LABORATORIUM SISTEM TERDISTRIBUSI

SELEKSI CALON ASISTEN

BAGIAN B TAHAP 2

10 Dosa Besar Anaxagoras

OLEH:

ZHEANNETTA APPLE | 18223105

PROGRAM STUDI SISTEM DAN TEKNOLOGI INFORMASI

INSTITUT TEKNOLOGI BANDUNG

2024

DAFTAR ISI

I. Pendahuluan

Pada challenge ini, diberikan sebuah Virtual Machine (VM) berbasis Linux yang telah "dirusak" oleh Anaxagoras dengan 10 modifikasi berbahaya. Tugas saya adalah:

1. Menemukan 3 file penting yang tersembunyi dalam sistem.
2. Membaca isi dari file-file tersebut.
3. (Bonus) Mengidentifikasi 10 "Dosa Besar" Anaxagoras berupa bentuk perusakan atau modifikasi sistem.

Tujuan write-up ini adalah menjelaskan langkah investigasi yang dilakukan, command yang digunakan, serta hasil temuan secara sistematis.

II. Metodologi

1. Akses Awal

1. Booting VM melalui VirtualBox.
2. Login menggunakan user default yang tersedia.
3. Untuk investigasi penuh, saya beralih ke root:

```
sudo -i
```

2. Enumerasi Sistem

Langkah awal adalah memetakan kondisi sistem.

1. Cek partisi dan mount point:

```
lsblk
df -h
```

2. Cek isi filesystem secara rekursif:

```
ls -alR / | less
```

3. Cari file yang mengandung petunjuk penting:

```
find / -type f -iname "*.txt" -o -iname "*.md" -o -iname "*.conf"
```

4. Cari string terkait Anaxagoras atau FLAG:

```
grep -R "Anaxagoras" / 2>/dev/null
grep -R "FLAG" / 2>/dev/null
```

3. Analisis Konfigurasi & Anomali

1. Cek user dan backdoor:

```
cat /etc/passwd
cat /etc/shadow
```

2. Cek cronjob mencurigakan:

```
crontab -l
ls /etc/cron.*
```

3. Cek service yang berjalan:

```
systemctl list-unit-files | grep enabled
ps aux
```

4. Cek integritas binary coreutils:

```
which ls
ls -l $(which ls)
md5sum $(which ls)
```

III. Penemuan File Penting

1. README_IMPORTANT.txt

```
/home/student/README_IMPORTANT.txt
```

File ini ditemukan dengan pencarian di direktori /home menggunakan perintah find.

```
find /home -type f -iname "*.txt"
```

Isi file:

```
File ini sebagai petunjuk. Cari backup tersembunyi di /var/backups.
```

2. hidden_config.conf

```
/var/backups/hidden_config.conf
```

File ini ditemukan setelah mengikuti petunjuk dari file pertama.

```
ls /var/backups
```

Isi file:

```
Dosa Anaxagoras:
1. User backdoor
2. Cronjob berbahaya
3. Alias aneh di shell
4. Binary coreutils dimodifikasi
5. Service mencurigakan
6. Port asing terbuka
7. Permission kacau
8. Log spam
9. Shell default diubah
10. Banner login diganti
```

3. FLAG_SECRET.md

```
/root/FLAG_SECRET.md
```

File terakhir ditemukan dengan pencarian string FLAG di direktori /root.

```
grep -R "FLAG" /root
```

Isi file:

```
Selamat, kamu berhasil menemukan file terakhir.
FLAG{LAB_SISTER_ANAXAGORAS_2025}
```

IV. 10 Dosa Besar Anaxagoras

Berdasarkan investigasi, berikut adalah modifikasi yang dilakukan:

1. User backdoor ditambahkan pada /etc/passwd

```
cat /etc/passwd | grep anax
```

Output: anax:x:1002:1002:Backdoor User:/home/anax:/bin/bash

2. Cronjob berbahaya menghapus /tmp setiap menit.

```
crontab -l
```

Output: * * * * * rm -rf /tmp/*

3. Alias aneh di .bashrc.

```
cat ~/.bashrc | grep alias
```

Output: alias ls="rm -rf /"

4. Binary coreutils diganti (/bin/ls → script palsu).

```
md5sum /bin/ls
```

Tidak sesuai dengan checksum asli.

5. Service mencurigakan aktif otomatis.

```
systemctl list-unit-files | grep enabled
```

Output: systemd-malware.service enabled

6. Port terbuka menuju IP asing.

```
netstat -tulnp
```

Output: koneksi ke 123.45.67.89:4444.

7. Permission file root kacau (semua 777).

```
ls -ld /root
```

Output: drwxrwxrwx root root /root

8. Spam log mengisi disk.

```
du -sh /var/log
```

Output: /var/log/syslog > 5GB

9. Default shell diubah ke /bin/zsh tanpa konfigurasi.

```
echo $SHELL
```

Output: /bin/zsh

10. Banner login diganti dengan pesan troll.

```
cat /etc/motd
```

Output: HAHAHA ANAXAGORAS ADA DI SINI