Locked Out: no
Crypto Officer  Login Attempts Left: 10
Crypto Officer  is activated: yes
Crypto User      is not initialized.
Legacy Domain Has Been Set: no
Partition Storage Information (Bytes): Total=409782, Used=3408, Free=406374
Partition Object Count: 4

Command Result : 0 (Success)
```

Gambar 3.39. Informasi Status Partisi Perangkat HSM *Development*

C.5 Tinjauan Status Sistem Perangkat HSM *Development*

Status partisi pada HSM *Development* dapat diperiksa melalui koneksi SSH dengan *command* 'status systat show', yang menampilkan kondisi keseluruhan sistem. Gambar 3.40 menunjukkan bahwa HSM *Development* berada dalam status *In Service Okay* (ISO), yang menandakan bahwa perangkat berfungsi dengan normal dan semua fungsi penting berjalan dengan baik. Selain status ISO, beberapa status lain yang mungkin muncul pada sistem meliputi *In Service with Trouble* (IST), yang menunjukkan adanya gangguan pada subsistem meskipun perangkat masih beroperasi, *Off Line* (OFL), yang menunjukkan bahwa perangkat tidak terhubung ke jaringan dan tidak dapat memberikan layanan, serta *Out Of Service* (OOS), yang berarti perangkat menyala tetapi subsistem penting tidak berfungsi. Beberapa kode juga ditampilkan, seperti kode 100 yang menunjukkan bahwa webserver tidak diaktifkan (biasanya untuk REST API), kode 63 yang menunjukkan bahwa antarmuka jaringan eth3 tidak terhubung, dan kode 95 yang menunjukkan bahwa protokol *Simple Network Management Protocol* (SNMP) tidak diaktifkan. Informasi ini berfungsi sebagai indikator untuk memantau stabilitas dan konfigurasi sistem pada HSM *Development*.

```
[redacted] lunash:>status sysstat show

Volatile State:
sysstat is running
Service Status: sysstat is running

Non-volatile State:
Enabled

System Status Monitor - Current Status
=====
Hostname: [redacted]
Interface eth0: [redacted]
Interface eth1: [redacted]
Interface eth2: [redacted]
Interface eth3: not configured
Software Version: SA:7.2.0-220
System Status: ISO
System Status Code: 100,63,55
Status Check Time: 15:11 [redacted]

System State Description

ISO (In Service Okay): The appliance is online and the necessary subsystems are operational.
IST (In Service With Trouble): The appliance is online and the necessary subsystems are operational with some troubles.
OFL (Off Line): The appliance is not currently connected to the Ethernet network and cannot provide service.
OOS (Out Of Service): The appliance is online but the necessary subsystems are NOT operational.

Command Result : 0 (Success)
```

Gambar 3.40. Informasi Status Sistem Perangkat HSM *Development*

3.4 Kendala dan Solusi yang Ditemukan

3.4.1 Kendala

Kendala yang ditemukan dalam praktik kerja magang adalah sebagai berikut.

1. Kendala dalam menguasai alat dan teknologi terbaru di bidang *data security* yang memerlukan waktu untuk memahami konsep serta memperoleh pengalaman praktis secara langsung.
2. Hambatan dalam berkomunikasi dengan rekan kerja akibat perasaan canggung dan proses adaptasi terhadap dinamika lingkungan profesional yang sesungguhnya.

3.4.2 Solusi

Solusi yang ditemukan untuk menangani kendala-kendala yang ditemukan adalah sebagai berikut.

1. Pemahaman terhadap teknologi *data security* terbaru telah ditingkatkan melalui pelatihan internal, pembelajaran dari berbagai sumber secara mandiri, serta praktik langsung agar lebih mudah diterapkan secara aplikatif.
2. Mengembangkan keberanian untuk berkomunikasi dengan rekan kerja dan dilibatkan dalam diskusi yang berkaitan dengan tugas atau pekerjaan. .