TEAMNAME

Briefing

hello friend,

FSociety is going to change the world, and we're looking for the greatest hackers to join our ranks and take down the evils of E Corp. In our data dump, you'll find a variety of missions and tests to determine whether you are ready to join our ranks and help us change the world. We wish you luck and hope to see you on the other side.

These documents contains all the information we have on a number of E Corp servers and some FSociety/Dark Army tests. The more information you recover from these servers, the better. You should keep a look out for information in the form of `flag{FLAG}`. You'll be able to submit this information to our secure uplink so that we can verify it and analyze it to develop our plans (Submit only the FLAG part of the information and not the surrounding bits). Different pieces of information are worth different amounts to FSociety, depending on their difficulty and relevance to our goals. At the end of the day, only the best and fastest hackers will be invited to join FSociety, so you'll need to be quick and smart about how you approach these missions.

We will select the new FSociety candidates based on the total number of points you acquire, followed by the earliest final submission time. The top team will be invited to join FSociety and will receive a stipend of $1000 to upgrade their hardware, while the second place team will have their information forwarded to the Dark Army to attempt placement there and will receive a stipend of $500 for travel expenses. There will be an additional $250 stipend to the team that successfully completes 90% of the challenges.

The information you need to verify pieces of information and to access our secure uplink is:

Team Name	TEAMNAME
Team Email	TEAMEMAIL
Team Login	TEAMLOGIN
Starting Point	https://mitctf.com/
Scoreboard	https://mitctf.com/scoreboard.html
Physical Challenge Spreadsheet	https://goo.gl/TKkcAU
Wifi	MIT (or Eduroam if applicable)
IRC Channel	#mitctf on irc.freenode.net

TL;DR:

- There are a number of challenges with flags of the form `flag{FLAG}`.
- You may submit flags at the terminal using your login. Don't include `flag{}`.
- Each service has a point value. Placement is determined by score, and then by time.
- $1000 for 1st, $500 for 2nd, $250 for the first team (if any) to solve 36 challenges.

ars

Points:	200
Author:	dvorak42

We picked up a strange message on the radio, maybe you can figure out what it means?

Files/Endpoints:

`/d0d7ec9b90d7f6215f7cf8747388d08a.mp3`

Notes:

babycode

Points:	100
Author:	dvorak42

We've found an intriguing message sprayed across New York. Hopefully you can make something of it.

Files/Endpoints:

`/1052feae8e00617dfc8139ec8849e8d9`

Notes:

babynetecho

Points:	300
Author:	dvorak42

We found an old Dark Army backdoor installed on Allsafe, seems like it phones home. Maybe you can figure out how to exploit it?

Files/Endpoints:

```
/3e0a93b042d1888c4003219d160d1b9d
babynetecho.mitctf.com:4400
```

Notes:

beepboop

Points:	300
Author:	maxj

Maybe you'll find something useful on your badge.

Notes:

billshomepage

Points:	200
Author:	maxj

Poor Bill, maybe his site needs some love.

Files/Endpoints:

`billshomepage.mitctf.com:5590`

Notes:

breakin

Points:	200
Author:	dvorak42

You'll need to hone your skills with getting privileged access to things. You'll need to sign up on the Physical Challenge Spreadsheet. Once you've picked enough boxes, you'll find the flag.

Notes:

compression

Points:	100
Author:	maxj

We've found a rather interesting file that we're trying to underzstd, maybe you can find some meaning from within.

Files/Endpoints:

`/1007696b23dae7dd57ecc75695d19c79`

Notes:

cronbox

Points:	200
Author:	dvorak42

Looks like we've found another E Corp Code Monkey's starter project. Doesn't even look finished before they moved onto other things.

Files/Endpoints:

```
/d5e1b1fd18e2545608fabe426460fde7
cronbox.mitctf.com:7311
```

Notes:

crosscert

Points:	200
Author:	dvorak42

Cross Community Emergency Response Team? Maybe not, I'm sure you'll find the right version.

Notes:

ecoin

Points:	300
Author:	maxj

Seems like E Corp is coming out with the currency of the future.

Files/Endpoints:

`ecoin.mitctf.com:9999`

Notes:

escape

Points:	100
Author:	dvorak42

If you need an escape from doing CTF challenges, go find something to challenge another team (or the organizers) to. Winning the game will net you part of the flag (check with the organizers to check whether the game counts).

Notes:

fastmaze1

Points:	100
Author:	maxj

We found a map of one of the E Corp datacenters, maybe you can find a good way through.

Files/Endpoints:

`fastmaze.mitctf.com:3301`

Notes:

fastmaze2

Points:	200
Author:	maxj

Seems like they've fixed the last bug, maybe you'll need to be better. (The password is the flag from the previous level.)

Files/Endpoints:

`/fd696307a09108cbfff458fa958e68fa.gpg`
`fastmaze.mitctf.com:4373`

Notes:

fastmaze3

Points:	300
Author:	maxj

Hmm, they seem to have gotten more clever.

Files/Endpoints:

`fastmaze.mitctf.com:3221`

Notes:

fsignal1

Points:	300
Author:	dvorak42

Looks like a new prototype messaging app from E Corp, though I'm sure they've left their share of backdoors.

Files/Endpoints:

```
/32428046e5445dd39e1521485f4bc3fb.zip
fsignal.mitctf.com:5545
```

Notes:

fsignal2

Points:	400
Author:	dvorak42

If only there were a way to talk to another user that's already online.

Files/Endpoints:

```
/32428046e5445dd39e1521485f4bc3fb.zip
fsignal.mitctf.com:5545
```

Notes:

fsignal3

Points:	500
Author:	dvorak42

If there only was a way to break this 'forward secure' property.

Files/Endpoints:

```
/32428046e5445dd39e1521485f4bc3fb.zip
fsignal.mitctf.com:5545
```

Notes:

fsocfanclub1

Points:	200
Author:	maxj

Seems like we've gathered quite a fan following. Maybe someone has something useful to share.

Files/Endpoints:

`fsocfanclub.mitctf.com:3581`

Notes:

fsocfanclub2

Points:	200
Author:	maxj

Looks like they fixed that last bug...

Files/Endpoints:

`fsocfanclub.mitctf.com:3181`

Notes:

getsocial

Points:	200
Author:	maxj

Why does E Corp even need another Twitter-clone.

Files/Endpoints:

```
/bdda8c38896efac06ae360ef61f26778
    getsocial.mitctf.com:8877
```

Notes:

gollum1

Points:	100
Author:	dvorak42

Seems like E Corp is experimenting with a shiny new post-quantum crypto scheme.

Files/Endpoints:

```
/a9736047cb29cc1c4bb8425adcc842fe.py
gollum.mitctf.com:3301
```

Notes:

gollum2

Points:	200
Author:	dvorak42

Seems like E Corp is experimenting with a shiny new post-quantum crypto scheme, maybe they've forgotten to protect against all attacks.

Files/Endpoints:

`/a9736047cb29cc1c4bb8425adcc842fe.py`
`gollum.mitctf.com:3301`

Notes:

gollum3

Points:	500
Author:	dvorak42

Seems like E Corp is experimenting with a shiny new post-quantum crypto scheme, though it seems pretty secure (NOTE: THIS CHALLENGE MIGHT BE IMPOSSIBLE).

Files/Endpoints:

```
/a9736047cb29cc1c4bb8425adcc842fe.py
gollum.mitctf.com:3301
```

Notes:

infiltrate

Points:	300
Author:	dvorak42

You'll need to find and infiltrate an E Corp training meeting while they're out at lunch. You'll need to sign up on the Physical Challenge Spreadsheet. You will only be able to attempt the challenge once. You should have two team members, a laptop, and something to take notes (and/or pictures) before you attempt the challenge. Check with an organizer at the beginning of your timeslot.

Notes:

oldie

Points:	300
Author:	dvorak42

We found an old test binary from the E Corp SEC certification. Might be useful to find any secrets inside?

Files/Endpoints:

`/4966519c11f1a29f22fce24c71f74cc1`

Notes:

raspberry

Points:	100
Author:	maxj

Maybe you'll find something useful on your badge.

Notes:

recurse

Points:	200
Author:	dvorak42

Luckily this compresses very well, but maybe you can recover something from this dump.

Files/Endpoints:

`/af0c7e3e3eb3a414ec5a6d8648482172.zip`

Notes:

resnet

Points:	200
Author:	maxj

Maybe you'll find something useful on your badge.

Notes:

rogue

Points:	400
Author:	dvorak42

Some E Corp employees seem to have gotten into playing some rogue-like in their free time. Though the UI and client seem to be a bit buggy, it might be easier to figure out the protocol and use that.

Files/Endpoints:

```
/19bfc0f2ba85fe8a58d9b81048702d50.zip
rogue.mitctf.com:4242
```

Notes:

ronscoffee

Points:	200
Author:	dvorak42

Looks like you can scan your coffee mug for some Internet Points (You can give the organizers a coffee cup with an image or link to an image and maybe Ron will get around to scanning it).

Files/Endpoints:

`/cdc5cba33ca8b31f58ca6da279008244.png`
`ronscoffee.mitctf.com:3443`

Notes:

secureca

Points:	400
Author:	maxj

HTTPS is the future, and E Corp seems to be getting into the forefront of Secure Certificates. Perhaps their rush to implement secure certificates has left a hole?

Files/Endpoints:

`secureca.mitctf.com:4949`

Notes:

shialabeouf

Points:	200
Author:	maxj

Maybe you'll find something useful on your badge.

Notes:

signals

Points:	200
Author:	dvorak42

Can you hear me now? Maybe I need more Ghz.

Notes:

steelmountain

Points:	400
Author:	maxj

Can you help breach the old Steel Mountain backup backup facility?

Files/Endpoints:

`steelmountain.mitctf.com:2017`

Notes:

tamper

Points:	200
Author:	dvorak42

You'll need to hone your skills with getting into things without leaving a mark. You'll need to sign up on the Physical Challenge Spreadsheet. Show the organizers how you successfully avoid Tamper-Evident tape and zipties and you'll get a flag.

Notes:

tbd1

Points:	300
Author:	maxj

Our mole inside E Corp has left a message at the deaddrop. Unfortunately it seems the firewall is limiting how much data we can send to our backdoor.

Files/Endpoints:

```
/393efd73ee8bb51648f10e1450aeddaa
tbd.mitctf.com:7777
```

Notes:

tbd2

Points:	300
Author:	maxj

Our mole inside E Corp has left a message at the deaddrop. Unfortunately it seems the firewall is still limiting how much data we can send through, even after bypassing the first layer.

Files/Endpoints:

```
/393efd73ee8bb51648f10e1450aeddaa
tbd.mitctf.com:7777
```

Notes:

vbox1

Points:	200
Author:	dvorak42

We found a backdoor to an E Corp dev box, someone seems to have left an interpreter running. Luckily one of our previous missions turned up part of the interpreter they're using, see if you can recover the 'flag'.

Files/Endpoints:

`/e95250a0365afc554ce47f2fc831b9a1.public`
`/21855a642c429ae894a3ae621fdf89df.py`
`/794cb246ad337d041cca5f58f5ac17ff.py`
`vbox.mitctf.com:4444`

Notes:

vbox2

Points:	300
Author:	dvorak42

The dev box might also contain some hidden features, maybe you can get even more access?

Files/Endpoints:

```
/e95250a0365afc554ce47f2fc831b9a1.public
  /21855a642c429ae894a3ae621fdf89df.py
  /794cb246ad337d041cca5f58f5ac17ff.py
          vbox.mitctf.com:4444
```

Notes:

vcoin

Points:	300
Author:	dvorak42

We came across an old E Corp project, looks like a precursor to ecoin. Maybe you can find something useful.

Files/Endpoints:

`/124354047b8064e1338a1543f1ebb4ed`

Notes:

Flags

Challenge	Points	Flag
ars	200	
babycode	100	
babynetecho	300	
beepboop	300	
billshomepage	200	
breakin	200	
compression	100	
cronbox	200	
crosscert	200	
ecoin	300	
escape	100	
fastmaze1	100	
fastmaze2	200	
fastmaze3	300	
fsignal1	300	
fsignal2	400	
fsignal3	500	
fsocfanclub1	200	
fsocfanclub2	200	
getsocial	200	

Flags

Challenge	Points	Flag
gollum1	100	
gollum2	200	
gollum3	500	
infiltrate	300	
oldie	300	
raspberry	100	
recurse	200	
resnet	200	
rogue	400	
ronscoffee	200	
secureca	400	
shialabeouf	200	
signals	200	
steelmountain	400	
tamper	200	
tbd1	300	
tbd2	300	
vbox1	200	
vbox2	300	
vcoin	300	

[EOM]