**DRACNMAP SCANNING TOOL**



GitHub is a great source of software. It is based on a library or version control system, providing developers an outlet for open source software and related updates. I recently took a look at Dracnmap, which can be found at:

<https://github.com/Screetsec/Dracnmap>

Dracnmap is an open source program primarily used to exploit a network by gathering information with the

help of Nmap (which stands for network mapper). Nmap comes with lots of options through a command line structure, resulting in a utility that is very robust but somewhat difficult to follow for new users. Dracnmap is somewhat of a dashboard and is designed to provide the ability to perform fast scanning using the sc ript engine of Nmap. It enables the ability to more easily perform a variety of automatic scanning techniques by

leveraging advanced Nmap commands in the background.

Nmap scripts are extremely powerful and can detect a wide range of vulnerabilities. Professional penetration testers leverage the power and speed of Nmap to scan for common vulnerabilities using Nmap plug-ins rather than using more complex vulnerability scanning tools.

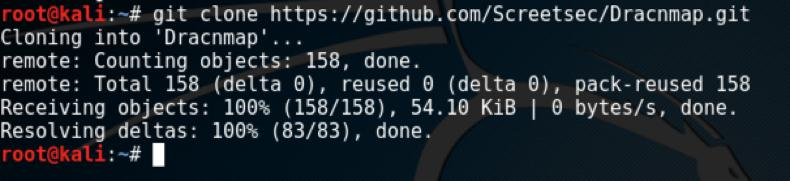
By the way…Dracos and Screetsec have an awesome [YouTube channel t](https://www.youtube.com/channel/UCpK9IXzLMfVFp9NUfDzxFfw)hat walks you through Dracnmap. I am not going to be able to really do any justice covering anything they already have on those channels. You will not be disappointed if you spend some time going through them. Not only is their tutorial great on Dracnmap, but check out their other tools and videos.

On another side note, check out TheFatRat for another method of getting around antivirus applications. Interesting stuff that, oddly enough, completely distracted me. Go figure.

**Getting Started**

The installation and opening of Dracnmap is relatively straight-forward, as always.

1. git clone <https://github.com/Screetsec/Dracnmap.git>

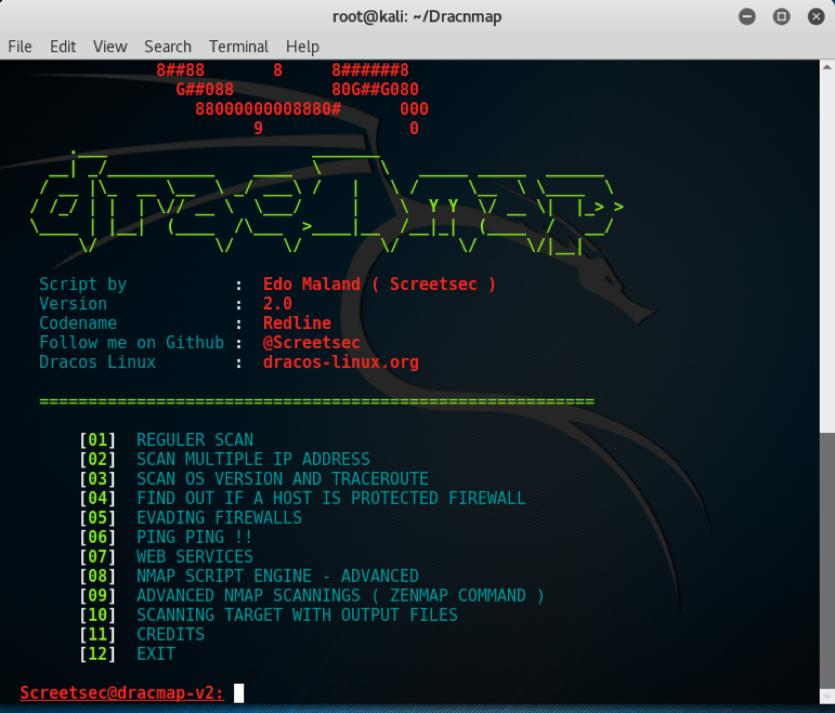


1. cd Dracnmap

2. chmod +x Dracnmap.sh



1. sudo ./Dracnmap.sh or sudo su ./Dracnmap.sh



As you play with Dracnmap (at least the way I am using it in the example below) you can see how it is more - or-less a front-end menu driven GUI for Nmap plugins.

One of the common scans I run with Dracnmap is to look for cross-site scripting vulnerabilities. This is a quick way for me to check to see if potential problems or vulnerabilities exist within Web application implementations. Here are the steps to run this type of scan:

1. Select option 7 for Web services

2. Select option 5 for Web base services

3. Enter target address (the system you want to scan)

4. View the results within the Nmap console that will appear

**Other Scanning Options with Dracnmap**

There some excellent scans built into Dracnmap. Some of my favorites include detecting Web application

firewalls, open relays, Web servers vulnerable to Sloworis DDoS attacks, enumerating users from an SMTP

server, SQL injection vulnerabilities, and brute force attacks with NSE scripts against various protocols and servers.

You can output scan results in different formats supported by Nmap, or use a XML export to import into other applications.

**Other Scanning Considerations with Dracnmap**

Nmap can be ‘noisy’, meaning it can be readily detected by many NGFWs and IPS systems, so please use Dracnmap sparingly. My friend (Keith) calls is ‘tripping over the garbage can lids’, which is pretty appropriate. Even though Nmap is a readily detected scanner, Dracnmap is a great way to get educated in

Nmap plug-ins and how to use them as you explore the power of Nmap.

**Credit Where Credit is Due**

I wanted to include the credits as listed in the Dracnmap app below:

########################################################################## Credits To

##########################################################################

Special thanks to:

Dracos Linux ( [www.dracos-linux.org](http://www.dracos-linux.org) ) Offensive Security for the awesome OS<http://www.offensive-security.com/> <http://www.kali.org/> <http://www.kitploit.com/> <http://www.linuxsec.org/>

My Friend for helpme ( Boy Suganda )

Big Thanks to : <http://www.github.com/>

*Have fun with Dracnmap, but, as always…..be careful out there!*