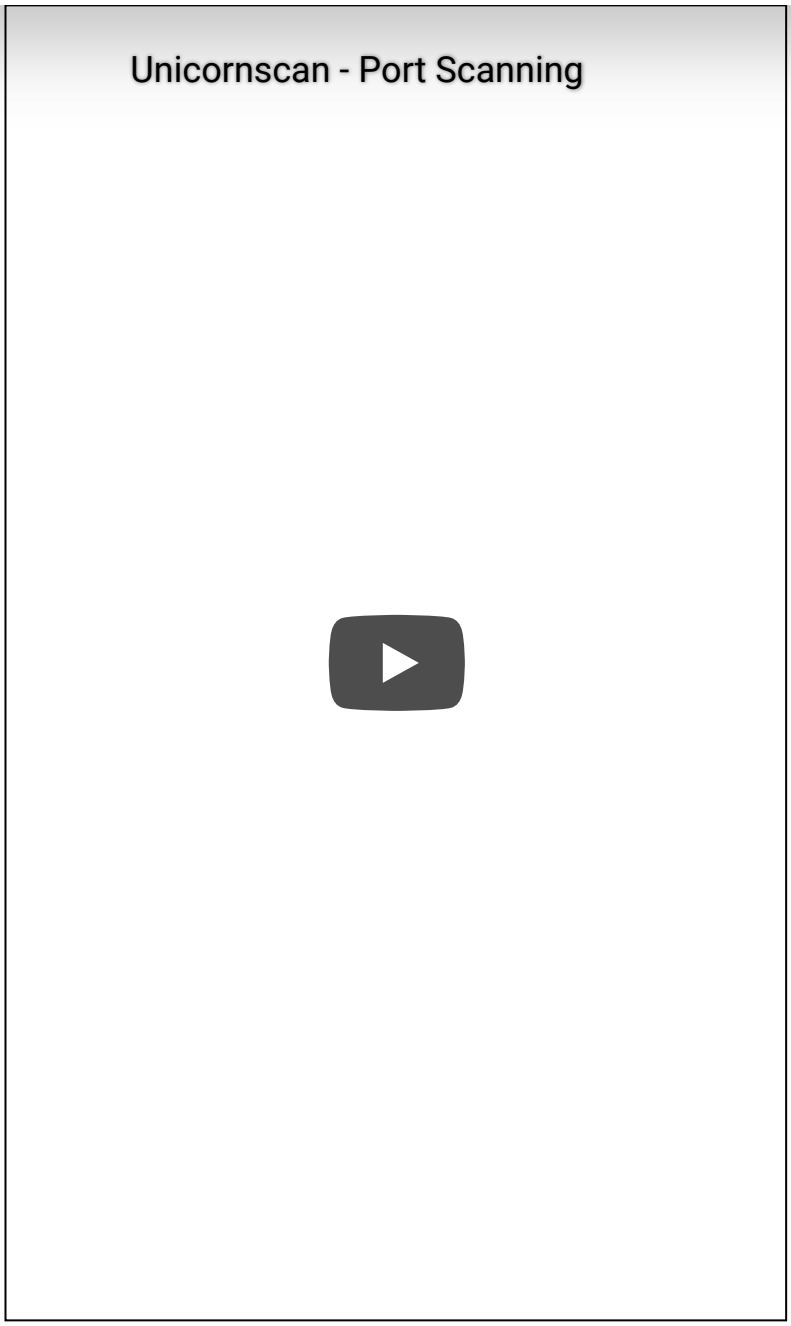
$HACKERSPLOIT _
PENETRATION TESTING - ETHICAL HACKING - LINUX

Unicornscan Port Scanning Tutorial



What is Unicornscan?

Unicornscan is a new information gathering and correlation engine built for and by members of the security research and testing communities. It was designed to provide an engine that is Scalable, Accurate, Flexible, and Efficient. You may be wondering, why not use

When using NMAP, packets can be traced back to you, and I'm here to make sure that doesn't happen.

- This can be used via your terminal, or a front-end user interface that is powered by the PostgreSQL database. *Just a bit of extra information!*
- Is this tool not convincing you that it's good? Well guess what, it has:
- Asynchronous stateless TCP scanning with all variations of TCP Flags.
- Asynchronous stateless TCP banner grabbing
- Asynchronous protocol-specific UDP Scanning (sending enough of a signature to elicit a response).
- Active and Passive remote OS, application, and component identification by analyzing responses.
- PCAP file logging and filtering.
- Relational database output.
- Custom module support.
- Customized data-set views.

How to use Unicornscan

This comes pre-installed into Kali.

Let's start off with the simple commands, to get the help menu, type in:

> *unicornscan –help*

First of all, as you can see there are various commands and we will be taking a look at a few of them. Let's start of with the interface name command. This is once again, something NMAP doesn't allow. This allows you to specify the interface name that you would like to use for performing a scan. For example, if you had ethernet and a wireless adapter, you can choose what adapter you would like to use in order to perform the scan. It may seem small, but TRUST ME, it is so convenient.

“

- *-v Is verbose output*

- *-i is an immediate mode*

Now let’s try protocol specific scanning

The command for this:

“ *unicornscan -v -I -mT [IP ADDRESS]*

- *This scan mode, tcp (syn) scan is default, U for UDP T for TCP `sf’ for TCP connect scan and A for ARP*

Now let’s a UDP scan:

“ *unicornscan -v -I -mT [IP ADDRESS]*

Let’s try scanning an entire network:

“ *unicornscan -r500 -mT -v -I [IP ADDRESS]/24*

- *-r500 tells you the rate of packets per second (total, not per host, and as you go higher it gets less accurate)*

Let's try specifying a port:

> *unicornscan -r500 -mT -v -I [IP ADDRESS]/24:22*

- *In this case, we are specifying the port. We are specifying port 22, the SSH port. You can choose any port you want*

Nmap equivalent scans for Unicornscan

> *unicornscan -mT -v -I [IP ADDRESS]*

Let's try performing an ACK scan:

> *unicornscan -mTsA -v -I [IP ADDRESS]*

- *The 's' and 'A' is for the ACK arguments*

Performing unique scans that NMAP offers: (an XMAS scan)

> *unicornscan -mTsFPU -v -I [IP ADDRESS]*

Where are the modules?

> *ls -lah /usr/lib/unicornscan/modules/*

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Website

Post Comment