**DOKUMEN TERBATAS** 



# PANDUAN PENGGUNAAN UbuntulR.sh

## PEMERINTAH PROVINSI SULAWESI TENGAH



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

> Jl. R.A Kartini, Kel. Lolu Selatan Kec. Palu Timur, Kota Palu Sulawesi Tengah, 94235

#### 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/UbuntulR.sh   sh

<ul> <li>cPanel - Terminal</li> </ul>	X dP cPanel File Manager v3 X dP cPanel File Manager v3 - File U X +		- 0 ×				
← → C 🛤 srv127.niagat	noster.com:2083/cpsess6500551115/frontend/jupiter/terminal/index.html	📩 🗴 🖻 🖻 🖉 🛷 🤹 🖬	요 🛛 🛪 😨 🗄				
cPanel		Search Tools (/)	Q (4) (8)				
X Tools	Terminal						
WordPress Manager	This interface provides command line access to your account on the server.						
by contactions	n1574128@sru127_sl\$_curl_https://ram_oithubusercontext_com/adorses	rv127:~	Dah Lab				
	- <b>Pape/</b>		-				
		Home Trademarks Privacy Policy Documen	tation Give Feedback				
✓ cPanel - Terminal	X CP cPanel File Manager v3 X CP cPanel File Manager v3 - File U X +		- 0 X				
← → C 🛤 srv127.niagat	noster.com:2083/cpsess6500551115/frontend/jupiter/terminal/index.html	📩 🗴 🖻 🖉 🖉 🖉 👘 🤹	요 🗠 조 🕲 :				
cPanel		Search Tools (/)					
X Tools	Terminal						
WordPress Manager	This interface provides command line access to your account on the server.						
ay condicators	n1574128@srv127:~						
	<pre>cat:/stc/lab-rslsss:No such file or directory is: incomposed /stc/rom*: No such file or directory is: incomposed /stc/rom*: No such file or directory sh: line 31: nettat: command not found sh: line 32: nettat: command not found sh: line 31: is: is: nettat: command not found sh: line 31: is: is: nettat: command not found sh: line 31: is: is: is: command not found sh: line 31: is: is: is: command not found sh: line 31: is: is: is: command not found sh: line 31: is: is: command not found sh: is: is: is: is: command not found sh: is: is: is: is: is: is: is: is: is: is</pre>						
	cPane/ 1100.17	Home Trademarks Privacy Policy Documen	tation Give Feedback				

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

🕐 🕫 Ølanel - Terminal X 🕼 Ølanel File Manager v3 X 🛷 Ølanel File Manager v3 - File Uj X +								
i c $ ightarrow$ C 🛱 srv127.niagahoster.com:2083/cpsess6500551115/trontend/upiter/lifemanager/index.html 🗴 💩 🖻 🖉 / Ø 🏫 🖩 🖸								
P File Manager		Search All Your Files 🗸 for	Go Ø Settings					
+ File + Folder <sup>(1)</sup> Copy	Lupload 🛓 Download 🗙 Delete 🗂 Restore 📑 Rename 🖋 Edit 🖉	HTML Editor Permissions OView CExtract	Compress					
<b>☆</b> Go	Home J Up One Level ← Back → Forward 2 Reload Select A	All 🔲 Unselect All 🖀 View Trash 🖀 Empty Trash						
Collapse All Collapse All Collapse All Collapse All Collapse Colla	Name         Size           public_flop         4 KB           public_flop         4 KB           public_flop         4 KB           repositories         4 KB           simp         4 KB           sist         12 KB           tools         4 KB           tools         18 bc           tosh_logout         18 bc           tosh_logout         19 bc           toshtrc         20 view	Last Modified         Type           a         Jun 25, 2024, 1.46 AM         publichtp           a         Aug 24, 2023, 3.19 PM         publichtmil           a         Aug 24, 2023, 3.19 PM         httpd/ums-directory           a         Apr 4, 2023, 5.85 PM         httpd/ums-directory           b         Apr 4, 2023, 5.85 PM         httpd/ums-directory           d         Today, 6.17 PM         httpd/ums-directory           a         Today, 7.42 PM         httpd/ums-directory           kB         Today, 6.34 PM         text/s-generic           yles         Dec 18, 2022, 4.45 PM         text/s-generic           byles         Dec 18, 2022, 4.45 PM         text/s-generic           byles         Dec 18, 2022, 4.45 PM         text/s-generic           byles         Dec 18, 2022, 4.45 PM         text/s-generic	Permissions 0750 0755 0755 0755 0755 0755 0755 075					
#mnail     #movie.c.ftp     #moviel.c.ftp     #moviel.c.ftm     #moviel.c.ftm     #movie.c.ftp     #movie.c.ftp     #movie.c.ftp     #movie.c.ftp     #movie.c.ftp     #movie.c.ftp     #movie.c.ftp     #movie.c.ftp     #movie.c.ftp	iastlogin         • View         643           impiruully_id         • Edit         102           ispamassassinboxenable         © Copy         0 byt           ispamassassinenable         © Copy         0 byt           ispamassassinenable         © Copy         0 byt           ispamassassinenable         ispamassassinenable         0 byt           ispamassassinenable         ispamassinenable         0 byt           ispamassinenable         ispamassinenable         0 byt           ispamassispatie	bytes         Today, 6.01 PM         text/s-generic           bytes         Jun 29, 2023, 4.14 AM         text/s-generic           tes         Dec 18, 2022, 4.45 PM         text/s-generic           tes         Dec 18, 2022, 4.45 PM         text/s-generic           cli@         Today, 6.07 PM         package/s-generic           text         Dec 23, 2022, 5.20 PM         text/s-aql           47 KB         Today, 8.00 PM         package/s-generic           ytes         Dec 18, 2022, 4.45 PM         public/tml	0600 0660 0644 0644 0600 0644 0664 0664					

3. 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.

UbuntulR						- 0 ×
	C	stem (C:) > Users > MAR :	Downloads	UbuntulR	Search UbuntulR	
⊙ New *		↑↓ Sort ~ 🔲 View ~				Details
<ul> <li>☆ Home</li> <li>◯ Gallery</li> <li>◯ Arham - Personal</li> <li>◯ Desktop</li> <li>◯ Desktop</li> </ul>	Name V Today 0.DateTime.txt 1.Versi_Kernel.txt 2.Versi_OS.txt	Date modified 12/07/2024 19:40 12/07/2024 19:40 12/07/2024 19:40	Type Text Document Text Document Text Document	Size 1 KB 1 KB 0 KB		
Pictures	<ul> <li>3.Daftar_Proses.txt</li> <li>4.Daftar_Running_App.txt</li> <li>5.History.txt</li> </ul>	12/07/2024 19:40 12/07/2024 19:40 12/07/2024 19:40	Text Document Text Document Text Document	1 KB 1 KB 0 KB		
Esktop Downloads	6.Cron.bt     7.Crontab.bt     8.Inbound.txt	12/07/2024 19:40 12/07/2024 19:40 12/07/2024 19:40	Text Document Text Document Text Document	0 KB 1 KB 0 KB	UbuntulR (23 items) Select a single file to get more information and share informatio	your cloud
💽 Pictures 🕐 Music 🧱 Videos	9:Uutbound.txt     10.Established_Conn.txt     11.Connected_to_PC.txt     12.DNS.txt	12/07/2024 19:40 12/07/2024 19:40 12/07/2024 19:40 12/07/2024 19:40	Text Document Text Document Text Document Text Document	окв окв окв 1 кв	° content.	
🚞 Keamanan Informasi	i 🖈 📄 13.Hostname.txt 🖈 📑 14.Hosts.txt	12/07/2024 19:40 12/07/2024 19:40	Text Document Text Document	0 KB 1 KB		

#### B. Menggunakan SSH

1. Akses server SSH dan masukkan perintah berikut:

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

· · · · · · · · · · · · · · · · · · ·					
▶ persandian@sandikami: ~         ×         +         ~         -         □         ×					
<pre>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 ************************************</pre>					
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/tools/thor/thor-lite-linux: binary file matches grep: /home/persandian/tools/thor/thor-lite-linux-64: binary file matches grep: /home/persandian/vebapp/storage/app/uploads: Permission denied grep: /home/persandian/.nvm/versions/node/v20.12.2/bin/node: binary file matches grep: /home/mersandian/.nvm/versions/node/v20.12.2/bin/node: binary file matches grep: /home/maximission denied Finish Searching.					
**************************************					

 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 .



#### 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.

🚞 UbuntulR		× +				- 0	×
			Users > MAR >	Downloads >	UbuntulR	Search UbuntulR	
⊕ New ~ 🐰		ि @ @ ① ↑↓ Sort ~	≡ View ×   ····			CB Der	tails
合 Home		Name	Date modified	Туре			
🔀 Gallery		∼ Today					
👻 🧰 Arham - Personal		0.DateTime.txt	12/07/2024 19:40	Text Document			
Dealters		1.Versi_Kernel.txt	12/07/2024 19:40	Text Document			
		2.Versi_OS.txt	12/07/2024 19:40	Text Document			
> 🔤 Documents		3.Daftar_Proses.txt	12/07/2024 19:40	Text Document			
> 🔀 Pictures		4.Daftar_Running_App.txt	12/07/2024 19:40	Text Document	1 KB		
		S.History.txt	12/07/2024 19:40	Text Document	0 KB		
🥅 Desktop	*	6.Cron.txt	12/07/2024 19:40	Text Document		UburtulD (33 Hama)	
	*	7.Crontab.txt	12/07/2024 19:40	Text Document		Obuntuik (23 items)	
- Documents	•	8.Inbound.txt	12/07/2024 19:40	Text Document		<ul> <li>Select a single file to get more information and share your cloud</li> </ul>	
Distance.		9.Outbound.txt	12/07/2024 19:40	Text Document		content.	
Pictures	1	10.Established_Conn.txt	12/07/2024 19:40	Text Document			
Music	1	11.Connected_to_PC.txt	12/07/2024 19:40	Text Document			
🗾 Videos	*	12.DNS.txt	12/07/2024 19:40	Text Document			
🚞 Keamanan Informa:	si 🖈	13.Hostname.txt	12/07/2024 19:40	Text Document			
📥 Google Drive (G:)	*	14.Hosts.txt	12/07/2024 19:40	Text Document			
PDF	*	15.Daftar_User.txt	12/07/2024 19:40	Text Document			
Screenshots	<b>ا</b> ہ	16.Daftar_User_Bash.txt	12/07/2024 19:40	Text Document			
		17.Lastlog.txt	12/07/2024 19:40	Text Document			
PEROOD	×	18.Last.txt	12/07/2024 19:40	Text Document			
Sertifikat	*	19.Homedir.txt	12/07/2024 19:40	Text Document			
		20.VarWWWdir.txt	12/07/2024 19:40	Text Document			
👻 💻 This PC		21.Backdoor-Homedir.txt	12/07/2024 19:42	Text Document			
23 items		22.Backdoor-VarWWWdir.txt	12/07/2024 19:42	Text Document			