Durham Shared Fail2Ban

October Update

“An experiment that has locked me out numerous times…..”

Presented by Paul Clark

26th Oct 2018

Amsterdam Netherlands, (C)Paul Clark

What is it?

Standard Fail2Ban client agent modified to perform the following:

- Report to a centralised database
- Retrieve unknown IP’s and pre-emptively initiate blocking
- Escalate Jail time/punishment based on time/No. of instances.

System Goals

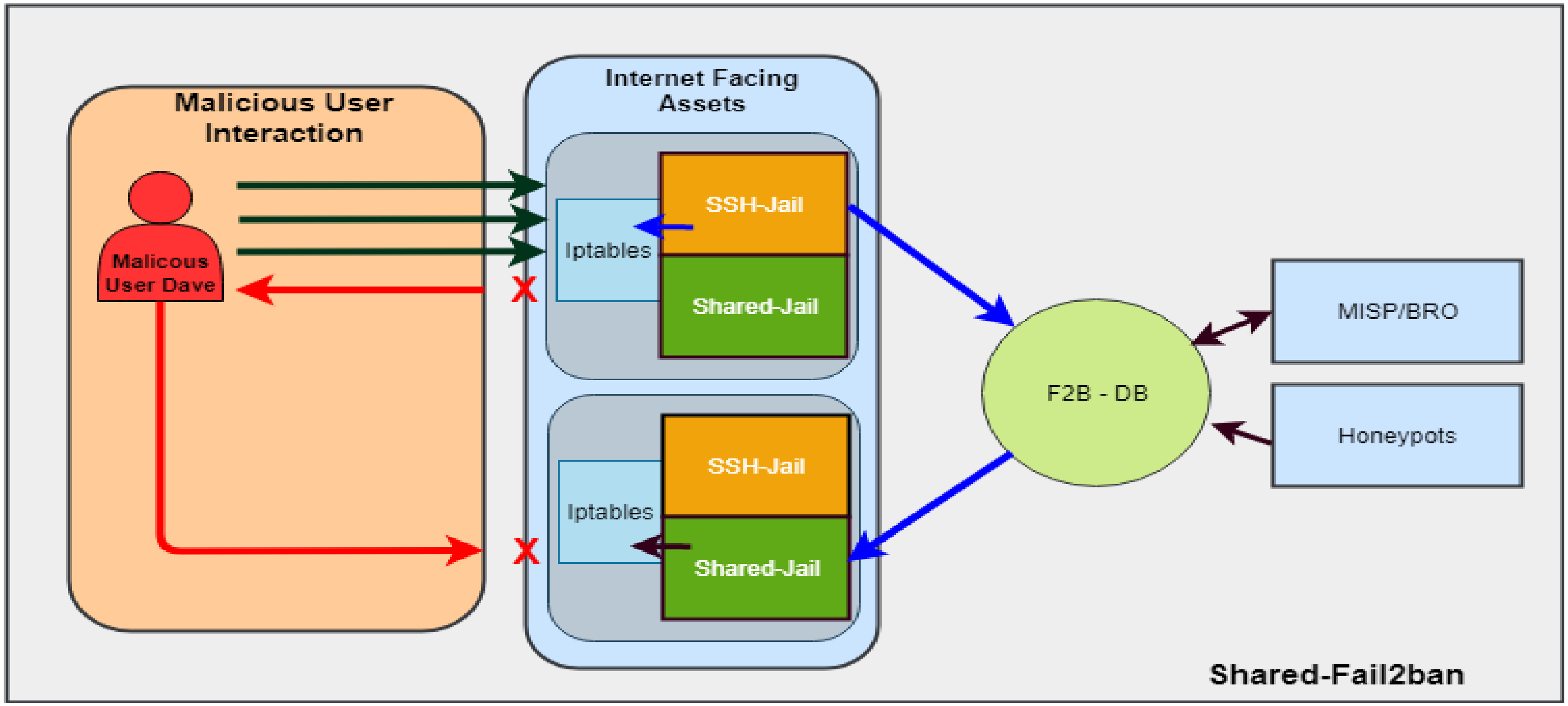
- Reduce target area by banning at initial source and mitigating further attempts against remote systems.

- Centralise Accounting to aid in data gathering/research.

- Export gathered data into external resources.

- Import data from external resources to allow automatic attack prevention prior to one occurring.

Basic Functionality

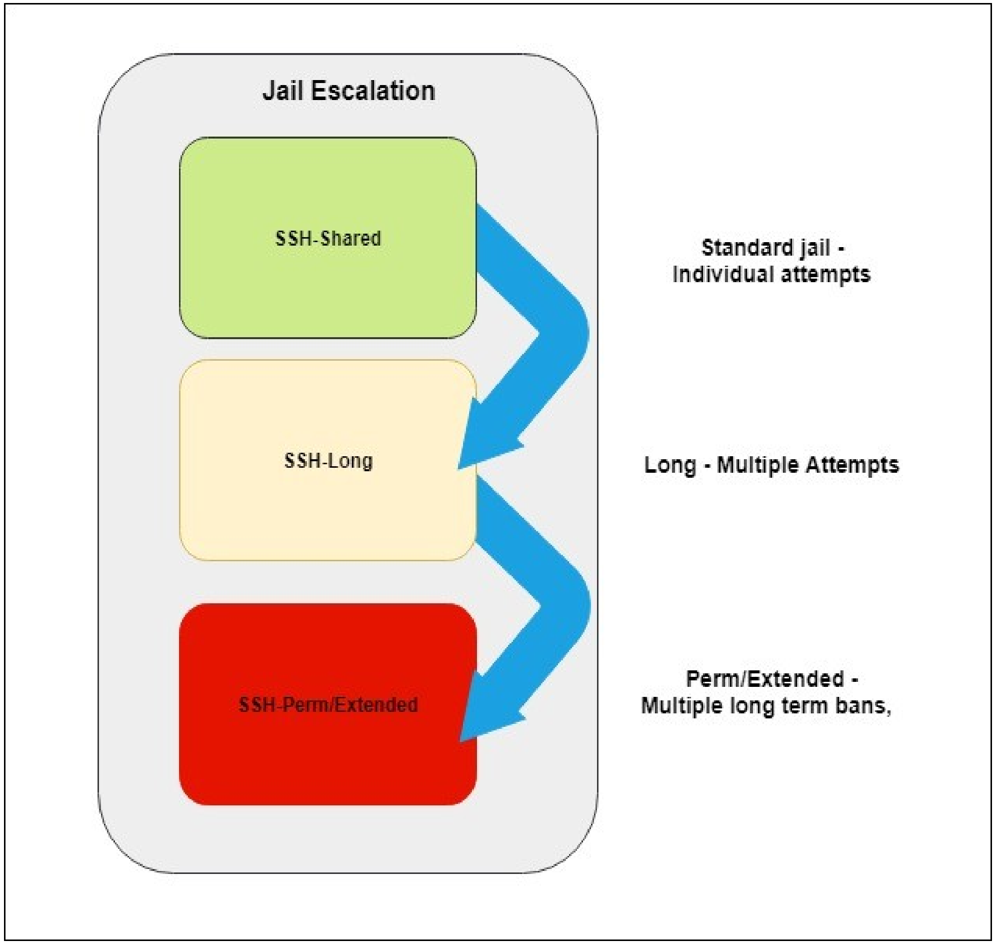


Durham
University

Escalation

Purpose:

- Minimise extended bans for common user error
- Persistent aggressive attempts banned for longer periods


Jail Escalation
SSH-Shared
SSH-Long
SSH-Perm/Extended
Standard jail - Individual attempts
Long - Multiple Attempts
Perm/Extended - Multiple long term bans,

Current Status

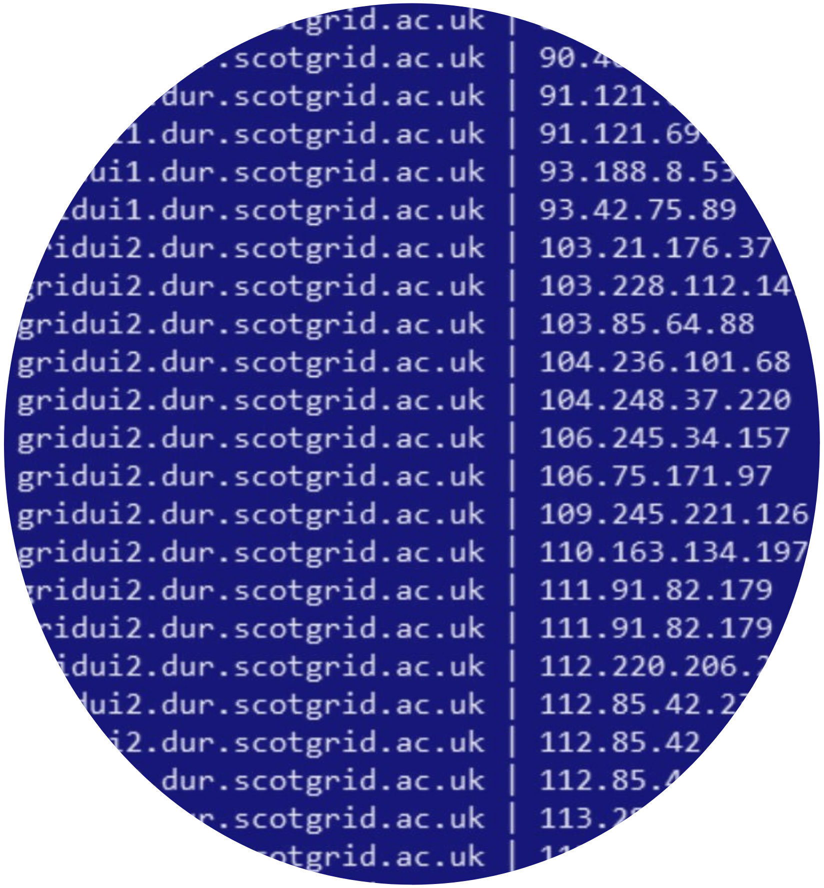
- Test system is fully functional in VM environment
- Initial test scripts exported to Python
- GridUI's implemented with basic sharing functionality
- Data gathering underway

Durham University

Traffic Highlights

Continuous attempts from:

- 58.218.92.44 – China
- 5.188.10.156 – Russia
- 193.201.224.214 – Ukraine



```
           tgrid.ac.uk |
        .scotgrid.ac.uk | 90.4
      dur.scotgrid.ac.uk | 91.121.
    1.dur.scotgrid.ac.uk | 91.121.69
   ui1.dur.scotgrid.ac.uk | 93.188.8.53
  dui1.dur.scotgrid.ac.uk | 93.42.75.89
 idui2.dur.scotgrid.ac.uk | 103.21.176.37
ridui2.dur.scotgrid.ac.uk | 103.228.112.14
gridui2.dur.scotgrid.ac.uk | 103.85.64.88
gridui2.dur.scotgrid.ac.uk | 104.236.101.68
gridui2.dur.scotgrid.ac.uk | 104.248.37.220
gridui2.dur.scotgrid.ac.uk | 106.245.34.157
gridui2.dur.scotgrid.ac.uk | 106.75.171.97
gridui2.dur.scotgrid.ac.uk | 109.245.221.126
gridui2.dur.scotgrid.ac.uk | 110.163.134.197
ridui2.dur.scotgrid.ac.uk | 111.91.82.179
 idui2.dur.scotgrid.ac.uk | 111.91.82.179
  dui2.dur.scotgrid.ac.uk | 112.220.206.
   ui2.dur.scotgrid.ac.uk | 112.85.42.2
    i2.dur.scotgrid.ac.uk | 112.85.42
      dur.scotgrid.ac.uk | 112.85.
        .scotgrid.ac.uk | 113.2
          otgrid.ac.uk |
```

Durham
University

Future Work

- Continue testing long term jails
- Push updated scripts to GitHub
- Investigate exporting gathered data to Central IT and MISP
- Implementation of SSH-honeypots to feed data into fail2ban
- Test jail types other than SSH

Durham University

Durham Shared Fail2Ban