Bug Bounty Hunting on Steroids
The Team

Anshuman Bhartiya

@anshuman_bh

Security Engineer, Bug Bounty Hunter

Automate all the things!!

All things as code!!

Mohammed Diaa

@mhmdiaa

Developer, Bug Hunter

Never send a human to do a machine’s job

Glenn ‘devalias’ Grant

@_devalias

Hacker, Polyglot Developer, Bounty Hunter,
#SecDevOpsInTheCloudCyber™ enthusiast...

Penetration Tester and Offensive Capability Development at TSS

@anshuman_bh @_devalias @mhmdiaa
Agenda

- Problem?
- Current Situation
- Target: Ellingson Mineral Corporation
- Introducing BountyMachine
- Lessons Learned
- Conclusion
Problem?

- Not all hacking is fun. A lot of manual repetitive work.
- Building everything from scratch is a bad idea..
- How do we scale across thousands of targets?
- Things change all the time, we need continuous monitoring
Current Situation
Redundancy Between Tools

Not invented here / anti unix philosophy is prevalent
An unmaintained tool is born

ToolA released: does a few things

ToolB released: handles some missing bits, but fails in other areas

Maintainers (often a single point of failure) move on to something new..

*Back to square one!*

[https://xkcd.com/927/](https://xkcd.com/927/)

@anshuman_bh @__devalias @mhmdiaa
You can’t build everything from scratch
Lack of Reliable Tool Comparisons

You don’t know the right tool for the job unless you try all of them.. and there are a lot...
The situation is improving!

The Bug Hunter’s Methodology by Jason Haddix (@jhaddix)

https://github.com/jhaddix/tbhm

Thanks, Jason! You’re awesome \m/
## Sub Bruting

### 1,136,964 LINE SUBDOMAIN DICTIONARY (ALL.TXT)

<table>
<thead>
<tr>
<th>Tool</th>
<th>Time to run</th>
<th>Threads</th>
<th>Found</th>
</tr>
</thead>
<tbody>
<tr>
<td>subbrute</td>
<td>errored</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>gobuster</td>
<td>21m15.857s</td>
<td>100</td>
<td>87</td>
</tr>
<tr>
<td>massdns</td>
<td>1m24.167</td>
<td>n/a</td>
<td>213</td>
</tr>
<tr>
<td>dns-parallel-prober</td>
<td>42m2.868s</td>
<td>100</td>
<td>43</td>
</tr>
<tr>
<td>blacksheepwall</td>
<td>256m9.385s</td>
<td>100</td>
<td>61</td>
</tr>
</tbody>
</table>
Poor Interoperability

Many tools just don’t play nicely with each other
ReconJSON

- JSON-based recon tool data output standard
- Increase interoperability between tools
- Enable a unix-philosophy recon tooling digital utopia!

Join the discussion:

https://github.com/ReconJSON/ReconJSON
Scaling & Reliability

Learning from the dev side of the tech world
Scaling & Reliability

- **Vertical scaling**
  - More server, more money, more problems

- **Horizontal scaling**
  - Flexible, fault tolerant, cheaper

- **Learn from the tech giants**
  - Great architectures and tools to leverage
Practical Research Environment

There are tons of assets that you can hack legally
I just want to hack things...

Wouldn’t it be nice to have:

● An organized database with all the assets that are legal to hack
  ○ Stick to the scope
● A supporting platform that collects data about these assets
  ○ Fast feedback loop
● A way to easily explore the asset data
  ○ Locate targets and #HackAllTheThings™
It’s all about identifying assets

What you don’t know about, you can’t protect
Unmaintained assets cause breaches

https://snyk.io/blog/owasp-top-10-breaches
Unmaintained assets cause breaches

<table>
<thead>
<tr>
<th>Component</th>
<th>Breaches</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>A9-Using Components with Known Vulnerabilities</td>
<td>12/50 breaches</td>
<td>24%</td>
</tr>
<tr>
<td>A5-Security Misconfiguration</td>
<td>10/50 breaches</td>
<td>20%</td>
</tr>
</tbody>
</table>
Real-time inventory of target assets

Ephemeral assets, they said.

It will be fine, they said.
Attack surface is always evolving

**Code changes**
- Bugs/regressions
- New code
- Backups

**New assets**
- Hosts
- Cloud services
- Subdomains
Target
ELLINGSON MINERAL CORPORATION

YES, WE ARE A CORPORATION. OUR PRODUCT IS THAT OF CURIOSITY.

IN BUSINESS SINCE THE MID-1990S
What we know...
Let’s start the demo...
Introducing BountyMachine
Technologies
Golang

https://golang.org/

@anshuman_bh @_devalias @mhmdiaa
Docker

https://www.docker.com

@anshuman_bh @_devalias @mhmdiaa
Kubernetes

https://kubernetes.io/

@anshuman_bh @_devalias @mhmdiaa
Argo

https://argoproj.github.io/argo

@anshuman_bh @_devalias @mhmdiaa
Architecture
It starts with a target
Everything is managed by queues
The output of a workflow can be passed to another
New results are identified by a diff worker
Notifications only include new results
The monitoring worker re-checks things as scheduled
To sum up...
Lessons Learned
Geographic Limitations
World Domination Headquarters

- GMT-7
- GMT+2
- GMT+10
Communication
Dealing with conflicts

- Check your ego
- Communicate openly, honestly and thoroughly!
- Stay open to new suggestions
- Delegate responsibilities
- Be flexible
- Code/data trumps assumptions
Technology
Technology

- Keep an open mind
- Explore what is out there
- Dig deep, understand how the underlying tech works
- Sometimes what you want doesn’t quite exist yet.. and that’s ok
- ‘Simple’ problems sometimes take a while to solve well
MVP? JIT!
MVP? JIT!

- Plan at the macro level
- Handle intricate details Just In Time (JIT)
- Backlog anything not needed now
- Move fast and (hopefully don’t) break (too many) things
- Done is better than perfect
About that demo...

Remember Ellingson Mineral Corp?
We started with...
subdomain takeover

press.ellingsoncorp.com

press.ellingsoncorp.com

ellingsonpress.github.io
blog.ellingsoncorp.com
help.ellingsoncorp.com

// TODO: fix the authentication mechanism
var admin_panel = "https://gibson.ellingsoncorp.com/bZOxeyhKfTFRdZE2jLky9GFYFEj7SoG"
Conclusion
Conclusion

- We can’t automate everything, but there is a lot we can
- Less wasted time means more fun hacks!
- Explore new tech, don’t be afraid to innovate
- Keep tooling simple and consumable (unix philosophy)
- Improve existing tools, don’t reinvent the wheel!
- Check your ego, collaborate, learn, share, and keep an open mind
Special Thanks

Thanks to the people who write open source tools.

Those who understand that “Sharing is Caring”.

For in the end, “None of us is good as all of us.”
Thanks!

Any questions? Reach out to us!

@anshuman_bh @_devalias @mhmdiaa