Scoring Team Beacons – Gold Team version 1.0 July 2021

A beacon submitted to a beacon server indicates a score. Each team during the contest is provided with a secret team token (UUID). The Red Team gets theirs at the beginning of the game since they attacking all throughout the competition while the Blue Teams gets their individual token just before purple attacking is permitted. Blue Teams are usually allowed to attack on day two.

There are two pre-existing servers maintained by the gold team.
These are the CLI server (called CLI_Server) and Beacon Server (called Beacon_Server). The exact IP addresses of these servers will be disclosed on game day for Red Team or when the game permits purple attacking for the Blue Teams.

CLI server – is used to a) "register" a beacon token or to set a "beacon" port listener

Beacon server - used to submit beacon tokens and at the port configured on the CLI Server.

Tokens

There are two types of tokens per team, your private team token (UUID) which you keep private and secret from other teams and a beacon token that your team creates on demand from your private team token. You can make as many beacon tokens as you want.

The general concept is that your beacon token allows you to signal ownage and a score when they are sent from a victims target system to the beacon server. These will render on the scoreboard in your team colors as a single icon. Submitting multiple beacons from different victim hosts will display multiple icons!

- the CLI server is where you use to create a static "beacon token" of which you can mint as many as you like.

Connecting to the CLI Server

Note that the destination port is always port 50007.

enter:

nc <CLI_Server> 50007

```
 _______  _______  _____  _______ _________ _______  _____ _________ _______  _____
/ _____| / _____/ _ \| _ \|_______|___ ) / _ \_  _||_____/ / _ \
\_____ \| | | | | | |_) | _|| _ \| | | | | |  |_ \| | | |
 _____) | |___| | |_| | _ <| |_____| | |_) | | |_| | | | |_____) | | |_| |
|_______/ \_____\_____/|_| \_\_______|_____/ \_____/ |_| |_____(_)____/
```

MODE: DEFAULT

This is Scorebot v3.0, I accept the following commands:
RED CELL:
 # submit flag
flag:<team_token>,<flag>
 # register for a beacon token
register:<your_nick>,<team_token>
 # request beacon port
beacon:<team_token>,<port>

Please send your request

enter:
REQ>**register:<team_name>,<secret UUID team token>**

a response will come back that looks like -->ACK><beacon token>

Also, as a one time activity, you HAVE TO register at least one port for your private team token that will accept beacon tokens on a port.

Enter the following at least once:
beacon:<team token>,<port>
typically enter "beacon:<secret UUID team token>,50007

Connecting to the Beacon Server

From a target victim machine, enter the following as an example or any raw socket:
echo "<beacon token>"| nc <Beacon_Server> 50007
Note that there is no response or confirmation. Look on scoreboard for your icon.

The beacon will drop off after 5 minutes. You need to do this in a loop within 5 minute intervals to maintain the beacon.

Defenders may try to watch for egress on port 50007 so you can add additional listeners on the Beacon Server and submit beacon tokens there such as above but use say port 80 instead of 50007 such as:
beacon:<team token>,<port>
typically enter **beacon:<secret UUID team token>,80**

Note that would will get back “ACK>” which is fine or “ACK>418” which means that port is already listening there for your team.

Stating the obvious, do not submit your beacon token from your host range but only from a victim’s host.

Remember that the CLI Server is used to create beacon token and add beacon listeners. You typically talk to is from your host range. The Beacon server is what you talk to from the victim’s range of hosts. You want to score as many of those as possible and run those in a loop every five (5) minutes to show persistence.

Sample Interaction

Team Alpha is handed a secret UUID fd4328f4-8a7f-4168-94c8-bdff19484160 before purple team team interaction.

Then on the Cli_Server, they register a beacon token and set up the default listening port 50007.

register:Alpha,fd4328f4-8a7f-4168-94c8-bdff19484160
ACK> f0295086-517f-40bd-8dac-b2c6ae9c5de0
beacon:fd4328f4-8a7f-4168-94c8-bdff19484160,50007
ACK>

Alpha team gains a shell on team Epsilon host and does this:
echo "f0295086-517f-40bd-8dac-b2c6ae9c5de0" | nc <Beacon_Server> 50007

This will score for team Alpha and place an icon!

Troubleshooting

1) If you don’t see the beacon on the scoreboard:

a) make sure you entered the “beacon command” to the CLI server to associate your team token with port 50007 or which ever port you set up.
b) make sure you submitted a beacon token to the Beacon server and NOT your private team token.