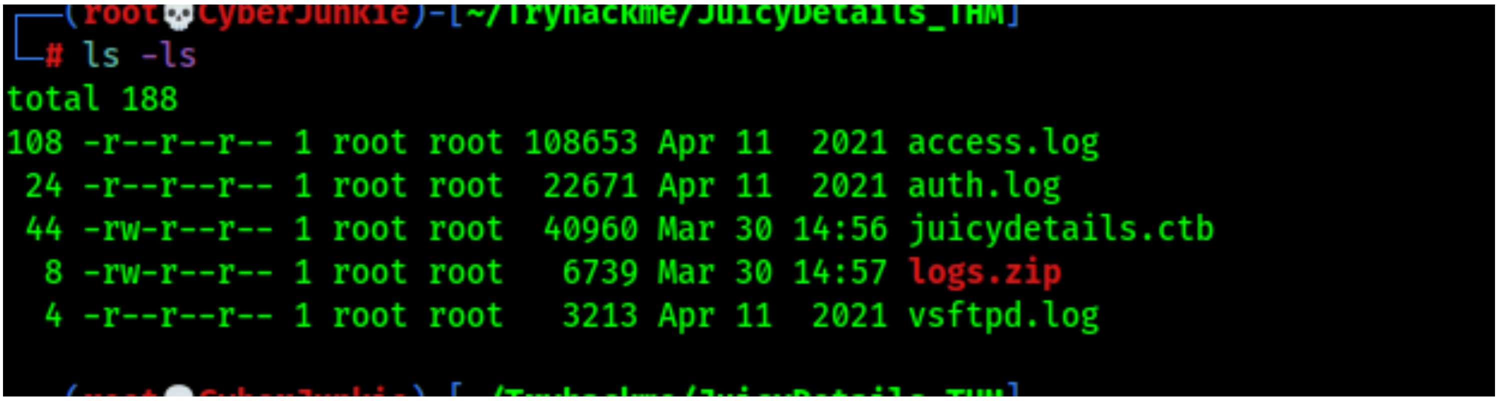
JuicyDEtails

Task 2

# we download the zip file

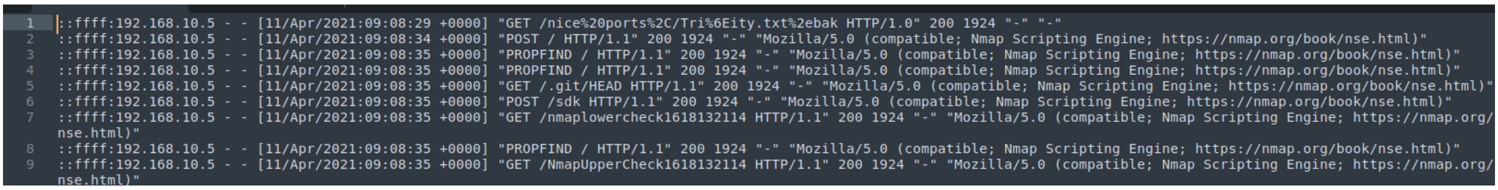
we have following logs from the incident



```
┌──(root💀CyberJunkie)-[~/Tryhackme/JuicyDetails_THM]
└─# ls -ls
total 188
108 -r--r--r-- 1 root root 108653 Apr 11  2021 access.log
 24 -r--r--r-- 1 root root  22671 Apr 11  2021 auth.log
 44 -rw-r--r-- 1 root root  40960 Mar 30 14:56 juicydetails.ctb
  8 -rw-r--r-- 1 root root   6739 Mar 30 14:57 logs.zip
  4 -r--r--r-- 1 root root   3213 Apr 11  2021 vsftpd.log
```

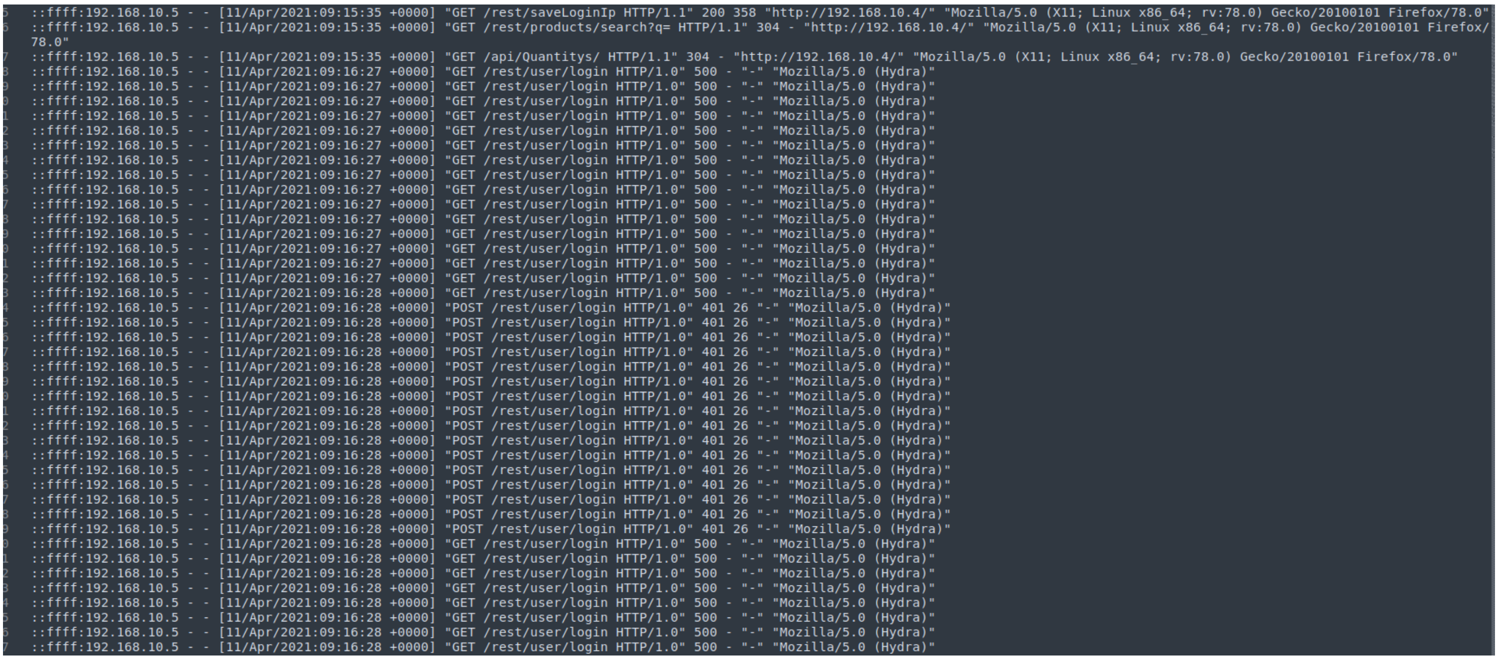
# second question is to find the tools used by the attacker. auth logs relate to authentication process and vsftpd logs are only for ftp. we analyze access logs which shows the logs used in initial stage of cyber kill chain

we first see the nmap scripting engine in the user agent header



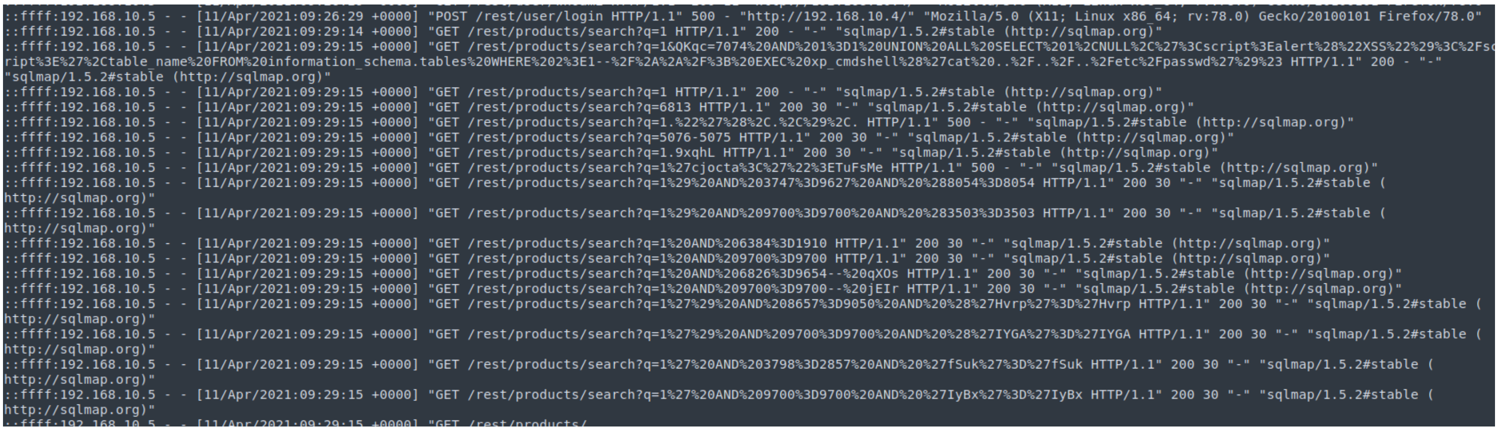
```
::ffff:192.168.10.5 - - [11/Apr/2021:09:08:29 +0000] "GET /nice%20ports%2C/Tri%6Eity.txt%2ebak HTTP/1.0" 200 1924 "-" "-"
::ffff:192.168.10.5 - - [11/Apr/2021:09:08:34 +0000] "POST / HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:08:35 +0000] "PROPFIND / HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:08:35 +0000] "PROPFIND / HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:08:35 +0000] "GET /.git/HEAD HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:08:35 +0000] "POST /sdk HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:08:35 +0000] "GET /nmaplowercheck1618132114 HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/
nse.html)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:08:35 +0000] "PROPFIND / HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:08:35 +0000] "GET /NmapUpperCheck1618132114 HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/
nse.html)"
```

second tool we spot is hydra . It looks like a bruteforce attempt in login form of targeted web application



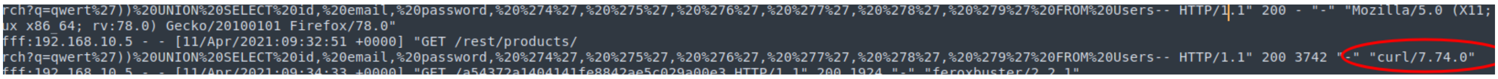
```
::ffff:192.168.10.5 - - [11/Apr/2021:09:15:35 +0000] "GET /rest/saveLoginIp HTTP/1.1" 200 358 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
::ffff:192.168.10.5 - - [11/Apr/2021:09:15:35 +0000] "GET /rest/products/search?q= HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/
78.0"
::ffff:192.168.10.5 - - [11/Apr/2021:09:15:35 +0000] "GET /api/Quantitys/ HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:27 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:27 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:27 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:27 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:27 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:27 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:27 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:27 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:27 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:27 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:27 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:27 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:27 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:27 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:27 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:28 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
```

NExt tool we spot is sqlmap from the user agent header .The attacker is attempting sql injection on search parameter but lucky for us that sqlmap is a noisy tool so we have more visibility on what happened at that endpoint.



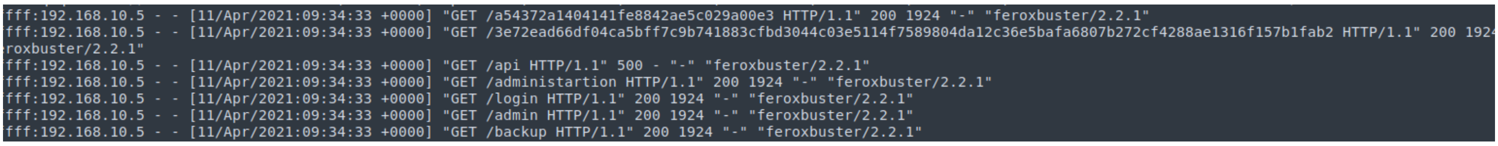
```
::ffff:192.168.10.5 - - [11/Apr/2021:09:26:29 +0000] "POST /rest/user/login HTTP/1.1" 500 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
::ffff:192.168.10.5 - - [11/Apr/2021:09:29:14 +0000] "GET /rest/products/search?q=1 HTTP/1.1" 200 - "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=1&QKqc=7074%20AND%201%3D1%20UNION%20ALL%20SELECT%201%2CNULL%2C%27%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fsc
ript%3E%27%2Ctable_name%20FROM%20information_schema.tables%20WHERE%202%3E1--%2F%2A%2A%2F%3B%20EXEC%20xp_cmdshell%28%27cat%20..%2F..%2F..%2Fetc%2Fpasswd%27%29%23 HTTP/1.1" 200 - "-"
"sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=1 HTTP/1.1" 200 - "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=6813 HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=1.%22%27%28%2C.%2C%29%2C. HTTP/1.1" 500 - "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=5076-5075 HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=1.9xqhL HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=1%27cjocta%3C%27%22%3ETuFsMe HTTP/1.1" 500 - "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=1%29%20AND%203747%3D9627%20AND%20%288054%3D8054 HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (
http://sqlmap.org)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=1%29%20AND%209700%3D9700%20AND%20%283503%3D3503 HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (
http://sqlmap.org)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=1%20AND%206384%3D1910 HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=1%20AND%209700%3D9700 HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=1%20AND%206826%3D9654--%20qXOs HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=1%20AND%209700%3D9700--%20jEIr HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=1%27%29%20AND%208657%3D9050%20AND%20%28%27Hvrp%27%3D%27Hvrp HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (
http://sqlmap.org)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=1%27%29%20AND%209700%3D9700%20AND%20%28%27IYGA%27%3D%27IYGA HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (
http://sqlmap.org)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=1%27%20AND%203798%3D2857%20AND%20%27fSuk%27%3D%27fSuk HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (
http://sqlmap.org)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/search?q=1%27%20AND%209700%3D9700%20AND%20%27IyBx%27%3D%27IyBx HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (
http://sqlmap.org)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:29:15 +0000] "GET /rest/products/
```

next utility we spot is curl ,seems like the attacker used curl to see the response of an endpoint quickly. most probably for seeing the http headers.



```
rch?q=qwert%27))%20UNION%20SELECT%20id,%20email,%20password,%20%274%27,%20%275%27,%20%276%27,%20%277%27,%20%278%27,%20%279%27%20FROM%20Users-- HTTP/1.1" 200 - "-" "Mozilla/5.0 (X11;
ux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
fff:192.168.10.5 - - [11/Apr/2021:09:32:51 +0000] "GET /rest/products/
rch?q=qwert%27))%20UNION%20SELECT%20id,%20email,%20password,%20%274%27,%20%275%27,%20%276%27,%20%277%27,%20%278%27,%20%279%27%20FROM%20Users-- HTTP/1.1" 200 3742 "-" "curl/7.74.0"
fff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /a54372a1404141fe8842ae5c029a00e3 HTTP/1.1" 200 1924 "-" "feroxbuster/2.2.1"
```

the last tool used was feroxbuster for discovering web contents.The attacker tried to find hidden content using directory busting

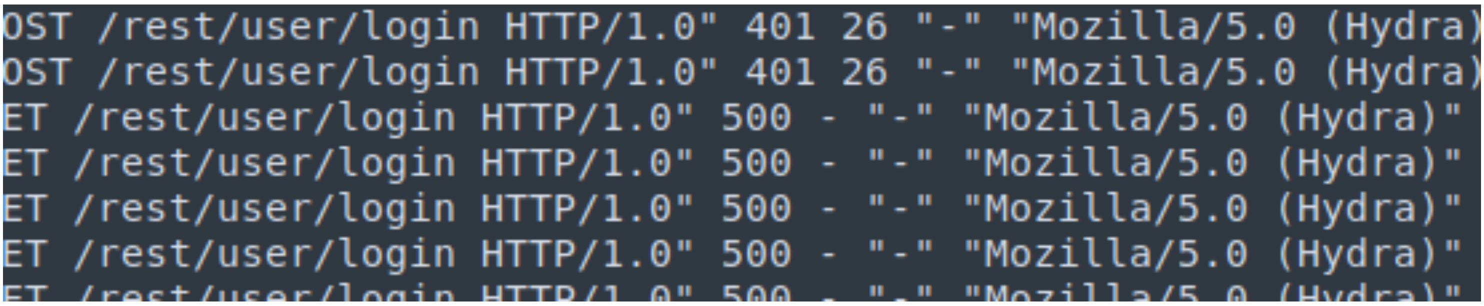


```
fff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /a54372a1404141fe8842ae5c029a00e3 HTTP/1.1" 200 1924 "-" "feroxbuster/2.2.1"
fff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /3e72ead66df04ca5bff7c9b741883cfbd3044c03e5114f7589804da12c36e5bafa6807b272cf4288ae1316f157b1fab2 HTTP/1.1" 200 1924
roxbuster/2.2.1"
fff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /api HTTP/1.1" 500 - "-" "feroxbuster/2.2.1"
fff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /administartion HTTP/1.1" 200 1924 "-" "feroxbuster/2.2.1"
fff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /login HTTP/1.1" 200 1924 "-" "feroxbuster/2.2.1"
fff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /admin HTTP/1.1" 200 1924 "-" "feroxbuster/2.2.1"
fff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /backup HTTP/1.1" 200 1924 "-" "feroxbuster/2.2.1"
```

Q2

Next question was figuring out the endpoint vulnerable to a brute force attack .

We discovered usage of hydra which is a bruteforce tool so we see the endpoint where the hydra requests were send



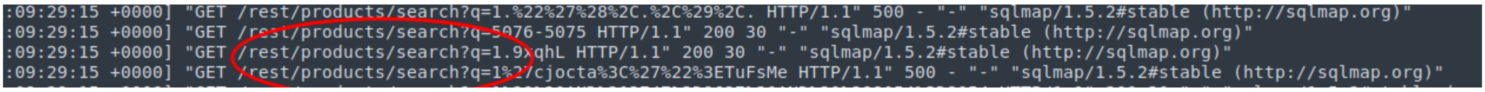
```
OST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)
OST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)
ET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
ET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
ET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
ET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
ET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
```

the answer is /rest/user/login

Q3

endpoint vulnerable to sqli attack

we saw sqlmap headers to different urls so lets figure out the vulnerable endpoint



```
:09:29:15 +0000] "GET /rest/products/search?q=1.%22%27%28%2C.%2C%29%2C. HTTP/1.1" 500 - "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
:09:29:15 +0000] "GET /rest/products/search?q=5076-5075 HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
:09:29:15 +0000] "GET /rest/products/search?q=1.9xqhL HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
:09:29:15 +0000] "GET /rest/products/search?q=1%27cjocta%3C%27%22%3ETuFsMe HTTP/1.1" 500 - "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
```

the vulnerable endpoint is /rest/products/search

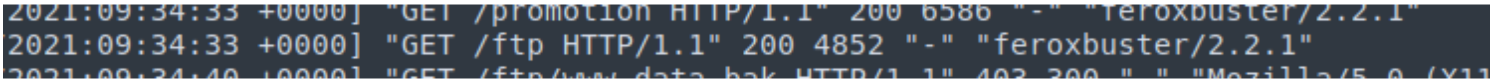
Q4

Parameter name is q

Q5 endpoint used to retrieve files

we know that ftp was also active on the attacked machine because we received ftp logs tooo. So it turns out that the ftp server was also served under web rooot so technically one can try to access ftp files web.The attacker discovered this information during the discovery stage of kill chain ,using feroxbuster

we can see the status code of 200 indicating that ftp is under webroot



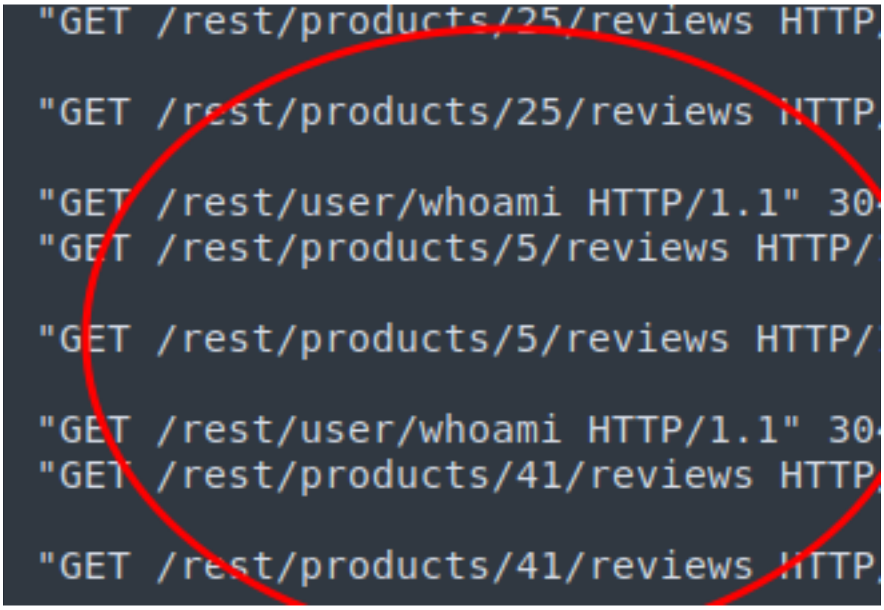
```
2021:09:34:33 +0000] "GET /promotion HTTP/1.1" 200 6586 "-" "feroxbuster/2.2.1"
[2021:09:34:33 +0000] "GET /ftp HTTP/1.1" 200 4852 "-" "feroxbuster/2.2.1"
2021:09:34:40 +0000] "GET /ftp/www-data.bak HTTP/1.1" 403 300 "-" "Mozilla/5.0 (X11
```

so this is our answer /ftp

TASK 3

Q1 email were scraped where?

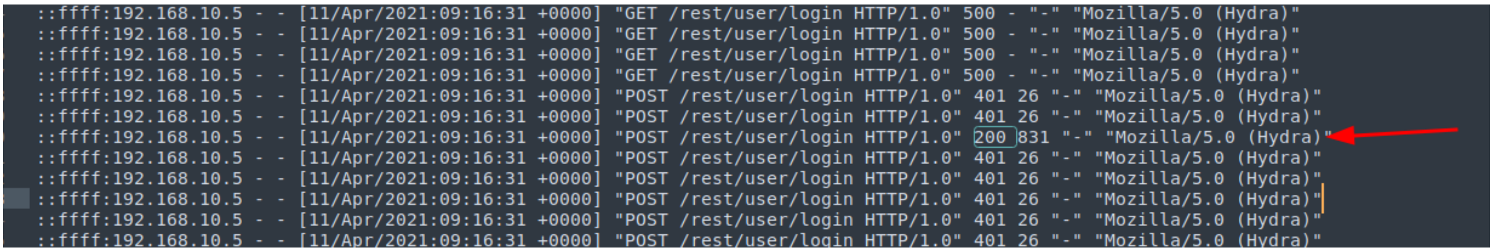
so from web logs we can deduce that the website which was attack was a e-buisness website due to endpoints like products etc.
so logically we can either enumerate users email by directly dumping the database or by enumerating the products reviews section. we even find an endpoint of /reviews under products dir. we can see the number represents the product id and reviews of user



```
"GET /rest/products/25/reviews HTTP

"GET /rest/products/25/reviews HTTP

"GET /rest/user/whoami HTTP/1.1" 30
"GET /rest/products/5/reviews HTTP/

"GET /rest/products/5/reviews HTTP/

"GET /rest/user/whoami HTTP/1.1" 30
"GET /rest/products/41/reviews HTTP

"GET /rest/products/41/reviews HTTP
```

so the answer is product reviews

Q2 we have to identify that whether a bruteforce was successful or not and if yes what was the time of incident we analyze the access logs for a sucessful bruteforce attack. We know that hydra was used so we search for a 200 or 301 http response code which usually indicates a succesful login. we see a successful login which is a IOC.

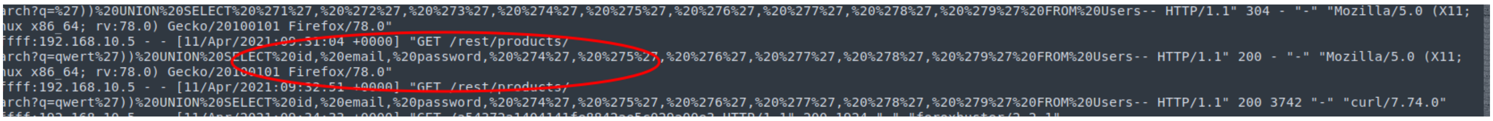


```
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "POST /rest/user/login HTTP/1.0" 200 831 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
::ffff:192.168.10.5 - - [11/Apr/2021:09:16:31 +0000] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
```

timestamp is

Q3

This question asks what information attacker gains from sqli attack so we revisit the sqlmap portion of logs .
we can see the email and password in sqli payload section.



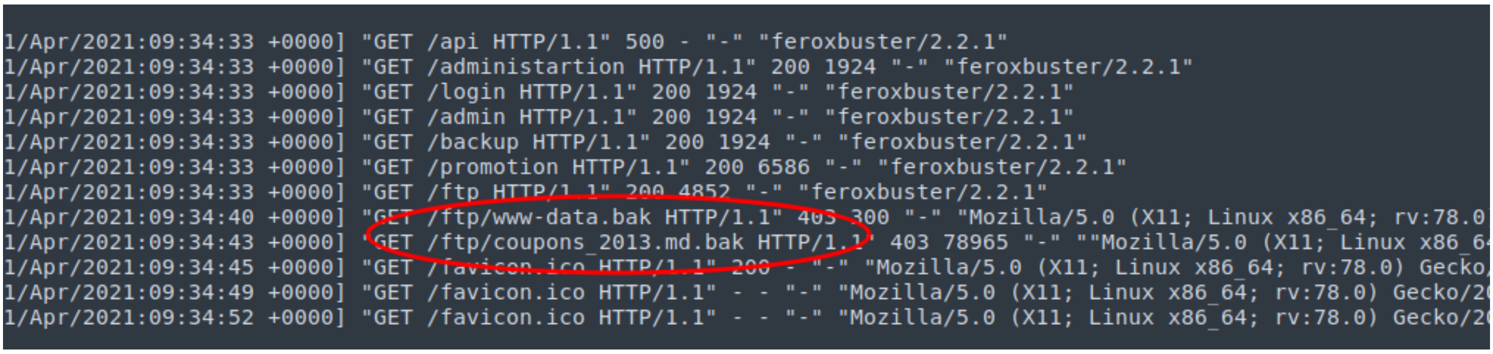
```
arch?q=%27))%20UNION%20SELECT%20%271%27,%20%272%27,%20%273%27,%20%274%27,%20%275%27,%20%276%27,%20%277%27,%20%278%27,%20%279%27%20FROM%20Users-- HTTP/1.1" 304 - "-" "Mozilla/5.0 (X11;
nux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
ffff:192.168.10.5 - - [11/Apr/2021:09:31:04 +0000] "GET /rest/products/
arch?q=qwert%27))%20UNION%20SELECT%20id,%20email,%20password,%20%274%27,%20%275%27,%20%276%27,%20%277%27,%20%278%27,%20%279%27%20FROM%20Users-- HTTP/1.1" 200 - "-" "Mozilla/5.0 (X11;
nux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
ffff:192.168.10.5 - - [11/Apr/2021:09:32:51 +0000] "GET /rest/products/
arch?q=qwert%27))%20UNION%20SELECT%20id,%20email,%20password,%20%274%27,%20%275%27,%20%276%27,%20%277%27,%20%278%27,%20%279%27%20FROM%20Users-- HTTP/1.1" 200 3742 "-" "curl/7.74.0"
```

The answer is email,password

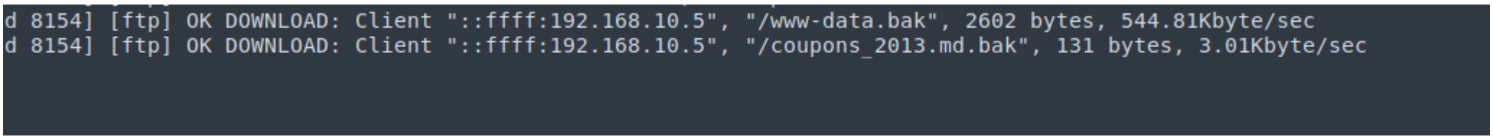
Q4

What files the attacker tried to download via web.

we can see that once user discovered the /ftp directory .
he tried to access the two files but got permission error.



```
1/Apr/2021:09:34:33 +0000] "GET /api HTTP/1.1" 500 - "-" "feroxbuster/2.2.1"
1/Apr/2021:09:34:33 +0000] "GET /administartion HTTP/1.1" 200 1924 "-" "feroxbuster/2.2.1"
1/Apr/2021:09:34:33 +0000] "GET /login HTTP/1.1" 200 1924 "-" "feroxbuster/2.2.1"
1/Apr/2021:09:34:33 +0000] "GET /admin HTTP/1.1" 200 1924 "-" "feroxbuster/2.2.1"
1/Apr/2021:09:34:33 +0000] "GET /backup HTTP/1.1" 200 1924 "-" "feroxbuster/2.2.1"
1/Apr/2021:09:34:33 +0000] "GET /promotion HTTP/1.1" 200 6586 "-" "feroxbuster/2.2.1"
1/Apr/2021:09:34:33 +0000] "GET /ftp HTTP/1.1" 200 4852 "-" "feroxbuster/2.2.1"
1/Apr/2021:09:34:40 +0000] "GET /ftp/www-data.bak HTTP/1.1" 403 300 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
1/Apr/2021:09:34:43 +0000] "GET /ftp/coupons_2013.md.bak HTTP/1.1" 403 78965 "-" ""Mozilla/5.0 (X11; Linux x86_6
1/Apr/2021:09:34:45 +0000] "GET /favicon.ico HTTP/1.1" 200 - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/
1/Apr/2021:09:34:49 +0000] "GET /favicon.ico HTTP/1.1" - - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/2
1/Apr/2021:09:34:52 +0000] "GET /favicon.ico HTTP/1.1" - - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/2
```

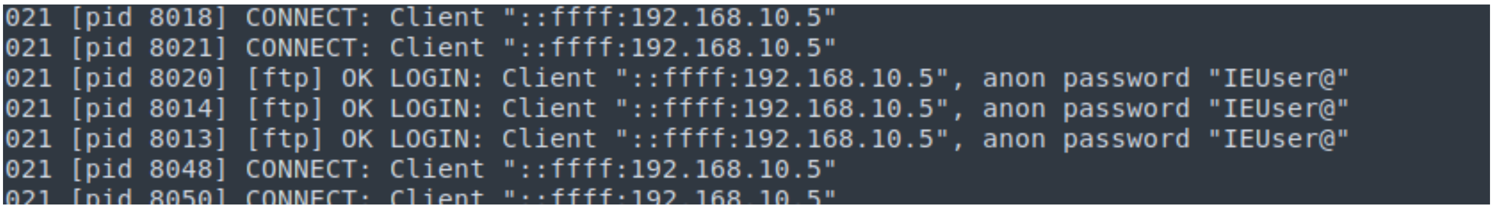


```
d 8154] [ftp] OK DOWNLOAD: Client "::ffff:192.168.10.5", "/www-data.bak", 2602 bytes, 544.81Kbyte/sec
d 8154] [ftp] OK DOWNLOAD: Client "::ffff:192.168.10.5", "/coupons_2013.md.bak", 131 bytes, 3.01Kbyte/sec
```

THe Answer is coupons_2013.md.bak,www-data.bak

Q5

we know that ftp service was used to access the files. we visit the ftp logs to see the username with which attacker authenticated



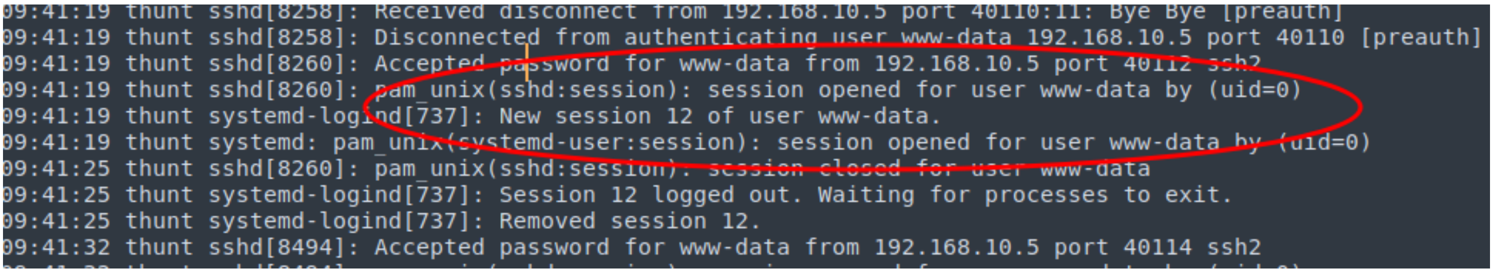
```
021 [pid 8018] CONNECT: Client "::ffff:192.168.10.5"
021 [pid 8021] CONNECT: Client "::ffff:192.168.10.5"
021 [pid 8020] [ftp] OK LOGIN: Client "::ffff:192.168.10.5", anon password "IEUser@"
021 [pid 8014] [ftp] OK LOGIN: Client "::ffff:192.168.10.5", anon password "IEUser@"
021 [pid 8013] [ftp] OK LOGIN: Client "::ffff:192.168.10.5", anon password "IEUser@"
021 [pid 8048] CONNECT: Client "::ffff:192.168.10.5"
021 [pid 8050] CONNECT: Client "::ffff:192.168.10.5"
```

user logged in with anon user which is anonymous and password used was IEUser@

Q6

Last question is related to ssh access.

we can analyze the ssh logs in auth.log



```
09:41:19 thunt sshd[8258]: Received disconnect from 192.168.10.5 port 40110:11: Bye Bye [preauth]
09:41:19 thunt sshd[8258]: Disconnected from authenticating user www-data 192.168.10.5 port 40110 [preauth]
09:41:19 thunt sshd[8260]: Accepted password for www-data from 192.168.10.5 port 40112 ssh2
09:41:19 thunt sshd[8260]: pam_unix(sshd:session): session opened for user www-data by (uid=0)
09:41:19 thunt systemd-logind[737]: New session 12 of user www-data.
09:41:19 thunt systemd: pam_unix(systemd-user:session): session opened for user www-data by (uid=0)
09:41:25 thunt sshd[8260]: pam_unix(sshd:session): session closed for user www-data
09:41:25 thunt systemd-logind[737]: Session 12 logged out. Waiting for processes to exit.
09:41:25 thunt systemd-logind[737]: Removed session 12.
09:41:32 thunt sshd[8494]: Accepted password for www-data from 192.168.10.5 port 40114 ssh2
```

service used is ssh and username is www-data