DOKUMEN TERBATAS



PANDUAN PENGGUNAAN THOR LITE

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

- Register Thor Lite di <u>https://www.nextron-systems.com/thor-lite/</u> dan akses *link* yang dikirimkan pada *email* untuk *download* aplikasi dan lisensi. *Download* versi Linux apabila menggunakan *server* Ubuntu.
- 2. Login CPanel dan buka file manager.
- 3. Buat folder baru sebagai tempat penyimpanan thor lite, misalnya "tools".

	nel File Manager v3 🛛 🗶 🌮 cPanel File Manager v3 - File U; 🗙 🕇 +			
← → ♂ III srv127.niagahoster.com:208	3/cpsess6500551115/frontend/jupiter/filemanager/index.html	* 🗅 🖻 🕘 🗾 /	🖉 👷 📴 🖸	
P File Manager	Sea	rch 🛛 All Your Files 🗸 🗸 for	Go	Settings
+ File + Folder 🔘 Copy + Move 🔮	Upload 🛓 Download 🗱 Delete 🏷 Restore 📄 Rename 🥒 Edit 😰 HTML Edi	tor 🎾 Permissions 🐵 Vie		
脅 Go	☆ Home J Up One Level ← Back → Forward Ø Reload Ø Select All □ Un	nselect All 💼 View Trash	🗑 Empty Trash	
Collapse All	Name Size	Last Modified	Туре	Permissions
- 늘 /home/n1574128	cagefs 4 KB	Dec 18, 2022, 4:48 PM	httpd/unix-directory	0771
+ 🖿 .cagefs	Lcl.selector 4 KB	Dec 12, 2023, 3:46 PM	httpd/unix-directory	0755
.cl.selector	Lchwpos 4 KB	Dec 18, 2022, 10:22 PM	httpd/unix-directory	0700
+ in .composer	composer X New Folder	c 18, 2022, 7:15 PM	httpd/unix-directory	0775
+ 🔤 .cpanel	in cpanel	day, 6:14 PM	httpd/unix-directory	0700
+ .cpnorde	New Folder Name:	c 18, 2022, 4:45 PM	httpd/unix-directory	0700
🖿 .razor	toois	c 18, 2022, 4:45 PM	httpd/unix-directory	
+ softaculous	New Folder will be created in:	c 29, 2023, 3:54 AM	httpd/unix-directory	0755
ssh	soffaculous A	c 18, 2022, 4:47 PM	httpd/unix-directory	0711
🖿 .trash	soamassassin	c 18 2022 4:45 PM	httpd/unix-directory	0700
+ etc	Create New Folder Cano	el c 19, 2022, 12:00 PM	httpd/unix-directory	0700
+ 🔤 mail	trash 12 KB	Today 1:46 AM	httpd/unix-directory	0700
+ in public_ftp	etc 4KB	Jul 8, 2024, 2:35 AM	http://unix.directory	
+ public_rum + mepositories	loge 4 KB	Jul 1 2024 8:32 AM	http://unix.directory	0700
+ 🖿 simp	mail 4/B	Today, 6:05 PM	mail	
+ in ssi		lup 25, 2024, 4:46 AM	nublicfte	0750
tools	public_tp 4 KB	Aug 24, 2024, 1:46 AM	publicity	0750
	4 KB	Aug 24, 2020, 3:19 PM	publicitum	0750
	repositones 4 KB	Aug 21, 2023, 1:02 AM	nttpa/unix-airectory	0755
	simp 4 KB	Apr 4, 2023, 5:36 PM		0755

4. Buka folder *tools* telah dibuat sebelumnya dan *upload file thor lite* beserta lisensinya.

cPanel - Tools	X 🔗 d'hanel Frie Manager v3 X 🕫 d'hanel Frie Manager v3 - Frie Uj X +	- o ×
< → C (#	srv127.niagahoster.com:2083/cpsess6500551115/frontend/jupiter/filemanager/upload-ajax.html?file=&fileop=&dri=%2Fho 🖈 💩 🖻 🦉 🦉 🦉 🤹 😰	🕘 🚯 :
P File Upload	i de la constante de	
2	Select the file you want to upload to "/home/n1574128/tools".	
	Maximum file size allowed for upload: =	
C	Overwrite existing files	
	Drop files here to start uploading	
	or	
	Select File	
t	thor-lite-34744b5a-e710708c-20240620-20241221.lic	
	100%	
t	thor10.7lite-linux-pack.zjp	
	100%	
3	36.46 MB complete	
	G Go Back to "/home/n1574128/tools"	

5. Lakukan *Extract* pada *file thor lite*.

CP anel - Terminal X CP CPa	anel File Manager v3 × 🕫 cPanel File	Manager v3 - File Up 🗙 🕂				
← → ♂ 😫 srv127.niagahoster.com:208	33/cpsess6500551115/frontend/jupiter/filema	inager/index.html	* •	🖻 🧶 🗾 /	′ ୭ 🚡 🖬 ଅ	¤r ④ 🚯 ÷
P File Manager			Search	All Your Files 🗸 🗸	for	Go Settings
+ File + Folder (D Copy + Move 1	🛓 Upload 🛛 🛓 Download 🛛 🗙 Delete	🕤 Restore 📑 Rename 🥖	Edit 🛛 🖉 HTML Editor	Permissions	♥ View ✓ Extract	✓ Compress
🕷 tools 🛛 Go	☆ Home 1 Up One Level ← Back	 → Forward <i>Q</i> Reload 	Select All Unselect	t All 🗂 View Tras	h 💼 Empty Trash	
Collapse All	Name		Size Last	Modified	Туре	Permissions
- = /home/n1574128	thor-lite-34744b5a-e710708c-20240f	520-20241221.lic	880 bytes Toda	y, 6:17 PM	text/x-generic	0644
+ 🖿 .cagefs	thor10 7lite-linux-pack zin		36.46 MB Toda	v 6:17 PM	nackage/x-generic	0644
.cl.selector	+ Dou	pload		,,	parender i denene	
clwpos	2.000	wilload				
+ 🖿 .composer	Viev	N				
+ cpanel	Mov	/e				
+ cphorde	(D Cop	y				
- razor	Renz	ame				
+ 🔤 .softaculous	₽ cha	nge Permissions				
🖿 .spamassassin	P chu	inge i er masions				
🖿 .ssh	A Dele	ete				
🖿 .trash	- Extr	act				
+ 🖿 etc	🖌 Com	npress				
logs						
+ mail						

6. Buka terminal *CPanel*, lalu masuk ke folder *tools* dan jalankan perintah berikut:

./thor-lite-linux -a Filescan --intense -norescontrol -cross-platform alldrives -p /home/



7. Setelah proses *scanning thor lite* selesai, maka di dalam folder *tools* akan terdapat *file* yang ber-ekstensi html yang merupakan *file* hasil dari proses *scanning*, kemudian *download file* tersebut.

CPanel - Terminal X CP cPanel - Terminal	el File Manager v3 🛛 🗴 🌮 cPanel File Manager v3 - File U/ 🗙 🕇		- 0 X
← → ♂ ♣ srv127.niagahoster.com:208;	/cpsess6500551115/frontend/jupiter/filemanager/index.html	* • • • • • •	🔒 🖬 🖆 । 🛒 🏵 🚯 ः
File Manager		Search All Your Files 🗸 for	Go Settings
+ File + Folder ② Copy + Move 🔮	Upload 🛓 Download 🗙 Delete 🐑 Restore 📄 Rename 🖋 Edit 😰 H	TML Editor 🎤 Permissions 🐵 View	🖉 Extract 📝 Compress
🕷 tools Go	☆ Home J Up One Level ← Back → Forward Ø Reload Ø Select All	🗆 Unselect All 🖀 View Trash 🖀 🛱	impty Trash
Collapse All	Name Size	Last Modified Ty	pe Permissions
- 늘 /home/n1574128	Config 4 KB	Jun 18, 2024, 5:49 PM htt	pd/unix-directory 0755
+ .cagefs	custom-signatures 4 KB	Jun 18, 2024, 5:49 PM htt	pd/unix-directory 0755
.chypos	b docs 4 KB	Jun 18, 2024, 5:49 PM htt	pd/unix-directory 0755
+ 🔤 .composer	ignatures 4 KB	Today, 1:45 AM htt	pd/unix-directory 0755
+ cpanel	tools 4 KB	Jun 18, 2024, 5:49 PM htt	tpd/unix-directory 0755
htpasswds	changes.log 36.88	KB Jun 18, 2024, 5:49 PM te:	xt/plain 0644
🖿 .razor	srv127.niagahoster.com_files_md5s.csv 601 by	rtes Today, 6:48 PM te:	xt/x-generic 0600
+ .sontaculous	srv127.niagahoster.com_thor_2024-07-12_1742.html	48 PM te:	xt/html 0664
ssh	srv127.niagahoster.com_thor_2024-07-12_1742.txt	C48 PM te:	xt/plain 0600
.trash	thor-lite-34744b5a-e710708c-20240620-20241221.lic	C17 PM te:	xt/x-generic 0644
F logs	thor-lite-linux	Edit 2024, 5:49 PM te:	xt/x-generic 0755
+ 🖿 mail	thor-lite-linux-64	2024, 5:49 PM te:	xt/x-generic 0755
+ public_ftp	thor-lite-linux-64.sig	2024, 5:49 PM te:	xt/x-generic 0644
+ m repositories	thor-lite-linux sig B Rename	2024. 5:49 PM te:	xt/x-generic 0644
+ 🖿 simp	thor-lite-util	Permissions 2024 5:49 PM te	xt/x-generic 0755
+ = ssi + = tmp	thor-lite-util sig × Delete	2024 5:49 PM te	xt/x-generic 0644
tools	Compression Compression	ess 17 PM pa	ckage/x-generic 0644
	E morrectine-intercept	po cini po	ionagera-generic 0044

8. Buka *file* .html yang telah di *download* sebelumnya untuk menampilkan hasil dari *scanning thor lite*.



B. Menggunakan SSH

 Register Thor Lite di <u>https://www.nextron-systems.com/thor-lite/</u> dan akses *link* yang dikirimkan pada *email* untuk *download* aplikasi dan lisensi. *Download* versi Linux apabila menggunakan *server* Ubuntu.

Command Prompt	× + ~		- 🗆 X
C:\Users\MAR\Downloads\T /c/Users/MAR/Downloads/T	hor>pwd hor		
C:\Users\MAR\Downloads\T	hor>ls -alt		
total 37468 drwxr-xr-x 1 MAR 197121 drwwyr-yr-x 1 MAR 197121	0 Jul 12 16	:13 .	
-rw-rr 1 MAR 197121 -rw-rr 1 MAR 197121	38234535 Jul 12 14 880 Jul 12 11	:13 : 1:13 thor10.7lite-linux-pack.zip 1:36 thor-lite-34744b5a-e710708c-20	240620-20241221.lic
C:\Users\MAR\Downloads\T	hor>		

2. Buka aplikasi *terminal* / cmd dan arahkan ke folder tempat aplikasi dan lisensi *thor* berada.



- 3. Kirim *file* aplikasi *thor lite* beserta lisensi dari *Local* ke *Remote Server* melalui SSH
 - Buat terlebih dahulu folder tools/thor di *remote server*, agar terlihat rapi.
 - Kirim *file* dengan menggunakan metode scp seperti contoh perintah di bawah ini:

scp -P 22123 thor-lite-34744b5a-e710708c-20240620-20241221.lic persandian@sandikami.diskominfo.sultengprov.go.id:/home/persandi an/tools/thor

🖾 Command Prompt X 🗾 persandian@sandikami: ~/too X + 🗸			×			
C:\Users\MAR\Downloads\Thor>pwd /c/Users/MAR/Downloads/Thor						
C:\Users\MAR\Downloads\Thor>ls -alt total 37468 0 Jul 12 16:13 . drwxr-xr-x 1 MAR 197121 0 Jul 12 16:13 . drwxr-xr-r- 1 MAR 197121 38234535 Jul 12 14:13 thor10.7lite-linux-pack.zip -rw-rr- 1 MAR 197121 880 Jul 12 11:36 thor-lite-34744b5a-e710708c-20240620-20241221.lic						
C:\Users\MAR\Downloads\Thor>scp -P 22123 thor10.7lite-linux-pack.zip persandian@sandikami.diskomi nfo.sultengprov.go.id:/home/persandian/tools/thor persandian@sandikami.diskominfo.sultengprov.go.id's password: thor10.7lite-linux-pack.zip 100% 36MB 4.1MB/s 00:08						
C:\Users\MAR\Downloads\Thor>scp -P 22123 thor-lite-34744b5a-e710708c-20240620-20241221.lic persan dian@sandikami.diskominfo.sultengprov.go.id:/home/persandian/tools/thor persandian@sandikami.diskominfo.sultengprov.go.id's password: thor-lite-34744b5a-e710708c-20240620-20241221.lic 100% 880 54.0KB/s 00:00						
C:\Users\MAR\Downloads\Thor>						

Keterangan:

- o scp: Perintah untuk menyalin file secara aman melalui SSH.
- -P 22123: Menentukan *port* SSH yang digunakan untuk koneksi (dalam hal ini, *port* 22123).

- thor-lite-34744b5a-e710708c-20240620-20241221.lic: Nama file local yang akan disalin.
- persandian@sandikami.diskominfo.sultengprov.go.id: Informasi
 username dan alamat domain
- /home/persandian/tools/thor: Path direktori tujuan di *remote server* di mana *file* akan di salin.
- 4. Lakukan *unzip* pada *file* aplikasi **thor10.7lite-linux-pack.zip** dengan perintah berikut:

unzip thor10.7lite-linux-pack.zip



5. Lakukan scanning aplikasi thor lite dengan menggunakan perintah berikut:

./thor-lite-linux -a Filescan --intense -norescontrol -cross-platform alldrives -p /home/



💽 Command Prompt X 🌌 persandian@sandikami: ~/toc X + 🗸			×
NER: persandian GROUP: persandian REASON_1: YARA rule WEBSHELL_PHP_Dynamic_Big / PHP webshell using \$a(\$code) for kind encoded blob to decode, e.g. b374k SUBSCORE_1: 50 REF_1: Internal Research SIGTYDE_ IGCLASS_1: YARA Rule MATCHED_1: Str1: " php" in "<?php\x0a\x0anamespace Spatie\LaravelIgnit<br s\\Du" at 0x0 Str3: "\$handler(\$" in "er? php\x0a\x0anamespace Spatie\LaravelIgnit s\\Du" at 0x0 Str3: "\$handler(\$" in "er? {x0a if (\$handler) {\x0a dler(\$value);\x0a }\x0a }\x0a }\x0a \x0a\x0a public " at 0x138 RU 1=02=07 TAGS_1: EXE, FILE, T1033, T1087_002, T1505_003, WEBSHELL RULENAME_1: WEBSHEL Big AUTHOR_1: Arnim Rupp (https://github.com/ruppde) REASONS_COUNT: 1 Info Finished module DURATION: 0 hours 1 mins 24 secs SCANNED_ELEMENTS: 22460	of ev 1: int avelIg ion\\R LEDATE L_PHP_	al wit ernal nition ecordo \$ha _1: 20 Dynam:	th S n\ er an 02 ic
Results			
Info Results ALERIS: 0 WARNINGS: 5 NOILLES: 5 ERRORS: 1 Info For details see the log files written to ["sandikami_thor_2024-07-12_0913.txt" or_2024-07-12_0913.html"]	"sandi	kami_t	th
Info Begin Time: Fri Jul 12 09:13:40 2024			
Into End Time: Fri Jul 12 09:15:07 2024 Info Scan took 0 hours 1 mins 27 secs			
Notice Thor Scan finished END_TIME: Fri Jul 12 09:15:07 2024 ALERTS: 0 WARNINGS: 5 N	OTICES	: 5 EF	RR
ORS: 1 persandian@sandikami:~/tools/thor\$			

Keterangan:

- -p /home/: path direktori /home/ sebagai target pemindaian
- 6. Kirim *file* ber-ekstensi html yang merupakan *file* dari hasil *scanning thor lite* ke *local*.
 - Akses direktori *local* menggunakan terminal untuk menentukan tempat dimana *file* hasil *scanning thor lite* akan di simpan dan jalankan perintah seperti berikut:





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/sandikami_thor_2024-07-12_0913
 .html : Path direktori tujuan di *remote server* di mana *file* akan di kirim.
- .: Direktori tujuan di mesin *local* (dalam hal ini, . menunjukkan direktori saat ini).

• Buka *file* html hasil dari *scanning thor lite* untuk melihat hasilnya.

