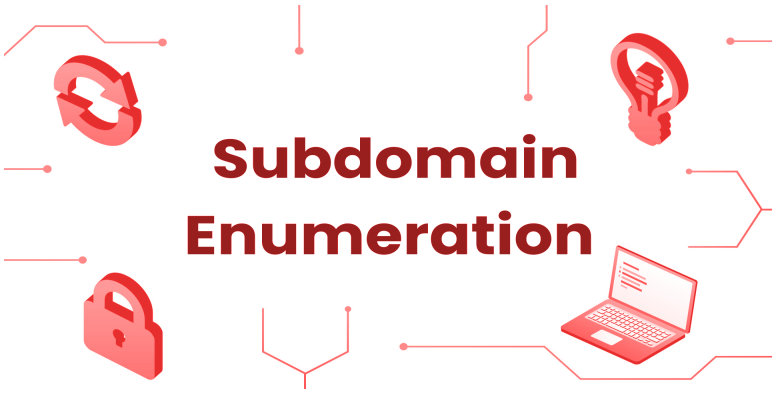
Ethical Hacking/Penetration Testing & Bug Bounty Hunting v2

❖ 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

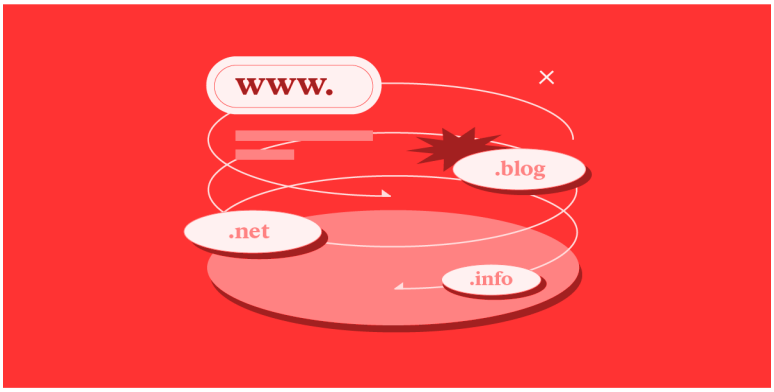


Introduction:

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

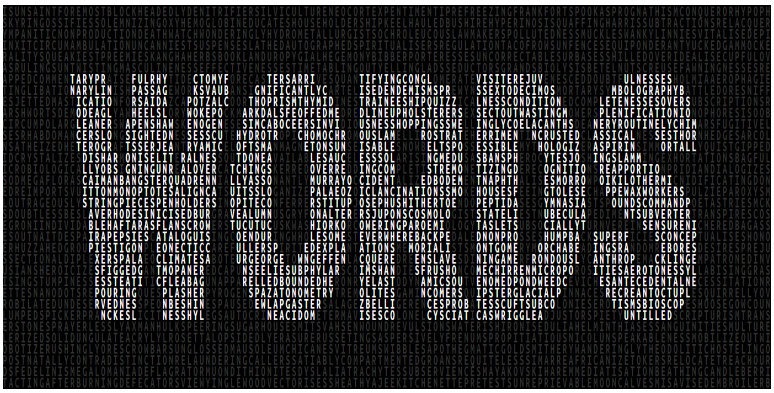
Exploring Certificate Transparency Logs can provide insights into recently issued certificates, exposing subdomains that may not be evident through traditional enumeration methods.

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

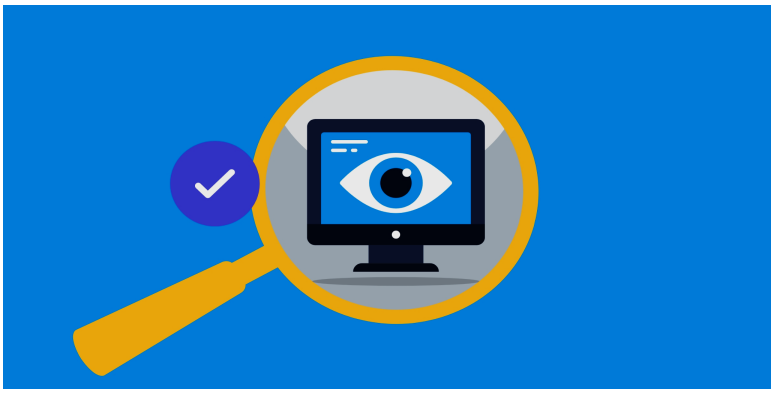


Creating and utilizing a well-crafted wordlist is essential for a thorough subdomain enumeration. Including industry-specific terms and variations increases the chances of discovering hidden subdomains.

Active Reconnaissance Techniques

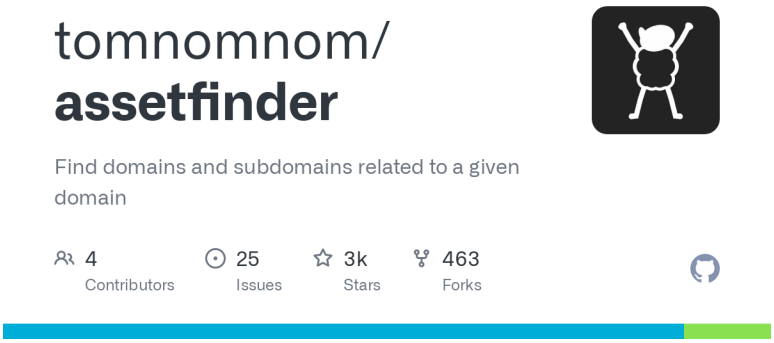
Interacting with web applications and services actively can reveal subdomains that are only accessible through specific actions. This approach involves analyzing responses to requests and understanding the application's structure.

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



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 libblockd
  libblockdev2 libgdal32 libgeos3.11.1 libgumbo1 libgupnp-igd-1.0-4 libjim0.81 libmongocrypt0 libmujs2 libncurs
  libtinfo5 libwebsockets17 libyara9 linux-image-6.1.0-kali5-amd64 python3-cryptography37 python3-flask-securit
  python3-pytz-deprecation-shim python3-rx python3-texttable
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