Lucy comes with various log files that can be accessed through the web gui. Here are a few examples:

System Logs (Apache Error Log, Apache Access Log & Postfix Mail Log)

The system logs can be found under admin/help/servicelogs within the web gui.

ATLS Campages to	ana tatap -	Support -	1.
Home / Service Logs		Status	
Service Log	S	Manual Changelog	
File	Select file	Test email Performance Test	~
Period Start	19.08.2020 10:24	System Monitoring Spam Test	i
Period End	20.08.2020 10:24	Backups	Ħ
Log		Migration Tool Exports	
		License	
		Tickets	
		Invoices	
		Update	
		Reboot	
		SSH Password	
		Enable SSH Access	
		Send Logs	
		Service Logs	
		Mail Manager	

Application Logs (Lucy specific logs)

Within the send log function (admin/help/logs) you have a download button that allows you to

download all LUCY related log files.

Home / Help Send Logs Lucy will send apache logs and system logs, without any personal c Proceed		Manual Changelo	g				
		Test E-m Performa					Download Logs
		onal c System M Sparn Te	Aonitoring st		/		
			Enable SSH Access				
opyright © 2016 Lucy 3.0		Send Log Service L		- ·	/		
				/			
							• 🖬
5			/				
s Name +	Type C	Compressed size	Pessword	Size	Ratio	Date modified	
	Type C	Compressed size	Password No	Size 719 KB		Date modified 10.05.2006 20:41	
Name +			-		98%		. D
Name *	Text Document	20 KB	No No	719 KB	98% 98%	10.05.2016 20:41	- 2
Name +	Text Document 1 File	20 KB 27 KB	No No	719 KB 1 1025 KB	98% 98% 98%	10.05.2016 20:41 09.05.2016 18:47	- D
Name * application.log application.log1 application.log2	Text Document 1 File 2 File	20 KB 27 KB 29 KB	No No No	719 KB 1 1025 KB 1 1025 KB	98% 98% 98%	10.05.2006 20-41 09.05.2006 18:47 09.05.2006 18:32	
Name * application.log application.log.1 application.log.2 application.log.3	Text Document 1 File 2 File 3 File	20 K8 27 K8 29 K8 30 K8 30 K8	No No No No	719 KB 1 1025 KB 1 1025 KB 1 1025 KB 1 1025 KB	98% 98% 98%	10.05 2006 2041 09.05 2006 1847 09.05 2006 1832 09.05 2006 1832	_ D
Name = application.log application.log.1 application.log.2 application.log.3 application.log.3	Text Document 1 File 2 File 3 File 4 File	20 K8 27 K8 29 K8 30 K8 30 K8	No No No No No	719 KB 1 1025 KB 1 1025 KB 1 1025 KB 1 1025 KB	98% 98% 98% 98% 98% 82%	10.05.2006 20-41 09.05.2006 18-47 09.05.2006 18-32 09.05.2006 18:17 09.05.2006 18:17	_ Q
Name = application.log application.log.1 application.log.2 application.log.3 application.log.4 beef.log	Test Document 1 File 2 File 3 File 4 File Test Document	20 K8 27 K8 29 K8 30 K8 30 K8 30 K8 2 K8	No No No No No No	719 KB 11025 KB 11025 KB 11025 KB 11025 KB 11025 KB 7 KB	98% 98% 98% 98% 98% 82% 0%	10.05.2006 20+41 09.05.2006 18+47 09.05.2006 18+32 09.05.2006 18:17 09.05.2006 18:17 10.05.2006 20:39	
Name = application.log application.log.1 application.log.2 application.log.3 application.log.4 beef.log beef.error.log	Test Document 1 File 2 File 3 File 4 File Test Document Test Document	20 K8 27 K8 29 K8 30 K8 30 K8 30 K8 30 K8 0 K8	No No No No No No	719 KB 1025 KB 1025 KB 1025 KB 1025 KB 1025 KB 7 KB 0 KB	98% 98% 98% 98% 98% 82% 0% 96%	10.05.2006 20-41 09.05.2006 18-47 09.05.2006 18-32 09.05.2006 18-32 09.05.2006 18-17 09.05.2006 17:54 10.05.2006 20-39 07.05.2006 23-32	
Name + application.log 1 application.log.2 application.log.3 application.log.4 bed.log bed.log console.log	Test Document 1 File 2 File 3 File 4 File Test Document Test Document Test Document	20 K8 27 K8 29 K8 30 K8 30 K8 0 K8 0 K8 3 K8	No No No No No No No	719 KB 1025 KB 1025 KB 1025 KB 1025 KB 7 KB 0 KB 50 KB	98% 98% 98% 98% 82% 0% 96% 82%	10.05.2006 20-41 09.05.2006 18-47 09.05.2006 18-32 09.05.2006 18-32 09.05.2006 17:54 10.05.2006 20-39 07.05.2006 20-32 11.05.2006 20-45	

- Lucy Core Application Logs
- BeEf Status & Error Logs
- Console Logs
- Rescue System & Worker Logs
- Scheduler Logs
- System Monitoring Logs

Campaign Logs

Within the campaign you can use the dashboard with its <u>campaign monitoring</u> to track all activities or use the <u>reporting</u> to export the campaign data. Other than that you have as well some campaign specific error logs you can access:

Summary			\frown	\frown
User Settings	0) .	(○) →	
Statistics			\bigcirc	\bigcirc
Recipients	0 messages	hcharts.com	Highcharts.com 0% of recipients clicked the link	Highcharts.com 0% of attacks are successful
Base Settings			IIIK	Succession
Schedule	Messages Sent	0 of 3		0.00%
Augropose Mahaita	Clicks	0 of 3		0.00%
Awareness Website	Successful Attacks	0 of 3		0.00%
Reports	Vulnerable Victims	0 of 3		0.00%
Checks				
Message Log				
Errors				

- Message log: contains all messages that have been successfully transmitted by LUCY
- Error log: contains all errors related to the campaign specific message transmission

Status logs

Under /admin/help/status LUCY keeps track of all user activities. You can filter for a specific date range. Each activity has a link. Details are visible when you click on the link. Example:

tatus						A Export	C Clea
Time		Message	User		Filter		
05.04.2019 23:13:36		1 Users Logged in	default@user.com		Туре		
05.04.2019 22:25:50		1 Users Logged out	default@user.com		Al		,
03.04.2019 18:25:50 - 04.04:2019 1	1:15:22	3 Users Logged in	Julia Fischer (ginger)	(juser.com)	From		
03.04.2019 14:58:14 - 05.04.2019 2	2:19:47	5 Users Logged in	default@user.com		05.04.2019		
03.04.2010 14:38:27		1 Users Logged out	default@user.com		То		
03.04.2019 09:01:23 - 03.04.2019 1	4:34:20	6 Users Logged in	default@user.com		05.04.2019		
03.04.2019 08:21:11		1 Messages Sent	System				Update
03:04:2019:08:11:52		1 Campaigns Added	default@user.com				Openance
02.04.2019 20.35.53 - 03.04.2019 0	8.09.40	2 Users Logged in	default@user.com				
02.04.2019 16:45:38		1 Campaigns Added	default@user.com		Current User		
02.04.2019 09:44:41 - 02.04.2019 1	5:44:03	4 Users Logged in	default@user.com		Name	NA	
02.04.2019.09.39.40		1 Users Logged out	default@user.com		Email	default@user.com	
02.04.2019 07:53:43 - 02.04.2019 0	7.58.20	2 Users Logged in	default@user.com		Phone	+41793637211	
01.04.2019 15:44:45		1 Users Logged out	default@user.com		Role	Administrator	
Home Status							Ca
natus							
Time	Message			User	Current User		
29.03.2019 20.56:34	Demo: car	npaign deleted		System	Name	NA	
29.03.2019 20:58:34	encr email	: campaign deleted		System	Email	default@user.com	
29.03.2019 20:58:34	phish-szer	ario: campaign deleted		System	Phone	+41793637211	
29.03.2019 20:56:34	test 1: can	spaign deleted		System	Role	Administrator	

Mail communication logs when using external mail server (mail relay)

Communication with an external mail server is logged to the /opt/phishing/runtime/resque_worker.log. If there were any errors, they are displayed in more or less details.

Example 1 of communication error:

[notice] [11:55:05 2019-06-27] (Job{worker} | ID: 6064cd8dsdsd396d5b84c3e21d
| AwarenessCampaignMailJob |
[{"campaign":154,"id":"phish.campaign.154.awareness"}]) has finished

```
Failed to connect to ssl:clientserver.mail.protection.outlook.com:587 [SMTP: Failed to
connect socket: Connection timed out (code: -1, response: )] #0
/opt/phishing/versions/4.5/web/protected/jobs/ScenarioChecksJob.php(294):
MailManager::send('test@phishing.s...', Array, 'phish:9300', Object(CampaignAwareness))
#1 /opt/phishing/versions/4.5/web/protected/jobs/ScenarioChecksJob.php(881):
ScenarioChecksJob→_mailCheck(Object(CampaignScenarioCheck)) #2
/opt/phishing/versions/4.5/web/protected/jobs/ScenarioChecksJob.php(906):
ScenarioChecksJob→ runCheck('mail check') Failed to connect to
ssl:smtp.server.mail.protection.outlook.com:587 [SMTP: Failed to connect socket:
php network getaddresses: getaddrinfo failed: Name or service not known (code: -1,
response: ]] #0 /opt/phishing/versions/4.5/web/protected/jobs/ScenarioChecksJob.php(294):
MailManager::send('test@phishing.s...', Array, 'phish:8153', Object(CampaignAwareness)) #1
/opt/phishing/versions/4.5/web/protected/jobs/ScenarioChecksJob.php(881):
ScenarioChecksJob→ mailCheck(Object(CampaignScenarioCheck)) #2
/opt/phishing/versions/4.5/web/protected/jobs/ScenarioCheckslob.php(906):
ScenarioChecksJob→ runCheck('mail check')
```

Example 2:

[notice] [14:24:29 2019-06-18] Starting work on (Job{worker} | ID: ca6254f0362b003ad8b63a6b3c3159d1 | PostfixJob | [{"campaign":114,"id":"phish.smtp.postfix"}]) [notice] [14:24:31 2019-06-18] (Job{worker} | ID: ca6254f0362b003ad8b63a6b3c3159d1 | PostfixJob [{"campaign":114,"id":"phish.smtp.postfix"}]) has finished [notice] [14:24:31 2019-06-18] Starting work on (Job{worker} | ID: 26425557e3b7b740a1476276a1854e34 | AwarenessCampaignMailJob | [{"campaign":114,"id":"phish.campaign.114.awareness"}]) PHP Error[8]: Undefined variable: php errormsg in file /usr/share/php/Net/Socket.php at line 196 #0 /usr/share/php/Net/SMTP.php(440): Net Socket \rightarrow connect() #1 /usr/share/php/Mail/smtp.php(385): Net SMTP \rightarrow connect() #2 /usr/share/php/Mail/smtp.php(271): Mail smtp→getSMTPObject() #3 /usr/share/php/Mail/smtp.php(258): Mail smtp→send or fail() #4 /opt/phishing/versions/4.5/web/protected/components/MailManager.php(131): Mail smtp→send() #5 /opt/phishing/versions/4.5/web/protected/components/CampaignAwarenessManager.php(748): send() #6 /opt/phishing/versions/4.5/web/protected/components/CampaignAwarenessManager.php(777): CampaignAwarenessManager→ prepareAndSendEmail() #7 /opt/phishing/versions/4.5/web/protected/jobs/AwarenessCampaignMailJob.php(90): CampaignAwarenessManager→sendAwarenessEmail() #8 /opt/phishing/versions/4.5/web/protected/vendor/chrisboulton/php-resque/lib/Resque/lob.php(198): AwarenessCampaignMailJob→perform() #9 /opt/phishing/versions/4.5/web/protected/vendor/chrisboulton/phpresque/lib/Resque/Worker.php(243): Resque Job→perform() #10 /opt/phishing/versions/4.5/web/protected/vendor/chrisboulton/phpresque/lib/Resque/Worker.php(205): Resque Worker→perform() #11 /opt/phishing/versions/4.5/web/protected/vendor/bin/resque(127): Resque Worker \rightarrow work() #12 /opt/phishing/versions/4.5/web/protected/commands/ResqueCommand.php(28): include() #13 /opt/phishing/versions/4.5/web/protected/components/ConsoleCommand.php(93): ResqueCommand→runUnlocked() #14 /opt/phishing/versions/4.5/web/protected/framework/console/CConsoleCommandRunner.php(71): ResqueCommand→run() #15

/opt/phishing/versions/4.5/web/protected/framework/console/CConsoleApplication.php(92): CConsoleCommandRunner→run() #16

/opt/phishing/versions/4.5/web/protected/framework/base/CApplication.php(180): CConsoleApplication→processRequest() #17

/opt/phishing/versions/4.5/web/protected/framework/yiic.php(33): CConsoleApplication→run() #18 /opt/phishing/versions/4.5/web/protected/yiic.php(13): require_once() #!/usr/bin/env php

Successfully sent emails are not logged in details, it is a simple "AwarenessCampaignMailJob" record that indicate the email has been successfully sent:

[notice] [14:34:18 2019-06-21] Starting work on (Job{worker} | ID: eed90cc4a2048479e59df3353481041f | AwarenessCampaignMailJob | [{"campaign":151,"id":"phish.campaign.151.awareness"}]) [notice] [14:34:19 2019-06-21] (Job{worker} | ID: eed90cc4a2048479e59df3353481041f | AwarenessCampaignMailJob | [{"campaign":151,"id":"phish.campaign.151.awareness"}]) has finished

From: https://wiki.lucysecurity.com/ - **LUCY**

Permanent link: https://wiki.lucysecurity.com/doku.php?id=log_files_in_lucy&rev=1564051796



Last update: 2019/07/25 12:49