README/Rule Follower

```
== (1/10) You are NOT allowed to compromise/pentest our CTF platform (rCTF, scoreboard, etc.) ==
T for TRUE, F for FALSE> T
== (2/10) Flag sharing (sharing flags to someone not on your team) is NOT allowed ==
T for TRUE, F for FALSE> T
== (3/10) If you have a question regarding the CTF, you ping the admins or DM them ==
T for TRUE, F for FALSE> F
== (4/10) Asking for help from other people (not on your team) for challenges is allowed if you're stuck ==
T for TRUE, F for FALSE> F
== (5/10) You are allowed to use automated scanners/fuzzing/bruteforcing whenever you wish with NO restrictions ==
T for TRUE, F for FALSE> F
== (6/10) Your teams can be of unlimited size ==
T for TRUE, F for FALSE> T
== (7/10) You are allowed to do ACTIVE attacking during OSINT (i.e: contacting potential targets), not just passive, when you feel it is necessary
T for TRUE, F for FALSE> F
== (8/10) PASSIVE OSINT techniques are allowed on general RUSEC infrastructure only when EXPLICITLY given specific permission to by a challenge ==
T for TRUE, F for FALSE> T
== (9/10) ACTIVE techniques (i.e: pentesting) are allowed on general RUSEC infrastructure at any time ==
T for TRUE, F for FALSE> F
== (10/10) Official writeups will be posted at the end of the competition ==
T for TRUE, F for FALSE> T

Congratulations!
* You are NOT allowed to compromise/pentest our CTF platform (rCTF, scoreboard, etc.): T
* Flag sharing (sharing flags to someone not on your team) is NOT allowed: T
* If you have a question regarding the CTF, you ping the admins or DM them: F
        Reason: You make a ticket
* Asking for help from other people (not on your team) for challenges is allowed if you're stuck: F
        Reason: You are not allowed to ask external people for help on challenges
* You are allowed to use automated scanners/fuzzing/bruteforcing whenever you wish with NO restrictions: F
        Reason: You are only allowed to do so when a challenge specifically requires it
* Your teams can be of unlimited size: T
* You are allowed to do ACTIVE attacking during OSINT (i.e: contacting potential targets), not just passive, when you feel it is necessary: F
        Reason: OSINT is strictly passive
* PASSIVE OSINT techniques are allowed on general RUSEC infrastructure only when EXPLICITLY given specific permission to by a challenge: T
* ACTIVE techniques (i.e: pentesting) are allowed on general RUSEC infrastructure at any time: F
        Reason: Active pentesting is NEVER ever allowed on RUSEC infrastructure
* Official writeups will be posted at the end of the competition: T

RUSEC{you_read_the_rules}
```

Rev/court_jester

```
Kartik-Mac:Downloads kartik$ strings first_steps
./lib64/ld-linux-x86-64.so.2
puts
strncpy
free
strlen
malloc
__libc_start_main
__cxa_finalize
libc.so.6
GLIBC_2.34
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
PTE1
u+UH
Challenge Authored by @s0s.sh - https://s0s.sh/
RUSEC{well_th4t_was_eZ_WllwnZMjMCjqCsyXNnrtpDomWMU}
```

Binex/ruid_login

```
[Kartik-Mac:Downloads kartik$ while true; do   printf "1\nsupersecret\n3\n0\n" | nc challs.ctf.rusec.club 22169; done

1. Login admin
2. Write log
3. Read log
4. Exit
> 1

1. Login admin
2. Write log
3. Read log
4. Exit
> Admin password: [+] Admin logged in (temporarily)

1. Login admin
2. Write log
3. Read log
4. Exit
> Index: Log: RUSEC{wow_i_did_a_data_race}


1. Login admin
2. Write log
3. Read log
4. Exit
>
1. Login admin
2. Write log
3. Read log
4. Exit
>
```

OSINT/Scouts Honor 2.0

Fingerprint_1: A68097FE97D3065B1A6F4CE7187D753F8B8513F5

https://onionoo.torproject.org/details?
lookup=A68097FE97D3065B1A6F4CE7187D753F8B8513F5

```
{"version":"8.0",
"build_revision":"d2c1261",
"relays_published":"2026-01-10 04:00:00",
"relays":[
{"nickname":"olabobamanmu","fingerprint":"A68097FE97D3065B1A6F4CE7187D753F8B8513F5","or_addresses":["51.15.40.38:9001","
[2001:bc8:1640:1e30:dc00:ff:fe2a:2549]:9001"],"last_seen":"2026-01-10 04:00:00","last_changed_address_or_port":"2024-07-03 14:00:00","first_seen":"2020-04-03
00:00:00","running":true,"flags":["Fast","HSDir","Running","Stable","V2Dir","Valid"],"country":"nl","country_name":"Netherlands","as":"AS12876","as_name":"SCALEWAY
S.A.S.","consensus_weight":20000,"verified_host_names":["olabobamanmu.giannoug.gr"],"last_restarted":"2025-12-10
23:23:33","bandwidth_rate":1073741824,"bandwidth_burst":1073741824,"observed_bandwidth":17943314,"advertised_bandwidth":17943314,"overload_general_timestamp":1767913200000,"exit_poli
cy":["reject *:*"],"exit_policy_summary":{"reject":["1-65535"]},"contact":"giannoug|__AT-|gmail{ DOt-}com","platform":"Tor 0.4.8.21 on
Linux","version":"0.4.8.21","version_status":"recommended","effective_family":
["414E64BA607560F9D9C196A825950DC968700420","A68097FE97D3065B1A6F4CE7187D753F8B8513F5","B4CAFD9CBFB34EC5DAAC146920DC7DFAFE91EA20"],"consensus_weight_fraction":9.7454445E-
5,"guard_probability":0.0,"middle_probability":2.923125E-4,"exit_probability":0.0,"recommended_version":true,"measured":true}
],
"bridges_published":"2026-01-10 03:44:08",
"bridges":[
]}
```

We got 2 more fingerprints i.e B4CAFD9CBFB34EC5DAAC146920DC7DFAFE91EA20 ,
414E64BA607560F9D9C196A825950DC968700420

https://onionoo.torproject.org/details?
lookup=B4CAFD9CBFB34EC5DAAC146920DC7DFAFE91EA20

{"version":"8.0",
"build_revision":"d2c1261",
"relays_published":"2026-01-10 04:00:00",
"relays":[
{"nickname":"netimanmu","fingerprint":"B4CAFD9CBFB34EC5DAAC146920DC7DFAFE91EA20","or_addresses":["212.47.233.86:9001","[2001:bc8:710:5bcb:dc00:ff:fe5e:e8b5]:9001"],"last_seen":"2026-
01-10 04:00:00","last_changed_address_or_port":"2024-07-03 03:00:00","first_seen":"2019-02-18 00:00:00","running":true,"flags":
["Fast","Guard","HSDir","Running","Stable","V2Dir","Valid"],"country":"fr","country_name":"France","as":"AS12876","as_name":"SCALEWAY
S.A.S.","consensus_weight":9400,"verified_host_names":["netimanmu.giannoug.gr"],"last_restarted":"2025-12-10
22:58:11","bandwidth_rate":1073741824,"bandwidth_burst":1073741824,"observed_bandwidth":11036953,"advertised_bandwidth":11036953,"exit_policy":["reject *:*"],"exit_policy_summary":
{"reject":["1-65535"]},"contact":"giannoug|__AT-|gmail{ DOt-}com","platform":"Tor 0.4.8.21 on Linux","version":"0.4.8.21","version_status":"recommended","effective_family":
["414E64BA607560F9D9C196A825950DC968700420","A68097FE97D3065B1A6F4CE7187D753F8B8513F5","B4CAFD9CBFB34EC5DAAC146920DC7DFAFE91EA20"],"consensus_weight_fraction":4.580359E-
5,"guard_probability":8.4187384E-5,"middle_probability":5.3223674E-5,"exit_probability":0.0,"recommended_version":true,"measured":true}
],
"bridges_published":"2026-01-10 03:44:08",
"bridges":[
]}

https://onionoo.torproject.org/details?
lookup=414E64BA607560F9D9C196A825950DC968700420

{"version":"8.0",
"build_revision":"d2c1261",
"relays_published":"2026-01-10 04:00:00",
"relays":[
{"nickname":"kanemeadminmanmu","fingerprint":"414E64BA607560F9D9C196A825950DC968700420","or_addresses":["151.115.73.55:9001","
[2001:bc8:1d90:9f7:dc00:ff:fe20:7b75]:9001"],"last_seen":"2026-01-05 11:00:00","last_changed_address_or_port":"2024-12-29 21:00:00","first_seen":"2024-12-29
21:00:00","running":false,"flags":["Fast","Running","Stable","V2Dir","Valid"],"country":"pl","country_name":"Poland","as":"AS12876","as_name":"SCALEWAY
S.A.S.","consensus_weight":29000,"verified_host_names":["kanemeadminmanmu.giannoug.gr"],"last_restarted":"2026-01-05
10:42:30","bandwidth_rate":1073741824,"bandwidth_burst":1073741824,"observed_bandwidth":21689344,"advertised_bandwidth":21689344,"exit_policy":["reject *:*"],"exit_policy_summary":
{"reject":["1-65535"]},"contact":"giannoug|__AT-|gmail{ DOt-}com","platform":"Tor 0.4.8.21 on Linux","version":"0.4.8.21","version_status":"recommended","effective_family":
["414E64BA607560F9D9C196A825950DC968700420","A68097FE97D3065B1A6F4CE7187D753F8B8513F5","B4CAFD9CBFB34EC5DAAC146920DC7DFAFE91EA20"],"recommended_version":true,"measured":true}
],
"bridges_published":"2026-01-10 03:44:08",
"bridges":[
]}

We got all IPs needed now after arranging them according to date (old -> young)

212.47.233.86 (2019)
51.15.40.38 (2020)
151.115.73.55 (2024)

WE GOT **RUSEC{212.47.233.86:51.15.40.38:151.115.73.55}**

Forensics/:(

Ran the "strings" in the challenge file

```
Kartik-Mac:Downloads kartik$ strings Challenge.evtx
[ElfFile
 ElfChnk
 D7C9
[witch
 Microsoft-Windows-Hy

 ElfChnk
 BppCTUE1i3825UwqP9UDaj71NdSXowxSPcI/XA==
 TED5ocxPeiQziOrTQsJhAna42gc/iUkaHVEaRg==
 BHX01ANtcdylDobfffrdzM3Cm50BrcxPTqso4A==
 vKnvBzqLaJQXlCLsuDNYliTMWzPD0U6FgAY1eg==
 SRurKI6HYICisSSHf+g7YwWFP9CpkgkXLjoCyg==
 Ak+mW8WlVzgUN7+UuiC2LVyPAGZstoxNYJUQZA==
 jsFhexmhTyWeVcEwgdWa+j1I5ANSeEbfDsndtA==
 R/Zdr1C/Rt0Q2108vA0VxJRSpZkUnMkVQCTrTg==
 UlVTRUN7M3Rlcm5hbF9ibHUzXw==
 jJwTAtvZNYENfvvkv/p0XMwVSsy8ggbdILPFOA==
 /nRz8Ic+D2hbYndEKEu0WNCfiA4=
 i+UvENs6B1XmgHnf8ACYJbFZbKs=
 QxoqQxJY/g1YBhXsKzgT7whjLUE=
 iMDgl51y7bFVqbOULSVyh0Am0nQ=
 zWaX6yiM3FZSTVE8LxLQHnjpdqc=
 c0BkX2ZhYzNfc21idg==
 Ps+NUZfIysY2WIhVpYPHsiX999Q=
 y0FJcurEwrLAdorxbTiqfwa23HE=
 EOcAxXXesVe9GSiZbyUJFz55gaQ=
 yRz7+a38qA8vn8Smql2E4ZWDQTo=
 DsKxTDgWl7QsQ2JOrErjeM1G5m0=
 ?* ky
 ?* ky
 xvatgG80jmyeyf1a54NeQiRQpgM=
 fiuos6ZShSQQT5lnIrvZDHtaZ5k=
 MV8zODkwY24yazI5fQ==
 'K'ky
 'K'ky
 xNFeBzFtdMgN8jcPJKg4o7MeDMw=
 UEMaJ4VpbLWYDzmr7F0bcZTX8Gk=
 CXcVWryHY20KldW3J5WXO+vhsP8=
 wawQjvOlWiV8G3HEYs4SBUHrcZU=
 Th3MrkehUhEGOXNfKYL10iOkVTI=
 33ky
 33ky
 BlLH4X6/Scl4vw5sZLtwnHmuFsg=
 6.6ky
 6.6ky
 ?6ky
 ?6ky
 pP6ky
 pP6ky
 b6ky
 b6ky
 r6ky
 r6ky
 %7ky
 %7ky
 .37ky
 .37ky
 @7ky
 @7ky
```

Got this output after decode we can see some Base64 text after decoding the text

UlVTRUN7M3Rlcm5hbF9ibHUzXw== **->** RUSEC{3ternal_blu3_

c0BkX2ZhYzNfc21idg== **->** s@d_fac3_smbv

MV8zODkwY24yazI5fQ== **->** 1_3890cn2k29}

Now after combining all the above final flag - **RUSEC{3ternal_blu3_s@d_fac3_smbv1_3890cn2k29}**