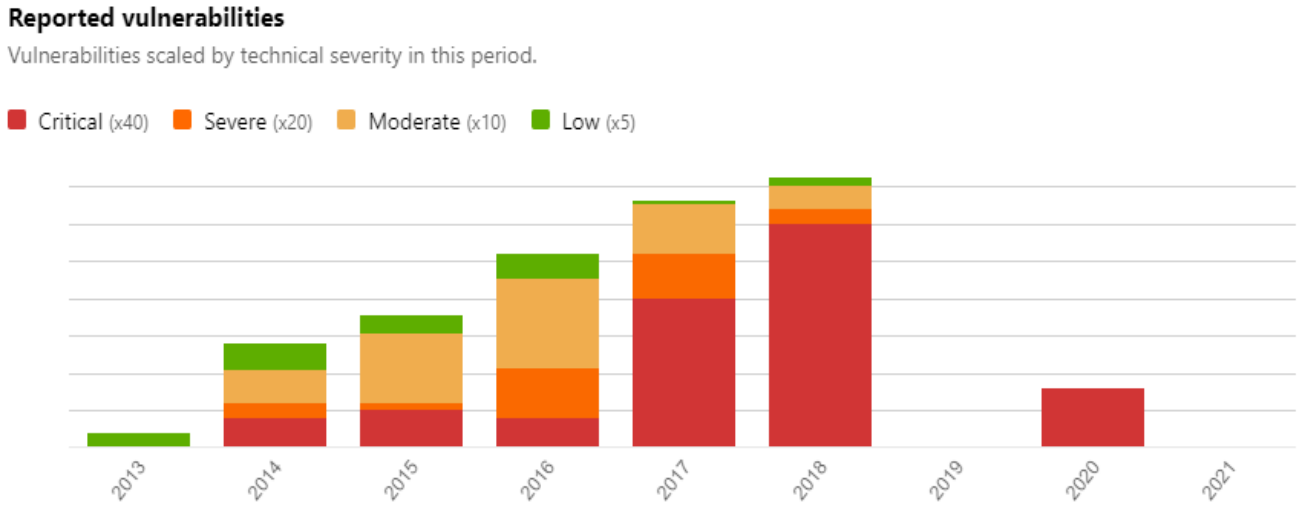
Hop the Fences, Steal the Cars

March 27th 2021

`whoami`

- Ciarán McNally – maK (He/Him)
- Director of Slándáil Research Limited (securit.ie)
- Working in IT security the past 8 years
- Background of sysadmin / network engineering / freelance web dev
- Have contracted in many different roles over the years
- Jack of all trades, master of none
- Previously an avid bounty hunter (Bugcrowd / Hackerone)



Slándáil Research Limited

The Security Game


WHO'S AWESOME?
YOU'RE AWESOME!
quickmeme.com

The Problems I see everywhere

- Web services are a fun and large attack surface
- Vulnerability Management, maintaining and monitoring network perimeters, software patching and maintaining visibility of your risks in a fast moving or growing businesses is a hard problem.
- Point-in-time penetration testing isn’t as useful as it once was

Visibility of the big oul' Network

Observation (some passive visibility into IP space)

Shodan	www.shodan.io
Binary Edge	www.binaryedge.io
IPv4info	ipv4info.com
Hurricane Electric	bgp.he.net
Robtex	www.robtex.com

Probing (some active visibility into IP space)

Nmap	nmap.org
Masscan	github.com/robertdavidgraham/masscan
Zmap	zmap.io
RustScan	github.com/RustScan/RustScan

Both IP & Domain Historical Insights

Project Sonar	opendata.rapid7.com

Others

- Search Engines
- TLS Certificate Transparency
- WHOIS Lookups
- Historical WHOIS
- AXFR DNS Transfers

Project Sonar - opendata.rapid7.com

Great tools to explore this data

SonarSearch github.com/Cgboal/SonarSearch
DNSGrep github.com/erbbysam/DNSGrep

How I leverage the data (github.com/mak-/sonarust)

- Last 5 years of forward/reverse DNS data (6 month intervals)
- Run a flask API on a Raspberry Pi that queries a connected 4TB HDD
- Sort the data into simple text files using the following formats
  - [Domain]
  - [Domain (reversed)] [IP]
  - [IP] [Domain]
- Leverage a fast C binary search over the flat files
  (github.com/pts/pts-line-bisect)
- Multiple years of DNS searched in seconds

Useful Searches

➢ Search for similar domains
“company”
- companydev.com
- company-staging.com

➢ Search for subdomains
“company.com”
- dev.company.com
- tool.company.com

➢ Search for other domains on same IP

BSides Dublin

For the cyberspace explorer

Further Data enrichment and discovery

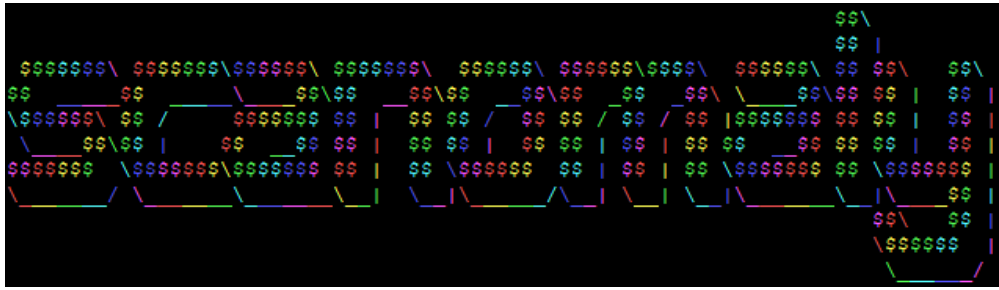
projectdiscovery.io
github.com/projectdiscovery/subfinder
github.com/projectdiscovery/nuclei
github.com/projectdiscovery/shuffledns

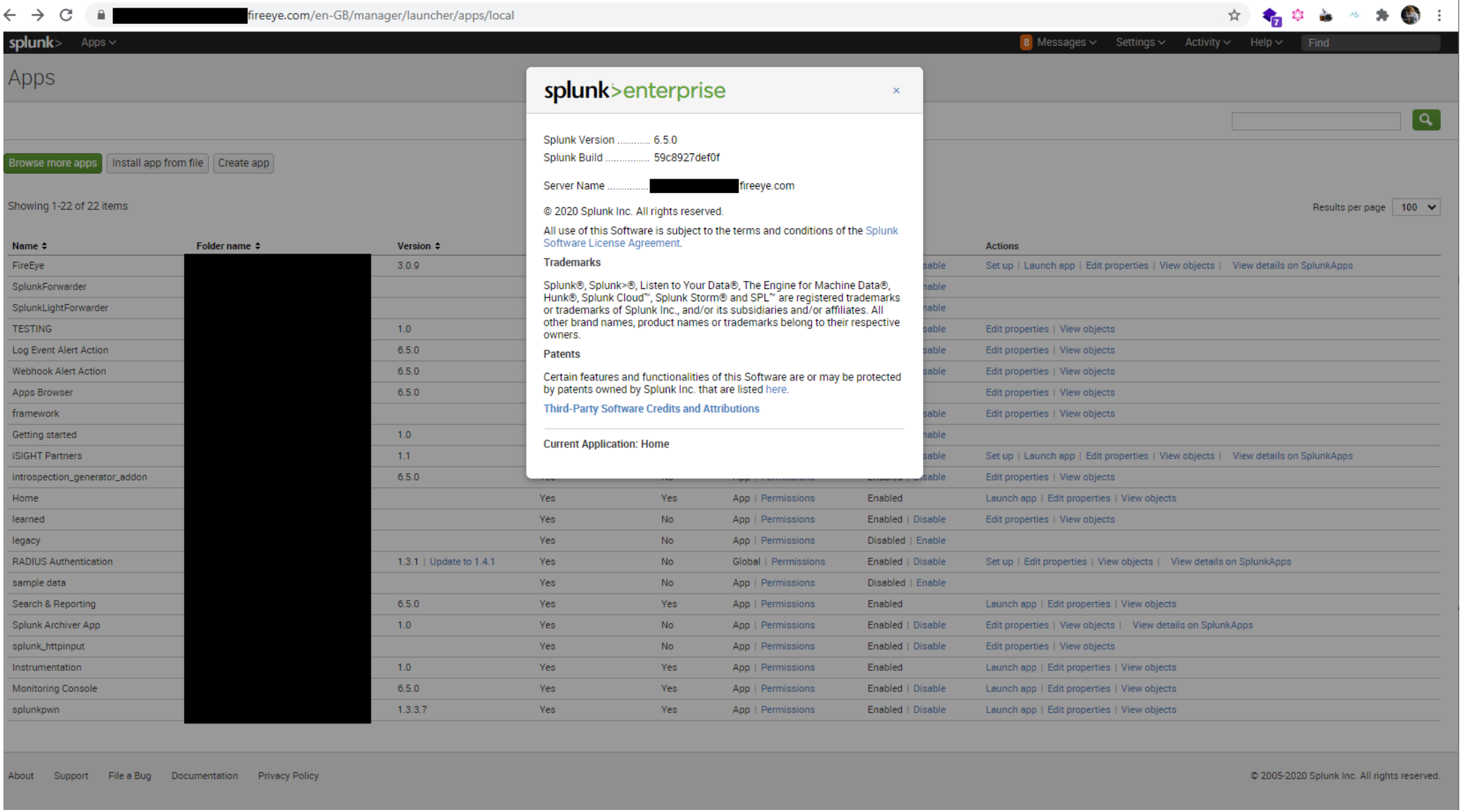
OWASP Amass
github.com/OWASP/Amass

Massdns
github.com/blechschmidt/massdns

Introducing scanomaly

- Built over the last 3-4 years to fit as part of other automation
- Modular, Flexible framework for automating things
- Initially built to explore large attack surfaces but later developed into a fully fledged web application fuzzer
- It stores web requests and responses in an SQLite database
- It’s configurable and you can run different modules depending on different responses.





BSides Dublin

terminal - Web Shell for Splunk -

[redacted]fireeye.com/en-GB/app/webShell/terminal

splunk> App: Web Shell for Splunk

```
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old

$ id
uid=0(root) gid=0(root) groups=0(root)

$ ifconfig
eth0      Link encap:Ethernet  HWaddr 3a:63:65:31:32:61
          inet addr:10.100.1.27  Bcast:10.100.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:521944 errors:33347 dropped:40 overruns:0 frame:33347
          TX packets:100170 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:129895322 (129.8 MB)  TX bytes:30421711 (30.4 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:4101223 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4101223 errors:0 dro
          collisions:0 txqueuelen:0
          RX bytes:305004519 (305.0 MB)


$
```

fireeye.com/en-GB/manager/FireEye_v3/apps/local/FireEye_v3/setup?action=edit

splunk> Apps Messages Settings Activity

FireEye_v3

FireEye Setup Page

Enable your FireEye Product(s)

- [x] NX
- [x] EX
- [ ] ETP
- [ ] AX
- [ ] FX
- [x] HX
- [ ] PX
- [ ] TAP

** Reminder: Make sure you restart splunk to see the dashboard changes take effect **

VirusTotal Setup

VirusTotal API Key

[redacted]

Daily Report Options

Enable the report, select the schedule, specify the recipient.

iSIGHTPartners_ThreatScape_App

Welcome to the iSIGHT Partners ThreatScape® App for Splunk

The ThreatScape App for Splunk integrates ThreatScape intelligence - the most comprehensive, contextually rich, and actionable cyber threat intelli
instance. To realize the benefits of this integration, you will need both a public and private API key to enter into the fields below. If you would like mo
integrate ThreatScape API data into Splunk, please visit here: http://www.isightpartners.com/act-today/request-consultation/

ThreatScape API Settings

Public Key

3469c13e72c44fc15fc48a82353c7f6e0239975b45c91d33c5344b98e94

Private Key

[redacted]

Retrieve indicators from (mm/dd/yyyy)

09/13/2016

Indicators and Warnings

- [x] Enable

Program	Rewarded for	Amount	Rewarded
FireEye Bug Bounty Program	Splunk - Remote code execution	$2,500.00	9 Sep 2020

BSides Dublin

[redacted]fireeye.com/welcome[redacted]

FIREEYE

Detection on Demand

Email Address

[redacted]

Create Password

Password

Confirm Password

Confirm Password

Must contain at least one number and one uppercase and lowercase letter, and at least 10 or more characters

Create Account

Already have an account? Login instead.

idp.fireeye.com/app/UserHome

FIREEYE | Launch App | Home | [redacted]

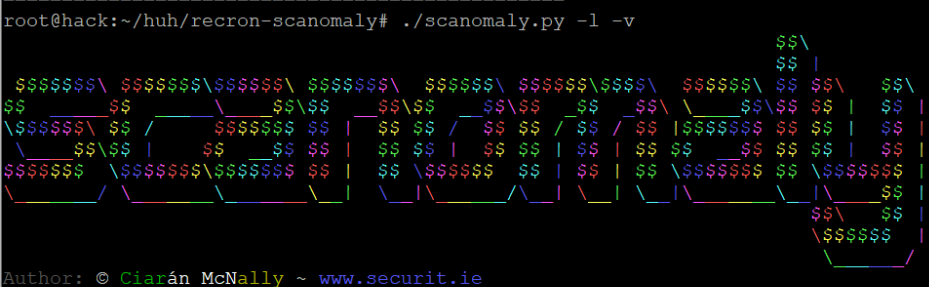
Work | +

- Statuspage — FireEye Service Status
- FireEye Support Portal & Community
- FireEye Documentation Portal
- FireEye MARKET — The FireEye Market

Program	Rewarded for	Amount	Rewarded
FireEye Bug Bounty Program	IDOR and account takeover	$2,000.00	23 Sep 2020

BSides Dublin

```
root@hack:~/huh/recron-scanomaly# ./scanomaly.py -l -v
```



```
Author: © Ciarán McNally ~ www.securit.ie
Software: https://github.com/mak-/scanomaly.git
================================================
[+] ==== Module Information ====
--------------------------
[+] Name: dirb
[+] Description: This is a Directory buster plugin for Scanomaly
[+] Author: Ciaran McNally
[+] Website: https://securit.ie
--------------------------
[+] Name: fuzz
[+] Description: Simple fuzzer (use *@* to specify where to fuzz) -dl [list to f
[+] Author: Ciaran McNally
[+] Website: https://securit.ie
--------------------------
[+] Name: basic
[+] Description: Basic http Authorization brute force
[+] Author: Ciaran McNally
[+] Website: https://securit.ie
--------------------------
[+] Name: dirb-single
[+] Description: This is a Directory buster plugin for a specified directory
[+] Author: Ciaran McNally
[+] Website: https://securit.ie
--------------------------
[+] Name: fuzzall
[+] Description: Fuzz multiple locations with common payloads
[+] Author: Ciaran McNally
[+] Website: https://securit.ie
--------------------------
[+] Name: s3bucket
[+] Description: This finds s3 buckets
[+] Author: Ciaran McNally
[+] Website: https://securit.ie
--------------------------
[+] Name: bypass
[+] Description: This module attempts to bypass 403's and 401's using common tri
[+] Author: Ciaran McNally
[+] Website: https://securit.ie
--------------------------
[+] Name: dirb-files
[+] Description: This is a Directory buster plugin for specified filetypes
[+] Author: Ciaran McNally
[+] Website: https://securit.ie
--------------------------
[+] Name: dirb-custom
[+] Description: This is a Directory buster plugin for a specified list
[+] Author: Ciaran McNally
[+] Website: https://securit.ie
--------------------------
[+] Name: paramethfuzz
[+] Description: Parameter brute forcing but with added fuzzing :)
[+] Author: Ciaran McNally
[+] Website: https://securit.ie
--------------------------
[+] Name: repo
[+] Description: This is a Directory buster for common repo, config & meta-info files
[+] Author: Ciaran McNally
[+] Website: https://securit.ie
--------------------------
[+] Name: fuzzenc
[+] Description: Simple URL encoded fuzzer (use *@* to specify where to fuzz) -dl [list to fuzz with]
[+] Author: Ciaran McNally
[+] Website: https://securit.ie
--------------------------
[+] Name: getpost
[+] Description: This is module can be used to capture GET and POST
[+] Author: Ciaran McNally
[+] Website: https://securit.ie
--------------------------
[+] Name: vhost
[+] Description: This scans a web server for v-hosts
[+] Author: Ciaran McNally
[+] Website: https://securit.ie
--------------------------
[+] Name: archives
[+] Description: A smart archives searcher (ideas from https://github.com/mazen160/bfac/)
[+] Author: Ciaran McNally
[+] Website: https://securit.ie
--------------------------
[+] Name: baseline
[+] Description: This is module can be used to establish a baseline for requests
[+] Author: Ciaran McNally
[+] Website: https://securit.ie
--------------------------
[+] Name: alt
[+] Description: Generate alts of folders and files
[+] Author: Ciaran McNally
[+] Website: https://securit.ie
--------------------------
[+] Name: parameth
[+] Description: A module for parameter brute forcing (based on maK-/parameth)
[+] Author: Ciaran McNally
[+] Website: https://securit.ie
--------------------------
```

scanomaly demo