

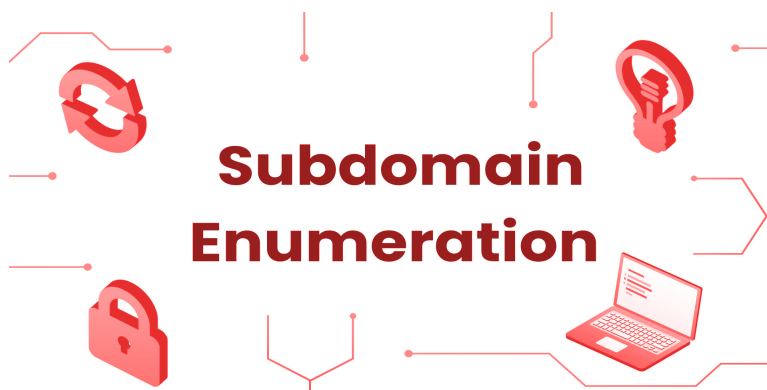
Ethical Hacking/Penetration Testing & Bug Bounty Hunting v2



❖ Introduction:-

In a digital landscape teeming with complexities and vulnerabilities, the role of ethical hackers and penetration testers has never been more crucial. The relentless surge of cyber threats demands a new breed of cybersecurity professionals who are not only equipped with technical prowess but also possess an unyielding commitment to safeguarding digital assets. Welcome to the transformative Udemy course "Ethical Hacking / Penetration Testing & Bug Bounty Hunting v2." This article serves as your guide to understanding the rich tapestry of topics covered in this course, enabling you to embark on a journey that combines technical mastery with ethical responsibility.

❖ **Mastering Subdomain Enumeration in Penetration Testing: Avoiding Common Mistakes**

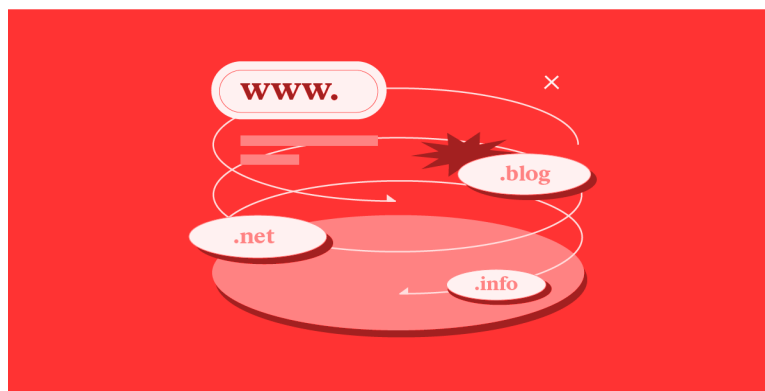


Introduction:

In the realm of penetration testing, mastering subdomain enumeration is a crucial skill that can unveil hidden vulnerabilities and strengthen the security posture of organizations. Lets delves into the nuances of subdomain enumeration, covering common mistakes to avoid, hacks for uncovering hidden subdomains, and techniques to master this vital aspect of penetration testing.

Basics and Common Mistakes to Avoid while doing Subdomain Enumeration

Understanding Subdomain Enumeration



Subdomain enumeration involves discovering all possible subdomains associated with a domain. In penetration testing, this process is fundamental for identifying attack surfaces and potential entry points. Common tools used for subdomain enumeration include Sublist3r, Amass, and DNSDumpster.

Common Mistakes to Avoid



Incomplete Enumeration: Rushing through the process may result in overlooking subdomains, leaving potential security gaps.

Overreliance on Automated Tools: While tools are valuable, solely relying on them can lead to missing manual verification opportunities.

Ignoring Historical Data: Failures to explore historical data may result in missing subdomains that were once active but have been decommissioned.

Hacks to Find Hidden Subdomains

Google Dorking for Subdomains



Leveraging Google's advanced search operators can reveal hidden subdomains. For instance, using "site:example.com" can unveil subdomains that search engines have indexed.

Certificate Transparency Logs



Exploring Certificate Transparency Logs can provide insights into recently issued certificates, exposing subdomains that may not be evident through traditional enumeration methods.

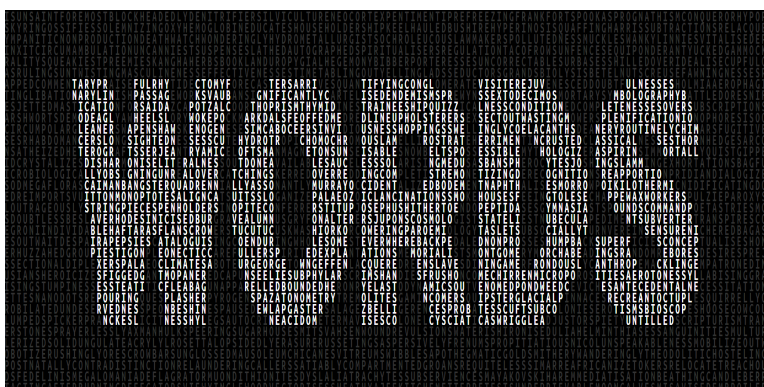
Brute-Forcing Techniques



Using tools like SubBrute or DNSRecon for brute-forcing subdomains can be effective, but it requires caution to avoid triggering security alerts.

Mastering Subdomain Enumeration Techniques

Comprehensive Wordlist Usage



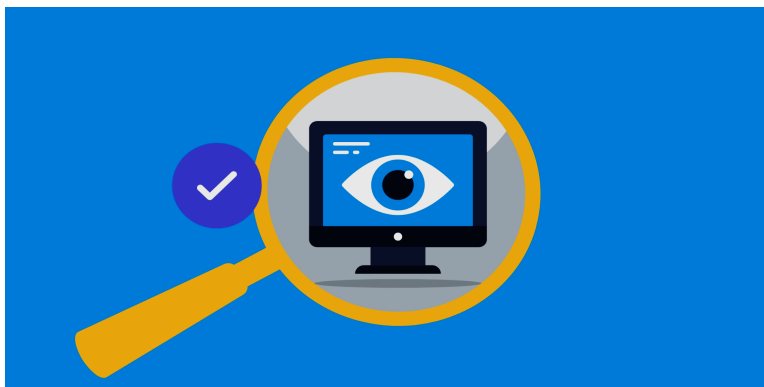
Creating and utilizing a well-crafted wordlist is essential for a thorough subdomain enumeration. Including industry-specific terms and variations increases the chances of discovering hidden subdomains.

Active Reconnaissance Techniques



Interacting with web applications and services actively can reveal subdomains that are only accessible through specific actions. This approach involves analyzing responses to requests and understanding the application's structure.

Continuous Monitoring



Subdomain enumeration is not a one-time task. Implementing continuous monitoring ensures that new subdomains are promptly discovered, especially in dynamic environments.

Understanding of Assetfinder

tomnomnom/ assetfinder



Find domains and subdomains related to a given domain

4 Contributors 25 Issues 3k Stars 463 Forks



Asset finder is a tool used for identifying and locating digital assets within a network or online space. It helps security professionals and researchers discover potential vulnerabilities by revealing exposed resources such as subdomains, IP addresses, and other digital artifacts. By systematically scanning and mapping an organization's online presence, asset finder enhances cybersecurity efforts and threat intelligence.

Installation and usage

Step 1 :- Install Assetfinder using the apt-get command

```
(root@kali)-[~]
└─# apt install assetfinder
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  golang-1.19-go golang-1.19-src libarmadillo11 libblockdev-crypto2 libblockdev-fs2 libblockdev-loop2 libblockdev-part2 libblockdev-partition2 libblockdev-raid2 libblockdev-transaction2 libblockdev2 libblockdev3 libblockdev3.11.1 libgumbo1 libgupnp-igd-1.0-4 libjim0.81 libmongocrypt0 libmujs2 libncurses6 libnetfilter-queue1 libnftables1 libnftnl1 libnftnl2 libnftnl3 libnftnl4 libnftnl5 libnftnl6 libnftnl7 libnftnl8 libnftnl9 libnftnl10 libnftnl11 libnftnl12 libnftnl13 libnftnl14 libnftnl15 libnftnl16 libnftnl17 libnftnl18 libnftnl19 libnftnl20 libnftnl21 libnftnl22 libnftnl23 libnftnl24 libnftnl25 libnftnl26 libnftnl27 libnftnl28 libnftnl29 libnftnl30 libnftnl31 libnftnl32 libnftnl33 libnftnl34 libnftnl35 libnftnl36 libnftnl37 libnftnl38 libnftnl39 libnftnl40 libnftnl41 libnftnl42 libnftnl43 libnftnl44 libnftnl45 libnftnl46 libnftnl47 libnftnl48 libnftnl49 libnftnl50 libnftnl51 libnftnl52 libnftnl53 libnftnl54 libnftnl55 libnftnl56 libnftnl57 libnftnl58 libnftnl59 libnftnl60 libnftnl61 libnftnl62 libnftnl63 libnftnl64 libnftnl65 libnftnl66 libnftnl67 libnftnl68 libnftnl69 libnftnl70 libnftnl71 libnftnl72 libnftnl73 libnftnl74 libnftnl75 libnftnl76 libnftnl77 libnftnl78 libnftnl79 libnftnl80 libnftnl81 libnftnl82 libnftnl83 libnftnl84 libnftnl85 libnftnl86 libnftnl87 libnftnl88 libnftnl89 libnftnl90 libnftnl91 libnftnl92 libnftnl93 libnftnl94 libnftnl95 libnftnl96 libnftnl97 libnftnl98 libnftnl99 libnftnl100 libnftnl101 libnftnl102 libnftnl103 libnftnl104 libnftnl105 libnftnl106 libnftnl107 libnftnl108 libnftnl109 libnftnl110 libnftnl111 libnftnl112 libnftnl113 libnftnl114 libnftnl115 libnftnl116 libnftnl117 libnftnl118 libnftnl119 libnftnl120 libnftnl121 libnftnl122 libnftnl123 libnftnl124 libnftnl125 libnftnl126 libnftnl127 libnftnl128 libnftnl129 libnftnl130 libnftnl131 libnftnl132 libnftnl133 libnftnl134 libnftnl135 libnftnl136 libnftnl137 libnftnl138 libnftnl139 libnftnl140 libnftnl141 libnftnl142 libnftnl143 libnftnl144 libnftnl145 libnftnl146 libnftnl147 libnftnl148 libnftnl149 libnftnl150 libnftnl151 libnftnl152 libnftnl153 libnftnl154 libnftnl155 libnftnl156 libnftnl157 libnftnl158 libnftnl159 libnftnl160 libnftnl161 libnftnl162 libnftnl163 libnftnl164 libnftnl165 libnftnl166 libnftnl167 libnftnl168 libnftnl169 libnftnl170 libnftnl171 libnftnl172 libnftnl173 libnftnl174 libnftnl175 libnftnl176 libnftnl177 libnftnl178 libnftnl179 libnftnl180 libnftnl181 libnftnl182 libnftnl183 libnftnl184 libnftnl185 libnftnl186 libnftnl187 libnftnl188 libnftnl189 libnftnl190 libnftnl191 libnftnl192 libnftnl193 libnftnl194 libnftnl195 libnftnl196 libnftnl197 libnftnl198 libnftnl199 libnftnl200 libnftnl201 libnftnl202 libnftnl203 libnftnl204 libnftnl205 libnftnl206 libnftnl207 libnftnl208 libnftnl209 libnftnl210 libnftnl211 libnftnl212 libnftnl213 libnftnl214 libnftnl215 libnftnl216 libnftnl217 libnftnl218 libnftnl219 libnftnl220 libnftnl221 libnftnl222 libnftnl223 libnftnl224 libnftnl225 libnftnl226 libnftnl227 libnftnl228 libnftnl229 libnftnl230 libnftnl231 libnftnl232 libnftnl233 libnftnl234 libnftnl235 libnftnl236 libnftnl237 libnftnl238 libnftnl239 libnftnl240 libnftnl241 libnftnl242 libnftnl243 libnftnl244 libnftnl245 libnftnl246 libnftnl247 libnftnl248 libnftnl249 libnftnl250 libnftnl251 libnftnl252 libnftnl253 libnftnl254 libnftnl255 libnftnl256 libnftnl257 libnftnl258 libnftnl259 libnftnl260 libnftnl261 libnftnl262 libnftnl263 libnftnl264 libnftnl265 libnftnl266 libnftnl267 libnftnl268 libnftnl269 libnftnl270 libnftnl271 libnftnl272 libnftnl273 libnftnl274 libnftnl275 libnftnl276 libnftnl277 libnftnl278 libnftnl279 libnftnl280 libnftnl281 libnftnl282 libnftnl283 libnftnl284 libnftnl285 libnftnl286 libnftnl287 libnftnl288 libnftnl289 libnftnl290 libnftnl291 libnftnl292 libnftnl293 libnftnl294 libnftnl295 libnftnl296 libnftnl297 libnftnl298 libnftnl299 libnftnl300 libnftnl301 libnftnl302 libnftnl303 libnftnl304 libnftnl305 libnftnl306 libnftnl307 libnftnl308 libnftnl309 libnftnl310 libnftnl311 libnftnl312 libnftnl313 libnftnl314 libnftnl315 libnftnl316 libnftnl317 libnftnl318 libnftnl319 libnftnl320 libnftnl321 libnftnl322 libnftnl323 libnftnl324 libnftnl325 libnftnl326 libnftnl327 libnftnl328 libnftnl329 libnftnl330 libnftnl331 libnftnl332 libnftnl333 libnftnl334 libnftnl335 libnftnl336 libnftnl337 libnftnl338 libnftnl339 libnftnl340 libnftnl341 libnftnl342 libnftnl343 libnftnl344 libnftnl345 libnftnl346 libnftnl347 libnftnl348 libnftnl349 libnftnl350 libnftnl351 libnftnl352 libnftnl353 libnftnl354 libnftnl355 libnftnl356 libnftnl357 libnftnl358 libnftnl359 libnftnl360 libnftnl361 libnftnl362 libnftnl363 libnftnl364 libnftnl365 libnftnl366 libnftnl367 libnftnl368 libnftnl369 libnftnl370 libnftnl371 libnftnl372 libnftnl373 libnftnl374 libnftnl375 libnftnl376 libnftnl377 libnftnl378 libnftnl379 libnftnl380 libnftnl381 libnftnl382 libnftnl383 libnftnl384 libnftnl385 libnftnl386 libnftnl387 libnftnl388 libnftnl389 libnftnl390 libnftnl391 libnftnl392 libnftnl393 libnftnl394 libnftnl395 libnftnl396 libnftnl397 libnftnl398 libnftnl399 libnftnl400 libnftnl401 libnftnl402 libnftnl403 libnftnl404 libnftnl405 libnftnl406 libnftnl407 libnftnl408 libnftnl409 libnftnl410 libnftnl411 libnftnl412 libnftnl413 libnftnl414 libnftnl415 libnftnl416 libnftnl417 libnftnl418 libnftnl419 libnftnl420 libnftnl421 libnftnl422 libnftnl423 libnftnl424 libnftnl425 libnftnl426 libnftnl427 libnftnl428 libnftnl429 libnftnl430 libnftnl431 libnftnl432 libnftnl433 libnftnl434 libnftnl435 libnftnl436 libnftnl437 libnftnl438 libnftnl439 libnftnl440 libnftnl441 libnftnl442 libnftnl443 libnftnl444 libnftnl445 libnftnl446 libnftnl447 libnftnl448 libnftnl449 libnftnl450 libnftnl451 libnftnl452 libnftnl453 libnftnl454 libnftnl455 libnftnl456 libnftnl457 libnftnl458 libnftnl459 libnftnl460 libnftnl461 libnftnl462 libnftnl463 libnftnl464 libnftnl465 libnftnl466 libnftnl467 libnftnl468 libnftnl469 libnftnl470 libnftnl471 libnftnl472 libnftnl473 libnftnl474 libnftnl475 libnftnl476 libnftnl477 libnftnl478 libnftnl479 libnftnl480 libnftnl481 libnftnl482 libnftnl483 libnftnl484 libnftnl485 libnftnl486 libnftnl487 libnftnl488 libnftnl489 libnftnl490 libnftnl491 libnftnl492 libnftnl493 libnftnl494 libnftnl495 libnftnl496 libnftnl497 libnftnl498 libnftnl499 libnftnl500 libnftnl501 libnftnl502 libnftnl503 libnftnl504 libnftnl505 libnftnl506 libnftnl507 libnftnl508 libnftnl509 libnftnl510 libnftnl511 libnftnl512 libnftnl513 libnftnl514 libnftnl515 libnftnl516 libnftnl517 libnftnl518 libnftnl519 libnftnl520 libnftnl521 libnftnl522 libnftnl523 libnftnl524 libnftnl525 libnftnl526 libnftnl527 libnftnl528 libnftnl529 libnftnl530 libnftnl531 libnftnl532 libnftnl533 libnftnl534 libnftnl535 libnftnl536 libnftnl537 libnftnl538 libnftnl539 libnftnl540 libnftnl541 libnftnl542 libnftnl543 libnftnl544 libnftnl545 libnftnl546 libnftnl547 libnftnl548 libnftnl549 libnftnl550 libnftnl551 libnftnl552 libnftnl553 libnftnl554 libnftnl555 libnftnl556 libnftnl557 libnftnl558 libnftnl559 libnftnl560 libnftnl561 libnftnl562 libnftnl563 libnftnl564 libnftnl565 libnftnl566 libnftnl567 libnftnl568 libnftnl569 libnftnl570 libnftnl571 libnftnl572 libnftnl573 libnftnl574 libnftnl575 libnftnl576 libnftnl577 libnftnl578 libnftnl579 libnftnl580 libnftnl581 libnftnl582 libnftnl583 libnftnl584 libnftnl585 libnftnl586 libnftnl587 libnftnl588 libnftnl589 libnftnl590 libnftnl591 libnftnl592 libnftnl593 libnftnl594 libnftnl595 libnftnl596 libnftnl597 libnftnl598 libnftnl599 libnftnl600 libnftnl601 libnftnl602 libnftnl603 libnftnl604 libnftnl605 libnftnl606 libnftnl607 libnftnl608 libnftnl609 libnftnl610 libnftnl611 libnftnl612 libnftnl613 libnftnl614 libnftnl615 libnftnl616 libnftnl617 libnftnl618 libnftnl619 libnftnl620 libnftnl621 libnftnl622 libnftnl623 libnftnl624 libnftnl625 libnftnl626 libnftnl627 libnftnl628 libnftnl629 libnftnl630 libnftnl631 libnftnl632 libnftnl633 libnftnl634 libnftnl635 libnftnl636 libnftnl637 libnftnl638 libnftnl639 libnftnl640 libnftnl641 libnftnl642 libnftnl643 libnftnl644 libnftnl645 libnftnl646 libnftnl647 libnftnl648 libnftnl649 libnftnl650 libnftnl651 libnftnl652 libnftnl653 libnftnl654 libnftnl655 libnftnl656 libnftnl657 libnftnl658 libnftnl659 libnftnl660 libnftnl661 libnftnl662 libnftnl663 libnftnl664 libnftnl665 libnftnl666 libnftnl667 libnftnl668 libnftnl669 libnftnl670 libnftnl671 libnftnl672 libnftnl673 libnftnl674 libnftnl675 libnftnl676 libnftnl677 libnftnl678 libnftnl679 libnftnl680 libnftnl681 libnftnl682 libnftnl683 libnftnl684 libnftnl685 libnftnl686 libnftnl687 libnftnl688 libnftnl689 libnftnl690 libnftnl691 libnftnl692 libnftnl693 libnftnl694 libnftnl695 libnftnl696 libnftnl697 libnftnl698 libnftnl699 libnftnl700 libnftnl701 libnftnl702 libnftnl703 libnftnl704 libnftnl705 libnftnl706 libnftnl707 libnftnl708 libnftnl709 libnftnl710 libnftnl711 libnftnl712 libnftnl713 libnftnl714 libnftnl715 libnftnl716 libnftnl717 libnftnl718 libnftnl719 libnftnl720 libnftnl721 libnftnl722 libnftnl723 libnftnl724 libnftnl725 libnftnl726 libnftnl727 libnftnl728 libnftnl729 libnftnl730 libnftnl731 libnftnl732 libnftnl733 libnftnl734 libnftnl735 libnftnl736 libnftnl737 libnftnl738 libnftnl739 libnftnl740 libnftnl741 libnftnl742 libnftnl743 libnftnl744 libnftnl745 libnftnl746 libnftnl747 libnftnl748 libnftnl749 libnftnl750 libnftnl751 libnftnl752 libnftnl753 libnftnl754 libnftnl755 libnftnl756 libnftnl757 libnftnl758 libnftnl759 libnftnl760 libnftnl761 libnftnl762 libnftnl763 libnftnl764 libnftnl765 libnftnl766 libnftnl767 libnftnl768 libnftnl769 libnftnl770 libnftnl771 libnftnl772 libnftnl773 libnftnl774 libnftnl775 libnftnl776 libnftnl777 libnftnl778 libnftnl779 libnftnl780 libnftnl781 libnftnl782 libnftnl783 libnftnl784 libnftnl785 libnftnl786 libnftnl787 libnftnl788 libnftnl789 libnftnl790 libnftnl791 libnftnl792 libnftnl793 libnftnl794 libnftnl795 libnftnl796 libnftnl797 libnftnl798 libnftnl799 libnftnl800 libnftnl801 libnftnl802 libnftnl803 libnftnl804 libnftnl805 libnftnl806 libnftnl807 libnftnl808 libnftnl809 libnftnl810 libnftnl811 libnftnl812 libnftnl813 libnftnl814 libnftnl815 libnftnl816 libnftnl817 libnftnl818 libnftnl819 libnftnl820 libnftnl821 libnftnl822 libnftnl823 libnftnl824 libnftnl825 libnftnl826 libnftnl827 libnftnl828 libnftnl829 libnftnl830 libnftnl831 libnftnl832 libnftnl833 libnftnl834 libnftnl835 libnftnl836 libnftnl837 libnftnl838 libnftnl839 libnftnl840 libnftnl841 libnftnl842 libnftnl843 libnftnl844 libnftnl845 libnftnl846 libnftnl847 libnftnl848 libnftnl849 libnftnl850 libnftnl851 libnftnl852 libnftnl853 libnftnl854 libnftnl855 libnftnl856 libnftnl857 libnftnl858 libnftnl859 libnftnl860 libnftnl861 libnftnl862 libnftnl863 libnftnl864 libnftnl865 libnftnl866 libnftnl867 libnftnl868 libnftnl869 libnftnl870 libnftnl871 libnftnl872 libnftnl873 libnftnl874 libnftnl875 libnftnl876 libnftnl877 libnftnl878 libnftnl879 libnftnl880 libnftnl881 libnftnl882 libnftnl883 libnftnl884 libnftnl885 libnftnl886 libnftnl887 libnftnl888 libnftnl889 libnftnl890 libnftnl891 libnftnl892 libnftnl893 libnftnl894 libnftnl895 libnftnl896 libnftnl897 libnftnl898 libnftnl899 libnftnl900 libnftnl901 libnftnl902 libnftnl903 libnftnl904 libnftnl905 libnftnl906 libnftnl907 libnftnl908 libnftnl909 libnftnl910 libnftnl911 libnftnl912 libnftnl913 libnftnl914 libnftnl915 libnftnl916 libnftnl917 libnftnl918 libnftnl919 libnftnl920 libnftnl921 libnftnl922 libnftnl923 libnftnl924 libnftnl925 libnftnl926 libnftnl927 libnftnl928 libnftnl929 libnftnl930 libnftnl931 libnftnl932 libnftnl933 libnftnl934 libnftnl935 libnftnl936 libnftnl937 libnftnl938 libnftnl939 libnftnl940 libnftnl941 libnftnl942 libnftnl943 libnftnl944 libnftnl945 libnftnl946 libnftnl947 libnftnl948 libnftnl949 libnftnl950 libnftnl951 libnftnl952 libnftnl953 libnftnl954 libnftnl955 libnftnl956 libnftnl957 libnftnl958 libnftnl959 libnftnl960 libnftnl961 libnftnl962 libnftnl963 libnftnl964 libnftnl965 libnftnl966 libnftnl967 libnftnl968 libnftnl969 libnftnl970 libnftnl971 libnftnl972 libnftnl973 libnftnl974 libnftnl975 libnftnl976 libnftnl977 libnftnl978 libnftnl979 libnftnl980 libnftnl981 libnftnl982 libnftnl983 libnftnl984 libnftnl985 libnftnl986 libnftnl987 libnftnl988 libnftnl989 libnftnl990 libnftnl991 libnftnl992 libnftnl993 libnftnl994 libnftnl995 libnftnl996 libnftnl997 libnftnl998 libnftnl999 libnftnl1000
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  assetfinder
0 upgraded, 1 newly installed, 0 to remove and 28 not upgraded.
Need to get 1,571 kB of archives.
After this operation, 4,976 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 assetfinder amd64 0.1.0+git20200415-0kali1 [1,571 kB]
Fetched 1,571 kB in 1s (1,074 kB/s)
Selecting previously unselected package assetfinder.
(Reading database ... 438475 files and directories currently installed.)
Preparing to unpack .../assetfinder_0.1.0+git20200415-0kali1_amd64.deb ...
Unpacking assetfinder (0.1.0+git20200415-0kali1) ...
Setting up assetfinder (0.1.0+git20200415-0kali1) ...
Processing triggers for kali-menu (2023.4.5) ...
Scanning processes ...
Scanning linux images ...
```

Figure:- The above figure shows the installation process of Assetfinder tool.

```
(root@kali)-[~]
└─# assetfinder -subs-only test.com
test.com
safebrowsing.test.com
www.test.com
ww.test.com
wpad.cisco.test.com
0.test.com
193-108-112-0.test.com
195-133-55-0.test.com
payannameh1000.test.com
2000.test.com
87-248-130-100.test.com
87-248-131-100.test.com
213-209-151-100.test.com
87-248-153-100.test.com
195-133-55-100.test.com
87-248-155-100.test.com
195-238-127-100.test.com
soheil0100.test.com
offershop100.test.com
test100.test.com
mx100.test.com
200.test.com
87-248-130-200.test.com
87-248-131-200.test.com
213-209-151-200.test.com
193-108-112-200.test.com
87-248-152-200.test.com
87-248-143-200.test.com
195-133-55-200.test.com
master3200.test.com
test300.test.com
30002400.test.com
```

Figure:- The above figure shows the result of assetfinder running on test.com

Reference:-

1. <https://github.com/tomnomnom/assetfinder>
2. <https://www.hackerone.com/application-security/guide-subdomain-takeovers>