

Empowering Red and Blue Teams with OSINT

c0c0n 2017, Le Meridian, Kochi.

://\$ whoami

- Shubham Mittal
 - Security Consultant @ NotSoSecure
 - Perimeter Security and OSINT
 - Author - @datasploit
 - Core Organizer - @reconvillage
 - Bike Rider, Beat Boxer

@upgoingstar | upgoingstaar@gmail.com

Agenda

- OSINT Overview
- For Red Teams (Offensive)
 - Company Profiling
 - Perimeter Scoping
 - Employee Profiling
- Tools of Trade
- Future Research Areas
- For Blue Team (Defensive)
 - Monitoring and Alerting
 - Intelligent SIEM Rules
 - DLP

OSINT – Open Source Intelligence

(Intelligence on Information publicly available)

Internet gives you RAW Data. Harvest it.

Open Source Intelligence (OSINT) is the collection and analysis of information gathered from publicly available sources.

Should be used by?

- Pen-testers
- Security Engineers
- Product Security Companies
- Cyber Investigators
- Sales / Market Research

How OSINT can help Red Teams

Red Teams

- Scoping Attack Surface
- Technology Profiling
- Github
- Paste(s)
- Employee Profiling
- Breach Data
- Nerdy Data

Digital Asset Scoping

- whois (who.is) > ASN ID
- Reverse Whois
 - `whois -h whois.radb.net -- '-i origin ASN-ID' | grep -Eo '([0-9.]{4}){4}/[0-9]+' | sort -n | uniq -c`
 - <https://mxtoolbox.com/SuperTool.aspx>
 - Nslookup (terminal)
 - Dig (dig reconvillage.org, dig reconvillage.org cname)
- Acquisitions.

Digital Asset Scoping – Subdomain Enumeration

- Sub-domain Enumeration
 - DNSSEC Walking (Kudos to [@jhaddix](#) for suggesting)
 - Certificate Transparency Reports, Forums
 - Shodan/Censys, Cname Records, DNS Dumpster, Netcraft, WolframAlpha
 - Tools - Sublist3r, DataSploit.

dnssecwalk (part of the ipv6 Toolkit)

<https://www.thc.org/thc-ipv6/>

```
Starting DNSSEC walking on server 8.8.8.8 about weberdns.de.
Found: 16a.weberdns.de.
Found: 16aaaa.weberdns.de.
Found: 16dual.weberdns.de.
Found: 32a.weberdns.de.
Found: 32aaaa.weberdns.de.
Found: 32aaaa-long.weberdns.de.
Found: 32dual.weberdns.de.
Found: 32dual-long.weberdns.de.
Found: 64a.weberdns.de.
Found: 64aaaa.weberdns.de.
Found: 64dual.weberdns.de.
Found: fg.weberdns.de.
Found: host-dane.weberdns.de.
Found: _443._tcp.host-dane.weberdns.de.
Found: host-dane-self.weberdns.de.
Found: _443._tcp.host-dane-self.weberdns.de.
Found: host-dnssec.weberdns.de.
Found: ip.weberdns.de.
Found: lx.weberdns.de.
Found: mail.weberdns.de.
Found: _25._tcp.mail.weberdns.de.
Found: ns0.weberdns.de.
Found: ns1.weberdns.de.
Found: ns1-v4.weberdns.de.
Found: ns1-v6.weberdns.de.
Found: ns2.weberdns.de.
Found: ns3.weberdns.de.
Found: pa.weberdns.de.
Found: sub.sub.weberdns.de.
Found: ttl-long.weberdns.de.
Found: ttl-short.weberdns.de.
Found: txt.weberdns.de.
Found: viola.weberdns.de.
Found: webmail.weberdns.de.
Found: www.weberdns.de.
Done, 35 entries found.
```

Custom Script(Certificate

Transparency Report) - DEMO

```
shubhammittal:Pythoncodes/ $ python certificate_transparency_domain_enum.py simple.com
#####
CT Subdomain Finder.py
This scripts walks through Certificate Transparency Reports, and enumerates Domains/Subdomain. Sweet?
#####

[+] Iterating through page #1
[+] Iterating through page #2
[+] Iterating through page #3
[+] Iterating through page #4
[+] Iterating through page #5
[+] Iterating through page #6
[+] Iterating through page #7
[+] Iterating through page #8
[+] Iterating through page #9
[+] Iterating through page #10
[+] Iterating through page #11
[+] Iterating through page #12
[+] Iterating through page #13
[+] Iterating through page #14
[+] Iterating through page #15
[+] Iterating through page #16
[+] Iterating through page #17

[+] List of enumerated subdomains

click.e.simple.com
simple.com
banksimple.com
bank.simple.com
akansai-san8.exacttarget.com
api.simple.com
www.simple.com
links.simple.com
pages.e.simple.com
android.fj.simple.com
status.simple.com
email.simple.com
```

<https://blog.webernetz.net/2016/11/22/how-to-walk-dnssec-zones-dnsrecon/>

Quick Checks

- HTTP / HTTPS?
- 404 Not Found? 403 Forbidden?
- 500 Internal Server Error?
- .git / .svn / htaccess.txt / bash_history / web.config / admin / , etc.

```
shubhammittal@kali:~$ (master*) $ python check_subdomain_from_file.py ripple.com
www.ripple.com: [<DNS IN CNAME rdata: ripple.com.>]
[+] HTTP - www.ripple.com: 200
[+] HTTPS - www.ripple.com: 200
alipay.ripple.com: No Records Found
api.ripple.com: No Records Found
auth1.ripple.com: No Records Found
blobvault.ripple.com: No Records Found
blog.ripple.com: No Records Found
charts.ripple.com: No Records Found
charts1.ripple.com: No Records Found
charts2.ripple.com: No Records Found
data.ripple.com: [<DNS IN CNAME rdata: p.shared.global.fastly.net.>]
[+] HTTP - data.ripple.com: 200
[+] HTTPS - data.ripple.com: 200
dev-api-remit.ripple.com: No Records Found
download.ripple.com: [<DNS IN CNAME rdata: d3eq3exmf3460d.cloudfront.net.>]
[+] HTTP - download.ripple.com: 200
[+] HTTPS - download.ripple.com: 200
forum.ripple.com: No Records Found
history.ripple.com: No Records Found
historytest.ripple.com: No Records Found
huginn.ripple.com: No Records Found
acme.i.ripple.com: No Records Found
aj1.i.ripple.com: No Records Found
aj2.i.ripple.com: No Records Found
altnet1.i.ripple.com: No Records Found
altnet2.i.ripple.com: No Records Found
```

```
test-north.rc.ripple.com: No Records Found
test-south.rc.ripple.com: No Records Found
ripdtop.ripple.com: [<DNS IN CNAME rdata: ripdtop.ops.ripple.com.>]
```

```
[+] HTTP - ripdtop.ripple.com: 401
[+] HTTPS - ripdtop.ripple.com: 401
```

```
s1.ripple.com: No Records Found
staging.ripple.com: No Records Found
id.staging.ripple.com: No Records Found
validators.ripple.com: [<DNS IN CNAME rdata: charts2.ripple.com.>]
[+] HTTP - validators.ripple.com: 200
wiki.ripple.com: No Records Found
```

```
[+] Following subdomains might be vulnerable to Subdomain Take Over Vulnerability.
['http', 'ripdtop.ripple.com']
```

Pro-active Search

```
tr.php?id= : http://www.exploit-db.com/ghdb/2000/  
tr.php?id= : http://www.exploit-db.com/ghdb/2001/  
option=com_mydyngallery : http://www.exploit-db.com/ghdb/2004/  
index.php?mod=sondages : http://www.exploit-db.com/ghdb/2006/  
trl.php?id=" Forced Matrix : http://www.exploit-db.com/ghdb/2009/  
com_ckforms : http://www.exploit-db.com/ghdb/2011/  
com_prayercenter : http://www.exploit-db.com/ghdb/2012/  
com_ccnewsletter : http://www.exploit-db.com/ghdb/2015/  
add_soft.php : http://www.exploit-db.com/ghdb/2016/  
/myspeech/ : http://www.exploit-db.com/ghdb/2023/  
myLDlinker.php : http://www.exploit-db.com/ghdb/2028/  
com_idoblog : http://www.exploit-db.com/ghdb/2029/  
com_gallery *func : http://www.exploit-db.com/ghdb/2036/  
"/modules/myTopics/ : http://www.exploit-db.com/ghdb/2038/  
com_ckforms : http://www.exploit-db.com/ghdb/2039/  
index.php?site=" "W-Agora : http://www.exploit-db.com/ghdb/2040/  
categoria.php?ID= comune : http://www.exploit-db.com/ghdb/2041/  
index.php?m_id= : http://www.exploit-db.com/ghdb/2043/  
openwebfund : http://aaa  
/index.asp?newsid= : http://www.exploit-db.com/ghdb/2044/  
"showCat.php?cat_id : http://www.exploit-db.com/ghdb/2045/  
inc_accountlistmanager.asp : http://www.exploit-db.com/ghdb/2049/  
com_jomestate : http://www.exploit-db.com/ghdb/2050/
```

inurl:com_ckforms

All Maps Videos Images News More Settings Tools

Page 6 of about 2,00,000 results (1.49 seconds)

Zoekresultaten voor 'Aloe Vera Sap/*?option=com_ckforms'
www.aloevera.nl/.../result/?...Sap%2F%2F%3Foption%3Dcom_ckf... - Translate this page
Default Description.

WATCH: In Spokane, Washington, Running is Tradition | Trail Runner ...
trailrunnermag.com/?option=com_ckforms&view=ckforms&id=29 ▼
Aug 7, 2017 - Spokane, Washington has a deep history of running—and a vast network of trails. This video, by HOKA One One, profiles the town's running ...

Feedback - Cello Wim Plast Ltd.
www.cellowimplast.com/index.php?option=com_ckforms&view=ckforms&id... ▼
Wim Plast Limited is one of the group company of 'cello' group. Wim Plast Limited incorporated on 7th October, 1988, and listed in the year 1994 at the Bombay ...

Network - Cello Wim Plast Ltd.
www.cellowimplast.com/index.php?option=com_ckforms&view=ckforms&id... ▼
Wim Plast Limited is one of the group company of 'cello' group. Wim Plast Limited incorporated on 7th October, 1988, and listed in the year 1994 at the Bombay ...

Contact - Passion Western
www.passionwestern.fr/index.php?option=com_ckforms...1... ▼ Translate this page
passion western country danse association favence nice var.

Technology Profiling - BuildWith

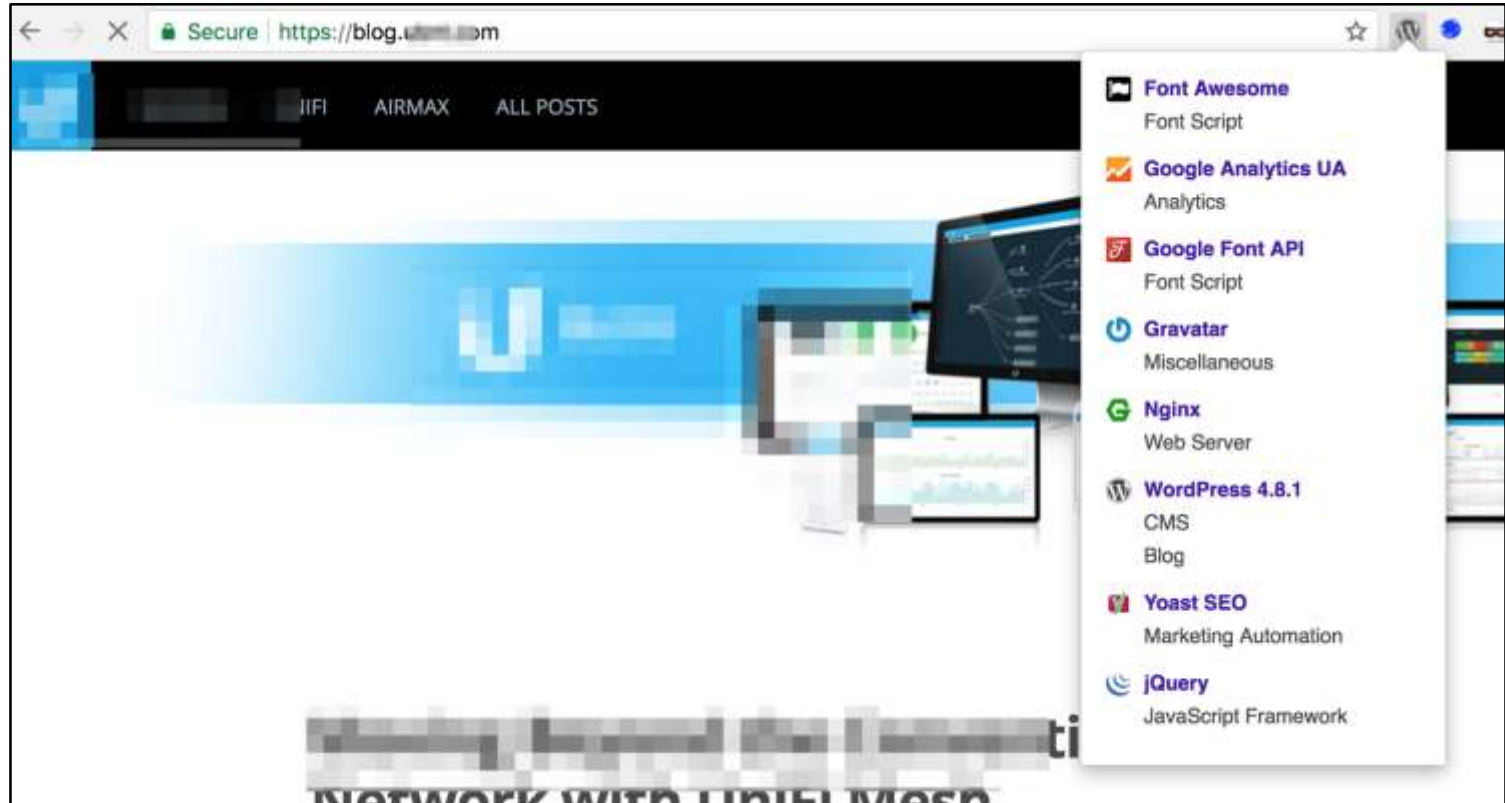
The screenshot shows the website **reconvillage.org** with a BuildWith technology profiling overlay. The overlay lists the following technologies:

- SSL Certificates**
 - DigiCert SSL**
Usage Statistics - Websites using DigiCert SSL
Certificate provided by DigiCert.
- Analytics and Tracking**
 - Google Analytics**
Usage Statistics - Websites using Google Analytics
Google Analytics offers a host of compelling features and benefits for everyone from senior executives and advertising and marketing professionals to site owners and content developers.
 - Google Universal Analytics**
Usage Statistics - Websites using Google Universal Analytics
- JavaScript Libraries and Functions**
 - Twitter Platform**
Usage Statistics - Websites using Twitter Platform
The page embeds the Twitter platform in one method or another.

The screenshot shows the website **reconvillage.org** with a BuildWith technology profiling overlay. The overlay lists the following technologies:

- Syndication Techniques**
 - Atom**
Usage Statistics - Websites using Atom
Atom Syndication Format is an XML language used for web feeds very similar to RSS.
- Operating Systems and Servers**
 - GitHub Hosting**
Usage Statistics - Websites using Github Hosting
This site is hosted on Github infrastructure.
- Web Master Registration**
 - Google Webmaster**
Usage Statistics - Websites using Google Webmaster
Webmaster tools provide you with a free and easy way to make your site more Google-friendly.
- Preferences**
 - ☐ Hide Descriptions
 - ☐ Hide Links

Wappalyzer




Github

[Repositories](#)
[Code 38K](#)
[Commits](#)
[Issues 1](#)
[Wikis](#)
[Users](#)

[Advanced search](#)

38,888 code results


[Python](#)

Showing the top three matches Last indexed 17 days ago

```

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
100
```

<https://hackerone.com/reports/248693>



Paste(s) Sites

powered by Google Custom Search

[test@test.com.password test@test.com.password test@test.com ...](#)
<https://pastebin.com/HethwdzE>
5 days ago ... test@test.com.password test@test.com.password test@test.com.password test@
test.com.password test@test.com.password ...

[avaJS question - GitHub](#)
<https://gist.github.com/.../38f79278d62ed8ceb2370f137d8c42ad>
function makeRequest(){, const auth0BaseUrl = Config.AUTH_URL, const mock = { username:
"test03@222222.com", password: "password!test", ...

[sessions-writing-tests.test.js - GitHub](#)
<https://gist.github.com/.../5d8f1ac81e70e9321f7e4b8f75ec2ace>
It(attempt with correct password succeeds, async () => {, await store.dispatch(
authenticateUser("email@test.com", "password"));, expect(store.getActions());

[mickaelandrieu's gists - GitHub](#)
<https://gist.github.com/mickaelandrieu?direction=asc&sort...>
casperjs --includes=utilities/login.js test@test.com password domain test bank.js. Unable to open file:
test@test.com. 1 file · 0 forks · 0 comments · 0 stars.

[Rails 3 with options for devise, jquery, cucumber, capybara, rspec ...](#)
<https://gist.github.com/odmweb/707640>
Aug 4, 2011 ... gem 'machinist', '>= 2.0.0.beta2', :group => :test if machinist, gem 'devise' if ..., puts "The seed
user is email 'user@test.com' pass 'please.'" end ...

[simple-express-server-bearer.js - GitHub](#)
<https://gist.github.com/.../196124622dccc7b6d45b2fd7401bf2a1>
const Users = [, { id: 1, name: 'Toto', email: 'toto@test.com', password: 'toto123' },], function generateToken()
{, return crypto.randomBytes(32).toString('hex');, ...

[creating and testing permissions and test groups in django tests ...](#)
<https://gist.github.com/treytruncie/a292366d8ae0de4e50f8>
self.user = User.objects.create_user(username="test", email="test@test.com", password="test"). def
tearDown(self):, self.user.delete(), self.group.delete(), ...

Secure https://publicbhost.dmca.gripe			
Sotusbase.com is the fastest database lookup that has ever existed. Check it out!			
HOME	ADVANCED SEARCH	NO-JS SEARCH	CONTACT
DIRECTORY			
Index of /			
../			
random/			
megs.co.nz_partialdump.7z	19244760	22-May-2017	12:49 AM
VK.COM_100M.rar	1202556637	22-May-2017	01:28 AM
Adobe_152M.tar.gz	1457520640	22-May-2017	12:47 AM
investbank.ae-2016-04-25.zip	540535651	22-May-2017	12:59 AM
DLN.net_3M_2016.7z	95881345	22-May-2017	12:28 AM
fling.com_40M_users.sql.7z	627507200	22-May-2017	12:47 AM
blackhatworld.7z	67100270	22-May-2017	12:25 AM
acne.org_ibf_members_11_25_2014.7z	45052409	22-May-2017	12:23 AM
FS3Hax.net.txt.gz	32544874	22-May-2017	12:59 AM
torrent-invitee.com_forum-2016-08-07.sql.gz	1016725702	22-May-2017	01:16 AM
Ashley_Madison_users.7z	1773584384	22-May-2017	12:47 AM
178_all.txt	266794656	22-May-2017	12:26 AM
index.php	3172	22-May-2017	05:05 PM
xst.7z	227685739	22-May-2017	01:12 AM
Keplit Plain (SHA1).7z	117776109	22-May-2017	01:14 AM
leet.cc_partial.txt.7z	77383482	22-May-2017	12:53 AM
Tumblr_2013_users.7z	2114751092	22-May-2017	01:35 AM
NaughtyAmerica.7z	299009564	22-May-2017	12:59 AM
zookk.com.7z	1802518298	22-May-2017	01:39 AM
MineField180K.7z	18419822	22-May-2017	12:50 AM
nulled.io.sql.7z	760252229	22-May-2017	01:06 AM
muslimmatch.com.7z	110125592	22-May-2017	12:56 AM
braxers.com April 2013.7z	13982175	22-May-2017	12:25 AM
Libero.it 900k.zip	42068740	22-May-2017	12:52 AM
STRATFOR USERS DATABASE.7z	46643274	22-May-2017	01:01 AM
17.Media.rar	775184173	22-May-2017	12:35 AM
STRATFOR EMAIL HACK.7z	96631480	22-May-2017	01:01 AM
Ashley_Madison_users.gz	1801781248	22-May-2017	12:47 AM
patreondump.tar.gz	3997819699	22-May-2017	01:41 AM
inweb.rar	427671552	22-May-2017	12:47 AM
Arma3Life.sql	105118884	22-May-2017	12:26 AM
OwnagePranks2016.7z	116115769	22-May-2017	12:59 AM
kaixin001.com.7z	98443782	22-May-2017	12:56 AM
taobao.7z	158520312	22-May-2017	01:03 AM
linkedin_all.7z	4535170532	22-May-2017	01:41 AM
Solomid.net_ipb_November_2014.txt.7z	11854746	22-May-2017	01:00 AM

Public Password Dumps

Not 'Google' Search Engines

- Metasearch engine – Polymeta.com
- People search engine -Pipl.com, Peekyou, Marketvisual
- Business/Company Search - Zoominfo
- Social Search Engine - Socialmention.com
- Phone Number Search Engine – Truecaller
- Wayback machine
- Computational knowledge engine – Wolframalpha
- Clustering Search Engine - search.carrot2.org

Domain IP History



Domain IP History

- Cloudflare / Incapsula / Sucuri.
- Domain History reveals earlier IP Addresses.
- IP still Live = Bypass rate limiting, firewall rules, etc.

IP history results for test.com.

IP Address	Location	IP Address Owner	Last seen on this IP
69.172.200.235	New York - United States	Cogeco Peer 1	2017-08-15
50.23.225.49	Dallas - United States	SoftLayer Technologies Inc.	2017-06-18
69.172.200.235	New York - United States	Cogeco Peer 1	2017-06-17
50.23.225.49	Dallas - United States	SoftLayer Technologies Inc.	2017-06-11
69.172.200.235	New York - United States	Cogeco Peer 1	2017-06-10
204.12.0.50	Newark - United States	HostMySite	2011-04-04

Public Scan Engines

- <https://www.qualys.com/forms/freescan/>
- <https://urlscan.io>
- <https://asafaweb.com>

Scan of **simple.com** — Simple | Online Banking With Built-In Budgeting & Saving Tools

You can [schedule a regular scan of this URL](#) so you can be automatically notified of any changes in the future.

Server: Unknown | X-Powered-By: Unknown | X-AspNet-Version: Unknown | X-AspNetMvc-Version: Unknown | Web-forms app: No | ASP.NET site: Unknown | ASP.NET version: Unknown | 6 requests were made by ASaWeb:

URL	Page title	Response size	Duration
1. http://simple.com/	Simple Online Banking With Built-In Budgeting & Saving Tools	31,632 bytes	120 ms
2. http://www.simple.com/trace.asp	404	22,239 bytes	628 ms
3. https://www.simple.com/c	404	22,239 bytes	394 ms
4. https://www.simple.com/foo/trace.asp	404	22,239 bytes	404 ms
5. https://www.simple.com/ (POST 1,001 params)	None	0 bytes	2 ms
6. https://www.simple.com/almah.axd	404	22,239 bytes	648 ms
		120,588 bytes	2,196 ms

Tracing: Pass Custom errors: Pass Stack trace: Pass Request validation: Not tested

HTTP to HTTPS: Warning Hash dos patch: Not tested ELMAH log: Pass Excessive headers: Pass

HTTP only cookies: Pass Secure cookies: Pass Clickjacking: Pass View state MAC: Not tested

MetaData

Data about the Data.

Can find:

- Applications used to generate PDF/Docx./etc. on servers
- Exif Data (Media File Data)
- Geolocations
- Author
- Platform

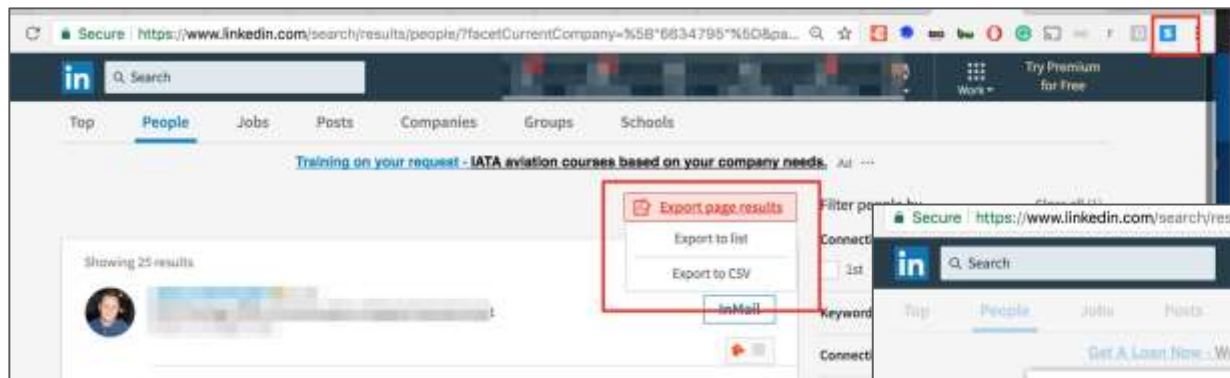
```
shubhammittal:Downloads/ $ exiftool test_document.pdf
ExifTool Version Number      : 10.14
File Name                    : test_document.pdf
Directory                   : .
File Size                   : 185 kB
File Modification Date/Time  : 2016:05:15 13:29:11+05:30
File Access Date/Time       : 2017:08:13 18:08:43+05:30
File Inode Change Date/Time  : 2016:05:15 13:29:11+05:30
File Permissions             : rw-r--r--
File Type                   : PDF
File Type Extension         : pdf
MIME Type                   : application/pdf
PDF Version                 : 1.5
Linearized                  : Yes
Tagged PDF                  : Yes
XMP Toolkit                 : Adobe XMP Core 5.6-c014 79.156797, 2014/08/20-09:53:02
Create Date                 : 2015:07:31 13:01:53-04:00
Metadata Date               : 2015:07:31 13:01:53-04:00
Modify Date                 : 2015:07:31 13:01:53-04:00
Creator Tool                : Adobe InDesign CC 2014 (Windows)
Instance ID                 : uuid:4791e430-b5a8-47f8-b1e0-c7b5df5435a4
Original Document ID        : xmp.did:bbc7e9fa-731f-3541-a38c-1379df186c6b
Document ID                 : xmp.id:73d6b67e-4760-c94e-b778-66690f3304c7
Rendition Class              : proof:pdf
Derived From Instance ID    : xmp.iid:1a9d5212-808d-2e49-a064-73f4917221cd
Derived From Document ID    : xmp.did:b63aa7a0-7b56-9f44-acb1-95d05affeaae
Derived From Original Document ID: xmp.did:bbc7e9fa-731f-3541-a38c-1379df186c6b
Derived From Rendition Class : default
History Action               : converted
History Parameters          : from application/x-indesign to application/pdf
History Software Agent      : Adobe InDesign CC 2014 (Windows)
History Changed              : /
History When                 : 2015:07:31 13:01:53-04:00
Format                      : application/pdf
Producer                    : Adobe PDF Library 11.0
Trapped                      : False
Page Count                  : 6
Creator                     : Adobe InDesign CC 2014 (Windows)
```

**TCPDF CVE-2017-6100 - Local File
Include Vulnerability**

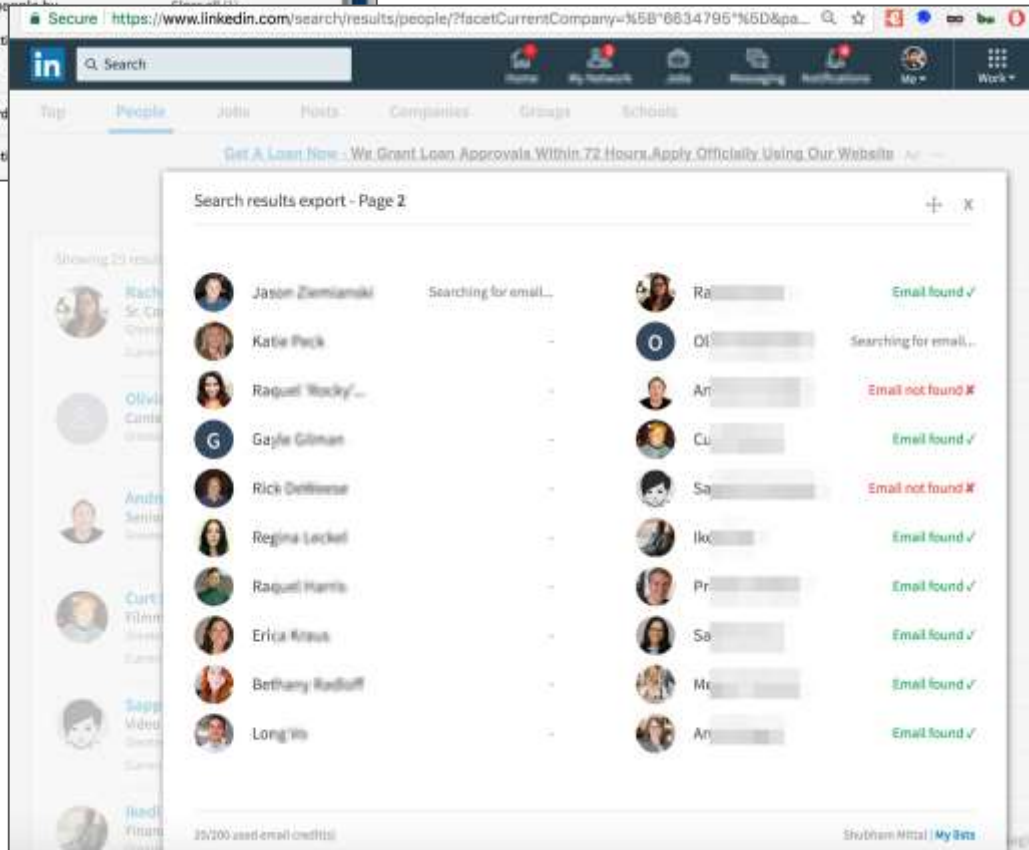
Employee Profiling

- Email-harvester
- DataSploit
- LinkedIn
 - https://www.linkedin.com/search/results/companies/?keywords=company&origin=SWITCH_SEARCH_VERTICAL
- Email Hunter
- Skrapp

```
shubhamittal:datasploit/ (master*) $ python domain/domain_emailhunter.py test.com  
--> Harvesting Email Addresses:.  
  
mike@test.com  
second@test.com  
alice@test.com  
sample@test.com  
pavel.boiko@test.com  
emily.bache@test.com  
someone@test.com  
recipient@test.com  
internal@test.com  
external@test.com  
contact@test.com  
anonymous@test.com  
me@test.com  
customer@test.com  
root@test.com  
matt@test.com  
ananda@test.com  
sender@test.com  
deepa@test.com  
address@test.com  
zoe.clarke@test.com  
lisa@test.com  
tony@test.com  
to@test.com  
alan.alston@test.com  
alicia.foster@test.com  
fiona.murphy@test.com  
kanar@test.com  
isaac@test.com  
miller-aichholz@test.com  
richard@test.com  
anand.kumar@test.com  
santosh@test.com  
henry.pan@test.com  
david.boyne@test.com  
iyad@test.com  
lucas@test.com  
matthew@test.com  
gaston@test.com  
pascal@test.com  
marco@test.com  
matt.hall@test.com  
halin@test.com  
kevin@test.com  
jane@test.com  
dirk@test.com  
user@test.com
```



Linked employee
email extract using
Skrapp / Hunter



```
shubhammittal:Pythoncodes/ $ python email_pattern_generator.py 'Andy Butler' isaca.org
[+] Generating Email ID Patterns for Andy Butler AT isaca.org

andy@isaca.org
butler@isaca.org
butler.andy@isaca.org
andy.butler@isaca.org
butlerandy@isaca.org
andybutler@isaca.org
a.butler@isaca.org
b.andy@isaca.org
abutler@isaca.org
butlera@isaca.org
ab@isaca.org
```

Custom Script

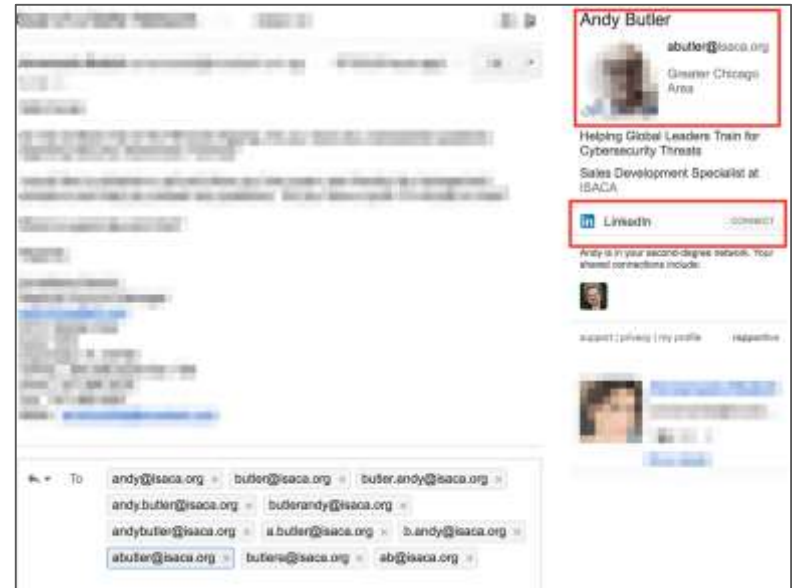
```
import sys

name = sys.argv[1]
domain = sys.argv[2]
print "[+] Generating Email ID Patterns for %s AT %s\n" % (name, domain)

names = name.split(' ')
firstname = str.lower(names[0])
lastname = str.lower(names[-1])
if len(names) > 2:
    middlename = str.lower(names[-2])

print "%s@s" % (firstname, domain) #shubham
print "%s@s" % (lastname, domain) #mittal
print "%s@s" % (lastname + "." + firstname, domain) # mittal.shubham
print "%s@s" % (firstname + "." + lastname, domain) # shubham.mittal
print "%s@s" % (lastname + firstname, domain) # mittalshubham
print "%s@s" % (firstname + lastname, domain) # shubhammittal
print "%s@s" % (firstname[0] + "." + lastname, domain) # s.mittal
print "%s@s" % (lastname[0] + "." + firstname, domain) # m.shubham
print "%s@s" % (firstname[0] + lastname, domain) # smittal
print "%s@s" % (lastname + firstname[0], domain) # mittals
print "%s@s" % (firstname[0] + lastname[0], domain) # sm
```

Code



Rapportive

Email-id to Username?

Social Media Accounts

Forum Searches (boardreader.com)

Clearbit / Full Contact

DataSploit

```
shubhammittal:datasploit/ (master*) $ python emailOsint.py upgoingstaar@gmail.com

---> Basic Email Check(s)..

Is it a free Email Address?: Yes
Email ID Exist?: Yes
Can this domain recieve emails?: Yes
Is it a Disposable email?: No

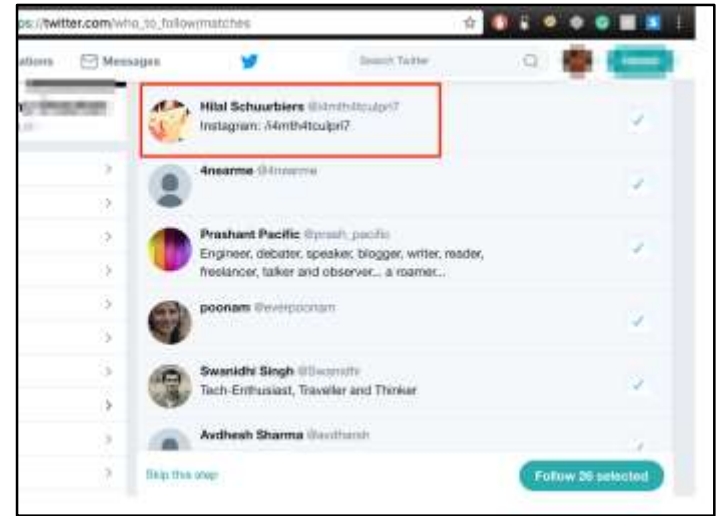
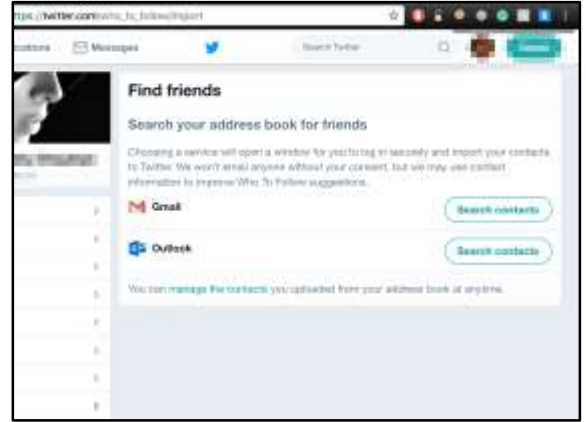
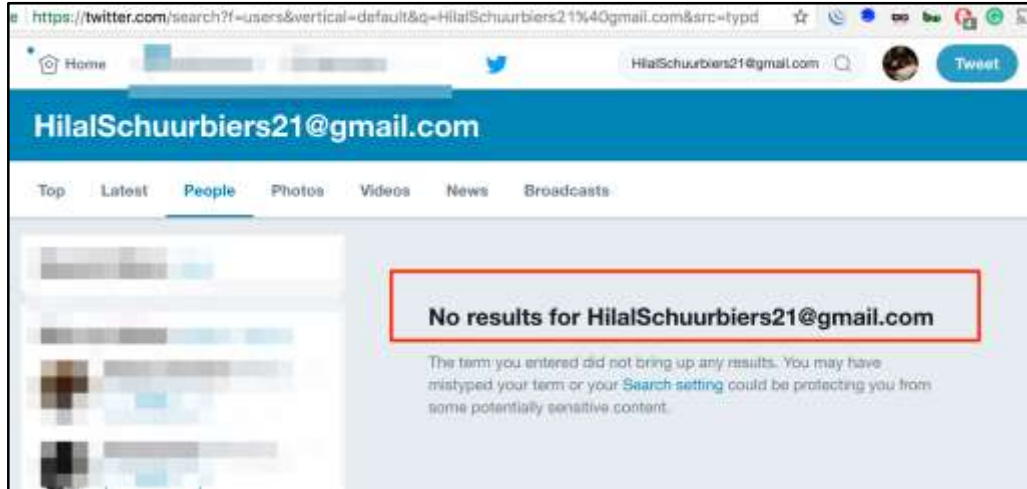
---> Searching Clearbit

twitter details:
bio: Author of @datasploit and manages @reconvillage. Tweets are Personal. #InfoSec #OSINT
handle: upgoingstar,
site: https://github.com/upgoingstar/,
followers: 1020,
location: Bangalore ,
favorites: 290,
following: 611,
id: 16852719,
statuses: 1312,
avatar: https://pbs.twimg.com/profile_images/2281757680/xhqe02vqyw37ivglli8f.jpeg,
site details:
```

>> User to Images , Reverse Image Search, User profiling (More useful for SE)

>> Find leaked creds, tokens, confidential urls/IPs, slack keys, api key, etc.

Email-id to Username?





JOIN THE BLUE TEAM!

We have cookies! And Caboose!

Blue Team.

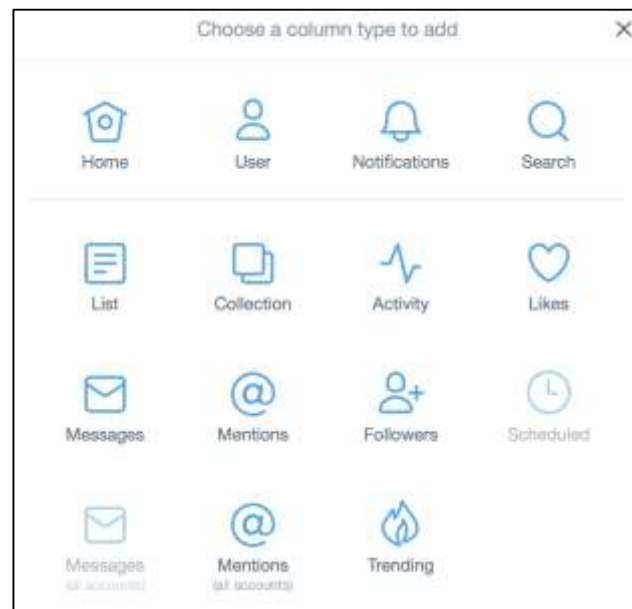
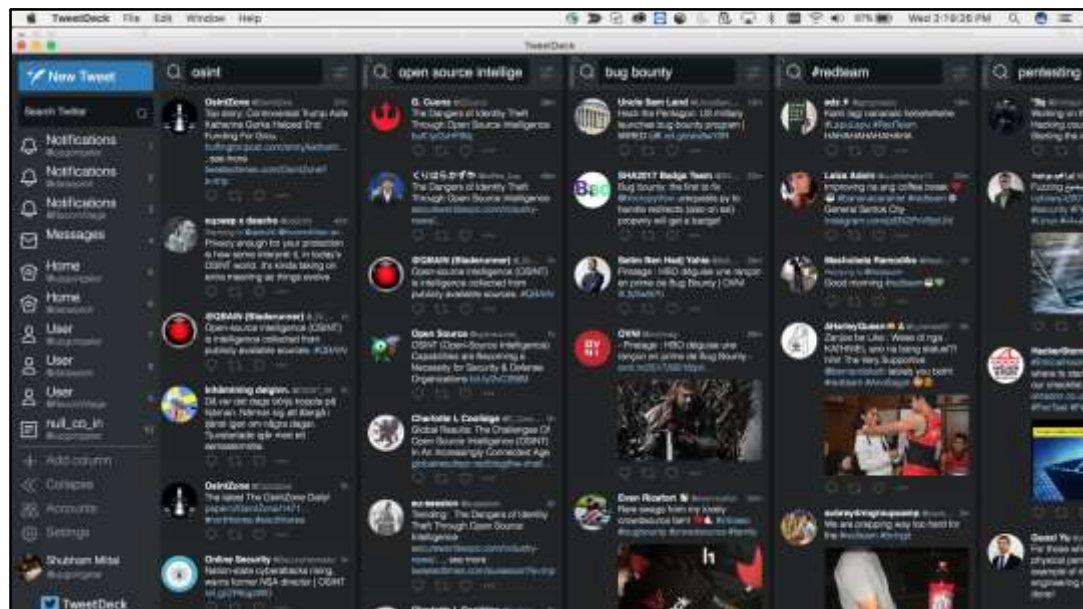
- Active Monitoring on keywords.
- Alerting (while reducing noise)
- Scan/OSINT your Attack Surface Area
 - Scoping is not required - Simply find the perimeter from Devops/Central Deployment Team.
- Keep an eye on Employees (Profile their personal code share accounts).
- Review Job Openings / Questions in Forums, etc.
- Defensive Measures - Data Loss Prevention
 - Strip off metadata from files going outside.

Tweetmonitor.py / Tweetdeck

```
shubhammittal:TweetMonitor/ (master*) $ python tweetmonitor.py -k hacked -m upgoingstaar@gmail.com
----- Twitter bot kicked off -----
>>AnnRodriguez055 posted: @erikacostell LOOK!!! TESSA GOT HACKED!! https://t.co/mrJtCv2c4s
[+] Mail sent to concerned authorities.
>>UwantSomaThis posted: @cassums_ @colleencpa @ChrisMillsShow @rosetaths Is that somehow evidence to you cass?
GT220
[+] Mail sent to concerned authorities.
>>Rchrisalhd posted: @AskPS_UK My account was hacked so...
```



Tweetmonitor.py / Tweetdeck



Scumblr

Scumblr

MENU

Results

Displaying results 1 - 25 of 53 in total

1 2 3 Next Last

Title	Status	Domain	Link	Created At	Updated At	
▶ <input type="checkbox"/> osint		github.com	Link	1 day ago	1 day ago	Show
▶ <input type="checkbox"/> Exploiting Public Information for OSINT		reddit.com	Link	2 days ago	2 days ago	Show
▶ <input type="checkbox"/> TIL There is a free OSINT-oriented Linux distro called, "Bouscador" designed in part by cyber cri...		reddit.com	Link	2 days ago	2 days ago	Show
▶ <input type="checkbox"/> Automated OSINT Toolset		reddit.com	Link	2 days ago	2 days ago	Show
▶ <input type="checkbox"/> What OSINT Tells Us About the Bakery Bombing		reddit.com	Link	2 days ago	2 days ago	Show
▶ <input type="checkbox"/> Gaming Meets OSINT: Using Python to Help Solve Her Story		reddit.com	Link	2 days ago	2 days ago	Show
▶ <input type="checkbox"/> Air-Hammer: New tool that leverages OSINT to break into WPA Enterprise networks		reddit.com	Link	2 days ago	2 days ago	Show
▶ <input type="checkbox"/> Creating an OSINT dashboard		reddit.com	Link	2 days ago	2 days ago	Show
▶ <input type="checkbox"/> List of OSINT tools and how you learn how to use them		reddit.com	Link	2 days ago	2 days ago	Show
▶ <input type="checkbox"/> OSINT basics: Finding accounts, profiling, honeypots, spam email probes, impersonation, and fault...		reddit.com	Link	2 days ago	2 days ago	Show
▶ <input type="checkbox"/> Scan Darknet with Python (Tutorial)		reddit.com	Link	2 days ago	2 days ago	Show

Filter

URL

URL Does Not Contain

Title

Title Does Not Contain

Tags


Assignee

Status

Google Alerts

Alerts

Monitor the web for interesting new content

 testalert

How often	At most once a day	⬆ ⬇ ⬆
Sources	Automatic	⬆ ⬇ ⬆
Language	English	⬆ ⬇ ⬆
Region	Any Region	⬆ ⬇ ⬆
How many	Only the best results	⬆ ⬇ ⬆
Deliver to	upgoingstaar@gmail.com	⬆ ⬇ ⬆

Create Alert

Hide options ▲

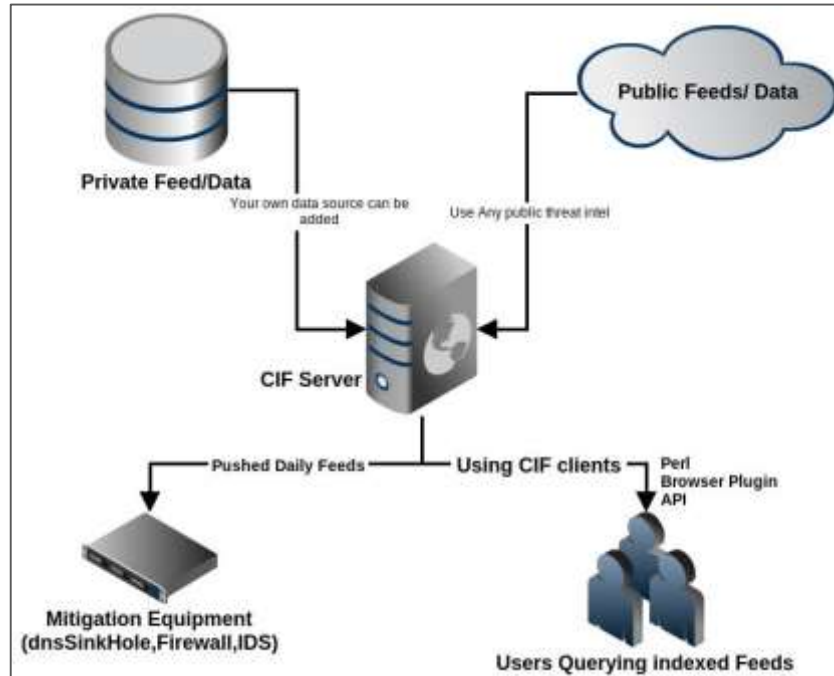
Page Monitor - ChangeDetect / Follow.net

<input type="checkbox"/>	<input type="star"/>	» Follow.net Stories	Inbox	[redacted]	has 1 new story - go2.follow.net/email/cli	10/09/2016
<input type="checkbox"/>	<input type="star"/>	» Follow.net Stories	Inbox	[redacted]	has 1 new story - go2.follow.net/email/cli	01/09/2016
<input type="checkbox"/>	<input type="star"/>	» Follow.net Stories	Inbox	[redacted]	has 1 new story - go2.follow.net/email/cli	30/08/2016
<input type="checkbox"/>	<input type="star"/>	» Follow.net Stories	Inbox	[redacted]	has 1 new story - go2.follow.net/email/cli	24/08/2016
<input type="checkbox"/>	<input type="star"/>	» Follow.net Stories	Inbox	[redacted]	has 6 new stories - go2.follow.net/email/cli	23/08/2016
<input type="checkbox"/>	<input type="star"/>	» Follow.net Stories	Inbox	[redacted]	has 2 new stories - go2.follow.net/email/cli	12/08/2016
<input type="checkbox"/>	<input type="star"/>	» Follow.net Stories	Inbox	[redacted]	has 1 new story - go2.follow.net/email/cli	11/08/2016
<input type="checkbox"/>	<input type="star"/>	» Follow.net Stories	Inbox	[redacted]	has 1 new story - go2.follow.net/email/cli	08/08/2016
<input type="checkbox"/>	<input type="star"/>	» Follow.net Stories	Inbox	[redacted]	new stories - go2.follow.net/email/cli	24/07/2016
<input type="checkbox"/>	<input type="star"/>	» Follow.net Stories	Inbox	[redacted]	has 4 new stories - go2.follow.net/email/cli	22/07/2016
<input type="checkbox"/>	<input type="star"/>	» Follow.net Stories	Inbox	[redacted]	has 40 new stories - go2.follow.net/email/cli	21/07/2016
<input type="checkbox"/>	<input type="star"/>	» Follow.net Stories	Inbox	[redacted]	has 1 new story - go2.follow.net/email/cli	20/07/2016
<input type="checkbox"/>	<input type="star"/>	» Follow.net Stories	Inbox	[redacted]	has 1 new story - go2.follow.net/email/cli	08/07/2016
<input type="checkbox"/>	<input type="star"/>	» Follow.net Stories	Inbox	[redacted]	has 3 new stories - go2.follow.net/email/cli	21/06/2016
<input type="checkbox"/>	<input type="star"/>	» Follow.net Stories	Inbox	[redacted]	new story - go2.follow.net/email/cli	09/06/2016
<input type="checkbox"/>	<input type="star"/>	» Follow.net Stories	Inbox	[redacted]	has 1 new story - go2.follow.net/email/cli	05/06/2016
<input type="checkbox"/>	<input type="star"/>	» Follow.net Stories	Inbox	[redacted]	has 1 new story - go2.follow.net/email/cli	04/06/2016



SIEM << Threat Intel Feed (robtex,etc., check for already blacklisted IPs)

Collective Intelligence Framework



Tools of Trade

Spiderfoot

Maltego

Recon-ng

Gosint

Scrublr

Belati

DataSploit

X-ray

Sublist3r

Exiftool

theHarvester

Tinfoleak

Foca

Gitrob

Future Research

- Data Co-relation
- Noise Reduction
- Tap Darknet



upgoingstaar@gmail.com | @upgoingstar