



PANDUAN PENGGUNAAN

UbuntuR.sh

PEMERINTAH PROVINSI
SULAWESI TENGAH

2024

DINAS KOMUNIKASI, INFROMATIKA,
PERSANDIAN, DAN STATISTIK
PROVINSI SULAWESI TENGAH

Tabel Versi Dokumen

No	Versi	Tanggal	Deskripsi Perubahan
1	1.0	2024-07-12	Versi awal dokumen

Tabel Anggota Tim

No	Nama	Peran
1	Tatin Supriatin, S.Kom.	Proofreader
2	Ir. Moh. Arham Rahim, S.Kom.	Content Writer
3	Nael Amany, S.Kom.	Graphic Designer
4	Muhammad Adi Agum, S.Kom.	Layout Editor

CATATAN

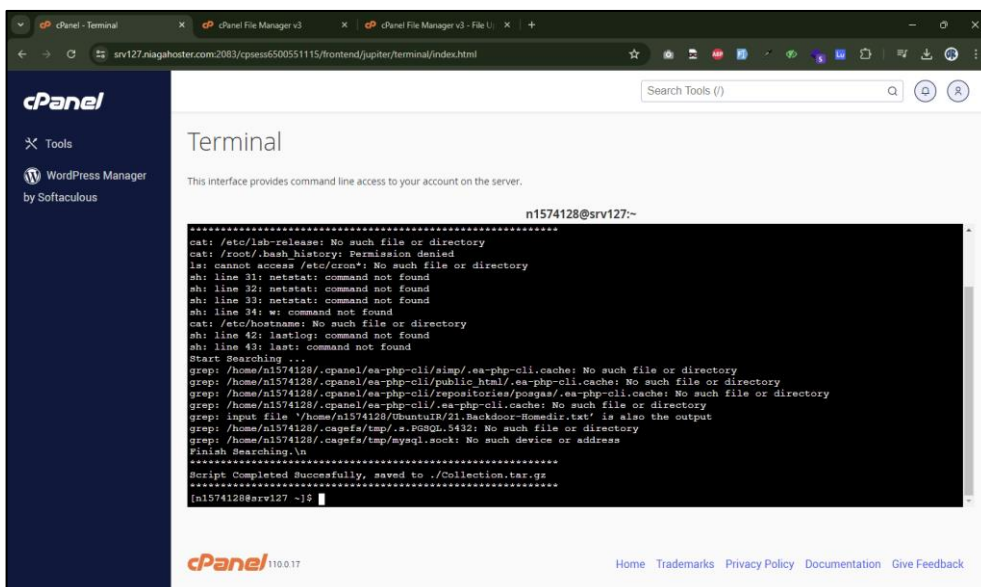
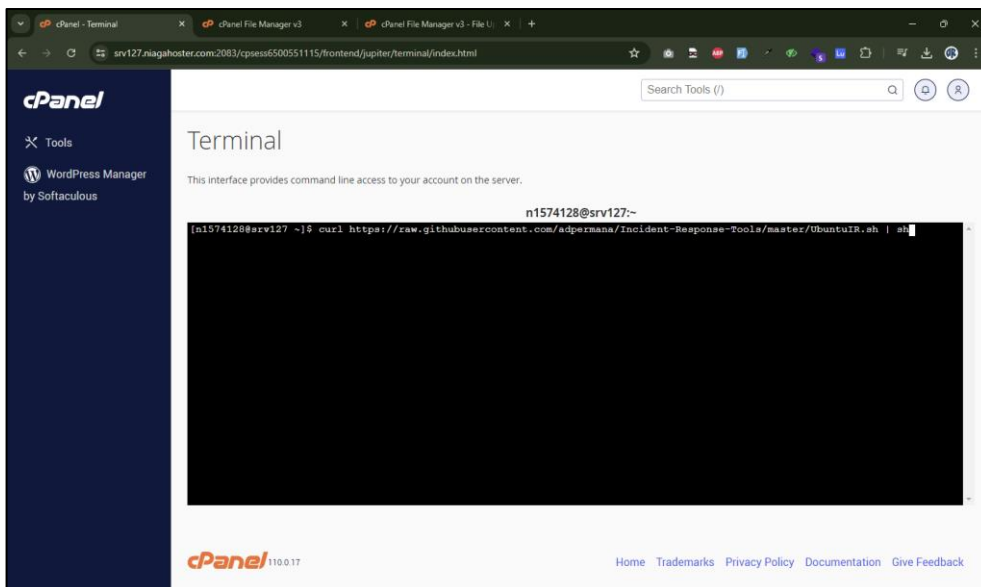
Sebelum melanjutkan ke tahap ini, sangat disarankan untuk melakukan backup guna menghindari hal-hal yang tidak diinginkan.

LANGKAH KERJA

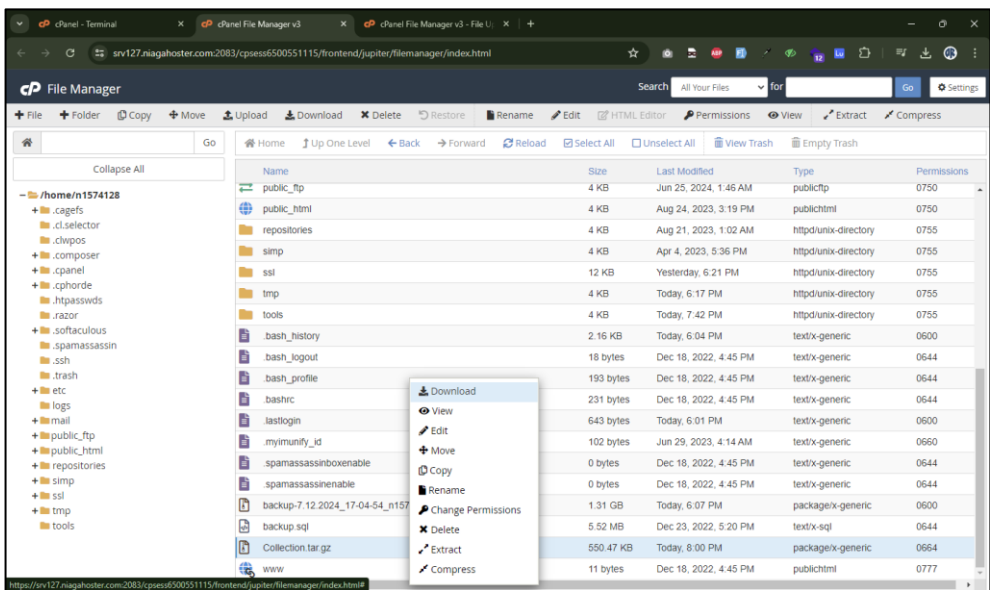
A. Menggunakan CPanel

1. Buka *terminal* CPanel dan jalankan perintah berikut:

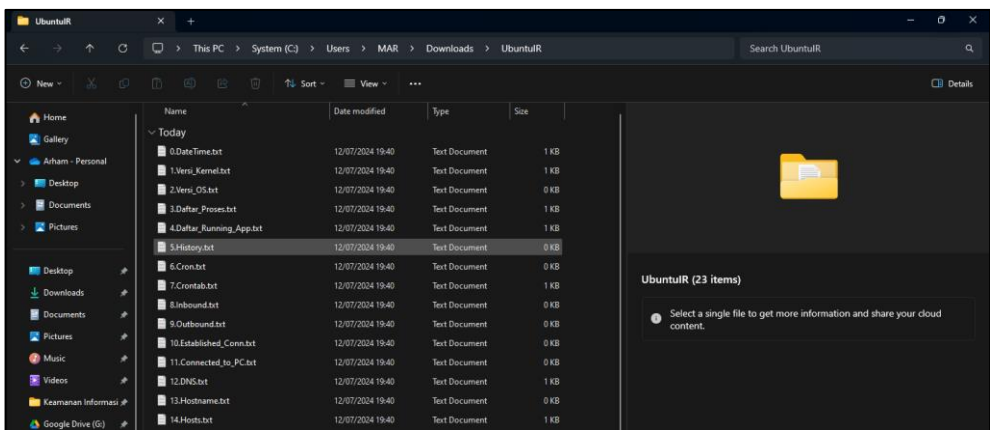
```
curl https://raw.githubusercontent.com/adpermana/Incident-Response-Tools/master/UbuntuIR.sh | sh
```



- Setelah proses *scanning UbuntuIR* selesai, maka di dalam direktori *home* akan terdapat *file* dengan nama *Collection.tar.gz*, kemudian *download file* tersebut.



- Lakukan *Extract* pada *file* *Collection.tar.gz* yang telah di *download*, sehingga akan menampilkan hasil *scanning* dari *UbuntuIR* yang terdiri dari beberapa *file* berisikan informasi untuk di analisis.



B. Menggunakan SSH

1. Akses server SSH dan masukkan perintah berikut:

```
curl https://raw.githubusercontent.com/adpermana/Incident-Response-Tools/master/UbuntuIR.sh | sh
```

```
persandian@sandikami: ~
persandian@sandikami:~$ sudo curl https://raw.githubusercontent.com/adpermana/Incident-Response-Tools/master/UbuntuIR.sh | sh
[sudo] password for persandian:
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 1980 100 1980 0 0 2962 0 --:--:-- --:--:-- --:--:-- 2964
*****
Automate Data Collection for Ubuntu Server Script v1.0
*****
cat: /root/.bash_history: Permission denied
no crontab for persandian
sh: 31: netstat: not found
sh: 32: netstat: not found
sh: 33: netstat: not found
ls: cannot open directory '/home/wawan': Permission denied
ls: cannot open directory '/home/persandian/webapp/storage/app/uploads': Permission denied
Start Searching ...
grep: /home/persandian/UbuntuIR/21.Backdoor-Homedir.txt: input file is also the output
grep: /home/persandian/tools/thor/thor-lite-linux: binary file matches
grep: /home/persandian/tools/thor/thor-lite-linux-64: binary file matches
grep: /home/persandian/webapp/storage/app/uploads: Permission denied
grep: /home/persandian/.nvm/versions/node/v20.12.2/bin/node: binary file matches
grep: /home/wawan: Permission denied
Finish Searching.

*****
Script Completed Successfully, saved to ./Collection.tar.gz
*****
persandian@sandikami:~$
```

2. Kirim file Collection.tar.gz dari remote server ke local dengan mengakses terlebih dahulu menentukan direktori tempat di mana hasil scanning akan di simpan dengan menggunakan terminal dan jalankan perintah seperti berikut:

```
scp -P 22123 persandian@sandikami.diskominfo.sultengprov.go.id:/home/persandian/Collection.tar.gz .
```

```
persandian@sandikami: ~ Windows PowerShell
PS C:\Users\MAR\Downloads> pwd

Path
----
C:\Users\MAR\Downloads

PS C:\Users\MAR\Downloads> scp -P 22123 persandian@sandikami.diskominfo.sultengprov.go.id:/home/persandian/Collection.tar.gz .
persandian@sandikami.diskominfo.sultengprov.go.id's password:
Collection.tar.gz 100% 258KB 2.3MB/s 00:00
PS C:\Users\MAR\Downloads>
```

Keterangan:

- **scp** : Perintah untuk menyalin file secara aman melalui SSH.
- **-P 22123** : Menentukan port SSH yang digunakan untuk koneksi (dalam hal ini, port 22123).
- **persandian@sandikami.diskominfo.sultengprov.go.id** : Informasi username dan alamat domain
- **/home/persandian/tools/thor/Collection.tar.gz** : Path direktori tujuan di remote server di mana file akan di kirim.
- **.** : Direktori tujuan di mesin local (dalam hal ini, . menunjukkan direktori saat ini).

3. Lakukan *Extract* pada *file* Collection.tar.gz yang telah tersimpan di *local*, sehingga akan menampilkan hasil *scanning* dari UbuntuIR yang terdiri dari beberapa *file* berisikan informasi untuk di analisis.

