Modul_27_2_12_Interpret_HTTP_and_DNS_Data_to_Isolate_Threat_Actor

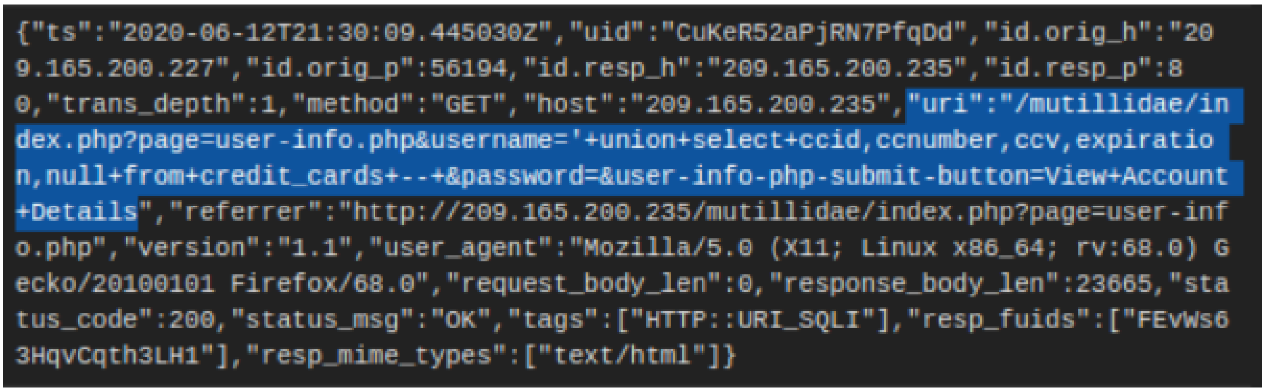
Part 1: Investigate an SQL Injection Attack

Step 2: Filter for HTTP traffic.

a)
Scroll through the results and answer the following questions:
What is the source IP address?

- 209.165.200.227
  What is the destination IP address?
- 209.165.200.235
  What is the destination port number?
- HTTP takže 80

c)
What is the timestamp of the first result?

- JUne 12th 2020, 21:30:09.445
  What is the event type?
- bro_http
  What is included in the message field? These are details about the HTTP GET request that was made by the client to the server. Focus especially on the uri field in the message text.
- 

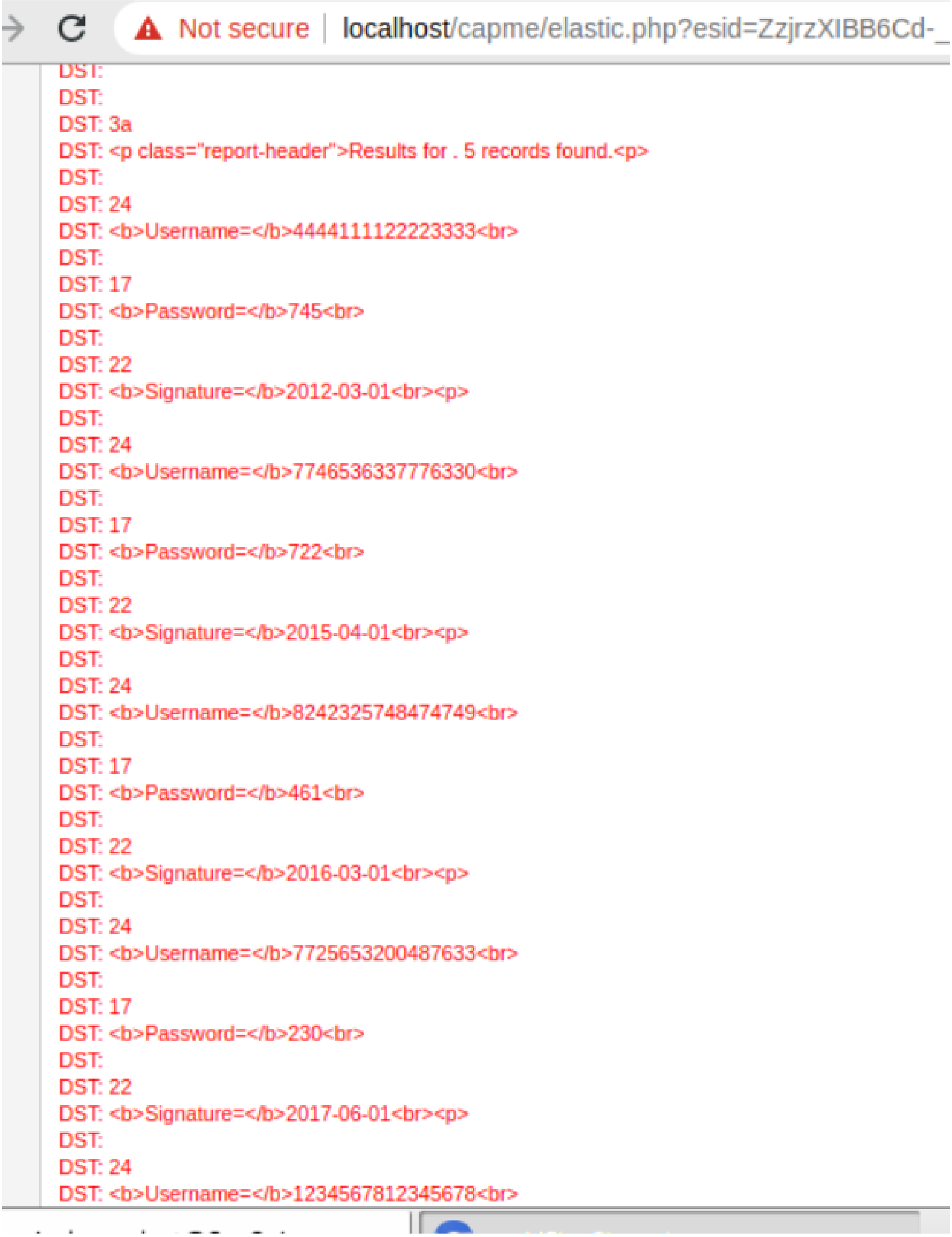
```
{"ts":"2020-06-12T21:30:09.445030Z","uid":"CuKeR52aPjRN7PfqDd","id.orig_h":"20
9.165.200.227","id.orig_p":56194,"id.resp_h":"209.165.200.235","id.resp_p":8
0,"trans_depth":1,"method":"GET","host":"209.165.200.235","uri":"/mutillidae/in
dex.php?page=user-info.php&username='+union+select+ccid,ccnumber,ccv,expiratio
n,null+from+credit_cards+--+&password=&user-info-php-submit-button=View+Account
+Details","referrer":"http://209.165.200.235/mutillidae/index.php?page=user-inf
o.php","version":"1.1","user_agent":"Mozilla/5.0 (X11; Linux x86_64; rv:68.0) G
ecko/20100101 Firefox/68.0","request_body_len":0,"response_body_len":23665,"sta
tus_code":200,"status_msg":"OK","tags":["HTTP::URI_SQLI"],"resp_fuids":["FEvWs6
3HqvCqth3LH1"],"resp_mime_types":["text/html"]}
```

- username, cc id, cc number, cc v (? version) z credit cards... a nakonec i heslo
  What is the significance of this information?
- prakticky krádež kreditních karet

Step 3: Review the results.

d)

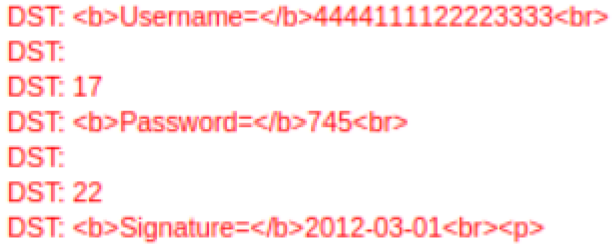
What do you see later in the transcript as regards usernames?



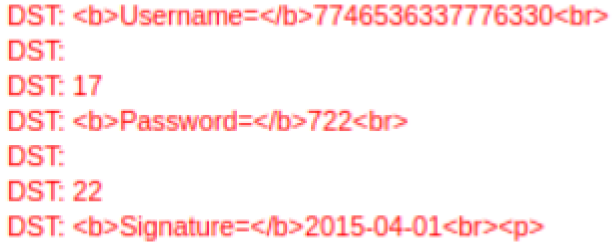
```
DST:
DST:
DST: 3a
DST: <p class="report-header">Results for . 5 records found.<p>
DST:
DST: 24
DST: <b>Username=</b>4444111122223333<br>
DST:
DST: 17
DST: <b>Password=</b>745<br>
DST:
DST: 22
DST: <b>Signature=</b>2012-03-01<br><p>
DST:
DST: 24
DST: <b>Username=</b>7746536337776330<br>
DST:
DST: 17
DST: <b>Password=</b>722<br>
DST:
DST: 22
DST: <b>Signature=</b>2015-04-01<br><p>
DST:
DST: 24
DST: <b>Username=</b>8242325748474749<br>
DST:
DST: 17
DST: <b>Password=</b>461<br>
DST:
DST: 22
DST: <b>Signature=</b>2016-03-01<br><p>
DST:
DST: 24
DST: <b>Username=</b>7725653200487633<br>
DST:
DST: 17
DST: <b>Password=</b>230<br>
DST:
DST: 22
DST: <b>Signature=</b>2017-06-01<br><p>
DST:
DST: 24
DST: <b>Username=</b>1234567812345678<br>
```

uživatelské jména a hesla k nim

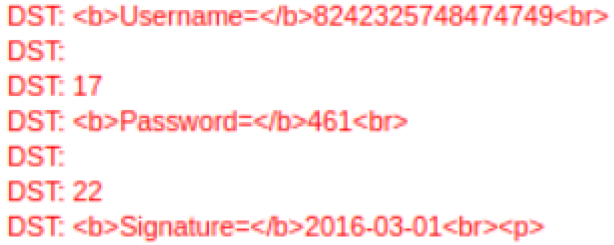
Give some examples of a username, password, and signature that was exfiltrated

- 

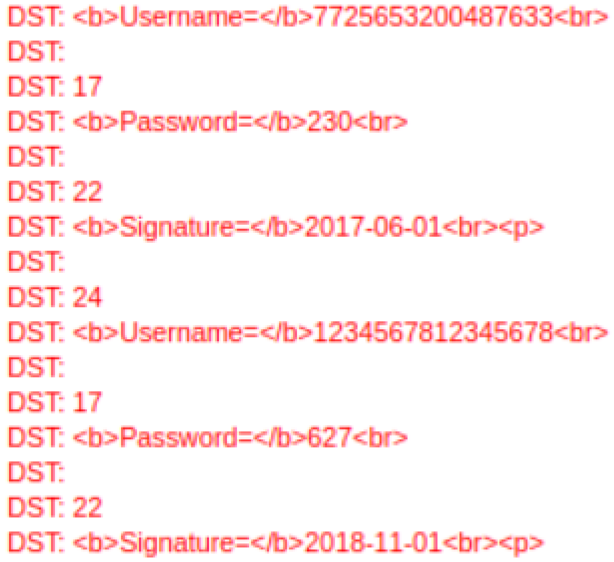
  ```
  DST: <b>Username=</b>4444111122223333<br>
  DST:
  DST: 17
  DST: <b>Password=</b>745<br>
  DST:
  DST: 22
  DST: <b>Signature=</b>2012-03-01<br><p>
  ```

- 

  ```
  DST: <b>Username=</b>7746536337776330<br>
  DST:
  DST: 17
  DST: <b>Password=</b>722<br>
  DST:
  DST: 22
  DST: <b>Signature=</b>2015-04-01<br><p>
  ```

- 

  ```
  DST: <b>Username=</b>8242325748474749<br>
  DST:
  DST: 17
  DST: <b>Password=</b>461<br>
  DST:
  DST: 22
  DST: <b>Signature=</b>2016-03-01<br><p>
  ```

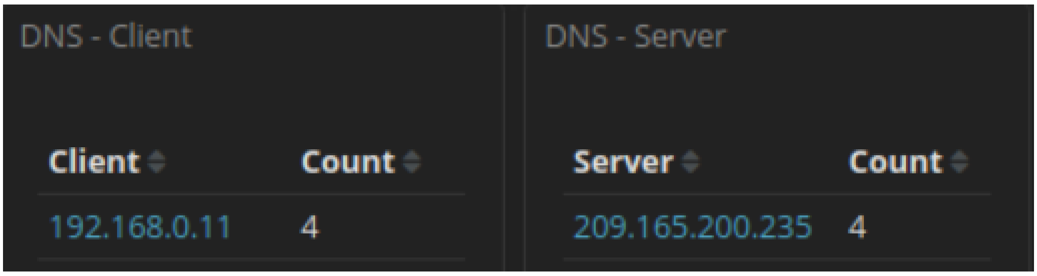
- 

  ```
  DST: <b>Username=</b>7725653200487633<br>
  DST:
  DST: 17
  DST: <b>Password=</b>230<br>
  DST:
  DST: 22
  DST: <b>Signature=</b>2017-06-01<br><p>
  DST:
  DST: 24
  DST: <b>Username=</b>1234567812345678<br>
  DST:
  DST: 17
  DST: <b>Password=</b>627<br>
  DST:
  DST: 22
  DST: <b>Signature=</b>2018-11-01<br><p>
  ```

Part 2: Analyze DNS exfiltration.

Step 2: Review the DNS-related entries.

e)Locate information about the DNS - Client and DNS - Server. Record the IP addresses of DNS client and server.



DNS - Client

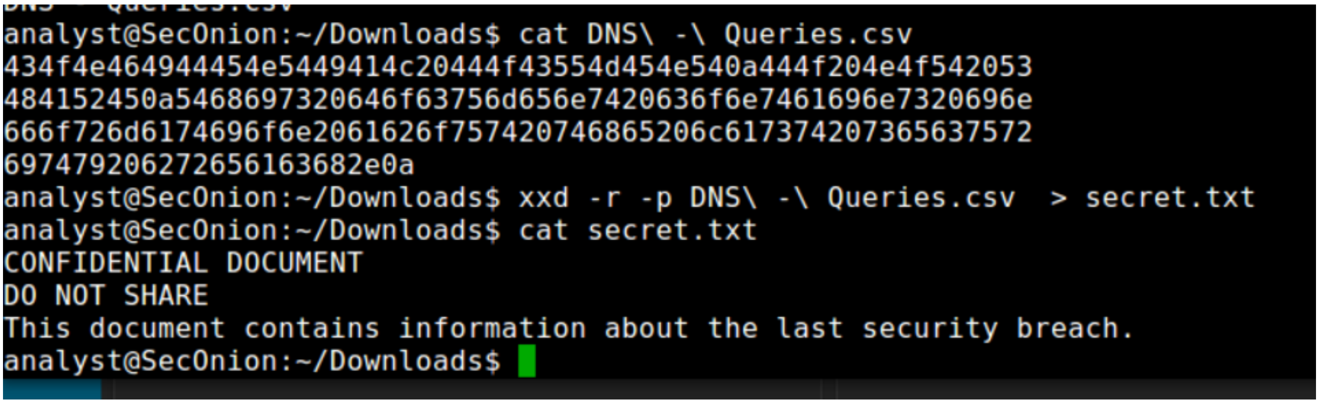
Client	Count
192.168.0.11	4

DNS - Server

Server	Count
209.165.200.235	4

Step 3: Determine the exfiltrated data.

c)



```
DNS - Queries.csv
analyst@SecOnion:~/Downloads$ cat DNS\ -\ Queries.csv
434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053
484152450a5468697320646f63756d656e7420636f6e7461696e7320696e
666f726d6174696f6e2061626f757420746865206c617374207365637572
697479206272656163682e0a
analyst@SecOnion:~/Downloads$ xxd -r -p DNS\ -\ Queries.csv  > secret.txt
analyst@SecOnion:~/Downloads$ cat secret.txt
CONFIDENTIAL DOCUMENT
DO NOT SHARE
This document contains information about the last security breach.
analyst@SecOnion:~/Downloads$ 
```

Were the subdomains from the DNS queries subdomains? If not, what is the text?

- CONFIDENTIAL DOCUMENT
- DO NOT SHARE
- This document contains information about the last security breach.

What does this result imply about these particular DNS requests? What is the larger significance?

- exfiltrace dat byla úspěšná a máme další security breach :) (dokud se to nevyřeší další threat actoři mohou exfiltrovat další data) (plus musí se ohlížet také na to, že data byla rozkouskována předtím, než byla poslána zpět útočníkovy)

What may have created these encoded DNS queries and why was DNS selected as the means to exfiltrate data?

- Jelikož DNS provoz je normální, může se použít na utajení nějaké komunikace stejně jako s HTTP provozem atd.
- Proč jsou vytvořeny -> může být nějaký virus či komplexní útok na nějakou zranitelnost hosta