Amass: A beginner’s guide for reconnaissance

In this article we will see how to use a tool named “amass” which is used for reconnaissance when doing website penetration testing or bug bounty. This tool is used to list sub-domains related to the target domain.

This is not a complete guide for the amass tool, but instead this is an introduction to the reconnaissance using amass. Amass github: https://github.com/OWASP/Amass

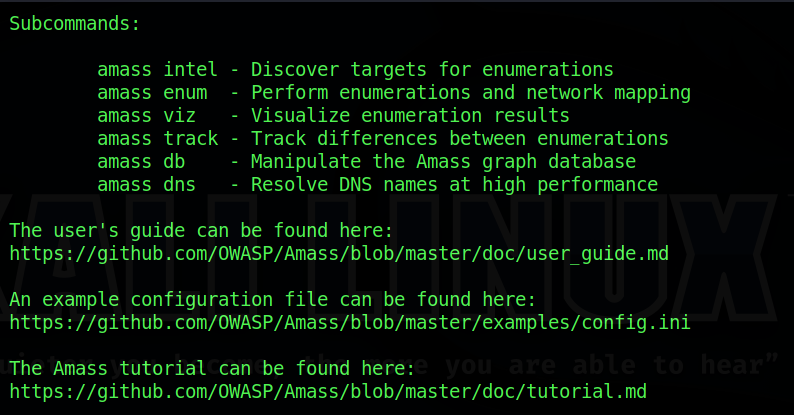
**Introduction**

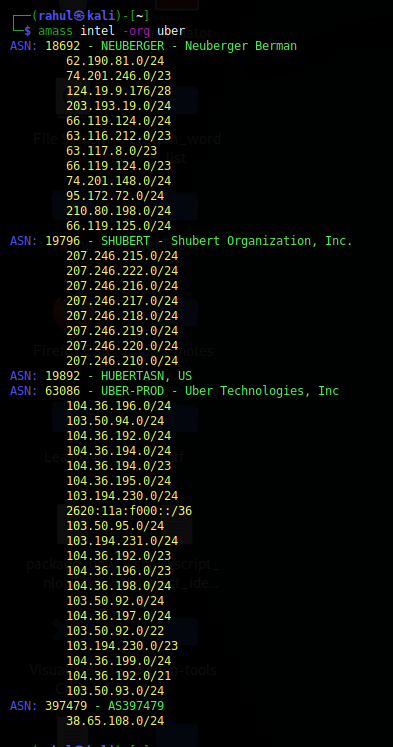
* Amass is an open source network mapping and attack surface discovery tool that uses information gathering and other techniques such as active reconnaissance and external asset discovery to scrap all the available data.
* In order to accomplish this, it uses its own internal machinery and it also integrates smoothly with different external services to increase its results, efficiency and power.
* This tool maintains a strong focus on DNS, HTTP and SSL/TLS data discovering and scrapping.

**Installation**

* To install this tool you can use the official package manager of kali Linux, and use this command “sudo apt-get install amass”
* And if you are on Mac than use this command “brew install amass”

**Usage**

* When using a new tool it is always a good habit to see the help menu or man page for that tool. So to get the help menu of this tool use this command “amass -help” or “amass -h”
* Now at the end of the help menu you can see that there is a list of subcommand, with the help of these subcommand we can perform many different operations, I am not going in detail of every command rather I will just explain the most important and used subcommands of amass. 
* The main two subcommand that are used most are “amass intel” and “amass enum”.
* To get the help for these subcommand you can use this command “amass intel -help”
* “amass intel” it collects the intelligence on the target in order to determine the starting point. It give us various details such as AS number, whois record of the website. We can find AS number using amass like this “amass intel –org uber”



* An Autonomous System (AS) is a group of IP networks run by one or more network operators with a single, clearly defined routing policy. When exchanging exterior routing information, each AS is identified by a unique number: the Autonomous System Number (ASN). We can easily find AS number of website from this website <https://bgp.he.net/>
* Now “amass enum” performs enumeration and mapping your target to determine possible attack avenues.
* We can use “amass enum” for finding sub-domains of a website. For that we can use a command like this “amass enum –d uber.com –o /root/uber.txt”
* In the above command “-d” is used to determine the domain name, “-o” is to determine the output file where we want to save our results. There are many more options available you can see that by using the help command like this “amass enum -help”.

So this was all about the basics of amass. Hop you like it and learned something new from it.

If you have any doubt, question, quires related to this topic or just want to share something with me, than please feel free to contact me.