TryHackMe Zeek Exercises — Task 3 Phishing, Task 4 Log4J, & Task 5 Conclusion

Posted Jan 16, 2023 • Updated Jan 17, 2023

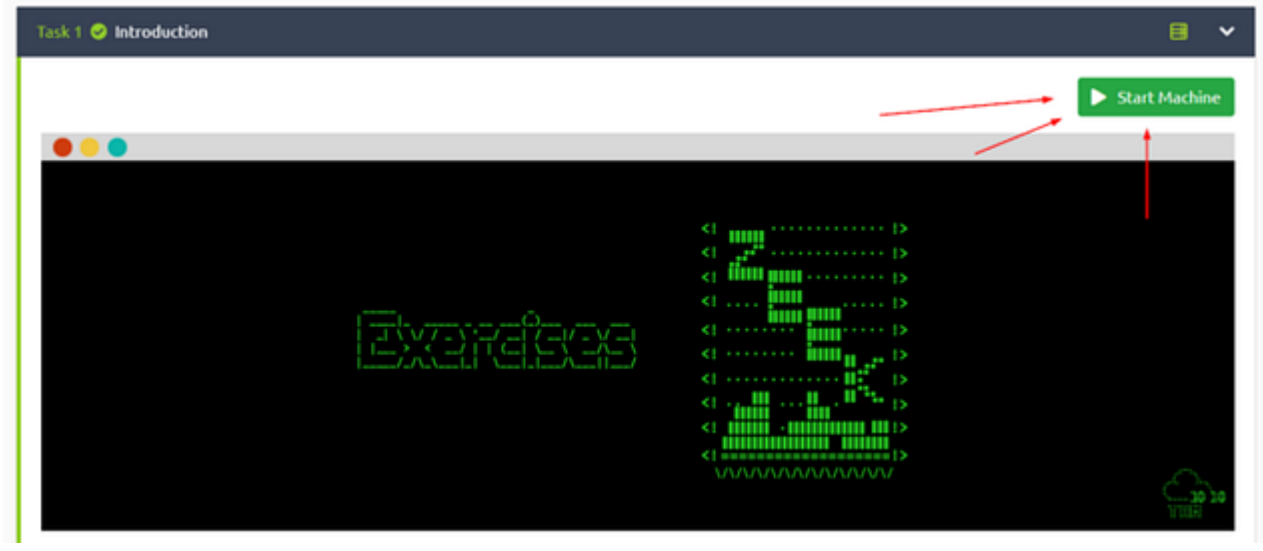
By Dan Rearden

14 min read

If you haven't done task 1 & 2 yet, here is the link to my write-up of it: Task 1 Introduction & Task 2 Anomalous DNS.

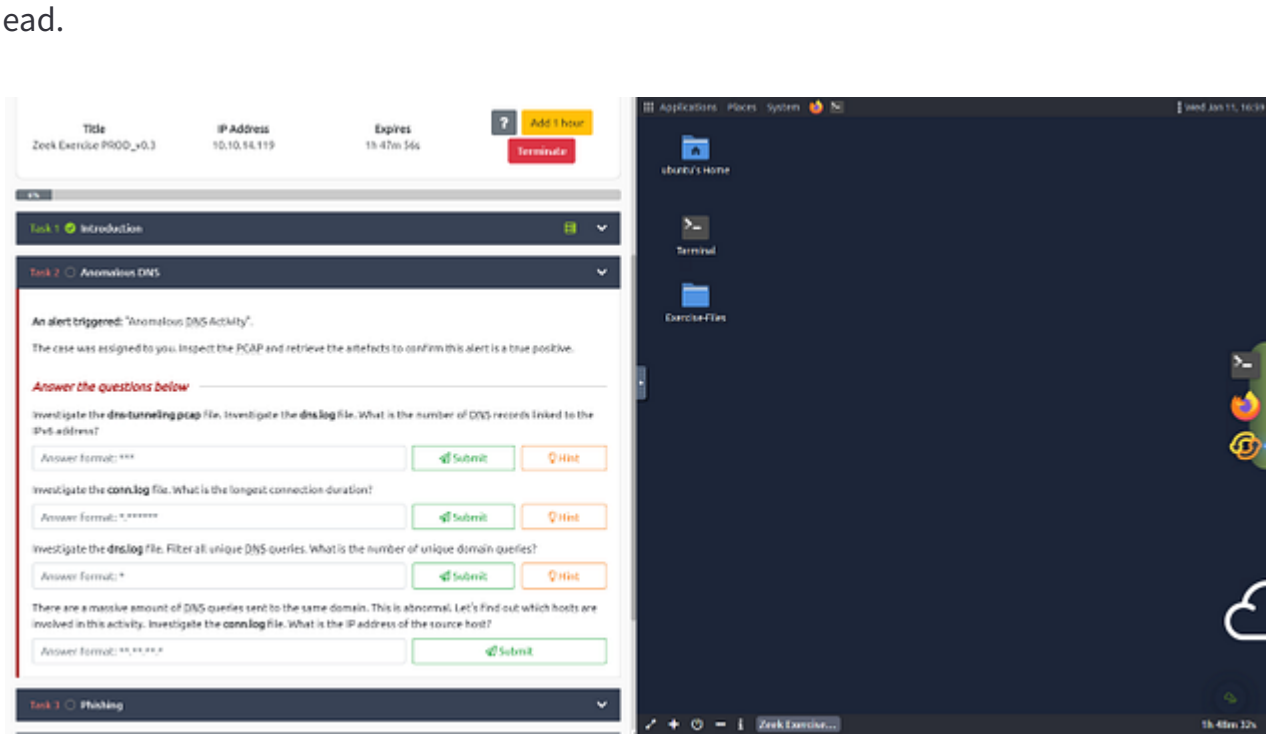
Getting the VM Started

Click the green button labeled Start Machine, at the top of Task 1.

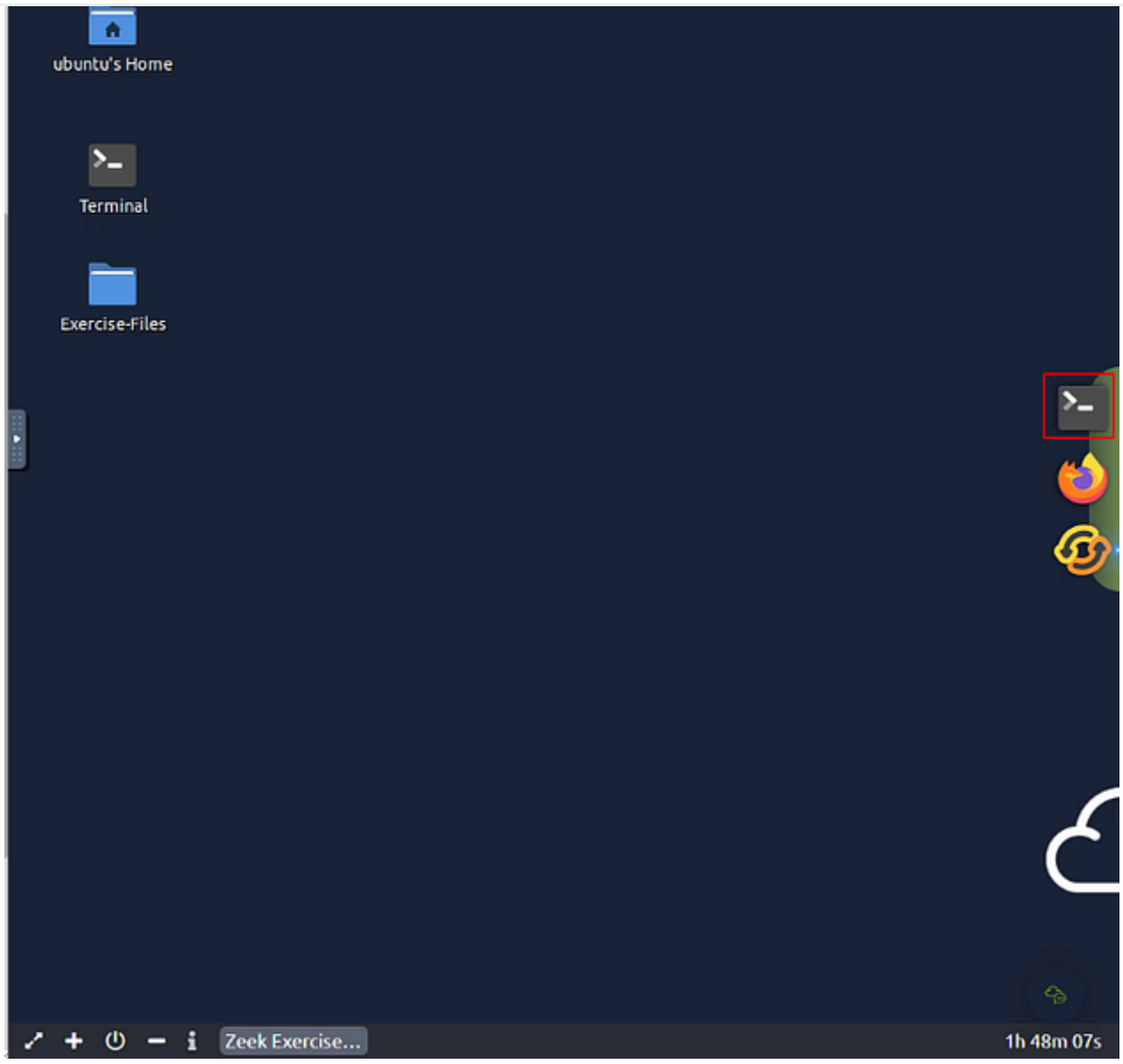


The screen should split in half if it doesn't go to the top of the page. You will see a blue button labeled Show Split View, click this button.

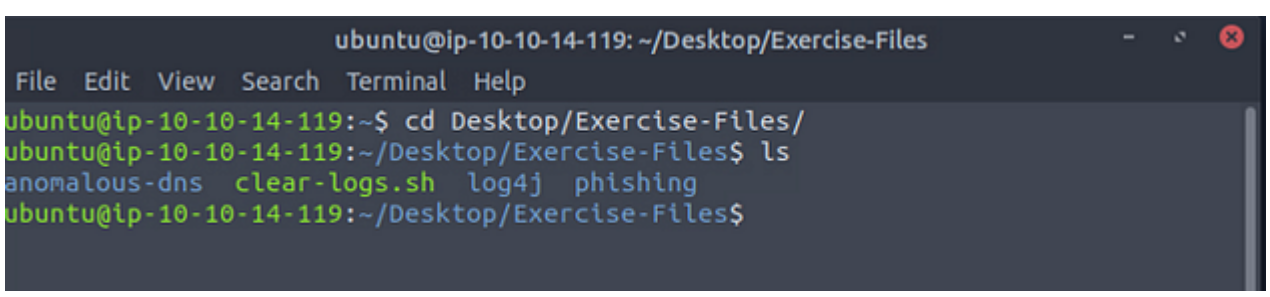
The screen should be split now, you have to wait for the VM to load. When it is finished loading it will look like it does below. You are ready to continue with the tasks ahead.



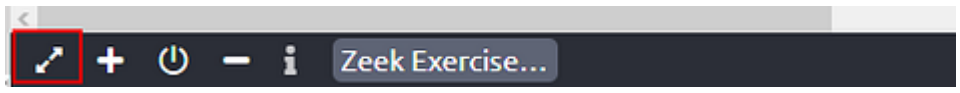
On the VM, you will see a terminal icon in the middle of the VM screen on the right. Click on it.



A terminal window will pop up, time to move to the Exercise-Files directory. To do this we will use the `cd` command, which stands for change directory. We will use this command in combination with Tab completion. With Tab complete, you only have to press Tab after starting to type, and if it only has one entry that matches, it will auto-complete it. So let's type out the command `cd Desktop/Exercise-Files/` , then press enter to run the command. Follow up with the `ls` command to see the contents of the directory.



At the bottom of the VM, is a panel click the diagonal arrow icons. This will open the VM to full screen and make it easier to copy and paste.



Task 3 Phishing

An alert triggered: "Phishing Attempt".

The case was assigned to you. Inspect the PCAP and retrieve the artifacts to confirm this alert is a true positive.

Answer the questions below

First, we need to move into the correct directory, to do this we need to use the command `cd phishing/` , then press enter. Using `ls` will list out the directories contents.

```
ubuntu@ip-10-10-243-38:~/Desktop/Exercise-Files$ cd phishing/
ubuntu@ip-10-10-243-38:~/Desktop/Exercise-Files/phishing$ ls
clear-logs.sh  file-extract-demo.zeek  hash-demo.zeek  phishing.pcap
```

see the contents of the current directory.

```
ubuntu@ip-10-10-20-250:~/Desktop/Exercise-Files/phishing$ zeek -r phishing.pcap
ubuntu@ip-10-10-20-250:~/Desktop/Exercise-Files/phishing$ ls
clear-logs.sh  dns.log                 hash-demo.zeek     pe.log
conn.log       file-extract-demo.zeek  http.log           phishing.pcap
dhcp.log       files.log               packet_filter.log
ubuntu@ip-10-10-20-250:~/Desktop/Exercise-Files/phishing$
```

Investigate the logs. What is the suspicious source address? Enter your answer in **defanged format**.

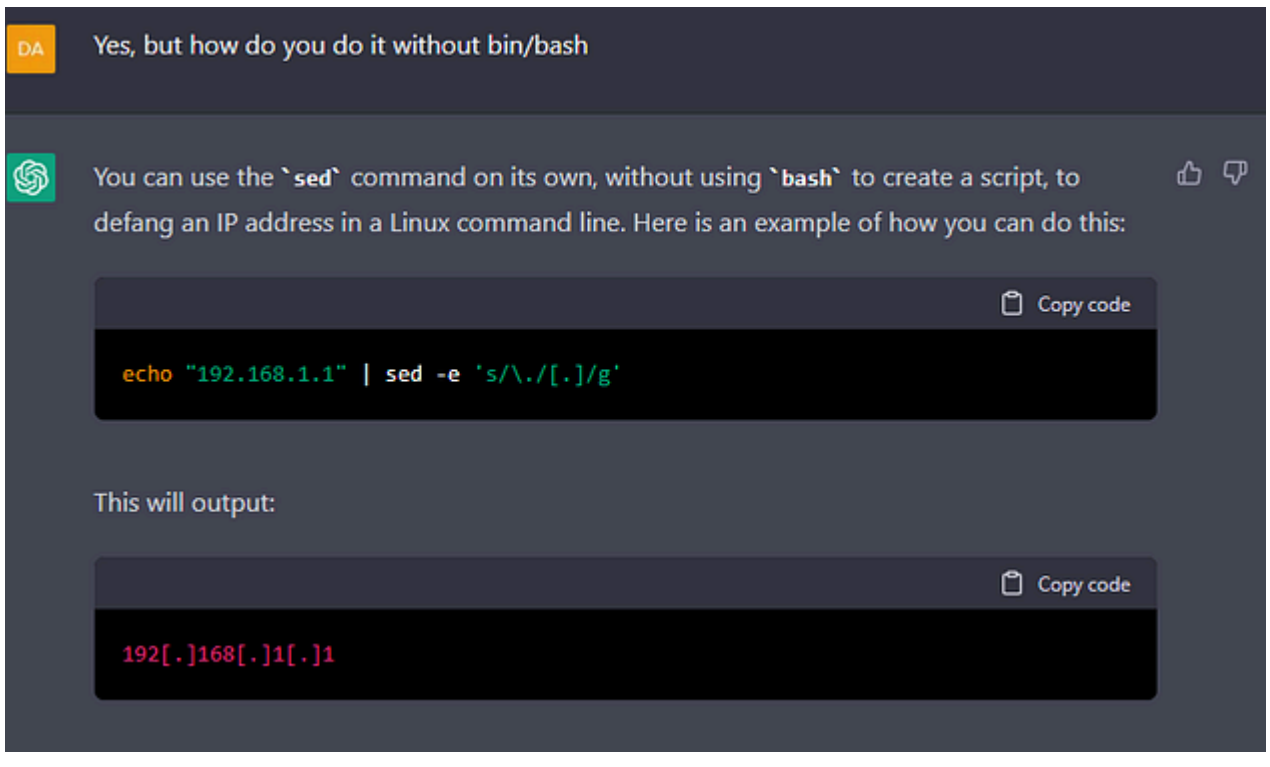
After doing some investigating myself, I came to the realization that they want to know what the infected local machine is. So I went to the dhcp.log file and looked at it with `cat dhcp.log | less` , pressing enter to open it.

```
ubuntu@ip-10-10-20-250:~/Desktop/Exercise-Files/phishing$ cat dhcp.log | less
```

At a quick glance at the different fields, we see that one of the field names is client_addr. This seems to be the field we want to use, time to use some zeek-cut.

```
#fields ts      uids    client_addr     server_addr     mac     host_name       client_fqdn     domain  requested_addr  assigned_addr   lease_tim
e       client_message  server_message  msg_types      duration
```

To keep with using the command line, I asked ChatGPT what is the command line script to defang an IP address. It gave me a bin/bash script to do this, I then asked it for one that doesn't require bin/bash. ChatGPT gave me this script `echo "IP address" | sed -e 's/\./[.]/g'` .



So with our newly learned code from ChatGPT, and the command line kung-fu we already know let us get the answer. So the command we use is `cat dhcp.log | zeek-cut client_addr | uniq | sed -e 's/\./[.]/g'` , and press enter to run. We take the field and run it through zeek-cut, and pipe the results through uniq. Uniq is used to remove any duplicates, then we pipe the results into sed to defang the IP address. After running the command we are left with a defanged IP address in the output of the terminal, and the answer to the question. Type the answer into the TryHackMe answer field, and click submit.

```
ubuntu@ip-10-10-20-250:~/Desktop/Exercise-Files/phishing$ cat dhcp.log | zeek-cut client_addr | uniq | sed -e 's/\./[.]/g'
[redacted]                    Answer
ubuntu@ip-10-10-20-250:~/Desktop/Exercise-Files/phishing$
```

Answer: 10[.]6[.]27[.]102

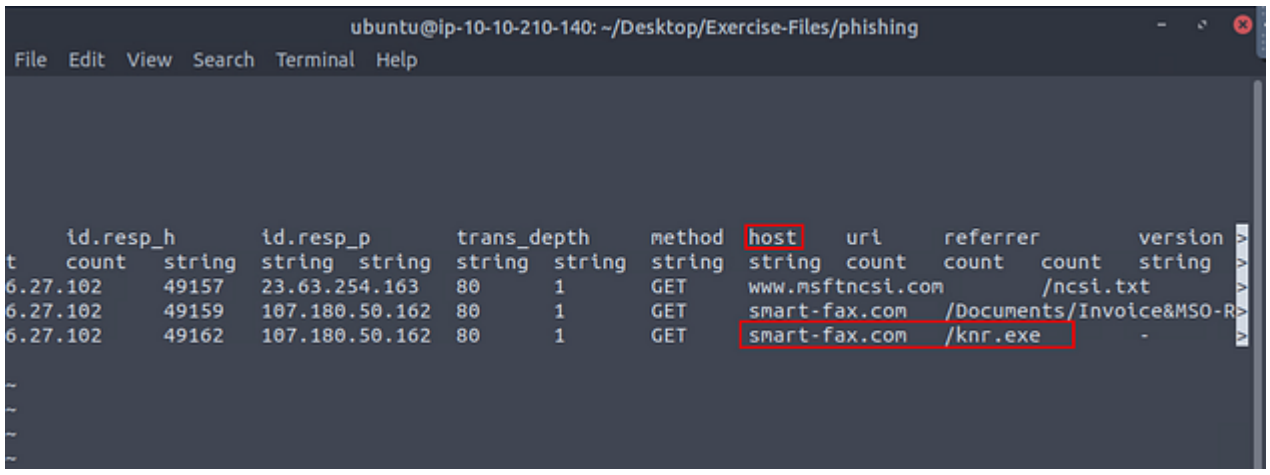
Investigate the **http.log** file. Which domain address were the malicious files downloaded from? Enter your answer in **defanged format**.

Now let's cat the HTTP log file and pipe it through less to see if we can figure out the name of the field we need to use.

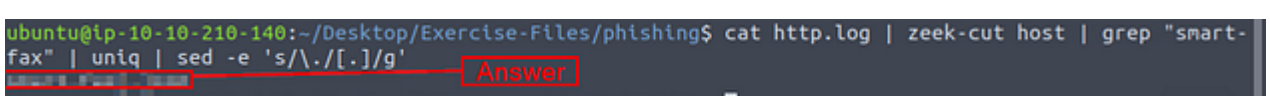
```
ubuntu@ip-10-10-210-140:~/Desktop/Exercise-Files/phishing$ cat http.log | less
```

Once less opens the HTTP log file, press the right arrow key once.

We can see the name of the field we are looking for is host, and if we remember the malicious file from task 2. We can see it here, along with the domain that it was downloaded from. Time to use some zeek-cut, so press `q` to exit less.



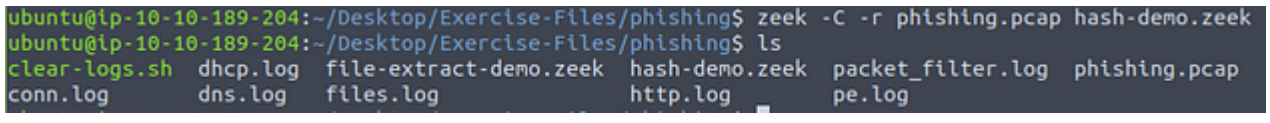
With the name of the field, and some command line kung-fu let's get the answer. The command we are going to run is `cat http.log | zeek-cut host | grep "smart-fax" | uniq | sed -e 's/\./[.]/g'` , press enter to run the command. We take the field and run it through zeek-cut, and pipe the results through grep. Using grep we pull out only the host that matches our string, we then pipe those results into uniq. With uniq we get rid of the duplicates, and we then pipe those results into sed. Finally with sed to defang the domain. After running the command we are left with a defanged domain in the output of the terminal, and the answer to the question. Type the answer into the TryHackMe answer field, and click submit.



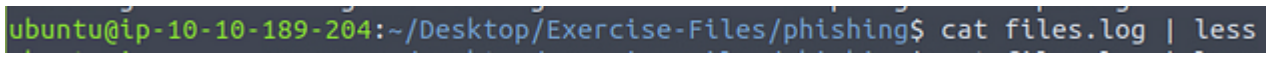
Answer: smart-fax[.]com

Investigate the malicious document in VirusTotal. What kind of file is associated with the malicious document?

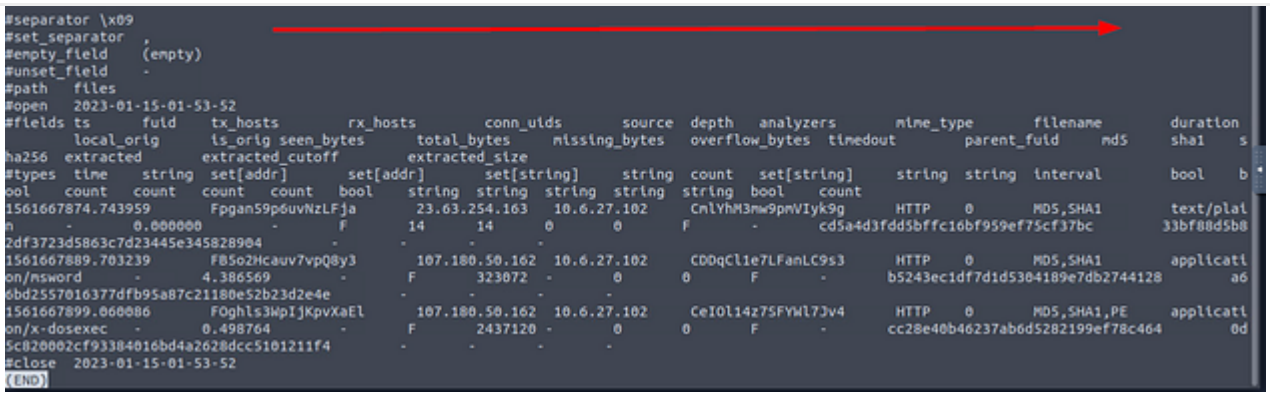
To start off, we need to run Zeek again, this time with the script hash-demo.zeek. The command we are going to run is `zeek -C -r phishing.pcap hash-demo.zeek` , and press enter to run. After Zeek is done, us the command `ls` to show the contents of the current directory.



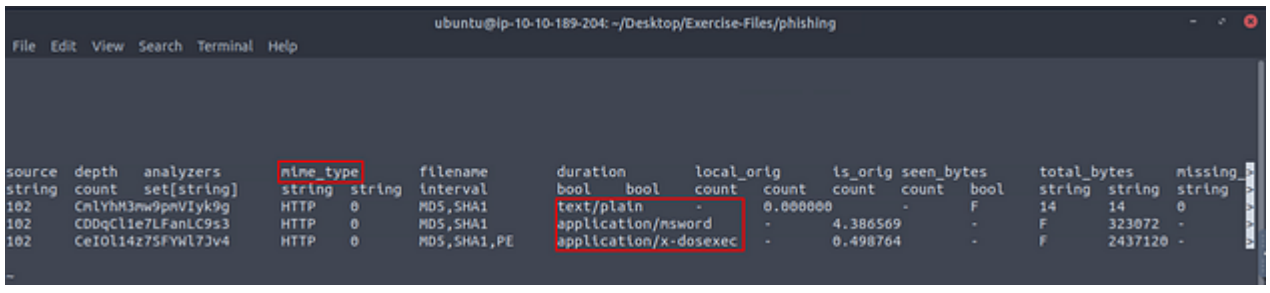
Now let's cat the files log file and pipe it through less to see if we can figure out the name of the field we need to use



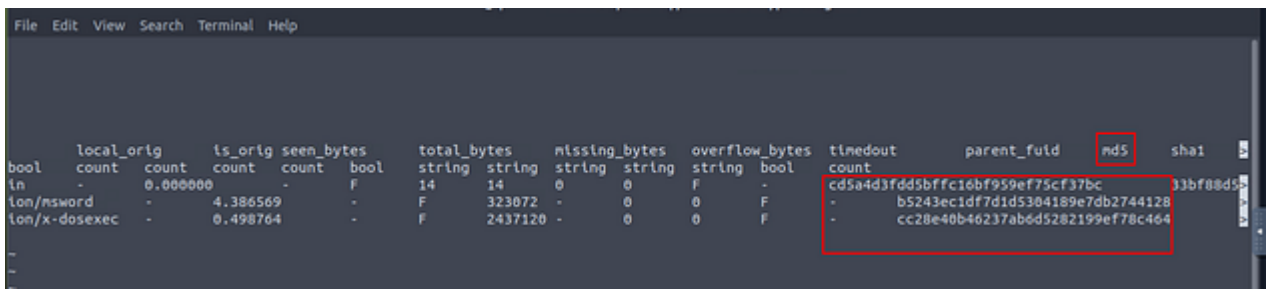
Once less opens the files log file, press the right arrow key once.



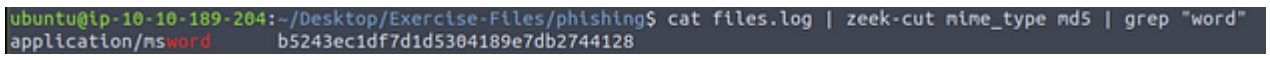
From the Zeek room, we know that we want to look at the mime_type field. We can see this by the fact that the application/msword is in this field.



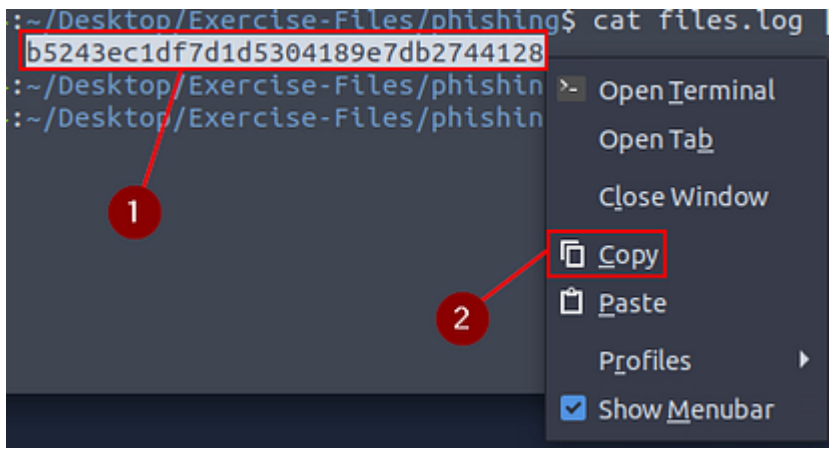
Next, we need to look at the hash field, use the right arrow key to move to the right till you reached the hashes. Once there, you will see the name of the md5 hash field. Now we have all the info we need for now, press `q` to exit less.



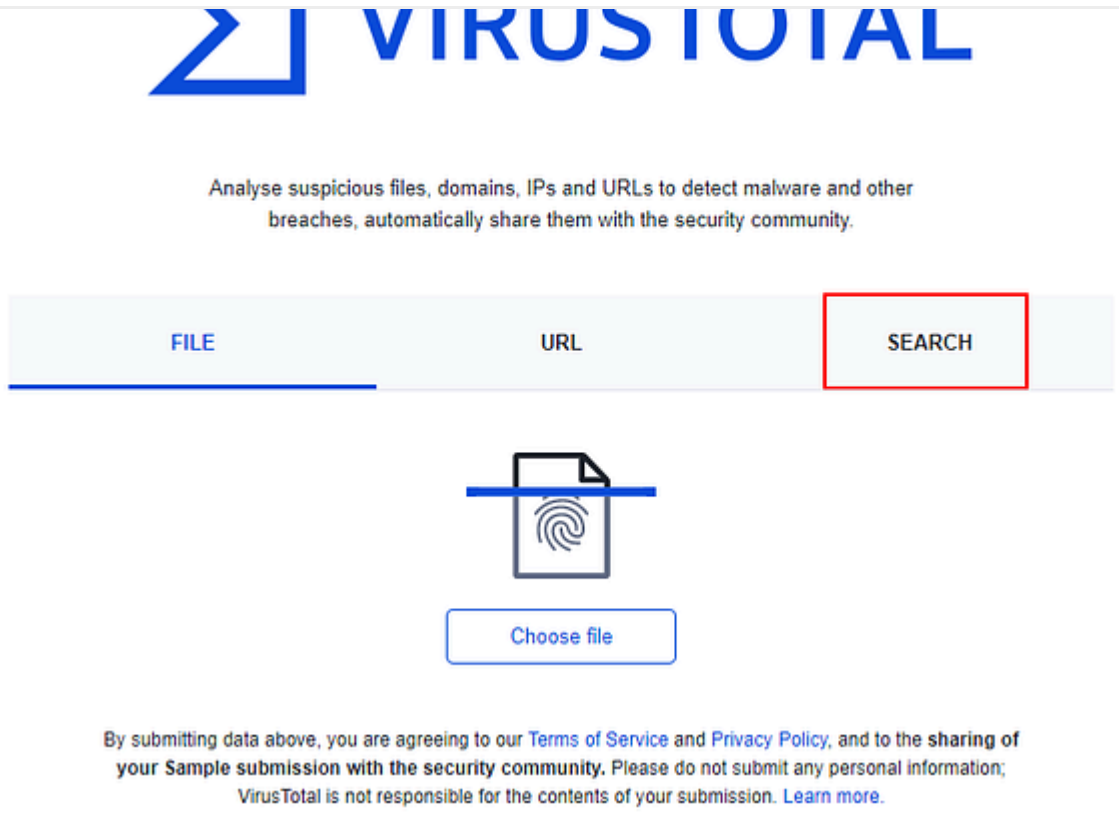
So to get the hash that we need we can use some command line kung-fu. The command we are using is `cat files.log | zeek-cut mime_type md5 | grep "word"` , then press enter to run. You will have the hash will be in the output of the terminal.



Highlight the hash, right-click on the highlighted hash, then click Copy on the drop-down menu.

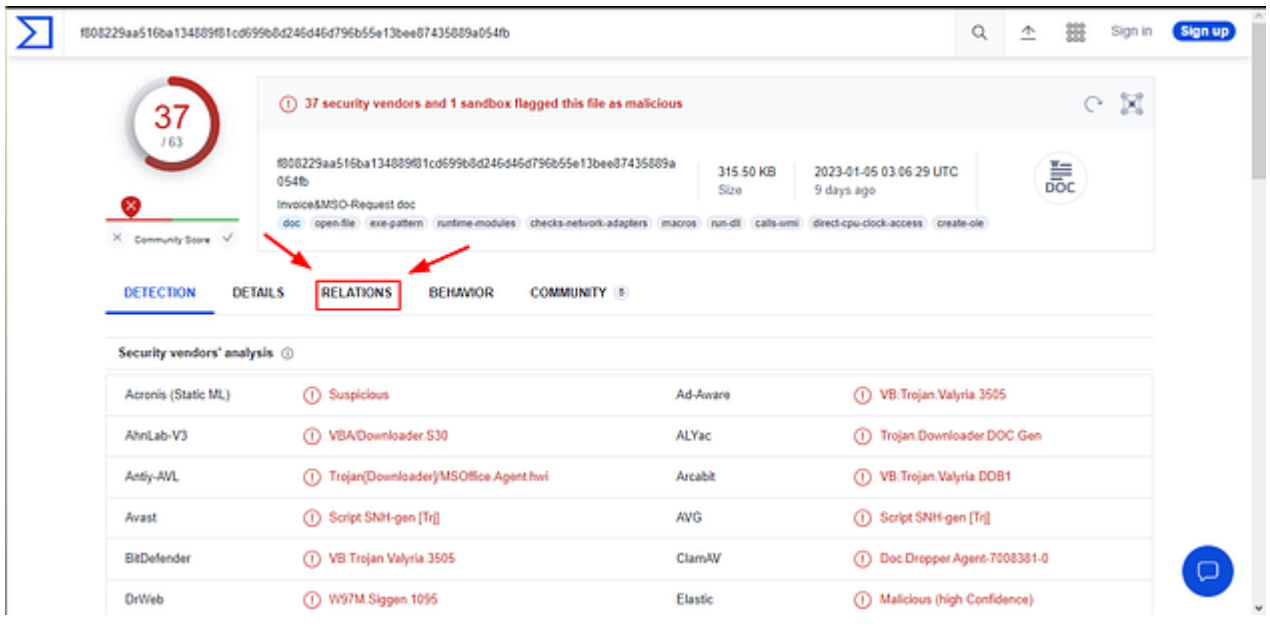


Open a browser, go to the VirusTotal website (I provided the link to the site). Once the site loads, click the SEARCH tab in the middle of the screen.

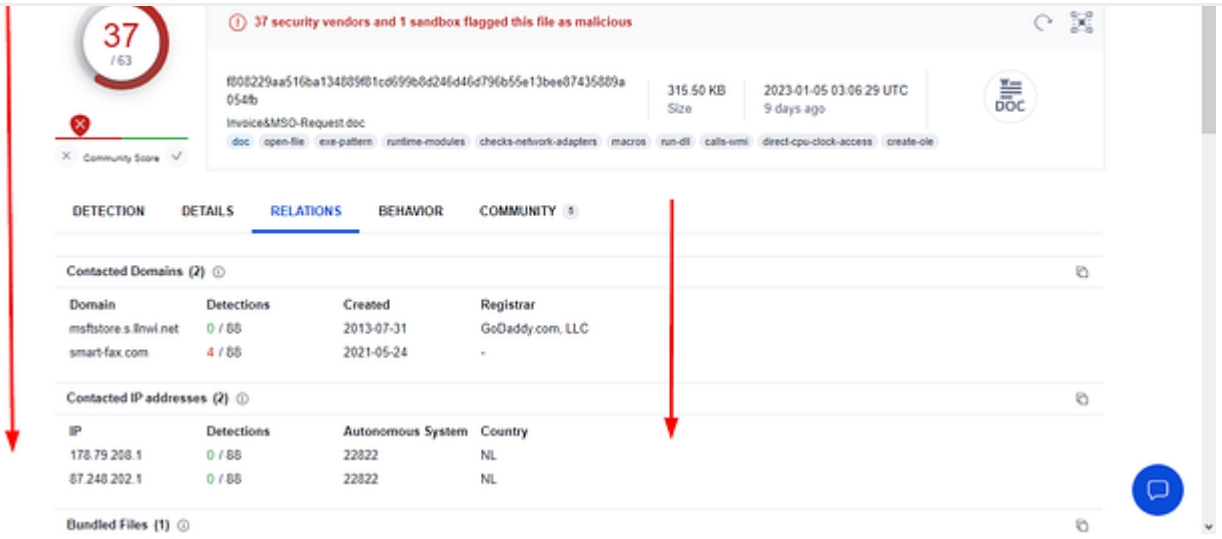


A search field will be in the middle of the page, using the keyboard shortcut ctrl + v to paste the hash in search field and press enter to search the hash.

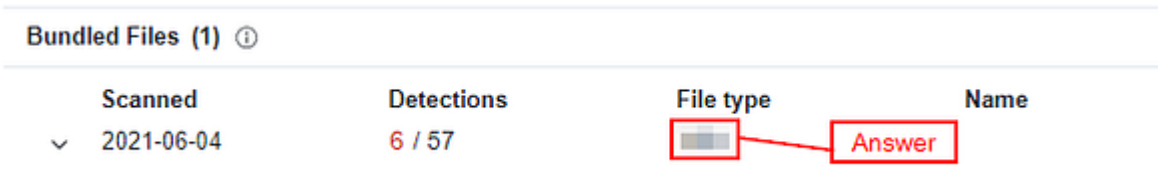
Once the DETECTION page loads, click the RELATIONS tab.



Once the RELATIONS page loads, scroll down till you see Bundled Files section.



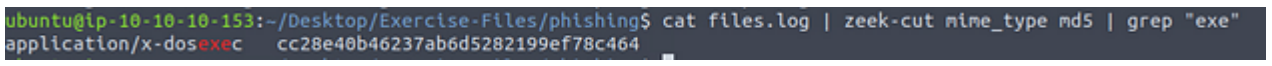
Once you reach the Bundled Files section, you will see a column labeled File type. The three-letter file abbreviation is the answer, type the answer into the TryHackMe answer field, and click submit.



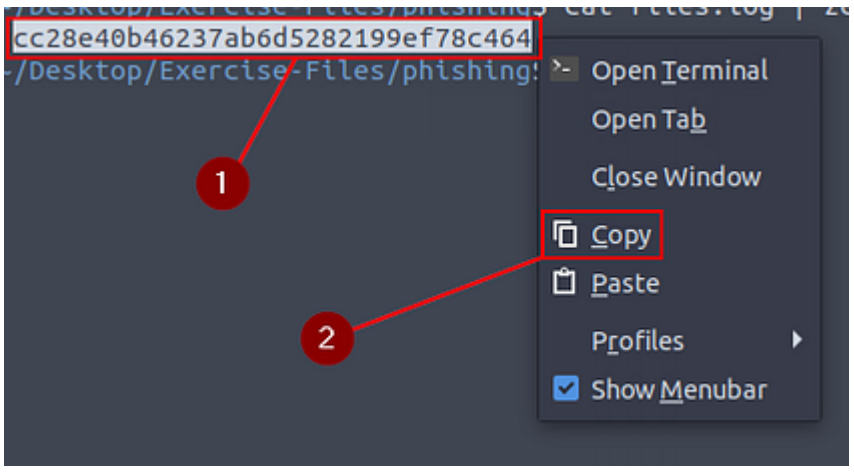
Answer: VBA

Investigate the extracted malicious .exe file. What is the given file name in Virustotal?

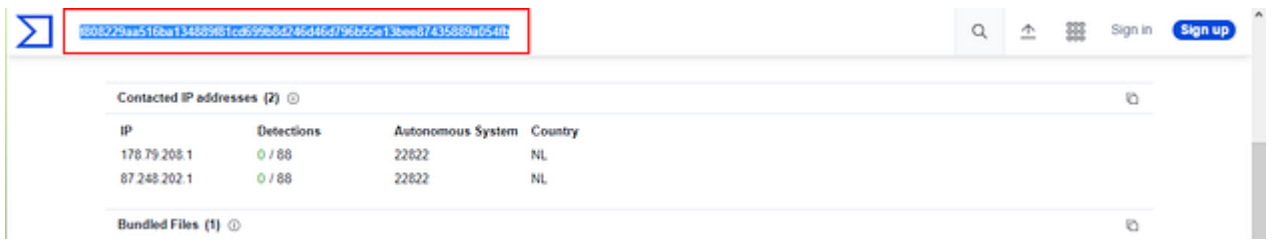
Head back to the terminal and leave VirusTotal open. Since we know the field to look at from the previous question, let's use zeek-cut and grep to get hash for the exe file. The command being `cat files.log | zeek-cut mime_type md5 | grep "exe"` , press enter to run the command.



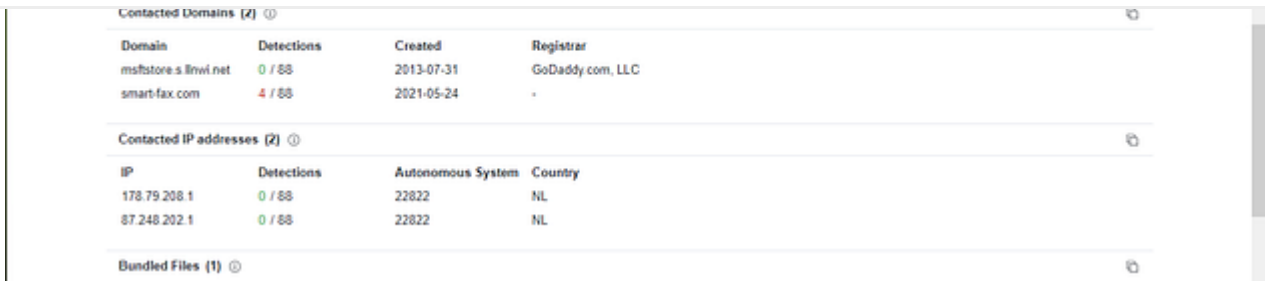
Highlight the hash, right-click on the highlighted hash, then click Copy on the drop-down menu.



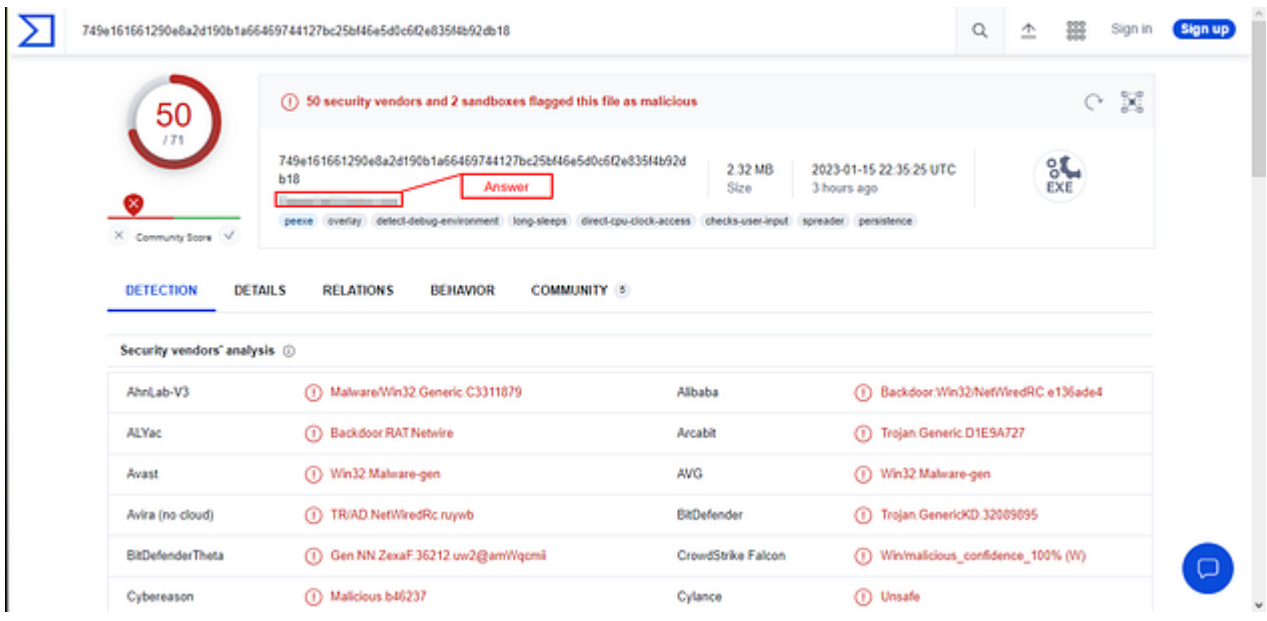
Back at VirusTotal highlight the hash at the top of the page, and press the delete key to remove it from the search field.



Use the keyboard shortcut ctrl + v to paste the new hash into the search field, then press enter to search it.



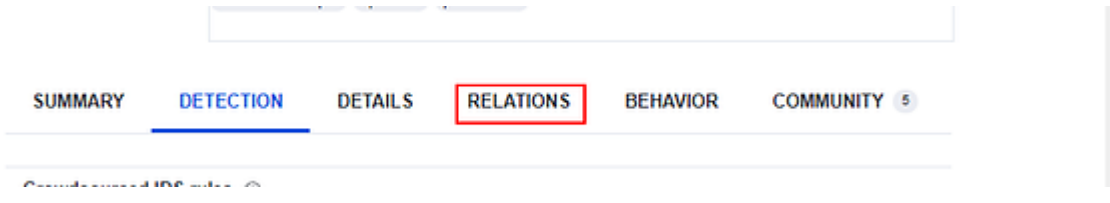
Once the DETECTION tab loads, you can see this is malicious. At the top is a box that has some general information about the file. Inside this box, under the hash, you will see the name of the file, and thus the answer to the question. Highlight copy (ctrl + c) and paste (ctrl + v) or type, the answer into the TryHackMe answer field, then click submit.



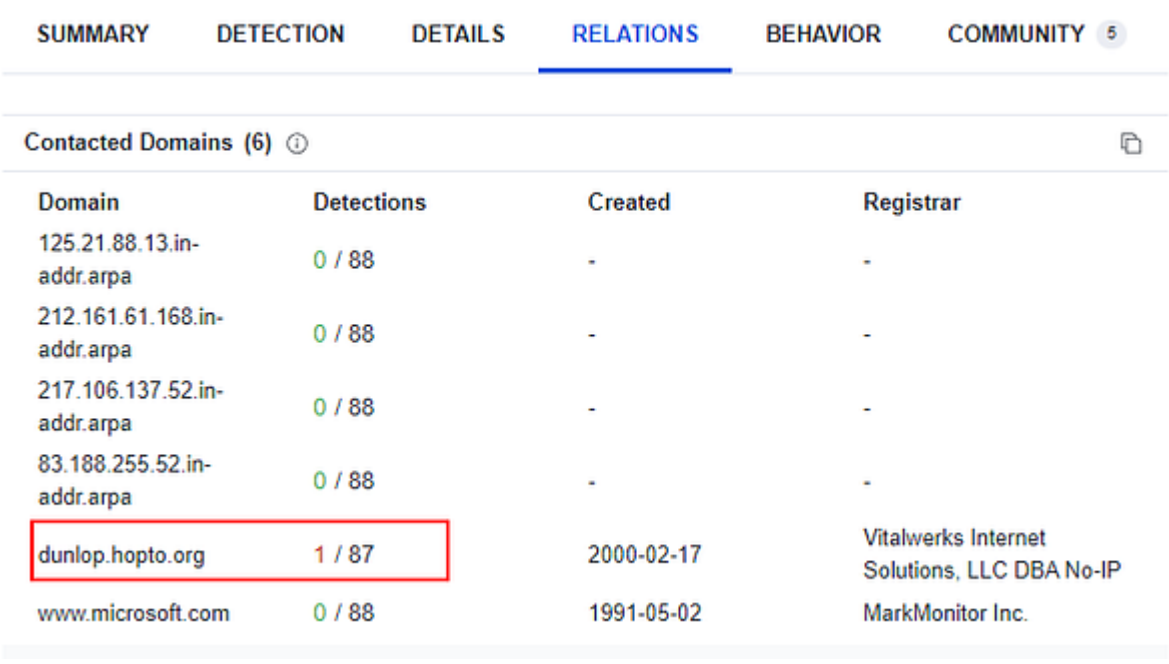
Answer: PleaseWaitWindow.exe

Investigate the malicious **.exe** file in VirusTotal. What is the contacted domain name? Enter your answer in **defanged format**.

Go back to VirusTotal, you already have the exe file hash searched in VirusTotal so we just need to do a little looking for the answer to this question. Once back on VirusTotal, click the RELATIONS tab.

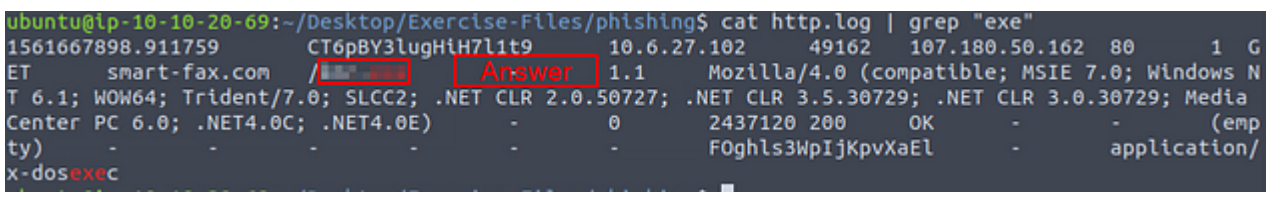


The first section is Contacted Domains, there is one that has a detection. You don't need the full domain for the answer, just every after dunlop.. You can type the answer in and defange it yourself or use the command `echo hopto.org | sed -e 's/\./[.]/g'` , and press enter to run. Highlight copy (ctrl + c) and paste (ctrl + v) from the VM or type, the answer into the TryHackMe answer field, then click submit.



Answer:hopto[.]org

Head back to your terminal in the VM, use the command `cat http.log | grep "exe"` , you will see the name of the malicious file. Type the answer into the TryHackMe answer field, then click submit.



Answer: knr.exe

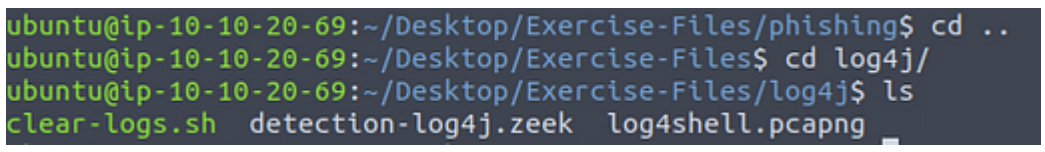
Task 4 Log4J

An alert triggered: “Log4J Exploitation Attempt”.

The case was assigned to you. Inspect the PCAP and retrieve the artefacts to confirm this alert is a true positive.

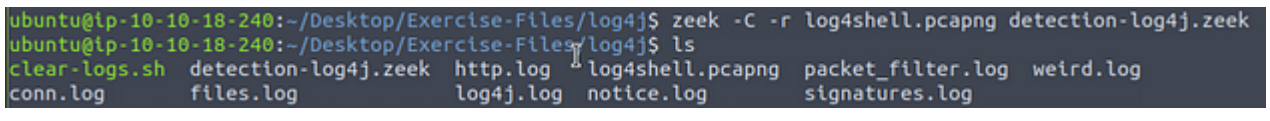
Answer the questions below

First we need to move from the phishing directory to the log4j directory. Use the command `cd ..` , to back out of the current directory. Then using the command `cd log4j/` , to move forward into the log4j directory. Finally, use the command `ls` to list the content of the current directory.



Investigate the **log4shell.pcapng file** with **detection-log4j.zeek** script. Investigate the **signature.log** file. What is the number of signature hits?

Start by using the command `zeek -C -r log4shell.pcapng detection-log4j.zeek` , press enter to run. Then use the command `ls` to see the contents of the current directory.

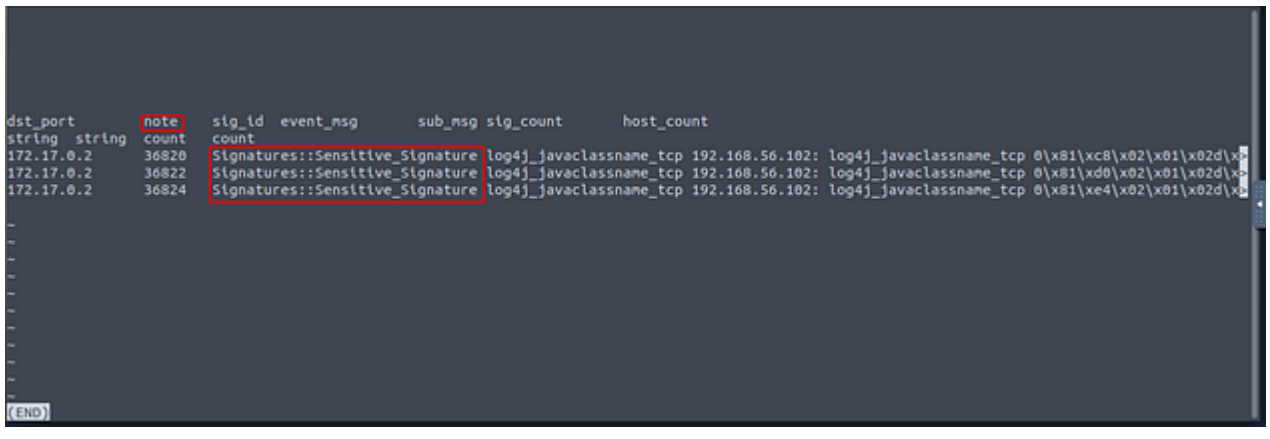


Now let’s cat the signatures log file and pipe it through less to see if we can find the answer.

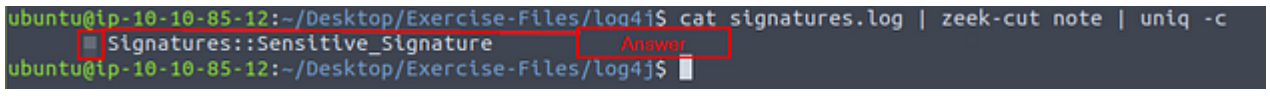
Once less opens the signatures log file, press the right arrow key once.

If you count the number of Signatures here in the note field you will get your answer. But I will show you the command line way of finding it.

Press `q` to exit less.



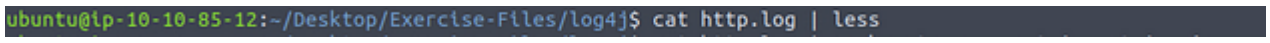
Back in the terminal, we want to use the command `cat signatures.log | zeek-cut note | uniq -c` , press enter after you were done typing the command. After you have run the command you will have the answer in the output of the terminal, type it into the TryHackMe answer field, then click submit.



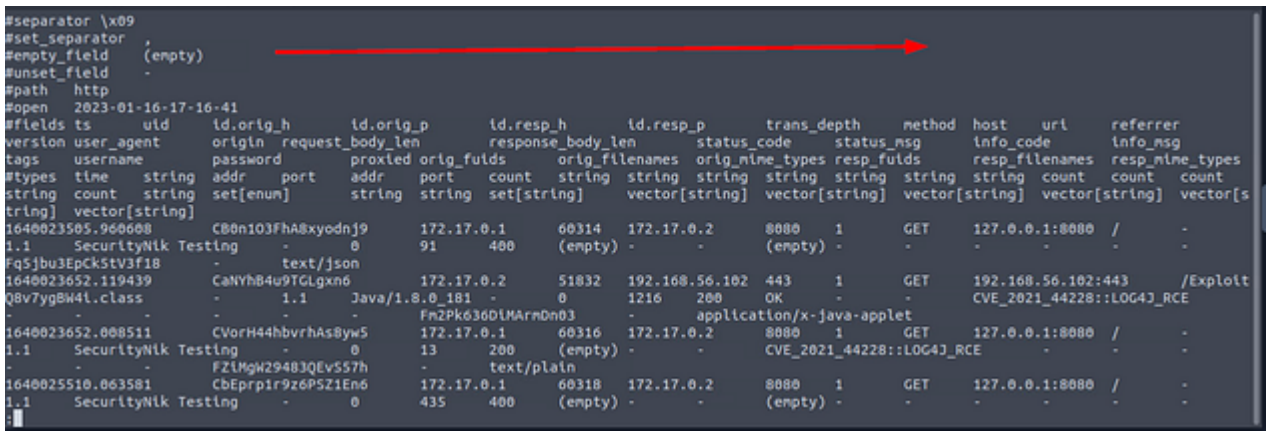
Answer: 3

Investigate the **http.log** file. Which tool is used for scanning?

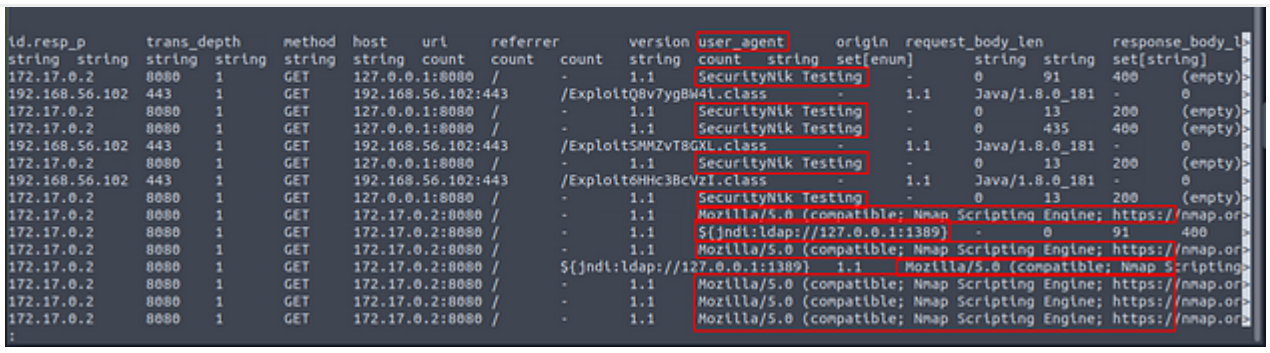
Now let's cat the http log file and pipe it through less to see if we can find the answer.



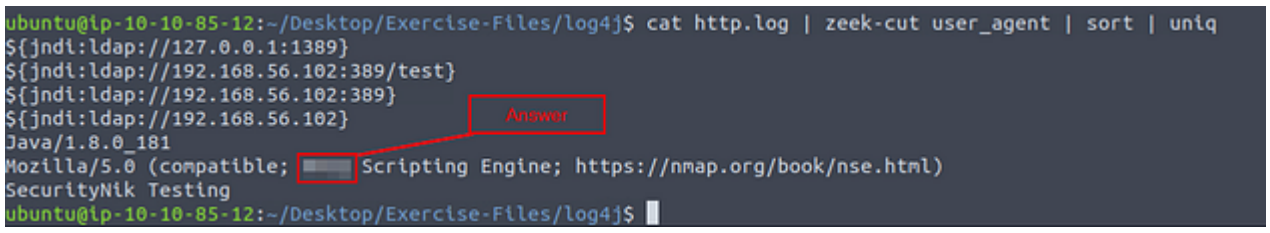
Once less opens the http log file, press the right arrow key once.



As we look through the user_agent field we can see some interesting information, so the field we are looking for is user_agent. Time to use some zeek-cut, so press `q` to exit less



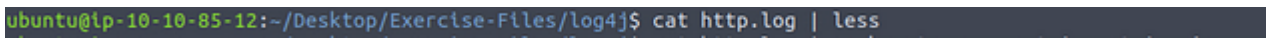
Knowing the field we want to look at let's run zeek-cut, sort, and uniq. The command being `cat http.log | zeek-cut user_agent | sort | uniq` , after you have finished typing out the command press enter. We use zeek-cut to "cut" that field out to look at, taking the results for zeek-cut we pipe it through sort. With sort, the results are sorted alphabetically, those results are then piped through uniq. Finally uniq will remove any dupilcates. After the command is finished running, look through the output you should be able to notice a famous network mapping program (wink wink). Once you find it, type the answer into the TryHackMe answer field, and click submit.



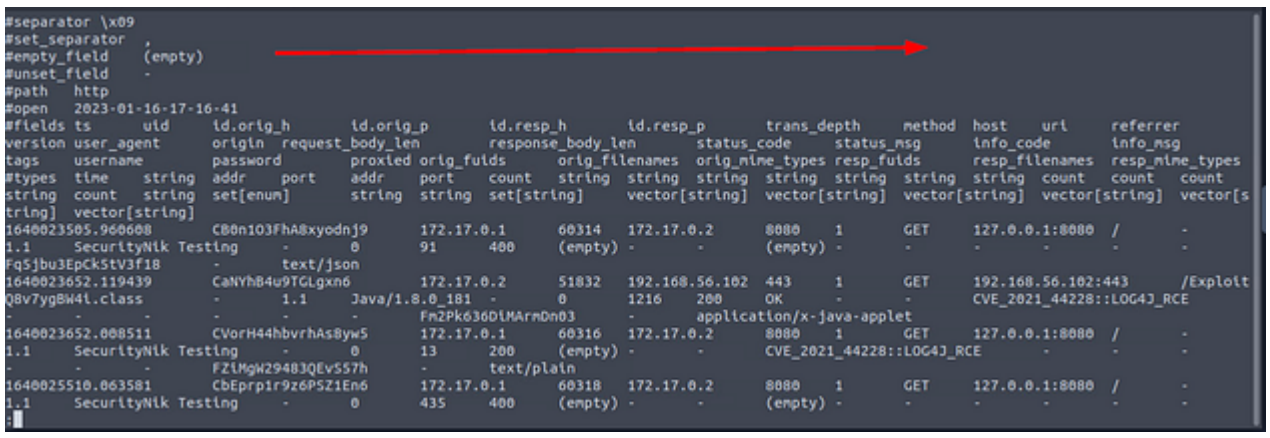
Answer: Nmap

Investigate the **http.log** file. What is the extension of the exploit file?

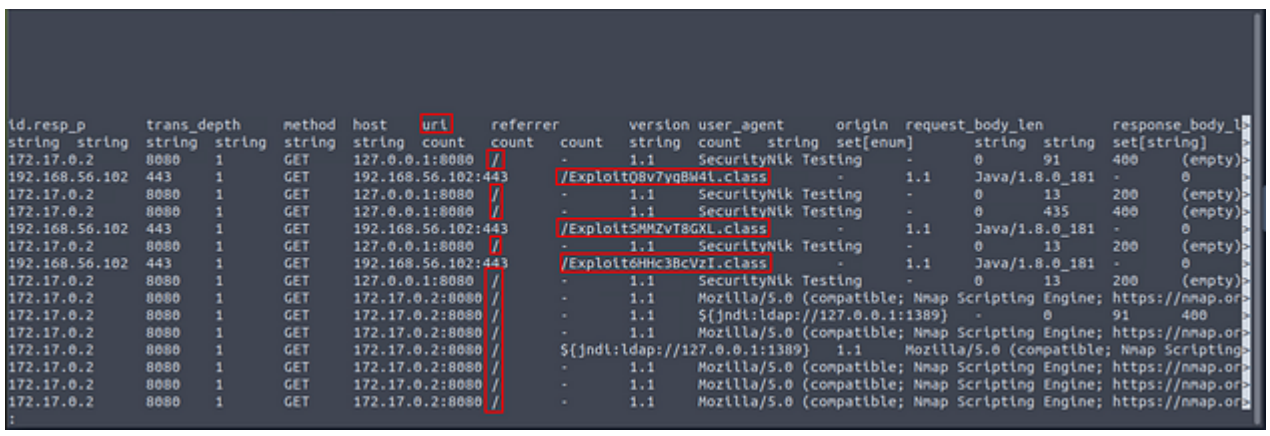
Now let's cat the http log file and pipe it through less to see if we can find the answer.



Once less opens the http log file, press the right arrow key once.

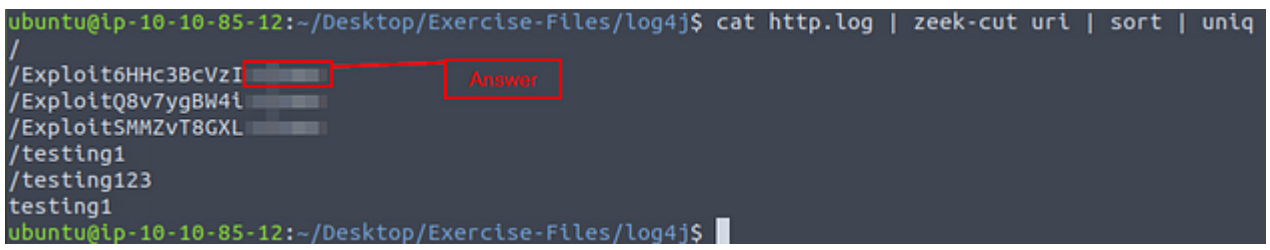


As we look through the user_agent field we can see some interesting information, so the field we are looking for is uri. Time to use some zeek-cut, so press `q` to exit less



Knowing the field we want to look at let's run zeek-cut, sort, and uniq. The command being `cat http.log | zeek-cut uri | sort | uniq` , after you have finished typing out the command press enter. We use zeek-cut to "cut" that field out to look at, taking the results for zeek-cut we pipe it through sort. With sort, the results are sorted alphabetically, those results are then piped through uniq. Finally uniq will remove

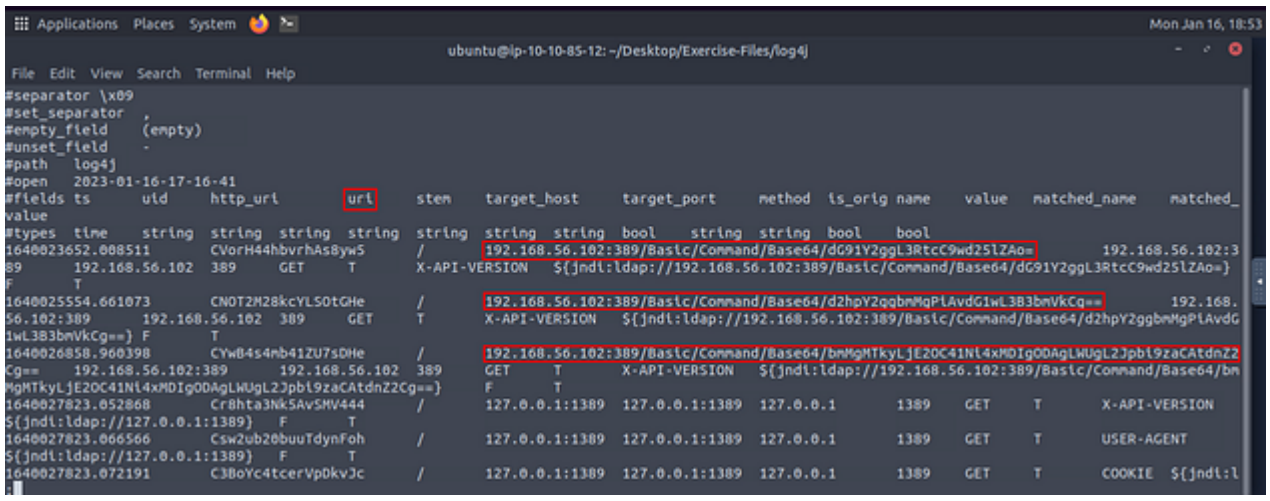
answer. Once you find it, type the answer into the TryHackMe answer field, and click submit.



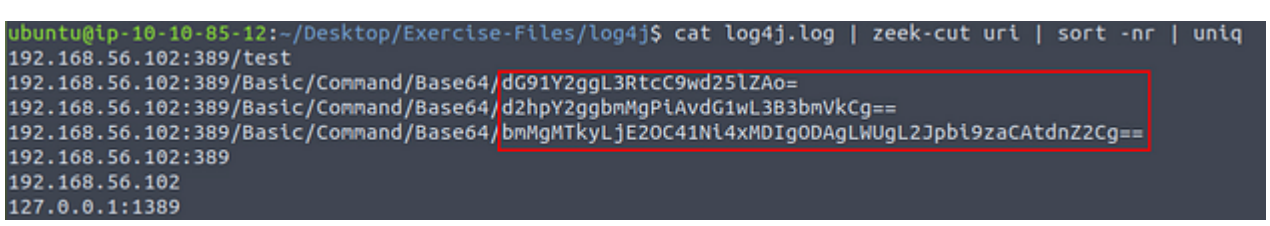
Answer: .class

Investigate the **log4j.log** file. Decode the base64 commands. What is the name of the created file?

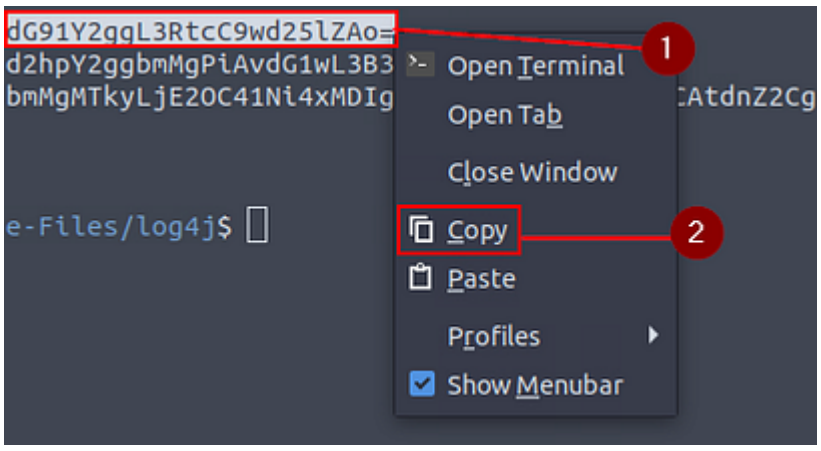
Now let's cat the log4j log file and pipe it through less to see if we can find the answer. Once the log4j file opens in less, looking through the fields along with the field contents we can see some of the base64 we need to decode. Time to use some command line kung-fu to help slim down the results.



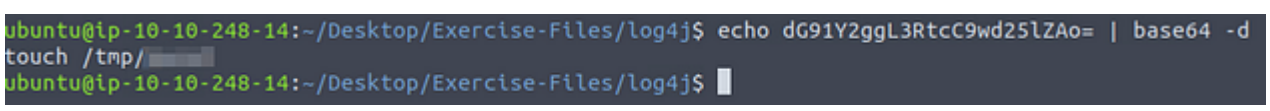
Time for the command line kung-fu, the command we want to run is `cat log4j.log | zeek-cut uri | sort -nr | uniq` , after you have done typing the command out press enter to run it. You will see three base64 codes in the output. Next we will be decoding them.



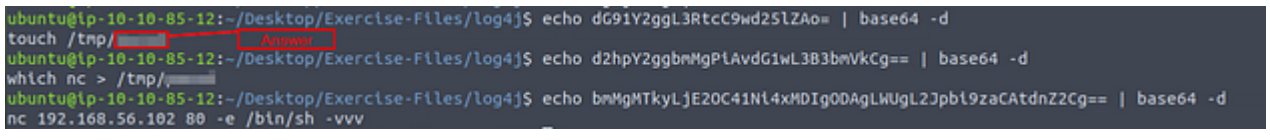
To decode all three the take the same steps to reach. First step is to highlight the base64 code, then right-click on it. On the drop-down menu click copy.



Then type `echo` into the terminal, using the paste shortcut for linux terminal, ctrl + shift + v, paste the base64 code into the terminal. Then pipe it to `base64 -d` , this command will take a base64 code and decode it. So the command is `echo {base64 code} | base64 -d` , press enter to run the code.



type the answer into the TryHackMe answer field, and click submit.



Answer: pwned

Task 5 Conclusion

Congratulations! You just finished the Zeek exercises.

If you like this content, make sure you visit the following rooms later on THM;

- **Snort**
- **Snort Challenges 1**
- **Snort Challenges 2**
- **Wireshark**
- **NetworkMiner**

Note that there are challenge rooms available for the discussed content. Use the search option to find them! Happy hacking!

🎉 🎉 🎉 CONGRATS!!! You have completed the Zeek Exercises Room!!! 🎉 🎉 🎉

Zeek-Exercises

TryHackMe, Zeek, SOC Level One Path

Share:

Further Reading

Jan 9, 2023

TryHackMe Zeek — Task 1 Introduction, Task 2 Network Security Monitoring and Zeek, & Task 3 Zeek Logs

Task 1 Introduction Introduction to hands-on network monitoring and threat detection wi…

Jan 10, 2023

TryHackMe Zeek — Task 4 CLI Kung-Fu Recall: Processing Zeek Logs, Task 5 Zeek Signatures, & Task 6 Zeek Scripts | Fundamentals

If you haven't done task 1, 2, & 3 yet, here is the link to my write-up of it: Task 1…

Jan 11, 2023

TryHackMe Zeek — Task 7 Zeek Scripts | Scripts and Signatures, Task 8 Zeek Scripts | Frameworks, Task 9 Zeek Scripts | Packages, & Task 10 Conclusion

If you haven't done task 4, 5, & 6 yet, here is the link to my write-up of it: Task 4 C…

OLDER

TryHackMe Zeek Exercises — Task 1 Introduction & Task 2 Anomalous DNS

NEWER

TryHackMe Brim — Task 1 Introduction, Task 2 What is Brim?, & Task 3 The Basics