

Penetration Testing Student

Information Gathering

Section 03 | Module 01

© Caendra Inc. 2019
All Rights Reserved

Table of Contents

Module 01 | Information Gathering

1.1 Introduction

1.2 Open-Source Intelligence

1.3 Subdomain Enumeration

1.4 The Importance of Information Gathering



Learning Objectives

By the end of this module, you should have a better understanding of:

- ✓ What OSINT is
- ✓ Basic techniques of collecting information about your target



Introduction



1.1 Introduction

Welcome to the **penetration testing** section of the course!

We start this module off by discussing all the phases of a penetration test, focusing on **tools, techniques, and methodologies** used by professionals to carry out a penetration test engagement.



1.1 Introduction

Information Gathering is the first and one of the most crucial phases of an engagement.

As you have already seen in the prerequisites section, this step of the process helps you understand the target organization, widen the attack surface and mount efficient and targeted attacks.



1.1 Introduction

Similarly to a black hat hacker, a penetration tester cannot leave any stone unturned.

In this module, you will see how to use public information to get a deeper understanding of the client's organization under the business and infrastructural point of view.



Open-Source Intelligence



1.2 Open-Source Intelligence

How does this support my pentesting career?

- Widening the attack surface
- Mounting targeted attacks
- Sharpening your tools in preparation for the next phases

1.2 Open-Source Intelligence

Until a few years ago, collecting information about a company involved:

- Getting information from the press
- Looking for addresses and phone numbers in the phone directory
- Visiting the company web site to get information about systems and products

1.2 Open-Source Intelligence

Nowadays, you can do the same thing more efficiently by exploiting information available on **social networks, public sites** and by **visiting the company websites**.



1.2.1 Social Networks Information Gathering

In the following slides, you will see how to use social networks to perform information gathering. In fact, many successful security breaches exploit the weakest link in the security chain: **humans!**

Every day, people get to work and actively use corporate systems and services, so their personal security posture on the Internet heavily influences the security of the companies they work for.

```
24 # The experiment will result in
25 # observations - an array of Observations, in which
26 # control - the control observation
27
28 def initialize(experiment, observations = [], control = nil)
29   @experiment = experiment
30   @observations = observations
31   @control = control
32   @candidates = observations - [control]
33   evaluate_candidates
34
35   freeze
36
37   experiment.context
38
39   experiment.name
40   experiment.name
41
42   # The experiment will result in
43   # observations - an array of Observations, in which
44   # control - the control observation
45   # candidates - the candidates for the experiment
46   # evaluate_candidates
47
48   # The experiment will result in
49   # observations - an array of Observations, in which
50   # control - the control observation
51   # candidates - the candidates for the experiment
52   # evaluate_candidates
53
54   # The experiment will result in
55   # observations - an array of Observations, in which
56   # control - the control observation
57   # candidates - the candidates for the experiment
58   # evaluate_candidates
59
60   # The experiment will result in
61   # observations - an array of Observations, in which
62   # control - the control observation
63   # candidates - the candidates for the experiment
64   # evaluate_candidates
65
66   # The experiment will result in
67   # observations - an array of Observations, in which
68   # control - the control observation
69   # candidates - the candidates for the experiment
70   # evaluate_candidates
71
72   # The experiment will result in
73   # observations - an array of Observations, in which
74   # control - the control observation
75   # candidates - the candidates for the experiment
76   # evaluate_candidates
77
78   # The experiment will result in
79   # observations - an array of Observations, in which
80   # control - the control observation
81   # candidates - the candidates for the experiment
82   # evaluate_candidates
83
84   # The experiment will result in
85   # observations - an array of Observations, in which
86   # control - the control observation
87   # candidates - the candidates for the experiment
88   # evaluate_candidates
89
90   # The experiment will result in
91   # observations - an array of Observations, in which
92   # control - the control observation
93   # candidates - the candidates for the experiment
94   # evaluate_candidates
95
96   # The experiment will result in
97   # observations - an array of Observations, in which
98   # control - the control observation
99   # candidates - the candidates for the experiment
100  # evaluate_candidates
```

1.2.1 Social Networks Information Gathering

With the advent of social networks, hackers can now access information on people and products which were very hard to find only a few years ago.

Criminals can (and actually do) now exploit this valuable information to mount **sophisticated attacks**.



1.2.1 Social Networks Information Gathering

When the employees of a company post information about current projects, trips to conferences, phone numbers, and email addresses on social networks, they are actually giving out a goldmine to criminals.

This not only helps criminals in mounting phishing and impersonation attacks but also gives them the means to create a **technical** map of the **systems and technologies** used by the company.

```
24 # The Experiment Data Structure
25 #
26 # observations - an array of Observations, in which
27 #               - the control observation
28
29 def initialize(experiment, observations = [], control = nil)
30   @experiment = experiment
31   @observations = observations
32   @control = control
33   @candidates = observations - [control]
34   evaluate_candidates
35
36   freeze
37
38   @experiment.context
39
40   @experiment_name
41   @experiment_name
42   @experiment_name
43   @experiment_name
44   @experiment_name
45   @experiment_name
46   @experiment_name
47   @experiment_name
48   @experiment_name
49   @experiment_name
50   @experiment_name
51   @experiment_name
52   @experiment_name
53   @experiment_name
54   @experiment_name
55   @experiment_name
56   @experiment_name
57   @experiment_name
58   @experiment_name
59   @experiment_name
60   @experiment_name
61   @experiment_name
62   @experiment_name
63   @experiment_name
64   @experiment_name
65   @experiment_name
66   @experiment_name
67   @experiment_name
68   @experiment_name
69   @experiment_name
70   @experiment_name
71   @experiment_name
72   @experiment_name
73   @experiment_name
74   @experiment_name
75   @experiment_name
76   @experiment_name
77   @experiment_name
78   @experiment_name
79   @experiment_name
80   @experiment_name
81   @experiment_name
82   @experiment_name
83   @experiment_name
84   @experiment_name
85   @experiment_name
86   @experiment_name
87   @experiment_name
88   @experiment_name
89   @experiment_name
90   @experiment_name
91   @experiment_name
92   @experiment_name
93   @experiment_name
94   @experiment_name
95   @experiment_name
96   @experiment_name
97   @experiment_name
98   @experiment_name
99   @experiment_name
100  @experiment_name
```



1.2.1 Social Networks Information Gathering

You, as a professional penetration tester can do the same, by performing queries on common social networks like *Facebook, Twitter, LinkedIn, Google+* and so on.

Given the vast array of social networks out there, choosing the right ones for your engagement depends on the specific client and engagement.

```
1 def initialize(experiment, observations = [], control = nil)
2   @experiment = experiment
3   @observations = observations
4   @control = control
5   @candidates = observations - @control
6   evaluate_candidates
7
8   freeze
9
10  def context
11    {
12      :experiment_name => @experiment.name
13    }
14  end
15
16  def match?
17    # TODO: Implement a match function between two candidates
18  end
19
20  def score(candidate)
21    1.0
22  end
23
24  def result(candidate)
25    "Result for candidate: #{candidate}"
26  end
27
28  def run
29    # TODO: Implement the run function
30  end
31
32  def to_s
33    "Experiment: #{@experiment.name}"
34  end
35
36  def inspect
37    "#<Experiment: #{@experiment.name}>"
38  end
39
40  def clone
41    Experiment.new(@experiment.name)
42  end
43
44  def == other
45    other.is_a?(Experiment) && other.name == name
46  end
47
48  def < other
49    other.name < name
50  end
51
52  def > other
53    other.name > name
54  end
55
56  def <= other
57    other.name <= name
58  end
59
60  def >= other
61    other.name >= name
62  end
63
64  def < other
65    other.name < name
66  end
67
68  def > other
69    other.name > name
70  end
71
72  def <= other
73    other.name <= name
74  end
75
76  def >= other
77    other.name >= name
78  end
79
80  def < other
81    other.name < name
82  end
83
84  def > other
85    other.name > name
86  end
87
88  def <= other
89    other.name <= name
90  end
91
92  def >= other
93    other.name >= name
94  end
95
96  def < other
97    other.name < name
98  end
99
100 def > other
101   other.name > name
102 end
103
104 def <= other
105   other.name <= name
106 end
107
108 def >= other
109   other.name >= name
110 end
111
112 def < other
113   other.name < name
114 end
115
116 def > other
117   other.name > name
118 end
119
120 def <= other
121   other.name <= name
122 end
123
124 def >= other
125   other.name >= name
126 end
127
128 def < other
129   other.name < name
130 end
131
132 def > other
133   other.name > name
134 end
135
136 def <= other
137   other.name <= name
138 end
139
140 def >= other
141   other.name >= name
142 end
143
144 def < other
145   other.name < name
146 end
147
148 def > other
149   other.name > name
150 end
151
152 def <= other
153   other.name <= name
154 end
155
156 def >= other
157   other.name >= name
158 end
159
160 def < other
161   other.name < name
162 end
163
164 def > other
165   other.name > name
166 end
167
168 def <= other
169   other.name <= name
170 end
171
172 def >= other
173   other.name >= name
174 end
175
176 def < other
177   other.name < name
178 end
179
180 def > other
181   other.name > name
182 end
183
184 def <= other
185   other.name <= name
186 end
187
188 def >= other
189   other.name >= name
190 end
191
192 def < other
193   other.name < name
194 end
195
196 def > other
197   other.name > name
198 end
199
200 def <= other
201   other.name <= name
202 end
203
204 def >= other
205   other.name >= name
206 end
207
208 def < other
209   other.name < name
210 end
211
212 def > other
213   other.name > name
214 end
215
216 def <= other
217   other.name <= name
218 end
219
220 def >= other
221   other.name >= name
222 end
223
224 def < other
225   other.name < name
226 end
227
228 def > other
229   other.name > name
230 end
231
232 def <= other
233   other.name <= name
234 end
235
236 def >= other
237   other.name >= name
238 end
239
240 def < other
241   other.name < name
242 end
243
244 def > other
245   other.name > name
246 end
247
248 def <= other
249   other.name <= name
250 end
251
252 def >= other
253   other.name >= name
254 end
255
256 def < other
257   other.name < name
258 end
259
260 def > other
261   other.name > name
262 end
263
264 def <= other
265   other.name <= name
266 end
267
268 def >= other
269   other.name >= name
270 end
271
272 def < other
273   other.name < name
274 end
275
276 def > other
277   other.name > name
278 end
279
280 def <= other
281   other.name <= name
282 end
283
284 def >= other
285   other.name >= name
286 end
287
288 def < other
289   other.name < name
290 end
291
292 def > other
293   other.name > name
294 end
295
296 def <= other
297   other.name <= name
298 end
299
300 def >= other
301   other.name >= name
302 end
303
304 def < other
305   other.name < name
306 end
307
308 def > other
309   other.name > name
310 end
311
312 def <= other
313   other.name <= name
314 end
315
316 def >= other
317   other.name >= name
318 end
319
320 def < other
321   other.name < name
322 end
323
324 def > other
325   other.name > name
326 end
327
328 def <= other
329   other.name <= name
330 end
331
332 def >= other
333   other.name >= name
334 end
335
336 def < other
337   other.name < name
338 end
339
340 def > other
341   other.name > name
342 end
343
344 def <= other
345   other.name <= name
346 end
347
348 def >= other
349   other.name >= name
350 end
351
352 def < other
353   other.name < name
354 end
355
356 def > other
357   other.name > name
358 end
359
360 def <= other
361   other.name <= name
362 end
363
364 def >= other
365   other.name >= name
366 end
367
368 def < other
369   other.name < name
370 end
371
372 def > other
373   other.name > name
374 end
375
376 def <= other
377   other.name <= name
378 end
379
380 def >= other
381   other.name >= name
382 end
383
384 def < other
385   other.name < name
386 end
387
388 def > other
389   other.name > name
390 end
391
392 def <= other
393   other.name <= name
394 end
395
396 def >= other
397   other.name >= name
398 end
399
400 def < other
401   other.name < name
402 end
403
404 def > other
405   other.name > name
406 end
407
408 def <= other
409   other.name <= name
410 end
411
412 def >= other
413   other.name >= name
414 end
415
416 def < other
417   other.name < name
418 end
419
420 def > other
421   other.name > name
422 end
423
424 def <= other
425   other.name <= name
426 end
427
428 def >= other
429   other.name >= name
430 end
431
432 def < other
433   other.name < name
434 end
435
436 def > other
437   other.name > name
438 end
439
440 def <= other
441   other.name <= name
442 end
443
444 def >= other
445   other.name >= name
446 end
447
448 def < other
449   other.name < name
450 end
451
452 def > other
453   other.name > name
454 end
455
456 def <= other
457   other.name <= name
458 end
459
460 def >= other
461   other.name >= name
462 end
463
464 def < other
465   other.name < name
466 end
467
468 def > other
469   other.name > name
470 end
471
472 def <= other
473   other.name <= name
474 end
475
476 def >= other
477   other.name >= name
478 end
479
480 def < other
481   other.name < name
482 end
483
484 def > other
485   other.name > name
486 end
487
488 def <= other
489   other.name <= name
490 end
491
492 def >= other
493   other.name >= name
494 end
495
496 def < other
497   other.name < name
498 end
499
500 def > other
501   other.name > name
502 end
503
504 def <= other
505   other.name <= name
506 end
507
508 def >= other
509   other.name >= name
510 end
511
512 def < other
513   other.name < name
514 end
515
516 def > other
517   other.name > name
518 end
519
520 def <= other
521   other.name <= name
522 end
523
524 def >= other
525   other.name >= name
526 end
527
528 def < other
529   other.name < name
530 end
531
532 def > other
533   other.name > name
534 end
535
536 def <= other
537   other.name <= name
538 end
539
540 def >= other
541   other.name >= name
542 end
543
544 def < other
545   other.name < name
546 end
547
548 def > other
549   other.name > name
550 end
551
552 def <= other
553   other.name <= name
554 end
555
556 def >= other
557   other.name >= name
558 end
559
560 def < other
561   other.name < name
562 end
563
564 def > other
565   other.name > name
566 end
567
568 def <= other
569   other.name <= name
570 end
571
572 def >= other
573   other.name >= name
574 end
575
576 def < other
577   other.name < name
578 end
579
580 def > other
581   other.name > name
582 end
583
584 def <= other
585   other.name <= name
586 end
587
588 def >= other
589   other.name >= name
590 end
591
592 def < other
593   other.name < name
594 end
595
596 def > other
597   other.name > name
598 end
599
600 def <= other
601   other.name <= name
602 end
603
604 def >= other
605   other.name >= name
606 end
607
608 def < other
609   other.name < name
610 end
611
612 def > other
613   other.name > name
614 end
615
616 def <= other
617   other.name <= name
618 end
619
620 def >= other
621   other.name >= name
622 end
623
624 def < other
625   other.name < name
626 end
627
628 def > other
629   other.name > name
630 end
631
632 def <= other
633   other.name <= name
634 end
635
636 def >= other
637   other.name >= name
638 end
639
640 def < other
641   other.name < name
642 end
643
644 def > other
645   other.name > name
646 end
647
648 def <= other
649   other.name <= name
650 end
651
652 def >= other
653   other.name >= name
654 end
655
656 def < other
657   other.name < name
658 end
659
660 def > other
661   other.name > name
662 end
663
664 def <= other
665   other.name <= name
666 end
667
668 def >= other
669   other.name >= name
670 end
671
672 def < other
673   other.name < name
674 end
675
676 def > other
677   other.name > name
678 end
679
680 def <= other
681   other.name <= name
682 end
683
684 def >= other
685   other.name >= name
686 end
687
688 def < other
689   other.name < name
690 end
691
692 def > other
693   other.name > name
694 end
695
696 def <= other
697   other.name <= name
698 end
699
700 def >= other
701   other.name >= name
702 end
703
704 def < other
705   other.name < name
706 end
707
708 def > other
709   other.name > name
710 end
711
712 def <= other
713   other.name <= name
714 end
715
716 def >= other
717   other.name >= name
718 end
719
720 def < other
721   other.name < name
722 end
723
724 def > other
725   other.name > name
726 end
727
728 def <= other
729   other.name <= name
729 end
730
731 def >= other
732   other.name >= name
733 end
734
735 def < other
736   other.name < name
737 end
738
739 def > other
740   other.name > name
741 end
742
743 def <= other
744   other.name <= name
745 end
746
747 def >= other
748   other.name >= name
749 end
750
751 def < other
752   other.name < name
753 end
754
755 def > other
756   other.name > name
757 end
758
759 def <= other
760   other.name <= name
761 end
762
763 def >= other
764   other.name >= name
765 end
766
767 def < other
768   other.name < name
769 end
770
771 def > other
772   other.name > name
773 end
774
775 def <= other
776   other.name <= name
777 end
778
779 def >= other
780   other.name >= name
781 end
782
783 def < other
784   other.name < name
785 end
786
787 def > other
788   other.name > name
789 end
790
791 def <= other
792   other.name <= name
793 end
794
795 def >= other
796   other.name >= name
797 end
798
799 def < other
800   other.name < name
801 end
802
803 def > other
804   other.name > name
805 end
806
807 def <= other
808   other.name <= name
809 end
810
811 def >= other
812   other.name >= name
813 end
814
815 def < other
816   other.name < name
817 end
818
819 def > other
820   other.name > name
821 end
822
823 def <= other
824   other.name <= name
825 end
826
827 def >= other
828   other.name >= name
829 end
830
831 def < other
832   other.name < name
833 end
834
835 def > other
836   other.name > name
837 end
838
839 def <= other
840   other.name <= name
841 end
842
843 def >= other
844   other.name >= name
845 end
846
847 def < other
848   other.name < name
849 end
850
851 def > other
852   other.name > name
853 end
854
855 def <= other
856   other.name <= name
857 end
858
859 def >= other
860   other.name >= name
861 end
862
863 def < other
864   other.name < name
865 end
866
867 def > other
868   other.name > name
869 end
870
871 def <= other
872   other.name <= name
873 end
874
875 def >= other
876   other.name >= name
877 end
878
879 def < other
880   other.name < name
881 end
882
883 def > other
884   other.name > name
885 end
886
887 def <= other
888   other.name <= name
889 end
890
891 def >= other
892   other.name >= name
893 end
894
895 def < other
896   other.name < name
897 end
898
899 def > other
900   other.name > name
901 end
902
903 def <= other
904   other.name <= name
905 end
906
907 def >= other
908   other.name >= name
909 end
910
911 def < other
912   other.name < name
913 end
914
915 def > other
916   other.name > name
917 end
918
919 def <= other
920   other.name <= name
921 end
922
923 def >= other
924   other.name >= name
925 end
926
927 def < other
928   other.name < name
929 end
930
931 def > other
932   other.name > name
933 end
934
935 def <= other
936   other.name <= name
937 end
938
939 def >= other
940   other.name >= name
941 end
942
943 def < other
944   other.name < name
945 end
946
947 def > other
948   other.name > name
949 end
950
951 def <= other
952   other.name <= name
953 end
954
955 def >= other
956   other.name >= name
957 end
958
959 def < other
960   other.name < name
961 end
962
963 def > other
964   other.name > name
965 end
966
967 def <= other
968   other.name <= name
969 end
970
971 def >= other
972   other.name >= name
973 end
974
975 def < other
976   other.name < name
977 end
978
979 def > other
980   other.name > name
981 end
982
983 def <= other
984   other.name <= name
985 end
986
987 def >= other
988   other.name >= name
989 end
990
991 def < other
992   other.name < name
993 end
994
995 def > other
996   other.name > name
997 end
998
999 def <= other
1000   other.name <= name
1001 end
1002
1003 def >= other
1004   other.name >= name
1005 end
1006
1007 def < other
1008   other.name < name
1009 end
1010
1011 def > other
1012   other.name > name
1013 end
1014
1015 def <= other
1016   other.name <= name
1017 end
1018
1019 def >= other
1020   other.name >= name
1021 end
1022
1023 def < other
1024   other.name < name
1025 end
1026
1027 def > other
1028   other.name > name
1029 end
1030
1031 def <= other
1032   other.name <= name
1033 end
1034
1035 def >= other
1036   other.name >= name
1037 end
1038
1039 def < other
1040   other.name < name
1041 end
1042
1043 def > other
1044   other.name > name
1045 end
1046
1047 def <= other
1048   other.name <= name
1049 end
1050
1051 def >= other
1052   other.name >= name
1053 end
1054
1055 def < other
1056   other.name < name
1057 end
1058
1059 def > other
1060   other.name > name
1061 end
1062
1063 def <= other
1064   other.name <= name
1065 end
1066
1067 def >= other
1068   other.name >= name
1069 end
1070
1071 def < other
1072   other.name < name
1073 end
1074
1075 def > other
1076   other.name > name
1077 end
1078
1079 def <= other
1080   other.name <= name
1081 end
1082
1083 def >= other
1084   other.name >= name
1085 end
1086
1087 def < other
1088   other.name < name
1089 end
1090
1091 def > other
1092   other.name > name
1093 end
1094
1095 def <= other
1096   other.name <= name
1097 end
1098
1099 def >= other
1100   other.name >= name
1101 end
1102
1103 def < other
1104   other.name < name
1105 end
1106
1107 def > other
1108   other.name > name
1109 end
1110
1111 def <= other
1112   other.name <= name
1113 end
1114
1115 def >= other
1116   other.name >= name
1117 end
1118
1119 def < other
1120   other.name < name
1121 end
1122
1123 def > other
1124   other.name > name
1125 end
1126
1127 def <= other
1128   other.name <= name
1129 end
1130
1131 def >= other
1132   other.name >= name
1133 end
1134
1135 def < other
1136   other.name < name
1137 end
1138
1139 def > other
1140   other.name > name
1141 end
1142
1143 def <= other
1144   other.name <= name
1145 end
1146
1147 def >= other
1148   other.name >= name
1149 end
1150
1151 def < other
1152   other.name < name
1153 end
1154
1155 def > other
1156   other.name > name
1157 end
1158
1159 def <= other
1160   other.name <= name
1161 end
1162
1163 def >= other
1164   other.name >= name
1165 end
1166
1167 def < other
1168   other.name < name
1169 end
1170
1171 def > other
1172   other.name > name
1173 end
1174
1175 def <= other
1176   other.name <= name
1177 end
1178
1179 def >= other
1180   other.name >= name
1181 end
1182
1183 def < other
1184   other.name < name
1185 end
1186
1187 def > other
1188   other.name > name
1189 end
1190
1191 def <= other
1192   other.name <= name
1193 end
1194
1195 def >= other
1196   other.name >= name
1197 end
1198
1199 def < other
1200   other.name < name
1201 end
1202
1203 def > other
1204   other.name > name
1205 end
1206
1207 def <= other
1208   other.name <= name
1209 end
1210
1211 def >= other
1212   other.name >= name
1213 end
1214
1215 def < other
1216   other.name < name
1217 end
1218
1219 def > other
1220   other.name > name
1221 end
1222
1223 def <= other
1224   other.name <= name
1225 end
1226
1227 def >= other
1228   other.name >= name
1229 end
1230
1231 def < other
1232   other.name < name
1233 end
1234
1235 def > other
1236   other.name > name
1237 end
1238
1239 def <= other
1240   other.name <= name
1241 end
1242
1243 def >= other
1244   other.name >= name
1245 end
1246
1247 def < other
1248   other.name < name
1249 end
1250
1251 def > other
1252   other.name > name
1253 end
1254
1255 def <= other
1256   other.name <= name
1257 end
1258
1259 def >= other
1260   other.name >= name
1261 end
1262
1263 def < other
1264   other.name < name
1265 end
1266
1267 def > other
1268   other.name > name
1269 end
1270
1271 def <= other
1272   other.name <= name
1273 end
1274
1275 def >= other
1276   other.name >= name
1277 end
1278
1279 def < other
1280   other.name < name
1281 end
1282
1283 def > other
1284   other.name > name
1285 end
1286
1287 def <= other
1288   other.name <= name
1289 end
1290
1291 def >= other
1292   other.name >= name
1293 end
1294
1295 def < other
1296   other.name < name
1297 end
1298
1299 def > other
1300   other.name > name
1301 end
1302
1303 def <= other
1304   other.name <= name
1305 end
1306
1307 def >= other
1308   other.name >= name
1309 end
1310
1311 def < other
1312   other.name < name
1313 end
1314
1315 def > other
1316   other.name > name
1317 end
1318
1319 def <= other
1320   other.name <= name
1321 end
1322
1323 def >= other
1324   other.name >= name
1325 end
1326
1327 def < other
1328   other.name < name
1329 end
1330
1331 def > other
1332   other.name > name
1333 end
1334
1335 def <= other
1336   other.name <= name
1337 end
1338
1339 def >= other
1340   other.name >= name
1341 end
1342
1343 def < other
1344   other.name < name
1345 end
1346
1347 def > other
1348   other.name > name
1349 end
1350
1351 def <= other
1352   other.name <= name
1353 end
1354
1355 def >= other
1356   other.name >= name
1357 end
1358
1359 def < other
1360   other.name < name
1361 end
1362
1363 def > other
1364   other.name > name
1365 end
1366
1367 def <= other
1368   other.name <= name
1369 end
1370
1371 def >= other
1372   other.name >= name
1373 end
1374
1375 def < other
1376   other.name < name
1377 end
1378
1379 def > other
1380   other.name > name
1381 end
1382
1383 def <= other
1384   other.name <= name
1385 end
1386
1387 def >= other
1388   other.name >= name
1389 end
1390
1391 def < other
1392   other.name < name
1393 end
1394
1395 def > other
1396   other.name > name
1397 end
1398
1399 def <= other
1400   other.name <= name
1401 end
1402
1403 def >= other
1404   other.name >= name
1405 end
1406
1407 def < other
1408   other.name < name
1409 end
1410
1411 def > other
1412   other.name > name
1413 end
1414
1415 def <= other
1416   other.name <= name
1417 end
1418
1419 def >= other
1420   other.name >= name
1421 end
1422
1423 def < other
1424   other.name < name
1425 end
1426
1427 def > other
1428   other.name > name
1429 end
1430
1431 def <= other
1432   other.name <= name
1433 end
1434
1435 def >= other
1436   other.name >= name
1437 end
1438
1439 def < other
1440   other.name < name
1441 end
1442
1443 def > other
1444   other.name > name
1445 end
1446
1447 def <= other
1448   other.name <= name
1449 end
1450
1451 def >= other
1452   other.name >= name
1453 end
1454
1455 def < other
1456   other.name < name
1457 end
1458
1459 def > other
1460   other.name > name
1461 end
1462
1463 def <= other
1464   other.name <= name
1465 end
1466
1467 def >= other
1468   other.name >= name
1469 end
1470
1471 def < other
1472   other.name < name
1473 end
1474
1475 def > other
1476   other.name > name
1477 end
1478
1479 def <= other
1480   other.name <= name
1481 end
1482
1483 def >= other
1484   other.name >= name
1485 end
1486
1487 def < other
1488   other.name < name
1489 end
1490
1491 def > other
1492   other.name > name
1493 end
1494
1495 def <= other
1496   other.name <= name
1497 end
1498
1499 def >= other
1500   other.name >= name
1501 end
1502
1503 def < other
1504   other.name < name
1505 end
1506
1507 def > other
1508   other.name > name
1509 end
1510
1511 def <= other
1512   other.name <= name
1513 end
1514
1515 def >= other
1516   other.name >= name
1517 end
1518
1519 def < other
1520   other.name < name
1521 end
1522
1523 def > other
1524   other.name > name
1525 end
1526
1527 def <= other
1528   other.name <= name
1529 end
1530
1531 def >= other
1532   other.name >= name
1533 end
1534
1535 def < other
1536   other.name < name
1537 end
1538
1539 def > other
1540   other.name > name
1541 end
1542
1543 def <= other
1544   other.name <= name
1545 end
1546
1547 def >= other
1548   other.name >= name
1549 end
1550
1551 def < other
1552   other.name < name
1553 end
1554
1555 def > other
1556   other.name > name
1557 end
1558
155
```


1.2.1 Social Networks Information Gathering

While LinkedIn, Twitter, and Facebook are good in terms of a “general purpose” shot, you have to choose between other social networks by understanding not only the target company industry but also some of the interests of its employees.

Example:

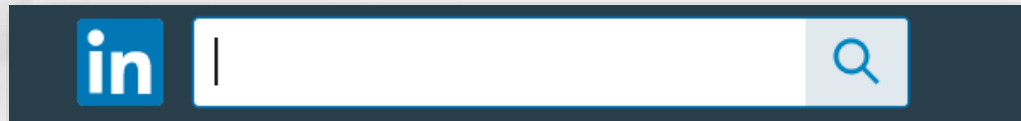
If the client is an advertising company, checking *Instagram* would be a great idea.

1.2.1.1 LinkedIn Example



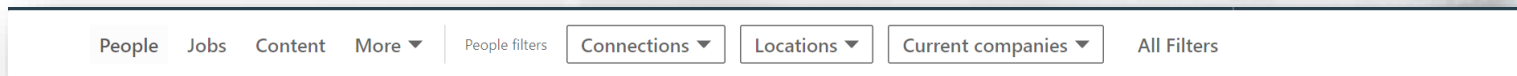
Let's now see how to use LinkedIn's advanced search to find all Google's employees in the US.

After logging in, you can open the advanced search by clicking on the magnifying glass icon on the right of the search bar.



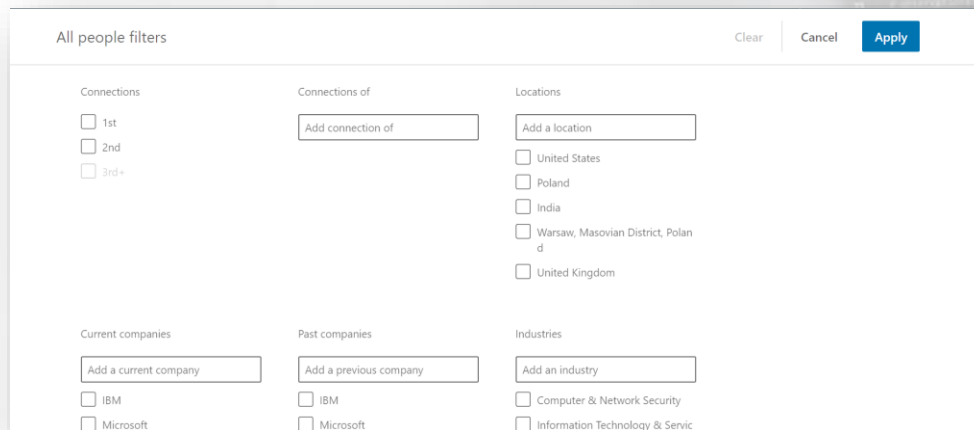
1.2.1.1 LinkedIn Example

Then, the additional search bar appears at the bottom:



A horizontal search filter bar with a white background and a thin border. It contains several tabs: 'People' (selected), 'Jobs', 'Content', and 'More' with a dropdown arrow. To the right of these tabs are three filter boxes: 'People filters', 'Connections' with a dropdown arrow, 'Locations' with a dropdown arrow, and 'Current companies' with a dropdown arrow. On the far right is a link labeled 'All Filters'.

If you choose “All Filters”, you will notice that even more search criteria appears:

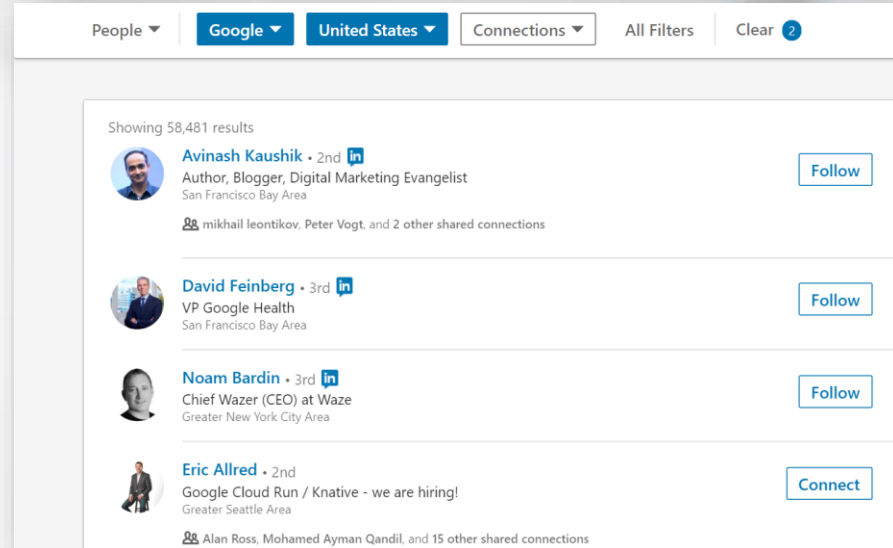


A dialog box titled 'All people filters' with 'Clear', 'Cancel', and 'Apply' buttons at the top right. The dialog is divided into several sections for filtering search results:

- Connections:** Includes checkboxes for '1st', '2nd', and '3rd+'.
- Connections of:** A text input field labeled 'Add connection of'.
- Locations:** Includes a text input field labeled 'Add a location' and a list of checkboxes: 'United States', 'Poland', 'India', 'Warsaw, Masovian District, Poland', and 'United Kingdom'.
- Current companies:** Includes a text input field labeled 'Add a current company' and checkboxes for 'IBM' and 'Microsoft'.
- Past companies:** Includes a text input field labeled 'Add a previous company' and checkboxes for 'IBM' and 'Microsoft'.
- Industries:** Includes a text input field labeled 'Add an industry' and checkboxes for 'Computer & Network Security' and 'Information Technology & Services'.

1.2.1.1 LinkedIn Example

The search will eventually return hundreds of profiles to help you deepen your knowledge of the target company.



1.2.1.1 LinkedIn Example

Many LinkedIn users also provide personal and work **phone numbers or email addresses** that can be exploited to mount a social engineering attack.



1.2.1.2 Linked Social Network Profiles

Many social networks allow users to **integrate** different accounts.

For example, you can link your Twitter and LinkedIn account; this feature automatically posts an update on a social network to others and can be exploited to **find missing information**.

1.2.1.2 Linked Social Network Profiles

You can find the **real name** of the person owning a **Twitter** account by performing a **web search** on LinkedIn, looking for matching updates.

LinkedIn forces its users to use their real name.



1.2.2 Public Sites Information Gathering

Social networks are not the only public source of information about companies. There are also many other interesting websites and databases that “leak” valuable information.

Let's check some out!

[illegible]

1.2.2.1 Crunch Base



CrunchBase is an IT startup database where you can find detailed information about founders, investors, employees, buyouts, and acquisitions.

You can perform lookups by company name or people names.

1.2.2.2 Government Sites

On the Internet, you can get a wide array of information about companies that have worked with a government or are currently working with one.

The information stored on those sites is different from government to government and from state to state.



1.2.2.2 Government Sites

For instance, the USA government provides the [System for Award Management](#) (SAM) and the [GSA eLibrary](#) which you can use to find information about contracts between private companies and the US Government.

<https://www.sam.gov/>
<http://www.gsaelibrary.gsa.gov/>



1.2.3 Whois

Another precious resource is the Whois database. You can use it to get information such as:

- Owner name
- Street addresses
- Email Address
- Technical contacts

regarding an Internet domain name.

```
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
```

1.2.3 Whois

You can query the database by using the `whois` command on Linux and OSX.

If you are running MS Windows, you can install the [Sysinternal's Whois](http://technet.microsoft.com/en-us/sysinternals/bb897435.aspx).

```
23 # @param @experiment - the experiment to test
24 # @param @observations - an array of Observations, in which
25 # @param @control - the control observation
26
27 def initialize(experiment, observations = [], control = nil)
28   @experiment = experiment
29   @observations = observations
30   @control = control
31   @candidates = observations - [control]
32   evaluate_candidates
33
34   freeze
35 end
36
37 experiment.context
38 end
39
40 # @return the name of the experiment
41 def experiment_name
42   @experiment.name
43 end
44
45 # @return the result a match between an
46 def matched?
47   @matched
48 end
49
50 def result
51   @result
52 end
```

1.2.3.1 Whois Example

Here we see some of the information you can get by performing a *whois* lookup for **apple.com**.



```
$ whois apple.com
```

```
Domain Name: apple.com  
Registry Registrant ID:  
Registrant Name: Domain Administrator  
Registrant Organization: Apple Inc.  
Registrant Street: 1 Infinite Loop  
Registrant City: Cupertino  
Registrant State/Province: CA  
Registrant Postal Code: 95014  
Registrant Country: US  
Registrant Phone: +1.4089961010  
Registrant Phone Ext:  
Registrant Fax: +1.4089741560  
Registrant Fax Ext:  
Registrant Email: domains@apple.com
```



1.2.3.1 Whois Example

You can also find technical contacts.



```
Registry Admin ID:  
Admin Name: Domain Administrator  
Admin Organization: Apple Inc.  
Admin Street: 1 Infinite Loop  
Admin City: Cupertino  
Admin State/Province: CA  
Admin Postal Code: 95014  
Admin Country: US  
Admin Phone: +1.4089961010  
Admin Phone Ext:  
Admin Fax: +1.4089741560  
Admin Fax Ext:  
Admin Email: domains@apple.com
```

1.2.4 Browsing Client's Sites

Social networks, public sites and the *whois* services each give you fragmented information that you can put together to better understand your client's business.



1.2.4 Browsing Client's Sites

Finally, don't forget that **browsing your client's actual websites** will give you plenty of information about:

- Products
- Services
- Technologies
- Company culture



1.2.4 Browsing Client's Sites

Many companies websites contain information about the board of directors profiles, current and future products, partners, suppliers, job vacancies and so on.

The more you know your target, the easier the later phases of your pentest will be.



1.2.5 Discovering Email Pattern

In case there is not a direct database or any other source of company emails, which often also works as logins to corporate services, you might want to try to identify them yourself.



1.2.5 Discovering Email Pattern

You should keep in mind, that companies tend to use one certain email schema for every employee; this makes internal communication of a company much easier.



1.2.5 Discovering Email Pattern

Usually, there is no complicated pattern. The structure of an email address should be intuitive, so other employees can easily communicate with each other by just knowing their co-worker name and/or surname.

Below are some examples of typical corporate email address format:

- **name.surname@company.com**
- **surname.name@company.com**
- **[first letter of name]surname@company.com**

1.2.5 Discovering Email Pattern

If you are able to find a company's employees (i.e., using their official website, LinkedIn, or other social networking sites), you might be able to guess their email address.

1.2.5 Discovering Email Pattern

Many mail systems tend to inform the sender that mail was not delivered because it does not exist.

This is an excellent opportunity for a penetration tester to guess corporate email formats.

```
23 # @param email - the email address to check
24 # @param domain - the domain to check
25 # @return - a boolean indicating if the email exists
26 def check_email(email, domain):
27     """
28     Check if an email address exists.
29     """
30     # Create a list of candidates
31     candidates = []
32     # Iterate over the domain
33     for i in range(1, len(domain)):
34         # Get the subdomain
35         subdomain = domain[:i]
36         # Create a list of candidates
37         candidates.append(subdomain + email)
38     # Iterate over the candidates
39     for candidate in candidates:
40         # Send an email
41         send_email(candidate)
42     # Return the result
43     return True
44
45 # Example usage
46 email = "john.doe@caendra.com"
47 domain = "caendra.com"
48 check_email(email, domain)
```



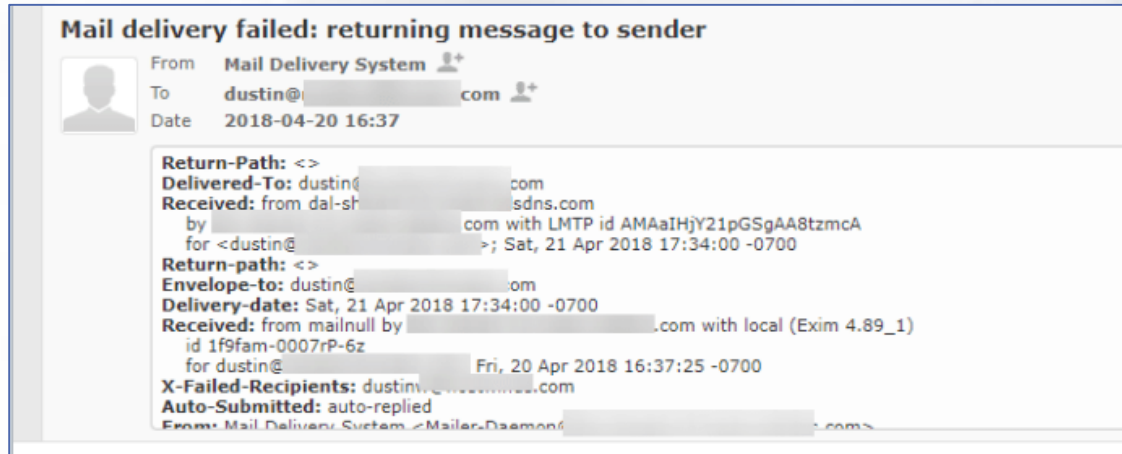
1.2.5 Discovering Email Pattern

You can try to first:

- Collect a reasonable number of employee data (name/surname)
- Try to construct a few possible email formats and apply them to each name/surname pair
- Try to send an email that does not alert potential victims (e.g., do not put a „phishing test” in subject, but choose something tricky like try to pretend it is just an advertisement)

1.2.5 Discovering Email Pattern

If you start to receive similar emails to the one below:



You should carefully inspect which of your sent emails did not generate such a message, which will be the one that will have the correct corporate mail schema.

Subdomain Enumeration



1.3 Subdomain Enumeration

We have previously talked about widening the attack surface. An additional way to do so is by discovering as many websites owned by the company as possible.



1.3 Subdomain Enumeration

It's common for websites of the same company to share the same top level domain name. For example, careers.company.com, mail.company.com or business.company.com

Through subdomain enumeration a penetration tester can possibly identify additional resources of a target.

1.3 Subdomain Enumeration

It is very likely that such resources may contain outdated, buggy software, sensitive information, or even administrative interfaces that are not secured.

If you take a look at some bug bounty program writeups, you can quickly conclude that such forgotten resources are something common even in prestigious companies.

```
21 def initialize(experiment, observations = [], control = null)
22   @experiment = experiment
23   @observations = observations
24   @control = control
25   @candidates = observations + [control]
26   evaluate_candidates
27
28   freeze
29
30   @context =
31     experiment.context
32
33   @experiment_name =
34     experiment.name
35
36   @experiment_name
37
38   @context
39
40   @context
41
42   @context
43
44   @context
45
46   @context
47
48   @context
49
50   @context
51
52   @context
53
54   @context
55
56   @context
57
58   @context
59
60   @context
61
62   @context
63
64   @context
65
66   @context
67
68   @context
69
70   @context
71
72   @context
73
74   @context
75
76   @context
77
78   @context
79
80   @context
81
82   @context
83
84   @context
85
86   @context
87
88   @context
89
90   @context
91
92   @context
93
94   @context
95
96   @context
97
98   @context
99
100  @context
```

1.3 Subdomain Enumeration

In this course, we will focus on passive subdomain enumeration.

This means that we will try to identify subdomains without directly interacting with the target, but through open sources.

```
20 def __init__(self):
21     self.__create()
22
23     # Experiment
24     # observations - an array of Observations, in chronological order
25     # control - the control observation
26
27     def initialize(self, observations = [], control = None):
28         @experiment = experiment
29         @observations = observations
30         @control = control
31         @candidates = observations + [control]
32         evaluate_candidates
33
34     # Method to experiment's control
35
36     # Return the name of the experiment
37     def experiment_name
38         experiment.name
39         return
40
41     # Return the result a match between an experiment
42     def match
43         return result
44
45     def result
46         return result
47
48     def result
49         return result
50
51     def result
52         return result
```



1.3 Subdomain Enumeration

Such an open source, can be a search engine.

For example, while Google is performing its indexing activities, it may index pages that were not meant for indexing. A penetration tester can leverage this to passively identify **some** target subdomains.

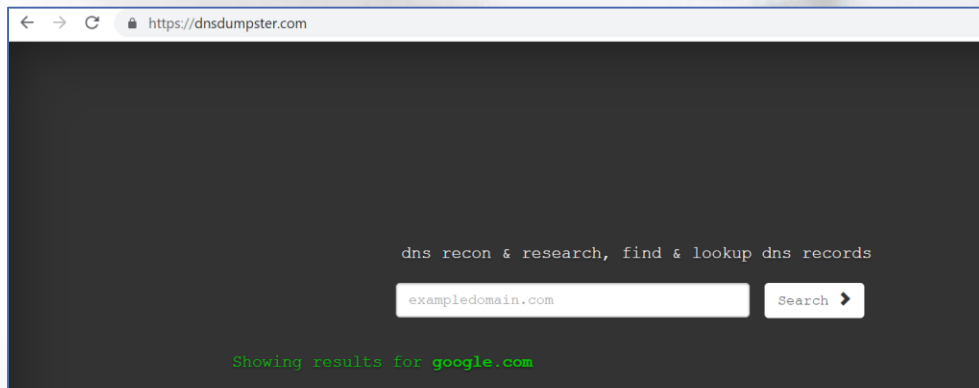
You can try this by typing the following in Google's search engine
site: company.com

1.3 Subdomain Enumeration

Another open source that can facilitate passive subdomain enumeration is dnsdumpster.com, that utilizes data from google-indexed subdomains, but also checks sites like Bing or virustotal for similar information.

1.3 Subdomain Enumeration

By typing in the main company domain, you will be presented with any subdomains found for this company.



1.3 Subdomain Enumeration

There is also a tool that extends the capabilities of DNS enumeration, called **sublist3r**.

It is pre-installed on the latest Kali Linux version but can be downloaded from [its github repository](https://github.com/aboul3la/Sublist3r) as well.

1.3 Subdomain Enumeration

In its basic usage, sublist3r will collect DNS data from various sources.

However, you should be aware that it is easily blocked by Google (its search engine does not like automated tools). For this reason, you should use it wisely.

1.3 Subdomain Enumeration

After running sublist3r with the **-d [domain]** flag, it starts searching for subdomains in various sources.

```
root@xluk3:~# sublist3r -d google.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[*] Enumerating subdomains now for google.com
[*] Searching now in Baidu..
[*] Searching now in Yahoo..
[*] Searching now in Google..
[*] Searching now in Bing..
[*] Searching now in Ask..
[*] Searching now in Netcraft..
[*] Searching now in DNSdumpster..
[*] Searching now in Virustotal..
[*] Searching now in ThreatCrowd..
[*] Searching now in SSL Certificates..
[*] Searching now in PassiveDNS..
```

1.3 Subdomain Enumeration

The aforementioned subdomain enumeration techniques will help you identify publicly available target assets. Each one of them may be vulnerable to attacks, which should be thoroughly checked during the penetration test.



1.3.1 Video – Subdomain Enumeration

Subdomain Enumeration

In the subdomain enumeration video you will get to know various techniques to enumerate your target's subdomains.



**Videos are only available in Full or Elite Editions of the course. To upgrade, click [HERE](#). To access, go to the course in your members area and click the resources drop-down in the appropriate module line.*

The Importance of Information Gathering



1.4 The Importance of Information Gathering

Before closing this module, we at eLearnSecurity want to stress **how important information gathering is!**



1.4 The Importance of Information Gathering

A strong phase of Information Gathering makes the difference between a good and a bad penetration tester.

A good penetration tester spends 90% of his time widening the attack surface because he knows this is what it is all about. The other 10% is just a matter of launching the correct commands with the appropriate tool with a high success rate.



1.4 The Importance of Information Gathering

Let's say you are playing darts.

Would you prefer having 1000 shots to throw at a microscopic target, or one single shot at an impossible to miss big target?



1.4 The Importance of Information Gathering

Lastly, as penetration tests are **cyclic processes**, each time you will get deeper inside your client's infrastructure, thus gaining access to more information.



1.4 The Importance of Information Gathering

Every information gathering stage will need the same focus and dedication as the first one.

Your penetration test will be **as strong as your weakest skill**, so do not underestimate information gathering!





References



References

CrunchBase

<http://www.crunchbase.com/>

Facebook

<https://www.facebook.com/>

LinkedIn

<https://www.linkedin.com/>

Twitter

<https://twitter.com/>



References

[Sysinternal Whois](#)

<http://technet.microsoft.com/en-us/sysinternals/bb897435.aspx>

[DNSdumpster.com](#)

<https://dnsdumpster.com/>

[Sublist3r](#)

<https://github.com/aboul3la/Sublist3r>



Videos

Subdomain Enumeration

In the subdomain enumeration video you will get to know various techniques to enumerate your target's subdomains, from basic to advanced ones.



**Videos are only available in Full or Elite Editions of the course. To upgrade, click [HERE](#). To access, go to the course in your members area and click the resources drop-down in the appropriate module line.*